The Post-Satoshi Manifesto

Eric Lombrozo

April 13, 2015

Introduction

Ever since a pseudonymous inventor known to the world as Satoshi Nakamoto published a seminal white paper[1] in 2009 on a peer-to-peer money transfer system using a remarkable new invention called a blockchain, there has been incredible excitement surrounding the possibility of creating global payment networks without the need for central currency issuers or central trusted authorities. Bitcoin has been born.

Six years later, this experimental network is still in operation. An entire user community, along with currency exchanges and merchant services, has sprung up around it. However, there is a very uncomfortable truth that underlies the present situation: the technology being presently used in this network has lagged behind the current state-of-the-art in theoretical understanding. Many mistakes or oversights in the original design including a number of issues that significantly hamper adoption efforts have been identified, yet very few have been corrected. This isn't so much for lack of awareness of these new developments by the core developers nor their lack of effort. Instead, it is mostly due to the fact that incorporating many of these ideas into the existing Bitcoin network is all but impossible given the current development process, as we shall see below.

Other projects have sprung up including basic theoretical research as well as new experimental networks and commercial undertakings. In these last six years, many new ideas have arisen in this space. It is a very quickly growing area of academic research and continues to receive a significant amount of investment capital. With the benefit of hindsight and new insight, it is becoming clear that the Bitcoin network is headed towards obsolescence if we don't change course. At the time of this writing, a significant part of the community remains in denial of this uncomfortable truth. However, the study of economically incentivized decentralized consensus networks is still in infancy. The greatest breakthroughs are yet to come. It will only get harder and harder to deny this as time goes on.

I do not pretend to have solutions to all the issues faced. I only claim to have identified a few serious problems that are plaguing development efforts and offer humble guidance in the hope that together we can all collaborate in solving

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"

them. In this vein I propose a three point agenda, each point progressively a harder problem to solve than the previous one.

Core Development Agenda

1. Clearly distinguish the network from the protocol from the currency.
2. Create a workflow for protocol evolution that more closely resembles Git.
3. Develop an open, transparent process with proper incentives to promote the development of candidate replacement protocols along with a mechanism for smooth transitioning.

I shall explain each one of these in turn...

1 Distinguish Network, Protocol, and Currency

Currently, the term "bitcoin" refers to several very different things. A convention commonly used is for capitalized "Bitcoin" to refer to the protocol, network, or community while an all-lowercase "bitcoin" refers to a unit of the currency. While these distinctions are pretty clear to those most heavily involved in core development, it is far from clear to most laypeople as well as many of the newer or less technically-inclined community members. Distinguishing these three things is crucial for at least three reasons:

- It is possible to fork a network and create a new currency while still using the same protocol (a phenomenon known as "altcoins").
- A single network can, in principle, support multiple currencies or multiple protocols.
- Most importantly, close association between the currency and the protocol has led to a serious conflict of interest (with bitcoin as well as other cryptocurrencies) as large stakeholders of the currency have pumped its value without any real forethought regarding the existing protocol and network's limitations. This has led to unrealistic promises made to the general public, speculators, and investors and has led to painful bubble-bust cycles and market manipulation.

It is proposed here that we continue using the term "bitcoin" to refer to the unit of currency but that we adopt the term "Satoshi protocol" for the protocol itself. The network, the actual interconnected computers used to transact in bitcoins, can continue to be called the "Bitcoin network" as it is very highly coupled with the currency at present, but this could conceivably change in the future.

The distinction between the protocol and the currency is by far the most crucial of all, so I would highly discourage the continued use of the terms "Bitcoin protocol" and "Bitcoin core development" in the context of core research and development - and especially in the context of funding it. There might be at any given time one Bitcoin protocol but many candidate protocols vying to replace it. Decades of incredible technological progress in computing technology have given us clear precedent: attaching anything to a single protocol means that thing will die when the protocol is inevitably replaced by a next-generation technology. I see no reason to believe blockchain protocols are an exception.

Protocol research should be carried out on test networks using test tokens, freeing up developers to experiment without risk of serious economic repercussions. The current core development process employs the use of a common testnet as well as several private ones. Currently, the common testnet's main purpose is to test software changes that are intended to be deployed to the mainnet, the network where real bitcoins are transacted. We need not just one common testnet - we need many of them trying out many different concepts and ideas in parallel so the entire community can participate in evaluating them.

Many of these testnets might turn out to be terrible, but without a healthy culture of free experimentation it is unlikely we'll be able to achieve any significant breakthroughs. Since protocol research, design, implementation, and testing are the very essence of core technological research and development in this space, it is crucial that these activities be able to go on without the corrupting influences of real currencies and markets. However, the need to run tests using real economic incentives poses considerable challenges which we'll revisit further ahead.

2 The Need For A Nonlinear Workflow

The second major issue is the fact that blockchains grow linearly but complex ideas and codebases do not.

The most commonly used version control system for software development is Git, a distributed revision control system initially designed by Linus Torvalds for Linux kernel development[2]. One of its key features is support for distributed nonlinear workflows. What this means is that multiple people can fork a project, independently make changes on their own computers, and then merge their changes back into the original project. The current Satoshi protocol's core software development process uses this tool almost exclusively for all source code contributions and updates.

While great for evolving complex ideas and codebases, such nonlinear workflows pose a significant challenge: forks are trivial, however merges are hard. Merges require a considerable amount of human time and effort to ensure they accomplish their stated objective without breaking something else. This means that in practice, code review is the biggest bottleneck in core development. Nonetheless, Git supports high-level tools to simplify the merge process considerably. There's a far more serious but analogous issue at play, as we shall now see.

In the case of blockchains, forks are also trivial. However, merges are not just hard - they are impossible! One of the most remarkable features of Satoshi's invention is objective verifiability. Objective verifiability means that once connected to the network, everyone will eventually come to agree on the exact same history of the network by using well-defined rules they can check for themselves. However, this construction means that it is impossible to objectively decide between two blockchains that use different rules. Therefore, taken to the extreme, this means the rules are essentially fixed for all time. We cannot merge any new consensus rules without breaking the network. This is the main obstacle to real technological innovation and the underlying reason the Satoshi protocol has been unable to keep up with the latest theoretical developments and ideas.

We need to relax the requirement of extreme objective verifiability and accept that ultimately, merges will require human coordination and human decisions...rules that cannot be preprogrammed into the software.

[2]Wikipedia Article on Git

NOTE: The sidechains project[3] shows promise in enabling the transfer of value tokens between different blockchains. This would allow experimentation with different blockchain ideas in parallel without the need to introduce an additional currency and without the need to merge new consensus rules into other blockchains. Sidechains are a potentially powerful tool for making technical protocol enhancements such as structure optimizations and support for more powerful scripts. However, I am not yet convinced that they will offer sufficient economic flexibility to be of general use in experimentation with economic incentives and economic security models.

[3]Back, Corallo, Dashjr, Friedenbach, Maxwell, Miller, Poelstra, Timón, and Wuille, "Enabling Blockchain Innovations with Pegged Sidechains"

3 Incentivized Protocol Evolution

If we cannot objectively decide on a blockchain branch along with its corresponding development workflow branch by following predetermined rules, what decision process do we take?

The implication is that decisions on protocol upgrades and replacements will generally involve subjective human judgment. Different opinions will exist over the merits of different approaches. In some cases the arguments will be based on technical merits, in others on economic consequences. In some, it will come down to a matter of personal taste.

With the current development process, only arguments over the technical merits are common. Quite understandably, none of the core developers feel they have the authority to impose any changes on the network that entail significant economic consequences. However, economic reality has changed significantly since the 2009 Nakamoto white paper leading to a greater and greater misalignment of incentives for network participants. Among these are the concentration of mining power and the centralization of blockchain databases. The security model behind the Satoshi protocol rests on certain economic assumptions that many no longer believe to be true.[4] [5] [6] In addition, many believe it is possible to achieve a greater level of economic security with even greater speed and scalability potential than the Satoshi protocol allows without sacrificing decentralization.[7] [8] [9]

Testnets need to be able to experiment with different economic incentives and economic security models. In order to try out some of the existing scalable economic security proposals based on game theory[10], it will be necessary to create artificial economic incentives in testnets. This is a challenging problem. I can perhaps offer the start of a suggestion inspired by a recent conversation I had with Vitalik Buterin: testnets should set expiration times where the experiment is terminated and all tokens are exchanged for something of value, possibly tokens in a different network, possibly something physical. That way, we can subsidize the experiment and test real economic parameters while containing any potential damage that would result were these tokens to become perpetually tradeable assets on a flawed testnet that no longer has any developer support. Since the exchange rate can be predetermined, this avoids some of the worst pitfalls leading to market manipulation and fraud. I believe this idea is a great start, but it clearly needs a lot more work.

The most profound and significant improvements to the protocol almost invariably involve hard forks - rule changes that are not backwards compatible

[4] Ittay Eyal and Emin Gün Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable"

[5] Nicolas T. Courtois and Lear Bahack, "On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency"

[6] Lear Bahack, "Theoretical Bitcoin Attacks wth less than Half of the Computational Power"

[7] Jae Kwon, "Tendermint: Consensus without Mining"

[8] David Mazières, "The Stellar Consensus Protocol"

[9] Yonatan Sompolinsky and Aviv Zohar, "Accelerating Bitcoin's Transaction Processing"

[10] Vitalik Buterin, "Notes on Scalable Blockchain Protocols

with older versions of the software. As noted in the previous section, hard forking changes are basically impossible to do right now without breaking at least some of the network. They require coordinating new version deployments to ensure that all network nodes are running the latest version of the software by the time the rule changes take effect. Some hard forks are even harder because they require not only updates to the core consensus software but also considerable retrofitting of many existing applications. Therefore, essentially no such changes are ever made, even in situations where there's unanimous consensus among the core developers that it would be a substantial improvement if only there were a practical way to do it.

We need an open, transparent process for subsidizing the development of new candidate protocols as well as a way to agree on which of them should replace the current protocol. In addition, we need a mechanism to ensure smooth transitions with minimal disruption to deployed infrastructure. As decisions involving rule changes must be made that require community-wide consensus, this process is necessarily political.

Any political process, much like any engineering project, involves difficult trade offs. Much more discussion on this topic is needed before we arrive at a workable, acceptable solution that serves the common good and remains sufficiently decentralized. I shall avoid attempting a solution to this problem here, only noting that any such solution is likely to require a public update schedule allowing all network participants sufficient time to voice objections, make counterproposals, vote on candidates, and upgrade their software before any hard forking rule changes come into effect.

Of the three issues listed, this one is by far the hardest to get right and also the easiest to get horribly, horribly wrong.