CRYPTOCURRENCY: RESOLVING SPLITS AND FORKS ON THE BLOCKCHAIN

A Research Paper submitted to the Department of Computer Science
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

David Gray

April 27, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISOR
Daniel Graham, Department of Computer Science

Cryptocurrency: Resolving splits and forks on the blockchain

CS 4991 Capstone Report, 2022

David Gray
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
dg9hm@virginia.edu

Abstract

Cryptocurrency is a technology that relies on a large collective of people agreeing on everything in order to have the technology move as smoothly as possible. Given that it is unlikely that everyone involved will always agree, this causes disagreements, known as forks and splits, which need to be resolved quickly in order to facilitate a good technology. Through my meta study of the various ways on resolving these differences on the blockchain I found various benefits and detractors. These include: Ethereum's usage of uncle blocks to resolve splits improves the security of the blockchain and in a fork just giving everyone a dividend of the forked currency allows the new currency to truly not rely on the original. Future work should include a study of any blockchain that implements the suggested resolutions, and possibly the implementation of that type of blockchain.

1 Introduction

In 2007 and 2008, there was a global market crash due to a housing crisis caused in part by central banking. This led people to question whether or not a central authority can be trusted, in answer to which decentralized currency in the name of cryptocurrency was introduced. With the lack of a central authority, deciding which transactions are valid then needed to be left up to the collective. When bitcoin was released, the white paper, written by Satoshi Nakamoto, went into detail outlining a process for coming to a consensus with the collective. However he does implicitly recognize there can be multiple versions of the blockchain, which is now known as a split [2009]. This consensus was provided by the longest chain rule, stating that the version of the blockchain with an absolute majority consensus is the true blockchain.

Since this initial idea was released for cryptocurrency and the blockchain, there have been various implementations since, including Ethereum. In the Ethereum white paper, this resolution was called into question, stating that the resultant splits lead to wasted blocks that could be used to secure the blockchain [Buterin 2013]. The second issue about cryptocurrency that was discovered soon after was the idea of a fork, where a cryptocurrency's codebase was mostly agreed upon, save a few key components. A notable example of this is Bitcoin Cash, a fork caused by increasing costs and decreasing reliability of Bitcoin that was resolved for this currency by increasing the block size. According to the Bitcoin Cash website, anyone who held Bitcoin at the time of the fork also automatically owned Bitcoin Cash [Bitcoin Cash 2017]. This poses questions of how to resolve the idea of possibly spending both the Bitcoin and Bitcoin Cash now owned by the same person.

2 Review of Research

Research in the area of cryptocurrency splits and forks is limited due to the age of cryptocurrency being less than 15 years. However some good studies within certain currencies do exist. The more comparative works more come from whitepapers on alternative cryptocurrencies, such as the aforementioned Ethereum whitepaper. It goes into depth explaining why their system of using "uncle" nodes is important for security while cutting waste, and it compares their protocol to the Bitcoin method of not using alternative chains at all [Buterin 2013]. Clearly that report is biased in favor of Ethereum rather being than an

objective study on split resolving methods, and there is no mention of forking the cryptocurrency.
A noteworthy study of Bitcoin splits comes from the Karlsruhe Institute of Technology in Germany, which discusses how splits occur and how they are resolved within Bitcoin [Neudecker and Hartenstein 2019]. Neudecker focuses solely on Bitcoin splits, and does not delve into other cryptocurrencies such as Ethereum and Bitcoin Cash for discussing other methods for resolving splits and forks.

3 Research Design

There are a number of ways employed in the meta study in order to determine how to best resolve splits and forks in a blockchain. The primary method used will be case studies of how various cryptocurrencies differ using their white papers' explanation as to why their method is best or how they chose to fork the cryptocurrency from the parent. The documents are biased as they say their method is the best; so a secondary approach used will be to incorporate other more objective research on why certain cryptocurrency split and fork resolving methods are better or worse in certain areas.

3.1 Cryptocurrencies to study

The cryptocurrency white papers that will be analyzed for this report are Bitcoin, Ethereum, Bitcoin Classic. These three were carefully selected for a multitude of reasons. Bitcoin was selected because it was the first cryptocurrency to exist, and therefore set the standard of how splits should be done. Ethereum was selected since this cryptocurrency came out as a critique of a few design choices of Bitcoin, including how they resolved splits. The last selection, Bitcoin Classic was chosen as this cryptocurrency is a hard fork from Bitcoin, a cryptocurrency already analyzed in this paper, and this fork is well documented in a white paper unlike other Bitcoin forks, such as Bitcoin Cash.

3.2 Specifics of the currencies

Bitcoin was the first cryptocurrency ever, so the creator was tasked with developing a method of resolving these splits. Nakamoto chose to use an approach of having proof of work decide when any particular block gets mined, which involves using a lot of CPU power to generate a random number using transaction information and the previous block less than a target value. This is a difficult task and Nakamoto decided that whoever got a desired number would go onto the blockchain. These blocks would be verified over time by other miners and then over time a longest chain of verified blocks would emerge. This longest chain was considered to be the valid chain, and that is how splits are resolved [Nakamoto 2009].

Ethereum was created in 2013 in response to design limitations within Bitcoin, namely in other chains are wasted computations. The Ethereum white paper argued that those computations can be used in the form of the Greedy Heaviest Observed Subtree, in which the other chains are used in what is considered to be the longest chain. This protocol will use the fact that splits exist to its advantage for higher security in the blockchain. These will compare blocks that have been split off recently, known as uncles, to validate the longest chain's transactions. This is because if the longest chain has some transactions, then uncles should have the exact same transactions somewhere in their respective chains. Any uncle blocks used in the mining of the longest chain receive a portion of the reward as an incentive to mine these blocks as well as the longest chain. The white paper argues that this will increase security as a chain with multiple uncles would be more likely to be mined than an attacker who has no uncles on their chain [Buterin 2013]. There was a paper published to study uncle blocks on miners, and ultimately, the paper concluded that this was good for individual miners and the whole block chain as computations were not wasted and everyone who contributed to uncle blocks still got a reward [Ritz and Zugenmaier, 2019].

Bitcoin classic is a fork of the Bitcoin blockchain that occurred in November of 2017. This fork occurred due to Bitcoin design choices a large group of the community did not agree with, namely the mining speed, the total supply, and block size. Once these differences became irreconcilable, a group founded Bitcoin Classic, which is a hard fork off of the Bitcoin blockchain. Everyone who owned any bitcoin on

November 24th, 2017 also owned the amount of Bitcoin Classic matching this value. There were two ways they could have done this split: 1) either give everyone Bitcoin Classic as a gift in relation to how much Bitcoin they owned, so they would own both, or 2) implement a way to require that owners only spend either Bitcoin or Bitcoin Classic. The former was chosen out of simplicity and because this approach made it possible to completely separate from that point on from the Bitcoin blockchain.

4. Results

For splits on the blockchain, the main differences between Bitcoin and Ethereum is whether or not to include uncle blocks. For simplicity, not including uncle blocks would reduce computation time and just require miners to only focus on the block they are mining and direct ancestors, not ones related to the ancestor.

Including uncle blocks, however, has more benefits, namely that miners are not using up computing resources to be beat by someone who may have gotten lucky on the random number generation. It also increases security since those other uncle blocks can be used to validate the longest chain [Buterin 2013]. The benefits of uncle blocks do not stop there, since this also provides an incentive to mine, even without as much computing power. Even if one does not mine on the longest chain, having that adjacent chain will yield a reward [Ritz and Zugenmaier, 2019]. For these reasons, the inclusion of uncle blocks has more benefits than detractors rather than not including uncle blocks, and thus cryptocurrencies overall would benefit from including uncle blocks in their cryptocurrencies.

On the subject of forks, the Bitcoin Classic fork was very similar to how Bitcoin Cash fork. In issued the relative amount of the new currency in relation to how much of the currency they forked off of without inclusion of checking to see if someone is attempting to spend both Bitcoin and the forked cryptocurrency. This was a necessary choice, and why this has been the only noted way of forking from the cryptocurrency. In order to truly remain separate from the original currency, it is important to have separation be permanent between the currencies. This allows for example Bitcoin Cash to grow to be a currency in their own right, rather than something that is constantly depending on Bitcoin.

5. Conclusion

In the current times, cryptocurrency is all over the world, with many implementations to get to the common goal of having a decentralized electronic currency. The work in developing these is no where near over, and therefore many facets of cryptocurrency need to be analyzed in order to see which design choices are worthwhile. Splits and forks were a natural start, as this was the first thing other designers had to decide too. Hopefully this provides a framework to analyze other features in the future.

6. Future Work

Cryptocurrency has many other design features that need to be analyzed. This technology is a culmination of a lot of computer science fields, including cryptography, networking, programming language design, and many others. These features should be analyzed relative to how important it is to the currency itself. For example, in this report splits were analyzed based on a Proof of Work model, where miners generate random numbers to prove their block of transactions is legitimate. However there is an alternative Proof of Stake model that Ethereum is switching to, where the proof that a block is legitimate comes from miners putting money on a block saying it is correct [Buterin 2013].

Another feature that needs to be analyzed is the scripts that are attached to transactions. These scripts are primarily to validate the people who are attempting to spend the cryptocurrency. However Ethereum decided to expand the scripting language to be able to do everything any other programming language can do, unlike Bitcoin scripts which are limited in actions [Buterin 2013]. These are just two features that can be further examined within cryptocurrency. It is important to note this is not an exhaustive list.

Technically, cryptocurrency is a wonderfully constructed technology, and when its features are analyzed impartially, it can lead to improvements within the technology. When these analyses are done, afterward the work is on the individuals tasked with maintaining cryptocurrencies to either improve the

existing blockchain with improvements suggested by papers, or to fork from a given blockchain with these improvements.

References

[1] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved February 23, 2022 from https://bitcoinwhitepaper.co/

[2] Vitalik Buterin. 2013. Ethereum Whitepaper. Retrieved February 23, 2022 from https://ethereum.org/en/whitepaper

[3] Bitcoin Cash. 2017. The History of Bitcoin Cash. Retrieved February 23, 2022 from https://bitcoincash.org

[4] Till Neudecker, Hannes Hartenstein. 2019. Short Paper: An Empirical Analysis of Blockchain Forks in Bitcoin. In *Financial Cryptography and Data Security*. *Institute of Telematics, Karlsruhe Institute of Technology, Germany, 9 pages.* https://link.springer.com/chapter/10.1007/978-3-030-32101-7_6

[5] F. Ritz and A. Zugenmaier, "The Impact of Uncle Rewards on Selfish Mining in Ethereum," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2018, pp. 50-57, doi: 10.1109/EuroSPW.2018.00013.

[6] Bitcoin Classic Foundation. 2017. Bitcoin Classic Project Whitepaper. Retrieved March 16, 2022 from https://bitcoin-classic.org/Bitcoin-Classic-Whitepaper.pdf