

Achieving State Machine Replication without Honest Players

Conor McMenamin
Universitat Pompeu Fabra
Barcelona, Spain
conor.mcmenamin@upf.edu

Vanesa Daza
Universitat Pompeu Fabra
Barcelona, Spain
CYBERCAT - Center for
Cybersecurity Research of Catalonia
vanesa.daza@upf.edu

Matteo Pontecorvi
NOKIA Bell Labs
Nozay, France
matteo.pontecorvi@nokia.com

ABSTRACT

Existing standards for player characterisation in tokenised state machine replication protocols depend on honest players who will always follow the protocol, regardless of possible token increases for deviating. Given the ever-increasing market capitalisation of these tokenised protocols, honesty is becoming more expensive and more unrealistic. As such, this out-dated player characterisation must be removed to provide true guarantees of safety and liveness in a major stride towards universal trust in state machine replication protocols and a new scale of adoption. As all current state machine replication protocols are built on these legacy standards, it is imperative that a new player model is identified and utilised to reflect the true nature of players in tokenised protocols, now and into the future.

To this effect, we propose the ByRa player model for state machine replication protocols. In the ByRa model, players either attempt to maximise their tokenised rewards, or behave adversarially. This merges the fields of game theory and distributed systems, an intersection in which tokenised state machine replication protocols exist, but on which little formalisation has been carried out. In the ByRa model, we identify the properties of strong incentive compatibility in expectation and fairness that all protocols must satisfy in order to achieve state machine replication. We then provide Tenderstake, a protocol which provably satisfies these properties, and by doing so, achieves state machine replication in the ByRa model.

CCS CONCEPTS

• Security and privacy → Distributed systems security; • Theory of computation → Algorithmic game theory.

KEYWORDS

Blockchain, State Machine Replication, Game Theory, Incentives, Distributed Systems

1 INTRODUCTION

Current state machine replication (SMR) protocols, a subset of which being blockchain protocols, depend on the existence of altruistic players who ignore token changes and honestly follow the protocol. If a player can deviate from a protocol to increase their tokens with no perceived effect on safety and liveness, it must be assumed that every such individual will choose to do this. In Flash

Boys 2.0 [17] and subsequent work¹, it is demonstrated that these deviation opportunities are rampant in Ethereum, and that players are actively availing of them. In any large-scale SMR protocol, most, if not all players, will not consider their deviations as affecting SMR. Therefore, it is essential that we assume non-adversarial players will seek to maximise tokens in tokenised protocols. As a direct consequence, SMR guarantees can no longer depend on honest-by-default users. We explicitly outline the ByRa (Byzantine or Rational) model as an updated player characterisation framework to reflect this weakness in current standards. By moving to the ByRa model, which we formally define in Definition 4.1, the caveat of honest player dependencies in current SMR protocols is removed. Furthermore, we demonstrate that it is possible to achieve SMR in the ByRa model by providing the Tenderstake protocol, an amendment to the Tendermint protocol [14, 24].

To progress towards global adoption, a tokenised SMR protocol must first ensure that all players will maximise their tokens by following the protocol. Implementing an SMR protocol that increases a player's tokens for following the protocol is known as incentivisation, and is a fundamental requirement for any SMR protocol. Much of the work on incentivisation in SMR protocols stems from the seminal work on *selfish mining* in Nakamoto-consensus [20]. In [20], it is demonstrated that certain players are incentivised to deviate from the prescribed protocol. This eventually leads to a scenario where SMR properties are violated, as discussed in [20]. It is only upon the performing of actions as required by the protocol by some majority that it is possible to guarantee the SMR properties of safety and liveness. This has remained the case in the age of tokenisation.

Despite this, there has been no thorough treatment and analysis of tokenised SMR protocols from a game-theoretic standpoint involving rational players, who want to maximise their net tokenised gains (referred to as utility increases in game-theoretic literature), and an adversary, who can corrupt the owners of some amount of the tokenised consensus resource and behave arbitrarily. These corrupted players are known as Byzantine. This characterisation of players as either Byzantine or Rational, which we refer to as the ByRa model, was first considered in distributed systems literature in [27], but never successfully with respect to SMR protocols, although attempts have been made [5, 25, 36]. The closest semblance to this model which has seen wide-scale adoption with respect to SMRs is the BAR (Byzantine, Altruistic and Rational) model [3]. The BAR model crucially includes some portion of altruistic players who disregard tokenised utility, and always follow the protocol. Examples of authors echoing our desire to move away from altruistic



This Technical Report is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 814284

¹<https://github.com/flashbots/pm> Accessed: 25/05/2021

dependencies are numerous, but this from Fairledger [25] puts it concisely: “We have to take into account that every entity may behave rationally, and deviate from the protocol if doing so increases its benefit”. Non-adversarial, honest-by-default characters do not exist in competitive games, and cannot be depended on in tokenised SMR protocols due to their gamified nature. Although many other works state the need to move away from altruistic dependencies, none have proven the critical nature of this dependency, or provided protocols which achieve SMR, in the ByRa model. In this paper, we fulfil both of these essential tasks.

Without the safety net of altruistic players, any successful instantiation of an SMR protocol in the ByRa model must guarantee that rational players will always follow the protocol. To ensure this, rational players must expect to strictly maximise their utility by following the protocol, a property we define as *strong incentive compatible in expectation* (SINCE).

Moreover, we must also guarantee that within such an incentive compatible protocol, the adversary cannot increase their share of tokens to a point where they control enough tokens to prevent SMR. Despite the existence of strong incentive compatibility in expectation, it may be possible for an adversary to receive more than their share of the tokens that get distributed, increasing their share of control. Therefore, we must additionally ensure that an adversary cannot increase the share of tokens they control, a property we define as *fairness*.

1.1 Our Contribution

We define the ByRa player characterisation model, the properties of SINCE and fairness, and in Definition 4.5, the basic requirements a prospective SMR protocol must meet in order to guarantee safety and liveness in the ByRa model. If these requirements are met for a protocol in the ByRa model, the protocol *achieves ByRa SMR*. Informally, to achieve ByRa SMR we require that players controlling a majority of tokens follow the protocol at all times. We then prove that the properties of SINCE and fairness are necessary and together sufficient to achieve ByRa SMR in the main theorem of the paper.

Theorem 5.8. For an SMR protocol Π , Π achieves ByRa SMR if and only if Π is strong incentive compatible in expectation and fair.

In addition to this new game-theoretical framework, we provide Tenderstake as a concrete instantiation of an SMR protocol that provably achieves SINCE and fairness in the ByRa model. Using Theorem 5.8, we then prove Tenderstake achieves SMR in the ByRa model.

1.2 Organisation of the paper

In Section 2 we review related work and present an overview of attempts to implement, and works in favour of, the ByRa model for SMR protocols. In Section 3 we provide a background on the SMR and game theory concepts needed to define the ByRa model. Section 4 introduces a new game-theoretic framework for analysing SMR protocols. This new framework defines the ByRa model, and outlines what we require from SMR protocols in the ByRa model, introducing the properties of SINCE and fairness. In Section 5 we prove that SINCE and fairness are necessary for a protocol to achieve ByRa SMR. We then prove that together, SINCE and fairness are

sufficient properties for a protocol to achieve ByRa SMR. In Section 6 we outline the Tenderstake protocol as an example, for the first time in literature, of a SINCE and fair ByRa SMR protocol. In Section 7 we reason that Tenderstake satisfies the necessary and sufficient properties of safety and liveness for SMR when players controlling a majority of the consensus votes follow the protocol in every round. We then prove that the Tenderstake protocol is SINCE and fair, which using Theorem 5.8, implies Tenderstake achieves ByRa SMR. We conclude in Section 8.

2 RELATED WORK

There is a growing appreciation that incentivisation is not only important, but necessary, to ensure the successful instantiation of an SMR protocol. Many works have argued for the incentivisation of players in SMR protocols [2, 5, 6, 10, 11, 16, 18, 22, 23, 26, 27, 32, 33, 35, 36] while many others demonstrate the critical need for incentive compatibility in tokenised SMR protocols [4, 8, 9, 12, 13, 15, 17, 20, 21, 29, 30, 34].

The characterisations of Byzantine and rational, coupled with that of altruistic players who always follow the protocol, segues into the BAR player characterisation model as introduced in [3]. However, as discussed in Section 1, tokenised SMR protocols cannot depend on altruistic players to ensure the critical properties of safety and liveness. We amend the player characterisations to only include those of Byzantine and rational players in what we call the ByRa model.

A very similar player model is discussed in [27], but with respect to a single binary action multiparty computation. We extend this basic binary action space for players to allow for indefinite sequentialised non-binary action profiles in line with those of SMR protocols. We introduce the necessity for strict maximisation of expected utility to ensure rational players always follow a protocol. This is opposed to [27], where it is claimed that equality of utility will suffice to ensure a rational player will choose one strategy over another. This is logically insufficient. Related to this concept of insufficient proof mechanisms, a common pitfall of legacy incentive compatible proofs is to prove that following a protocol is a Nash Equilibrium in the presence of honest players [18, 21, 22, 32]. In the ByRa model this assumption is not possible, and therefore those proofs are not sound. We also allow the adversary to behave arbitrarily, as opposed to [27] where the adversary only tries to minimise the utility of rational players. Although there are buzzwords associated with this paper such as *Price of Malice* and *Price of Anarchy*, no name is attributed to the player model. We refer to our version of this player model as the ByRa model. The only examples of this player model in SMR literature making meaningful attempts to remove altruistic entities are in [5, 36].

Table 1 exhibits the shortcomings of related work in providing protocols that guarantee rational players always follow the protocol (SINCE), and that prevent an adversary from increasing their share of stake to destroy the system (Fair). Table 1 also includes our proposal, Tenderstake as a standard against which to compare these works.

In [5], it is implicitly assumed rewards are paid to all players who contribute to consensus on a block. This is non-trivial in the ByRa model, as rewards in their system depend on message delivery.

Paper	Network Model	Player Model w/o Honest Players	Evolving-Stake Adversary	SINCE	Fair
Rationals vs. Byzantines [5]	Broadcast Synchrony ²	✓	✗	✓ ³	✓ ⁴
Blockchain Without Waste [35]	Synchrony	✓	✗ ⁵	✓ ⁶	✗
Blockchains Cannot Rely on Honesty [36]	Synchrony	✓	✗	✗	✗
Fruitchains, Snow White [18, 32]	Partial Synchrony	✗	✗	✗	✗
Casper Incentives [16]	Partial Synchrony	✗	✗	✗	✗
FairLedger [25]	Synchrony	✗	✗	✗	✗
Tenderstake (Algorithm 1)	Partial Synchrony	✓	✓	✓	✓

Table 1: Comparison of main works claiming incentive compatibility. ²An idealised model where every message, including adversarial messages, are known to be instantly delivered to all players. ³No explicit reward mechanism provided, non-trivial for BFT protocols. ⁴Enforced by the idealised network model/ unspecified reward mechanism. ⁵No adversary in player model. ⁶Author creates a dominating cost unrelated to quantity of stake for deviation.

From a protocol’s perspective, these messages need to be recorded by a proposer at some point in the protocol, and rational proposers may be incentivised to omit players, as is the case in previous works from subsets of the same authors [7, 8]. We address this omission in the Tenderstake protocol, providing an explicit solution in the ByRa model.

Although [36] provides an SMR protocol which approaches SINCE, they do not provide a rigorous player model excluding altruistic players, and in the presence of a deviating adversary, there are strategies which strictly outperform the recommended protocol strategy for rational players, preventing both strong incentive compatibility and fairness.

A purely economic approach to SMR protocols is taken in [35], which focuses on Proof-of-Stake protocols. Their player model only considers rational players, and depends on a dominating cost for certain deviations that is not quantifiable within the protocol game of maximising stake. Namely, the author assumes rational players in a longest chain rule Proof-of-Stake system will never try to fork the blockchain, as doing so devalues stake in terms of some external fiat currency more than any possible reward. We believe this does not necessarily affect the decisions of all rational players, which is also acknowledged in [35] where participation in the protocol is restricted to players with a “sufficient coin holding”. Another concern about such an arbitrary external cost arises when we consider settings where the stake/ cryptocurrency in question becomes a dominant fiat currency, and the majority of participants only consider utility as measured in said stake. In this paper, we demonstrate that it is possible to construct a protocol, Tenderstake, that strictly maximises stake by following the protocol. As following the protocol maximises the value of stake in [35], Tenderstake captures the same maximisation of value without the potentially problematic dependency on unquantifiable external costs unrelated to quantity of stake.

One of the legacy works in relation to fairness and incentive compatibility of SMR protocols is Fruitchains [32]. The Fruitchains player model consists of an altruistic majority of players and a cooperative rational minority. Fruitchains crucially relies on an underlying blockchain satisfying an SMR protocol in order to guarantee fairness of rewards. They fail to consider the incentives of all parts of the system, relying on an altruistic majority in order to guarantee the underlying blockchain satisfies the required SMR

properties. They then add a small section where claims of incentive compatibility for non-cooperative rational players are made. The authors claim a protocol is incentive compatible if fairness of rewards has already been guaranteed. As fairness in their system is only guaranteed if a majority of players follow the protocol, there is no logical result which proves that rational players will always follow the protocol, required for incentive compatibility. This is insufficient to guarantee SMR in the ByRa model. This fatal dependence on an underlying correct-by-default SMR protocol/ trusted third-party is also demonstrated in [16, 25], where claims of incentive compatibility and fairness do not hold in the ByRa model.

3 PRELIMINARIES

This section covers the concepts and definitions required to reason about SMR protocols from a game-theoretic perspective. First we define SMR and a general notion of a blockchain which provides some intuition for our SMR definitions, and primes the reader for our description of the Tenderstake protocol in Section 6. We then provide the game theory framework necessary to formally reason about SMR protocols involving rational and adversarial players, and how SMR can be achieved in the presence of these types of players. In the following we let $negl()$ be a function which for any polynomial $p()$ there exists a constant $\kappa_0 \in \mathbb{N}$ such that $negl(\kappa) < \frac{1}{p(\kappa_0)}$ for all $\kappa \geq \kappa_0$. This $negl()$ is known in literature as a *negligible* function.

In this paper, we are interested in a distributed set of n players $\{P_1, \dots, P_n\}$ interacting with one and other inside a protocol which will produce some output that all players correctly participating in the protocol can agree on. This output will be a *replicated state machine*. First, we define a state machine.

Definition 3.1. A *state machine* consists of set of variables, and sequence of commands/ updates on those variables, producing some output.

The concept of a state machine alone does not capture the notion that potentially many players can reconstruct a common view of the same state of a machine, and requires extension.

Definition 3.2. For a set of players $\{P_1, \dots, P_n\}$ and a state machine, *state machine replication* (SMR) is a process that allows each player to execute a common sequence of commands acting on the

machine's state in the same order, thus maintaining a common view of the machine's state.

Progressing towards our goal of analysing SMR protocols, we must first define what we require from an SMR protocol. We take inspiration for our definition from [1], where their system model is clearly and concisely explained, and is very similar to ours.

Notation 3.3. With respect to protocols and recommended protocol actions, a *correct* player is a player who always follows the recommended protocol actions.

Definition 3.4. An SMR protocol Π deciding on a potentially infinite sequence of state machine updates satisfies the following properties:

- *Safety*: For any two correct players P_i, P_j in Π , $i \neq j$, if P_i decides on an SMR update V_i at position k in the sequence, and P_j decides on an SMR update V_j at position k in the sequence, then $V_i = V_j$.
- *Liveness*: For any position k in the sequence, every correct player eventually decides on an SMR update for position k .

To achieve SMR, we utilise the concept of a blockchain. This is done in a generic manner so as to allow for direct comparison with most blockchain instantiations.

Definition 3.5. A *block* B is a data structure used to communicate changes to the state machine view of each player. Blocks consist of a pointer(s) to previous block(s), and a set of instructions with which to update the state. State machine updates in a block are applied to the state described by the block(s) to which they point. The *genesis block* B^1 describes the starting state of the system and is a priori agreed upon by all players. The global state at any point in the system is then described by applying the state machine updates according to some ordering rule starting from the genesis block. A *blockchain* $C = [B^1, \dots, B^H]$ is the ordered data structure created by traversing the block pointers from the genesis block to all blocks to be applied to the global state according to the ordering rule. H denotes the *height* of the blockchain.

In our system, an SMR protocol Π consists of n players owning shares of a finite resource, which we will refer to as *stake*, and denoted $Stake^1$ at initialisation. Π proceeds in fixed-time periods, which we refer to as *rounds*, beginning in round 1. For any height $H > 1$ of the blockchain, players participate in Π to decide on a block for that height. Reaching consensus on a block will involve one or more successful protocol steps. After a block has been decided for height $H \geq 1$, the total stake in the system is denoted $Stake^H$ with player shares of $Stake^H$ denoted s_1^H, \dots, s_n^H . Without loss of generality, we assume $\sum_{i=1}^n s_i^H = 1$, and for all $i \in \{1, \dots, n\}$, $H \geq 1$, $s_i^H < \frac{1}{2}$.

Now we introduce some basic game theory to allow us to properly reason about SMR protocols in our system as games, taking inspiration for our definitions from [31]. The games we are concerned with, SMR protocols, are played by players with strict incomplete information, meaning some subset of players will not know the action choices of other players for certain rounds when they are required to choose their own actions. As such, we need to be able to describe what a player knows (and implicitly what they do not),

which we call their private information. Furthermore, we must be able to describe what motivates players in games. This motivation is provided by a utility function, which attributes a numerical score to each action a player can take. In games, players choose the action which maximises their utility function.

Definition 3.6. A *game*, denoted \mathbb{G} , progressing in rounds with strict incomplete information for a set of n players $\{P_1, \dots, P_n\}$ can be described by the following:

- For every P_i , a set of *actions* X_i . We denote by X_{-i} the set of actions that each player excluding P_i can take. For $x_{-i} \in X_{-i}$, x_{-i} is described by a vector of actions of length $n - 1$, with each vector position mapping to a unique player.
- For every player P_i and round r , a set of *private informations* T_i^r . A value $t_i^r \in T_i^r$ is a private information value that P_i can have at round r . We denote by t_{-i}^r the private informations held by all players excluding P_i at round r .
- For every player P_i , current round $r \geq 1$, and some round $r' \geq r$, the *utility function* for P_i with respect to round r' is defined as :

$$u_i^r : T_i^r \times \underbrace{X_i \times \dots \times X_i}_{r'+1-r} \times \underbrace{X_{-i} \times \dots \times X_{-i}}_{r'+1-r} \rightarrow \mathbb{R} \quad (1)$$

where $u_i^r(t_i^r, x_i^r, \dots, x_i^{r'}, x_{-i}^r, \dots, x_{-i}^{r'})$ is the utility achieved by P_i in round r' with private information t_i^r , if player P_i takes the actions $x_i^r, \dots, x_i^{r'}$ in rounds r, \dots, r' respectively, and the actions of all other players are described by $x_{-i}^r, \dots, x_{-i}^{r'}$ in rounds r, \dots, r' respectively.

Although utility functions evaluate actions given the actions of all other players, the actions of the other players may not be known in advance. Therefore, players will need to be able to choose their actions solely based on their private informations. The actions a player takes given some private information are computed through a strategy, which is defined in Definition 3.7.

Definition 3.7. A *strategy* of a player P_i is a function $str_i : T_i^r \rightarrow X_i$, $r \geq 1$, which defines the action to be taken by P_i given some private information value. A strategy str_i is *mixed* if for a player P_i with m_i possible strategies $Str_i = \{str_i^1, \dots, str_i^{m_i}\}$, they select a strategy to follow from Str_i according to some probability distribution. For every player P_i , str_{-i} describes the mixed strategies taken by all players excluding P_i .

Definition 3.8. For an SMR protocol Π , the *recommended strategy*, denoted str_Π , is the strategy that Π requires players to follow in order to successfully achieve SMR.

4 A GAME-THEORETIC FRAMEWORK FOR SMR

In this section we formalise the ByRa framework for SMR protocols, where participants are either adversarially or rationally motivated. This is in response to the existential threat posed by the growing trend of players managing SMR protocols acting in a profit-maximising manner [17] in protocols where security guarantees depend on honest players. Furthermore, this framing is made quite naturally, given SMR protocols are accurately modelled as

games with strict incomplete information as defined in Definition 3.6.

This is a crucial progression from existing standards in distributed systems literature where some number of non-adversarial players are honest-by-default. Due to the distributed nature of SMR protocols, as a baseline we must account for some portion of adversarial players who can behave arbitrarily with unknown utility functions. With SMR protocols considered as games, the remaining non-adversarial players must follow some known utility function, and attempt to choose the actions which maximise it. To ensure the honest behaviour of rational players in this setting, following the protocol strategy must maximise the utility of rational players. We define these player characterisations here formally as the ByRa model.

Definition 4.1. The *ByRa model* consists of *Byzantine* and *Rational* players. A player is:

- *Byzantine* if they deviate arbitrarily from the recommended strategy within a game with unknown utility function. Byzantine players are chosen and controlled by an adversary \mathcal{A} .
- *Rational* if they choose uniformly at random from all mixed strategies which maximise their known utility function assuming all other players are rational.

Remark 4.2. Our definition of rational players omits tie-breaking assumptions that bias a rational player to certain strategies over others with equal utility. For example, if we have a fair coin tossing game that costs 1 token to play and correct guesses gain 3 tokens, a rational player in our system will choose heads with probability 0.5. If we have a protocol that requires rational players to always choose heads, it is necessary to make the payoff for heads strictly greater than that of tails.

A rational player who assumes all other players are rational is known as an *oblivious* rational player [27, 28]. A rational player who is not oblivious knows there are players in the system controlling a non-negligible share of stake, controlled by an adversary, who may try to break safety and liveness. Adding this to the private information of a rational player adds a probability of safety and liveness failing if protocol actions are not followed by the remaining players, which becomes 1 in the presence of a maximal adversary. This outcome has a critical cost for rational players (as used in [5, 27, 28, 35]), which can be made arbitrarily high to prevent rational players from deviating from protocol actions. Under the non-oblivious assumption, all rational players will follow the protocol, and proofs of following protocol actions become trivial.

We believe this is highly unrepresentative of rational players in SMR protocols today, particularly in light of the clear recent evidence that miners can and are deviating from protocol actions to increase their on-chain rewards [17]. As such, in the rest of this paper, we assume all rational players are oblivious, and prove our main lemmas and theorems given this weakest possible assumption about adversarial share distributions.

To consider rational players in any game, it is necessary to explicitly define what their utility functions are. Inkeeping with the tokenised assumptions of our model, we let rational player utility be measured in stake as described by the blockchain. By their nature, tokenised SMR protocols require it to be expensive to deviate

from the protocol actions, encouraging honest behaviour through stake rewards, and/or stake punishments for dishonest behaviour. Given the unprecedented levels of SMR protocol usage as a result of tokenisation, we see stake as the driving utility measure for the players who participate in these protocols.

As total stake is only meaningful with respect to a particular time-point, and SMR protocols are played indefinitely, rational players will seek to maximise their total stake at all possible rounds sufficiently far into the future. Therefore, when discussing incentivisation and player utility, it is necessary to refer to stake/share/total stake with respect to rounds. As we are using the round variable as a counter, and some rounds may be unsuccessful, it cannot be independently used to determine the height, and vice versa. Rather than add notation to relate the two, we treat them separately, and make it clear from context which is being used. When referring to stake/share/total stake with respect to particular rounds, we use superscripts involving r , whereas when discussing these variables with respect to the height of the blockchain, we use superscripts involving H .

In the ByRa model, and SMR protocols in general, it is necessary to specify an upperbound on adversarial share of stake, below which SMR can be achieved if all non-adversarial players follow the protocol, and above which SMR cannot be guaranteed.

Notation 4.3. For an SMR protocol Π , we denote by α the maximal share of stake such that for players controlling greater than $1 - \alpha$ of the stake following the SMR protocol, safety and liveness are achieved. The exact value of α will depend on the network distribution assumptions, in line with the results of [19], which must be contained in the threat model.

For some security parameter $\kappa \in \mathbb{N}$, our goal is to guarantee that SMR can be achieved (that is, both safety and liveness are satisfied) in the ByRa model with probability greater than $1 - \text{negl}(\kappa)$ over any polynomial in κ rounds.

We first need to introduce an equivalence relation for mixed strategies over finite rounds. When we state the protocol strategy which needs to be followed to achieve SMR, although there is an infinite number of strategy encodings, we only require players to follow strategies which result in actions as outlined by the protocol. We are indifferent to how this is achieved. If a strategy is encoded differently to the recommended protocol strategy, but results in actions as prescribed by the protocol with probability greater than $1 - \text{negl}(\kappa)$ over any polynomial in κ rounds, we see this as equivalent to the recommended protocol strategy.

Definition 4.4. For a player P_i at initialisation, and round $r' \geq 1$, two mixed strategies str_i^a and str_i^b are *equivalent with respect to round r'* if for all rounds r , $1 \leq r \leq r'$, and private informations $t_i^r \in T_i^r$, it is the case that $str_i^a(t_i^r) = str_i^b(t_i^r)$. We use $str_i^a \equiv^{r'} str_i^b$ to denote this equivalence relation. If $str_i^a \equiv^{r'} str_i^b$ for all rounds r' polynomial in κ , str_i^a and str_i^b are *equivalent*, denoted by $str_i^a \equiv str_i^b$.

With this equivalence relation, we can now define what it means for a protocol to achieve SMR in the ByRa model. In this paper, after deciding on a block at height $H \geq 1$, we denote the adversarial share of stake by $s_{\mathcal{A}}^H$.

Definition 4.5. For an SMR protocol Π and round r , let p_{Π}^r be the probability that players controlling more than $1 - \alpha$ of the total stake follow a mixed strategy $str \equiv str_{\Pi}$ up to and including round r for any $s_{\mathcal{A}}^1 < \alpha$. Π achieves ByRa SMR if for all rounds r' polynomial in κ it holds that $p_{\Pi}^{r'}$ is greater than $1 - \text{negl}(\kappa)$. Otherwise, Π fails in the ByRa model.

Towards the goal of achieving ByRa SMR, we need to formally define rational utility as measured in stake. For a rational player P_i with private information t_i^r and round $r' \geq r$, we have:

$$u_i^{r'}(t_i^r, x_i^r, \dots, x_{-i}^r) = s_i^{r'} \cdot \text{Stake}^{r'}. \quad (2)$$

However, in a game with strict incomplete information as is the case in an SMR protocol, a rational player P_i with private information t_i^r will not know their own future private information values (required to choose their actions), the private informations of the other players, or str_{-i} , before choosing str_i . Therefore, P_i must choose the mixed strategy which maximises P_i 's expected stake at round r' , denoted $E(s_i^{r'} \cdot \text{Stake}^{r'})$, according to the probability distribution that P_i attributes to possible values for these unknowns. This distribution will be contained in $t_i^{r'}$.

Thus, knowing $t_i^{r'}$ is sufficient to calculate P_i 's expected utility of a particular strategy at round r' , which we express mathematically by $E(s_i^{r'} \cdot \text{Stake}^{r'} | t_i^{r'}, str_i)$. We state this formally in Definition 4.6.

Definition 4.6. For an SMR protocol Π and rational player P_i with private information t_i^r , mixed strategy str_i , and a particular round $r' \geq r$, the expected utility of str_i for P_i at round r' is denoted $\bar{u}_i^{r'}(t_i^r, str_i)$ and is described by $\bar{u}_i^{r'}(t_i^r, str_i) = E(s_i^{r'} \cdot \text{Stake}^{r'} | t_i^r, str_i)$.

As such, for a rational P_i in an SMR protocol Π with private information t_i^r , P_i will choose the mixed strategy str_i which maximises $\bar{u}_i^{r'}(t_i^r, str_i)$. To establish the existence, or not, of such a mixed strategy, we introduce an inequality in Definition 4.7 which allows us to pairwise rank mixed strategies by expected utility.

Definition 4.7. For an SMR protocol Π , rational player P_i and two mixed strategies $str_i^a, str_i^b, str_i^c$ strictly dominates str_i^b in expectation if there exists $r'' \geq r, r''$ polynomial in κ , such that for all $r' > r'', \bar{u}_i^{r'}(t_i^r, str_i^a) > \bar{u}_i^{r'}(t_i^r, str_i^b)$. If str_i^a strictly dominates str_i^b in expectation, we denote this relationship by $str_i^a >_u str_i^b$.

Using the strict dominance in expectancy relationship, we can formally define what we require from an SMR protocol in order for rational players to follow the recommended protocol strategy. This requirement is strong incentive compatibility in expectation, and is defined in Definition 4.8.

Definition 4.8. An SMR protocol Π is *Strong INcentive Compatible in Expectation* (SINCE) if for any rational player $P_i, str_{\Pi} >_u str_i$ for all mixed strategies $str_i \in Str_i$, with Str_i the set of mixed strategies available to P_i , such that $str_i \neq str_{\Pi}$.

For a protocol to be SINCE in the ByRa model ensures that all rational players will follow the recommended protocol strategy. However, SINCE is not on its own sufficient to ensure the safety and liveness of an SMR protocol in ByRa model. It is still possible for an adversary to gain more than their fair share of rewards, and as such, increase their total share above the critical threshold of α . Towards achieving SMR in the ByRa model, it must be ensured that

the adversarial share remains strictly bounded by the threshold α required to achieve SMR if all non-adversarial players follow the protocol. We explicitly define what we mean by fairness in the ByRa model in Definition 4.9.

Definition 4.9. An SMR protocol Π with adversary \mathcal{A} is fair in the ByRa model if $P(s_{\mathcal{A}}^r \leq s_{\mathcal{A}}^1) > 1 - \text{negl}(\kappa)$ for any round $r \geq 1$.

With SINCE and fairness, we have two intuitive properties which turn out to be crucial in achieving ByRa SMR. In Section 5, we show that it is impossible to guarantee the actions of players controlling more than $1 - \alpha$ of the stake if these properties do not hold. Explicitly, we prove that the properties of SINCE and fairness are necessary, and together sufficient, to achieve ByRa SMR.

5 ACHIEVING SMR IN THE ByRa MODEL

Towards our final goal of proving that the properties of SINCE and fairness are necessary, and together sufficient, to achieve ByRa SMR, the first step is to prove in Lemma 5.6 that SINCE is necessary. To allow us to prove this result, we introduce notation which allows us to consider, for a potential SMR protocol, the strategies from which rational players choose.

Definition 5.1. For a rational player P_i with a set of mixed strategies Str_i , let $Str_i^{\text{NSD}} \subseteq Str_i$ be such that for all $str_i \in Str_i^{\text{NSD}}$, there does not exist a $str_i^u \in Str_i$, such that $str_i^u >_u str_i$.

That is, if a mixed strategy $str \in Str_i$ is in the set Str_i^{NSD} , there is no strategy for P_i which strictly dominates str in expectancy. We provide the following Lemmas towards establishing that rational players will choose strategies exclusively from Str_i^{NSD} .

Lemma 5.2. For an SMR protocol Π , a rational player P_i , any strategy $str_i^a \in Str_i$, and $|Str_i| \geq 2$, either $str_i^a \in Str_i^{\text{NSD}}$ or there is some $str_i^b \in Str_i^{\text{NSD}}$ such that $str_i^b >_u str_i^a$.

PROOF. We will do this by induction over the cardinalities of Str_i . First we check $|Str_i| = 2$. If str_i^a is in Str_i^{NSD} , we are finished. Assume otherwise. That is, $str_i^b >_u str_i^a$, which implies $str_i^a \not>_u str_i^b$, and as such, $str_i^b \in Str_i^{\text{NSD}}$ as required.

Assume the inductive hypothesis for $|Str_i| = k$.

Now, given this assumption, we must prove our hypothesis holds for $|Str_i| = k + 1$. Consider a strategy $str_i^c \in Str_i$. We need to prove either $str_i^c \in Str_i^{\text{NSD}}$, or there exists $str \in Str_i^{\text{NSD}}$ with $str >_u str_i^c$. If str_i^c is not strictly dominated by any strategy $str \in Str_i$, then $str_i^c \in Str_i^{\text{NSD}}$.

Assume instead there exists some strategy $str_i^a \in Str_i, str_i^a >_u str_i^c$. Consider $Z_i = Str_i \setminus \{str_i^c\}$. By the inductive assumption, either $str_i^a \in Z_i^{\text{NSD}}$, or there exists $str_i^b \in Z_i^{\text{NSD}}$ such that $str_i^b >_u str_i^a$. If $str_i^a \in Z_i^{\text{NSD}}$, then $str_i^a \in Str_i^{\text{NSD}}$, which implies there exists $str \in Str_i^{\text{NSD}}$ such that $str >_u str_i^c$. Otherwise, if $str_i^a \notin Z_i^{\text{NSD}}$, there exists $str_i^b \in Z_i^{\text{NSD}}$, with $str_i^b >_u str_i^a$. As $str_i^b >_u str_i^a$, and $str_i^a >_u str_i^c$, this implies $str_i^b >_u str_i^c$. As $str_i^b \in Z_i^{\text{NSD}}$, and $str_i^b >_u str_i^c$, this implies $str_i^b \in Str_i^{\text{NSD}}$. Therefore, there exists $str \in Str_i^{\text{NSD}}$ such that $str >_u str_i^c$. \square

As rational players choose uniformly at random from all mixed strategies which maximise utility, from Lemma 5.2 for a rational

player P_i these mixed strategies will be contained in Str_i^{NSD} . Moreover, Definition 4.1 states that P_i chooses from these mixed strategies in Str_i^{NSD} with uniform probability. Therefore, to ensure rational players follow str_{Π} with probability at least $1 - \text{negl}(\kappa)$, we must identify the conditions where for any rational player P_i , $Str_i^{\text{NSD}} = \{str_{\Pi}\}$. We state this explicitly in Observation 5.3.

Observation 5.3. A rational player P_i follows str_{Π} with probability greater than $1 - \text{negl}(\kappa)$ if and only if $Str_i^{\text{NSD}} = \{str_{\Pi}\}$.

The precise conditions where $Str_i^{\text{NSD}} = \{str_{\Pi}\}$ for a rational player P_i are identified in Lemma 5.4.

Lemma 5.4. For an SMR protocol Π and a rational player P_i , $Str_i^{\text{NSD}} = \{str_{\Pi}\}$ if and only if Π is strong incentive compatible in expectation.

PROOF. If an SMR protocol Π is SINCE, then for any rational player P_i , str_{Π} strictly dominates all other strategies in expectation. From Lemma 5.2, this implies $Str_i^{\text{NSD}} = \{str_{\Pi}\}$.

Now we need to show if $Str_i^{\text{NSD}} = \{str_{\Pi}\}$, then Π is SINCE. From Lemma 5.2, we know for any strategy str_i^a , either $str_i^a \in Str_i^{\text{NSD}}$ or there is some $str_i^b \in Str_i^{\text{NSD}}$ such that $str_i^b >_u str_i^a$. As the only strategy in Str_i^{NSD} is str_{Π} , this implies for any strategy $str_i^a \neq str_{\Pi}$, $str_{\Pi} >_u str_i^a$. This implies Π is SINCE, as required. \square

Corollary 5.5. For an SMR protocol Π and a rational player P_i , $P(P_i \text{ chooses } str_{\Pi}) > 1 - \text{negl}(\kappa)$ if and only if Π is strong incentive compatible in expectation.

PROOF. Follows from Observation 5.3 and Lemma 5.4. \square

This allows us to prove SINCE is a necessary property to achieve ByRa SMR.

Lemma 5.6. For an SMR protocol Π , if Π is not strong incentive compatible in expectation, then Π fails in the ByRa model.

PROOF. Consider such a protocol Π . As a consequence of not SINCE, for a rational player P_i , this means $P(P_i \text{ chooses } str_{\Pi})$ is not greater than $1 - \text{negl}(\kappa)$, applying Corollary 5.5. From Definition 4.5 we are required to consider $s_{\mathcal{A}}^1$ maximal. Given this rational P_i and a maximal adversary, there is now players controlling greater than or equal to α of the total stake who will not choose a strategy equivalent to str_{Π} with non-negligible probability in κ . Using the notation of Definition 4.5, this means p_{Π}^r is not greater than $1 - \text{negl}(\kappa)$ for some $r \geq 1$, which implies Π fails in the ByRa model. \square

Using similar arguments, we are able to prove fairness is also necessary for a protocol to achieve ByRa SMR.

Lemma 5.7. For an SMR protocol Π , if Π is not fair then Π fails in the ByRa model.

PROOF. If Π is not fair, there exists $r \geq 1$ such that $P(s_{\mathcal{A}}^r > s_{\mathcal{A}}^1)$ is not negligible in κ . From Definition 4.5, we are required to consider the case where $s_{\mathcal{A}}^1$ is maximal. In this case, the probability that the adversary controls greater than or equal to α of the stake at round r is non-negligible in κ given $P(s_{\mathcal{A}}^r > s_{\mathcal{A}}^1)$ is non-negligible in κ . Given the uniform strategy selection probability of Byzantine players across all possible strategies, this implies that p_{Π}^r is not greater than $1 - \text{negl}(\kappa)$. Therefore, Π fails in the ByRa model. \square

Collecting the results of this section, with some additional proof-work, we are equipped to prove the main theorem of the paper, Theorem 5.8.

Theorem 5.8. For an SMR protocol Π , Π achieves ByRa SMR if and only if Π is strong incentive compatible in expectation and fair.

PROOF. For an SMR protocol Π , we will first prove that if Π achieves ByRa SMR then Π is SINCE and fair. Using the contrapositive of Lemma 5.6, we have that if Π achieves ByRa SMR (does not fail in the ByRa model), then Π is SINCE. Similarly, using the contrapositive of Lemma 5.7, we have that if Π achieves ByRa SMR, then Π is fair.

We now need to prove if Π is SINCE and fair then Π achieves ByRa SMR. By SINCE and Corollary 5.5, this implies all rational players will always choose str_{Π} . Furthermore, as Π is fair, from Definition 4.9, we know rational players will maintain greater than $1 - \alpha$ of the stake in every round with probability greater than $1 - \text{negl}(\kappa)$. Therefore, we have players controlling greater than $1 - \alpha$ of the stake who will follow str_{Π} with probability greater than $1 - \text{negl}(\kappa)$, which is precisely the definition of Π achieving ByRa SMR from Definition 4.5. \square

This crucial theorem completes the first part of the paper, identifying the properties of SINCE and fairness as both necessary, and together sufficient, for a protocol to achieve ByRa SMR, independently of network assumptions and adversarial capabilities. We now proceed to outline the Tenderstake protocol, demonstrating that it is possible to satisfy SINCE and fairness in the ByRa model.

6 Tenderstake

In this section, we provide the encoding of Tenderstake, and give an overview of the main differences between the Tenderstake protocol and Tendermint. We assume a partially synchronous network communication model as in Tendermint [24]. Players are connected to nodes in a dynamic wide area network, with each node having direct connections to a subset of all other nodes, forming a sparsely connected graph of communication channels between nodes. Non-Byzantine player messages are transmitted through *gossiping*; players send a message to neighbouring nodes, who echo messages to their neighbours until all nodes eventually receive the message. Formally, there is global stabilisation round $GSR > 0$, such that all messages sent at round $r_{send} > 0$ are delivered by round $r_{deliver} = \max(r_{send}, GSR) + \Delta$ for some unknown number of rounds $\Delta > 0$.

We assume rational players are aware that there is a fixed, but unknown, upperbound Δ on message delivery between players in synchrony, which we refer to as Δ -synchrony, but are unaware of how many players are in Δ -synchrony at any given time. For a message m , a call to **broadcast**(m) sends a m to all players, including oneself, under the same gossiping specification. This is partial synchrony as defined in [19].

6.1 Threat Model

In Tenderstake, protocol actions take negligible amounts of time compared to network delays, so if all non-Byzantine players behave correctly and receive the same sequence of messages their machines

will be in the same state. Rational players ignore messages which have not been signed using a protocol-associated private key.

We consider an adversary \mathcal{A} with the following properties:

- (1) \mathcal{A} can read all messages sent by non-Byzantine parties, but cannot existentially forge signatures.
- (2) \mathcal{A} can control and coordinate all Byzantine players in any way, with unknown utility function.
- (3) At initialisation we have $\frac{1}{3} - \delta < s_{\mathcal{A}}^1 < \frac{1}{3} = \alpha$, for some $\delta > 0$, in line with the partially synchronous network distribution limits [19].
- (4) At initialisation, \mathcal{A} can choose to corrupt any $1 \leq f < n - 2$ players, say P_1, \dots, P_f with shares s_1^1, \dots, s_f^1 , such that $\sum_{i=1}^f s_i^1 = s_{\mathcal{A}}^1$.
- (5) Given \mathcal{A} corrupts players P_1, \dots, P_f as Byzantine for consensus on a block at height H with shares $s_1^{H-1}, \dots, s_f^{H-1}$, the adversarial share at the proceeding height is calculated as $s_{\mathcal{A}}^H = \sum_{i=1}^f s_i^H$.

Remark 6.1. In this work, we focus on static adversaries. It is possible to extend our results to an adaptive adversary who can re-select the set of Byzantine players after every decision. To do so requires significant additional code and further assumptions that preserve adversarial stake throughout corruptions. We choose to leave this as future work, as it only stands to detract from the primary focus of the paper, that is, to demonstrate the importance of ByRa SMR and how it can be achieved in real-world protocols with Tenderstake.

6.2 Protocol Outline

We now describe the pseudocode of Tenderstake as outlined in Algorithm 1. As the goal of Section 6 is to amend Tendermint to achieve ByRa SMR, readers of [14] will notice that we use large parts of the code and descriptions from that work. We describe the entire code here for completeness, and highlight the differences in Tenderstake to Tendermint as they arise. The two fundamental additions to the Tendermint protocol used by Tenderstake are proof-of-transition and slashing functionalities, described in detail in Sections 6.2.1 and 6.2.2 respectively, and included in the code of Algorithm 1. Proof-of-transition ensures players who send a message at a particular height/ epoch/ step have gotten there by following the protocol, while the slashing functionality enforces the use of proofs-of-transition, as well as the sending of valid messages in general, by punishing players for sending invalid messages.

In Tenderstake, every correct player is initialised by passing a block *Genesis* to the *Initialise* function (line 1). This ensures all players start from a common state. Block *Genesis* contains information on player shares, stake and per-block reward at initialisation.

The algorithm is presented as a set of **upon** rules that are to be executed automatically once the corresponding logical condition is *TRUE*. Variables with sub-index i denote player P_i 's local state variables, while those without are value placeholders. The sign $*$ denotes any value. We use the convention of $> \frac{x}{3} m$ **with** *COND* to stand for the logical statement which is *TRUE* if and only if players controlling more than $\frac{x}{3}$ of the total stake with respect to P_i 's blockchain C_i (represented as a vector in line 2) deliver messages,

Algorithm 1 Tenderstake protocol for a player P_i

```

1: function Initialise(Genesis)
2:    $C_i := [Genesis]$  ▷  $P_i$ 's blockchain as a vector
3:    $h_i := 1$  ▷ Tracks height of  $C_i$ 
4:    $epoch_i := 1$ 
5:    $step_i \in \{propose, prevote, precommit\}$ 
6:    $lockValue_i := nil$ 
7:    $lockEpoch_i := -1$ 
8:    $validValue_i := nil$ 
9:    $validEpoch_i := -1$ 
10:   $Stake_i := Genesis.stake()$  ▷ Total stake
11:   $Shares_i := Genesis.shares()$  ▷ Vector of player shares
12:   $Reward_i := Genesis.reward()$  ▷ Per-Block reward
13:   $DevProofs_i := [nil \text{ for } j \in \{1, \dots, n\}]$  ▷ Deviation proofs
14:   $prevoteProofs_i := nil$ 
15:   $precommitProofs_i := nil$ 
16: upon start do StartEpoch(1)
17: function StartEpoch(epoch)
18:    $epoch_i \leftarrow epoch$ 
19:    $step_i \leftarrow propose$ 
20:   if proposer( $h_i, epoch_i$ ) =  $P_i$  then
21:     if  $validValue_i \neq nil$  then
22:        $proposal_i \leftarrow validValue_i$ 
23:     else
24:        $proposal_i \leftarrow getValue().include(DevProofs_i)$ 
25:     broadcast (PROPOSAL,  $h_i, epoch_i, proposal_i, validEpoch_i, prevoteProof_i$ )
26:   else
27:     schedule OnTimeoutPropose( $h_i, epoch_i$ ) to be executed after timeout()

28: upon (PROPOSAL,  $h_i, epoch_i, v, -1, proof$ ) with  $valid(proof)$  from proposer( $h_i, epoch_i$ )
while  $step_i = propose$  do
29:   if  $valid(v)$  and ( $lockEpoch_i = -1$  or  $lockValue_i = v$ ) then
30:     broadcast (PREVOTE,  $h_i, epoch_i, v, prevoteProof_i$ )
31:   else
32:     broadcast (PREVOTE,  $h_i, epoch_i, nil, prevoteProof_i$ )
33:    $step_i \leftarrow prevote$ 

34: upon (PROPOSAL,  $h_i, epoch_i, v, validEpoch, proofProposal$ ) with  $valid(proofProposal)$ 
from proposer( $h_i, epoch_i$ ) and  $> \frac{2}{3}$  (PREVOTE,  $h_i, validEpoch, v, proofPrevote$ ) with
 $valid(proofPrevote)$  while ( $step_i = propose$  and ( $validEpoch \geq 0$  and  $validEpoch < epoch_i$ ))
do
35:    $prevoteProof_i \leftarrow proof(> \frac{2}{3} (PREVOTE, h_i, validEpoch, v) \cup prevoteProof_i)$ 
36:   if  $valid(v)$  and ( $lockEpoch_i < validEpoch$  or  $lockValue_i = v$ ) then
37:     broadcast (PREVOTE,  $h_i, epoch_i, v, prevoteProof_i$ )
38:   else
39:     broadcast (PREVOTE,  $h_i, epoch_i, nil, prevoteProof_i$ )
40:    $step_i \leftarrow prevote$ 

41: upon  $> \frac{2}{3}$  (PREVOTE,  $h_i, epoch_i, *, proof$ ) with  $valid(proof)$  while  $step_i = prevote$  for the
first time do
42:    $precommitProof_i \leftarrow proof(> \frac{2}{3} (PREVOTE, h_i, epoch_i, *))$ 
43:   schedule OnTimeoutPrevote( $h_i, epoch_i$ ) to be executed after timeout()

44: upon (PROPOSAL,  $h_i, epoch_i, v, *, proofProposal$ ) with  $valid(proofProposal)$  from
proposer( $h_i, epoch_i$ ) and  $> \frac{2}{3}$ 
(PREVOTE,  $h_i, epoch_i, v, proofPrevote$ ) with  $valid(proofPrevote)$  while
 $valid(v)$  and  $step_i \geq prevote$  for the first time do
45:   if  $step_i = prevote$  then
46:      $lockValue_i \leftarrow v$ 
47:      $lockEpoch_i \leftarrow epoch_i$ 
48:      $precommitProof_i \leftarrow proof(> \frac{2}{3} (PREVOTE, h_i, epoch_i, v))$ 
49:     broadcast (PRECOMMIT,  $h_i, epoch_i, v, precommitProof_i$ )
50:      $step_i \leftarrow precommit$ 
51:      $validValue_i \leftarrow v$ 
52:      $validEpoch_i \leftarrow epoch_i$ 
53: upon  $> \frac{2}{3}$  (PREVOTE,  $h_i, epoch_i, nil, proof$ ) with  $valid(proof)$  while  $step_i = prevote$  do
54:    $precommitProof_i \leftarrow proof(> \frac{2}{3} (PREVOTE, h_i, epoch_i, nil))$ 
55:   broadcast (PRECOMMIT,  $h_i, epoch_i, nil, precommitProof_i$ )
56:    $step_i \leftarrow precommit$ 
    
```

with each message m satisfying the logical condition *COND*. If m contains a proposed deviator, that deviator's share does not count towards the tally (it would be irregular that a player would affirm a message which tried to destroy their own stake).

Algorithm 1 Tenderstake protocol (ctd.)

```

57: upon  $> \frac{2}{3}$  (PRECOMMIT,  $h_i$ ,  $epoch_i$ , *,  $proof$ ) with  $valid(proof)$  for the first time do
58:    $prevoteProof_i \leftarrow proof(> \frac{2}{3}$  (PRECOMMIT,  $h_i$ ,  $epoch_i$ , *))
59:   schedule  $OnTimeoutPrecommit(h_i, epoch_i)$  to be executed after  $timeout()$ 

60: upon  $> \frac{2}{3}$  (PRECOMMIT,  $h_i$ ,  $epoch_i$ , nil,  $proof$ ) with  $valid(proof)$  while
    $step_i = precommit$  do
61:    $StartEpoch(epoch_i + 1)$ 

62: upon (PROPOSAL,  $h_i$ ,  $epoch$ ,  $v$ , *,  $proofProposal$ ) with  $valid(proofProposal)$  from
   proposer( $h_i$ ,  $epoch$ ) and  $> \frac{2}{3}$ 
(PRECOMMIT,  $h_i$ ,  $epoch$ ,  $v$ ,  $proofPrecommit$ ) with  $valid(proofPrecommit)$  do
63:    $newDeviators \leftarrow v.deviators() \setminus C_i.deviators()$ 
64:   if  $valid(v)$  then
65:     if  $|newDeviators| > 0$  then ▷ True if deviators in  $v$  not in  $C_i$ 
66:        $adjustForSlashing(newDeviators)$ 
67:        $prevoteProof_i \leftarrow proof(> \frac{2}{3}$  (PRECOMMIT,  $h_i$ ,  $epoch$ ,  $v$ ))
68:        $C_i.append(v.include(prevoteProof_i))$ 
69:        $Stake_i \leftarrow Stake_i + Reward_i$ 
70:        $h_i \leftarrow h_i + 1$ 
71:       reset  $lockEpoch_i$ ,  $lockValue_i$ ,  $validEpoch_i$ ,  $validValue_i$  to initial values
72:        $StartEpoch(1)$ 

73: upon  $> \frac{1}{3}$  (*,  $h_i$ ,  $epoch$ , *,  $proof$ ) with ( $epoch > epoch_i$  and  $valid(proof)$ ) do
74:    $prevoteProof_i \leftarrow proof(> \frac{1}{3}$  (*,  $h_i$ ,  $epoch$ , *, *))
75:    $StartEpoch(epoch)$ 

76: function  $OnTimeoutPropose(height, epoch)$ 
77:   if  $height = h_i$  and  $epoch = epoch_i$  and  $step_i = propose$  then
78:     broadcast (PREVOTE,  $h_i$ ,  $epoch_i$ , nil,  $prevoteProof_i$ )
79:      $step_i \leftarrow prevote$ 

80: function  $OnTimeoutPrevote(height, epoch)$ 
81:   if  $height = h_i$  and  $epoch = epoch_i$  and  $step_i = prevote$  then
82:     broadcast (PRECOMMIT,  $h_i$ ,  $epoch_i$ , nil,  $precommitProof_i$ )
83:      $step_i \leftarrow precommit$ 

84: function  $OnTimeoutPrecommit(height, epoch)$ 
85:   if  $height = h_i$  and  $epoch = epoch_i$  then
86:      $StartEpoch(epoch_i + 1)$ 

87: upon  $m$  from  $P^j$  with  $valid(m) = FALSE$  for the first time do
88:    $DevProofs_i[j] \leftarrow proof(valid(m) = FALSE)$ 
89:   broadcast (SLASH,  $P^j$ ,  $h_i$ ,  $epoch_i$ ,  $m$ ,  $DevProofs_i[j]$ )

90: upon (SLASH,  $P^j$ ,  $m$ ,  $proof$ ) from  $P^k$  with  $valid(proof)$  do
91:   if  $DevProofs_i[j] = nil$  then
92:      $DevProofs_i[j] \leftarrow proof$ 
93:     broadcast (SLASH,  $P^j$ ,  $m$ ,  $DevProofs_i[j]$ )

94: function  $adjustForSlashing(newDeviators)$ 
95:    $slashedShare \leftarrow sum(Shares_i[newDeviators])$ 
96:    $Shares_i[newDeviators] \leftarrow 0$ 
97:    $Shares_i \leftarrow \lfloor \frac{Shares_i[k]}{1 - slashedShare} \rfloor$  for  $k \in [1, \dots, n]$ 
98:    $Reward_i \leftarrow (1 - slashedShare) Reward_i$  ▷ Same reward adjustment as in FAIRISCAL
99:    $Stake_i \leftarrow (1 - slashedShare) Stake_i$  ▷ Remove deviating stake
100:   $Stake_i \leftarrow Stake_i + sum(\{Genesis.shares()[j] \text{ for } j \in newDeviators\}) \cdot Reward_i$  ▷
   Slash Bonus, not dependant on ordering

```

As the total voting power in the system is 1, this means if there are new deviators proposed in a particular valid value (line 24) with total share s_{dev} , the maximum total voting share for that value is $1 - s_{dev}$. This ensures any player P_i at height H with share s_i^{H-1} after deciding on the block at height $H - 1$ can only have 0 or s_i^{H-1} voting power. Rules ending with ‘for the first time’ should only be executed on the first time the corresponding condition is *TRUE*.

The algorithm proceeds in epochs, with each epoch having a dedicated proposer. The mapping of epochs to proposers is known to all players, with the function $proposer(h, epoch)$ returning the proposer for epoch $epoch$ given current blockchain height h . Player state transitions are triggered by message reception and by expiration of the timeout function $timeout()$. Timeouts are to be called once per step during each epoch, and only trigger a transition if the

player has not updated their step or epoch variable since starting the timeout function.

In [14] it is proved that non-Byzantine players need to incorporate increasing timeouts in the number of epochs at a particular height to guarantee eventual progression. In Tenderstake, we also incorporate increasing timeouts in epochs, but instead leave the precise definition of the timeout function $timeout()$ to each player. We do however place the following restriction on the $timeout()$ calculation: the value of $timeout()$ is increasing in the number of epochs at every height, such that $\lim_{epoch \rightarrow \infty} timeout(epoch) \rightarrow \infty$.

The intuition behind this choice is leaving it sufficiently general so as to not risk choosing some specific delta/ function for delta which would expose us to unnecessary optimisation analysis, while also ensuring Tenderstake retains the property of increasing timeouts in the number of epochs at each height required in the original Tendermint protocol to guarantee safety and liveness.

Messages in Tenderstake contain one of the following tags: PROPOSAL, PREVOTE, PRECOMMIT and SLASH. The PROPOSAL tag is used by the proposer of the current epoch to suggest a potential decision value (line 25), while PREVOTE and PRECOMMIT are votes for a proposed value, as in Tendermint. SLASH messages identify player deviations, and are described in detail in Section 6.2.2.

Every player P_i stores the following variables in the Tenderstake protocol: $step_i$, $lockValue_i$, $lockEpoch_i$, $validValue_i$, $validEpoch_i$, $Stake_i$, $Shares_i$, $Reward_i$, and $DevProofs_i$, initialised in lines 5-13. The $step_i$ tracks the current step of the protocol execution during the current epoch. The $lockValue_i$ stores the most recent value for which a PRECOMMIT message was sent by P_i for a non-*nil* value, with $lockEpoch_i$ the epoch in which $lockValue_i$ was updated. As P_i can only decide on a value v if more than $\frac{2}{3}$ voting power equivalent PRECOMMIT messages are received for v , possible decision values can be any value locked by more than $\frac{1}{3}$ voting power equivalent players. Therefore any value v for which PROPOSAL and more than $\frac{2}{3}$ voting power equivalent PREVOTE messages are received in some epoch is a possible decision value. The $validValue_i$ stores this value, while $validEpoch_i$ stores the epoch where this update occurred. The $Stake_i$ tracks the total stake in the system, and $Shares_i$ the current player shares of $Stake_i$. The $Reward_i$ is the total reward to be distributed among all players for deciding on the next value in C_i . The $DevProofs_i$ vector tracks locally observed deviators as identified by SLASH messages.

6.2.1 Proof-of-Transition Functionality. In Tenderstake, every PROPOSAL, PREVOTE and PRECOMMIT message must be accompanied by a *proof-of-transition* which evidences the transition to the current step claimed by each player is valid. These proofs are stored in the local player variables $prevoteProof_i$ and $precommitProof_i$, with $prevoteProof_i$ also acting as proof for PROPOSAL messages when a player is selected as proposer. For example, in line 57, each PRECOMMIT message must be accompanied by a *proof* which shows that the respective players were at a protocol step which allowed them to send a PRECOMMIT message (lines 49, 55 or 82). This would be true either if the player received PREVOTE messages correctly satisfying the condition at line 53, both of the conditions at lines 44, 45, or the condition at 80. As these conditions have specific PREVOTE message reception rules, and given there is only

one valid PRECOMMIT messages in each case, $valid(proof)$ is true if and only if the message was generated correctly, i.e. by receiving a set of PREVOTE messages which would trigger that PRECOMMIT message according to the protocol.

6.2.2 Slashing Functionality. If any messages/ proofs are not valid in Tenderstake, players trigger the *Slashing functionality* and send a SLASH message (line 89), which contains a proof that the offending message was indeed invalid (described in detail in Section 6.2.3). SLASH messages, along with proofs-of-transition, are a key addition to Tenderstake in order to prove ByRa SMR, as players identified as deviating by a correct player through a SLASH message will eventually be seen by all correct players. When a player is identified as deviating, their proof-of-deviation is added to the local *DevProofs* vector of the observing player. Then when a player is selected as proposer, and $validValue_i = nil$, they add all deviation proofs not already identified in C_i to their proposed value (line 24). After being seen by all correct players, any deviator will eventually be added to a correct player’s proposed value and removed from the protocol through the *adjustForSlashing* function (line 94).

The *adjustForSlashing* function takes as input new decided deviators, deletes their stakes (lines 96, 99), adjusts the remaining player shares to sum to 1 (line 97), recalibrates the per-block reward to keep the per player reward constant throughout a Tenderstake instance (line 98), and distributes the initial reward $Genesis.reward()$ times the initial shares of the deviating players among the remaining players in proportion to their stake (line 100).

6.2.3 Proof-of-Deviation. Crucial to the slashing functionality are the *proofs-of-deviation* which can be generated upon the reception of any invalid message. As invalid messages can take various forms, we explicitly define each form of invalid message and how to generate the corresponding proof-of-deviation. Invalid messages in Tenderstake can (1) contradict another message from the same sender, (2) propose invalid values, (3) contain an invalid proof-of-deviation or (4) contain an invalid proof-of-transition.

Remark 6.2. Any message which does not contain one or more of the deviations outlined in this section is *valid*.

We do not encode proofs-of-deviation here as their exact implementations are beyond the scope of the paper. However, we describe the maximum amount of information necessary to prove that a player has deviated, which can then be represented in some, possibly condensed form within a SLASH message to prove a player has deviated. In the following we assume a player P_i performs the corresponding deviation.

- (1) **Contradictory messages:** If a player sends two messages m and m' such that they both contain valid proofs-of-transition, but it is not possible to transition from either of the messages to the other, these messages together constitute a proof of deviation. For example, if there are two messages m and m' from P_i with the same h_i , $epoch_i$ and $step_i$ tags, or if P_i proposes a newly generated $getValue()$ after sending a PRECOMMIT message in a preceding epoch at the same height for a different value (which would mean $validValue_i \neq nil$).
- (2) **Invalid proposed values:** As the blockchain value validity predicate is shared by all parties and known a priori, any

message from P_i containing an invalid proposed value v can be used as a proof of deviation.

- (3) **Invalid slashing:** A slash message is invalid if the accompanying proof-of-deviation is not valid. If the proof-of-deviation is not valid, the corresponding slash message/ proposed value (if it first appears in a proposed value) stands as a proof of deviation.
- (4) **Invalid proof-of-transition:** If a message m is received from a player P_i , where P_i has not attached (a proof of) messages with tag, height, epoch and value variables which validly trigger the logical conditions necessary to send m , this constitutes an invalid proof-of-transition. These messages, or lack thereof, constitute a proof-of-deviation. As P_i signs m , the contents of m can be verified, and as such P_i ’s attempted proof-of-transition can be proved to belong to P_i (as the signature must correspond to m and the contained proof-of-transition), and proved to be invalid by all players. Any message sent by P_i which does not adhere to one of the protocol-specified **broadcast** formats⁷ is considered to contain an invalid proof-of-transition. This is because there is no protocol-specified transition that would create such a message.

6.2.4 Life-Cycle of an Epoch. Every epoch starts by a proposer suggesting a value in a Tenderstake message (line 25). If $validValue_i = nil$, this proposed value is generated by the external $getValue()$ function (line 24), as in Tendermint. In Tenderstake, players also include in their newly generated propose values any deviation proofs they have received that are not currently in C_i . Otherwise if $validValue_i \neq nil$, the proposer proposes $validValue_i$. The proposer attaches $validEpoch_i$ to the message so other processes are informed of the last epoch in which the proposer observed $validValue_i$ as a possible decision value.

Upon receiving a valid $\langle PROPOSAL, h_i, epoch_i, v, validEpoch, proofProposal \rangle$ message, a correct player P_i accepts the proposed value v if both the external function $valid(v)$ returns *TRUE* and either P_i has not locked any value ($lockEpoch_i = -1$) or P_i has locked on v (line 29). For a valid proposed value v with $validEpoch \geq 0$, if $validEpoch > validEpoch_i$ (the proposed value was more recent than P_i ’s locked value) or $lockValue_i = v$, P_i will accept v (line 36). Otherwise, P_i rejects the proposal by sending a PREVOTE message for *nil*. P_i will also send a PREVOTE message for *nil* if the timeout triggered in line 27 expires and they have not sent a PREVOTE message for any other value during this epoch yet (line 78).

If a correct player P_i receives a PROPOSAL message for a valid value v and PREVOTE messages for v from players controlling more than $\frac{2}{3}$ of the share as described by v , then it sends a PRECOMMIT message for v . Otherwise, they send a PRECOMMIT message for *nil*. A correct process will also send a PRECOMMIT message for *nil* if the timeout triggered in line 43 expires and they have not sent a PRECOMMIT message for their current epoch yet (line 82). A correct player decides on a value v if it receives in some epoch $epoch$ a PROPOSAL message for v and PRECOMMIT messages for v from players controlling more than $\frac{2}{3}$ of the share as described by v . On a decision, v , including proof of the PRECOMMIT messages

⁷Can be thought of as junk, but also includes attempted communication between players, such as to coordinate collusion.

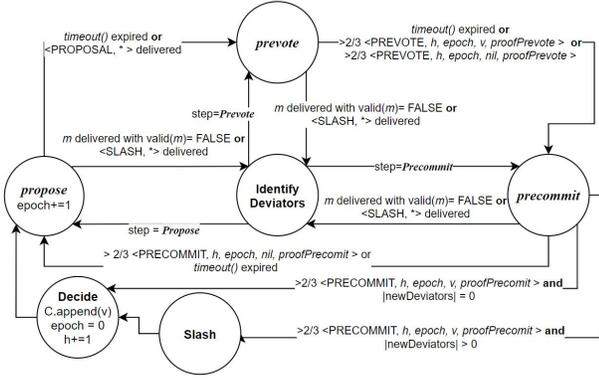


Figure 1: A state diagram representation of Tenderstake

allowing P_i to decide on v , are appended to C_i (line 68). Otherwise, to ensure progression, if the timeout triggered at line 59 expires, the player proceeds to the next epoch (line 86).

7 PROVING Tenderstake ACHIEVES ByRa SMR

In this section we prove that Tenderstake achieves SMR in the ByRa model. To this end, we first prove that it is an SMR protocol when more than $\frac{2}{3}$ of the share is controlled by honest players at all times.

Lemma 7.1. It is not possible to generate a valid deviation proof for an honest player.

PROOF. A valid deviation proof for some player P_i must identify a message from P_i that is invalid according to one of the methods listed in Section 6.2.3, which covers all possible message deviations. By definition, honest players follow all protocol rules and only send valid messages. We also know that honest player messages cannot be forged under our threat model assumption regarding unforgeable signatures from Section 6.1. Furthermore, as \mathcal{A} is static, every message signed by a currently honest player must have been generated honestly (by that same player) at some point in the protocol. Therefore, all honest player messages are valid, and as such, no valid proof-of-deviation described in Section 6.2.3 can be generated for honest players. \square

Lemma 7.2. Tenderstake achieves SMR when players controlling more than $\frac{2}{3}$ of the stake are honest.

PROOF. (*Sketch*) We outline a proof demonstrating that proposed values (line 24) satisfy safety and liveness in Tenderstake. An initialisation of Tenderstake is equivalent to a standard Tendermint initialisation, in addition to the proof-of-transition and slash functionalities as described in Sections 6.2.1 and 6.2.2 respectively. For deciding on a value at a particular height $H > 1$, voting share is described by the value decided at height $H - 1$, or the current proposed value (line 24) if it is valid and contains newly identified deviators. From Lemma 7.1, we know no valid proof of deviation can be generated for an honest player. Therefore, honest players can never be included as prospective deviators in valid proposed values in line 24. This ensures that any valid value proposed will maintain honest voting share of more than $\frac{2}{3}$.

Proof-of-transition values are simply additional pieces of information attached to standard Tendermint messages. Identically to Tendermint, Tenderstake does not consider invalid messages for any of the steps needed to decide on a block (lines 29, 44, 62, 34). Consider an epoch during synchrony, with timeouts larger than the message delivery delta Δ for all honest players (necessary to ensure liveness, as in Tendermint) and an honest proposer. This epoch occurs eventually at every height (if no decision has been reached in earlier epochs) as the network communication model and proposer rotation are identical to Tendermint, and the timeout function is increasing and unbounded in the number of epochs. As more than $\frac{2}{3}$ of the voting share is controlled by honest players at all times, honest players will decide on the proposed value during that epoch. This holds for any height $H > 1$, and the safety and liveness of Tenderstake follows. \square

With Tenderstake as an SMR protocol under an honest majority, we now need to prove Tenderstake achieves ByRa SMR. To do this, we will prove that Tenderstake is SINCE and fair in the ByRa model, and apply Theorem 5.8. To prove SINCE, we first need some results that bound the reward a player can achieve for deciding on a value. As each decided value requires an accompanying $> \frac{2}{3}$ PRECOMMIT messages to be valid, the maximum amount of values a player can attempt to decide on at once is 1, as the proceeding value will need to point to the decided value and the value's $> \frac{2}{3}$ PRECOMMIT messages. By bounding the reward a player can get for deciding on values and deviators (the only rewarding actions) sufficiently low, we are able to prove that this reward is negligible compared to the potential punishment for being caught, thus preventing rational players from sending invalid messages.

Lemma 7.3. In any instance of Tenderstake, P_i receives less than $s_i^1 \text{Genesis.reward}()$ in total for identifying deviators from the *adjustForSlashing* function.

PROOF. We can see that the rewards for deciding on new deviators at height H are distributed at line 100. We will prove that the sum of the rewards distributed by calling line 100 throughout an instance of Tenderstake are less than $s_i^1 \text{Genesis.reward}()$.

Let there be a set of players newDevs^H controlling *slashedShare* at height $H - 1$ identified as deviating for the first time in the value at height H . In the *adjustForSlashing* function, this results in P_i 's share being updated according to line 97, which implies $s_i^H = \frac{s_i^{H-1}}{1 - \text{slashedShare}}$. Furthermore, letting Reward^{H-1} be the total reward after deciding on a value at height $H - 1$, the new total reward for height H is $\text{Reward}^H = (1 - \text{slashedShare})\text{Reward}^{H-1}$ (line 98), while the total stake before distributing rewards for height H is adjusted to $(1 - \text{slashedShare})\text{Stake}^{H-1}$ (line 99), preserving the total stake of non-deviators. We then have to add the slash bonus of $\sum_{j \in \text{newDevs}^H} \text{Genesis.shares}()[j]\text{Reward}^H$ (line 100).

First observe that:

$$\begin{aligned} s_i^H \text{Reward}^H &= \frac{s_i^{H-1}}{1 - \text{slashedShare}} (1 - \text{slashedShare})\text{Reward}^{H-1} \\ &= s_i^{H-1} \text{Reward}^{H-1}. \end{aligned} \quad (3)$$

Secondly, notice that when no new deviators are identified, and *adjustForSlashing* is not called, both s_i and Reward_i are unchanged

from the previous height, as they are only adjusted in *adjustForSlashing*. This means:

$$s_i^H \text{Reward}^H = s_i^1 \text{Reward}^1 = s_i^1 \text{Genesis.reward}(), \forall H \geq 1. \quad (4)$$

We know for a set of new deviators newDevs^H at height H , P_i receives $s_i^H \text{Reward}^H \sum_{j \in \text{newDevs}^H} \text{Genesis.shares}()[j]$ (line 100). Furthermore, from Equation 4, we have that $s_i^H \text{Reward}^H = s_i^1 \text{Genesis.reward}()$ for all $H \geq 1$. This implies P_i receives an identifying deviator bonus from *adjustForSlashing* of $s_i^1 \text{Genesis.reward}() \cdot \sum_{j \in \text{newDevs}^H} \text{Genesis.shares}()[j]$ at height H . Summing over all heights up to and including H gives a total reward of $s_i^1 \text{Genesis.reward}() \cdot \sum_{k=1}^H (\sum_{j \in \text{newDevs}^k} \text{Genesis.shares}()[j])$ for identifying deviators through *adjustForSlashing*.

As $\cup_{1 \leq k \leq H} \text{newDevs}^k \subset \{1, \dots, n\}$ for all $H > 1$, it must be that $\sum_{k=1}^H (\sum_{j \in \text{newDevs}^k} \text{Genesis.shares}()[j]) < 1$ for all $H > 1$. This means the total reward for identifying deviators in Tenderstake through the *adjustForSlashing* function is less than $s_i^1 \text{Genesis.reward}()$, as required. \square

Lemma 7.4. In addition to any rewards from the *adjustForSlashing* function, P_i receives $s_i^1 \text{Genesis.reward}()$ for every decided value in Tenderstake.

PROOF. The only reward received by P_i not in *adjustForSlashing* is distributed at line 69. Letting Reward^H be the total reward distributed at line 69 for height H , P_i receives $s_i^H \text{Reward}^H$. We have already seen in Equation 4 that $s_i^H \text{Reward}^H = s_i^1 \text{Genesis.reward}()$, for all $H \geq 1$, which is the required result. \square

Remark 7.5. In Tenderstake, share increases are counteracted by reward decreases to keep per-decision rewards constant (Lemma 7.4). This avoids a common, critical, mistake in incentive compatible reward mechanisms where early share increases permanently increase the size of per-decision rewards a player receives.

Lemma 7.6. Tenderstake is SINCE in the ByRa model.

PROOF. To prove SINCE in the ByRa model, we require that every protocol action strictly dominates all other possible actions in expectation for rational players assuming all other players are rational. We do this by proving the following:

- (1) Rational players do not send invalid messages.
- (2) Rational players send valid messages when possible.
- (3) Rational players obey a timeout function which is increasing and unbounded in epochs at every height.

Firstly, consider invalid protocol messages. As an invalid message takes one of the forms described in Section 6.2.3, it can eventually be identified by all players and the offending player stake destroyed through the Slashing functionality (Section 6.2.2). As identifying deviations of other players is strictly increasing in stake (line 100) and does not affect proceeding rewards due to Lemma 7.4, all rational players prefer to eventually identify valid deviations than not identify valid deviations. As stake is only meaningful with respect to a valid blockchain, P_i must construct C_i sequentially in its height. Therefore, for h_i the height of C_i , P_i 's messages can only refer to a value at a height less than or equal to $h_i + 1$.

Combining Lemmas 7.3 and 7.4, for any height $H > 1$, the maximum additional reward achievable by sending an invalid message up to that height is less than $2s_i^1 \text{Genesis.reward}()$. This is because by Lemma 7.3, the additional reward for identifying deviators is less than $s_i^1 \text{Genesis.reward}()$, and by Lemma 7.4, the per-decided value reward excluding any reward for identifying deviators is $s_i^1 \text{Genesis.reward}()$, a constant. Therefore, attempting to decide on a value and/or deviators (the only ways to be rewarded in Tenderstake) with an invalid message results in a payoff of less than $2s_i^1 \text{Genesis.reward}()$. Due to Lemma 7.4, the rewards for proceeding value-decisions remain constant, while all rewards for identifying deviators must sum up to less than $s_i^1 \text{Genesis.reward}()$ from Lemma 7.3. Given proofs-of-deviation can be provided at any time and all rational players will send SLASH messages when possible, the cost of sending an invalid message, full destruction of stake (line 96) and effective removal from the protocol, dominates these once-off and bounded potential rewards for sending an invalid message. As such, no rational player will send an invalid message.

Given no rational player will send an invalid message, we now need to check that rational players will send messages when valid messages can be sent, as per the protocol. The alternative is not sending messages. Given the arbitrary scheduling of message delivery in any distributed network where other players have unknown timeouts, and the positive reward for deciding on a block, sending messages strictly increases the expected rate of messages received by all other players. This in turn strictly increases the expected rate of player progression through the protocol, as progression can only occur when proofs can be generated. This strictly increases the expected number of blocks, and rewards, added to the blockchain.

Lastly, we must ensure that rational players obey a timeout function which tends to infinity in the number of epochs at each height. To do this we first show that rational players obey some non-zero timeout, and then that this timeout is increasing and unbounded in number of epochs.

If a rational player does not wait for messages to be delivered, they will never be able to contribute to prevotes for valid values unless they are a proposer. After entering a new epoch they will call line 27, immediately followed by line 76, sending a *nil* prevote. Moreover, given they send a *nil* prevote and advance to the *prevote* step, they will also send a *nil* precommit (line 80) as when they receive more than $\frac{2}{3}$ prevotes it includes their own *nil* prevote, triggering line 41 before it is possible to receive more than $\frac{2}{3}$ prevotes for a valid value. By the same argumentation, they will never be able to decide on a value in the epoch it is proposed as they will first receive more than $\frac{2}{3}$ precommits for inconsistent values given their *nil* precommit message, triggering line 57 and then immediately line 84, preventing a decision. Compare this to obeying some timeout for messages to be delivered. Waiting for some number of rounds strictly increases the probability of receiving valid proposed values, and sending a prevote for a valid value. This subsequently increases the probability of all players sending valid precommits. By further obeying a timeout for precommits it increases the probability of receiving the quorum of precommits needed to decide on a value. Therefore, rational players prefer to wait some number of rounds for messages to be delivered.

Now we must ensure rational players do not wait indefinitely for messages. Recall that in Tenderstake, rational players are modelled as assuming for some unknown but fixed Δ , they are in Δ -synchrony with some subset of players. At any round r , in order to calculate expected utility for some future round, P_i will have a private distribution of expected message delivery times from other players in synchrony⁸, and thus an expected number of decisions up until that future round. Let τ_i^r be such that according to P_i 's private information, messages taking longer than τ_i^r are sent by players out of synchrony with P_i with statistical significance⁹.

If the subset of players in synchrony with P_i , including P_i , do not control more than $\frac{2}{3}$ of the total stake, P_i is indifferent to timing out, as no decision is possible. Otherwise, consider the subset of players in synchrony with P_i , including P_i , controlling more than $\frac{2}{3}$ of the total stake. As messages sent by players out of synchrony with P_i take arbitrarily long to deliver, the number of decisions that can be made by using a timeout of τ_i^r and transitioning to a proposer in synchrony with P_i is arbitrarily large. Furthermore, as P_i is unaware of how many players are in synchrony with P_i , the probability of that subset controlling more than $\frac{2}{3}$ of the stake will be positive. This implies P_i has positive expectancy to obey such a timeout τ_i^r . Therefore, rational players obey some timeout, and will not wait indefinitely for messages.

We finally need to show that for a rational P_i at any given height, P_i will follow increasing, unbounded timeouts in the number of epochs at every height. For a maximum message delivery time of Δ rounds during synchrony, if P_i follows a timeout of $\tau_i < \Delta$, P_i is not necessarily able to contribute to deciding on a value. Assume players controlling more than $\frac{2}{3}$ of the stake are in Δ -synchrony (if this is not the case, no information can be gained) and no decision has been made for some number of epochs. As players behave honestly in all non-timeout actions (points 1 and 2), the only variable which can affect the probability of deciding for this height is τ_i . Assume for all rational players there is a value $\tau_{max} > 0$, such that they choose timeouts less than τ_{max} for all epochs.

If $\tau_{max} < \Delta$, it is possible that players may always timeout, sending *nil* messages and not contributing to decisions. Given there has been *epoch* epochs of not deciding on a value, and all other actions are being followed (which we have shown to be the case), it must be that $P(\tau_{max} < \Delta | epoch \rightarrow \infty) \rightarrow 1$. This implies choosing a timeout up to and including τ_{max} after sufficiently many epochs of no decision results in decision with $negl(\kappa)$ probability for proceeding epochs. Therefore, rational players will eventually only follow timeouts greater than τ_{max} if no value has been decided, for any value of τ_{max} .

This is sufficient to say rational players follow increasing, unbounded timeouts, and as such, the recommended protocol. \square

Lemma 7.7. Tenderstake is fair in the ByRa model.

PROOF. As all rational players follow the protocol, and $s_{\mathcal{A}}^1 < \frac{1}{3}$, no rational player decides on another rational player as deviating.

⁸The distribution of expected message delivery times will be a function of some starting estimate at initialisation (perhaps based on a *Genesis* suggested value, as in [14]), and the observed responsiveness of all other players up until round r .

⁹This statistical significance can be with respect to a function $negl(\kappa)$, although rational players may perceive a higher utility by choosing a weaker significance level. This optimisation is unnecessary for the proof.

Therefore, the share of stake controlled by rational players is only increasing (line 97), meaning the adversary's share is only decreasing, upperbounded by their starting share. This implies $s_{\mathcal{A}}^H \leq s_{\mathcal{A}}^1$ for all $H \geq 1$, which is precisely the definition of a fair protocol. \square

Theorem 7.8. Tenderstake achieves ByRa SMR.

PROOF. Follows by applying Lemma 7.6 and Lemma 7.7 to Theorem 5.8. \square

8 CONCLUSION

We provide a game-theoretic framework for analysing SMR protocols. Although many previous attempts have been made, we are, to the best of our knowledge, the first to formally treat SMR protocols as games involving only rational and adversarial players. We detail the ByRa model for player characterisation in SMR protocols, an update to the legacy BAR model, removing the dependency on altruistic players in an era of unprecedented market capitalisation of tokenised SMR protocols. We demonstrate that the properties of strong incentive compatibility in expectation and fairness as described in this paper, are both necessary, and together sufficient to achieve SMR in the ByRa model. We then provide the Tenderstake protocol as an example of a protocol that achieves ByRa SMR, which is of independent interest both as a strong incentive compatible in expectation and fair protocol in the ByRa model, but also as a yardstick for addressing the shortcomings of current protocol guarantees in the ByRa model. The proof techniques we use provide several methodologies with which SMR protocols can be analysed in this new game-theoretic framework. The improvements we make to the Tendermint protocol as described in Section 6 have immediate practical implications given the current industrial deployment of Tendermint-style protocols, such as in *Cosmos*¹⁰. The application of our framework to all future SMR protocol analysis and development serves as critical future work. Another important consideration for future work is that of the ByRa model under an adaptive adversary as stated in Remark 6.1.

REFERENCES

- [1] Ittai Abraham, Srinivas Devadas, Danny Dolev, Kartik Nayak, and Ling Ren. 2017. Efficient Synchronous Byzantine Consensus. <https://eprint.iacr.org/2017/307>. Retrieved: 18/05/2021.
- [2] Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Alexander Spiegelman. 2018. Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus. In *21st International Conference on Principles of Distributed Systems (OPODIS 2017) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 95)*, James Aspnes, Alysson Bessani, Pascal Felber, and João Leitão (Eds.), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 25:1–25:19. <https://doi.org/10.4230/LIPIcs.OPODIS.2017.25>
- [3] Amitanand S. Aiyer, Lorenzo Alvisi, Allen Clement, Mike Dahlin, Jean-Philippe Martin, and Carl Porth. 2005. BAR Fault Tolerance for Cooperative Services. *SIGOPS Oper. Syst. Rev.* 39, 5 (Oct. 2005), 45–58. <https://doi.org/10.1145/1095809.1095816>
- [4] Humoud Alsabah and Agostino Capponi. 2020. Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization. <https://ssrn.com/abstract=3273982>. Retrieved: 18/05/2021.
- [5] Yackolley Amoussou-Guenou, Bruno Biaias, Maria Potop-Butucaru, and Sara Tucci-Piergiovanni. 2020. Rational vs Byzantine Players in Consensus-Based Blockchains. In *Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems (Auckland, New Zealand) (AAMAS '20)*, International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 43–51.

¹⁰*Cosmos*. <https://cosmos.network/> Accessed: 25/05/2021

- [6] Yackolley Amoussou-Guenou, Bruno Biais, Maria Potop-Butucaru, and Sara Tucci-Piergiorgianni. 2021. Rational Behaviors in Committee-Based Blockchains. In *24th International Conference on Principles of Distributed Systems (OPODIS 2020) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 184)*, Quentin Bramas, Rotem Oshman, and Paolo Romano (Eds.). Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 12:1–12:16. <https://doi.org/10.4230/LIPIcs.OPODIS.2020.12>
- [7] Yackolley Amoussou-Guenou, Antonella Del Pozzo, Maria Potop-Butucaru, and Sara Tucci-Piergiorgianni. 2018. Correctness and Fairness of Tendermint-core Blockchains. <https://arxiv.org/pdf/1805.08429>. arXiv:1805.08429 Retrieved: 18/05/2021.
- [8] Yackolley Amoussou-Guenou, Antonella Del Pozzo, Maria Potop-Butucaru, and Sara Tucci-Piergiorgianni. 2021. On Fairness in Committee-Based Blockchains. In *2nd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2020) (Open Access Series in Informatics (OASIS), Vol. 82)*, Emmanuelle Anceaume, Christophe Bisière, Matthieu Bouvard, Quentin Bramas, and Catherine Casamatta (Eds.). Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 4:1–4:15. <https://doi.org/10.4230/OASIS.Tokenomics.2020.4>
- [9] Nick Arnosti and S. Matthew Weinberg. 2019. Bitcoin: A natural oligopoly. In *10th Innovations in Theoretical Computer Science, ITCS 2019 (Leibniz International Proceedings in Informatics, LIPIcs)*, Avrim Blum (Ed.). Schloss Dagstuhl–Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Germany. <https://doi.org/10.4230/LIPIcs.ITCS.2019.5> Funding Information: Supported by NSF CCF-1717899.; 10th Innovations in Theoretical Computer Science, ITCS 2019 ; Conference date: 10-01-2019 Through 12-01-2019.
- [10] Sarah Azouvi and Alexander Hicks. 2020. SoK: Tools for Game Theoretic Models of Security for Cryptocurrencies. <https://arxiv.org/abs/1905.08595>. arXiv:1905.08595 Retrieved: 19/05/2021.
- [11] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. 2019. SoK: Consensus in the Age of Blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies (Zurich, Switzerland) (AFT '19)*. Association for Computing Machinery, New York, NY, USA, 183–198. <https://doi.org/10.1145/3318041.3355458>
- [12] Bruno Biais, Christophe Bisière, Matthieu Bouvard, and Catherine Casamatta. 2017. *The blockchain folk theorem*. IDEI Working Papers 873. Institut d'Économie Industrielle (IDEI), Toulouse. Retrieved: 19/05/2021.
- [13] Georgios Birmpas, Elias Koutsoupias, Philip Lazos, and Francisco J. Marmolejo-Cossio. 2020. Fairness and Efficiency in DAG-Based Cryptocurrencies. In *Financial Cryptography and Data Security*. Springer International Publishing, Cham, 79–96.
- [14] Ethan Buchman, Jae Kwon, and Zarko Milosevic. 2019. The latest gossip on BFT consensus. <https://arxiv.org/abs/1807.049385>. arXiv:1807.04938 Retrieved: 21/05/2021.
- [15] Eric Budish. 2018. *The Economic Limits of Bitcoin and the Blockchain*. Working Paper 24717. National Bureau of Economic Research. <https://doi.org/10.3386/w24717>
- [16] Vitalik Buterin, Daniel Reijnders, Stefanos Leonardos, and Georgios Piliouras. 2019. Incentives in Ethereum's Hybrid Casper Protocol. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, Seoul, South Korea, 236–244. <https://doi.org/10.1109/BLOC.2019.8751241>
- [17] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2019. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. <https://arxiv.org/abs/1904.05234>. arXiv:1904.05234 Retrieved: 19/05/2021.
- [18] Phil Daian, Rafael Pass, and Elaine Shi. 2019. Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake. In *Financial Cryptography and Data Security*. Springer International Publishing, Cham, 23–41. https://doi.org/10.1007/978-3-030-32101-7_2
- [19] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. 1988. Consensus in the Presence of Partial Synchrony. *J. ACM* 35, 2 (April 1988), 288–323. <https://doi.org/10.1145/42282.42283>
- [20] Ittay Eyal and Emin Gün Sirer. 2018. Majority is Not Enough: Bitcoin Mining is Vulnerable. *Commun. ACM* 61, 7 (June 2018), 95–102. <https://doi.org/10.1145/3212998>
- [21] Giulia Fanti, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang. 2019. Compounding of Wealth in Proof-of-Stake Cryptocurrencies. In *Financial Cryptography and Data Security*, Ian Goldberg and Tyler Moore (Eds.). Springer International Publishing, Cham, 42–61.
- [22] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. 2017. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In *Advances in Cryptology – CRYPTO 2017*, Jonathan Katz and Hovav Shacham (Eds.). Springer International Publishing, Cham, 357–388.
- [23] Abhiram Kothapalli, Andrew Miller, and Nikita Borisov. 2017. SmartCast: An incentive compatible consensus protocol using smart contracts. In *Financial Cryptography and Data Security - FC 2017 International Workshops, Revised Selected Papers*, Andrew Miller, Michael Brenner, Kurt Rohloff, Joseph Bonneau, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, Markus Jakobsson, and Peter Y.A. Ryan (Eds.). Springer-Verlag Berlin Heidelberg, Sliema, Malta, 536–552. https://doi.org/10.1007/978-3-319-70278-0_34
- [24] Jae Kwon. 2014. Tendermint: Consensus without Mining. <https://tendermint.com/static/docs>. Retrieved: 19/05/2021.
- [25] Kfir Lev-Ari, Alexander Spiegelman, Idit Keidar, and Dahlia Malkhi. 2020. FairLedger: A Fair Blockchain Protocol for Financial Institutions. In *23rd International Conference on Principles of Distributed Systems (OPODIS 2019) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 153)*, Pascal Felber, Roy Friedman, Seth Gilbert, and Avery Miller (Eds.). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 4:1–4:17. <https://doi.org/10.4230/LIPIcs.OPODIS.2019.4>
- [26] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. 2019. A Survey on Blockchain: A Game Theoretical Perspective. *IEEE Access* 7 (2019), 47615–47643.
- [27] Thomas Moscibroda, Stefan Schmid, and Roger Wattenhofer. 2006. When Selfish Meets Evil: Byzantine Players in a Virus Inoculation Game. <https://doi.org/10.1145/1146381.1146391>. 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, 35–44.
- [28] Thomas Moscibroda, Stefan Schmid, and Roger Wattenhofer. 2009. The Price of Malice: A Game-Theoretic Framework for Malicious Behavior. <https://doi.org/10.1080/15427951.2009.10129181>. *Internet Mathematics* 6, 2 (2009), 125–156. <https://doi.org/10.1080/15427951.2009.10129181>
- [29] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>. Retrieved: 19/05/2021.
- [30] Kevin Alarcón Negy, Peter R. Rizun, and Emin Gün Sirer. 2020. Selfish Mining Re-Examined. In *Financial Cryptography and Data Security*, Joseph Bonneau and Nadia Heninger (Eds.). Springer International Publishing, Cham, 61–78.
- [31] Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V. Vazirani. 2007. *Algorithmic Game Theory*. Cambridge University Press, Cambridge.
- [32] Rafael Pass and Elaine Shi. 2017. FruitChains: A Fair Blockchain. In *Proceedings of the ACM Symposium on Principles of Distributed Computing* (Washington, DC, USA) (PODC '17). Association for Computing Machinery, New York, NY, USA, 315–324. <https://doi.org/10.1145/3087801.3087809>
- [33] Ioanid Rosu and Fahad Saleh. 2020. Evolution of Shares in a Proof-of-Stake Cryptocurrency. <http://dx.doi.org/10.2139/ssrn.3377136>. Retrieved: 19/05/2021.
- [34] Tim Roughgarden. 2020. Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559. <https://arxiv.org/pdf/2012.00854>. arXiv:2012.00854 Retrieved: 18/05/2021.
- [35] Fahad Saleh. 2020. Blockchain Without Waste: Proof-of-Stake. <http://dx.doi.org/10.2139/ssrn.3183935>. In *Review of Financial Studies*, Vol. 34. March, 2021, 1156–1190.
- [36] Jakub Sliwinski and Roger Wattenhofer. 2020. Blockchains Cannot Rely on Honesty. <https://disco.ethz.ch/courses/fs19/sirocco/honesty.pdf>. Retrieved: 21/05/2021.