# Coalition-Safe Equilibria with Virtual Payoffs

Aggelos Kiayias *

*University of Edinburgh & IOHK*

Aikaterini-Panagiota Stouka†

*University of Edinburgh & IOHK*

January 3, 2020

**Abstract**

Consider a set of parties invited to execute a protocol Π. The protocol will incur some cost to run while in the end (or at regular intervals), it will populate and update local tables that assign (virtual) rewards to participants. Each participant aspires to offset the costs of participation by these virtual payoffs that are provided in the course of the protocol. In this setting, we introduce and study a notion of coalition-safe equilibrium. In particular, we consider a strategic coalition of participants that is centrally coordinated and potentially deviates from Π with the objective to increase its utility with respect to the view of *at least one* of the other participants. The protocol Π is called a coalition-safe equilibrium with virtual payoffs (EVP) if no such protocol deviation exists. We apply our notion to study incentives in blockchain protocols. Compared to prior work, our framework has the advantages that it simultaneously (i) takes into account that each participant may have a divergent view of the rewards given to the other participants, as the reward mechanism employed is subject to consensus among players (and our notion is well defined independently of whether the underlying protocol achieves consensus or not) (ii) accounts for the stochastic nature of these protocols enforcing the equilibrium condition to hold with overwhelming probability (iii) provides a versatile way to describe a wide variety of utility functions that are based on rewards recorded in the ledger and cost incurred during ledger maintenance. We proceed to use our framework to provide a unified picture of incentives in the Bitcoin blockchain, for absolute and relative rewards based utility functions, as well as prove novel results regarding incentives of the Fruitchain blockchain protocol [PODC 2017] showing that the equilibrium condition holds for collusions up to $n-1$ players for absolute rewards based utility functions and less than $n/2$ for relative rewards based utility functions, with the latter result holding for any "weakly fair" blockchain protocol, a new property that we introduce and may be of independent interest.

## 1 Introduction

A game involves a number of participants that engage with each other following a certain strategy profile which incurs individual costs and rewards. The utility of each participant, which rational participants aspire to maximize, is some compound real-valued function that takes into account the costs incurred and rewards resulting by the interaction. A common characteristic is that costs and rewards are bestowed authoritatively via some infrastructure that is typically

*Electronic address: akiayias@inf.ed.ac.uk

†Electronic address: a.stouka@ed.ac.uk

external to the game execution. Contrary to this, in this work, we study a game-theoretic setting where rewards are *virtual* and are recorded as an outcome of the interaction of the participants individually in each participant's local view. Thus, while costs are incurred authoritatively as before, rewards are "in the eye of the beholder" and in the end of the interaction two participants may have diverging views about the rewards that each game participant has received, while any single participant $P$ cares fundamentally that the other participants conclude in their local views that $P$ has received rewards.

Our motivation comes from the setting of distributed ledgers. These protocols were originally studied as an instance of the state machine replication problem [68] but recently were popularised again due to the introduction of the Bitcoin blockchain protocol [60]. Bitcoin is a cryptocurrency based on a blockchain protocol that maintains a public ledger containing the history of all transactions. The protocol was formally analyzed in the cryptographic setting in [31, 63]. The main idea behind the protocol is that transactions are organized into blocks and blocks form a chain, as each block contains the hash of the previous block. The longest chain is selected to determine the public ledger. A block is produced when a proof of work puzzle [11, 25, 42, 65] is solved by a node called miner. The miner that produces a block earns an amount of Bitcoin as a reward. One distinguishing feature of blockchain protocols is the emphasis they put on the incentives of the participating entities. Classically, consensus [49] was considered in various threat models, such as fail-stop failures or Byzantine. However the incentive and game theoretic aspects of the protocol have received less attention.

In blockchain protocols, the rewards that are bestowed to the participants are not assigned in an authoritative manner by some external entity, but rather are recorded as an outcome of bookkeeping that takes place by the interaction of the participants. In such setting, the relevant question is whether a strategic coalition of participants has an incentive to follow the protocol or to deviate. In its simplest form we consider a "monolithic" such coalition (abstracted as an adversary) that considers deviating from the protocol in a coordinated fashion with the aim to increase the joint utility of its members.

Different aspects of incentives in Bitcoin were studied in [10, 12, 18, 22, 26, 41, 46, 54, 57] and some type of incentive compatibility for blockchain protocols was studied in the context of a few protocols, see e.g., [7, 14, 64] (cf. Appendix A for background information on game theoretic notions). With respect to studying the participation in the core blockchain protocol, Kroll et al. in [41] show that a certain modeling of the Bitcoin protocol is a Nash equilibrium, while Eyal and Sirer in [26] show that Bitcoin is not incentive compatible because of a type of attack called selfish mining that works for any level of hashing power (for *Nash equilibrium* and *incentive compatibility* definition see Appendix A). Then again, Kiayias et al. in [46] show that there are thresholds of hashing power where certain games that abstract Bitcoin have honest behavior as a Nash equilibrium. The above seemingly contradictory results stem from differences in the game theoretic modeling of the underlying blockchain protocol and the utility function that is postulated. In addition, the existing notions of equilibria (cf. Section 1.2 below) do not appear to be sufficient to completely capture the rational behavior of participants. First, given the anticipated long term execution length of such games it is important to consider the variance of utility and thus merely looking at expected utility might be insufficient. Second, the reward mechanism employed is subject to consensus among participants and given that the protocol itself aims to achieve such consensus, each participant may have a divergent view of the rewards given to the other participants. Thus it is important that the model used to examine the protocol takes into account the possibility of such divergence and the game should be well defined independently of whether the resulting interaction achieves consistency or safety, as such properties should be the result of the rational interaction of participants, not a precondition for it!

### 1.1 Our Results

**Execution model:** Our model generalizes the execution model of [31] and it is based on the "real-world" protocol execution model of [19–21, 44] with the additional feature that certain operations of the protocol are abstracted as oracles and calling such oracles incurs a certain cost to the callee. In this way, the cost of each participant is solely dependent on participants' actions and aggregates the expenditure that is incurred during the execution based on the oracle queries posed. For example in the case of a proof-of-work blockchain protocol this may amount to the number of queries posed to the hash function.

**Utility with Virtual Payoffs:** At any point of an execution, each participant has a local view regarding the virtual rewards of all participants, including themselves. The key observation for defining utility in our setting is that given that the rewards are virtual, it is not particularly advantageous for a participant to be in a state where according to its own bookkeeping she has collected some rewards; instead what is important, is what *other* participants believe about one participant's rewards. In this way we define two types of reward functions $R^{\max}, R^{\min}$ which will correspondingly give rise to two utility functions. The $R^{\max}$ rewards of a coalition represent the maximum amount of rewards a coalition has received quantified over all *other* participants (which do not belong to the coalition), while $R^{\min}$ is similarly the minimum amount of rewards.

**Equilibria with Virtual Payoffs (EVP):** Based on these functions (reward, cost and utility functions), we present a formal notion of approximate Nash equilibrium, called coalition-safe Equilibrium with Virtual Payoffs (EVP). Informally, a protocol $\Pi$ is an EVP if it guarantees that with overwhelming probability, a rational strategic actor (hence called the *adversary*) who controls a coalition of participants, cannot gain by deviating more than an insignificant amount in terms of utility in the view of *any* of the other participants. As a result, for a given protocol $\Pi$, if there is a small, but non-negligible, probability that the utility of the adversary deviating from $\Pi$ becomes significantly higher in the view of a single other participant then such protocol will *not be* an EVP.

In more details, our notion of equilibrium is defined by examining two independent executions of the protocol in question. In the first execution the adversary controlling a coalition follows the protocol while in the second execution it might deviate in some strategic fashion. In both executions the participants who are not controlled by the adversary (we refer to them as honest participants) follow the protocol. The way in which we examine these two executions is by comparing the utilities of the adversary in these two executions for all possible environments. The underlying protocol is EVP when with overwhelming probability the $U^{\max}$ utility of the adversary when it deviates is not significantly higher compared to its $U^{\min}$ utility when it follows the protocol. This means that in order for our protocol not to be an EVP, there will be an alternative strategy and an environment with respect to which, the execution where the adversary deviates in the view of one honest participant results, with a non-negligible probability, to a significantly higher utility compared to the *lowest* utility determined for the adversarial coalition in the execution where it follows the protocol when quantified over *all* the honest participants.

**EVP Analysis of Blockchain Protocols:** In our analysis, we revisit three important utility definitions for blockchain protocols: (i) absolute rewards (ii) absolute rewards minus absolute cost and (iii) relative rewards. With the term absolute rewards we refer to the amount of the rewards that a set of participants receives at the end of the execution. With the term absolute cost we mean the cost that this set of participants pays during the execution expressed in absolute terms. With the term relative rewards we refer to the rewards of this set of participants divided by the total rewards given to all the participants. We note that the first and the third

type of utility have been considered in a number of previous works, specifically, [41,64] used the first type and [14,26,46] used the third type. In addition the second type was used in [12,48,69].

Using our model we prove positive and negative results regarding the incentives in Bitcoin unifying previous seemingly divergent views on how the protocol operates in terms of incentives, cf. Theorems 1,3,5. Specifically, we prove that Bitcoin with fixed target is an EVP in the static setting with utility based on absolute rewards, and absolute rewards minus absolute costs, while it is not with respect to relative rewards, cf. Figure 1.

Next, we prove regarding incentives of Fruitchain, [64], the following new result: when the utility is based on absolute rewards minus absolute cost, the Fruitchain protocol is an EVP in the static setting against a coalition including even up to *all but one* of the participants (Theorem 8). Moreover we define a property called "$(t, \delta)$-weak fairness" that is weaker than "fairness" defined in [64] or "ideal chain quality" described in [31] and the "race-free property" in [14] (for more details see Section 4) and is sufficient for proving that a protocol is EVP when the utility is based on relative rewards (Theorem 6). This allows us to also prove the following result: when the utility is based on relative rewards, the Fruitchain protocol is EVP in the static synchronous setting against any coalition including fewer than half of the number of the participants (assuming participants of equal hashing power, cf. Theorem 7). Further, we note that the approximation factor in the EVP is merely a constant additive factor. Regarding the level of rewards, in [64] the total rewards $V$ of an execution are derived from from (a) the flat rewards of the fruits (for details regarding what a fruit according to [64] is, see subsection 5) and (b) the transaction fees from the transactions inside the fruits; in both cases these are distributed evenly among the miners and $V$ is a fixed constant in the whole execution. Our result is also stronger in this respect, for both absolute and relative rewards based utilities, where we show that the protocol is an EVP even if rewards are a function of the security parameter or the length of the execution.

We note that our model is synchronous and in our results we consider that the adversary is static and decides in the beginning of the execution the participants it will control and the cost it will pay during each round. We will refer to it as "static adversary with fixed cost." This type of cost model is consistent with cloud mining [1] where participants establish a contract and they pay a fixed rental fee per time unit. In addition we suppose that the difficulty in mining a block is fixed. Interesting directions for future work is devising protocols that are EVPs against a dynamic adversary which adaptively fluctuates its mining resources, while the protocol itself adjusts mining difficulty; designing and proving that such EVP protocols exist is an interesting open question.

| | AbsR/AbsR-C | RelR |
|---|---|---|
| Bitcoin fixed target | $n-1$ $^{(*)}$ | NO$^{(1)}$ |
| Bitcoin variable target | NO$^{(2)}$ | NO$^{(3)}$ |
| Fruitchain | $(n-1)$ $^{(\dagger)}$ | $< n/2$ |

Figure 1: Overview of our results as well as previous results that are consistent with the EVP model. AbsR stands for a utility based on absolute rewards, AbsR-C for a utility based on absolute rewards minus absolute cost, while RelR stands for a utility based on relative rewards. The function in $n$ specifies the larger coalition size for which the equilibrium stands. $^{(1),(3)}$ are derived from [26], $^{(2)}$ is derived from [28]. The $^{(*)}$ result is informally postulated in [41]. A weaker bound of the $^{(\dagger)}$ result in terms of coalition size ($< n/2$) was shown in [64].

### 1.2 Other Related Work

A closely related work that focused on Byzantine Agreement and rational behavior is [35]. Some distinctions between our work and [35] are that (i) their utility model is tailored to the setting of (single shot) binary Byzantine agreement, while we focus on distributed ledgers that record transaction and rewards for the participants, (ii) in the definition of equilibrium they consider the expectation of utility as opposed to bounds on utility that are supposed to hold with high probability, (iii) at equilibrium, the rational adversary may deviate from the protocol as long as the properties of Byzantine agreement are not violated, while we consider any protocol deviation as potentially invalidating our equilibrium objective as long as the adversarial coalition benefits in the view of one of the other participants.

One model, introduced in [8], that combines Byzantine participants, i.e., participants that can deviate from the protocol arbitrarily, in addition to honest and rational participants, is "BAR." This model includes three types of participants: altruistic, Byzantine and rational and was used to analyse two types of protocols, IC-BFT (Incentive-Compatible Byzantine Fault Tolerant) and Byzantine Altruistic Rational Tolerant (BART) protocols [8]. The first type of protocols (i) satisfies the security properties of a Byzantine Fault Tolerant protocol (safety and liveness) in a setting with Byzantine/honest participants and (ii) guarantees that the best choice for rational participants is to follow the protocol. This guarantee is provided under the following assumptions: (a) if following the protocol is a Nash equilibrium then the rational participants will adopt it as a strategy, (b) rational participants do not collude, and (c) the expected utility of the rational participants is computed considering that the Byzantine participants react in such a way that minimizes the utility of the rational participants. One of the advantages of the IC-BFT model is that it can be used to argue that rational participants have incentives to follow the protocol due to property (ii) and thus they can be considered as honest and in such case the resulting protocol will still be resilient to some Byzantine behaviour due to property (i).

Another game theoretic notion that takes into account malicious and rational participants in the context of multi-party computation is called "$\epsilon$-$(k,t)$-robust Nash equilibrium" defined in [4]. In this type of equilibrium no participant in a coalition of up to $k$ participants should be able to increase their utility given that there exist up to $t$ malicious participants. Note that in our case following [64] when we consider coalitions we study their joint utility (by summing individual rewards) and not the utility of each participant separately something that results in a more relaxed notion in this respect (but still suitable for the distributed ledger setting: following [31, 64] when we study proof of work cryptocurrencies, each participant represents a specific amount of computational power. So a coalition of participants could also be thought to represent one miner).

In [30] a framework for "rational protocol design" is described that is based on the simulation paradigm. That framework was extended and used for examining the incentive compatibility of Bitcoin in [12]. The basic premise is that the miners aim to maximize their expected revenue and the framework describes a game between two participants: a protocol designer D and an attacker A. The Designer D aims to design a protocol that maximizes the expected revenue of the non adversarial participants and keep the blockchain consistent without forks. The adversary A aims to maximize its expected revenue. One difference of our model compared to [12] is that we let the adversary deviate from the protocol not only if its expected utility increases significantly by deviating, but even if it can increase its actual utility significantly just with not negligible probability. In addition [12] focuses exclusively on the incentive compatibility of Bitcoin and only when utility is equivalent to absolute rewards minus absolute cost.

Other related works that study the incentive compatibility of Bitcoin according to a specific utility are [26,41,46]. In addition, the incentives of nodes who do not want necessarily to engage in mining but they want to use the Bitcoin system for transactions have been studied in [37].

As we already mentioned, in [64] the Fruitchain protocol is presented, which preserves the

security properties of Bitcoin protocol and satisfies a $\delta$-approximate fairness property (assuming honest majority) that is shown to be enough for incentive compatibility when the utility is equivalent to absolute rewards. In addition, in [64] a definition of approximate Nash equilibrium is described, denoted by"$\rho$-coalition-safe $\epsilon$-Nash equilibrium" that guarantees protocol conformity with overwhelming probability. Our EVP definition is both more general and more explicit in the sense that: (i) It includes a formal description of the properties of the protocol's executions that give rise to the random variables that should be compared. (ii) It includes a formal definition of reward and utility functions. (iii) It takes into account in a rigorous way the fact that local views of honest participants may diverge and it is well defined even when the underlying protocol view of participants are inconsistent.

Some other works that investigate the interplay between Cryptography and Game theory in different settings are [3, 4, 34, 43, 62]. Some proof-of-stake blockchain protocols (protocols that do not rely on proof of work to achieve consensus) that can be proved to be incentive compatible using some notion of equilibrium are [15, 47]. A framework for identifying attacks against the incentive schemes of the blockchain protocols is proposed in [40]. In [17], proof of work blockchain protocols are modeled as stochastic games while in [56] a survey of game theoretic applications in the blockchain setting is presented.

Previous works on the general topic of rational multi-party protocols include [5,24,29,58,71] while a related line of research explored cheap talk [4,32,51,70]. For example cheap talk [23,27] was used in [4] for simulating an honest mediator given (i) secure private channels between agents that incur no cost, (ii) a punishment strategy such as having the participants stop the protocol if misbehaviour is detected.

A game theoretic notion that can be used to handle protocols operating in asynchronous networks is the "ex post Nash equilibrium" and was used in this context in [6, 38]. The way this was used in our context, was to include also adversarial nodes in addition to rational nodes and in [6] the adversarial nodes would determine some specific choices in the protocol execution (such as the initial signal the agents get and the order in which agents are scheduled). The equilibrium condition is required to hold regardless of the choices of the adversarial nodes and even if the rational participants know these choices.

Another property (apart from these we have already referred to) related to "fairness" is "t-immunity" in [4]. This property also considers utility as an expectation. Note that the notion of fairness has also been used in [53]. A notion of weak fairness has also been used in [55] for a different purpose. Specifically in [55] fairness refers to exchanges between participants; both or neither of the participants receive the intended output.

Finally we note that coalition-safety has been examined also in the context of cheap talk [52] and in computational games with mediator [62].

## 2 Our Model

Our definition of coalition-safe equilibria with virtual payoffs is built on a model of protocol execution that extends the model described in [31], and is based on [19–21, 44]. This model constitutes the basis for analyzing incentives in an arbitrary blockchain protocol $\Pi$ (but is not necessarily restricted to blockchain protocols). The main components of the model are: a system of interactive Turing machines ITMs ($\mathcal{Z}$,$\mathcal{C}$), a strategic coalition of participants that abstractly are referred to as the "adversary", $\mathcal{A}$ which is also an ITM, and the ITM instances (ITIs) $P_1, P_2, ..., P_n$ that represent the participants of our protocol that run the blockchain protocol $\Pi$. $\mathcal{C}$ is the control program that controls the interactions between the ITIs. $\mathcal{Z}$ is the "environment" or in other words the initial Turing machine that represents the external world to the protocol. It gives inputs to the participants and the adversary and it receives outputs from them. The adversary is static and controls a set of $t'$ participants $T \equiv \{P_{i_1}, ..., P_{i_{t'}}\} \subseteq \{P_1, ..., P_n\} \equiv S$ in the beginning of the execution. In the definition of equilibrium we will put forth, we consider

executions where adversary follows an arbitrary strategy while the remaining participants follow $\Pi$.

The execution is synchronous and is progressing in rounds as in [31], which means that at the end of each round all the honest participants receive all the messages sent from all the other honest participants. However, compared to [31], instead of just a random oracle on which a cryptographic hash function is modeled, we allow for many oracles where each oracle represents a cryptographic task, such as issuing a digital signature. We denote those by $O_1, \ldots, O_l$. The environment $\mathcal{Z}$ is forced by the control program $\mathcal{C}$ to activate all the participants in sequence performing a "round-robin" participant execution. Each participant can ask each oracle $O_k$ an upper bounded number of queries $q_k$ during each round and each query has a cost $c_k$. The limitation in access is controlled by the control program $\mathcal{C}$. The participants produce messages delivered via a "Diffuse Functionality" as in [31].

The Diffuse functionality adjusts the protocol execution in rounds and determines the communication between the honest participants and the adversary. Specifically it allows the adversary to see the messages produced by the honest participants and delay them until the end of the round. So the adversary can deliver first its messages. However at the end of each round, the Diffuse functionality delivers to all the honest participants all the messages sent from the other honest participants. Note that the Diffuse functionality gives the opportunity to the adversary to deliver first its own messages to the honest participants. We provide this capability to the adversary "for free", i.e., robustness will be defined even in settings where the adversary has an inexpensive way of influencing message delivery to its advantage.

In order to model our notion of equilibrium we need to compare between two possible executions across arbitrary environments. Given this, it is important to fix the number of rounds the environment runs the protocol. To accomodate this, we will define as *$r$-admissible* an environment which performs the protocol a number of rounds $r = p(\kappa) \neq 0$, where $p$ a polynomial, after which it will terminate the execution. Note also that in line with [20, 21] the input of the environment will be $1^{p'(\kappa)}$, where $p'$ a polynomial.

## 2.1 The Reward and Cost Functions

We associate with a protocol $\Pi$, a *reward function* that determines the virtual rewards of each set of participants given a local view of a participant that does not belong to the coalition after the last complete round $r$ of the execution. Each participant may have a different local view and as a result different conclusion regarding the rewards of other participants. Note that in a blockchain protocol this local view is reflected in the blockchain maintained by the participant. Formally: $\mathbb{E}$ is the set of all the executions of the protocol $\Pi$ with respect to any adversary and environment. Note that an execution $\mathcal{E}$ is completely determined by the adversary $\mathcal{A}$, the environment $\mathcal{Z}$, the control program $\mathcal{C}$ and the randomness of these processes, as all the honest participants follow the protocol $\Pi$. The randomness determines the private coins of the participants, the environment, the adversary, and the oracles like the random oracle if they exist as e.g., in [31]. We use $\mathcal{E}_{\mathcal{Z},\mathcal{A}}$ to denote this random variable, where we have specified the environment and the adversary but not the randomness.[1]

The function $R_T^j : \mathbb{E} \longrightarrow \mathbb{R}$ is called the reward function and maps an execution $\mathcal{E} \in \mathbb{E}$ to the virtual rewards of a set $T$ of participants according to the local view of a participant $P_j \in S \setminus T$ after the last complete round $r$ of the execution. As an example, in the Bitcoin blockchain protocol we can consider that the rewards for each participant to be the block rewards from the blocks that it has produced plus the transaction fees of the transactions included in these blocks. We define also $R_T^{\min}(\mathcal{E}_{\mathcal{Z},\mathcal{A}}) \equiv \min\{R_T^j(\mathcal{E}_{\mathcal{Z},\mathcal{A}})\}_{j:P_j \in S \setminus T}$, and $R_T^{\max}(\mathcal{E}_{\mathcal{Z},\mathcal{A}}) \equiv \max\{R_T^j(\mathcal{E}_{\mathcal{Z},\mathcal{A}})\}_{j:P_j \in S \setminus T}$.

[1] For simplicity we omit reference to the control program because it is the same in all the executions.

The function $C_i : \mathbb{E} \longrightarrow \mathbb{R}$ is called the cost function and maps an execution $\mathcal{E} \in \mathbb{E}$ to the cost of a participant $P_i$ until the end of the last complete round $r$ of the execution $\mathcal{E}$. Specifically $C_i(\mathcal{E}) = \sum_{k=1}^{l} c_k \cdot q_{i,k}(\mathcal{E})$, where $q_{i,k}(\mathcal{E})$ is the number of the queries that $P_i$ asked the oracle $O_k$ until the end of the last complete round $r$ of the execution $\mathcal{E}$. Note that $q_{i,k}(\mathcal{E}) \leq q_k \cdot r$.[2]

**Remark 1.** *We assume that rewards and costs are directly comparable and any exchange rate between virtual rewards and cost tokens is constant and is applied directly. Extending our results to a setting where a fluctuating exchange rate in the course of the execution exists between virtual rewards and cost tokens is an interesting direction for future work.*

### 2.2 Utility with Virtual Payoffs

We next define the (virtual) utility of a coalition of participants that are controlled by a single rational entity, the adversary. The utility may take various forms and we will consider settings where the adversary cares about its absolute rewards, its relative rewards or its absolute rewards minus its absolute cost. Other types of utility may also be defined, e.g., the adversary may want to minimize the rewards of a specific participant. We will describe the utility of a coalition controlled by a static adversary that includes the set of participants $T \equiv \{P_{i_1}, ..., P_{i_{t'}}\} \subseteq \{P_1, ..., P_n\} \equiv S$.

**Definition 1.** *We define the utility function of a $T$-coalition in the view of the $j$-th participant as a function $U_T^j : \mathbb{E} \longrightarrow \mathbb{R}$ that maps an execution of $\mathbb{E}$ to a real value.*

Based on the above, we define also $U_T^{\max}(\mathcal{E}_{\mathcal{Z},\mathcal{A}}) \equiv \max_{j \in S \setminus T}\{U_T^j(\mathcal{E}_{\mathcal{Z},\mathcal{A}})\}$ and $U_T^{\min}(\mathcal{E}_{\mathcal{Z},\mathcal{A}}) \equiv \min_{j \in S \setminus T}\{U_T^j(\mathcal{E}_{\mathcal{Z},\mathcal{A}})\}$. Using the reward and cost functions from the previous sections, we define below a few types of utilities that will be relevant in our analysis:

**Definition 2.** *Different types of utility of a coalition $T$ defined over an arbitrary $\mathcal{E} \in \mathbb{E}$:*

- **Absolute Rewards.** $U_T^j(\mathcal{E}) = R_T^j(\mathcal{E})$,
- **Absolute Rewards minus Absolute Cost.** $U_T^j(\mathcal{E}) = R_T^j(\mathcal{E}) - \sum_{l:P_l \in T} C_l(\mathcal{E})$,
- **Relative Rewards.** $U_T^j(\mathcal{E}) = \dfrac{R_T^j(\mathcal{E})}{R_S^j(\mathcal{E})}$, *if $R_S^j(\mathcal{E}) \neq 0$ and 0 otherwise.*
- **Relative Rewards minus Relative Cost.** $U_T^j(\mathcal{E}) = \dfrac{R_T^j(\mathcal{E})}{R_S^j(\mathcal{E})} - \dfrac{\sum_{l:P_l \in T} C_l(\mathcal{E})}{\sum_{l:P_l \in S} C_l(\mathcal{E})}$,

  *if $R_S^j(\mathcal{E}), \sum_{l:P_l \in S} C_l(\mathcal{E}) \neq 0$ and 0 otherwise.*

Note that the total rewards of an execution may be equal to zero. So when we define relative rewards or relative cost we should take care that the denominator will never be zero.

### 2.3 Coalition Safe Equilibria with Virtual Payoffs

We will examine two executions of a protocol with the same environment, but with different adversary and randomness: In the first execution $\mathcal{E}_{\mathcal{Z},H_T}$ the adversary runs the $H_T$ program which controls a set $T$ with cardinality less or equal $t$ and follows the protocol $\Pi$, i.e., plays "honestly." In the second execution $\mathcal{E'}_{\mathcal{Z},\mathcal{A}}$ the adversary is denoted by $\mathcal{A}$ and is an arbitrary PPT static adversary that controls the set of users $T$ which includes at most $t$ participants and might deviate in some arbitrary way from the $\Pi$. For example, in a proof of work blockchain protocol a possible deviation would be to perform selfish mining [26].

[2] Note that the rewards function is defined for a set of participants, but the cost function is defined for a specific participant. In addition we use "$\equiv$" to denote equality of sets, random variables and functions.

In more details, $H_T$ is a static adversary that controls a set $T$ of participants and follows the protocol but it takes advantage of its network presence. Note that in our case "taking advantage of its network presence" means that the adversary delivers its messages first, when multiple competing solutions/messages (such as proof of work instances) are produced during a round.[3]

**Definition 3.** *Let $\epsilon, \epsilon'$ be small positive constants near (or equal to) zero and $r$ a polynomial in $\kappa$, the security parameter. The protocol is $(t, \epsilon, \epsilon')$-equilibrium with virtual payoffs (EVP) according to a utility $\{U_T^j\}_{j \in S \setminus T}$ when for every PPT static adversary $\mathcal{A}$ that controls an arbitrary set $T$ including at most $t$ participants and for every $r$-admissible environment $\mathcal{Z}$, it holds that*

$$U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_T}) + \epsilon \cdot \mid U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_T}) \mid + \epsilon'$$

*with overwhelming probability in $\kappa$. $\mathcal{E}_{\mathcal{Z},H_T}$, $\mathcal{E'}_{\mathcal{Z},\mathcal{A}}$ are two independent random variables that represent two independent executions with the same environment $\mathcal{Z}$ and adversary $H_T$ and $\mathcal{A}$ respectively.*

**Remark 2.** *Note that we need absolute value on the right side of the inequality because $U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_T})$ can be negative when for example it is equal to the profit of a participant. We use two parameters, $\epsilon$ and $\epsilon'$, to explicitly account for multiplicative and additive deviations in the utility of the diverging adversarial coalition of participants.*

**Remark 3.** *When the adversary selects the strategy that the participants controlled by the adversay do not ask any query and do not participate at all, then its utility is zero for all possible choices of utility from Definition 2. As a result if a protocol is an EVP then this implies that the utility of $H_T$ will be not significantly smaller than 0. This parallels the participation constraint that is encountered in optimization problems in economics [39].*

The definition is generic and includes all probabilistic polynomial time (PPT) static adversaries but in our results we will consider for simplicity a *static PPT adversary with fixed cost* who decides in the beginning how many queries the participants that it controls will ask (and thus how much cost will incur). Recall that this type of cost model in the setting of proof-of-work blockchains is consistent with cloud mining [1]. Formally, we have the following.

**Definition 4.** *A static adversary with fixed cost is an adversary that chooses in the beginning of the execution to control a set $T \equiv \{P_{i_1}, ..., P_{i_{t'}}\} \subseteq \{P_1, ..., P_n\} \equiv S$ of $t'$ participants and it commits to the number of queries (of the available $q_k$) each participant $P_{i_m}$, $(m = 1, \ldots, t')$ that it controls will ask each oracle $O_k$ during each round of the execution. This number is denoted by $q_k - x_{m,k}$. This type of adversary can choose any strategy, but it is committed to paying during each round the cost that it chose in the beginning of the execution.*

## 3 Incentives in Bitcoin

As in [31] we will consider that there is only one oracle: the random oracle that models a cryptographic hash function. There are $n$ participants that are activated by the environment in a "round-robin" sequence. When each participant is activated by the environment, it asks at most $q$ queries this oracle. Each query to this random oracle has probability $p$ to give a solution which is a valid block that extends the chain. The messages/solutions are delivered

[3] We do not consider in this present treatment the cost of having a high presence in the network. Moreover, it is relatively easy to see that if network dominance is given at no cost, it is a rational choice for an adversary to opt for it in the Bitcoin setting since it will guarantee that more rewards will be accrued over time. We note that a similar type of reasoning was adopted also in [12] and the corresponding adversary was referred to as "front running."

via the Diffuse Functionality. The expected number of solutions per round by all participants is denoted by $s$. Note that our model is synchronous and $s$ is assumed to be close to zero.

Regarding Bitcoin with fixed target in a synchronous setting we prove the following results under a PPT static adversary with fixed cost. We will consider that each query to the random oracle has a cost $c$. We suppose that each block gives a *fixed flat reward* $w$ to its creator. Recall $t'$ is the number of the participants controlled by the adversary, $S$ is the set of all the participants and $T$ the set controlled by the adversary.

The results are as follows (the proofs of all the theorems are given in appendix C):

**Absolute rewards:** When the utility is based on absolute rewards (cf. Def.2), then Bitcoin with fixed target is EVP against a coalition that includes even up to all but one of the participants. This is in agreement with the result of [41]. The intuition behind this result is that if the adversary cares only about how many blocks it produces then it has no incentives to deviate from the protocol for example by creating forks or by keeping its blocks private. The reason is that if it deviates from the protocol then it increases the possibility that its blocks will not be included in the public ledger compared to following the protocol. Moreover, the number of the blocks the adversary produces during a round depends only on $p, q, t'$ and not on which chain the adversary extends.

**Theorem 1.** *For any $\delta_1 \in (0, 0.25)$ such that $4 \cdot \delta_1 \cdot (1+s)+s < 1$, where $s$ the expected number of solutions per round, Bitcoin with fixed target in a synchronous setting where the reward of each block is a constant, is $(n-1, 4 \cdot \delta_1 \cdot (1+s)+s, 0)$-EVP according to the utility function absolute rewards (Def. 2).*

Note that the better synchronicity we have (the fewer expected number of solutions per round $s$) then the better EVP[4] we have (the lower $4 \cdot \delta_1 + (1+4 \cdot \delta_1) \cdot s$ is). Recall $4 \cdot \delta_1 + (1+4 \cdot \delta_1) \cdot s$ is related to how much the adversary can gain if it deviates.

Note that in the theorem we allow the adversary to control all but one of the participants (and not all) because we want at least one honest local chain according to which we can determine the rewards of the adversary.

We extend the above result also in the setting where the block reward changes every at least $l \cdot \kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter during the execution.

**Theorem 2.** *Supposing that (i) the block reward changes every at least $l \cdot \kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter and (ii) the environment terminates the execution at least $l \cdot \kappa$ rounds after the last change of the block reward then it holds: for any $\delta_1 \in (0, 0.25)$ such that $4 \cdot \delta_1 \cdot (1+s)+s < 1$, where $s$ the expected number of solutions per round, Bitcoin with fixed target in a synchronous setting is $(n-1, 4 \cdot \delta_1 \cdot (1+s)+s, 0)$-EVP according to the utility function absolute rewards (def.2).*

For the proof see Appendix C.3.

Note that in the analysis above, we assume throughout that the target used in the proof of work function remains fixed as in [31]. It is easy to see that if this does not hold then the adversary using selfish mining [26] can cause the protocol to adopt a target that becomes greater than what is supposed to be and thus the difficulty in mining a block will decrease as the total computational power would appear smaller than it really is. In this case, the adversary can produce blocks faster and as such it can magnify its rewards resulting in a negative result in terms of EVP (see also [36]). It is an easy corollary that the protocol will not be an EVP in this case.

[4]By "better EVP" we mean that the actual values of $\epsilon, \epsilon'$ are smaller.

**Absolute rewards minus absolute cost:** When the utility is based on absolute rewards minus absolute cost then the Bitcoin protocol with fixed target is EVP against a coalition that controls even up to all but one of the participants, assuming the cost of each query $c$ is small enough compared to the block reward $w$. This is in agreement with the result of [12]. Again the better synchronicity we have, the better EVP we have.

**Theorem 3.** *Suppose that there exists $\phi \in (0, 1-s)$ such that $c < p \cdot w \cdot \phi/(1 + p \cdot q \cdot (n-1))$. Then, supposing that the reward of each block is a constant $w$, it holds: for any $\delta_1 \in (0, 0.25)$, such that $c \leq p \cdot w \cdot (1-\delta_1) \cdot \phi/(1 + p \cdot q \cdot (n-1))$ and $4 \cdot \delta_1 \cdot (1+s) + s < 1 - \phi$, where $s$ the expected number of solutions per round, Bitcoin with fixed target in a synchronous setting is $(n-1, (4 \cdot \delta_1 \cdot (1+s) + s)/(1-\phi), 0)$-EVP according to the utility function absolute rewards minus absolute cost (Def. 2).*

**Remark 4.** *The assumption that there exists $\phi \in (0, 1-s)$ such that $c < p \cdot w \cdot \phi/(1+p \cdot q \cdot (n-1))$ means that the reward of each block is high enough to compensate the miners for the cost of the mining. When the cost is high compared to the rewards and the difficulty of mining not fixed then unexpected behaviours appear as proved in [28].*

Note that the smaller the cost of each query is, the better EVP we have (because we can select smaller $\phi$ such that $(4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s)/(1-\phi)$ is smaller).

We extend the above result also to the case when the block reward changes every at least $l \cdot \kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter.

**Theorem 4.** *Assume that (i) the block reward changes every at least $l \cdot \kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter and (ii) the environment terminates the execution at least $l \cdot \kappa$ rounds after the last change of the block reward. Let $w_j$ for $j \in \{0, ..., m\}$ be all the block rewards respectively for each player. Assuming that there exists $\phi \in (0, 1-s)$ such that $c < p \cdot w_j \cdot \phi/(1 + p \cdot q \cdot (n-1))$ for all $j \in \{0, ..., m\}$, then it holds: for any $\delta_1 \in (0, 0.25)$, such that $c \leq p \cdot w_j \cdot (1-\delta_1) \cdot \phi/(1 + p \cdot q \cdot (n-1))$ for all $j \in \{0, ..., m\}$ and $4 \cdot \delta_1 \cdot (1+s) + s < 1 - \phi$, where $s$ the expected number of solutions per round, Bitcoin with fixed target in a synchronous setting is $(n-1, (4 \cdot \delta_1 \cdot (1+s) + s)/(1-\phi), 0)$-EVP according to the utility function absolute rewards minus absolute cost (Def. 2).*

For the proof see Appendix C.5.

**Relative rewards:** When the utility is based on relative rewards, i.e., the ratio of rewards of the strategic coalition of the adversary over the total rewards of all the participants, Bitcoin with fixed target cannot be an EVP with small $\epsilon, \epsilon'$. This result is in agreement with [13, 26]. The core idea is to use the selfish mining strategy [22, 26, 33, 61, 67] to construct an attack that invalidates the equilibrium property. This kind of attack was used also in [31] as argument for the tightness of "chain quality" (chain quality refers to the percentage of the blocks in the public ledger that belong to the adversary). Without loss of generality, we will assume that the reward of each block is the same and equal to $w$ (the negative result carries trivially to the general case). The result is in agreement with [26] and an argument regarding incentive compatibility of Bitcoin presented in [64]. However it seems to contradict the result from [46], which shows that in a "strategic-release game" that describes Bitcoin, honest strategy is Nash equilibrium when the adversary controls a small coalition. This difference arises because that model assumes that all honest miners act as a single miner which implies that when an honest participant produces a block, all the other honest participants adopt this block, something that does not happen in our setting where the adversary is assumed to have network dominance. Note that in [31, 64] and in our case the adversary has the advantage that it can always deliver its block first and the honest participants adopt the first block they receive. As a result, the blocks of the adversary never become dropped in a case when both the adversary and an honest participant produce a block during a round.

| Notation | |
|---|---|
| $p$ | probability with which a query to the random oracle gives a block |
| $p_f$ | probability with which a query to the random oracle gives a fruit |
| $q$ | number of queries each participant can ask the random oracle during each round |
| $t'$ | number of participants controlled by the adversary |
| $t$ | upper bound of $t'$ |
| $r$ | round after which an execution terminates |
| $n$ | number of participants |
| $w$ | flat reward per block (Bitcoin) |
| $w_f$ | flat reward per fruit (Fruitchain [64]) |
| $s$ | expected number of solutions per round |
| $x$ | the number of the queries the coalition does not ask during each round |
| $S$ | the set of all the participants |
| $T$ | the set of the participants controlled by the adversary |

**Theorem 5.** *Let $t \in \{1, ..., n-1\}$ and $t' < \min\{n/2, t+1\}$. Then for any $\epsilon + \epsilon' < \frac{t'}{n-t'} \cdot (1 - \delta') - \frac{t'}{n} \cdot (1 + \delta'') \cdot (1 + s)$, for some $\delta', \delta''$, where $s$ the expected number of solutions per round, following Bitcoin with fixed target in a synchronous setting is not a $(t, \epsilon, \epsilon')$-EVP according to the utility function relative rewards (Def. 2).*

**When Transactions Contribute to the Rewards.** Until now we have supposed that only the flat block reward contributes to the rewards. We next examine what happens when the rewards come also from the transactions included in the mined blocks.

In the description of our model we did not specify the inputs that the environment gives to each participant because these inputs did not contribute to the rewards. We can consider that the inputs are transactions as in [12, 31] and give transactions fees to the participant that will include them in the block that it will produce. The transactions have a sender and a recipient (who can be honest or adversarial participants) and constitute the way in which a participant can pay another participant. So in this setting a participant gains rewards if it produces a block and this block is included in the public ledger (the rewards of each block are the flat reward and the transaction fees) and/or if it is the recipient of a transaction that is included in a block of the public ledger. In this setting the attacks described in [18, 54] arise. For example the environment can collaborate with the adversary and send Bitcoin to the participants via the transactions that it gives to them as inputs. Specifically the environment can incentivize the recipients to support an adversarial fork by making these transactions valid only if they are included in this adversarial fork.

In addition we can consider that the environment gives the same transactions to all the participants during each round and a transaction cannot be included in more than one block. So if a participant creates an adversarial fork by producing a block that does not include the transactions with high transaction fees then the other participants have incentives to extend it even if they should deviate from the protocol. This happens because in this way they have the opportunity to include the remaining transactions in their blocks and receive the high fees. This attack was described in [22] and will be more effective when the flat block reward becomes zero and the rewards will come only from the transactions. These observations are in agreement with Theorem 7 in [12] according to which there are some distributions of inputs that make Bitcoin not incentive compatible. It is an easy corollary to prove that the protocol is not an EVP in this setting.

# 4 Incentives in a Fair Blockchain Protocol

In this section we will describe a property, called "$(t, \delta)$-weak fairness", which is sufficient for proving that a protocol is EVP when the utility is based on relative rewards (cf. Def.2). This property can aid in the design of EVP protocols.

A protocol will satisfy "$(t, \delta)$-weak fairness" property when with overwhelming probability the following hold: firstly when the adversary (which controls at most $t$ participants) deviates, then the fraction of the rewards that the set of all the honest participants gets is at least $(1-\delta)$ multiplied by its relative cost and secondly when the adversary is $H_T$, which means that it follows the protocol, any set of participants gets at least $(1-\delta)$ multiplied by its relative cost.

**Definition 5.** *A blockchain protocol satisfies $(t, \delta)$-weak fairness if for any $r$-admissible environment $\mathcal{Z}$, for any PPT adversary $\mathcal{A}$ which controls a set $T$ with at most $t$ participants and for any $j : P_j \in S \setminus T$, where $S$ the set of all the participants, we have with overwhelming probability in the security parameter $\kappa$:*

- $R^j_{S\setminus T}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \geq (1-\delta) \cdot \frac{\sum_{l:P_l \in S\setminus T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} \cdot R^j_S(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})$
- *for any subset $S_H \subseteq S$ it holds* $R^j_{S_H}(\mathcal{E}_{\mathcal{Z},H_T}) \geq (1-\delta) \cdot \frac{\sum_{l:P_l \in S_H} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} \cdot R^j_S(\mathcal{E}_{\mathcal{Z},H_T})$ *where $\delta \in [0, 1)$.*

Note that $\sum_{l:P_l \in S_H} C_l(\mathcal{E}_{\mathcal{Z},H_T}) / \sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})$ represents the computational power of $S_H$[5], because honest participants and $H_T$ ask all the queries during each round. In addition $\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T}) \neq 0$ as the execution lasts at least one round. We do not divide with $R^j_S(\mathcal{E}_{\mathcal{Z},H_T})$ as we do not exclude the case that is equal to zero.

According to the following theorem when a protocol satisfies the $(t, \delta)$-weak fairness property and the total rewards are greater than zero with overwhelming probability then following the protocol is EVP under an adversary that controls at most $t$ participants. This theorem will be also used in order to prove that the Fruitchain protocol [64] is EVP when the utility is based on relative rewards.

**Theorem 6.** *When a protocol satisfies $(t, \delta)$-weak fairness and in addition for any $j : P_j \in S\setminus T$, for any PPT adversary $\mathcal{A}$ which controls a set $T$ with at most $t$ participants and for any $r$-admissible environment $\mathcal{Z}$ it holds $R^j_S(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) > 0$ with overwhelming probability in the security parameter $\kappa$, then following the protocol is $(t, 0, \delta)$-EVP according to the utility function relative rewards (def.2).*

For the proof see Appendix D.1.

**Comparison between $(t, \delta)$-weak fairness and other notions:** Our property is weaker than $(T, \delta)$-*approximate fairness w.r.t. $\rho$ attackers* defined in [64] and *ideal chain quality* defined in [31].

The property $(T, \delta)$-*approximate fairness w.r.t. $\rho$ attackers* defined in [64] says that in any sufficient long window of the chain with $T$ blocks, any set of honest participants with computational power $\phi$ will get with overwhelming probability at least $(1-\delta) \cdot \phi$ fraction of the blocks regardless what the adversary with a fraction of computational power at most $\rho$ does.

*Ideal chain quality* defined in [31] says that any coalition of participants (regardless the mining strategy they follow) will get a percentage of blocks in the blockchain that is proportional to their collective hashing power.

[5] $\sum_{l:P_l \in S_H} C_l(\mathcal{E}_{\mathcal{Z},H_T}) / \sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T}) = (c \cdot q \cdot r \cdot t_H)/(c \cdot q \cdot r \cdot n)$ where $t_H$ the number of participants of $S_H$

Our property is weaker than $(T_0, \delta)$-*approximate fairness w.r.t.* $t/n$ *attackers* ($n$ is the number of all the participants)[6] defined in [64] and *ideal chain quality* in [31] in the sense that when the adversary deviates from the protocol we demand that only the whole set of the honest participants gets a fraction of rewards at least $(1-\delta)$ multiplied by its relative cost, not all the subsets of the honest participants. In the same way our definition is also weaker than *race-free property* defined in [14][7].

# 5 Incentives in the Fruitchain Protocol

In this section, we analyze incentives of [64]. As before we assume the participants use a hash function which is modeled as a random oracle. The number of the queries to the random oracle by each participant during a round is bounded by $q$. Let the total number of the participants be $n$. Each query to the random oracle can give with probability $p$ a block and with probability $p_f$ a fruit, where $p_f$ is assumed to be greater than $p$. This is achieved via the 2-for-1 POW technique of [31]. At the beginning of each round, when the honest participants are activated, they "receive" the fruits and the blocks from the Diffuse Functionality, they choose the chain that they will try to extend and they include in the block they try to produce "a fingerprint" of all the "recent" fruits (as defined in [64]) that have not been included in the blockchain yet. Then they ask the random oracle $q$ queries. When an honest participant finds a fruit or a block, it gives it to the Diffuse Functionality and it continues asking the remaining queries. Even if it finds more than one fruit during a round, it gives all the fruits to the Diffuse Functionality. The adversary is activated at the end and it can ask $t' \cdot q$ queries, where $t'$ is the number of the participants that it controls. We consider that the rewards come only from the fruit[8] and the difficulty in mining a block is fixed. In our case each query to the random oracle has a cost $c$. In the proofs we will assume that the adversary is static, the model is synchronous and the Diffuse Functionality works as [31], and each fruit gives reward equal to $w_f$.

**Relative rewards:** According to the following theorem if the adversary controls fewer than half of the participants and wants to maximize its relative rewards which means that its utility is based on relative rewards (Def. 2), then following the Fruitchain protocol is EVP. This theorem allows us to understand in a formal way how mining simultaneously fruits and blocks can eliminate the impact of selfish mining [26] on the incentive compatibility of the protocol. We note that the core advantage stems from the 2-for-1 POW technique used for simultaneous mining which was initially proposed for the mitigation of selfish mining in [31] in the context of achieving Byzantine agreement for honest majority and later was adapted in [64] for a similar purpose in the context of fair blockchains.

**Theorem 7.** *Let $\delta \in (0,1)$ and $T_0$ such that the Fruitchain protocol satisfies $(T_0, \delta)$-approximate fairness property. Then the Fruitchain protocol is $(n/2-1, 0, \delta)$-EVP according to the utility function relative rewards (Def. 2), under an $r$-admissible environment where $r \geq T_0/(p_f \cdot (\frac{n}{2}+1) \cdot (1-\delta) \cdot q)$.*

[6] To be precise it is weaker than fairness under the restriction that the environment performs the protocol so many rounds that with overwhelming probability any honest participant has a local chain of length at least $T_0$. Note that this happens because in our definition we have not used $T_0$ as parameter.

[7] Note that when a cryptocurrency is pseudonymous and not anonymous then it is difficult to secure that every subset of honest participants will take the appropriate percentage of the blocks, because maybe it is the case where the adversary cannot decrease much the percentage of the blocks that belongs to the whole set of the honest participants, but it can act against a specific participant with some characteristics revealed from the graph of the transactions. For example there are some works that analyze the statistical properties of the Bitcoin transaction graph and describe identification attacks in Bitcoin, [59,66]

[8] Note that in the Fruitchain protocol [64] the fainess property holds for the fruits; actual blocks are possibly still vulnerable to selfish mining attacks [26]. So if we consider that also the blocks give a flat reward then we cannot use the fairness property proved in [64].

For the proof see Appendix D.2. It uses Chernoff bound and Theorem 6.

Note that for any $\delta \in (0,1)$ and appropriate $T_0$ the Fruitchain protocol satisfies $(T_0, \delta)$-approximate fairness property (Subsection 4.2 in [64])[9].

**Remark 5.** *The above theorem holds also when we take into account also the transaction fees from each fruit and at the end of the execution we distribute evenly the total rewards among the miners of the fruits (as assumed in [64][10]).*

**Absolute rewards minus absolute cost:** We will prove that the Fruitchain [64] protocol in a synchronous setting is EVP according to utility based on absolute rewards minus absolute cost (Def. 2) if the adversary controls all but one participants, when the cost of each query $c$ is small enough compared to the reward of each fruit $w_f$. Note that the smaller the cost of each query is, the better EVP we have.[11]

The intuition behind the proof is that (i) the rewards come from the fruits that are produced by mining and (ii) the total number of the fruits the adversary can produce is bounded (with overwhelming probability) whatever strategy it follows. So if the adversary can have this number of fruits even if it follows the protocol, it has no reason to deviate.

**Theorem 8.** *Assume that each fruit gives a constant reward and there exists $\phi \in (0,1)$ such that $c < p_f \cdot w_f \cdot \phi$. Then for any $\delta_1 \in (0, 0.25)$, such that $c \leq p_f \cdot w_f \cdot (1-\delta_1) \cdot \phi$ and $4 \cdot \delta_1 < 1 - \phi$ the Fruitchain protocol in a synchronous setting is $(n-1, 4 \cdot \delta_1/(1-\phi), 0)$-EVP according to the utility function absolute rewards minus absolute cost (Def. 2) .*

For the proof see Appendix D.3.

**Remark 6.** *The assumption that there exists $\phi \in (0,1)$ such that $c < p_f \cdot w_f \cdot \phi$ means that the reward of each block is high enough to compensate the miners for the cost of the mining. Finally note that trivially if we consider that $c = 0$ then the assumption of the above theorem holds for $\phi$ close to zero and the utility is just absolute rewards (Def. 2).*

# References


[1] How does cloud mining bitcoin work? `https://www.coindesk.com/information/cloud-mining-bitcoi`

[2] *Algorithmic Game Theory*. Cambridge University Press, 2007. Nisan, N., Roughgarden, T., Tardos, E., & Vazirani, V. (Eds.). doi:10.1017/CBO9780511800481.

[3] Ittai Abraham, Lorenzo Alvisi, and Joseph Y. Halpern. Distributed computing meets game theory: Combining insights from two fields. *SIGACT News*, 42(2):69–76, June 2011.

[4] Ittai Abraham, Danny Dolev, Rica Gonen, and Joe Halpern. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation. In *Proceedings of the Twenty-fifth Annual ACM Symposium on Principles of Distributed Computing*, PODC '06, pages 53–62, New York, NY, USA, 2006. ACM.

[5] Ittai Abraham, Danny Dolev, and Joseph Y. Halpern. An almost-surely terminating polynomial protocol for asynchronous byzantine agreement with optimal resilience. In *Proceedings of the Twenty-seventh ACM Symposium on Principles of Distributed Computing*, PODC '08, pages 405–414, New York, NY, USA, 2008. ACM.


[9] In [64] the number of queries $q$ each participant can ask during each round is 1.

[10] To be precise in [64] the rewards of each fruit are shared evenly among the miners of the fruits included in a long enough preceding part of the chain.

[11] Note that here synchronicity does not affect how good the EVP is in contrast to our theorems regarding Bitcoin with fixed target. This happens because when honest participants find more than one fruit during a round, all of them can be included in the chain eventually, in contrast to Bitcoin where when two honest participants find a block during a round then only one of them can be included in the chain.

[6] Ittai Abraham, Danny Dolev, and Joseph Y. Halpern. Distributed protocols for leader election: A game-theoretic perspective. In Yehuda Afek, editor, *Distributed Computing*, pages 61–75, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

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

[8] Amitanand S. Aiyer, Lorenzo Alvisi, Allen Clement, Mike Dahlin, Jean-Philippe Martin, and Carl Porth. Bar fault tolerance for cooperative services. In *Proceedings of the Twentieth ACM Symposium on Operating Systems Principles*, SOSP '05, pages 45–58, New York, NY, USA, 2005. ACM.

[9] Robert J. Aumann. *Acceptable Points in General Cooperative n-Person Games. Contributions to the Theory of Games (AM-40)*, volume 4, pages 287–324. Albert William Tucker, Robert Duncan Luce, Princeton: Princeton University Press, 1959. Book DOI: `https://doi.org/10.1515/9781400882168`.

[10] Moshe Babaioff, Shahar Dobzinski, Sigal Oren, and Aviv Zohar. On bitcoin and red balloons. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, EC '12, pages 56–73, New York, NY, USA, 2012. ACM.

[11] Adam Back. Hashcash. `http://www.cypherspace.org/hashcash`, 1997.

[12] Christian Badertscher, Juan Garay, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. But why does it work? a rational protocol design treatment of bitcoin. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 34–65, Cham, 2018. Springer International Publishing.

[13] Suguman Bansal. *Reasoning about incentive compatibility.* POPL 2016 Student Research Competition, 2016.

[14] Iddo Bentov, Pavel Hub'avcek, Tal Moran, and Asaf Nadler. Tortoise and hares consensus: the meshcash framework for incentive-compatible, scalable cryptocurrencies. *IACR Cryptology ePrint Archive*, 2017:300, 2017.

[15] Iddo Bentov, Rafael Pass, and Elaine Shi. Snow white: Provably secure proofs of stake. *IACR Cryptology ePrint Archive*, 2016:919, 2016.

[16] B.Douglas Bernheim, Bezalel Peleg, and Michael D Whinston. Coalition-proof nash equilibria i. concepts. *Journal of Economic Theory*, 42(1):1 – 12, 1987.

[17] Bruno Biais, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta. *The Blockchain Folk Theorem.* Swiss Finance Institute Research Paper No. 17-75, 2018.

[18] Joseph Bonneau. Why buy when you can rent? - bribery attacks on bitcoin-style consensus. In Jeremy Clark, Sarah Meiklejohn, Peter Y. A. Ryan, Dan S. Wallach, Michael Brenner, and Kurt Rohloff, editors, *Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*, volume 9604 of *Lecture Notes in Computer Science*, pages 19–26. Springer, 2016.

[19] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings of the 42Nd IEEE Symposium on Foundations of Computer Science*, FOCS '01, pages 136–145, Washington, DC, USA, 2001. IEEE Computer Society.

[20] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, Jan 2000.

[21] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2000. `https://eprint.iacr.org/2000/067`.

[22] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, and Arvind Narayanan. On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 154–167, New York, NY, USA, 2016. ACM.

[23] Vincent P. Crawford and Joel Sobel. Strategic information transmission. *Econometrica*, 50(6):1431–1451, 1982.

[24] Varsha Dani, Mahnush Movahedi, Yamel Rodriguez, and Jared Saia. Scalable rational secret sharing. In Cyril Gavoille and Pierre Fraigniaud, editors, *Proceedings of the 30th Annual ACM Symposium on Principles of Distributed Computing, PODC 2011, San Jose, CA, USA, June 6-8, 2011*, pages 187–196. ACM, 2011.

[25] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Ernest F. Brickell, editor, *Advances in Cryptology — CRYPTO' 92*, pages 139–147, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

[26] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Nicolas Christin and Reihaneh Safavi-Naini, editors, *Financial Cryptography and Data Security*, pages 436–454, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[27] Joseph Farrell. Cheap talk, coordination, and entry. *The RAND Journal of Economics*, 18(1):34–39, 1987.

[28] Amos Fiat, Anna Karlin, Elias Koutsoupias, and Christos Papadimitriou. Energy equilibria in proof-of-work mining. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, EC '19, pages 489–502, New York, NY, USA, 2019. ACM.

[29] Georg Fuchsbauer, Jonathan Katz, and David Naccache. Efficient rational secret sharing in standard communication networks. In Daniele Micciancio, editor, *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, volume 5978 of *Lecture Notes in Computer Science*, pages 419–436. Springer, 2010.

[30] Juan Garay, Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Rational protocol design: Cryptography against incentive-driven adversaries. In *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, FOCS '13, pages 648–657, Washington, DC, USA, 2013. IEEE Computer Society.

[31] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, pages 281–310, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[32] Dino Gerardi. Unmediated communication in games with complete and incomplete information. *Journal of Economic Theory*, 114(1):104 – 131, 2004.

[33] Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 3–16, New York, NY, USA, 2016. ACM.

[34] Adam Groce and Jonathan Katz. Fair computation with rational players. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 81–98, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[35] Adam Groce, Jonathan Katz, Aishwarya Thiruvengadam, and Vassilis Zikas. Byzantine agreement with a rational adversary. In Artur Czumaj, Kurt Mehlhorn, Andrew Pitts, and Roger Wattenhofer, editors, *Automata, Languages, and Programming*, pages 561–572, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[36] Cyril Grunspan and Ricardo Pérez-Marco. On profitability of selfish mining. *CoRR*, abs/1805.08281, 2018.

[37] Önder Gürcan, Antonella Del Pozzo, and Sara Tucci-Piergiovanni. On the bitcoin limitations to deliver fairness to users. In Hervé Panetto, Christophe Debruyne, Walid Gaaloul, Mike Papazoglou, Adrian Paschke, Claudio Agostino Ardagna, and Robert Meersman, editors, *On the Move to Meaningful Internet Systems. OTM 2017 Conferences*, pages 589–606, Cham, 2017. Springer International Publishing.

[38] Joseph Y. Halpern and Xavier Vilaça. Rational consensus: Extended abstract. In *Proceedings of the 2016 ACM Symposium on Principles of Distributed Computing*, PODC '16, pages 137–146, New York, NY, USA, 2016. ACM.

[39] Jr. Harvey S. James. *Incentive compatibility*. Encyclopedia Britannica, inc., 4 2014. Encyclopedia Britannica `https://www.britannica.com/topic/incentive-compatibility`.

[40] Charlie Hou, Mingxun Zhou, Yansquir Ji, Phil Daian, Florian Tramer, Giulia Fanti, and Ari Juels. Squirrl: Automating attack discovery on blockchain incentive mechanisms with deep reinforcement learning, 2019.

[41] Edward W Felten Joshua A Kroll, Ian C Davey. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Proceedings of WEIS*, 2013.

[42] Ari Juels and John G. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *NDSS*. The Internet Society, 1999.

[43] Jonathan Katz. Bridging game theory and cryptography: Recent results and future directions. In Ran Canetti, editor, *Theory of Cryptography*, pages 251–272, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[44] Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Universally composable synchronous computation. In Amit Sahai, editor, *Theory of Cryptography*, pages 477–498, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[45] Yoav Shoham Kevin Leyton-Brown. *Essentials of Game Theory: A Concise Multidisciplinary Introduction (Synthesis Lectures on Artificial Intelligence and Machine Learning)*. Morgan & Claypool Publishers, 2008.

[46] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, EC '16, pages 365–382, New York, NY, USA, 2016. ACM.

[47] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017*, pages 357–388, Cham, 2017. Springer International Publishing.

[48] Abhiram Kothapalli, Andrew Miller, and Nikita Borisov. Smartcast: An incentive compatible consensus protocol using smart contracts. In Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson, editors, *Financial Cryptography and Data Security*, pages 536–552, Cham, 2017. Springer International Publishing.

[49] Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, 1982.

[50] Stefanos Leonardos, Daniel Reijsbergen, and Georgios Piliouras. Presto: A systematic framework for blockchain consensus protocols, 2019.

[51] Matt Lepinski, Silvio Micali, Chris Peikert, and Abhi Shelat. Completely fair SFE and coalition-safe cheap talk. In Soma Chaudhuri and Shay Kutten, editors, *Proceedings of the Twenty-Third Annual ACM Symposium on Principles of Distributed Computing, PODC 2004, St. John's, Newfoundland, Canada, July 25-28, 2004*, pages 1–10. ACM, 2004.

[52] Matt Lepinski, Silvio Micali, Chris Peikert, and Abhi Shelat. Completely fair sfe and coalition-safe cheap talk. In *Proceedings of the Twenty-third Annual ACM Symposium on Principles of Distributed Computing*, PODC '04, pages 1–10, New York, NY, USA, 2004. ACM.

[53] Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. Inclusive block chain protocols. In Rainer Böhme and Tatsuaki Okamoto, editors, *Financial Cryptography and Data Security*, pages 528–547, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[54] Kevin Liao and Jonathan Katz. Incentivizing blockchain forks via whale transactions. In Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson, editors, *Financial Cryptography and Data Security*, pages 264–279, Cham, 2017. Springer International Publishing.

[55] J. Liu, W. Li, G. O. Karame, and N. Asokan. Toward fairness of cryptocurrency payments. *IEEE Security Privacy*, 16(3):81–89, May 2018.

[56] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. A survey on applications of game theory in blockchain, 2019.

[57] Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. Demystifying incentives in the consensus computer. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 706–719, New York, NY, USA, 2015. ACM.

[58] Anna Lysyanskaya and Nikos Triandopoulos. Rationality and adversarial behavior in multiparty computation. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, pages 180–197, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[59] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 127–140, New York, NY, USA, 2013. ACM.

[60] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. `http://bitcoin.org/bitcoin.pdf`.

[61] K. Nayak, S. Kumar, A. Miller, and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *2016 IEEE European Symposium on Security and Privacy (EuroS P)*, pages 305–320, March 2016.

[62] Rafael Pass and Joe Halpern. Game theory with costly computation: Formulation and application to protocol security. In *Proceedings of the Behavioral and Quantitative Game Theory: Conference on Future Directions*, BQGT '10, pages 89:1–89:1, New York, NY, USA, 2010. ACM.

[63] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 643–673, Cham, 2017. Springer International Publishing.

[64] Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In *Proceedings of the ACM Symposium on Principles of Distributed Computing*, PODC '17, pages 315–324, New York, NY, USA, 2017. ACM.

[65] R. L. Rivest, A. Shamir, and D. A. Wagner. Time-lock puzzles and timed-release crypto. Technical report, Cambridge, MA, USA, 1996.

[66] Dorit Ron and Adi Shamir. Quantitative analysis of the full bitcoin transaction graph. In Ahmad-Reza Sadeghi, editor, *Financial Cryptography and Data Security*, pages 6–24, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[67] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. Optimal selfish mining strategies in bitcoin. In Jens Grossklags and Bart Preneel, editors, *Financial Cryptography and Data Security*, pages 515–532, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.

[68] Fred B. Schneider. Implementing fault-tolerant services using the state machine approach: A tutorial. *ACM Comput. Surv.*, 22(4):299–319, 1990.

[69] Itay Tsabary and Ittay Eyal. The gap game. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 713–728, New York, NY, USA, 2018. ACM.

[70] Amparo Urbano and José Enrique Vila. Unmediated communication in repeated games with imperfect monitoring. *Games and Economic Behavior*, 46(1):143–173, 2004.

[71] John Ross Wallrabenstein and Chris Clifton. Equilibrium concepts for rational multiparty computation. In Sajal K. Das, Cristina Nita-Rotaru, and Murat Kantarcioglu, editors, *Decision and Game Theory for Security*, pages 226–245, Cham, 2013. Springer International Publishing.

# A Game Theoretic Notions

- A strategy profile, which indicates how each participant behaves in the game, is an $\epsilon$-*Nash equilibrium* when the following holds: if all but one of the participants follow their strategy indicated by the strategy profile, the remaining participant has no incentives to deviate from its indicated strategy as well, as its utility can only be increased by a small insignificant amount bounded by $\epsilon$, see e.g., [45]. Extended notions of equilibria capture strategic coalitions as well, cf. [9, 16], giving rise to "Strong" Nash Equilibria. Note that

if we show that a blockchain protocol is an $\epsilon$-Nash equilibrium, we know that nobody has the incentive to deviate from the protocol, if everybody else follows the protocol.

- The concept of *Incentive compatibility* appears in a few different forms in the literature. "Dominant-strategy incentive-compatibility" is satisfied when there is not a strictly better strategy than telling the truth or following the protocol respectively whatever the other participants do. "Bayesian-Nash incentive-compatibility" is a weaker notion and a protocol satisfies it when there is a type of Nash equilibrium called "Bayesian Nash equilibrium", where all the participants tell the truth supposing that all the other participants do the same [2]. In cryptocurrency literature some times the incentive compatibility notion is used as equivalent to the Nash equilibrium notion [50]. More broadly, maximizing the profits or maximizing the utility can be seen as an *optimization problem* that includes at least two constraints. The first constraint is *incentive compatibility* and the second constraint is the *participation constraint* which suggests that when a participant participates in the game, this does not result in lower utility compared to not participating [39].

# B Chernoff Bounds

Let $X_i : i \in \{1, ..., n\}$ are mutually independent Boolean random variables and $\forall i Pr(X_i = 1) = p$. Let $X = \sum_{i=1}^{n} X_i$ and $\mu = pn$. Then we have for any $\delta \in (0, 1]$

$$Pr(X \leq (1 - \delta)\mu) \leq e^{-\delta^2 \mu/2}$$

and

$$Pr(X \geq (1 + \delta)\mu) \leq e^{-\delta^2 \mu/3}$$

# C The Theorems and Proofs Regarding Incentives in Bitcoin

In this section we will use our definition to examine if the Bitcoin with fixed target in a synchronous setting is EVP according to different utilities under a PPT static adversary with fixed cost, when each query to the random oracle has a cost and the difficulty in mining blocks (or in other words the target of each block) is fixed. The block reward will be fixed or will change every at least $l \cdot \kappa$ rounds, where $l$ a positive constant and $\kappa$ the security parameter, as we do not take into account transaction fees (we consider only the flat reward).

In more detail, as in [31][12] we will consider that there is only one oracle: the random oracle. The difficulty in mining each block is fixed. Each honest participant asks during each round $q$ queries the random oracle. In our case each query to the random oracle has cost $c$ and not zero. The probability with which a query is successful is $p$ and $n$ is the number of the participants. Let $s$ be the expected number of solutions per round and as the model is synchronous, it is near zero. The security parameter is $\kappa$ which is the domain of the hash function.

The adversary is static and it controls an arbitrary set $T \equiv \{P_{i_1}, ..., P_{i_{t'}}\}$ with $t'$ participants. Let $x_m$ be the queries the participants controlled by the adversary $P_{i_m}$ will not ask the random oracle during each round. $x = \sum_{m=1}^{t'} x_m$ is the total number of the queries that all the participants controlled by the adversary collectively do not ask during each round. Note that $x$ is a constant not a random variable as it is determined in the beginning by the static adversary with fixed cost. It holds $0 \leq x \leq q \cdot t'$.

Let $R_T^j(\mathcal{E})$ be the rewards of the blocks that are produced by $T$ and are included in the local chain of $P_j$ after the last complete round $r$ of the execution $\mathcal{E}$.

Some clarifications regarding [31] that are useful for our proofs are described in the following subsection.

[12] We will use some notation and some proof techniques from [31].

## C.1 Clarifications about Proofs in Bitcoin

The honest participants ask during each round all the available $q$ queries even if they find a block in the middle of the round. If the honest participants find more than one block during a round they give to the Diffuse functionality only the first block. In addition even if an honest participant receives from the Diffuse Functionality in the middle of a round a block produced by another participant, it will not change the block that it tries to extend. As a result, although forks with two or more honest blocks are permitted, a chain cannot be extended by two honest blocks in a round. On the other hand, these restrictions do not hold for the participants controlled by the adversary because if a participant controlled by the adversary finds more than block during a round it can give all the blocks to the Diffuse functionality. In addition, the honest participants choose the first block they receive in the case of a tie, which means that the adversarial blocks are always preferred by the honest participants, as the adversary can deliver its block first.

Successful round (defined in [31]) for a subset of participants is a round where at least one of the participants included in this subset has found a solution. The following lemma is an extension of "Chain-Growth" Lemma 7 of [31].

**Lemma 1.** *For every r-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, at the end of each round of an execution $\mathcal{E}_{\mathcal{Z},H_T}$, the local chains of all the honest participants have the same number of blocks that is equal to the successful rounds for all the participants.*

*Proof.* This can be proved by induction on the round $r$ using the clarifications above regarding the honest participants and using the fact that every participant controlled by $H_T$ follows the protocol.

Let an arbitrary execution $\mathcal{E}_{\mathcal{Z},H_T}$. For the basis $r = 1$ : if the first round is not a successful round then all the participants have a local chain with length zero equal to the number of the successful rounds which is also zero. If the first round is successful then all the participants have a local chain of length 1. This holds because:

- the participants cannot have at the end of the first round a local chain with length zero as all the participants at the end of the first round will receive from the Diffuse Functionality all the blocks produced during the first round. Note that $H_T$ follows the protocol and always sends its blocks to the Diffuse functionality.

- the participants cannot have at the end of the first round a local chain with more than one block given that even if more than one block have been produced during the first round, these blocks can extend the length of the local chains only by one. This holds because (i) if the participants (also the participants that are controlled by $H_T$) find more than one block they give to the Diffuse functionality only the first block and (ii) even if a participant receives from the Diffuse Functionality in the middle of a round a block produced by another participant, it will not change the block that it tries to extend.

For the induction step we suppose that at the end of the round $r$ all the participants have local chains with length equal to the successful rounds and we can prove with the same arguments that at the end of round $r + 1$, if the round $r + 1$ is successful, all the participants will extend their chain by one block. □

Note that at the end of each round although the local chains of participants will have the same length, they may contain different blocks in the last part, because forks with two or more honest blocks are permitted.

**Lemma 2.** *For every r-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, at the end of each round of an execution $\mathcal{E}_{\mathcal{Z},H_T}$, the number of the blocks that are produced by the set $T$ of the participants*

*controlled by the adversary and are included in a local chain of an arbitrary honest participant are equal to the number of the successful rounds for $T$.*

*Proof.* This can be proved also by induction on the round $r$ taking into account the fact that $H_T$ delivers always its blocks first and the participants adopt the first block they receive. Specifically when both a participant controlled by the adversary and an honest participant have produced a block during a round then all the participants will adopt the block produced by the participant controlled by the adversary.

Note that $H_T$ will give to the Diffuse Functionality at most one block per round for each participant controlled by the adversary and even if there are more than one block produced by $H_T$ during a round they extend the length of the chains by one. So the local chains of the honest participants at the end of each round may contain different blocks produced by the adversary, but all will have the same number of blocks produced by the adversary.

Let an arbitrary execution $\mathcal{E}_{\mathcal{Z},H_T}$. This can be proved by induction on the round $r$. For the basis $r = 1$ : if the first round is not a successful round for $T$ then all the participants have a local chain with zero blocks produced by the participants controlled by the adversary which is equal to the number of the successful rounds for $T$ that is also zero. If the first round is successful for $T$ then all the participants have a local chain that includes exactly one block produced by the adversary $H_T$. This holds because:

- the participants cannot have at the end of the first round a local chain with no block produced by $T$, because:
  - $H_T$ follows the protocol and always sends its blocks to the Diffuse functionality which means that all participants receive its blocks.
  - the participants will adopt a block produced by $T$ at the end of the first round even if another participant has also produced a block during the first round because $H_T$ delivers its blocks first.
- the participants cannot have at the end of the first round a local chain with more than one block produced by $T$ because even if more than one block have been produced by $H_T$ during the first round these blocks can extend the length of the local chains only by one given that $H_T$ follows the protocol.

For the induction step we suppose that at the end of the round $r$ all the honest participants have local chains that include blocks produced by $T$ whose number is equal to the successful rounds for $T$. Then:

- If round $r+1$ is not a successful round for $H_T$ then the number of the blocks produced by $T$ that are included in the local chain of an arbitrary honest participant does not change.
- If round $r+1$ is successful for $T$ then all the honest participants include exactly one more block produced by $T$, not necessary the same, because of the arguments described above.

□

## C.2 Absolute Rewards

In this subsection we examine if Bitcoin is EVP when utility is equivalent to absolute rewards, which means $U_T^j \equiv R_T^j$.

Our theorem assumes that the block reward is fixed and equal to $w$. However it holds also when we assume that (i) the block reward changes every at least $l \cdot \kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter and (ii) the environment terminates the execution at least $l \cdot \kappa$ rounds after the last change of the block reward. The exact theorems and proofs of

this case are given in the next subsection. The intuition is that the number of the successful rounds of a period is independent of the number of the successful rounds of a following period with different block reward. The same it holds for the number of blocks produced by a set of participants.

By Lemma 2 we can conclude that

**Lemma 3.** *For every r-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, where $\kappa$ the security parameter it holds*

$$R_T^{\max}(\mathcal{E}_{\mathcal{Z},H_T}) \equiv R_T^{\min}(\mathcal{E}_{\mathcal{Z},H_T}) \equiv X_r^T(\mathcal{E}_{\mathcal{Z},H_T}) \cdot w$$

*where $X_r^T(\mathcal{E}_{\mathcal{Z},H_T})$ are the successful rounds for $T$ until the last complete round $r$ of execution $\mathcal{E}_{\mathcal{Z},H_T}$.*

*Proof.* The rewards of $T$ according to the local chain of an honest participant $P_j$ come from the flat reward of each block included in this local chain that is produced by a participant of $T$. Moreover the flat reward of all the blocks gives the same amount of Bitcoin equal to $w$.

By Lemma 2, at the end of the last complete round $r$ of execution $\mathcal{E}_{\mathcal{Z},H_T}$ all the honest participants have local chains whose number of blocks produced by $T$ is equal to the successful rounds for $H_T$ at the end of the round $r$. So the maximum reward of $T$ is equal to the minimum reward, as all the local chains of all the honest participants contain the same number of blocks produced by $T$, and it is equal to the successful rounds for $T$ at the end of round $r$ multiplied by $w$.

□

**Theorem.** *For any $\delta_1 \in (0, 0.25)$ such that $4 \cdot \delta_1 \cdot (1 + s) + s < 1$, where $s$ the expected number of solutions per round, the Bitcoin with fixed target in a synchronous setting where the reward of each block is a constant, is $(n - 1, 4 \cdot \delta_1 \cdot (1 + s) + s, 0)$-EVP according to the utility function absolute rewards (def.2) .*

Note that our model is synchronous and as a result the expected number of solutions per round $s$ are close to zero.

*Proof.* Let arbitrary $\delta_1 \in (0, 0.25)$ such that $4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s < 1$. We choose also an arbitrary $r$-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, where $\kappa$ the security parameter and an arbitrary adversary $\mathcal{A}$ static with fixed cost that is PPT and it controls an arbitrary set $T$ with $t'$ participants where $t' \in \{1, ..., n - 1\}$. Note that when the adversary controls 0 participants then the theorem is proved trivially as the utility of the adversary is zero regardless its strategy.

We will examine two executions of the Bitcoin with the same environment, but with different adversary : In the first execution $\mathcal{E}_{\mathcal{Z},H_T}$ the adversary is $H_T$ and in the second execution $\mathcal{E'}_{\mathcal{Z},\mathcal{A}}$ the adversary is $\mathcal{A}$. Note that the environment is the same in the two executions, which means that it gives the same inputs to the participants and it sends the same messages to the adversary, although it will receive different responses from the adversary and specifically it will receive no response from $H_T$. In addition the environment will decide before the start of the execution the round $r = p(\kappa) \neq 0$ after which it will terminate the protocol. So the two executions will last the same number of rounds as they have the same environment.

In more detail, $H_T$ follows protocol and ignores the messages that receives from the environment $\mathcal{Z}$. So in the execution $\mathcal{E}_{\mathcal{Z},H_T}$ the environment can do only the following:

- It gives transactions as input to all the participants.
- It can send messages to $H_T$, but $H_T$ will ignore it.
- It has decided when $\mathcal{E}_{\mathcal{Z},H_T}$ ended.
- It receives outputs from the participants.

Firstly by Lemma 3 and by Chernoff bound we have that:

$$U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \equiv R_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \equiv X_r^T(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot w > \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot r \cdot (1 - \delta_1) \cdot w > 0 \quad (1)$$

with overwhelming probability in $r$ and as $r = p(\kappa)$ also in $\kappa$. In more detail this can be proved as follows :

- $X^{T,m}(\mathcal{E}_{\mathcal{Z},H_{T'}})$ is a Boolean random variable, where $X^{T,m}(\mathcal{E}_{\mathcal{Z},H_{T'}}) = 1$ when round $m$ was successful for $H_T$. The variables $\{X^{T,m}(\mathcal{E}_{\mathcal{Z},H_{T'}})\}_{m=1,\ldots,r}$ are independent Bernoulli trials.
- $X_r^T(\mathcal{E}_{\mathcal{Z},H_{T'}}) \equiv \sum_{m=1}^{r} X^{T,m}(\mathcal{E}_{\mathcal{Z},H_{T'}})$ is the number of the successful rounds for $H_T$ until the last complete round $r$ of $\mathcal{E}_{\mathcal{Z},H_{T'}}$.
- $\forall m\ E[X^{T,m}(\mathcal{E}_{\mathcal{Z},H_{T'}})] = 1 - (1-p)^{qt'}$, where $p$ is the probability with which one query to the random oracle is successful and $q$ is the number of the queries that each participant can ask the oracle during each round. We consider $E[X^{T,m}\mathcal{E}_{\mathcal{Z},H_{T'}})]$ as constant. Note that $H_T$ asks all the available queries.

By Lemma 3 we have that:

$$R_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \equiv R_T^{\max}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \equiv X_r^T(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot w \quad (2)$$

By Chernoff bound we have that for any $\delta_2 \in (0,1)$ and as a result also for $\delta_1$:

$$Pr[X_r^T(\mathcal{E}_{\mathcal{Z},H_{T'}}) > (1-\delta_1) \cdot (1-(1-p)^{qt'}) \cdot r] \geq 1 - e^{-\frac{(\delta_1)^2 \cdot (1-(1-p)^{qt'}) \cdot r}{2}} \quad (3)$$

In addition with probability 1 we will prove the following that is stated in [31]:

$$(1-\delta_1) \cdot (1-(1-p)^{qt'}) \cdot r \geq \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot r \cdot (1 - \delta_1) \quad (4)$$

Specifically, it holds $1 - p \leq e^{-p}$ and as a result $1 - (1-p)^{q \cdot t'} \geq 1 - e^{-p \cdot q \cdot t'}$.

Moreover, we have that $1 - e^{-x} \geq x/(1+x)$ for $x \geq 0$ (here $x = p \cdot q \cdot t'$). and as a result :

$$1 - (1-p)^{qt'} \geq 1 - e^{-p \cdot q \cdot t'} \geq \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'}$$

The above inequalities can be proved taking the functions $f(x) = (1 - e^{-x}) \cdot (1 + x) - x$ and $g(x) = e^{-x} - 1 + x$ for $x \geq 0$ and studying their minimum value using their monotony.

So by the above inequality (4), by Lemma 3 and by equation (3) we conclude equation (1) .

In addition for any $\delta \in (0,1)$ and as a result also for $\delta_1$ it holds with overwhelming probability in $r$ and also in $\kappa$ that:

$$U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq Z_r(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \cdot w < p \cdot q \cdot t' \cdot r \cdot (1 + \delta_1) \cdot w \quad (5)$$

where $Z_r(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})$ is the number of the blocks the adversary has produced until the last complete round $r$ of $\mathcal{E'}_{\mathcal{Z},\mathcal{A}}$.

This can be proved with Chernoff bound taking into account the fact that the adversary cannot gain rewards from more blocks than these it has produced. In more detail,

- $Z_{i,j,k}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})$ is a boolean random variable and $Z_{i,j,k}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) = 1$ when at round $i$ of $\mathcal{E'}_{\mathcal{Z},\mathcal{A}}$ the $j$-th query to the random oracle of the $k$-th participant controlled by the adversary is successful. $Z_{i,j,k}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})$ are independent Bernoulli trials.

- $Z_r(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \equiv \sum_{i=1}^{r} \sum_{k=1}^{t'} \sum_{j=1}^{q-x_k} Z_{i,j,k}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})$.

  $$R_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq Z_r(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \cdot w$$

  as the adversary cannot gain rewards for more blocks than these it has produced.

- $E[Z_{i,j,k}] = p$

  By Chernoff bound we have that for any $\delta \in (0,1)$ thus also for $\delta_1$

$$Pr[Z_r(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) < p \cdot (q \cdot t' - x) \cdot r \cdot (1+\delta_1)] \geq 1 - e^{-\frac{(\delta_1)^2 \cdot p \cdot (q \cdot t' - x) \cdot r}{3}} \tag{6}$$

In addition with probability 1 it holds:

$$p \cdot (q \cdot t' - x) \cdot r \cdot (1+\delta_1) \leq p \cdot q \cdot t' \cdot r \cdot (1+\delta_1)$$

By the above equation we can conclude (5).
Finally by equations (1),(5) we have that

$$U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{1'}}) \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s) \tag{7}$$

with overwhelming probability in $r$ and also in $\kappa$.
In more detail this can be proved as follows:

- Let $F$ be the final event where it holds

  $$U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{1'}}) \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s)$$

  We want to prove that $Pr[F] \geq 1 - negl(r)$.

- Let $A$ be the event where

  $$U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{1'}}) > \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot r \cdot (1 - \delta_1) \cdot w$$

  By (1) we have $Pr[A] \geq 1 - negl(r)$.

- Let $B$ be the event where

  $$U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) < p \cdot q \cdot t' \cdot r \cdot (1 + \delta_1) \cdot w$$

  By (5) we have that $Pr[B] \geq 1 - negl(r)$.

- Using the above statements we have that

  $$Pr[A \cap B] = Pr[A] - Pr[A \cap \neg B] \geq 1 - negl(r)$$

  At this point in order to prove (7) we only have to prove that

  $$Pr[A \cap B] \leq Pr[F]$$

  In order to prove the above statement we will suppose that the event $A \cap B$ holds and we will prove that the event $F$ holds.

  So we have that when $A \cap B$ holds then:

$$
\begin{aligned}
U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) &\leq p \cdot q \cdot t' \cdot r \cdot (1+\delta_1) \cdot w \\
&\leq \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot r \cdot (1-\delta_1) \cdot w \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s) \\
&< U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s)
\end{aligned}
$$

This means that when $A \cap B$ holds then also $F$ holds that is what we want to prove.

Note that

$$\frac{1+\delta_1}{1-\delta_1} \leq 1 + 4 \cdot \delta_1$$

as $\delta_1 \in (0, 0.25)$. This can be proved if we find the minimum of the function

$$f(x) = -(1+x)/(1-x) + 1 + 4x$$

by its monotony.

Moreover $p \cdot q \cdot t' \leq p \cdot q \cdot n = s$, where $s$ the expected number of solutions of all the participants per round. Note that when the system is synchronized $s$ is close to 0. □

### C.3 Utility Equivalent to Absolute Rewards-Block Reward Changes

We will prove that the previous result holds also in the case when (i) the block reward changes every at least $l \cdot \kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter and (ii) the environment terminates the execution at least $l \cdot \kappa$ rounds after the last change of the block reward.

By Lemma 2 we have the following lemma.

**Lemma 4.** *For every $r$-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, where $\kappa$ the security parameter it holds*

$$R_T^{\max}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv R_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv \sum_{j=1}^{m+2} X_{r_j}^T(\mathcal{E}_{\mathcal{Z},H_{I'}}) \cdot w_{j-1}$$

*where $r_1, ..., r_m$ are the rounds when the block reward changes, $r_0$ is the first round, $r_{m+1}$ the last complete round of execution $\mathcal{E}_{\mathcal{Z},H_{I'}}$, $r_{m+2} = r_{m+1} + 1$, $w_0, w_1, ..., w_m = w_{m+1}$ are the block rewards respectively and $X_{r_j}^T(\mathcal{E}_{\mathcal{Z},H_{I'}})$ are the successful rounds for $T$ between the rounds $r_{j-1}$ and $r_j - 1$ included $r_{j-1}$ and $r_j - 1$.*

Note that $X_{r_j}^T(\mathcal{E}_{\mathcal{Z},H_{I'}})$ is a sum of independent Boolean random variables that are Bernoulli trials. In addition

**Lemma 5.**

$$R_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq \sum_{j=1}^{m+2} Z_{r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \cdot w_{j-1},$$

*where $r_1, ..., r_m$ are the rounds when the block reward changes, $r_0$ is the first round, $r_{m+1}$ the last complete round of execution $\mathcal{E}_{\mathcal{Z},H_{I'}}$, $r_{m+2} = r_{m+1} + 1$, $w_0, w_1, ..., w_m = w_{m+1}$ are the block rewards respectively, $Z_{r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})$ is the number of blocks produced by the adversary between the rounds $r_{j-1}$ and $r_j - 1$ included $r_{j-1}$ and $r_j - 1$.*

**Theorem.** *Supposing that (i) the block reward changes every at least $l \cdot \kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter and (ii) the environment terminates the execution at least $l \cdot \kappa$ rounds after the last change of the block reward then it holds: for any $\delta_1 \in (0, 0.25)$ such that $4 \cdot \delta_1 \cdot (1+s) + s < 1$, where $s$ the expected number of solutions per round, the Bitcoin with fixed target in a synchronous setting is $(n-1, 4 \cdot \delta_1 \cdot (1+s) + s, 0)$-EVP according to the utility function absolute rewards (def.2).*

*Proof.* We have for $j \in \{1, ..., m\}$ for any $\delta_2 \in (0, 1)$

$$X^T_{r_j}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot w_j > \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot (r_j - r_{j-1}) \cdot (1 - \delta_2) \cdot w_j > 0$$

with overwhelming probability in $r_j - r_{j-1}$ and as $r_j - r_{j-1} \geq l \cdot \kappa$ also in $\kappa$.

In addition

$$(X^T_{r_{m+1}}(\mathcal{E}_{\mathcal{Z},H_{T'}}) + X^T_{r_{m+2}}(\mathcal{E}_{\mathcal{Z},H_{T'}})) \cdot w_m > \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot (r_{m+1} - r_m + 1) \cdot (1 - \delta_2) \cdot w_m$$

with overwhelming probability in $r_{m+1} - r_m + 1 \geq l \cdot \kappa$.

Moreover for $j \in \{1, ..., m\}$ for any $\delta_1 \in (0, 1)$ it holds

$$Z_{r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) < p \cdot q \cdot t' \cdot (r_j - r_{j-1}) \cdot (1 + \delta_1)$$

with overwhelming probability in $r_j - r_{j-1}$ and as $r_j - r_{j-1} \geq l \cdot \kappa$ also in $\kappa$.

Also

$$Z_{r_{m+1}}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) + Z_{r_{m+2}}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) < p \cdot q \cdot t' \cdot (r_{m+1} - r_m + 1) \cdot (1 + \delta_1)$$

with overwhelming probability in $r_{m+1} - r_m + 1 \geq l \cdot \kappa$.

So for $j \in \{1, ..., m\}$ it holds for any $\delta_1 \in (0, 0.25)$

$$Z_{r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \cdot w_j < X^T_{r_j}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot w_j \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s)$$

with overwhelming probability in $\kappa$.

In addition

$$(Z_{r_{m+1}}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) + Z_{r_{m+2}}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})) \cdot w_m < (X^T_{r_{m+1}}(\mathcal{E}_{\mathcal{Z},H_{T'}}) + X^T_{r_{m+2}}(\mathcal{E}_{\mathcal{Z},H_{T'}})) \cdot w_m \cdot l$$

with overwhelming probability in $\kappa$, where $l = (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s)$.

As a result with overwhelming probability in $\kappa$ it holds for any $\delta_1 \in (0, 0.25)$

$$\begin{aligned}
&R^{\max}_T(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \\
&\leq \sum_{j=1}^{m} [Z_{r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \cdot w_{j-1}] + (Z_{r_{m+1}}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) + Z_{r_{m+2}}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})) \cdot w_m \\
&< \sum_{j=1}^{m} [X^T_{r_j}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot w_{j-1} \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s)] \\
&+ (X^T_{r_{m+1}}(\mathcal{E}_{\mathcal{Z},H_{T'}}) + X^T_{r_{m+2}}(\mathcal{E}_{\mathcal{Z},H_{T'}})) \cdot w_m \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s) \\
&\overset{w_m = w_{m+1}}{\leq} (\sum_{j=1}^{m+2} X^T_{r_j}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot w_{j-1}) \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s) \\
&\equiv R^{\min}_T(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot (1 + 4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s)
\end{aligned}$$

□

### C.4 Absolute Rewards Minus Absolute Cost

In this subsection we prove that if a static adversary with fixed cost wants to maximize its profit and the cost of each query to the random oracle is small enough compared to the block reward, then the adversary has no incentives to deviate from the Bitcoin protocol even if it controls $n - 1$ participants.

When we say profit we mean absolute rewards minus absolute cost or in other words the flat reward the adversary gets from the blocks that it has produced and are included in the public ledger minus the cost that it has paid due to the queries to the random oracle.

Note that the smaller the cost of each query is, the better EVP we have. We suppose in this subsection for simplicity that the reward of each block is fixed and equal to $w$. However the theorem also holds when we assume that (i) the block reward changes every at least $l \cdot \kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter and (ii) the environment terminates the execution at least $l \cdot \kappa$ rounds after the last change of the block reward. The exact theorems and proofs of this case are given in the next subsection.

**Theorem.** *Suppose that there exists $\phi \in (0, 1-s)$ such that $c < p \cdot w \cdot \phi/(1 + p \cdot q \cdot (n-1))$. Then, supposing that the reward of each block is a constant $w$, it holds: for any $\delta_1 \in (0, 0.25)$, such that $c \leq p \cdot w \cdot (1-\delta_1) \cdot \phi/(1 + p \cdot q \cdot (n-1))$ and $4 \cdot \delta_1 \cdot (1+s) + s < 1 - \phi$, where $s$ the expected number of solutions per round, the Bitcoin with fixed target in a synchronous setting is $(n-1, (4 \cdot \delta_1 \cdot (1+s) + s)/(1-\phi), 0)$-EVP according to the utility function absolute rewards minus absolute cost (def.2).*

*Proof.* We choose an arbitrary $r$-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, where $\kappa$ the security parameter and an arbitrary adversary $\mathcal{A}$ static with fixed cost that is PPT and it controls an arbitrary set $T$ with $t'$ participants where $t' \in \{1, ..., n-1\}$. The adversary as described above has chosen the number of the queries that each participant controlled by the adversary will not ask during each round. Let $x$ the total number of the queries that all the participants controlled by the adversary will not ask during each round.

We will have two executions of the Bitcoin protocol with the same environment, but with different adversary : In the first execution $\mathcal{E}_{\mathcal{Z},H_T}$ the adversary is $H_T$ and in the second execution ${\mathcal{E}'}_{\mathcal{Z},\mathcal{A}}$ the adversary is $\mathcal{A}$.

Let $\phi \in (0, 1-s)$ such that $c < p \cdot w \cdot \phi/(1 + p \cdot q \cdot (n-1)) \leq p \cdot w \cdot \phi/(1 + p \cdot q \cdot t')$. We choose an arbitrary $\delta_1 \in (0, 0.25)$ such that $c \leq p \cdot w \cdot (1-\delta_1) \cdot \phi/(1 + p \cdot q \cdot (n-1))$ and $4 \cdot \delta_1 + (1 + 4 \cdot \delta_1) \cdot s < 1 - \phi$ . Then by hypothesis and by the fact that $H_T$ follows the protocol and asks all the queries that are available to the participants controlled by the adversary during each round we have that :

$$U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_T}) > \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot r \cdot (1-\delta_1) \cdot w - c \cdot q \cdot t' \cdot r \tag{8}$$

$$\geq \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot r \cdot (1-\delta_1) \cdot w - \frac{q \cdot t' \cdot r \cdot p \cdot w \cdot (1-\delta_1) \cdot \phi}{(1 + p \cdot q \cdot t')} \tag{9}$$

$$= \frac{p \cdot q \cdot t'}{1 + p \cdot q \cdot t'} \cdot r \cdot (1-\delta_1) \cdot w \cdot (1-\phi) \tag{10}$$

$$> 0 \tag{11}$$

with overwhelming probability in $r$ and also in $\kappa$.

Regarding ${\mathcal{E}'}_{\mathcal{Z},\mathcal{A}}$, given that during each round the adversary asks all the available queries except for the $x$ queries that it has specified in the beginning of the execution, the following holds with overwhelming probability in $\kappa$:

$$U_T^{\max}({\mathcal{E}'}_{\mathcal{Z},\mathcal{A}}) < p \cdot (q \cdot t' - x) \cdot r \cdot (1+\delta_1) \cdot w - c \cdot (q \cdot t' - x) \cdot r \tag{12}$$

By our assumption that $c \leq p \cdot w \cdot (1-\delta_1) \cdot \phi/(1 + p \cdot q \cdot t')$ for $\phi \in (0, 1-s)$ we have that $f(x) = p \cdot (q \cdot t' - x) \cdot r \cdot (1+\delta_1) \cdot w - c \cdot (q \cdot t' - x) \cdot r$ for $x \in [0, \infty)$ is decreasing.

So it holds with overwhelming probability in $\kappa$ that:

$$U_T^{\max}({\mathcal{E}'}_{\mathcal{Z},\mathcal{A}}) < p \cdot q \cdot t' \cdot r \cdot (1+\delta_1) \cdot w - c \cdot q \cdot t' \cdot r \tag{13}$$

As a result it holds with overwhelming probability in $r$ and in $\kappa$

$$
\begin{aligned}
&U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) - U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \\
&\overset{(13),(8)}{<} p\cdot q\cdot t'\cdot r\cdot(1+\delta_1)\cdot w - \frac{p\cdot q\cdot t'}{1+p\cdot q\cdot t'}\cdot r\cdot(1-\delta_1)\cdot w \\
&= \frac{p\cdot q\cdot t'}{1+p\cdot q\cdot t'}\cdot r\cdot(1-\delta_1)\cdot w\cdot(1-\phi)\cdot(\frac{(1+\delta_1)\cdot(1+p\cdot q\cdot t')}{(1-\delta_1)\cdot(1-\phi)} - \frac{1}{1-\phi}) \\
&\overset{10}{<} U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}})\cdot\frac{4\cdot\delta_1+(1+4\cdot\delta_1)\cdot s}{1-\phi}
\end{aligned}
$$

□

### C.5 Utility Equivalent to Absolute Rewards Minus Absolute Cost-Block Reward Changes

We will show that the result of the previous subsection holds also when we assume that (i) the block reward changes every at least $l\cdot\kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter and (ii) the environment terminates the execution at least $l\cdot\kappa$ rounds after the last change of the block reward. By Lemmas 4,5 and by the fact that the adversary is static with fixed cost we have the following lemmas

**Lemma 6.** *For every $r$-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, where $\kappa$ the security parameter it holds*

$$U_T^{\max}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv \sum_{j=1}^{m+2} X_{r_j}^T(\mathcal{E}_{\mathcal{Z},H_{I'}})\cdot w_{j-1} - \sum_{j=1}^{m+2}\sum_{l:P_l\in T} C_{l,r_j}(\mathcal{E}_{\mathcal{Z},H_{I'}})$$

*where $r_1,...,r_m$ are the rounds when the block reward changes, $r_0$ is the first round, $r_{m+1}$ the last complete round of execution $\mathcal{E}_{\mathcal{Z},H_{I'}}$, $r_{m+2}=r_{m+1}+1$ , $w_0,w_1,...,w_m=w_{m+1}$ are the block rewards respectively, $X_{r_j}^T(\mathcal{E}_{\mathcal{Z},H_{I'}})$ are the successful rounds for $T$ and $\sum_{l:P_l\in T}C_{l,r_j}(\mathcal{E}_{\mathcal{Z},H_{I'}})$ the cost for $T$ respectively between the rounds $r_{j-1}$ and $r_j-1$ included $r_{j-1}$ and $r_j-1$.*

Recall that the cost of each round is fixed and determined in the beginning of the execution.

**Lemma 7.**

$$U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq \sum_{j=1}^{m+2} Z_{r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})\cdot w_{j-1} - \sum_{j=1}^{m+2}\sum_{l:P_l\in T} C_{l,r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \tag{14}$$

*where $r_1,...,r_m$ are the rounds when the block reward changes, $r_0$ is the first round, $r_{m+1}$ the last complete round of execution $\mathcal{E'}_{\mathcal{Z},\mathcal{A}}$, $r_{m+2}=r_{m+1}+1$ , $w_0,w_1,...,w_m=w_{m+1}$ are the block rewards respectively, $Z_{r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})$ is the number of blocks produced by the adversary between the rounds $r_{j-1}$ and $r_j-1$ included $r_{j-1}$ and $r_j-1$.*

**Theorem.** *We assume that (i) the block reward changes every at least $l\cdot\kappa$ rounds where $l$ a positive constant and $\kappa$ the security parameter and (ii) the environment terminates the execution at least $l\cdot\kappa$ rounds after the last change of the block reward. Let $w_j$ for $j\in\{0,...,m\}$ be all the block rewards respectively. Assuming that there exists $\phi\in(0,1-s)$ such that $c < p\cdot w_j\cdot\phi/(1+p\cdot q\cdot(n-1))$ for all $j\in\{0,...,m\}$, then it holds: for any $\delta_1\in(0,0.25)$, such that $c\leq p\cdot w_j\cdot(1-\delta_1)\cdot\phi/(1+p\cdot q\cdot(n-1))$ for all $j\in\{0,...,m\}$ and $4\cdot\delta_1\cdot(1+s)+s<1-\phi$, where $s$ the expected number of solutions per round, the Bitcoin with fixed target in a synchronous setting is $(n-1,(4\cdot\delta_1\cdot(1+s)+s)/(1-\phi),0)$-EVP according to the utility function absolute rewards minus absolute cost (def.2).*

*Proof.* Let $t' \in \{1, ..., n-1\}$, $\phi \in (0, 1-s)$ such that $c < p \cdot w_j \cdot \phi/(1+p \cdot q \cdot (n-1)) \leq p \cdot w_j \cdot \phi/(1+p \cdot q \cdot t')$ for all $j \in \{0, ..., m\}$ and arbitrary $\delta_1 \in (0, 0.25)$ such that $c \leq p \cdot w_j \cdot (1-\delta_1) \cdot \phi/(1+p \cdot q \cdot (n-1))$ for all $j \in \{0, ..., m\}$ and $4 \cdot \delta_1 + (1+4 \cdot \delta_1) \cdot s < 1 - \phi$.

By the previous lemmas, by the assumption that for any $j \in \{0, ..., m\}$, $c \leq p \cdot w_j \cdot (1-\delta_1) \cdot \phi/(1+p \cdot q \cdot t')$ and by Chernoff bound we have with overwhelming probability in $\kappa$ :

$$
\begin{aligned}
U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \equiv & \sum_{j=1}^{m}[X_{r_j}^T(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot w_{j-1}] + (X_{r_{m+1}}^T(\mathcal{E}_{\mathcal{Z},H_{T'}}) + X_{r_{m+2}}^T(\mathcal{E}_{\mathcal{Z},H_{T'}})) \cdot w_m - \\
& \sum_{j=1}^{m+2}[\sum_{l:P_l \in T} C_{l,r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})] \\
& > \sum_{j=1}^{m}[\frac{p \cdot q \cdot t'}{1+p \cdot q \cdot t'} \cdot (r_j - r_{j-1}) \cdot (1-\delta_1) \cdot w_{j-1} \cdot (1-\phi)] + \\
& \frac{p \cdot q \cdot t'}{1+p \cdot q \cdot t'} \cdot (r_{m+1} - r_m + 1) \cdot (1-\delta_1) \cdot w_m \cdot (1-\phi) \\
& > 0
\end{aligned}
$$

and

$$
\begin{aligned}
U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq & \sum_{j=1}^{m}[Z_{r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \cdot w_{j-1}] + (Z_{r_{m+1}}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) + Z_{r_{m+2}}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})) \cdot w_m - \\
& \sum_{j=1}^{m+2}\sum_{l:P_l \in T} C_{l,r_j}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \\
& < \sum_{j=1}^{m}[p \cdot (q \cdot t') \cdot (r_j - r_{j-1}) \cdot (1+\delta_1) \cdot w_{j-1} - c \cdot (q \cdot t') \cdot (r_j - r_{j-1})] + \\
& p \cdot (q \cdot t') \cdot (r_{m+1} - r_m + 1) \cdot (1+\delta_1) \cdot w_m - c \cdot (q \cdot t') \cdot (r_{m+1} - r_m + 1)
\end{aligned}
$$

As a result, we can prove in the same way as the previous subsection that it holds with overwhelming probability in $r$ and in $\kappa$ the following :

$$
U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) - U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \leq U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \cdot \frac{4 \cdot \delta_1 + (1+4 \cdot \delta_1) \cdot s}{1-\phi}
$$

□

### C.6 Negative Results: Relative Rewards

In this subsection we prove that when the utility is based on relative rewards, i.e., the ratio of rewards of the strategic coalition of the adversary over the total rewards of all the participants, the Bitcoin with fixed target in asynchronous setting is not EVP. In this way we show how our model can be used to prove negative results. The core idea is to use the selfish mining strategy [22, 26, 33, 61, 67] to construct an attack that invalidates the equilibrium property. This kind of attack was used also in [31] as argument for the tightness of "chain quality". Without loss of generality, we will assume that the reward of each block is the same and equal to $w$ (the negative result carries trivially to the general case).

In more detail, for an arbitrary $t \in \{1, ..., n-1\}$ and $t' < \min\{n/2, t+1\}$ we show that the protocol is not a $(t, \epsilon, \epsilon')$-EVP for $\epsilon + \epsilon' < \frac{t'}{n-t'} \cdot (1-\delta') - \frac{t'}{n} \cdot (1+\delta'') \cdot (1+s)$, for $\delta', \delta''$ small. Recall that $s = p \cdot q \cdot n$ are the expected number of solutions per round.

**Theorem.** *Let $t \in \{1, ..., n-1\}$ and $t' < \min\{n/2, t+1\}$. Then for any $\epsilon + \epsilon' < \frac{t'}{n-t'} \cdot (1 - \delta') - \frac{t'}{n} \cdot (1 + \delta'') \cdot (1 + s)$, where $s$ the expected number of solutions per round, for some $\delta', \delta''$, following the Bitcoin with fixed target in asynchronous setting is not $(t, \epsilon, \epsilon')$-EVP according to the utility function relative rewards (def.2).*

*Proof.* Let $t \in \{1, ..., n-1\}$. We consider an arbitrary $r$-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$ and we will describe a PPT static adversary $A_0$ with fixed cost (who controls a set $T$ with $t' < \min\{n/2, t+1\}$ participants) such that it holds with high probability :

$$U_T^{\max}(\mathcal{E}'_{\mathcal{Z},A_0}) - U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \tag{15}$$

$$\geq \frac{t' \cdot (1 - \delta_1) \cdot (1 - \epsilon''')}{(n - t') \cdot (1 + \delta_4)} - \frac{t' \cdot (1 + p \cdot q \cdot n)}{n} \cdot \frac{(1 + \delta_2)}{(1 - \delta_3)} \tag{16}$$

$$= B \tag{17}$$

for any $\delta_1, \delta_2, \delta_3, \delta_4 \in (0, 1)$ and a small $\epsilon''' > 0$.

After that we prove our theorem by contradiction. In more detail, we suppose that there exist $\epsilon, \epsilon'$ such that $\epsilon + \epsilon' < B$ so that the Bitcoin with fixed target in asynchronous setting is $(t, \epsilon, \epsilon')$-EVP and we will end up in contradiction . In other words we suppose that there exist $\epsilon, \epsilon'$ such that $\epsilon + \epsilon' < B$ so that

$$U_T^{\max}(\mathcal{E}'_{\mathcal{Z},\mathcal{A}}) - U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \leq \mid U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \mid \cdot \epsilon + \epsilon' \tag{18}$$

with overwhelming probability, where $A$ an arbitrary PPT static adversary with fixed cost that controls a set $T$ with at most $t$ participants and $Z$ an arbitrary $r$-admissible environment with input $1^{p'(\kappa)}$.

Then we have

$$U_T^{\max}(\mathcal{E}'_{\mathcal{Z},\mathcal{A}}) - U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \tag{19}$$

$$\leq \mid U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \mid \cdot \epsilon + \epsilon' \tag{20}$$

$$\leq \epsilon + \epsilon' \tag{21}$$

$$< B \tag{22}$$

with overwhelming probability.

However this does not hold because there exists $A_0$ that satisfies (16).

In order to prove equation (16): firstly we find an upper bound for $U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}})$ that holds with overwhelming probability in the security parameter $\kappa$.

Recall that $T$ is an arbitrary set with $t' < \min\{n/2, t+1\}$ participants that adversary $A_0$, whom we will describe later, controls.

By Lemma 2

$$R_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv R_T^{\max}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv X_r^T(\mathcal{E}_{\mathcal{Z},H_{I'}}) \cdot w$$

As a result by Chernoff bound it holds for any $\delta_2 \in (0, 1)$ with overwhelming probability in $r$ and also in $\kappa$ :

$$0 < R_T^{\max}(\mathcal{E}_{\mathcal{Z},H_{I'}}) < p \cdot q \cdot t' \cdot (1 + \delta_2) \cdot w \cdot r. \tag{23}$$

By Lemma 1

$$R_S^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv R_S^{\max}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv X_r^S(\mathcal{E}_{\mathcal{Z},H_{I'}}) \cdot w \tag{24}$$

As a result for any $\delta_3 \in (0, 1)$ with overwhelming probability in $r$ and also in $\kappa$ :

$$R_S^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv R_S^{\max}(\mathcal{E}_{\mathcal{Z},H_{I'}}) > \frac{p \cdot q \cdot n}{1 + p \cdot q \cdot n} \cdot r \cdot (1 - \delta_3) \cdot w > 0 \tag{25}$$

Recall that the executions last at least one round. So we know that with overwhelming probability in $\kappa$ for any $j$ such that $P_j$ honest

$$U_T^j(\mathcal{E}_{\mathcal{Z},H_{I'}}) \equiv \frac{R_T^j(\mathcal{E}_{\mathcal{Z},H_{I'}})}{R_S^j(\mathcal{E}_{\mathcal{Z},H_{I'}})}$$

as $R_S^j(\mathcal{E}_{\mathcal{Z},H_{I'}}) \neq 0$.

As a result we have that for any $\delta_2, \delta_3 \in (0,1)$ it holds with overwhelming probability in $r$ and also in $\kappa$ that:

$$\begin{aligned} U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) &\leq U_T^{\max}(\mathcal{E}_{\mathcal{Z},H_{I'}}) && (26)\\ &\leq \frac{R_T^{\max}(\mathcal{E}_{\mathcal{Z},H_{I'}})}{R_S^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}})} && (27)\\ &\overset{(23),(25)}{\leq} \frac{p\cdot q\cdot t'\cdot(1+\delta_2)\cdot w\cdot r}{\frac{p\cdot q\cdot n}{1+p\cdot q\cdot n}\cdot r\cdot(1-\delta_3)\cdot w} && (28)\\ &= \frac{t'\cdot(1+p\cdot q\cdot n)}{n}\cdot\frac{(1+\delta_2)}{(1-\delta_3)} && (29) \end{aligned}$$

Now we will describe the adversary $A_0$ who does a type of selfish mining, [22,26,33,61,67], which was described also in [31] and we will find a lower bound for $U_T^{\max}(\mathcal{E}_{\mathcal{Z},A_0})$ with high probability (not negligible).

$A_0$ chooses to ask all the queries. Initially extends the chain coming from an honest participant, but when it finds a block it does not send it to the Diffuse Functionality. It continues working on its private chain until another participant announces a block. Then the adversary reveals one of its blocks to all the honest participants. When this happens all the honest participants adopt its block instead of the block coming from the honest participant. If the adversarial private chain becomes smaller than the chain coming from an honest participant then the adversary adopts the honest participant's chain. Note that when one of the participants controlled by the adversary finds a block during a round, the adversary uses the rest available queries for finding a block that extends this block.

- $X_r^{S\setminus T}(\mathcal{E'}_{\mathcal{Z},A_0}) \equiv \sum_{m=1}^{r} X^{S\setminus T,m}(\mathcal{E'}_{\mathcal{Z},A_0})$ is the number of the successful rounds for $S\setminus T$ until the last complete round $r$ of $\mathcal{E'}_{\mathcal{Z},A_0}$.
- $Z_r(\mathcal{E'}_{\mathcal{Z},A_0}) \equiv \sum_{i=1}^{r}\sum_{k=1}^{t'}\sum_{j=1}^{q-x_k} Z_{i,j,k}(\mathcal{E'}_{\mathcal{Z},A_0})$. $Z_r(\mathcal{E'}_{\mathcal{Z},A_0})$ is the number of the blocks the adversary $A_0$ has produced until the last complete round $r$ of $\mathcal{E'}_{\mathcal{Z},A_0}$.

We have that

$$R_S^{\max}(\mathcal{E'}_{\mathcal{Z},A_0}) \equiv R_S^{\min}(\mathcal{E'}_{\mathcal{Z},A_0}) \equiv X_r^{S\setminus T}(\mathcal{E'}_{\mathcal{Z},A_0})\cdot w \quad (30)$$

This holds because of Lemma 1 and due to the fact that the adversary $A_0$ does not contribute to the extension of the public ledger as it only replaces blocks. In addition it announces its blocks to all honest participants.

In addition with overwhelming probability in $\kappa$ by Chernoff bound

$$R_S^{\min}(\mathcal{E'}_{\mathcal{Z},A_0}) \equiv R_S^{\max}(\mathcal{E'}_{\mathcal{Z},A_0}) > 0$$

and as a result with overwhelming probability in $\kappa$

$$U_T^j(\mathcal{E}_{\mathcal{Z},A_0}) = \frac{R_T^j(\mathcal{E}_{\mathcal{Z},A_0})}{R_S^j(\mathcal{E}_{\mathcal{Z},A_0})}$$

Regarding $R_T^{\min}(\mathcal{E'}_{\mathcal{Z},A_0})$: the adversary $A_0$ announces its block only if an honest participant finds a block and when this happens, it announces it to all the honest participants. The honest participants always adopt its blocks . So $R_T^{\max}(\mathcal{E'}_{\mathcal{Z},A_0}) \equiv R_T^{\min}(\mathcal{E'}_{\mathcal{Z},A_0})$ with probability 1. The number of the adversarial blocks $B(\mathcal{E'}_{\mathcal{Z},A_0})$ in the local chain of an arbitrary honest at the end of the last complete round $r$ of the execution $\mathcal{E'}_{\mathcal{Z},A_0}$ are, as stated in [31], with high probability equal to the number of the blocks $Z_r(\mathcal{E'}_{\mathcal{Z},A_0})$ produced by the adversary minus a quantity bounded by $\epsilon'' \cdot p \cdot q \cdot r \cdot t'$, for small $\epsilon'' > 0$.

This happens because when the adversary $A_0$ has found more than one block during each round it means that all these blocks form a chain and extend the length of the local chains of all the honest participants. Note that when the execution ends, the adversary may have a small quantity of blocks that are unused in the case the honest participants did not have enough successful rounds.

Recall that contrary to the adversary, when the honest participants have found more than one block during a round, these blocks do not form a chain, because (i) an honest participant never sends more than one block to the Diffuse Functionality, and (ii) when an honest participant receives a block from another participant, it does not extend this new block until the end of the round.

By Chernoff bound we have with high probability for any $\delta_1 \in (0,1)$ and a small $\epsilon''' > 0$

$$R_T^{\min}(\mathcal{E'}_{\mathcal{Z},A_0}) \geq p \cdot q \cdot t' \cdot r \cdot (1-\delta_1) \cdot w \cdot (1-\epsilon''') \tag{31}$$

Moreover by Chernoff bound it holds with overwhelming probability in $\kappa$ for any $\delta_4 \in (0,1)$

$$R_S^{\max}(\mathcal{E'}_{\mathcal{Z},A_0}) \leq p \cdot q \cdot (n-t') \cdot r \cdot w \cdot (1+\delta_4) \tag{32}$$

So we have with high probability for any $\delta_4, \delta_1 \in (0,1)$ and small $\epsilon''' > 0$

$$\begin{aligned}
U_T^{\max}(\mathcal{E'}_{\mathcal{Z},A_0}) &\geq U_T^{\min}(\mathcal{E'}_{\mathcal{Z},A_0}) && (33)\\
&\geq \frac{R_T^{\min}(\mathcal{E'}_{\mathcal{Z},A_0})}{R_S^{\max}(\mathcal{E'}_{\mathcal{Z},A_0})} && (34)\\
&\geq \frac{p \cdot q \cdot t' \cdot r \cdot (1-\delta_1) \cdot (1-\epsilon''') \cdot w}{p \cdot q \cdot (n-t') \cdot r \cdot w \cdot (1+\delta_4)} && (35)\\
&= \frac{t' \cdot (1-\delta_1) \cdot (1-\epsilon''')}{(n-t') \cdot (1+\delta_4)} && (36)
\end{aligned}$$

Finally by the above and by equality (26) for any $\delta_1, \delta_2, \delta_4, \delta_3 \in (0,1)$ and small $\epsilon''' > 0$ it holds with high probability :

$$\begin{aligned}
&U_T^{\max}(\mathcal{E'}_{\mathcal{Z},A_0}) - U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{I'}}) && (37)\\
&\geq \frac{t' \cdot (1-\delta_1) \cdot (1-\epsilon''')}{(n-t') \cdot (1+\delta_4)} - \frac{t' \cdot (1+p \cdot q \cdot n)}{n} \cdot \frac{(1+\delta_2)}{(1-\delta_3)} && (38)\\
&= B && (39)
\end{aligned}$$

□

# D Our Proofs Regarding Incentives in a Fair Blockchain Protocol and the Fruitchain Protocol

## D.1 Proof of Theorem 6

*Proof.* We choose an arbitrary $r$-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, where $\kappa$ the security parameter and an arbitrary adversary $\mathcal{A}$ static that is PPT and it controls a set $T$ that

it includes $t' \leq t$ participants . We will examine two executions of the blockchain protocol with the same environment $\mathcal{Z}$, but with different adversary : In the first execution $\mathcal{E}_{\mathcal{Z},H_T}$ the adversary is $H_T$ and in the second execution $\mathcal{E'}_{\mathcal{Z},\mathcal{A}}$ the adversary is $\mathcal{A}$.

We will prove that with overwhelming probability in the security parameter for any $j$ : $P_j$ honest we have:

$$U_T^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \equiv \frac{R_T^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})}{R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})} \leq \frac{\sum_{l:P_l \in T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} + \delta \cdot \frac{\sum_{l:P_l \in S \setminus T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} \tag{40}$$

By $(t,\delta)$-weak fairness and by the fact that for any $j : P_j$ honest it holds with overwhelming probability $R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) > 0$ we have the following result:

for any $j : P_j$ honest it holds with overwhelming probability in the security parameter

$$\begin{aligned}
&R_{S\setminus T}^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \geq (1-\delta) \cdot \frac{\sum_{l:P_l \in S \setminus T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} \cdot R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \Rightarrow \\
&R_T^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \cdot (1 - (1-\delta) \cdot \frac{\sum_{l:P_l \in S \setminus T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})}) \Rightarrow \\
&R_T^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \cdot (\frac{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} - (1-\delta) \cdot \frac{\sum_{l:P_l \in S \setminus T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})}) \Rightarrow \\
&\frac{R_T^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})}{R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})} \leq \frac{\sum_{l:P_l \in T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} + \delta \cdot \frac{\sum_{l:P_l \in S \setminus T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})}
\end{aligned}$$

Note that with overwhelming probability $R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) > 0$ and as a result

$$U_T^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \equiv \frac{R_T^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})}{R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}})} \tag{41}$$

By weak fairness and by the fact that it holds with overwhelming probability $R_S^{\min}(\mathcal{E}_{\mathcal{Z},\mathcal{H}_\mathcal{T}}) > 0$ we have the following result:

$$U_T^{min}(\mathcal{E}_{\mathcal{Z},H_T}) \geq (1-\delta) \cdot \frac{\sum_{l:P_l \in T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} \tag{42}$$

By equations (40), (42) we have that with overwhelming probability in the security parameter

$$\begin{aligned}
U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) - U_T^{min}(\mathcal{E}_{\mathcal{Z},H_T}) \leq & \frac{\sum_{l:P_l \in T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} + \\
& \delta \cdot \frac{\sum_{l:P_l \in S \setminus T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} - (1-\delta) \cdot \frac{\sum_{l:P_l \in T} C_l(\mathcal{E}_{\mathcal{Z},H_T})}{\sum_{l:P_l \in S} C_l(\mathcal{E}_{\mathcal{Z},H_T})} \\
& \leq \delta
\end{aligned}$$

□

## D.2 Proof of Theorem 7

*Proof.* Given that the Fruitchain protocol satisfies $(T_0,\delta)$-approximate fairness property when the adversary controls at most $n/2-1$ participants, then it satisfies also $(n/2-1,\delta)$-weak fairness property under the restriction that the environment performs the protocol so many rounds that with overwhelming probability (in the security parameter) any honest participant has a chain of at least $T_0$ fruits. Note that by chain growth rate proved in [64] when $r \geq \frac{T_0}{p_f \cdot (\frac{n}{2}+1) \cdot (1-\delta) \cdot q}$ and the adversary controls at most $n/2-1$ participants, then indeed it holds that with overwhelming

probability any honest participant has a chain of at least $T_0$ fruits. In addition, by Chernoff bound and by the fact that the execution lasts at least one round, it holds with overwhelming probability in $\kappa$ the following: for any $j : P_j$ honest, for any PPT static adversary $\mathcal{A}$ that controls at most $n/2-1$ participants and for any $r$-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$ $R_S^j(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) > 0$. So by Theorem 6 we have that the Fruitchain protocol is $(n/2-1, 0, \delta)$-EVP under an $r$-admissible environment where $r \geq \frac{T_0}{p_f \cdot (\frac{n}{2}+1) \cdot (1-\delta) \cdot q}$. □

### D.3 Proof of Theorem 8

In this setting the adversary again is PPT, static with fixed cost, it controls a set of participants $T = \{P_{i_1}, ..., P_{i_{t'}}\} \subseteq \{P_1, ..., P_n\} = S$ and chooses in the beginning the number $x_m$ of the questions that each participant controlled by the adversary $P_{i_m}$ will not ask during each round of the execution.

*Proof.* Let an arbitrary $\delta_1 \in (0, 0.25)$ such that $c \leq p_f \cdot w_f \cdot (1-\delta_1) \cdot \phi$ and $4 \cdot \delta_1 < 1 - \phi$. We choose also an arbitrary $r$-admissible environment $\mathcal{Z}$ with input $1^{p'(\kappa)}$, where $\kappa$ the security parameter and an arbitrary adversary $\mathcal{A}$ static with fixed cost that is PPT and it has corrupted a set $T$ with $t'$ participants, where $t' \in \{1, ..., n-1\}$. Note that if the adversary controls zero participants then the proof is trivial because adversary's utility is always zero. Let $x = \sum_{m=1}^{t'} x_m$ be the total number of the queries that all the corrupted participants collectively do not ask during each round. Note that $x$ is a constant, not a random variable, as it is determined in the beginning by the static adversary. It holds $0 \leq x \leq q \cdot t'$.

We will examine two executions of the Fruitchain protocol with the same environment, but with different adversary: in the first execution $\mathcal{E}_{\mathcal{Z},H_{T'}}$ the adversary is $H_T$ and in the second execution $\mathcal{E'}_{\mathcal{Z},\mathcal{A}}$ the adversary is $\mathcal{A}$. Note that the last complete round of the executions is $r$.

Firstly we have:

$$U_T^{min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \geq q \cdot t' \cdot p_f \cdot r \cdot (1-\delta_1) \cdot w_f - c \cdot q \cdot t' \cdot r \geq q \cdot t' \cdot p_f \cdot r \cdot (1-\delta_1) \cdot w_f \cdot (1-\phi) > 0 \quad (43)$$

with overwhelming probability in $\kappa$.

The above equation is proved by Chernoff bound and taking into account that all the fruits produced by $T$ will be included in the local chain of all the honest participants at the end of the round $r$.

In addition, the adversary cannot earn rewards for more fruits than that it has produced. Moreover $c \leq p_f \cdot w_f \cdot (1-\delta_1) \cdot \phi$ . As a result by Chernoff bound

$$U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) \leq (q \cdot t' - x) \cdot p_f \cdot r \cdot (1+\delta_1) \cdot w_f - c \cdot (q \cdot t' - x) \cdot r \leq q \cdot t' \cdot p_f \cdot r \cdot (1+\delta_1) \cdot w_f - c \cdot q \cdot t' \cdot r \quad (44)$$

with overwhelming probability in $\kappa$.

As a result

$$U_T^{\max}(\mathcal{E'}_{\mathcal{Z},\mathcal{A}}) - U_T^{min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \leq (\frac{1+\delta_1}{1-\delta_1} - 1) \cdot \frac{1}{1-\phi} \cdot U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \quad (45)$$

$$\leq 4 \cdot \delta_1 \cdot \frac{1}{1-\phi} \cdot U_T^{\min}(\mathcal{E}_{\mathcal{Z},H_{T'}}) \quad (46)$$

with overwhelming probability in $\kappa$. □