The Future Is Forked

May 1, 2018

Author's note: I originally wrote this essay a number of months ago. Since then there's been a bunch of discussion around governance thanks to essays from Fred Erhsam, Vlad Zamfir, Will Warren, and others. As well as debates within the Ethereum community. While I haven't addressed any of these recent events in this piece—or how my views on the subject have changed—I hope to in future essays.

There were two major forks or attempted forks of Bitcoin in 2017 cementing that forks are not rare black swans [1]. They're happening often, but most people know little about how they work exactly. While forks are powerful, they are still a work in progress—and each fork helps us learn something new about them and how they fit into the ecosystem.

Forks provide checks and balances within an ecosystem

Forks are a fascinating construct. As many have pointed out, they are incredibly useful adaptive mechanisms which add a new dimension to the Exit, Voice, Loyalty framework. In that 1970 essay, Albert Hirschman categorized the actions people can take when they disagree with the organizations they belong to, whether a company, government, or ecosystem: they can either leave the organization ("exit") or speak up and try to change it from within ("voice"). These actions are modulated by how loyal people feel to the organization.

Every response we have to organizations is some mix of exit, voice, and loyalty. For example, threatening to quit your job exercises voice; once you leave, it's exit. It's pretty rare to see novel combinations, which is what forks are. Forks are new and powerful schelling points in how ecosystems operate. They combine voice and exit—and critically lower the friction to both significantly. **Since cryptocurrency ecosystems have no higher regulatory authority that can ultimately check them—it is crucial to have a feasible internal impeachment mechanism like forking.**

There are many things that help businesses based on network effects lock in their users. For marketplaces and social networks, competitors must start from scratch if they don't want to be part of the existing ecosystem. In contrast, **forks give stronger rights to those who want to challenge an ecosystem and make it easier to compete.** The threat of a fork holds the incumbent ecosystem accountable while also enabling more exploration of the landscape of potential outcomes. Unchecked, monopolies often stop innovating and responding to the harms they cause. For true monopolies, only the shadow of antitrust action keeps them honest—and even then, only to the minimum degree required. In crypto, there is no centralized regulatory body. It is the specter of forks that ensures developers innovate and remain responsive rather than resting on their network effects.

In my view, the primary brilliance of forks is not about creating a new blockchain, but about their ability to signal a credible check on developers—keeping them honest and aligned with the broader ecosystem [2]. I don't think it's innate to forks that they put the new chain and old chain on equal footing. In fact, it seems capricious to choose equal footing as the threshold. Forks are not a fixed atomic construct. There are many ways they can work—both their technical aspects and the community norms around them. These factors will change how they play out and tilt in practice. Whether they favor incumbents or challengers, how peaceful vs disruptive they are, etc. The technical and social norms that dictate these outcomes should be debated in depth, forks are certainly not perfected yet. For example, an interesting line of thought multiple researchers have worked on is how to address the susceptibility of the voice aspect of forks to sybil attacks. Some of the futures and prediction market ideas around this are worth reading up on. These and more factors will be a subject of future essay.

Forks discriminate between current and future users

Imagine your parents got divorced, but they forgot to tell you. You'd be upset right? That's what forks in the cryptocurrency ecosystem are like for new users.

A common misconception on forks is that because users and investors get tokens in both blockchains, they will be economically agnostic towards both. Users shouldn't have any biases and the merits of the two blockchains will determine their fate. The thinking is that developers, companies, and miners will compete over which blockchain wins—but the costs will be abstracted and users will be shielded, minimizing the disruption of forks.

This is not true.

Debates over specific blockchains aside, forks as they are currently structured are not agnostic from a user perspective. **Specifically, current forks separate the incentives of future buyers from current holders.**

Existing holders are given tokens in both blockchains. As long as they do not sell their tokens, they still are economically agnostic between the two blockchains. In fact, many have come out net positive from recent forks, as the sum of both chains have increased relative to the original pre-fork chain. Whether that should be an expected feature of chain forks, or an artifact of current markets, is an important but separate topic. [3]

These economics aren't true for new buyers. If they bought both the original *and* forked token it would be true. But this isn't how most new buyers view the market, nor is that their fault. Exchanges, wallets, and our whole ecosystem don't discuss or package up both tokens in this way. Our default is to treat them as separate asset classes, so why should new buyers think otherwise? However, these forks are often directly competitive and each expects their success to come at the expense of the other. Thus, new buyers post-fork are unintentionally taking directional bets on the market, while old holders are agnostic to direction.

Existing holders and new buyers not being equal isn't inherently bad. It's not obvious it should be changed—many aspects of the cryptocurrency space tilt towards

incumbency. However, we need to consider what our ecosystem's commitment to new users is and should be. Because it's one thing for forks to not be user neutral, and another for users to not be aware of it.

Users are unaware of this directional risk they take and must take on non-trivial complexity to understand it. While those fully enmeshed in the cryptocurrency world may often comment on how fast and inscrutable crypto's movements are, we forget we still have orders of magnitude more context and knowledge than new buyers. Even worse, we often take pride in crypto's complexity and ability to evade predictability. If you talk with anyone who has only recently started buying bitcoin, they have little visibility into the dynamics between different blockchains, much less different forks. They instead rely on following what high-profile companies and investors recommend. This is a useful and important function, but is often centralized with poor accountability. The legibility of these cryptocurrencies to new investors and users is important long term. **The more illegible the cryptocurrency ecosystem is to new investors and users, the more wary they will be of joining and the more they will rely on the advice of experts and the defaults of companies**. Removing these experts and brands is not what's most important; they have their place in the ecosystem. Rather, making the ecosystem legible so that customers can understand and hold these companies and experts accountable is key.

User legibility and attention will only grow more important as more projects try to build on-chain governance. But there are still many open questions about on-chain governance that should be discussed in the community. Many blockchain projects are being built with an assumption of an active and educated electorate. But both attention and understanding are scarce resources that these projects will need to grapple with. Projects planning for on-chain governance may find their democracy is most akin to all the worst parts of the San Francisco Ballot Proposition system. Users are often not able to be an active, educated electorate—and even if they are, they often don't care to be. And while the cryptocurrency community is large with many active participants, its growth in complexity and rate of change outpaces the rate at which most can keep up. This leads to trust and centralization in the institutions they offload this responsibility to. Everyone developing in this ecosystem needs to either build with that as a vulnerability in mind and/or figure out how to decrease the

friction of user comprehension and participation. **Unless we match crypto's growth in complexity with equal progress in making it legible and welcoming to new users—it will grow in natural centralization**

When attention and legibility are scarce, defaults and brand matter

As long as people have scarce attention (this is an unsolved problem, and maybe an unsolvable one too), whoever owns the relationships with end users will have disproportionate influence via the defaults they set, whether implicit or explicit. Examples of this include:

1. Exchanges adding cryptocurrencies. The market cap of cryptocurrencies often goes up significantly when they are added to large exchanges. This is so common that many active traders try to find inside information or read between the tea leaves of Twitter posts to guess when a cryptocurrency will be added to an exchange. Market caps of cryptocurrencies will even rise on the rumor of being added to an exchange.
2. Investing in pre-sales and ICOs based off of prominent investors and advisors. Many investors in all rounds of cryptocurrency projects today have not read the whitepapers of the projects they want to put money in. They are instead basing their investment on the perceived credibility of the existing investors and advisors. This is not unique to crypto, but simply a statement of the ubiquity of human scarcity of attention and legibility.

I don't think these examples are necessarily bad or irrational. Sometimes it's not feasible to make things fully understandable and have all users be be active and engaged. When this happens, centralization is the tradeoff that balances everything wanted with the scarcity of attention. **Scarcity always begets centralization**, and cognitive scarcity is no different. Prominent exchanges, investors, and advisors are incentivized to maintain their reputations, so in the long run, it's not unreasonable for people to trust their recommendations. Or at least for the short run, to trust that *others* will trust their recommendations (creating a Schelling point).

As cryptocurrencies become more mainstream, 'normal' users will increasingly demand centralization as the solution to their scarcity of attention and legibility. They will not want to need to spend the cognitive cycles that many of us currently spend thinking about the ecosystem. They will want the benefits without much of the costs—and will turn to companies to provide them. It's why centralized exchanges have been one of the most financially successful parts of the ecosystem so far. Whether in proxy voting or how they represent forks to users, the decisions made by those entrusted by customers will have significant impact. But while the fundamental scarcity of human cognitive load is inevitable, cryptocurrencies has a few unique attributes are promising:

1. **The defaults aren't set yet.** One of the most exciting things about cryptocurrencies to me is that we have not yet solidified how the ecosystem is shaped and norms are set. All of us in the ecosystem are together helping shape what cryptocurrencies will look like. Eventually, like all industries, it will start to calcify. It's likely we'll look back and wish some things had played out differently. But the clay is still wet, and there are precious few spaces of importance where that can be said [4]. A subset of the ecosystem will end up making the choices that all future constituents will live with, and how we think about our decisions now should be informed byt hat.
2. **Moving the complexity-legibility frontier.** This problem can also be solved by improving the legibility of cryptocurrencies at any level of complexity. Crypto, due to its software nature and nascent stage, is well suited for this. There are few structures that have calcified, and software is malleable and easy to experiment and improve. Cryptocurrencies are currently very complex and illegible, but software is easier to make legible than any other substance. There are many working on this at all the different areas of crypto—and they should be applauded for their work. Cryptocurrencies will be at their best not when they are viewed as complex and inscrutable, but when we make even the most complex topics accessible and intuitive to all.

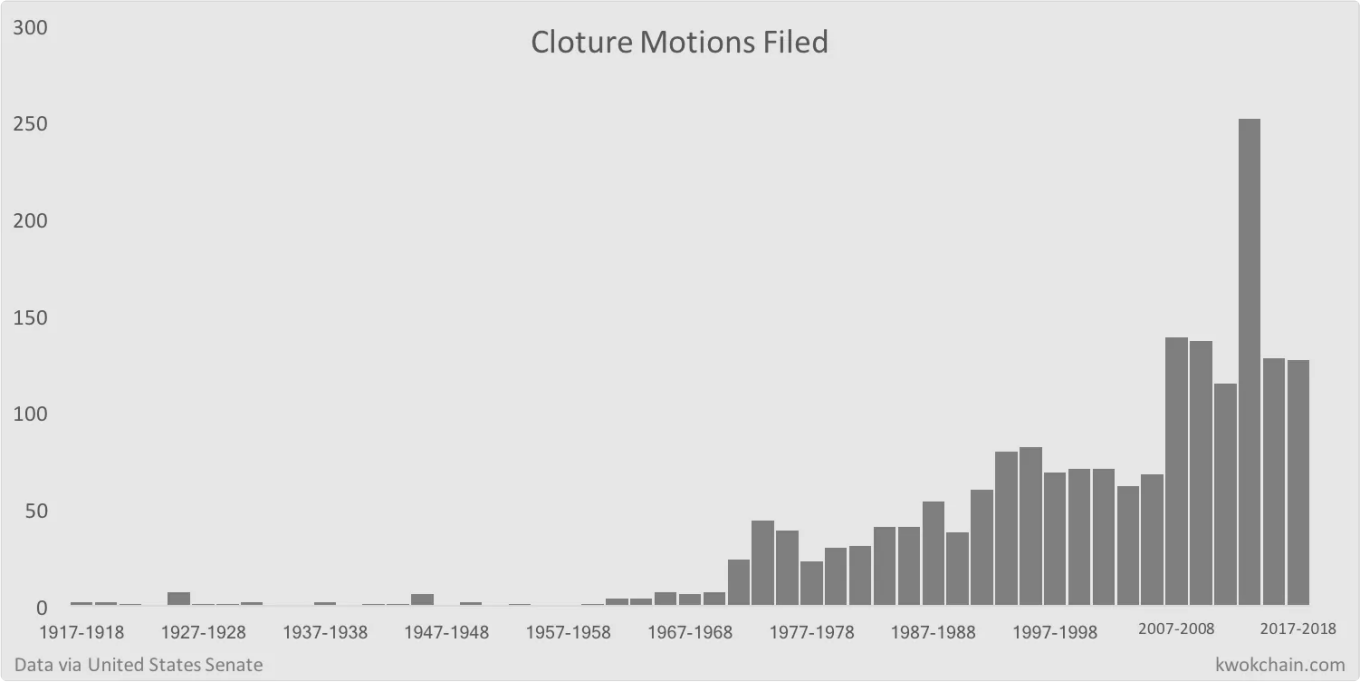
Credits

Thanks to Nader Al-Naji, Michael Dempsey, Keila Fong, Alex Hartz, Noah Jessop, Chris McCann, Kevin Simler, and Casey Winters for their help with this post. And conversation with Will Warren for getting me to start actually sharing these.

Post-scripts

[1] The prevalence of forks should cause people to adjust their priors. Forks are happening at a frequency that was not anticipated, and whenever this happens people should refactor their mental model. I believe two things are happening.

The first is that forks were originally meant to be a check, not a tool. I think that forks as envisioned were meant to be like impeachment or the filibuster. Not meant to be used often (or hopefully ever), but a threat always looming to keep developers from misaligning significantly. However, like the filibuster they went from rare usage to common usage over time.



The second is that forks are the real frontier of the metagame. They are the place where blockchains are most susceptible to attack and where the least explicit checks have been created. Forks are where the rules of the ecosystem are implicit and not enforceable. This makes it the ideal environment for looking for where there will be an advantage to new strategies. Both those we'll look back on as innovation and those we'll look back on as attacks. Through this lens, we should expect the amount of forks

we've seen. In fact, we should expect new strategies utilizing forks. Forks are very asymmetric in payoff currently. A way to tell that the metagame is present is by debate over what tactics are fair game or out of bounds. In cryptocurrencies this is particularly important because as a space it lacks most of the ways by which ecosystems prevent the meta-game from moving up the stack. Will be interesting to see how it plays out and likely should be much further public discussion on this area.

[2] I've often wondered whether people's mental models for democracy match. Is democracy the goal, or the tool? We fall into the trap of believing democracy is the goal itself—and then are repeatedly surprised when we see democracies fail around the world. **Democracy seems more to be along the efficient frontier of a bunch of factors we care about in governments.** This is not a complete or ranked list, but things like accountability, legibility, effectiveness, enforceability, etc. are all factors that seem to matter in how we evaluate governments. And of course, not just when they are working well, but also what their checks are when they are not working well.

For example, imagine a dictatorship, but it had perfect visibility into the wants of its populace and citizens had a tamper-proof secret button that if 50% of populace pressed, a new dictator would be put into power. Would that be an inherently inferior government to current democracies? China is the government that comes to mind when considering this thought experiment. Though it's often thought of as not being held accountable, it can also be viewed as a government that promises growth in its people's standards of living or faces populist revolts. It's still an open question whether this is sustainable long term. A less controversial, but even more striking example is companies. Within the structure of our democracy, the primary subunit of activity and governance is the corporation, which is quite non-democratic. **Understanding the different factors that make us desire democracy for our countries but corporations for our businesses is crucial to understanding where cryptocurrency ecosystems will fall along the spectrum.** What is clear is that many of these institutions lack much of the technology to make their accountability censorship resistant and feasible.

Democracy as it currently exists is unlikely to be the platonic frontier of what matters in governments. Democracy as we know it is the version we have *because* of our inability to credibly guarantee certain accountability functions (coupled with the

irreversibility of government misalignment). If blockchain were to make these technically feasible, would we come to a different conclusion about the dominant structure of governance on top of it? After all, every human organization is topologically equivalent. The differences between them are a function of the underlying structural dynamics and the resulting differences in their specific features. So what does that mean for the structure of ideal blockchain governance? My guess is that it looks hybridized between companies and governments. Because of the lower tail risk and easier exit option, companies have settled on a governance structure significantly more centralized and akin to a dictatorship (but with legible metrics and easy exit ability). Maybe we'll find that the legibility and accountability of cryptocurrencies are more core than its decentralization at all levels. Again, a topic for another time.

[3] Though the recent forks have been quite controversial, they've actually been surprisingly calm compared to what we'd expect. This is largely because most investors have learned a strange lesson from the last few forks: forks create free money. And it's true. Despite belief that dividing the network effect of a cryptocurrency would lead to a weakening of the overall system, the opposite has happened in the last few forks. They have led to a net increase in the combined value of the two blockchains relative to the pre-fork blockchain. Here's an essay well worth reading by Vitalik on some potential causes for this. It should be the subject of longer essays and debates, but here are a few factors that I think should be considered in this debate.

- Internal dissent is a net drag, so separating partisan factions leads to higher EV of both vs. them combined. Both because of a) belief that partisan fork will be more able to enact changes they have wanted (see North during Civil War) and b) sides that have strong partisan leanings have more incentive to come in to weigh scales now that they have mechanism to express their directional view
- Cryptocurrencies are net growing, so growth covers up all. This is particularly interesting, because it is turning zero sum games into non-zero sum games. But eventually they'll revert
- Separating them creates an adversarial dynamic, which actually creates healthy competition and leads to better alignment and progress for both teams

There hasn't been much public debate about what factors cause a fork to be zero sum or net positive. There are a number of factors that affect this and forks are not created equal. And I'd love to see more people write on this.

[4] Privacy norms in the US are the example I think of regularly. There are three mental models people tend to weight when thinking about how privacy norms are shaped.

1. The government dictates privacy norms
2. The people dictate privacy norms
3. A small subset of people have the power to structurally influence privacy norms, and these people are chosen by a process that is either non-correlated or anti-correlated with whether we'd want them deciding privacy norms

I think many of those reading (and maybe this is more a statement on the skew of who reads my writing and would get to the footnotes) would feel that (3) is the group with the most influence on privacy norms. These are people like Mark Zuckerberg, Evan Spiegel, Larry Page, and others at their companies (and the executives, friends, employees, and investors who influence them). These people are chosen by whether their companies became the dominant company in their space—a filter I think we can agree is not primarily based on their views on privacy. Or if it is, it likely skews towards them not being constrained by privacy concerns. Though many disagree, I actually think by and large these founders and companies have been impressively cognizant of the influence and responsibility they have over our privacy norms, considering they don't have to be. Of course, similar to the point above on China, perhaps we are underweighting the implicit contract and norm regulation that the people have over this group. As seen in the recent Facebook privacy woes.

Cryptocurrencies feel very similar to me. At some point this fork that has happened between the cryptocurrency world and tech world will re-merge. And when it does, some things that have won out in cryptocurrencies will become the architecture and the norms for important parts of our world. And we will look back and be thankful or rueful about how they were determined. I think if you ask anyone from the early days of internet and web protocol standards they'd have similar thoughts. Despite public rhetoric about the anarchical nature of crypto, I think many in the cryptocurrency

community are very thoughtful about the potential implications of these decisions. Balancing them is tough, predicting how they will play out is harder. But it's important work, and I'm glad to be able to witness how it plays out.

Tagged: crypto, forks, governance

‹ Understanding how Uber & Lyft Grow in Markets

Populism ›