Probabilistic Formal Methods Applied to Blockchain's Consensus Protocol

Cristian Mirto
SnT
Luxembourg
cristian.mirto@uni.lu

Jiangshan Yu
SnT
Luxembourg
jianshan.yu@uni.lu

Vincent Rahli
SnT
Luxembourg
vincent.rahli@uni.lu

Paulo Esteves-Verissimo
SnT
Luxembourg
paulo.verissimo@uni.lu

***Abstract*—In distributed systems, the problem of achieving consensus in presence of faulty (possibly malicious) nodes has been quite difficult to solve. Indeed, the well-known FLP result says that, without any assumption on the synchronism of the network, the consensus problem is unsolvable deterministically. The Nakamoto *Proof-of-Work* consensus protocol addresses this problem in a probabilistic fashion. However, formal computer-aided proofs of its probabilistic properties are still missing. The probabilistic nature of blockchain's technology cannot be disregarded when it comes to analyzing its properties. Our plan is to apply probabilistic formal methods for the verification of such properties in major blockchain consensus protocols, including Proof-of-Work, Proof-of-Stake, and other variants.**

I. Introduction

The blockchain technology has seen an increasing interest in the last years. Invented by Satoshi Nakamoto in order to enforce consensus in the context of Bitcoin's transaction system [7], blockchain has been employed also in other applications than cryptocurrencies, such as smart contracts, digital voting, or supply chains.

The *Proof-of-Work* (PoW) mechanism represents a paradigm shift for Byzantine consensus protocols. It is an enabler to achieve the primary goal of Bitcoin's blockchain, which is to eliminate the need of central authorities. In particular, the Bitcoin blockchain is a permissionless system where anyone can join and leave the consensus at any time. No classic Byzantine consensus scheme can achieve it. The basic idea of PoW is that, in order to vote, nodes need to perform some computational work to solve a crypto puzzle.

This new view enabled Bitcoin to prevent sybil attacks in a peer-to-peer network without the need of trusted authorities. Still, at its core, Proof-of-Work consensus protocol provides only *probabilistic* assurances about its correct behavior.

II. Related Work

Being employed in highly sensitive sectors, it is mandatory to perform a formal security analysis of blockchain consensus protocols. In his seminal paper, Nakamoto provided an analysis of the infeasibility of the double-spending attack. However, this analysis did not consider other factors that can be exploited to threaten its security properties, such as rational behaviors and network attacks. Indeed, it has been shown [2] that it is possible for an attacker to mount a double spending attack, though having less than 51% of the total computing power, by exploiting the rational behavior of the honest nodes. Besides, the peer-to-peer network also plays a very important role, and network level attacks should also be considered. For example, *eclipse attacks* [5] show the possibility of attacking the blockchain consensus, by isolating target nodes.

Recently, the interest of the scientific community in rigorously analyzing blockchain properties has steadily increased. In particular, in [4] Garay *et al.* proved that a probabilistic notion of *eventual consistency* holds in blockchains, for which every honest node eventually shares the same ledger up to a window of T final blocks. They also proved a *chain quality* property, which, roughly speaking, ensures that in a row of subsequent blocks just a small fraction of them can be constructed by malicious miners. They assume that (A) each participant has the same computing power; (B) the execution of the blockchain protocol is stand-alone, i.e. a single protocol instance is executed in isolation and not concurrently with other instances; and (C) the number of participants is fixed but unknown to the nodes. In their modeling, however, only synchronous communication is taken into account. In a follow-up of this work, Pass *et al* proved similar properties considering a partially synchronous network [8].

We believe that, in support of these analyses, a formal verification of the identified properties is desirable to ensure the security of blockchain consensus protocols. In this perspective, a recent and elegant work [9] by Pirlea and Sergey, provided the first formalisation of blockchain's consensus protocol in the theorem prover Coq [1]. The authors were able to prove that eventual consistency can be achieved, but their analysis did not take into account any Byzantine setting.

III. Research proposal

Pirlea and Sergey proposed the first work in this direction. However, as the authors pointed out, the work is still preliminary. For simplicity, their work has opted to take a simple model, and did not consider complicated scenarios involving rational behavious and computing power distri-

bution. For example, their model assumes the absence of in-flight messages between any pair of nodes (a *quiescent* state), assumes a clique topology for the network and do not consider the presence of malicious nodes.

We are aiming at providing a refined formal analysis on blockchain consensus under the presence of Byzantine participants. In particular, we aim at providing an analysis with the consideration of non-even computing power distributions, and the network latency. In addition, we plan to build a model where the rational behavior of nodes is considered. Moreover, we plan to address also the churn rate, namely the participant turnover rate regarding active and nonactive users.

The most important feature that we want to underline is the probabilistic nature of blockchain protocols. With this in mind, we plan to make use and extend the probabilistic model checker PRISM [6] for our proposed analysis.

Acknowledgment

This work is partially supported by the Fonds National de la Recherche Luxembourg (FNR) through PEARL grant FNR/P14/8149128.

References

[1] *The Coq Proof Assistant*. URL: http://coq.inria.fr/.

[2] Ittay Eyal and Emin Gün Sirer. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable". In: *Financial Cryptography*. Vol. 8437. Lecture Notes in Computer Science. Springer, 2014, pp. 436–454.

[3] Michael J. Fischer, Nancy A. Lynch, and Mike Paterson. "Impossibility of Distributed Consensus with One Faulty Process". In: *J. ACM* 32.2 (1985), pp. 374–382.

[4] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. "The Bitcoin Backbone Protocol: Analysis and Applications". In: *IACR Cryptology ePrint Archive* 2014 (2014), p. 765.

[5] Ethan Heilman et al. "Eclipse Attacks on Bitcoin's Peer-to-Peer Network". In: *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, 2015, pp. 129–144.

[6] M. Kwiatkowska, G. Norman, and D. Parker. "PRISM 4.0: Verification of Probabilistic Real-time Systems". In: *Proc. 23rd International Conference on Computer Aided Verification (CAV'11)*. Vol. 6806. LNCS. Springer, 2011, pp. 585–591.

[7] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf.*

[8] Rafael Pass, Lior Seeman, and Abhi Shelat. "Analysis of the Blockchain Protocol in Asynchronous Networks". In: *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*. Vol. 10211. Lecture Notes in Computer Science. 2017, pp. 643–673.

[9] George Pîrlea and Ilya Sergey. "Mechanising blockchain consensus". In: *CPP 2018*. ACM, 2018, pp. 78–90.