

Details

Field Note #126. On "Contrarian Lemmings"

www.sandeepamesh.com

artwork created by this author

"bulls"

Lemmings



"bears"

Contrarian Lemmings

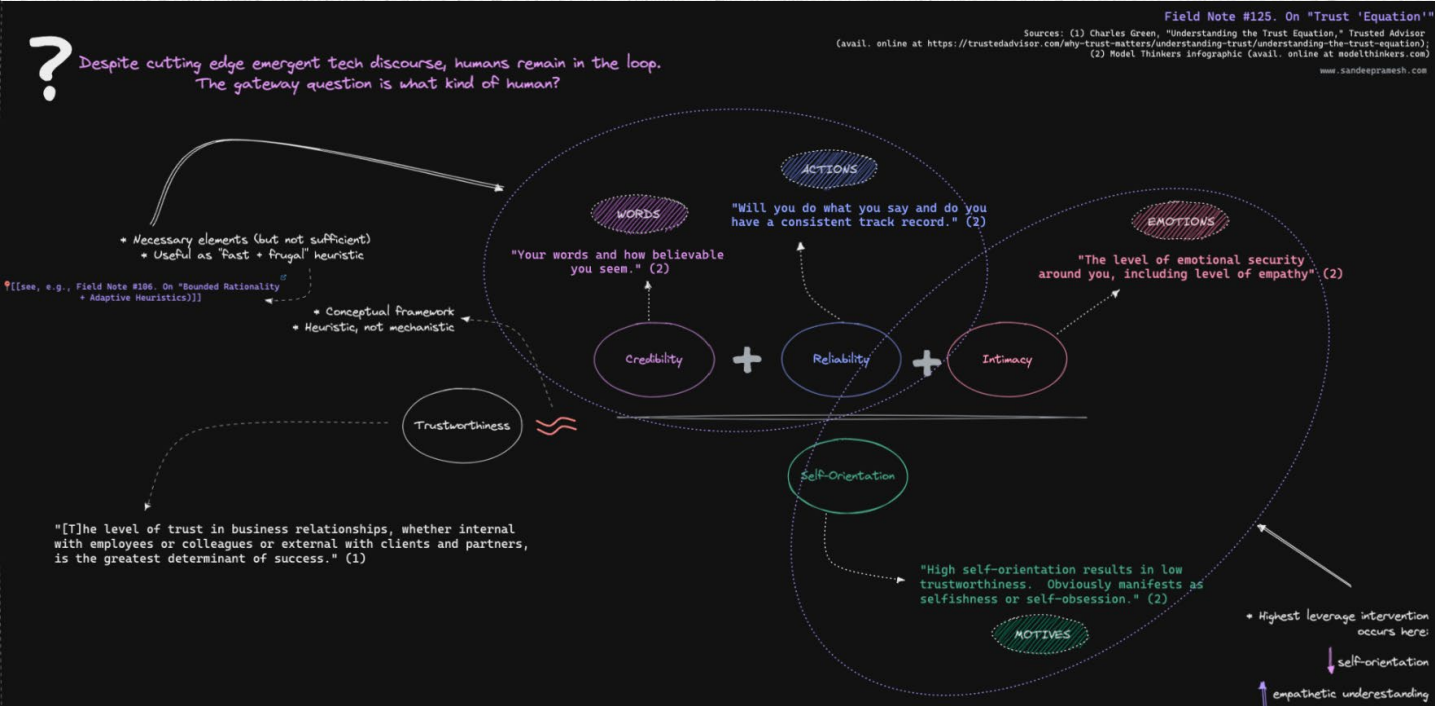


#fn

1. [FN 1 On Event-Driven Crypto](#)
2. [FN 2 On Cryptoeconomic Design](#)
3. [FN 3 On Info Smog](#)
4. [FN 4 On Evolving Towards a Fundamental Investment Framework for Crypto](#)
5. [FN 5 On Why You Probably Don't Need a Blockchain](#)
6. [FN 6 On Crypto Information Diets](#)
7. [FN 7 On Morphological Token Framework](#)
8. [FN 8 On Impossibility of Decentralization](#)
9. [FN 9 On Cryptography Basics](#)
10. [FN 10 On Amara's Law + Exponential](#)
11. [FN 11 On Dixon Decentralization](#)
12. [FN 12 On Placeholder Thesis circa 2017](#)
13. [FN 13 On Cowen & Tabarrok Textbook \(pt. 2\)](#)
14. [FN 14 On Intro to Smart Contracts](#)
15. [FN 15 On Metatransactions & User Experience](#)
16. [FN 16 On Knightian Risk, Uncertainty, Profit](#)
17. [FN 17 On Tail Risk x Crypto, or Toward a Hedged Crypto Venture Fund?](#)
18. [FN 18 On a Simplistic \(and Basic\) Justification of Tokens](#)
19. [FN 19 On Hazlitt's Economics in One Lesson](#)
20. [FN 20 On Chain Optionality](#)
21. [FN 21 On Non-Financial Applications of Blockchains](#)
22. [FN 22 On Heuristics, or Simplicity in face of Complexity](#)
23. [FN 23 On Decentralized Computing Stack](#)
24. [FN 24 On Thin Applications](#)
25. [FN 25 On Public Blockchain and Power to Root Users](#)
26. [FN 26 On 1N](#)
27. [FN 27 On Data Silos and the Blockchain Stack](#)
28. [FN 28 On Blockchain, Not Slow Database](#)
29. [FN 29 On Token as Killer App](#)
30. [FN 30 Toward a Modern Crypto Fund](#)
31. [FN 31 On Problems of Distributed Databases](#)
32. [FN 32 On Web 3 pre Buzzword, per Gavin Wood](#)
33. [FN 33 On Double Diamond and Forming Cloud](#)
34. [FN 34 On The Bell-Mason Framework \(An Intro\)](#)
35. [FN 35 On Web3 without the Hype \(p1\)](#)
36. [FN 36 On Quantum Investing](#)
37. [FN 37 On Fundamental Investment Framework, TradFi Ed.](#)
38. [FN 38 On Threshold Question](#)
39. [FN 39 On Web3 without Hype \(part 2\)](#)
40. [FN 40 On Framing the Threshold](#)
41. [FN 41 On Answering the Threshold Question](#)
42. [FN 42 On Blockchain Applicability Framework](#)
43. [FN 43 On DeAI](#)
44. [FN 44 On Investing Epistemology, Convergence + Divergence](#)
45. [FN 45 On Deep Learning Infrastructure Innovation](#)
46. [FN 46 On Benet Contextualizing Web3 in 2018](#)
47. [FN 47 On Federated Learning Précis](#)
48. [FN 48 On Foscett's Pyramid](#)
49. [FN 49 On Cypherpunk Hero](#)
50. [FN 50 On Cynefin and Complexity](#)
51. [FN 51 Deep On Computational Burden](#)
52. [FN 52 On Save AI, Save World](#)
53. [FN 53 On Multiple Compute Nodes and Data Level Privacy](#)
54. [FN 54 On Overcoming the Matthew Effect in Crypto](#)
55. [FN 55 On Intertemporal Investing Edge](#)
56. [FN 56 On Oracle Problem](#)
57. [FN 57 On Metaphor and Counter-Conventional Investing](#)
58. [FN 58 Mandelbrot's 10 Heresies of Finance](#)
59. [FN 59 On Toolkit Theory and Innovation Cycles](#)
60. [FN 60 On Main Web3 Challenges](#)
61. [FN 61 On Less Centralized Notes](#)
62. [FN 62 On Risk of Ruin Visualized](#)
63. [FN 63 On Gensyn Litepaper](#)
64. [FN 64 On AI and Compute, or Moore's Law on Roids](#)
65. [FN 65 On Raven Protocol Whitepaper](#)
66. [FN 66 On Trading Psychology & Money Management](#)
67. [FN 67 On DeFi History](#)
68. [FN 68 On Wisdom of Ed Thorp](#)
69. [FN 69 On Critical Reading & Investing](#)

70. [FN 70. On Decentralized Finance Foundations \(module 2\).](#)
71. [FN 71. On AI Snake Oil](#)
72. [FN 72. On Illusion of Explanatory Depth](#)
73. [FN 73. On Music and Trading](#)
74. [FN 74. On Problems DeFi Solves](#)
75. [FN 75. On Mapping Web3 Layers](#)
76. [FN 76. On \(San\)Deep System](#)
77. [FN 77. On DeFi Token Basics](#)
78. [FN 78. On Token Supply, Adjustment, and Swaps](#)
79. [FN 79. On Blockchain Concepts & Mechanisms](#)
80. [FN 80. On Lessons from Adaptive Market Theory](#)
81. [FN 81. On Virtual Machines and Related Terms](#)
82. [FN 82. On Dai](#)
83. [FN 83. On Klarman \(and Crypto?\)](#)
84. [FN 84. On Effectuation](#)
85. [FN 85. On Effectuation Deux](#)
86. [FN 86. On "Evaluating Start Up Leadership"](#)
87. [FN 87. On DataFi](#)
88. [FN 88. On DeFi Credit Con't](#)
89. [FN 89. On Polygon Lite](#)
90. [FN 90. On Poker and \(Crypto\) Investing](#)
91. [FN 91. On "Thus Spake Spitznagel, or Amor Fati"](#)
92. [FN 92. On Cynicism Pathology](#)
93. [FN 93. On Philosophy + Investing](#)
94. [FN 94. On Four Decision Making Phases](#)
95. [FN 95. On "Epistemic Arrogance, or Scandal of Prediction](#)
96. [FN 96. On "Chance"](#)
97. [FN 97. On "Metacrisis + Crypto"](#)
98. [FN 98. On Via Negativa or Voss + Camp Negotiation](#)
99. [FN 99. On "Venture Debt"](#)
100. [FN 100. On "Serendipity + Altamirage"](#)
101. [FN 101. On Metacrisis + Crypto \(part 2\).](#)
102. [FN 102. On Strategies for Turbulence](#)
103. [FN 103. On AGI and ASI Gloss](#)
104. [FN 104. On "Datafication"](#)
105. [FN 105. On "Tech - In Medias Res"](#)
106. [FN 106. On Bounded Rationality & Adaptive Heuristics](#)
107. [FN 107. On Non-Neutrality of Phone + Social](#)
108. [FN 108. On AI and WebN](#)
109. [FN 109. On Platform Logic](#)
110. [FN 110. On VC and Its Discontents](#)
111. [FN 111. On AI and Power](#)
112. [FN 112. On Levin + Weekend Contemplation](#)
113. [FN 113. On Seduction of Decentralization Rhetoric](#)
114. [FN 114. On Axes of Decentralization](#)
115. [FN 115. On "Fallen Angels"](#)
116. [FN 116. On Risk Creep + Risk Sweep](#)
117. [FN 117. On Decision Integrity](#)
118. [FN 118. On Not Just Panic at the Crypto](#)
119. [FN 119. On \(Self\) Trust\(less\).](#)
120. [FN 120. On "Market Wu Wei"](#)
121. [FN 121. "Pin to Wall"](#)
122. [FN 122. "Pin to Wall 2"](#)
123. [FN 123. On Leverage Points + Edge](#)
124. [FN 124. On Parasite + The Asymmetric Operator 1](#)
125. [FN 125. On Trust Equation](#)

Details



Cary Wolfe, "Bring the Noise: The Parasite and the Multiple Genealogies of Posthumanism," introduction to
Michel Serres, The Parasite (trans. L. Schehr) (1982, English), pp. xi-xxviii.

Details

Field Note #124. On "Parasite + The Asymmetric Operator"

Source: Cary Wolfe, "Bring the Noise: The Parasite and the Multiple Genealogies of Posthumanism," introduction to Michel Serres, The Parasite (trans. L. Schehr) (1982, English), pp. xi-xxviii. www.sandeepamesh.com

Praxis of Thought. Instantiate It.

"Serres is not content to say that we must rethink certain notions, redefine certain concepts; he doesn't 'say' it, doesn't argue for it, he just 'does' it, and in so doing, he sets out new coordinates for the 'praxis of thinking.'" (p. xiv)

Analytical but
Experimental

? Can we have an investment approach not in the pre-established key? What is it?

"Can we rewrite a system," Serres asks, "not in the key of preestablished harmony," but rather as "the book of differences, noise, and disorder?" After all, "the difference is part of the thing itself, and perhaps it even produces the thing. Maybe the radical origin of things is really that difference." (p. xiv)

"Serres's writing... is not analytical but experimental; not cumulative and aggregative but discursive; not linear but meandering, doubling back on itself to remind itself of stones left unturned, details too readily smoothed over, conclusions too well-varnished. And then we're plunged back into the welter, back into the complexity of it all. Back into the sea foam of noise." (p. xiii)

Innovation as Undetermined, Unstable

"The hand is no longer a hand when it has taken hold of the hammer, it is the hammer itself... The hand and thought, like one's tongue, disappear in their determinations." Thus, Serres asserts, "inventive thinking is unstable, it is undetermined, it is undifferentiated, it is as little singular in its function as is our hand." (p. xxx)

Noise as Creative / Generative.

- noise is not singularly 'bad'
- noise is embedded in the signal
- cannot entirely separate the duality noise/signal

"For Serres... noise is 'productive' and creative: 'noise,' through its presence and absence, the intermittence of the signal, produces the new system" (p. xiii).
Quoting Bateson: "All that is not information, not redundancy, not form and not restraints—is noise, the only possible source of 'new' patterns."

So-called 'noise' is dependent on perspective of the observer. 'Noise...for whom?'

"As he puts it, 'a given noise, the sound of the conversation in the room, is a noise for the conversation I am having with my interlocutor on the phone, but it is a message for my guests. And for them, my conversation is a noise for their own. It all depends on the position of the observer.'" (p. xiii)

More we embed in a system, the more we mistakenly over-prioritize signal over noise.

"He represses the parasites," Serres writes, "in order to send or receive communications better and to make them circulate in a distinct and workable fashion... Whoever belongs to the system perceives noises less and represses them more, the more he is a functioning part of the system." And he does so, from Luhmann's point of view, because noise, environmental complexity, is an overwhelming adaptive and evolutionary 'problem' for systems that wish to continue their autopoiesis." (p. xiii)

First Act: collapsing the wave function.

But, ethically, thoughtfully, how to collapse it?

"In a way, this does nothing more than acknowledge Bateson's well-known appropriation of Kant when he notes that the most elementary act is 'the selection of a fact' (a selection based on a given map or code or schema) from an object that is actually constituted by 'an infinite number of potential facts.'" (p. xxiii)

How do we act otherwise?
How do we stop this compulsion with the 'singular' and the artificially 'tidy' narratives?
And, pragmatically in the investment domain, how might we instantiate this alternative?

critique of quest for contained system as ignorance

"When we do not understand, when we defer our knowledge to a later date, when the thing is too complex for the means at hand, when we put everything in a temporary black box, we prejudice the existence of a system. When we can finally open the box, we see that it works like a space of transformation. The only systems, instances, and substances come from our lack of knowledge. The system is nonknowledge. The other side of nonknowledge. One side of nonknowledge is chaos; the other, system. Knowledge forms a bridge between the two banks. Knowledge as such is a space of transformation." (p. xxiv., qtd. Serres)

nonknowledge
chaos
system
knowledge

The Parasite: Play Position, Not Content.

"The producer plays the contents, the parasite, the position. The one who plays the position will always beat the one who plays the contents. The latter is simple and naive; the former is complex and mediatized... To play the position or to play the location is to dominate the relation. It is to have a relation only with the relation itself. Never with the stations from which it comes, to which it goes, and by which it passes. Never to the things as such and, undoubtedly, never to subjects as such... And that is the meaning of the prefix 'para-' in the word 'parasite': it is on the side, next to, shifted; it is not on the thing, but on its relation." (qtd. Serres, p. xxi)

add meaning in French

static

biological

Key Term: "Quasi-object"

social

The Parasite

The Observer as the Asymmetric Operator

"The observer always makes less noise than the observed. He is thus unobservable by the observed. That is why he troubles and is never troubled, that is why he is an asymmetric operator... He is in the position of the subject." (qtd. Serres, p. xxiv)

Seduction of Unitary

"We want a principle, a system, an integration, and we want elements, atoms, numbers. We want them, and we make them. A single God, and identifiable individuals." (p. xii, qtd. Serres in Genesis)

critique of single unit

+ the unit is FRACTAL

"We've never hit upon truly atomic, multiple, indivisible terms that were not themselves, once again, composite... The bottom always falls out of the quest for the elementary. The irreducibly individual recedes like the horizon, as our analysis advances." (Id. at xii, qtd. Serres in Genesis)

the milieu
liminal
transformation space
Noise
b/t system and environ.

My Breadcrumbs:
• Gregory Bateson, Cybernetic Explanation (1967) (quoted)
• Niklas Luhmann, Social Systems (quoted)
• LaFontaine (referenced)
• Agamben, Homo Sacer (not referenced)
• Nagarjuna (not referenced)
• Derrida, Gift of Death (referenced)
• Deleuze (referenced)

Details

On Main Question Explored

- "[H]ow do we change the structure of systems to produce more of what we want and less of that which is undesirable?"
 - This necessarily involves subjective value judgments in the design layer of innovation and product build. When this question is skirted, footnoted, or outright ignored, avoidable and highly impactful negative externalities (that are less subjective / for which greater consensus exists; e.g., survival, agency, anti-dystopianism) are destined.

On Lore of Leverage Points

- Given the embedded nature of leverage in our collective imaginary, we can take this as a caution to resist the temptation to generalize complex systems; to resist the temptation to find recipes.
 - "The idea of leverage points is not unique to systems analysis--it's embedded in legend: the silver bullet; the trintab; the miracle cure; the secret passage; the magic password; the single hero who turns the tide of history; the nearly effortless way to cut through or leap over huge obstacles. We not only want to believe that there are leverage points, we want to know where they are and how to get our hands on them. Leverage points are points of power." (p. 145)

On Ranking Effectiveness of Types of Leverage (from most powerful to least powerful)

- All leverage points are not created equal. Thus, the question explored is what type of leverage should we be on the look out for when we are interacting with complex, difficult-to-predict (indeed, in many cases, unpredictable as such) systems?

1. Transcend Paradigms.

- "There is yet one leverage point that is even higher than changing a paradigm. That is to keep oneself unattached in the arena of paradigms, to stay flexible, to realize that *no* paradigm is "true," that every one, including the one that sweetly shapes your own worldview, is a tremendously limited understanding of an immense and amazing universe that is far beyond human comprehension. It is to "get" at a gut level the paradigm that there are paradigms, and to see that that itself is a paradigm, and to regard that whole realization as devastatingly funny." (p. 164)
- "In the end, it seems that mastery has less to do with pushing leverage points than it does with strategically, profoundly, madly, letting go and dancing with the system." (p. 165)

2. Change the Paradigm.

- Invoking Kuhn and Jay Forrester, Meadows defines paradigm as a "shared idea in the minds of society, the big unstated assumptions...or set of beliefs about how the world works." (p. 162-63)
- Change of paradigms is high leverage because it can be highly event-driven (at the individual or even societal levels): "[T]here's nothing physical or expensive or even slow in the process of paradigm change. In a single individual it can happen in a millisecond. All it takes is a click in the mind, a falling of scales from the eyes, a new way of seeing. Whole societies are another matter--they resist challenges to their paradigms harder than they resist anything else." (p. 163-64)
- Paradigm change occurs how? By starting with critique. "You keep pointing at the anomalies and failures in the old paradigm. You keep speaking and acting, loudly and with assurance, from the new one. You insert people with the new paradigm in places of public visibility and power. You don't waste time with reactionaries; rather, you work with active change agents and with the vast middle ground of people who are open-minded." (p. 163-64)

3. Change the Goals within the System.

- We must ask the point of the game we are playing, otherwise we are not tuned to the goals of the system. As such, we function--even "successfully"--as highly ignorant puppets, unaware. With awareness of system goal, we can then agitate for change.

4. Embrace Multidisciplinarity: Let Go & Observe Self-Organization.

- "Insistence on a single culture shuts down learning and cuts back resilience. Any system, biological, economic, or social, that gets so encrusted that it cannot self-evolve, a system that systematically scorns experimentation and wipes out the raw material of innovation, is doomed over the long term on this highly variable planet. The intervention point here is obvious, but unpopular. Encouraging variability and experimentation and diversity means "losing control." Let a thousand flowers bloom and *anything* could happen! Who wants that? Let's play it safe and push this lever in the wrong direction by wiping out biological, cultural, social, and market diversity!" (p. 160-61)

5. Change Rules.

- Power to change rules is impressive, but these are not high leverage points in the long run because they can set off maladaptive loops: "It's a recipe for unleashing 'success to the successful' loops, until they generate enormous accumulations of power and huge centralized planning systems that will destroy themselves." (p. 159)

Details

6. Augment Info Flows.

- This is a popular lever, particularly given the tech industry's reinterpretation of a real estate mantra; from "location, location, location" to "data, data, data." "Adding or restoring information can be a powerful intervention, usually much easier and cheaper than rebuilding physical infrastructure," but begs the question of informational quality and validity of goals served within the existing system. The system boundaries don't really change; they become more refined (perhaps, or obscured if the data is low-quality, misused, or useless) (p. 157)

7. Reinforcing Feedbacks.

- Popular in VC-land with far too many books and writings on "fly wheel" and such, "[r]einforcing feedback loops are sources of growth, explosion, erosion, and collapse in systems. A system with an unchecked reinforcing loop ultimately will destroy itself. That's why there are so few of them. Usually a balancing loop will kick in sooner or later." (p. 155)

8. Strengthen Balancing Loops.

- Anti-manipulation and a push toward transparency.
- "Companies and governments are fatally attracted to the price leverage point, but too often determinedly push it in the wrong direction with subsidies, taxes, and other forms of confusion. These modifications weaken the feedback power of market signals by twisting information in their favor. The *real* leverage here is to keep them from doing it." (p. 154)

9. Create Delays.

- **Defined.** "A delay in a feedback process is critical *relative to rates of change in the stocks that the feedback loop is trying to control.
- "Delays that are too short cause overreaction, "chasing your tail," oscillations amplified by the jumpiness of the response. Delays that are too long cause damped, sustained, or exploding oscillations, depending on how much too long. Overlong delays in a system with a threshold, a danger point, a range past which irreversible damage can occur, cause overshoot and collapse." (p. 152)
- **Not Much To Do.** "I would list delay length as a high leverage point, except for the fact that delays are not often easily changeable. Things take as long as they take." (p. 152)
- **Slower > Faster.** "There's more leverage in slowing the system down so technologies and prices can keep up with it, than there is in wishing the delays would go away." (p. 152)
 - Cf. Peter Thiel's view that this forced slowing down risks totalitarianism (related to his call for a return to classical liberalism). But the totalitarian risk is a function of how the delays occur.

10. Stock and Flow / Physical Structures

- **Weak point of leverage.** "The leverage point is in the proper design in the first place. After the structure is built, the leverage is in understanding its limitations and bottlenecks, using it with maximum efficiency, and refraining from fluctuations or expansions that strain its capacity." (p. 151)

11. Buffers

- **Low leverage** because these buffers are "usually physical entities, not easy to change." (p. 150)
- **Query: non-physical, informational buffers? Redundancy as a means to ensure system survival?**

12. Parameter Changes.

- **Weakest point of intervention.** "It's not that parameters aren't important--they can be, especially in the short term and to the individual who's standing directly in the flow. People care deeply about such variables as taxes and the minimum wage, and so fight fierce battles over them. But changing these variables *rarely changes the behavior of the national economy system*." (p. 148)
- "Parameters become leverage points when they kick off one of the items higher on the list [above]. Interest rates, for example, or birth rates, control the gains around reinforcing feedback loops." (p. 149)
 - **Also, systems tend to stay away from critical parameter points:** "These kinds of critical numbers are not nearly as common as people seem to think they are. Most systems have evolved or are designed to stay far out of range of critical parameters. Mostly, the numbers are not worth the sweat put into them." (p. 149)

Details

A Gloss.

In my experiences from the "rarified" hedge fund world, the insistence upon evaluating downside risk was axiomatic. Words and phrases like margin of safety, protection, bidirectional (long/short), hedge, reflexivity, tail risk, edge (not social network, not proprietary flow), and non-cosmetic diversification were yawn-inducing because they were so obvious. Whether or not executed or calibrated well is another issue. The yawn can transform into a snore, leaving many asleep at the switch. In my experiences in early stage venture, including liquid & illiquid crypto, the overwhelming tendency observed was an anchoring to the upside (or a paying of lip service to risk mitigation). Conversations with venture investors (counterparts to the "hedgies") have tended to congeal around words and phrases like belief, vision, Midas, TAM, open-ended growth, "penetration is only 1% today," inevitability, double/triple/quadruple down, and escape velocity. What seems clear is that survival is a precondition to success. To realize the wondrous convexity of a high octane asset class (e.g., early stage venture, crypto, etc.) with a wide probability space, the axiom of axioms is that you must be financially (and otherwise) alive.

A Sketch.

Compounding is a wonder of the world...

Field Note #122
sandeepramesh.com

additive $1 + 0 = 1$
multiplicative ruin $1 \times 0 = 0$

... provided you're alive to witness it.

♦ For details, see Field Note #17. On "Tail Risk x Crypto"
<https://www.sandeepramesh.com/Field-note-62/>

Details

Distillation of:

Field Note 62. On "Risk of Ruin Visualized"

A useful reminder not just for crypto investors.

Especially useful for professional investors responsible for any amount of OPM.



Details

On Self-Investigation around Loss

- "I can anticipate some of the first questions you want to ask: 1. What do I have to do to win consistently? 2. Why do I lose? The most likely problem is that you are lost. You are using the wrong logic maps. You are using what you have been taught to use or what has worked for you in the past in business and/or a profession." (p. xii)
- "There is a Holy Grail...It is simple and easy, and you only have to remember five simple words: Want what the market wants....It is the number one commandment of trading, and if you abide by it you will never have to seek help elsewhere." (p. xiii)

On Content vs. Process

- "I have come to the conclusion that most traders...are primarily concerned with content as opposed to process....This is not necessarily bad; it just doesn't have a great payoff. We traders do it with each other when we ask:
 - How much did you make this month?
 - Did you go long the gold?
 - What kind of car do you drive?
 - Will you show me your P&L statements?
 - Can you give me someone who is using your approach profitably?
 - Did you know that this market is heavily oversold?

All the above examples center on content rather than process....[T]he primary difference between winners and losers is whether they focus on content or process." (p. 3)

Process of Wanting What the Market Wants

- The key to dancing well--and profiting in the market--is an ability to relax and simply go with the flow. That is what this book is about--*getting with the process;* letting go and going with the flow." (p. 3)
- On the standard torturous engagement with markets: "Even when we are winning, there is an undercurrent of fear that the next trade will probably be a loser. We exhaust ourselves as we try to control the present and the future while our minds futilely search for ways to recreate the past." (p. 4)
- "The market is where it is because that is where it is supposed to be, and it is supposed to be there because that is where it is....Once you grasp this concept, you will: 1. Know more about the market than 95 percent of those who have money invested in it. 2. You will have started down a yellow brick road to more profits." (p. 10)
 - What happens when you confront the Wizard?

On a Different Relationship with the Market

- On the market as a teacher: "It is also simple because the market is a master teacher. It will always tell you exactly what to do and when to do it. If you mess up, it will tell you exactly where you went wrong and what you should have done instead. As one of the greatest teachers in the world, the market is always willing to be there for you and to show you exactly how to act." (p. 11)"
- Let go as not a mere neo-spiritual popularized mantra but as a requirement to successful engagement with the markets: "We don't enjoy the miracle of our children's growth if we worry about how they will turn out. We don't enjoy maturing if we are worrying about what malady will take us from this life. We lose the freedom to soar the comes from enjoying the vast riches that life and the market are offering us in the here and now. In trading, if you set your heart on a certain trade result, you enter into a state of rigidity. On the other hand, if you sent your heart free, you enter a state of flow." (p. 11)
- "Once you decide and put on a trade, let it grow, mature, and ripen. Don't keep digging up the seeds....[A]sk yourself this simple question: Do I care which way the market moves? If you care, you are addicted. If you honestly don't care, you are trading well and you *want what the market wants.* Any time you care, you are wanting what *you* want--not what the market wants. The market is neutral. It doesn't know or even care what you want." (p. 11-12)
- "To sum, the primary reason for trading is the most important reason for doing anything: to find out who you are. That perspective makes all the difference....Trading is a self-discovery process and a very personal experience." (p. 13-14)
- On echo of wu-wei: "As a trader, you always know when you are trying to go against the path of least resistance. Tension immediately builds up in your body and mind. If you are tense about trading, you are not 'floating down the river.' Once you learn to determine the underlying structure of a market, you can make peace with the behavior of the market and simply 'float like a butterfly, sting like a bee.' (p. 29)

Details

On "Neighborhoods without Neighbors"

- "In a world of risky stranger, it is difficult to trust. Indeed, the fear of strangers and of risks is proportional to the decline of trust. Increasingly, relationships between people, even those who live in the same neighborhood or community, are characterized by a lack of clarity about the expected form of behavior." (p. 127)
 - Most attention--visible clearly in the field of cryptoeconomics--is placed on coordination of collective behavior through economic incentivizes. However, it is clear that this is woefully insufficient to establish clarity around expected behaviors.
- "One of the factors contributing to the growth in the number and variety of strangers has been the increasing lack of clarity of the terms on which people relate to each other. According to many commentators, such lack of clarity has led to the weakening of trust, which in turn has had profoundly destructive consequences for society." (p. 128)

On Expertise

- Irony that we are more dependent on science in a technological era but more mistrustful of scientific expertise.
 - "One of the ironies of our times is that while society is more dependent on science and technology than ever before, it is also more suspicious of their consequences." (p. 131)
 - "Some argue that the growing specialization of expertise contributes to the growth of unintended consequences. One of these consequences is the fragmentation of expert knowledge, which in turn makes it difficult for people to have access to reliable knowledge....Others argue that with the tremendous increase in information, society becomes overloaded with the facts[,] and people inevitably find it difficult to know what to believe." (p. 131)
- Rise of a new type of "specialist" taking advantage of information vacuums, uncertainties, and anxieties:
 - "The past two decades have seen the consolidation of a distinct contemporary form of expertise. It is an expertise that is characteristic of a society that lacks confidence about its future direction. This new expertise flourishes on uncertainty and on the lack of clarity in many of the basic relations between people. The new expertise preaches the messages that no one should be expected to cope with the uncertainties of life and that everyone is entitled to benefit from the skills of professional advisers. In the past, the provision of such advice was the monopoly of religious figures. Today, advice and guidance has been transformed into an expertise that is highly specialized and institutionalized." (p. 133)

On Professionalization of Everyday Life

- "The weakening of taken-for-granted relations and of trust is clearly paralleled by the professionalization of everyday life. The professionalization of everyday life has undermined routine relations and has flourished on account of the weakening of fundamental human bonds." (p. 134)
 - The extreme of this trend seems to be continuing as each part of our life is increasingly characterized by a reflexive deferral to outside expertise for otherwise routine activities.
- "The transformation of parenting from a routine expectation of adulthood to a skill indicates the low estimation in which people are seen. What humanity has coped with since the beginning of time now requires the certification of experts." (p. 134)
- The deferral to expertise is complicated and requires discernment as to where expertise is needed and not needed as well as the negative effects of expertise in areas where it is deemed warranted. Furedi, in a somewhat incendiary manner, claims:
 - "Although such experts always claim to 'empower' their clients, their every action has the effect of reinforcing people's lack of confidence in themselves. Professional helpers are rarely aware of how their 'helping' contradicts their claim to empower." (p. 136)

Erosion of Self and Social (both)

- On diminished subject & agency. "The incompetence of ordinary people is the fundamental premise for professional intervention in personal life." (p. 136)
 - "The erosion of trust can best be interpreted as the decline of trust in ourselves. This weakening of self-belief and the idea that we are capable of managing elementary relations between people has created a demand for experts. The growth of such expertise is proportional to the decline of belief in the problem-solving skills of people." (p. 137)
- The degradation of the social (physical, psychological, etc.) has meant that the "confidence that collective identity generated in the past was dissipated. Instead, individuals came to experience circumstances as forces beyond their control. Individuation without a parallel process of reintegration into some new social network can contribute to the creation of an atmosphere of mistrust....Where once neighbors and colleagues might have been seen as friends and allies, today they are more likely to be perceived as competitors and as potential threats." (p. 141)

Details

On Inadequacy of Current Understanding of Panic

- Panic is typically treated as a specific condition tied to a specific occurrence, instead of recognizing its broader underlying structure.
 - Panic defined as 'sudden and excessive feeling of alarm or fear' but "virtually no attempt to compare the different types of panics to see whether they are part of any wider pattern. Instead, analyses of specific panics treat their causes as separate and unconnected events." (p. 45)
- Reporting on panics tends to be cherry-picked.
 - "Authors are clearly selective about which responses are treated as panics and which are not. Consequently, some intense anxieties and fears are interpreted as panic-like, while others are not. Otherwise critical social scientists can recognize some manifestations of panic but not others. This double standard often corresponds to the writers' social, cultural and political outlook." (p. 46)

On Role of Media

- The well-established and well-known critique of media:
 - "The media play an important role in shaping society's perception of risk. Studies have shown that the media's emphasis on certain crimes or diseases leads the public to acquire a heightened sense of danger in relation to them." (p. 51)
 - This is obvious in today's world, but the same effect may well be transpiring in more distributed media, not just traditional, centralized media. See, e.g., the algorithmic channeling of information on social platforms and the rise of the "newsletter industrial complex."
- Media amplifies or attenuates, but does not create the risk perceptions.
 - "[I]t is important to remember that the media amplify or attenuate but do not cause society's sense of risk." (p. 53)
- Furedi's view is based on his observation of a pre-existing negative bias in people that forms the basis for media's amplification / attenuation function.
 - "There exists a disposition towards the expectation of adverse outcomes, which is then engaged by the mass media. The result of this engagement is media which are continually warning of some danger. But the media's preoccupation with risk is a symptom of the problem and not its cause. It is unlikely that an otherwise placid and content public is influenced into a permanent state of panic through media." (p. 53)

On Risk Awareness

- Increase in scientific understanding / increase in knowledge does not necessarily imply an increase in panic orientation toward risk.
 - "The association between scientific advance and the parallel growth in risk awareness is, in fact, far from self-evident. The assumption of an automatic growth in risk awareness alongside the development of knowledge ignores the social influences that shape human consciousness. In principle, the advance of knowledge does not necessarily lead to anxiety about hazards. In some situations it can lead to a high degree of confidence." (p. 54)
- Don't conflate risk and danger.
 - "[B]ut the awareness of risk should not be confused with real danger. To do so would be to flatter our disposition to panic and overreact with the claim of new insight and awareness." (p. 54)

Caution Re: Ex-Risk / Catastrophe Risk Awareness

- Furedi does not critique the existence of such risks, but calls us to interrogate societal disposition toward fearing such risks outside of the technological domain (i.e., the predisposition that pre-dated tech-induced exponential risk).
 - "Another variant of technical explanations of risk consciousness is to link it to the dangerous consequences of accelerated technological development.... As with all technical explanations of risk, that of Luhman does not address why society is also disposed towards fearing dangers in spheres that lie outside the domain of technology. Unfortunately, this emphasis on the consequences of technological developments recurs in many of the influential explanations of the subject." (p. 55)



Details

- The key question is about how we select problems to focus on.
 - "[T]he issue at stake is not whether perceptions of risk are real or not, but what is the basis for such responses. It is not particularly fruitful to counterpose the real to the unreal. A 'real' hazard like industrial waste can be seen as acceptable in one situation but interpreted as a deadly threat in another. The question worth investigating is how society goes about selecting its 'problems.' The focus on the process of problematization would raise the most significant question of all: why is there, today, such an increase in the range of experiences that are problematized?" (p. 59)
- Risk fluidity.
 - "[T]he very definition of something as a risk is bound up with changing relations and perceptions within society. That is why the development of risk consciousness has both a historical and social context." (p. 59)
 - However, beware of common misinterpretations of such statements, often configured as a broad critique of 'postmodernism' as a vehicle for perpetual 'indeterminacy.'

Against Implicit Disempowering Agents of Positive Change

- A view over-indexed to risk of ruin or catastrophe can lead to a disempowerment, an overwhelm, and confusion about response & responsibility.
 - "Like the genie let out of the lamp, risk is no longer subject to human control. The representation of risk as a transcendental technical problem, caused by human endeavor, demonstrates a clear attitude about the human character. It suggests that we have the power to destroy but not to do very much about the dangers which hover over our everyday life." (p. 58)
 - "The future is seen as a terrain which bears little relationship to the geography of the present. Since the process of change appears unresponsive to human management, its future direction becomes more and more incomprehensible. Society's estrangement from the process of change is expressed in a future that is so strange as to be unrecognizable." (p. 61)
 - "It is important to note that when the future is deemed to be very threatening, it is present-day society that is condemned. For if our actions are likely to have such an impact on the future, then it is we who are responsible for what happens in the period ahead." (p. 62)

Hyper Individualization as a Cause of Existential Risk Anxiety

- "The relative weakness of institutions which link the individual to other people in society contributes to an intensification of isolation. The process of individuation enhances the feeling of vulnerability.
- Many people are literally on their own. Such social isolation enhances the sense of insecurity. Many of society's characteristic obsessions -- with health, safety, and security -- are the products of this experience of social isolation." (p. 67)
- "When social roles are continually subject to modification and when what is right and what is wrong is far from settled, people are entitled to feel unsure about the future. All of these processes strengthen the process of individuation. What emerges is a decidedly cautious individual." (p. 68)

Details

On Trap of Rationality

- "The *implicit* view in the rational approach to the operating environment is something like 'this is what we want; this is what is going to happen in the world; so we know what we are going to do in that world in order to get what we want.' Herein lies the trap." (p. 79)
- **Top-down engineering fails in a world that is hyper-turbulent.** "The world is continuously changing, it is complex and it throws out events and properties which are outside any range of prediction....The black swan theory refers to the implications of large-impact, hard-to-predict and rare events beyond the realm of normal expectations. In the hyperturbulent world, black swans come thicker and faster, no longer an exception but inclining to be the norm." (p. 79)

Toward a New Ethics (of Investing + Innovation)

- **A new ethical orientation is not just some whimsical or moralist or post-economic luxury; it is required to properly navigate a world laced with daisy chain of risks, characterized by hyperturbulence.**
 - "Organization management, dominated by the management sciences, has analyzed and systematized situations to bring them under control to pursue goals such as 'return to shareholders' or 'public value.' But as the global contextual crisis looms ever more strongly, such limited and limiting goals, often disguising more nefarious aims associated with power and greed rather than sustainability and strategic adaptation, are dissociated from the real world." (p. 79)
- **Five Principles:**
 1. **Give up on control myth.** "[O]ur ever more sophisticated models...break down in the face of the real complexity and mystery of the world."
 2. **Revive subjective experience.** "The implications for how we see the world and our place in it are critical for our understanding of it and our behavior towards it and, more profoundly, as part of it."
 - **The impoverishment of the subject is the reason for organized irresponsibility, nefarious activities, ethical degradation, and normalization of ignorance.**
 3. **Integrity over Integration.** "The traditional model of organization is struggling. Start by replacing integration with the more flexible and adaptable notion of integrity."
 4. **Present vs. Calculating the Future.** "We underestimate the importance of living more deeply and consciously in the present."
 5. **Blur subject and object boundary.** "The subject-object split is the hallmark of the Enlightenment, the separation of self from the world. We need to recognize a new context." (p. 80)

On Ethical Imperative and AI

- **Humans are necessary when decision making requires integrity, defined as both integration of bigger picture context and ethical stance.**
 - "So integrity implies taking into account the *big when* and the *big where* as a greatly expanded present moment. Integrity also involves an ethical dimension, a sensitivity to values, and a degree of consistency in relation to those values that transcend the optimizing and satisficing nature of the situation in question." (p. 83)
- **Human-centric ethics is critical in a world that tends promote economics as finality.**
 - "In a system where economics is dominant, the ethical is considered secondary and even itself 'unethical' by viewpoints such as the Chicago school, who assert there is only one social responsibility of business--to use its resources to engage only in activities designed to increase its profits and shareholder monetary value." (p. 83)

Ethics Is Action

- "[I]n the second-order paradigm, the decision-maker is considered part of the system under decision and can only tell himself or herself what the 'best' decision is. This...is the origin of ethics and that ethics cannot be articulated as a code. The rewards of ethical action lie in the action itself." (p. 84)
- **In the face of undecidable questions real decisions are demanded. This is why and where multidisciplinary perspectives--e.g., philosophy, literature, ethics--are required to cultivate the ethical investor in an age of hyperturbulence and undecidability.**
 - "So there is a close relationship between ethics and choice in the rapid responses and anticipations needed in the face of turbulence. The implication here is that a state of mind or consciousness of the decider is critical for high adaptive performance. If the decider changes state, the decision field changes state therefore, both the practical options and their ethical implications come into the foreground." (p. 87)

Details

Risk Analysis: Two Ways

- Working definition of risk analysis has intimate connection with time with the question being what is one's orientation & relationship with time (and its derivative, the spectrum of Knighting risk-and-uncertainty).
 - "[R]isk analysis...seeks to control for future possibilities, y adjusting exposure to undesirable contingencies and maximizing the chances of desirable ones in the most cost-effective way possible." (p. 489)
- Risk is not some technical discipline; you can't hide behind or genuflect in front of your supposed VaR. Rather, risk is epistemological: "Seen genealogically, risk is a *style of thinking*.... risk thinking, as a set of techniques, brings a sense of authority and control, of science one might say; a safe basis for action and enterprise." (p. 489)
- Aspiration of risk analysis: "makes possible the intelligent navigation of an imperfect and potentially frightening world, and the effective use of resources to deal with all manner of contingencies." (p. 490)
- However, inappropriate or uncritical use of risk analysis has a tendency to create new (and possibly worse, risks): "if inappropriately used, risk analysis can itself be a source of risk. It can lead to fantasies characteristic of the worst romantic excesses of enlightenment thinking." (p. 490)
 - "Most worrying is the tendency for certain risk practices to 'sweep under the carpet' future risks, and to leave them hidden from sight" (p. 490)

Risk and Fantasy of Control

- On risk as a child of enlightenment: "[R]isk analysis might be regarded as not only a product of enlightenment thinking, but also the means to deliver the ultimate enlightenment fantasy: the idea that successive generations will learn more about the world, and so become more able to manipulate it for human gain and containment." (p. 489)
- On unintended consequences: "Processes of innovation not only bring new gains, but also manufacture new risks that serve to undercut old certainties" (p. 490)

Ever-Present Black Swan Can't Be Engineered Away

- On preparedness (precautionary principle?) and the ever-present black swan.
 - "Emergency preparedness needs to deal with the range of possible contingencies, not only the most probable ones. One needs to plan for an *envelope* of contingencies, and where this is in conflict with the very reasonable idea of making the optimum use of resources, there is a need to adapt planning to allow an escalation of response in order to deal with low-probability/high-consequence occurrences. The dangers of being unprepared for rare events are clear, especially so after an extended incident-free period." (p. 490)
- Risk spreading over time does not remove the risk.
 - "[T]he basis of 'engineering out' the possibility of such events has been regulated in terms of the 'tolerability' of a certain, non-zero, level of risk. This residual risk is expressed as a probability of failure per annum. It follows that if considered over a sufficiently long time period, *some kind* of incident will occur. In this way, the calculation of a tolerable level of residual risk amounts to 'spreading' the risk out over a timeline until it produces a small yearly rate of exposure. Of course, when a failure does occur, no matter how unlikely, a *whole incident* will take place, *not a tiny proportion* of an incident." (p. 490)

Danger of Normalizing Risk

- On risk creep and normalization:
 - "potential for institutional creep to occur, in which, in the absence of failures, the level of 'acceptable' risk rises implicitly over time." (p. 491).
 - "sophisticated risk-management techniques produced a fantasy of control within a community of professionals, who were in the thrall of a collective exercise of normalization of deviance." (p. 491)

See also Ulrich Beck, Risk Society, Reflexive Modernity

- On Post-Industrial Society as a "Risk Society." Characterized by hyper-uncertainty, turbulence: "Yet the expansion of information has also caused conflicts over the meaning and impacts of risk amongst competing interest groups. Despite its enjoying comparative health and longevity, transboundary dangers cast a shadow of discomfiture over contemporary western society. Thus, the implicit bargain for techno-scientific development and heightened risk consciousness might well be the amplification of insecurity." (Mythen, Ulrich Beck: A Critical Introduction to the Risk Society (2004))
- "In matters of risk, it would seem that 'the more we know, the less we understand' (Id. at 3)
- "[A]lthough the language of risk is prolific, the concept itself remains cloaked in ambiguity." (Id. at 4)

Details

On Two Angel Approaches: Predictive Control and Non-Predictive Control Strategies

- Two broad classifications of angel investing approaches: (1) prediction-based decision making and (2) non-predictive control based decision making
 - "Predictive strategies include market research using formal tools such as surveys, detailed financial models leading to careful calculations of risk-adjusted expected return, etc., and are very familiar to virtually anyone involved in writing business plans. Using prediction to obtain control over future outcomes assumes a logic that suggests: To the extent you can predict the future you can control your outcomes." (p. 117)
 - Non-predictive control strategies include effectuation approaches. See (Field Note 84: On "Effectuation" and Field Note 85: On "Effectuation Deux")
 - "Effectual logic inverts predictive rationality in several ways. Actors begin with who they are, what they know and whom they know, rather than with a predetermined vision or externally validated 'opportunity.' They then imagine a series of viable and valuable courses of action that they can implement using only what they can afford to lose. This means that they do not evaluate opportunities based on expected return in order to determine venture goals. Nor do they stubbornly hold too closely to preconceived goals as a way to determine which stakeholders to pursue or which resource-owners to chase." (p. 117)

Note on Methodology of Study

- 121 investors; 1,038 new venture investments; 414 exits, 90% over a 10-year period (presumably, based upon original submission year: 1996-200)

On Decisions & Uncertainty Gradient

See, e.g. myriad of notes on this topic, esp. Field Note 16 and Field Note 50.

- Angels geared toward respecting the space of uncertainty must focus on risk mitigation or fall prey to nihilistic or exuberant strains of YOLO.
 - "Angel investors emphasizing control [not as in ownership, but as in control over one's process and crucially, loss limitation / bet size as distinct from prediction] invest with failure in mind, using the effectual principle of affordable loss rather than expected values (based on predictions) as the basis of making investment decisions." (p. 120)
- Effectuation literature's emphasis of "affordable loss" -- that is, defining your action based on your pre-defined loss amount -- is akin to an investing mindset that focuses on survivability as a precondition to any alpha capture.
 - "Affordable loss focuses on getting to market quickly and cheaply based on the means at hand. These investors tend to over-weight the benefits of low upfront investments relative to potential inefficiencies this may create later in the development of the venture." (p. 120)
 - A "predictive emphasis is likely to lead to bigger bets on forecasts for market potential and profits....[I]nvestors may be more prone to escalation of commitment when those predicted payoffs are large. The combination of increasing the magnitude of investments and increasing the likelihood of escalation of commitment means that investors focused on prediction are likely to make systematically larger investments than investors that do not emphasize prediction." (p. 121)
- Smaller bet sizes are a logical consequence.
 - "Angel investors emphasizing control seem likely, therefore, to reduce the occurrence of investment failures....the investors ensure that the venture is in a less precarious position when negative surprises occur, and remain flexible to positive surprises because they are not over-committed to their initial goals." (p. 121)
- Don't be the venture on prediction. "Investors focused on positioning their ventures toward specific forecasts increase their dependence on accurate predictions of a variety of unpredictable variables, such as preferred channels, competitive offerings, cost curves, customer adoption rates, and so on." (p. 121)

Non-Predictive Investing Can Under-Allocate...But That Can Only Determined Ex Post Facto

- "[W]hen investors follow prediction-based strategies, their investment performance in the given venture depends heavily on the accuracy of their predictions. However, when investors follows [sic] control-based strategies, their investment grows only as a function of survival, and they may underinvest in any given opportunity." (p. 122)
- "[C]ontrol oriented investor may miss 'homeruns'--i.e. ventures in markets with explosive growth and high rates of return that require larger amounts of financing very fast. However, the control-based process keeps the bar for survival significantly lower, where an external shock or limited options for exit from the investment do no necessarily lead to investment failure." (p. 122)

Details

Decentralization's Discursive Problem

- "'Decentralization' is one of the words that is used in the cryptoeconomics space the most frequently, and is often even viewed as blockchain's entire *raison d'être*, but it is also one of the words that is perhaps defined the most poorly." (Id.)

3 Axes of Decentralization

These are related axes; the neat categorization belies interdependencies, though "in general they are quite independent of each other." (Id.)

1. Architectural.

- Measurement: Number of physical units (e.g. computers) in the system
- "How many of those computers can it tolerate breaking down at any single time?" (Id.)

2. Political.

- Measurement: Number of individuals / organizations
- How many "ultimately control the [architectural units] that the system is made up of?" (Id.)

3. Logical.

- Measurement: Interface & data structures
- "[I]f you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?"

3 Virtues of Decentralization

1. Fault Tolerance.

- "[D]ecentralized systems are less likely to fail accidentally because they rely on many separate components" that together resist system-wide / network-wide downtime. (Id.)

2. Attack Resistance.

- Harder to attack many than the one; often proponents of decentralization discuss the lack of single point of failure; decentralized systems "lack sensitive central points that can be attacked at much lower cost than the economic size of the surrounding system." (Id.)

3. Collusion Resistance.

- "[I]t is much harder for participants in decentralized systems to collude to act in ways that benefit them at the expense of other participants" (Id.)

Logically centralized		Logically decentralized	
Politically centralized	Politically decentralized	Politically centralized	Politically decentralized
Architecturally centralized	Traditional corporations Civil law	?	?
Architecturally decentralized	?	Traditional CDNs, Esperanto (initially)	BitTorrent, English language
	Blockchains, Common law		

SOURCE: Vitalik Buterin, "The Meaning of Decentralization," avail. online (Feb. 6, 2017)

Not a Panacea

- It's critical to reject the binary logic that is often bandied about in crypto and venture ecosystems when it comes to decentralization vs. centralization. Even architecturally decentralized systems in terms of physical computers may be centralized at other architectural and political chokepoints; for example:
 - "All nodes in a blockchain run the same client software, and this client software turns out to have a bug"
 - "All nodes in a blockchain run the same client software, and the development team of this software turns out to be socially corrupted"
 - "The research team that is proposing protocol upgrades turns out to be socially corrupted"
 - "In proof of work blockchain, 70% of miners are in the same country; and the government of this country decides to seize all mining farms for national security purposes"
 - "In a proof of stake blockchain, 70% of the coins at stake are held at one exchange"

Paradox of Coordination

- Greater coordination--often espoused by blockchain systems--has tendency to increase centralization, for example via lower friction to collude
- One approach is to thread the needle by promoting positive forms of coordination, while minimizing the negative forms.
- This is tricky because it presupposes one can on a second & third-order basis determine "good" from "bad." Such neatness runs in the face of complex systems.
- "Perhaps the best solution may be to rely heavily on the one group that is guaranteed to be fairly decentralized: the protocol's users." (Id.) But how?

Details

On Advice

- Distinguish between specific critique and "meta advice"
 - If someone smart, successful, competent provides targeted, narrow critique on specific work, then that is valuable
 - Reject advice about general "shoulds": "[I]f they are telling you what you ought to be studying, how you ought to approach things, what is the right way to think about things, you should probably ignore most of that." (~2:43:38)
- "Successful people are very well calibrated on their own ideas, in their own field and their own...area and they know exactly what works and what doesn't and what's good and what's bad, but they're not calibrated on your ideas. And so...they will say...this is a dumb idea, don't do this and you shouldn't do that. That stuff is generally worse than useless." (~2:44:34)
- Specific critique as an opportunity to improve what you're doing and ignore everything else.
- At best we know what we are doing; we can't opine on others.
- Advice is also historically contingent and a product of unique series of moments that are unlikely to be generally applied to others given their idiosyncrasies and their historical context.
- "I'm a firm believer that you have to build up your own intuition. So over time...you have to take your own risks that seem like they make sense to you and then learn from that and build up so that you can trust your own gut about what's a good idea....Sometimes you'll make mistakes and they'll turn out to be dead end and that's fine." (~2:46:55)"

✓ x


On Death

- Death is a factor that promotes change, turnover, and opportunity to do something different at a larger scale system level
- Most mammals: when they think it's a hopeless situation, they physically give up and die even though they could have persisted. Evolutionarily that doesn't seem like a good strategy to give up, but the issue of actually giving up suggests meta-cognitive controls where survival is not the top drive. Other considerations exist. This appears uniquely mammalian.
 - ✓ Cf. David Goggins's heuristic termed his "40% rule": when you are ready to give up, you are only 40% done; there's still 60% of reserves and resources available to call upon

On First Person / Third Person Science

- Science on the material / external world, there is a third person distance.
- When you are working on science of self, you are now your own experiment
- Exploring our own mind and consciousness is important and not captured by third person science

Elaboration on these key themes presented by Levin Forthcoming.



Investing is the "last liberal art." Failure to appreciate the interdisciplinary nature of the world we are in—particularly, in rapid-paced age of exponential tech—is certain financial suicide. Seeking wisdom from seemingly disparate domains is the ultimate hedge to bias and one-way thinking.

- All intelligence is collective intelligence. Biology uses a **multi-scale competency architecture** of nested problem-solvers in diverse problem spaces.
- **Goal-directedness** is an invariant for recognizing, building, and controlling/communicating with **Agents in unconventional embodiments**: the "cognitive boundary" model for scaling.
- Anatomical control as example – **collective intelligence of cells operating in morphospace**. Bioelectric networks are their proto-cognitive medium (ancestor of brain function), huge opportunities for biomedicine complementing bottom-up (hardware-focused) approaches.
- Synthetic bioengineering provides an **astronomically large option space for new bodies and new minds**, without standard evolutionary back-stories – a rich pool of novel beings with many implications for evolution, biomedicine, robotics/AI, and ethics.

Michael Levin, "Understanding the Collective Intelligence of Cells (Mar. 3, 2022), avail. At <https://www.youtube.com/watch?v=MdOHSUMb214>

Details

On AI Is Not Neutral

- "Artificial intelligence is not an objective, universal or neutral computational technique that makes determinations without human direction. Its systems are embedded in social, political, cultural, and economic worlds, shaped by humans, institutions, and imperatives that determine what they do and how they do it. They are designed to discriminate, to amplify hierarchies, and to encode narrow classifications." (p. 211)
- "Datasets in AI are never raw materials to feed algorithms: there are inherently political interventions. The entire practice of harvesting data, categorizing and labeling it, and then using it to train systems is a form of politics." (p. 221)

On AI Centralization & Decentralization Risks

- Centralization risk is clear from the concentrations of power that deploy the AI workflows. As well as the planetary extraction costs that are often ignored to "increase profits and centralize control for those who wield them." (p. 221)
 - "AI began as a major public project of the twentieth century and was relentlessly privatized to produce enormous financial gains for the tiny minority at the top of the extraction pyramid." (p. 217)
- Democratization is also problematic: "[t]o suggest that we democratize AI to reduce asymmetries of power is a little like arguing for democratizing weapons manufacturing in the service of peace." (p. 223)
 - Also begs the question of how "democratization" is instantiated. See also critique of "decentralization" as a floating signifier, an umbrella term that may be used to obscure negative externalities.

On Status Quo's Algorithmic Exceptionalism Narrative

- Algorithmic Exceptionalism: "the idea that because AI systems can perform uncanny feats of computation, they must be smarter and more objective than their flawed human creators." (p. 211-212)
- This leads to a narrative mystification. "Narratives of magic and mystification recur throughout AI's history, drawing bright circles around spectacular displays of speed, efficiency, and computational reasoning. It is no coincidence that one of the iconic examples of contemporary AI is a game." (p. 212)
- "That deep learning approaches are often uninterpretable, even to the engineers who created them, gives these systems an aura of being too complex to regulate and too powerful to refuse....the technique of 'obscuring by mystification' is often employed in public settings to argue for a phenomenon's inevitability. We are told to focus on the innovative nature of the method rather than on what is primary: the purpose of the thing itself." (p. 214)
- "[E]nchanted determinism obscures power and closes off informed public discussion, critical scrutiny, or outright rejection." (p. 214)

On Polarity of Utopianism and Dystopianism Rooted in Same Reductive Logic

- Tech Utopianism: "offers computational interventions as universal solutions applicable to any problem" (p. 214)
- Tech Dystopianism: "blames algorithms for their negative outcomes as though they are independent agents, without contending with the contexts that shape them and in which they operate." (p. 214)
 - Note that dystopians seem to ignore that their fear is already manifest: "This view rarely contends with the reality that so many people around the world are *already* dominated by systems of extractive planetary computation." (p. 214)
- "[M]achine learning exploits what it does know to predict what it does not know: a game of repeated approximations. Datasets are also *proxies* -- stand-ins for what they claim to measure. Put simply, this is transmuting difference into computable sameness. This kind of knowledge schema recalls what Friedrich Nietzsche described as 'the falsifying of the multifarious and incalculable into the identical, similar, and calculable.'" (p. 221-222)
- Epistemological confusions and errors in object recognition and labeling

More: Status Quo Gives Finger to Complexity; see also prior Field Notes on prediction, complexity, etc.

- "The belief that accurate prediction is fundamentally about reducing the complexity of the world gave rise to an implicit theory of the social: find the signal in the noise and make order from disorder. This epistemological flattening of complexity into clean signal for the purposes of prediction is now a central logic of machine learning." (p. 213)
- On Enchanted Determinism: "AI systems are seen as enchanted, beyond the known world, yet deterministic in that they discover patterns that can be applied with predictive certainty to everyday life." (p. 213)

On AI Negative Externalities

- Carbon footprint: "AI's carbon footprint is never fully admitted or accounted for by the tech sector." (p. 218)
- Labor politics: "Thousands of people are needed to support the illusion of automation: tagging, correcting, evaluating, and editing AI systems to make them appear seamless." (p. 219)
- Datafication (see Field Note 104. On "Datafication")

Details

On Broken—or, at Least Misshapen—Early-Stage Venture Model

Gaps in early-stage VC fund model with respect to the following:

- data-driven, objective research
- access to standardized reporting
- diligence duration / length to initiate position
 - interesting time to scale investment / "double down" on perceived winners is exceptionally low because (a) cognitive bias has metal teeth at this point and (b) game theoretic pressure against passing on the follow-on due to negative reputational risk in entrepreneurial community
- social capital reliance on deal sourcing and (implicit) investment justification
- back-office requirements
- process rigor, coherent & written risk protocols. (pp. 3-4)

Lack of professionalism in the industry, likely turbocharged by increased channels for AUM formation (creating a long tail).

- "There were no (and remain no) academic achievements required to enter the industry, no formal licensing or certification for getting hired, no training, documented processes, or industry oversight/best practices, and no federal or state oversight, to be a general partner of a venture fund, with full discretion over the LP's capital. Simply stated, the venture capital industry has never been professionalized...." (p. 5)

Early-stage venture returns are depressing

- "Most venture funds don't deliver real alpha for their investors when proper benchmarks (Russell 2000 + 400 basis points) are incorporated into the analysis." (p. 2)
 - Note also: "inherent survivorship bias in any industrywide index or asset-class performance computation" + poor / inconsistent reporting by funds + non-fund structures (SPVs, syndicates, angels) (id.)
- "The need to reach for sizable enough returns to get out of the negative J-curve hole oftentimes leads investors to take on undue risk, making inappropriately risky investments in individual companies at the expense of the overall risk metrics of the fund/portfolio." (p. 2)

An interesting point that early-stage venture has normalized startup failure narrative to apologize for lack of VC skill

- "By simply expanding the definition of success beyond the conventional venture fund model...and incorporating more of a data-driven 'Moneyball' approach..., the universe of fundable startups would also expand." (p. 3)
 - Quoting Griffith, "A Boom with a View" (2017): "But startup failure isn't a natural law like gravity. It's not a given. Normalizing the failure narrative only conceals the truth, misleads founders, and in certain cases, explains away bad behavior." (qtd. Griffith, p.3)

Toward Professionalized Early-Stage Venture

Lower fees

- "typical 2/20 fee structure creates a major impediment to alpha creation due to the J-curve/capital account drawdown...and perverse incentives for general partners to take undue portfolio risk (concentrated portfolios, 'potential unicorn' security selection." (p. 8)
 - Query whether this solves the behavioral "swing for fences" seduction, particularly pronounced in early-stage venture where probability space is indeterminate or at a minimum, tremendously wide

Diversified portfolios

- "Because of the perverse incentives, the lack of standardized reporting from startups, and the syndicate/co-investment nature of the industry, venture capital funds tend to concentrate their capital, neglecting the fundamental benefits of diversification." (p. 8)
 - Also note that AUM / bankroll plays a role; fund needs a minimum stack to execute. Size of stack is much higher if the same fund GP is to execute the staged deployment of capital across Seed, Ser. A, and Ser. B.
 - Does this mean that incumbent VC is required to lead the charge? That seems disenchanting and improbable. What alternatives exist?



Details

Transparent/disciplined selection process

- "'Style boxes' could be created, fund profiles could be applied, and manager skill could be measured." (p. 8)

Managed risk/smart beta

- "The goal of properly diversifying portfolios is to mitigate the nonsystemic, company-specific risks at the fund level. The next level of proper risk management once transparency and discipline are also embraced is defining the actual security selection strategy....[G]iven that the commonly accepted principal reason startups succeed and fail is *timing* (or when asking long-time, successful venture capitalists, *luck*), trying to pick winners is simply not an equation for success....Simply stated, nobody knows what a good deal looks like until after the fact. But there is an opportunity for pattern fit of bad deals...." (p. 8)

After-tax returns: QSBS Sec. 1202 and 1244

- "Why more investors don't utilize these laws is a mystery. There is little knowledge sharing on these laws from the organizations advising angel investors or the organizations helping startups get funding....Nor are most venture firms tracking the implications of these tax laws on their portfolio companies and reporting it on the K-1s for their taxable LPs that could utilize either 1244, 1202, or both. This is potentially in violation of the governing principles of general partnerships...." (p. 9)

Toward Diversification in Early-Stage Venture

Numerosity + Staged Capital Deployment + Systematic Scoring

- Seed Stage: 100-200 companies
- Ser. A: 60-120 companies from Seed Stage pool
- Ser. B: 30-60 companies from Ser. A pool (p. 5)

Bet sizing at each stage follows the Gigerenzer 1/N Heuristic (See Field Note 26 On "1/N")

- "Each company should have the same amount of dollars across the funds at each stage to avoid unconsciously magnifying nonsystematic risks." (p. 5)
- "Relative to the conventional early-stage (Seed to B Round) venture fund strategy that is 60% to 70% of capital deployed over 20-30 companies and 30%-40% held back for follow-on funding of better deals, this model would do the following:
 - minimize nonsystematic risk via proper diversification at each round,
 - minimize systematic risk via the staged capital deployment,
 - maximize the time-weighted and dollar-weighted returns for the investors via the weightings of deployed capital in the later (and presumably) less risky portfolios." (p. 6)

On the Ruse of Midas

Conventional stock picking largely fails; it's even more failure prone in early-stage venture where game dynamics are less efficient.

- "Given the body of work showing that stock picking and/or timing the market (systematic risk) is difficult or nearly impossible with any degree of consistency, we must recognize that managing market/timing/systematic risk in the venture fund context is equally difficult, if not impossible." (p. 5)
- "To execute this strategy, standardized reporting and performance analytics on the underlying companies would be necessary to inform the selection" of companies that warrant investment in subsequent staged rounds from the initial Seed pool. (p. 6)
 - Query: what is the methodology for selection of the initial Seed pool(s)? Geographic, demographic, sector, founder composition, legibility of idea, etc.? Or is it simply a function of reaching N = 100-200 with "common sense" guardrails?
- "Decision-process risk can be best understood as the degree to which decisions are made with a construct or process that fails to minimize the various cognitive effects, heuristics, and tendencies inherent in decision making as recognized in the field of behavioral economics or behavioral finance. These effects include anchoring, herd behavior, framing effects, narrative fallacy, confirmation bias, familiarity bias, and status quo bias." (p. 7)
 - But see Field Note 22 On "Heuristics, or Simplicity in face of Complexity" for a calibration of when and why certain heuristics are appropriate--and indeed "rational"--depending on one's environment.
- On simple algorithm beats complex, see, e.g., prior Field Notes on risk, uncertainty, heuristics.

Details

- Linear Pipes. Pipes are dominant business design for the industrial economy. Linear value creation: company builds product / service --> pushes them to customers. Value produced upstream; consumed downstream.
- Education Pipe. Teachers push knowledge to receptive students. There is a linear movement of value from a producer to one or many consumers in all examples of pipe businesses.
- Forces Enabling Platforms.
 - Increasing interconnectedness
 - Decentralized production
 - AI
- Plug n' Play. Platforms create plug-and-play infrastructure that enables producers and consumers of value to connect and interact with each other in a manner that wasn't possible in the past.
 - External developers can extend platform functionality using its APIs and contribute back to the very infrastructure of the business.
- Value of Platform.
 - Provide open, participative, plug-and-play infrastructure for producers and consumers to plug into and interact with each other.
 - Curate participants on platform and govern social and economic interactions that ensue.
- Multi-Dimensional Value Flow. Enabling interactions on a plug-and-play infrastructure requires a multi-directional flow of value between different participants. This is different from pipes, which solely create and push value out to consumers in a linear flow of value.
 - Platform business does not create the end value; rather, the business only enables value creation. As a result, participants on the platform take on production as well as consumption roles.
 - Must focus on both producers and consumers (vs. pipes that focus on latter)
- Ecosystems are the key enablers of value creation on platforms and a new source of competitive advantage. Platform giants will create massive value, not through their access to physical resources but through leveraging data to orchestrate physical and digital resources across their ecosystem.
- Pipe Scale = scale powered by ability to coordinate internal labor and resources toward efficient value creation and toward delivery of the created value to an aggregated consumer base.
 - Inputs to business—labor and resources—no longer need to be aggregated internally; pervasive connectivity allows the aggregation of labor and resources even when they exist externally. This ability to aggregate resources without the need for physical concentration and centralized control leads to a new design for platform business models.
- Platform Scale = scale powered by ability to leverage and orchestrate global ecosystem of producers and consumers toward efficient value creation and exchange. The management of platform scale involves the design and optimization of value-exchange interactions between producers and consumers.
- Less Focus on Content Ownership. Rely more on ability to orchestrate interactions between producers and consumers. This enables content creation, content sharing, content scaling.
- Dollar to Data. Business units should be measured not just in terms of dollars absorbed but also in terms of monetizable data absorbed. *But see [[FN 104. On "Datafication"]] on problems of data-as-oil logic*
- Destination to Distribution. Connectivity between platform participants is always-on vs. in pipe-oriented businesses that embed a focus on "destination" thinking (where to go) vs. distribution thinking (how things move). Goal of platform is to enable interactions vs. specific product push. Maximize interactions and interaction ease.
- 5 Drivers of Platform Scale
 1. Minimal marginal costs of production and distribution.
 2. Positive Feedback powers Network FX. As producers participate more often, they attract consumers, who attract more producers.
 3. Behavior design and community culture. Central challenge in managing user and partner participation on a self-serve system is compliance; inducement of behavioral norms productive to the platform interactions
 4. Learning filters. Without strong filters, higher abundance leads to lower relevance. Thus, need a curation engine, especially as information flows scale.
 5. Virality. Virality doesn't require a user's recommendation; any engagement with the platform creates an exhaust output that signals its use. Word of mouth is not required anymore.

- Simon DeDeo, "No Safe Level of Use: Strategies for Post-Social Media" (21 May 2021), avail at <https://simondedeo.com/?p=854>
- Simon DeDeo, "The 11th Reason To Delete Your Social Media Account: the Algorithm Will Find You" (25 Apr. 2021), avail at <https://simondedeo.com/?p=705>
- Tristan Harris & Anderson Cooper, "Brain Hacking" on 60 Minutes, (9 Apr. 2017) available at <https://www.youtube.com/watch?v=awAMTQZmvPE>
- Jaron Lanier, Ten Arguments for Deleting Your Social Media Accounts Right Now (2018)
 - Cal Newport, Digital Minimalism: Choosing a Focused Life in a Noisy World, (2019)

Details

Social Media as True Addiction

- It's not hyperbolic to call social media the engine of addiction.
 - "Because the stimuli for the algorithm don't mean anything, because they genuinely are random, the brain isn't adapting to anything real, but to a fiction. That process—of becoming hooked on an elusive mirage—is addiction. As the algorithm tries to escape a rut, the human mind becomes stuck in one." (Jaron Lanier, [Early VR Tech Pioneer / Long-Term Industry Insider w/ Potential Bias Given Position @ Microsoft, Ten Arguments for Deleting Your Social Media Accounts Right Now \(2018\)](#), at 15)
- Ad-driven social media is explicitly designed to keep you addicted.
 - "The goal is to figure out how to keep you online, how to create the circumstances under which you are kept online, and how to shift your own preferences and behaviors in order to make achieving the first two goals easier and more decisive." (Simon DeDeo, Asst. Prof. at Carnegie Mellon in Dept. of Social and Decision Sciences & External Prof. at Santa Fe Institute, "The 11th Reason To Delete Your Social Media Account: the Algorithm Will Find You" (25 Apr. 2021), avail at <https://simondedeo.com/?p=705>)

Social Media Has Tendency To Degrade Human Flourishing

- TL;DR: social media makes you a worse human being.
 - "The algorithm not only seeks out your buttons, but learns how to cultivate, and magnify, the ones that you had dealt with, in ways that are essentially invisible." (DeDeo, "The 11th Reason")
- Magnified behaviors include: rage, increased interpersonal conflict, reflexive argumentation, comparison, jealousy, lethargy, passivity, fatalism, self-hatred, sadness, procrastination, entitlement, grandiosity, confusion, pathological performativity

Social Media Crushes Knowledge Work Through Social Snacking, Info Overload, and Polarizing Misinformation

- These platforms customize / personalize feeds based on algorithmic mass mining at scale heretofore unimaginable. This means that I'm not even seeing the same information as others. Perhaps discursive polarization today is not because the "other side" is stupid or ignorant, but because the "other side" is bombarded with information that makes it appear to be the only side that exists with any merit, endlessly fed by algorithmically curated information that mercilessly reinforces existing ideas. The result is an echo chamber of diabolical proportions.
- This is particularly deleterious to investing/trading/risk mitigation.
- Signal:noise ratio becomes monstrously skewed to noise.

Social Media Is Not Neutral

- Social media makes you an asshole while waving the banner of neutrality; the effects are not immediately noticeable in increments, imperceptibly compounding over time into a ghastly form.
 - "I don't want to be an asshole. Or a fake-nice person. I want to be authentically nice, and certain online designs seem to fight against that with magical force....[S]ince social media took off, assholes are having more of a say in the world." (Lanier, [Ten Arguments](#), at 44)
 - "[B]ehavior has become polarized on ad-based social platforms as experiences ricochet between two extremes. Either there's a total shitstorm of assholes...or everyone is super careful and artificially nice." (Lanier, [Ten Arguments](#), at 51)
- Technology is *not* neutral. It's a "race to the bottom of the brain stem."
 - Quoting **Tristan Harris**, fmr. Google employee: Technology is "not neutral. They want you to use it in particular ways and for long periods of time. Because that's how they make their money." (clip from 60 Minutes where Anderson Cooper interviews Tristan Harris, available at <https://www.youtube.com/watch?v=awAMTQZmvPE>)



Details

Social Media as Tools of Surveillance

- It's wise to assume that tech companies watch everything you do as a large-scale and deeply penetrating surveillance apparatus.
 - "[W]hen you type something into a status-update box, and then delete, this information is transmitted to their servers. The location of your cursor on the screen, your hesitations, where you linger as you doom-scroll—all of these things are logged and transmitted." (DeDeo, "The 11th Reason")
 - "[T]hey log what you type but do not send, because of an interesting article that was written on how people have second thoughts on what they tweet." (DeDeo, "The 11th Reason")
- Polarization of groups is encouraged because it increases usage of social platforms and thus increases their profitability.
- Social media creates a depressing simulacrum: "[p]eople are clustered into paranoia peer groups because they can be more easily and predictably swayed. The clustering is automatic, sterile, and, as always, weirdly innocent." (Lanier, *Ten Arguments*, at 65).

Solution Requires Fundamental Re-Evaluation

- If I accept the premise that social media is an addiction, then the response must be to take drastic actions and possibly fully reject certain parts of the digital landscape. However, the complex question is whether wholesale approaches can actually work for most people (can they even work for me?) given the embeddedness of tech in day-to-day interactions. See *Field Note 105 on the notion of "forced choice" and "rigged game."*
- "Many of us think of social media as a glass of wine—a harmless indulgence at low levels of use, and a total blast on special occasion. I used to think this, too, but I now think that it's much more like the modern cigarette: saturated with highly addictive chemicals, with only the most surface-level social benefits, and with a near-guarantee that a significant number of users will receive long-term damage. Nearly all of this harm comes from the simple fact that, in ad-supported social media, you are the product." (Simon DeDeo, "No Safe Level of Use: Strategies for Post-Social Media" (21 May 2021), available at <https://simondedeo.com/?p=854>)
- "[G]radually changing your habits one at a time doesn't work well—the engineered attraction of the attention economy, combined with the friction of convenience, will diminish your inertia until you backslide toward where you started." (Cal Newport, *Comp. Sci. Assoc. Prof. @ Georgetown, Digital Minimalism: Choosing a Focused Life in a Noisy World*, (2019), at 59)

On Digital Minimalism

- **Definition:** "A philosophy of technology use in which you focus your online time on a small number of carefully selected and optimized activities that strongly support things you value, and then happily miss out on everything else." (Newport, at 28)
- Digital minimalism is highly intentional, as tech tools are used only in specific ways with specific operating parameters, whereas the opposite approach heavily indexes toward "keeping (vague) options open" and "accepting any (vague) benefit irrespective of downside." Thus, minimalism stands in stark contrast to FOMO-driven acceptance of ambiguous benefits social platforms and other tech tools may provide.

On Digital De-Clutter Protocol

- 30 day period of taking a break from "optional technologies" (that is, I can step away from them for 30 days without incurring severe harm in my professional and personal domains) *and* intentionally cultivating new behaviors/activities that line up with enhanced sense of well-being.
- Thus, this extends beyond social media platforms, but to all tech tools and services that fall under the "optional" banner.
- At the end of the 30 day period, tech tools are added back with a "zero based budget" approach. Every tool reintroduced must be specifically justified in its service of my life goals and values.
- For tools that I re-introduce, I must also clearly define operating procedures such as when I'll use the tool, for how long, which features to disable, etc.
- Criteria for re-introducing technology tools and services: (1) does the tool clearly support an important value of mine? If yes, (2) is that tool the *best* and most leveraged way to support that value?



Details

On Objections & Potential Responses

I've personally struggled with the following objections to the above critique of social media. And, after much self-reflection and investigation, my responses are presented.

Objection: There Are Benefits to Social Media.**Responses**

- Even if there are benefits, the loss of control—the highly addictive quality—outweighs. "These costs, of course, also tend to compound. When you combine an active Twitter presence with a dozen other attention-demanding online behaviors, the cost in life becomes extreme....you end up 'crushed and smothered' under the demands on your time and attention, and in the end, all you receive in return for sacrificing so much of your life is a few trinkets... many of which could probably be approximated at a much lower cost, or eliminated without any major negative impact.... It's easy to be seduced by the small amounts of profit offered by the latest app or service, but then forget its cost in terms of the most important resource we possess: the minutes of our life." (Newport, at 42)
- Even if there are benefits, the utility of these platforms is not at stake. What is at stake, instead, is my increased and deleterious dependence—at largely unconscious or vaguely conscious levels—upon them. "Each one of these services probably offers....something useful that would be hard to find elsewhere: the ability, for example, to keep up with baby pictures.... The source of our unease is not evident in these thin-sliced case studies, but instead becomes visible only when confronting the thicker reality of how these technologies as a whole have managed to expand beyond the minor roles for which we initially adopted them.... What's making us uncomfortable, in other words, is this feeling of losing control—a feeling that instantiates itself in a dozen different ways each day, such as when we tune out with our phone during our child's bath time, or lose our ability to enjoy a nice moment without a frantic urge to document it for a virtual audience." (Newport, at 206)
- Most of these benefits are weak substitutes for more genuine interaction. For example, keeping up with life events of friends can easily occur directly off-platform and indeed, off-line.
- Adopting investment/trading/risk philosophy again here requires a strategy of collecting open-ended options with the potential for massive upside. Ask: does social media platform x, y, z and tech tool a, b, c provide the potential for massive upside, together with a pre-defined and affordable risk of loss?
- Related to the above investment-oriented framework is a pragmatic approach of utilizing a MinMax heuristic. MinMax might be seen as a decision rule to maximize gains while minimizing the "risk of ruin" (i.e., an unacceptable level of loss that effectively knocks you out of the game or is otherwise too severe to accept regardless of the gains). As a life heuristic, MinMax means to maximize perceived positive optionality and relentlessly exclude weak or lukewarm options. It's a strategy for cutting out the uninspiring middle.



Details

Objection: The *Specific* Benefit of Connectivity that Social Media Provides Is Critical.

“Will I lose positive optionality of opportunities that might come from edges of the network?”

Responses:

- A gross misunderstanding, as this objection conflates weak and numerous "connection" with deeper and genuine "conversations." Smashing the "like" button on Facebook, the heart on Twitter and Instagram are plastic veneers for meaningful discourse.
 - "[M]any of these tools are engineered to hijack our social instincts to create an addictive allure. When you spend multiple hours a day compulsively clicking and swiping, there's much less free time left for slower interactions. And because this compulsive use emits a patina of socialness, it can delude you into thinking that you're already serving your relationships well, making further action unnecessary." (Newport, at 143)
- Increased online presence trades off directly with off-line relationships in such a way that the most heavy online users are the most connected and yet, the most alone.
- Real world interactions are more important than online ones. However, these are not mutually exclusive and the notion of "real" and "online" increasing blur. Prioritizing "real world" as defined by physical 3D also risks slipping into a philosophy of materialism.
 - "Our brains evolved during a period when the only communication was offline and face-to-face....these offline interactions are incredibly rich because they require our brains to process large amounts of information about subtle analog cues such as body language, facial expressions, and voice tone. The low-bandwidth chatter supported by many digital communication tools might offer a simulacrum of this connection, but it leaves most of our high-performance social processing networks underused—reducing these tools' ability to satisfy our intense sociality." (Newport, at 142)
- Seems like the non-naïve response is to do one's level best to find ways of turning up the (high integrity) signal and removing the noise. To determine the "high integrity," a cultivation of and inquiry into self/other at the hyper local level is needed.

Details

On Misuse of "Bounded Rationality"

- The concept of bounded rationality has become ambiguous. We need to be clear about how we describe it as the term "has become a diluted, fashionable [one], used by the proponents of quite disparate visions of reasonableness: from optimization under constraints to judgmental errors and human irrationality." (p. 37)

On 3 Premises of Bounded Rationality

- For Gigerenzer, a proper representation of "bounded rationality" has 3 related premises.
- Premise 1. Psychological Plausibility. This means that in assessing human decision-making and behavior, we must acknowledge the messy realities of what it means to operate as a human, not some anthropomorphized super-computer.
 - "The challenge is to base models of bounded rationality on the cognitive, emotional, social, and behavioral repertoire that a species actually has." (p. 38)
- Premise 2. Domain Specificity. Heuristics are specialized, tuned to the domain at hand; they are not general purpose. But, they are comprised of more generalized building blocks that cut across different heuristics.
- Premise 3. Ecological Rationality. Rationality here is defined "not in optimization, omniscience, or consistency," but rather suitability to the environment. (p. 38)
 - Cognitive tasks (classification, estimation, binary choices) vs. Adaptive tasks (multi-variate, complex, unknown)
 - See also Field Note 50: *On Cynefin and Complexity*

On Optimization

- Optimization--defined as trying to maximize some function--tends to fail for several reasons:
 1. computational burden is excessively high if there are multiple competition goals (vs. a controlled binary choice)
 2. not possible if goals are incommensurable (e.g., time spent helping kids with homework vs. time spent meditating vs. time spent going for a job)
 3. if alternatives are unbounded, then search function to acquire information becomes interminable (e.g., optimization assumes a finite set)
 4. "computational explosion" if one applies an optimization method to multitude of decisions we face in real time (p. 41)
- "Models of judgment and decision making have ignored search and stopping rules traditionally and have focused exclusively on the decision rule: Are cue values combined by multiple linear regression? By Bayes's rules? Or in some other fashion?" (p. 45)

On Over-Focus on Consistency

- Local consistency is not a requirement
- "From a functional view, however, consistency in choice and judgment is not a general norm to follow blindly, but rather a tool for achieving certain proximal goals. For a given goal, consistent behavior can be an advantage, a disadvantage, or unimportant." (p. 41)

No Holy Grail

- "Leibniz had a beautiful dream of discovering the universal logical language in which God had written the book of nature. This language, the Universal Characteristic, would replace all reasoning with one calculus." (p. 42)
- Against the Leibniz Universal Characteristic, bounded rationality suggests the metaphor of a "backwoods mechanic and used part dealer." (p. 43, referencing Wimsatt, 1999).
- "The backwoods mechanic has no general-purpose tool nor are all spare parts available to him. He must fiddle with various imperfect and short-range tools, a process known as vicarious functioning." (p. 43)
- See also Field Note 10: On Amara's Law + Exponential, Field Note 84: On Effectuation, Field Note 85; On Effectuation Part Deux, as they relate to "tinkering."



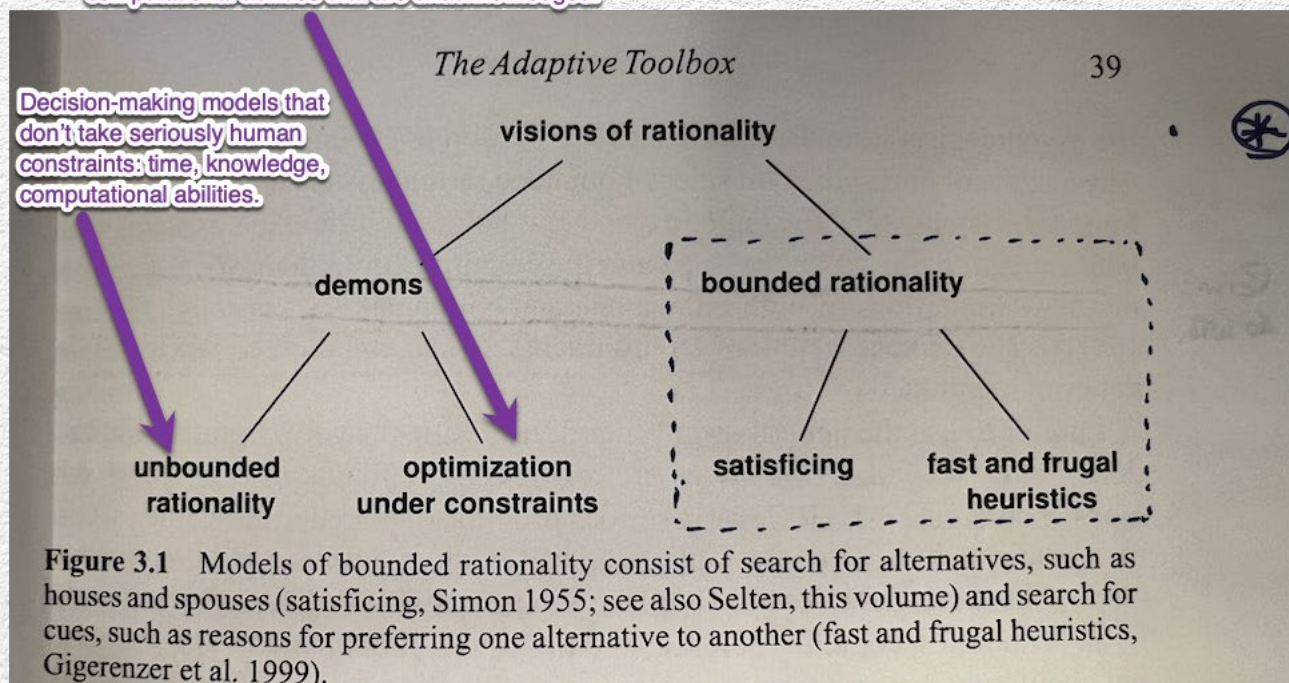
Details

Don't Ignore Simple Heuristics

- "Simple linear models dispense with optimal weighting; heuristics that use *one-reason decision making* dispense with summing. For example, Take The Best and other lexicographic heuristics rely only on one cue to take the decision and ignore all others." (p. 45)
- "[S]imple, psychologically plausible decision tools need not be inferior to complex combination schemes; there are situations where there is no trade-off between simplicity and accuracy." (p. 45)
- Heuristics take advantage of the environmental structure: "Heuristics that are matched to particular environments allow agents to be *ecologically rational*, making adaptive decisions that combine accuracy with speed and frugality." (p. 47)
- Heuristics are robust: "Given that simple heuristics tend to be more robust when environments are noisy and information is scarce..., one-reason decision making can actually become more accurate than regression." (p. 47)
- Scandal of overfitting: "If there is uncertainty in an environment, in the sense of some degree of unpredictability and changing environments, robustness becomes an issue. A model with many free parameters can achieve a good fit to a given body of data but may not generalize well to new data if it *overfitted* the old data." (p. 47)

On Visions of Rationality

Different from "unbounded rationality" model because it recognizes limit to information search via some kind of cut-off or stop to the info search. However, knowing when to stop itself requires constraints time, knowledge, and computational abilities that are unacknowledged.



Source: Gerd Gigerenzer, "The Adaptive Toolbox" in Gigerenzer & Selten, ed., *Bounded Rationality* (2001), p. 39

Annotations: @sandeephedge

Details

On Unintended Consequences in Tech (and Fat Tailed Domains)

- "The widespread adoption of new technologies always has unintended consequences...with emergent and highly complex impacts." (p. 1)
- Examples (n.b. "-->" is NOT meant to suggest linear cause/effect or sequence in time; it's just a note-taking convenience)
 - ✓ Cars --> city developments --> food and resource distribution --> social interactions --> employment centers --> etc. "At the same time, they disconnected people from the local economy and community, generated harmful emissions, and had a major impact on health and wellbeing. There is almost no aspect of modern Western life that has not been impacted by the automobile." (p. 1)
 - ✓ Phone is rather self-evident in today's world (at least awareness of, but not response to and responsibility for)
 - ✓ GPS --> designed with pragmatic purpose of helping one find locations; unintended is degradation of geo awareness, increase in dependency
 - ✓ Bathroom Scale --> meant to measure body weight, but has led to over-indexing of the metric: "One's body weight has come to be obsessively overvalued and used as a meaningful index of health beyond its actual diagnostic value," which has created a condition for "[t]ech-enabled quantification [that] makes for a certain ease of self-objectification." (p. 4)
 - ✓ "The point is not that tracking one's body weight is bad. The point is that the widespread and easy availability of doing so, through a simple advance in technology, made it possible to value body weight in a way that was not possible before. The scale increased the salience and visibility of body weight, changing the ways in which it could be valued, thought about, and otherwise related to psychologically. This had unforeseen outcomes." (p. 4)
 - ✓ Plow --> ease of labor --> storage facilities for food surplus --> change in habitats --> favoring of masculine upper body build --> anthropocentricity / degrading of relationship with animals and other sentient beings
(see also, multi-part interview b/t N. Hagan and D. Schmachtenberger)

On Technological Orthodoxy

- Technological orthodoxy represents the view that technology is itself neutral and independent of a human value system. On this view, tech gets its valence or charge from post-facto human use.
- Included within this view is a related one that technology is net positive.
 - ✓ "For most of history, the process of tech design has either assumed that such second- and third-order effects do not occur or that tech innovation is net positive." (p. 1)
- Techno-optimism: "ideology of the inherent positivity of technology" (p. 5)
- On functionality vs. morality:
 - ✓ "According to this view, technology is about what works for everyone--universal *functionality*--rather than what is good for everyone--universal *morality*." (p. 5)
- On failure of responsibility:
 - ✓ "This is an abnegation of responsibility for the impacts of technology. It is an ideology that places the onus of right action on 'users' rather than on designers." (p. 6)
- View of technology as isolated unit vs. ecology: "We must also move away from focusing on the impact of a single piece of technology towards a focus on ecologies of technologies. Sets of functionally bound technologies must become the unit of analysis for considering the second- and third-order effects across all domains of human life." (p. 17)

On Axiological Design (toward an alternative)

- Tech is values-laden; recognition is a starting point for more adaptive, purposeful design that can be a hedge against risk of (existential) ruin
 - ✓ "It is important not to consider any technology as existing all by itself. Humans have come to live in massive networks of operationally related technologies, which have come to form whole ecologies and infrastructures supporting every aspect of conscious experience." (p. 6)
- Against the tech orthodoxy, enter "axiological design" or the "application of principled judgment about value to the design of technology." (p. 1)
- Here, tech is not peripheral; it's not even quite central. Rather, it is embedded, always already existing in context.
 - ✓ "Rather than serving primarily in the background for labor or infrastructure, technological advances re in the immediate foreground--in the palm of our hands--central to the most intimate and consequential aspects of our lives, including education, communication, relationships, and politics." (p. 2)

Details

- Distinguish between "naively optimistic design" (pro-tech first-order thinking), "luddite design" (romanticized throw back to tech-lite), and "nihilistic design" (disavows values as criteria for tech design)
 - ✓ **Nihilistic design:** "Thinking about design in this way leads innovators to 'move fast and break things' and focus effort on 'disruptive' technologies. Whereas naively optimistic design made the assumption that technology could advance sacrosanct values, nihilistic design decoupled technological innovation from any serious considerations about value at all." (p. 10)
- "The future we get will depend on both the legal regulation of use and dissemination of technology and the cultural influences on technology adoption. Primarily though, a positive future will depend upon elements intrinsic to the design of the technologies themselves. Without the kind of axiological design described here, technology will continue to downgrade humans." (p. 17)

On Externalities: Two Ways

- Modern technology externalities can be mapped according to physical externalities and psychosocial externalities.
 - (1) Physical: material, environmental, 3D.
 - (2) Psychosocial: behavioral, non-physical, cognitive, social.
- Psychosocial consequences tend to have a temporal lag, making it easier for them to be ignored during tech design.
 - ✓ "Changes to human behavior and value systems may play out over the long term as second- or third-order effects, but they are nevertheless part of the matrix of impacts in which technology innovation must place itself." (p. 2)

On Rigged Game

- "New technologies themselves become uniquely valuable insofar as they confer advantage. Use of the new technology therefore becomes effectively obligatory, as failure to make use of it results in the loss of competitive advantage. Cultural and personal value systems change to accommodate these new selection pressures.....as this technology saturated social reality and the scope and impact of the technology became exponentially greater, it became massively disadvantageous not to have a smartphone." (p. 15)
 - ✓ **Personal example:** not having smart phone meant my kids couldn't enter school in 2021 b/c of school admin policy of scanning a QR code to verify self-reporting of potentially covid-related symptoms (analog phone lacked camera)

Issue of Scaling Local Ethics = Key Challenge

- "We can no longer limit ourselves to thinking only about the impacts across material economies, finance, and ecology. The question of how this might work at scale is still being explored." (p. 16)
- **Intervention at multi-prong level** (see, e.g. Schmachtenberger architecture: infrastructure, social structure, superstructure Field Note 101: On Metacrisis + Crypto (part 2)).
- **Intervention at individual--what some may term "spiritual" or ethical level is critical in my view, which is often preceded by some kind of crisis condition.** Heightened awareness of risk might be a sufficient substitute to spark self-inquiry.
- "Preferable futures require a return to considerations of human nature and conditioning, and how the two interact to influence behavior and thus the experience of being human....Future technologies must be designed according to methods that take human value and experience seriously enough to be constrained by their limits--such as sanity, dignity, and justice." (p. 18)

Details

Data Economy Hegemony

- Shift in business logic over the past decade from data as a cost center to data acquisition at all costs. Accepted and normalized, data has become a crucial component of our political economy.
 - ✓ "For the increasing number of companies participating in the 'data economy' or 'digital economy,' deleting data because of storage costs would be like burning piles of money or dumping barrels of oil down the drain because renting a warehouse was too much trouble." (p. 1)

Data as Capital with Embedded Accumulation Logic

- Status quo treats data as a commodity in a neutral manner, which has enabled improper behaviors, particularly at the corporate and investing layers
- The way we talk about data is not descriptive, but motivated
 - ✓ "What does it mean to see the world in a way that asserts everything is data? This is not a just a neutral observation about the nature or substance of the world. Such statements do not merely *reveal* or *reflect* the world. They *order* and *construct* the world." (p. 2)
 - ✓ "By operating rhetorically, they change how we understand and interact with the world, and they put those with data capital in a position of access and authority." (p. 2)
 - ✓ "When we talk about data as being 'collected,' 'gathered,' or even 'mined,' the image conjured is one of neutral accumulation, as if data existed out in the world as a distinct thing, readily available to be harvested. However, analysing the process in terms of extraction emphasises the people targeted by, and the exploitative nature of, dataveillance." (p. 6)

Data Mining vs. Data Manufacturing

- The widespread usage of "data mining" obscures the way that data actually functions in our political economy
 - "Data is not out there waiting to be discovered as if it already exists in the world like crude oil and raw ore. Data is a recorded abstraction of the world created and valorised by people using technology. The framing of data as a natural resource that is everywhere and free for the taking reinforces regimes of data accumulation." (p. 2)
- There is an imperialist logic to data accumulation; a kind of "data colonialism"
 - "The goal of transforming everything into data and the search for new sources of data echoes imperialist modes of accumulation." (p. 3)
 - "Through the world of using platforms and devices, people are turned into commodities that take the form of personal data, which is sold to advertisers and data brokers." (p. 4)
 - "The imperative, then, is to constantly collect and circulate data by producing commodities that create more data and building infrastructure to manage data. The stream of data must keep flowing and growing." (p. 4)

Data Model Today: "Collect First, Figure Out Use Later"

- The (Lacanian?) drive for data has deprioritized intentional use. Rather, the organizing business imperative is "collect as much as possible with the assumption of figuring out data use later." "This has accelerated the practices of data extraction. To what extent has ML/AI unwittingly accepted this--and normalized--this hyper datafication?
 - "The point is illustrated by the fact that data is very often collected without specific uses in mind. Indeed, the practice of collecting data first and figuring it out later is increasingly a core part of how businesses and government bodies operate. 'It does not matter that the amounts [of data] collected may vastly exceed a firm's imaginative reach or analytic grasp. The assumption is that it will eventually be useful, i.e., valuable'" (p. 4)

Data Deployment

- Data has been purposed toward the following main activities: 1. to profile and target people; 2. to optimize systems; 3. to manage and control; 4. to model probabilities; 5. to build platforms; 6. to grow asset value (see p. 5)

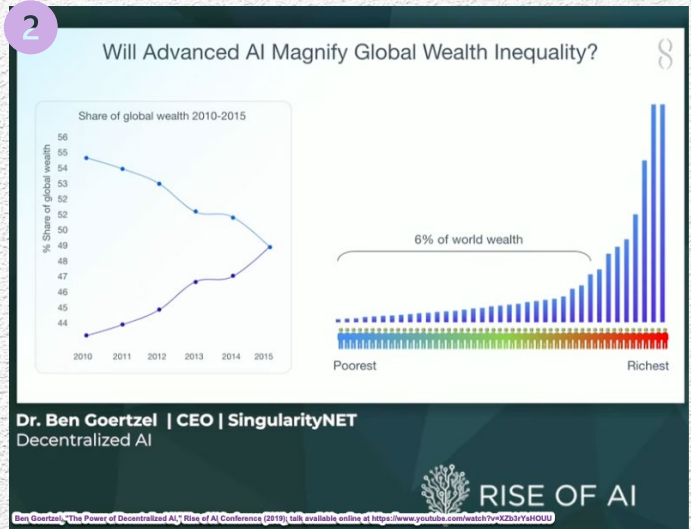
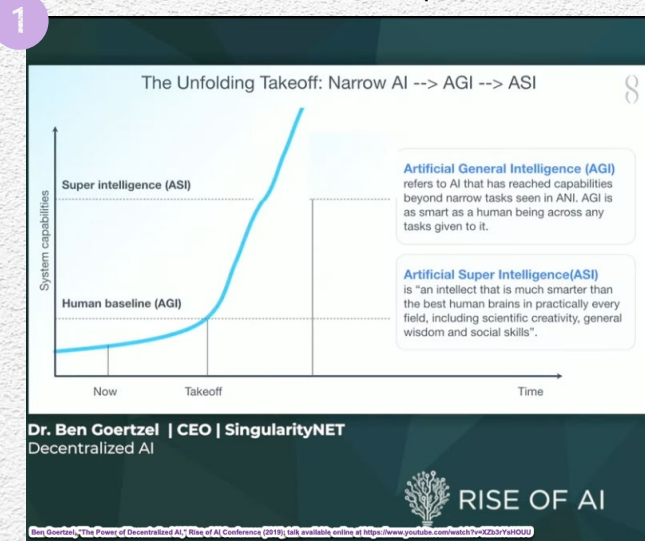
False Choice

- EULA (end user license agreement) is not a matter of choice, but acquiescence.
 - "One study concluded it would take 76 days, working for 8 hours a day, to read the privacy policies a person typically encounters in a year" (p. 7)
 - "EULAs are the ideal type of *pro forma* 'consent,' which may be better-termed acquiescence. That is, EULAs are less a method of consent in any meaningful and more a form of compliance. As Jaron Lanier argues, 'The reason people click 'yes' is not that they understand what they're doing, but that that is the only viable option other than boycotting a company in general, which is getting harder to do.'" (p. 8)

Details

1 On Status Quo AI Development

- Face recognition and game playing are a small corner of known AI algorithms that are strong in certain ways but limited in others. Deep neural nets are good at finding simple patterns across large data but it is just learning patterns in what is being presented vs. forming more abstract representations of data being scanned
- Not going to see AIs based on current version of deep neural networks inventing a new type of government or new type of art; rather, we see more of replication that is tethered to the data trained on

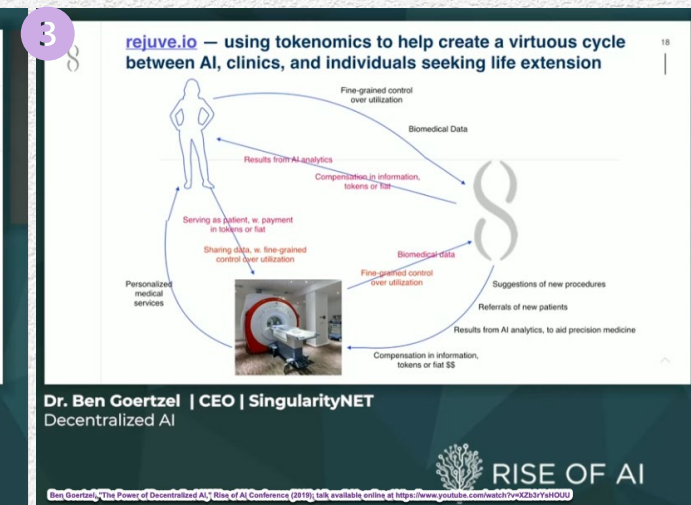
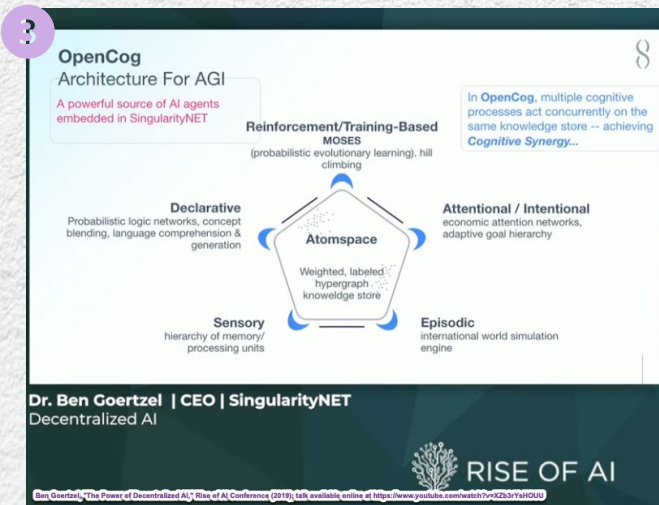


2 Identifiable Risks (Known (Un)knowns)

- AI magnifying global wealth inequality as a precursor to larger scale conflicts
- Mega-corporations and nation states leading the practical deployment of AI around the globe (i.e., the concentration of power dystopia)
- Narrow scope: will AI be in service of corporate profit maximization or serving the hegemony of nation-states? Intervention at the level of societal ethics is needed here as well.

3 On SingularityNET

- Blockchain based platform for AI marketplace
- Network of AI agents that self-organizing with flexible system of evolving APIs to communicate and share memory with each other
- Trying to build an alternate parallel ecosystem for AI on decentralized architecture vs. centralized platform



Details

On Flaw of Top Down, "Command & Control" Strategies

- When operating in turbulent environments where probability spaces are exceptionally wide, and at times, entirely undefined, a "traditional strategic-planning model" that emphasizes execution based upon forecasting initiative is comfortably wrong.
- "The world is now changing so quickly that no business can plan for every eventuality." (63)
- When used properly, tools like scenario planning, simulations, and options-based thinking can enable decision-makers "to consider multiple future states in assessing strategic investments, rather than rely on a single, deterministic forecast." (63)
- Living plans that continuously update preserves pragmatic action without siloed thinking (and fighting last year's battle).
 - "Thinking of strategy-making as continuous and generating a living plan enables executives to build on what's best about existing tools for coping with uncertainty--leading to more-flexible strategies and more-agile strategy-making." (63)

Extreme but Plausible Scenarios

- Against traditional scenario planning models that more or less arbitrarily build a set of "normal" cases spread across biased views of "worst case," "base case," and "best case," the recommendation is to consider extreme scenarios.
- Similar to the injunction to view problems from the tails by "examining what we call *extreme but plausible scenarios.*" (p. 64, emphasis in original)
- "The goal of this analysis is not to understand which outcome is most probable but to uncover new and different ways to compete and win, given a plethora of possible outcomes, and to reveal 'no regret' moves that should prove worthwhile under most scenarios." (64)

Strategic Hedges & Options

- Flexibility and preserving optionality can better adapt for rapidly changing environments.
- However, the practical challenge is to calibrate the amount of flexibility, ensuring it doesn't become too diffuse.
- In other words, "flexible but not loose"
- "[C]ompanies have sidelined real options analysis prematurely, paying far too much attention to the mechanics of determining the *absolute value* of a specific real option rather than relying on the tool's basic principles to understand the *relative value* of competing strategy alternatives." (64, emphasis in original)
- Flexibility vs. No Position
 - "It's important to note that investing in strategic hedges and options is not the same as placing a bet on every square. Trying to reduce risk in that way makes it nearly impossible for a company to score a big win...and locks in the certainty of many small losses that add up to real money." (65)
 - Too much flex--too many bets, too much diversification--frays attention and has negative psychological effect of amplifying information overwhelm and decision fatigue.
- Staged bets can solve for the risk of placing "too many bets" and not focusing on productive options. In other words, place the most bets when the relative uncertainty / probability space is highest; dial in as evidence of traction manifests.

Experimentation

- Similar to the entrepreneurial spirit of tinkering and running low-cost experiments before locking a more defined path.
- Critically, the experiments should tie to larger scale issues; limiting the scope of the experiment-as-experiment stifles innovation.
 - "[S] all experiments are perfectly fine (in fact, encouraged), but each experiment should be tied to something very big to ensure that the test is worth running. Correctly applied, experiments prove the viability of big bets." (66)

Re-Test Metrics

- Metrics, provided one doesn't view them deterministically, can be useful in fostering prudent decision-making against a backdrop of uncertainty.
- As a meta rule, the metrics ought to be re-evaluated (vs. militaristically executed against) as new developments emerge that require a re-testing of assumptions.
 - "Signposts and trigger points are never static. By design, they reflect management's best understanding of the 'known unknowns' affecting a company's strategy at a particular point in time. As more 'unknown unknowns' become known, signposts and trigger points must be revised and refined." (68)
- There's a cultural re-orientation needed to move away from a singular focus on performance measurement to assumption alteration.
 - "To become more adaptable to changing conditions, leaders must approach performance monitoring with a new mindset. The central question cannot be 'How did we perform?' Instead it must be 'Should we alter course?'" (69)

Details**On the Need to Understand Metacrisis**

- Need to address bigger picture, wide-ranging "x-risks" since they subsume the narrower problems being worked on, including in crypto
- A few high-level frameworks, esp. for technologists dealing with coordination (e.g., crypto)

Tech Stack != Values Neutral

- Simple example of portable camera: affects the way you perceive the world. Holding a piece of tech tunes your attention in a particular way, affecting behaviors
- Tech is an "extension of our actuation capacities"
 - Actuation: way that evolution selects for sensory processes and sense-making that informs choice. With new actuation capacity, it will tune your sensory processes (perception), thereby implicating choice-making
- There is no metacrisis without modern, exponential tech
- Cannot also reject tech given its pervasiveness
- What is required is a fundamental change in our relationship to tech and its (re)design
 - Tech design will predispose patterns of human behavior" (Schmachtenberger, ~15:50)

On Psycho-Social Externalities (Not Just Physical)

- Tech incentivizes behavior where the use of that tech confers an advantage
- Example: social media tech designed for picture capture and emphasis leads to large scale image-focused culture and dysmorphia writ large, as a consequence of design
- Example 2: the plow (see also Hagens multi-part podcast series with Schmachtenberger)
 - Before plow was horticulture and uneven usage of animals
 - Plow meant that caloric output (vs. human labor and hunting and gathering) was so great that the use of it became "obligate" for advantage and survival
 - If a technology confers a lot of capacity, it also means that everyone must use it (the tech stack as a whole, not necessarily a particular instance), particularly given rivalrous game theory system we are in
 - Plow caused a change in relationship with animals. It was a strong shift away from animal rights, respect, animalistic sensibilities toward a more mechanized and oppressive relationship toward the productive animal
 - Social ethic thus became tuned toward anthropocentrism, viewing non-humans as instruments
 - Plow ended animism, changed value systems toward utilitarian, de-emphasized women (due to requirement of upper body strength to utilize plow), storing of surplus (leading to wealth surplus and uneven distribution of wealth). All these consequences came from a technology that didn't anticipate or intend
 - The technology is also not isolate; it is part of an ecosystem, a stack.
- Ask: How does tech design code human minds and behavior, particularly potential second and third order consequences?

Chance IV vs. Chance II (motion-generated chance)

Thesis is that change in infrastructure drives changes in social structure and superstructure. But it also operates from "top down" such that intervention at the superstructure level curates the kind of tech stack we can design to orient toward a more harmonious society.

1. Infrastructure: the whole tech stack, modes of production, transportation, waste management, energy, etc. In the hunter-gatherer format, the infrastructure would be the spears, tools to make them, etc.
2. Social Structure: the collective agreement field such as law, governance, and the institutions that mediate these relationships
3. Superstructure: the values of the people, including religion, ideology, motivations, etc.

On Rugged Game

- Don't really have choice or agency in participating in certain tech ecosystems. For example, can't really opt out of the ad-driven business models without having a material negative disadvantage in society
- So much power asymmetry that can't really have true choice
- When there is such radical information asymmetry, the "buyer beware" caution has no power b/c of the extreme data and info disadvantage
- How do we have a superstructure for a more informed society as well as productive laws and regulations at the social layer that can bind the superstructure to the infrastructure.
- Status quo is seeing more emphasis on infrastructure level that is creating negative impacts on superstructure; the bidirectionality is out of phase.

Details

On Conflict Theory, Mistake Theory

- Mistake theory as plausible deniability for the negative consequences that weren't really unintended or entirely unanticipated
- Conflict theory is central to understanding civilizational risks: what conditions create the conflicts from arising in the first place?
- Can we predict all the ill effects of a new piece of tech or a new tech ecosystem? No, but we can do far better than status quo. Even thinking through with framework like physical vs. psycho-social externalities would be an improvement.

Details

Chance IV: "comes to you, unsought, because of *who you are* and *how you behave*. It is one-man-made, as personal as your signature." (76, emphasis mine)

On the Term "Serendipity"

- History of the term might be traced to 1557 and even prior to that found in Indian & Persian folklore
- Horace Walpole is credited with coining the term "serendipity" based on inspiration from the 1557 fairy tale, The Three Princes of Serendip, by Christoforo Armeno
- Serendipity is NOT isolated to "accidental" occurrence. It might include accidental discovery, but is not narrowly limited to it.
 - "[S]erendipity is the facility for encountering unexpected good luck, as the result of accident, sagacity, or general exploratory behavior." (71)
- Serendipity as a "quality--a gift for discovering things, by *accident* or *sagacity*, while hunting for something else. In today's parlance, we have usually watered down serendipity to mean the good luck that comes by accident--a result, not an ability. We have tended to lose sight of the element of sagacity, by which term Walpole originally wished to stress that some distinctive personal receptivity is involved." (71)

On "Altamirage"

- "[O]ne may introduce the term *altamirage* to identify the quality underlying Chance IV. Let us define it as the facility for encountering unexpected good luck as the result of highly individualized action. Altamirage goes well beyond the boundaries of serendipity in its emphasis on the role of personal *action* in chance." (87)

On Lock & Key: "One Way Function"

- "We must bear in mind that, by the time Chance IV finally occurs, the easy, more accessible problems will already have been solved earlier by conventional actions, conventional logic, or by the operations of the other forms of chance. What remains late in the game, then, is a tough core of complex, resistant problems. Such problems yield to none but an unusual approach, much as does the odd lock in an old door open only to the rare key." (76)

Chance IV vs. Chance II (motion-generated chance)

- Distinguishing Chance II's "motion" attribute with Chance IV's "uniqueness" attribute: "Chance IV connotes no generalized activity...Instead...discrete behavior performance focused in a highly specific manner. Whereas the lucky connections in Chance II might come to anyone as the happy by-product of a kind of circular stirring of the pot, the links of Chance IV can be drawn together and fused only by *one* quixotic rider cantering in on his own homemade hobby horse to intercept the problem at an odd angle." (76)

On Chance Types I - IV != Mutual Exclusive, but Co-Productive

- "[I]t may be a thorny matter to draw an arbitrary line between the contributions of Chance I through Chance IV. No need to--it is not an either/or matter." (91)
- "[T]he most novel, if not the greatest discoveries occur when several varieties of chance coincide" (93)

On "Bad" Luck

- "The snags and backlashes of bad luck are everywhere. It is a hard fact that in laboratory research unpredictable circumstances are more often arrayed against you than in your favor." (94)
- Insurmountable Opportunities. The juxtaposition breaks toward an optimistic bias, while acknowledging the "impossible." And so, the possibility of the impossible, to invoke Jacques Derrida.
 - "Despite all the setbacks, researchers still press on in the laboratory. If, in their muddled ignorance, they see through a glass darkly, it will still appear as a glass half full rather than half empty. Vulnerable everywhere, experimenters persist in their contrary, buoyant optimism about the future....But most of their approach acknowledges a simple fact pointed out by Pogo when he said with greater whimsy and far greater accuracy: 'We are confronted with insurmountable opportunities.'" (96)

Details

Venture Debt Defined

- Straight debt, not pseudo-equity.
- "Venture debt does not mean debt from angel investors or VCs that is commonly converted to equity, nor does venture debt mean loans to start-ups that have developed to the point of attractiveness to traditional lenders. Instead, venture debt as defined here is loans to early stage, rapid-growth start-ups that have no traditional means of paying it back--including personal guarantees, which no rational start-up entrepreneur will sign because most start-ups fail." (1171)
- Notion of sustainable financing of entrepreneurial ventures.
- "[V]enture debt is a separate and sustainable form of **entrepreneurial finance**, rather than mere VC spillover."

Counter-Conventional Opportunity

- Conventional logic is that debt and start ups "don't mix" due to lack of traditional credit metrics that inform standard underwriting decisions.
- Venture debt is shunned by traditional lenders because: (a) higher risk of default vs. mature businesses; (b) personal guarantees don't work because no founder would agree to them given high risk of failure; (c) capital ratios will be higher given higher risk nature of underlying businesses; (d) aren't set up to hold warrants or equity kickers, as their business model is premised solely on interest payments and avoiding losses.
 - As a result, traditional lenders require cash flows and tangible assets to serve as collateral.
 - Start-up assets (if any) are likely to be in the form of intangible IP (patents or trade secrets), which are much more difficult to foreclose on and realize value (1175).
 - Quoting Mark Van Osnabrugge & Robert Robinson (who wrote a book on angel investing), "[a]lmost as a rule, since most early-stage firms do not have positive cash flow, profitability, or solvency, banks rarely lend to them without a personal guarantee or collateral." (1176)
 - Since startups lack track records, positive cash flows, and tangible collateral, regulators view them as risky loan candidates and require banks to reserve a larger amount of capital.
 - Accounting conventions make it quite hard to capitalize expenditures on developing software...The result is that a company with a substantial investment in developing a valuable asset still might show almost no assets on its balance sheet. (cf. Mann text)

Venture Debt Game Theory

- Company must be VC-backed. This is essential because the exit for venture lenders is that VCs will follow on and keep investing in their early bets. Reliance on venture capital for repayment of venture debt creates a symbiosis.
- A start-up will still have no cash flows, tangible collateral, or track records after early-stage VC investments, but the presence of venture capital--and to a lesser extent the start-up's intellectual property (IP)--effectively substitute for traditional loan repayment criteria and make venture debt an attractive proposition to a specialized set of lenders." (1173)
 - "[S]imilar to a bridge loan, venture debt is about 'funding to subsequent rounds of equity' rather than relying on the underlying start-up's ability to repay the loan through cash flows." (1173)
 - Venture debt is the business of funding to subsequent rounds of equity (1184)
 - Angels tend not to have an explicit policy of follow-on investing, which is why VC-backing should be a requirement for venture debt. And when they do follow on, it suggests that no professional VC was willing to invest.
- Early-stage opportunity is more interesting given funding gap / void prior to more traditional loan metrics manifesting.
 - "[B]ecause VCs are far more likely to follow-on their investments early in the start-up's development, we discover the counterintuitive proposition that VCs actually prefer to lend to start-ups in their early stages as opposed to their later stages when cash flows and tangible collateral may emerge." (1173)
- One venture debt strategy is to wait for later rounds to see which companies the VCs back and which startups survive. However, this is a bad strategy because as startups mature, more traditional financial measures manifest, and venture capital becomes a diminishing proposition.
 - As the startup progresses toward exit stage, VC support takes a back seat to the startup's revenues, product, managerial team, and other factors that become the determinant of success. (1186)
 - In the early stages, "not enough can go wrong" between the initial and follow-on rounds to preclude the VC from supporting its horse.
 - There is also a social game theory element, whereby if an early VC doesn't follow on to give the startup runway and chance to prove itself a failure or breakout success, it will lose deal flow.



Details

- VCs also have dedicated follow-on reserves to support portfolio firms from the beginning, so it is structurally built in to the expectation set that VCs want to follow on their initial investment.
- Where the VC is in its fund life is important because older vintage funds near the end of investment period will have fewer reserves for follow-on investments.
- Series A / early-stage companies carry **less** funding risk because of the likelihood that VCs will stick with them for at least one more round even if they stumble. (I186)
- Warrant upside is also better in the early stages because the strike is much lower, more than compensating for the lower probability of success versus a more mature startup nearer to exit.

Venture Debt Deal Parameters

- Deal Size. Lower amount for Big 4 Bank Lenders (up to \$2mm); higher amount for non-bank lenders (average of \$3mm+). Overall, between \$2-10mm loan size.
- Straight Debt. These are not structured as convertible debt that flips to equity upon certain events, which makes venture loans attractive to equity investors since they don't get diluted.
- Term. 24-36 mos. with 3-9 mos. interest only.
- Amortization. Fully amortized over life of loan.
- Interest Rate. Double digits, approaching 20% for early stage deals that Vencore Capital does.
- Warrants. 5-15% of loan amount in warrant coverage
- Event-Driven. Venture debt works well in fields marked by clear milestones, as in device subfield within life sciences (milestones: technological, clinical, regulatory)

Landscape

- Major 4 Banks: Silicon Valley Bank, Comerica, Bridge Bank, Square I
- Minor 9 Non-Banks: Bluecrest Capital Finance, Hercules Technology Growth Capital, Horizon Technology Finance Management, Lighthouse Capital Partners, Pinnacle Ventures, TriplePoint Capital, Velocity Financial Group, Vencore Capital (very early stage), Western Technology Investment
- Bank VCs have a lower cost of capital because their main business is not in venture loans as such but in capturing the deposit account business of startups and their ecosystem partners. "Bank VCs, on the other hand, have a lower cost of capital through their deposit accounts and thus are able to offer lower interest rates, usually prime plus 1-2%. Not only are banks charging less interest, their loans are at the lower end of the venture debt range (up to \$2 million), meaning less of a principal base on which interest can accrue. Therefore, interest payments are not a sufficient financial motivator for banks to provide venture debt. It turns out that the real financial motivator for banks is the *chance to secure the start-up's deposit accounts.* Banks require start-ups to deposit and maintain their cash in the bank as a condition to receiving venture debt, and they are often able to attract VC deposit accounts to boot." (I182-83).
- "[R]egulatory impediments translate to smaller loans for banks and less flexibility in deal structuring, including more covenants in loan agreements. It is on these perceived weaknesses that non-banks pounce, offering larger loans and fewer-to-no covenants." (I183)

On Default Risk Surprisingly Low

- Warrants compensate for default risk in unsuccessful startups on the downside.
- "While it is the case that most start-ups fail, lending early in the start-up's development means that follow-on venture capital is usually sufficient to repay loans *before* VCs stop supporting failing start-ups." (I187)
- Whether a company fails is not as important as *when* it fails. Start-ups typically don't fail in the early rounds before the loan is repaid. Start-up failures outnumber failed loans. (I187)

On Information Rights

- Venture lenders **don't usually take board seats** because "lenders who sit on boards of the borrowers and use that position of control to benefit themselves at the expense of other firm claimants can face lender liability for their actions." (I193)
- Control-exercising lenders also face equitable subordination risk in bankruptcy, which limits their ability to foreclose on IP collateral.

On Collateral

- There are creative ways to protect downside value such as contracting for first priority in the proceeds of IP sales. This would appear to be moot because even an unsecured creditor takes priority over equity in a liquidation, but the rules may be different because most high-tech liquidations occur through an assignment for the benefit of creditors ("ABC") transaction, as opposed to formal bankruptcy proceeding. (I189) ==NTS: Follow Up==

Details

On Why Equity Holders Like Venture Credit

- Main financial attraction for equity investors and founders is that it extends start-up's runway and therefore avoids dilution. Using debt to grow and achieve milestones gets a higher valuation when more equity is eventually sold.
- Venture debt gives the company 6-12 months of runway so they can get better valuation in the next round and sell fewer shares.
- "Once entrepreneurs, angels, and early-stage VCs all own a piece of the start-up's equity, reaching milestones and upping firm valuation benefits them all by allowing funding needs to be met with less equity sold. Venture debt does dilute existing equity somewhat through the warrant kicker, but far less than another premature equity round would." (1197)
- **VCs like venture debt because it increases the fund's IRR calc:** "Although VC fund investors agree to contribute a certain amount of capital to the fund up front, the capital is not counted in IRR computations until it is actually drawn down by VCs. Therefore, if a VC can delay and/or reduce (by attracting new investors) its next equity draw through venture debt, the VC's apparent performance--if not actual performance--improves. Improving IRR is another reason VCs stage their investments rather than providing all cash to start-ups up front." (1197-98)
- **VCs also like venture debt because it gives them more time to evaluate the start-up.** "For existing portfolio companies, more time until the next VC investment allows VCs more of an opportunity to evaluate the start-up's prospects and development to decide whether they will fund the next equity round, attempt to bring in another VC as the lead, or walk away." (1198)
 - **Poker analogy:** "venture debt allows VCs to see one more card before placing another bet." (1198)
 - "Of course, if VCs fold on losers too soon, they will break their implicit promise to VCs to stick with their portfolio start-ups for a certain period of time and, as a result, suffer a reputational hit with both VCs and the entrepreneurial community. Therefore, folding is more of a realistic option in the later stages and thus more of a concern for the larger, non-bank VCs who lend in those stages." (1198) Deal Size. Lower amount for Big 4 Bank Lenders

On Why Equity VCs Don't / Can't Lend

1. Double digit returns are not high enough for the VC model.
2. Venture debt increases transaction costs for VCs because they have to find a different set of LPs to fund the loan or by having to coordinate a syndicate.
3. **Legal Concerns:** "VCs owe fiduciary duties to other equity investors either as directors or controlling shareholders, making a VC's venture loan to the start-up a self-interested transaction under corporate law." (1207)

Details

On Negotiation as Process of Discovery

- Goal is to observe and take in as much information as possible
- "[O]ne of the reasons that really smart people often have trouble being negotiators [is] they're so smart they think they don't have anything to discover." (25)
- Default negotiation model is premised upon adversarial relationship (whether explicit or not). Interestingly, the battle is often waged internally: "For those people who view negotiation as a battle of arguments, it's the voices in their own head that are overwhelming them. When they're not talking, they're thinking about their arguments, and when they are talking, they're making their arguments." (28)

On Active Listening

- Outcome of true active listening: "you'll disarm your counterpart. You'll make them feel safe."
- The voice in their head will begin to quiet down." (28)
- Essentially, active listening removes the obfuscating inner dialogue that is pinned to performance (sounding smart, "winning" an argument, etc.) and instead opens up the space of receptivity.
- Disfavor assumptions; favor hypotheses with the negotiation process one of testing them rigorously.

On Voice Tactics

- Late-Night, FM DJ Voice: deep, soft, slow, and reassuring. Use selectively to make a point. Inflect voice downward, keeping it calm and slow. You create an aura of authority and trustworthiness without triggering defensiveness.
- Playful/positive voice: this should be your default voice. It's the voice of easygoing, good-natured person. Attitude is light and encouraging.
- Direct/assertive voice: use rarely. Will cause problems and create pushback.

On Mirrors

- Defined: Repeat the last 3 words or critical 1-3 words of what someone has just said.
- Art of insinuating similarity, which facilitates bonding. Use mirrors to encourage the other side to empathize and bond with you, keep people talking, buy your side time to regroup, and encourage your counterparts to reveal their strategy.
- Beware getting caught up in the tactical execution; the purpose of mirrors is to establish a safe bridge to facilitate open, transparent, genuine communication vs. "outwitting" or "Jedi mind-tricking" someone

On Labels

- Labels identify a perceived emotion or argument of the counterpart, phrased generally as such:
- "It seems like..." "It sounds like..." "It looks like..."
- Strip the sentence of personal pronouns; the use of "it" is deliberate to as to reduce risk that the personal motivation hijacks the convo
- Even if incorrectly labelled, the act of labeling highlights points of confusion; facilitates issue-spotting
- Label then remain silent as an invitation for the counterpart to react and respond; the silence can be uncomfortable and there will be a tendency to fill it with more explanation. Resist the temptation.

Beware "Yes" & Supplemental Notes from Jim Camp's, *Start with No* (2002 book)

- Conceive of "no" as the opening of a negotiation. Instead of worrying about "no," embrace it.
- Typically "no" signifies a temporary decision as a knee-jerk response to preserve the status quo than to introduce uncertainty.

Jim Camp, *Start with No* (2002), some complementary notes for which are presented below:

- Invite the No: "Pete, I'm not sure that anything I do fits with you. I just don't know. So if this doesn't make sense, just tell me, and I'll go on my way. Is that a bad idea?"
- Mission & Purpose must be set in the mind of your counterpart to help him/her see and decide that I am a character of great integrity and a must-have to take company to next level.
- Outcome goals, quantifiable goals, are stupid and out of your control.
- No vision, no decision: every decision is preceded by some vision in mind's eye that caused us to initiate an action
- Focus on What and How questions (cf. Voss's "calibrated questions")
- One question at a time! Keep it short. Do not stack questions.
- Nurture Reverse: "Gee that's a great question. I'd like to toss it back to you b/c I've got so many ideas buzzing in my head. What should I be aware of?"
- 3+: give counterpart multiple opportunities to say No.
- Hard Negative Strip Line: re-center the pendulum by going the other way. "Wow, this is bad. I don't know how we can ever recover from this." "You're not listening to anything I'm saying; am I wrong?"
- Soft Positive Strip Line: "Before you sign, are you sure this is something you want to do?" "That's great, appreciate your enthusiasm, but we still have a lot of challenges to work on."
- Uncover their Pain with nurturing hands
- Cost: Time = 1x, Energy = 2x, Money = 3x, Emotion = 4x. Note the emotional toll in continuing with bad negotiations / relationships. Keep the cost to a minimum on all dimensions, not just time and money
- Get past the shell game: who are the parties involved in decision making?
- Address baggage upfront, both sides

Details**On Holistic Perspective (and Complexity)**

- Way of assessing totality of risk that the world is facing in a big picture sense
- Holistic addressing of crises vs. treating problems as isolated instances (see Field Note 50_On Cynefin and Complexity)
- Implication: invoking Charles Kettering, "Problem fully understood is half solved"
 - Corollary is problem not fully understood is probably unsolvable as it leaves out critical elements.
- Goal is to understand the problem space to think through the design criteria necessary to address connected risks of magnitude
- Do these risks have underlying patterns? What is the leverage point that allows us to address the *class* of existential / catastrophic risk vs. intervening in isolation.

On Metacrisis

- Catastrophic risks ("cat risk"), including climate change, which is one of many environmentally (e.g., dead zones in ocean, biodiversity loss, pollinator loss, top soil erosion, etc.).
- Larger frame is planetary boundaries.
 - We have been running a linear materials economy that extracts from nature and has negative externalities and waste.
 - Linear materials economy connected to financial economy requiring an exponential growth yoy (referred elsewhere as "embedded growth obligation")
- AI risk arguably being the most catastrophic, near-term risk
 - AGI risk, AI optimizing for wrong things (e.g., algos polarizing the world, impairing democracy and genuine communicative interactions)
- BioTech existential risks: exponential tech is price deflationary, making nuclear level problems accessible to smaller groups.
- Collectively, the term "metacrisis" is not one cat-risk, but all of them.
- There's a clear asymmetry: "to make it through, you have to prevent all of them; to fail, you only have to have one of them happen" (~10:56 mark)

Multipolar Trap

- Anybody starts overfishing, then nobody has no reason not to overfish. And
 - First mover in tech; race to the bottom; tragedy of commons
- Metacrisis is underpinned by multipolar traps. We must address perverse incentives that create misalignment within society.
 - "A multipolar trap arises when individual actors have the incentive to take some action which is detrimental to the group as a whole ("defect" in game theory parlance) and obtain a benefit from it...other actors in the system...are then faced with the choice to either defect themselves or slide into irrelevance." (source: <https://www.worldanvil.com/w/parastellis/a/multipolar-trap-article>)

Technology Narrative & Third Attractor

- Attractor is the idea that in a complex system, we can't predict precisely but things move in a general direction
 - Natural example: pathway of raindrop on hillside. We can't predict or calculate the precise travel path of the dynamical system, but we can determine the general direction (e.g., based on the basins toward which the rain goes)
- Importantly, catastrophic risk need not be generated by some high impact action, but rather a perpetuation of the status quo given that the system has created the conditions for existential threat (occasioned by technology and its exponentiality)
 - Status quo is worst response: feeding catastrophes and dystopias at the same time; trapped and escalating the poorly designed system; catastrophes and dystopias feeding each other.
- Narrative of tech utopianism is false. The nuance is that the exponential nature of technology also distributes dangers.
- If people can make dangerous weapons, the default response is to create surveillance state. This creates dystopia risk.
- Network dynamics and Metcalfe's law tend toward natural monopolies, which is celebrated in VC, creating a system of "break things" as fast as possible in the race to create the oft-touted flywheel.



Details

Framing the Solution Space

- Framework matters. Seeing problems as independent vs. as manifestations of an underlying system makes the totality of problem appear too hegemonic, disempowering action. However, appreciating and detecting underlying patterns orients our thinking and action toward repositioning underlying structures where action has high leverage.
- Studying problem space to determine patterns allows us to move into a space of possibility.
- Forced Transparency. Solves for plausible deniability and mistruths, which addresses the multipolar trap because if you don't know what the other actors are doing, you are forced to preemptively perpetuate rivalrous dynamic.
- Information asymmetry becomes more symmetrical under transparent vs. opaque designs
- AI as a facilitator of what is uniquely human vs. disintermediation mantra. This is AI helping to address the scale issue in support of human uniqueness vs. an AI singleton model.
 - Specific example: Can we train GPT-3 to train on luminaries such that education can be delivered from e.g., Feynman and have humans to act as interface between the AI and the student? (goosebumps: a beautiful, elegant idea)
- Hope at the level of human nature.
 - Narrative of humans as fundamentally flawed is itself flawed.
 - Examples of cultures across long period of time that are designed toward peace and others funneled toward violence. Plasticity of human culture and behavior provides seed of inspiration to design system that can cultivate positive culture.
- Optimism toward the unknown unknowns and pessimism toward the specific solutions in the spirit of red team. What does it mean to commit to something you don't know how to do? That presents an optimistic commitment creates most probability of success and peace in failure. Pessimism in serve of effective optimism.
- Critique of many crypto projects is that the red-teaming of projects is too narrow and out to be applied as well to externalities that exist outside of the narrow problem/solution prompt.
 - Danger of throwing out political economy theories that have been battle-tested and deeply debated over time

Additional Breadcrumbs

- Meditations on Moloch: best article describing multipolar traps (<https://slatestarcodex.com/2014/07/30/meditations-on-moloch/>)
- * Rules for Rulers: benevolent dictators cannot exist with system driving toward corruption
- * Richard Haass on problems vs. predicaments

Details

Life Is Based Upon Contingencies. (And, So Too the Particulars of Investing & Entrepreneurship)

- Requires humility and self-awareness to admit (especially openly in high performance work domains like investing & startups) the role of chance. And then the gumption to leverage it.
 - If you are completely candid with yourself, you will soon discover how much your discoveries hinge on contingencies....[S]kill alone will not be enough, for much of the novelty in creativity is decided only when you are bold enough to thrust at chance." (63)
 - To him, biomedical research is taking one step after another into pitch darkness--not a fussy rearranging of familiar furniture in a floodlighted room. He senses the depth of his commitment to an entire life of uncertainty, testing, and challenge, to an acceptance of failure far more often than success. Yet he will take the chance." (64)
- Recall the notions of tinkering. See, e.g., Field Note 84_On Effectuation]], Field Note 85_On Effectuation Deux, Field Note 10_On Amara's Law + Exponential
 - "The investigator groping away at a major problem knows he is engaged in a trial and error business, and freely accepts its implicit 'back to the drawing board' philosophy." (65)
- There is a clear zest for life that is decidedly not passive; it is exuded when one opens to chance. There is a bias to action seen, but an action that is not independent; rather, it is contingent upon the mysteries of life, the unknown, the "pregnant void."
 - "In his quest, the investigator is kin to other explorers, pioneers, and mountain climbers. He begins his journey not realizing its full implications. Beginning, he is swept along by an exciting chain of contingencies. Rewards, apart from the stimulation of the search itself, come more as an afterthought. In the risking, he is most alert, most alive; *in the seeking, he has found.* He needs to take the chance." (65)

On Chance I

- Chance I: "good luck that occurs is completely accidental. It is pure blind luck that comes with no effort on our part." (73)

On Chance II

- Chance II: "something else has been added. Motion." (73)
- Chance II's motion concept excludes pure wasted action, but is not characterized by some fine-tuned goal-setting exercise that requires brute execution. There is a clear uncertainty in play.
 - "The action is ill-defined, restless, driving, and it depends on your basic need to release energy, not on your conscious intellect." (73)
 - Chance II's motion indicates "the posture of creativity is forward-leaning. A certain basal level of action 'stirs up the pot,' brings in random ideas that will collide and stick together in fresh combinations, lets chance operate. Motion yields a network of new experiences which, like a sieve, filters best when in constant up-and-down, side-to-side movement." (73)
- Consistent motion is key and "distinguishes Chance II; its premise is that *unluck* runs out if you persist." (73)
 - "increase the number of collisions between events" (74)
- Can be characterized as a "kinetic" movement (see discussion on p. 74 with reference to Charles Kettering, famed American investor)

On Chance III

- There is a subtly distinguishing Chance III and Chance IV. The Chance IV occurrence is more mysterious and non-linear, extending beyond the capacity for perception.
 - Chance III: "we see blind luck, but it tiptoes in softly, dressed in camouflage. Chance presents only a faint clue, the potential opportunity exists, but it will be overlooked except by that *one person* uniquely equipped to observe it, visualize it conceptually, and fully grasp its significance." (74)
 - "Chance III involves a special receptivity and discernment unique to the recipient." (74)
 - Chance III is what Louis Pasteur had in mind when he said "Chance" favors only the prepared mind." (74)

On Chance IV

- The most mysterious type of Chance, worthy of further reflection and separate treatment. Gripping this concept is like trying to hold on to wet soap in the shower.
 - Chance IV: "comes to you, unsought, because of who you are and how you behave. It is *one-man-made,* as personal as your signature." (76)

Details

On Epistemic Arrogance

- Epistemic Arrogance Defined: "our hubris concerning the limits of our knowledge" (138)
- Confidence scales (nonlinearly?) with knowledge growth, undermining the ability to convert knowledge into wisdom.
 - "True, our knowledge does grow, but it is threatened by greater increases in confidence, which make our increase in knowledge at the same time an increase in confusion, ignorance, and conceit." (138)
- Epistemic arrogance is not localized, but seemingly a human condition: "[B]ig problem of humankind: we are simply not wise enough to be trusted with knowledge." (139)
- Double Whammy. Overestimate our knowledge while simultaneously underestimating the ground of uncertainty.
 - "Epistemic arrogance bears a double effect: we overestimate what we know, and underestimate uncertainty, by compressing the range of possible uncertain states (i.e., by reducing the space of the unknown)." (140)
 - "Our human race is affected by a chronic underestimation of the possibility of the future straying from the course initially envisioned" (141)
- Distinguish between Techne and Episteme. "Epistemic arrogance does not preclude skills. A plumber will almost always know more about plumbing than a stubborn essayist and mathematical trader." (145)
- When confronted with a prediction (especially in domains characterized by fat tailed distributions, the Talebian "Extremistan"), question the error rate more than the prediction itself.
 - "No matter what anyone tells you, it is a good idea to question *the error rate* of an expert's procedure. Do not question his procedure, only his confidence." (145)

Possible Antidotes to Epistemic Arrogance

- Simplicity. "As an example of a computer using a single metric, the ratio of liquid assets to debt fares better than the majority of credit analysis." (146)
See, e.g. Field Note 22_On Heuristics, or Simplicity in Face of Complexity, Field Note 26_On 1N
- Hold the Juxtaposition. "We cannot truly plan, because we do not understand the future--but this is not necessarily bad news. We could plan *while bearing in mind such limitations.* It just takes guts." (157)
See also Field Note 36_On Quantum Investing

On Why Prediction Persists

- Information Smog-Filled World. *See, e.g., Field Note 3_On Info Smog*
 - "The more information you give someone, the more hypotheses they will formulate along the way, and the worse off they will be. They see more random noise and mistake it for information." (144)
- Notion of Ideas as Possessions Held Dearly.
 - "The problem is that our ideas are sticky: once we produce a theory, we are not likely to change our minds--so those who delay developing their theories are better off. When you develop your opinions on the basis of weak evidence, you will have difficulty interpreting subsequent information that contradicts these opinions, even if this new information is obviously more accurate." (144)
 - "Remember that we treat ideas like possessions, and it will be hard for us to part with them." (144)
- Cognitive Biases.
 - "Two mechanisms are at play here: the confirmation bias...and belief perseverance, the tendency not to reverse opinions you already have." (144)
- Tendency to Take Responsibility for Successes Only.
 - "We humans are the victims of an asymmetry in the perception of random events. We attribute our successes to our skills, and our failures to external events outside our control, namely to randomness. We feel responsible for the good stuff, but not for the bad. This causes us to think that we are better than others at whatever we do for a living." (152)

On Magnitude of Loss

- It's not merely about frequency but magnitude. It's not about how often you are right, but how big your losses are. "What matters is not how often you are right, but how large your cumulative errors are. And these cumulative errors depend largely on the big surprises, the big opportunities." (149)

Details

Defining Decision-Making

- "process whereby an individual, group or organization reaches conclusions about what future actions to pursue given a set of objectives and limits on available resources." (p. 1)
- Iteration (not merely repetition) is an attribute of sound decision-making: "This process will be often iterative, involving issue-framing, intelligence-gathering, coming to conclusions and learning from experience." (p. 1)

4 Phases of Decision-Making Process

1. Framing Phase; 2. Intelligence-Gathering Phase; 3. Choice Phase; 4. Learning from Feedback Phase
- These phases take hold after a framing / gateway decision is made relating to "(i) are we solving the right problem, (ii) who should be involved in the decision and (iii) which of the above four phase(s) deserves the most attention" (p. 1)*

On Framing Phase

- Decision Frame vs. Thinking Frame. Thinking frames inform and necessarily precede the decision frames.
- Decision frame "defines the acts, contingencies and outcomes as perceived by the decision maker" while thinking frame deals with "deeper cognitive structures, such as knowledge bases, scripts, schemata, cognitive maps and inference mechanisms that shape the decision frame." (pp. 1-2)
- Myopic decision framing occurs when the lens is narrow. "Many firms use their own past performance, or that of close competitors, as the relevant reference point for judging their success." (p. 2)
- This is a problem with investment strategies that benchmark against close comps instead of a wider set of alternatives. See, e.g., crypto investors benchmarking against BTC, which leads to the embarrassingly low standard that crypto strategies are ok to suffer 80% drawdowns.
- "The failure to adopt a portfolio perspective is another notable framing bias of the behavioral decision literature; each decision is addressed in isolation of others." (p. 2)
- * Seek disconfirming evidence: "Managers seldom approach their inference- and hypothesis-testing tasks with a mindset aimed at disproving received wisdom. Aversion to contrary evidence and institutionalized filtering reinforce old beliefs and habits. Often, a new generation of managers or successful start-up competitors are

On Intelligence-Gathering Phase

- Biases that affect this phase include: (a) overconfidence, (b) flawed heuristics; and (c) confirmation bias (p. 2)
- "Overconfidence or hubris reflects poor secondary knowledge, that is not knowing what we don't know....The overconfidence bias is especially likely to plague decisions for which little data exist and in which judgment must necessarily play a major role." (p. 2)
- "During periods of discontinuity, many established rules of thumb become outdated and dangerous when accepted as truth." (p. 2)
- The challenge is calibrating and updating heuristics, which are unavoidable in complex domains. See, e.g., Field Note 22_On Heuristics, or Simplicity in face of Complexity and Field Note 26_On IN

On Choice Phase

- Aversion to ambiguity hampers sound choice-making. "One factor especially complicates strategic choices, namely people's natural aversion to ambiguity....Uncertainty (in the sense of second-order probability distributions) and even ambiguity (in the sense of ill-defined probability distributions) is ignored by *integrating* over a presumed subjective probability distribution -- defined on the target probability. Behaviorally, however, people tend to prefer a known probability over an unknown one of equal mathematical expectation." (p. 3)
- High ambiguity projects tend to be undervalued
- Desire to seek comfort in quantification presents a danger; e.g., DCF models of "garbage in, garbage out"

On Learning Phase

- Performance-driven culture vs. learning-driven culture
- * "Those characteristics that enabled the firm to find a profitable niche in the first place -- such as creativity, flexibility, informality and tolerance of failure -- must largely be suppressed to deliver reliable results and reduce performance variance. If so, the firm's short-term performance may be optimized at the expense of its long-term survival prospects, due to lack of requisite variety." (p. 3)
- Low "N" meaning lack of large enough sample size limits learning feedback loops
- Key is to convert post-mortem lessons into pre-mortem anticipations, which requires "culture that permits mistakes and diversity." (p. 3) In this sense, risk management is decidedly cultural and requires an "ambidextrous organization, including a strong willingness to challenge the very mental models that made the firm successful." (p. 3)

Details

Starting Point

- Philosophy comes from two Greek words meaning love and wisdom.
- "A philosopher, then, is a person who loves wisdom and is dedicated to the search for meaning. The pursuit of wisdom an active, unending process of discovery. The true philosopher is filled with the passion to understand, a process that never ends." (85)
- Philosophy is "the most difficult discipline for one simple reason: it requires us to think. Unlike the sciences philosophy does not come prepackaged with absolute answers.... But philosophy has no such absolutes. Whatever truth it holds is inherently personal and individual and exists only for those who have worked for it." (84)
- Hagstrom loosely decomposes philosophy into metaphysics, aesthetics & ethics, and epistemology, focusing on the latter as it pertains to investing.

On Epistemology's Importance to Investing

- "The 'cash-value' of studying philosophy is very real. Put quite simply, it teaches you to think better. Once you commit yourself to philosophy, you find that you have set yourself on a course of critical thinking....With a perpetually open mind that relishes new ideas and knows what to do with them, you are set firmly on the right path." (103)
- "How we think about investing ultimately determines how we do it. If we can consciously adopt an epistemological framework, always considering at some level whether our thinking process is rigorous and cohesive, we can go a long way toward improving our investment results." (87)
- As a way to address complexity and uncertainties in markets, philosophical investigation is necessary to inform and reform our cognitive perceptions: "philosophy is the critical variable for understanding complexity and that any investigation of the science of complexity must also address philosophical implications." (87)
- Philosophical investigation allows us to question assumptions, effecting a process of re-definition and re-description, which are "very powerful tools capable of breaking gridlock that sometimes occurs in the pursuit of understanding....one reason we have such difficulty understanding markets is that we have been locked into an equilibrium description of how they should behave. To reach a higher level of understanding, we must remain open-minded to accepting new descriptions of systems that appear complex, whether they are financial markets, social and political systems, or the physical world." (89)

Work on Substrate Level Understanding

- "The successful investor should enthusiastically examine every issue from every possible angle, from every possible discipline, to get the best possible description--or redescription--of what is going on. Only then is an investor in a position to accurately explain."
 - I'd add that the descriptive task ought to operate at the substrate levels. That is, time is best spent working on multivalent descriptions of market substrates (i.e., at the systems level) than on the surface events that transpire on a day-to-day, fleetingly. The logic is that the latter are consequences of an underlying system structure. Failure to understand the base levels (as far down as within current capability) necessarily means a failure to truly understand the surface instantiations.
- Working on substrate-level understanding is the only way to properly engage markets given complexity that is accelerating: "We live and work in a world in which the pace of change is staggering; just when you think things can't possibly move any faster, the pace once again accelerates. In such a world, successful performance demands flexible thinking. In an environment of rapid change, the flexible mind will always prevail over the rigid and absolute." (103)

Multidisciplinary Thinking Is Demanded

- "In studying the great minds in investing, the one trait that stands out is the broad reach of their interests. Once your field of vision is widened, you are able to understand more fully what you observe, and then you use those insights for greater investment success." (103)
- "The very nature of the investigation compels us to travel over a wide field of thought crisscrossing in every direction." (qtd. Wittgenstein, 91)
- Multidisciplinary thinking, occasioned by philosophy, is a hedge to stubbornness and myopia: "Too often, we misjudge stubbornness for conviction. We are willing to risk the appearance of being wrong long before a willingness to personally confess our own errors." (96)

Against Indeterminacy

- Quoting McIntyre: "If there is order behind complex systems, and if complexity is remediable by alternative descriptions, doesn't it follow that some redescription will make that order apparent while others will not?" (88)
- "[D]isorder is nothing more than order misunderstood." (88)

Details

Cynicism Defined

- Definition: "a belief that other people are selfish, greedy, and dishonest." (p. 72)
- Skewed Perception: "When we look at the world through a cynical lens, people appear to be out for themselves, acts of kindness hide ulterior motives, and trusting others makes you a sucker." (p. 72)

Cynicism Is Self-Fulfilling

- "People with a dim view of others' actions gossip and are prone to backstabbing--behavior that brings out the worst in their colleagues, causing the cynics' suspicion and mistrust to become self-fulfilling prophecies." (p. 72)

Cynicism's Negative Consequences

- Cynicism bias is asymmetrically harmful: high downside at the individual psychological level, at the organization level (distrust, poor performance, underestimation of positive asymmetric), with upside that can be captured through critique, constructive criticism, and the balance of open-mindedness with skepticism.
- "Individually, cynics earn less money over the course of their lives, are more likely to experience depression, and are at greater risk of heart disease than noncynics are." (p. 72)

Cynicism Driver 1: Badness Attunement

- Cynicism asymmetrically focuses on the negative. It is an out-of-balance perception that steepens its own curve.
- "The greatest threat to human beings is other people, who may cheat, steal, and take advantage of our trust. Nature's answer to such social threats is to equip us with a psychological armadillo shell...we are vigilant for signs that someone may be trying to pull one over us." (p. 73)

Cynicism Driver 2: Preemptive Strike

- The premise is centered on Cobra Kai mantra: strike first, strike hard.
- "Cynics often act as though the best defense is a good offense....[C]ynical individuals--those who disagree with statements such as 'Most people are generally good' -- are less willing to donate time or money to help others." (p. 73)
- Mutually Assured Destruction. "Preemptive strikes may look savvy, but they hurt everyone involved. People reciprocate kindness and retaliate against cruelty." (p. 73)
- "Because cynics expected their partners to cheat, they were more likely to begin the game by cheating. In subsequent rounds cynics' partners were less likely to trust and more likely to cheat as well, which the researchers call 'behavioral assimilation.'" (p. 75)

Cynicism Attribute 3: Genius Illusion

- The misguided belief is that cynics are smarter. For the cynic him/herself, the internalized notion is that his/her cynicism is "hard-earned wisdom." (p. 75)
- However, the cynical posture actually produces less smart predictive and manifest outcomes. "Although they may accuse others of blindly trusting, it seems that cynics themselves blindly *mistrust.* By viewing everyone through the same dark lens, they fail to notice cues that distinguish cooperators from cheaters. Yet as long as people continue believing that cynicism is smart, cynics will be rewarded." (p. 75)

Maladaptive Organization Policies that Fuel Cynical System

- Zero-sum leadership: "stacked ranking" of performance: "top performers on each time reaped rewards while stragglers were warned or fired." (p. 75)
- Effects are information silos, active distrust, undermining of the collective, and deep dissatisfaction or *dukkha*: "Such a culture encourages people to outshine colleagues, sparking unhealthy competition. When workers are pitted against one another, they have little reason to contribute to collective ideas and are more likely to hide knowledge from their peers -- damaging relationships and killing innovation." (p. 75)
- Overmanagement. "Leaders who don't trust their people are more likely to restrict, pressure, and surveil them to ensure that they do the bare minimum and to prevent shirking and cheating -- and employees read that mistrust loud and clear. They in turn trust their organization less, feel less motivated, and are--ironically--*more* likely to game the system." (p. 75)
 - Perversion: example of "mouse jigglers" that make it seem like a worker is active at the desk where the Slack button shows up as "online"
 - Empathetic breakdown

Details

Focus on the ***Geometric* Mean of Outcomes**

- "[W]e should have focused more on raising and tightening our grouping of outcomes wherever possible (especially the worst of them) toward paths that we can say we love. In other words, we should have focused more on the geometric mean of our outcomes. After all, that grouping would likely include a better place where we would be **now**." (p. 198)
- "We are more likely to say that we should have considered **cost-effectiveness** as the main criterion in our decisions to take or not take risks. Of course, the degree of safety is part in parcel to this criterion: being very safe and very unsafe can both be very costly." (p. 198)
- "arithmetic costs can be surpassed by geometric portfolio effects" (p. 206)

Unabashed Sluggers (Eventually) Lose

- "What if Babe Ruth had been given just one at bat for this entire career (rather than his 10,617 career plate appearances--among the 50 highest in baseball history)? His optimal strategy would no longer have been his home run-maximizing, King of Strikeouts strategy. After all, it would be very unlikely that he would ever get to realize that home run expectation with only one at-bat. With one at-bat, that expectation becomes meaningless. Ruth would need a new valuation metric: His optimal strategy would have been something more like the on-base-percentage-maximizing strategy of Billy Beane." (p. 199)

Expose Yourself to Risk Deliberately, not Gratuitously

- "You aim high in a way that, even if you don't hit your target, you will also love the other things you're likely to hit instead--your alternative potential outcomes" (p. 200)
- "You get one shot at the bullseye. From the dichotomy of control in investing, you control what you can control when taking that one shot; and once the arrow has left your bow, it's out of your control. Your risk mitigation strategy should help you with both accuracy **and** precision so that you love that shot--the William Tell shot--whatever it is. It should help you fight--and **win**--the war against luck." (p. 200)

On Compounding

- "Multiplicative compounding is a **most powerful** force....It is to be harnessed and used. But when it throw you over Bernoulli Falls, then it becomes the **most destructive** force. It can make you stronger, just as long as it doesn't kill you...." (p. 202)

Nietzsche & Investing

- "Nietzsche's formula for greatness in a human being is also our formula for greatness in investing. And it is the same formula etched in stone along the banks at the crashing Rhine Falls. Far more important than any particular investment strategy is the disposition of **amor fati**. Get it, and you're way ahead of the game." (p. 205)
- Referencing Nietzsche, "My formula for greatness in a human being is amor fati: that one wants nothing to be different, not forward, not backward, not in all eternity. Not merely bear what is necessary, still less conceal it...but love it." (p. 203)
- This is not defeatist. "Rather, to Nietzsche, **amor fati** was tweaking your payoff from those rolls of the dice such that you will love whatever you get." (p. 203)
- And this is critical: "No, this is a call to **alter** that fate--not the die itself, but its effect--such that we can declare, "Thus I willed it!" (p. 204)

On Ergodicity or Single Arrow in Time

- We are not a casino, or a portfolio of our distribution of possible simultaneous returns. Rather, we are one wager compounded through time. We only get one chance, and, if we shine a bright light on that, we will avoid many mistakes--start thinking about the right things, with a better internal valuation metric: making sue this chance maximizes its chance. Tighten the potential outcomes while maximizing the most likely." (p. 204)
- It is "[w]ondrous to contemplate [alternative histories], but to us they are mere Dickensian ghosts, the ghosts of what could have been. All except for one, that is -- the one that **was**, the one that got us **here**." (p. 197)
- "Hindsight is always obvious in showing how we could have taken or not taken certain risks in order to have loved our path. This is the ubiquitous retrospective safe haven fallacy." (p. 198)



Details

Every Decision Matters

- "Every moment, every return, doesn't just happen and then, like that, it's gone. It is a mathematical fact: it stays with you *forever.*...[A] big loss today will impact your ending wealth decades from now, just as if it happened decades from now (affecting a much higher wealth). It doesn't matter when it actually happens, it reverberates like ripples on the water, and for eternity." (p. 204)
- "This is why we need to evaluate every one-period investment as if we were to parlay that investment over and over, compounded many times--for an eternity even--whether we actually will or not. Effectively--and mathematically--*we will.*" (p. 205)
- "[E]ach of the moments that occur along *this* path must be valued. They aren't all just part of some average moment; any one moment can really screw up our fate....it is the big losses that really matter to compounding...more than even the big gains for that matter." (Universa, 2019)

Misperceptions re: Risk Mitigation

- "[S]o much of risk mitigation in investing has become mere theater, superficial irony, or a punt. In that sense, while the science of probability finally broke itself free from the reactionary views of humanity on fate, risk mitigation seems to be headed back toward this nihilism of where it started. Modern finance has given upon safe haven investing as *the source* of greater investment value." (p. 206)
- "[A] cost-effective safe haven is not about *slashing* risk. To the contrary, we mitigate risk deliberately so that we can do more, not do less. We can find ourselves in the position of our great stoic Marcus Aurelius when he said, "It is not death that a man should fear, but he should fear never beginning to live." (p. 205)
- "Hiding away and taking no risk is also very risky---and, in the long-run, is another reliable way to screw up our fate. The objective is not to avoid risk, but to optimize it--to the point of appreciating and even embracing disasters." (Universa, 2019)

Details

On Successful Poker Player Attributes

- bankroll management (i.e., position sizing, bet sizing, risk management)
- practice, constant review
- "being cognitively flexible" (Id.)
- "ability to immerse oneself in the game" (Id.)
- "emphasis on adaptive strategic approaches" (Id.)
- discipline: "several mentioned that knowing the mathematics of the game was important here, not because of what it does for making specific decisions but because it gives the pro the basis for remaining disciplined." (Id.)

Emotional Control Is Paramount

- Sometimes (but not necessarily given difficulty to tease out internal state based on purely externally visible information) at odds with the general crypto Twitterverse, qualities that cultivate peak performance: "patience, control, calmness, a looking-inward mode of existence, the quiet moment of Zen-like tranquility" (Id.)
- "Tommy Angelo offered this gem: 'When I play poker, if I am hopeful that I will win, it is inevitable I will sometimes be disappointed. When I start with a good hand and I hope to win the pot, I invite disappointment. When I am disappointed, I do not play my best. At my best, I am hopeless.'" (Id.)
- "I maintain that more money is lost at poker because of poor management of emotional highs and lows than any other factor, more than stupidity, more than bad game selection, more than bad luck." (Id.)

Optimal Emotional State

- "The optimal state for a poker player to be in is the one where, when he loses he walks away from the table with the same sense of satisfaction as when he wins, where he heads home feeling as good about himself and his life as he does driving back from a football game." (Id.)

Limit Variances to Capitalize on Emotional Asymmetry

- If losses are psychologically more impactful than commensurate wins, then limiting the drawdown variance is useful to cultivate staying power psychologically.
 - ✓ Side note: perhaps this is one reason why adopting a strict Kelly Criterion to bet sizing is quite difficult.

On Fatigue, or Physical Fitness Matters

- "Fatigue is a stone-cold killer.... Fatigue compromises cognitive functions; tired people think more slowly, make more mistakes and have trouble remembering things. It diminishes your ability to concentrate; when you're tired you tend to lose track of events, particularly when they are complex. Tired people tend to screw up conditionalized situations--like those in classic 'if-then' arrangements." (Id.)
- The pattern of ignoring fatigue is "particularly common among younger players who mistakenly think that youth has immunized them to the effects of fatigue." (Id.)

Recency Bias

- "We have a lamentable tendency to downplay the significance of the historic relative to the contemporary. The best way to counter this is to keep accurate records which will help you from getting derailed by recent developments." (Id.)

Fundamental Attribution Error

- "We applaud our own supposed skill in circumstances where we've actually benefitted from dumb luck.... We have an unhappy but perfectly understandable tendency to misattribute the causes of the good and bad things that happen to us." (Id.)
- "[W]e tend to attribute causes to internal, personal factors rather than recognize the roles of external, contextual and chancy elements in the world about us. And, of course, it's closely related to our tendency to weave illusions about ourselves." (Id.)

Gambler's Fallacy

- "[W]hen a statistician says 'things tend to even out in the long run,' we have to focus on the two qualifiers in that sentence: *tend* and *long run*. 'Tend'...doesn't mean *must*. 'Long run' implies an *infinitely* long run for mathematical certainty and, frankly, you don't have that kind of time." (Id.)

Details

Problem. No specialized framework to build EVM-compatible blockchains with interoperability.

Ethereum has limitations of scaling (low transaction throughput) and low sovereignty ("shared throughput/clogging risk, tech stack not customizable, governance dependence") (p.1)

Standalone Chains

- Sovereign chains compatible with Ethereum network
- Security is tied to the chain itself and not outsourced, meaning standalone chains have their own validators.
- Tradeoff: "highest level of independence and flexibility, with the tradeoff of sometimes challenging validator pool establishing." (p. 6)

Secured Chains

- These chains avail themselves of Polygon's "security as a service" feature instead of having native validator pools
- Service can be provided via Ethereum directly (via fraud proofs or validity proofs) or professional validator pool
- Tradeoff: "high level of security, with the tradeoff of sacrificing a portion of independence and flexibility." (p. 6)

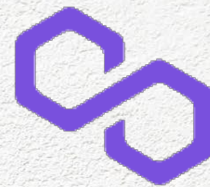
Solution Thesis. "With Polygon, any project can have it's dedicated, optimized instance of Ethereum which combines the best features of stand-alone blockchains (sovereignty, scalability, and flexibility) and Ethereum (security, interoperability and developer experience) (p. 5)

- "[P]rotocol and a framework for building and connecting Ethereum-compatible blockchain networks." (p. 2)
- Framework: efficient deployment of ETH-compatible blockchains; developer tooling & environments.
- Protocol: message passing between Polygon chains and between Polygon chain and Ethereum
- Feature set: compatibility with existing Ethereum tool environment (e.g., Metamask)

Decentralized Ethos

We don't believe in traditional companies, hierarchy and management." Query: how decentralized is the total network and along which vectors (governance, capital, devs)?

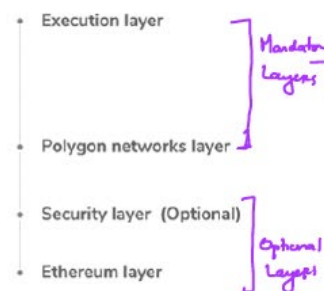
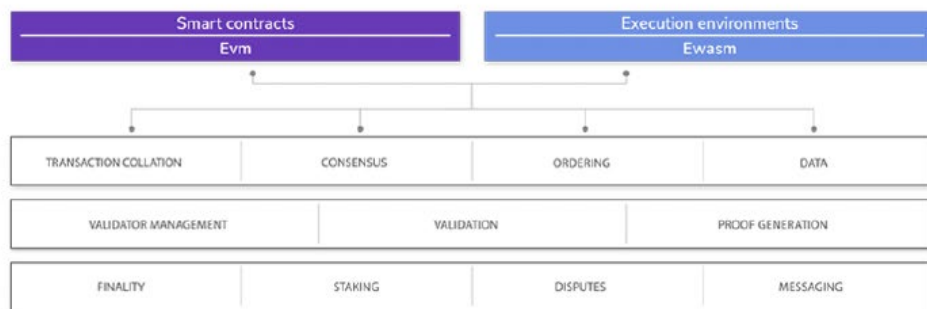
* Ask: given decentralized movement, how critical is the core team and at what stage does the core team's relevance taper?



Architecture / Design

Four layers: two mandatory

1. Ethereum Layer: implemented as smart contracts in charge of finality/checkpointing, staking, dispute resolution, messaging between ETH and Polygon chains (p. 7)
2. Security Layer: security-as-a-service / validator-as-a-service "implemented as a meta blockchain that runs in parallel to Ethereum" (p.7)
 - "fully abstract and can have multiple instances, implemented by different entities with different characteristics" including implementation directly on Ethereum (p. 7)
3. Network Layer (mandatory): functional layer, collating transactions, block production
4. Execution Layer (mandatory): execution VM, execution logic (state)



Source: Polygon Lightpaper (Feb. 2021)

Annotations: @sandeephedge



Details



ETH Compatibility

Industry dominance, established tech stack, tools, languages, standards, enterprise adoption



Scalability

Dedicated blockchains, scalable consensus algorithms, custom **Wasm execution environments**

↳ write apps on web w/o javascript.



Interoperability

Native support for arbitrary message passing (tokens, contract calls etc), bridges to external systems



Security

Modular "security as a service", provided either by Ethereum or by a pool of professional **validators**



User Experience

Comparable to Web2, **zero-gas** transactions, **instant (deterministic) transaction finality**



Sovereignty

Dedicated throughput/resources, fully customizable tech stack, sovereign governance

↑ Elaborate



Developer Experience

Equivalent to Ethereum, **no protocol level knowledge required, no token deposits, fees or permissions**



Modularity

High customizability, extensibility and upgradeability, short time-to-market, community collaboration

→ Explain. cf. Cetus

Source: Polygon Lightpaper (Feb. 2021)

Annotations: @sandeephedge

	Sidechains	Sharding	Quorum	Cosmos	Polkadot	Polygon
Ethereum Compatibility	• ▲	• ▲	•	• ▲		•
Scalability	•	• ▲	•	•	• ▲	•
Security		•			•	•
Sovereignty	•		•	•	• ▲	•
Interoperability		•		• ▲	•	•
User Experience	•		•	•	•	•
Developer Experience		• ▲				•

▲ Conditional / Limited

Source: Polygon Lightpaper (Feb. 2021)

Annotations: @sandeephedge

Further research to validate this competitive distinction.

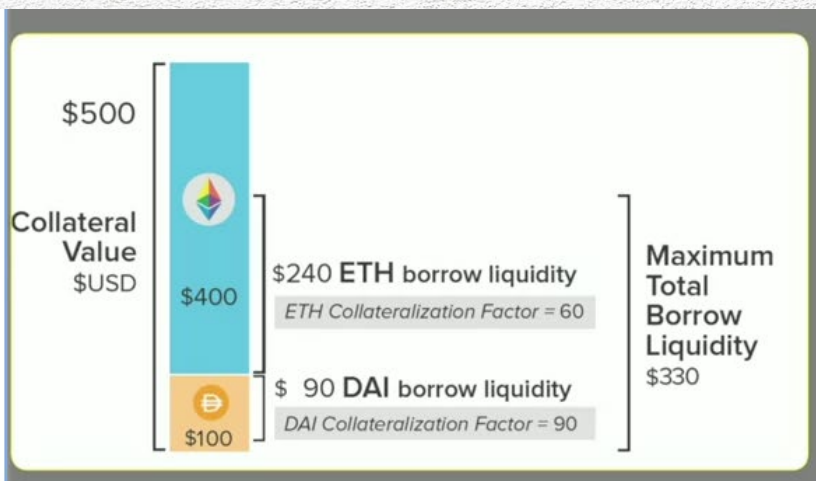
Details

Compound Overview

- Lending market with variety of ERC-20 assets for borrowing/lending
- Assets are pooled together so every lender & borrower are tied to the same variable rate (unlike DAI)
- Overcollateralization: because credit rating doesn't exist given pseudonymity, overcollateralization provides protection
- When collateralization ratio is triggered, borrower's position is liquidated
- Just as with DAI, liquidation can be executed via keeper, which receives a bonus

Collateralization Ratios

- More volatile assets have lower collateral factors
- Collateralization ratio ~ reserve multiplier
- Example: 100 DAI deposited with collateralization factor of 90. Collateralization ratio = $100/90 = 1.11x$



Deposit Amounts:

- (a) \$400 worth of ETH
- (b) \$100 worth of DAI

Collateralization Factors

- (c) 60 for ETH ($100/60 = 1.67x$ ratio)
- (d) 90 for DAI ($100/90 = 1.11x$ ratio)
- DAI factor is higher than ETH due to perceived relative stability (less volatile)

Borrow Limits:

- * (c)/100 * (a) = $0.6 \times \$400 = \240 worth of ETH
- * (d)/100 * (b) = $0.9 \times \$100 = \90 worth of DAI

Total fiat equiv borrow amount: $\$240 + \$90 = \$330$

Blended collateralization ratio = $500 / 330 = 1.51x$

Source: Campbell Harvey, DeFi Deep Dive, avail for free at Duke/Coursera, Module One: Credit & Lending

Supply and Borrow Rates

- interest is compounded nearly continuously (~15s)
- utilization rate = total borrowed / total supply; this is a parameter that feeds into the interest rate
- once close to capacity, borrowing can be discouraged / curbed by algorithmically increasing the rate non-linearly
- reserve factor: % of the borrow payments that are set aside in reserve pool as a means of self-insurance
- Facilitates short positions. E.g., deposit stable coin into Compound --> borrow ETH --> sell into open market. If ETH price falls, buy in open market at lower price to repay the loan (+ borrow cost)

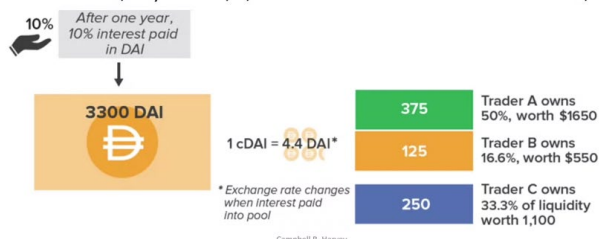
cToken

- cToken is ERC-20 token that represents share of the deposit pool; collateralized by the pool
- cToken can furthermore be leveraged, creating a multiplier

Credit/Lending: Compound

Example

- Currently, 1 cDAI = 4 DAI, but after interest accrues the ratio will change. Let interest = 10%, at year end, 3,300 DAI. Trader redeems 250 cDAI for 1,100 DAI



Campbell R. Harvey

63

Source: Campbell Harvey, DeFi Deep Dive, avail for free at Duke/Coursera, Module One: Credit & Lending



Details

Compound Governance

- Decentralized governance attaches to parameters such as collateral factor, reserve factor, base rate, slope, kink (i.e., inflection point when borrowing cost goes non-linear to curb demand)
- On Phased Decentralization: initially, developers control but was short-term mechanism with plan to go fully decentralized
- See June 15, 2020 7th Governance Proposal: model for decentralization path
- Protocol exists as long as ETH exists

Credit/Lending: Compound

Traditional Finance Problem	Compound Solution
<i>Centralized Control:</i> Borrowing and lending rates are controlled by institutions.	Compound rates are determined algorithmically and gives control of market parameters to COMP stakeholders incentivized to provide value to users.
<i>Limited Access:</i> Difficulty in accessing high-yield USD investment opportunities or competitive borrowing.	Open ability to borrow or lend any supported assets at competitive algorithmically determined rates (temporarily subsidized by COMP distribution).
<i>Inefficiency:</i> Suboptimal rates for borrowing and lending due to inflated costs.	Algorithmically pooled and optimized interest rates.
<i>Lack of Interoperability:</i> Cannot repurpose supplied positions for other investment opportunities.	Tokenized positions via cTokens can be used to turn static assets into yield-generating assets.
<i>Opacity:</i> Unclear collateralization of lending institutions.	Transparent collateralization ratios of borrowers visible to entire ecosystem.

Campbell R. Harvey

74

Source: Campbell Harvey, DeFi Deep Dive, avail for free at Duke/Coursera, Module One: Credit & Lending

Aave Overview

- 2017 launch, similar to COMP
- Rates tend to be more predictable in this protocol
- Two markets: typical ERC-20 markets and Uniswap liquidity provider tokens
- Flash loans: zero duration, no counterparty risk, cheap. Fee goes to the asset pool to provide more incentive to the liquidity suppliers
- Effectively can refinance positions across protocols depending on quoted rates
- Aave innovation is "stable rate loan"
 - * supply rate is not stable (always variable) given contingency upon the borrowing demand
 - * stable rate != fixed rate given there are adjustments in extreme liquidity crunches
- Credit Delegation: users can allocate collateral to potential borrowers to support borrowing activity

Details

Chapter 1: What Is Data DeFi?

- Central question: how can data be used as a financial asset?
- Each dataset (or data service) is linked to datatoken
 - * dataset x -- token x
 - * dataset y -- token y
- Ocean datatokens are similar to access tokens: "The purpose of a datatoken is similar to traditional access tokens (OAuth 2.0 - used in "login with Google" for example), where a third-party is granted access to server resources on behalf of the owner without sharing credentials. With these access tokens, users can access web services and applications without giving away their password." (Id.)
- Data DeFi: "where data and data services become a new financial asset class" (Id.)
- Treating data assets as financial instruments maps well to current DeFi applications, including data marketplaces, data-as-collateral to power credit creation, data-as-insurable asset, real-time data price discovery
- "This innovation creates 'data legos'; any existing dApp can work to serve our new asset class." (Id.)
- Tokens need not just be access tokens providing access to datasets; they can be financialized (cf. "over-financialization" risk; however, from an investment/trading standpoint, the risk is mitigated, if not outright solved, through position sizing, margin cushion, and risk management tools to avoid ruin)

Chapter 2: Intro to Ocean Market

- Data marketplace as a "directory of data services, where individuals and corporations alike can buy and sell data assets." (Id.)
- One-liner identity: "A marketplace to find, publish and trade datasets" (Ocean landing page)

What can you do on the Ocean Market?

- Get paid to provide access to your own data and data services
- Buy access to a private dataset instantly
- Browse the market and evaluate datasets for a fee
- Participate in the data economy by investing in datasets

Chapter 3: Creation of Datatoken on Ocean Market

- "Datatokens are like the plankton, they sustain the entire Ocean Protocol ecosystem." (Id.)
- Ocean provides the datatoken framework with the following attributes:
- Only metadata and encrypted URL pointing to the dataset are on-chain:

Make your data accessible. The data should be accessible through a URL. Files can be **hosted anywhere as long as no extra authentication is needed** on the host platform; it could be on AWS, Google Drive, IPFS, your own website, etc. The data is **never stored on the blockchain, only the metadata and the encrypted URL are.** As you can see in this example of token creation, no personally identifiable information is stored on the blockchain

- Access to dataset being sold can be time-bound (e.g., disables after 1Y)
- Datatoken pricing: fixed pricing set by data creator / provider and dynamic whereby market defines beyond a base price
- Balancer is used to effect the dynamic pricing (i.e., automated market maker + liquidity pool to be able to swap tokens)

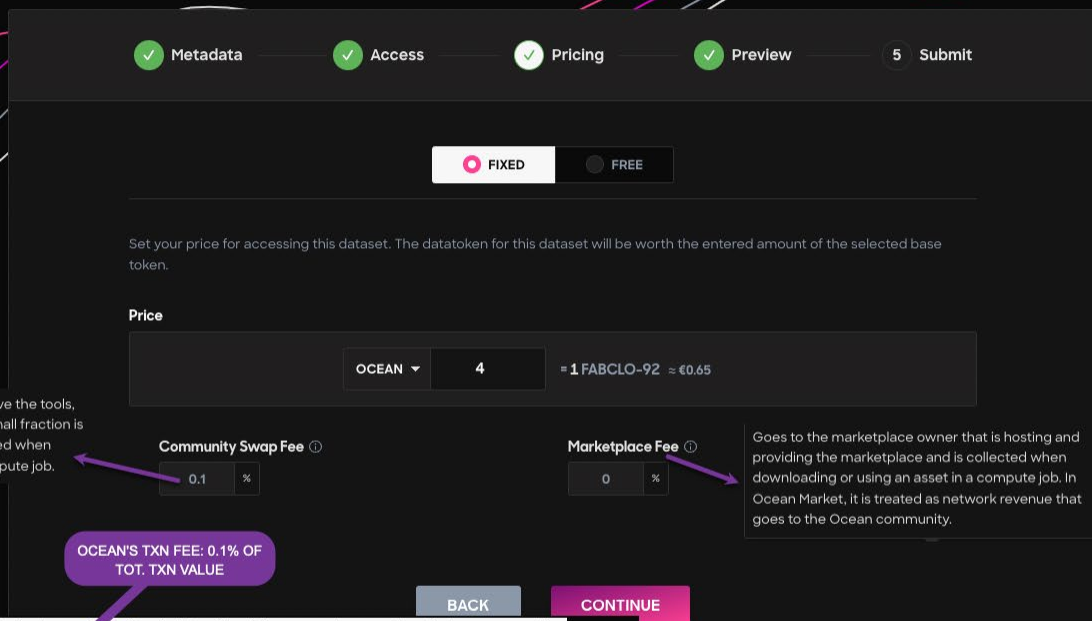


Details

• On Fees

Publish into  ETH ^①

Highlight the important features of your dataset or algorithm to make it more discoverable and catch the interest of data consumers.



Metadata Access Pricing Preview 5 Submit

☒ FIXED ☐ FREE

Set your price for accessing this dataset. The datatoken for this dataset will be worth the entered amount of the selected base token.

Price

OCEAN 4 = 1 FABCLO-92 ≈ €0.65

Community Swap Fee ^① 0.1 %

Marketplace Fee ^① 0 %

OCEAN'S TXN FEE: 0.1% OF TOT. TXN VALUE

BACK CONTINUE

Goes to Ocean DAO for teams to improve the tools, build apps, do outreach, and more. A small fraction is used to burn OCEAN. This fee is collected when downloading or using an asset in a compute job.

Goes to the marketplace owner that is hosting and providing the marketplace and is collected when downloading or using an asset in a compute job. In Ocean Market, it is treated as network revenue that goes to the Ocean community.

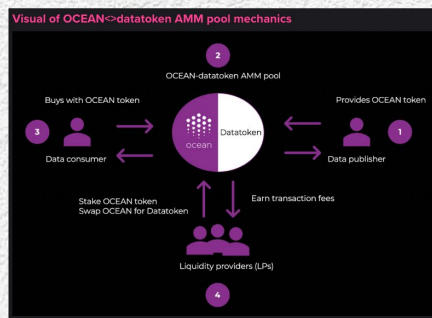
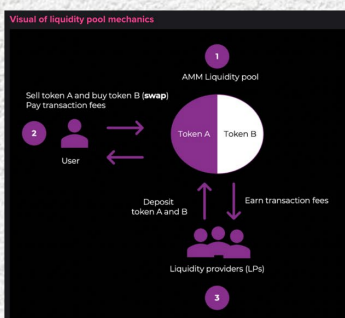
5.2 Ethereum requires the payment of a transaction fee (a "Gas Fee") for every transaction that occurs on the Ethereum network. The Gas Fee funds the network of computers that run the decentralized Ethereum network. This means that you will need to pay a Gas Fee for each transaction that occurs via the Ocean Marketplace. In addition to the Gas Fee, we have hardcoded 0.1% of the total value of the transaction for the Ocean Protocol community development fund.

Customer acknowledges and agrees that the Commission will be transferred directly to the Ocean Protocol community development fund through the Ethereum network as part of any transactions or payments.

Ocean Terms of Service, <https://market.oceanprotocol.com/terms>

Chapter 4: Zooming into Liquidity Pools

- Core utility of AMM is that there need not be transacting counterparties in an exchange, meaning illiquid or less liquid markets can be "liquified"
- Liquidity Providers (LPs) "are users which provide their tokens in the pool and can be viewed as shareholders or partners that bought shares of your dataset or service. In exchange for providing liquidity, they earn a share of transaction fees when: traders swap tokens, buyers consume the data and pay for this consumption, liquidity providers add or remove tokens from the pool." (Id.)
- Pool Initialization. Pool needs to be seeded with initial amount of tokens as a means to bootstrap liquidity.
 - * See also Field Note 78: On Token Supply, Adjustment, and Swaps for more details on pricing mechanisms.



Notes:

- * Ocean uses Balancer; liquidity provided in one token instd of token pair.
- * Fixed ratio of 70% OCEAN to 30% datatoken.
- SOURCE: <https://www.oceanacademy.io/introToDataDefi/chapter-4>



Details

Chapter 5: How To Earn on Ocean Market

- Ways to earn:
 1. Data Provider / Seller
 2. Data Purchase / Buyer
 3. Contributor: provide data to projects in the Ocean Marketplace seeking user data (enabling "decentralized data unions")
 4. Staking (benefits from % of transaction fees)
 5. Buy/Sell datatokens (investing/trading/speculating)

Balancer pools are thin (as of Sept. 30, 2022):

Pool address	Assets	Swap fee	Market cap	My liquidity	Volume (24h)
0xa6cf...f28e	50% WETH • 50% OCEAN	0.3%	\$39.6K	-	-
0xd6af...87c5	70% OCEAN • 30% BPT	0.15%	\$861.91	-	-
0x1dd2...e8ad	25% USDC • 25% OCEAN • 25% WBTC • 25% DATA	3%	\$1.1K	-	-
0xecff...0125	25% WETH • 25% ENTP • 15% OCEAN • 15% NMR • 10% LINK • 10% DATA	0.15%	\$908.68	-	-
0x8302...8443	33% USDC • 33% OCEAN • 33% ALBT	0.3%	\$563.99	-	-
0x8321...23d0	30% OCEAN • 30% MANA • 20% ENJ • 20% LRC	0.3%	\$144.72	-	-
0x1c37...791c	70% LOCK • 15% WBTC • 5% WETH • 5% OCEAN • 5% LINK	1%	\$2.1K	-	-

Balancer pools w/ OCEAN as of Sept. 30, 2022

Chapter 6: Due Diligence for Liquidity Providers

- On Impermanent Loss: loss is crystallized when you exit the pool
- Rug Pull risk: malicious data provider creates AMM liquidity pool, attracts OCEAN liquidity, then removes OCEAN from the pool, siphoning value from other LPs
- Minting Attack: LPs in pool are artificially diluted
- Make sure data publishers have skin in the game; e.g., restrictions on manipulating token supply, lock-up schedule
- Query: does the data publisher use a service like 3Box that links social media credentials to data publishers verified ETH address?
- Resource: <https://rugpullindex.com/>

Details

On Assessing People

- People are the atomic unit of a startup, and there are time-independent general requirements that leadership must possess
- Wealth should be treated as a handicap: "being wealthy is a significant handicap to an entrepreneur because success isn't absolutely essential for wealthy people, and they are therefore not driven by an urgent need to acquire and preserve cash." (11)
- The "wealth handicap" can be overcome through substantial skin in the game on part of the entrepreneur
- Leadership must be fully dedicated, meaning "should not be involved in more than one or two outside organizations, since excessive outside involvement is irresponsible and places his or her firm at significant risk." (11)
- Bias against sales background for CEO or CEO equivalent: "Although a CEO (and the rest of the team) should have some sales ability, the need for such ability pales in comparison with the need for him or her to understand finance, control, marketing, and products." (12)
- Attributes of strong CEO / leader include:
 - ✓ Intelligence + energy
 - ✓ Integrity, quality + discipline
 - ✓ Openness / transparency in actions and cultivation of culture
 - ✓ Functionally appropriate background (yet not calcified in tradition)
 - ✓ Team-building coordination and delegation skills
 - ✓ Humility
- Against the playbook of having a startup CEO that bows out in post-product/market fit stage: "Changing CEOs is similar to performing a heart transplant: it takes a long time to find a compatible donor, the operation is lengthy and complex, the body requires a long period of healing and adjustment afterward, and there are no guarantees that the procedure will ultimately be successful." (17)
- Culture of focusing on cash generation: "start-up should have a virtual reverence for cash, minimize spending (this includes keeping salaries down), and maintain a clear focus on profitability." (23)

Checklist Questions for CEO / Leadership

1. Does the CEO candidate possess the levels of intelligence, energy, ethics, and quality that are required to establish the clock and culture for the proposed company?" (17)
2. "Has the CEO demonstrated management, team-building, and leadership ability involving product development, in a resource-constrained environment, and on a do-it-from-scratch (e.g., start-up) basis?" (17)
3. "Can the CEO articulate and sell the company vision to attract the financing, engineering, and other key talent needed for the (advanced or predevelopment) seed stage?" (18)
4. "Does the CEO have extensive experience in management, and has he or she demonstrated competence in product development, marketing, and sales by adhering to the principal objectives of the seed plan?" (18)
5. "Is the CEO a leader and team builder across departments, and can he or she lead/manage the entire team and help attract key personnel at various phases of the product development stage? This will be necessary in order for the company to start building all the required functions." (18)
6. "Has the CEO been successful in attracting financing, recruiting key employees, and finding directors for the board?" (19)
7. "Does the CEO have insight into the content, scheduling, and management interdependencies of engineering and marketing in the early phases, and of manufacturing and sales in the later phases?" (19)
8. "Can the CEO function actively as a company missionary in pre-selling, negotiating strategic alliances, and lining up co-development partners during the product development stage?" (19)
9. Pre-history: "The simple tests include the team members' having worked with one another long enough to be certain that they can build a company together." (25)

Details

Principle 1: Bird in Hand, or Be Anti-Godot	Principle 2: Affordable Loss, or Pre-Define Your Risk	Principle 3: Crazy Quilt, or Get Out There
<ul style="list-style-type: none"> Begin with pre-existing means and resources vs. waiting for perfect opportunity. Who you are, what you know, whom you know. 	<p>"Evaluate opportunities based on whether the downside is acceptable, rather than on the attractiveness of the predicted upside." (x)</p> <ul style="list-style-type: none"> Equivalent to setting a stop loss (price-based and/or time-based) in trading, pre-defining risk of loss in an entrepreneurial activity is essential to ease the mind, operate with resolve within productive constraints, and set a bright line for knowing when to quit Evaluate, create, and develop ideas from the perspective of "downside risk" or "risk mitigation" Success criteria should be based on collecting commitments from stakeholders, which means effectively increasing the collective skin in the game Opportunities are created, not found. Creation requires iteratively acting and garnering feedback. This activity lies in the complex domain vs. the obvious and complicated domains (adopting the Cynefin framework, see e.g. [[FN 50_On Cynefin and Complexity]]) 	<ul style="list-style-type: none"> Interaction with potential stakeholders generates clarity (clarity is not an antecedent to interaction). * "[T]he process of interacting with stakeholders has two contrasting effects: On the one hand, with each new partner, the means of the venture increase (again, we are not talking only about financial means), enabling new possibilities. On the other hand, as commitments accumulate, the goal of the venture crystallizes and the direction becomes more specific." (160) * Seek commitments from various stakeholders. Together, the initial idea is co-created through the participatory visions, together with increasing exposure / skin in the game, collectively. * "[E]ntrepreneurship is less about selling a vision, which is a one-sided exchange, and more about co-creating a vision with others, building a mutually beneficial partnership." (170)
<p>Heavy Bias to Act</p> <ul style="list-style-type: none"> "Indeed, that job is not to wait in the shower for the moment of divine intervention but rather to get out in the world and create something. The process of creating does not happen in isolation; instead, it is a function of interacting with others, using mundane resources already at hand. Resources that may be as unattractive, common and valueless as the plastic bag by the side of the road ... until those resources get in the hands of the entrepreneur and are transformed from foul to funky. Glamorous? You decide. Valuable? Absolutely." (8) 		
<p>Heavy Bias to Act</p> <p>"One academic study found that only 28% of a sample of Inc. 500 firms had completed a formal business plan (see Bhidé, 2000)"</p>	<p>"More than 73% of Initial Public Offerings are not funded by VCs (see Gompers and Lerner, 2001 at 145)"</p>	<p>"[T]he average amount of money it takes to create a business in the US is less than \$30,000" (see Kaufmann Foundation, 2009)</p>

On the Effectual Pitch vs. the Causal Pitch

- "The causal ask is like a traditional sales pitch: You develop a vision. You figure out the resources you need to achieve that vision. You identify the individuals or organizations who can provide those resources. You craft a pitch that can induce them to give you what you want. You deliver the pitch, and you either get the resources you're looking for--or you don't."
- Thus, the causal pitch process is pinned to a "work from the end" paradigm whereby the vision is pre-determined. The task is simply resource gathering.
- "The effectual ask is the start of a conversation. Your ask may be a 'pitch' of some sort, but ultimately you want to get others to give you their pitch in return."
- The goal of the effectual ask is more flexible: it is to get others to commit to the project and help shape its direction.
- The distinction between effectual ask and causal ask may be subtle in its manifestation, but the orientation is philosophically different. The former is a flexible approach that seeks discovery and commitments vs. the latter that seeks execution of a cemented pitch.
- "The effectual ask is not necessarily a quid pro quo situation, but approaching each interaction openly and truly engaging with the other person will often lead you down unexpected paths and present opportunities for mutual benefit." (176)
- "Remember, it's about building relationships with commitment stakeholders, not about getting what you think you need at a given moment." (177)

Details

Preliminaries

- Entrepreneurs aren't different than anyone else. There is a science of entrepreneurship. Everyone can learn to be an entrepreneur because the core operation is to view things differently.
- Predictive signal for success is how one deals with failure + bias to action

Attributes of (Successful) Entrepreneurs

- "Do the doable" vs. waiting for perfect opportunity, and then keep pushing it.
- Entrepreneurial worldview sees the need for human intervention, so they don't come from a view of "deterministically written inevitability"...what we do matters (it may not be all that matters).
- Don't try to calculate all the odds first because your actions influence the odds
- Two ways of cooking, *assuming you know the basics of cooking*: (a) have a meal idea, get the ingredients, and make it vs. (b) open the fridge and see what you have first
- Ask, "would I do this even if I lose the capital?" "This looks interesting, think I'd enjoy it, so I think I can put \$50k and 6 mos of my life, so let's go and see."
- Opportunities are everywhere; it's simply about acting in small ways and pushing it to next step iteratively

Effectuation Defined

- Effectuation is a decision-making approach that rejects prediction-based protocols when dealing with uncertain environments.
- To better understand this, we can compare effectuation with standard causal rationality, which *starts with* a pre-determined goal and "works backward" to identify the best achievement means.
- Popular instances of causal thinking in business generally centers on conducting market research to *find* a pre-existing problem versus a more effectual approach of starting with (a) available means & resources (see Principle 1: Bird in Hand) and amount of capital & time at risk (see Principle 2: Affordable Loss) and then allowing an opportunity and goals to emerge contingently from interaction with diverse people with intersecting interests.

Effectuation Theory vs. Causal Theory Elaborated

- Causal approaches to entrepreneurship are goal-driven and linear.
- Common tropes include "working backwards" and "start with the end in mind." This approach may work well once product/market fit has been established and contingencies have been reduced. However, during the "0 to 1" phase, the causal model limits discovery of better alternatives and forecloses collaborative input from committed stakeholders.
- The effectual entrepreneur is high in control, low in prediction
- Effectuation shares philosophy with DevOps
- DevOps (portmanteau of Development and Operations) integrates the software development and operations teams (as opposed to the siloed nature of traditional software development), which leads to faster development cycles, continuous delivery, iteration, and tighter feedback loops.
- DevOps shares characteristics of an effectuation process insofar as it prioritizes working with readily available resources and advocating a heavy bias toward action, iteration, and collaboration.

On Entrepreneurship vs. Traditional VC Model

- Only 1/3 of IPO companies are VC funded. It's actually abnormal to think that you need VC funding to grow a successful business. Funding comes typically from customers, suppliers, distributors, and even competitors.
- Technology is useful for scaling, not building.

On Skin in the Game from Stakeholders

- Every conversation should be about getting to a commitment.
- Only when someone puts some skin in the game should you take their advice / suggestions.
- Must get ideas from your customers; don't dream up the product. Instead, listen to what the customers want. Don't do all the creative work yourself, but engage the customer in creative ways. Must have customers building your market for you.



Details

Core Effectuation Principles

Principle 1: Bird in Hand

- You don't need some elaborate idea.
- Just start with who am I, what do I know, and whom do I know? Given this, what kind of ventures can I start?
- So, you aren't starting with a market map or the expected return. Rather, the orientation is what am I willing to lose to give this a try?

Principle 2: Affordable Loss

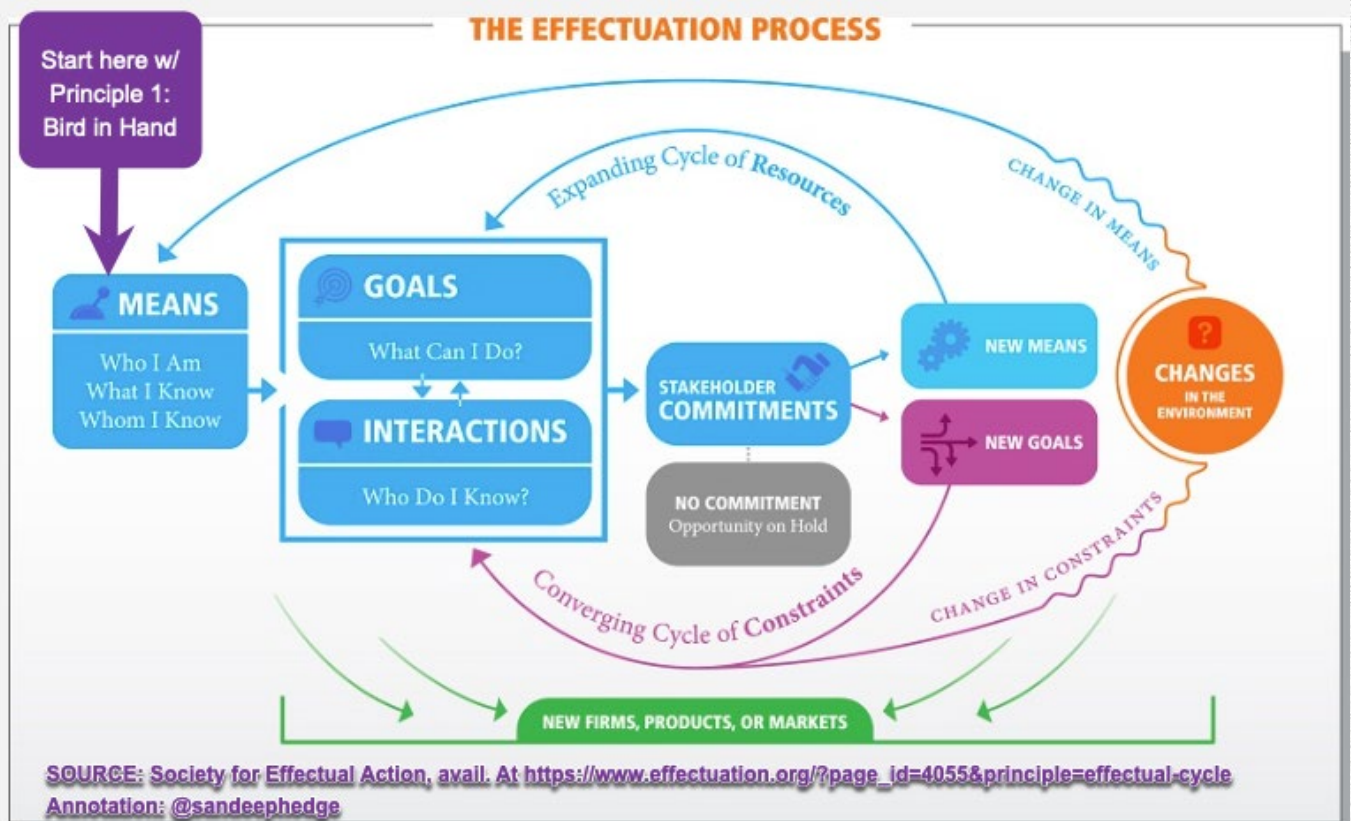
- How can you pre-commit to the loss. In other words, come up with ways you can enforce the stop loss.
- Similar to downside risk assessment and mitigation. Pre-define your loss in a binary fashion, which is a hedge to risk of ruin in the entrepreneurial domain. The key to thriving is surviving.

Principle 3: Crazy Quilt

- Go talk to a lot of people about your ideas. You aren't just gathering information and advice.
- What you are truly trying to do is to get the other person to invest their affordable loss with you.
- And, affordable loss doesn't necessarily mean money. Bring in stakeholders, each of whom is only investing what they are able to lose.
- This will generate a lot of surprises.
- You are using unpredictability as a strategy.

Principle 4: Make Lemonade

- Always bias toward optimism
- Simple yet potent as success in a non-linear domain is often about sustained action and adjustment



Details

3 Pillars of (Value) Investing	Lack of Coherent Strategies	Falsity of Being Fully Invested
<ol style="list-style-type: none"> Bottom-up approach to investment selection Absolute-performance goal Emphasis on risk, not just return <ul style="list-style-type: none"> "There are three central elements to a value-investment philosophy. First, value investing is a bottom-up strategy entailing the identification of specific undervalued investment opportunities. Second, value investing is absolute performance, not relative performance oriented. Finally, value investing is a risk-averse approach; attention is paid as much to what can go wrong (risk) as to what can go right (return)." (105) 	<ul style="list-style-type: none"> Many pay lip service to maintaining process over chasing results "Investors adopt many different approaches that offer little or no real prospect of long-term success and considerable chance of substantial economic loss. Many are not coherent investment programs at all but instead resemble speculation or outright gambling." (xiii) 	<ul style="list-style-type: none"> "Most institutional investors, unlike value investors, feel compelled to be fully invested at all times. They act as if an umpire were calling balls and strikes--mostly strikes--thereby forcing them to swing at almost every pitch and forego batting selectivity for frequency. Many individual investors, like amateur ballplayers, simply can't distinguish a good pitch from a wild one. Both indiscriminating individuals and constrained institutional investors can take solace from knowing that most market participants feel compelled to swing just as frequently as they do." (89) "Good investments ideas are rare and valuable things, which must be ferreted out assiduously." (151)
	<p>Cont'd</p> <ul style="list-style-type: none"> "Relative performance-oriented investors will typically choose to be fully invested at all times, since cash balances would likely cause them to lag behind a rising market. Since the goal is at least to match and optimally beat the market, any cash that is not promptly spent on specific investments must nevertheless be invested in a market related index. Absolute performance-oriented investors, by contrast, are willing to hold cash reserved when no bargains are available." (109) "For a value investor a pitch must not only be in the strike zone, it must be in his 'sweet spot.' Results will be best when the investor is not pressured to invest prematurely. There may be times when the investor does not lift the bat from his shoulder...." (89) 	
<p>Institutional Handicaps</p> <ul style="list-style-type: none"> Performance pressures: the need to generate always-on returns Compensation structures that amplify biases (e.g., over-leverage, over-exposure, poor hedging) "The greatest challenge is maintaining the requisite patience and discipline to buy only when prices are attractive and not to sell when they are not, avoiding the short-term performance frenzy that engulfs most market participants." (xviii) "[I]nstitutional investors become enmeshed in short-term relative performance derby, whereby temporary price fluctuations become the dominant focus." (xvi) 		<p>Critique of Indexing</p> <ul style="list-style-type: none"> "This is not to say that fundamental analysis is not useful. It certainly is. But information generally follows the well-known 80/20 rule: the first 80 percent of the available information is gathered in the first 20 percent of the time spent. The value of in-depth fundamental analysis is subject to diminishing marginal returns." (156-57)

Behavioral Edge

- Investing as such is simple; maintaining patience and discipline is challenging
- "Most investors are primarily oriented toward return, how much they can make, and pay little attention to risk, how much they can lose" (xviii)
- Risk avoidance is not equivalent to "missing out" of returns. The error in assuming so is an ignorance of the risk of ruin. "This view holds that high return is attainable only by incurring high risk and that long-term investment success is attainable only by seeking out and bearing, rather than avoiding, risk." (82)
- You must be comfortable "underperforming" most of the time to win in the end. "[P]erseverance at even relatively modest rates of return is of utmost importance in compounding your net worth. A corollary to the importance of compounding is that it is very difficult to recover from even one large loss, which could literally destroy all at once the beneficial effects of many years of investment success." (83)

Details

Maker DAO Overview

- Primary value-add: introduce crypto-collateralized stablecoin
- Stablecoin is only as stable as its peg
- DAI was one of the first decentralized stablecoins. The advantage of decentralization here is that crypto collateral does not require third party audit and vaulting; the collateral is visible in real time to anyone
- The tradeoff for decentralized stablecoins is volatility
- MakerDAO structure is a two-token model with DAI (stablecoin) and MKR (governance token)

Mechanics of DAI

- (1) User deposits protocol-approved ERC-20 token (e.g., ETH) deposited into a smart contract Vault (i.e., escrowed and visible on network)
 - (2) User mints DAI up to defined collateralization ratio
 - (3) "Debt" is created in DAI that must be paid back by Vault holder
 - (4) User can take the DAI and use it in various ways such as:
 - * sell for cash
 - * more ETH and repeat steps 1-3, creating leveraged position in ETH)
- * Over-collateralization is required to handle price volatility of underlying crypto asset.
 - * Essentially, minting DAI establishes a CDP (Collateralized Debt Position) in the centralized finance world

ETH into Vault	Mkt px (USD)	Tot. Val. (USD)	Collateralization Ratio	Amt. of DAI to Mint
5	\$200	\$1,000	150%	666.7
Source: @sandeephedge				

$$\$1,000 / 150\% = 666.7$$

- Unwise to mint the full amount allowable under the collateralization ratio because of auto-liquidation (unlike in traditional markets where margin call provides opportunity to cure the under-collateralization)
- Thus, protect yourself with a buffer, effectively increasing the programmatic over-collateralization
- In appreciation scenario of the asset deposited into Vault, you can mint more DAI to maintain the collateralization ratio (plus the self-imposed buffer)

Liquidation

- In a vaulted asset depreciation scenario, there are essentially 3 options: (a) increase the amount of collateral deposited into the Vault; (b) repatriate the underlying Vaulted asset (e.g., ETH), crystalizing the P&L; or (c) keeper (external, incentivized party) liquidates the loan
- Mechanics of Liquidation:
 - * Keeper goes into the Vault and liquidates the vaulted asset
 - * Those assets are auctioned off, generating enough money to pay down the loan
 - * Keeper receives a fee for this action
- Stabilization of DAI. There are two forces that reinforces the stability of DAI: (a) overcollateralization and (b) market actions (in liquidation, ETH is sold, DAI is purchased, creating positive pressure on DAI price)
- Stability Fee. Variable interest rate paid in DAI by Vault holders on any DAI debt created.
- DAI Savings Rate (DSR). Variable rate that any DAI holder earns on deposited DAI. The rate is compounded on a "per block basis" (hence, near continuous)
- Stability Fee is programmed to be \geq to the DSR
- DAI Debt Ceiling. If protocol reaches debt ceiling, no further DAI can be minted. This, along with other parameters, can be adjusted within the overall framework.
- Protocol Debt. If collateral drops substantially, position is closed, and protocol accrues Protocol Debt, which should (in theory) be covered by a buffer pool of DAI



Details

Governance

- MKR is governance token that controls the MakerDAO
- Holders can vote on protocol upgrades, including allowing new collateral types and adjusting parameters (e.g., collateralization ratios)
- MKR holders are incentivized to make decisions in the interest of the network because of "fork risk." Forking, occasioned by open source environments, creates an ever-present check to decisions antagonistic to community / network interests
- Global Settlement. In scenario where buffer pool can't pay back the Protocol Debt, then newly minted MKR tokens are auctioned in exchange for DAI, which is then used to repay the Protocol Debt. Effectively, an "equity raise" diluting the MKR token to raise more DAI-denominated funds.

DAI Drawbacks

- Supply constrained by most-used collateral: always constrained by demand for ETH-collateralized Debt
- No clear arbitrage loop to ensure peg

Use Case: Problems Being Solved

Traditional Finance Problem	MakerDAO Solution
<i>Centralized Control</i> : Interest rates are influenced by the US Federal Reserve and access to loan products controlled by regulation and institutional policies.	MakerDAO platform is openly controlled by the MKR holders.
<i>Limited Access</i> : Obtaining loans is difficult for a large majority of the population.	Open ability to take out DAI liquidity against an overcollateralized position in any supported ERC-20 token. Access to a competitive USD-denominated return in the DSR.
<i>Inefficiency</i> : Acquiring a loan involves costs of time and money.	Instant liquidity at the push of a button with minimal transaction costs.
<i>Lack of Interoperability</i> : Cannot trustlessly use USD or USD-collateralized token in smart contract agreements.	Issuance of DAI, a permissionless USD-tracking stablecoin backed by cryptocurrency. DAI can be used in any smart contract or DeFi application.
<i>Opacity</i> : Unclear collateralization of lending institutions.	Transparent collateralization ratios of vaults visible to entire ecosystem.

Campbell R. Harvey

Source: Campbell Harvey, Decentralized Finance Deep Dive, [avail. for free at Duke/Coursera](#), Credit & Lending (part i)
 Annotations: @sandeephedge

Details

Virtual Machine

- Basic Definition: "machines that attempt a higher level of abstraction than your usual operating system"
- Created on top of OS
- Approximate the computing power of physical machines using virtual architecture
- Benefits include accessing network resources irrespective of geography / borders

VMs and Blockchains

- VMs enable interoperability allowing one to deploy a smart contract written in a given language to operate on another blockchain without the need to learn a new programming language

EVM

- Essentially a computation engine, "not hugely dissimilar to the virtual machines of Microsoft's .NET Framework, or interpreters of other bytecode-compiled programming languages such as Java." (Ethereum Book)
- Ethereum virtual machine can be thought of as a distribute state machine (implying capabilities beyond account balances to full machine states)
- EVM is deterministic, meaning given set of inputs necessarily create the same corresponding outputs
- EVM is terminable, meaning there are checks to endless looping (e.g., gas limits). *See also* "halting problem" in [[FN 63_On Gensyn Litepaper]] and section below on "Turing Completeness"
- EVM as isolated, meaning bugs/hacks can be contained without affecting underlying protocol

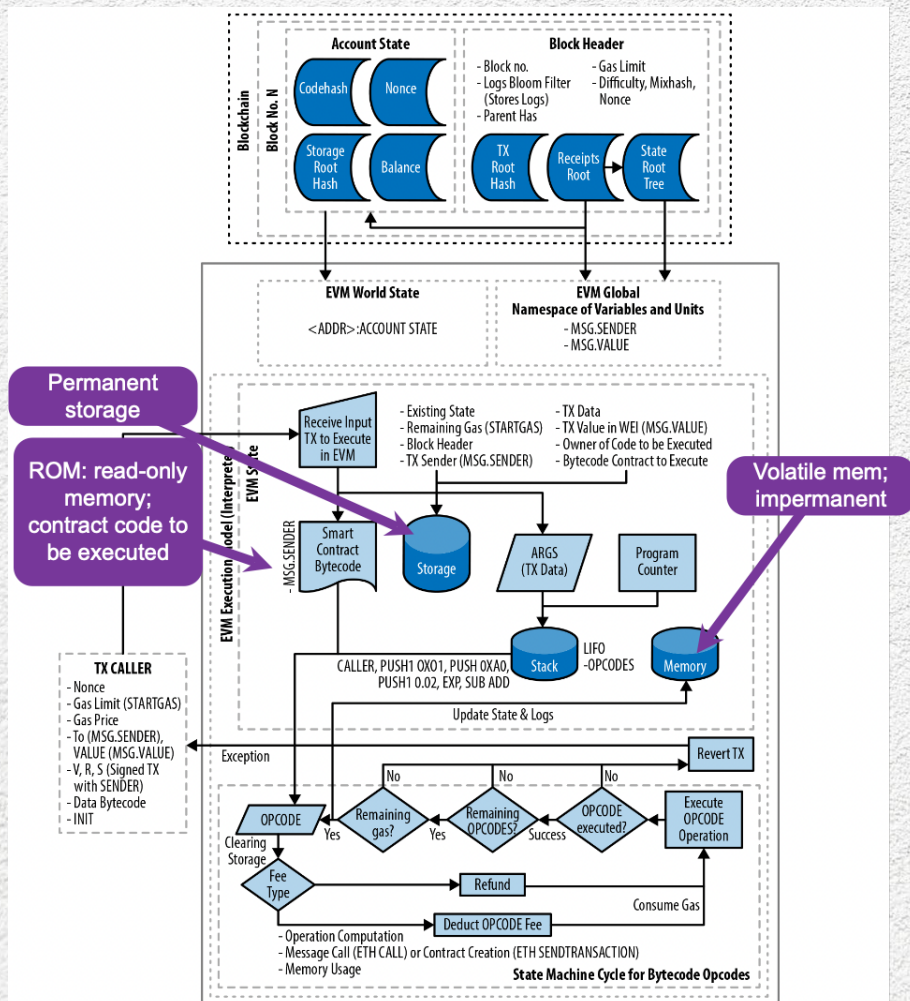


Figure 1. The Ethereum Virtual Machine (EVM) Architecture and Execution Context

Source: Ethereum Book, Ch. 13, fig. 1

Annotations: @sandeephedge

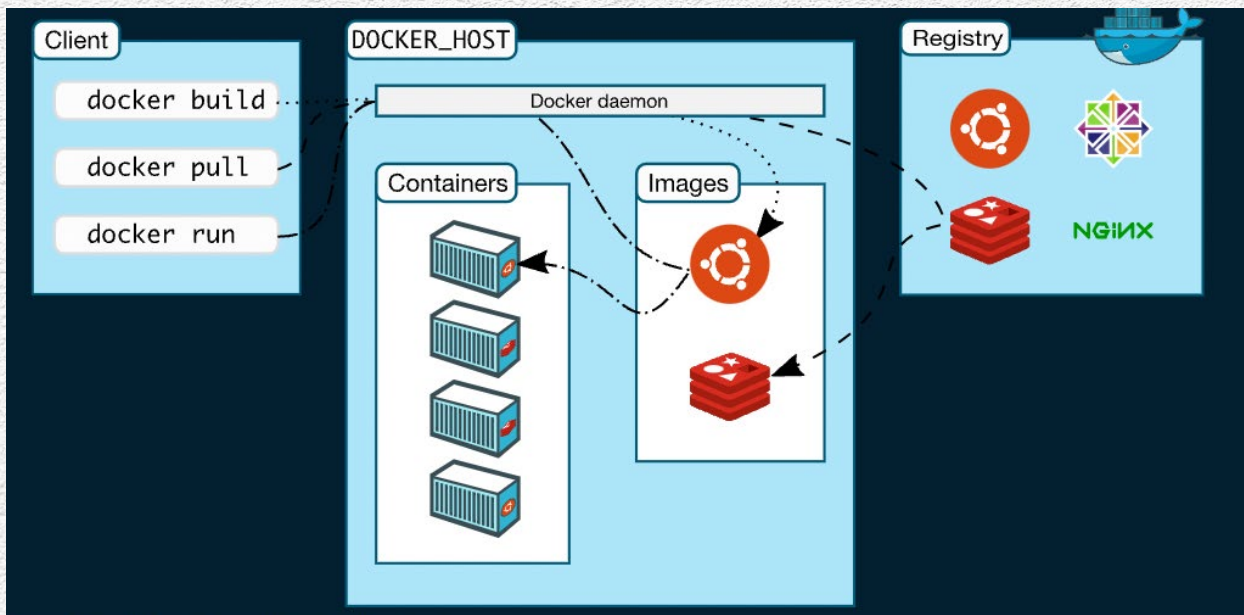
Details

Turning Completeness

- What is a Turing Machine? Turning thought of a tape divided in squares with binary logic (1s, 0s). The machine looks at tape one box at a time, and that info codes up a question or problem to solve. At any moment, the machine is in a particular state. It transforms string of 1s, 0s and into another string of 1s, 0s. Then goes into halting state. (Source: <https://www.youtube.com/watch?v=dNRDvLACg5Q>)
- A programming language is Turing complete IF it can do everything a Turing Machine can do. (1) conditional branching (if/then/else); (2) arbitrary amount of memory to get as much memory as you need. (Source: <https://www.youtube.com/watch?v=RPQD7-AOjMI>)
- Essentially, Turing-complete system can theoretically perform any logical step of a computational function
- EVM is considered "quasi-Turing complete" because "all execution processes are limited to a finite number of computational steps by the amount of gas available for any given smart contract execution" (Ethereum Book)

Docker

- Written in Go, a platform for developing and running apps separate from underlying infrastructure
- * "Docker provides the ability to package and run an application in a loosely isolated environment called a container" (<https://docs.docker.com/get-started/overview/>)
- Client-Server Relationship:



Source: <https://docs.docker.com/get-started/overview/>

Details

Adaptive Market Hypothesis

Financial markets are not static. As such, why should investment strategies be static? Catering to LP demands and biases for "coherence" are structural issues that allow the independent investor to massively outperform the so-called professional hedge funds in crypto. As well, given crypto is intertwined with venture and meme-style entrepreneurship, the extreme bias toward action ("shoot first, ask later or never") often results in financial suicide.

- "According to the AMH, profit opportunities exist when more resources are present and competition is lower. As competition increases, by natural selection, the players, who have competitive advantage over others, survive and adapt. Those who are not able to adapt disappear, reducing competition, starting the evolutionary cycle all over again." (67)

Essential Attributes of Adaptive Market Theory

1. **Risk premium is dynamic.** "The trade-off between risk and return is not stable over time"
2. **Market efficiency is relative.** "Market efficiency is a continuum; it is not simply efficient or inefficient."
3. **Adaptation is essential to survival.** "It is necessary to use adaptable investment approaches to handle changes in the market environment."
4. **Alpha decay.** "With time what once was alpha, eventually, due to innovation and competition becomes beta. Persistent alpha opportunities are not possible; fleeting alpha opportunities may be possible."

Heuristics Exist: Don't Ignore Them; Use Them Intentionally

- "[H]umans adapt heuristics or simple rules to make decisions. If humans use heuristics to make decisions and they adapt them to survive, behavioral biases are simply a natural consequence of human heuristic-based decision making." (67)
- "[N]euroscience, neuroeconomics (or even neurofinance), and psychology...supports the fact that heuristics (not utility optimization) are at the core of human decision making. Put simply, humans use heuristics that they adapt over time with experience." (68); See, e.g. *[[FN 22_On Heuristics, or Simplicity in face of Complexity]]*

Against the Home Bias: Embrace the Diaspora

- "Just as investors have a home bias for equities in their nearest and most familiar market, market players also have a home bias in the types of markets they trade.... Home bias is important because most players will have difficulty changing their allocations to other markets when opportunities dry up in markets they are familiar with or accustomed to." (71)
- "Loss aversion and prospect theory explain that investors value opportunities in relative terms and that they asymmetrically are more disappointed by losses than they are pleased with gains. Loss aversion implies that investors are more likely to have stronger behavioral reactions in the case of large losses." (71)

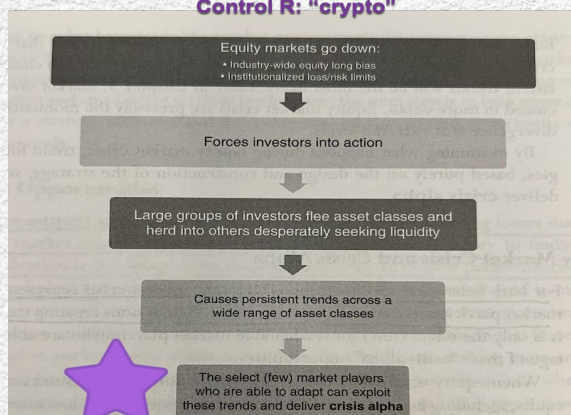
Build Investment Approaches Assuming (Hyper)Turbulence, Not Doldrums

- "Most investment strategies are susceptible to suffering devastating losses during an equity market crisis. Given this, for almost any investor, the key to finding true diversification is in finding an investment that is able to deliver performance during these turbulent periods." (72)

Capture Crisis Alpha

Previously, I've paraphrased Taleb in writing that when given the choice between being convex and being intelligent, choose to be convex. However, upon reflection, the choice is false. Being convex = being intelligent. Choosing convexity is choosing intelligence. Anything else is IYI ("intellectual yet idiot(ic)").

Control F: "equity"
Control R: "crypto"



Source: Alex Greyserman & Kathryn Kaminski, Trend Following with Managed Futures: The Search for Crisis Alpha (ed. 1) (2014), p. 74
Annotations: @sandeephedge

Details

**TABLE 4.1** Specific factors that affect adaptation and illustrative examples.

Specific Factors That Affect Adaptation

Examples

Institutional restrictions

Systemized drawdown limits
 Systemized risk limits (e.g., Basel III)
 Allocation constraints
 Asset class and market restrictions
 Margin and collateral constraints

Market functionality

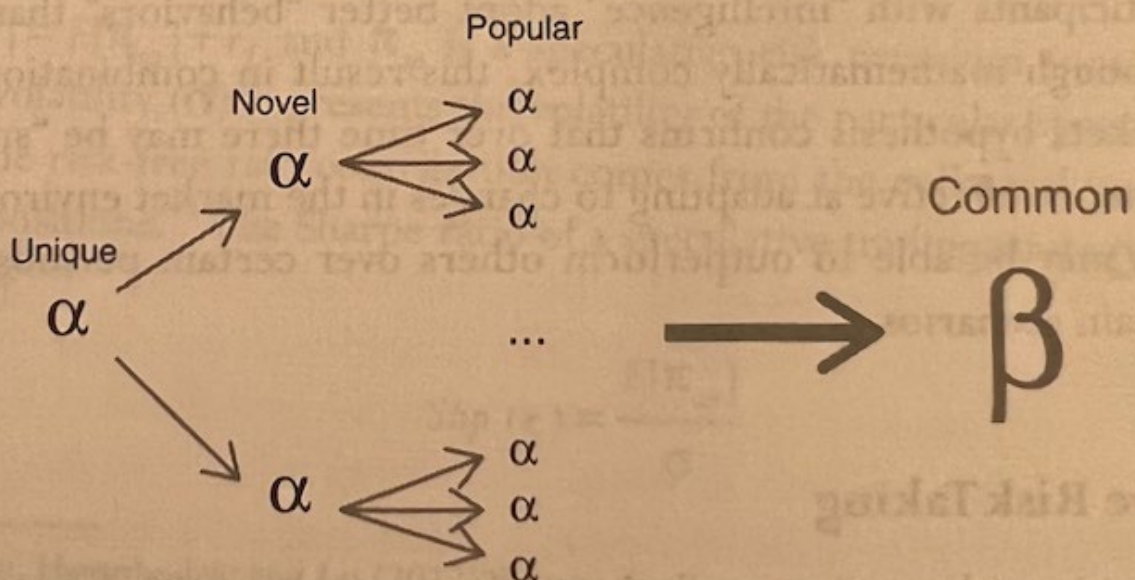
Liquidity
 Counterparty risk
 Asymmetry between long and short

Behavioral biases

Long equity bias
 Loss aversion
 Anchoring
 Herding

All of these factors exist in spades in the crypto investing environment.

Source: Alex Greyserman & Kathryn Kaminski, *Trend Following with Managed Futures: The Search for Crisis Alpha* (ed. 1) (2014), p. 69
 Annotations: @sandeephedge



Source: Alex Greyserman & Kathryn Kaminski, *Trend Following with Managed Futures: The Search for Crisis Alpha* (ed. 1) (2014), p. 75
 Annotations: @sandeephedge

Details

Hashing Function

- BTC: SHA-256
- Ethereum: Keccak-256
- These are one-way functions that are not meant to be undone. Hash does not encrypt a document.

Cryptography

- 2 types: symmetric and asymmetric
- Symmetric: same key that is used to encrypt and decrypt
- Asymmetric (most of what we do in the crypto space): public and private keys. The public key is mathematically derived from the private key. Hard to go from public key to private key but really easy to go from private key to public key.
- Asymmetric relies on elliptic curve cryptography (ECC)

Tech Big Picture: Application:

The diagram illustrates a secure communication process. It starts with a message being compressed. A random session key is generated based on mouse movements and keystrokes. The message is encrypted with this session key using symmetric encryption. The session key itself is encrypted with the receiver's public key using asymmetric encryption. The encrypted message and the encrypted session key are sent via email. The recipient uses their private key to decrypt the session key, then uses the session key to decrypt the message. Finally, the message is decompressed.

Steps

1. Message compressed
2. Random session key (based on mouse movements and keystrokes) is generated.
3. Message encrypted with session key (Symmetric key)
4. Session key is encrypted with receiver's public key (Asymmetric key)
5. Encrypted message + encrypted session key sent via email
6. Recipient uses their private key to decrypt the session key
7. Session key is used to decrypt the message
8. Message decompressed

http://www.ppt.org/doc/pptintro/

Addresses

- Public address is derived from private key.
- Private key goes through elliptic curve algorithm --> public key --> manipulated to create the public address.
- Generate private key of 256 bits (64 hexadecimal / 32 bytes) --> use Elliptic Curve Digital Signature Algorithm (ECDSA) to derive 512 bit public key.
- Sign transaction with private key
- Anyone with your public key can verify that person signing actually owns / is in possession of private key (hence public / private key pair)
- Ethereum key pair flow: public key is 512 bits --> hash public key with Keccak-256 --> take last 40 hex characters (20 bytes) as the public address, noting that when prefixed with 0x, that's 42 hex characters

Signatures & Transaction Mechanics

- Digital signatures: the way a transaction is organized. For example, you need to prove that you have the private key without revealing the actual key.

1 Tech Big Picture: ECDSA

- Private key is a number called "signing key" (SK). It is secret.
- Public key is the "verification key" and is mathematically linked to the private key

Note: Easy to generate a public key with a private key. Not easy to go the other way.

i.e., one-way function

2 Tech Big Picture: ECDSA

- Digital signature

Note: Easy to generate a public key with a private key. Not easy to go the other way.

3 Tech Big Picture: ECDSA

- Verification

Note: r not used until verification step

Consensus

- Consensus mechanism: process by which nodes agree on blockchain transaction state
- Rephrased: verify without needing to trust
- Vitalik: "The purpose of a consensus algorithm, in general, is to allow for the secure updating of a state according to some specific state transition rules, where the right to perform the state transitions is distributed among some economic set."
- Proof of Stake: right to mine doled out randomly but in proportion to amount staked (i.e., % of network participation)
- Chief challenge with PoS is the tendency to increase centralization: more staked, more influence, high probability of receiving block reward

Details

Custody

- Escrow is a basic primitive in DeFi to be able to custody the funds directly in the smart contract
- Benefits: allows for contract to retain fees, disburse incentives, facilitate token swaps, bonding curves, loans, auctions, insurance funds
- Risks: tokens can be permanently custodied in a failure case; contract needs a release mechanisms

Supply Adjustment: Burn

- Burn (reduce supply): remove from circulation
- Burning can take 2 forms: (a) manually send token to unowned ETH address (i.e., no one has private key for it) or (b) send to contract that is incapable of spending the tokens
- The latter is better given risk that the unowned ETH address in the future becomes owned
- Accidental Burns: EIP-55 (Ethereum Improvement Protocol) is basically a "checksum" that flags if address is invalid, meaning transaction will fail. And, given atomicity principle, if the transaction fails, revert to the original state.
- Purpose of Burning: increase scarcity, penalize bad action / slashing, redemption (e.g., burn token representing share in a pool to recover the underlying)

Supply Adjustment: Mint

- Increases supply, but contract specifies the rules in terms of inflation
- Incentivizes a range of user behavior

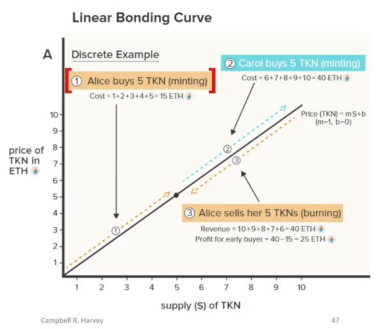
Bonding Curves

- Definition: algorithmic representation of a pricing relationship
- Can also have different bonding curves for buying and selling, creating a spread that is captured by the contract in escrow

Supply adjustment

Linear bonding curves

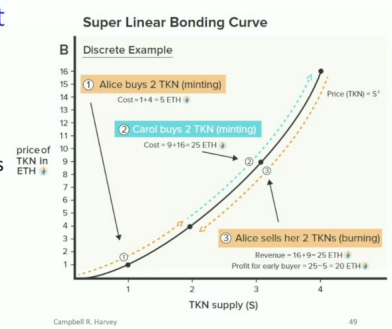
- Alice is rewarded for being an early investor



Supply adjustment

Super-linear bonding curves

- Example: $TKN = S^2$
- More extreme rewards for early investors



Incentives

- Staked Incentive: put money into a pool and receive a "bonus" based on the stake.
- Slashing: penalty / disincentive to remove portion of user's staked balance
- Keepers: class of EOA (externally owned account) incentivized to perform an action in protocol
- Keeper downside: direct rewards for keepers means that gas prices can inflate due to competition for the rewards; more keeper activity begs higher transaction demand begets higher gas
- Fees: funding mechanism to provide liquidity

Volume & Fakes on *Centralized Exchanges*

- Easy to fake volume in DeFi (e.g., just transferring tokens back and forth between wallets owned by single entity)
- Scrutinize forensically non-centralized exchanges and bias toward skepticism (e.g., real exchanges have few large trades that cluster around integer values so beware of smoothening of trade history and "normal" distributions; should be high volume correlations across exchanges so beware of anomalies; and, dissimilar spreads)
- Some suggest that only 4.5% of total volume is real on centralized exchanges

Details

Introduction & Transaction Mechanics

- 2 types of Ethereum accounts: (1) EOA (externally owned account) or (2) contract account, which is a smart contract on every node of Ethereum blockchain which can accept and disburse accounts
- Sending transaction to smart contract allows for that contract to interact with other contracts (e.g., composability and metaphor of Legos)
- Atomicity = revert to original state if intermediate transaction steps fail.
 - ✓ If a workflow includes multiple steps and one of the steps fails, the system reverts to the first step. If there is a problem with intermediate steps, then revert back to where you began.
 - ✓ This is a key attribute of DeFi because it reduces risk of failure. Specifically, "funds can move between many contracts...with the knowledge and security that if one of the conditions is not met, the contract terms reset as if the money never left the starting point." (Campbell, "Transaction Mechanisms" in DeFi Primitives course)
- Gas: transactions have gas fee that varies based on transaction complexity. More data intensity, more gas fee. This is a problem for big data applications such as AI/ML. *See, e.g., Field Note #45: On "Deep Learning Infrastructure Innovation"*
 - ✓ Gas fee is set competitively
 - ✓ If the gas price is too high, it discourages smaller transactions
 - ✓ Ideally, want a DeFi world where cost is minimal, so cost of transacting at scale is a major bottleneck that needs to be solved
- Mempool = public memory pool.
 - ✓ When transaction is proposed, it goes into a "holding area" to be validated
- MEV = miner extractable value is an issue with PoW systems.
 - ✓ The issue here is front-running as a part of the way the system works (to be distinguished from illegal front-running in centralized finance world)
 - ✓ Miner may exclude a transaction or favor a transaction. If enough miners are doing this, then the amount of money you can make by legally front running certain transactions.

Fungible Tokens

- ERC-20 parameters:
 - ✓ `totalSupply()` ## read token's total supply
 - ✓ `balanceOf(address)` ## read balance in specified address
 - ✓ `transferFrom (from address_x, to address_y, amt)` ## send amt from address_x to address_y
 - ✓ `approve(owner, spender, amount)` ## allow spender to use amount on behalf of owner
- Fungible "Equity" Token:
 - ✓ represents ownership in pool or underlying asset
 - ✓ e.g., if you have 10,000 TKN representing underlying pool of 100 ETH, 100 TKN = 1 ETH. If ETH increases at 5% p.a., 100 TKN = 1 ETH plus 5% p.a. appreciation
- Utility Token :
 - ✓ token needed to access or run contract
 - ✓ value is determined by how useful the contract is
 - ✓ utility can take form of collateral, reputation or stake, maintaining stability, pay app-specific fees
- Governance Token :
 - ✓ voting rights
 - ✓ many smart contracts have clauses stipulating how the system can change, subject to voting mechanisms
 - ✓ Beware: admin-controlled functionality belies decentralization; must check out the "decentralization upgrade process" often mediated by the governance token. Must critically assess the path toward decentralization if the bootstrapped process is still contingent upon a root level admin.

Non-Fungible Tokens

- ERC-721 as the non-fungible token standard
- Each NFT has unique ID
- Analogy: deed
- ERC-1155: doesn't require individual contract, which can be cumbersome if there are many contracts. ERC-1155 allows mixture of fungible and non-fungible, introducing notion of a "multi-token model."

Main Ideas

- **Build your own system tuned to your values, but leverage "existing code"**

Details

Root Document

- Core document summarizing the planning system at a high level
- Components of Cal's Root Document:
 - (1) Core Documents
 - (2) Productivity
 - (3) Discipline

Component 1: Core Documents

- Two types of core documents:
 - (1) Values document
 - (2) Career & Personal Strategic Plans (one plan for each)
 - ✓ Larger projects may have sub-plans and sub-routines.

System Maintenance

- Audit values 1x week that includes best practices for mental health
- Review strategic plans & sub-plans 1x week
- Idea notebook / idea storage to log thoughts on values & plans above

Component 2: Productivity

- Build weekly plan that is highly flexible vs. mechanical
- Answers: what am I working on this week, any habits to implement, etc.
- Daily: review weekly plan, calendar, value plan / orientation and then time-block the day (i.e., schedule everything into blocks)
- Flow: Strategic Plan --> Weekly Plan --> Daily Plan
- Shutdown: have clear work shutdowns and ritualize it to close open work loops

Component 3: Discipline

- Evolving list of habits to strictly follow without negotiation (e.g., workout, call quotas, etc.)
- Typically measurable, trackable

Bimodal Philosophy of Deep Work

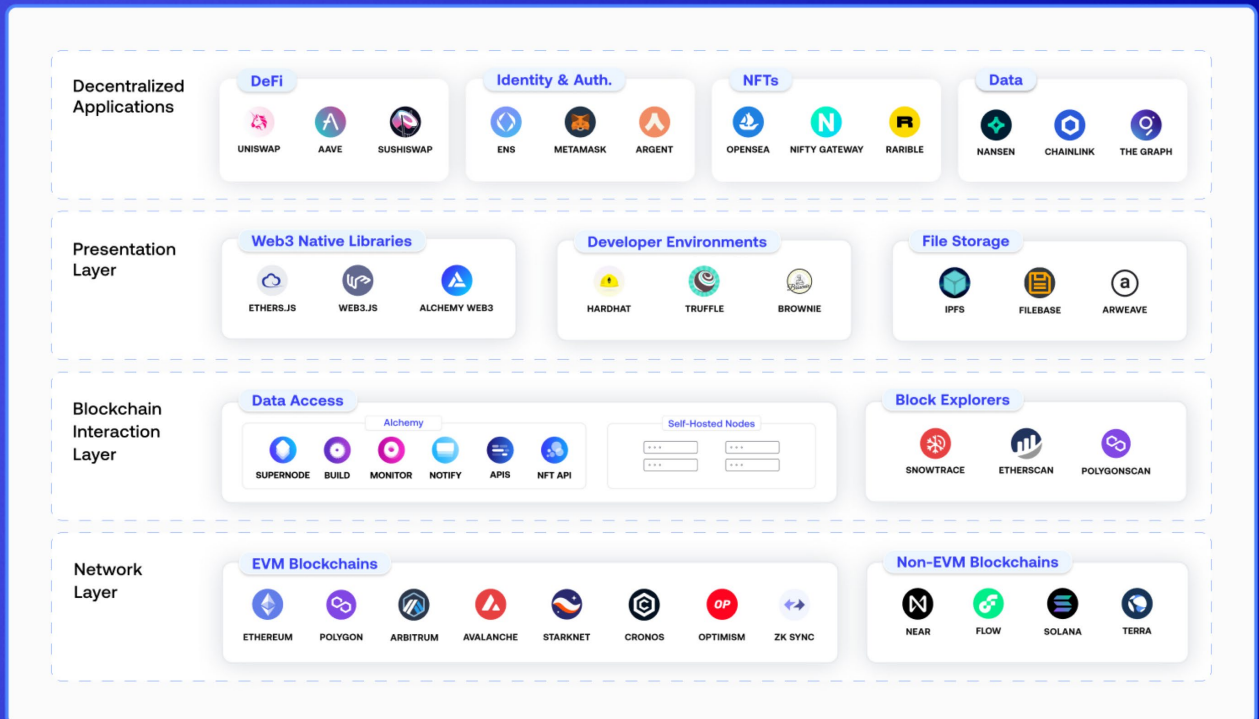
- Divide time clearly between defined stretches of focused, deliberate work and everything else
- During deep work, act monastically: intense and uninterrupted concentration
- During shallow time, focus is not prioritized
- Chain method visual "hack" -- create a visual of unbroken chain of deep work segments (e.g., tracking visually task completion for tasks that matter vs. perfunctory "check-the-boxing")

Tips and Heuristics

- Focus on wildly important. Execute against a small number of wildly important goals (note the intentional hyperbole to force one to distill the essence of meaningful activity)
- Act on lead (vs. lag) measures such as time spent in state of deep work (which can be visually tracked; see "chain method" above)
- Quit social media (see also literature notes for [[LN_Cal Newport, Digital Minimalism (2019)]]), or at a minimum establish clear procedures to limit activity; and within such limitation, act intentionally / with purpose.
- Don't reply to emails if (a) it's ambiguous, (b) it's not a question or proposal that interests you; (c) nothing really good would happen if you did respond and nothing really bad would happen if you didn't.
 - ✓ TL;DR -- send fewer emails and ignore those that are too difficult to process. Solution: you will be freed from the Panopticon that is the inbox.

Main Ideas

The Web3 Stack



SOURCE: Isaac Lau, "A Developer's Guide to the Web3 Stack," avail. online (Mar. 2022)

Details

Network Layer: EVM vs. Non-EVM

- Historically, Ethereum has been primary framework for dApp development with the EVM (Ethereum Virtual Machine) storing key info (accounts, balances, machine state)
- "Most importantly for developers, the EVM provides a framework for the storage and execution of smart contracts which allows developers to program on-chain logic." (Id.)
- EVM compatible chains share common software layer, Solidity, to run smart contracts.
- EVM-Blockchains: Ethereum, Polygon, Arbitrum, Optimism, Hermez, ZKSync, Starknet, Avalanche, Cronos
- The case for non-EVM blockchains is that the Ethereum framework is too limiting. "Generally, non-EVM blockchains are designed with data and transaction scalability from the get-go and allow for higher transactions per second" (Id)
- Non-EVM Blockchains: Flow (uses native Cadence), NEAR (uses Rust or Assemblyscript), Solana (uses Rust C, C++), Terra (uses Rust)
- "For early developers and new protocols, we believe there is a compelling argument for developing around EVM-compatible blockchains to take advantage of existing tooling, infrastructure, and developer documentation. That being said, we also recognize the niche capabilities of non-EVM blockchains for more experienced developers, their growing community base, and increased development in tooling support for early adopters." (Id)

Details

EVM-Based Developer Environments

- Selecting which chain to build on requires assessing the developer ecosystem and tooling available to support project
- "EVM-compatible chains benefit from years of Ethereum development and have a host of battle-hardened options when it comes to development environments." (Id.)
- Hardhat: "a development environment for Ethereum software. It consists of different components for editing, compiling, debugging and deploying your smart contracts and dApps, all of which work together to create a complete development environment." (Hardhat website)
 - ✓ N.B. compiling: translating human readable source code into computer-executable machine code; converting source code written in programable language into assembly code.
- Truffle: similar to Hardhat; additional tooling for frontend development; also available for VS Code.
- Brownie: Python-based development & testing framework keyed to EVM smart contracts; build off of web3.py package

Non-EVM Blockchain Developer Environments

- Flow allows ability to test Cadence-based smart contracts via VS Code
- Anchor is runtime framework for building on Solana

Interaction Layer: Read & Write

- Block explorers: window into the lower network layer; real-time and historical data retrieval (transaction data, addresses, balances, fees, and other data stored on-chain)

Nodes

- Running self-hosted node costs \$86k/y [N.B. -- validate and understand cost inputs]
- Self-hosting presents complexities: "Instead of building protocols and dApps, developers found themselves spending their engineering resources managing bugs, regressions, disk issues, CPU traffic spikes, etc. from nodes." (Id)

Frontend

- Similar to web2, current lead choice is to build using React.js library
- For data access layer, dApps use Ether.js, Web3.js (vs. HTTP request libraries like Axios and Fetch)

Storage

- Small size data can be stored on-chain, but larger size data or more complicated formats like raw audio and video need to leverage off-chain storage solutions (e.g., data stored in off-chain networks with only hashes stored on-chain; here, verification process is needed to ensure integrity between on-chain and off-chain linkage). *See [[FN 39_On Web3 without Hype (part 2)]]*
- * IPFS: usage has increased with rise of NFTs
- * See also Arweave

Details

Module 3: Problems DeFi Solves

- Inefficiency:
 - ✓ DeFi can accomplish financial transactions with high volumes of assets and low friction that would otherwise cause organizational burden for traditional finance
 - ✓ Reusable. Contracts can be reused, so that you don't have to specialize them for each application, nor do they need to be rebuilt. This is linked to the idea of composability.
 - ✓ Size of transaction is theoretically irrelevant; currently, gas price is a limiter, but should be solved.
 - ✓ No organizational overhead. Technology of inclusion and financial democracy. Once that contract is deployed, it lives forever.
 - ✓ Keepers are external participants incentivized to maintain a service for DeFi protocol. E.g., they monitor collateral posted for a transaction. If collateral dips below certain value, they liquidate the position. So, the keepers provide a service to a dApp to keep it running the way it should and reducing risk. The payment the keepers get is market based, often structured as an auction whereby you pay market price for the transaction. In traditional finance, you don't pay market rate, but rather fee bloat.
 - ✓ Forking. Creates competition and allows for superior products to emerge.
 - ✓ Vampirism. An exact or near-exact copy of DeFi platform designed to poach liquidity or users by offering larger incentives than the platform it is copying.
- Limited Access:
 - ✓ Gives underserved groups such as un- and underbanked the ability to operate in internet of value
 - ✓ 18mm in US that are unbanked
 - ✓ Problems are restricted in centralized finance
 - ✓ Generally, centralized financial organizations intentionally neglect lower profit margin portions of populations
 - ✓ In the DeFi ecosystem, while some peers have more resources than others, the transactions are treated identically as those with fewer resources
 - ✓ Removing centralized infrastructure bloat allows DeFi systems to lower lending rate
 - ✓ IDO = Initial DeFi Offering
 - ✓ DFT supply 2mm
 - ✓ Set DFT to 0.10 USDC
 - ✓ However, the 0.10 exchange rate is arbitrary; what allows for proper price discovery prior to open market trading? Or, is the price discovery simply a function of eventual efficiency in open market trading, which presumes sufficient liquidity exists?
- Opacity:
 - ✓ Traditional finance is only transparent to the regulatory, meaning we must trust the regulator
 - ✓ In DeFi, the smart contracts are open to public scrutiny
 - ✓ Staking enforces agreements by imposing a slashing penalty for inappropriate behavior & an incentive reward for proper behavior
- Centralized Control:
 - ✓ Governments and large institutions hold virtual monopoly over money supply, inflation rate, and access to investment opportunities
 - ✓ Forking is a check to centralized control because code can be relaunched with a different governance model
- Lack of Interoperability:
 - ✓ In traditional finance, difficult to integrate (e.g., not seamless to transfer funds from checking account to brokerage account even if owned by same ParentCo)
 - ✓ DeFi Legos (cliched, but metaphor is sensible): you can build a base infrastructure and others can build on top, combining existing protocols, combining them, creating new ones that plug in
 - ✓ Tokenization of non-virtual goods more subject to costs of trust
 - ✓ Networked liquidity: don't need a prime broker to facilitate



Details

Module 4: DeFi Myths and Facts

Claim: DeFi is a small part of the market compared to CeFi and will never overcome CeFi

Counterclaim: while true today, we are at very beginning at ~1% of disruption potential and vector is steep.

Claim: DeFi is hard to use and won't have widespread adoption

Counterclaim: don't rule out improvement & transformation of U/X. Internet evolution is example.

Claim: Crypto mainly used for illegal activity.

Counterclaim: initially Silk Road existed, but crypto is not fully anonymous (like cash). 79% of value of US currency is in \$100 bills but most people don't carry that denomination, implying use for illegal activity.

Claim: Gov't CBDC will put crypto out of business.

Counterclaim: doesn't solve for lack of trust and opacity. Central banks can still steal, control, manipulate.

Blockchains are not secure; e.g., government hacked ~~h~~te hackers to get back the Colonial Pipeline ransom.

Counterclaim: There was no blockchain "hack" as hackers put private keys on internet-connected computer. Also, centralized exchanges get hacked. Has nothing to do with blockchain tech; just has to do with missteps in custody.

Crypto has no fundamental value.

Counterclaim: it is possible to have value without having "fundamental" value. Also, collateralized backing for certain assets. There are many types of cryptoassets. Value can also come from services or utility. See also farther above about value stemming from intangibles.

Mining is a waste of energy.

Counterclaim: PoW vs. other mechanisms that are more environmentally friendly.

Crypto too volatile to be useful.

Counterclaim: sloppy claim because not specific. E.g., stables are not volatile in the same way. That said, reason for volatility: uncertainty over valuation and relative illiquidity. Also, volatility ought to decrease in the future but with intangible value underpinning the assets, it's hard to know.

Quantum computing will render space irrelevant.

Counterclaim: QC is not relevant for cryptographic hashing in PoW. Transition to PoS makes quantum computing even less relevant. However, QC holds promise to reverse 1-way function. But, the way we sign transactions can be changed to be quantum resistant.

Transactions are too expensive and too slow so DeFi is going nowhere.

Counterclaim: erroneous extension of status quo; assumes no change, no improvement.

Need smart phone and internet to make this work and scale.

Counterclaim: device costs and internet access increasingly commoditized.

Pump and dump and Ponzi in DeFi, making it uninvestible.

Counterclaim: not unique to crypto.

DeFi is too hard and complex to understand; plus, it's constantly changing.

Counterclaim: if you have reasonable understanding, that will open opportunities.

DeFi too risky.

Counterclaim: not unique; applies to all tech. If you want risk-free, hold negative yielding T-bills, e.g.

DeFi is too early; just wait.

Counterclaim: early is an advantage; time to get involved is sooner than later.

DeFi requires degree in CS, so avoid.

Counterclaim: not true, see most people in the space. Same quality that's needed in DeFi is the same that's needed in all disciplines: creativity.

Conclusion

- Vision = secure, efficient, immutable, and indisputable transactions and functionality via smart contracts
- Removes middle people
- World of near zero transaction costs creates new assets
- Trust in network rather than Central Bank
- Tokenization of almost any asset
- Financial inclusion

Investment Evaluation Questions

- Problem solved?
- Problem magnitude?
- Is DeFi best approach to solve?
- Competitive landscape?
- Entry barriers?
- Horizontal & vertical scaling?

Details

Key Ideas

- "[T]he market is like a jazz piece when you know all the players and know the rhythm, but you can't predict where the opening theme will be resolved." (337)
- "To grow, the market needs to build on itself; it sucks in material (new investors) from the environment; turns it into waste (takes their money); then builds on it (the change in price attracts new money)." (334)
- "By borrowing from the training techniques of the musician, the prospective master of any other elemental life-sustaining activity, such as speculation, can walk with the gods and stand with giants." (339)

CATEGORY	FOR MUSICAL MASTER (qtd. Niederhoffer, p. 339-340) n.b. numbers refer to original numbering in text.	FOR SPECULATION MASTERY (qtd. Niederhoffer, p. 339-340)
Consistency	1. Allow no day to pass without practicing with your instrument.	Study the market every day.
Tools	2. Get to know how your equipment is made and how it performs under all weather conditions.	Visit the exchanges. Be wary of rain and wind, and learn how to program in an assembly language.
Dynamics	3. Start each day of practice by playing a single tone with varying degrees of touch and dynamic quality.	Start with the stock market first.
Atomize	4. Play one hand at a time where required by technical difficulty.	One position is enough.
Self Game	5. Never fool around, even when no one is listening. Perfect practice makes perfect performance.	Don't boast or tell friends how great your system is or throw a few contracts in "just for fun."
Track	6. Whenever you make a mistake, go back and repeat the passage correctly when no one is around.	Keep a record of all your losing trades. Were you in over your heads?
Preparation prior to Performance	7. Master all the technical aspects of your play and get in condition months before your performance. Then, when you perform or compete, you'll be able to concentrate on the intellectual and refined aspects. Shading and dynamics create great performances.	Paper trade before you start. Save up adequate capital. When you trade, vary the size of the position based on your assessment of the distribution of return and risk.
Internalize	8. Play from memory. You can't soar when you're looking at a transcript. But take notes and keep a diary of all the pluses and minuses after your play.	Calculators or computers should not be consulted during the trading day.
Master Basics	10. Study the most elemental pieces and decisions from the standpoint of an expert. You will be astonished at how difficult it is to play a Czerny, or even a Clementi Sonata perfectly.	How would Soros have traded that one lot?
Refresh	11. Don't become stale trying to overcome the difficulties of a piece. Come back after a breather, and approach it from the beginning as if you didn't know it.	Take a break when you're losing.
Quiet Confidence	12. Cultivate and nurture all emotions during practice. Open the floodgates during performance. But restrain ostentatious, visible emotions when performing.	No high fives, crying, alibiing, or bemoaning missed trades during the trading day.
Study	13. Surround yourself with great masters of your art. Attend their performances. Study their books. And pay up for their lessons.	At least four books by Soros, and three about him are available.
Now	15. Don't replay the notes or fingering you missed during a performance. Once you look back, you'll be off on all the coming music.	Forget about the great prices you could have traded at. Should you enter, add, or exit <i>right now</i> ?

Main Ideas

1. We are uniquely overconfident when it comes to explanatory knowledge (knowledge that involves complicated causal links *even in* areas where complexity is minimized)
2. Some causes for this particular overconfidence include assuming that understanding higher level structure necessarily extends to subcomponents and lack of opportunities to test one's explanatory accuracy.
3. Writing and debate help with the second cause, perhaps I hold both in high regard.
4. It's important not to dismiss heuristics; the illusion of explanatory depth is problematic when using heuristics carelessly or failing to understand that a heuristic is being used to begin with (e.g., the map != territory).

Details

Thesis: Humans are uniquely overconfident when it specifically comes to explanatory knowledge

- "People feel they understand complex phenomena with far greater precision, coherence, and depth than they really do; they are subject to an illusion--an illusion of explanatory depth." (Abstract)
- "[P]eople's limited knowledge and their misleading intuitive epistemology combine to create an illusion of explanatory depth...Most people feel they understand the world with far greater detail, coherence, and depth than they really do. The illusion for explanatory knowledge--knowledge that involves complex causal patterns--is separate from, and additive with, people's general overconfidence about their knowledge and skills. We therefore propose that knowledge of complex causal relations is particularly susceptible to illusions of understanding." (20)

Causes for False Confidence in Explanatory Understanding

- Confusion of higher with lower levels of analysis. For systems that have "stable subassemblies" (i.e., units within a hierarchy that are stable enough to warrant separate analysis), there is a tendency to extrapolate that just because one understands the higher level order, that he/she also understands the lower levels.
 - ✓ "In explaining a car one might describe the function of a unit, such as the brakes, in general terms, and then turn to describing the functions of subcomponents, such as pistons and brake pads, which in turn can be broken down even further. The iterative nature of explanations of this sort may lead to an illusion of understanding when a person gains insight into a high level function and, with that rush of insight, falsely assumes an understanding of further levels down in the hierarchy of causal mechanisms." (3)
- Rarity of Production. Because we are not often in an environment where we need to rigorously test our explanations, this laziness or lack of a testing environment means we think we know and understand more than we really do.
 - ✓ "[W]e rarely give explanations and therefore have little information on past successes and failures." (3)
- Difficulty in Self-Testing Understanding. "[E]xplanations of complex causal systems have indeterminate end states (and thus more indeterminate potential end states) leading to greater difficulty in self-testing of one's knowledge." (14)

Overconfidence in Explanatory Depth is Unique

- While overconfidence is observed in studies about "general knowledge," the claim in this paper is that the overconfidence is particularly acute for explaining causal linkages in the knowledge graph about an idea.
- "[I]ntuitive theories about causally complex phenomena may have several distinctive features that may promote overconfidence." (13)
- "[T]he well-established blanket approach to overconfidence with 'general knowledge' is almost certainly misleading. Large inter-domain differences in calibration imply that structural properties of knowledge have a powerful impact on the process of knowledge assessment. 'General knowledge' is a chimera--a mythological composite creature." (26)

Utility of the Illusion, but Find Middle Ground

- Prevents us from infinite search. "Since it is impossible in most cases to fully grasp the causal chains that are responsible for, and exhaustively explain, the world around us, we have to learn to use much sparser representations of causal relations that are good enough to give us the necessary insights: insights that go beyond associative similarity but which at the same time are not overwhelming in terms of cognitive load." (27)
- "The illusion might be an essential governor on our drive to search for explanatory underpinnings; it terminates potentially inexhaustible searches for ever-deeper understanding by satiating the drive for more knowledge once some skeletal level of causal comprehension is reached." (27)

On Necessity of Writing

- Writing forces clarity and exposes logical gaps. "We frequently discover that a theory that seems crystal clear and complete in our head suddenly develops gaping holes and inconsistencies when we try to set it down on paper." (2)

Details

AI Ambiguity

- Like "Decentralization," the Term Functions as a Floating Signifier
- *see [[FN 8_On Impossibility of Decentralization]]*
- AI is an umbrella term "used to refer to a large number of related but different applications." (Source A)
- "[C]ompanies exploit the fact that AI is an umbrella term without a precise definition." (Source A)
- "This confusion is made worse by a careless vocabulary choice: in the machine learning community, the word 'prediction' refers to all applications of machine learning. So deep learning is often billed as an extraordinary tool for prediction, when prediction is in fact the one thing it's really bad at." (Source B)

AI Hype

1. **Lower Research Threshold.** "[O]ut of 400 recent papers in top AI conferences, none documented their methods in enough detail such that an independent team could verify that their research was correct." (Source A)
2. **Error Detection Is Hard.** "AI methods are tricky to use correctly, and when errors occur, they are hard to detect. As a result, there are widespread errors due to adopting AI in at least 17 different fields...This is in part because a misplaced trust in AI leads to lesser scrutiny of flashy results." (Source A)
3. **Venture Perversion.** "[V]enture capitalists who fund startups and clients who buy AI tools are swayed by these claims and don't inspect them too carefully."
4. **Cognitive Bias.** "Bombarded with hype from researchers, companies, and journalists, it's hard for any of us to evaluate claims about AI critically...[W]e share cognitive biases that make us especially susceptible to hype...[and] we tend to anthropomorphize AI." (Source A)

Analogy: claiming that AI will make render all professions obsolete is like saying typewriter will render all writers obsolete. (Source B)

AI Dogma

- The error is simple: assuming that past predicts the future and reducing all domains into "knowable" categories.
 ✓ See, e.g. [[FN 16_On Knightian Risk, Uncertainty, Profit]] and [[FN 50_On Cynefin and Complexity]]

Poor Predictive Capabilities

- Example: COMPAS attempts to use big data to tease out patterns for predictive purposes in the criminal justice system. However, "it was as good as leaving the decisions up to people with no background in criminal justice." (Source A)
- AI has efficacy in domains with little uncertainty
- "Limitations of AI are amplified when there are no clear rules, when collecting additional data is hard or impossible, and when reasonable people can disagree about the right answer." (Source A)
- "AI remains notoriously bad at nuance and context" and therefore a poor decision or policy maker. AI succeeds as an implementation agent. (Source A)
- "AI can learn where the line is. *But the hard part is drawing the line.*" (Source A, emphasis in orig.)
- Domain expertise is more than just data labeling; identifying the problem and critical variables itself is a challenge in complex domains which dominate life.
- Key issue with predictive AI is lack of explainability

On Artificial General Intelligence (AGI)

- Perhaps suffers from Amara's Law (see [[FN 10_On Amara's Law + Exponential]]) in overestimating what's possible in the short-run but underestimating in the long-run: "Note that AI experts have a more modest estimate that Artificial General Intelligence or Strong AI is about 50 years away, but history tells us that even experts tend to be wildly optimistic about AI predictions." (Source C at 6)

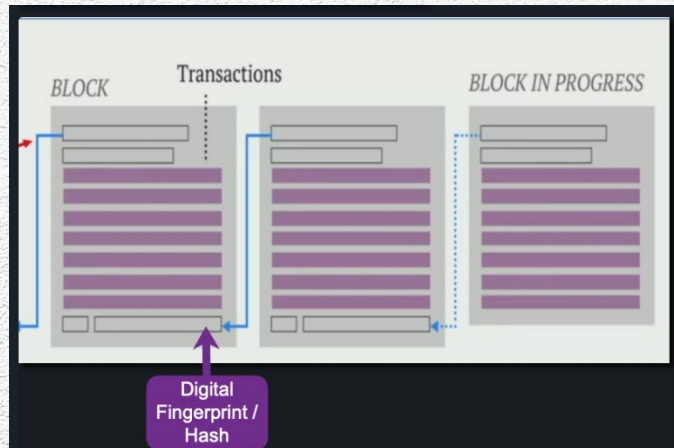
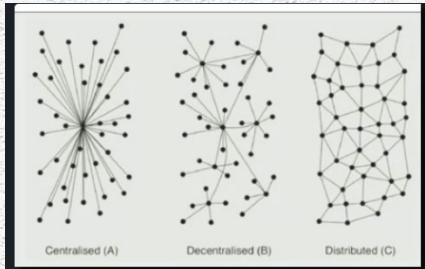
On the Need for AI Decentralization?

- AI is not some autonomous agent, but will reflect the biases and agendas of entities in control. At a broad level, this situation compels one to consider the role and impact of decentralization in AI/ML and supporting infrastructure. Does it not? *See, e.g., [[FN 63_On Gensyn Litepaper]], [[FN 65_On Raven Protocol Whitepaper]] for specific examples.*
- * AI is impressive in "perception" applications; ethical quandaries apply here: "There have been some notable failures of face recognition, but I'm comfortable predicting that it will continue to get much more accurate (and that's exactly why we should worry)." (Source C at 7)

Details

Intro

- Blockchain def'n: software protocols that allow multiple parties to operate under shared assumptions and data without trusting each other



Hashing

- Collision: two different inputs that give the same hash (e.g., hello and ohell with a simple hash / encoding algorithm)
- Cryptographic hash (e.g., SHA 256) that generates 64 hexadecimal characters. It is NOT encryption b/c it is a ONE-WAY FUNCTION (cannot be decrypted)
- Ethereum uses Keccak-256
- Nonce: number only once. Miners are basically hunting for the unique nonce.
- Antminer 17 does 53 trillion hashes per second

Technology Advantages & Disadvantages

- Verification of ownership (quickly check the immutable history recorded on chain to see if someone owns something)
- Efficient exchange of ownership (direct transactions w/o middlemen where everyone is treated with equal status)

Cryptocurrency

- Asymmetric key cryptography: private key --> cryptographic algorithm --> public key. It's a one-way operation. It's easy to go from private key to public key, but with current technology, can't go from public key to private key

Smart Contracts, Gas, Oracles

- Gas: ~ fee for cloud computing. Also, solves infinite loop problem: gas is limiter that allows contract looping to stop; if there's a coding error that causes a loop, then it would stop once gas runs out.
- Turing completeness
- gwei = giga wei = 1 billionth of ETH
- EIP = Ethereum Improvement Protocol
- ERC = Ethereum Request for Comment
- Oracle brings information outside of blockchain ecosystem into it
- The "Oracle Problem": how can we create oracle that is trust minimized while being off-chain.

Stablecoins and dApps

- Allows people to get into the crypto space as an on-ramp that's not as volatile as BTC
- Before Federal Reserve, banks issued their own currency, which was backed by collateral of public stock portfolio.
- More modern example is Eurodollar, which is US dollar account that's off-shore, so is no longer subject to Federal Reserve oversight.
- Types of Stablecoins:
 - ✓ Fiat collateralized stablecoins: USDT, USDC
 - ✓ Crypto collateralized stablecoins: MakerDAO DAI, which is over-collateralized
 - ✓ Non-collateralized stablecoins: algorithmic pegs with poor track record

Main Ideas

1. Investors are imprisoned in reading silos (they're in the Panopticon, and thus, don't realize it)
2. (Proper) reading boosts investment acumen (and don't fall into the trap of passive reading / "consumption" culture)
3. Don't underestimate the value of literature in investing
4. Critical selection and reading methodology prevents drowning in information floods
5. Every text demands answering 4 questions (each one conditional upon validation of the prior): (1) what's the text about as a whole? (2) what's being written in detail? (3) is the text true, in whole or part? (4) why do I care?
6. There are specific strategies to explore each of the four questions

Details**Proper) Reading Boosts Investment Acumen.**

- "[L]earning to be a careful reader has two enormous benefits to investors: it makes you smarter in an overall sense, and it makes you see the value of developing a critical mindset, not necessarily taking information at face value. This critical mindset, in turn, has two aspects that relate to the reading process: (1) evaluate the facts, and (2) separate fact from opinion." (117)
- Reading must be active. It is hard work. "By itself, reading is insufficient. You must put yourself--your own good brain and some of your soul--into the process, by reflecting on what you read. Indeed, the harder you work to understand and absorb the material, the more deeply embedded it becomes." (124)

On Literature (not Just Non-Fiction).

- "We shouldn't underestimate the power of literature in a world where most of the business reading consists of corporate profiles, technical manuals and self-help guides." (Quoting Ben Doty, 120)

Recurring Problem of Information Silos.

- Like traditional academia, the investing domain is often "too narrow, too territorial, too self-absorbed with parochial issues to focus on what they should be about," which is generating returns. (104)

Information vs. Understanding.

- Most of the reading in investing is centered around fact acquisition over understanding deepening.
- Investors concerned with understanding over tacking on facts to bolster a "pre-built" and biased thesis "acquire new insights through reading...[such that] not only will you substantially add to your working knowledge of various fields, you will at the same time sharpen your skill at critical thinking." (105)
- "Thoughtfully choosing investments requires the same mental skills as thoughtfully reading a book." (105)
- Heuristic. You know that you are reading for understanding instead of mere fact gathering if the material you are reading forces you to stop, think, re-read, ponder, muse.

Selection Solves Info Overwhelm.

- "For us to be able to start the communication chain with good information, we need to develop the skill of discrimination: learning to select, from the sea of information that threatens to drown us, that which will truly add to our knowledge." (109)

Critical Reading Methodology.

- According to Mortimer Adler, one must proceed with 4 structural questions when properly engaging with (non-fiction, esp.) material: 1. What is the book about as a whole? 2. What is being said in detail? 3. Is the book true, in whole or part? 4. What of it / who cares?

Question 1: What is the book about as a whole?

- The strategy to answer this threshold question is to maximize return on time, determining quickly whether the material is relevant to one's cause or not. 1. Read the Preface for author's motivation 2. Read TOC for overview 3. Read Index for familiar and unfamiliar terms 4. Systematically skim 5. Read Conclusion



Details**Question 2: What is being said in detail?**

- The strategy here is to "start with a complete but somewhat superficial reading." (111)
- Rabbit Hole Risk. Get through the book without getting bogged down in small points, unfamiliar terms; avoid the tendency to "know it all" and go off into serial or parallel rabbit holes.
- "Pay attention to what you understand and skip over the parts that are difficult. Caution: This requires concentration. Even though you are skimming the book, you should not let yourself daydream...Adler suggests we adopt the role of a detective, constantly looking for clues that will tell us if the book deserves a deeper examination." (111)

Question 3: Is the book true, in whole or part?

- The strategy to tackle this question (conditional on validation from the prior "complete but somewhat superficial read") is analytical reading, "the most thorough and complete way to absorb a book." (111)
- Three goals with analytical reading: (1) develop detailed sense of what book contains; (2) interpret contents through the author's POV; and (3) assess author's success/failure in expressing that POV.
- Thus, the imperative is to meet the author on his/her own terms, which prevents dismissing ideas that may be contrary to our existing knowledge.

Question 4: Who cares?

- The strategy here is "synoptical reading" or "comparative reading."
- Synoptical Reading: "In this level of reading, we are interested in learning about a certain subject, and to do so we compare and contrast the work of several authors rather than focusing on just one work by one author." (112)
- Versus analytical reading, in synoptical / comparative reading, we do not accept the author's POV as a pre-given; rather, the synoptical "investigation must serve your own needs." (113)

Main Ideas

1. Survival vs. Vanity. "Strategies that allow you to survive are not the same thing as the ability to impress colleagues." I've chosen poorly in the past. Now, particularly in crypto, my firm conviction (for my style) is that survival = win.
2. Build Leverage around Disaster Case. "Assume that the worst imaginable outcome will occur and ask whether you can tolerate it. If the answer is now, then reduce your borrowing."
3. Sources of Edge: informational, analytical, timing, and discipline. Of the four, discipline is the one that can be implemented here and now. Discipline starts with following no. 1 above.
4. Independence; Too Big to Win. "It is vastly less stressful to be independent--and one is never independent when involved in a large structure with powerful clients. It is hard enough to deal with intricacies of probabilities, you need to avoid the vagaries of exposure to human moods. True success is exiting some rate to modulate one's activities for peace of mind."

Details

On Survival.

- "Strategies that allow you to survive are not the same thing as the ability to impress colleagues." (Man for All Markets, xv)
- Risk of Ruin vs. Risk of Immaterial: "Betting too much, even though each individual bet is in your favor, can be ruinous....On the other hand, playing safe and betting too little means you leave money on the table." (Man for All Markets, 145)
- "The lesson of leverage is this: Assume that the worst imaginable outcome will occur and ask whether you can tolerate it. If the answer is no, then reduce your borrowing." (Man for All Markets, 309)
- On Kelly Criterion.
 - ✓ Benefits include avoiding total loss / risk of ruin
 - ✓ Basic operation: bigger the edge, larger the bet; smaller the risk, larger the bet
 - ✓ Issues / Caveats: (1) full strict Kelly Criterion causes large return variation, so practitioners may fractionalize the bets (e.g., 0.5 Kelly or less); (2) requires long time horizon; (3) "Kelly requires exact probabilities of payoffs such as those in most casino games; to the extent these are uncertain, which is generally the case in the investment world, the Kelly bet should be based on a conservative estimate of the outcome." (Man for All Markets, 311)

On Edge.

- Edge defined: "excess return after adjusting for risk, net of costs. Also, when an edge is discovered, the money that's poured into it makes the edge go away because it moves prices toward correct pricing." (Words from Wise, 10)
- According to Thorp, any one of the following allow one to effectively beat the market:
 - ✓ Information. "Get good information early. How do you know if your information is good enough or early enough? If you are not sure, then it probably isn't" (Man for All Markets, 299)
 - ✓ Discipline. "Be a disciplined rational investor. Follow logic and analysis rather than sales pitches, whims, or emotion. Assume you may have an edge only when you can make a rational affirmative case that withstands your attempts to tear it down. Don't gamble unless you are highly confident you have the edge." (Man for All Markets, 299-300)
 - ✓ Analytical Superiority. "Find a superior method of analysis." For Thorp, that included (until competition arbitrated the abnormal profits away) statistical arb, convertible hedging (and card counting in blackjack) (Man for All Markets, 300)
 - ✓ Be Early, Trade Infrequently. "When securities are known to be mispriced and people take advantage of this, their trading tends to eliminate the mispricing. This means the earliest traders gain the most and their continued trading tends to reduce or eliminate the mispricing. When you have identified an opportunity, invest ahead of the crowd." (Man for All Markets, 300)
- "I tell people that EMH [Efficient Market Hypothesis] is not true, but for you it probably is true. That is, most people don't have an edge. If you think you have an edge, it needs to be logically demonstrable. You've got to be able to defend it against a good devil's advocate. If you can't do that, you probably won't have an edge." (Words from Wise, 10)



Details

On Indexing vs. Active Management.

- "I like to put things into context of Sharpe's principle -- that active investing is zero sum game on net. For liquid asset classes like US bonds and stocks, for instance, that means that everybody who is active or not indexing are collectively a big index fund, on average. That big actively-traded 'index fund' is being managed, so it's also paying costs. So, a couple of percent is being drained out of that pool compared with the guys who are paying very low amounts for passive indexing. So, these active investors collectively have a couple percent disadvantage. So, all the institutions that are battling for an edge in those liquid asset classes aren't going to get alpha collectively. They should just index those parts of the portfolio" (Words from Wise, 7)

On Peace of Mind and Independence.

- "But such restraint requires some intuition, some self-knowledge. It is vastly less stressful to be independent--and one is never independent when involved in a large structure with powerful clients. It is hard enough to deal with intricacies of probabilities, you need to avoid the vagaries of exposure to human moods. True success is exiting some rat race to modulate one's activities for peace of mind." (Man for All Markets, xvi)
- "[M]ost stock-picking stories, advice, and recommendations are completely worthless." (Man for All Markets, 147)

Details

Evolution of Finance

- Barter is early example of p2p transactions, but it is highly inefficient in that one needs perfect match (the "matching problem"), which is what money as a form of exchange solved.
- Purposes of money:
 - ✓ Primary purposes: Medium of Exchange (allows for non-barter transactions, solving the matching problem) and Unit of Account (a way to compare the value of various goods & services)
 - ✓ Secondary purposes: Store of Value (value can be retained instead of decaying e.g., food) and Transfer of Value (easy to transfer)
- Traditional Attributes of Money:
 - ✓ Durability
 - ✓ Portability (gold is not portable, let alone security of the move)
 - ✓ Divisibility (fractional units)
 - ✓ Uniformity (versions of the same currency have same value; dollar printed today = tomorrow)
 - ✓ Limited Supply (unlimited supply means zero value)
 - ✓ Acceptability: legal tender for all debts, public & private
 - ✓ Stability: if unstable, people will seek alternatives
- Brief History of Money:
 - ✓ 9,000 BCE Barter in Egypt
 - ✓ 600 BCE Coins in Lydia
 - ✓ 1290 Banknotes from China (Marco Polo then introduced to Europe), first paper currency
 - ✓ 1871 e-Money: first wire transfer from Western Union; 3% fee back then. We've gone 150 years w/o greatly reducing the costs
 - ✓ 1950 Credit Cards via Diners Club
 - ✓ 1967 First ATM introduced by Barclays
 - ✓ 1983 Telephone Banking
 - ✓ 1994 Internet Banking
 - ✓ 1997 Contactless Payment via RFIDs
 - ✓ 2005 Chip & Pin introduced with credit cards
 - ✓ 2008 Bitcoin -- 10/31/2008 White Paper; 1/3/2009 Genesis Block
 - ✓ 2014 Apple Pay as a more secure pay vs. credit card given facial / thumbprint
 - ✓ 2021 all leading banks have blockchain initiatives

Can Money Have Intangible Value?

- Example: Iraqi Swiss Dinar was currency of Iraq until first Gulf War in 1990 (plates made in Switzerland, printed in UK). Iraq was then split into 2 regions: north (Kurds) and south (Saddam) Because of eventual sanctions, there was import ban into Iraq, so UK couldn't send freshly printed Dinar into Iraq. So, Central Bank of Iraq told citizens that it had 3 weeks to exchange Old Dinar for New Dinar. However, the Kurdish north continued using the Old Dinar. Saddam cranked printing press to finance the regime and the exchange of the Saddam New Dinar was 300 to 1 Old (unbacked) Dinar.
- Insight: the old Dinar still had value even though totally unbacked.
- Other examples: stone currency in Island of Yap whereby the stones didn't have fundamental value but were still used.
- The message is that there is a difference between tangible and intangible value.
- US Dollar has tangible value because it has legal tender and must be accepted; government can tax you & you must pay in USD; consequence (if you refuse to accept USD, you can be jailed)
- Other forms of intangible value: IP, R&D, patents, specialized software, trademarks, customer lists.



Details

Overview of CeFi Problems

1. Centralized Control

- * Centralization of banking system and centralization of big tech.
- * *Centralization of Finance and Centralization of Commerce (viz. e-Commerce)*

2. Limited Access

- * 1.7bn unbanked and billions underbanked
- * As alternative, entrepreneurs are forced to use credit card to finance business w/ extractive rates, hampering growth

3. Inefficiency

- * 3% for a credit card swipe, part of which gets passed on to the consumer in price
- * 5-7% wire transfer fee
- * 2-day settlement for stock transaction
- * Slow transfer of funds
- * Fraud, chargebacks, insecurity
- * No micro transactions
- * Difficult to get paid; difficult to receive funds on internet

4. Lack of Interoperability

- * Siloed institutions
- * Hard to move money from one bank to another
- * Hard to move money from bank to non-bank
- * *Question: what about versus tech firms like Plaid that attempt to interconnect? Is it centralization alone?*

5. Opacity

- * Bank customers don't know the health of the bank
- * Must rely on costly regulation and promise of bailouts
- * Little transparency

Impact of Problems

- Missed growth opportunities. Cost of capital too high versus ROI for entrepreneurs. E.g., if bank won't lend to entrepreneur but instead up the credit card limit with a 24% rate, then the entrepreneur's 25% ROI projection is immediately hampered.
- Inequality of Opportunities.
 - ✓ Projects should be financed based on the quality of the idea and soundness of execution plan, not the incumbency advantage of big players
 - ✓ Many have no access to internet commerce to buy or sell
 - ✓ Given unbanked / underbanked, opportunity is unevenly distributed

Early Centralized P2P

- Precedent: Forexter.com, which matched customers 1:1 eliminating the bank spread and only offering bank a small fee for the matching service.
- Precedent: "dark pool" trading such that large block transactions can be traded p2p
- AT: Fintech (PayPal, Zelle, Stripe, Plaid, etc.). They can only go so far b/c they are using the legacy banking infrastructure, meaning the 5 problems resurface: **CLIO (centralized, limited access, interoperability, inefficient, opaque)**

Crypto Origins

- Stuart Haber and Scott Stornetta (1991) invest blockchain idea, which introduced time stamping of documents ("How to Time-Stamp a Digital Document")
- Adam Back (2002) invents Proof of Work, based on key paper by Cynthia Dwork and Moni Naor (1992) aimed at eliminating spam/junk mail where it required doing some work prior to sending email, which is no biggie on small scale, but infeasible at scale.
- Satoshi Nakamoto (2008) put these ideas together.



Details

- Bitcoin Features
 - ✓ Eliminated double spend / "right click" problem that doomed digital currencies prior
 - ✓ Censorship resistance: every transaction is kept on immutable ledger and distributed across many computers
 - ✓ Cryptographic or Algorithmic scarcity: 21mm bitcoin limit; last coin mined 2140
 - ✓ User sovereignty: only owner determines how to spend it; nobody else can do it for you because you have the keys
 - ✓ Portability: can send / receive quickly
- Comparison to Fiat
 - ✓ USD since 1971 has been pure fiat / floating
 - ✓ Demand comes from: (a) taxes, (b) purchase of goods denominated in USD; (c) repayment of debt in USD
 - ✓ Economic expansions / contractions impact value
 - ✓ Fed has ability to inflate currency Bitcoin Features
- Ethereum
 - ✓ Founded by Vitalik Buterin in 2015
 - ✓ Allows for running of computer programs / programmability
 - ✓ Ethereum = distributed computational platform via smart contract platform Bitcoin Features
- dApps
 - ✓ dApp puts people together in p2p manner without centralized intermediary

Main Ideas

- Most traders/investors spend most of their time looking for entry signals, but fail to account for two far more critical pieces of a well-designed trading/investment program: psychological well-being and bank roll management (the two are indeed positively correlated)
- These two areas cover a range of topics from prior Field Notes: value of heuristics, avoiding risk of ruin, hedging, interdisciplinary thinking, convexity over analysis (both are important, to be sure, but if you had to choose one, choose convexity over being classically smart), sidestepping the anvil of info overload, and position sizing.
- To restate the thesis: psychological state has an outsized impact over technical acumen; and risk management principles--while decidedly less interesting at virtual cocktail parties than selectively parroting views from the latest super hot crypto twitter thread--have an overwhelming impact on trading/investment success.
- Most (perhaps, all) trading/investing errors are due to thinking you know what will happen next. (See also Field Note 58: On Mandelbrot's 10 Heresies of Finance)
- In a nearly 5 hr. seminar by Mark Douglas (see also The Disciplined Trader (1990) and Trading in the Zone (2000)), the essence of successful trading/investing is pegged to the above areas.

Details

On Four Skills

- Learn to identify an edge: this is the "easiest"--or more accurately, the easiest area in which to fool oneself--and thus, where most people put their focus
- Learn to think and function in probabilities: "think from the market's perspective, not your own"
- Learn to identify and stop self-sabotaging behaviors
- Recognize "trading euphoria"--a riskless state of mind--and stop trading/investing

On Money Motive

- Successful traders/investors have transcended the money game. Indeed, trading/investing is a form of self-expression. Markets are the canvas upon which to paint one's worldviews.
- Mental flexibility and not caring intrinsically about the pecuniary reward are key ingredients to success

Think in Probabilities

- Edge: simply means a higher probability outcome
- Putting money into your account is a function of execution, not analysis
- Only the best traders/investors truly accept the risk (beyond words); they are totally reconciled to the risk with no conflict
- Think of losses as simply the cost of doing business
- Thinking in probabilities means fully understanding: (a) anything can happen; (b) every moment is unique (even while in the trade); (c) random distribution between wins and losses in any set of variables that define an edge; (d) you don't need to know what will happen for consistent results (e.g., strong form of prediction is not required); (e) edge is a higher probability of one thing happening over another

Trading Fears Decomposed

- Fear of being wrong: if you fear being wrong, you will put more significance on upticks because they will make you feel better at the expense of counter evidence. You'll get out of this trade when pain of losing one more dollar is greater than the pain of being wrong.
- Fear narrows our perception so as to create the feared outcome
- You can't just put a stop in the market (because you can move it and will be tempted to do so); you'll have to be at total peace with the loss; completely reconciled with losing money
- All trading errors are due to thinking you know what will happen next.
- Identify the dysfunctional beliefs that prevent me from seeing the neutral nature of the up and down ticks. What causes me to perceive them that taps into fear? Then, draw out the energy from these belief systems and feed them into beliefs that serve my purposes.
- Trade from a carefree mode without fear, which limits your attention and openness / access to what you have learned



Details

Additional One-Liners and Tidbits

- Risk / Reward ratio of 3:1
- Progression and further development: increase position sizes
- Courage is its own reward
- When monitoring thoughts, ask, "Is this an expression of who I am / want to be? Will doing x contribute to my preferred belief to another belief?"
- Trade symmetrical markets
- Take the easy and obvious trades. Don't complicate.
- Affirmations: speak power to them yourselves.
- Self-Discipline: it's not a personality trait; it's just a tool. Once the countervailing energy dissipates, it is totally effortless and as a part of our new identity, so there is no "forced action" or "disciplinary" quality at all to the experience.
- When you get a signal from the methodology, stop thinking / analyzing. Just put the trade on. I resolve to stop analyzing!
- Edge-u-cated guess → the probabilities are in your favor. That's all we're doing here.
- Understanding probabilities is not the same as functioning in probabilities.
- Goal is to be a consistently successful trader with an income I can rely on.
- Market structure: all it takes is one person / group / entity to completely knock your trade the other way. You do not know what the trade will do given every moment is absolutely unique. And, you do not need to know to make money.

Main Ideas

- One-Liner: "Raven Protocol is a decentralized and distributed deep learning training protocol which provides cost-efficient and faster training of deep neural networks by utilizing the compute resources in the network." (Raven Protocol WP, p. 4)
- Long-Range Vision: "Raven Protocol is the central hub for performing AI training and development. The platform will integrate AI services such as data exchanges, data labeling/annotation services, shared models, and implemented algorithms that may be developed by other projects or members of the AI community....With the correct incentivization in place, AI training can be accessible to the masses either for free or at deep[ly] discounted rates; this would undoubtedly push AI technology to levels unimaginable at present." (Raven Protocol WP, p. 19)

Details

Context

- Status quo is witnessing AI acceleration due to "trends of improved algorithms, exponential growth in computational power, explosion of data, and the development of AI hardware such as GPUs." (Id. at pdf p. 2)

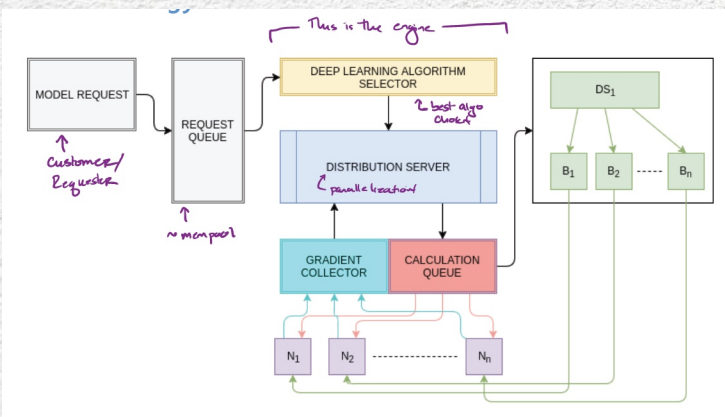
Problem

- Deep learning is costly: time and economic cost
 - ✓ labor & engineering hours, opex, capex, maintenance capex and recurring opex
 - ✓ "Training a simpler 19 layer Convolutional Neural Network on a million images (Imagenet) usually takes around 2 weeks of continuous training. This translates to 336 hours on an ec2 instance @ 2.6 USD per hour costing roughly around 1,000 USD...[for] just one trained model." (Id. at pdf p. 5)
- Localized deep learning training is limited despite chip advances (implying that aggregating latent compute supply is essential)
 - ✓ "Training deep neural networks on GPUs is still a localized way of training the network and can only scale so much given the limitation in the number of cores that can be fitted inside a block of a single GPU chip." (Id. at pdf p. 5)

Solution

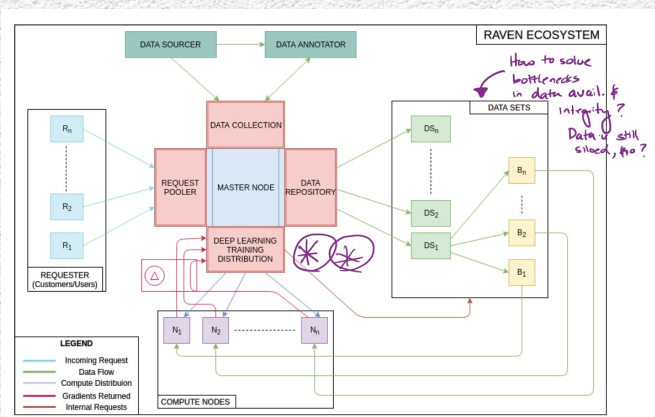
- Core Identity Statement. "Raven Protocol is a decentralized and distributed deep learning training protocol which provides cost-efficient and faster training of deep neural networks by utilizing the compute resources in the network." (Id. at pdf pg. 4)
- Lowering the computational burden of deep learning and modern AI/ML techniques requires distribution of compute directed toward model training
- Utility token to enter, participate in, and build a network solves the cold start (aka "chicken and egg") issue that plagues traditional platforms (need supply to attract demand; need demand to attract supply)
- Decentralization benefits in the context of model training: speed, cost reduction, transparency X

Process Flow



SOURCE: Raven Protocol Whitepaper (May 2019) at p. 10

ANNOTATION: Sandeep C. Ramesh



SOURCE: Raven Protocol Whitepaper (May 2019) at p. 6

ANNOTATION: Sandeep C. Ramesh



Details

Token, Governance

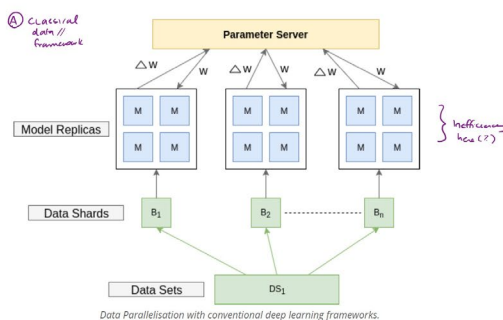
- Utility token, bootstrap funding
- Scant on details; follow up with community and team
- Compute will be permissioned: "Those participating by lending their systems as compute nodes for training models are requested explicit permission by Raven. Such awareness is created among users to differ from companies that have, in the past, taken advantage of user-ignorance. We have clear focus in being transparent and explicit on how much of the user's resources will be utilized by our network." (Id. at pdf p. 11)

Issues / Follow Ups

- Proof of calculation: need to better understand this "primary guideline for the regulation and distribution of incentives to the compute nodes in the network." (Id. at pdf p. 11)
- AI-tuned stable coin for interoperability
- "Further in the future, Raven Protocol will incorporate additional features that will involve more stakeholders such as a dataset marketplace or a data labeling and annotation marketplace....Critical to such an interoperability is the data and model format that each AI-service expects. Raven will create the layer to translate the interoperability seamlessly, as well as passthrough the costs associated with using each service. Meaning that, we will need an AI-stable coin developed at the back-end, in partnership with larger AI projects."
 - ✓ *Is this necessary? Why can't we use any other stable coin? The project also contemplates using USD payments; is that merely a bridge to a stable coin?*
- Explicit reliance on USD: "To provide a fair ground for the transactions, various costs inside the Raven Ecosystem will be pegged to USD, which will provide transparency to the customers." (Id. at pdf p. 16)
- Proof of calculation: need to better understand this "primary guideline for the regulation and distribution of incentives to the compute nodes in the network." (Id. at pdf p. 11)

On Parallelization

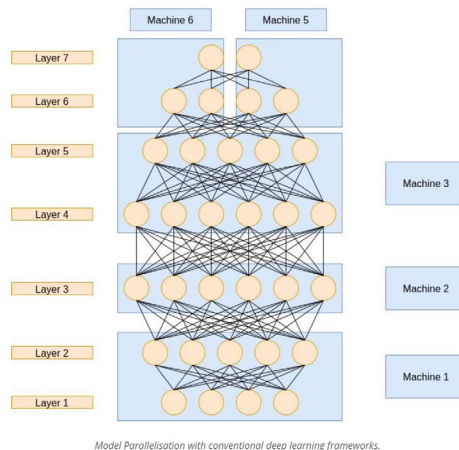
3.1 Data Parallelisation



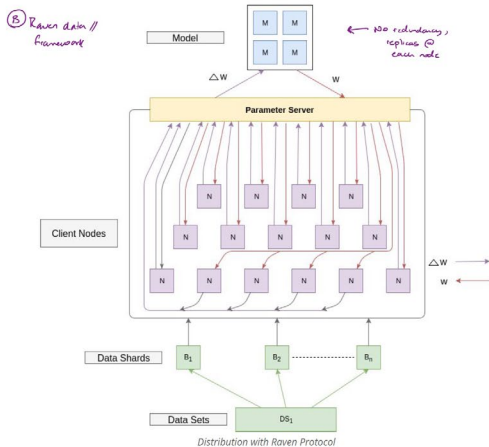
SOURCE: Raven Protocol Whitepaper (May 2019) at p. 12
 ANNOTATION: Sandeep C. Ramesh

3.2 Model Parallelisation

Model Parallelism is another way of distributed training for large scale deep learning. Traditionally, this was achieved by keeping the dataset in a different system, which is



SOURCE: Raven Protocol Whitepaper (May 2019) at p. 14



SOURCE: Raven Protocol Whitepaper (May 2019) at p. 13
 ANNOTATION: Sandeep C. Ramesh

Main Ideas

- In the modern era (post ~2012), demand for compute has been doubling every 3-4 mos (per 2019 evidence compliments of Sastry et al. at OpenAI) because of (a) hardware improvements and (b) economic investment fueling innovation
- This mega trend sets the stage for a heightened importance on exploring decentralized solutions to compute. There's a lot of work to do. How can we do more and better?

Details

3 Drivers of AI

- Algorithmic innovation (difficult to track)
- Data (supervised or interactive environments) (difficult to track)
- Amount of compute available for training (practically measurable and hence a proxy for gauging AI advancement)

More Compute = Better Results

- While increased computational burden might suggest inefficiency in algorithmic innovation, "at least within many current domains, more compute seems to lead predictably to better performance, and is often complementary to algorithmic advances." (Id. at pdf p. 1)
 - ✓ Further reading: Hestness et al., "Deep Learning Scaling is Predictable, Empirically" (2017)] (<https://arxiv.org/abs/1712.00409>)
- Compute needs increase by factor of 10 per annum

History

- Pre-2012: pre-GPU usage for ML
- 2012-2014: limited GPUs
- 2014-2016: large scale GPUs, hitting data parallelism diminishing returns
- 2016-2017: more parallelism, specialized hardware

History: "Moore and Post-Moore"

- We can simplify the empirical look further into two eras:
 - ✓ Era 1 -- 1959 - 2012: compute usage tracks Moore's law, meaning a ~2Y doubling time for compute
 - ✓ Era 2 -- 2012 - onward: compute usage explodes, meaning ~3-4mo. doubling time for compute
- Rationale for the transition from Era 1 to Era 2: (a) technological advancements removing prior limits on compute and (b) more economic investment to fuel experiments and breakthroughs
- Interestingly, the "history of investment in AI broadly is usually told as a story of booms and busts, but we don't see that reflected in the historical trend of compute used by learning systems. It seems that AI winters and periods of excitement had a small effect on compute used to train models over the last half-century." (Id. at pdf p. 7)
 - ✓ This idea of looking beyond the economic / investment cycles to explain underlying development is actually specifically addressed by Toolkit Theory; *see* [[FN 59_On Toolkit Theory and Innovation Cycles]]

Data Parallelism Defined Simply

- Contra pipelined, serial processing, data parallelism allows concurrent execution of an application on many processors.
- Same task performed concurrently (i.e., in parallel) across many nodes.

Exponential Increases in Compute to Continue

- Hardware innovation: AI-specific chips being built to increase FLOPS/watt and FLOPS/\$ (i.e., Floating Point Operations Per Second; measuring computer performance)
- Reconfiguring hardware to make more economically efficient (increasing yield)
- Parallelism advances (e.g., combining algorithmic innovations)
- More economic resources diverted to training vs. inference; that is, amounts spent on training are low relative to limits (total hardware budget = \$1tn p.a.) and relative to amounts spent on inference

Implications: Be Proactive, Can't Afford Reactivity

- "But even the reasonable potential for rapid increases in capabilities means it is critical to start addressing both safety and malicious use of AI today. Foresight is essential to responsible policymaking and responsible technological development, and we must get out ahead of these trends rather than belatedly reacting to them." (Id. at pdf p. 3)

A Note on Measurement: pfs-day

- pfs-day similar to kWh in energy domain

Main Ideas

- **One-Liner:** "The Gensyn Protocol is a layer-1 trustless protocol for deep learning computation that directly and immediately rewards supply-side participants for pledging their compute time to the network and performing ML tasks...facilitating task distribution and payments programmatically through smart contracts." (Id. at pdf pg. 4)
- **Long-term vision:** "The Gensyn Protocol will enable anyone to train ML models for any task using a self-organizing network that encompasses every source of compute power in existence....By decentralizing ML compute, the Gensyn Protocol brings a crucial infrastructure component natively to Web3, reducing reliance on Web2 and further strengthening and decentralizing the entire ecosystem....Foundation models, trained on the Gensyn Protocol, will be decentralized and globally owned, allowing humanity to equally benefit from collaborative ML development and training. Building on these foundation models using fine-tuning will be as simple as defining a task and paying a fair market price for the fine-tuning work, removing the barriers that currently exist." (Id. at pdf pp. 15-16)

Details

Intro / Conclusion

- AI compute demand exceeds supply with former doubling every 3 mos.
- Most advanced deep learning models are not open sourced (e.g., OpenAI's DALL-E)
- Building foundation models is extremely resource intensive (technical and economic)
- Status quo model training is siloed due to uneven resources; this siloed functioning limits rate of AI/ML progress (and cedes power to incumbents that own the resources and can bias outcomes to fulfill their ideologies)
- Solution to siloed training is to increase compute utilization vs. current state of ~40% of global processor utilization
- Chip / hardware advances are limited, meaning technological innovation in hardware won't solve accelerating computational intensity
- Trade-off of running local models by purchasing / owning hardware (scale constraint) and paying for expensive cloud-based resources (economic constraint)
- Existing projects working on decentralizing computing services cannot handle state dependent machine learning tasks; instead, they are tuned to "embarrassingly parallel problems such as 3D rendering, where computational work can be trivially split and verified" given state independence (id. at pdf p. 2)
- Volunteer networks are limited; they lack incentives that lead to scale and system integrity (at scale)
- Ethereum is too expensive as an alternative due to expensive on-chain replication of work → "Training a small MNIST neural network (~400M processor operations) takes ~8 minutes on an average laptop but would take ~80 days on Ethereum at a cost of approximately \$32m.

Problem

- Three core problems slowing ML progress: (1) access to compute; (2) access to data; (3) access to knowledge (ground truth labelling). Gensyn only addresses (1)
- State Dependence: Deep learning is state dependent, making verification of work prohibitively expensive
 - ✓ Replication of work takes a long time, costs money, and lacks trust in a decentralized environment; solving for distrust is key to solving the "verifier's dilemma"
- Marketplace Creation:
 - ✓ Cold-start challenge when creating n-sided marketplace; in Gensyn's case, need supply (compute) and demand (AI/ML tasks) at critical threshold to avoid a "ghost town" platform
 - ✓ Monitoring and tracking completed work & payments for system services
- Work Estimation (up front): challenging-to-impossible to know how much compute needed for task execution and whether task will loop endlessly (halting problem)
 - ✓ Halting problem is more acute because deep learning frameworks moved from static graph to dynamic construction
- Privacy: Data-level privacy vs. model-level (former more important)
- Parallelization: key for scale, otherwise training is limited to single or few machines.
 - ✓ "Combining the performance requirements of the ML work with the untrusted and unreliable nature of the compute sources means that a high degree of parallelization is essential in any solution." (Id. at pdf pg. 4)



Details

Solution

- Probabilistic Proof-of-Learning: selective replication vs. wholesale replication can create sufficient verification of ML work done; Gensyn seems to rely heavily on Jia et al., "Proof-of-Learning" Definitions and Practice" in IEEE Symposium on Security and Privacy (2021) in designing trust mechanics
- Staking and slashing utilized as carrot and stick financial incentives to maintain network integrity
- 4 Participants: Submitter: customer; Solver: model trainer; Verifier: checks Solver's work; Whistleblower: checks
- Verifiers (as a class, not individually)
- Solution to halting problem: "estimate of required work is generated by constructing and unrolling a computational graph into the required operations"
- Solution to computational limits: parallelization whereby tasks can be split and handled asynchronously
- Gensyn expects to capture glut of compute supply from mothballed Eth miners due to the merge (however, specifics on strategy and tactics for actually siphoning those compute resources are not provided)

Process Flow

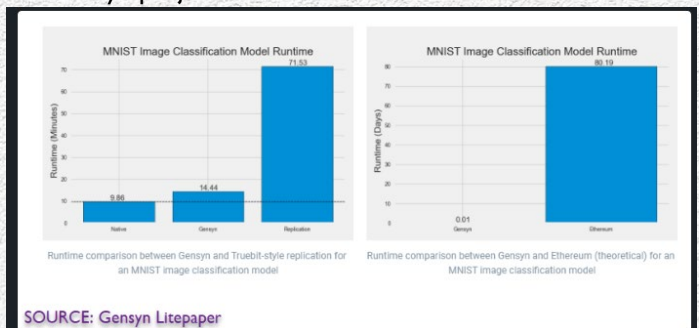
- Task Submission --> Profiling --> Training --> Proof Generation --> Proof Verification --> Settlement
- Additional operations related to Whistleblower activities: Graph-Based Pinpoint Challenge, Contract Arbitration, Settlement
- Task Submission: customer submits tasks, describing task in machine-readable format, submitting model binary, and publicly available training data
- Profiling: Verifier performs profiling tasks and generates variation thresholds (process of labeling); Whistleblowers expected to re-run profiling work to keep the Verifiers honest
- Training: tasks entered by Submitter (i.e., customer) go into task pool (~ Eth mempool); one Solver is chosen (but how?); generates proof-of learning at checkpoints, storing the metadata on-chain
- Proof Generation: see again Jia et al.
- Proof Verification: Verifiers pick completed tasks from pool and re-run portions of the work
- Graph-Based Pinpoint Challenge: does replication of Verifier work necessarily verify the original Solver work?
 - ✓ Challenges and arbitration are transparency on chain
 - ✓ Intentional errors are created to ensure Whistleblower has incentive to work (jackpot payouts)
- If task is properly completed and checked per the process flow above, then Solver and Verifier get paid (how, how much, what's the payment algorithm?)

Figures

- Query what the assumptions are behind the figures and Gensyn projections.

Provider	Approximate hourly cost for ML training work (V100-equivalent)	Scalability
Ethereum	\$15,700	Low
Truebit (+ Ethereum)	\$12	Low
GCP on-demand	\$2.50	Medium
AWS on-demand	\$2	Medium
Golem Network	\$1.20	Low
Vast.ai	\$1.10	Low
AWS spot instances (unreliable)	\$0.90	Medium
GCP spot instances (unreliable)	\$0.75	Medium
Gensyn (projected)	\$0.40	High
Single GPU in datacentre	\$0.40	None
Single personal GPU	\$0.28	None

SOURCE: Gensyn Litepaper



Governance

- Foundation and Software Development Co. model
- Phased decentralization approach (philosophical, unspecified milestones)
- Foundation Treasury will take TBD % fee for each task

Roadmap (High Level)

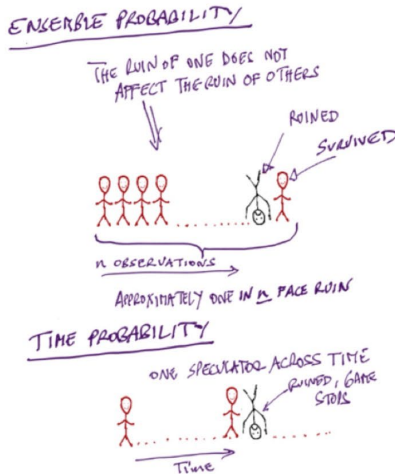
- Testnet --> Canarynet (parachain on Kusama relay chain; token will have real value) --> Mainnet (parachain on Polkadot relay chain; hardened token)

Key Sources of Inspiration

- Nassim Taleb, Skin in the Game (2018)
- Ole Peters, "The Ergodicity Problem in Economics" in Nature Physics 15 (2019)
- Robert Frey, Lecture on Drawdowns at Real World Risk Institute (2021)

Main Ideas

There's a lot of talk about "conviction" and "concentration" in the investing and trading domains. Often (but not always) these are "cocktail party" terms uttered by those utterly insensitive to, ignorant of, and inexperienced with risk. In convex domains--like crypto trading/investing--survival = winning (and because of the convexity, winning big).

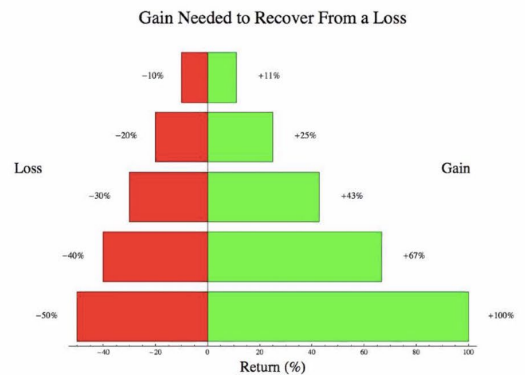


The difference between 100 people going to a casino and one person going to a casino 100 times, i.e. between (path dependent) and conventionally understood probability. The mistake has persisted in economics and psychology since age immemorial.

Source: Nassim Taleb, Skin in the Game (2018)



Recovery from Drawdowns



11/9/21

Real World Risk Institute

Source: Robert Frey, Lecture on Drawdowns at Real World Risk Institute (2021)

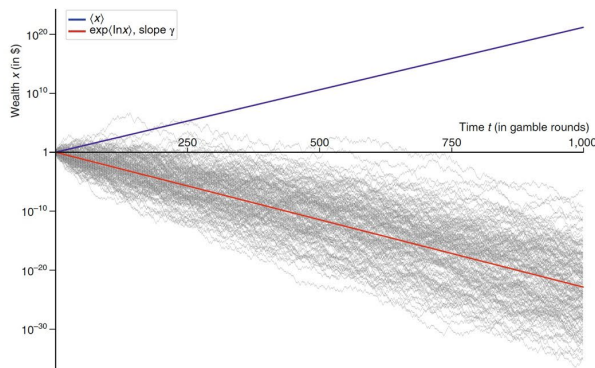


Fig. 2 | Randomly generated trajectories of the repeated example gamble. The example gamble is given in equation (2). The expectation value, $\langle x \rangle$, (blue line) is the average over an infinite ensemble, but it doesn't reflect what happens over time. The ergodic growth rate for the process (slope of the red line) tells us what happens to a typical individual trajectory. 150 trajectories are shown, each consists of 1,000 repetitions.

Source: Ole Peters, "The Ergodicity Problem in Economics" in Nature Physics 15 (2019) at 1219.

Source: Robert Frey, Lecture on Drawdowns at Real World Risk Institute (2021)s

Ensemble average, which is highly misleading in its ignorance of time & path dependence (i.e., if you lose too much, the game is over for you and expected value is meaningless)

Protect against ruin.

Key Sources of Inspiration

- Sonke Ahrens, How To Take Smart Notes: One Simple Technique to Boost Writing, Learning, and Thinking (2017)
- Christian Tietze, zettelkasten.de/posts

Main Ideas

One problem when interacting with and evaluating crypto ecosystems is that of information "smog" (see e.g., Field Notes 3 on info overload and 6 on crypto info diets). Adding an additional layer of waste is poor information digestion. I found increased indigestion from classical note taking and so investigated alternatives.

Traditional note taking emphasizes information capture. As a result, notes are banished to a coffin, rarely revisited, and if revisited, completely decontextualized, requiring re-reading source materials as if from scratch.

Establish a note-taking approach--essentially a version of "Zettelkasten" / "slip box"--that displays the following attributes:

1. **Less Hierarchical**
Instead of treating notes as file management systems that exist in pre-determined *a priori* categories, notes should be seen as less centralized. In this way, the connections can cluster and emerge, leading to cross-disciplinary insight and genius. This decentralized system / process enables insight. After all, you can't plan for insight. Rather, you can only create the conditions to invite it.
2. **Atomicity**
Notes must be reduced to the core idea. This facilitates clear connections.
3. **Associative Ontologies, not Hierarchies**
Forget about classifying notes. Instead, allowing the connections to organically emerge in a "structured meander" prevents insights missed due to rigid and forced categories.
4. **Future Proof**
Notes must be self-contained such that my future self would understand the note fully without needing any outside context, let alone having to re-read the source material.
5. **Cure Archive Fever**
See also "collector's fallacy." Resist the seduction of compiling reading material--and even reading binges--without interacting with the material by making it my own and connecting to the network of notes.
6. **Writing Is Inseparable from Thinking**
"Notes on paper, or on a computer screen... do not make contemporary physics or other kinds of intellectual endeavors easier, they make it possible." (Neil Levy, Oxford Handbook of Neuroethics)
7. **Combats Confirmation Bias**
The criterion for placing a note in the system is whether it adds to the discussion, not whether it confirms the discussion. Therefore, disconfirming evidence is just as useful as confirming evidence. The emphasis shifts from our preconceptions to being open to whatever connections arise. The note system is agnostic to information it is fed; all it cares about is relevance.

Main Ideas

- Web3 challenges can be assessed at application, system, and economy (and legal) levels. At the application level, challenges include (a) composability (esp. back-end), (b) high switching costs from Web2 apps, and (c) self-custody / recovery frictions. At the system level: (a) scalability, (b) interoperability, and (c) security. At the economy level: (a) incentives and (b) cost.

Details: Section 5**On Sweep of Web3.**

- Web3 covers full web architecture from front-end to back-end, essentially "delivering internet architecture in a decentralized way." (Id. at 17)
- DAOs are underappreciated today relative to their potential to transform human action.
 - ✓ Flattened hierarchies; enhanced accountability via on-chain settings
 - ✓ "DAO has extended the scope of decentralization, which was previously bound to machines, to a broader area that involves human beings. The shift of *how to operate a digital organization* would pose a great impact on the future world, more than they are presented today." (Id. at 18)

On Curse of Web2 Scale.

- Once the acquisition of user stage reaches critical mass, the incentive to turn a profit requires traditional software companies to sell user data outright or (possibly worse) redirect that data toward training AI models. (See, e.g., [[FN 52_On Save AI, Save World]] and [[FN 45_On Deep Learning Infrastructure Innovation]])
 - ✓ "Users have no choice, facing the dilemma between privacy and convenience." (Id. at 18)

On Challenges at the Application / User Level.

- Composability at the back-end is challenging even if APIs are standardized.
 - ✓ "The barriers are whether composable components are compatible with each other and whether data can flow seamlessly across different components. For such reasons, the data need to be designed in the same structure for the re-usage by these components." (Id. at 19)
- User switching costs from familiar Web2 to unfamiliar Web3 applications are high.
 - ✓ "The lack of integration with modern web browsers and mobile applications limits the wide adoption of Web3 to end-users....How to decrease the migration cost is a challenge." (Id. at 20)
- Loss of private keys / recovery challenges.
 - ✓ "Methods to recover accounts, or at least the internal data, are an urgent requirement for applications in the Web3 space. Moreover, applications that adopt off-chain storage require more strict verification for data integrity because additional checks on whether the data in external storage matches on-chain hash value are needed. The data recovery in external pages is difficult due to the absence of traceability and accountability." (Id. at 20)

On Challenges at the Blockchain / System Level.

- Scalability: "represents the ability to process transactions along with the increased scale of networks, which is reflected by the increase or decrease in its performance.
 - ✓ "This is a long-term issue existing in blockchain systems due to intrinsic decentralization." (Id. at 20).
- Interoperability: "Creating interchangeable communication channels to connect isolated decentralized ledgers is still a challenge" (Id. at 21).
- Scalability: "represents the ability to process transactions along with the increased scale of networks, which is reflected by the increase or decrease in its performance.
 - ✓ can't have Polkadot token on Ethereum, e.g.; wrapped tokens are suboptimal because they create waste and complexity by virtue of being representative tokens
- Contract Security: "Examples include the integer underflow/overflow attacks, DAO attacks and Parity Multi-Sig Wallet attacks. Even worse, the scripting nature of contract programming languages...and the non-updatable feature of smart contracts will significantly limit the growth of Web3 applications." (Id. at 21).

On Challenges at the Economy / Market Level.

- Diminishing rewards / incentives as adoption increases: "Users adopt Web3 applications largely due to their considerable potential revenues....However, as more and more users participate in the game, the threshold of obtaining rewards becomes extremely high. Thus, designing a positive incentive mechanism that can cover as many users is crucial to attract new players joining the network." (Id. at 21)
- Cost: high gas and transaction fees, requiring more off-chain solutions without problematic centralized dynamics reentering through the backdoor.

Main Ideas

Developed by Eric von Hippel in the 1970s, "toolkit theory" posits that producers innovate by allowing users the ability to tinker with frameworks or modules, thereby capturing local knowledge for the benefit of product development.

Toolkits create a more distributed innovation space coordinating producer and user knowledge by encouraging producers to ship frameworks for users to engage, parameterize, and iterate based on local needs and "sticky" information that exists *in situ*.

Examples (in crypto): ERC20 standard, ERC721 standard, DAO frameworks

(Possible) Implication: through the toolkit lens, crypto innovation is most potent the closer it is to framework layers on the theory that they enable more innovation upstream. "The outputs of the toolkit entrepreneurial process are an input into the design space for product developers, enabling them to create specific products for the local sticky conditions of their users." (Id. at 9)

Details

Toolkit Theory.

- Toolkit theory posits that producers innovate by allowing users the ability to tinker with frameworks or modules, thereby capturing local knowledge for the benefit of product development.
- "Toolkits for user innovation are coordinated sets of 'user friendly' design tools that enable users to develop new product innovations for themselves." (Quoting von Hippel and Katz)
- "The foreground of analysis here is...the way that toolkits put to use local knowledge about user needs." (Id. at 3)
- Against the producer-centric or top-down approach to customer discovery and development, the toolkit theory recovers local knowledge to create better feedback loops for customer and product development.
 - ✓ "The producer centric solution is to have the producer's engineers or consultants do the work of identifying local users' needs (e.g., by working with them) and then developing customized products in-house." (Id. at 5-6)
- "Toolkits facilitate decentralized innovation by enabling centralized expertise to be encoded into technical rules that are realized in the toolkit software and interfaces. This enables greater use of distributed local knowledge." (Id. at 7)

Toolkit Attributes.

1. Iteration: trial-and-error feedback cycles
 2. User-Generated Insight: users innovate and modify a generalized framework to suit their particular needs based on local, "sticky," *in situ* knowledge
 3. Interoperability: users can mostly use their existing tools and languages to innovate
 4. Access to Libraries: users can leverage pre-existing modules, dictionaries, etc.
- "The depth and quality of these design libraries, and the security of their use and knowing that they will execute as intended, offer a potentially substantial source of competitive advantage to open and user innovation through toolkits and a basis for business models that pay for access to or use of these libraries." (Id. at 14)

Toolkit Benefits.

- Speed and Cost. "The costs of innovation processes are reduced by moving design and innovation activity to where relevant information is located. Information is used at the edges, allowing users to develop producible (i.e., able to be manufactured) custom products via iterative trial-and-error." (Id. at 6)

Examples.

- DAO innovation is best understood under the toolkit framework.
 - ✓ "DAO tools are better described as DAO toolkits because they are deployed in the individual context of each DAO. Each DAO selects different parameters (e.g., number of tokens, voting processes, authorizations over wallets) to fit to their local needs. DAOs also implement new combinations of different tools, forming their own toolkit of composable tools. Each DAO must do this because it has 'sticky' local information about its own community...culture...and aims." (Id. at 3)



Competitive Advantages.

- Building dominant frameworks and standards confers a non-obvious competitive advantage for the producers.
 - ✓ "Manufacturers who move early and establish a dominant position to set standards for a user design language have a good chance of being generally adopted by the user community in that marketplace." (Id. at 6)
 - ✓ "Control of that standard enables the manufacturing firm an edge in offering easy, fast, error-free translations of designs made by users into their own production capabilities, even if the toolkit language itself becomes an open standard." (Id. at 6)

Toolkit Innovation Linked to Investment Cycles.

The Toolkit	Cycle
Ethereum Virtual Machine (EVM) + ERC20 token standard	2017 Initial Coin Offering (ICO) boom
... + Automated Market Makers (AMMs) toolkit	2020 decentralised finance (defi) summer
... + ERC721 standard + Non Fungible Token (NFT) marketplaces	2021 NFT summer
... + voting tools (e.g. Snapshot) + compensation mechanisms (e.g. Coordinape)	2022 year of the DAO
... + ?	Next cycle

SOURCE: Darcy Allen & Jason Potts, "Web3 Toolkits: A New Theory of Crypto Dynamics" (working paper) (May 2022) at 13.

<div>06.24.22</div> <div>#17</div>	<div>SR NOTES ON:</div> <div>author, <u>title</u>, source (date)</div>
Main Ideas	Details
<div>• xx</div>	<div> <div>Universe of Chains vs. World of dApps</div> <div> Specified chains vs. general purpose chains Dapp and chain more intimately tied in design vs. build on top Subchains bear security burden vs. security ensured by general purpose chain Subchain communication less important than sovereign subchain vs. "The Universe of Chains envisions a new global network architecture where businesses and consumers use hundreds and thousands of app-specific blockchains and rely on a base interchain layer for cross-chain communication." "The World of dApps, meanwhile, imagines a few less-specialized and more general-purpose blockchains that offer scale, security and throughput in a modular fashion to entrepreneurs and developers." </div> <div> Key scaling issues: 1. security in distributed node processing environment and 2. efficient cross-chain communication. </div> <div> Cosmos: internet of blockchains. (a) Cosmos SDK to launch chains in modular manner (b) Inter Blockchain Communication protocol (IBC) to connect chains together </div> <div> Polkadot <ul style="list-style-type: none"> Interoperable layer "Parachains" as opposed to chains operating on their own </div> <div> NEAR: next gen sharded chain <ul style="list-style-type: none"> Sharding is different than ETH 2.0 b/c of auto rebalances resources amongst shards and doesn't discriminate b/t different shards Acts as "single blockchain with 'chunks' of shards that allow for quick and efficient cross-shard communication" "not a blockchain connector, but intends to be a dApp platform with a low configuration overhead that encourages developers to build directly on top of its existing shards." </div> <div> <ul style="list-style-type: none"> QUERY: are these visions / world views mutually exclusive? What's the third way? </div> </div>
Resources	
<div>• xx</div>	
Backlinks [internal]	
<div>#fieldnotes</div> <div>#xx</div>	<div>Prepared by Sandeep Ramesh strictly for educational (neither investment nor business) purposes.</div>

Main Ideas

Experiencing and understanding financial markets as turbulent generates 10 non-standard observations, according to the inimitable Mandelbrot.

1. Markets = Turbulent. Against wishful thinking and financial orthodoxy (e.g., Gaussian, bell curve, normal distributions), financial markets display wild variation. Embrace convexity.
2. Markets = Dangerous. It is easy and seductive to underestimate the extreme risk laden in financial markets. There is a strong observed tendency to pay lip service to "turbulence." It is also easy and seductive to ignore the difference between ensemble probability and time probability. It is the latter that actually matters to an individual.
3. Timing Matters: Buy & Hold Is Illogical. Holding forever or "setting and forgetting" sounds either heroic / brave (in the first case) or lazy / defeatist (in the second case). Both are ignorant to the fact that volatility is concentrated; it clusters. The heuristic thus follows: take profits.
4. Prices are Discontinuous. They Jump. These jumps are more pronounced in an age where information cascades are more frequent.
5. Time Deforms. Market participants do not operate on some single universal clock or time scale.
6. All Markets are Built Upon Same Structure. Market processes change only in scale, but not in nature.
7. Markets are Uncertain; Bubbles Exist.
8. Markets are Deceptive. Acknowledge our tendency to look for faces in the clouds.
9. Can't Forecast Prices but Can Estimate Risk. "Markets are turbulent, deceptive, prone to bubbles, infested by false trends. It may well be that you cannot forecast prices. But evaluating risk is another matter entirely." (Id. at 247)
10. Value is Overvalued. "To be sure, I do not argue there is no such thing as intrinsic value....But the turbulent markets of the past few decades should have taught us, at the least, that value is a slippery concept, and one whose usefulness is vastly over-rated." (Id. at 252)

Details

One. Markets = Turbulent.

- Against wishful thinking and financial orthodoxy (e.g., Gaussian, bell curve, normal distributions), financial markets display wild variation.
 - ✓ "It shows turbulence in a wild kind of variation far outside the normal expectations of the bell curve; in a concentration of changes here and there; in a discontinuity in the system jumping from one value to another; and in one set of mathematical rules that can, in large measure, describe it all." (Id. at 228)
- * Invoking a Talebian heuristic, it's better to be convex than right.
 - ✓ "To drive a car, you do not need to know how it goes; similarly, to invest in markets, you do not need to know why they behave the way they do. Compared to other disciplines, economics tends to let its theory gallop well ahead of its evidence." (Id. at 229)

Two. Markets = Dangerous.

- It is easy and seductive to underestimate the extreme risk laden in financial markets. There is a strong observed tendency to pay lip service to "turbulence."
 - ✓ "Turbulence is dangerous. Its output--the pressure or velocity of water, the average or change in price--can swing wildly, suddenly. It is hard to predict, harder to protect against, hardest of all to engineer and profit from. Conventional finance ignores this, of course. It assumes the financial system is a linear, continuous, rational machine. That kind of thinking ties conventional economists into logical knots." (Id. at 230)
- It is also easy and seductive to ignore the difference between ensemble probability and time probability. It is the latter that actually matters to an individual.
 - ✓ Traditionalists "assume that the 'average' stock market profit means something to a real person; in fact, it is the extremes of profit or loss that matter most." (Id. at 231)
 - ✓ "Unlike a broker, most investors do not care about 'average' returns. For them, the rare, out-of-the-average catastrophes loom larger....The ultimate fear is financial ruin." (Id. at 231-32)
- Conventional models assume risk of ruin is 10^{-20} , but in reality it is closer to 1 in 10 to 1 in 30.



Three. Timing Matters: Buy & Hold Is Illogical.

- Holding forever or "setting and forgetting" sounds either heroic / brave (in the first case) or lazy / defeatist (in the second case). Both are ignorant to the fact that volatility is concentrated; it clusters. The heuristic thus follows: take profits.
 - ✓ "Suppose big news has inflated a stock price by 40 percent in a week, more than twice its normal volatility. What are the odds that, anytime soon, yet another 40 percent run will occur? Not impossible, of course, but certainly not large. A prudent investor would...[t]ake a profit." (Id. at 234-35)

Four. Prices are Discontinuous. They Jump.

- Continuity in prices is a poor and dangerous assumption. These jumps are more pronounced in an age where information cascades are more frequent.
 - ✓ "Continuity is a fundamental assumption of conventional finance...Bachelier, Markowitz, Sharpe, and Black-Scholes all assume continuous change from one price to the next....Alas, the assumption is false and so the math is wrong. Financial prices certainly jump, skip, and leap--up and down." (Id. at 237)

Five. Time Deforms.

- Market participants do not operate on some single universal clock or time scale.
 - ✓ "Conventional financial analysis is a welter of conflicting views of time. One, implicit in conventional finance theory: Time is measured by the clocks and is the same for all investors." (Id. at 238)
 - ✓ "In fractal analysis, time is flexible. The multifractal model describes markets as deforming time--expanding it here, contracting it there. The more dramatic the price changes, the more trading time-scale expands. The duller the price chart, the slower runs the market clock." (Id. at 239-40)
 - ✓ "Time does not run in a straight line, like the markings on a wooden ruler. It stretches and shrinks, as if the ruler were made of balloon rubber. This is true in daily life: We perk up during high drama, nod off when bored. Markets do the same." (Id. at 240)

Six. All Markets are Built Upon Same Structure.

- Market processes change only in scale, but not in nature.
 - ✓ "One of the surprising conclusions of fractal market analysis is the similarity of certain variables from one type of market to another." (Id. at 241)

Seven. Markets are Uncertain; Bubbles Exist.

- See above re: critique of Gaussian. Nothing further is needed to substantiate this claim.

Eight. Markets are Deceptive.

- Acknowledge our tendency to look for faces in the clouds.
 - ✓ "It takes no great leap of the imagination to see how such spurious patterns could also appear in otherwise random financial data. This is not to say that price charts are meaningless, or that prices all vary by the whim of luck. But it does say that, when examining price charts, we should guard against jumping to conclusions that the invisible hand of Adam Smith is somehow guiding them. It is a bold investor who would try to forecast a specific price level based solely on a patter in the charts." (Id. at 247)

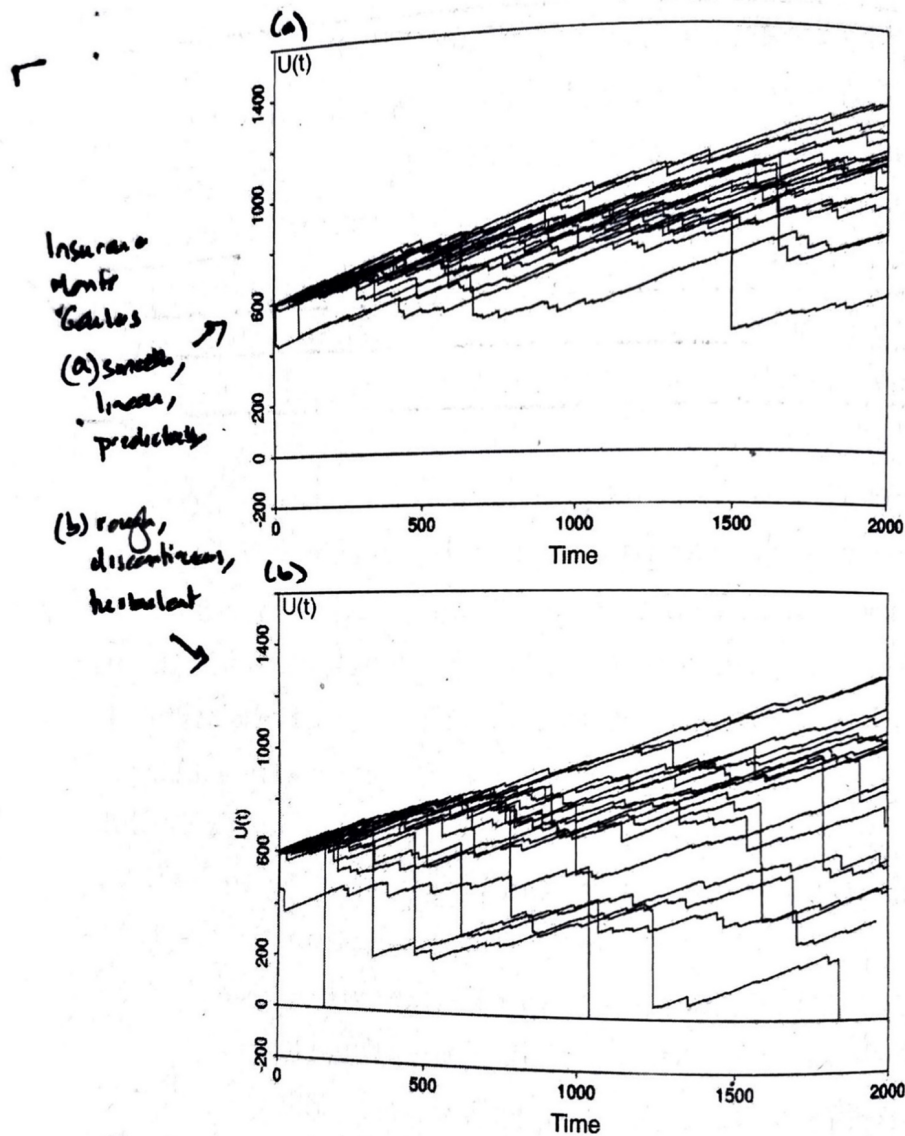
Nine. Can't Forecast Prices, but Can Estimate Risk.

- "Markets are turbulent, deceptive, prone to bubbles, infested by false trends. It may well be that you cannot forecast prices. But evaluating risk is another matter entirely." (Id. at 247)
- "You cannot beat the market, says the standard market doctrine. Granted. But you can sidestep its worst punches." (Id. at 249)

Ten. Value is Overvalued.

- "All this implies that value is somehow a single number that is a rational, solvable function of information. Given a certain set of information about an asset...everybody if equally well-placed to act will deduce it has a certain value; they will all hang the same price tag on it. Prices can fluctuate around that value; and it can be hard to calculate. But value, there is. It is a mean, an average, something certain in a chaos of conflicting information. People like the comfort of such thinking. There is something in the human condition that abhors uncertainty, unevenness, unpredictability. People like an average to hold onto, a target to aim at--even if it is a moving target." (Id. at 250)
- "To be sure, I do not argue there is no such thing as intrinsic value....But the turbulent markets of the past few decades should have taught us, at the least, that value is a slippery concept, and one whose usefulness is vastly over-rated." (Id. at 252)
- "The prime mover in a financial market is not value or price, but price difference; not averaging, but arbitraging....These arbitrage tactics assume no 'intrinsic' value in the item being sold; they simply observe and forecast a difference in price, and try to profit from it." (Id. at 252)

Details



Roads to ruin. These charts, from Embrechts 1997, simulate the profits or losses of several different insurers collecting premiums and paying claims; each line from left to right through time shows the outcome for a different hypothetical insurer. The top chart shows what happens if you assume claims follow a nice, mild pattern of variation: a hugely profitable industry. The bottom chart shows what happens if you assume wild variation in claim sizes: some bankruptcies. Which is

SOURCE: Benoit Mandelbrot & Richard Hudson, *The (Mis)Behavior of Markets: A Fractal View of Financial Turbulence* (2004), p. 232

Main Ideas

- Conventional investors and siloed thinkers underappreciate the importance of metaphors to narrate novelty and fuse horizons (I'd argue, preconditions to outsized, counter-conventional returns).
- Metaphors are the connective tissue of apparently (and falsely) disparate ideas; they are the wrappers providing mental grips on slippery substances.
- Quoting W. Brian Arthur: "I have a very strong belief that science and thinking progresses not so much by theorems but by metaphors. Metaphors are what we absorb, that go in deep, that we digest, perhaps also consciously forget. But two years later you start to write about evolution in the economy and (suddenly you find yourself) deeply informed about how it takes place." (Id. at 131)
- However, metaphors can lose their potency when overuse suffocates their open-endedness.

Details

Underappreciated Importance of Metaphors.

- Connective tissue of apparently (and falsely) disparate ideas.
 - ✓ "Though often dismissed as mere rhetorical window dressing, metaphors play an important role in innovative thinking. In particular, the cognitive use of metaphor can reveal potentially fruitful connections and novel ways of seeing that lead to new insight." (Id. at 129)
- Complex domains are discursively enmeshed in an ocean of metaphor.
 - ✓ "Complexity science is premised on the assumption that seemingly disparate phenomena, both natural and social, evolved and constructed, can be understood using a common conceptual framework. The signature concepts used to talk about complex systems—emergence, adaptation, networks, evolvability, phase transitions, self-organized criticality, fitness landscapes, robustness, learning, edge of chaos, even the very notion of complexity itself—remain more metaphorical and suggestive than definitional and precise." (Id. at 130)
- Metaphor shapes perception, a pre-requisite to action.
 - ✓ "[T]he use of metaphors shapes our basic perception and understanding of the world." (Id. at 130)

Defining the Undefinable: Metaphor.

- Metaphor is a wrapper to give us a mental grip on a slippery substance.
- Metaphor is transgressive and cross-boundary. It uses language, logic, symbols from one field and deploys to another, which it doesn't conventionally belong.
- Metaphors defamiliarize the familiar.
- The inexactness and jagged edges of a metaphor are where its true power lies.
- Depth of metaphor lies in its open-endedness.

The Conventional Critique of Metaphors.

- Resistance Point: metaphors are not rigidly constructed and thus not available to falsification via gold standard scientific verification.
 - ✓ "As such, metaphors are sometimes viewed as incomplete— or worse, shoddy thinking." (Id. at 130)

Overcoming the Conventional Critique.

- View metaphors as successive ladders to continuously evolving insights.
 - ✓ "Metaphors and models are not locked in battle for relevance but can be seen as successive ladders, stacked one upon the other, which continue to underpin good thinking." (Id. at 131)
- View metaphors as an invitation, not a destination.
 - ✓ "A metaphor is not merely a flawed and fuzzy model, nor is it a final answer. A useful metaphor is an invitation to hard work that can be indispensable to innovation." (Id. at 131)
- Metaphors underpin heuristics-based thinking, which can be useful in complex domains where information is constitutively incomplete. (See, e.g., FN 50_On Cynefin and Complexity, FN 22_On Heuristics, or Simplicity in face of Complexity)
 - ✓ Metaphor vs. Model. Metaphor penetrates complexity via simplicity. Model penetrates simplicity via complexity.
- Metaphors seed nuanced understandings and breakthroughs.

On Metaphors Slipping into Cliché.

- Once treated as literal and reflexively invoked ad nauseam, the power of the metaphor fades to black.
 - ✓ "Metaphor metaphorical intrusion smoothed by time and long wear is apt to become a dead metaphor or cliché." (Id. at 133)

Main Ideas

- Oracles and oracle networks serve as critical middleware to bridge on-chain and off-chain ecosystems
- The "oracle problem" is double: (a) the general problem of pushing data on/off chain and (b) ensuring that the oracle (network) is itself moved toward decentralization
- Clear example where on/off-chain data coordination is necessary: parametric insurance smart contracts (predefined payouts upon predefined "external world" trigger events such as seismic threshold for quake insurance without claims ambiguity and cost inefficiencies associated with typical insurance pricing and adjustment processes)

Details

Oracles Defined.

- "A blockchain oracle is a secure piece of middleware that facilitates communication between blockchains and any off-chain system, including data providers, web APIs, enterprise backends, cloud providers, IoT devices, e-signatures, payment systems, other blockchains, and more."
 - ✓ **Listen:** monitor chain activity for smart contract requests for off-chain data
 - ✓ **Fetch:** pull data from off-chain 3P APIs
 - ✓ **Format:** data format compatibility between off-chain and on-chain environments to ensure communication
 - ✓ **Validate:** cryptographic proofs to provide accountability, reputation, and quality auditability
 - ✓ **Compute:** off-chain computation (e.g., blend data inputs from different oracle sources)
 - ✓ **Broadcast:** feed information on-chain
 - ✓ Output: send on-chain information off-chain

Utility of Oracles.

- Securely facilitating interaction between smart contracts (on-chain) and off-chain API economies expands the scope of smart contract use cases
 - ✓ And as such, the "blockchain oracle problem is one of the most important barriers to overcome...to achieve mass adoption" for smart contracting platforms and use cases. (Id.)
 - ✓ "Blockchain-based smart contracts and traditional data and API economies have immense potential to combine into hybrid smart contracts and form the future architecture of data-driven automation, but the question is how do these two worlds connect?" (Id.)
- Examples: parametric insurance contracts (pre-defined insurance risk), security/instrument price feeds, and any case where information is not natively on-chain.

Answer To: Why Can't We Build Oracle at Base Layer?

- Governance / Collective Coordination Problem: each time a new external data source needs to be added, a community vote is likely invoked
 - ✓ "Every time a new data source needs to be added to the network or an existing data aggregation method must be adjusted, it requires massive social governance."
- Complexity and Vulnerability Increase
 - ✓ "This [middleware oracle] ensures that blockchains have a lower attack surface and retain their determinism by maintaining a singular focus on consensus, while oracles have the required flexibility needed to generate determinism from a complex and subjective off-chain world without creating dependences and limitations that put at risk other applications."

Key Issue: External Data Quality.

- Major concern is "how to ensure external data inputted into the blockchain is high quality? Even a basic data request for the price of Bitcoin is quite challenging because simply looking at a website or a single exchange may not be as accurate or reliable as a paid API subscription to a professional data aggregator that has decades of experience filtering data and creating market coverage and is financially incentivized to maintain high-quality services. It's extremely difficult to manage and enforce quality for off-chain data."

Main Ideas

- "In the immediate-marshmallow world of investing, it is so hard to be the one sitting with folded arms, not taking the sweet enticement of now, and focusing instead on intermediate means for positional advantage to be exploited later." (Spitznagel at 238)
- The ultimate edge in investing is often "time." However, discourse surrounding the "temporal edge" often creates a false polarity of "short term" vs. "long term," missing the nuance of the intermediate.

Details

Critique of the "Long Term" Cliche; Toward the Agile.

- Internal Inconsistency. Initiating a position "now" and embracing a "long term" approach creates an unnecessary rigidity that prevents one's openness to taking advantages of opportunities that arise "inter-temporally." In this way, the "long term" betrays agility. In this sense, prefer agile alpha over "long term" alpha.
- "Long term is something of a cliche, and often even internally inconsistent: Acting for the long term generally entails an immediate commitment, based on an immediate view of the available opportunity set, and waiting an extended period of time for the result--often without due consideration to or differentiation between intertemporal opportunities that may emerge during that extended period of time." (Id. at 5)
- Rationalization. Often, the mantra of "long term" is invoked as a rationalization to "save" an investment thesis that might have broken.
- "[S]aying that one is acting long term is very often a rationalization used to justify something that is currently not working out as planned." (Id. at 5)

The Edge of Time is Intertemporal.

- Given innate tendencies to favor immediacy and directness over intermediacy and indirectness, "[i]t is no wonder, then, that having an intertemporal perspective and perception is such an underestimated and overlooked advantage, and yet it is also one of the most influential, a distinct intelligence, and key to our success." (Id. at 139)
- * On hyperbolic discounting / time inconsistency: "This pattern, present in all of us and distorted to extreme and even dangerous levels in the cases of addictions, is to be impatient now, all the while holding fast to the self-delusion of being able to be patient later." (140)
- * Reversing the default behavior (impatient now, patient later) renders an investment strategy to be "patient now for the sole purpose of becoming intensely and rapaciously impatient later; though difficult to perceive, this is the teleological causal arrow of time in roundabout investing." (Id. at 140)
- * Again, this is not a "long term" model. What is suggested is more nuanced in its appreciation for intertemporal opportunities.
 - ✓ "[A]dopting an intertemporal depth of field is *most definitely not* about merely "having patience," nor is it the cliched "long-term view," anchored in the present moment, that is a constant refrain among many investors--most notably the time frame of "forever" advocated by value investors such as Warren Buffet. In fact, is is quite contrary to it. Long term is but a trajectory from now to the distant future that effectively, and by definition, must ignore the sequence of many ripe time slices in the middle. Austrian Investing is about an *intertemporal exchange* as the very source of profit--now for an anticipated later." (142)
- The immediacy bias has pernicious psychological effects where the "now" (contra neo-spiritualists and false Vedanta preachers) becomes tyrannical. Similarly, the reflexive (and often vapid) call for "just be long term" has a quality of passivity with a dose of fatigue. The resolution is to uphold a middle way, an intermediate view, and an acknowledgement that the temporal field has a gradient.
 - ✓ "Without a depth of field perspective, we become victimized by time. Immediacy is a tyrant, ratcheting up stress and exacerbating feelings of being time-bankrupt. And there are immense external magnifiers on our time inconsistency. When time is scarce, indeed down to the last grains in the hourglass, as the grim reaper waits, desperation sets in. There is no future, no forward moments, there is only now, now, now." (Id. at 161)

The Enslavement of Immediacy.

- The structural disadvantage of Wall Street culture, observationally 10x worse (and hence an opportunity for greater edge for the discerning) in the crypto trading / investing / YOLO / FOMO game:
 - ✓ "Even today as the evolutionary march continues, with technology seeping into every corner of the seven continents, we still struggle with the most fundamental challenge: our perception of time." (165)

Main Ideas

- Coined by Merton in 1968, drawing upon Biblical reference in which St. Matthew declared, "For unto everyone that hath shall be given, and he shall have abundance; but from him that hath not shall be taken away even what which he hath." (cited by Merton, 1968: 58)
- Basically, describes a power law in which "rich get richer" or "advantages beget more advantages."
- Berger & Kuckertz examine the operation of the Matthew Effect in venture investing and make a subtle, yet highly under-appreciated claim that effectively clips the "left tail" of the Matthew Effect. That is, while the incumbents accrue more benefits by virtue of incumbent status (not necessarily commensurate value creation or contribution), the new entrants are not exiled into irrelevance. Rather, their empirical study found that more effort--"proof of work" if you will--can overcome the Matthew Effect: "New entrants can probably best compensate their missing status and liabilities of newness by putting in more effort" (Id. at 310).

Details

The Status Quo.

- "Entering status dominated environments as new entrant is difficult endeavor. Accumulated advantages go along with the tendency of incumbents to succeed, whereas entrants are likely to lose (Matthew effect)" (Id. at 293)
- "New entrants to an environment suffer from the so-called liabilities of newness, which result from lacking a history or track record, and links to other players....At the same time, more established and connected actors in the environment acquire resources more easily and earn higher rewards for their actions, which results in the rich getting richer, while the poor are getting poorer, a vicious circle phenomenon Merton (1968) has termed the Matthew effect." (Id. at 295)
- "If new entrants are not in the position to identify and exploit opportunities because of the liabilities they face, there is a need to move into a better position to do so. There are generally two strategies how to proceed on the path to success: To try on one's own or to find a partner. The lone warrior might try to succeed by relying on past experience, externalized, accessible knowledge, or the trial and error approach." (Id. at 296)
- The newness deficit is grounded in legitimate lack (though the energy to overcome is disproportionately challenged): "[T]he new entrant also needs to 'learn the ropes' in the VC industry in terms of organizational knowledge, task mastery, and role clarity, which will be relevant for future deals." (Id. at 297)
- Status signals do have influence in de-risking interactions: "First, status is associated with an extensive social network, access to information, tacit knowledge, and higher quality that can improve both the screening and the value-add effect. Secondly, the status of a VC firm sends a signal to stakeholders outside the VC industry, such as suppliers or customers involved with the startup, that serves to reduce uncertainty and hence can contribute to improved performance." (Id. at 299-300)

Breaking the Matthew Effect: Hard Work and Alliances.

- Alliance formation with high status venture: "Forming alliances leads to the aggregation of expertise, experience, and network resources, and is widely agreed to grant superior competitive advantage." (Id. at 297)
- Especially in tech, experience erodes quickly and becomes a shackling liability if unaddressed: "[M]ore experience does not necessarily equate with greater success, because beyond a certain threshold, a VC firm's experience may even hamper the performance of the firms it invests in." (Id. at 298)
- Work. "[N]ew entrants will have to compensate the lower status by contributing more effort to the partnership...the additional effort can improve the overall performance of the deal, as the value-add effect of the VC firms will be higher." (Id. at 300)
- "New entrants can probably best compensate their missing status and liabilities of newness by putting in more effort." (Id. at 310)
- "That is, new entrants might be able to overcome the burdens of being new, by first learning the ropes from more established players in syndicated deals. Actors, which are not really in the center might be adequate points of first contact, because the high status players prefer especially in contexts of large uncertainty peers in terms of status." (Id. at 310)
- * "[O]ur findings clearly show that new entrants can successfully overcome the burdens of being new and exhibiting low status positions and that an established VC firm is not a necessary condition for success." (Id. at 313)

Main Ideas

- Modern mobile and IoT devices store tremendous amounts of data in a nearly continuous fashion given our devices tend to be "always on" and even, always on us (e.g., Apple watch tracking sleep behaviors). Machine learning models are being applied to this vast data repository, but in "many cases, these ML models are produced (trained) using personal, potentially privacy-sensitive data" (Id. at 19).

Details

Privacy-Aware Decentralized Compute.

- Decentralized AI: "utilizing, in parallel, multiple deices of various processing and storage capabilities belonging to potentially different organizations and individuals to support AI-based services via ML models and ML model training." (Id. at 19)
 - Benefits of decentralized AI over centralized analogue include scalability and data privacy
- Federated Learning: "most popular technique for training models without requiring access to users' raw data." (Id. at 19)
 - Benefits of decentralized federated learning over centralized analogue: attack resistance
- AI Task Offloading: "protocols [that] assist computationally limited devices in performing AI tasks since they may not have the computational capabilities to support efficient training and inference or the storage to save the model's parameters." (Id. at 19)
 - One specific way to offload AI tasks for resource-constrained devices is via Split Learning techniques that work by "offloading parts of the model from computationally limited devices that store/own the data (data owners) to one or more compute nodes that collaboratively train the model with the client." (Id. at 19).
 - Split Learning separates data owners from compute nodes, thus separating privacy-laden data from the ML model training.
- Data owners with computationally constrained devices participate in decentralized Federated Learning protocol with help from Split Learning (i.e., having several compute nodes to allow model training locally)

Issues.

- "By adding more compute nodes to the pipeline, the average train time needed for one batch is reduced, as the workload to apply inference and back-propagation is distributed among the nodes allowing more data owners to be served in parallel....On the other hand, when the batch size is increased the data load transferred between the nodes is greater, thus we have larger transferring and computation time...due to the extra overhead added for the communication between the two compute nodes." (Id. at 22)
- Adding may, potentially non-colluding, compute nodes to a decentralized AI system can lead to multiple new directions for further research, mainly on privacy and security." (Id. at 23)
- "Due to the split learning protocol, a substantial part of a user's updated model will be stored plaintext, to a third party. In addition, in contrast to pure FL [federated learning], data owners also have to reveal additional information, the activations of the split layer." (Id. at 23)
 - But, can homomorphic encryption solve?
- "The assumption that the compute nodes are benign is significantly weak." (Id. at 23)
 - "We strongly believe that Decentralized AI can benefit from the utilization of TEEs in compute nodes." (Id. at 23)
 - However, see [[Problems with TEEs]], arguing that TEEs work fine in centralized systems where the controller has a lot to lose (reputation, e.g.) and not much to gain. However, in decentralized environments, the trust is not presumed and so the asymmetry flows the other way: the entity has much to gain and not much to lose.

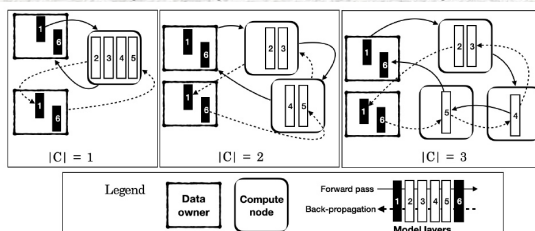


Figure 1: A snapshot from a learning round for three scenarios: (i) having one compute node, (ii) having two compute nodes, and (iii) having three compute nodes

Source: Joana Tirana et al., "The Role of Compute Nodes in Privacy-Aware Decentralized AI" in 6th Int'l Workshop on Embedded and Mobile Deep Learning (July 2022), p. 21

FL architecture w/
multiple compute
nodes.

Main Ideas

- High Level Thesis: Democratization solves (more precisely, substantially reduces probability of) AI malfeasance. Save AI, save the world.

Details

Data Concentration.

Web 2.0



1998: "I sell books."

2017: "I sell whatever the f I want."

Source: Siraj Raval, "Decentralized Artificial Intelligence" at Engineers.sg Meetup, Singapore avail. at YT (video) (2018)

- Implication: as automation accelerates and enmeshes deeper into the fabric of our lives (see [[FN 49_On Cypherpunk Hero]]), data ownership is a critical defense against perverse incentives and misguided intentions (see also [[FN 11_On Dixon Decentralization]], [[FN 12_On Placeholder Thesis circa 2017]], and elsewhere)
- "You have no value if you give away your data" (S. Raval at 8:17). Perhaps hyperbolic, but less so in the envisioned context of exponential automation of our lives.
- "Everything that can be automated, will be automated." (S. Raval at 8:36)

Web 3 Solution Space.

Web 3.0

Shrinking Economy, Data Ownership, Accountability, Towards General Intelligence



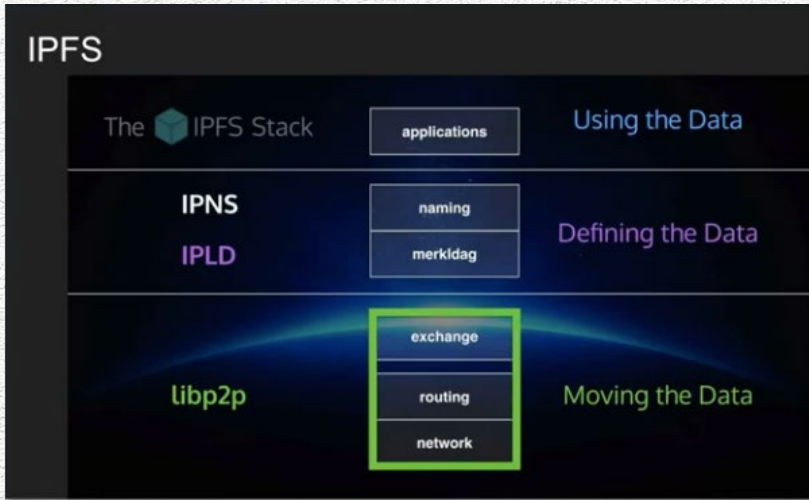
Source: Siraj Raval, "Decentralized Artificial Intelligence" at Engineers.sg Meetup, Singapore avail. at YT (video) (2018)



Details

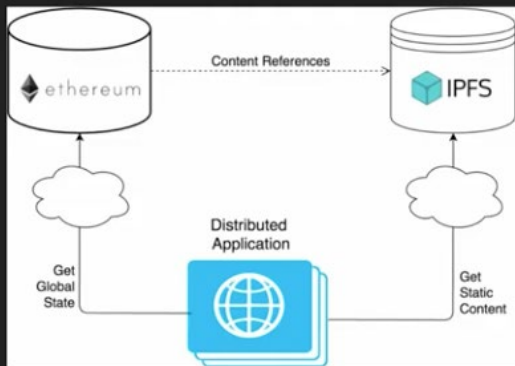
- Requires coordination and composability

IPFS



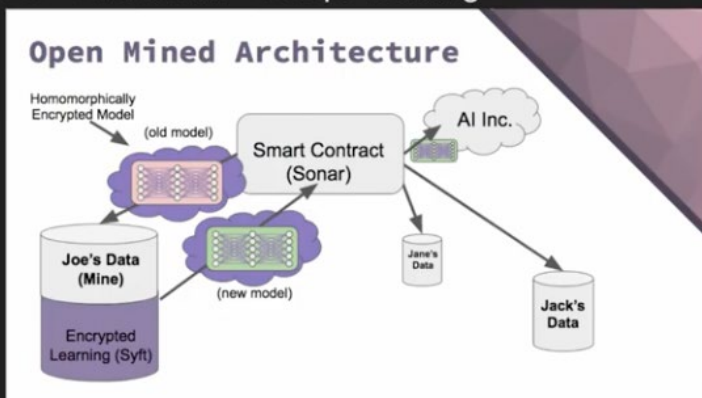
Source: IPFS as presented by Siraj Raval, "Decentralized Artificial Intelligence" at Engineers.sg Meetup, Singapore avail. at YT (video) (2018)

IPFS + Ethereum



Source: IPFS as presented by Siraj Raval, "Decentralized Artificial Intelligence" at Engineers.sg Meetup, Singapore avail. at YT (video) (2018)

IPFS + Ethereum + Deep Learning



Source: Siraj Raval, "Decentralized Artificial Intelligence" at Engineers.sg Meetup, Singapore avail. at YT (video) (2018)

Main Ideas

- The fate of deep learning is tied to solving the computational burden. The computational expense comes from two aspects that increase deep learning efficacy: extremely large data sets and overparameterization that enhances model flexibility (and thus improves chances that predictive features are captured).
- Per Thompson et al. (2022): "[T]he growing computational burden of deep learning will soon be constraining for a range of applications, making the achievement of important benchmark milestones impossible if current trajectories hold." (Id. at 15)

Details

On Overparameterization.

- Example: image classification system CoCa has 2.1B parameters for imagenet's 1.2M datapoints
- "[D]eep learning is intrinsically highly reliant on computing power. This arises from the role of overparameterization and how this scales as additional training data are used to improve performance." (Id. at 2)
- "[T]here are significant benefits to having a neural network containing more model parameters than data points available for training, that is by overparameterizing it. Classically this would lead to overfitting, but stochastic gradient-based optimization methods provide a regularizing effect due to early stopping, moving the neural networks into an interpolation regime, where the training data is fit almost exactly while still maintaining reasonable predictions on intermediate points." (Id. at 2) [unpack to deepen understanding]
- More parameters means more flexibility. For deep learning, fewer parameters is worse because it may miss the predictive features.
- "[W]hile the price of including so many parameters may be high, it also offers flexibility for the model. In contrast, smaller models may be more efficient, but if they do not include the parameters that matter for the answer...this would imply lower RMSE [root mean square error; prediction error] values being unachievable for any amount of computation. In other words, the performance of that model will eventually plateau at a low level as available computation/number of samples increase, since it lacks important predictive features. In contrast, the model with many parameters will eventually achieve a high level of performance, but the cost of more data and computation." (Id. at 4)
- Large neural nets = universal function approximation [follow up], meaning you need large data sets and large parameters.
- "[W]e arrive at the central tradeoff between traditional machine learning methods (like regression) that use small numbers of parameters and deep learning methods that use enormous numbers of parameters. The more parameters that one adds to a model the greater the flexibility and hence potential for better performance. Indeed, it has been shown that sufficiently large neural networks are *universal function approximators*, hence in theory, any desired performance level can be achieved by making the model large enough and including enough training data. But these additional parameters also make the model more expensive to train (even before any needed increase in amount of training data) and can make it do less well when the amount of data (or computation) is not large enough." (Id. at 4)

On Non-Linear Cost Increase.

- "The challenge of overparameterization is that the number of deep learning parameters must grow as the number of data points grows. Since the cost of training a deep learning model scales with the *product* of the number of parameters with the number of data points, this implies that computational requirements grow as at least the *square* of the number of learning networks must grow to improve *performance,* because a linear improvement in performance generally requires a faster-than-linear increase in the amount of training data." (Id. at 2)
- Quartic Function: "[C]ombining the computational overhead from overparameterization and the data requirements for statistical learning yields a back-of-the-envelope estimate that the computation required to train an overparameterized model should grow at least as a fourth-order polynomial with respect to performance....This is, of course, just a lower bound." (Id. at 2)

Hardware Efficiency Gains Don't Solve.

- "Scaling deep learning computation by scaling up hardware hours or number of chips is problematic in the longer-term because it implies that costs scale at roughly the same rate as increases in computing power, which...will quickly make it unsustainable." (Id. at 5)
- For much of the 2010s, moving to more-efficient hardware platforms (and more of them) was a key source of increased computing power. For deep learning, these included mostly GPU and TPU implementations, although it has increasingly also included FPGA and other ASICs. Fundamentally, all of these approaches sacrifice generality of the computing platform for the efficiency of increased specialization." (Id. at 13)



Details

Algorithm Efficiency Gains Don't Solve.

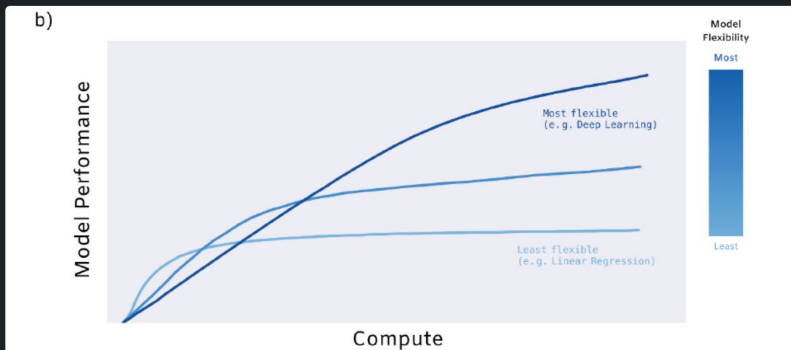
- "[D]eep learning performance improvement is strongly dependent on rapid scale-up of computing power, whether or not algorithmic improvement is account for and whether or not one looks at all models or only cutting-edge ones." (Id. at 7)
- "This rapid increase in computing burden far outpaced the ~35x total improvements in neural network training efficiency." (Id. at 4)

History.

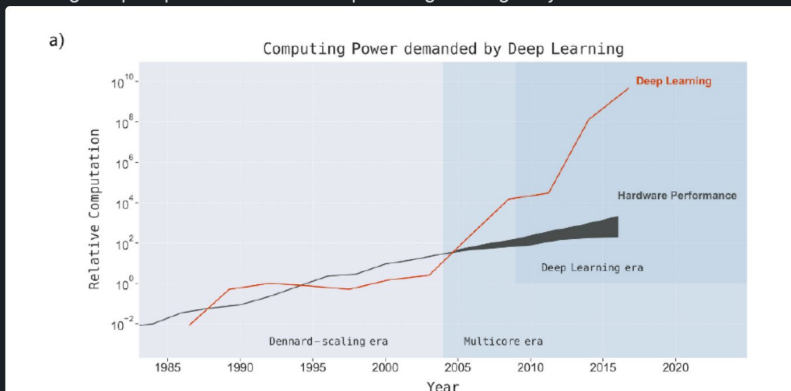
- 1960 Frank Rosenblatt, 3-layer neural network
- Turning point: when deep learning met GPUs and more recently, ASIC-based
- "But the amount of computing power used in the largest cutting-edge systems grew even faster, at approximately 10x per year from 2012 to 2019." (Id. at 4)
- "[A]cross many areas of deep learning, progress in training better models has depended on large increases in the amount of computing power being used. A dependence on computing power for improved performance is not unique to deep learning but has also been seen in other areas such as weather prediction, computer chess, computer Go, and oil exploitation. In those areas there has been enormous growth in the cost of systems, with many cutting-edge models now requiring some of the largest computer systems in the world. This could well be deep learning's fate if current trends continue." (Id. at 10)
- "[P]ace of innovation as researchers find better ways to harness computing power, which Rich Sutton has argued is "the only thing that matters in the long run." (Id. at 11)
- "Deep Learning is facing an important challenge: either find a way to increase performance without increasing computing power, or have performance stagnate as computational requirements become a constraint." (Id. at 13)
- "[D]eep learning's prodigious appetite for computing power limits how far it can improve performance in its current form, particularly in an era when improvements in hardware and performance are slowing. This article shows that the growing computational burden of deep learning will soon be constraining for a range of applications, making the achievement of important benchmark milestones impossible if current trajectories hold." (Id. at 15)

More Model Flexibility, More Computational Intensity

Id. at 3.



Growing compute power for modern deep learning: running away



Details

One-Liners.

- Decentralization ethos and complexity theory are connected: "One of the key messages that comes from complexity is that you should work with fine-grained objects, leverage distributed cognition, and ensure disintermediation." (Id. at 2)
- "[O]ver-constraining a complex situation leads to chaotic behavior" (Id. at 42)
- Goal of managing emergence and insights (paradox)

The Motivation.

- "[O]ne of its [Cynefin framework's] most valuable uses is for development of a model that reflects the context and the uniqueness of each organization." (Id. at 21)
- Complex domains require multiple hypotheses, ideally tested in parallel.
 - ✓ "[W]e are not looking for the right answer but for a series of ideas that we can test to find out what works, as more than one idea may be viable. The complex domain is the domain of multi-hypotheses, so aim to run a number of parallel experiments that test these hypotheses and maximize the potential for learning." (Id. at 11)
- Resist reduction (not to be confused with simplicity / heuristics-based tactics) in the face of complexity.
 - ✓ "This is a significant change from the more traditional approaches, which try to reduce a problem to a set of rational actions and acknowledges that in some instances we cannot predict the outcomes. Instead of obsessing about predicting the future, we can move to controlling the future, and we therefore don't need to predict everything." (Id. at 12-13)
- "[O]ver-constraining a complex situation leads to chaotic behavior" (Id. at 42)
- Distinguish between ideas and options. "[E]xplore all the possibilities to establish the options." (Id. at 31)
- "We are not trying to establish if a hypothesis is right or wrong, only that there is enough coherence to support an experiment." (Id. at 31)

Against Over-Indexing to Porter 5 Forces Style Analysis in Unordered Systems.

- "This is a significant change from the more traditional approaches, which try to reduce a problem to a set of rational actions and acknowledges that in some instances we cannot predict the outcomes. Instead of obsessing about predicting the future, we can move to controlling the future, and we therefore don't need to predict everything." (Id. at 12-13)
- Contextualization: "data precedes the model, unlike the traditional pattern of the model coming before the data....[W]e don't draw the model beforehand but let the domains and, in particular, the boundaries develop as part of the process." (Id. at 21)

The Framework Components

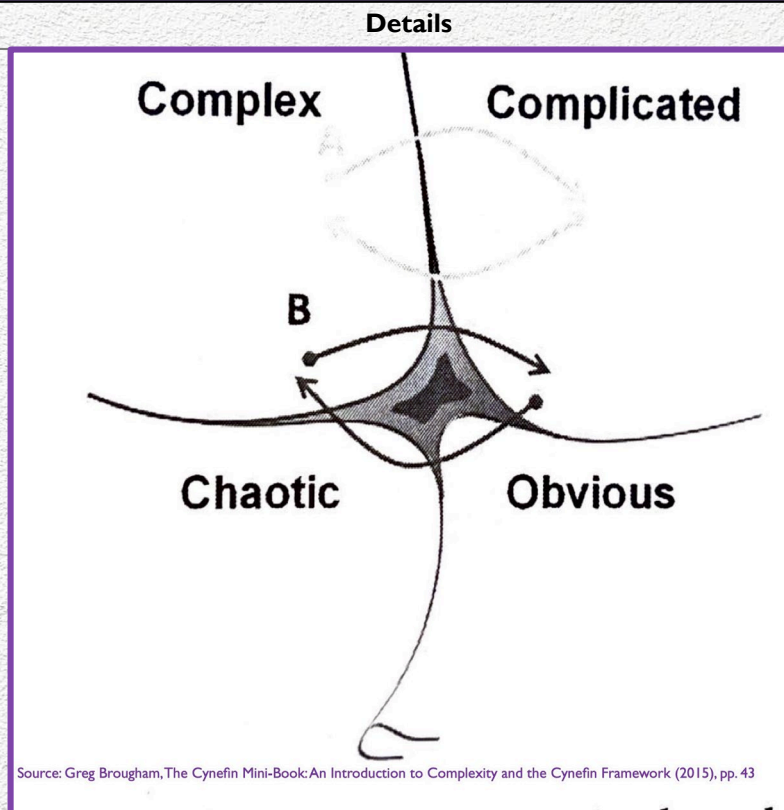
- Ordered System
 - ✓ highly constrained
 - ✓ predictable behavior
 - ✓ obvious causal links
 - ✓ extrapolation is legitimate
 - Subsystem / Degree: Obvious vs. Complicated
 - Obvious: cause and effect are evident from experience
 - Complicated: cause and effect are separated by time, requiring analysis to solve
- Unordered System
 - ✓ dispositional in nature, meaning has a movement (evolutionary or devolutionary, but not stasis)
 - ✓ causality only determined ex post, not ex ante
 - Subsystem / Degree: Complex vs. Chaotic
 - Complex: cause-effect apparent in hindsight
 - Chaotic: randomness
- The Fifth Domain: Dis-Ordered : transitional, unclassified state (not a permanent location)

On Dispositionality.

- There is movement, not stasis in and through complex systems: "[C]omplex systems are dispositional in nature, meaning that they are disposed to move or evolve in a certain direction, but we cannot determine causality so the only way we can manage this type of system is by probing, sensing, and responding. That is, we run a series of experiments to see if we can move the system in a direction that is desirable or beneficial to us." (Id. at 32)

Adopt All 3 Logical Models: deduction, induction, abduction (hunch-driven, "lead backwards")





	NATURE	RESPONSE	PREPARE
CHAOS	Unknowable unknowns Temporary state - no time No evidence of any constraint High turbulence no patterns Old certainties no longer apply	Act-Sense-Respond Speed of authoritative response vital Follow and enforce heuristics Focus on constraints not solution Use the opportunity to innovate	Establish heuristics & Parables Human sensor networks Crews as crisis management teams Simulation games for key managers Multi-perspective dissent feedback
COMPLEX	Unknown unknowns Messily coherent, patterns discernible Partial changing constraints Flux within stabilities Evidence supports contradiction	Probe-Sense-Respond Monitor safe-to-fail experiments All contradiction within heuristics Flex constraints to manage emergence Agility key to amplification/dampening	Create time and space for reflection Human sensor networks operational SNS & like to create networks Scenario planning (inc. micro) Build and monitor 'requisite diversity'
COMPLICATED	Known unknowns Ordered, predictable, forecastable Constraints evident and enforceable Stable with constraints Evidence susceptible to analysis	Sense-Analyse-Respond Determine experts or process to resolve Manage & enforce process Monitor effectiveness of constraints Focus on exploitation not exploration	Right people & process, right time Process engineering with feedback Diversity of experts in network Sound analytical practice Stand aside but stay in touch
OBLIVIOUS	Known unknowns Familiar, certain, well worn pathways Constraints self-evident to all Stable within universal constraints Self evident solutions	Sense-Categorise-Respond Ensure sound process in place Monitor for noncompliance & deviance Test for complacency Protect some pet mavericks	Watch for outliers Usable process Right support people for key staff Automate, but not automata Anonymous appeal/whistle blowers

Source: Greg Brougham, The Cynefin Mini-Book: An Introduction to Complexity and the Cynefin Framework (2015), pp. 9

Main Ideas

The strict linkage between the cypherpunk and the libertarian--which linkage can be traced to a 1993 Wired cover story by Steven Levy () "Crypto Rebels" <https://www.wired.com/1993/02/crypto-rebels/>--is misleading, betraying nuance and depth of the movement.

Details

One-Liner.

- "If the shaman is the necromancer, the one who bridges the gap between life and death, the neuromancer is the one who bridges psychological life and technology." (Id. at 12)

Cypherpunk Origin.

- Cypherpunk was a community of hackers in Silicon Valley, formed in the early 1990s by by Tim May of IBM along with Eric Hughes and John Gilmore. Initially organized as a group of 16 people who would meet every Saturday in an office building near Palo Alto, spawning an unmoderated, pseudonymous, anonymous newsletter that included famous people like Julian Assange, Whitmore Diffie (co-creator of public key cryptography), Nick Szabo (pioneered smart contracts), Hal Finney (believed by some to be Satoshi Nakamoto), David Chaum (father of digital cash precursor to Bitcoin).
- Term cypherpunks is a combination of the British spelling of "cipher," standing for secret / code. Designation credited to Jude Milhon (https://en.wikipedia.org/wiki/Jude_Milhon).

The Socio-Techno-Political Motivation.

- Taking cues from postmodern Frankfurt School and specifically, Michel Foucault (see, e.g., "biopolitics"), the cypherpunk movement organized against the center.
 - ✓ "The key question at the heart of the cypherpunk movement was not freedom, but the crisis of freedom in a situation of extensive social control of dominant institutions over private individuals." (Id. at 3)
 - ✓ Response and Responsibility: "cypherpunk movement reacted to the perceived emergence of a surveillance order in a post-industrial era and the way in which it has subtly eroded the democratic fabric of American society and ultimately human freedom." (Id. at 3)
 - ✓ Goal of movement: "They envisioned that the Internet would make more pervasive the phenomenon of surveillance of individuals; their goal was to develop tools to secure communication and trade on the Internet and avoid government surveillance." (Id. at 13)
 - ✓ Blockchain, BTC, decentralization, and related terms act as pragmatic vehicles for the cypherpunk hero. "Successful distributed technologies such as Bitcoin and Blockchain have given new life to the ideas of the cypherpunk movement." (Id. at 16)

The Cypherpunk Hero.

- The hero exists and redefines the boundaries as a way to re-orient the central local of power without hopefully re-creating it in different guise. This risk is apparent with the wave of "pseudo-punks" merely masquerading as mission-driven rebels.
- "[T]he cyberpunk is a technological rebel who rejects the invasive relationship with technologies, a relationship in which human minds are exploited while they are navigating intense, complex, immersive digital realities." (Id. at 12)
- "The cyberpunk hero is a hacker who lives on the edge of society, an alienated loner in a dystopic society driven by rapid technological progress. He/she resists giant corporations and their plans to colonize users' minds and resists technocratic governments and their aim to control their citizens." (Id. at 12)

The Panopticon.

- Metaphor (and physical structure) geared toward conformity and enforcing normativity.
- Panopticon: "an ideal prison designed to keep inmates under observation at all times. In Bentham's mind, control can be equated to behavior modification, in the sense that inmates feel compelled to regulate their own behavior because they know they are being watched at all times....technocratic totalitarianism can probably be crystallized around the notion of a reverse Panopticon, in which citizens are subject to behavior modification without acknowledging it." (Id. at 5)

Main Ideas

- Structure: Data <--> Information <--> Knowledge <--> Wisdom
- Activity: Background Research <--> Evaluation Assessment <--> Variant View <--> Bet
- Tool: Information Diet <--> Investment Framework <--> Written Product <--> Position Sizer

Details

Problem: Info Overload.

- "Not only are we in some danger of being supplied with a surfeit of information, but the networking of networks, including the Internet of the global village, is in danger of degenerating into anarchy and the lawlessness of an information jungle." (Id.)
- Signal: Noise; the medium != the message. "Modern IT as applied in networking enables us to have much better systems of communication with our fellow human beings across the world, but we have to ensure that what we communicate advances our mutual understanding as well as increasing our mutual stores of information. Much confusion over this has been introduced by concentration on the growth of IT to the neglect of concern about the content of the information transferred." (Id.)

Consecutive + Integrated Thought = Super Power.

- The "growing mind to develop its power of creativity...needs to exercise itself on intricate and detailed structures of ideas, and not just on statements of facts, simply stated one after another, in random order and with no consideration of their interrelations." (Id.)
- **On linked learning:** "The point is that a random thought must find a place to fit in an existing context in order to make sense. Otherwise, it finds difficulty in obtaining an anchorage, a pattern in which it can fit, unexpectedly, and become fixed and a permanent part of an enlarged context." (Id.)
- **Significance is found in the liminal.** "We need time to reflect, to consider, to consult a range of comment by different minds. We should therefore not take any new fact, or piece of equipment, however interesting or marvelous, and look at it in isolation. In systems terms, it is the tensions and interconnections between the elements of a situation, or parts of a machine which provides the dynamic force for its development, and its significance."
- **Different media types (print, audio, video) enhance one another.** "These examples underline the value of attending to the interrelations between the different media, and of the ways in which each can be used to enhance the effectiveness of the others."

Data.

- First stage of cognition
- Single items, atomic units, bits
- "While these data have not yet been organized into systems of relationships, they have no special significance for us beyond the fact that they are there."

Information.

- Linked data, connections, organized data, relationships forming a system of ideas
- "The distinction [between data and information] is real because the process of organizing is real and requires a conscious mental activity. It is possible because we have the power of the imagination: we can convert the isolated percepts into organized concepts, and this is the secondary stage of cognition." (Id.)

Knowledge.

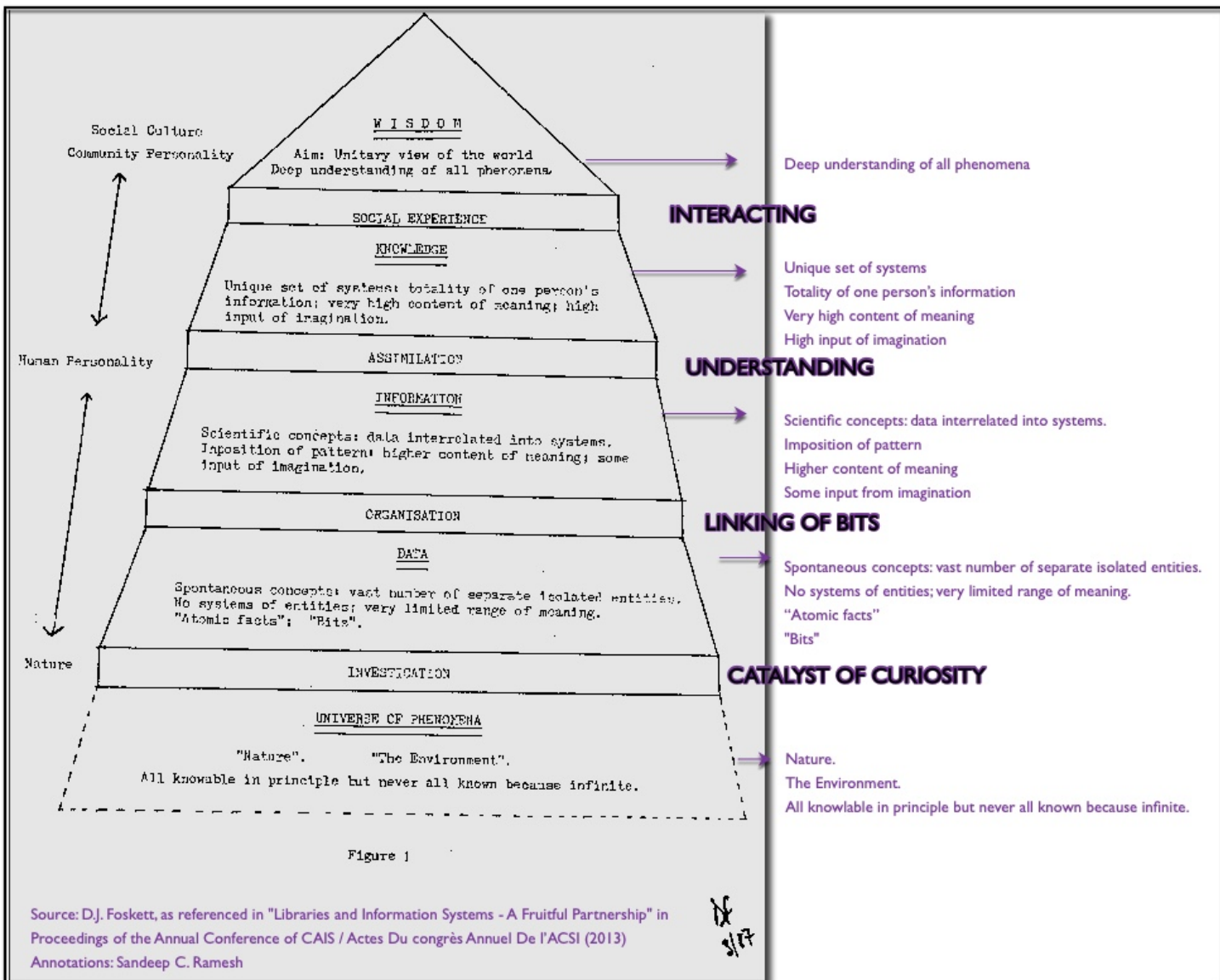
- Structured information that has been assimilated by the subject mind
- Knowledge draws globally, but is built locally
- Knowledge is inherently unique: "This is more than a store of information, even though most of its content may be public, known to other people. But nobody knows just what I know, and however hard I try, and however patient my audience may be, I can never say everything I know, I may be able to communicate information...[B]ut I cannot communicate knowledge." (Id.)

Wisdom.

- Transforming knowledge to wisdom requires communicative interactions: "[T]he means by which knowledge can become wisdom through social experience is communication." (Id.)
- Wisdom, unlike knowledge, can be communicated since it is a "distilled essence of knowledge, and not the whole of it." (Id.)



Details



Main Ideas

- "Federated learning (FL) can realize a distributed training machine learning models in multiple devices while protecting their data privacy, but some defect still exists such as single point failure and lack of motivation. Blockchain as a distributed ledger can be utilized to provide a novel FL framework to address those issues." (Id. at 302)
- 4 Problems with Current Federated Learning Approaches (which Blockchain Architectures Can Address):
 1. Single point of failure
 2. Poison attack
 3. Lack of motivation (lack of voluntary data contribution)
 4. Privacy leakage

Details

Federated Learning Defined.

- Distributed machine learning method
- Proposed in 2016 by Google to train local data while protecting user's on-device privacy
- Federated learning methods can solve data silos and privacy leakage problems of more traditional machine learning approaches
- "Multiple devices are scattered to execute machine learning algorithms locally. The trained local updates are submitted to a central server and aggregated to optimize the global training parameters. Compared with traditional machine learning, [Federated Learning] can address data island issues and prevent the leakage of local data privacy." (Id. at 302)

Blockchain's Relevance.

- Building secure system in environment of low trust is needed to amalgamate large data sets suitable for model training
- "Blockchain distributed trust provides a novel method to design FL frameworks and paradigm. Blockchain can ensure secure interaction in an untrusted environment through transaction records and distributed consensus, so FL can work in the context of blockchain. At the same time, the consensus and incentive mechanism are naturally suitable for building an economic market, which can effectively stimulate the sharing and interaction of information in FL." (Id. at 302)

Problems with Current Federated Learning Approaches.

1. Single Point of Failure.
 - Status quo federated learning approaches rely on trained local updates submitted to central server, then aggregated for global training parameters
 - Central server vulnerability to attacks and downtime mean that "local model updates are distorted, and the accuracy of subsequent local model updates are undermined." (Id. at 303)
 - Central server overload: "[W]hen a number of models are transmitted simultaneously, the central server may overload the network due to bandwidth limitation." (Id. at 303)
2. Poison Attack.
 - Poison attack defined: "Cyber poison attacks alter the area where the computer system makes smart decisions. The attacker creates a loophole in the core data rule and trains the system to adhere to that rule to exploit it. As a result, the system's data model becomes skewed, and the output is no longer as originally intended.
 - Traditional federated learning lacks ability to audit compromised trainers.
 - "Thus, malicious clients can adversely affect the global model by intervening in the local model to upload incorrect mask gradients and unsponsored shares to the center server." (Id. at 303)
3. Lack of Motivation.
 - Standard federated learning methods assume that local devices contribute data resources voluntarily
 - "Participants lack the incentive to execute model training because they apply their data and computing resources. Selfish mobile devices will be reluctant to participate in model learning without impartial financial compensation." (Id. at 303)
4. Privacy Leakage.
 - "FL frameworks leak the privacy of training data, even if the training resource is stored in the local device." (Id. at 303)
 - "A malicious center server is also able to exploit sensitive information by Generative Adversarial Network (GAN)." (Id. at 303-304) [follow up]



Details

TABLE II
SUMMARY OF DIFFERENT BFL ARCHITECTURE IN TERMS OF SOLVED ISSUES, TYPE OF BLOCKCHAIN, CONSENSUS MECHANISM.

Architecture	Solved issues	Type of blockchain	Consensus mechanism
✓ BlockFL [7]	Single point failure, lack of motivation	Public	PoW
✓ FLChain [8]	Single point failure, lack of motivation	Public	—
FLChain [9]	Single point failure	Public	PBFT/PoW
RFL [10]	Poison attack, lack of motivation	Consortium	PBFT
✓ DeepChain [11]	Single point failure, lack of motivation, privacy leakage	Public	Blockwise-BA
FedBC [12]	Single point failure, privacy leakage	—	—
✓ BC-FL [13]	Single point failure, lack of motivation	Public	PoW
✓ BlockFLA [14]	Single point failure, poison attack, lack of motivation	Public & private	PoW & PBFT
Chain FL [15]	Single point failure	Private	PoA
PSFL [16]	Poison attack	—	—
✓ BFEL [17]	Single point failure, poison attack	Public & consortium	DPoS/PBFT & PoV
✓ Biscotti [18]	Single point failure, poison attack, privacy leakage	public	PoF
✓ VFChain [19]	Single point failure, poison attack	Public	Algorand
✓ BLADE-FL [20]	Single point failure	Public	PoW
✓ BFLC [21]	Single point failure, poison attack, lack of motivation	Public	Committee
✓ VBFL [22]	Single point failure, poison attack, lack of motivation	Public	PoS

Source:

Dongkun Hou et al., "A Systematic Literature Review of Blockchain-Based Federated Learning Architectures, Applications and Issues" in 2nd Info.

TABLE IV
SUMMARY OF APPLICATIONS OF BFL.

Application field	Function	Refs
Industrial IoT	Device failure detection	[36]
	Data sharing	[37]
Edge computing	Content caching	[38]
Fog computing	Cloud application	[39]
Internet of Vehicles	Traffic and road analysis	[40]
	Knowledge sharing	[41]
	Data sharing	[42]
Smart grid	Power consumption prediction	[43]
Heavy haul railway	Intelligent control	[44]
Medicine	Predictive diagnosis by IoHT	[45] [46]
	COVID-19 detection by CT	[47]
	Predictive diagnosis by records	[48]
Location prediction	Next-Location prediction	[49]
Unmanned aerial vehicles	Mobile crowdsensing	[50]
	Disaster response	[51]
News	Recommendation scheme	[52]

Source:

Dongkun Hou et al., "A Systematic Literature Review of Blockchain-Based Federated Learning Architectures, Applications and Issues" in 2nd Info. Comm. Tech. Conf. pp. 302-307 (May 2021)

Main Ideas

Source: Juan Benet, "What Exactly Is Web3?," talk at Berlin Web3 Summit 2018 avail. online (Oct. 2018)



Web 3.0 is a broad movement and a group of associated technologies aiming to make the web and the internet more decentralized, verifiable, and secure.

The goals of Web 3.0 include (a) trustless infrastructure; (b) removing intermediaries; and (c) giving users power and ownership over their data, identity, security, and transactions.

The technologies add capabilities and functionality for securely linking data and programs, cryptographic verifiability, transaction processing, P2P connectivity, and trustless interoperability. They also provide decentralized computation and storage, enabling fully autonomous applications (dapps). The movement includes many blockchain and dweb projects, as well as some linked data efforts.

see e.g., semantic web

Details

The Context.

- Epistemological confusion surrounding meaning of web3
- Experiential lacuna confronting crypto natives to actually understand the magnitude of the shift from pre-computing to post-computing world
- Hyperbolic discounting adds to the difficulty to appreciate exponential or phase-like transitions
- Constraints of the software systems and underlying architecture structure the outcomes; there is a sensitivity to initial conditions that arguably have led to significant negative consequences such as data monopolies (see, e.g., [\[\[FN 43_On DeAI\]\]](#))

The History.

- Technological development in waves: mainframes > pc > gui > internet protocols > web 1.0 > web 2.0 > mobile > blockchains > web 3.0
- Web 1.0 was characterized by read-only and static nature
- Web 2.0 was characterized by read-write and dynamic / interactive nature, spawning social networks, e.g.
- Web 3.0 is building verifiability at the core layer, which enables read-write-trust triptych
- The progression of linking: from linked content (1.0) to linking programs to content (2.0) to linking content and programs to each other (3.0), losing intermediary layers while gaining public verifiability

Web 2.0 and Web 3.0.

- Web 3.0 keystone property is verifiability.
- Variant perception is that many don't fully understand the implications of having a verifiable layer embedded in the underlying protocol (recall the assumption about sensitivity to initial conditions at the protocol and infrastructure layers that necessarily inform how we interface with internet and each other)
- Hypertext analogy: term coined in 1965 but use case in the web 1.0 didn't manifest for decades later. At the time many couldn't envision the evolution from hypertext to the web. This is a specific example of Amara's Law (see [\[\[FN 10_On Amara's Law + Exponential\]\]](#))
- Gavin Wood's definition of web 3.0: "an inclusive set of protocols to provide building blocks for application makers. These building blocks...present a whole new way of creating applications. These technologies give the user strong and verifiable guarantees about the information they are receiving, what information they are giving away, and what they are paying and what they are receiving in return." [\[\[FN 32_On Web 3 pre-Buzzword, per Gavin Wood\]\]](#)



Details

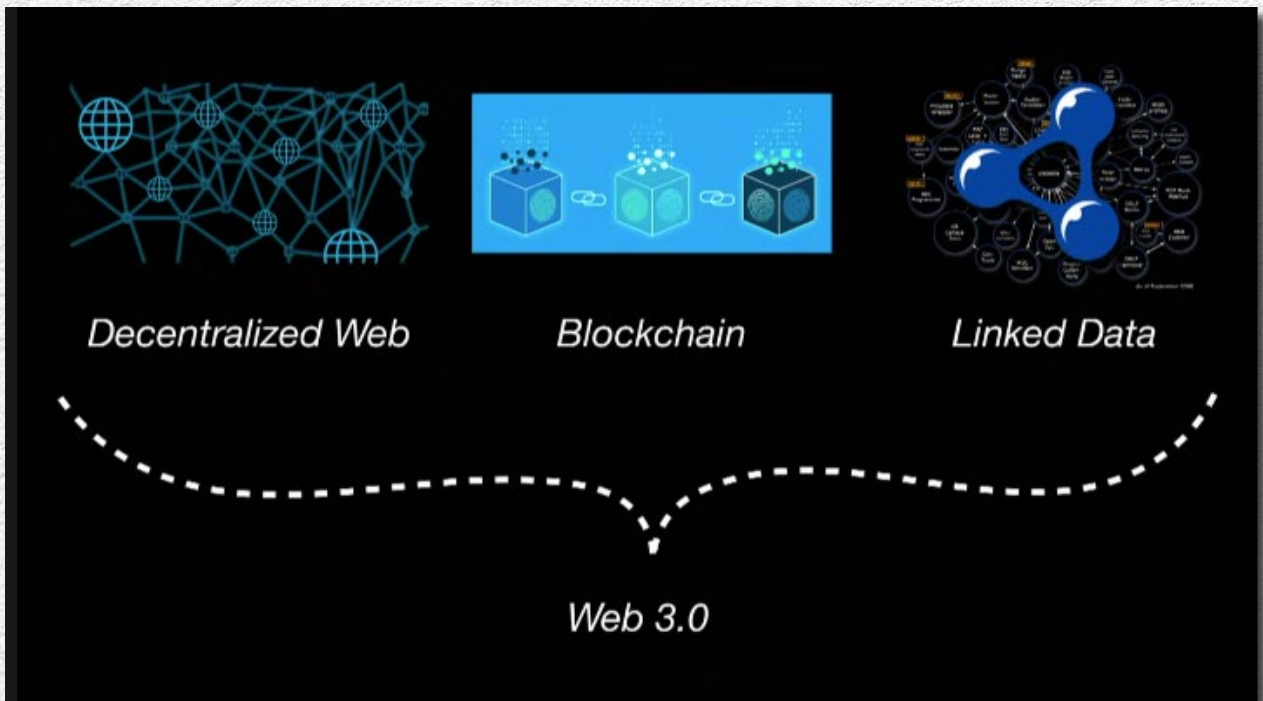
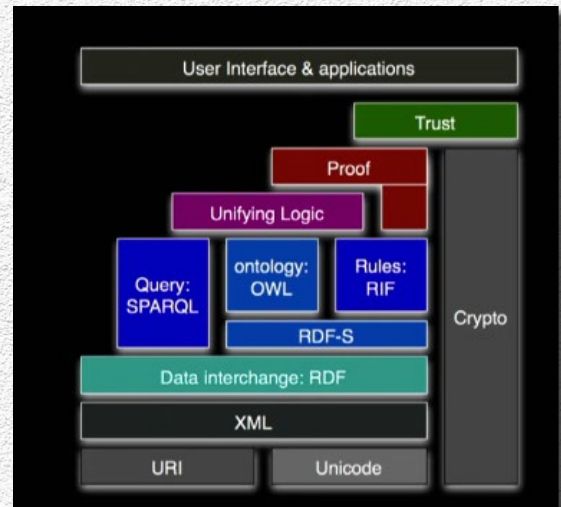
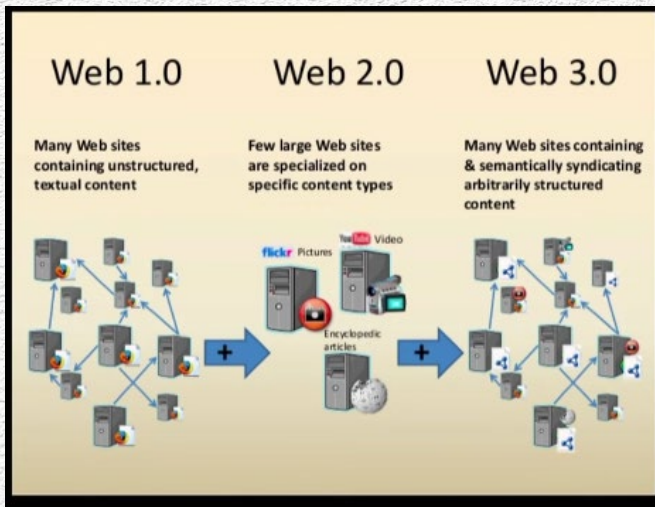
Blockchain Utility.

- p2p movements are disadvantaged vs. centralized incumbents given lack of economic resources to enable true competition
- Economic models of blockchain enable this competition (see [\[\[FN 29_On Token as Killer App\]\]](#))
- Blockchain use case foundations keyed to decentralizing computation and decentralizing storage, which allows for fully autonomous applications that don't require system administrator (see e.g., [\[\[FN 25_On Public Blockchain and Power to Root Users\]\]](#))

Breadcrumbs.

- Barlow, "Declaration of Independence of Cyberspace"
- Tim Berners-Lee and SOLID / pods / semantic web3

Source: as presented in Juan Benet, "What Exactly Is Web3?," talk at Berlin Web3 Summit 2018 avail. online (Oct. 2018)



Main Ideas

- Decentralized compute "creates a freer and cheaper base from which to research and develop artificial intelligence." (Id.) Solving the bottlenecks of state dependency and computational expense are critical steps.
- "Vastly increasing the scale of accessible compute, whilst simultaneously reducing its unit cost, opens the door to a completely new paradigm for deep learning for both research and industrial communities." (Id.)

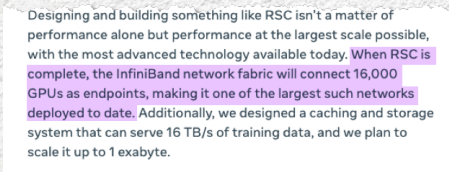
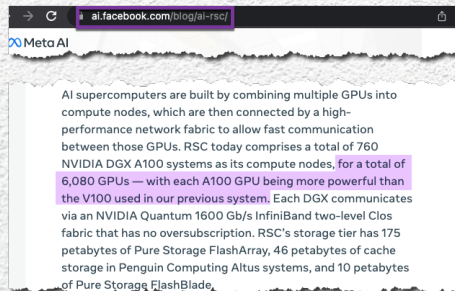
Details

The Status Quo.

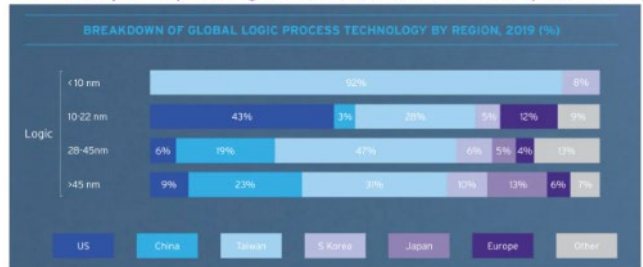
- Deep learning is both ubiquitous, embedding itself in the daily fabrics of our lives in both subtle and overt ways:
 - ✓ "Every face you see on a video call and all the audio you hear is manipulated. To improve call quality, neural networks selectively adjust the resolution in Zoom and suppress background noise in Microsoft Teams." (Id.)
 - ✓ * "In 2020, a neural network operated the radar on a US spy plane, language models now write better scam emails than humans, and self-driving car algorithms outperform humans in many environments." (Id.)
- Deep learning has been hyped and sensationalized, but advances are real.
 - ✓ 2016 AlphaGo beats Lee Sedol, world Go champion.
 - ✓ 2017, updated AlphaGo Zero beats prior version by starting from scratch with random moves, effectively self-learning for 40 days over 30 million games.
- However, the current state of AI merely scratches the surface, and a closer approximation to human intelligence likely requires Artificial General Intelligent (AGI, "strong AI"). [N.B. purposely avoiding a confrontation with notions of "consciousness" in the philosophical & spiritual treatments]

Problem 1: Centralization of Compute Is Accelerating.

- BigTech Hardware Colonization
 - ✓ Meta/FB announced the AI Research SuperCluster ("RSC") with a mid-2022 vision of 16,000 GPU endpoints, establishing one of the fastest AI supercomputers in the world; and, Sino-US & geopolitical frictions on display.



Source: Gensyn, "Deep Learning's New Infrastructure," avail. online (March 7, 2022)

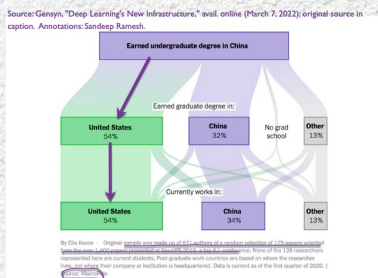


Chip war: US-aligned countries dominate the sub-22nm chip production process.

- ✓ This Big Tech centralization of the hardware and data layers creates large expense load and increasingly impoverished privacy / control protections.
- ✓ AWS operating margins ~30%; estimates of gross margins ~60% [n.b. validate GM est.]

Problem 2: Brain Drain.

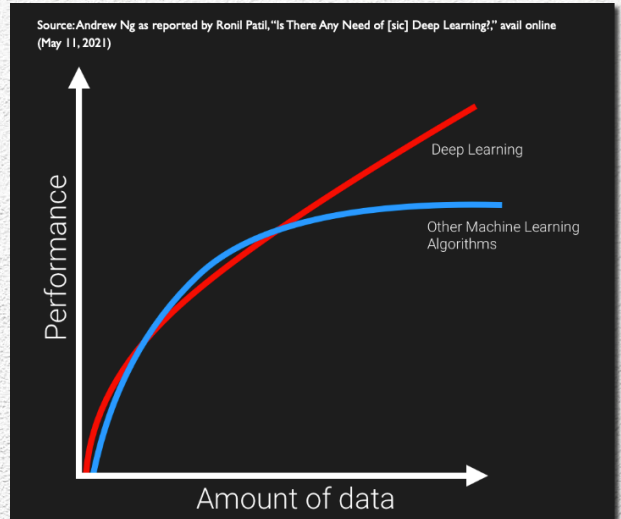
- Issue can be reframed as centralization of talent, creating chokepoint in innovation.



Details

Problem 3: Insatiable Data Need

- Deep learning models perform better with large data



The Solutions.

- Solve cost and control burdens by (a) decentralizing compute (i.e., breaches the margin moats of Big Tech) and (b) building open and transparent access via public permissionless blockchain.
- Main bottlenecks to decentralized compute:
 - ✓ State dependency: neural network "requires the state of the previous layer....[and] all the weights in every layer are determined by the previous step. So if you want to verify that someone has trained a model...you need to train the model all the way up to that point, which is very computationally expensive." (Id.)
 - ✓ High financial cost: "It cost ~\$12m in 2020 for a single training run of GPT-3, > 270x more than the estimated ~\$43k for the 2019 training of GPT-2." (Id.)
 - ✓ The cost is exponential: "In general, model complexity (size) of the best neural networks is currently doubling every three months." (Id.)
- To solve these technical challenges, decentralized compute solution requires a "system that trustlessly manages state dependent verification whilst also being inexpensive in terms of overhead and rewarding to those who contribute compute." (Id.)
- Gensyn-specific approach: (a) solution to state-dependent verification through "model training checkpoints with probabilistic checks that terminate on-chain...trustlessly" with "overhead [that] scales linearly with model size (keeping verification costs constant)." [N.B. follow up]; and (b) widening supply of GPUs by leveraging slack compute (e.g., under/un-used gaming GPUs and ETH miners that will be rendered unnecessary in PoS transition)

Source: Gensyn, "Deep Learning's New Infrastructure," avail. online (March 7, 2022)

Service	Est. \$/h for NVIDIA V100 (or eqv)	Scale
Ethereum	\$15,700	Low
GCP on-demand	\$2.50	Medium
AWS on-demand	\$2.00	Medium
AWS spot instances (unreliable)	\$0.90	Medium
GCP spot instances (unreliable)	\$0.75	Medium
Gensyn (projected)	\$0.40	High
Single GPU in data centre	\$0.40	Low
Single personal GPU	\$0.28	Low

High scale + low cost: the Gensyn protocol provides a cost similar to an owned GPU in a data centre at a scale which can surpass AWS. (Prices as at Nov 2021).

Breadcrumbs.

- Notion of web 3 as combination of web 1 decentralization & web 2 capitalism
- Functional Encryption and data-level privacy: e.g., Alice has $a = 3$, $b = 5$; Bob wants to compute $a+b$ without knowing that $a = 3$, $b = 5$ [N.B. follow up <https://blog.openmined.org/privacy-teaching-series-what-is-functional-encryption/>]

Main Ideas

- It's far better to be convex than to be "right" or "smart"
- Attitudes toward how the world, knowledge, and markets are structured necessarily informs investment strategies and decisions
- Two main epistemological frames: convergence and divergence

Details

Primary Philosophical Attitude: To Converge or Diverge.

- Individual investment decisions stem from an underlying assumption about how a given market operates.
 - ✓ "A good description of style should include a philosophical framework that embodies a worldview of market behavior" (Id. at 77)
 - ✓ "The development of a simple taxonomy for trading style based on a worldview can serve as an important differentiator among money managers and provide insight on how managers expect to generate returns." (Id. at 77)

Divergent Attitude Assumes a Complex, Unpredictable World.

- "Divergent traders accept the limitations in one's ability to understand all of the structural linkages between supply and demand....For a divergent trader, the world is complex and hard to understand." (Id. at 79)
- "Most investors would characterize themselves as convergent traders and believe that they have the cognitive powers to know fair value in order to buy cheap and sell rich assets. Unfortunately, a changing environment makes this extremely difficult. While markets are humbling environments, an alternative of doing nothing may not be appropriate." (Id. at 79)
- "Value investors have a strong confidence of knowledge (low ignorance) relative to the market. A convergent trader will naturally gravitate toward negative convexity trades either in options or in fixed-income." (Id. at 80)

Impact of Fundamentals Contingent upon Realized vs. Theoretical Volatility Difference.

- "Markets are clearly driven by volatility in fundamental news but the portion of volatility that can be explained by fundamentals may be small related to actual volatility, the volatility measured in a market. The greater the discrepancy between theoretical volatility, which can be explained by fundamental factors, and actual volatility will suggest the value of one strategy over another." (Id. at 80)

Converge AND Diverge (but it's hard in a single platform)

- "If there is a desire for broad diversification, holding only one type of worldview will expose a portfolio to unique and powerful risks that can have significant effect on performance." (Id. at 81)

EXHIBIT 1

Convergent versus Divergent — Worldview

Convergent	Divergent
Stationary, stable world.	Non-stationary, unstable world.
World is knowable and static; structural knowledge.	World is uncertain and dynamic; structural ignorance.
Market participants generally form rational expectations; errors are random.	Market participants form rational beliefs but may make mistakes and have biases.
Market adjusts relatively quickly to new information.	Learning takes time; slower adjustment to information.
Divergences from equilibrium are short-lived.	Divergences exist and may be dramatic.
Fundamentals do not change dramatically in the short run.	Fundamental changes are often unanticipated.

See also Knightian risk vs. uncertainty (gradient, not binary)

Also information cascades, reflexivity

Tails can be extreme; long volatility

Rzepczynski, "Market Vision and Investment Styles: Convergent versus Divergent Trading" in J. of Alt. Investments (Winter 1999)

EXHIBIT 2

Convergent versus Divergent — Trading/Return Behavior

Convergent	Divergent
Strong sense of fair value.	No prediction of fair value.
Arbitrage trading; value trading; contrarian.	Trend-following; momentum trading.
Negative convexity trades.	Positive convexity trades.
Profits made from reversion to the mean.	Profits made from the extremes; "mean fleeing" expectations.
Concave payoff functions.	Convex payoff functions.
Negatively skewed returns.	Positively skewed returns.

Rzepczynski, "Market Vision and Investment Styles: Convergent versus Divergent Trading" in J. of Alt. Investments (Winter 1999)

Details

EXHIBIT 3

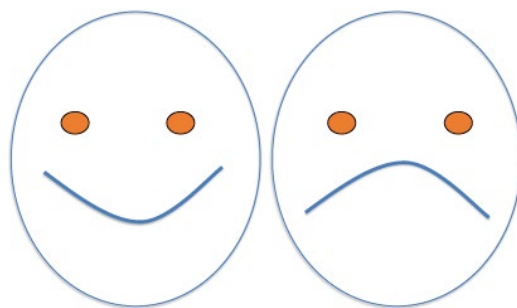
Convergent versus Divergent Trading
by Asset Type

Asset Type	Convergent	Divergent
Equity	Value-based; contrarian; pairs trading.	Momentum, growth.
Fixed-Income	Arbitrage; credit value decisions.	Interest rate directional.
Hedge	Arbitrage (fixed- income, convertible); long-short equity; sector fund.	Managed futures.
Currency	Arbitrage; fundamentals.	Trend-following.

Rzepczynski, "Market Vision and Investment Styles: Convergent versus Divergent Trading" in J. of Alt. Investments (Winter 1999)



Benefits

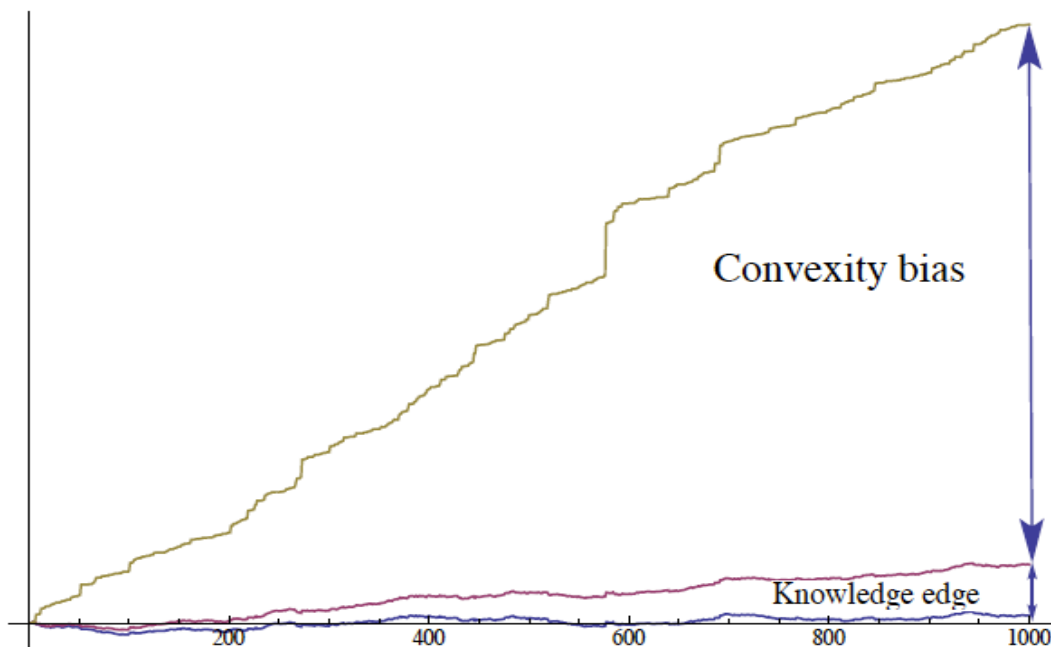


Source: Nassim Taleb, Real World Risk Institute (Nov. 2021)

70



Performance



Source: Nassim Taleb, Real World Risk Institute (Nov. 2021)

Main Ideas

- Conventional AI services are centralized (central controller, mediator, governor, task executor), limited at design stage (inflexible, less responsive to change and dynamical systems), and display poor functionality in terms of reliability and scalability.
- Distributed AI is a movement in the right direction, but still shares resources with centralized servers.
- Decentralized AI aims to flatten centralization fully.

Details

Decentralization != Buzzword.

- "Decentralization is not a buzzword, hype or myth, although such concerns have been widely raised on decentralization-oriented initiatives, such as Web3 and the metaverse. Decentralization is also not a new or mysterious concept. It has a 200-year history and is ground in political science (such as subsidiarity, democracy, liberty, equality, and the decentralist movement), management and decision science (e.g., systems theory, self-organization, and self-determination), and economics (e.g., decentralized free markets and fiscal decentralization)" (Id. at 6)

From Distributed to Decentralized, a Further Flattening of Designed Coordination to Ad Hoc Interactions.

- "P2P and D2D authentication, collaboration, and communication at running time replace the design-time protocols and specifications for authentication, collaboration, cooperation, communication, and governance. This shift from distributed loose couplings to *ad hoc* and running-time P2P interactions enhances the effect of decentralization." (Id. at 7)

From Web 1.0 to 3.0.

- Web 1.0: static, consumer-oriented; Web 2.0: dynamic, producer and platform-oriented; Web 3.0: decentralized ecosystem
- Virtues of Web 3.0 promise include: (i) Incumbent Hegemony: response/challenge to the overcentralization of big tech in current Web 2.0 model; (ii) Network Vulnerability: addresses single point of failure risk in centralized architectures; (iii) Liquidity: enables contracting, exchange, trade, and management of public or private goods and services (Id. at 7)

Metaverse.

- Metaverse Journey: "evolved from *digital twins* represented by the online virtual world Second Life to *creative games* empowered by virtual and augmented reality and more recently online *virtual and multiplayer games* enabled by social interactions, training and trading creatures, and virtual economy with nonfungible tokens." (Id. at 8)
- Metaverse attributes: virtualized, immersive experience; human/device interfacing; rich ecosystem of trading markets; "suite of enabling technologies for infrastructure, interfacing, interaction, design and development tools" (Id. at 8)

Traditional AI is Centralized.

- "Conventional AI aims, technologies, systems, and services are centralized, static, predefined at design time, and user-neutral. CeAI presents their outputs as either a standalone system or a multiagent system. When a multiagent system carries the AI task, CeAI usually has a central controller, mediator, matchmaker, coordinator, or communicator (for message passing) to manage and govern agents and task execution." (Id. at 8)
- Problem with Centralized AI: "inflexibility, high vulnerability, poor reliability, and low scalability and adaptability, to complex real-world demand and large-scale problem solving." (Id. at 8)

Distributed AI is Not Enough.

- Distributed AI uses multiagent systems, parallelization. "A DAI system decomposes a problem or task to subproblems or subtasks and then assigns them into specialized agents for handling; the agent-based partial solutions are then synergized to form the solution to the problem. While taking a bottom-up approach, DAI usually involves mediation, cooperation, coordination, and communication between agents for task decomposition, assignment, execution, and consensus-building." (Id. at 8)

Decentralized AI.

- Encompasses: "decentralizing multiagents, AI tasks, task execution, resource allocation, storage and management, transaction management, intelligence management, and consensus-building between decentralized agents and AI tasks, etc." (Id. at 8-9)
- Decentralized AI advances the above "[w]ithout sharing resources, capabilities and computation with centralized servers and mediation by controlling the authority," and thereby "maximizes the power of end and edge devices and resources." (Id. at 9)



Details

TABLE 1. Differences between CeAI and DeAI

Aspect	CeAI	DeAI
Methodology	Top-down, holism, authority, and autocracy	P2P, bottom-up, reductionism, autonomy, and democracy
Objective	Global objectives	Local objectives
Intelligence	General and strong intelligence	Local, edge and weak intelligence
Task	Global and central task	Local and distributed task
Data/repository	Central and single resourcing and storage	Local, distributed, multiple, end resourcing and storage
Model	Central and global model	End, and local model
Architecture	Central, vertical and hierarchical control, mediation, matchmaking, gateway, and server/client structure	Horizontal, P2P, D2D, distributed, chain, and flat structure
Process	Consensus-building, aggregation, and orchestration	Partition, decomposition and splitting
Mechanism	Predefined, vertical, design-time alliance, coordination, cooperation, normalization, and standardization	Ad hoc, horizontal, run-time self-motivation and organization, and negotiation
Computation	Central, global computing infrastructure	Distributed, local computing systems
Communication	Broadcasting and hierarchical	P2P, D2D
Decision	Global goal-driven authority, and strategic minority	Local goal-driven personalization and majority voting
Output	Global, aggregated, and integrative	Local, individual, and personalized
Privacy	Weak protection	Strong protection
Security	Central authorization, monitoring, risk, and governance	Local or distributed authorization, monitoring, and risk
Pros	Unification, capacity, order, efficiency, stability, strategic, concentrated resources, computing, and data	Personalization, flexibility, adaptivity, resilience, transparency, autonomy, expandability, high fault tolerance, scalability, throughout, low cost, and risk
Cons	Low flexibility, adaptivity, autonomy, robustness, reliability, accountability, fault tolerance, high vulnerability, risk, cost, and catastrophic mistake	Low capacity, energy, resource, computation, and stability, high latency, and chaos

Longbing Cao, "Decentralized AI: Edge Intelligence and Smart Blockchain, Metaverse, Web3 and DeSci" in IEEE Intelligent Systems (May/June 2022), p. 13

Main Ideas

- Conventional AI services are centralized (central controller, mediator, governor, task executor), limited at design stage (inflexible, less responsive to change and dynamical systems), and display poor functionality in terms of reliability and scalability.
- Distributed AI is a movement in the right direction, but still shares resources with centralized servers.
- Decentralized AI aims to flatten centralization fully.

Details

Decentralization != Buzzword.

- "Decentralization is not a buzzword, hype or myth, although such concerns have been widely raised on decentralization-oriented initiatives, such as Web3 and the metaverse. Decentralization is also not a new or mysterious concept. It has a 200-year history and is ground in political science (such as subsidiarity, democracy, liberty, equality, and the decentralist movement), management and decision science (e.g., systems theory, self-organization, and self-determination), and economics (e.g., decentralized free markets and fiscal decentralization)" (Id. at 6)

From Distributed to Decentralized, a Further Flattening of Designed Coordination to Ad Hoc Interactions.

- "P2P and D2D authentication, collaboration, and communication at running time replace the design-time protocols and specifications for authentication, collaboration, cooperation, communication, and governance. This shift from distributed loose couplings to *ad hoc* and running-time P2P interactions enhances the effect of decentralization." (Id. at 7)

From Web 1.0 to 3.0.

- Web 1.0: static, consumer-oriented; Web 2.0: dynamic, producer and platform-oriented; Web 3.0: decentralized ecosystem
- Virtues of Web 3.0 promise include: (i) Incumbent Hegemony: response/challenge to the overcentralization of big tech in current Web 2.0 model; (ii) Network Vulnerability: addresses single point of failure risk in centralized architectures; (iii) Liquidity: enables contracting, exchange, trade, and management of public or private goods and services (Id. at 7)

Metaverse.

- Metaverse Journey: "evolved from *digital twins* represented by the online virtual world Second Life to *creative games* empowered by virtual and augmented reality and more recently online *virtual and multiplayer games* enabled by social interactions, training and trading creatures, and virtual economy with nonfungible tokens." (Id. at 8)
- Metaverse attributes: virtualized, immersive experience; human/device interfacing; rich ecosystem of trading markets; "suite of enabling technologies for infrastructure, interfacing, interaction, design and development tools" (Id. at 8)

Traditional AI is Centralized.

- "Conventional AI aims, technologies, systems, and services are centralized, static, predefined at design time, and user-neutral. CeAI presents their outputs as either a standalone system or a multiagent system. When a multiagent system carries the AI task, CeAI usually has a central controller, mediator, matchmaker, coordinator, or communicator (for message passing) to manage and govern agents and task execution." (Id. at 8)
- Problem with Centralized AI: "inflexibility, high vulnerability, poor reliability, and low scalability and adaptability, to complex real-world demand and large-scale problem solving." (Id. at 8)

Distributed AI is Not Enough.

- Distributed AI uses multiagent systems, parallelization. "A DAI system decomposes a problem or task to subproblems or subtasks and then assigns them into specialized agents for handling; the agent-based partial solutions are then synergized to form the solution to the problem. While taking a bottom-up approach, DAI usually involves mediation, cooperation, coordination, and communication between agents for task decomposition, assignment, execution, and consensus-building." (Id. at 8)

Decentralized AI.

- Encompasses: "decentralizing multiagents, AI tasks, task execution, resource allocation, storage and management, transaction management, intelligence management, and consensus-building between decentralized agents and AI tasks, etc." (Id. at 8-9)
- Decentralized AI advances the above "[w]ithout sharing resources, capabilities and computation with centralized servers and mediation by controlling the authority," and thereby "maximizes the power of end and edge devices and resources." (Id. at 9)



Details

TABLE 1. Differences between CeAI and DeAI

Aspect	CeAI	DeAI
Methodology	Top-down, holism, authority, and autocracy	P2P, bottom-up, reductionism, autonomy, and democracy
Objective	Global objectives	Local objectives
Intelligence	General and strong intelligence	Local, edge and weak intelligence
Task	Global and central task	Local and distributed task
Data/repository	Central and single resourcing and storage	Local, distributed, multiple, end resourcing and storage
Model	Central and global model	End, and local model
Architecture	Central, vertical and hierarchical control, mediation, matchmaking, gateway, and server/client structure	Horizontal, P2P, D2D, distributed, chain, and flat structure
Process	Consensus-building, aggregation, and orchestration	Partition, decomposition and splitting
Mechanism	Predefined, vertical, design-time alliance, coordination, cooperation, normalization, and standardization	Ad hoc, horizontal, run-time self-motivation and organization, and negotiation
Computation	Central, global computing infrastructure	Distributed, local computing systems
Communication	Broadcasting and hierarchical	P2P, D2D
Decision	Global goal-driven authority, and strategic minority	Local goal-driven personalization and majority voting
Output	Global, aggregated, and integrative	Local, individual, and personalized
Privacy	Weak protection	Strong protection
Security	Central authorization, monitoring, risk, and governance	Local or distributed authorization, monitoring, and risk
Pros	Unification, capacity, order, efficiency, stability, strategic, concentrated resources, computing, and data	Personalization, flexibility, adaptivity, resilience, transparency, autonomy, expandability, high fault tolerance, scalability, throughout, low cost, and risk
Cons	Low flexibility, adaptivity, autonomy, robustness, reliability, accountability, fault tolerance, high vulnerability, risk, cost, and catastrophic mistake	Low capacity, energy, resource, computation, and stability, high latency, and chaos

Longbing Cao, "Decentralized AI: Edge Intelligence and Smart Blockchain, Metaverse, Web3 and DeSci" in IEEE Intelligent Systems (May/June 2022), p. 13

Main Ideas

- It is common that blockchain ecosystem participants persistently fail to answer (with any rigor) the elementary question of whether a blockchain as such is applicable to address the situation at hand.
- The Blockchain Applicability Framework ("BAF") investigates three questions:
 - (1) Is a blockchain applicable?
 - (2) If so, does the application require permissionless / permissioned, public / private (or hybrid)?
 - (3) And, what consensus mechanism is well-suited to the application?

Details

On Motivation.

- "A very common trait that is found is that some of the blockchain users and enthusiasts cannot identify whether there is any need for blockchain in their application." (Gouriseti et. al., at 1)
- One of the unique elements of the blockchain technology that made it such a captivating technology to researchers is its plethora of features. Some of the features include smart contracts, cryptocurrency and tokenizing, immutable distributed ledger, cryptographic hashing, and digital signature. In addition, there are multiple types of blockchains, such as permissioned/private and permissionless/public, and various consensus models, such as proof-of-work, proof-of-authority, proof-of-burn, and proof-of-stake. Therefore, it is often non-trivial to determine if an application requires a blockchain. If so, what kind of blockchain and consensus is most appropriate?" (Id. at 1)

On Blockchain Applicability Framework ("BAF") Architecture.

- ~100 evaluative questions and 18 subdomains spread across 5 core domains:
 1. Data and participation
 2. Technical attributes
 3. Security
 4. Trust Parameters
 5. Performance and Efficiency
- Binary decision trees risk oversimplification. Thus, a probabilistic approach is preferred.
 - ✓ "Since blockchain technology has several features, including immutable distributed ledger, smart contracts, cryptocurrency designability, multi-channel architectures with customizable access controls and visibility restrictions..., auditability features, and other features, binary decision-making based on the response to a control [question] could potentially lead to an oversimplification of the technology and its scope." (Id. at 10)

Threshold Question: Checklist (WIP)

I have extracted these domains, subdomains, and questions from Gouriseti et. al. as they specifically pertain to the Threshold Question.

Source: Nikhil Gouriseti et. al., "Evaluation and Demonstration of Blockchain Applicability Framework" in IEEE Transactions on Engineering Management (2019)
As Modified by: Sandeep C. Ramesh

Data & Participation

Data Attributes

- Is there a need to store data?
- Is all the data coming from a single entity?
- Does a traditional database technology meet the needs?
- Is there a need to modify historical data?

Read & Write

- Are there multiple parties/participants?
- Is there a need for more than one participant to update the data?

Technical Attributes

Codebase and Networks

- Is there a trusted third party in the system?

Smart Contracts

- Are policies and (smart) contracts involved and managed?

Transaction Constraints

- Are exchanges and transactions involved?
- Is there a need for the transactions to be validated by votes/consensus?

Security

Governance

- Is there a need of censorship in the system?

Security

Governance

- Is there a need of censorship in the system?

Trust Parameters

Visibility

- Will all the nodes have different view of the system state based on the centralized system decision?
- Is there a need for a fully transparent system?
- Is it required for some nodes to not see information/transactions performed on the blockchain?

Integrity

- Is there a centralized system to ensure the integrity of the data?

Validation

- Is there a centralized system to verify the change in the state of the system?

Performance and Efficiency

System Performance

- Is compromise with the system performance in terms of latency acceptable?
- Is compromise with the system performance in terms of throughput acceptable?

Market Design

- Is a contractual based market approach needed?
- Do the benefits outweigh the associated costs?

Main Ideas

- There's a "Babylonian confusion" surrounding the term "blockchain" and its usage
- There is inconsistency and bias in many decision schemes that attempt to address whether blockchain is applicable (what I refer to internally as the "Threshold" or "Gateway" Question)
- The analytical steps to cross (or not) the Threshold: (1) should you use a blockchain? (2) If so, what type? (3) If no, what alternatives are best?

Details

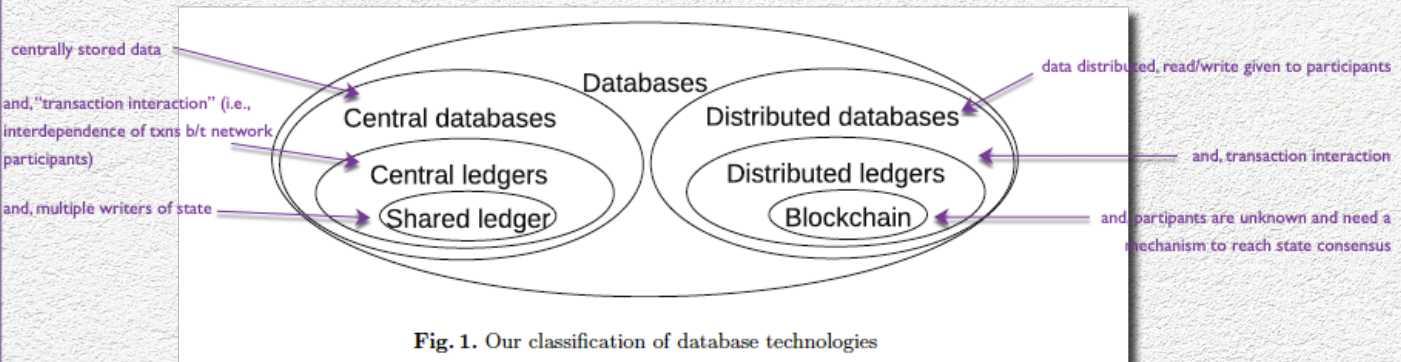


Fig. 1. Our classification of database technologies

Source: Koens & Poll, "What Blockchain Alternative Do You Need?" in Data Privacy Management, Cryptocurrencies & Blockchain Technology (Garcia-Alfaro et. al., eds.), pp. 113-129 (2018)

Annotations: Sandeep C. Ramesh

Table 2. Scheme questions classification

No.	Question	Class.
1	Traditional approach is insufficient? [6, 10, 17, 21]	D
2	Can other technologies offer a solution? [2, 6, 31, 49]	D
3	Aiming to remove third parties? [24, 33, 57]	P
4	Are you working with digital assets? [7, 33]	P
5	Where is consensus determined? [4, 5, 8, 19, 23, 24, 29, 43, 45]	P
6	Do you need censorship resistance? [49]	E
7	How is the incentive structure determined? [34]	E
8	Are there contractual relations? [6, 14, 31, 33, 45]	P
9	Rules of tx do not change frequently? [13]	P
10	Sensitive identifiers stored? [2, 11, 14, 21]	P
11	Requires a market approach? [14]	P
12	Looking to reduce costs? [14]	P
13	Looking to improve discoverability? [14]	P
14	Is there a real (business) problem? [2, 6, 31]	P
15	Can participants adapt? [2, 6, 29]	P
16	Do the benefits justify the cost of adoption? [2]	P
17	Is this a 'blockchains are free' play? [2]	P
18	Need an immutable log? [11, 13, 29, 32]	E
19	Are there relative simple business rules? [14, 17, 29]	P
20	Many participants transacting? [29, 31]	P
21	Is data integrity required? [7]	P
22	Do you need to share operational data? [7]	P
23	Are there transaction rules set? [12]	P
24	Who stands behind the assets? [12]	P
25	Can the project be open sourced? [21]	P
26	Participants trust each other? [4, 5, 7, 8, 12, 16, 20, 23, 29, 33, 45, 49, 56]	P
27	Participants interests aligned? [4, 5, 8, 13, 18, 23, 31, 33, 43]	P
28	Need a database? [4, 5, 7, 8, 10-13, 16, 18, 20, 23, 24, 32, 33, 43, 45, 47, 56]	T
29	Can you use a TTP? [2, 4, 5, 8, 10-12, 16, 17, 20, 21, 23, 29, 31, 33, 34, 43, 45, 56, 57]	T
30	Shared write access? [4, 5, 8, 10-14, 16-18, 24, 33, 34, 43, 47, 49, 56]	T
31	Participants known? [4-6, 8, 12, 18, 23, 31, 33, 34, 45, 47, 56]	T
32	Need to control functionality? [4, 8, 19, 23, 33, 43, 45, 49]	T
33	Public transactions? [2, 4, 5, 7, 8, 14, 17-19, 21, 29, 32, 33, 43, 45, 47, 49]	T
34	Is there transaction interaction? [10, 12, 21, 24]	T
35	Do you need high transaction throughput? [14, 17, 21, 24, 29, 31, 33, 45]	L
36	Do you need to store large transactional data? [21, 33]	L

D = the questions we are trying to answer in the first place. Disqualified due to

P = process-related questions that don't strictly differentiate technologies

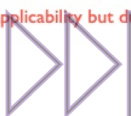
E = design-related questions that don't strictly differentiate technologies; rather, they are more relevant in deciding tradeoffs

T = questions that explicitly allow us to distinguish technologies

L = questions about established (current) limitations to blockchain that may lead a conclusion to adopt a non-blockchain approach not due to applicability but due

Source: Koens & Poll, "What Blockchain Alternative Do You Need?" in Data Privacy Management, Cryptocurrencies & Blockchain Technology (Garcia-Alfaro et. al., eds.), pp. 113-129 (2018)

Annotations: Sandeep C. Ramesh



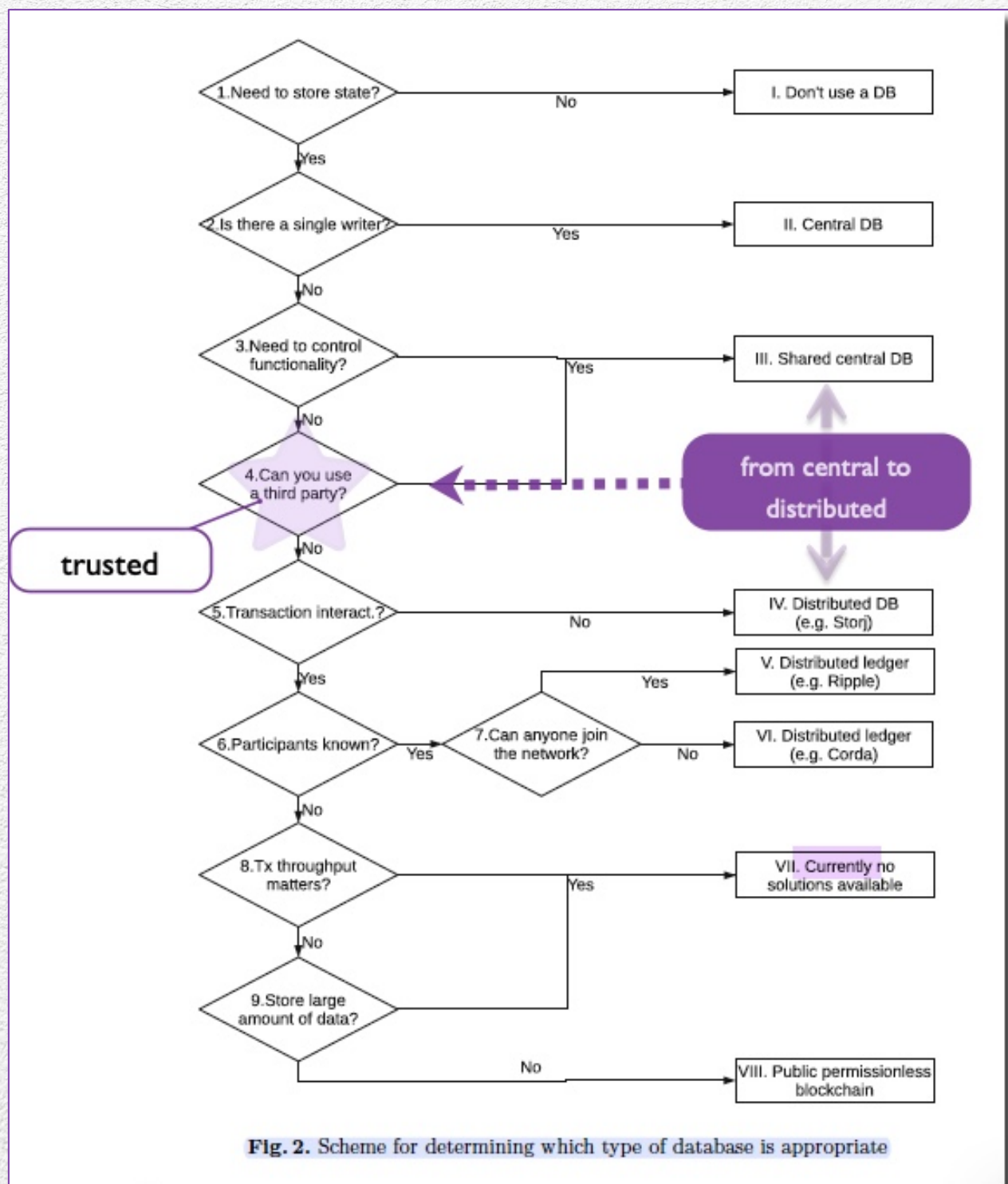


Fig. 2. Scheme for determining which type of database is appropriate

Source: Koens & Poll, "What Blockchain Alternative Do You Need?" in *Data Privacy Management, Cryptocurrencies & Blockchain Technology* (Garcia-Alfaro et al., eds.), pp. 113-129 (2018)

Annotations: Sandeep C. Ramesh

Main Ideas

- **The Issue:** "[A] key question relates to the matter of how to determine whether a blockchain solution is suitable for a given business; if so, which configuration of a blockchain system should be used?" (Id. at 155,246)
- **On Decentralization Gradient.** Based on consensus mechanism, we can adopt the following classification scheme as a stable analytical ground:
 - ✓ Public Blockchain / Permissionless Blockchain: fully decentralized (or, less open-ended, fully decentralized ethos with phased ramp to realization)
 - ✓ Hybrid Blockchain / Public Permissioned Blockchain: centralized blockchain with predefined trusted nodes (e.g., consortium model)
 - ✓ Private Blockchain / Permissioned Blockchain: fully centralized blockchain with few number of nodes with read/write access
- **On Blockchain Generational Phases.**
 - ✓ Blockchain 1.0: focus on cryptocurrency, viz. Bitcoin
 - ✓ Blockchain 2.0: movement beyond the currency use case via focus on smart contracts, viz. Ethereum
 - ✓ Blockchain 3.0: instantiation of financial (decentralized finance) and social (NFT) use cases
 - ✓ Blockchain 4.0: intersection of AI, ML, and blockchain-as-a-service

Diagrams

TABLE 1. Appearance of frequent decision constructs in the reviewed flowcharts.

Decision Constructs	[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]	[25]	[40]	[41]
Data Store		✓		✓		✓	✓				✓	
Multiple Participants	✓		✓	✓	✓	✓	✓	✓			✓	✓
Participant Trust	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓
Data Privacy	✓		✓	✓	✓	✓				✓		
Trusted Third Parties	✓	✓	✓	✓	✓	✓	✓			✓		✓
Public Verifiability		✓	✓	✓			✓	✓	✓			
Access Control	✓		✓	✓		✓				✓		✓
Transaction History		✓	✓		✓		✓			✓		✓
Immutability					✓	✓	✓	✓	✓		✓	
High Performance								✓	✓			
Scalability			✓	✓				✓	✓	✓		
Data Durability	✓				✓		✓	✓				✓
Data Replication		✓							✓		✓	

TABLE 2. Components of conceptual frameworks.

Concepts of Frameworks	[42]	[43]	[16]	[44]	[45]	[46]
Data and Storage	-Immutability -Historical records	-Integrity	-Integrity -Availability -Confidentiality -Interoperability	-Integrity -Data retention -Interoperability -Accessibility	-Immutability -Auditability -Interoperability	-DB suffices -Historical assets -Redundant dataset
Process and Transactions	-Workflow -Transactions	-Automation		-Functional operation	-Identity verification and authentication	
Participants and Stakeholders	-Distribution -Trust -Identity	-Decentralized network -Intermediary check	-Trust -Permissions -Modularity	-Participant control -Identity	-Multiple writers -Participant & intermediary trust -Ownership of data	-Multi-stakeholders -Access authority
Design Issues	-Inefficiency -Transparency	-Automation	-Scalability -Consensus mechanism -Anonymity -Transparency -Governance	-Transparency -Scalability -Flexibility -Efficiency	-Transparency -Security	-Data protection requirements
Regulation Issues		-Values and rights	-Ecosystem requirements -Regulations	-Legal foundation -Data privacy	-Governance rules	-Regulation readiness
Business Issues		-Added value	-Cost -User adoption	-Maintenance & operational costs	-Financial considerations	-Risk identification -Business process identification -Resource planning
Validation	Applied to test 23 projects in proof-of-concept stage	Applied to four applications	Expert interviews	Semi-structured interviews	Interviews	Applied to assess suitability of a power utility network project

Reference	Context	Decision Model	Decision Model Specifications
[26] [47]	General	Relative-weight approach	BAF has 100 controls under 5 main domains and 18 subdomains: Data and participation: attributes, authority, reader, and writer Technical attributes: codebase and network, smart contracts, transaction constraints, process, miner, and consensus Security: governance, security attributes, and access control Trust parameters: visibility, integrity, and validation Performance and efficiency: system performance, expandability, and market design
[49]	General	AHP	Motivating factors: reliability, automation of transactions, decentralization, transparency, and immutability Impeding factors: scalability, interoperability, cost, technical maturity, and knowledge
[50]	Knowledge-based conversation system (KCBS)	AHP, FAHP, FTOPSIS	Proposing a decision model for the best fitting blockchain platform for KBKS: Decentralized architecture, storage and sharing, computing performance, and scalability, along with network performance, attack resistance, fault tolerance, deployment cost, reliability, availability of service, flexibility and opening, processing speed, concurrent capacity, and space recovery
[51]	General	AHP, TOPSIS	Assessing the feasibility of blockchain technology in different industries and identifying 15 factors: 1- Existence of regulations 2-Level of technology maturity 3- Proportion of digitized assets 4-Richness of ecosystem 5-Potential to increase revenue 6-Potential to reduce cost 7- Enhanced security and data integrity 8- Building trust 9- Potential to increase transaction speed 10- The need for improved visibility 11- Enhanced auditability 12- Potential to improve efficiency 13- Potential to yield high return on investment 14- The need for reduced fraud 15- The need for improved traceability
[52]	Logistics	AHP, VIKOR	Evaluating the feasibility of blockchain technology in logistics operations by identifying: Criteria: scalability (C1), privacy (C2), interoperability (C3), audit (C4), latency (C5), visibility (C6), trust (C7), and security (C8) Alternatives: identifies 9 distinct operations, including materials handling, warehousing, order processing, transportation, packaging, fleet management, labeling, vehicle routing, and product return management
[54]	Supply chains	Fuzzy DEMATEL	Evaluating the factors affecting decision to adopt blockchain technology in a logistics company: Cause: peer-to-peer networks, instant money transfer, distributed ledger, smart contracts, immutability, authentication, and security Effects: cryptocurrency creation, transparency, privacy, traceability, real-time processing, and reduced transaction delays
[55]	Logistics	Fuzzy ANP	Suitability evaluation of blockchain-based systems using fuzzy ANP using the case study of a logistics company Trust: lack of trusted third parties, accountability, immutability, multiple non-trusting writers, and peer-to-peer transactions Context: traceability of transactions, verifiability of transactions, data transaction notarization, data transparency, security, and privacy Performance: latency and transaction speed, maintenance costs, redundancy, and scalability Customer: roles of management, need for verifiers, and autonomous/generic transactions between transactions of different writers
[56]	Shipping companies	BOCR, Fuzzy FAHP	Analysis of key factors influencing integration of blockchain into shipping companies in Taiwan by identifying: Benefits: reducing intermediary costs, reducing information delays, reducing bribery and fraud, and reducing transaction costs Opportunities: maintaining transaction security, reducing trust risks, increasing network effects, and improving transaction efficiency Costs: platform construction costs, system management costs, manpower training costs, and system conversion costs Risks: information transfer and development speed, data security and privacy, incomplete regulatory systems, and incomplete response mechanisms
[57]	Supply chains	MCDM, GRA	Adoption of blockchain in supply chains based on an analysis of the following influencing factors: Organizational factors: inter-organizational trust and relational governance Technological factors: data transparency and data immutability Social: social influence and behavioral intention Operational: interoperability and product types
[58]	Supply chain management	III-AHP, III-FTOPSIS	A multi-criteria evaluation model based on hesitant fuzzy sets for blockchain technology in supply chain management classifying factors under 5 main criteria and 17 sub-criteria, as follows: Customer: satisfaction, traceability, reliability, and transparency Product: quality, safety, value, sustainability, and flexibility Implementation: suitability, market needs, and technology Logistics: speed and inventory management Cost: implementation, maintenance, and consumption Five different sectors (i.e., food, medicine, energy, jewelry, and textiles) were determined using the Delphi approach and comprehensive literature analysis

INSIGHTS

1. Evaluation criteria is contingent upon developmental stage. This view rejects the static "clipboard" framework that is insensitive to the evolution of blockchain and the ecosystem within which the tech exists.
2. Assessment intensity depends on my purpose: quick check, position initiation (dip toe in water), conviction building / bias testing.

TABLE 4. Blockchain platform selection criteria.

Reference	[66]	[67]	[68]	[69]	[70]	[71]	[53]	[72]
Context	General	Supply Chains	General	Supply Chains	Logistics	ERP	ERP	IoT
Usability		✓	✓	✓		✓	✓	
Functionality	✓		✓	✓	✓	✓	✓	✓
Performance	✓	✓	✓	✓	✓	✓	✓	✓
Platform Support	✓	✓	✓	✓	✓	✓	✓	✓
Security		✓	✓	✓		✓	✓	✓
Privacy					✓	✓	✓	✓
Network Topology	✓	✓	✓	✓		✓		
Modularity	✓				✓	✓	✓	✓
Interoperability	✓	✓		✓	✓	✓	✓	✓
Cost					✓	✓	✓	

Main Ideas

- Mapping web3 architecture is a critical pre-requisite to understanding design tradeoffs
- One web3 architectural map consists of 3 "decoupled components" (access, computation, storage) and 3 "transaction routes" (on-chain, off-chain, hybrid)
 - ✓ See *also* Field Note 23. On "Decentralized Computing Stack," in which Trent McConaghy maps similar elements of decentralized computing: communications, processing, storage
- Architecture Trade-Off Analysis Method allows us to compare/contrast the design choices as we select different transaction routes for the decoupled components

Details: Section 3**On Web3 Architecture Components.**

- "The architecture is the foundation of software systems. It defines the system structure and external world interface via underlying components and their relationship. This section provides our architectural design for Web3 systems." (Id. at 7)
- "Decoupled Components" → client/access, computation, and storage
- "Technical Routes" → on-chain processing, off-chain processing, hybrid / combination of on-chain & off-chain processing

On Decoupled Components & Technical Routes

- Three main processes to system operations that describe data flow from client to backend server: (a) data access, (b) data computation, and (c) data storage.
- Data Access: user sends request, typically formatted as a transaction, to the client, which is instantiated as a wallet. In other words, the wallet functions as the connection point between the user and the network.
 - ✓ Browser-Based Wallet. Browser extension allows user to import private key to the embedded wallet.
 - ✓ Agent-Based Wallet. Users grant trusted third-party custody over private keys in order to capture U/X benefit of simplicity at the expense of security. Agent-Based Wallets also "enable batch processing when confronting a high-density situation of requests from users." (Id. at 9)
- Data Computation: user requests are processed by underlying blockchain that operates according to smart contract specifications.
 - ✓ Contract-Based Computation: this is an on-chain solution in which all computations are performed on-chain via smart contracts.
 - ✓ Hybrid Computation: partial on-chain, partial off-chain computation in which "verification mechanisms are required...to guarantee integrity between on-chain and off-chain data." (Id. at 9)
- Data Storage: executed data moves into storage; small size data can be stored directly on-chain, but larger size data or more complicated formats like raw audio and video typically leverage off-chain storage.
 - ✓ On-Chain Storage: data stored publicly on-chain.
 - ✓ Off-Chain Storage: data stored in off-chain networks with only the hashes stored on-chain; in this circumstance, verification process is needed to ensure integrity between the on-chain and off-chain data link.
 - ✓ Hybrid Storage: mixed on/off-chain storage with high density data stored off-chain, and light metadata stored (account history, certificates) stored on-chain.



Details: Section 4

On ATAM Evaluation Framework.

- ATAM = Architecture Trade-Off Analysis Method
- "The architecture trade-off analysis method is initially used in software development to recommend the most suitable architecture for a specific system. The method majorly discusses the trade-offs between different design types and their sensitivity points for risk mitigation." (Id. at 11)

On 8 Evaluation Criteria per ATAM.

1. Performance (typically measured as throughput / TPS)
2. Scalability (performance impact as network grows)
3. Cost: necessary because zero cost system (gas-less) succumbs to loop logic error
 - follow up on loop logic error: Sukrit Kalra et al, "Zeus: Analyzing Safety of Smart Contracts" in The Network & Distributed System Security Symposium (2018)
4. Security (at the data level / data integrity & authorized access)
5. Anonymity (hiding identity, breaking link between physical entity and virtual public addresses)
6. Confidentiality (hiding sensitive data)
 - Anonymity vs. Confidentiality: "Confidentiality focuses on states rather than entities." (Id. at 12)
7. Availability (ensuring network remains intact / avoiding single point of failure)
8. Usability (u/x, u/i from perspective of end user)

On Web Architectures Compared.

- "Adding auxiliary techniques (agent, off-chain computation, off-chain storage) will impact the properties from different sides. [P]erformance, scalability, gas cost, and usability get improved at different levels depending on how many layers have been modified. This is because external techniques can support much more volume of data and participating parties." (Id. at 15)
- "In contrast, negatively, security, anonymity, and availability have decreased, compared to the baseline (Type 1), due to the in-transparency of off-chain processing procedures." (Id. at 15-16)

Table 1: Web Architecture Evaluation

LEGEND

Decoupled Components as follows:

A = Access / Client

B = Computation

C = Storage

Transaction Routes as follows:

1 = on-chain

2 = hybrid

3 = off-chain

Key question when designing Web3 architecture is how important Security, Anonymity, and Availability are to the problem area.

Architecture	Property							Stakeholders		
	Performance	Scalability	Gas Cost	Security	Anonymity	Confidentiality	Availability	Usability	Web3 User	Service Provider
A_1, B_1, C_1 -Type1	○	○	○	○	○	○	○	○	○	○
$A_1, B_1, C_{2/3}$ -Type2/3	●	●	●	●	○	●	●	●	+	-
A_1, B_2, C_1 -Type4	●	●	●	●	○	●	●	●	+	-
$A_1, B_2, C_{2/3}$ -Type5/6	●	●	●	●	○	●	●	●	++	--
A_2, B_1, C_1 -Type7	●	●	●	○	●	○	○	●	+	-
$A_2, B_1, C_{2/3}$ -Type8/9	●	●	●	●	●	●	●	●	++	--
A_2, B_2, C_1 -Type10	●	●	●	●	●	●	●	●	++	--
$A_2, B_2, C_{2/3}$ -Type11/12	●	●	●	●	●	●	●	●	+++	---

○ Baseline, ● Property enhance, ● Property decrease; (Compared to Type1)

Source: Wang et al, "Exploring Web3 from the View of Blockchain" at 14.

on-chain data access, data computation, and data storage

Main Ideas

- The threshold or gateway issue when approaching the debate around use cases (particularly, non-currency use cases) is whether a particular problem is "suitable for" blockchain intervention.
- I use the phrase "suitable for" instead of "requiring of" in order to pay respect to Amara's Law (see Field Note 10, On "Amara's Law + Exponential"); it is my bias toward positive optionality and humility before the phenomenon of technological emergence.
- Wüst and Gervais provide a simple flow chart to assist in crossing the threshold issue centered on the concepts of (a) state, (b) root access, read/write, (c) trust, and (d) system robustness.

Details

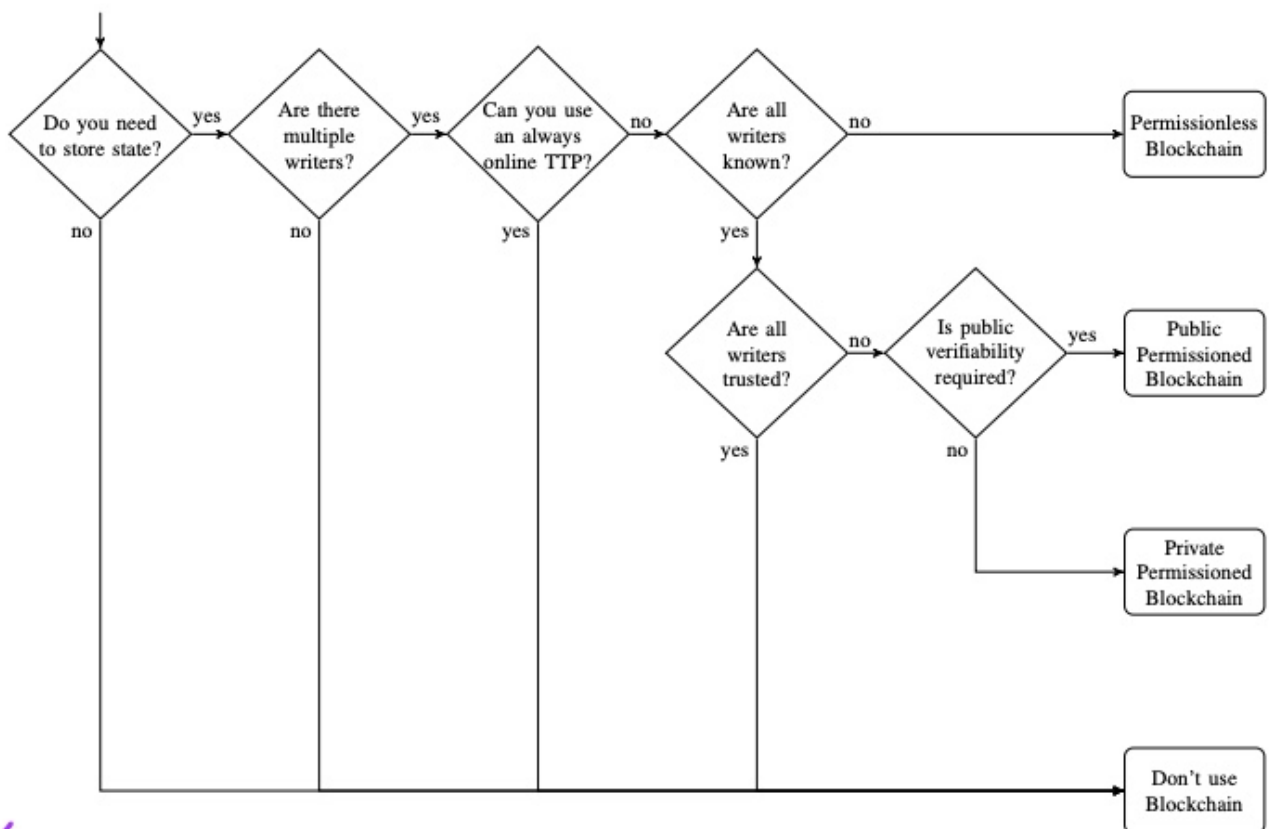


Fig. 1: A flow chart to determine whether a blockchain is the appropriate technical solution to solve a problem (Table I should be considered in the decision making process as well). Writers refer to entities with write access to the database/blockchain, i.e. in a blockchain setting, a writer corresponds to a consensus participant. If a trusted third party (TTP) is available that is not always online, this can be used to establish a known group of writers, i.e. the TTP can function as a certificate authority in such a setting. Public and private permissioned blockchains differ in that a public blockchain allows anyone to read the contents of the chain and thus verify the validity of the stored data, while a private blockchain only allows a limited number of participants to read the chain. Note that for any blockchain based solution it is possible to make use of cryptographic primitives in order to hide privacy-relevant content.

SR NOTES ON:
s: TradFi Edition

Structured Framework for Fundamental Investment Analysis: TradFi Edition



Main Ideas

- "Web3" seems to serve as a floating signifier, at times meaning nothing and everything. "You can't be wrong if you're vague enough" is the posture many Web3 commentators adopt.
- Against this, in the name of understanding, it's better to be specific and wrong.
- "Unclear definitions and non-agreed consensus indicate that Web3 either is just a hyped concept without practical development or, has more than one single direction for the development." (Id. at 2)
- **Web3: 7 Properties, 3 Entities, 3 User Flows**

Details: Section 1

Web3 vision is to provide distributed internet services without trusted third parties whereby users own their data.

- "The very primary principle shared by Web3 applications is that users can hold the data with full control, covering identifiers/tokens/ownership/etc., rather than being managed by centralized organizations as in Web1 and Web2." (Id. at 1)
- "With the emphasis on *decentralization*, Web3 moves data away from these centralized authorities and establishes applications and services surrounding blockchain technologies." (Id. at 1-2)

In the ideal, Web3 applications are deployed on decentralized networks based via public blockchains hosted by p2p servers.

- Properties of Web3:
 1. Open (or, Visible): data accessible and stored on open networks built and maintained by public communities
 2. Trustless: user can interact with applications without intermediation of trusted third parties
 3. Permissionless (or, Portability): user identity is untethered from specific platforms
 4. High Privacy: users can operate anonymously or at a minimum, pseudonymously
 5. High Availability (or, Robustness): decentralized blockchain architecture reduces risk of server crash or point failures
 6. Compatibility (or, Interoperability): applications are untethered from single blockchain platform
 7. Participation: users are not passive consumers, but also contribute to services of the network and receive rewards

Details: Section 2**3 Entities Involved in Web3 Architecture.**

- Web3 User: "[A] data owner who can propose the request by sending a transaction from the client." (Id. at 4)
- Service Provider: "[O]ffers the user an on-chain interface and the service that can both process the request and interact with blockchain platforms." (Id. at 4)
- Blockchain Maintainer: "[P]rovides an operating environment for smart contracts that take the task of processing business and data storage." (Id. at 4)

Web3 User Flow.

- Identity Creation Algorithm: Create distributed ID (wallet)
- Transaction Generation Algorithm: Connect wallet to app
- Transaction Execution Algorithm: App executes instructions via

Identity Creation in a Web3 Protocol has 3 Sub-Algorithms.

- i. private key generation
- ii. public key generation
- iii. address generation
 - ✓ These algorithms are run by a Web3 client (e.g., client-based wallet or browser extension-based wallet)
 - ✓ Transaction generation algorithm includes: signature, transaction metadata (transaction-related data (e.g., receiver), nonce), and payload (points to applicable smart contract)
 - ✓ Contract execution is run by the blockchain maintainers, which includes a reward to incentivize the network maintenance and state change via consensus update (state retrieval initiated by client)



Details: Section 2 cont'd

Web3 Defined via Basic Algorithm Visualized.

1. signature generated
2. transaction data (e.g., receiver, nonce)
3. points to appropriate contract
4. current state
5. new state
6. confirmed state
7. retrieval = confirmed state

Annotations mine.

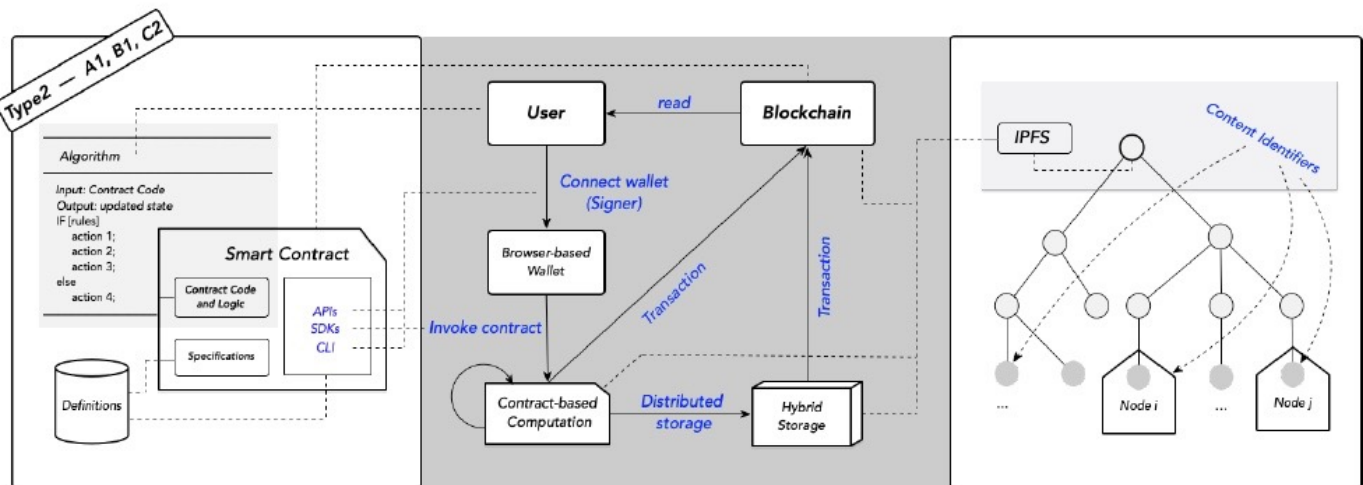
Source: Wang et. al. (June 2022) at 6.

where the output satisfies:

$$\begin{aligned}
 & \left[\begin{array}{l} \text{1} \quad \text{2} \quad \text{3} \\ \text{sig} \leftarrow \text{Sign}(sk, metadata, payload) \\ \text{Tx} \leftarrow \text{TranGen}(\text{sig}, metadata, payload) \\ \text{4} \quad \text{5} \quad \text{6} \quad \text{4} \\ s \leftarrow \text{ContractExec}(s, Tx, contract) \\ (s', Tx') \leftarrow \text{Consensus}(s, Tx, contract) \end{array} \right] \Rightarrow (s', Tx') \\
 & [(s'', Tx'') \leftarrow \text{Retrieval}(addr, contract)] \Rightarrow (s'', Tx'')
 \end{aligned}$$

$$\text{7} \quad (s', Tx') = (s'', Tx'')$$

Web3 Architecture & Interactions for Specific Application.



Annotations in orig.
Source: Wang et. al. (June 2022) at 6.

Fig. 1: An Instance of Web3 User Case

Main Ideas

- The Bell-Mason Diagnostic is an under-appreciated framework to evaluate tech startups on 12 dimensions across 4 growth stages. Against "gut-driven investing," the Diagnostic attempts to provide rigor and systematic thinking to evaluate and calibrate the health of tech startups as they attempt to navigate toward steady state.

Details

On the Framework Motivation.

- Born out of experience with startup management and marketing; Bell was researcher at MSFT's Media Presence Research Group, prof. at Carnegie-Mellon, and other; Mason was CEO of the marketing consulting firm, Acuity
- Developed in the early 1990s
- Purpose of framework is to provide a rigorous and systematic way to compare/contrast different startups across common standards, compared to the "ideal" startup at a particular growth stage
 - ✓ "Contrast this with the 'gut-feel' common wisdom that has guided investor and employee decisions for as long as there's been a high-tech industry, with reference to fabled rules of thumb such as : people people people; market, product, team; I look for vision above all else" and so on. (Bell at 62)
 - ✓ "By plotting the actual against our ideal, the graph reveals hot spots requiring attention by graphically portraying the start-up's strengths, weaknesses, and overall balance at each stage." (Bell at 623)

On the Four Framework Elements.

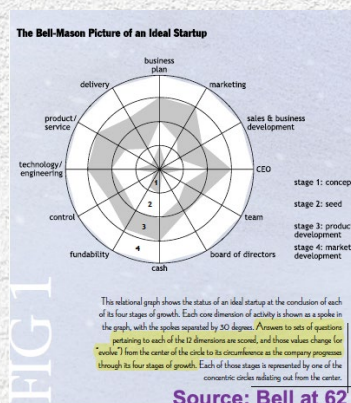
- Stage: captures four stages of venture (concept, seed, product development, market development); the fifth stage of maturity is not captured
- Dimensions: 12 categories of evaluation designed to "reduce and structure complexity" (Bell & Mason at 621)
- Heuristics: rules--or more aptly, heuristics--upon which to compare/contrast company against a hypothetical "ideal"
- Visualization: plotting on a radial Kiviat / radar graph for quick assessment of subject company vs. the representation of the hypothetical "ideal"

On the Four Framework Stages.

- Concept: "It takes nothing to enter this stage except an idea and a kitchen or dining room table at which to sit and begin exploring and planning the proposed venture." (Bell & Mason at 622)
- Seed: "The seed stage typically lasts six months, but it can take over a year to prove technology/product efficacy if the proposed company utilizes a particularly difficult technology."
- Product Development with 4 substages
 - hiring and planning
 - designing and building
 - alpha testing
 - beta testing
- Market Development with 3 substages
 - Market calibration
 - Market expansion
 - Steady-state operation
 - ✓ "These four stages correspond to key product, market, and corporate development milestones--and are measurable and predictably sequential." (Bell at 63)

On the Twelve Dimensions.

- "Each of the twelve dimensions is evaluated at each of the four stages of growth by comparing the start-up with what we define to be an 'ideal' for that stage of growth." (Bell & Mason at 622)
- "The entire diagnostic consists of over 700 rules and a detailed, stage or sub-stage may embody 70 questions. However, a general set of 25 rules are provided...." (Bell & Mason at 622)
- Rules/targeted questions/heuristics calibrate based on stage: "The rules for each dimension become more stringent with each stage in the start-up's growth." (Bell & Mason at 623)



Main Ideas

- Proffered by the British Design Council, the Double Diamond Framework is one of many generalized frameworks for non-linearly moving from "problem" to "solution," which has personal relevance in my continued exploration of the seemingly unbounded surface area of crypto, web3, blockchain, digital assets, and related topics. Nessler's 2016 article (and 2018 update) provides a more detailed (at the risk of being overwrought, depending on the user's deftness and preconceptions) look at the Double Diamond.

Details

On British Design Council's Original Double Diamond Framework.

- Non-linearity in moving from problem to solution
- Requires tinkering and hypothesis testing in the face of ambiguity
- Converges and diverges at various points in the process from discovery to delivery
- Left half focuses on "doing the right thing" (strategy) and the right half focuses on "doing things right" (design)

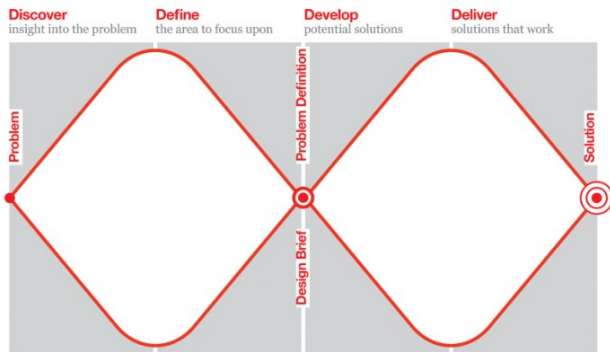
On IDEO's Human Centric Design ("HCD") Framework.

- Origin of movement toward implementation encourages exploration, experimentation, and meandering
- Per Feynman, "Study hard what interests you the most in the most undisciplined, irreverent, and original manner possible."

On Stanford's Design Thinking Framework.

- Empathy emphasis helps to ensure the problem being solved is not encased in a siloed intellect
- Themes of iteration, tinkering, hypothesis testing are carried through

On Nessler's Double Diamond (Synthesis of Above Frameworks).



Design Council's Double Diamond, img source:

<http://static1.squarespace.com/static/55fa0341e4b06660c65bd4f0/t/5642c682e4b0b633d4fcc1fd/1447216776499/>

INSPIRATION

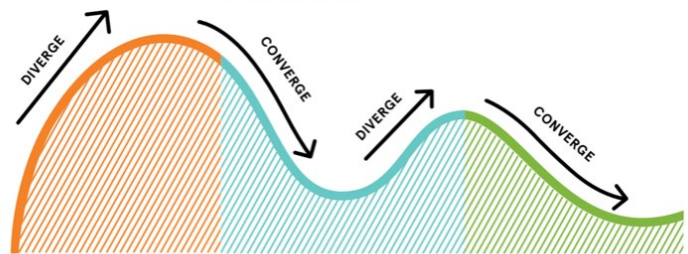
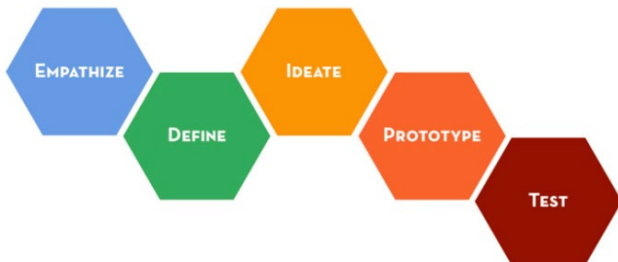
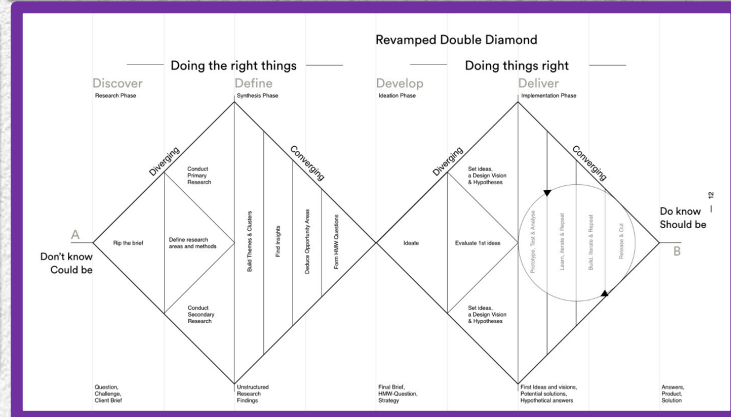
I have a design challenge.
How do I get started?
How do I conduct an interview?
How do I stay human-centered?

IDEATION

I have an opportunity for design.
How do I interpret what I've learned?
How do I turn my insights into tangible ideas?
How do I make a prototype?

IMPLEMENTATION

I have an innovative solution.
How do I make my concept real?
How do I assess if it's working?
How do I plan for sustainability?

IDEO HCD process, img source: <https://cdn.evbu.com/eventlogos/160332149/designthinkingphases.png>Stanford d.school Design Thinking process, img source: <http://dschool.stanford.edu/wp-content/uploads/2012/02/steps-730x345.png>

Main Ideas

- Despite the rebranding of crypto as "web3," Gavin Wood (co-founder & CTO of Ethereum, co-founder Polkadot) coined the term circa 2014. His web3 one-liner: "With so much of the world's data channeled through a few cables, the inconvenient truth is that unless we put in place open software protocols, our increasingly digital society will continue to be at risk from malicious 'authorities' both within society and...from outside." (Id.)
- Scant on solutions, but the problem of the existing internet is well articulated for its intended general audience.

Details

On Problems with Current Internet.

- Animating ideology: "Centralization is not socially tenable long-term, and government is too clumsy to fix things." (Id.)
- Web today is a "big baby [that] has grown old without growing up." (Id.)
- Internet is broken by design; it is constitutively flawed and cannot be recovered on its own terms.
- Internet merely became a mirror of the existing social structures and inequities already present. Far from a leveler, the net served as a mirror and arguably a distorted mirror. "As the global economy went online, we replicated the same social structures that we had before.... Markets, institutions, and trust relationships have been transposed to this new platform, with the density, power and incumbents changed, but with the same old dynamics." (Id.)
- Our interactions online are mediated, which has a paternalistic overtone as well as an extractive one. "On Web 2.0, you are not empowered to make payments per se. In reality, you must contact your financial institution to do it on your behalf. You are not trusted to do something as innocuous as pay your water bill. You are treated like a child appealing to a parent. If you wish to contact your friend online, then likely you will need to appeal to Facebook to relay your message." (Id.)
- It is not that centralization is by definition evil or extractive; rather, it is not by definition aligned with citizen interests. The relationship is one of dependence. "The goliaths that run these services -- often critical to our lives and jobs -- have no (obvious) evil intent, but nor do they act with benevolence or principle. They make money from our fealty, feeding us information, and cutting us off when inconvenient." (Id.)

On Web 3.

- Web 3.0 defined: "an inclusive set of protocols to provide building blocks for application makers."
- Web 2.0 building blocks: HTTP, AJAX, MySQL
- Trusted parties will still exist, but their roles will become commoditized. "There will still be room for trusted parties, insurance outfits, backup services and so forth. But their tasks will be commoditized and their activity verifiable. As these service providers are forced to compete in a global, open and transparent market, web users will be relieved of price-gouging and rent-seeking." (Id.)
- Emergent perspective on solution set: "[W]e can't predict the first successful use cases of this new platform and when they might appear. As with the development of the internet before it, the timeline could be measured in decades rather than months. But when Web 3.0 emerges, it will bring a whole new meaning to the phrase 'the Digital Age.'" (Id.)

Details

The Common View of Blockchains vs. Distributed Databases.

- Particularly during drawdown periods, the critiques of not just crypto as an asset class but underlying blockchain technology become more visible. The common critique of blockchains as inferior databases can be summed up as follows: "Blockchains suck. They're just slow distributed databases. Distributed databases have been around for decades. Just use X instead." (Id.)
 - ✓ X = PostgreSQL, MySQL, MongoDB, other SQL or NoSQL database

The Main Technical Critique of Blockchain: "Status Quo Solves"

- "[C]hained hashes are nothing new. Git uses them. Proof of Work isn't new either. It's simply a rate limiting algorithm that's been around forever." (Id.)
- MongoDB clusters or Citus Data in Postgres specifically solve
 - ✓ "A sharded cluster in MongoDB is a collection of datasets distributed across many shards (servers) in order to achieve horizontal scalability and better performance in read and write operations." (Source: MongoDB)
 - ✓ "Citus is an open source extension to Postgres that gives you the superpower of distributed tables" (Source: Citusdata.com)

The Main Answer to the Critique: "Distributed Databases Aren't Simple; Stop Oversimplifying Them"

- Distributed databases that promise scalability suffer from data consistency. Send/receive between distributed nodes can be unreliable.
 - ✓ "[L]et's consider deploying a geographically distributed database over the internet, where network delays and connection timeouts are common. The internet and most internal datacenter networks (often Ethernet) are asynchronous packet networks. On *asynchronous* networks, a node may send a message to another node, but the network gives no guarantees as to when it will arrive, or whether it will arrive at all." (Id., emphasis mine)
 - ✓ Message might be lost, stuck in queue, node may have crashed, node may have paused, time lag, etc.
- Depending on the specific use case the loss of data integrity may be acceptable as a tradeoff for another gain. However, certain applications--money being the paradigmatic use case--data integrity guarantee is mission critical.
 - ✓ "When building analytics systems, it's fine to lose a couple of data points out of millions, but when building systems that offer strong guarantees around data consistency, linearizability, ordering and causality, we have to guarantee the fidelity of every single data point, even if it's changed concurrently by multiple users." (Id.)
- Conflict resolution is problematic for distributed databases.
 - ✓ "Conflict resolution, transaction verification and transaction auditability, i.e., consensus, is a core function of blockchains and has been built into them at a base level." (Id.)
 - ✓ This stands in contrast to distributed databases need for a system administrator to handle node communication inconsistencies, failures, and conflicts.

Consensus Drawbacks of Specific Databases.

- Relational (SQL) Databases.
 - ✓ "Many popular relational database systems (which are usually considered "ACID") use weak isolation, and can cause all sorts of inconsistencies with concurrent writes. For example, if we submit multiple parallel value decrement transactions (e.g., on financial account balances), with weak isolation levels, we can easily end up with a negative balance. And these weak isolation levels (usually the default setting) are what makes relational databases scale well." (Id.)
 - ✓ ACID = Atomicity, Consistency, Isolation, Durability ("set of properties of database transactions intended to guarantee data validity despite errors, power failures, and other mishaps" per Wikipedia.)
 - ✓ What about "serializable isolation (i.e., on transaction at a time" and "serializable snapshot isolation" or "optimistic locking (typically implemented at the application level) which scales well, but only if you don't expect frequent conflicts"? (Id.) **NTS: Further research.**
 - ✓ Failovers given that "any network partition will break the replication link immediately, very quickly producing 'split brain' situations, which require manual file systems constantly diff-ing to resolve conflicts. This leaves us with the master-slave / standby models in traditional SQL databases."



Details

- ✓ Master node (where "write" happens) and replicas. Failover from replica to new master occurs via humans (in which there is inevitable downtime as someone needs to manually administer the failover) or automatically (in which the program logic cannot account for the wide variety of situations, thereby possibly resulting in major flaws like "writes" on one server but not another; see GitHub 2012)
- ✓ Even if database uses timestamps like blockchain, "how much can we trust our system clock? Yes, we have NTP to synchronize the clock, but at any given moment the machine clock can be off by tens of seconds or even minutes. This is why Google uses atomic clocks in their datacenters for their Spanner database." (Id.)
- NoSQL such as MongoDB
 - ✓ Despite the use of "sharding and implement[ation] of consensus protocol for leader election...[t]hey use something called 'eventual consistency,' which is exactly what it sounds like....In 'eventual consistency,' writes can be acknowledged but may actually never be executed." (Id.)
- No ability to handle malicious nodes given centralized administration of distributed databases.

Blockchain Features

- Persistence + Robustness due to distributed architecture immune to single node failures taking down the entire network.
- Fraud Prevention + Censorship Resistance due to consensus mechanisms tuned to preserving data integrity, animated by economic rewards.
- "Blockchains were built for transaction consistency in a datastore, allowing for auditability, atomicity, linearizability, durability, and most importantly, data integrity." (Id.)
- "To achieve consistency, blockchains follow the order-execute architecture. This means that the blockchain network orders transactions first, using a consensus protocol, and then executes them in the same order on all peers sequentially."

Main Ideas

- **Investment Fund Hybridity.** Asymmetric: self-styled *liquid* crypto venture fund. Given the hybrid nature of the crypto asset class, bucking traditional capital structure distinctions and being the "crossover" arena, "liquid venture" rings true. Query virtues (or vices) of a "hedged crypto fund." [See also Field Note 17 \(On "Tail Risk x Crypto," or "Toward a Hedged Crypto Venture Fund?"\)](#)
- **Technology Company with Fund Mandate.** Asymmetric: differentiated "value add" investor providing infrastructure services (e.g., relay nodes) to assist early-stage concepts, not simply "dumb" check + perfunctory recruiting & media / brand service (not trivializing any of these, to be sure). [See also Field Note 15 \(On "Metatransactions & User Experience"\)](#)
- **Talebian Influence.** IYI, SITG, Turkey, Asymmetry. I'd add some of my favorites that have personally impacted my relationship with the gradient of risk and uncertainty: convexity ($f \neq f(x)$), risk of ruin, ergodicity, tails, non-linearity, heuristics, Knightian uncertainty. [See also Field Note 22 \(On "Heuristics \(or Simplicity in the Face of Complexity\)" and Field Note 26 \(On "I / N"\)](#)

Details

On Asymmetric Strategy, Edge, Brand.

- Liquid crypto venture fund
 - ✓ SR: Is this akin to my [working hypothesis of a hedged crypto venture fund, where the hedges are executed in the public markets](#). Single-name or "alpha" shorts become problematic when one also has a venture strategy because it may be at a minimum *gauche*, and at a maximum *conflicting*, to bet long illiquid entrepreneurship and short liquid (but maybe not, [depending on the specific shorting program](#): e.g., short frauds, but not necessarily on business fundamental thesis-driven or business event-driven bases). Hedging, however, is more "neutral" and offers little-to-no such strategy conflicts in a venture model.
- Technology company with a fund mandate
 - ✓ SR: More aligned with entrepreneurship and a wonderful inversion of the old hat "fund with a technology mandate."
 - ✓ If you're going to be a long-term investor that's differentiated in crypto ecosystem, you need tech underpinning.
- Stage: early, but query specifically how to define; focused on crypto native strategies vs. traditional finance ported over into crypto (a la technical/quants/market makers like Jump, Citadel)
 - ✓ SR: [also, traditional fundamental hedge funds, and currently, distressed / credit strategies that may think they can apply a classic playbook to the novel asset class \(which may be true for centralized businesses, esp. exchanges, miners\); but early-stage technology distress is perhaps more in the purview of venture debt funds that might have expertise in navigating the difficulties of foreclosing on IP and other intangibles.](#)
- Value Add / Strategic Capability: implement unique approach to supporting founders beyond passive money check, recruiting / network, perfunctory Tweeting
 - ✓ Differentiation example: provide off-chain infrastructure early-stage concepts. Essentially infrastructure-as-a-service at stage where it may not make sense to enlist a third-party infrastructure provider (Alchemy, Coinbase/Bison Trails, etc.)
 - ✓ Running infrastructure, staking notes, etc. will become table stakes.
 - SR: [Other concrete examples of infrastructure services as value-add contributors vs. not just other VCs but also 3P providers? What might evolve beyond the table stakes once competition increases to offering value beyond recruiting & media?](#)
- Org Structure: small team + leverage automation. Has API for everything allowing small overhead: HR, Finance, Tech, Security. Risk Management system also API automated (but isn't this table stakes; not a real differentiator?)

On NFTs.

- Revaluation catalyst: new incremental buyers to support the exorbitant supply, exacerbated by cheaper-to-mint SOL
- Consideration: (a) own blue chips, which worked on ETH; (b) position in the stream of luck to capture something rare and hold

On Risk.

- Don't become forced seller. SR: [more intriguing is how be on the other side of the forced selling](#). Presumably, given stress/distress in crypto, assets held by struggling funds might trade at discount for exogenous fund-related reasons.
- Prudently select return enhancers in staking ecosystem and lending markets. SR: [need to dig in further esp. considering lending debacles, incl. counterparty risk.](#)

Details

Portfolio Companies Mentioned.

- BetDEX
- Blockasset
- Bridgesplit
- Dialect
- Fast Break Labs
- Hyperspace

Long Range Vision.

- Every financial instrument will move on-chain. Institutional interest naturally follows. Potentially 900 trillion of value can / will be moved on chain. If you can adapt and avoid competing on technical analysis or market making, you'll do great..
 - ✓ SR: On this view, edge is (a) durational (time arbitrage) and (b) "modern" value add (i.e., not simply cash + recruiting / networking + table stakes media). Additional sources of edge that apply include at the investing level: (a) risk management / position sizing / hedging / avoiding the Talebian Turkey status and (b) informational (given overlay of private markets where information asymmetry is likely higher).

On Crypto Manipulation.

- Can't have market manipulation in crypto, particularly DeFi, when there are no real regulations.
 - ✓ SR: is this semantic more than substance?

On Ruse of Expertise.

- Rebrand of crypto to web3 expands aperture of opportunity set
- Went from BTC to ETH to tokens to DeFi to NFTs, Gaming, Metaverse, Infrastructure
- Problem: Cannot establish domain expertise in all these areas
- Solution: Fund strategy is to identify the intersections and crossovers
 - ✓ SR: This captures an (a) analytical and (b) informational edge.

Main Ideas

Some might consider these views on tokens by B. Srinivasan as "old hat" in a fetishized quest for argumentative novelty. "Oh I've read that before," was my stance too. However, particularly during not just a crypto risk-off, but a sweeping multi-asset class drawdown, my humbler perspective is to revisit "vintage" arguments, as they very well might share the aging attribute of fine wine (or not, but a revisit is still warranted).

On Tokens as Paid API Keys.

- The framing of tokens as paid API keys is useful.
 - ✓ "[W]hen you buy an API key from Amazon Web Services for dollars, you can redeem that API key for time on Amazon's cloud. The purchase of a token like ether is similar, in that you can redeem ETH for compute time on decentralized Ethereum compute network. This redemption value gives tokens inherent utility." (Id.)
- Leaving aside legal characterization / securities law boundaries, even if the token bearer doesn't actually use the token for its designed utility, value exists. Simply, tokens as paid API keys means that these tokens aren't "worthless" as sweeping critics may claim.
- Unlike traditional API keys, tokens are tradable and liquid, whether peer-to-peer or intermediated by exchanges.

On Tokens as Important Funding Mechanism.

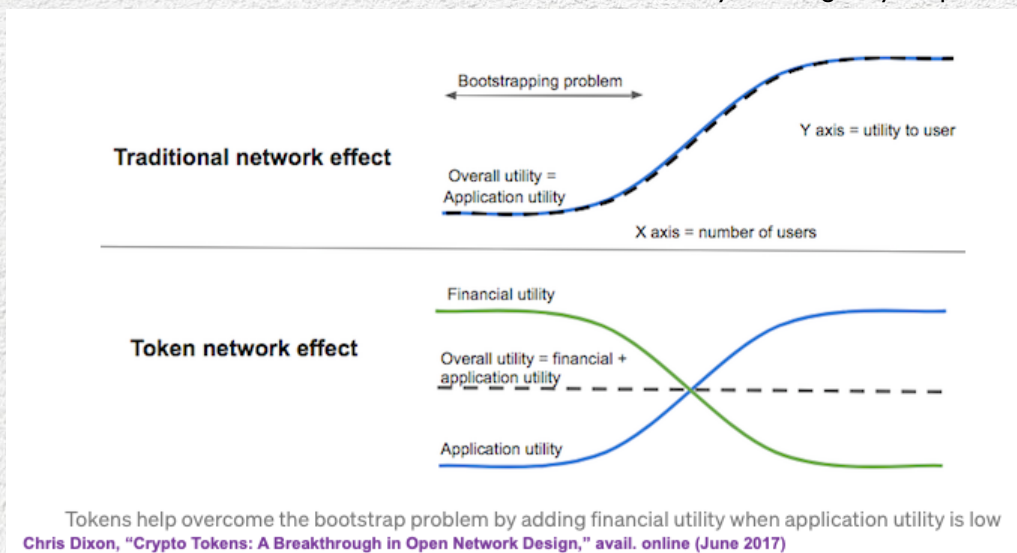
- Tokens are critical to counter big tech hegemony. As explored in Field Notes 11 and 12 (the Dixon and Placeholder theses, respectively) decentralization is important to counter the innovation-snuffing force of incumbency that develops a zero-sum relationship with its customers through data extraction, privacy affronts, and generally increased vulnerabilities. And, tokens are key to decentralization and wider participation (access to U.S. and international buyers without the need to solve operability and architectural silo problems with legacy financial system).
 - ✓ "[T]oken launches can be an alternative to traditional equity-based financings--and can provide a way to fund previously unfundable shared infrastructure, like open source." (Id.)
- Tokens are non-dilutive financings, more similar to super-charged Kickstarter sale of API keys vs. equity crowdfunding.

On Distinction between Token and Tokenized Equity.

- "[S]ome people might want to issue a token and explicitly advertise it as a way to share in the profits of their efforts as a company. For example, the issuer might want to make token holders entitled to corporate dividends and voting rights, or make the company's total ownership stock denominated in tokens. In these cases, we really are talking about tokenized equity (namely securities issuance), which is very different than the appcoin examples.... The critical distinction is whether the token is simply a useful and tradable digital item like a paid API key." (Id.)

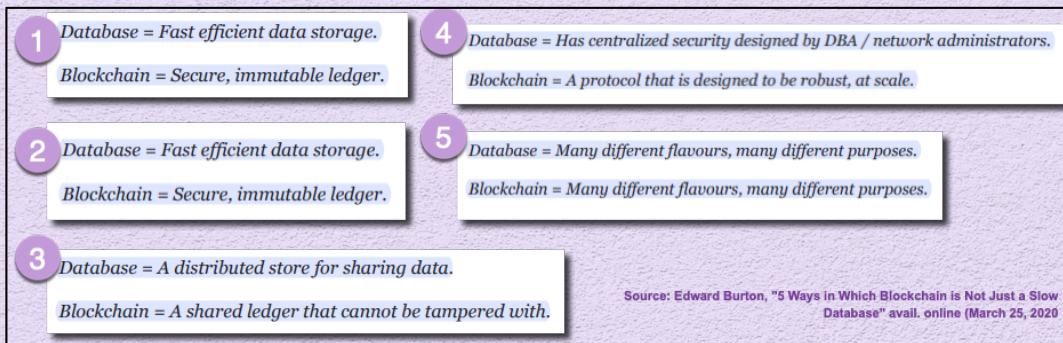
On Tokens as Rewarding the Early Adopters.

- The fusing of customer and skin-in-the-game aligned investor. "[T]oken launch model will provide a technically feasible way for tech companies (and open source projects in general) to spread the wealth and align their userbase behind their success. This is a better-than-free business model, where users make money for being early adopters." (Id.)



Main Ideas

Often, critiques of blockchain as a whole draw comparisons with modern database technology, making some version of the claim that the blockchain is just an inferior type of database. Burton offers 5 reasons why this is an incorrect comparison:



Reason 1. Blockchain = Ledger != Database

- Distinction between provenance (recording, tracking) and storage
- "A distributed ledger should be used to keep track of things, to register and record their movements and histories. A distributed ledger shouldn't be used to store data / files or assets." (Id.)
- Distributed ledger : account book :: database : bank
- This seems like a limitation to the more open-ended visions of blockchain. However, it is one of the more coherent approaches toward the compatibility of blockchain and database versus the false dichotomy often presented: either blockchain or database.

Reason 2. Blockchain Intentionally Immutable

- Database is designed for CRUD operations
 - ✓ C = create; R = read; U = update; D = delete
- Blockchain prizes immutability as a feature not a bug such that there is an audited trail of information.
- The "truth machine" metaphor is somewhat misleading; the concentration should be on immutability, not truth as such: "A blockchain does not make data more 'trustworthy,' it keeps an immutable log of everything that happens to something (mapped to an on-chain asset)." (Id.)

Reason 3. Blockchain Essentially Distributed

- Blockchain is not an inferior distributed database because the immutability & decentralization attributes of blockchain allow *sharing*, particularly in untrustworthy environments.
 - ✓ "A distributed database (with its CRUD operations) will either need to be heavily permissioned, or controlled by a centralized party. This is to stop party A from maliciously (or accidentally) tampering with data from party B. A database is designed to have a database admin, to be an efficient controllable tool to store the data of an organization. There are issues in creating 'mutually beneficial' datastores, and blockchain is a valid technology to log and report on assets that are shared between non-trusting parties." (Id.)
 - ✓ "Where you need to share accounts or a 'ledger,' a blockchain is more appropriate than a database. Where you need to share 'data,' a database is more appropriate. In most real life scenarios, you will probably want to do both." (Id.)

Reason 4. Blockchain != Slow or Inefficient

- Often the slowness or inefficiency claim comes from an uncritical observer of the bitcoin blockchain where the consensus mechanism (proof of work, adjusting block difficulty) is designed as a feature based on making the security of the system more robust.
- * "There is nothing inherent to blockchain that makes it 'slow and inefficient,' there is simply a high profile example of a blockchain that intentionally uses a lot of computing power to improve the security of its network." (Id.)

Reason 5. Blockchain = Umbrella Term, Not Specific

- One must be discerning about the use case, instead of making sweeping claims of "blockchain good" or "blockchain bad," which eliminates nuanced understanding.
- "Just like MySQL is worse than MongoDB for big data; there are no 'good' and 'bad' databases, simply technologies applied for differing purposes, and the trick as ever is to make sure you pick the right one." (Id.)

Details

On the Problem of Information Silos.

- Informational Silo defined: "isolated system that is incapable of communication with other information systems." (Id. at 6)
- Due to separate services that contain isolated parts of an actor's overall data mesh, the resulting information silo "obstructs information sharing, consequently hindering the development of data analytics." (Id. at 6)
- Data silos create higher communication costs & lower analytic insights "as the recommendation of the accurate service is often based on data analysis on historical records that now have been separated into different locations." (Id. at 1)

On the Problem of Data Misuse.

- The risk of data misuse, including emission of sensitive data to third parties intentionally or by accident, is heightened when there are different service providers responsible for isolated data silos within an organization.
- Blockchain architecture can solve: "Built-in encryption and digital signature schemes of blockchain can integrate with other security countermeasures such as authentication and access control so as to enhance the system security and preserve the data privacy. For example, data encryption and access control implemented on top of blockchain can effectively reduce the chance of data misuse and privacy leakage." (Id. at 1) *Note, this statement reads conclusionary. Need backup.*

On the Blockchain Stack.

- Abstraction (important for U/X): hides the underlying complexity of diverse computing facilities & blockchain systems
- Seamless interoperability: across different underlying blockchain systems
- Infrastructure --> Framework --> Middleware --> Application Layer

Source: Xiaoyun Li et al. (2020)

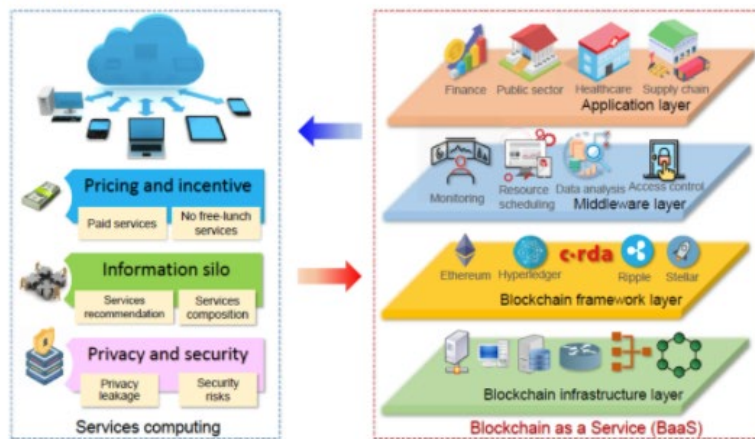


Fig. 1. When services computing meets blockchain

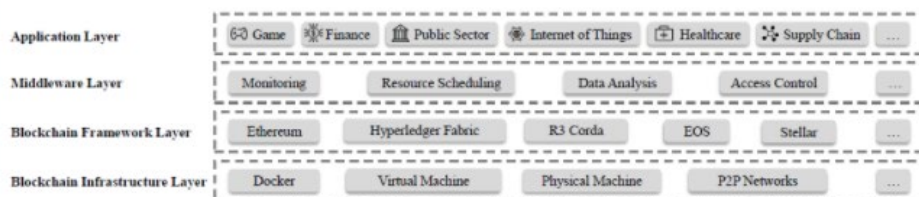


Fig. 4. BaaS architecture

On Middleware Part of the Blockchain Stack.

- Middleware purpose is to connect the framework layer (e.g., where LI sits) and the application layer (e.g., decentralized apps serving customers), acting as an "interconnection agent."
- Enables abstraction: "middleware layer hides the complexity of the underlying blockchain and offers the user-friendly interfaces to application developers in the above application layer. This layer essentially includes some fundamental system manipulation services such as monitoring, data analysis, resource scheduling, and access control." (Id. at 10)
- Classic example of middleware service is that of an oracle, which "acts as a data carrier to mediate invocation from smart contracts and external services within the inter-organizational business processes." (Id. at 12)

Details

On 4th Century Precedent for Simple Allocation Heuristics.

- Asset allocation rule from the 4th century, complements of Rabbi Issac bar Aha, "One should always divide his wealth into three parts: a third in land, a third in merchandise, and a third ready to hand." (Babylonian Talmud, qtd. Id. at 1915)

On On Estimation Error in Optimal Allocation Models.

- Markowitz in 1952: "derived *optimal* rule for allocating wealth across risky assets in a static setting when investors only care about the mean and variance of a portfolio's return."
- Main issue with this optimal risk allocation model is estimation error:
"Because the implementation of these portfolios with moments estimated via their sample analogues is notorious for producing extreme weights that fluctuate substantially over time and perform poorly out of sample, considerable effort has been devoted to the issue of handling estimation error with the goal of improving the performance of the Markowitz model." (Id. at 1916)

On I / N as a Benchmark.

- "We wish to emphasize...that the purpose of this study is *not* to advocate the use of the I/N heuristic as an asset-allocation strategy, but merely to use it as a benchmark to assess the performance of various portfolio rules proposed in the literature." (Id. at 1917)
- ✓ But see, Field Note #22: On Heuristics, or Simplicity in face of Complexity.

On the Key Findings.

- No optimization model tested consistently outperformed the I/N allocation model.
 - "[O]f the 14 models evaluated, none is consistently better than the naive I/N benchmark in terms of Sharpe ratio, certainty-equivalent return, or turnover....[W]e demonstrate that this is true: (i) for a wide range of models that include several developed more recently; (ii) using three performance metrics; and (iii) across several datasets." (Id. at 1918)
- Large time series of high integrity data is required to properly assess estimation error.
 - "[W]e find that the critical length of estimation window is 3000 months for a portfolio with only 25 assets, and more than 6000 months for a portfolio with 50 assets. The severity of estimation error is startling if we consider that, in practice, these portfolio models are typically estimated using only 60 or 120 months of data." (Id. at 1918)
- Simulations also show the need for very long estimation windows.
 - "From our simulation results, we conclude that portfolio strategies from the optimizing models are expected to outperform the I/N benchmark if: (i) the estimation window is long; (ii) the ex ante (true) Sharpe ratio of the mean-variance efficient portfolio is substantially higher than that of the I/N portfolio; and (iii) the number of assets is small." (Id. at 1918)
 - ✓ The reason for the condition (iii) is that larger number of assets implies more parameters to be estimated, meaning higher likelihood of estimation error
 - ✓ This implies that diversification benefits are overstated (see Taleb on Markowitz vs. reality).

On I / N Reducing Risk of Ruin.

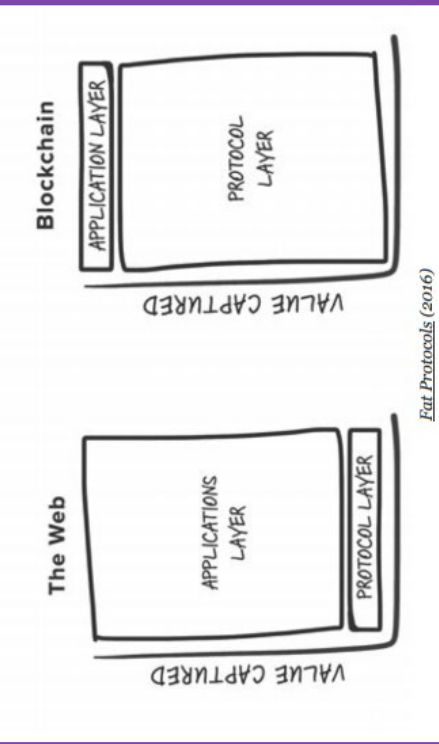
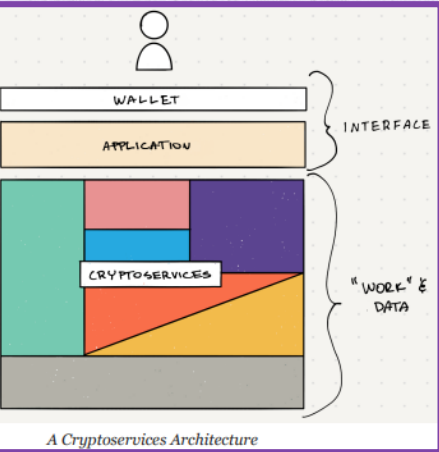
- Risk of Ruin Reduced: "'allocation mistakes' caused by using the I/N weights can turn out to be smaller than the error caused by using the weights from an optimizing model with inputs that have been estimated with error....[B]ecause the effect of estimation error on the weights is so large, even the models designed explicitly to reduce the effect of estimation error achieve only modest success." (Id. at 1919)
- Implies Positive Case for Fund of Funds(?): "A second reason why the I/N rule performs well in the datasets we consider is that we are using it to allocate wealth across portfolios of stocks rather than individual stocks. Because diversified portfolios have lower idiosyncratic volatility than individual assets, the loss from naive as opposed to optimal diversification is much smaller when allocating wealth across portfolios." (Id. at 1920)

On What Constitutes N?

- I/N rule has best chance of success when the following conditions are in play:
 - ✓ N is large "because this improves the potential for diversification, even if it is naive, while at the same time increasing the number of parameters to be estimated by an optimizing model." (Id. at 1920)
 - ✓ It's important to note that this statement is comparative: larger N means that the optimizing rules tend to underperform given more degrees of freedom / more parameters / higher likelihood of estimation error.
 - ✓ Short data history given the need for extremely long estimation windows for the optimizing strategies to have a chance at outperforming the naive I/N rule.

Main Ideas	Details
<ul style="list-style-type: none"> Srinivasan One-Liner: Public blockchains are "massively multiclient databases, where every user is a root user." Key features of public blockchains: <ol style="list-style-type: none"> (1) Canonical API without centralization (2) Lossless import/export (3) Incentivized interoperation (4) Cryptographic data integrity 	<p>On the Strawman of "Blockchain = Useless; Relational Databases Solve." The common technical critique of blockchains (specifically, public blockchains) is that the status quo solves.</p> <ul style="list-style-type: none"> "As the narrative goes, why not just use PostgreSQL for your application? It's mature, robust, and high performance. Compared to relational databases, the skeptic claims that blockchains are just slow, clunky and expensive databases that don't scale." <p>On Balaji Srinivasan's Rebuttal.</p> <ul style="list-style-type: none"> First, Srinivasan's one-liner answer to the critique: "[P]ublic blockchains are massively multiclient databases, where every user is a root user." (Id.) Second, an elaboration: Blockchains "are useful for storing shared state between users, particularly when that shared state represents valuable data that users want to export without fail – like their money." (Id.) Existing centralized cloud providers do not have a solution for shared state between accounts: "[T]hese cloud diagrams all implicitly assume that a single entity and its employees (namely, the entity with access to the cloud root account) is the only one laying out the architecture diagram and reading from or writing to the application it underpins. More precisely, these diagrams typically assume the presence of a single economic actor, namely the entity paying the cloud bills." (Id.) <p>On Issues Confronting Existing Cloud Architecture. Central assumption of existing cloud architecture is that of a single corporate entity (i.e., direct and indirect access to root account), not multiple corporate economic actors. This has several implications: applications don't (1) have interoperable software; (2) allow for standardized data export/import; and (3) provide certainty around tamper proofing. The reason this assumption exists is because "there is simply no financial incentive to enable users to export their data, let alone to enable competitors to quickly import said data." (Id.)</p> <p>On Import/Export Problem, or the Data Portability Problem.</p> <ul style="list-style-type: none"> "Data Portability Problem" defined: data siloes between different organizations / economic actors, but also within a single organization. "Data portability requires common technical standards to facilitate the transfer from one data controller to another, such as the ability to export user data into a user-accessible local file, thus promoting interoperability, as well as facilitate searchability with sophisticated tools...." (Wikipedia, "Data Portability") Current data standards fail to facilitate efficient data portability. Even though the financial incentives aren't yet present for a general solution to the data export/import problem, mechanisms have been created for many important special cases," but there is no generalized solution. (Id.). <ul style="list-style-type: none"> Current mechanisms addressing the data portability problem include (a) APIs, (b) related JSON, (c) PDF formats; (d) CSVs (unlike APIs, these are not hosted and so there's no canonical source of validity since the data can be changed without integrity checks); (e) MBOX; (f) SFTP (secured file transfer protocol, used for ACH payments). These special case solutions cannot be generalized: "Each of these mechanisms is widely used. But they are insufficient for enabling the general case of tamper-resistant import and export of valuable data between arbitrary economic actors...." (Id.) <p>On Public Blockchains Solve Import/Export Problem</p> <ul style="list-style-type: none"> The following public blockchain attributes solve the data portability problem: generally applicable (vs. special cases addressed by existing mechanisms of APIs, CSVs, etc.); tamper resistance, ensuring data integrity; data standard facilitating interoperability (efficient and effective ways of using same data in an open environment); coordination of arbitrary economic agents (creates a financial incentive that embeds cooperation in a presumptively adversarial network).
Resources	
<ul style="list-style-type: none"> n/a 	
Backlinks [internal]	
#fieldnotes #gateway	

References



Resources

- n/a

Backlinks [internal]

#fieldnotes
#framework

Details

On The 2016 Fat Protocol Thesis. Monegro's Fat Protocol thesis holds that most of the value in crypto will be captured at the base protocol layer, not the top application layer. Unlike traditional web companies, in the decentralized web stack, the protocol layer is thus "fat" while the application layer is "thin."

- "Big Web companies tend to expand their platforms [existing at the application layer] and monopolize information by locking users into proprietary interfaces. Cryptonetworks, on the other hand, tend to provide single services, and can't 'own' the interface because they don't control the data." (Id.)

On the Virtues of Fat Protocol / Thin Apps for Startups. Virtues for startups include ability to compete with well-funded, entrenched incumbents that "own" customers by taking a different path outside of the established system. Open-source frameworks proffered by the "cryptoservices architecture" allow startups to build quickly and cheaply by agonistically leveraging existing infrastructure and innovation.

- "A cryptoservices architecture is great for startups. Entrepreneurs can launch new applications quickly and cheaply by outsourcing a lot of the functionality to various networks. And every app is on equal footing when it comes to protocol costs and resources (unlike web infrastructure like AWS where the smaller you are, the more expensive it is). (Id.)

On BYOD (Bring Your Own Data). Unless choosing to delegate keys to a custodian, crypto users effectively own their data such that data become portable.

- "As a crypto user, you bring your own data. Nobody has monopoly control. When you log into a crypto app by connecting your wallet, you're sharing the 'keys' it needs to find your information across the relevant networks. You can share them with any app, so your data comes with you as you move from interface to interface. And you keep control of the 'private key' (basically a password) needed to operate on it, like signing messages or authorizing transactions." (Id.)
- "A cryptoservices architecture combined with a non-custodial data model allows startups to compete more effectively against centralized incumbents." (Id.)
- "Giving ownership and control to the users offloads a lot of costs while fulfilling many of today's consumer demands. It does require companies to give up a lot of what makes traditional online services defensible. But what you lose in control, you gain in potential efficiency and scale....As a network, thin applications can scale more effectively across markets." (Id.)

Success of the Thin Needed for Success of the Fat. Application layer success is needed for protocol layer success since the former contributes scale and value to the underlying network. In other words, the applications render the protocol useful.

On Value Pool vs. Investment Returns. It is a basic statement that even though most of the network value is captured at the protocol layer (according to the Fat Protocol thesis), this does not mean there are no financial / investment returns to be captured at the thin application level.

- "[T]hat less overall value ends up at the application layer *does not* mean there are fewer outsized return opportunities available to application businesses. Nor does it mean there's *always* returns in protocols. Value capture is more about TAM and other macro elements, while returns vary by things like cost basis, growth rates, and ownership concentration. What's different between protocols and applications is how these elements combine." (Id.)

On the Decentralized Value Chain. The value chain goes as follows: protocol provides bundled services for the applications, which ultimate serve specific customers.

- "In a way, it's similar to the retail model where storefronts act as 'interfaces' to various commodity products and differentiate themselves by brand, curation and customer experience. But instead of 'B2B2C' think of crypto as P2B2C for *Protocol to Business to Consumer*. Protocols provide specific services, which are bundled at the application layer for distribution to consumers." (Id.)

Prepared by Sandeep Ramesh strictly for educational (neither investment nor business) purposes.

Main Ideas	Details
<ul style="list-style-type: none"> "[T]here's no one magic system called 'blockchain' that magically does everything. Rather, there are really good building blocks of computing that can be used together to create effective decentralized applications." (Id.) Three elements of computing: (1) storage, (2) compute / processing, (3) communications Three elements of decentralized computing: (1) storage, database, file system; (2) stateful business logic, stateless business logic, high performance compute; (3) networks of data, value, state <div> <div>Blockchain Infrastructure Landscape</div> <div>Blockchain technology is manifesting in each block, as this image shows [2]:</div> <div> <div>THE 3 ELEMENTS OF COMPUTING: DECENTRALIZED</div> <div> <div>STORAGE</div> <div>COMMUNICATIONS</div> <div>PROCESSING</div> </div> <div> <div>TOKEN STORAGE Bitcoin, Zcash, ..</div> <div>STATEFUL BIZ LOGIC Ethereum, Lisk, Rchain, Tezos, .. Client-side compute (JS, Swift)</div> <div>DATA TCP/IP, HTTP, Tokenized Tor</div> <div>FILE SYSTEM or BLOB IPFS/FileCoin, Eth Swarm, Storj, Sia, Tiron, LAFS</div> <div>STATELESS BIZ LOGIC Crypto Conditions (e.g. BigchainDB), Bitshares, Eos, and all stateful biz logic</div> <div>VALUE Interledger, Cosmos</div> <div>DATABASE BigchainDB + IPDB, IOTA</div> <div>HIGH PERF. COMPUTE TrueBit, Golem, iExec, Nyriad, VMs, client-side compute</div> <div>STATE Polkadot, Aeternity</div> <div>DATA MARKET Ocean, Enigma, DataBroker, Datum</div> </div> </div> </div>	<p>On Building Blocks Framework. While the map must never be confused for the territory, having a map remains critical in evaluating the otherwise incoherent blockchain ecosystem. This is particularly true from an investment standpoint where there are direct consequences to informational overload, analytical paralysis, cognitive biases, etc. However, current schema are largely insufficient for investment (and broader business) purposes, relying too heavily on technical classifications geared perhaps toward system designers and architects. This might be one shortfall of the following McConaghy framework (granted, it wasn't likely designed with the investor in mind).</p> <p>On Decentralized Storage.</p> <ul style="list-style-type: none"> Element 1: Token Storage. Activities: token issuance, transfer, burn, prevention of double-spend. Element 2: Database. Activities: storing structured data (e.g., relational databases), documents (e.g., JSON), key-value stores, time series, graphs. Retrieving data via queries (e.g. SQL). <ul style="list-style-type: none"> "Traditional distributed (but centralized) databases like MongoDB and Cassandra routinely store hundreds of Terabytes and even Petabytes of data, with throughput that can exceed 1 million writes per second." (Id.) "Query languages like SQL are profound because they separate implementation from specification, and are therefore not bound to any particular application. SQL has been a standard for decades. This is why the same database system can be used across many different industries." (Id.) "To put another way: to generalize beyond Bitcoin to more applications without any application-specific code, you don't need to go all the way to Turing completeness. You just need a database. This has corresponding benefits in simplicity and scale." (Id.) Element 3: File System / Blob. Activities: store large files (movies, mp3s, large data sets), organized in directories & files. Element 4: Data Market. Activities: connect data owner with data consumer; exists at higher-level than databases and file systems <p>On Processing.</p> <ul style="list-style-type: none"> Building Block 1: Stateless or Combinatorial Business Logic. <ul style="list-style-type: none"> "This is any arbitrary logic that does not retain state internally. In electrical engineering terms, it can be framed as *combinatorial digital logic* circuits." (Id.) Building Block 2: Stateful or Sequential Business Logic. <ul style="list-style-type: none"> "This is any arbitrary logic that *does* retain state internally. That is, it has memory." (Id.) "More generally, stateful business logic is a Turing machine that takes in a sequence of inputs, and returns a sequence of outputs. Systems that manifest (a practical approximation of) this are called Turing-complete systems." (Id.) Building Block 3: High-Performance Compute (HPC). <ul style="list-style-type: none"> "This is processing to do 'heavy lifting' compute for things like rendering, machine learning, circuit simulation, weather forecasting, protein folding, and more." (Id.) <p>On Communications.</p> <ul style="list-style-type: none"> Level 1: Data. TCP/IP remains a key decentralized building block for connecting data networks. Level 2: Value. TCP/IP connects networks at data level where double-spend is possible. To connect networks of value, double-spend must be prevented. Level 3: State. Projects like Polkadot aim to connect networks of state (e.g., different chains).
Resources	
<ul style="list-style-type: none"> n/a 	
Backlinks [internal]	
#fieldnotes #framework	

Main Ideas	Details
<ul style="list-style-type: none"> Especially in highly complex and uncertain domains (e.g., crypto investing), simple & robust heuristics can outperform complex and so-called optimal ones. The apparent reflexive nature of crypto markets evokes a Knightian uncertainty. Resource limitations point to increased value of simple heuristics. 3 key factors that help us determine approximately where on the risk vs. uncertainty continuum our decision scenario exists: (1) available amount of data that is relevant and reliable (see also M. Lopez de Prado); (2) type of model considered; and (3) structure of the decision environment. These factors are under-explored in the paper, or at least not directly elaborated. The I / N heuristic tells us to equally allocate our bankroll across N assets. Importantly, this is a position sizing heuristic. It, by itself, does not tell us what comprises N, nor how to select N. As a sizing rule, the simplicity of I / N massively reduces cognitive burden, and crucially, outperforms traditional finance's adoption of Markowitz's mean-variance model. 	<p>On Simplicity & Robustness in the Face of Complexity. Complex decision environments do not necessarily warrant complex solutions. In fact, simple and robust heuristics can outperform complex and so-called optimal ones.</p> <ul style="list-style-type: none"> "[W]e question the common belief that complex problems automatically call for complex solutions. As an alternative, we suggest that simple, yet robust strategies provide important insights and offer potential solutions for managing financial systems under uncertainty." (Id. at 135) <p>This is true of financial domains where there is Knightian uncertainty (see Field Note #16. On "Knightian Risk, Uncertainty, Profit" (+ Crypto)). The apparent reflexive nature of crypto markets highlights this degree of uncertainty.</p> <ul style="list-style-type: none"> "If financial systems are fundamentally uncertain, theoretical and empirical results from psychology and decision science suggest that simple heuristics may provide more accurate and robust predictions than more flexible models." (Id. at 135) <p>Resource limitations point to increased value of simple heuristics:</p> <ul style="list-style-type: none"> Given the complexity of many real-world situations and agents' limited computational resources (eg of time and memory capacity) evolution selected strategies that work well under uncertainty. Nature successfully bets on <i>heuristics</i>—simple rules-of-thumb that can yield effective and efficient results by ignoring irrelevant information—in many different species and task domains." (Id. at 137) <p>On the Specter of Frank Knight. One cannot properly understand complex decision-making environments, particularly in investing, without visiting the work of Frank Knight (see Field Note #16).</p> <ul style="list-style-type: none"> "Knight argued that a situation of <i>risk</i> is characterized by the existence of an objective basis to derive outcome probabilities....Knight contrasted these scenarios with <u>conditions in which outcome probabilities are not logically deducible and cannot be directly inferred from data</u>—a class of situations he referred to as decision making under <i>uncertainty</i>." (Id. at 136) <p>On Knightian Risk vs. Uncertainty as Part of a Continuum.</p> <ul style="list-style-type: none"> "Whereas Knight's original distinction was dichotomous and qualitative, most real-world situations are embedded in wider contexts and lie somewhere in-between. Thus, <u>Knight's categories of risk vs uncertainty constitute the extremes of a continuum of varying degrees of uncertainty.</u>" (Id. at 136) <p>3 key factors that help us determine approximately where on the risk vs. uncertainty continuum our decision scenario exists: (1) available amount of data that is relevant and reliable (see M. Lopez de Prado's work on data problems in predictive machine learning & investing); (2) type of model considered; and (3) structure of the decision environment. (see Id. at 136). These factors are under-explored in the paper, or at least not directly elaborated.</p> <ul style="list-style-type: none"> "[S]ituations with <u>high levels of uncertainty, a large number of alternative options, and small amounts of relevant data</u> tend to favor simple methods over more flexible ones." (Id. at 139) <p>On Position-Sizing. The I / N heuristic tells us to equally allocate our bankroll across N assets. Importantly, this is a position sizing heuristic. It, by itself, does not tell us what comprises N, nor how to select N. As a sizing rule, the simplicity of I / N massively reduces cognitive burden, and crucially, outperforms traditional finance's adoption of Markowitz's mean-variance model.</p> <ul style="list-style-type: none"> "[W]hen DeMiguel and colleagues compared this [Markowitz's] model and its modern variants with a simple I / N heuristic ...the mean-variance model failed to outperform the seemingly naïve I / N strategy. As the surprising success of the I / N heuristic generalizes to diversifications in international stock markets and over different asset classes it seems smart that Markowitz himself used this simple strategy instead of his own method of portfolio optimization." (Id. at 138)
Resources	
<ul style="list-style-type: none"> Gigerenzer, "Risk Savvy: How To Make Good Decisions" (2014) DeMiguel et al. "Optimal Versus Naïve Diversification" (2009) 	
Backlinks [internal]	
#fieldnotes #heuristic #investing #positionsizing #complexity	

Main Ideas	Details
<ul style="list-style-type: none"> The Issue Presented. Where does it make sense to use blockchains in non-financial applications? On Buterin's Middle Way. It is critical to avoid extremes, particularly in domains where the probability space is impenetrably wide, and multidisciplinary attitudes and teams are necessary to enter the arena. On Four Non-Financial Use Categories. <ul style="list-style-type: none"> (1) Account Management / keys; (2) Interoperability; (3) Negative Reputation; (4) Proving Limited Quantity Of these categories, Buterin places highest conviction in the first two: "Out of all the above list, the two I am personally by far the most confident about are interoperability with other blockchain applications and account management. The first is on-chain already, and the second is relatively cheap (need to use the chain once per user, and not once per action), the case for it is clear, and there really isn't a good non-blockchain-based solution." 	<p>The Issue Presented. <i>Where does it make sense to use blockchains in non-financial applications?</i></p> <ul style="list-style-type: none"> "[A]re blockchains only good for finance (say, because network effects mean that money has a unique need for a 'global view'), with all other applications better done using centralized or more local systems?" (Id.) <p>On Buterin's Middle Way. <i>It is critical to avoid extremes, particularly in domains where the probability space is impenetrably wide and multidisciplinary attitudes and teams are necessary to enter the arena.</i></p> <ul style="list-style-type: none"> "My own view tends to be...far from the 'blockchain everywhere' vie2wpoint, but also far from a 'blockchain minimalist. I see the value of blockchain in many situations, sometimes for <i>really important</i> goals like trust and censorship resistance but sometimes purely for convenience." (Id.) <p>Use Case Category: "Key Changes." <i>Account management benefits from the properties of blockchains.</i></p> <ul style="list-style-type: none"> Four examples: <ul style="list-style-type: none"> 1. User wants to switch keys for fear that current key will be lost or stolen. 2. User wants to switch to a different cryptographic algorithm (e.g., away from SHA-256) due to far off specter of quantum computing compromise 3. User has lost a key and wants to regain account access 4. User wants to regain sole access to an account after the associated key has been stolen First two examples can be done in self-sovereign manner since the user can authenticate a message with current key stating "Current Key is hereby superseded by New Key." However, if a bad actor steals superseded Current Key sometime in the future, then the bad actor can publish a new message stating "Current Key is hereby superseded by New Key B" thereby "frog jumping" the true user's key switch. The problem to solve in the above case is to "prevent the previous key controlling an account from being able to change the key," which shares similarities to the double spend problem in the case of digital currencies. Therefore, "like creating a decentralized currency, doing account management in a decentralized way requires something like a blockchain. A blockchain can timestamp the key change messages, providing common knowledge over" the sequence of events. <p>Use Case Category: "Interoperability with Other Blockchain Applications." <i>Basic claim: "some things should be on-chain to better interoperate with other on-chain applications."</i></p> <ul style="list-style-type: none"> "Proof of humanity" example: "Proof of humanity being an on-chain NFT makes it easier [for] projects to automatically airdrop or give governance rights to accounts that have proof of humanity profiles." Oracles example: "Oracle data being on-chain makes it easier for defi projects to read....But the main value that being on-chain provides is simply <i>being in the same place as the stuff that you're interacting with, which needs a blockchain for other reasons.</i>" <p>Answer To: "But, We Should Only Use Blockchains Where No Other Solution Comes Close." <i>This common critique confronts Amara's Law that we tend to overestimate tech's impact in the short run and underestimate its impact in the long run.</i></p> <ul style="list-style-type: none"> "This attitude makes sense in a world where transaction fees are very expensive, and blockchains are uniquely incredibly inefficient. But it makes less sense in a world where blockchains have rollups and sharding and transaction fees have dropped down to a few cents, and the difference in redundancy between a blockchain and a non-blockchain decentralized storage might only be 100x." <p><i>Prepared by Sandeep Ramesh strictly for educational (neither investment nor business) purposes.</i></p>
Resources	
<ul style="list-style-type: none"> Weyl, Ohlhaber, and Buterin, "Decentralized Society: Finding Web3's Soul" (May 2022) 	
Backlinks [internal]	
#fieldnotes	
#usecase	

Main Ideas	Details
<ul style="list-style-type: none"> Expertism in crypto is misguided The web 3 stack can be abstracted into useful categories that still belie the underlying complexity Be chain agnostic; no “one chain to rule them all” reality in sight Be pragmatic when it comes to permissioned blockchains On optionality preservation as a critical philosophical approach: quoting Gavin Wood, “The critical thing is that optionality be retained— similarly by Linux being open source, you keep the optionality to audit and understand the codebase; this was instrumental in gaining its adoption in Android and by large enterprises such as IBM.” 	<p>On the Impossibility of Expertise in Crypto. The rapid pace of innovation, the technical depth, the regulatory opacity, and the broad probability space for business outcomes over an indeterminate time series, interlaced by cultural, ideological, and philosophical motivations make expertise in crypto or blockchains impossible. "Putting myself in the shoes of such high-flying decision-makers, I can only imagine how utterly bemused I would be by the dizzying array of acronyms, promises and variety of software on display (anyone up for buzzword bingo?)" (Id. at Part 1)</p> <ul style="list-style-type: none"> "[E]ven the topmost expert in the field of blockchains simply cannot with 100% certainty define the stack of protocols that will form the future 'Web 3.0.'" (Id. at Part 1) <p>On the Web 3 Stack.</p> <div> <div> <div>The Web 3.0 Abstracted Stack</div> <div>Source: Id. at Part I.</div> <div>Diagram v1.0 by @stephantual - 26 May 2017</div> <div> <div>Dapps Browsers (Parity, status.im, Mist, LETH, Metamask, etc.)</div> <div>Decentralized Applications (slock.it, Gnosis, Melonport, Zonafide, Etherisc, jaak.io, etc.)</div> <div> <div>Messaging (whisper, telehash, etc.)</div> <div>Storage (IPFS, SWARM, StorJ, maidsafe, etc.)</div> <div>State Machines (EVM, MSC/qtum-like, custom, etc.)</div> <div>Consensus (PoW, PoS, PoA, PoET, etc.)</div> <div> <div>Data Feeds (Oracleize.it, Town Crier, etc.)</div> <div>Off-chain Computing (Cloud, Ewasm VMs, etc.)</div> <div>Governance (DAOs, futarchy, hard/soft forks, etc.)</div> <div>State Channels (Raiden, Lightning Network, etc.)</div> <div>Cryptographic Network & Transport Protocols (RLPx, roll your own, etc.)</div> <div>Optional Internet Routing Protocols (none, Tor, I2P, etc.)</div> </div> </div> </div> <p>On Chain Agnosticism. Provocatively and against the grain of more mainstream views, the notion of "one chain to rule them all" is a ruse and fools gold for those with an improper balance of open-mindedness and skepticism.</p> <ul style="list-style-type: none"> "[S]tay chain and protocol agnostic at a time when fragmentation in our vertical is taking place at an exponential rate. We are at least years away from any form of generally accepted dApp standardization in the same fashion AMP is generally accepted as the archetypal model for web service stack as of 2017." (Id. at Part 2) <i>SR: the AMP stack is a set of software components for the operation of web-based software applications. For example: Apache / MySQL / PHP packages or with more generalized terminology, web server / relational database management system / general purpose scripting language.</i> "There are many use cases, especially in the IoT space...where the main challenge is transferring data and executing function calls between platforms. For example, I might want to find, from an Ethereum smart contract, the GPS coordinates of a given object that's registered on Hyperledger." (Id. at Part 2) "It's likely that if you are serious about blockchain development beyond PoCs, you will find yourself in a situation where you'll need to create you[r] very own state transition engine, specific to your industry vertical (healthcare, legal, IoT, etc.) with its own...characteristics." (Id. at Part 3) <p>On Pragmatism Surrounding Private Blockchains. By cutting through the ideology of “purity” and embracing the messiness of innovation, complexity, and uncertainty, one can acknowledge the utility of private permissioned chains. Maximalism is a bug.</p> <ul style="list-style-type: none"> "Some question why one might want to negate every single advantage of running Blockchain code by deploying it on someone else[s] centralized network, but the reality is that many companies will be happy to use cloud-hosted or BaaS [i.e., blockchain as a service] products regardless." (Id. at Part 3) <p><i>Prepared by Sandeep Ramesh strictly for educational (neither investment nor business) purposes.</i></p> </div></div>
<div>SR Synthesis</div> <ul style="list-style-type: none"> The rapid pace of innovation, the technical depth, the regulatory opacity, and the broad probability space for business outcomes over an indeterminate time series, interlaced by cultural, ideological, and philosophical motivations make expertise in crypto or blockchains impossible. This is a Gordian Knot. The Gordian Knot is impossible to untangle. The only appropriate solution is to cut it. When there is a problem that is intricate and intractable, the solution is not to work within its logic, but transcend it. From an investor standpoint, the ways to cut this knot, inter alia, I'm exploring are (a) disciplined, non-concentrated, non-over-levered position sizing, (b) portfolio diversification (but how to avoid "cosmetic" diversification?), (c) hedging & shorting, and most critically, (d) multidisciplinary and humble teams. How else? 	
<div>Backlinks [internal]</div> <div> <div>#fieldnotes</div> <div>#framework</div> <div>#polkadot</div> </div>	

Main Ideas

- **Hazlitt's Critical Lesson:** "We are all accustomed to measuring our income and wealth in terms of money. The mental habit is so strong that even professional economists and statisticians cannot consistently break it. It is not easy to see relationships always in terms of real goods and real welfare. Who among us does not feel richer and prouder when he is told that our national income has doubled (in terms of dollars, of course) compared with some preinflationary period? Even the clerk who used to get \$75 a week and now gets \$120 thinks that he must be in some way better off, though it costs him twice as much to live as it did when he was getting \$75. He is of course not blind to the rise in the cost of living. But neither is he as fully aware of his real position as he would have been if his cost of living had not changed and if his money salary had been reduced to give him the same reduced purchasing power that he now has, in spite of his salary increase, because of higher prices. Inflation is the autosuggestion, the hypnotism, the anesthetic, that has dulled the pain of the operation for him. Inflation is the opium of the people." (Id. at 173-174)

Resources

- Faustino Ballve, Essentials of Economics: summarizes principles
- Percy Greaves, Understanding the Dollar Crisis
- Ludwig von Mises, Human Action
- Murray Rothbard, Man, Economy, and State

Backlinks [internal]

#fieldnotes
#austrianeconomics
#economics

Details

On Failure To See Long-Term and Second-Order Effects. We are all aware of the virtues of focusing on the long-term. The probability space as duration increases tends to widen. This orientation toward the long-term, properly understood, enforces creative thinking and exploration of contingencies.

- "The act of economics consists in looking not merely at the immediate but at the longer effects of any act or policy; it consists in tracing the consequences of that policy not merely for one group but for all groups." (Id. at 17)

On the Money Illusion. That money / income is synonymous with wealth should be understood as a cognitive bias that reason alone cannot penetrate.

- "But as most people are so firmly in the habit of thinking of their wealth and income in terms of money, they consider themselves better off as these monetary totals rise, in spite of the fact that in terms of things they may have less and buy less." (Id. at 26)
- "Yet so powerful is the verbal ambiguity that confuses money with wealth, that even those who at times recognize the confusion will slide back into it in the course of their reasoning." (Id. at 165)
- "Mere inflation—that is, the mere issuance of more money, with the consequence of higher wages and prices—may look like the creation of more demand. But in terms of the actual production and exchange of real things it is not. It should be obvious that real buying power is wiped out to the same extent as productive power is wiped out. We should not let ourselves be deceived or confused on this point by the effects of monetary inflation in raising prices or 'national income' in monetary terms." (Id. at 29)

On Pernicious Inflation Distortion. In order to combat price distortions stemming from monetary inflation that induces malinvestments, a hedged investment book, combined with disciplined position sizing, becomes highly attractive. Indeed, necessary. Survival in markets is a precondition to upside.

- "Even a relatively mild inflation distorts the structure of production. It leads to the overexpansion of some industries at the expense of others. This involves a misapplication and waste of capital. When the inflation collapses, or is brought to a halt, the misdirected capital investment—whether in the form of machines, factories or office buildings—cannot yield an adequate return and loses the greater part of its value." (Id. at 170)
- "[A]rtificial reduction in the interest rate...tends, in fact, to encourage highly speculative ventures that cannot continue except under the artificial conditions that gave them birth. On the supply side, the artificial reduction of interest rates discourages normal thrift, saving, and investment. It reduces the accumulation of capital." (Id. at 186)
- **The clincher:** "Each generation and country follows the same mirage. Each grasps for the same Dead Sea fruit that turns to dust and ashes in its mouth. For it is the nature of inflation to give birth to a thousand illusions." (Id. at 171)

On the Employment Illusion. Production is the goal, not employment. Employment rises as a consequence of production maximization. Goodhart's Law: When the measure becomes the target, it ceases to be the correct measure.

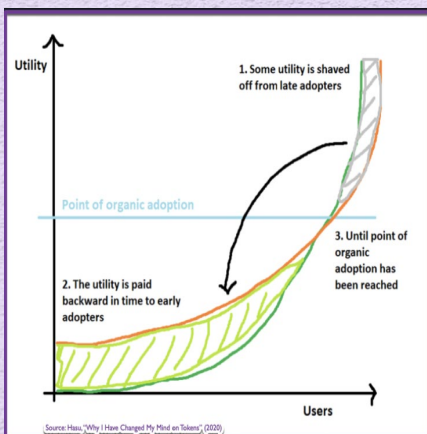
- "When providing employment becomes the end, need becomes a subordinate consideration. 'Projects' have to be invented. Instead of thinking only of where bridges must be built, the government spenders begin to ask themselves where bridges can be built." (Id. at 32)

On Cost Efficiencies as True Profit Driver (not price increases). If cost efficiencies are the prime driver of profits, query how this logic confronts and adapts to open-source ecosystems.

- "Contrary to a popular impression, profits are achieved not by raising prices, but by introducing economies and efficiencies that cut costs of production." (Id. at 162)

Main Ideas

- Token Maximalism, Governance Minimalism.
- "Token maximalism simply shouldn't go along with governance maximalism just because developers feel a need to give additional functionality to their tokens. Governance minimalism is still king, even if the project has a native token."
- "Don't just ask 'why does xyz need a token?' but also 'how can xyz support a token?'"
- "[P]rotocols that tokenize late adopter utility to reward early adopters will most likely outcompete protocols that don't and rely entirely on organic growth."



Resources

- n/a

Backlinks [internal]

#fieldnotes
#beginnercrypto
#tokens

Details

- **On Three Common Critiques of Tokens.**
 - **Governance Attack Vector.**
"Governance itself is an attack vector because it allows bad actors to change the rules of the protocol and -- in the worst case -- steal user deposits. [T]his defeats the whole purpose of using smart contracts to begin with." (Id.)
 - **Re-Instantiation of Rent-Seeking.**
"Our goal in crypto is to replace rent-seeking companies and institutions with open and fair protocols. Extracting rent from users is regressive and violates this core value." (Id.)
 - **Open-Source Architecture Means Rent Equilibrates to Zero (and so why do you need a token?)**
"Since protocols are open-source and can be forked by anyone, the equilibrium rent is always zero. It's only a matter of time until we converge on that equilibrium and then the value of governance tokens will likewise collapse to zero. That's why anyone selling them today must be a scammer." (Id.)
- **Answer To: Governance Attack Vector.** All valuable projects require human input, interaction, and discretion that impacts protocol governance and decision-making. While governance may be an attack vector, it remains a necessary attribute of useful projects. The goal ought to be to minimize the attack surface, not to neuter the pragmatic success of the project by removing it
 - "For protocols where human input is required, including at the early / formation stages of a network, fees are also required to incentivize agents to act in the best interest of the system. Those fees are organized and distributed via tokens." (Id.)
- **Answer To: Re-Instantiation of Rent-Seeking.**
 - No ethical hang-ups over charging user fees, so this an ideological strawman critique
 - **Open-source self-corrects:** "The mechanisms of the market (competition, open-source code, etc.) will themselves ensure over time that this rent won't be larger than necessary." (Id.)
- **Answer To: Open-Source Architecture Means Rent Equilibrates to Zero.**
 - **Without rent, there is nothing worth forking.** "[I]t's simply too hard to compete with incumbent networks if you can't reward your early adopters." (Id.)
 - **Tokens solve "chicken-and-egg" or "cold start" problem:** "Projects have found a hack to bridge the difficult early adoption phase by funneling the utility of future adopters to early ones, thereby smoothing out their respective utility functions." (Id.)
 - **Pre-mining allows project to hire team that otherwise would not work for free; same as equity allocation for a typical startup.**
 - "No other project since Bitcoin has managed to bootstrap itself without rewarding their early contributors and been more than a mere copycat (thus excluding Litecoin)." (Id.)
 - "Without a direct financial incentive, it's incredibly difficult to get both sides of a market to stop whatever they are doing and move to a new system together. A new system, that -- even if its slightly cheaper to use -- would have a weaker brand, weaker liquidity, no developers, no community, no integrations with other projects, etc. Overall, I think there's a very good chance that beyond a certain size, projects are basically resistant to forks. It's just a matter of getting to that point." (Id.)

Main Ideas	Details
<ul style="list-style-type: none"> Market participants and market structures have changed substantially over the years, giving way to modern investors untethered to classical investment views that have become dogma. There is no better place to see the transition from effective wisdom to veritable dogma than in crypto. What does appear to remain constant is the primacy of the question: <i>how much?</i> That is, bet sizing—and hedging—to avoid the risk of ruin. Diversification is a start, not the end. This mandate is particularly strong in crypto given the interconnected "daisy chain" of risks that can render attempts at diversification merely cosmetic. My working hypothesis is that traditional crypto venture funds have been ignoring a skill set and toolkit known to liquid investors: hedging (and perhaps shorting, though crypto market infrastructure is not developed enough here). Crypto is a hybrid asset class whereby the illiquid vs. liquid attribute is blurred. This might open the space for a hybridized venture x hedge fund model, what one might term "hedged venture." Always-on hedging—in particular, tail risk hedging—is required, not just a diversified book. Again, anyone devoted to the crypto space understands this directly. 	<ul style="list-style-type: none"> On Agility Trumping Investment Dogma. Market participants and market structures have changed substantially over the years, giving way to modern investors untethered to classical investment views that have become dogma. There is no better place to see the transition from effective wisdom to veritable dogma than in crypto. What does appear to remain constant is the primacy of the question: <i>how much?</i> That is, bet sizing—and hedging—to avoid the risk of ruin. <ul style="list-style-type: none"> "[Investors] will also need to limit their vulnerability to severe downturns that threaten to suddenly erase hard-gained returns and, judging from the insights of behavioral finance, also increase the probability of subsequent portfolio <u>mistakes</u>." (Id. at xi, Forward by M. El-Erian) "To succeed, investors will need to construct global portfolios with more agile alpha and beta engines, more forward-looking differentiation, and more resilient sizing of positions." (Id.) On Diversification as Necessary but Not Sufficient. Diversification is a start, not the end. This mandate is particularly strong in crypto given the interconnected "daisy chain" of risks that can render attempts at diversification merely cosmetic. <ul style="list-style-type: none"> "[T]his happened during the 2008 crisis when many large and small investors, who appeared to be cosmetically diversified, realized that their portfolios were exposed to <u>hidden tail risk</u>. Thus, it is important to understand how <u>large-scale liquidations</u> may endogenously result in the covariance structure between asset returns to change, and contagion may occur." (Id. at 18) "[E]ven assets that are fundamentally uncorrelated may become correlated on the tails if they are affected by a common liquidity factor." (Id. at 18) On Open-Minded Approach to Portfolio Risk. My working hypothesis is that venture funds singularly focused on crypto have been ignoring a skill set and toolkit known to liquid investors: hedging (and perhaps shorting, though crypto market infrastructure is not developed enough here). Crypto is a hybrid asset class whereby the illiquid vs. liquid attribute is blurred. This might open the space for a hybridized venture x hedge fund model, what one might term "hedged venture." <ul style="list-style-type: none"> "[H]aving an open-minded and dynamic approach to managing portfolio risk for all magnitudes of positive and negative surprises is <u>no longer a luxury but a necessity</u>." (Id. at 8-9) "Often it is more efficient to sacrifice basis risk and close match of hedges by using correlation to our advantage to obtain cost-efficient hedges. For instance, credit-market tail risk events are frequently hedged better with equity options that with customized credit-hedge instruments. Indeed, this might blur the distinction between an active position and a hedge, but in the final analysis, the <u>characterization of a position is less important than the economic benefits it confers</u>." (Id. at 3) <p>Tail hedging ought to be viewed not just as defense, but offense.</p> <ul style="list-style-type: none"> On Tail Risk Hedging as Always-On vs. Just-in-Time. Always-on hedging—in particular, tail risk hedging—is required, not just a diversified book. Again, anyone devoted to the crypto space understands this directly. <ul style="list-style-type: none"> "[T]he benefit of having appropriate amounts of disaster insurance is financial survival. When applied to investing, there is a secondary benefit as well, that the survivors are better able to take advantage of reduced liquidity and attractive prospective returns. Thus, tail "hedging" is an offensive strategy for the long term, even though it comes at a cost." (Id. 1-2) On Cash as a Hedge. "Strategic cash" is not "trash" (contra Dalio) in crypto. <ul style="list-style-type: none"> "For catastrophic loss events, <u>there is no substitute for having a pristine source of liquidity</u>. However, in a world where nominal yields are low and inflation is likely to rise, the "real" (nominal minus inflation) <u>return on cash should be considered against the other alternatives</u>." (Id. at 7-8)
Resources	
<ul style="list-style-type: none"> n/a 	
Backlinks [internal]	
#fieldnotes #tailrisk #hedging	

Main Ideas	Details
<ul style="list-style-type: none"> Uncertainty is the inherently unknowable, impenetrable by increasingly refined analysis. The rewards of engaging with true uncertainty is the source and justification for entrepreneurial profits It is a mistake to treat induction and deduction as exclusive methods. Rather, both are insufficient and yet, both are required. Over-indexing to induction favors concreteness at the exclusion of principled reasoning. Over-indexing to deduction favors generalization at the expense of supportive evidence. Perhaps, one must realize the interaction between inductive and deductive lenses is endless & paradoxically stable only in its instability. Analogy is the animating force behind reasoning. The imprecision of analogy means that cold machine-like certainty is a ruse. At the same time, the imprecision is what allows for possibility, serendipity, and tail events (positive & negative). Despite the desire to reduce uncertainty, the irony is that our life would be far less appealing without it. 	<ul style="list-style-type: none"> On Risk vs. Uncertainty. <i>Uncertainty is the inherently unknowable, impenetrable by increasingly refined analysis.</i> <ul style="list-style-type: none"> "The practical difference between the two categories, risk and uncertainty, is that in the former the distribution of the outcome in a group of instances is known (either through calculation <i>a priori</i> or from statistics of past experience), while in the case of uncertainty this is not true, the reason being in general that it is impossible to form a group of instances, because the situation dealt with is in a high degree unique. The best example of uncertainty is in connection with the exercise of judgment or the formation of those opinions as to the future course of events, which opinions (and not scientific knowledge) actually guide most of our conduct. (Id. at 233) "The actual procedure of making decisions in practical life is a rather inscrutable or "intuitive" formation of "estimates," subject to a wide margin of error or uncertainty." (Id. at 314) <i>SR: These are obvious statements in some sense, but the simplicity is what can confound investors, who seductively chase some version of a "holy grail" answer.</i> On Entrepreneurial Profit. <i>The rewards of engaging with true uncertainty is the source and justification for entrepreneurial profits.</i> <ul style="list-style-type: none"> "The entrepreneur is the owner of all real wealth, and ownership involves risk; the coordinator 'makes decisions,' but it is the entrepreneur who 'accepts the consequences of decisions.'" (Id. at 45) <i>SR: See also, N. Taleb, Skin in the Game</i> On Induction and Deduction. <i>It is a mistake to treat induction and deduction as exclusive methods. Rather, both are insufficient and yet, both are required. Over-indexing to induction favors concreteness at the exclusion of principled reasoning. Over-indexing to deduction favors generalization at the expense of supportive evidence. Perhaps, one must realize the interaction between inductive and deductive lenses is endless & paradoxically stable only in its instability.</i> <ul style="list-style-type: none"> "The relations between deduction and induction are intimate, and a rigid separation or contrast between the two methods is misleading." (Id. at 7, fn. 1) On Analogy. <i>Analogy is the animating force behind reasoning. The imprecision of analogy means that cold machine-like certainty is a ruse. At the same time, the imprecision is what allows for possibility, serendipity, and tail events (positive & negative).</i> <ul style="list-style-type: none"> "Remembering that we are speaking of the surface facts, not metaphysical interpretations, we may say that all reasoning rests on the principle of analogy." (Id. at 201) "We perceive the world before we react to it, and we react not to what we perceive, but always to what we infer." (Id. at 201) On Soul in the Game vs. Mere Venturer, Interloper, Casual Observer. <ul style="list-style-type: none"> "[T]he specialist in any line of risk-taking naturally knows more about the problem with which he deals than would a venturer who dealt with them only occasionally. Hence, since most of these uncertainties relate chiefly to the exercise of judgment, the uncertainty itself is reduced by this fact also." (258)
Resources	
<ul style="list-style-type: none"> n/a 	
Backlinks [internal]	
#cryptonotebook #risk #uncertainty	<ul style="list-style-type: none"> On Life. <i>Despite the desire to reduce uncertainty, the irony is that our life would be far less appealing without it.</i> <i>SR: Query how to strike the balance. In markets, my working hypothesis (inductively & deductively generated) is that there are essentially 3 choices: (a) opt-out of the market regime on grounds that it is too uncertain, (b) engage and delude yourself self-righteously to finding the "holy grail" or "Rosetta stone," or (c) engage and in a Wu Wei like fashion, redirect the uncertainty through humble heuristics and non-concentrated position sizing, combined with putting both skin and soul in the game.</i>

Main Ideas

- Problem: payment of transaction fees in native LI currency increases onboarding friction, particularly for new users.
- Example: to interact with a dApp on Ethereum, user must be qualified on an exchange, convert fiat into ETH, and maintain funds in the wallet to cover gas fee / transaction cost, which amount varies based on network congestion.
- Solution: metatransaction, which is broadly defined as an abstraction layer involving a relayer / intervening code that interacts with the underlying blockchain and pays the transaction fee on behalf of the user such that the user can interface with a dApp without needing to hold the native LI currency.

SR Synthesis

- ✓ Relayers are businesses that earn fees from the dApp for providing a more seamless U/X for the dApp user. Instead of users paying the transaction fees (e.g., gas on the Ethereum network), the dApp effectively covers the payment and, via certain metatransaction schemes, can do so without any reference or need for the native LI currency.
- ✓ Establishing these relayer nodes may be a useful value-add service provided by investors (venture or otherwise) for early stage dApps.

Resources

- GSN

Backlinks [internal]

#cryptonotebook
#metatransaction
#relayer

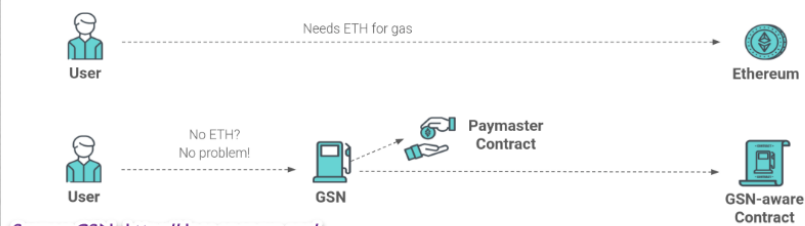
Details

- On the problem of native currency transaction fees: "[T]ransaction fees are typically exclusively paid in the native platform currency. This restriction causes a wide range of challenges, such as deteriorated user experience, mandatory rent payments by decentralized applications, and blockchain community rivals (e.g., coinism)." (Seres at 178)
 - Deteriorated U/X. User that wants to perform a transaction on a decentralized application must still use the underlying LI currency. "This results in additional usability frictions and UI complexities, which could be avoided if transaction fees could be paid directly via another currency." (Seres at 178)
 - Mandatory Rent. That a user of dApp must still own native currency implicitly pays rent to the ecosystem.

SR: Away from ideology, is this really a problem? Is not the economic rent justified? Rather, the chief concern appears to be the poor U/X that results from requiring transaction fees to be paid in native currency.
 - Social Coinism. Requiring native currency transaction fee emboldens tribalism as relates to coins.

SR: Social coinism seems to be present regardless of the fact that transactions are settled in native currencies.
- The U/X solution as understood by GSN on Ethereum network is that users—esp. new users—can interact with dApps without needing native ETH to pay gas / transaction fee. This boosts user onboarding, reducing U/X friction for dApps.
- "Without GSN, anyone who sends an Ethereum transaction needs to have ETH to pay for gas fees. This forces new users to pass KYC and purchase ETH before they can start using any dApp. This can be a major hurdle for users without prior crypto experience that are unfamiliar with the concept of needing to keep ETH in their wallet for gas. This is also a UX pain for existing users that need to continually replenish their ETH balance to pay for gas fees even if they have tokens worth thousands of dollars in their wallet." (GSN)

Ethereum Gas Station Network (GSN)



- Solution may lie in metatransactions, which are "transactions that pay fees to miners or other intermediaries in a currency other than the [native currency]." (Seres at 179). This is achieved using relayers that perform the conversion between the native currency and the non-native currency. (Seres at 180).

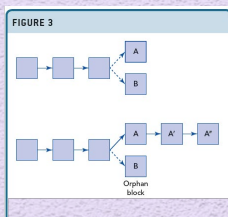
SR: Relayers are businesses that earn fees from the dApp for providing a more seamless U/X for the dApp user. Instead of users paying the transaction fees (e.g., gas on the Ethereum network), the dApp effectively covers the payment and, via certain metatransaction schemes, can do so without any reference or need for the native LI currency.
- On balkanization of Layer 1s: "[I]n the context of blockchains, financial incentives exacerbate competition. We count historically about 900 Linux distributions within the last 28 years, and the last 10 years have brought to fruition circa 900 blockchain coins and about 1400 blockchain tokens deployed on existing blockchains." (Seres at 178)

Main Ideas	Details
<ul style="list-style-type: none"> Two types of smart contracts: code-only and ancillary Genealogy of smart contracts: Szabo (1996), Grigg & Howland (1996) via Ricardian Contracts Challenges to widespread adoption of smart contracts will have less to do with legal validity and more to do with how parties transact business Specific issues facing smart contract mass adoption: (1) third party interpreter needed, (2) oracle problem, (3) code risk, (4) lack of flexibility due to auto-execution (automation as both feature and bug) 	<ul style="list-style-type: none"> Definition. Smart contracts "describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform....[T]he code can either be the sole manifestation of the agreement between the parties or <u>might complement a traditional text-based contract and execute certain provisions</u>, such as transferring funds from Party A to Party B." (Id. at 1) Gas Gateway. Prior to compiled smart contract executing on chain, transaction fee is required (e.g., gas on Ethereum), which "acts as an important gate to prevent overly complex or numerous smart contracts from overwhelming the EVM [Ethereum Virtual Machine]." (Id. at 2.) General Use Case Category: <u>procure-to-pay</u>. "When a product arrives and is scanned at a warehouse, a smart contract could immediately trigger requests for the required approvals and, once obtained, immediately transfer funds from the buyer to the seller." This solves "dunning." <i>SR: Dunning = persistent requests for satisfaction of payment or debt. Another category use case is <u>parametric insurance</u>, which is not functionally dissimilar to CDS. Current contemplations of use case obviously tilt toward finance by way of (and limitation of) analogy.</i> <u>Genealogy of Smart Contracts</u>. <ul style="list-style-type: none"> Nick Szabo in "Smart Contracts: Building Blocks for Digital Market" (1996), avail. online. "I call these new contracts "smart," because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises." Ian Grigg & Gary Howland in "The <u>Ricardian Contract</u>," describing a bond trading system. <i>SR: Understanding the history of smart contract will be useful in contextualizing how they are used today.</i> <u>Two classes of smart contracts</u>: (a) "<u>code-only</u>" contracts that have no textual reference and (b) "<u>ancillary</u>" smart contracts that effectuate particular provision(s) of a broader text-based agreement. Code-only contracts ought to be enforceable under existing contract common and statutory laws: "[T]he fact that an agreement is rendered only in code...presents no particular barrier to contract formation outside the barriers imposed by the UCC and statutes of frauds." (Id. at 4). And, accordingly, <u>legal validity is a matter of state contract law</u>. <u>Widespread Adoption Challenges</u>. "The challenge to widespread smart contract adoption may therefore have less to do with the limits of the law than with potential clashes between how smart contract code operates and how parties transact business." (Id. at 5) <u>Specific challenges</u> to widespread smart contract adoption: <ol style="list-style-type: none"> (1) <u>Trusted third party interpreter</u> required in cases where the contracting parties do not possess the technical skills to properly interpret the code-based agreement; (2) <u>Oracle problem</u>: required entity to push information on-chain from off-chain reality; presents a single point of failure risk; (3) <u>Code risk</u>: multisig security helps alleviate, but see Parity hack whereby hacker reinitialized the smart contract to own the multisig wallet; (4) <u>Automated execution</u> is a feature and a bug; it is a bug in that <u>reversibility is challenging</u>, and self-help remedies are more difficult (e.g., forbearance, re-negotiation); also, <u>intentional ambiguity</u>, whereby issues are kept <u>vague</u> for later resolution is restricted. "[I]t is important not to simply think how existing concepts and structures can be ported over to this new technology. Rather, the <u>true revolution of smart contracts will come from entirely new paradigms that we have not yet envisioned</u>." (Id. at 12)
SR Synthesis	
<p>Basic Smart Contract Negotiation Checklist:</p> <ul style="list-style-type: none"> ✓ Favor "ancillary" smart contract type over strictly code-based variant (e.g., use smart contracts to execute specific provisions of a broader text-based contract) ✓ Clear specification of variables in contract & trigger events ✓ Provision for what happens if there is oracle failure, error, ambiguity, business failure ✓ Define risk allocation in event of coding error ✓ Specify governing law and venue ✓ Specify order of precedence between text and code in event of a text vs. code internal contract conflict ✓ Consider insurance protection 	
Resources	
<ul style="list-style-type: none"> Szabo, "Smart Contracts" (1996) Grigg, "Ricardian Contract" (1996) Parity attack and vulnerability of multisig security See C.Dixon, Skeuomorphism 	
Backlinks [internal]	
<p>#cryptonotebook #smartcontract</p>	

Main Ideas

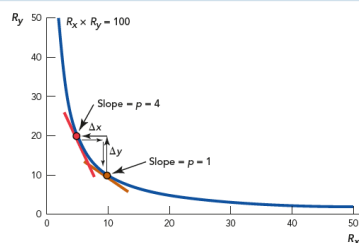
- "DeFi is a field dominated by creative destruction, namely that new products displace older products at a high rate." (Id. at 17).
- Decentralized finance, therefore, could be broader based and more open than traditional finance. Indeed, decentralized finance could prosper in precisely those regions of the world that do not have reliable legal systems or governments with the power to regulate heavily." (Id. at 18)

Figures



A situation in which there are two competing blocks such as A and B in the top panel is soon resolved. The miner who solves the next block must choose whether to build on chain A or B. Suppose they choose A so the new block is A'. Now the chain with A' is the longest chain and further blocks will build on that chain. Block B becomes an orphan block and transactions in that block are treated as invalid.

FIGURE 4



A constant product automated market maker lets traders make any trade along a given curve such as $R_x \times R_y = \$100$. As they do so, the implicit price changes.

Resources

- Follow ups: Oracle Problem, technical details on Bitcoin primitives (cf. Narayanan et. al., [Bitcoin and Cryptocurrency Technologies](#))

Backlinks [internal]

#cryptonotebook
#bitcoin
#defi

Details

- Bitcoin novelty was combinatory. "[P]ublic-private key cryptography, cryptographic hashes, and blockchains preceded bitcoin. But Satoshi Nakamoto... assembled these tools in a new and remarkable way." (pdf pg. 8)
- Bitcoin Block Difficulty. For the Bitcoin blockchain, block discovery rate will be approx. 1 block every 10 mins.
SR: Block size limited to 1MB. Transaction is approx. 500 bytes. Thus, 2,000 transactions (1MB) per block. 10 min block discovery rate. TPS = 3.3 transactions.
- TPS Limitation. Per the calc. above, Bitcoin has a 3.3 TPS vs. 5,000+ TPS via Visa, Mastercard.
SR: Block size limitation of 10 mins per block is by design in order to slow down the rate at which miners can validate transactions. This designed slowness allows the system to adjudicate competing blocks more easily and helps prevent mining concentration / hash power concentration (in theory).
- Longest Chain Norm. "The longest chain norm simply states that miners should build on top of the longest chain (technically the chain that required the most hash power to build but longest is close enough)." (Id. at 10)
SR: See figure 3 in left pane. When two or more blocks are competing for finality, miner that first finds the rare hash decides which chain to append.
- 6 Block Rule of Thumb. Since there are occasionally orphaned blocks on the Bitcoin blockchain, it is advisable to wait 6 blocks deep, especially for large transactions. "A block six or more levels deep is very safe, in essence the data on those blocks is immutable, because the computing power necessary to rewrite six or more blocks is immense." (Id. at 11).
- 100 Block Time to Reward. Miners (in the Bitcoin network) don't receive the block reward until 100 blocks have been validated, incentivizing miners to further adhere to the Longest Chain Norm.
- Energy Cost Issue. At BTC price of \$40k, energy cost for proof of work mining is \$10bn / yr. When compared broadly, this is trivial given \$10bn annual spend on U.S. Halloween costumes. But when compared to traditional payment processors, the energy costs for PoW are very high.
 - Social cost—defined as "the cost to society of making the transaction, which includes the costs of electricity and computers that the miners use"—of Bitcoin is \$130 per transaction vs. 16 cents per transaction for traditional payment processors. (Id. at FN 8).
- Smart Contracts Analogy. "If bitcoin can be thought of as an invisible hand process for transferring money, the new blockchains are invisible hand processes for performing more general forms of computation." (Id. at 14)
- Smart Contract Benefit: borderless (no trade restrictions, tariffs)
- AMMs = smart contract replacement for traditional exchange order books. In constant product AMM contract, price is set based on a curve with arbitrageurs ensuring that AMM price equilibrates to "market" price. (See figure 4 in left pane).
- "DeFi is a field dominated by creative destruction, namely that new products displace older products at a high rate." (Id. at 17).
- Promise of DeFi extends to regions where there are less established norms and legal regimes. "Decentralized finance...relies on smart contracts and cryptographic identification that work exactly the same way everywhere. Decentralized finance, therefore, could be broader based and more open than traditional finance. Indeed, decentralized finance could prosper in precisely those regions of the world that do not have reliable legal systems or governments with the power to regulate heavily." (Id. at 18)
- DeFi is cheaper and can facilitate cross-border microfinance akin to a decentralized Grameen Bank.

Main Ideas

- Decentralization at the internet's data layer reduces cost to produce info networks thereby challenging data monopolies.
- Data monopolies are problematic because they snuff innovation by making it prohibitively expensive for startups to compete with incumbency advantage.

SR Synthesis

- ✓ Decentralization at the data layer of the web enables startups to compete against the hegemony of winner-take-all incumbents from web 2 era (see also Field Note 11: On "Dixon Decentralization")
- ✓ Convexity underlies the choice to bet against the centralized incumbents and in favor of the decentralized edges
- ✓ Closed data business model is zero sum and extracts value from customers
- ✓ Token values user demand and growth; stock values profits
- ✓ Financial incentives & behavioral dynamics endemic to cryptonetworks can combat the incumbency advantage of current big tech

Resources

- n/a

Backlinks [internal]

#cryptonotebook
#cryptoeconomics
#decentralization

Details

- Technology's Deflationary Energy:** "Information technology evolves in multi-decade cycles of expansion, consolidation and decentralization. Periods of expansion follow the introduction of a new open platform that reduces the production costs of technology as it becomes a shared standard." (Id. at 1)
SR: Tech production costs decline, new businesses are built, incumbents get challenged. Decentralized networks and open-source models increase potency of this challenge to entrenched incumbents.
- Countering the Hegemony of Closed-System Incumbency** → "Those who succeed the most and establish successful platforms 'on top' of the open standard later tend to consolidate the industry by leveraging their scale (in assets and distribution) to integrate vertically and expand horizontally at the expense of smaller companies. Competing in this new environment suddenly becomes expensive and startups struggle to create value in the shadow of incumbents, compressing venture returns." (Id. at 2)
 - And again, "[C]ost of innovation for younger companies is increasing as it becomes more expensive for smaller companies to compete and create independent value." (Id. at 3)
 - "The sheer scale in distribution of the incumbents is simply too expensive to overcome without a radical shift in market structure and business models." (Id. at 4)
- The Gambit:** "The way to play a consolidating market is to invest heavily into the consolidating incumbents (which are likely to continue growing strongly for a long period of time) and to invest progressively in the insurgent platforms that will grow to commoditize the incumbent business models and create a new wave of innovation."
- Closed Data Business Model:** "The business model of the web comes down to one thing: amassing large, uniquely valuable data sets and monetizing by charging users directly, placing ads, skimming transaction fees, etc....rely on data being closed and proprietary...by restricting our ability to access information in order to extract profits, web incumbents prevent us from accessing the enormous potential of truly open data." (Id. at 4)
- Cryptonetwork Defined:** "decentralized information networks coordinated via a scarce, programmable digital token (or cryptoasset) whose supply is programmed and enforced by a blockchain or similar consensus network." (Id. at 4)
- Arrow of Progress:** "[C]rypto collapses the cost of building and scaling information networks by replacing centralized coordination with universal financial incentives." (Id. at 5)
- Potentiality:** Cryptoeconomics is a "high-leverage business model which provides the potential to reach unprecedented levels of scale at near-zero capex for the innovators." (Id. at 5)
- Token vs. Equity Philosophy:** "[T]he price of Twitter's stock only reflects Twitter Inc's ability to monetize the data—and not the actual worth of the service. Tokens solve this inefficiency by deriving financial value directly from user demand as opposed to 'taxing' by extracting profits." (Id. at 5)
- The Thesis Restated:** "Our thesis is that decentralization and standardization at the data layer of the internet is collapsing the production costs of information networks, eliminating data monopolies and creating a new wave of innovation. Cryptonetworks accomplish this by replacing expensive, centralized coordination (e.g., PayPal) with universal financial incentives (e.g., Bitcoin). These networks introduce a new, natively digital asset class which shifts value away from equity in companies to tokens in decentralized networks." (Id. at 6)
- "Cryptocommodities" to describe infrastructure tools (storage, compute, etc.)

Main Ideas	Details
<ul style="list-style-type: none"> Internet Era 1 (1980s-2000s): open protocols controlled by community Internet Era 2 (mid-2000s-present): centralized platforms win, accelerated by mobile Internet Era 3 (now-future): decentralized cryptonetworks Centralization snuffs innovation and creates zero sum game with customers 2 stage p/m fit paradigm: (a) p/m fit between platform and devs & entrepreneurs; (b) p/m fit between platform and end users 	<ul style="list-style-type: none"> <u>Internet Era 1 (1980s-2000s)</u>: open protocols controlled by community. <ul style="list-style-type: none"> "This meant that people or organizations could grow their internet presence knowing the rules of the game wouldn't change later on." Companies born (but not grown) during Era 1: Yahoo, Google, Amazon, Facebook, LinkedIn, YouTube against the backdrop of a diminishing AOL <u>Internet Era 2 (mid-2000s-present)</u>: centralized platforms win, accelerated by mobile. <ul style="list-style-type: none"> "The explosive growth of smartphones accelerated this trend as mobile apps became the majority of internet use. Eventually users migrated from open services to these more sophisticated, centralized services. Even when users still accessed open protocols like the web, they would typically do so mediated by GAFA [Google, Apple, Facebook, Amazon] software and services." GAFA, born in Era 1, grew to dominate in Era 2 Benefit of Era 2 was increased access to internet around the globe. The negative consequence was the centralization of power. "[I]t became much harder for startups, creators, and other groups to grow their internet presence without worrying about centralized platforms changing the rules on them, taking away their audiences and profits." <u>Internet Era 3 (now-future)</u>: so-called web 3, or the rise of increasingly decentralized architecture whereby "[c]ryptonetworks combine the best features of the first two internet eras: community-governed, decentralized networks with capabilities that will eventually exceed those of the most advanced centralized services." "Software is simply the encoding of human thought, and as such has an almost unbounded design space." <p><i>SR: This lightweight modality means that regulation is extremely difficult; like water, software finds a way around</i></p> Decentralization is not really about resistance to centralized authority, the common Libertarian or quasi-Libertarian argument. Instead, decentralization is important to counter the innovation-snuffing force of incumbency that develops a zero-sum relationship with its customers through data extraction, privacy affronts, and generally increased vulnerabilities. Cryptonetwork Definition: "networks built on top of the internet that 1) use consensus mechanisms such as blockchains to maintain and update state, 2) use cryptocurrencies (coins/tokens) to incentivize consensus participants (miners/validators) and other network participants." Cryptoeconomic design features that help counter the zero-sum nature of incumbent centralized "web 2" platforms from the mid-2000s: (a) <u>open-source code</u> visible to all (or, at minimum, more than in centralized platforms); (b) <u>participant voice</u> via governance on-chain and social discourse off-chain; and (c) <u>exit rights</u> via option to leave the network at individual level or fork at community level. <u>Limitations</u> of cryptonetworks: performance + scalability + U/X <u>Decentralization can innovate more quickly</u>: see, e.g., battle between Wikipedia and Encarta; the latter was a better product initially, but the former iterated more quickly due to active community in tune with the more decentralized ethic <p><i>SR: Community-based iteration is turbocharged with economic incentives / token design that accelerates the iteration rate</i></p> "The lesson is that when you compare centralized and decentralized systems, you need to consider them dynamically, as processes, instead of statically, as rigid products." <u>Two-stage product market fit</u>: (a) p/m fit between platform & devs; (b) p/m fit between platform and end users. <ul style="list-style-type: none"> "This two-stage process is what causes many people—including sophisticated technologists—to consistently underestimate the potential of decentralized platforms."
SR Synthesis	
<ul style="list-style-type: none"> ✓ Centralized internet platforms are forced to move from a positive sum relationship with customers to a zero sum relationship in the name of further growth later in the S-curve ✓ Centralized internet platform stifle entrepreneurial spirit, tinkering, experimentation, and innovative risk-taking due to the winner-take-all dynamics ✓ Even though these winner-take-all dynamics (as part of network effects) are visible in decentralized systems (e.g., ETH), the moats are not as wide; and, community-participation both on-chain via governance and off-chain via social discourse makes those network effects less monolithic 	
Resources	
<ul style="list-style-type: none"> Quantity and quality of devs on platform as fundamental signal; can we tease this out and then test this rigorously? 	
Backlinks [internal]	
#cryptonotebook #decentralization	

Main Ideas	Details
<ul style="list-style-type: none"> Amara's Law: cognitive biases (viz. hyperbolic discounting) cause us to overestimate tech's effect in ST & underestimate it in LT Promethean (hacking, pragmatics, tinkering) > pastoral (credentialism) mindset Rough Consensus in software dev: seek razor sharp clarity in immediate next steps & embrace ambiguity in LT outcomes; this posture counteracts Amara's Law since focus on next steps hedges tendency to overestimate short term & ambiguity in vision keeps leveraged serendipity open ended 	<ul style="list-style-type: none"> "People change, then forget that they changed, and act as though they always behaved a certain way and could never change again." (Marc Andreessen in Introduction, p. 25) "While it might seem like software is constantly in the news, <u>what we have already seen is dwarfed by what still remains unseen.</u>" (Id. at 106) And furthermore, "[t]hose who have correctly calibrated the impact of software are winning. Those who have miscalibrated it are losing." (Id. at 107) <i>SR: This is the thesis for crypto, blockchain, and exponential technology (with corresponding narratives surrounding and enabling them)</i> <u>Amara's Law</u>: "We tend to overestimate the effect of technology in the short run and underestimate the effect in the long run" (Id. at 135) <i>SR: Logic underpinning Amara's Law → tech change is exponential, which the human brain cannot properly conceptualize; hyperbolic discounting is cognitive bias that affects human time preferences</i> On the Pastoral vs. Promethean Mindset: "Those with a Promethean mindset and an aggressive approach to pursuing a new path can break out of the <u>credentialist life script</u> at any age. Those who are unwilling or unable to do so are holding on to it more tenaciously than ever. Young or old, those who are unable to adopt the Promethean mindset end up defaulting to what we call a pastoral mindset: one marked by yearning for lost or unattained utopias. Today, many still yearn for an updated version of romanticized 1950s American middle-class life for instance, featuring flying cars and jetpacks." (Id. at 2017) <i>SR: Many peers in trad'l finance are unwittingly adopting pastoral mindset as relates to a direct confrontation with crypto beyond the headlines, wishing it goes away</i> "The bigger risk is getting attached to a particular what and when, a specific vision of a paradise to be sought, preserved or reclaimed. This is often a <u>serious philosophical error</u>—to which pastoralist mindsets are particularly prone—that <u>seeks to limit the future.</u>" (Id. at 257) <i>SR: Pastoral mind is attached to particular outcomes, short-circuiting the exponentiality of tech. This is why value investors are ill-equipped to tarry with blockchain and crypto. The attachment to particular end state / utopia is also the error "bitcoiners" or any maximalists make.</i> <u>Credentialism Bias vs. Hacker Ethos</u>: "[A]lmost all effective responses to the problems and opportunities of the coming decades will emerge out of the hacker ethos, despite its apparent peripheral role today. The credentialist ethos of extensive planning and scripting towards deterministic futures will play a minor supporting role at best." (Id. at 262) <u>On Tinkering</u>: "[T]inkering is focused on steady progress rather than optimal end-states that realize a totalizing vision. It is usually driven by individual interests and not obsessively concerned with grand and paternalistic "best for all" objectives. The result is that purist visions seem more comforting and aesthetically appealing on the outside, while pragmatic hacking looks messy and unfocused. At the same time, purist visions are much less open to new possibilities and bricolage, while pragmatic hacking is highly open to both." (Id. at 487) <i>SR: See also Taleb on tinkering.</i> Donald Knuth, software pioneer: "Premature optimization is the root of all evil" On "Rough Consensus": "Traditional processes of consensus-seeking drive towards clarity in long-term visions but are usually fuzzy on immediate next steps. By contrast, rough consensus in software deliberately seeks ambiguity in the long-term outcomes and extreme clarity in immediate next steps.... <u>Clarity in next steps counteracts the tendency to overestimate what is possible in the short-term, while comfort with ambiguity in visions counteracts the tendency to underestimate what is possible in the long-term.</u>" (Id. at 534, 536)
Overflow	
<ul style="list-style-type: none"> ✓ "The most interesting place to be is usually at the very edge, rather than the innermost sanctums" (Id. at 1647) ✓ "Tinkering is a process of serendipity-seeking that does not just tolerate uncertainty and ambiguity, it requires it. When conditions for it are right, the result is a snowballing effect where pleasant surprises lead to more pleasant surprises." (Id. at 1448) ✓ Convexity: "Since the process begins with low-stakes experimentation, the cost of failures is naturally bounded. The upside, however, is unbounded: there is no necessary limit to what unexpected leveraged uses you might discover for new capabilities." (Id. at 1440) ✓ Work: "Any sufficiently advanced kind of work is indistinguishable from play" (Id. at 1682) 	
Resources	
<ul style="list-style-type: none"> Cheat Richards, <u>Certain to Win</u> (application of maneuver warfare concepts for business environments) James Carse, <u>Finite and Infinite Games</u> (on the pragmatic vs. purist approach) 	
Backlinks [internal]	
<p>#cryptonotebook</p> <p>#software</p>	<p>Prepared by Sandeep Ramesh strictly for educational (neither investment nor business) purposes.</p>

Main Ideas

- "Cryptoeconomics brings the invisible hand to computation"
- Blockchains are based on cryptographic primitives that originate ~400 BCE
- Two-way, non-reversible functions facilitate secure communication over insecure network
- Public-private key pair allow for digital signatures, NFTs, Tokens

SR Synthesis

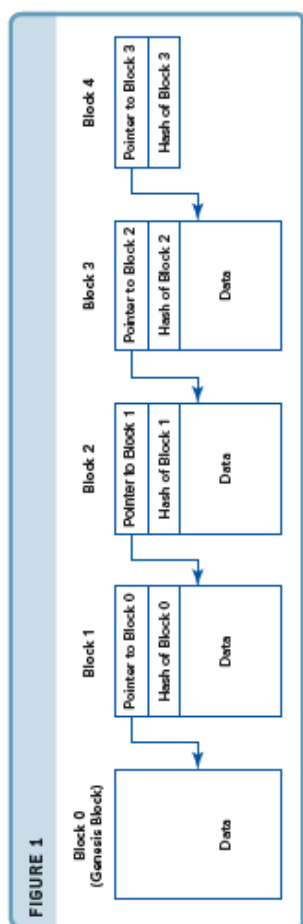


FIGURE 1

Resources

- xxxx

Backlinks [internal]

#cryptonotebook
#cryptography
#cryptoeconomics

Details

- "Cryptoeconomics brings the invisible hand to computation." (pdf. p. 1)
SR: That is, decentralized consensus
- Cryptographic history dates back over 2,000 yrs to Kama Sutra (~400 BCE), advising using secret language to communicate between lovers.
- Ordinary transposition cypher: code that can be broken by analysis such as transposing or displacing letters to encrypt a message.
- One-time pad cypher: randomized, so cannot be broken via analysis
- Cryptographic problem with transposition cyphers was how to share the decryption key *in secret*. Answer: two-way function or the Diffie-Hellman nonreversible function; 1976, Whitfield Diffie & Martin Hellman developed cryptography for secure communication of a secret key over an insecure network.
- "[C]ommercial internet as we know it would not be possible without cryptography." (Id. at 2)
- Rivest, Shamir, Adelman showed that you can have a different keys for the encrypt and decrypt functions, which sets the stage for public and private key pairs. Public key used to encrypt and send a message, while the private key is used to decrypt.
- Advantages of public-private key system: (1) you only need to create the key pair once; (2) system works in reverse; that is, you can use a private key to encrypt a message and decode it with a public key (useful for attestation, to publicly prove that someone did something or is someone).
- Digital signature: a message that can only be decrypted using a public key.
- To prevent someone from copying the digital signature, you use a unique digital signature for each message by binding the signature to a cryptographic hash, which is akin to a "digital fingerprint, a much shorter message that in practice can be uniquely associated with any message." (Id. at 3)
- The output of the cryptographic hash algorithm—commonly, SHA 256, which hashes an asset into 1s and 0s, creating 2^{256} possible hashes, which is pragmatically random.
SR: the SHA 256 output is further truncated via hexadecimal format
- "[D]igital signatures offer three key properties: authenticity, message integrity, and nonrepudiation."
 - Authenticity: digital signature strongly attests to the identity associated with a public key
 - Message integrity: compare the hash within the signature with the hash of the message
 - Nonrepudiation: only the private key holder can digitally sign (decrypted with the public key), so he/she cannot disavow the signature.
- NFT: "just a cryptographic hash of an artwork (or other digital file) signed with a digital signature" (Id. at 5)
- NFT is not an odd phenomenon, as there is clear analog with collectibles; NFT prices are debatable, but not the existence of NFTs as such.
- Token: message + digital signature
- Public, distributed blockchain de-centralizes, de-localizes trust
- "[I]f the hash of the most recent block matches the hash listed then we can be quite confident that *none* of the previous blocks have been tampered with." (Id. at 8). In order to change a single piece of data on-chain, every subsequent block would also need to be changed. Thus, blockchain is "highly immutable—changing any element in any block requires making changes to every subsequent block and that is much more difficult than changing one element of a block. Blockchains, therefore, greatly increase the security of databases and the more blocks subsequent to a given block, the greater the security." (Id. at 8).

Main Ideas

- For a permissionless blockchain to be fully decentralized, there must be sufficient number of independent participants at the consensus layer & equal resource power distribution among them.

SR Synthesis

- ✓ There are two required conditions for full decentralization: (1) sufficient number of independent consensus participants in the system and (2) equal resource power distribution among them.
- ✓ We can tag these conditions as (1) the numerosity condition and (2) the resource distribution condition.
- ✓ For there to be equal resource distribution, there must be Sybil costs, which exists when it becomes more costly for a party to run multiple nodes on a blockchain vs. a single node. Absence of Sybil costs removes a cost deterrent in the system, allowing for resources to be gathered by fewer parties with pre-existing means to aggregate resources.
- ✓ The only way to ensure Sybil cost in a permissionless system is ironically through a trusted third party that can verify *real world* identities (not simply wallet addresses, as multiple unique addresses may be controlled by a single entity), making full decentralization a practical impossibility.

Resources

- jian.liu@eecs.berkeley.edu;
- dawnsong@cs.berkeley.edu
- Follow up on: DPoS, Selfish Mining Attacks (33% attack)

Backlinks [internal]

#cryptonotebook
#decentralization

Details

- Def'n: "Blockchain is a public ledger that stores transaction history, while nodes record the history on the blockchain by generating blocks through a consensus protocol that provides a synchronized view among nodes." (pdf. 1)
- "As a result, the decentralization of the Bitcoin system has become poor, thus deviating from its original goal." (Id. at 1)
SR: Computational power in POW systems—viz. Bitcoin blockchain—concentrated in mining pools, betraying a decentralized ethos.
- Tokens suffer from 2 main problems that undermine level of decentralization: "1) an insufficient number of independent participants because of the coalition of participants (e.g., mining pools) and 2) a significantly biased power distribution among them." (Id. at 2)
- Sybil Cost: condition exists when cost to run n nodes is greater than the cost to run a single node.
SR: The existence of Sybil cost in a system ensures that consensus enablers are economically incentivized to run a single node, which increases decentralization by preventing power concentration
- Conclusion of paper: "PoW and PoS systems do not have both enough participants running nodes and an even power distribution among the participants. However, unlike PoW and PoS coins, DPoS [delegated proof of stake] coins can have an even power distribution among a fixed number of participants when Sybil costs exist. If the Sybil costs do not exist, however, rational participants would run multiple nodes for higher profits. In that case, DPoS systems cannot guarantee that any participants possess the same power." (Id. at 2)
SR: Authors further posit that there is not yet a way for Sybil cost to exist in blockchain systems because the only current way to ensure that power is distributed among the participants is via a trusted third party identity management system that can verify only one node is run per real world identity.
- Resource distribution is a proxy for degree of decentralization: "[T]he more resources a participant has, the greater their influence on the system. Therefore, the resource power distribution implicitly represents the level of decentralization in the system." (Id. at 2)
- "The level of decentralization largely depends on two elements: the number of players running nodes in a consensus protocol and the distribution of effective power among the players. In this paper, full decentralization refers to the case where a system satisfies that 1) the number of players running nodes is as large as possible and 2) the distribution of effective power among the players is even. Therefore, if a system does not satisfy one of these requirements, it cannot become fully decentralized." (Id. at 4)
- Condition 2 Elaboration: "[I]t should not be more profitable for too many players to combine into a few nodes than it is when they run their nodes directly. If delegating is more profitable than not delegating, many players with resource power would delegate their power to a few players." (Id. at 5)
SR: Implication is that the only way to achieve even distribution of power is when each player only has one and only one node.
- Sybil Cost Elaboration: "Sybil cost represents the additional costs for a player running multiple nodes when compared to the total cost for multiple players each running one node. In order for a system to implement the Sybil cost, we can easily consider real identity management where a trusted third party (TTP) manages the *real identities* of players. When real identity management exists, it is certainly possible to implement a Sybil cost. However, the existence of a TTP contradicts the concept of decentralization, and thus, we cannot adopt such identity management for good decentralization." (Id. at 6)
- "[A]chievement of good decentralization in the consensus protocol and non-reliance on a TTP contradict each other." (Id. at 13)

Main Points & SR Synthesis

- Algorithmic mediation of consensus
- Disruptive promise of blockchain technology is to expand concept of value beyond economic terms
- Blockchain use case is the enablement of token itself & perhaps this is sufficient justification for the tech contra common critiques re: use cases
- Morphological framework categorized by Tech, Behavior, Coordination

Essential Diagram

COORDINATION

Underlying Value	Supply Strategy	Incentive Enablers	Incentive Drivers
Asset-based	Schedule-based	Right to work	Get access (to content/service)
Network Value	Pre-mined scheduled distribution	Right to use	Get discount
Share-like	Pre-mined one-off distribution	Right to vote	Get revenue (increase existing business)
	Discretionary	Unit of account	Get reward (new economy creation)
	Matching demand	Medium of exchange	Dividend/Earning Potential (for holding or staking)
		Store of value	Appreciation potential (Speculation)
			Participate in governance
			Gain reputation

Fig. 6, Id. at 9

Details

- Blockchain utility is premised upon the “possibility to reach a shared consensus on a univocal truth describing the history of states of a digital ecosystem, in the form of a ledger of transactions.” (Id. at 1)
SR: Promise of overcoming centralized low-trust mediators is delivered through algorithm. This is what is meant by the refrain “trust code” and should be taken as a worthy yet Messianic promise.
- “The disruptive potential lays in expanding the concept of value that can be partitioned and traded beyond purely economic terms to include, for example, reputation, work, copyright, utility, and voting rights. Once tokenized, all these manifestations of value can be detected, accounted for, and leveraged in the context of a system of incentives and fair wealth and power redistribution.” (Id. at 2)

SR: On this view, token is the focus, not blockchain as such. The latter enables the former, where the transformative potential exists.

Stated further, “tokenization represents a form of digitalization of value, and just like the Internet enabled the free and fast circulation of digitized information, so the blockchain is allowing the ‘almost free’ and borderless flow of digitized value.”

(Id. at 2)

- Digital scarcity enables “new digital economy relying on assets that are liquid, divisible, borderless (easily transportable and quickly transferable), and, unlike currencies, have the potential to appreciate over time.” (Id. at 2)
- Token description: “a unit of value that an organization creates to self-govern its business model, and empower its users to interact with its products while facilitating the distribution and sharing of rewards and benefits to all its stakeholders.” (Id. at 2)
- Analytical framework needed to accommodate the heterogeneity of token types and functions. “General Morphological Analysis” is a methodology used “to describe and assess problem complexes, characterized by non-quantifiable and multi-dimensional properties, by mapping all possible relationships, or configurations, occurring in the given problem complex” with the goal of “identifying recurring patterns and building non-quantified inference models.” (Id. at 4).

TECHNOLOGY

Chain	Permission	Number of Blockchains	Representation Type
New Chain, new code	Permissioned	Single Chain	Common
New Chain, forked code	Permissionless	Cross Chain	Unique
Forked Chain, forked Code			
Issued on top of a protocol			

Fig. 4, Id. at 7

BEHAVIOR

Burnability	Expirability	Spendability	Fungibility	Divisibility	Tradability
Burnable	Expirable	Spendable	Fungible	Fractional	Tradable
Non-Burnable	Non-Expirable	Non-Spendable	Non-Fungible	Whole	Non-Tradable
			Hybrid	Singleton	Delegable

Fig. 5, Id. at 8

Backlinks [internal]

#cryptonotebook
#cryptoframework
#tokenomics

*****Protocol/Company/Organization Sources*****

- ☐ [] Whitepaper
- ☐ [] Github, Code Audits
- ☐ [] Official Blog, Newsletter, Socials
- ☐ [] Official Comms. (Telegram, Discord, Signal)
- ☐ [] Events: Developer Days, AMAs, Conference Transcripts, "Earnings" Transcripts

*****3rd Party Research akin to Traditional Equity Research*****

- ☐ [] BAML
- ☐ [] BTIG
- ☐ [] Cowen
- ☐ [] Messari
- ☐ [] The Block Research

****Crypto-Specific 3rd Party Research Sites****

- ☐ [] BlockScience (<https://medium.com/block-science>)
- ☐ [] Delphi Digital (<https://blog.delphidigital.io/>)
- ☐ [] Diar (<https://diar.com/>)
- ☐ [] Cryp2gem (<https://cryp2gem.medium.com/>)
- ☐ [] Gauntlet Research (<https://gauntlet.network/research>)
- ☐ [] LibreHash (<https://librehash.org/>)
- ☐ [] Into the Block Deep Dive tab (<https://medium.com/intotheblockdeepdive/home>)
- ☐ [] Nonfungible (<https://nonfungible.com/>) (N.B. media focused)
- ☐ [] Santiment (<https://medium.com/santiment>)
- ☐ [] Smith + Crown (<https://smithandcrown.com/research/>) (N.B. research somewhat ballad)
- ☐ [] Woobull (<https://woobull.com/tag/research/>)

*****Crypto Publishing Venture and Hedge Funds*****

Thematic pitches, but because these funds are crypto mainstream and vocal, be careful of chewing too much as it may contribute to groupthink; be wary of "media co monetizing through venture"

- ☐ [] a16z (<https://a16z.com/category/blockchain-cryptocurrencies/>)
- ☐ [] Placeholder VC (<https://www.placeholder.vc/>)
- ☐ [] Outlier Ventures (<https://outlierventures.io/research/>)
- ☐ [] Dragonfly Research (media arm of Dragonfly Capital) (<https://medium.com/dragonfly-research/articles>)
- ☐ [] Pantera Capital (<https://panteracapital.com/insights/>)
- ☐ [] Electric Capital (<https://www.electriccapital.com/resources/>)
- ☐ [] Jump Crypto (<https://jumpcrypto.com/writing/>)

****Crypto Twitter Leechati****

Quite possibly the equivalent of "Street Consensus" but agendas are unclear; handle with extreme caution/skepticism

- ☐ [] Balaji Srinivasan (<https://twitter.com/balajis>)
- ☐ [] Chris Dixon (<https://twitter.com/chrisdixon>)
- ☐ [] Vitalik Buterin (<https://vitalik.ca/>)
- ☐ [] Arthur Hayes (<https://cryptoarturhayes.medium.com/>)
- ☐ [] Nic Carter (https://medium.com/@nic__carter) (media focused)
- ☐ [] Punk 6529 (<https://twitter.com/punk6529>)
- ☐ [] Ben Yu (<https://twitter.com/intenex?lang=en>)
- ☐ [] Ryan Watkins (https://twitter.com/RyanWatkins_)
- ☐ [] Wilson Withiam (<https://twitter.com/WilsonWithiam>)
- ☐ [] Mason Nystrom (<https://twitter.com/masonnystrom>)
- ☐ [] Roberto Talamas (<https://twitter.com/RobertoTalamas>)
- ☐ [] Li Jin on Web3 Creator Economy only (<https://li.substack.com/>) (media focused)

Main Ideas	Details
<ul style="list-style-type: none"> Blockchain innovation centers on the consensus mechanism / protocol So long as that protocol is reputation-based, blockchain is merely incremental advancement of database management field Most profitable use case for blockchain is enabling DAOs 	<ul style="list-style-type: none"> On Ambiguity of Terms & Definitions. “Things are confusing out there in part because <u>not enough care is taken in defining terms before discussing the subject. And when terms are defined, they sometimes include <i>desired outcomes</i> as part of their definition.</u>” (87) <i>SR: The lack of precision and clarity around defining key terms is an acute problem in the popular blockchain & crypto discourse.</i> Ed Corno (IBM) defines blockchain as “shared, replicated, permissioned ledger with consensus, provenance, immutability, and finality.” (87) <i>SR: Interesting to the note that Corno doesn't define blockchain as “permissionless,” but rather a more nuanced permissioned with consensus description.</i> Most of the Corno attributes of blockchain are not novel. <ul style="list-style-type: none"> “Shared, replicated ledgers requiring permissioned access have been around for a long time” and “ [p]rovenance simply means a ledger containing all relevant information, starting from the beginning of any relationship...[and] is nothing new, at least in principle.” (88) Blockchain innovation centers on <u>consensus mechanism / protocol</u> used to achieve consensus. Immutability and finality are desired properties that stem from that mechanism and are not endemic to blockchain as such. (88) Conventional methods to achieve consensus rely upon reputation-based mechanisms. “‘Trust’ in this context means believing that personal and business reputations have too much long-run economic value to be squandered by exploiting an attractive one-time gain.” (88) Corporate version of blockchain is unlikely to stray from the reputation-based <u>consensus</u>. If this is true, “then the efficiency gains of ‘blockchain’ boil down to the gains associated with making databases more synchronized across trading partners, more cryptographically <u>secure</u>, more visible, more complete, etc. In short, there is nothing revolutionary or radical going on here—it’s just the <u>usual advancement of technology</u> and methods associated with the on-going problem of database management. Labeling the endeavor blockchain in this case has <u>more to do with good marketing practices.</u>” (88) <i>SR: See also Ezra Klein, “A Viral Case Against Crypto, Explored” (audio, Apr. 5, 2022) on the claim that blockchain technology hype is fueled by venture capitalist desire to invent a new tech story in order to re-create mega unicorns from prior decade.</i> DBMS = database mgmt systems all specify both read privilege and write privilege Key question is <u>how do we ensure a nefarious actor doesn't misuse the write privilege and put faulty information on-chain?</u> Conventional answer has been to create proprietary databases with restricted read/write privileges managed by trusted parties. This is the client-server / hub-spoke architecture. Game the Write Privilege. Andolfatto suggests that if sufficient reputation-based consensus cannot be met for the particular situation, then a <u>delegation system can work</u> as a middle ground: “The idea is to replicate the trusted historian with a set of delegates drawn from the community (a set potentially consisting of the entire community). Next, have these delegates play a validation/consensus game” to achieve consensus.” (93) Competitive Adv. of Blockchain = DAOs. “The comparative advantages of DAOs are that they permit (i) a higher degree of anonymity, (ii) permissionless access and use, and (iii) commitment to contractual terms (smart contracts).” (94)
SR Synthesis	
<ul style="list-style-type: none"> ✓ “[I]f we're ultimately going to depend on reputation-based consensus mechanisms, then we need no new innovation (like blockchain) to organize a database....standard protocols, for example, in the form of SQL Server 2017, can accommodate what is needed technologically and operationally.” (93) <i>✓ SR: However, reputation is not a binary attribute. There are degrees of reputation & implied trustworthiness.</i> ✓ If Andolfatto's hypothesis that the main competitive advantage of blockchain technology is to enable DAOs, perhaps it follows that any project not explicitly structured as a DAO has a particularly high presumptive bar for defending why the project is a 10x improvement over the status quo and not simply an incremental and typical on-going advancement in the database management field. 	
Resources	
<ul style="list-style-type: none"> n/a 	
Backlinks [internal]	
<p>#cryptonotebook #DAO #usecase</p>	



Sandeep Ramesh • You

Investor. Crypto. (Ex-Tiger Cub, BX, Wachtell, etc. 🐼)

3d •

Field Note 4: On “evolving towards a fundamental investment framework for crypto”

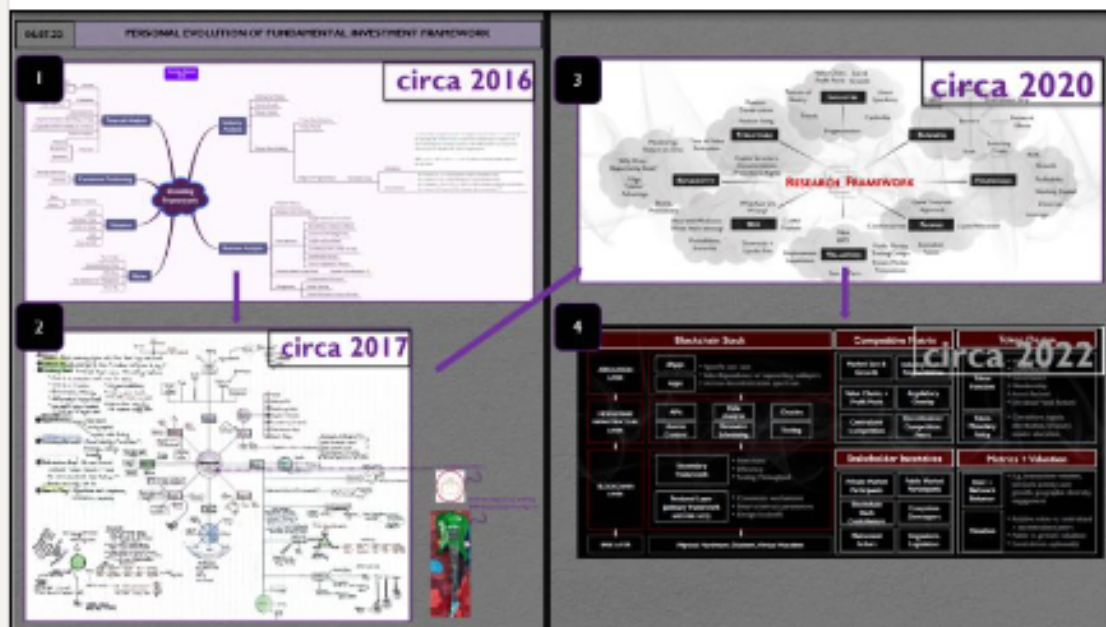
Around 2016 (~8 years after entering the workforce), I began more formally sketching & "mapping" personal fundamental investment frameworks (depicted).

That the map != the terrain does not mean one should walk a terrain without a map. Nor does it mean that one should rip up old maps; topographies can be surprisingly similar.

In crypto investing, a map is more necessary than ever to avoid the piercing problem of info overwhelm, data smog, analysis paralysis, and information fatigue (cf. Field Note 3: On "info smog").

Looking for fellow "crypto cartographers" to iterate and refine fundamentally-oriented crypto investment heuristics, lenses, frameworks, and... maps.

#crypto #cryptoinvesting



Main Ideas

- Information overload, info glut, data smog, analysis paralysis, and information fatigue all describe the condition of knowledge workers
- This article provides a literature review of the "info overload" problem, but lacks specific solutions, which demand personal interventions on knowledge management

SR Synthesis

- ✓ As it relates to crypto specifically, the informational and data smog is particularly thick given (a) the experimental & early-stage nature of the space, (b) low barriers to entry for espousing (any) views, (c) reliance on social media distribution channels that lead to spread irrespective of information authentication or validity, and (d) the cultural brashness of a startup (viz. crypto) mind that overapplies—instead of responsibly uses—the "shoot first, aim later" approach.
- ✓ **Implication: rebuild my "Crypto Information Diet"**

Resources

- Simpson & Prusak, Troubles with Info. Overload: Moving from Quantity to Quality in Info. Provision, Int'l J. of Info. Mgmt. 16(6), pp. 413-25.

Backlinks [internal]

#cryptonotebook
#informationdiet
#informationoverload

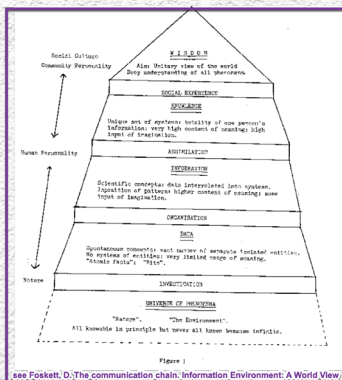
Details

- Problem.** "Living in an 'information society,' we are bombarded with information whether or not we actively seek it. We are all affected by the increasing number of sources from which information emanates." (Id. at 17)
- "[T]he unsolvable problem is that human information processing cannot catch up with the speed of mechanical information production" (Id. at 21)
- Info overload disempowers.** "It is apparent that an abundance of information, instead of better enabling a person to do their job, threatens to engulf and diminish his or her control over the situation.... The problem of information overload is obviously not going to recede and solutions need to be found" (Id. at 18)

SR: Knowledge management and behavioral modifications at the individual level are crucial to address the now systemic information overload, particularly in crypto with low barriers to entry for participation & communication.

- Infoglut, data smog, analysis paralysis, information fatigue

SR: referencing D. Fosskett's pyramid (below), the root of overwhelm appears to stem from the data layer (the discrete bits of information) in crypto given the open APIs and transparent nature of on-chain archiving. From that easily available and "untagged" or "multipurpose" data—combined with the low barrier of entry and exponential distribution of information through social platforms, esp. algorithmic—creates a highly distorted signal:noise ratio.



- The info paradox: too much information but not the right information. "The dilemma is clear: on the one hand, managers receive too much information, while on the other hand, they don't get enough of the right information." (Id. at 22)

SR: especially for a fundamental investment philosophy, the priority is on developing value added information / research. Simpson & Prusak schematic provides a way to map and score the value added elements of pieces of information:

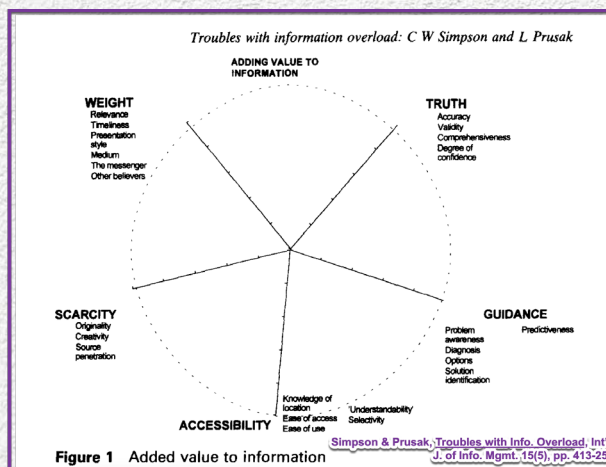


Figure 1 Added value to information

Simpson & Prusak, Troubles with Info. Overload, Int'l J. of Info. Mgmt. 16(6), pp. 413-25.

Main Ideas	Details
<ul style="list-style-type: none"> Anchor framework(s) critical to understanding and assessing digital assets; identifies investment universe Blockchain stack can be abstracted into techno-economic-juridical layers Design of the stack includes off-chain behavior, infrastructure layer, and on-chain subsystems 	<ul style="list-style-type: none"> Purpose: create an <u>anchor framework</u> for understanding and assessing digital assets. Blockchain stack can be separated into layers of (a) <u>technology</u>, (b) <u>economics</u>, and (c) <u>legal rule sets</u>. System design becomes essential to assessment of incentives and interactions of the above layers <p><i>SR: the parameterizations, optimizations, and interactions amongst these layers synthesize into a system. Crypto token is a functional piece of the stack that allows for system coordination. Qualitatively, the better the token coordinates incentives up and down the stack, the more value it holds. Only after understanding system design does it make sense to move into the investment-focused questions (how the token captures value, how much it captures, bounds around what token is worth)</i></p> Cryptoeconomic design stack includes off-chain behavior, infrastructure layer, and on-chain subsystems. Off-chain behavior: “Characterizing the stakeholder and user types that interact with a network can be useful in describing a cryptoeconomic system: <u>design goals for cryptoeconomic systems may involve incentivizing user groups to perform key platform functions, identifying game-able mechanics, informing rewards engine design, and understanding how a token’s suitability for a planned function will be affected by speculator behavior.</u>” (Id. at 12-13) Stakeholder groups (not mutually exclusive): <ul style="list-style-type: none"> Consensus Participants (e.g., Augur reporters, Dash master nodes, BTC block producers, The Graph curators); <u>plus Governance, DAO Treasury</u> <u>Developers</u>: those interacting with network to extend its uses, including dApp builds or side protocols that interact with the network, manufacturing or running hardware (e.g., ASIC builders) <u>Malicious Actors</u>: hackers, price manipulators <u>Capital Providers</u>: investors, speculators in token and venture equity <u>Regulators</u>: policy heads, regulatory personnel at VC funds like friends at Paradigm & Bain Crypto, evangelizing bodies & non-profits (e.g., Graph Foundation, Luna Foundation Guard, Ethereum Foundation, etc.) <u>End Users</u>: those that consume the utility/functionality <p><i>SR: often the most overlooked, yet most central group. People tend not to think of the developers as end users because from “traditional” business lens, the devs are typically siloed inside an org chart buried under business and capital markets functions. This may be one reason why popular views often too heavily critique crypto use cases. Query whether such excessive skeptics are looking for end users in the wrong places (the retail user vs. the developer/user). Hypothesis: second-order question then becomes who is the terminal end user. Skipping the first-order question necessitates as incorrectly pessimistic view & risks missing the investment & value creation potential.</i></p> Digital infrastructure: “Humans typically interact with some form of mediating centralized software that, in turn, enables them to interact with an underlying <u>distributed system</u>. Such infrastructure is <u>rarely open-source</u>, can be first-party or third-party, and is able to handle unexpected changes through frequent upgrades and therefore is not trustless.” (Id. at 13) <p><i>SR: see Schneider, “Decentralization: An Incomplete Ambition,” J. of Cultural Econ. (2019). NTS: further work on Oracles as a concrete way to research the centralization of middleware and its impacts.</i></p> Blockchain: “[R]oot-level distributed database that <u>supports all of the above stack</u>. It is code executed by nodes in a distributed environment.” (Id. at 13). <p><i>SR: Includes core consensus layers, arguably most sidechains (though query if these are better understood as part of middleware/digital infra), L2s, smart contract primitives.</i></p>
<div>SR Synthesis</div> <p>Source: adapted from Fig. 2 (id. at 13)</p>	
<div>Resources</div> <ul style="list-style-type: none"> None 	
<div>Backlinks [internal]</div> <div> #cryptonotebook #cryptoeconomics #cryptoframework </div>	

Main Ideas	Details
<ul style="list-style-type: none"> Event-driven strategy is distinct from more common intrinsic (network) value & technical approaches to crypto 4 event categories: (1) “flow events” (viz. volume); (2) hard forks; (3) BTC-Alt lead/lag cycle; (4) inverse rel’n b/t BBB spreads & BTC (n.b. not event-driven) 	<ul style="list-style-type: none"> Crypto strategies generally fall into two camps: (a) estimating intrinsic value through network-based models (e.g., Metcalfe) and (b) trading on technicals <i>SR: treat systematic approaches separate from conventionally understood “technical” methods given the former’s lower interest in optimizing buy/sell signals in favor of more principled focus on bankroll management / systematic bet sizing (e.g., avoid risk of ruin)</i> Differentiated approach: <u>event-driven crypto</u> lens. Author’s purpose: “This note is intended to offer a new perspective on Bitcoin investing by identifying event-driven strategies to take advantage of crypto-specific short-medium term dislocation in the price discovery process.” (Id. at pdf pg. 1) Event Types <ul style="list-style-type: none"> (a) <u>“Flow Events”</u> – liquidation events, tax season outflows, volume flows, ETFs <ul style="list-style-type: none"> Liquidations: author focuses on ICO-driven time arbitrage whereby investors send ETH to ICO project leaders (→ ETH buy pressure), who eventually sell ETH to convert to native project token and/or fund operations (→ ETH sell pressure). <i>SR: ICO wave is functionally over, so analysis is dated (2018). Also, begs question of where edge is here and why this dynamic would not be priced in unless one has some highly refined timing view for when a major treasury liquidation would occur. However, forced DAO treasury liquidation events might present opportunities for investible edge given idiosyncratic reasons for crypto asset sales, esp. for non-large cap projects (greater inefficiencies, greater arbitrage opportunities).</i> (b) <u>Forks</u> – hard forks, hash power arbitrage <ul style="list-style-type: none"> Hard forks (vs. backward compatible soft forks) ≈ corporate spinoffs; buy the legacy chain on theory that price will deflate as attention overextends to the new chain. <i>SR: case-by-case as the legacy chain may not have community or ideological underpinning like ETC or BCH. Observe the difference in Luna Classic, though not a hard fork (project re-constituting as de novo chain stripped of algo. stable product).</i> Hash power arbitrage: idea that price ratio between legacy chain and current chain should roughly equal their difficulty ratio as miners make hash power allocation decisions based on the relative mining difficulty of the post-forked chains. <i>SR: this idea only applies to proof-of-work mining chains (difficulty adjustment relates specifically to protocols with POW consensus mechanisms); also, need to better understand the theory (are mining incentives strictly economic in fork scenarios?) and practice (are there any technical, hardware, other switching costs in mining legacy chain vs. current chain?)</i> (c) <u>Bitcoin-Altcoin Cycles</u> – BTC price increase precedes Altcoin price increases <i>SR: interesting backdrop, but not useful for my fundamental strategy, as one must still properly select the “alt coins.” Also, crypto ecosystem is more mature than when article was written, so the internal correlation to BTC perhaps not as strong (though still there).</i> (d) <u>Credit Decoupling Events</u> – inverse relationship between corporate BBB spreads and BTC prices <i>SR: not compelling, no edge in meaningfully predicting spreads, not event-driven. The inverse relationship between spreads and BTC likely has to do with liquidity demand as opposed to some unique relationship with crypto.</i>
SR Synthesis	
<ul style="list-style-type: none"> ✓ Event-driven framework <u>doesn’t necessarily obviate need to determine valuation bounds and heuristics</u> (unless there is a merger arb style opportunity where price bounds are pre-determined) ✓ Of the 4 identified event categories in the article, the only ones to further explore are (1) <u>forced treasury liquidations</u> and (2) <u>hard forks or other snapshot splits</u>. ✓ Additional event types / hard catalysts worthy of exploration (<i>inter alia</i>): <ul style="list-style-type: none"> - <u>governance</u> events (not just forks); includes <u>activism / suggestivism</u> campaigns (e.g., Gnosis in 2020, Anchor in 2022) - <u>major funding rounds</u> (primary, secondary sales) - <u>major technical milestones</u> (e.g., ETH merge as highly visible example, but edge in <u>non-large cap</u> likely higher) - <u>regulatory / legal arb</u> ✓ Contra article, <u>event-driven strategy is highly situation-specific; can’t buy a generalized “Greenblatt” basket of forks</u> 	
Resources	
<ul style="list-style-type: none"> Autonomous (research provider) Santiment (on-chain, social info) Snapshot.org (governance, community actions) DeepDAO.io (treasury) 	
Backlinks [internal]	
<p>#eventdriven #investmentstrategy #cryptonotebook</p>	