

get in touch at contact@axiombtc.capital
follow us on twitter @axiombtc

Abstract to Only The Strong Survive

This is intended as a standalone piece that covers the same arguments as <u>Only The Strong Survive</u> as concisely as possible and assumes no prior technical knowledge. We would still recommend anybody interested in this space to take the time to understand the longer paper, but we hope this serves as a helpful introduction.

In our view, the true innovation of Bitcoin is often mischaracterized. Usually, this mischaracterization adopts a digital lens, which leads people to believe "blockchain" is next in a long line of software innovations to emerge from Silicon Valley. We believe Bitcoin is a financial innovation that happens to have digital properties, not a digital innovation that happens to have a financial application. The innovation of Bitcoin can most helpfully be viewed both technically and socially. Technically, the innovation is the proof-of-work consensus mechanism and the difficulty adjustment. Socially, the innovation is an immutable and uncheatable distributed ledger.

Bitcoin is *both* a social and technical innovation and these must be understood in relation to one another. The distributed ledger only works in theory because of strong arguments suggesting legitimate and long-term decentralization and security, and the proof of work consensus mechanism and the difficulty adjustment only work in practice with humans who are incentivized to contribute. What ties this together is *money*. Bitcoin's distributed security is endogenous and depends on its value as money; and its value as money is endogenous and depends on its distributed security.

There are two main problems with *Decentralized Finance* as it exists today beyond Bitcoin: that it is not decentralized and that it is not finance.

That DeFi is not decentralized follows from breaking the link articulated above between the social and technical innovations and the role played by *money* in aligning incentives to achieve these innovations in practice. A token incentivizing use of a non-Bitcoin timechain intended to be something other than money immediately faces three problems: i) it will lose a fight for liquidity with *actual money*, ii) it becomes a poor economic signal for coordinating security provision, and iii) the timechain itself bloats.

Everything Fights for Liquidity: why would a non-monetary token need to have a nonzero holding period and hence a non-negligible value in the first place? In short, why would anybody hold something that is money, but only for X, for any period other than the nanosecond required to transact it? It's analogous to the choice between dollar bills

DISCLAIMER: This document is issued by Axiom Venture Partners Limited ("Axiom"), an appointed representative of Kingsway Capital Partners Limited. Kingsway Capital Partners Limited ("Kingsway") is authorised and regulated by the Financial Conduct Authority in the United Kingdom (the "FCA"). Axiom does not offer investment advice or make any recommendations regarding the suitability of its products. This communication does not constitute an offer to buy or sell shares or interest in any Fund. Nothing in these materials should be construed as a recommendation to invest in a Fund or as legal, regulatory, tax, accounting, investment or other advice. Potential investors in a Fund should seek their own independent financial advice.

Past performance is not necessarily a guide to future performance. Axiom has taken all reasonable care to ensure that the information contained in this document is accurate at the time of publication, however it does not make any guarantee as to the accuracy of the information provided. While many of the thoughts expressed in this document are presented in a factual manner, the discussion reflects only Axiom's beliefs and opinions about the financial markets in which it invests portfolio assets following its investment strategies, and these beliefs and opinions are subject to change at any time.

and casino chips of the same denomination. In crypto, the (non)answer is almost always "yield," to which we will return below in discussing the space's dubious *financial* credentials.

Poor Economic Signal for Coordinating Security Costs: Bitcoin's security is provided by bridging the physical and digital realm by creating an unforgeable digital reflection of the real cost of energy. If you can't rely on endogenous value as money, there will be no sensible basis on which to evaluate the merits of the real cost of security contribution. It can be done if the tokens have value for any other reason, but again we arrive at a serious coordination problem, the resolution of which does not benefit from any inherent economic incentive. The solution to the coordination problem is precariously rooted in the desire for there to be a solution.

Timechain Bloat: If there is enough data in a timechain to capture something other than Bitcoin's bare minimum of "monetary balances" then it is highly likely it will become too large as a data structure to be practically or economically feasible to remain sufficiently decentralized. If it is de facto centralized, it may as well be a cloud application, given that would do away with the economically useless tokens. This de facto centralization has come to the fore many times in the recent past with "founding teams" and "validators" literally halting a network to resolve some perceived issue or threat.

That DeFi is not finance follows from tacit admission of losing the fight for liquidity to *actual money* and cobbling together a value proposition around really being securities. This is to say, the reason you hold a given crypto token rather than buy and sell for the nanosecond required to tap into its "utility" is to receive a "yield".

A *yield* is the generated *flow* above maintenance or depreciation of the carrying capacity of some *stock* of economically productive assets. Less the recouped seeds for the next year's crop, a harvest is a *yield* from a sewn field. Less the financing costs, the interest on a bond is a yield. If the issuing business is solvent and profitable in unit economics-terms and hence the par value of the principal is relatively assured, the market will settle on a value that implies a probability of all the interest being paid as promised. The markets assesses the productive carrying capacity of economic *stock* generating the ability to pay the *flow* of the interest.

So what *yield* is being *farmed* in crypto? There is transparently none. There are flows, but they are not *generated* by economically productive assets over time but rather appear near instantaneously as a result of speculative pricing across non-productive assets. The word "speculative" is not a denigration. There is nothing wrong with speculative value. But there is something bizarre and circular about discrepancies between different speculations on the potential future value *itself* forming the basis of profitable arbitrage that is then mislabeled as "yield".

This mislabeling usually takes some combination of three forms: i) rehypothecation, leverage, and securitization; ii) systemic fragility despite apparent local stability, and iii) misleading metrics purporting to demonstrate both value and health.

Rehypothecation, Leverage, and Securitization: the "new value" created to satisfy "yields" is entirely a combination of manipulating existing value by such means as collateralizing a crypto token to mint a new token, then reusing both as collateral to mint new tokens again. Or, issuing a new crypto token with no explicit collateral but the promise to governance rights and future cash flows over some pool of tokens.

Systemic Fragility: the value of almost every crypto token relies on the value of some other token by which it is collateralized or against which it is securitized. This value is purely speculative and has no link to productive capital or real "yield" and creates the potential for a deleveraging spiral and general collapse of the ecosystem.

Misleading Metrics: the typical metrics used to capture the value and health of the ecosystem take no account of this systemic fragility and report the equivalent of a commercial bank's net assets without accounting for metrics such as leverage ratios or capital risk tiers. If you can endlessly rehypothecate and securitize on purely speculative

value, it should come as no surprise that these kinds of metrics can go up and up and up ... until they suddenly and dramatically collapse.

The "investment" rationale is a category error that arises from misapplying the traditional venture capital methodology in an area similar enough to seem familiar, natural, and possibly even identical, but *just different enough* to be deeply questionable.

Software has a unique economic characteristic of being unboundedly reproducible at near-zero marginal cost. Companies producing and looking to profit from proprietary software are amongst the most inherently operationally leveraged in the history of industrial capitalism. This creates strategic priorities for early-stage software investors that the best venture capitalists figured out a long time ago, and that might look crazy from a traditional capital allocation and business development perspective without having realized these fundamental economic differences.

One can't point to the return on capital implicit in your unit economics and say, "but it's unsustainable to try to grow faster than that!" What's "unsustainable" is losing the race to win the market and going out of business entirely. What's sustainable is to cover operating losses brought about by rapid growth with financing until the market is all but won. It is sensible to treat all of this as, effectively, R&D. Some of it may be actual R&D – i.e. in technology – but in spirit, it is R&D into company design. The company is running profitless experiments aimed at discovering what it ought to one day look like when profitable.

But this does not apply in crypto. Though all of it seems like it applies, if you haven't really thought it through. There is no likely final, profitable, sustainable, yielding state to be aspired to. There is also no realistic prospect of this ever existing.

Many Bitcoin scaling solutions are often lazily described as clunky workarounds to the technical limitations of the Bitcoin timechain. But we vigorously reject this notion on the technical grounds that layered architecture is objectively optimal engineering. Cramming all the features of Lightning, Liquid, DLCs, RGB, and so on, into the mainchain is not only probably technically impossible, but in a more conceptual sense – arguably an *aesthetic sense* – is just an obviously bad idea. It would introduce unknowable attack vectors and hence holistic fragility.

The naïve view is that this compounds the utility of every functionality. The mature view is that it compounds only the vulnerabilities; each functionality is primarily affected to the extent it has become more vulnerable, and utility dramatically decreases, both at the level of individual functionalities and the protocol as a whole. If TCP/IP had been configured to enable video streaming, for example, it would have broken immediately, if it had ever worked at all. This is a feature, not a bug. It reflects the mindset not of a cargo cult bureaucrat, but rather of a prudent and humble engineer, mindful of Gall's Law from John Gall's *Systemantics* – a fitting end to this abstract and prompt towards the full paper, *Only The Strong Survive*:

"A complex system that works is invariably found to have evolved from a simple system that worked. The inverse proposition also appears to be true: A complex system designed from scratch never works and cannot be made to work. You have to start over, beginning with a working simple system."