Summary of Beyond Bitcoin

Tim Sigl

Bonneau et al. state in *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies* that there are three fundamental design decisions when it comes to implementing a blockchain. The first one is Transaction & Scripts, the second one is Consensus and Mining, and the last design decision with the least potential for innovation is the Peer-to-peer Communication Network. Modification of the Bitcoin network can be implemented as hard forks, soft forks or replay policy updates depending on employed changes. Some altcoins are just hard forks of Bitcoin with different parameters for block time and block size. Alternative design ideas by the authors for the consensus protocol are a non-deflationary coin scheme, asic-resistant puzzles, useful puzzles, proof-of-stake or designated authorities as trusted node. Anonymity and privacy of Bitcoin can be improved by peer-to-peer mixing, distributed mix networks or SNARKs.The authors conclude that it is still unclear which deviations are desirable, because new design ideas are tested best in a real blockchain network. According to them it is unknown if Bitcoins success is due to its specific design or just due to their first-mover advantage. The paper does not raise any new ideas or models. But this shouldnt be expected since it is only a Systematization of Knowledge paper. From my personal point of view the paper gives a good summary of different techniques and design decisions on how to change Bitcoin. The only odd design decision mentioned in the paper is the use of designated authorities because it seems contradicting to the idea of decentralization.

Croman et al. assume in *On Scaling Decentralized Blockchains: A Position Paper* that the max. block size is 4MB if the transaction should reach at least 90% of the nodes. The lower border for the block time is 12 seconds with a block size of 80KB. They state that changing just the parameters of Bitcoin will not grant significant speed-ups. A fundamental protocol redesign is necessary for future-proof scaling. Especially block time and block size should not be adjusted to extreme levels because lower powered miners with less bandwidth could be disadvantaged. The authors rethink the design of a block chain on five different planes. In the network plane the transaction processing is one of the bottlenecks for slowing down the tps of the network. The second plane is the consensus plane which can be adjusted the most. Bitcoin suffers from the tradeoff between consensus speed, bandwidth and security. This problem can be eliminated by changing the chain selection rule or by using an alternative consensus protocol like proof of stake. Other ideas include sharding, side chains or a small consortium of trusted entities. On the storage plan they suggest to shard the storage of the UTXO or to use distributed hash tables. They also present a view plane which is used for splitting up the state of the blockchain in different views for different stakeholders / nodes. The last plane is the side plane in which they suggest using off-chain transactions to remove congestions of the main network. They conclude reparametrization of Bitcoin's parameters is only a first step towards a blockchain with more throughput. In my mind the paper gives a very good overview of different scaling options. Especially the adjustments to the consensus plane including sharding and side chains seem promising.

In the last paper *A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective* Yue et al. are constructing use-cases for blockchain technology in 5G

and other future mobile networks. They are motivated by third parties like cellular providers who could abuse their power to forge, censor or trace back transactions. Also new features like spectrum sharing or network slicing could be incentivised or orchestrated by blockchain technology. Smart contracts could be used to automate contracts between users and centralized authorities to clarify and simplify contracts. The authors identify nine modules of blockchain infrastructure. 1. The identity management which allows users to stay anonymous, 2. program development which defines the implementation of the blockchain 3. digital asset creation, 4. information propagation, 5. block proposal, 6. block verification, 7. block confirmation, 8. blockchain access and lastly 9. blockchain storage. Different paradigms for blockchain namely permissionless, private and consortium based blockchains should be used depending on the requirements of the application. The authors conclude that blockchain technology has potential in every application that relies on trusted third parties. They highlight the advantages of blockchain when it comes to decentralized trust, automation and flexibility with smart contracts. Overall the survey opens the mind for new use cases for blockchain and shows the potential for incentivisation of shared spectrum and other network specific requirements.