Analysis of hashrate-based double-spending

Rakesh Gopinath Nirmala Arunakumari Yedurupaka

I. Motivation

Bitcoin is the peer-to-peer cryptocurrency based on transactions, blockchains and hash calculations originally explained by Satoshi Nakamoto. It provides greater degree of anonymity, safety reducing the dependency on third parties (banks). However, it lacks to shed enough light on the quantitative variables such as the wait-time, hash-rates of different entities, probabilities of success or failure involved and their relation to double-spending attacks. This has led to the perplexing perceptions and myths. This paper builds on Satoshi's work, clears the air of confusion and presents some interesting observations that dispels the various myths. It also analyzes the economics of double-spending attacks.

II. Contributions

The major contributions of the paper is it provides a more formal and detailed analysis of the various quantitative aspects of Bitcoin, the effect of these variables on the double-spending attack thereby invalidating the various myths and misconceptions. It also models the economics of double-spending attack, elucidates the various cost factors involved and the trade-offs between them and formalizes an equation to determine the profitability of the attack through a stochastic process. The author through the profitability equation also points out the safe state for the merchants.

III. Solution

The author explains that the Hashrate-based double spending attack is a process in which the attacker and the honest network, each with their own relative hash rates, competes to extend their blockchain (longer blockchain with most proof-of-work is accepted) using the concept of discrete-time Markov chain. The success of the attacker depends on winning over the honest network. Successful attack can be carried out with any attacker hashrate eliminating the need for majority.

He proves that the probability of the success of an attack depends on the number of confirmations rather than the amount of wait time. He also reasons out the underlying assumption revolving the 6 confirmations and claims that the 6 confirmations could be a overkill for a casual attacker while it is not so powerful against serious attackers.

It is observed that the probability of success of double-spending decreases exponentially while waiting for more confirmations and that the decay rate is dependent on the relative hashrate of the attacker.

It states two major observations. One is that the success rate will never become zero irrespective of the number of confirmations. The other observation is that the success rate never falls below 100% if the attacker controls more hashrate than the honest network.

In addition, the period of wait time proves to be relevant only if the attacker fails to endure his hashrate for a longer time. In such an event, even the majority hashrate does not guarantee success.

Finally, the economics of the double-spending involving the amount to be shelled out by the attacker, the effect of targeting multiple merchants (decreases the assets) and the cost of purchase from each merchant provides a more deeper insight into the profitability and security aspects of an attack.

IV. Strong Points

1) The major plus of the paper is that it explains the complex concepts, attack and the various variables that determines the success and failure rates of the attack in a more comprehensive manner with sufficient proofs, evaluations and graphs. It is well written and also well organised.
2) The paper plays a crucial role in clarifying the various misconceptions such as the 6 confirmations myth, success of double-spending as a function of wait time etc. and provides a more deeper understanding of the problem and the role of different variables.
3) The author also explains the amount of complexity involved in carrying out a successful and profitable double-spending attack considering the different variables in play in realistic environment and the differences between the adversarial system and the real environments.

V. Weak Points

1) The paper does not discuss any relation between the variables involved in the calculation of proof-of-work and the effect of those on the success or failure of the double-spending. Though not fully confident, I feel there might be some aspects of proof-of-work that has some influence on the double-spending.
2) In section 4 (Waiting for Confirmations), it is said that the assumption made by Satoshi is not used. However, there is no enough explanation for not considering that assumption. It is little unclear as to why it is not used.

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 4th ed. Harlow, England: Addison-Wesley, 2004. Available: https://www.math.ucdavis.edu/ tracy/courses/math129/Guide$_{T}o_{L}aTeX.pdf$