Formalization of network properties for resilient DLTs

Stefan Nowak
IMT Atlantique - Chaire Cyber CNI
stefan.nowak@imt-atlantique.fr

Marc-Oliver Pahl
IMT Atlantique - Chaire Cyber CNI
marc-oliver.pahl@imt-atlantique.fr

Romaric Ludinard
IMT Atlantique - IRISA
romaric.ludinard@imt-atlantique.fr

***Abstract*—Blockchain technology has gained importance in the previous years. Emerging through cryptocurrencies like Bitcoin in the early 2010s, it is now used in various fields like power grid, smart cars, or bank transactions. With the growing interest in blockchain, the question of their security became important, so does the question of their performances.**

A centreal question is the differences between Proof-of-Work and Proof-of-Stake. Proof-of-Work is a mechanism used by a large majority of the current blockchain. Introduced by Bitcoin, it lacks in performance and needs large resources. On the other hand, Proof-of-Stake is an alternative which allows blocks to be quickly created and with a lesser energy consumption, but at the expense of the security.

The objectives of this thesis are to study these two mechanisms, their advantages and vulnerabilities, and, if it is possible, to find a mechanism with both the efficiency and low consumption of Proof-of-Stake and the security of Proof-of-Work, and also to study the application of DLTs to improve the security of IT and OT systems.

I. Introduction

Blockchain is one of the most popular topics of the last decade. Since the creation of Bitcoin in 2009, this subject draws a lot of interest. It became a major topic in 2016 with the apparition of Ethereum and Blockhain 2.0.

Most blockchain systems created in the 2010s are based on the Bitcoin Proof-of-Work mechanism. But this mechanism faces multiple issues. The major ones are its high energy consumption and the slow pace at which new blocks can be created and added to the blockchain. [1]

To resolve these problems, another protocol was proposed: Proof-of-Stake. However, it comes with a major drawback. Proof-of-Stake systems are by far less secure than Proof-of-Work systems. [9]

The main questions this thesis aims to answer are the following:

- How to implement a secure Proof-of-Stake mechanism ?
- How can DLTs help securing IT and OT systems ?

II. Background

A blockchain is a chain of blocks, which have a similar structure to a linked list. Blockchains work on a distributed network, where miners nodes are responsible for creating blocks. Each block consist of two part: the header and the content of a block.

The header contains information about the block and its position in the blockchain, while the content is the set of transactions,or more generally data, stored on the blockchain through this block.

When a miner add a new block to the blockchain, it is linked to the previous block by containing in its own header the hash of the header of previous one. The first block of a blockchain is called the genesis block, and it is the only block not linked to another one.

The header also contains the root of the Merkle tree of the transactions stored in this block [1], ensuring that the hash of the header depends on the block's content. Therefore, since modifying its content will completely change the hash, any block in the blockchain is immutable.

A. Proof-of-Work

Proof-of-Work is a mechanism used in many blockchain system to make a block valid. It generally consist in the miner needing to solve a cryptographic puzzle for the block to be valid. This puzzle must be hard to solve, ensuring that the miner has to work to make his block valid, but also easy to verify if the solution is given.

The most known proof-of-work system is Hashcash, used by Bitcoin. It works as follow : the hash of the block (traditionally calculated with SHA-256) must be lower than a fixed threshold to be valid. To reach this goal, the miner edit a nonce in the header, modifying the block without altering its content. Such a mechanism is easy to check, hash function are easy to compute, but such function makes it hard to create a block such that the hash is valid. Therefore, it is a valid cryptographic puzzle for a proof-of-work system.

Proof-of-Work is used in many cyptocurrencies blockchains, the main one being Bitcoin and Ethereum 1.0.

B. Proof-of-Stake

Proof-of-Stake is an alternative to Proof-of-Work. While proof-of-work systems require the miner to have enough mining power to create a new block a win the reward, proof-of-stake systems give the right to create new blocks to those who owns the more resources. In Bitcoin for example, miners who owns more Bitcoins are more likely to be selected to create a new block.

More precisely, members of the network make a deposit of a portion of their assets, then an algorithm randomly selects one of those members to create a new block. The probability

to be selected by this algorithm increases with the amount of the deposit.

This system is mainly based on the fact that the more assets are held by the minters, the more important the security of the system is for him. This way, the network members who hold more assets are less likely to provoke a security breach, like voluntarily creating a fork in the blockchain.

III. Proof-of-Work vs. Proof-of-Stake

Proof-of-Work mechanism face multiples issues. The main one is the energy consumption. Solving a cryptographic puzzle takes both time and a lot of energy. The Proof-of-Work promotes a competition between miners who all work at the same time to solve the same puzzle, but only one solution will be accepted. Many miners spend a lot of energy for nothing.

This is one of the problems which is solved by Proof-of-Stake. When a forger is selected, he is the only one working on the block creation, meaning that the energy consumption is greatly decreased. It is also quicker to create blocks with these kind of systems.

Another advantage of Proof-of-Stake systems against Proof-of-Work is their bigger resistence against 51% attacks. [6] These attacks occurs when one entity owns more than 50% of the mining power of the network. It is an issue with Proof-of-Work blockchain [7] as mining pools, a gathering of multiples miners to maximize profits, are quite frequent. The mechanism of Proof-of-Stake systems makes these attacks harder as they imply that the attacker must own a large portion of the assets.

But there is one major issue faced by Proof-of-Stake systems : they are less secure than Proof-of-Work ones. [8] One of the main issue faced by Proof-of-Stake systems is that, since creating a new block does not require a large amount of resources and is basically free, minters can voluntarily work on conflicting blocks to maximize their benefits. [9] But there are other types of attacks targetting Proof-of-Stake protocols. [10]

IV. Current Work

In order to ask these questions, this thesis starts with a survey of the evolution of the research on blockchain security during the previous decade. The objective of this survey is to gather intel on blockchain security strengths and flaws in order to get a better understanding of the subject and to identify open question.

Being a major topic of the last decade, many articles were written during the previous decade. While researchers mainly focus on Bitcoin during the first half of the decade, the creation of Ethereum and many other since 2015 made the topic more diverse. [2]

Focusing on the security aspect, the first half of the decade was mainly focused on Bitcoin most common risks, like double spending and 51% attack. Since 2015, multiple articles about Bitcoin network-vulnerabilities are released, some of them both about Bitcoin and Ethereum, like eclipse attacks, balance attacks, or routing attacks. [3]

With Ethereum also came security flaws on smart contracts [4]. The most common is the DAO attack in 2016, exploiting a vulnerability of a function in the DAO smart contract, which resulted in 3.6 millions Ether stolen and a hard fork on the Ethereum blockchain. Many other vulnerabilities not specific to one contract also exists, like reentrancy or leaking ether vulnerabilities.

V. Conclusion

While Proof-of-Stake protocol solves two of the main issues of the Proof-of-Work mechanism, its cost in security prevent it from being massively deployed on blockchain systems. Some solutions have been presented to mitigate these security issues [11], and with Ethereum transitioning from Proof-of-Work to Proof-of-Stake in Ethereum 2.0 [3], it may become a more popular system.

But the main question which emerged from this comparison is the following. Is it possible to create a mechanism which satisfy both the low energy consumption and quick block generation of Proof-of-Stake protocol and the security of Proof-of-Work ?

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[2] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *CoRR*, 2018. [Online]. Available: http://arxiv.org/abs/1802.06993

[3] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks and defenses," *CoRR*, 2019. [Online]. Available: http://arxiv.org/abs/1908.04507

[4] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts," *IACR Cryptol. ePrint Arch.*, 2016. [Online]. Available: http://eprint.iacr.org/2016/1007

[5] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, Eds. ACM, 2016. [Online]. Available: https://doi.org/10.1145/2976749.2978341

[6] I. Lin and T. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, 2017. [Online]. Available: http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf

[7] X. Yang, Y. Chen, and X. Chen, "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information." IEEE, 2019. [Online]. Available: https://doi.org/10.1109/Blockchain.2019.00041

[8] P. Gazi, A. Kiayias, and A. Russell, "Stake-bleeding attacks on proof-of-stake blockchains," *IACR Cryptol. ePrint Arch.*, 2018. [Online]. Available: http://eprint.iacr.org/2018/248

[9] W. Li, S. Andreina, J. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," ser. Lecture Notes in Computer Science, J. García-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, Eds. Springer, 2017. [Online]. Available: https://doi.org/10.1007/978-3-319-67816-0_17

[10] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, "A survey on long-range attacks for proof of stake protocols," *IEEE Access*, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2901858

[11] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," J. Katz and H. Shacham, Eds. Springer, 2017. [Online]. Available: https://doi.org/10.1007/978-3-319-63688-7_12

[12] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *IACR Cryptol. ePrint Arch.*, 2014. [Online]. Available: http://eprint.iacr.org/2014/452