Brief Announcement: Game Theoretical Framework for Analyzing Blockchains Robustness

Paolo Zappalà, Marianna Belotti, Maria Potop-Butucaru, Stefano Secci

Brief Announcement: Game Theoretical Framework for Analyzing Blockchains Robustness

Paolo Zappalà
Cedric, Cnam, 75003 Paris, France
paolo.zappala@cnam.fr

Marianna Belotti
BDTD, Caisse des Dépôts et Consignations, 75013 Paris, France
Cedric, Cnam, 75003 Paris, France
marianna.belotti@caissedesdepots.fr

Maria Potop-Butucaru
Lip6, Sorbonne Université, 75005 Paris, France
maria.potop-butucaru@lip6.fr

Stefano Secci
Cedric, Cnam, 75003 Paris, France
stefano.secci@cnam.fr

Abstract

Blockchains systems evolve in complex environments that mix classical patterns of faults (e.g crash faults, transient faults, Byzantine faults, churn) with selfish, rational or irrational behaviors typical to economical systems. In this paper we propose a game theoretical framework in order to formally characterize the robustness of blockchains systems in terms of resilience to rational deviations and immunity to Byzantine behaviors. Our framework includes necessary and sufficient conditions for checking the immunity and resilience of games and a new technique for composing games that preserves the robustness of individual games. We prove the practical interest of our formal framework by characterizing the robustness of three different protocols popular in blockchain systems: a HTLC-based payment scheme (a.k.a. Lightning Network), a side-chain protocol and a cross-chain swap protocol.

2012 ACM Subject Classification Networks

Keywords and phrases Blockchains, Game Theory, Byzantine-Altruistic-Rational behaviours

Digital Object Identifier 10.4230/LIPIcs.DISC.2020.49

1 Introduction

Distributed Ledger Technologies (DLTs) allow sharing a ledger of transactions among multiple users forming a peer-to-peer (P2P) network. DLTs characterized by a block architecture are called "Blockchains"; transactions are stored in blocks that are chained to each other by means of cryptographic methods, namely hash functions. Blockchain systems are the composition of various protocolar building blocks enabling its users to transfer cryptoassets in a decentralized manner. Beyond the traditional blockchain protocols that exist today [7, 12, 17], the literature proposes other protocols that respectively define and regulate interactions outside the blockchain (*layer-2 protocols* [10]) and between different blockchains (*cross-chain protocols* [9]). Each of these protocols establishes the instructions that a user must follow in order to interact with or through a blockchain.

In a Blockchain system, agents can be classified in three different categories accordingly to [3]: (i) players who follow the prescribed protocol are called *altruistic*, (ii) those who act in order to maximise their own benefit are said to be *rational* and, (iii) players who may arbitrarily deviate from the prescribed protocol are defined as *Byzantine*. Moreover, protocols can be classified in: *Byzantine Altruistic Rational Tolerant* (BART) protocols that guarantee the safety and liveness properties in the presence of rational deviations and

Incentive-Compatible Byzantine Fault Tolerant (IC-BFT) that incentivize rational agents to follow the prescribed protocol, also in presence of Byzantine players.

In this context, game theory helps in designing IC-BFT protocols guaranteeing that rational players follow the prescribed protocol's instructions. Concerning layer-2 and cross-chain protocols, game theoretical analysis are carried out by [4, 5, 6, 8]. More precisely, authors in [4, 5] design IC-BFT off-chain channels. In [6, 8] authors adopt the Nash equilibrium solution concept to respectively evaluate the stability of various network structures and the stability of existing cross-chain swap protocols.

Our contribution. This paper presents a game theoretical framework to analyze the robustness of blockchains systems, in terms of resilience to rational deviations and immunity to Byzantine behaviors; it is the first one, as of our knowledge, with respect to the current state of the art. The closest work to ours was proposed in [2] where the authors introduce the concept of *mechanism* (a pair game-prescribed strategy). In order to characterize the robustness of a distributed system authors in [2] introduce the notions of k-resiliency and t-immunity. In a k-resilient equilibrium there is no coalition of k players having an incentive to simultaneously change strategy to get a better outcome. On the other hand, the concept of t-immunity evaluates the risk of a set of t players to have a Byzantine behavior. The property of t-immunity is often impossible to be satisfied by practical systems [1]. We thus introduce the concept of *t-weak-immunity*. A mechanism is t-weak-immune if any altruistic player receives no worse payoff than the initial state, no matter how any set of t players deviate from the prescribed protocol. We further extend the framework in [2] by proving the necessary and sufficient conditions for a mechanism to be optimal resilient and t-weak-immune. Moreover, we define a new operator for mechanism composition and prove that it preserves the robustness properties of the individual games. In this way, we characterize the robustness of complex protocols via the composition of simpler robust building blocks.

The effectiveness of our framework is demonstrated by its capability to capture the robustness of various blockchain protocols. We studied (k, t)-robustness and (k, t)-weak-robustness (i.e., optimal k-resilience and t-weak-immunity) of Lightning Network protocol [14], a side-chain protocol [15] and the very first implementation of a cross-chain swap protocol proposed in [13] and formalized in [11]. Our analysis spotted the weakness of the Lightning Network protocol [14] to Byzantine behaviour. More precisely, the protocol's strategy to close a channel (i.e., an off-chain payment line) is neither weak immune nor immune. Thus, we provide an alternative protocol (i.e., an alternative closing module) satisfying weak immunity. The protocols regulating transactions in side-chains (i.e., secondary independent blockchain)

Table 1 Immunity and resilience properties for Lightning Network [14], the modified version with a different closing module, a side-chain protocol [15] and a cross-chain swap protocol [11, 13].

Protocol	Optimal Resilience	Weak Immunity	Immunity
Lightning Network [14]	**Yes**	**No**	**No**
Closing module	Yes	No	No
Other modules	Yes	Yes	No
Modified Lightning Network	**Yes**	**Yes**	**No**
Alternative closing module	Yes	Yes	No
Other modules	Yes	Yes	No
Side-chain (Platypus [15])	**Yes**	**Yes**	**No**
Cross-chain Swap [11, 13]	**Yes**	**Yes**	**No**

proposed in [15] is weak immune since players following the protocol never get negative utility when all the other players act as adversaries. Composition of games is used to prove the weak immunity of the cross-chain swap protocol proposed in [11, 13]. Each blockchain corresponds to a game that is weak immune, thus the composition preserves the weak immunity. Our results are reported in Table 1. The details can be found in [16].

References

1 Ittai Abraham, Lorenzo Alvisi, and Joseph Y. Halpern. Distributed computing meets game theory: combining insights from two fields. *Acm Sigact News*, 42(2):69–76, 2011.

2 Ittai Abraham, Danny Dolev, Rica Gonen, and Joe Halpern. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Principles of Distributed Computing*, PODC '06, page 53–62, 2006.

3 Amitanand S. Aiyer, Lorenzo Alvisi, Allen Clement, Michael Dahlin, Jean-Philippe Martin, and Carl Porth. Bar fault tolerance for cooperative services. In *Proceedings of the twentieth ACM symposium on Operating systems principles*, pages 45–58, 2005.

4 Georgia Avarikioti, Eleftherios Kokoris Kogias, and Roger Wattenhofer. Brick: Asynchronous state channels. *arXiv preprint*, 2019. `arXiv:1905.11360`.

5 Georgia Avarikioti, Felix Laufenberg, Jakub Sliwinski, Yuyi Wang, and Roger Wattenhofer. Towards secure and efficient payment channels. *arXiv preprint*, 2018. `arXiv:1811.12740`.

6 Georgia Avarikioti, Rolf Scheuner, and Roger Wattenhofer. Payment networks as creation games. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pages 195–210. Springer, 2019.

7 Marianna Belotti, Nikola Božić, Guy Pujolle, and Stefano Secci. A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys & Tutorials*, 21(4):3796–3838, 2019.

8 Marianna Belotti, Stefano Moretti, Maria Potop-Butucaru, and Stefano Secci. Game theoretical analysis of Atomic Cross-Chain Swaps. In *40th IEEE International Conference on Distributed Computing Systems, ICDCS*, 2020. URL: `https://hal.archives-ouvertes.fr/hal-02414356`.

9 Michael Borkowski, Daniel McDonald, Christoph Ritzer, and Stefan Schulte. Towards atomic cross-chain token transfers: State of the art and open questions within tast. *Distributed Systems Group TU Wien, Report*, 2018.

10 Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. Sok: Off the chain transactions. *IACR Cryptology ePrint Archive*, 2019:360, 2019.

11 Maurice Herlihy. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing*, pages 245–254, 2018.

12 Christopher Natoli, Jiangshan Yu, Vincent Gramoli, and Paulo Esteves-Verissimo. Deconstructing blockchains: A comprehensive survey on consensus, membership and structure. *arXiv preprint*, 2019. `arXiv:1908.08316`.

13 Tier Nolan. Re: Alt chains and atomic transfers, 2013. Accessed on July 30, 2020. `https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949`.

14 Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016. `https://lightning.network/lightning-network-paper.pdf`.

15 Alejandro Ranchal-Pedrosa and Vincent Gramoli. Platypus: Offchain protocol without synchrony. In *2019 IEEE 18th International Symposium on Network Computing and Applications, NCA*, pages 1–8, 2019.

16 Paolo Zappalà, Marianna Belotti, Maria Potop-Butucaru, and Stefano Secci. Game Theoretical Framework for Analyzing Blockchains Robustness, May 2020. URL: `https://hal.archives-ouvertes.fr/hal-02634752`.

17 Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4):352–375, 2018.