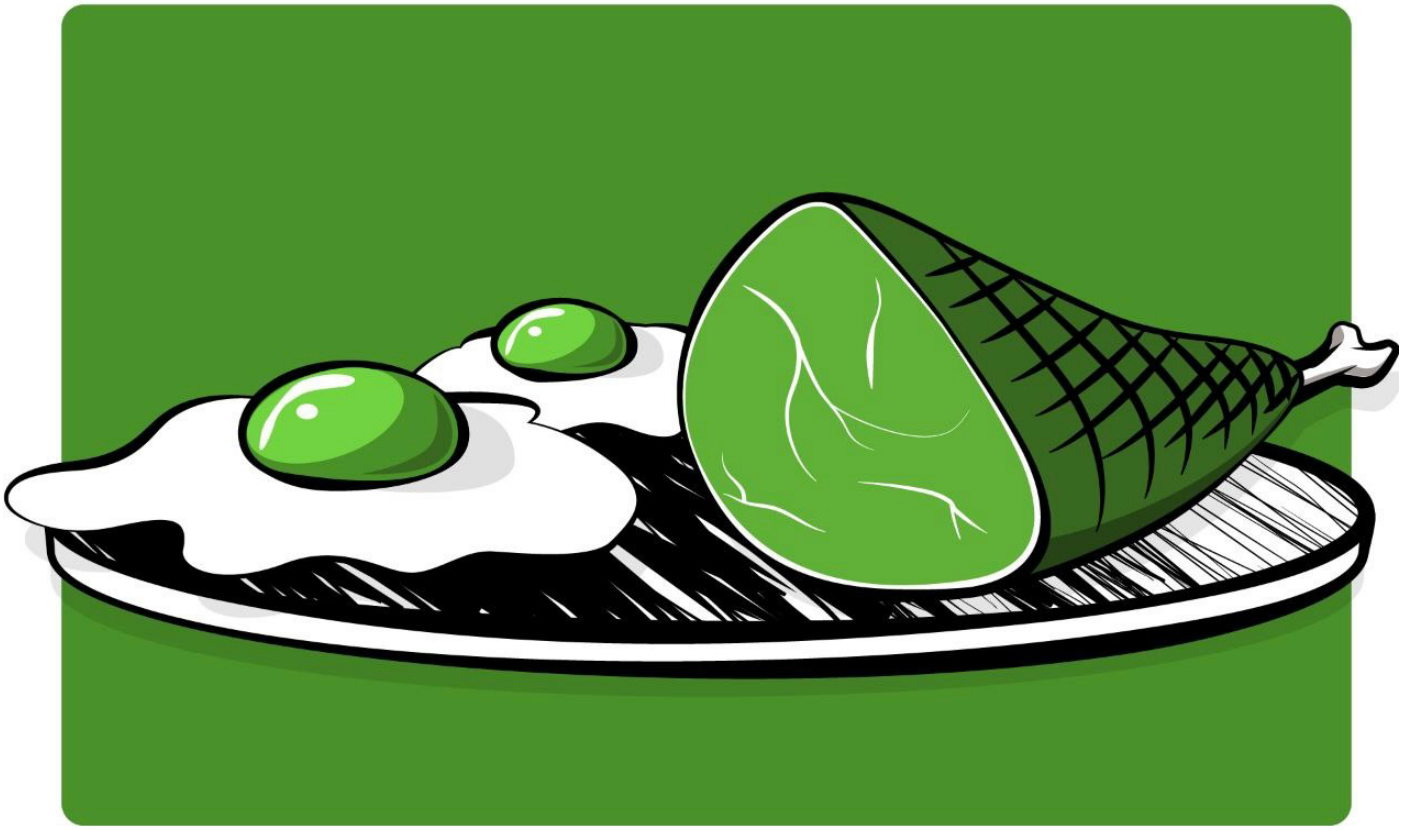
Green Eggs and Ham

Decentralized Finance: The Good, The Bad, And The Ugly

Allen Farrington & Anders Larson



***

*What follows does not represent the views of either author's employer and is **not financial or investment advice**. It is intended as a philosophical, technical, and economic assessment of a novel class of internet protocols. These protocols mostly happen to give rise to natively digital assets, which lend themselves to naturally emerging online and effectively public markets, and which present direct investment opportunities. Nonetheless the following is merely **and only** our opinion of how these technologies are likely to progress. Readers considering investing in any asset discussed herein should **do their own research and should not rely on our work**.*

***

"I'm just here so I don't get fined"

- Marshawn Lynch testifying on behalf of Sam Bankman-Fried

A common refrain in the wake of the collapse of FTX, as with Celsius, BlockFi, and Voyager before it, was that this was *CeFi* not *DeFi* (centralized finance, not decentralized finance) and, if anything, only further demonstrates the need for *DeFi*. Pundits railing against *DeFi* are therefore missing the mark in their overbroad hostility, it has been said. In our previous paper, *Only The Strong Survive*, we made each of the following observations:

1 - our main problem with *DeFi* is that it is not decentralized and it is not finance.
2 - nonetheless, we support the idea of *decentralized finance* in theory, even if *DeFi* isn't it in practice.
3 - we believe a variety of decentralized finance will emerge on bitcoin, and to some extent already has.

In that paper we did not explain what we deemed to be workable decentralized finance in theory, or what constraints might limit how workable decentralized finance might develop. Tying all these threads together is the aim of this paper. We will distinguish between "DeFi" to mean what actually exists in crypto and has done for the past three years or so, and "decentralized finance" to mean an ideal, sensible, workable version.[1]

- In Part I, *Decentralized Finance, Conceptually*, we will investigate the conceptual characteristics a candidate "decentralized finance" would need to have.
- In Part II, *Decentralized Finance, Technically,* we will add some additional technical characteristics and turn these insights into a framework for evaluating workable decentralized finance.
- In Part III, *The Short, Sad Saga of FTX,* we will recap the FTX debacle.
- In Part IV, *Let's Play The Blame Game*, we will apply our framework to FTX and evaluate to what extent it is helpful to blame CeFi, DeFi, and whomever else.
- In Part V, *DeFi's Fatal Conceit*, we argue that, as it stands today, we don't think it is likely that crypto DeFi will become decentralized finance as it is both culturally and technically doubling down in the wrong direction.

PART I: DECENTRALIZED FINANCE, CONCEPTUALLY

"And then this protocol issues a token, we'll call it whatever, 'X token.' And X token promises that anything cool that happens because of this box is going to ultimately be usable by, you know, governance vote of holders of the X tokens. They can vote on what to do with any proceeds or other cool things that happen from this box. And of course, so far, we haven't exactly given a compelling reason for why there ever would be any proceeds from this box, but I don't know, you know, maybe there will be, so that's sort of where you start."

- *Sam Bankman-Fried on boxes*

We will start with the history of development in crypto DeFi to properly frame our analysis. Thereafter, we will set up this analysis by doing our best to define both "decentralized" and "finance," so as not to assume they are well-defined and exhaustive. In Part I, we will focus on conceptual criteria we would expect of "decentralized finance." In Part II, *Decentralized Finance, Technically*, we will address more specific technical criteria.

A brief (and generous) history of crypto DeFi

Crypto DeFi at the time of writing is far more sophisticated and complex than, for example, the majority of the output of the 2017 ICO bubble. Unfortunately, our feeling is that this sophistication and complexity only serves to mask its flaws. Hence the evolution of the state of the art is worth briefly recapping.

The first iteration of token proliferation was not even described as "DeFi" necessarily - a term which came into vogue around 2019. The earlier period was based around ICOs and was focused on a handful of now more or less debunked theses: i) the fat protocol thesis, or what we might call "native tokens": "*I'm launching a blockchain and you can buy premined coins from me*," ii) the utility token thesis: "*I am building a business and you can invest in it by buying a token that rides on a layer-one blockchain*," or, iii) the velocity of money thesis, or MV=PQ: "*my blockchain/application will settle a lot of transactions (stablecoin or otherwise) and the token will appreciate as it will be needed for gas fees*" - either native or utility tokens depending on the exact construction.[2]

---

[1] We are wary that "DeFi," as we define it, has been such a disaster as to irreparably taint the expression "decentralized finance," and that perhaps something like "peer to peer finance" or "open finance" might be better branding at this juncture. The subtlety of the "peer-to-peer" vs "decentralized" distinction in particular is one we will pick up on at various points throughout the paper. Nonetheless, we also feel that sticking with "decentralized finance" better and more unavoidably makes point 1 above: that DeFi is not decentralized and is not finance.

[2] It is worth mentioning some examples of tokens that went to zero while the companies issuing them went on to be very successful or even get acquired. Doc.ai used ICO money to build the company and was then acquired by Sharecare and refunded ICO token holders just before the acquisition at a massive loss. Salt Lending also built a successful loan business but the token went below the ICO price and the SEC eventually forced it to refund holders.

After the failure of nearly all such projects, it was more or less internalized by the industry that the reintroduction of borderline-barter, floating value private monies is less than ideal. This would arguably be true for any economic exchange, never mind those with the fundamental premise of openness. But the idea of removing them immediately creates several problems. Native tokens and utility tokens defined interaction on the network. Without them it isn't clear what "the network" means. The only workable answer is a tokenless smart contract to be utilized by other tokens.[3] But this is also unideal because, first, such a smart contract could never be updated and would have to be set up and deployed in its final form, and second, it is unclear how development would be funded.

An intermediate theoretical step would be to retain root control of the smart contract and attempt to monetize, but this would somewhat defeat the purpose of automatic execution if *what is being executed* can be amended on a whim.

Another approach, for certain kinds of exchange applications, would be to add fees and to distinguish between users and "liquidity providers," who interact with the same smart contract in different ways. Liquidity providers put up tokens that enable the application at the risk of loss (or "impermanent loss," to be detailed below) and users pay fees to access it, which go to liquidity providers.

The evolution of these applications, and in some sense the solution to some of these problems, was different varieties of the *governance token*: root access to the smart contract would be tokenized. This would, in theory, go a long way to protecting users from instantaneous governance abuses given the mechanism of implementing changes is *also* transparent and onchain; it would separate the users of the smart contract from the token in which they aren't necessarily interested; it would mean that the method of monetization (usually usage fees of some sort) can be distributed to governance token holders; where applicable, governance tokens could also be issued to liquidity providers, either at initiation, or as the rolling reward for enabling the service; this in turn would mean the token can be valued relatively accurately as "application equity" such that ownership can be dispersed and partial to the value of the service, making governance abuses even less likely, and enable price discovery around the true value of the service being provided by the smart contract in the first place. And finally, it would enable funding of development by the straightforward channel of investment in these tokens.

As of 2022, we propose the following taxonomy:[4] "native tokens" are the likes of ETH, SOL, BNB, ADA, MATIC, etc., as well as bitcoin. "Governance tokens" are as just described although we will further dissect this category further down.[5] Stablecoins, including wrapped bitcoin and even wrapped ETH, represent tokenized exposure to an asset with no native existence on that blockchain. Some "utility tokens" still exist and it is arguably the case that many so-called governance tokens are really just bolt-on utility tokens, which we will discuss further down. There is a final, miscellaneous category that typically have no smart contracting abilities, whether at the protocol or governance level, but are more like gift vouchers for the business that issues them. We will call these "voucher tokens," for lack of a better name.

With this in mind, let us now investigate the characteristics both "decentralization" and "finance" would need to have in order to be credible, starting with the latter.

Finance, Defined

Finance is not just the movement of money. This is imprecise. For example, gambling is not finance. Nor are payments if they don't involve a *financing* component. Finance is the use of money to facilitate the pricing of capital. Capital means factors of production that are not directly consumable, but which intend to produce goods or services at a profit, generating a return, and compensating the contributors of capital. This may also go for individuals rather than enterprises, in which case the goal is not as easily conceived of as "profit" but rather as "affordability."

---

[3] We will always refer to "smart contract" in the context of automatically executing code on a blockchain, and "contract" to mean a real-world agreement between parties subject to a credible enforcement mechanism.

[4] No taxonomy will be perfect, but we have tried to strike a balance between thoroughness and clarity. Arguably the only "correct" taxonomy is an encyclopaedic listing of the properties of every token under the sun, which is rather beside the point of the analysis we will go on to offer. Mikey 0x provides a far more granular taxonomy than we do here (and with a far more favorable analysis, it must be said!).

[5] "Application equity" is a useful expression to understand why they ought to have value, but we will stick to "governance token" throughout as it is widely understood in the industry.

There are a range of activities that constitute facilitating the pricing of capital, yet which involve the use of money in quite different ways. A personal loan is quite different to a business loan. A personal loan may enable a customer to purchase something from a business they would otherwise not be able to, which in turn allows the business to be profitable, which in turn generates a return for their capital providers. A derivative is quitedifferent, but ultimately has the same purpose of reducing the uncertainty of the future and its possible effects on return-seeking capital already allocated or intended to be allocated.

A crucial concept that goes a step further is that of a security. Imagine we start with a contract[6] entitling one counterparty to the rights to some flows of money, to be provided by the other counterparty under future circumstances that may be specified, variable, contingent, down to that counterparty's judgment, or some combination of these. A security is a contract that gives these rights to its holder, such that they can be traded beyond the original counterparty. This means that the market can crowdsource what these future money flows are worth *right now*, and hence allocate capital to a far wider range of capital-forming enterprises than holders of mere money would be able to identify and exploit on their own.

Note that a loan, if tradeable, is a security, as is a derivative. In fact, every tradeable financial instrument that is not money is a security, even if it is merely the right to some asset: possessing an asset itself is not the same as possessing the right to claim this asset from a counterparty.

In financial terms, native tokens are perhaps best thought of as an analogue to a gift voucher, yet which is perpetual, rather than ever truly redeemed (although there may be some more complicated mechanics such that it is partially redeemed, partially re-issued, and so on). It is a voucher for a network rather than a company. It is pseudo-money - money that can only be redeemed for one computational service – that is, to whatever extent they were not centrally issued as securities! Voucher tokens are gift vouchers for a company, in a much more limited sense, given the company necessarily operates on the network on which the token is issued for the concept to make any sense. They tend to be burned when they are redeemed.

Governance tokens, on the other hand, are clearly securities. As a working definition, a security is a tradeable contract exchanging money upfront for well-defined but uncertain streams of money in the future.[7] We emphasize that we do not attach this label to suggest they *should be regulated*. That may or may not be the case, but it is irrelevant to our argument. All that matters is that *this is an accurate financial analysis*. Later, it will become relevant that they are not regulated, regardless of whether or not they should be.

Finally, utility tokens are clearly securities as well, just with an even more opaque avenue for returns and hence investment theses: the streams of money in the future are uncertain but also *poorly* defined. In practice, most seem to amount to the hope of selling for a higher price in the future. As mentioned above, many so-called "governance tokens" are really bolt-on utility tokens providing simulated decentralization and governance with no fee sharing.

Decentralization, Defined

Let us move on to "decentralized." There is a subtlety here that we mentioned in a footnote above and will return to several times throughout the paper. The implication is one of removing centralized gatekeepers, which are prevalent in traditional finance. But what then? Can *some* people interact without going through centralized third parties? Or can *everybody*? This is not a trivial difference.

---

6 A *real-world* contract, not a smart contract.

7 The Howey Test is commonly used as a simple yet widely understood gauge of whether or not a contract constitutes an "investment contact" - a subcategory of security in US Federal Law, hence even more specific. According to the test, an investment contract exists if: i) there is an investment of money, ii) in a common enterprise, iii) with the expectation of profit, iv) to be derived from the effort of others. It is indisputable that governance and utility tokens fit the test at the point of crypto VC funding and token allocation: i) VCs invest money, ii) that goes towards the development of the contract in exchange for a share of it, iii) valued based on the fees they expect the contract to generate, the potential to sell into a liquid market, or both, iv) based on the success of the development, the secondary market enthusiasm for the development, or both. And even if there is no VC investment, per step 1, if the token is premined and later realizes some market value, later sales constitute the realization of an investment contract. We cite it not to endorse it or claim it is objectively a correct or even the best such definition, but rather for familiarity's sake in communicating the concept it attempts to capture.

The former is arguably better captured by "peer-to-peer": direct lines of communication between counterparties who wish to exclude third parties, centralized or not. Whereas the latter implies *nobody can be excluded*. When we apply this understanding to *contractual rights to flows of money*, "excluding nobody" can only be understood to mean that everybody is able to buy and sell these contracts if they want to. In other words, they are tradeable, which in turn means they are securities. But securities necessarily have counterparties - the party who *issued* the security and from whom the security is a contractual right to claim some flow of money - and every tradeable financial instrument besides money is a security.

We assume the idea is to represent both money and securities with tokens on blockchains, given this is pretty much exclusively what has happened in crypto DeFi. But we will note in passing, and return to several times, that the "peer-to-peer" understanding is just as valid. "*Contractual rights to flows of money*" as digital bearer assets needn't take the form of tokens, even if this has been almost entirely ignored to date in crypto.

We established above that to be considered "finance" at all, in a candidate *decentralized finance*:

i) the flows of money have to be facilitating the pricing of capital and not just the movement of money for its own sake

With the clarification that the instruments of decentralized finance need to be securities, we can add a second fundamental conceptual criteria for a security to be meaningfully *decentralized*:

ii) the money used as a flow to facilitate the pricing of capital also has to be decentralized

Let us recap the candidates for money: native tokens, governance tokens, voucher tokens, utility tokens, and stablecoins (including wrapped bitcoin).

We can tick off governance tokens, voucher, and utility tokens immediately as they are centrally and costlessly issued and cannot be money, never mind decentralized money.

Stablecoins are fascinating in that they can be thought of as simultaneously money *and* securities. Recall, they are not literally the money they are supposed to represent, but a right to claim it. They "work" as money to the exact extent that they work as securities: if the claim of redemption for "real" money is widely believed to be credible, they will tend to be treated as a viable money substitutes, or *fiduciary media*, to be more precise. This is worth bearing in mind whenever we encounter them again.

Stablecoins can importantly be split between issued and algorithmic.[8] While far closer to credible *money*, issued stablecoins are, naturally, not decentralized. They are issued by a custodian who represents a single point of failure.

Algorithmic stablecoins are a far subtler proposition. For the same reasons as centralized stablecoins acting as fiduciary media, it is fair to recognize them as credible money insofar as they are also credible securities. We acknowledge that in the best designed cases it is also fair to recognize them as credibly decentralized. We have a serious issue with algorithmic stablecoins, but as it is a technical one and not a conceptual one, we will save this critique for Part II, *Decentralized Finance, Technically*. For now, we are happy to say that algorithmic stablecoins can be credibly decentralized money.

This leaves us with native tokens. Are they money? Can they be? To be clearer about the implications of the question, we are asking this of the native tokens of layer-one blockchains.

We do not think it is controversial to describe bitcoin as money: it is designed to be money and essentially nothing else. What of ETH, SOL, BNB, ADA, MATIC, and so on? We also do not think it is controversial to say that these are, at best, vastly inferior moneys, and more akin to computational resources.

---

[8] Note these are our definitions for the purposes of explanation. As was stated in a previous footnote, many taxonomies are possible and some will surely be more precise than our own.

The blockchains unanimously describe themselves as "smart contracting platforms," and the native tokens as "gas" for paying for computation.[9] Of course, we should look at how these assets are used rather than taking statements made by their creators at the time of their creation as gospel. Not only might they be used as money regardless of these statements and accompanying design decisions, but, as it happens, Ethereum developers have gone on to make centralized changes to optimize monetary policy to compete with bitcoin as money (EIP-1559 and others). But we would argue the centralization that enabled this change is self-defeating.

A similar problem in this regard is that all (not just ETH) were premined to a greater or lesser extent. This is a touchy and sometimes overblown point given the purpose of a premine is typically to fund protocol development in exactly the same way as with a seed investment in a company. But this observation properly captures how these tokens came about and how they should be conceived of: they are securities. Their issuance and control are far too centralized to constitute credibly decentralized money, as is the scope of what they are intended to be "spent" on.

One counterargument might be that the de facto state capture of Ethereum in gradually becoming more and more OFAC compliant could, at the same time, be said to give it practical grounds to become more accepted as money via state enforcement, and more transparent than fiat currencies in traditional finance also. However, the cost is, once again, explicitly the loss of decentralization, so whatever kind of money it is, it is not decentralized and therefore cannot contribute to credibly decentralized finance.[10] Conceiving of ETH, and similar, as first and foremost computational resources (i.e. gas tokens) which happen to have taken on vastly inferior monetary properties to bitcoin strikes us as more appropriate. Recall, above we described them as, "*pseudo-money - money that can only be redeemed for one computational service - that is, to whatever extent they were not centrally issued as securities*!" which we again feel is appropriate.

Why So Serious?

In Part I we have covered the conceptual criteria we feel is necessary to credibly capture *decentralized finance.* The reader might be wondering, are we just ruling out everything we dislike based on pedantic definitions and ignoring the reality of development in crypto DeFi?

We understand this impulse, but we reject it. This is absolutely worth being pedantic about.

If we are not pedantic about the necessity of pricing capital and we are willing to admit any flow of money for any reason, we invite entirely overlooking that the *pretense of capital formation* is the sole conceptual source of speculative value in these assets and the infusion of tens of billions of dollars' worth of return-seeking *investment*.

If we are not pedantic about the flows of money pricing capital, it is not plausible that *capital* is being priced, given capital formation relies on market signals of likely profitability and returns. What is being "priced" is far more likely to be something along the lines of collectibles or commodities. In other words, if the flows aren't in money, we aren't talking about finance in the first place.

And if we are not pedantic about this money being decentralized, we negligently invite the greatest rug pull of all time. In other words, if the money isn't decentralized, then none of this is.

Even so, we feel the relevant and necessary criteria doesn't stop here. These criteria were merely conceptual. If the reader prefers, she can withhold judgment on whether or not crypto DeFi fits this conceptual framework and continue to Part II, *Decentralized Finance, Technically,* in which we will investigate further technical criteria we believe are necessary for credible decentralized finance.

---

[9] We refer the reader to Section 1*, The Innovation From First Principles* of *Only The Strong Survive* for an additional argument that the native token of a layer-one blockchain has to be money in order to have technical and economic coherence, although that argument is outside the scope of this paper.

[10] As an amusing side note, consider that the de facto state capture of Ethereum in gradually becoming more and more OFAC compliant could, at the same time, be said to give it practical grounds to become more accepted as money via state enforcement, and more transparent than fiat currencies in traditional finance also.

PART II: DECENTRALIZED FINANCE, TECHNICALLY

"In the short run, the market is a voting machine, but in the long run, it's a weighing machine."
- Benjamin Graham on crypto

Following the conceptual criteria set out in Part I, we assume a "decentralized security" is facilitating the pricing of capital with flows of decentralized money. We will now be more specific about how such a security would have to technically operate in order to credibly capture a "decentralized contractual right to claim from a counterparty":

We list below some characteristics a security may have that would lend to it being sensibly described as "decentralized" also:

1. There is a counterparty but neither "the law" nor any credible enforcement mechanism of real-world contractual guarantees is a point of centralization and so the flow of money per the claim on counterparty commitments and holder rights operates on trust.
2. The contracts are enforced automatically, and the counterparty has no choice but to meet its commitments. This also avoids the "centralization" of the legal system required to enforce the contract as its ultimate backing, hence "smart contracts".
3. There is a counterparty, subject to the centralization of "the law" or a similar credible enforcement mechanism, but it is custody, trading, and clearing that no longer require centralization because the security takes the form of a freely, trustlessly transferable digital bearer asset.

Point 1) - DeFi as Trust

There is a counterparty but neither "the law" nor any credible enforcement mechanism of real-world contractual guarantees is a point of centralization and so the flow of money per the claim on counterparty commitments and holder rights operates on trust.

Point 1 describes interpersonal credit, and points to the difference between "decentralized" and "peer-to-peer" as we have delineated the two. In a space in which *nobody can be excluded*, contractual rights to flows of money must be freely tradeable and hence must be securities. The purpose of securities is to scale capital formation beyond what this kind of backed-by-trust credit can support. Why would you need to construct a contract to be *freely tradeable and priced* exclusively between people who know and trust each other already?[11] In addition, the point of a blockchain is (in theory) to engineer trustlessness, and so one wonders why blockchains would be a worthwhile means of achieving this "decentralization" in the first place, and we are once again back to pondering peer-to-peer applications instead …

The point of the centralization of *the law* is to avoid governance abuses that are invariably likely to arise when counterparties do not know one another. This is a rather amusing point to focus on given ex-bitcoin crypto's faux-libertarian pretenses, disdain for securities regulations, and repeated insistence that issued stablecoins and native, governance, utility, and voucher tokens are not unregulated securities. Securities always involve handing over a definite amount of money now in exchange for the contractual promise of a usually indefinite amount of money in the future.

But promises can be broken. This is such an incredibly simple premise of human behavior it is surprising and unfortunate that it needs to be explained. Millions of dollars - billions even - will more often than not be taken in violation of "promises made" instead of given to strangers *unless* there is a credible enforcement mechanism to prevent this. FTX is a perfect example, which we will get to further down.

---

[11] This subtlety is exactly what is being exploited in both fedimint and Tether's Pear Credit, which both feature "digital tokens" representing forms of financial contract. Their "free tradability" is created by instantaneous redemption and reissuance by the trusted counterparty in the case of fedimint, and recursively extending the chain of trusted counterparties in the case of Pear Credit, whereas "price discovery" is rather beside the point of their intended use. The fact these tokens are not "on a blockchain" - because they don't need to be, because they transparently operate on trust - means in both cases there are no fees and instant transfer, a trade-off thought to be very much worth it.

Reputation may be such a mechanism in a free market, but it is defaulting back to trust and can be very useful but will only get you so far: fraud is rampant in "free markets for reputation" *even when* there is the credible threat of legal action.[12]

Issued stablecoins (including wrapped bitcoin) rely on trust. They are not *actual* dollars or bitcoin, but IOUs for bitcoin or dollars that are technically and legally unenforceable. As it happens, they may even be *illegal*, and hence in some sense *less than* legally unenforceable. Any actual bitcoin or dollars exchanged for such a token may well never be returned. "Holders" of soBTC (wrapped bitcoin on Solana) allegedly custodied by FTX, are discovering this at the time of writing.[13] Voucher and utility tokens rely on trust even more obviously so, as their utility is entirely at the discretion of the issuer.

In the case of governance tokens, on the other hand, the question is not as straightforward to answer. One response might be that they do not rely on trust, because claims are automatically enforced by the smart contract (so more in line with Point 2, which we get to just below) not by trust at all, and the terms of enforcement are open and transparent.

But this is not quite addressing the question. We must consider who has entered into a contract with whom, what promises around flows of money were codified, and what commitments are still live. The buyer of the governance token traded money upfront for the rights to some kind of nominal return generated by relationship with the smart contract, be it fee revenue, further token issuance, or by some other method. By this understanding, the smart contract *itself* is the counterparty, and we are firmly in Point 2 on automatic enforcement of commitments. In other words, this again seems like "application equity".

But if we investigate this analogy further, we realize that, if we have regular equity, there are two important differences to the above naive analysis: i) the commitments to which we are contractually entitled do not end with "the company," as if it too were an autonomous entity, but with the management of the company and the board. In other words, those controlling the resources which generate the flows of money to which we are entitled. And ii) *there is* a credible enforcement mechanism of these commitments: securities law!

The proper analysis here is that i) fellow governance token holders control the resources generating the flows of money and hence they, not the smart contract, are the counterparties, and, ii) in *this relationship*, there is no credible enforcement mechanism after all! We do in fact *trust* that they will not utilize their governance tokens in a way that alters the governance mechanism of the smart contract, or the smart contract itself, to our disadvantage. More simply, regardless of whether or not we trust them, we can't stop them.

An interesting corner case is where governance tokens are constructed so as to only be capable of amending certain parameters of the smart contract, the idea being that holders would want the flexibility to amend these based on differing market conditions in the future. For the sake of clarity, let us call governance tokens which collectively have the ability to arbitrarily amend the smart contract "unrestricted" and those that can only tweak predetermined parameters "restricted".

This acknowledgment introduces some subtlety here around the exact relationship between automated enforcement, per Point 2 that follows, and human decision making and trust. Hence, we will continue this discussion just below in the following subsection.

Governance tokens aside for a moment, we would argue Point 1 therefore does not apply. Operating on trust is not a means of achieving credibly decentralized finance.

---

[12] We don't intend for this discussion to digress into a debate on the merits of anarcho-capitalism. We occasionally use "the law" as shorthand that everybody understands, but "credible enforcement mechanism" is both more precise and more general. This could easily be provided by private enterprise and it would make no difference to our argument. What we criticize in crypto is not an aversion to *the state*, per se, but rather enthusiasm for the absence of credible enforcement of any kind.

[13] It is worth pointing out, however, that stablecoins on their own, issued or algorithmic and not in relation to the construction of more involved securities or to the pricing of capital, needn't pass this narrowing of criteria. Recall, payments are not *finance*, unless they are *financed*; the simple act of paying does not require a security. Stablecoins in crypto are clearly useful and are clearly widely used, but we consider this a useful application of these blockchains (and interestingly not of bitcoin). It is not *DeFi.*

Point 2) - DeFi as Smart Contracts

The contracts are enforced automatically and the counterparty has no choice but to meet its commitments. This also avoids the "centralization" of the legal system required to enforce the contract as its ultimate backing, hence "smart contracts".

What if the counterparty has no choice but to meet their liabilities because enforcement happens via smart contract execution? This at least has some potential, but we must immediately return to take issue with governance tokens and algorithmic stablecoins.

There is a fundamental trade-off at play here that much of crypto DeFi seems not to want to address: if you employ immutable automatic enforcement, you are ruling out human judgment, hence most capital allocation, and hence most of finance. But if you allow human judgment, you *need* some form of enforcement other than automatic or you are operating solely on trust, which can't scale, and hence can't be credibly described as decentralized. The question is how best to deal with the trade-offs that are unavoidable given what finance *is and is for.*

That is not to say that those parts of finance that do not rely on human judgment are without value, however. Quite the contrary, the commitment to uncertain future flows offered by varieties of hedging and market making, for example, can almost certainly be enforced entirely with smart contracts given appropriate trustless information feeds.

Unfortunately, very few smart contracts in crypto DeFi are truly immutable, because such a smart contract could never be updated and would have to be set up and deployed in its final form.[14] This was exactly the problem allegedly "solved" by governance tokens, on which we can now resume our analysis.

The distinction between restricted and unrestricted governance tokens is crucial. We will give some credit to the design methodology of restricted governance tokens in that they appear to be sincere attempts to address the fundamental trade-off just outlined. Yet, the immutability of restricted governance tokens creates governance pressures from the desirability of flexibility and inflexibility alike.

Which parameters can be tweaked, by whom, and by how much, once decided upon, is still immutable by definition. While it may seem wise to introduce flexibility to changing circumstances, that flexibility cannot be open-ended or else the governance token becomes unrestricted and defeats the purpose of this subtlety. If flexible enough to *later change* what parameters can be tweaked, by whom, and by how much, the governance is unrestricted; if restricted, then the perfect decision needs to be made at the outset and we are once again in the conundrum of needing to deploy this smart contract in its final form. This enormously *restricts* our ability to involve human judgment in the allocation of capital.

At the same time, the introduction of *any* parameters that can be tweaked creates a trust issue that we are inadvertently making impossible to solve, given we are stipulating that these are the only tweaks allowed. In other words, it is entirely possible that these tweaks will encompass ways of abusing governance power. For example, the tweakable parameter could relate to the control of issuance of the governance token, in which different parties will naturally have different interests. If the governance is so restricted as to only tweak this parameter and not be capable of addressing *how parameters are tweaked*, then holders simultaneously have to trust each other *and* be subject to the automatic enforcement of whatever actions other holders take.

---

[14] We should note that this was the historical norm around 2019-2020 prior to more perverse methods of monetization becoming the standard. In some cases, it still exists, however. Tornado Cash is a topical example, which is interesting precisely because *it cannot currently be shut down*. Nobody controls the code. And yet, Infura, a centralized entity, accountable to US law and which at times accounts for the majority of access to the Ethereum blockchain, can and has blocked access. This raises some obvious questions about the extent to which the industry surrounding a given blockchain harms its claims to censorability, and hence to credible decentralization, which we will leave for now. It is also worth pushing this logic further in light of Ethereum trending towards OFAC compliance, as mentioned several times. There is a precedent of Ethereum rolling back changes (DAO exploit) and hard forking to change core features (delaying difficulty bomb, EIP-1559, the merge) so there seems to be a real possibility that regulators try to force developers and leading infrastructure companies to fork out offending applications, splitting Ethereum into 2 camps. Pirate applications would still run on the "original" fork but the liquidity on that chain would likely die of anaemia.

To a large extent, unrestricted governance tokens are implicitly trying to overcome this tension. However, if the power to amend a smart contract beyond the restricted tweaking of parameters exists, it can be acquired, and once acquired, the smart contract can be amended to anything at all. A potential amendment, if not the likely one, would be to remove the governance rights of everybody else. Given governance tokens are securities, this violates the initial (real-world) contract with counterparties. If this is at all possible and cannot be credibly enforced against, then we are back relying on trust that it won't happen.

Theoretical commentary side, we must finally address the practical reality of the vast prevalence of bolt-on utility tokens masquerading as governance tokens. In this case, root access to the smart contract is not actually democratized, but a centralized team of developers retains control of the direction of the project, either by holding the keys or by driving upgrades to v2, v3, and so on.

A generous interpretation of this setup would be that the developers and backers tackle the fundamental trade-off of human judgment in capital allocation and credible decentralization by raising capital with decentralization theatre while continuing to allocate it with human judgment. A more cynical interpretation purpose of such bolt-on utility tokens was and is transparently to skirt securities laws and banking regulations in raising this capital by moving from the model of, *you give me money, I give you tokens*, to, *you put money in this smart contract, it gives you governance tokens so long as your money stays in*.[15]

The other usage of smart contracts in DeFi we said we would get back to is that of algorithmic stablecoins. We believe that the unfortunate reality is that most algorithmic stablecoins are unsound in the long run.

The only way to *guarantee* redemption of a reserve of fiduciary media is to i) physically have the reserve, and ii) have your promise to redeem be subject to a credible enforcement mechanism. Actual dollars in bank accounts have no crypto-native existence and so cannot be controlled by a smart contract. Bitcoin has a crypto-native existence but, at the time of writing, no way to trustlessly manipulate on other blockchains. Keep this in mind, however, as we will come back to the prospect of a trustless peg further down.

Absent direct, *physical,* exposure, the only option is synthetic price exposure. If we are looking to automate this, we need to guarantee convertibility into some other priced asset.

But you can't guarantee the price of *any asset*, and so we end up issuing fiduciary media denominated in asset x, but backed by asset y, where the price ratio of x:y floats. Therefore, we immediately encounter a capital efficiency problem because the only way to guarantee protection against a z% drawdown in asset y is to overcollateralize the fiduciary media of asset x by z/(100-z) times.[16] Arbitrarily high overcollateralization could in theory work, *if also paired with* having reason to believe that asset y will at least be relatively stable in price against asset x, if not likely to appreciate. But all approaches in crypto DeFi have driven in exactly the other direction on both counts: using native, governance, utility, or voucher tokens as the reserve asset(s), with no reason whatsoever to expect helpful movements in their prices relative to asset x (almost always USD) and advertising the "capital efficiency" of the low collateralization requirements.[17]

We end up in the bizarre situation of accidentally fractionally reserved fiduciary media, where the collateralization ratio is a function of a floating price of an unregistered security and the reserves aren't really reserves at all because they will be liquidated per big enough movements in this price.

If (or when) the collateral stays under the value of the issued media for long enough, regardless of what ingenious mechanism of satisfying redemptions has been created with supposedly immutable smart contracts,

---

15 We have done our best above to give the design of these tokens the benefit of the doubt in teasing out how they *could* work. But looking at the practical reality and building on this cynical interpretation, it is sadly undeniable that governance tokens have done very little to protect crypto DeFi users from governance abuses. There are many examples in which whale VCs vote at the last minute to change the governance against the wishes of the community (restricted or unrestricted governance abuse) or in which the developers just ignore what the community wants and make changes against its will (bolt-on utility token abuse). Governance tokens in crypto DeFi are a bit of a LARP that the community is now largely moving on from: for instance, Uniswap v3 was released with a business license: i.e. the credible enforcement mechanism of *the law.*

16 For example, protection against an 80% drawdown requires 80/(100-80) = 80/20 = 4x overcollateralization.

17 The biggest example being Maker DAO, which had to back DAI with USDC during the March 2020 drawdown in Eth. More recently, it capitulated and is now backing DAI with US Treasuries, giving billions of dollars' worth of USDC to Coinbase to yield farm.

secondary markets will begin to reflect the doubt that these redemptions can be met and either the peg will break, the reserves will drain completely (possibly near instantaneously in a novel digital spin on free banking-esque note duelling) or some mix of the two. As with all fractional reserve banking, everything is great so long as credit is expanding and prices are going up. But leverage bites both ways …

To give credit where it is due, some algorithmic stablecoins have sophisticated mechanisms incentivizing holders to dynamically adjust their collateral, including adversarial positioning relative to other holders such that entirely selfish motives push all to protect system collateralization as a whole. While these incentives may work on a short-term, case-by-case basis, they cannot help in the long run if market panic in asset y lends itself to a simple calculus that liquidating and losing the reserve entitlement is cheaper than potentially endlessly committing more falling reserves to prop up a fixed face value of fiduciary media.

So, again, it will probably only work in the long run if we have reason to believe that asset y will at least be relatively stable in price against asset x, if not likely to appreciate. This *might* work with decentralized money as the backing, but do we believe this of native, governance, utility, and voucher tokens? We leave that up to the reader …

There is an interesting parallel here to our critique of governance tokens. Although rooted in a smart contract, and hence the behaviors by which humans can interact with the system are precisely and transparently specified, this still can't force humans to act in the desired way! Humans can think outside the smart contract and choose to ignore entirely the incentives it provides. Either the smart contract decides or humans decide, but the smart contract cannot make humans decide. This circle cannot be squared.

Algorithmic stablecoins are not fundamentally flawed in the same way, to be clear. With governance tokens, the "smart contract" is effectively an illusion of having designed away the potential for governance abuse. With algorithmic stablecoins we assume the smart contract is genuine,[18] and the vulnerability is not one of "governance abuse," as such, but that the incentives it provides may simply be ignored given real-world circumstances which the smart contract cannot be said to *understand*.

All this said, Point 2 does leave an opening for credible decentralized finance: *actual* smart contracts that manipulate decentralized securities or decentralized money natively or via a trustless peg.

Point 3) - DeFi as the Network, Not the Asset

There is a counterparty, subject to the centralization of "the law" or a similar credible enforcement mechanism, but it is custody, trading, and clearing that no longer require centralization because the security takes the form of a freely, uncensorably transferable digital bearer asset.

In this case, we assume the security has some credible enforcement mechanism (most likely real-world legal registration) hence the question of rights and commitments of money flows is solved without solely trust in the issuer and without automatic enforcement, per Points 1 and 2. Instead, we consider decentralizing custody, trading, and clearing.

This latter property exists in crypto, as well as in bitcoin, and is often touted as one of the main benefits: that financial instruments can be directly controlled by the user without centralized gatekeepers for custody or middlemen for exchange and clearing. An obvious problem presents itself here in that the former property does not apply. Issued stablecoins, and native, governance, utility, and voucher tokens are unregistered securities, the governance of which relies on trust that cannot scale past people who already know one another.

We have already made this point several times, however, and so will instead focus on two different and subtler problems: the censorability of the network, and the concept of "Maximum Extractable Value", or MEV.[19] To be clear, neither completely prevent workable decentralized securities, but they are strong vectors of (re)centralization. At the very least they are major inconveniences that ought to be avoided in decentralized finance if at all possible.

---

[18] We leave aside the possibility that an algorithmic stablecoin also has a governance token, in which case all of this is effectively complexity and decentralization theatre, and our critique of governance tokens dominates all else.

[19] Originally called "miner extracted value" until it was realized parties beyond just miners can extract value in similar ways.

We won't go through every layer-one blockchain as similar arguments apply to Ethereum, Solana, and BSC, by far the largest by market capitalization of these native tokens and supported on these chains. Solana and BSC barely need any discussion as they are unequivocally centralized. It is not at all uncommon for "validators" to take the network offline for hours at a time.

Ethereum is more complicated as it is notionally much more decentralized in terms of number of users and distribution of tokens. However, the shift in consensus mechanism has almost immediately led to OFAC compliance in ~70% of blocks produced.[20] In other words, enough large and centralized entities are technically interdependent on each other and we can easily imagine them in time becoming jointly liable for each other's behavior in validating blocks. The exact mechanics are outside the scope of this paper, but we would argue that the nature of Proof of Stake is such that this vector of recentralization is only likely to get worse over time.[21]

There is a subtlety here worth drawing attention to in emphasizing how dire censorability is for hoped-for decentralization. Blockchains are necessarily distributed global states. In and of itself, this is an enormously more centralized starting point than the reality in traditional finance of securities issuance, trading, clearing, custody, and, ultimately, *ownership*. Insofar as valid alterations to this global state are permissionless and pseudonymous, we can credibly claim decentralization. However, the ability to censor transactions destroys such a hope.

MEV is similar:[22] in any network with privileged actors there will be asymmetries of access and information. In smart-contracting blockchains, there are necessarily such privileged actors because assembling transactions in the most profitable way requires a lot of expertise and enormous computational power. A market naturally arises in which (relatively unsophisticated) block proposers auction those slots to (sophisticated) block builders. This enables a range of trading behavior such as front-running and sandwich trading that would be illegal in traditional finance. It is estimated over $600m has already been extracted from DeFi on Ethereum alone. Hence this represents another vector of recentralization around the well-capitalized, who by definition have the best access to the single global state being proposed as the record of all securities ownership.

The thread running through these concerns is the existence of a global state in which these securities are represented in the first place. It is worth asking why this would even in theory be needed? What do we achieve for which we must trade the centralized overhead of a blockchain, centralized censorability, and centralized visibility? What are transaction fees paying for if not hard-won trustlessness?

We can only think of one worthwhile answer: global access. If there is an advantage to the issuer of a security of having effectively global price discovery and liquidity, this may well be worth it. But if not, we aren't so sure. Again, there are other means of creating digital bearer assets that work within more restrictive trust regimes than a blockchain, and which are better described as "peer-to-peer" than as "decentralized."[23]

Let us now combine these theoretical insights into a framework for practically workable decentralized finance.

Workable Decentralized Finance, a Recap

To recap: Point 1 gets us nowhere: we cannot operate securities on trust alone in a meaningfully "decentralized" environment. Point 2 allows for smart contracts (without backdoor governance) that manipulate decentralized securities or decentralized money natively or via a trustless peg. Point 3 allows for registered securities which are decentralized insofar as seeking to take advantage of a blockchain network rather than a blockchain asset.

---

20 One might quibble that there is nothing in OFAC regulations that compels censorship at the base layer by validators currently. Some people don't like the term "compliance" as nobody is complying with existing laws or regulations and the behavior is more like *complicity in overreach.* However, we feel

21 Classic reads on this topic include Paul Sztorc here and Andrew Poelstra here. More recently, Dylan LeClair and Sam Rule have a cautious take here. Lyn Alden has a more sceptical outlook here. VItalik Buterin has a more positive outlook in general, but still bites the bullet on MEV, here. Adam Gibson gives a philosophical explanation of Proof of Work here, which concludes with an effective dismissal of Proof of Stake's ability to achieve anything like the decentralization of the former. Finally, Nic Carter and Lane Rettig explore the issue at some length on this podcast.

22 BIS has a short but helpful writeup here.

23 But consider again, our argument in Section 1, *The Innovation From First Principles,* of *Only The Strong Survive*, is what blockchains are really *for* in the first place.

It also provides two ideal characteristics of such a network - that it is not censorable and that either confidential or off-chain transactions can reduce and minimize MEV, if not remove it entirely - and one ideal threshold characteristic of the securities themselves - that their issuer truly requires global price discovery and liquidity.

If we allow that bitcoin is decentralized money, then this all pops out the following: Point 2 allows for the Lightning Network, DLCs, LBTC on Liquid, RBTC on RSK. Point 3 allows for RGB or TARO assets (insofar as they are legally enforceable and hence do not operate on unscalable trust alone) given they are rooted in bitcoin's network and transferred off-chain; or for registered security tokens on Liquid, RSK, or Sequentia - as their transfer can be confidential. The combination of Points 2 and 3 allow for immutable smart contract execution of hedging contracts, automated market making, and more, between bitcoin and decentralized securities on any of the aforementioned scaling layers in which this is technically possible. The caveat to Point 3 is more cultural than technical and could be thought to amount to: *are you sure you need blockchain-based tokens at all rather than other, more trust-dependent means of achieving digital bearer assets? Why not use a system like fedimint or Pear Credit?*[24]

As mentioned in the introduction, we believe a variety of decentralized finance will emerge on bitcoin, and to some extent already has.

Evidently, this narrowing down of worthwhile characteristics ends with fairly bitcoin-centric criteria. It is worth considering what, if anything, could lend these characteristics back to crypto DeFi, and the answer isn't quite nothing: if the native tokens of layer-one blockchains were credibly decentralized money then most of our reasoning around bitcoin would likewise apply and most of the concerns outlined at length above would disappear.[25]

Otherwise, we see one feasible combination of factors by which decentralized finance could come to be on non-bitcoin blockchains. First, there needs to be a way to manipulate decentralized money in these ecosystems while retaining custody and without counterparty risk. Second, real economic returns must be the root of subsequent layers of financialization. Note these first two points once again amount to: *it has to actually be finance and it has to actually be decentralized.*

Third, securities involving human judgment in the deployment of capital need to have credible mechanisms of enforcement that do not rely on trust. If these first two factors are enabled, then automatic execution per Point 2 can become useful, whereas currently, it amounts to little more than complexity theatre and a velocity catalyst. In other words, either the code governs or the law governs, with no LARPy governance tokens muddying the water on the relevance of human involvement. Fourth, the transfer of these assets would ideally be enabled off-chain, confidentially, or some as-yet-undiscovered method for avoiding MEV, or at least minimizing it. Fifth, the networks *themselves*, as well as the native tokens of the networks, would need to be credibly decentralized and incapable of censoring valid updates to global state. Sixth, the case needs to be made that global price discovery and liquidity is worth the trade-off of a handful of centralization vectors that come with using a blockchain in the first place rather than some other method of creating more trust-dependent digital bearer assets.[26]

But frankly, while this may be feasible, we think it is unlikely for a simple reason: the culture in crypto focuses on moving in the other direction on almost all of these points besides the first.

There are toxic incentives to monetize by token issuance rather than putting capital at risk to provide a valuable service, which we analyze in more detail in Part IV, *Let's Play The Blame Game.* Every effort is made to insist that stablecoins, native, governance, utility, and voucher tokens are not unregistered securities even though they are, and are automatically enforced even though they are not; as crypto base layers race ahead with proliferating complexity, both MEV and censorability via re-centralization are becoming worse and worse problems; and there appears to be little appreciation of the concept that this would likely imply a dramatic price decline in the native token of whatever blockchain achieves all the aforementioned. This is likely because, were this to happen, it could not be

---

24 This is not an exhaustive list, but covers only those with which the authors have some familiarity.

25 That the narrative around Ethereum has gradually shifted from "world computer" to "web3" to "DeFi" and now to "Eth is also money" is symptomatic of this realization setting in. We highly recommend Ryan Gentry and Dhruv Bansal's talk at Bitcoin Miami 2021 for a thorough analysis of the folly of this line of argument (and note we also referenced this excellent talk in *Only The Strong Survive*).

26 We addressed this possibility, as well as what might motivate its proliferation, in Section 6, *Why We Might Be Wrong,* of *Only The Strong Survive*: *"Crypto programmability is never truly matched on bitcoin and the value spiral and Pfefferian holding period problem alike are nipped in the bud by provably enforceable atomic swaps such that Ethereum, Solana, Cardano, EOS, Tezos, Tron, etc., effectively become sidechains."*

reconciled with the prevailing investment ethos and theses that relies on leverage and exit liquidity, amongst other unsavory factors - all of which are catalyzed by global price discovery and liquidity. True peer-to-peer is a non-sequitur in such an environment: it leaves retail out the market and money on the table.

Most unfortunately of all, we would even argue that this rough direction *was once the norm and the aspiration*, even if the stage reached was questionable and incomplete. The evolutionary step touched on briefly in the very first subsection of adding fees and distinguishing between users and liquidity providers is an importantly different construct to the majority of what has been developed since and outlined just above. This involves putting capital at risk and offering a service users pay for.[27]

This was *actually capitalistic*, but the problem was that hardly anybody used it or cared about it besides the developers. This was very probably because, without facilitating the underlying pricing of capital or manipulating decentralized money, it is not entirely clear what the use case was or whether it was worth the *real* risk. Nobody wanted 2% yield on stablecoins, especially not at the risk of "impermanent loss," least of all VCs. So-called "generalized mining" (i.e. wash trading to simulate usage of the applications to try to honeypot wider adoption) was indulged in, for a time. But as it would shortly turn out, the catalyst for adoption was *precisely*: toxic incentives to monetize by token issuance, exaggerate via "yield farming," and realize via immediate and total exit liquidity. In the end, these dwarfed every other incentive by which DeFi might have inched towards credibly decentralized finance.

As mentioned in the introduction, we approve of the idea of *decentralized finance* in theory, even if *DeFi* isn't this in practice. What DeFi *is* in practice leads naturally to FTX …

PART III: THE SHORT, SAD SAGA OF FTX

"2+2=5"

- Winston Smith auditing Alameda's balance sheet

From the golden child of crypto to the pariah of the industry, the fall of FTX and Alameda is arguably the single largest failure in the history of the crypto space.

Alameda came first. It was a trading firm, specializing both in arbitrage and directional trading strategies of crypto DeFi tokens of all stripes. These are common in all advanced markets, with crypto being especially lucrative due to the inefficiencies in information, and the ability to centrally and costlessly issue these tokens with no credible enforcement mechanism for the commitments attached.

Then came FTX, an exchange. In its truest form an exchange should have one simple task: pair buyers and sellers and take a fee for facilitating the trade. This can be a steady and profitable business. Zvi Moshowitz puts it crisply as follows:

"*FTX builds a pretty good product outside of the fraud and the insolvency and the stealing customer deposits, and does a lot of things very well. The competition really is pretty terrible so it doesn't take much to offer a superior product.*"

FTX's claim to fame was in offering the riskiest trading experience in crypto DeFi. It allowed for high leverage and futures products that were hard to find elsewhere - in particular the ability to use just about any stablecoin, native, governance, utility, or voucher token as trading collateral at risk of liquidation. Instead of a customer giving the exchange all the money they would like to trade up front, the exchange begins to lend to the customer in order for them to speculate on tokens. FTX was not the only exchange to offer this service, but it was by far the most aggressive.

---

[27] "Impermanent loss" is a bizarre and basically euphemistic expression aiming to capture the following: if you put some amount of ETH in a liquidity pool, and ETH 10x's relative to the paired token, then you will only benefit from a far smaller gain than you would have if you had just held your ETH because the pool will force you to sell for the paired token the entire way up, and that is nowhere near made up for by the fees generated.

Risk management is the foremost priority of any financial firm offering credit. From real estate on the one hand to crypto DeFi tokens that can be costlessly and centrally issued ad infinitum and then used as collateral for leverage on the other, the lender must manage this risk. We will not go into too much detail here, but essentially this task boils down to mitigating timing mismatches.[28]

Here is where it gets truly wacky. Like many in crypto DeFi, Alameda had the idea of creating their own DeFi token, FTT, in advance of launching FTX: a kind of ICO for both a token and a company. The alleged commitment to holders was derived from the promise that a portion of profits from FTX would be used to buy up the token. Of course, there was no credible enforcement mechanism, and so although we might think of FTT as pseudo-equity in FTX, it is subordinate to *actual* equity and subject to the whims of its centralized issuers: FTX management. FTT was a voucher token that meant whatever FTX and Alameda decided it meant.

With the exceptionally dubious premise for valuation of this costlessly and centrally issued voucher token in mind, consider that both FTX and Alameda at various points decided to use FTT as collateral for leverage. This added a ticking time bomb of truly insane risk.

Insofar as it found any value in the market, FTT could only really be thought of as a bet on the success and health of FTX. By utilizing FTT as collateral, FTX made its balance sheet both more leveraged and, on top of this, as vulnerable as a whole as FTT was in particular. Although few outside suspected it at the time, especially as FTX was "rescuing" the likes of Voyager and BlockFi (i.e. bailing *in* their customer deposits), FTX's balance sheet was mighty vulnerable …

Although details are still emerging, the picture is becoming clearer that Alameda appears to have made *enormous* losses on directional bets on crypto DeFi, including VC-like investments, up to and around the time of the Terra/Luna collapse in May. By some accounts Alameda may have lost over $15 billion, much of it on leverage that was then called in. It is suspected Alameda veered in this direction once its early edge in market making deteriorated as the overall crypto market began to mature.

In order to prevent Alameda's collapse (which likely would have immediately caused the failure of FTX also, given their often-illegal interrelationship)[29] The Wall Street Journal reports that FTX lent Alameda over half its customer deposits to Alameda to plug this gap. It is plausible that FTT was used as collateral for this loan on the FTX side.

Lucas Nuzzi at CoinMetrics has speculated that a September 28th transfer of $4bn worth of vested FTT may well have been Alameda paying FTX back for this initial loan. This is all rather amusing given FTX is the entity that creates, issues, and allegedly redeems FTT in the first place. In any case, the customer deposits were gone, and FTX ended up with a balance sheet leveraged to a voucher token it created and almost exclusively traded on its own exchange. Macro analyst Lyn Alden captured the absurdity of the situation nicely as follows:



[28] For a nice walk through all of this in FTX's case, we recommend Matt Levine's Money Stuff article for Bloomberg, *FTX Had A Death Spiral*.

[29] It appears that customers sending international wires to deposit with FTX were actually wiring to Alameda.

A November 2nd CoinDesk article leaked details of this precarious situation. This in turn prompted a tactical open market sale of FTT by Binance which was too large for the market or the team at Alameda to prop up (Binance held around 10% of the token supply after investing early in FTX and being bought out in 2021 for a combination of stablecoins and FTT). This led to the death spiral of self-fulfilling rumors as panic spread and depositors desperately tried to withdraw their (mostly non-existent) deposits. FTX took less than 48 hours to go from functionally but secretly to *actually* insolvent.[30]

As a kind of amusing epilogue, it is worth covering what happened with the Solana-based "decentralized exchange" Serum and its governance token SRM as FTX was beginning to wobble earlier in 2022. The situation wasn't critical to the collapse but nicely demonstrates in practice several points we made above in theory.

In short, because FTX owned enough SRM to unilaterally alter the smart contract and "unrestrictedly govern", in effect, it was able to inflate the token supply by 60% in two huge mints on February 19th and May 25th. The relevance of these dates is that the GBTC arbitrage trade was beginning to invert around February, causing issues at BlockFi and 3AC, while Terra/Luna collapsed in May, and hence the mints were almost certainly related to trying to offset Alameda trading losses. Nonetheless, some portion of these tokens went on the FTX balance sheet and were marked at $2.2bn at the time of the CoinDesk leak, despite the total market capitalization of SRM being $88m.

So, who and what do we blame? Is this the fault of DeFi? Of decentralized finance? Or of a centralized financial entity, riding the hype of "crypto", deliberately operating in a jurisdiction with barely credible enforcement mechanisms, freeing it up to take actions that would be deemed illegal in most advanced market economies?

The straightforward answer is the latter. There is no doubt that immense and potentially unprecedented fraud was involved in FTX's collapse.

But we would also argue that DeFi masquerading as decentralized finance, and all the financial ignorance and misunderstanding this feeds on, had a crucial part to play as well. So too did the industry surrounding and promoting DeFi, exploiting financial ignorance, and requiring precisely the likes of FTX to facilitate cashing out while others were cashing in. Let's play the blame game …

PART IV: LET'S PLAY THE BLAME GAME

"What bothers me isn't that fraud is not nice. Or that fraud is mean. For fifteen thousand years, fraud and short-sighted thinking have never, ever worked. Not once. Eventually you get caught, things go south. When the hell did we forget all that? I thought we were better than this, I really did."

- Steve Carrell as Mark Baum on Crypto VCs

It is hopefully clear from our explanation above that pretty much nothing about FTX was "decentralized". We might think of it as CeFi or "centralized finance" so as to distinguish it from DeFi. To reiterate the popular claim we identified in the introduction and which we intend to analyze:

this was CeFi, not DeFi, and, if anything, only further demonstrates the need for DeFi.

Then again, FTX was predicated on the centralized access to and manipulation of DeFi, so what are we to think? Who are we to blame?

---

30 In one final, hilarious twist, it also appears that FTX US tried to access its customers' bank accounts and was considered dangerous malware.

With our framework from Part II, *Decentralized Finance, Technically*, we can more properly distinguish between DeFi and decentralized finance, and tease out the importance of the former to FTX specifically and crypto in general

Pricing Capital

In Part I, *Decentralized Finance, Conceptually,* we outlined two conceptual criteria we believe are relevant and necessary for a candidate decentralized finance to be credible:

i) the flows of money have to be facilitating the pricing of capital and not just the movement of money for its own sake

and,

ii) the money used as a flow to facilitate the pricing of capital also has to be decentralized

Recall "pricing capital" is only meaningful insofar as it enables capital allocation that generates a return. It is really the *return* that is being priced.

Throughout Part II, *Decentralized Finance, Technically,* we referenced point ii) several times in building out our framework, but we did not again allude to point i). This was quite simply because we would have needed to point out every other paragraph that the generation of real economic returns is not happening. This would have distracted from the entirely separate set of flaws we were analyzing. But it is now appropriate to bring it up again as the final nail in the coffin of crypto DeFi.

As mentioned in the introduction, our main problem with *DeFi* is that it is not decentralized and it is not finance. Although covered at length in *Only The Strong Survive*, let us briefly review what DeFi *has actually achieved* in relation to capital, finance, and flows of money …

But Where Does the Yield Come From?

The absence of real returns on capital forces us to immediately question why these assets have any value. Returns can be, and often are, reframed as "yield," and crypto has taken a liking to presenting its financial credentials with this terminology. But where does the yield come from?

As we wrote in Section 3, *Crypto Is Not Finance*, of *Only The Strong Survive*:

"*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 part 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 market assesses the productive carrying capacity of economic* stock *generating the ability to pay the* flow *of 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 on the potential future value itself forming the basis of profitable arbitrage that is then mislabelled as a 'yield'."

Crypto DeFi engages in arbitrary and automatable combinations of seigniorage, securitization, rehypothecation, and leverage. It is the purest form of financialization ever conceived: the financialization of … nothing at all. To be absolutely clear, there is no link whatsoever to returns on capital employed, hence no link to any real yield.

And yet "yield farming" was the largest so-called "use case" for crypto DeFi in the cycle leading up to the collapse of FTX and was the composable primitive of just about everything else. Promises of "guaranteed yield" blitzed the markets with a ferocity that was impossible to keep up with. The meme became so powerful that individuals and entire firms alike dedicated all their resources to chasing the freshest "yield farming" opportunity presented to the market. Where did this yield come from?

The simple answer is it came from a combination of seigniorage and securitization and infusion from so-called "venture capitalists" and was then fueled by trading, leverage, and rehypothecation.

The Yield is the Friends We Made Along the Way

The more involved answer is that the false perception of yield emerges from the perverse incentives created by the absence of our two fundamental conceptual criteria for decentralized finance: i) no real economic returns, and ii) there being no decentralized money; combined with two novel properties of crypto to which we have alluded several times but on which we will now focus: iii) the ability to costlessly and centrally issue tokens, and, iv) immediate and total exit liquidity.

A concept that ties much of this together is that of a "vampire attack": the forking of the open source code of a smart contract or protocol *without a token* so as to add a governance token or a bolt-on utility token masquerading as governance.[31] The rationale to do this is as follows; a governance token can redistribute the fee revenue from the service provided by the smart contract to its holders, or a utility token can promise rewards of the application's increasing popularity to its holders via later repurchase. Both strongly incentivize those holders to use and promote the service.

Users getting in on something early before it becomes wildly popular and both contributing to and financially benefiting from that rise can give the newer project a bootstrapped momentum that becomes self-fulfilling in a way the (presumably useful) original service likely never would have, *even if it never had a fee in the first place*.

This approach incentivizes customers to become investors, and investors to find more customers. Because these mechanics are widely understood in the space, there is intense pressure on just about every crypto DeFi project to pre-emptively add a governance token to ward off such an attack. This pressure is only increased for those on the verge of becoming popular, or perhaps which already have. Given we have the ability to costlessly and centrally issue tokens, tokens proliferate, and we get rampant securitization.[32]

At the same time, given there are no real returns on which these securitizations are based, the easiest way to make a popular service in the first place is to create some means of financially manipulating tokens so as to produce the false perception of yield![33] Hence DeFi projects proliferate and we get rampant trading, leverage, and rehypothecation.

The final ingredients are the lack of decentralized money and immediate and total exit liquidity.

---

31 i.e. it doesn't matter whether or not this governance token provides any "governance" capabilities to its holder. It just needs to look like it is capable of providing investment returns for this argument to hold.

32 We can trace the chronology of so-called "decentralized exchanges" relying solely on funnelling fees to liquidity providers to issuing governance tokens in light of this pressure: as discussed at the end of Part II, *Decentralized Finance, Technically,* it never attracted much attention beyond the original developers and the VCs who attempted "generalized mining" to make the applications appear to have more activity than they did. The problem with this approach is that all the value needs to already exist to be manipulated. Centrally and costlessly issue a governance token, on the other hand, and the flywheel of the perception of yield is much easier to kickstart.

33 Similarly to the immediately previous footnote, it is notable that before all this became normalized, almost exactly the inverse was true. Uniswap, one of the first automated market maker projects and considered "blue chip" DeFi, was initially created as a form of protest. The 2017 Bancor ICO created the concept of an AMM DEX on Ethereum, and the Uniswap founders forked it, removed the token, and relaunched. Fast forward 4 years and Uniswap is on developer-directed "version 3," issued under a business licence, has a governance token, UNI, and a "Chief Legal Officer" (decentralized much?) insulting industry rivals on Twitter who dare to criticize his employer's lobbying efforts transparently targeted at regulating other decentralized exchanges out of existence. *And this in turn* is surely in part explained by community disgruntlement with PancakeSwap, a fork of Uniswap launched on BSC that eventually overtook the original in volume, as if forking open source projects wasn't rather the point of all of this... and note, the purpose of Uniswap as an application is to … trade other tokens … 97.7% of which have turned out to be rug pulls …

The lack of decentralized money has a subtle implication around how the false perception of yield, hence the securities, are priced. The funding provided in exchange for tokens is money (almost always USD, via primary offerings to crypto VCs and hedge funds) hence the tokens are most often quoted in this same denomination. But they do not generate fee revenue for holders in this denomination, but rather in the denomination of whatever tokens are being manipulated. This means the value of the governance token in question is, in practice, dependent on seeking to tactically boost the market price of the manipulated tokens (i.e. wash trade them) in order to create the false perception of yield for just long enough to cash back out into real money. It is therefore not dependent on improving the service or attempting to ground the entire edifice in real returns.

Attempting to ground a project in real returns and gradually improve it as it proves its value in the marketplace is the essence of capital formation. But it takes a long time. Immediate exit liquidity ties together the toxic cocktail of poorly interlocking incentives. Any potentially good idea will be pressured into a positive feedback loop of token issuance and aimless velocity and spiral out of control. Ironically, it will do so in a way that both introduces at least one security and possibly more, and yet deviates further and further from creating any real capital such a security might usefully price in the first place.

Some of this might sound like a natural analogue to a VC investing in the equity of a company, but this comparison is revealing of several important differences:

i) Per Part II, *Decentralized Finance, Technically*, there is no credible enforcement mechanism for the supposed commitments. ii) The hope in a VC investment is for an *eventual* return on capital to justify the price of the equity being bought. And, iii) founders and VCs do not have immediate exit liquidity in any start-up equity, never mind *all* start-up equity. Their equity will become valuable and tradeable (hence possible to exit) to the extent a return generating operation is successfully developed.

None of this applies in crypto DeFi: given there is no prospect of returns, but only “yield” traceable to token issuance, the incentive is not to invest in long-term productive stocks of capital but in the short-term perception of flows of *other* money into *this* money. Given VCs have immediate and total exit liquidity, their incentives are to not to nurture a highly uncertain business for as long as it takes to stabilize its return profile, but to maximize i) the amount of tokens they are allocated for free *as early as possible* and, ii) the price at which they can unload it *as quickly as possible*. Given protocol developers (the equivalent of companies) are similarly directly exposed to the immediate price rather than the long-term value of the capital they are responsible for creating, their incentives are equally aligned with VCs and misaligned with buyers and holders of the token. And given there is no credible enforcement mechanism, even referring to a “responsibility” is naive as they can do whatever they want. Unsurprisingly, what they tend to do aligns perfectly with their own warped incentives.

There are two main avenues by which these incentives are followed: fuelling and magnifying the short-term perception of yield and creating exit liquidity. While there are developers and investors in crypto *just trying to build useful things without a token,* this is the purpose of vast swathes of the crypto industry, and is enabled by VCs, hedge funds, and exchanges.

Crypto VCs seed both the initial tokens and any higher-level protocols that in turn allow for leverage and rehypothecation to increase flows and inflate valuations. If these protocols throw off additional “governance tokens” - i.e. they throw securitization into the mix as well - all the better: yet more tokens to be priced, traded, leveraged, and rehypothecated! Crypto exchanges create an onramp for retail dollars to provide the liquidity necessary for superficial validation of price movements, which in turn gives VCs an offramp to cash out. Crypto hedge funds typically specialize in arbitraging the relatively inefficient markets typically found on crypto exchanges, especially in light of the opportunity for insider trading given the securities in question are unregistered. But they sometimes also take directional bets and even seed native, governance, utility, and voucher tokens in a similar manner to crypto VCs. Often, the line between crypto VCs and hedge funds is blurry.

What is amusing, especially in hindsight, is that very little of this needs to be risky because, even if this is all done in perfectly good faith and belief in the potential value of the protocols and tokens created, it is functionally equivalent to extracting trading value from retail investors, just with a little wash trading thrown in as a honeypot. There is some timing risk for crypto VCs and hedge funds seeding the tokens, but given the exit liquidity is immediate, the period of directional exposure can easily be dwarfed by the size and immediacy of the pay-out. Running a crypto

exchange needn't be risky at all as it only requires facilitating trades without any directional exposure whatsoever. Likewise arbitraging inefficient markets as a crypto hedge fund.

And yet Alameda and FTX managed to do this in about as risky a way as possible; so risky, in fact, that they resorted to fraud to try to cover it up. As we know, even that didn't work …

Alameda, FTX, FTT, and more …

It is important to point out that the opacity of the mechanics just outlined is basically the entire idea. Fraud is easier to disguise when you create an allure of grandeur to mask a concept so basic a middle schooler can see it doesn't add up.

There were three core pillars to the story of the collapse: Alameda, FTX, and FTT. Alameda was a crypto hedge fund which aimed to make money arbitraging and making directional bets on native, governance, utility, and voucher tokens. While not strictly speaking a venture capital firm, it fulfilled essentially the same role given the blurriness mentioned above. FTX was a crypto exchange that offered leverage and other bespoke products to customers looking to speculate on token prices. Lastly there was FTT, a voucher token created by FTX with the value proposition to buyers that some of the profits from FTX would be used to purchase this token at various points in time. All three of these intertwined with each other, building layers of unnecessary and unjustifiable risk into a gigantic house of cards.

But key to appreciate is that none of this would have been possible without DeFi: Alameda arbitraged and directionally traded DeFi tokens of all stripes. FTX enabled this trading on an exchange explicitly encouraging leverage. Both entities "invested" in tokens, perhaps most notably having an important hand in getting Solana off the ground, an entire blockchain the entire purpose of which was to accelerate DeFi, including being amongst the largest holders of its native token, SOL. FTT was, of course, a DeFi token, as was almost everything else on FTX's balance sheet at the time of collapse. Terra/Luna was DeFi and kicked off the contagion leading to this debacle. And there is no incentive for anybody involved to try to base any of this on truly peer-to-peer technology because that would undermine the creation of a maximally liquid and global marketplace from which to extract trading fees.

These institutions may have been CeFi, but their existence, operation, and failure were predicated on DeFi.

PART V: DEFI'S FATAL CONCEIT

"And they're like '10X' that's insane. 1X is the norm.' And so then, you know, X token price goes way up. And now it's $130 million market cap token because of, you know, the bullishness of people's usage of the box. And now all of a sudden of course, the smart money's like, oh, wow, this thing's now yielding like 60% a year in X tokens. Of course I'll take my 60% yield, right? So they go and pour another $300 million in the box and you get a psych and then it goes to infinity. And then everyone makes money."

- Sam Bankman-Fried (Op. Cit.) on boxes

While all the parties involved in this scandal were centralized entities, it is important to realize that the "investment strategy" employed by the symbiosis of crypto VCs, exchanges, and hedge funds is utterly dependent on DeFi, and furthermore that DeFi, without real returns, has no avenue for appreciation or even much usage without this CeFi catalyst fuelling the fire. The idea that DeFi had nothing to do with this, or that the solution is *even more DeFi*, is little more than gaslighting.

Do You Need a Token for That?

For all the centralized machinations, for all the financial engineering to pump prices, and even for all the fraud, it is clear enough that the root cause of the chaos is the seigniorage of centralized and costless issuance of tokens. You cannot fund, lever, rehypothecate, securitize, exchange, and cash out on a token that has not been issued.

In *Only The Strong Survive*, we repeatedly addressed the rhetorical question: *do you need a token for that?* Functionally, the answer is almost always that you do not, since tokens invariably capture one of: "money for x, controlled by y," which will lose the fight for liquidity to "money for everybody, controlled by nobody", or, unregistered securities the governance of which essentially runs on trust, as discussed at length above.

But conceptually, this points to an even bigger problem - what we might call *DeFi's fatal conceit*: *token issuance* in crypto is about as centralized as can be. Typically, developers have preferential access to or even control of a protocol in which they sell some or other variety of "application equity," a fee generating smart contract in which they sell "governance tokens," whether with access to the smart contract or as bolt-on utility tokens performing decentralization theatre, or a related business for which they sell utility or voucher tokens. In all cases, this is always having first costlessly allocated a decent proportion of the tokens to themselves and their crypto VC and hedge fund backers.

This is a stark contrast to the *decentralized* token issuance of bitcoin, which happens via mining and, therefore, Proof of Work. Hence it is not "seigniorage" at all, but rather the product of the costly enabling of a functioning decentralized network.

Counterintuitive as it may be, and contrary once again to faux-libertarian pretenses, removing the apparent centralization of a credible enforcement mechanism of counterparty commitments is an *incredibly centralizing force*. Be it legal shareholder rights, free market enforcement, automatic enforcement, or however else it is achieved, credible enforcement levels the playing field between the sellers and buyers of securities by ensuring that promises are kept.

In other words, the principal-agent problem is real and serious. Removing a means of keeping it in check, whether in the pursuit of so-called decentralization or otherwise, inevitably has the effect of pushing agency costs unboundedly high. Ultimately, this is profoundly *centralizing* both in the costs themselves and in their aftermath. The already powerful reap illegitimate agency benefits while this is not yet widely appreciated, and once it is, the powerless cannot participate in the wealth creation and risk mitigation securities enable.

Insofar as it is predicated on centrally and costlessly issued tokens, DeFi is unavoidably and unforgivably centralized. True decentralized finance would use decentralized money, automatic enforcement where no human judgment is required, and credible real-world enforcement where it is.

And let us not forget, the very first domino in the great crypto crash of 2022, and from which the eventual collapse of FTX can be directly traced, was the depeg of the UST "stablecoin," programmatic hyperinflation in Luna, and sudden collapse of the entire Terra/Luna ecosystem. Terra/Luna was not CeFi in the slightest but classic DeFi. It was an algorithmic stablecoin of the more poorly designed variety. Its demise can be traced to this more insidious form of centralization in token issuance - in this case to construct an astonishingly stupid edifice capturing *all of*: funding, leverage, rehypothecation, securitization, exchange, and cashing out.

Present co-author Allen Farrington along with Nic Carter went into rigorous detail in *All Falls Down*, but the design of Terra/Luna can more or less be summed up with the following comparison, quoted from the paper:

"*A bank that claims it literally cannot go bankrupt because it can always issue more equity will very soon discover it* can *go bankrupt because the market will take this claim as well-enough proof that the bank is utterly incompetent at capital allocation.*

Given a fractional reserve bank is fundamentally highly leveraged, the redemption of liabilities in these circumstances will almost certainly exceed the absolute value of the reserve assets and *the equity base by many multiples. 'Issuing equity' is not creating new value, it is diluting the old value of existing shareholders. If a bank is having its liabilities called in at a higher value than there even is of reserves to liquidate and equity to dilute, it will collapse. This is more or less what just happened to Terra. The only difference was that the spiral of default was driven by an algorithm rather than by any social process. The 'capital allocation' was not the result of dumb humans but of dumb code. It was the dumbest 'smart contract' of all time.*"

And so, we come full circle to the fundamental trade-off of automatic enforcement and the necessity of human judgment for capital allocation. Terra/Luna tried to have it both ways, and quickly ended up having neither. So much for DeFi - what then of decentralized finance?

The Great Definancialization

We believe the core of the cultural fissure between crypto and bitcoin comes down to *financialization.* While the ethos of bitcoin is to definancialize, the ethos of crypto is to financialize. We repeat our characterization of this tendency from above: DeFi engages in arbitrary and automatable combinations of seigniorage, securitization, rehypothecation, and leverage. It is the purest form of financialization ever conceived: the financialization of … nothing at all.

At the time this was an observation, but we can now offer an *explanation*: without real returns on capital, without real yields, yet *with* the ability to centrally and costlessly issue tokens, financialization is the only avenue not only for exit liquidity, but for any activity whatsoever. The financialization of everything was absolutely behind FTX's various shenanigans. We believe the cultural - in some sense, *structural* - commitment and impulse to financialization means crypto is likely to stray further and further away from decentralized finance. Peer-to-peer finance is impossible to imagine in crypto because it presupposes only decentralized money.

As Steven Lubka recently wrote for CoinDesk, summarizing the FTX debacle from a bitcoiner's perspective, *"Bitcoin is trying to definancialize an overly leveraged, financialized world. Crypto is trying to further financialize everything. Crypto wants art, music, games, login credentials and anything else they can get their hands on to become financialized. Bitcoiners think leverage, subsidization of risk and turning everything into a speculative asset is actually massively net-negative for civilization.*"

Financialization is itself a product of easy and political money, a necessarily centralized phenomenon. In fact, crypto as a broader economic phenomenon is impossible to fully comprehend without appreciating the infusions of tens of billions of dollars into crypto exchanges, VCs, and hedge funds, as described above. This capital is allocated in the first instance in order to desperately chase yield for insolvent pensions funds due to worldwide monetary debasement and artificially low interest rates. We would argue it is fundamentally *misallocated* due to the drive of easy money to financialize everything it can.

Yield chasing is egregious in crypto DeFi, but it is not unique. What is unique is the absence of any real yields being financialized. That said, the presence of real yields to financialize hardly fixes the overall problem.

One way to conceive of what a security *does* is that it crystallizes potential future value into an instrument that can be priced in the present. If price signals are honest because money is sound, this is an extremely useful method to enable the efficient allocation of capital. But if they are dishonest because money is easy and political, it amounts to little more than stealing from the future and consuming more than has been produced. If we do this solely because we have liabilities to meet in the present - i.e. yield chasing - but are indifferent to the effect on our liabilities in the future, we drive even more capital misallocation, make these liabilities even more unaffordable when they come due, and set up more and increasingly desperate yield chasing down the line.

Under such circumstances, the proliferation of securities is not a good thing at all. It is a symptom of a broken system of money. As Parker Lewis writes in *Bitcoin Is The Great Definancialization*,

"*At a fundamental level, there is nothing inherently wrong with joint-stock companies, bond offerings, or any pooled investment vehicle for that matter. While individual investment vehicles may be structurally flawed, there can be (and often is) value created through pooled investment vehicles and capital allocation functions. Pooled risk isn't the issue, nor is the existence of financial assets. Instead, the fundamental problem is the degree to which the economy has become financialized, and that it is increasingly an unintended consequence of otherwise rational responses to a broken and manipulated monetary structure*."

The key potential of bitcoin is to return to sound money, proper pricing of capital, and *definancialization.* This would mean a reduction in the number and importance of securities, because securities would no longer have to play the role of de facto money while money continues to fail.

However, crucially, those that remain would be far more useful, functional, and true to their core purpose of enabling the proper pricing of capital.

This is the root of our cultural concern for crypto DeFi. The cultural, and arguably even structural, commitment to financialization is extremely difficult to reconcile with this core purpose of securities. In a sense, none of this is surprising given the foundations of crypto DeFi. If you jump straight to "decentralized securities" without first nailing down decentralized money and peer-to-peer technology, the urge to financialize is obvious, because what other value or utility can you even attempt to provide?

The unfortunate reality for crypto is that most people have no need to ever interact with securities, or for that matter, with finance proper. If their money were truly sound, there would be no need to chase yield, no need to *invest* outside one's intentionally risk-seeking expertise, and no need to trade upfront money for the rights to future flows of money outside the direct operation of a return-seeking business. Peer-to-peer digital bearer assets may be of use, but global price discovery and liquidity, not so much.

This sentiment can be reframed in terms of *Defi's Fatal Conceit*: in an ideal world, the human judgment necessary for real capital allocation is not something in which most people should have to or want to partake unless they actively seek out this risk.

Decentralized money, insofar as it enables saving and spending - soundly and uncensorably - is a worthy goal. If we consider traditional finance to be exploitative, opaque, inefficient, and so on, we would posit that the ideal solution is not necessarily to democratize the ability to engage in finance, however more fairly, transparently, and efficiently we might hope to achieve that. The ideal solution is rather to remove any dependency on finance whatsoever for the vast majority of people who shouldn't ever need to interact with it.

We again commend stablecoins - *by far* crypto's most worthy achievement and best provision of value and utility - for meaningfully extending the ability of millions to save more soundly and spend more freely all over the world and in a more decentralized manner than what for most is the alternative, if not perfectly so. But the idea, however implicit, that everybody should hold their own securities is profoundly misguided. Furthermore, the idea that this drive to financialization ought to be so thoroughly "decentralized" that we ought to securitize not only pseudo-financial flows but contrive reasons to securitize inherently technical projects as well, is even more regressive.

The "Fat Protocol" thesis, oft-championed as a brilliant new incentive mechanism for the development of free and open-source software, is better understood as a way of privately capturing the value of things that are naturally public, and providing an avenue to immediately realize this captured value before any real capital has been created.[34] If bitcoin can be understood as a way to *genuinely* decentralize public value transfer, crypto can equally be understood as a method of privately capturing and recentralizing some of this value leak: of *financializing* the commons.

On the other hand, the cultural norm in bitcoin development is to shirk tokens if at all possible and find ways to incorporate bitcoin, both the network and the asset, into peer-to-peer projects as directly and trustlessly as possible; in particular, to find ways to enable users to monetize with decentralized money *and without financializing the projects themselves*.[35] This usually requires real capital put at risk in order to offer a service users pay for. There are no privileged, centralized parties extracting rents from users hoping to overcome this cost with speculative gains. Thus applications can be meaningfully democratic and credibly decentralized. The Lightning Network fits this profile to a tee - as do circa-2019 liquidity pools in crypto DeFi, it must be said! It is hence instructive to compare the paths of each in the meantime as one impatiently veered into costless and centralized token issuance to further financialize this service, and the other on patiently building real tools with a peer-to-peer ethos, no token, no exit liquidity, and no centralized control.

---

[34] Co-author Allen Farrington has written here about how the drive to optically open but economically closed systems of user control is largely a symptom of crypto's incestuous relationship with Silicon Valley, but this argument is somewhat outside the scope of this paper.

[35] Interested readers are encouraged to look into LNURL-auth, Nostr, TBD's Web5, and Synonym's Slashtags, amongst others, for some such attempts. The reader may recall from an earlier footnotes that fedimint and Pear Credit do involve "tokens" of a sort to achieve more directly financial than technical ends. And yet, each go out of their way to ensure these tokens *are not securities*. They rely on trust for redemption and realization of value, and hence there is no prospect of speculative returns. That is to say, they have an actual use case.

The aversion to tokens for intrinsically technical and nonfinancial projects strips the developers both of centralized control of the free and open-source software they are creating and of immediate and total exit liquidity in its value. The only way to realize this value privately is to utilize this commons tool within a return generating enterprise that compounds capital.

That is to say, the default assumption is that securities are not required. But if they are, they tend to be predicated on pricing capital and utilizing decentralized money. Not DeFi but decentralized finance.

Green Eggs and Ham

"I do not like them in a house.
I do not like them with a mouse.
I do not like them here or there.
I do not like them anywhere."

- *Dr Seuss on centrally and costlessly issued tokens*

Our core issue with DeFi is that it is not decentralized and it is not finance. Nonetheless, we support the idea of *decentralized finance* in theory, even if *DeFi* isn't in practice. We also believe a variety of decentralized finance will emerge on bitcoin, and to some extent already has. These were the core claims of our previous paper, *Only The Strong Survive*, but we did not explain what we deemed to be workable decentralized finance in theory, or what constraints might limit how it might develop.

In this paper, we have given a framework by which claims to "decentralized finance" can be assessed, and found, once again, that the vast majority of DeFi does not read favorably. While we admit there are some avenues for DeFi to approach decentralized finance, and that it is not quite a technical impossibility, we think they are highly unlikely to be pursued. We think culture is the more important driver, and as of this writing that the culture of crypto DeFi is actively pushing in the wrong direction.

The FTX debacle, of which we gave a brief overview, is a perfect example of the consequences of this attitude. Claiming that FTX "*only further demonstrates the need for DeFi"* is misguided at best. DeFi enabled FTX to happen. The relationship between DeFi and the FTX debacle can be best described as, "*it takes two to tango*."

Decentralized finance as we hope to see it develop would have none of the properties we identified as key to crypto DeFi and inevitable in FTX: it would facilitate the pricing of capital, not the illusion of velocity and a valve for exit liquidity; it would natively interact with decentralized money, not centrally and costlessly issued tokens; and it would operate uncensorably, enabling truly *decentralized* participation in the wealth it is able to create.

We see paths for *this* vision of decentralized finance to gradually be built, but DeFi ain't it.

Thanks to Brad Mills, Lane Rettig, Eric Wall, and Edan Yago for edits and contributions.

It should go without saying that not everybody mentioned above agrees with any or all of our theses or conclusions. In fact, some passionately disagree, in which cases we appreciate their input even more greatly. Several contributors preferred to remain anonymous as well.