Analysis of hash rate-based double-spending

Bernardo Gonzalez Riede Xin Ren

I. Motivation

Regarding how to prevent double-spending in Bitcoin transaction, there are some widespread beliefs, for example, double-spending requires having more than half of the network hash rate, 6 confirmations grants absolute protection and the length of time waited is an allegedly major factor in determining security. The author of this paper dispelled or clarified some myths with mathematical analysis, formulas , graphs and charts.

II. Contributions

In the paper, the author shows that successful double-spending is possible with any attacker hash rate. If the attacker has more hash rate than the honest network, the probability of successful attack is always 1 regardless how many confirmations merchants wait for, while if the attacker has less hash rate than the honest network, there is still always a non-zero probability for the attack to be successful regardless how many confirmations merchants wait for, even though waiting for more confirmations exponentially decreases the probability of double-spending success(The decay rate depends on the attacker's relative hash rate). The probability of success depends on the number of confirmations and not on the amount of time waited. An alternative network with a shorter time between blocks can thus obtain more security with a given amount of wait time. The time constant might be relevant, if we assume that the attacker cannot sustain his hash rate for a prolonged period of time. If merchants wait for 6 confirmations, and a attacker is unlikely to amass more than 10% of the hash rate, the probability of successful attack would be a negligible risk of less than 0.1% which is acceptable, that is why 6 confirmation is often-cited as being able to provide absolute safety. The author also presents the maximal safe transaction value as a simplified function of the attacker's hash rate and the number of conformations so that the merchants can know if the transaction is safe or not.

III. Solution

The double spending attack is tackled as a race between the attackers own computing power, the dishonest network, versus the honest network. Assumptions about the attack are that the total hash rate of the honest network and the attacker is constant, as well as the mining difficulty. The race between the two networks is modeled as a continuous-time Markov chain with the relative probabilities of the two networks to find the next block. Based on this model, a formula is given to calculate the probability that the attacker will be able to catch up or jump ahead in terms of successful chained blocks.

Furthermore a second model, which uses a negative binomial variable, is introduced, defining the probability for the attacker to mine m blocks in the same time n blocks are mined by the honest network. Through the aforementioned models and formula, a final formula is given to calculate the probability for the double-spend to succeed from the number of conformations the merchant waits for and the hash rate of the dishonest network, with assumptions that the attacker cannot release his branch before the vendor accepting the transaction due to the vendor being able to notice a chain without the transaction being present.

While assuming a smaller dishonest network than honest network, the previously gained knowledge is put into perspective by inspecting the economical aspects of the attack. A failed attack means lost opportunities to gain the bitcoins rewarded by finding a new block. By relating the value of goods an attacker might try to obtain by double-spending to the value an attacker might lose by forking an invalid chain, a formula and further on a table is created which shows a safe transaction value (in BTC) given an expected relative size of the dishonest network and the number of confirmation to wait for.

IV. Strong Points

1) Basic structure of the Bitcoin blockchain was explained in the paper so that readers without Bitcoin background can easily understand the paper.
2) The author explained and showed his analysis with mathematical formulas used in graphs and charts for easy comprehension. Different depictions for showing relationship between number of confirmations and computing power.
3) Clear assumptions with intermediary observations to be able to follow the reasoning.

V. Weak Points

1) There needs to be a consistency about usage of hash rate q of the attacker's network, either $q>=0.5$ or $q>0.5$
2) In Economics of double-spending, the author presents the maximal safe transaction value as a simplified function of the attacker's hash rate and the number of conformations so that the merchants can know if the transaction is safe or not, but the attacker's hash rate is not always known to the merchants.
3) Labeling the graphs axis would make for faster comprehension of them.
4) References are missing.