Analyse de la fiabilité des blockchains via la théorie des jeux

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

▶ **To cite this version:**

Paolo Zappalà, Marianna Belotti, Maria Potop-Butucaru, Stefano Secci. Analyse de la fiabilité des blockchains via la théorie des jeux. ALGOTEL 2021 - 23èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, Jun 2021, La Rochelle, France. hal-03206203

HAL Id: hal-03206203
https://hal.science/hal-03206203

Submitted on 23 Apr 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Analyse de la fiabilité des blockchains via la théorie des jeux

P. Zappalà [*], M. Belotti [†], M. Potop-Butucaru [‡], S. Secci[§]

Abstract

Les blockchains sont développés dans des environnements sujets aux fautes (e.g pannes franches, fautes transitoires, comportements Byzantins) dues aux comportements égoïstes, rationnels ou irrationnels caractéristiques aux systèmes économiques. Dans cet article nous proposons un modèle basé sur la théorie des jeux permettant de caractériser formellement la fiabilité des blockchains du point de vue de leur résilience face aux déviations rationnelles. De plus, notre modèle permet de caractériser l'immunité des blockchains face aux comportements Byzantins. Notre modèle comprend également des conditions nécessaires et suffisantes pour vérifier la résilience et l'immunité des jeux et une technique novatrice permettant la composition des jeux. Notre opérateur de composition préserve la fiabilité des jeux simples. Nous appliquons notre modèle pour caractériser la fiabilité de plusieurs protocoles blockchain : Bitcoin (la plus populaire blockchain de type permissionless), Tendermint (la première blockchain permissioned utilisée par les praticiens), Lightning Network, un protocole side-chain et un protocole pour les swaps cross-chain.

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". They enable its users to transfer cryptoassets in a decentralized manner by means of modular protocols adopted by the users themselves. Beyond the traditional blockchain architectures (i.e., *layer-1 protocols*), the literature proposes other protocols that respectively define and regulate interactions in an overlaying network (*layer-2 protocols*) and interactions between different blockchains (*cross-chain protocols*). In a Blockchain system players can be classified in three different categories as stated in [2]: (i) players who follow the prescribed protocol i.e., *altruistic*, (ii) those who act in order to maximise their own benefit i.e., *rational*, and (iii) players who may deviate from the prescribed protocol in an irrational way, i.e. *Byzantine*.

Interactions among users are modeled with game theory, which is used to design incentive mechanisms aiming at preventing any possible deviation from a prescribed protocol that blockchain users need to follow. Robustness of protocols governing DLTs (e.g., consensus protocols, communication protocols and storage protocols) has been addressed in several recent works. Most of the game theoretical models adopted to design secure and robust blockchain protocols, surveyed in [5, 10], (i) address protocols characterizing specific blockchain implementations, (ii) analyze miners' behaviours in the consensus phase and (iii) adopt Nash Equilibria as solution concept.

In the literature, analysis of systems robustness with respect to participating actors can be classified according to the agents' nature [2]. Concerning rational agents, the robustness analysis includes the study of the equilibria and the evaluation of their properties. The most studied and adopted solution concept in the literature is Nash Equilibrium, i.e., a strategy profile in which no player has interest in individually deviating from her own strategy. Authors in [1] define some properties to characterise strategy profiles: (i) *practical* strategy profiles equilibria are those which

[*]Paolo Zappalà is with Orange Labs, 92320 Chatillon, France and LIA, Avignon Université, 84029 Avignon, France (e-mail: paolo.zappala@orange.com)

[†]Marianna Belotti is with Cedric, Cnam, 75003 Paris, France, and also with Département de la Transformation Numérique, Caisse des Dépôts, 75013 Paris, France (e-mail: marianna.belotti@caissedesdepots.fr).

[‡]Maria Potop-Butucaru is with Lip6, CNRS UMR 7606, Sorbonne University, 75005 Paris, France (e-mail: maria.potop-butucaru@lip6.fr).

[§]Stefano Secci is with Cedric, Cnam, 75003 Paris, France (e-mail: stefano.secci@cnam.fr).

exclude weakly dominated strategies, (ii) *k-resilient* equilibria are those strategy profiles such that if there is no coalition with at most k players having an incentive to deviate from the prescribed protocol. In order to analyse robustness with respect to Byzantine agents, authors in [1] introduce the concept of *t-immunity*, i.e., no player gets a lower outcome if there are at most t Byzantine players that can play any possible strategy.

Our contribution. This paper presents a game theoretical framework aiming at characterizing blockchain protocols, modeled as games, in terms of robustness, i.e. resilience to rational deviations and immunity to Byzantine behaviors. Robustness analysis of blockchain protocols were performed before in [1] by adopting the concept of *mechanism* (i.e., a pair game-prescribed strategy). In order to characterize the robustness of a distributed system authors in [1] introduce the notions of (i) k-resilience, (ii) practicality and (iii) t-immunity. More precisely, k-resilience and practicality analyze the robustness with respect to rational agents, while t-immunity deals with Byzantine agents. In this paper we use the concept of mechanism proposed in [1] to model different types of blockchain protocols and we define a set of properties to be satisfied in terms of robustness. Since the property of t-immunity is often impossible to be satisfied by practical systems [1], we 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 [1] by proving some necessary and sufficient conditions for a mechanism to be optimal resilient and t-weak-immune. In order to make the method scalable to any modular protocol, we define a new operator for mechanism composition and prove that it preserves the robustness properties of the individual games. Using our framework we studied the properties of a set of layer-1, layer-2 and cross-chain protocols: Tendermint [4], Bitcoin [6], Lightning Network protocol [9], the side-chain protocol [8] and the very first implementation of a cross-chain swap protocol proposed in [7] and formalized in [3]. Thanks to the analysis of protocol robustness we spotted the weakness of the Lightning Network protocol to Byzantine behaviour and therefore we propose and further analyze an alternative version of the protocol. Our results are reported in Table 1 and in [12]. An earlier version with partial results was published in [11].

Table 1: Immunity and resilience properties for Tendermint [4], Bitcoin [6], Lightning Network [9], a side-chain protocol [8] and a cross-chain swap protocol [3, 7] with respect to the number of rational deviating agents (k) and the number of Byzantine deviating agents (t) where n is the total number of players in the game.

Protocol	k-Resilience	t-Immunity	t-Weak Immunity
Tendermint	**Yes, k** $< n/3$	**No**	**Yes, t** $< n/3$
Bitcoin	**Yes, k** $< 3n/20$	**No**	**No**
Lightning Network	**Yes, k** $< 3n/20$	**No**	**No**
Closing module	Yes	No	No
(Alternative closing module)	(Yes)	(No)	(Yes)
Other modules	Yes	No	Yes
Side-chain (Platypus)	**Yes, k** $< n/3$	**No**	**Yes, t** $< n/3$
Cross-chain Swap	**Yes**	**No**	**Yes**

2 Game theoretical framework

Mechanisms and Robustness. Given a distributed systems protocol, players can either decide to follow or not the prescribed instructions. The aim of our model is to understand whether the players are incentivized to follow or deviate from the prescribed protocol given the presence of some rational or Byzantine agents. In the following (i) we recall and extend the game theoretical framework based on the concept of mechanism (introduced in [1]) and its properties, (ii) we define new properties on protocol robustness and (iii) we study properties interdependence.

Let us consider a game in normal form $\Gamma = \langle N, \mathscr{S}, u \rangle$ where players find themselves in an initial state, i.e., before starting the application of the protocol. For the sake of simplicity we assign $u_i(\sigma) = 0$ for every $\sigma \in \mathscr{S}$ when the player i is indifferent between the outcome of the strategy profile σ and the initial state one. Analogously, we assign positive utility, $u_i(\sigma) > 0$, when the outcome of σ corresponds to the final state provided by the protocol and negative utility,

$u_i(\sigma) < 0$, when the outcome of σ is worse than the initial state one. The values of u_i, for all $i \in N$, correspond to the marginal utility with respect to the initial state. Every decision-making problem is modeled by a game $\Gamma = \langle N, \mathscr{S}, u \rangle$, which shows all the possible strategies available to the players, including following the prescribed protocol and all its possible deviations. A specific protocol consists of a strategy profile $\sigma = (\sigma_1, \ldots, \sigma_n) \in \mathscr{S}$ and it is denoted by a pair (Γ, σ), called *mechanism* [1]. Every player i is advised to play strategy $\sigma_i \in \mathscr{S}_i$ i.e., the recommended strategy σ is the prescribed protocol. Evaluating the robustness to deviations of a distributed protocol corresponds to identifying the properties of the mechanism (Γ, σ). Players can decide to deviate for two different reasons. On one hand, they can cooperate in order to find a strategy profile that provides a better outcome than the one given by the protocol. On the other hand, some players can behave maliciously for no specific reason and harm the altruistic ones. These two behaviours are prevented, according to [1], if prescribed protocols are respectively (i) k-resilient and/or (ii) t-immune.

A mechanism (Γ, σ) is *k-resilient* if there is no coalition of at most k players having an incentive to simultaneously change strategy to get a better outcome. Formally, a strategy profile $\sigma \in \mathscr{S}$ is a *k-resilient equilibrium* if for all $C \subseteq N$ with $1 \leq |C| \leq k$, all $\tau_C \in \mathscr{S}_C$ and all $i \in C$, we have $u_i(\sigma_C, \sigma_{-C}) \geq u_i(\tau_C, \sigma_{-C})$. The concept of k-resilience denotes the tendency of a set of k players to cooperate to move to an equilibrium that differs from the prescribed one. Hence k-resilience generalizes the concept of Nash equilibrium.

A mechanism (Γ, σ) is *t-immune* if, given at most t players choosing any strategy different from the prescribed one, the other players receive at least the utility they would get if everyone followed the protocol. Formally, a strategy profile $\sigma \in \mathscr{S}$ is *t-immune* if for all $T \subseteq N$ with $|T| \leq t$, all $\tau_T \in \mathscr{S}_T$ and all $i \in N \setminus T$, we have $u_i(\sigma_{-T}, \tau_T) \geq u_i(\sigma)$.

The property of t-immunity is very strong and hardly satisfiable since it requires that the protocol provides the best outcome no matter how a set of t players deviates. We therefore introduce a weaker version of the property; *t-weak-immunity*. This new property guarantees that non deviating players receive at least the utility value of the initial state (i.e., players receive a positive outcome).

Definition 1 (t-weak-immunity)**.** A mechanism (Γ, σ) is *t-weak-immune* if for all $T \subseteq N : |T| \leq t$, all $\tau_T \in \mathscr{S}_T$ and all $i \in N \setminus T$, we have $u_i(\sigma_{-T}, \tau_T) \geq 0$.

A player that joins a t-weak-immune mechanism will not suffer any loss (i.e., outcome with negative utility) if there are at most t deviating players in the game. We say that a mechanism is *weak immune* if it is t-weak-immune for all $t \in N$.

Composition of Games and Mechanism. Blockchains systems are complex protocols designed in a modular way. In order to study the robustness of such complex protocols, we need to analyze the individual modules and infer the properties of the system by composition. For this scope we introduce the new notion of *composition of games* that, to the best of our knowledge, has never been defined in the literature. Given two different games A and B, the composition of games is defined by the operator $\odot$, hence $A \odot B$ denotes the composition of game A and B. Given two games that are played separately and independently, the composition corresponds to players picking a strategy from each game and receiving as utility the sum of the utilities of the two games.

Definition 2 (Games Composition)**.** Given $A = \langle N, \mathscr{S}_A, u_A \rangle$ and $B = \langle N, \mathscr{S}_B, u_B \rangle$ two games in normal form with the same set of players N, two different sets of strategies $\mathscr{S}_A = \{\mathscr{S}_{Ai} : i \in N\}$ and $\mathscr{S}_B = \{\mathscr{S}_{Bi} : i \in N\}$ and two different utility functions: $u_A : \mathscr{S}_A \to \mathbb{R}^N$ and $u_B : \mathscr{S}_B \to \mathbb{R}^N$ then, it is possible to define a new game $C = A \odot B$, called composition of A and B, characterized as follows: $C = \langle N, \mathscr{S}_C, u_C \rangle$, where N is the set of the players, $\mathscr{S}_C := \{(s_{Ai}, s_{Bi}), s_{Ai} \in \mathscr{S}_{Ai}, s_{Bi} \in \mathscr{S}_{Bi}, \forall i \in N\}$ is the set of strategies and $u_C(\{(\sigma_{Ai}, \sigma_{Bi})\}) := u_A(\{\sigma_{Ai}\}) + u_B(\{\sigma_{Bi}\})$ is the utility function.

The following propositions allow us to (i) model the building blocks of complex protocols, (ii) study the properties of the subsequent mechanisms and (iii) deduce the properties of the composed protocol through the composition of mechanisms.

Concerning the solutions of the composition of games, we prove that Nash equilibria can be identified by selecting equilibria within the single games. It is not possible to create or destroy Nash equilibrium strategies by composing independent games.

Theorem 1 (composition nash equilibria)**.** *Let $A = \langle N, \mathscr{S}_A, u_A \rangle$ and $B = \langle N, \mathscr{S}_B, u_B \rangle$ be two games in normal form representation. Then, $\{(\sigma_{Ai}, \sigma_{Bi})\}$ is a Nash equilibrium for $A \odot B$ if and only if $\{\sigma_{Ai}\}$ and $\{\sigma_{Bi}\}$ are Nash equilibria respectively for A and B.*

Concerning robustness properties for composition of games, we can state the following results on resiliency and weak immunity for two composed games. The results can be generalized for the composition of multiple games.

Theorem 2 (resiliency)**.** *Let $A = \langle N, \mathscr{S}_A, u_A \rangle$ and $B = \langle N, \mathscr{S}_B, u_B \rangle$ be two games and let (A, σ_A) and (B, σ_B) be two mechanisms respectively k-resilient and k'-resilient. Then, $(A \odot B, \{\sigma_{Ai}, \sigma_{Bi}\})$ is a $\min(k, k')$-resilient mechanism.*

Theorem 3 (weak immunity)**.** *Let $A = \langle N, \mathscr{S}_A, u_A \rangle$ and $B = \langle N, \mathscr{S}_B, u_B \rangle$ be two games and let (A, σ_A) and (B, σ_B) be two mechanisms respectively t-weak-immune and t'-weak-immune. Then, $(A \odot B, \{\sigma_{Ai}, \sigma_{Bi}\})$ is a $\min(t, t')$-weak-immune mechanism.*

References

[1] Ittai Abraham, Danny Dolev, Rica Gonen, and Joe Halpern. 2006. 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* (Denver, Colorado, USA) *(PODC '06)*. Association for Computing Machinery, New York, NY, USA, 53–62. https://doi.org/10.1145/1146381.1146393

[2] Amitanand S. Aiyer, Lorenzo Alvisi, Allen Clement, Michael Dahlin, Jean-Philippe Martin, and Carl Porth. 2005. BAR fault tolerance for cooperative services. In *SOSP '05*.

[3] Maurice Herlihy. 2018. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing*. 245–254.

[4] Jae Kwon. 2014. Tendermint: Consensus without mining. *Draft v. 0.6, fall* 1, 11 (2014).

[5] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y. Liang, and D. I. Kim. 2019. A Survey on Blockchain: A Game Theoretical Perspective. *IEEE Access* 7 (2019), 47615–47643.

[6] Satoshi Nakamoto. 2008. A peer-to-peer electronic cash system. (2008).

[7] Tier Nolan. [n.d.]. Re: Alt chains and atomic transfers. accessed on January 10, 2020. https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949.

[8] Alejandro Ranchal Pedrosa and Vincent Gramoli. 2019. Platypus: Offchain Protocol Without Synchrony. In *18th IEEE International Symposium on Network Computing and Applications, NCA 2019, Cambridge, MA, USA, September 26-28, 2019*, Aris Gkoulalas-Divanis, Mirco Marchetti, and Dimiter R. Avresky (Eds.). IEEE, 1–8. https://doi.org/10.1109/NCA.2019.8935037

[9] Joseph Poon and Thaddeus Dryja. 2016. The bitcoin lightning network: Scalable off-chain instant payments.

[10] Wenbo Wang, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, and Yonggang Wen. 2018. A survey on consensus mechanisms and mining management in blockchain networks. *arXiv preprint arXiv:1805.02707* (2018), 1–33.

[11] Paolo Zappalà, Marianna Belotti, Maria Potop-Butucaru, and Stefano Secci. 2020. Brief Announcement: Game Theoretical Framework for Analyzing Blockchains Robustness. In *34th International Symposium on Distributed Computing (DISC 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

[12] Paolo Zappalà, Marianna Belotti, Maria Potop-Butucaru, and Stefano Secci. 2020. Game theoretical framework for analyzing Blockchains Robustness. Cryptology ePrint Archive, Report 2020/626. https://eprint.iacr.org/2020/626.