Beyond Bitcoin

Lars Erik Wik

February 8, 2022

Summary

Bitcoin — along with other cryptographic currencies — are way ahead of theory in that they seem to work in practice, but are lacking a theoretical foundation to support them. Joseph Bonneau et al. [1] tries to convey why Bitcoin is worthy of research, by laying out open questions for the research community to tackle. We simply cannot rely on the fact that Bitcoin has worked up until now, therefore it will continue to do so in the future.

A worrying concern to the future of cryptographic currencies, is whether or not they're scalable in relation to the rapid increase in their popularity. Kyle Croman et al. [2] analyzes how Bitcoin is limited in its ability to gain a sufficient transaction throughput in comparison to mainstream payment processors such as Visa. They show that adjusting parameters — such as block- size and intervals can help improve the throughput to some extent, but that we'll eventually have to rethink the protocol design.

Another reason to why cryptographic currencies are worthy of research, is that the underlying technology — blockchain — can turn out to be useful in other research areas. E.g. Keifen Yue et al. [3] discusses how blockchains and smart contracts can be used to handle spectrum sharing between operators in mobile broadband networks. A blockchain can keep track of users' shares without the need for a third party. Additionally shares can be rented through smart contracts.

References

[1] Joseph Bonneau et al. "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". In: *2015 IEEE Symposium on Security and Privacy*. 2015, pp. 104–121. DOI: 10.1109/SP.2015.14.

[2] Kyle Croman et al. "On Scaling Decentralized Blockchains - (A Position Paper)". In: *Financial Cryptography Workshops*. 2016.

[3] Kaifeng Yue et al. "A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective". In: *IEEE Communications Surveys Tutorials* 23.4 (2021), pp. 2191–2217. DOI: 10.1109/COMST.2021.3115797.