Bitcoin Governance

nakamotoinstitute.org/mempool/bitcoin-governance

Pierre Rochard

July 8, 2018

First published on Pierre Rochard's Medium blog

Why do we care?

Bitcoin's governance matters because Bitcoin is the first successful, most liquid, and most widely known crypto-currency. In the words of Michael Goldstein, "Sound money is a foundational pillar of civilization, and Bitcoin restores this powerful tool for social coordination." If Bitcoin's governance model is flawed, it could prevent Bitcoin from reaching its full potential. If Bitcoin's governance is flawed, Bitcoin's stakeholders should work to fix it.

Conversations regarding Bitcoin's governance tend to focus on who the decision makers ultimately are, perennial candidates include miners, nodes, and investors. The purpose and mechanics of governance are often just implied or even disconnected from reality. Views on the efficacy of past governance are often driven by who "won" or "lost" a specific decision, rather than the adequacy of the decision making process itself.

What is Bitcoin governance?

Bitcoin governance is the process by which a set of transaction and block verification rules are decided upon, implemented, and enforced, such that individuals adopt these rules for verifying that payments they received in transactions and blocks fit their subjective definition of "Bitcoin". If two or more individuals adopt the same set validation of rules, they form an inter-subjective social consensus of what "Bitcoin" is.

What is the purpose of Bitcoin's governance?

There is a wide range of views regarding what the purpose of Bitcoin's governance should be. What outcomes should governance optimize for?

- Matt Corallo argues that trustlessness is the most important property of Bitcoin. Matt defines trustlessness as "the ability to use Bitcoin without trusting anything but the open-source software you run". Without the property of trustlessness, all other positive outcomes are jeopardized.

- Daniel Krawisz argues that maximizing the value of a bitcoin is what governance de facto optimizes for. Daniel states that “the general rule about Bitcoin upgrades […] is that upgrades which increase Bitcoin’s value will be adopted and those which do not will not.”

In the context of Bitcoin’s governance, these two views mirror the classic divide between deontological and consequentialist ethics respectively. I favor Matt’s deontological approach of focusing on trustlessness. Throughout monetary history, from ancient coin producers to modern central banks, trusting others to produce money has resulted in abuse of that trust. Compromising on trustlessness could help the Bitcoin price find a local maximum, at the expense of finding a much higher global maximum. Furthermore, there is no evidence that Bitcoin’s price has been correlated with upgrades to the Bitcoin protocol. Perhaps Bitcoin’s fundamental value is affected by upgrades, but Bitcoin is so illiquid and volatile that the price does not reliably reflect fundamental value. If we can’t observe the consequences of an upgrade on Bitcoin’s value, the consequentialist approach seems inadequate.

Before we can evaluate the current Bitcoin governance process against the stated goals of maintaining trustlessness or increasing the value of Bitcoin, we should attempt to define how the current Bitcoin governance process actually works.

How does the current Bitcoin governance process work?

The Bitcoin governance process maintains a set of verification rules. At a high level, this long set of verification rules covers syntax, data structures, resource usage limits, sanity checks, time locking, reconciliation with the memory pool and main branch, the coinbase reward and fee calculation, and block header verification. Amending these rules without tradeoffs is no easy feat.

Most of these rules were inherited from Satoshi Nakamoto. Some have been added or amended to address bugs and denial-of-service vulnerabilities. Other rule changes occurred to enable innovative new projects. For example, the new Check Sequence Verify opcode was added to enable new scripts.

Research

Every rule change begins with research. For example, SegWit began with research into fixing transaction malleability. Transaction malleability had become a serious issue because it prevented the Lightning Network from deploying on Bitcoin. Industry and independent researchers collaborated on what eventually became SegWit.

Critics have pointed out occasional disconnects between what researchers want to research, user expectations, and what is good for the network’s properties. Additionally, academic computer scientists prefer “scientific simulations” over “engineering experiments”. This has

been a source of tension in the research community.

Proposal

When a researcher has discovered a solution to a problem, they share their proposed changes with other protocol developers. This sharing could be in the form of an email to the bitcoin-dev mailing list, a formal white paper, and/or a Bitcoin Improvement Proposal (BIP).

Implementation

A proposal is implemented in the node software by the researcher(s) who proposed it, or by other protocol developers who are interested in it. If a researcher can not implement a proposal, or the proposal does not attract favorable peer review, then it will linger at this stage until it is either abandoned or revised.

While this may give the impression that the contributors to Bitcoin protocol development can veto a proposal, a researcher can make their case to the public and route around existing developers. In this scenario, the researcher is at a disadvantage if they lack reputation and credibility.

Another problem at the implementation phase is that the maintainers of the reference implementation will not merge in an implementation if it is widely seen as contentious by the Bitcoin protocol developers and the wider Bitcoin community. The reference implementation's maintainers have a deliberate policy of following consensus changes rather than trying to impose them. The C++ reference implementation, hosted at github.com/bitcoin/bitcoin, is the direct successor of Satoshi's codebase. It continues to be the most popular Bitcoin node implementation due to its maturity and reliability.

To circumvent the reference implementation's maintainers and make consensus changes regardless is as simple as copying the Bitcoin codebase and releasing the proposed changes. This happened with the BIP-148 User Activated Soft Fork (UASF).

A proposal to change validation rules can have a softfork or a hardfork implementation. Some proposals can only be implemented as a hardfork. From the perspective of pre-fork nodes, a softfork implementation is forward-compatible. With a softfork, the pre-fork nodes do not need to upgrade their software in order to continue validating the pre-fork consensus rules. However, these pre-fork nodes are not validating rule changes made by the soft-fork. From the perspective of pre-fork nodes, a hardfork is **not** forward-compatible. Pre-fork nodes will end up on a different network as post-fork nodes.

There has been controversy about the effects of hard and softforks on the network and users. Softforks are seen as being safer than hardforks, because they do not require an explicit opt-in, but this can also be seen as coercive. Someone who disagrees with a softfork must hardfork to reverse it.

Deployment

Once implemented in the node software, users must be persuaded to use the node software. Not all node users are equal in their importance. For example, “blockchain explorers” also have more power as many users rely on their node. Additionally, an exchange can determine which validation rule set belongs to which ticker symbol. Speculative traders, large holders, and other exchanges provide a check on this power over ticker symbols.

While individual users may signal on social media that they are using a certain version of node software, this can be sybil attacked. The ultimate test of consensus is whether your node software can receive payments that you consider to be bitcoins, and you can send payments that your counter-parties’ node software considers to be bitcoins.

Softforks have an on-chain governance feature called BIP-9 Version bits with timeout and delay. This feature measures miner support for softforks on a rolling basis. Miner support for proposals is used as a proxy measure for the wider community’s support. Unfortunately this proxy measure can be inaccurate due to mining centralization and conflicts of interest between miners and users. On-chain “voting” by miners also perpetuates the myth that Bitcoin is a miner democracy, and that the miners alone decide on transaction and block validity. BIP-9 is useful to the extent that we recognize and accept the limitations of proxy measurements.

Enforcement

Changes to the validation rules are enforced by the decentralized p2p network of fully validating nodes. Nodes use the verification rules to independently verify that payments received by the node operator are in valid Bitcoin transactions and are included in valid Bitcoin blocks. Nodes will not propagate transactions and blocks which break the rules. In fact, nodes will disconnect and ban peers which are sending invalid transactions and blocks. As StopAndDecrypt put it, “Bitcoin is an impenetrable fortress of validation.” If everyone determines that a mined block is invalid then the miner’s coinbase reward + fees is worthless.

The role of miners is to provide a time-stamping function secured with proof-of-work. The amount of hashrate provided is based on the cost of hardware and electricity on one hand, and revenue from the coinbase reward + fees on the other hand. Miners are mercenaries, and in the past they have provided their time-stamping function without full rule validation. Due to mining centralization, miners can not be trusted to enforce the validation rules on their own.

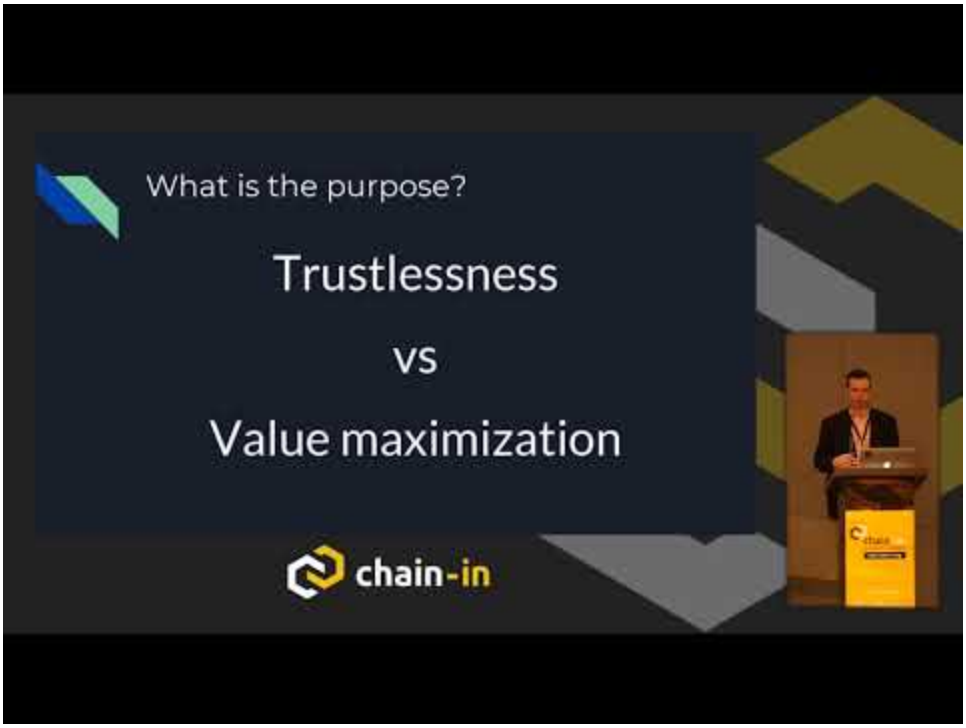
Has the current Bitcoin governance model resulted in more trustlessness?

In my opinion, the current Bitcoin governance model has prevented a degradation of trustlessness. The dramatic increase in on-chain Bitcoin transactions over the past 5 years seemed to have no end in sight. If Bitcoin's governance model had not been resistant to last year's miner signalling for a doubling the maximum block weight, a precedent would have been set of valuing transaction throughput above trustlessness.

Has the current Bitcoin governance model resulted in upgrades that increase Bitcoin's value?

I think it's impossible to establish a causal relationship. The price is much higher than it was 2 years ago, but it seems to be an endogenous process driven by trader psychology, not technological fundamentals. Regarding fundamentals, it's undeniable that Bitcoin's governance has delivered on consensus changes which the Lightning Network depends on to operate. I've been experimenting with establishing channels and making Lightning payments: there is no doubt in my mind that LN increases Bitcoin's value.

This post is based on my speech at the Chain-In conference:



Watch Video At: https://youtu.be/yzQ4OPjPPP0

Read in Russian

Back to the Memory Pool