Rational Behaviors in Committee-Based Blockchains

Yackolley Amoussou-Guenou

Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France
Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

Bruno Biais

HEC Paris, 1 Rue de la Libération, 78350 Jouy-en-Josas, France

Maria Potop-Butucaru

Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

Sara Tucci-Piergiovanni

Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France

Abstract

We study the rational behaviors of participants in committee-based blockchains. Committee-based blockchains rely on specific blockchain consensus that must be guaranteed in presence of rational participants. We consider a simplified blockchain consensus algorithm based on existing or proposed committee-based blockchains that encapsulate the main actions of the participants: *voting* for a block, and *checking its validity*. Knowing that those actions have costs, and achieving the consensus gives rewards to committee members, we study using game theory how strategic participants behave while trying to maximize their gains. We consider different reward schemes, and found that in each setting, there exist equilibria where blockchain consensus is guaranteed; in some settings however, there can be coordination failures hindering consensus. Moreover, we study equilibria with trembling participants, which is a novelty in the context of committee-based blockchains. Trembling participants are rational that can do unintended actions with a low probability. We found that in presence of trembling participants, there exist equilibria where blockchain consensus is guaranteed; however, when only voters are rewarded, there also exist equilibria where validity can be violated.

2012 ACM Subject Classification Computer systems organization → Dependable and fault-tolerant systems and networks; Theory of computation → Solution concepts in game theory

Keywords and phrases BFT Consensus, Blockchains, Game Theory

Digital Object Identifier 10.4230/LIPIcs.OPODIS.2020.12

1 Introduction

Most cryptocurrencies rely on distributed technology ledgers. Each user of the cryptocurrency may have a local copy of the ledger. The most popular among the distributed ledger technologies is probably blockchain. A blockchain is a growing sequence of blocks, where each block contains transactions and is linked to the previous block by containing the hash of the latter. Modifying information in a block changes its hash, and the subsequent blocks should be changed in consequence. Blockchains then offer many guarantees, such as tamper resistance. The number of blocks since the genesis to the current is called the *height* of the blockchain, and there should ideally be only one block per height. The way blockchain systems are built (in particular how to add blocks) can be roughly separated in two classes: (i) *forkable* blockchains, where for each height, one participant is drawn at random and has the charge to produce a new block; or (ii) *committee-based* blockchains, where for each height, a committee is selected and is in charge of agreeing on which block to append next.

Forkable blockchains are the most famous and the most popular. There are many techniques to build such blockchains. The protocol to add a new block in the most popular

24th International Conference on Principles of Distributed Systems (OPODIS 2020).
Editors: Quentin Bramas, Rotem Oshman, and Paolo Romano; Article No. 12; pp. 12:1–12:16
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

blockchains (Bitcoin [22], Ethereum [25]) is called *proof-of-work* (PoW), introduced in [13]. In PoW, a participant needs to prove that it worked to have the right to add the next block. More in details, for a participant to be selected to add a block in the blockchain, it has to be the first to resolve a crypto-puzzle: the more computing power, the higher the chances are to win. This gives rise to many problems, first to increase the chance to solve the problem faster, one needs specialized equipment and a lot of computing power. All participants do these computations, but there is only one winner. These non-environment-friendly computations are not useful other than to solve the crypto-puzzle. Another issue with PoW is that although the probability of having multiple winners at the same time is extremely low, it is not impossible. From time to time, there are multiple winners and blocks proposed for the same height; these are called *forks*, and to ensure consistency and avoid double-spending, fork management should be implemented. To try solving these issues, some blockchains propose to replace the PoW with other protocols such as *proof-of-stake*, *e.g.*, Ouroboros [18]. In proof-of-stake, the more stakes a stakeholder has in the blockchain, the higher are its chances to add a block to the chain. This solves the problem of energy consumption, but not the presence of fork; the selection of the leader is somehow still random. Proof-of-stake may also introduce some concentration of power by the richest stakeholders. Other *proof-of-** proposals have been made, but all suffer from the fork issue, and sometimes many more.

On the other hand, there are committee-based blockchains, *e.g.*, Algorand [16], HotStuff [26], Tendermint [7], *etc.* They have the purpose of avoiding forks by relying, instead of one participant drawn at random for each block, on a committee that has to agree on the next block to add. The committees run blockchain consensus algorithms. Those algorithms are inspired by well-known algorithmic techniques such as the one from classical consensus [8, 12, 19, 21, 24]. Committee-based blockchains can guarantee the absence of forks. Compared to Bitcoin and proof-fo-work blockchains, committee-based blockchains seem slower since they require many messages to be exchange, and the selection of the committee members is a complex problem.

In both cases, forkable or non-forkable, blockchain systems usually have economical or financial advantages, specifically for block creators. These advantages serve to give an incentive to maintain the blockchain. With advantages given, participants of such systems may try to maximize their profit. Those participants do not necessarily want to harm the system; they often want to stay in the system but gain the most from it. Such participants are called *rational.* To avoid blockchains collapsing due to the presence of rational participants, we must study them, and ensure that the blockchain consensus properties always hold.

Contributions. In this work, we analyze the behavior of rational participants in committee-based blockchains. We show the different equilibria that exist given different methods of rewarding the committee members. We analyze if the equilibria do satisfy the consensus specifications or not. In particular, we found that there always exist equilibria that satisfy the blockchain consensus properties, but these equilibria are not unique and coordination failures may occur, leading to liveness issues. Let ν be the number of votes required for a block to be considered produced. The different equilibria are summarized in Table 1.

Additionally, we introduce the notion of "trembling hand" which to the best of our knowledge is a novelty in distributed systems. The trembling hand can be viewed as a failure of rational participants. The idea of trembling hand and acknowledging errors has been studied in different fields, such as in economics (*e.g.*, [11]), in networks (*e.g.*, [10]), *etc.* With low probability, the player can tremble and do an unintended action. We conduct the same equilibrium analysis and found that there exist equilibria satisfying the consensus properties.

Table 1 Summary of the Equilbria with Rational Players.

	Reward All	Reward Only Senders
$\nu = 1$	Proposition 5 In equilibrium, exactly one message is sent: **Consensus**	Proposition 1 In equilibrium, All players send a message: **Consensus; but inefficient: too costly**
$\nu > 1$	Proposition 7 In equilibrium, either: - No message is sent: **No Termination: No block, coordination failure**, or - Exactly ν messages are sent. **Consensus**	Proposition 3 In equilibrium, either: - No message is sent: **No Termination: No block, coordination failure**, or - All players sent a message: **Consensus; but inefficient: too costly**

Table 2 Summary of the Equilbria with "Trembling" Players.

	Reward All	Reward Only Senders
$\nu = 1$	Proposition 13 In the equilibrium, one message sent if valid: **Consensus**	Proposition 9 In the equilibrium, either - n messages always sent: **Validity not guaranteed** - n messages sent only if valid: **Consensus**
$\nu > 1$	Proposition 15 In equilibrium, either: - No message is sent: **No Termination** - $\nu - 1$ messages always sent + 1 if valid: **Consensus**	Proposition 11 In equilibrium, either: - No message is sent: **No Termination** - (if $\nu < n$) n messages always sent: **Validity not guaranteed** - $\nu - 1$ messages always sent + $(n - \nu + 1)$ if valid: **Consensus**

However, there also exist equilibria inducing liveness or safety issues because the consensus properties cannot be guaranteed. Equilibria with trembling participants are summarized in Table 2. In all cases, we found that equilibria, when all committee members are rewarded, are efficient in terms of the number of messages.

Related work. Many analyses have been made on strategic behaviors in blockchains. However, they mainly focus on forkable systems (*e.g.*, [6, 14]). To the best of our knowledge, very few works have been dedicated to analyze or discuss the rational behaviors among participants in committee-based blockchains. Some exceptions have to be noted.

The work of Abraham *et al.* in [2] is probably the first to consider strategic behaviors in committee-based blockchains. They introduced interesting incentive mechanisms, but did not provide a formal framework for their analysis, nor did they consider the cost of the actions.

Recently, Fooladgar *et al.* show in [15] that the proposed reward distribution in Algorand does not lead to an equilibrium. Interestingly, as in our paper, [15] considers the cost of actions of the players; but as opposed to us, among other things, players have basically one action, either following the protocol or not, so it either incurring all costs or no cost at all. In our work, we refine the approaches; We consider that multiple actions are available to the players, and that they just pay the costs of the actions they did, and not all of them.

In [4], we provide a framework for the analysis of strategic behaviors in the presence of rational players can either exhibit strategic or adversarial behaviors for committee-based blockchains. We however only considered one reward mechanism and did not study trembling hand effects. In this work, we extend the model in [4]; we consider systems with participants that behave strategically and can exhibit trembling hand effects. Additionally, in this work, we study the behavior of the participants under different reward schemes, as opposed to [4].

Previous works studying rational behavior in consensus algorithms (such as [1, 17, 20]) did not take into consideration the rewards given when a decision is reached, nor the cost of participants' actions. They usually proposed incentive-compatible protocols. Blockchains highlighting the costs and rewards, we take them into account in our analysis.

2 Model

2.1 System Model

We consider a system composed of a finite and ordered set Π of n players, called *committee*, of synchronous sequential players denoted by their index, namely $\Pi = \{1, \dots, n\}$.

Communication. The players communicate by sending and receiving messages through a *synchronous network*. We assume that the players proceed in rounds. A *round* consists of three sequential phases, in order: the send, the delivery and the compute phase. Since we consider synchronous communication, there is a known upper bound on the message transfer delay. Such upper bound is used by the players to set the duration of their rounds, in particular, the duration of the delivery phase is such that for all players, all messages sent at the beginning of the round are received before the end of the delivery phase. At the end of a round, a player exits from the current round and starts the next one. We assume the existence of a *reliable broadcast* primitive. A broadcast is reliable if the following conditions hold: (i) safety: every message delivered by a player has been previously sent by a source, and (ii) liveness: every player eventually delivers every message sent by a source. Messages are created with a digital signature, and we assume that digital signatures cannot be forged. When a player i delivers a message, it knows the player j that created the message.

Players Behavior. We consider that players are *rational*. Rational players are self-interested and their objective is to maximize their expected gain. They will deviate from a prescribed protocol if and only if doing so increases their expected gain. They differ from honest players who always follow the prescribed protocol.

We also consider trembling players. With low probability, an external function can return an unexpected value. They do not want such value, but are not in control of that, and are not aware when the returning value is "normal" or not. They only know the probability of such an event happening. A trembling player is also a rational player.

2.2 Consensus in Presence of Rational Players

A blockchain is a growing sequence of blocks. The number of blocks since the genesis to the current is called the height of the blockchain. In committee-based blockchains, for each height, a committee is selected and is in charge of agreeing on which block to append next.

As proposed by many articles (*e.g.*, [3], [5], [9], [16], [26], ...), committee-based blockchains can be developed using consensus algorithms. In particular, at each height, the protocol used by the corresponding committee must implement the consensus. In the section, we adapt the definition of consensus properties to take into account the presence of rational players.

We say that a protocol is a consensus algorithm in presence of rational players if the following properties hold:

- *Termination:* every rational player decides on a value (a block);
- *Agreement:* if two rational players decide respectively on values B and B', then $B = B'$;
- *Validity*: a decided value by any rational player is valid; w.r.t a predefined predicate.

Problem. We study the behavior of rational players in a consensus protocol. The goal is to know whether consensus is guaranteed in committee-based blockchains in the presence of rational players. For the study, we use the notion of *Nash equilibrium*, which is intuitively a "stable" situation where no player has an incentive to unilaterally deviate.

The question we answer is: *What are the different Nash equilibria and do they satisfy the consensus properties?* It is important to note that we do not propose a protocol such that all rational behave as honest, but rather study the behavior of rational players in a blockchain consensus algorithm under different reward mechanisms.

2.3 Protocol Studied

In committee-based blockchains, for each height, there is a committee supposed to reach a consensus on the block to append. The agreement procedure can be seen as a vote in potentially multiple sequential rounds. Focusing on one height, the consensus procedure is as follows. For each round:

- A proposer is selected for the current round. The proposer of the round proposes a block (the proposal) and send it to the rest of the committee members.
- Once a player receives the proposal, it should check its validity and vote (by sending a message) for the block only if it is valid; otherwise, it should not vote if invalid.

At the end of the round, all committee members collect the vote messages and count them. Let ν be the number of votes required for a block to be considered produced (the decision of the consensus). If the proposal receives votes for at least ν different committee members, then the block is consider *produced*; otherwise the next round starts with a new proposer, proposing a new block and the procedure restarts until a decision is made. When a player considers a block produced (*i.e.*, collects ν votes for the block), due to the communication model we consider, all players will also consider the block as produced since they have the same set of messages at the end of any round.

As explained above, these two phases encapsulate the main and important ideas of consensus protocol for committee-based blockchains. Moreover, Chan and Shi in [9], extended this two phases approach (Propose and Vote) to present multiple algorithms for different communication and failures models; pointing out the importance and sufficiency of these phases in consensus algorithms for blockchains.

In the following, we describe the actions rational players have. We present it as a protocol shown in Algorithm 1. Definition of the game and actions is done in the next section. We consider the choice of (i) checking or not the validity of a block and (ii) sending or not the vote for a proposed block. We consider that the actions of checking the validity of the block and of sending the message (of type vote) are costly.

Protocol of Rational Players. Rational players have some freedom at executing the prescribed protocol. We represent their possible actions in Algorithm 1, where specific variables have been introduced; namely,

- $action^{\text{check}} \in \{\texttt{false}, \texttt{true}\}$, if the player decides to check the validity of the proposal or not; and
- $action^{\text{send}} \in \{\texttt{false}, \texttt{true}\}$, if the player decides to vote for the proposal or not (depending on the validity information the player has about the proposal).

$\texttt{isProposer}(t, h)$ returns the identifier of the proposer for the current round (line 10).

All players sets their actions locally, in more details, player i sets its action variable $action^{\text{check}}$ (resp. $action^{\text{send}}$) by calling the dedicated function σ_i^{check} (resp. σ_i^{send}) representing its strategy.

The strategy σ_i^{check} determines if i, the receiving player, chooses to check the validity of the proposal or not, which is a costly action. If the player chooses to check the validity (line 17), it will also update the knowledge it has about the validity of the proposal and it will pay a cost c_{check}. If otherwise, the player keeps not knowing if the proposal is valid or

Algorithm 1 Pseudo-code for a given height h modeling the rational player i's behavior.

```
1:  Initialization:
2:    $vote := nil$
3:    $t := 0$                                                   /* Current round number */
4:    $decidedValue := nil$
5:    $action^{\text{check}} := nil$
6:    $action^{\text{send}} := nil$
7:    $validValue[] := \{\bot, \bot, \ldots, \bot\}$                /* $validValue[r] \in \{\bot, \texttt{false}, \texttt{true}\}$ */

8:  Round PROPOSE($t$) :
9:    Send phase:
10:     if $i == \texttt{isProposer}(t, h)$ then
11:       $proposal \leftarrow \texttt{createValidValue}(h)$
12:       broadcast $\langle \mathsf{PROPOSE}, h, t, proposal \rangle$
13:   Delivery phase:
14:     delivery $\langle \mathsf{PROPOSE}, h, t, v \rangle$ from $\mathsf{proposer}(h, t)$
15:   Compute phase:
16:     $action^{\text{check}} \leftarrow \sigma_i^{\text{check}}()$   /* $\sigma_i^{\text{check}}() \in \{\texttt{false}, \texttt{true}\}$ sets the action of checking or not the validity of the
        proposal */
17:     if $action^{\text{check}} == \texttt{true}$ then
18:       $validValue[r] \leftarrow \texttt{isValid}(v)$            /* The execution of $\texttt{isValid}(v)$ has a cost $c_{\text{check}}$ */
19:     $action^{\text{send}} \leftarrow \sigma_i^{\text{send}}(validValue)$ /* $\sigma_i^{\text{send}} : \{\bot, \texttt{false}, \texttt{true}\} \rightarrow \{\texttt{false}, \texttt{true}\}$ sets the action of sending the
        vote or not */
20:     if $action^{\text{send}} == \texttt{true}$ then
21:       $vote \leftarrow v$                /* The player decides to send the vote, the proposal might be invalid */

22: Round VOTE($t$) :
23:   Send phase:
24:     if $vote \neq nil$ then
25:       broadcast $\langle \mathsf{VOTE}_i, h, t, vote \rangle$           /* The execution of the broadcast has a cost $c_{\text{send}}$ */
26:   Delivery phase:
27:     delivery $\langle \mathsf{VOTE}, h, t, v \rangle$          /* The player collects all the votes for the current height and round */
28:   Compute phase:
29:     if $|\langle \mathsf{VOTE}, h, t, v \rangle| \geq \nu \wedge decidedValue = nil \wedge vote \neq nil \wedge vote = v$ then
30:       $decidedValue = v$; exit
31:     else
32:       $vote \leftarrow nil$
33:       $t \leftarrow t + 1$
```

not (*validValue*[t] remains at $\bot$). Note that this value remains at $\bot$ even if the player is the proposer. This is because we assumed, without loss of generality, that checking validity has a cost and that the only way of checking validity is by executing the `isValid`(v) function.

Note that the strategy σ_i^{send} depends on the knowledge the player has about the validity of the proposal. The strategy determines if the player chooses to send its vote for the proposal or not (line 19 - 25). If the player chooses to vote for the proposal, it will pay a cost c_{send}.

Let us note that a rational player that did not check the validity of the block could consider as decision of the committee an invalid value if it collects more than ν votes for an invalid proposal. We also note that in the model model considered, the Agreement property always holds, since, at the end of each round, all players have the same set of messages delivered.

Note that the creation of proposal (line 11 of Algorithm 1) will be subject to the trembling hand effect in Section 5.

2.4 Game

Action space. At each round t, when a player receives the proposal, it decides whether to check the block's validity or not (at cost c_{check}), and then given the validity information, it decides whether to send a vote message (at cost c_{send}) or not.

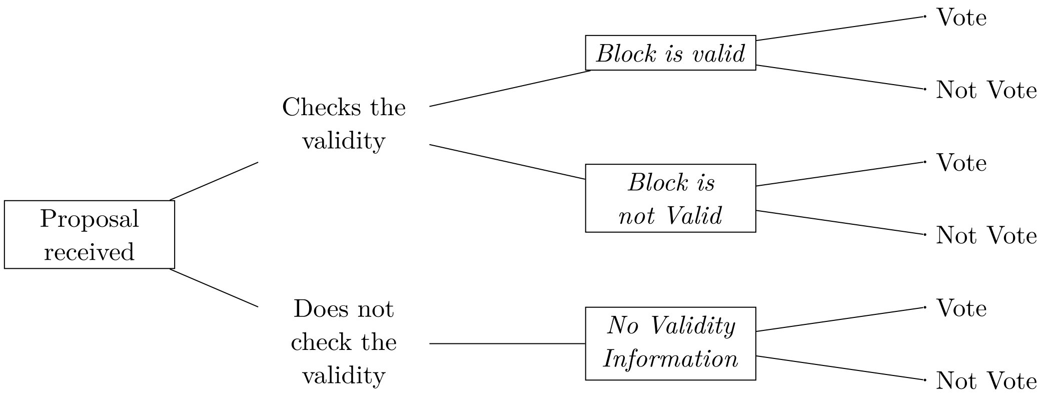

Figure 1 Decision Tree of one Player after Reception of the Proposal.

Information sets. At the beginning of each round $t > 1$, the information set of the player, η_i^t, includes the observation of the round number t, as well as the observation of what happened in previous rounds, namely (i) whether the player decided to check validity, and in that case, it knows the validity of the block, (ii) how many messages were sent, and (iii) whether a block was produced or not.

Then, in each round $t > 1$, the player decides whether to check the validity of the current block. At this point, denoting by b_t the block proposed at round t, when the player does not decide to check validity $\texttt{isValid}(b_t)$ is the null information set, while if the player decides to check, $\texttt{isValid}(b_t)$ is equal to 1 if the block is valid and 0 otherwise. Therefore, at this stage, the player information set becomes $H_i^t = \eta_i^t \cup \texttt{isValid}(b_t)$, which is η_i^t augmented with the validity information player i has about b_t, the proposed block.

Strategies. At each round $t \geq 1$, the strategy of player i is a mapping from its information set into its actions. At the point at which the player can decide to check block validity, its strategy is given by $\sigma_i^{\text{check}}(\eta_i^t)$. Finally, after making that decision, the player must decide whether to vote or not, and that decision is given by $\sigma_i^{\text{send}}(H_i^t)$. The decision tree of a player is depicted in Figure 1. We note that when the player does not check the validity of the proposal, it does not know if the block is valid or not.

We denote by $\sigma = (\sigma_1, \ldots, \sigma_n)$ the *strategy profile* where $\forall i \in \{1, \ldots, n\}$, player i use strategy σ_i, where $\sigma_i(H_i^t)$ is the pair $(\sigma_i^{\text{check}}(\eta_i^t), \sigma_i^{\text{send}}(H_i^t))$.

Rewards and Costs for the Players. We study the cases in which:

1. when a block is produced, only the committee members which voted are rewarded (and receive R); or
2. whenever a block is produced, all committee members are rewarded (and receive R).

We will explicitly state the case we are studying.

We also assume that when an invalid block is produced, all players incur a cost κ[1]. Note that κ is not incurred when no block is produced. We assume that the reward R, is larger than the cost c_{check} of checking validity, which is larger than the cost c_{send} of sending a vote message. Lastly, the reward obtained is smaller than the cost κ of producing an invalid block. That is, $\kappa > R > c_{\text{check}} > c_{\text{send}} > 0$.

[1] Such a cost corresponds, for example, to the loss of confidence in the blockchain system caused by the invalid block produced, hence hurting the whole ecosystem.

Objective of Rational Players. Let T be the round at which the game stops. If a block is produced at round $t \leq n$, then $T = t$. Otherwise, if no block is produced, $T = n + 1$. In the latter case, the *termination* property is not satisfied. In our analyses, we focus on what happens during the first round; in particular, when $T \geq 2$, we say that termination is not satisfied at round 1.

As explained above, we study two types of rewards. The analyses are done independently. In each setting, all rational players have the same gain function detailed in the following when we focus only on the first round.

1. **Reward Only Sender**: When the reward is given only to players that vote for the produced block, for the first round, the expected gain of rational player i is:

$$U_i(\sigma) = E\left[\begin{array}{c} R * \mathbb{1}_{(\sigma_i^{\text{send}}(H_i^1) \wedge \text{block produced at round 1})} - c_{\text{send}} * \mathbb{1}_{\sigma_i^{\text{send}}(H_i^1)} \\ -c_{\text{check}} * \mathbb{1}_{\sigma_i^{\text{check}}(\eta_i^1)} - \kappa * \mathbb{1}_{(\text{invalid block produced at round 1})} \end{array}\right], \tag{1}$$

   where $\mathbb{1}_{(.)}$ denotes the indicator function, taking the value 1 if its argument is true, and 0 if it is false.

2. **Reward All**: When the reward is given to the whole committee once a block is produced, for the first round, the expected gain of rational player i is:

$$U_i(\sigma) = E\left[\begin{array}{c} R * \mathbb{1}_{(\text{block produced at round 1})} - c_{\text{send}} * \mathbb{1}_{\sigma_i^{\text{send}}(H_i^1)} \\ -c_{\text{check}} * \mathbb{1}_{\sigma_i^{\text{check}}(\eta_i^1)} - \kappa * \mathbb{1}_{(\text{invalid block produced at round 1})} \end{array}\right]. \tag{2}$$

Equilibrium concept. We consider the players are playing Nash equilibria, and we focus only on their behavior during the first round.

Let $\sigma = (\sigma_1, \ldots, \sigma_n)$ be a strategy profile, where σ_i is the strategy of player i. We write (σ_{-i}, σ'_i) to represent the strategy profile $(\sigma_1, \ldots, \sigma_{i-1}, \sigma'_i, \sigma_{i+1}, \ldots, \sigma_n)$ where player i deviates, and the others continue playing their strategy. A strategy profile is a *pure Nash equilibrium* [23] if no player can increase its gain by unilaterally deviating. Formally, σ is a pure Nash equilibrium if and only if $\forall i \in \{1, \ldots, n\}$, and $\forall \sigma'_i$ a strategy for i, $U_i(\sigma) \geq U_i((\sigma_{-i}, \sigma'_i))$. We simply use *Nash equilibrium* instead of pure Nash equilibrium.

The following sections present our results.

In Sections 3 & 4, we do not have trembling hand effects, therefore, we cannot have invalid blocks since the proposal should be valid (line 11 of Algorithm 1). Focusing on liveness issues, we study whether players vote or not in equilibria.

In Section 5, trembling effects are considered, and the proposal may be invalid. Therefore, for safety reasons, players may check the proposal's validity before voting or not.

3 Reward Only Committee Members that Vote

In this section, we consider that only committee members that voted for a produced block are rewarded. Equation 1 describes the gain of each rational player.

We study the different equilibria with respect to the value of ν, the minimum number of votes required to consider a block as produced.

First, we analyze the case where 1 vote for a proposed block is sufficient to considered it as produced, *i.e.*, $\nu = 1$.

▶ **Proposition 1.** *In one round, with only rational players in the committee, if $\nu = 1$, and when only players that vote for the produced block are rewarded, there is only one Nash equilibrium. In the unique equilibrium, all players vote for the proposed block.*

In this equilibrium, all players vote, and the block is produced. No player has an incentive to deviate and not send, such deviation will mean for the player that it will not be rewarded while the block is produced.

▶ Remark 2. Note that in the Nash equilibrium of Proposition 1, the consensus properties are satisfied, in particular, there is always a block produced at the end of the first round.

We now consider the situation where strictly more than one vote is needed to consider a block as produced, *i.e.*, $\nu \in \{2, \ldots, n\}$.

▶ **Proposition 3.** *In one round, with only rational players in the committee, if $\nu > 1$, and when only players that vote for the produced block are rewarded, there are two Nash equilibria; either (i) all players vote, or (ii) no player votes.*

In the first equilibrium, if a rational player anticipates that no players will vote, its only vote will not make the proposal produced, since $\nu > 1$, therefore, the player prefers not voting. In the second type of equilibrium, if a player anticipates that all other players are voting, it prefers voting as well; otherwise, if the player does not send, it will not have a reward.

▶ Remark 4. There are two Nash equilibria in Proposition 3. In the equilibrium where no player votes, Termination is not guarantee at round 1. In the second equilibrium where there are n votes, the consensus properties are satisfied in the first round.

4 Reward All Committee Members

In this section, we consider that all committee members are rewarded once a block is produced. Equation 2 describes the gain of each rational player.

We study the different equilibria with respect to the value of ν, the minimum number of votes required to consider a block as produced.

First, we analyze the case where 1 vote for a proposed block is sufficient to considered it as produced, *i.e.*, $\nu = 1$.

▶ **Proposition 5.** *In one round, with only rational players in the committee, if $\nu = 1$, and when all players are rewarded once a block is produced, in the Nash equilibria, exactly one player votes, and the others do nothing.*

If the player supposed to vote does not vote, no block is produced, and hence it does not have any reward. Therefore, it prefers voting, since a block is always produced in equilibrium, if a player not supposed to send deviates and votes, it will pay the cost of sending for nothing since it will be rewarded even without voting.

▶ Remark 6. Note that there exists at most n equilibria corresponding to Proposition 5. In all the equilibria corresponding to Proposition 5, the consensus properties are satisfied.

We now consider the situation where strictly more than one vote is needed to consider a block as produced, *i.e.*, $\nu \in \{2, \ldots, n\}$.

▶ **Proposition 7.** *In one round, with only rational players in the committee, if $\nu > 1$, and when all players are rewarded once a block is produced, in the Nash equilibria, either (i) exactly ν players vote, or (ii) no player votes.*

If a rational player anticipates that no players will vote, since $\nu > 1$, its only vote will not make the proposal produced, therefore, it is better off not voting. In the other type of equilibrium, exactly ν players vote; if a player supposed to send does not vote, the block is not produced and the deviating player is not rewarded any more; if a player not supposed to send deviates (by voting) it will incur a cost of sending, when it will be rewarded in any case, so it prefers not to vote.

▶ Remark 8. There are two types of Nash equilibria in Proposition 7.

- The equilibrium where no player votes does not guarantee *Termination* at round 1.
- In the second type of equilibrium in this setting, there are exactly ν messages sent. There can be at most $\binom{n}{\nu} + 1$ equilibria corresponding to that setting[2]. In each of them, the consensus properties are satisfied.

A summary of the different equilibria in Sections 3 & 4 can be found in Table 1. When only 1 vote is required to consider a proposal as produced, in all equilibria, blocks are always produced. When we require strictly more than 1 vote to consider a block as produced, although there are equilibria where the consensus is guaranteed, there is also an equilibrium where no player votes, anticipating that the others will not vote as well: a coordination failure, leading to a violation of the Termination. This happens in the two reward mechanisms: reward all committee members, or reward only the members that voted. However, in the equilibria where all committee members are rewarded, less messages are sent, making it a more efficient (and less costly) mechanism with respect to the number of messages.

5 Trembling Players at Proposal

Now, we assume that there is some negligible probability p for the `createValidValue` function (line 11 of Algorithm 1) to return an invalid proposal, and all players are aware of the trembling effect. When proposing a value there is a probability that the hand of the player trembles and proposes an invalid block instead of a valid block; *i.e.*, in some sense, we take into account the possibility of making a mistake for the proposal.

Note that now, checking the validity of a block may be important, there is a risk of producing an invalid block, violating the validity property of the consensus. To ensure that the reward covers the costs of checking and voting, in this setting we assume that $(1-p)(R - c_{\text{send}}) - c_{\text{check}} > 0$. We also note that it is better for the player to vote (resp. not vote) without checking than checking and voting (resp. not voting) irrespective to the block validity; that would mean incurring a cost $-c_{\text{check}}$ for nothing. It is also not in their best interest to check the validity of the proposal and vote if the proposal is invalid, that would mean increasing the chances of producing an invalid block and incurring a cost $-\kappa$. In the analyses, we then consider only the three relevant strategies: a rational player can (i) vote without checking proposal validity, (ii) not vote nor check proposal validity, and (iii) check the proposal validity and vote only if the proposal is valid.

In the following, we make the same analyses as in Sections 3 & 4, *i.e.*, we analyze the behavior of rational players when only voters are rewarded; and their behaviors when all committee members are rewarded.

5.1 Reward Only Committee Members that Vote

In this subsection, we consider that only committee members that voted for a produced block are rewarded. Equation 1 describes the gain of each rational player.

[2] $\binom{n}{\nu} = C_n^{\nu}$ is the number of combinations for choosing ν out of n elements.

We study the different equilibria with respect to the value of ν, the minimum number of votes required to consider a block as produced.

First, we analyze the case where 1 vote for a proposed block is sufficient to consider it as produced, *i.e.*, $\nu = 1$.

▶ **Proposition 9.** *In one round, with only rational players in the committee, if $\nu = 1$, when only players that vote for the produced block are rewarded, and if there is a probability p that the proposer proposes an invalid block, there are two Nash equilibria. In equilibrium, either (i) if $\kappa \geq R - c_{send} + c_{check}/p$, all players check the validity of the proposal and vote only if it is valid; or (ii) all players vote for the proposal without checking the validity of the proposal.*

As in Proposition 1, one can note that in equilibrium, all players do (try to) vote.

▶ Remark 10. There are two Nash equilibria in Proposition 9. In the equilibrium where all players check and vote, if the proposal is invalid, there is no Termination at the first round, however Validity is always ensured. While in the second equilibrium where no player checks but votes, Termination is always guaranteed at the end of the first round, even if the proposal is invalid, which violates the Validity.

We now consider the situation where strictly more than one vote is needed to consider a block as produced, *i.e.*, $\nu \in \{2, \dots, n\}$.

▶ **Proposition 11.** *In one round, with only rational players in the committee, if $\nu > 1$, when only players that vote for the produced block are rewarded, and if there is a probability p that the proposer proposes an invalid block, there are three Nash equilibria. Either (i) no player votes nor checks the proposal validity; or (ii) if $\nu < n$, all players vote for the proposal without checking the validity of the proposal; or (iii) if $\kappa \geq R - c_{send} + c_{check}/p$, $n - \nu + 1$ players check the validity of the proposal and vote only if it is valid, and the $\nu - 1$ remaining players only vote without checking the validity of the proposal.*

Proof of Proposition 11. We prove that the strategy profiles described in the proposition are Nash equilibria.

- First, we prove that the strategy profile where no player votes is a Nash equilibrium. The gain at equilibrium of any player is 0. If one player deviates and votes, there is only 1 vote and the block is not produced since $\nu > 1$, the gain at deviation is $-c_{\text{send}} < 0$. If the player deviates by checking block validity, it will pay the cost $-c_{\text{check}} - (1-p)c_{\text{send}} < 0$. The strategy profile is indeed a Nash equilibrium.
- We now prove that the strategy profile where all players vote without checking the proposal validity is a Nash equilibrium. Let $\nu < n$, the gain at equilibrium of any player is $R - c_{\text{send}} - p\kappa$. Even if one player deviates, the block will be produced in any case (since $\nu < n$) no matter its validity. If a player deviates by checking validity and voting if the proposal is valid, its gain will be $(1-p)(R - c_{\text{send}}) - c_{\text{check}} - p\kappa$; if the player deviates and does not check proposal's validity nor votes, its expected gain at deviation is $-p\kappa$, the gain at deviation is lower than the gain at equilibrium. The strategy profile is indeed a Nash equilibrium.
- It remains to prove that the strategy profile where some players are supposed to check the proposal validity and check only if the block is valid and the remaining players vote without checking block validity is also a Nash equilibrium.

  We can first note that only valid blocks can be produced following the equilibrium, and invalid blocks do not have the necessary ν votes, since only $\nu - 1$ players vote without checking, and so for invalid proposal.

- The expected gain of a player not supposed to check is $(1-p)(R-c_{\text{send}})$. If it deviates and does not vote, its gain at deviation is 0; if it deviates by checking and voting only if the proposal is valid, its expected gain at deviation is $(1-p)(R-c_{\text{send}})-c_{\text{check}}$, which is lower than the gain at equilibrium.
- The expected gain of a player supposed to check is $(1-p)(R-c_{\text{send}})-c_{\text{check}}$. If it deviates and does not vote, its gain at deviation is 0. If it deviates by voting without checking the proposal's validity, any block proposed will be produced, no matter its validity since ν votes are sent in any case, so the expected gain of the deviating player is $R-c_{\text{send}}-p\kappa$, which is lower than the gain at equilibrium if and only if $\kappa \geq R-c_{\text{send}}+c_{\text{check}}/p$.

The strategy profile is indeed a Nash equilibrium.

Moreover, there is no more equilibrium. We sketch the proof by exhibiting the main other equilibrium candidates.

- Let $x \geq 0$. Assume by contradiction that there exists an equilibrium where $n-\nu-x$ players check the block validity and vote only if the proposal is valid, and the remaining $\nu+x$ players vote without checking the block validity.
  That means any block proposed will be produced, since $\nu+x \geq \nu$ players vote without checking validity. Let i be a player supposed to check. It expected gain is $R-c_{\text{send}}-c_{\text{check}}-p\kappa$, while if i deviates and votes without checking proposal validity, its expected gain will be $R-c_{\text{send}}-p\kappa$. Contradiction, the strategy profile is not an equilibrium.
- Let $x > 1$. Assume by contradiction that there exists an equilibrium where $n-\nu+x$ players check the block validity and vote only if the proposal is valid, and the remaining $\nu-x$ players vote without checking the block validity.
  Let i be a player supposed to check. It expected gain is $(1-p)(R-c_{\text{send}})-c_{\text{check}}$. If i deviates and votes without checking proposal validity, there will be $\nu-x+1<\nu$ votes for invalid an block proposed, and so it will not be produced, where there will be n votes for a valid block proposed; the expected gain at deviation for i is $(1-p)(R-c_{\text{send}})$. Contradiction, the strategy profile proposed is not an equilibrium. ◀

▶ Remark 12. There are three types of Nash equilibria in Proposition 11.

- The equilibrium where no player votes does not guarantee *Termination* at round 1.
- In the equilibrium where no player checks, Termination is always guaranteed at the end of the first round, even if the proposal is invalid, which violates the Validity property.
- In the last equilibrium, valid blocks are produced and invalid blocks are not. Termination is not guaranteed at round 1 but Validity is always ensured. There can be at most $\binom{n}{n-\nu+1}$ equilibria corresponding to that setting.

5.2 Reward All Committee Members

In this section, we consider that all committee members are rewarded once a block is produced. Equation 2 describes the gain of each rational player.

We study the different equilibria with respect to the value of ν, the minimum number of votes required to consider a block as produced.

First, we analyze the case where 1 vote for a proposed block is sufficient to consider it as produced, *i.e.*, $\nu = 1$.

▶ **Proposition 13.** *In one round, with only rational players in the committee, if $\nu = 1$, when all players are rewarded once a block is produced, if there is a probability p that the proposer proposes an invalid block, and if $\kappa \geq R - c_{send} + c_{check}/p$, in all Nash equilibria, exactly one player checks the validity of the proposal and votes only if it is valid, while the other players do nothing.*

As in Proposition 5, one can note that in equilibrium, the task of validating (checking) and producing a block is delegated to one player.

▶ Remark 14. Note that there exists at most n equilibria corresponding to Proposition 13. In all the equilibria corresponding to Proposition 13, if the proposal is invalid, there is no Termination at the first round, however, Validity is always ensured.

We now consider the situation where strictly more than one vote is needed to consider a block as produced, *i.e.*, $\nu \in \{2, \dots, n\}$.

▶ **Proposition 15.** *In one round, with only rational players in the committee, if $\nu > 1$, when all players are rewarded once a block is produced, if there is a probability p that the proposer proposes an invalid block, and if $\kappa \geq R - c_{send} + c_{check}/p$, in all Nash equilibria, either (i) no player votes, or (ii) 1 player checks the proposal validity and votes only if it is valid, exactly $\nu - 1$ other players vote without checking validity, and the others do nothing.*

Proof of Proposition 15. We prove that the strategy profiles described in the proposition are Nash equilibria.

- First, we prove that the strategy profile where no player votes is a Nash equilibrium. The gain at equilibrium of any player is 0. If one player deviates and votes, there is only 1 vote, and the block is not produced since $\nu > 1$, the gain at deviation is $-c_{\text{send}} < 0$. If the player deviates by checking block validity, it will pay the cost of checking for nothing and will have the gain $-c_{\text{check}} - (1 - p)c_{\text{send}} < 0$. The strategy profile is a Nash equilibrium.
- It remains to prove that the strategy profile where some players are supposed to check the proposal validity, and vote only if the block is valid; some players vote without checking block validity; and the others do nothing is a Nash equilibrium.

  We first note that only valid blocks can be produced following the equilibrium, and invalid blocks do not have the necessary ν votes, since only $\nu - 1$ players vote without checking.
  - First, the players that do not vote nor check validity have an expected gain of $(1-p)R$. Let i be such a player. If i deviates and votes without checking, any proposal will be produced, no matter its validity, therefore, the gain of the player at deviation is $R - c_{\text{send}} - p\kappa$, which is lower than the gain at equilibrium. If instead, i deviates and checks the validity of the proposal and votes only if it is valid, only valid blocks will be produced, so the gain at deviation will be $(1 - p)(R - c_{\text{send}}) - c_{\text{check}}$, which is lower than the gain at equilibrium.
  - Now, turns to the players not supposed to check but vote. Their expected gain at equilibrium is $(1 - p)R - c_{\text{send}}$. Let i be such a player, if it deviates and does not vote nor checks, no block will be produced and its gain at deviation is $0 < (1 - p)R - c_{\text{send}}$. If it deviates by checking and voting only if the proposal is valid, its expected gain at deviation is $(1 - p)(R - c_{\text{send}}) - c_{\text{check}}$, which is lower than the gain at equilibrium since $c_{\text{send}} < c_{\text{check}}$.
  - Finally, we can analyze the one player supposed to check. Without loss of generality, assume that it is player with index 1. The expected gain of player 1 is $(1 - p)(R - c_{\text{send}}) - c_{\text{check}}$. If it deviates and does not vote, no block will be produced, so its gain at deviation is $0 < (1 - p)(R - c_{\text{send}}) - c_{\text{check}}$; if it deviates by voting without checking the proposal's validity, any block proposed will be produced, no matter its validity since ν votes are sent in any case; therefore, the expected gain of player 1 at deviation is $R - c_{\text{send}} - p\kappa$, which is lower than the gain at equilibrium if and only if $\kappa \geq R - c_{\text{send}} + c_{\text{check}}/p$.

  The strategy profile is indeed a Nash equilibrium. No deviation is profitable.

There is no more equilibrium in this setting.

First, let us note that in any case, exactly ν players should vote (counting also those supposed to vote after checking). If there are less than ν players supposed to vote (but at least one), no block is produced so one such player can deviate and not vote, economizing its cost. If there are more than ν players supposed to vote, one can deviate by not voting and economizing that cost.

We can show that the other main equilibrium candidates are not equilibria.

- By contradiction, assume that there exists an equilibrium where ν players vote without checking the proposal's validity and the others do not vote nor check.
  Let i be a player supposed to vote. It expected gain at equilibrium $R - c_{\text{send}} - p\kappa$, while if i deviates by checking the proposal validity and voting only if valid, only valid proposal will be produced, so its expected gain will be: $(1-p)(R - c_{\text{send}}) - c_{\text{check}}$ which is greater than the equilibrium. Contradiction, the strategy profile is not an equilibrium.
- By contradiction, assume that there exists an equilibrium where ν players vote (counting also those supposed to vote after checking) and the others do not vote nor check. Suppose that in the set of players supposed to vote, at least two i and j check the validity of the proposal and vote only if it is valid. In this strategy profile, only valid proposals will be produced. The expected gain at equilibrium of i is $(1-p)(R - c_{\text{send}}) - c_{\text{check}}$. If instead, i deviates and always votes without checking validity, its expected gain at deviation is $(1-p)R - c_{\text{send}}$, which is greater than the gain at equilibrium. Contradiction, the strategy profile is not an equilibrium. ◀

▶ Remark 16. There are two types of Nash equilibria in Proposition 15.

- Termination is not guaranteed at round 1 in the equilibrium where no player votes.
- In the second type of equilibrium in this setting, there are exactly ν votes when the proposal is valid, but $\nu - 1$ votes when the proposal is invalid. Termination is not guaranteed at round 1 but Validity is ensured. There can be at most $n * \binom{n-1}{\nu-1}$ equilibria corresponding to that setting.

A summary of the different equilibria with trembling players can be found in Table 2. When all players are rewarded once a block is produced, there is no "bad" equilibrium, *i.e.*, an equilibrium where Validity is violated, while when only players that vote for a produced block are rewarded when $\nu < n$, there exists a "bad" equilibrium (Propositions 9 and 11).

6 Discussions

Before concluding, we discuss some interesting points that are not directly addressed in the core of this paper.

Fixed amount of Reward for the Committee. First, we quickly highlight what happens if there is a fixed reward for the committee members that is shared by them. Let μ be the number of players that are rewarded in the committee, and let $\frac{R}{\mu}$ be the fraction of the reward each player rewarded gets. Our equilibrium analysis still holds, but attention should be given to the bounds. For example, in Proposition 9, instead of $\kappa \geq R - c_{\text{send}} + c_{\text{check}}/p$ we should have $\kappa \geq R/n - c_{\text{send}} + c_{\text{check}}/p$, since all players vote in case of a valid proposal. (here, $\mu = n$).

Honest Players. Recall that honest players always follow the prescribed protocol, *i.e.*, they always check the validity of the proposal, and vote only if the proposal is valid.

We did not include honest players in this paper for the following reason: their presence does not change the different equilibria we have; they may however change the bounds under which some equilibria exist.

Denote by h the number of honest players in the committee. Generally, if there are h honest players and ν messages are required for the production of a block, h votes are guaranteed for valid blocks only; then for the rational players, the goal is to give the $\nu - h$ remaining votes.

7 Conclusion

We analyze the behavior of rational players in committee-based blockchains under assumptions of synchrony of messages and under different mechanisms of rewards. Although our analysis focuses on a single round, the behaviors of the rational players can be repeated in multi-round settings, since each new round has the same setting as the first round, and therefore, be viewed as independent. This paper study the case where there is one proposer at the time and does not consider the case of multiple proposers as in Algorand which has multiple proposers at the same time and rely on probabilistic consensus while we consider only deterministic consensus. We found that although there always exist equilibria where the consensus properties are guaranteed, there also exist equilibria, where those properties are violated, both in the case where the proposal is always valid, or by trembling effect can be invalid. When all committee members are rewarded once a block is produced, in equilibrium, the validity property is always guaranteed; while rewarding only those who vote for the produced block leads to the existence of equilibrium where an invalid block can be produced. Moreover, equilibria when all committee members are rewarded are more efficient in terms of the number of messages. Thus, rewarding all members of the committee seems to be an interesting reward scheme, and need more investigations, in particular in more general settings.

In this work, we consider only the game representing the consensus agreement in committee-based blockchains, from a liveness point of view. Interestingly, it helps clearly identifying coordination problems that are likely to be present in more general settings.

References

1 Ittai Abraham, Danny Dolev, and Joseph Y. Halpern. Distributed protocols for leader election: A game-theoretic perspective. *ACM Trans. Economics and Comput.*, 7(1), 2019.

2 Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Alexander Spiegelman. Solidus: An incentive-compatible cryptocurrency based on permissionless byzantine consensus. *CoRR*, abs/1612.02916v1, 2016.

3 Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Alexander Spiegelman. Solida: A blockchain protocol based on reconfigurable byzantine consensus. In *OPODIS 2017, Lisbon, Portugal*, 2017.

4 Yackolley Amoussou-Guenou, Bruno Biais, Maria Potop-Butucaru, and Sara Tucci-Piergiovanni. Rational vs byzantine players in consensus-based blockchains. In *AAMAS '20, Auckland, New Zealand*, 2020.

5 Yackolley Amoussou-Guenou, Antonella Del Pozzo, Maria Potop-Butucaru, and Sara Tucci-Piergiovanni. Correctness of tendermint-core blockchains. In *OPODIS 2018, Hong Kong, China*, 2018.

6 Bruno Biais, Christophe Bisière, Matthieu Bouvard, and Catherine Casamatta. The blockchain folk theorem. *The Review of Financial Studies*, 32(5), April 2019.

7 Ethan Buchman, Jae Kwon, and Zarko Milosevic. The latest gossip on BFT consensus. Technical report, Tendermint, July 2018. arXiv:1807.04938.

8 Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *OSDI'99, New Orleans, Louisiana, USA, February 22-25, 1999*, 1999.

9 Benjamin Y. Chan and Elaine Shi. Streamlet: Textbook streamlined blockchains. *IACR Cryptol. ePrint Arch.*, 2020.

10 Simon Collet, Pierre Fraigniaud, and Paolo Penna. Equilibria of games in networks for local tasks. In *OPODIS 2018, Hong Kong, China*, 2018.

11 Fiery Cushman, Anna Dreber, Ying Wang, and Jay Costa. Accidental Outcomes Guide Punishment in a "Trembling Hand" Game. *PloS one*, 4(8), 2009.

12 Cynthia Dwork, Nancy A. Lynch, and Larry J. Stockmeyer. Consensus in the presence of partial synchrony. *J. ACM*, 35(2), 1988.

13 Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *CRYPTO '92, Santa Barbara, California, USA*, 1992.

14 Ittay Eyal and Emin Gün Sirer. Majority is not enough: bitcoin mining is vulnerable. *Commun. ACM*, 61(7), 2018.

15 Mehdi Fooladgar, Mohammad Hossein Manshaei, Murtuza Jadliwala, and Mohammad Ashiqur Rahman. On incentive compatible role-based reward distribution in algorand. *CoRR*, 2019.

16 Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *SOSP 07, Shanghai, China*, 2017.

17 Joseph Y. Halpern and Xavier Vilaça. Rational consensus: Extended abstract. In *PODC 2016, Chicago, IL, USA, July 25-28*, 2016.

18 Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *CRYPTO '17, Santa Barbara, CA, USA*, 2017.

19 Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3), July 1982.

20 Anna Lysyanskaya and Nikos Triandopoulos. Rationality and adversarial behavior in multi-party computation. In *CRYPTO 2006, Santa Barbara, California, USA*, 2006.

21 Jean-Philippe Martin and Lorenzo Alvisi. Fast byzantine consensus. *IEEE Transactions on Dependable and Secure Computing*, 3(3):202–215, July 2006.

22 Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

23 John Nash. Non-cooperative games. *Annals of Mathematics*, 54(2), 1951.

24 Sam Toueg. Randomized byzantine agreements. In *Third Annual ACM Symposium on Principles of Distributed Computing, Vancouver, Canada*, 1984.

25 Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151, 2014.

26 Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan-Gueta, and Ittai Abraham. Hotstuff: BFT consensus with linearity and responsiveness. In *PODC 2019, Toronto, Canada*, 2019.