A Summary and Reponse to “On Scaling Decentralized Blockchains (A Position Paper)”
(*Croman et al, 2016, “C3 - The Initiative For Cryptocurrencies & Contracts”*)
https://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf
Bryant Hagadorn
2/3/2019

Summary:

In the wake of a rising awareness of many cryptocurrencies at the time and a growing problem in the community around the scalability and transaction costs on the Bitcoin blockchain, the authors attempt to address at a high-level many ideas surrounding two fundamental ways to change the blockchain: *Bitcoin Improvement Proposals* (BIPs), a community discussion democratically operated, and *Blockchain forks* (where a large group with two or more of the same blocks mined decide to continue the chain, leaving it backwards-compatible (soft) or with a new set of rules (hard)).

While the authors don’t dive into the detailed specifics of any trending BIPs (besides a few mentioned in groups) or forks, they support their position for improvements of scalability, which as they mention is, “not a well-defined, singular property of a system”, by separation of concerns into three logically sequential parts:

1. **Measurement study and exploration of reparameterization** - A set of classical definitions and experimental measurements of those definitions, using worst and best case scenario. Some are fundamental proving that the current Bitcoin transaction time is an ideal time indeed, while others point out that 57%, at the time of the writing, of the cost of throughput on the network is spent on electricity alone.
2. **Painting a broad design space for scalable blockchains** - Here the authors argue that changing block size and block interval, or even the use of something like Corallo’s Relay Network (which spreads information to low-latency miners globally), aren’t effective solutions and that “fundamental protocol redesign is needed for blockchains to scale significantly while retaining their decentralization” A broad design is laid out with respect to five different planes: Network, Consensus, Storage, View, and Side.
3. **Posing open challenges** - The authors present an articulated view for understanding bottlenecks that accompany scalability and design of more scalable blockchain systems. It dives deeply into the aforementioned difficulty in defining what exactly scalability means for blockchain system, citing used and unused (but could be) metrics, fairness, trust, and ultimately the question “to what extent can we push system parameters without sacrificing security”. This important question doesn’t become a continual theme until now, and seems to be the important distinction in open challenges and questions about scalability.

The authors do a thorough job of starting with a narrow and well-known focus, current metrics and exploration into their definition along with experimental analysis of different metrics in a hypothetical scenario. Moving broader, the authors then present a lexicon for discussing

the different aspects for the current and any future designs using planes, to frame the discussion and position. After defining their use of the terminology, the authors make an opinion about what is and isn't possible, starting with basic logistical short-term suggestions and ending on more fundamental and diametrically opposed philosophies, such as the extent of centralization a system could take on.

Response:

While the summary of this paper previously certainly has its objective opinions, the goal of my response will be to tie a modern perspective into this fundamental paper. Three years proves how long it can be in the world of blockchain and technology in general, the Bitcoin ledger was only seven years old at the time of this release and now at ten years, it's amazing how the true fundamentals of blockchain technology have been removed from their cryptocurrency roots (not to discredit them) in 2019, as well as how predictive of the future this paper could be considered. With that theme, I'll discuss a few parts I find particularly parallel to the state of blockchain today.

One of the key fundamentals of Hyperledger Indy, an identity layer of blockchain, around Hyperledger is the ability and concept of "microledgers". In this paper, one of the essential planes is the "Side Plane", which allows off-the-chain consensus. At the time, Bitcoin Lightning was referenced, but the new term "microledger" has been dubbed inside of the Decentralized Key Management System (https://github.com/hyperledger/indy-sdk/blob/677a0439487a1b7ce64c2e62671ed3e0079cc11f/doc/design/005-dkms/DKMS%20Design%20and%20Architecture%20V3.md#43-microledgers) and inside of the Hyperledger Indy system. The Side Plane is criticized in the position paper in Bitcoin Lightning for its centralization of routes and topology, which undermine the privacy and security concerns that decentralization helps solve, but praised for its performance. To date, the DKMS architecture and the ideals around having 99% of data being done off-ledger in microledgers are still major concerns. The Hyperledger Indy Agent protocol is still evolving for future-proof of microledgers, and while there might be private implementations that solve this for their use-case specific cases, it remains largely still unsolved to the general open-source public. One of the key important aspects concerning the tradeoff between scalability vs. privacy and security is perhaps the *use-case specific implementation*. For example, a system of IoT sensors measuring water flow for a utility company don't need the guarantees of security or privacy that might accompany an IoT device that transmits financial information from a point-of-sale system for a large retailer and thus can make tradeoffs and risks. However, the past three years haven't proven to be entirely lost and much of the work around consensus has drastically changed the scalability problems pointed out.

Hyperledger and the general blockchain technology community has many areas where the author's position on the Consensus Plane (message input that determines transaction outputs) has matured or issues have largely been addressed. The authors argue for improving proof-of-work protocols and have many merits to their arguments, such as the replacement of "longest-chain" rules to something like the GHOST protocol. Ethereum ended up adapting something similar called the Inclusive protocol, (http://www.cs.huji.ac.il/~yoni_sompo/pubs/15/inclusive_full.pdf), which uses randomness to

break up ties rather than uncles. Here we can see how Ethereum does so with Golang code (https://github.com/ethereum/go-ethereum/blob/f3579f6460ed90a29cca77ffcbcd8047427b686b/core/block_validator.go#L225):

```
expd := CalcDifficulty(config, header.Time.Uint64(), parent.Time.Uint64(), parent.Number, parent.Difficulty)
```

Beyond improving proof of stake, like has been done and suggested, the entire concept of Proof of Stake or Proof of Elapsed time has been scrapped in favor of other solutions. Hyperledger Indy introduces the concept of a Redundant Byzantine Fault System (seen in Hyperledger Indy-Plenum). Here's a brief summary provided graciously by the contributors

> *"RBFT implements a new approach whereby multiple instances of the protocol run simultaneously, a Master instance, and one or more Backup instances. All the instances order the requests, but only the requests ordered by the Master instance are actually executed. All nodes monitor the Master and compare its performance with that of the Backup instances. If the Master does not perform acceptably, it is considered malicious and replaced."*
> (https://github.com/hyperledger/indy-plenum/wiki)

This is an area where blockchain has changed dramatically from even its analysis in 2016 to now, specifically around use cases (this one being services). "Permissioned" blockchains, as they are now called, are helping to solve the Consensus Plane problem and the scalability by placing in root layers of trust such as the Sovrin network. While not all of the answers are solved, it's great to see the scalability issues solved when they can be by use case.

TLDR: While I have many more thoughts and reactions that I could add here, I think using the stark contrast of thinking over the past three years in blockchain technologies around scalability has changed or narrowed its approach with use cases. The problems the authors present are not completely solved, but hopefully I have shown that Hyperledger specifically has advanced our understanding and heavily taken into account the accurate and great points made by the authors.