Few Explanations for <Fast-to-Finalize Nakamoto-Like Consensus>

Shuyang Tang*

Cryptoape Research & Shanghai Jiao Tong University
htftsy@sjtu.edu.cn

Abstract. A novel Nakamoto-like consensus was proposed by Tang et al. (ACISP 2019) to speed up the convergence (block finality) rate by determining a weight of a block in the blockchain by a tunable potential function of the block hash. However, the convergence of the scheme was evaluated only in an experimental way and a sudden utilization of another blockchain was not clearly explained. This article asymptotically analyses the convergence of Nakamoto-like consensus of Tang et al. by proposing a general framework for formalizing consensus schemes comprising both the classical Nakamoto consensus (bitcoin consensus) and the consensus of Tang et al. The framework contains two categories of schemes, namely, small-step consensus like the bitcoin consensus and giant-step consensus of Tang et al. Furthermore, the essence of the second chain, the even-trigger, is shown to be a necessity of realizing giant-step consensus.

Keywords: Blockchains · Distributed Consensus · Proof of Work

1 Introduction

The original consensus of the bitcoin blockchain, known as *Nakamoto consensus* has been notorious for its slow rate of convergence (block finality). Namely, for the sake of security, a block suffers a long interval between being proposed and being confirmed by a significant amount of newer blocks[1]. Tang et al. explained that the slow convergence of the classical Nakamoto consensus of bitcoin is caused by the insufficient measurement of hash power in the existing proof-of-work [1]. In essence, the proof-of-work in bitcoin is measuring the hash power of a block proposer with only one bit of information. In other word, block weight is evaluated with a binary function ($0-1$ function) on the hash by whether a given hash is smaller than a target. Therefore, Tang et al. proposed a novel way of assigning a block with a weight by a tunable *potential function* on the hash and an alternative blockchain built with such functional block weights have a faster

* The only correpsonding author: Shuyang Tang (e-mail: htftsy@sjtu.edu.cn).

[1] We refer to this consensus as *bitcoin consensus* or *classical Nakamoto consensus* interchangeably in this paper. We strongly recommend readers not sufficiently familiar with the Nakamoto consensus to read our brief introduction to bitcoin consensus presented in Appendix. E.

convergence rate to attain the same level of security (see a brief description of this scheme in Sec. 2.2).

Before the construction of Tang et al., several hybrid schemes are proposed to provide instant transaction confirmations. For example, the lightning network [2] or committee-based consensus [3–7] (some of them adopt a sharding)[2]. However, these schemes are built on top of an existing blockchain rather than modifying the "layer-one" blockchain itself. That is to say, the chain of Tang et al. is not a substitution of any instant-confirmation scheme, but a plus to all of them. We believe that the work of Tang et al. has the potential of making a difference to proof-of-work in cryptocurrencies and changing the public view of blockchains if issues listed below are properly fixed. This is the purpose of this article.

Indeed, few issues are not well-explained in the paper of Tang et al. Firstly, they leveraged another existing blockchain to reach a certain synchronization without explaining why. Secondly, the relation between their scheme and bitcoin consensus is unclear. They claimed that bitcoin can be regarded as one special instantiation of their framework. However, bitcoin consensus is obviously different from their consensus with a binary potential function. Most importantly, they demonstrated the improvement on the convergence rate only in an experimental way without theoretical basis. It is not even clear what potential functions can lead to a convergence (obviously certain functions can not).

1.1 Our Contribution

Unifying [1] with The Bitcoin Consensus. This article defines a class of *trigger* functionalities and proposes a framework of *functional Nakamoto consensus* that each protocol in the framework corresponds to a trigger functionality (or "trigger"). The class of triggers is divided into two categories corresponding to two classes of consensus schemes, namely, *small-step* triggers of small-step consensus like the bitcoin consensus and *giant-step* triggers of giant-step consensus of alternative chains proposed by Tang et al.

Asymptotic Convergence Results. Based on this framework, we formalize the convergence rate by proposing two useful convergence theorems and tell that certain potential functions can never attain a secure convergence. Afterwards, we introduce two useful convergence theorems. Applications of two theorems are presented including a case where a secure convergence can never be attained and that asymptotically any polynomial can be a secure convergence gap for the bitcoin blockchain.

Explanation for The Second Chain in [1]. Finally, we explain the necessity of the weak synchronization (reached by another blockchain) in the construction of Tang et al. in case of power splitting attacks and selfish mining [10]. There is a weak synchronization from an *event-trigger* acting like a clock that clicks once for every certain time interval in our defined general framework. We explain that giant-step consensus have to explicitly realize

[2] There are also instant confirmations like *Algorand* [8] from committee-based proof-of-stake [9] consensus, but this work focuses on proof-of-work only.

such an event-trigger (hence [1] adopts an existing blockchain) but small-step consensus do not (hence bitcoin needs no event-trigger).

1.2 Related Works

[11,12] started a tend of analyzing Nakamoto chains focusing on two key properties for consistency, namely, common prefix and chain quality. However, its analysis on bitcoin consensus was based on the assumption of a fully synchronous network. [13] proved the consistency and liveness of bitcoin consensus in an asynchronous network. [14] proposed a novel chain of blocks and fruits to attain a better fairness. [15] proposed a blockchain with key-/micro- blocks for scalability. The idea of assigning blocks with a weight (and chain forks are resolved according to block weights) was also seen in the GHOST protocol [16] and a proof of space scheme known as *SpaceMint* [17]. *Delegated proof-of-space* had a similar approach of electing leaders with a "score" accumulating by time (though we found no formal proof for it). Also, a similar idea was proposed in [18] to reduce the mining variance.

1.3 Paper Organization

Sec. 2 introduces necessary notations and preliminaries. Sec. 3 describes the framework with formal definitions of the ledger structure, trigger functionalities and formalizes the protocol execution. Sec. 4 provides two theorems of secure convergence and shows applications of these theorems. Sec. 5 shows that an event-trigger is a necessity of realizing a giant-step consensus. Apart from adopting another blockchain like the construction of Tang et al., few more approaches are possible to realize such an event-trigger.

2 Notations and Preliminaries

2.1 Notations and Assumptions

For any $M \in \mathbb{N}$, $[M]$ stands for $\{1, 2, \ldots, M\}$ ($[0] = \emptyset$). $A \approx_\kappa B$ if $A/B = 1 \pm o(1/\kappa)$. For a distribution $\mathcal{D}$ (a set S), $x \leftarrow_\$ \mathcal{D}$ ($x \leftarrow_\$ S$) randomly selects a x according to the distribution $\mathcal{D}$ (uniformly from the set S). For a mapping $f : \mathcal{X} \to \mathcal{Y}$ and a subset $\mathcal{X}' \subseteq \mathcal{X}$, $f|_{\mathcal{X}'} : \mathcal{X}' \to \mathcal{Y}$ maps each element x of $\mathcal{X}'$ into $f(x)$. In this work, slightly differently from the algebraic literature, we refer to a function $f(x) = \tilde{\Theta}(x^r)$ as a *polynomial* if $r > 0$ is a positive constant. To describe the probability of happening event A conditioned on B, we adopt both the notation $\Pr[A|B]$ more familiar to statistics and notation $\Pr[B : A]$ more familiar to the cryptographic literature interchangeably (same to expectations).

As the first step of analyzing a consensus (especially a highly complicated consensus) is to consider fully synchronous network channels like [11], most of the time, we do not consider network delay issues. We assume an adversary controlling α fraction of all hash power ($\alpha < \frac{1}{2}$). Despite the fact that we consider

a permissionless environment, we may still assume N total participants with equal hash power to facilitate formalizations. In this case, αN (assume that it is an integer) of them are controlled by the adversary and we assume that the rest of them are honest, i.e., always execute according to our determined protocols. Notations utilized throughout this article are partially illustrated in Tab. 1. We formulate the hash as follows.

Definition 1 (Hash Formulation). *We consider one cryptographic hash function H with the range of a totally-ordered $\mathcal{R}$. $\mathcal{R}$ is finite but large enough with a cardinality of $|\mathcal{R}| = O(2^{2\kappa})$. The oracle $\mathcal{H}$ returns the hash (by H) of a random input for each query. We denote by $\mathcal{H}^t_{min}$ the* least-hash oracle *that outputs the least output among t queries to $\mathcal{H}$.*

A brief introduction to an abstracted Nakamoto consensus is presented in Appendix. E.

2.2 The Consensus of [1]

From the ledger structure alone, the blockchain of Tang et al. [1] is still a chain of blocks with the block structure (seemingly) same to that of bitcoin. However, each block has a weight assigned by $\widehat{\phi}(h)$ where h is the block hash and $\widehat{\phi} : \mathcal{R} \to \mathbb{R}_0^+$ is a predetermined monotonically non-increasing function from the hash range to nonnegative real numbers. Each establishment of $\widehat{\phi}$ corresponds to a different scheme.

The growth of the chain is somewhat a generalization of the bitcoin chain in two aspects. The first one is the threshold of block proposal. A block with block hash h can be proposed if $\widehat{\phi}(h) > 0$[3], while in bitcoin an explicit target is determined and h must be smaller than it. Second, in case of a chain fork, a chain branch with a total weight (i.e., the summation of all weights of blocks on the branch) greater than the other one with a certain gap of Γ wins the fork competition and remains always on the main chain (the branch of the greatest total weight) with an overwhelming probability. Such a gap is the *secure convergence gap* for $\widehat{\phi}$[4]. This is the generalization of the "six-block confirmation" principle in bitcoin.

However, the security of this scheme forces all miners to mine for a while before being able to propose a block by adopting another blockchain like the blockchain of bitcoin. In detail, it assumes an existing blockchain $\boldsymbol{A} = (A_0, A_1, \ldots)$ (each A_i is a block) with a steady chain growth rate. Each block B_i of Tang et al.'s chain has a field pointing to a block of $\boldsymbol{A}$ denoted as B_i.btcBlock (the same notation of [1]). To propose a new block B_ℓ to their constructed chain $\boldsymbol{B} = (B_0, B_1, \ldots)$, it must point to the next block of $B_{\ell-1}$.btcBlock, i.e.,

$$(B_\ell.\text{btcBlock}).\text{preBlock} = (B_\ell.\text{preBlock}).\text{btcBlock},$$

[3] The hash difficulty of this scheme can be viewed as the greatest x that $\widehat{\phi}(x) \neq 0$. Therefore, this scheme is not actually "a consensus without a target".

[4] In this paper, we "destruct" $\widehat{\phi}$ into two functions as $\widehat{\phi}(h) = \rho(h)\phi(h)$ (see details later).

where A_i.preBlock $:= A_{i-1}$ and B_i.preBlock $:= B_{i-1}$ for each $i \in \mathbb{N}^+$. Clearly, the other blockchain is acting as an *event-trigger* which can be regarded as a clock that clicks for each block generation. Tang et al. gave no explanation for adopting this event-trigger. To fix the gap, we have provided an explanation in Sec. 5.

3 The Framework

3.1 Ledger Structure

We provide an abstraction of the ledger structure of blockchains. In the classical Nakamoto blockchain, the ledger is considered as a "thin" tree of blocks, the *main chain* of the ledger is the longest valid path from the root (the genesis block) to the deepest block of the tree. Only transactions of main chain blocks are effective. In our model, such a measurement of block depth is replaced by a *branch weight*.

Definition 2 (The Ledger Structure). *The ledger T is in the form of a tree, denoted as $T = (\boldsymbol{B}, \mathsf{h}, \mathsf{pre}, \mathsf{w})$, where $\boldsymbol{B}$ is the set of all blocks, $\mathsf{h} : \boldsymbol{B} \to \mathbb{N}$ maps each block to its height (the number of blocks from the genesis to it) and $\mathsf{pre} : \boldsymbol{B} \to \boldsymbol{B}$ maps each block to a previous block such that*

- *there exists only one genesis block $B_{gen} \in \boldsymbol{B}$ that $\mathsf{h}(B) = 0$*
- *and $\mathsf{pre}(B_{gen}) = B_{gen}$,*
- *and that for each $B \in \boldsymbol{B}$ that $B \neq B_{gen}$, $\mathsf{h}(\mathsf{pre}(B)) = \mathsf{h}(B) - 1$.*

$\mathsf{w} : \boldsymbol{B} \to \mathbb{R}^+$ maps each block to a weight.

It is easy to verify that any structure satisfying the properties above is in the form of a tree rooted at B_{gen}. We denote the genesis block of a ledger T as $\mathsf{genesis}(T)$. In later descriptions, we refer to the block set of ledger T as $T.\boldsymbol{B}$ (same to h, pre and w). A detailed list of confirmed transactions and certain metadata (known as the *block body*) within each block is not crucial to our results and are not considered to be part of our abstracted block.

Definition 3 (Chain Branch). *In a ledger $T = (\boldsymbol{B}, \mathsf{h}, \mathsf{pre}, \mathsf{w})$, The chain branch to a block $B \in \boldsymbol{B}$ is the sequence of blocks*

$$\mathsf{branch}(B) := (B_0 = \mathsf{genesis}(T), B_1, \ldots, B_\ell = B)$$

such that $\mathsf{pre}(B_i) = B_{i-1}$ for each $i \in [\ell]$. The weight of the chain branch $\mathsf{branch}(B)$ is

$$\mathsf{weight}(\mathsf{branch}(B)) := \sum_{i=0}^{\ell} \mathsf{w}(B_i).$$

The main chain $\mathsf{MC}(T) := \mathsf{branch}(B^*)$ of T is the chain branch to a $B^* \in \boldsymbol{B}$ with the greatest branch weight.

We introduce a few notations to facilitate later descriptions. To a tree ldger $T = (\boldsymbol{B}, \mathsf{h}, \mathsf{pre}, \mathsf{w})$ and $B, B' \in \boldsymbol{B}$, $T.\mathsf{reach}(B, B')$ is true iff there is a sequence of blocks $B_0, B_1, \ldots, B_\ell$ such that $\mathsf{pre}(B_0) = B$, $\mathsf{pre}(B') = B_\ell$ and $\mathsf{pre}(B_i) = B_{i-1}$ for each $i \in [\ell]$. For a tree ledger T and any block $\widehat{B} \in T.\boldsymbol{B}$, we denote by $T|_{\widehat{B}} = (\widehat{\boldsymbol{B}}, \widehat{\mathsf{h}}, \widehat{\mathsf{pre}}, \widehat{\mathsf{w}})$ the ledger segment with

$$\widehat{\boldsymbol{B}} := \{B \in T.\boldsymbol{B} : T.\mathsf{reach}(\widehat{B}, V)\}$$

$\widehat{\mathsf{h}} := \mathsf{h}\big|_{\widehat{\boldsymbol{B}}}$, $\widehat{\mathsf{pre}} := \mathsf{pre}\big|_{\widehat{\boldsymbol{B}}}$, and $\widehat{\mathsf{w}} := \mathsf{w}\big|_{\widehat{\boldsymbol{B}}}$.

3.2 The Trigger Functionality

A trigger functionality (or *trigger* for simplicity) $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$ is parameterized by a tuple (Ω, ϕ, ρ) where each element of the tuple is possibly parameterized by κ. Although we aim at a permissionless environment where consensus participants are not predetermined and that dynamic joining and quitting are allowed, we still assume N participants $P_1, P_2, \ldots, P_N$ with equal hash power to facilitate descriptions. Assuming that αN is an integer, $P_1, P_2, \ldots, P_{\alpha N}$ are controlled by the adversary $\mathcal{A}$ ($\alpha < 1/2$).

Initial Phase. The global ledger T_0 is initially set as empty $T_0 := (\emptyset, \lambda B.\_, \lambda B.\_, \lambda B.\_)$. $\mathsf{withhold}_0 := \emptyset$. Afterwards, the execution phase is iterated.

Execution Phase. The execution proceeds by *rounds*. The functionality has a confidential set of tip blocks $\mathsf{withhold}_R \in \mathcal{P}(T_R.\boldsymbol{B})$ for each round. In later descriptions, for each ledger T_R, we denote by $\widetilde{T_R}$ the ledger without blocks of $\mathsf{withhold}_R$, i.e.,

$$\widetilde{T_R} := \left(\boldsymbol{B}' := T_R.\boldsymbol{B} \setminus \mathsf{withhold}_R,\ \ T_R.\mathsf{h}\Big|_{\boldsymbol{B}'},\ T_R.\mathsf{pre}\Big|_{\boldsymbol{B}'},\ T_R.\mathsf{w}\Big|_{\boldsymbol{B}'}\right).$$

For each round $R \in \mathbb{N}^+$, $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$ sequentially acts as follows.

1. It lets $T_R := T_{R-1}$ and $\mathsf{withhold}_R := \mathsf{withhold}_{R-1}$,
2. Sends to all participants $P_1, P_2, \ldots, P_N$ the tuple $(\texttt{START}, R, \widetilde{T_{R-1}})$, sends to $\mathcal{A}$ the tuple $(\texttt{START}, R, T_{R-1})$,
3. Receives from $P_{\alpha N+1}, R, P_{\alpha N+2}, \ldots, P_N$ tuples in the form of $(\texttt{MINE}, R, P_i, B_i^{\mathrm{pre}})$ (reject if $B_i^{\mathrm{pre}} \notin \widetilde{T_{R-1}}.\boldsymbol{B}$). For each P_i of them,
   - Gets the minimal hash among $\frac{\Omega}{N}$ hash attempts $h_i \leftarrow_{\$} \mathcal{H}_{\min}^{\Omega/N}$,
   - If $\rho(h_i) = 1$, builds the block for P_i as B_i^R with block hash h_i, includes B_i^R into $T_R.\boldsymbol{B} \leftarrow T_R.\boldsymbol{B} \cup \{B_i^R\}$ and updates T_R such that

   $$T_R.\mathsf{pre}(B_i^R) = B_i^{\mathrm{pre}} \bigwedge T_R.\mathsf{h}(B_i^R) = T_R.\mathsf{h}(B_i^{\mathrm{pre}}) + 1 \bigwedge T_R.\mathsf{w}(B_i^R) = \phi(h_i),$$

4. Let $U := \alpha\Omega$, interact with $\mathcal{A}$ till $U = 0$, each time receive from $\mathcal{A}$ a tuple $(\texttt{AD\_MINE}, R, B^{\mathrm{pre}}, t, \mathsf{th})$, if $t \in \mathbb{N}^+$ and $t \leq U$,

- Reject if $B^{\text{pre}} \notin T_R.\boldsymbol{B}$ or $T_R.\mathsf{h}(B^{\text{pre}}) = R$[5],
- Let $U \leftarrow U - t$, get $h \leftarrow \mathcal{H}^t_{\min}$,
- If $\rho(\mathsf{nc}) = 1$, builds the block B by including B into $T_R.\boldsymbol{B} \leftarrow T_R.\boldsymbol{B} \cup \{B\}$ and updating T_R such that

$$T_R.\mathsf{pre}(B) = B^{\text{pre}} \bigwedge T_R.\mathsf{h}(B) = T_R.\mathsf{h}(B^{\text{pre}}) + 1 \bigwedge T_R.\mathsf{w}(B) = \phi(h),$$

  let $\mathsf{withhold}_i := \mathsf{withhold}_i \cup \{B\}$ if $\mathsf{th} = 1$,

5. Issues the tree to all participants and finishes the round by sending tuples $(\texttt{END}, R, \widetilde{T_R})$ to each P_i and $(\texttt{END}, R, T_R)$ to $\mathcal{A}$.

It is easy to observe that $\max_{B \in T_R.\boldsymbol{B}} T_R.\mathsf{h}(B) \leq R$ holds always for any adversary and participants. Such a property is crucial to the prevention of power splitting attacks to functionalities with $\mathsf{ord}(\rho) = 0$ (see definitions later). Also, this tells that the realization of such a trigger functionality is far from trivial. We will introduce a way of realizing the functionality in Sec. 5.

3.3 Execution Model

As aforementioned, in this article, we consider a static-corruption, i.e., $P_1, P_2, \ldots, P_N$ are corrupted by the environment $\mathcal{Z}(1^\kappa)$. $\mathcal{Z}$ directs the trigger functionality $\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}$ [6]. Due to the complication of our model, we have put certain trivial details (like the interaction with the public-key infrastructure, detailed protocol of receiving and organizing transactions) out of consideration by leveraging the trigger functionality which has already comprised the hybrid of a public-key infrastructure $\mathcal{F}_{\mathsf{PKI}}$, random oracles, and the tree functionality $\mathcal{F}_{\mathsf{tree}}$ of related works. $\mathcal{Z}$ also simulates the global view of the execution outside the scope of any participant. In our defined execution model, honest participants $P_{\alpha N+1}, P_{\alpha N+2}, \ldots, P_N$ always mine blocks after the chain branch with the greatest total weight (in its view) and will only mine on one block for a greater weight for each round via $(\texttt{MINE}, R, P_i, B_i^{\text{pre}})$. However, the adversary $\mathcal{A}$ is allowed to mine on more than one blocks, but not allowed to mine too long a chain of blocks due to the restriction of the trigger functionality(since the functionality has guaranteed that $\max_{B \in T_R.\boldsymbol{B}} T_R.\mathsf{h}(B) \leq R$).

Obviously, although the execution is randomized, the strategy of non-adversary participants is deterministic. Therefore, the difference in execution traces comes from only two sources: the randomness and the strategy of $\mathcal{A}$. Thereby, the protocol execution is parameterized by only the trigger functionality $\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}$ and the

[5] Such a restriction on the maximal height of the tree ledger is the goal of event-triggers. Without this, gaint-step consensus schemes are vulnerable facing power splitting attacks as shown in Sec. 5.

[6] To exclude possible misunderstandings, please kindly note that although we have adopted some universal composition(UC)-liked notations to formalize the protocol execution, due to the high complication of our problem, our proofs are not done under the UC model.

adversary. The *view* of any moment during the protocol execution, which comprises all states and memory of all participants and the global ledger, is thereby notated as $\mathsf{view} \leftarrow_{\$} \mathrm{EXEC}^{\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}}_{\mathcal{A},\mathcal{Z}}(1^{\kappa})$. Since the protocol is randomized, the view is defined as a random view trace by a random moment within a polynomial amount of protocol execution steps (this slightly differs from related works). To facilitate later proofs, we use $\mathsf{view}^* \leftarrow_{\$} \mathrm{EXEC}^{\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}}_{\mathcal{A},\mathcal{Z}}(1^{\kappa}, \mathsf{view})$ to notate a random view trace by a random moment within a polynomial number of protocol execution steps starting from view. We denote the tree ledger of view as $\mathsf{tree}(\mathsf{view})$.

4 Convergence Results

We also have a definition for *sound trigger functionality* as follows.

Definition 4 (Sound Trigger Functionality). *The trigger functionality $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$ is sound if and only if satisfying the following conditions.*

Admissible Tuples.

$$\phi \in [\![\mathcal{R} \to \mathbb{R}^+]\!] \bigwedge \rho \in [\![\mathcal{R} \to \{0,1\}]\!]$$

Both $\phi(x)$ and $\rho(x)$ are monotonically non-increasing in x. We denote $\widehat{\phi}(x) := \phi(x)\rho(x)$ in later contents to facilitate descriptions.

Finitely-Ordered Functionality. *There exists a smallest nonnegative number d and constant c such that*

$$\Pr[x \leftarrow_{\$} \mathcal{H}_{min}^{c\Omega\cdot\kappa^d} : \rho(x) = 1] > \frac{1}{2}.$$

Such a smallest d is called the order *of the functionality, denoted as $\mathsf{ord}(\rho)$. In later descriptions, we denote $\widehat{\Omega} := \Omega \cdot \kappa^d$ for simplicity. Moreover, we partite the space of all sound trigger functionalities into two classes. The class $\mathscr{F}_s$ comprises* small-step *triggers with $\mathsf{ord}(\rho) > 0$ for any $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho} \in \mathscr{F}_g$. $\mathscr{F}_g$ consists of* giant-step *triggers with $\mathsf{ord}(\rho) = 0$ for any $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho} \in \mathscr{F}_g$.*

Sound Evaluation. *We denote*

$$\Phi^{\beta}_{\Omega,\phi,\rho} := E\left[\phi(x)\rho(x) \middle| x \leftarrow_{\$} \mathcal{H}_{min}^{\beta\widehat{\Omega}}\right].$$

There exists a constant $0 < \chi < 1 - 2\alpha$ such that for any constant $0 < \beta < 1$,

$$(1-\chi)\beta \le \frac{\Phi^{\beta}_{\Omega,\phi,\rho}}{\Phi^{1}_{\Omega,\phi,\rho}} \le (1+\chi)\beta$$

holds.

Bounded Maximum Weight. $\max_{x\in\mathcal{R}} \phi(x) \le \mathsf{ext}(\kappa)\Phi^1_{\Omega,\phi,\rho}$ *for a certain sub-polynomial $\mathsf{ext}(\cdot)$.*

$\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-models corresponding to sound trigger functionalities are *sound models*.

We at first formally define a secure convergence.

Definition 5 (Secure Convergence Gap). *Γ (a function in κ) is a secure convergence gap in the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-model, if for any $\mathcal{A}$ in the execution model, any view trace $\mathsf{view} \leftarrow_{\$} EXEC_{\mathcal{A},\mathcal{Z}}^{\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}}(1^{\kappa})$ and any block B, B' of $\mathsf{MC}(\mathsf{tree}(\mathsf{view}))$ and $\widetilde{B'} \in \mathsf{tree}(\mathsf{view}).\boldsymbol{B}$ that $\mathsf{pre}(B') = \mathsf{pre}(\widetilde{B'}) = B$, if $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$ is a sound trigger functionality and*

$$\mathsf{weight}\left(\mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}\right)\Big|_{B'}\right)\right) - \mathsf{weight}\left(\mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}\right)\Big|_{\widetilde{B'}}\right)\right) \geq \Gamma,$$

then

$$\Pr\left[\widetilde{B'} \in \mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}^{*}\right)\right) \Big| \mathsf{view}^{*} \leftarrow_{\$} EXEC_{\mathcal{A},\mathcal{Z}}^{\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}}(1^{\kappa}, \mathsf{view})\right] = \mathsf{negl}(\kappa),$$

where $\mathsf{negl}(\cdot)$ is a negligible function.

We denote the *least convergence gap* in the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-model as $\Gamma^{\Omega,\phi,\rho}$. Note that $\Gamma(\kappa)$ is a function of κ, though we always abbreviate it into Γ to avoid redundancy.

Definition 6 (Finality Time). *The finality time of the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-model is $\mathsf{ctime}(\Omega,\phi,\rho) := \Omega \times \Lambda^{\Omega,\phi,\rho}$ where*

$$\Lambda^{\Omega,\phi,\rho} := E_{h_1,h_2,\ldots \leftarrow_{\$} \mathcal{H}_{min}^{\Omega}}\left[\min_{r\in\mathbb{N}}\left\{\sum_{i=1}^{r}\phi(h_i) \geq \Gamma^{\Omega,\phi,\rho}\right\}\right].$$

4.1 The Convergence Theorem

Definition 7 (Practical Secure Convergence Gap). *A secure convergence gap Γ in the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-model is* practical *iff*

$$\Gamma \leq p(\kappa) \cdot k^{\mathsf{ord}(\rho)} \Phi_{\Omega,\phi,\rho}^{1}$$

is satisfied with a certain polynomial $p(\cdot)$.

Theorem 1 (The Sufficiency Theorem). *If $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$ is a sound trigger functionality, in the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-model, if there exists an $\epsilon > 0$ such that,*

$$\Pr\left[\phi(x) > \frac{\Gamma}{\kappa^{\epsilon}} \Big| x \leftarrow_{\$} \mathcal{H}_{min}^{\alpha\widehat{\Omega}}\right]$$

is negligible in κ, then Γ is a secure convergence gap in the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-model.

Proof. We consider a view trace $\mathsf{view} \leftarrow_{\$} \mathrm{EXEC}^{\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}}_{\mathcal{A},\mathcal{Z}}(1^\kappa)$, $B, B' \in \mathsf{MC}(\mathsf{tree}(\mathsf{view}))$ and $B', \widetilde{B'} \in \mathsf{tree}(\mathsf{view}).\boldsymbol{B}$ that $\mathsf{pre}(B') = \mathsf{pre}(\widetilde{B'}) = B$, such that

$$\mathsf{weight}\left(\mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}\right)\Big|_{B'}\right)\right) - \mathsf{weight}\left(\mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}\right)\Big|_{\widetilde{B'}}\right)\right) \geq \Gamma.$$

We show that

$$\Pr\left[\widetilde{B'} \in \mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}^*\right)\right) \middle| \mathsf{view}^* \leftarrow_{\$} \mathrm{EXEC}^{\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}}_{\mathcal{A},\mathcal{Z}}(1^\kappa, \mathsf{view})\right] \tag{1}$$

is negligible for an adversary in the execution model and a polynomial $\psi(\kappa)$. For a view view^*, we denote by $\widehat{\mathsf{view}^*}$ the first view (executing from view to view^*) that the branch after $\widetilde{B'}$ becomes the main chain (i.e. having a greater branch weight than the branch after B'). To reach a branch weight greater than the current main chain by Γ after $\widetilde{B'}$, the worse adversary always mine on the branch after $\widetilde{B'}$. At the same time, honest nodes mine after the main chain, which is the branch after B' until $\widehat{\mathsf{view}^*}$. Denoting $r(\kappa) := \Pr\left[\phi(x) > \frac{\Gamma}{\kappa^\epsilon} \middle| x \leftarrow_{\$} \mathcal{H}^{\alpha\widehat{\Omega}}_{\min}\right]$, at least one of κ^ϵ attempts from $\mathcal{H}^{\alpha\widehat{\Omega}}_{\min}$ ($d = \mathsf{ord}(\rho)$, $\widehat{\Omega} = k^d \cdot \Omega$) should have a weight over $\frac{\Gamma}{\kappa^\epsilon}$. Therefore,,

$$\Pr\left[\widetilde{B'} \in \mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}^*\right)\right) \middle| \begin{array}{c}\mathsf{view}^* \leftarrow_{\$} \mathrm{EXEC}^{\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}}_{\mathcal{A},\mathcal{Z}}(1^\kappa, \mathsf{view}) \\ \left|\widehat{\mathsf{view}^*}\right| - |\mathsf{view}| \leq \kappa^{d+\epsilon}\end{array}\right] \leq r(\kappa) \cdot \kappa^\epsilon$$

which is also negligible in κ (d is the order of Ω, ϕ, ρ). Now we consider the case that $\left|\widehat{\mathsf{view}^*}\right| - |\mathsf{view}| > \kappa^{d+\epsilon}$,

$$\begin{aligned}
&\Pr\left[\widetilde{B'} \in \mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}^*\right)\right) \middle| \begin{array}{c}\mathsf{view}^* \leftarrow_{\$} \mathrm{EXEC}^{\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}}_{\mathcal{A},\mathcal{Z}}(1^\kappa, \mathsf{view}) \\ \left|\widehat{\mathsf{view}^*}\right| - |\mathsf{view}| > \kappa^{d+\epsilon}\end{array}\right] \\
\leq &\mathsf{poly}(\kappa) \cdot \Pr\left[\sum_{i=1}^{\kappa^\epsilon} \left(\phi\left(x_i\right) - \phi\left(y_i\right)\right) \geq \Gamma \middle| \begin{array}{l}x_1, x_2, \ldots \leftarrow \mathcal{H}^{\alpha t\widehat{\Omega}}_{\min} \\ y_1, y_2, \ldots \leftarrow \mathcal{H}^{(1-\alpha)t\widehat{\Omega}}_{\min}\end{array}\right] &(2)\\
\leq &\mathsf{poly}(\kappa) \cdot \Pr\left[\sum_{i=1}^{\kappa^\epsilon} \xi_i > 0 \middle| \xi_1, \xi_2, \ldots \leftarrow_{\$} \mathcal{D}\right] &(3)
\end{aligned}$$

where $\mathcal{D}$ is a certain distribution randomly selecting a $x \leftarrow_{\$} \mathcal{H}^{\alpha\widehat{\Omega}}_{\min}$, a $y \leftarrow_{\$} \mathcal{H}^{(1-\alpha)\widehat{\Omega}}_{\min}$ and outputting $\widehat{\phi}(x) - \widehat{\phi}(y)$ for each sampling. We denote the expectation of $\mathcal{D}$ as $-\mathrm{E}_{\mathcal{D}}$ and the variance as $\mathrm{V}_{\mathcal{D}}$. Asymptotically, the distribution of $\left(\sum_{i=1}^{\kappa^\epsilon} \xi_i\right)$ converges to the Gaussian distribution according to the central limit theorem as κ grows. Such a gaussian distribution has the expectation of $-\kappa^\epsilon \mathrm{E}_{\mathcal{D}}$

and the variance of $\kappa^{\epsilon}\mathrm{V}_{\mathcal{D}}$. Thereby,

$$\Pr\left[\sum_{i=1}^{\kappa^{\epsilon}}\xi_i > 0 \middle| \xi_i \leftarrow_{\$} \mathcal{D}\right] < (1+\tau)\int_{s=0}^{+\infty}\frac{1}{\sqrt{2\pi\kappa^{\epsilon}\mathrm{V}_{\mathcal{D}}}}\exp\left(-\frac{(s+\kappa^{\epsilon}\mathrm{E}_{\mathcal{D}})^2}{2\kappa^{\epsilon}\mathrm{V}_{\mathcal{D}}}\right)\mathrm{d}s \tag{4}$$

for a small τ. We deform (4) into

$$\begin{aligned}&(1+\tau)\sum_{L=1}^{+\infty}\int_{s=\kappa^{\epsilon}\mathrm{E}_{\mathcal{D}}(L-1)}^{\kappa^{\epsilon}\mathrm{E}_{\mathcal{D}}L}\frac{1}{\sqrt{2\pi\kappa^{\epsilon}\mathrm{V}_{\mathcal{D}}}}\exp\left(-\frac{(s+\kappa^{\epsilon}\mathrm{E}_{\mathcal{D}})^2}{2\kappa^{\epsilon}\mathrm{V}_{\mathcal{D}}}\right)\mathrm{d}s\\ \leq&(1+\tau)\sum_{L=1}^{+\infty}\frac{\kappa^{\epsilon}\mathrm{E}_{\mathcal{D}}(L-1)}{\sqrt{2\pi\kappa^{\epsilon}\mathrm{V}_{\mathcal{D}}}}\exp\left(-\frac{(L\cdot\kappa^{\epsilon}\mathrm{E}_{\mathcal{D}})^2}{2\kappa^{\epsilon}\mathrm{V}_{\mathcal{D}}}\right).\end{aligned} \tag{5}$$

To show that the result of (5) is negligible in κ, it suffices to prove that $\frac{V_{\mathcal{D}}}{E_{\mathcal{D}}^2}$ is not greater than any polynomial of κ. From the definition of a sound trigger functionality, $\xi_{max} := \max_{x\in\mathcal{R}}\phi(x) \leq \mathsf{ext}(\kappa)\Phi^{1}_{\Omega,\phi,\rho}$ for a sub-polynomial $\mathsf{ext}(\cdot)$. Thereby,

$$\begin{aligned}\frac{V_{\mathcal{D}}}{E_{\mathcal{D}}^2} &\leq \frac{\xi_{max}E_{\mathcal{D}}-E_{\mathcal{D}}^2}{E_{\mathcal{D}}^2} = \frac{\xi_{max}}{\Phi^{1-\alpha}_{\Omega,\phi,\rho}-\Phi^{\alpha}_{\Omega,\phi,\rho}}-1\\ &\leq \frac{\xi_{max}}{(1-\chi)(1-\alpha)\Phi^{1}_{\Omega,\phi,\rho}-(1+\chi)\alpha\Phi^{1}_{\Omega,\phi,\rho}}-1\\ &\leq \frac{\mathsf{ext}(\kappa)}{(1-\chi)(1-\alpha)-(1+\chi)\alpha}-1\end{aligned}$$

which is sub-polynomial.

Theorem 2 (The Necessity Theorem). *If Γ is a secure convergence gap in the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-model, then for any function $\varphi(\kappa)$ that $\varphi(\kappa)=O(1)$,*

$$\Pr\left[\phi(x)-\phi(y) > \frac{\Gamma}{\varphi(\kappa)}\middle|\begin{matrix}x\leftarrow_{\$}\mathcal{H}_{min}^{\alpha\widehat{\Omega}}\\ y\leftarrow_{\$}\mathcal{H}_{min}^{(1-\alpha)\widehat{\Omega}}\end{matrix}\right]$$

is negligible in κ.

Proof. Suppose that there exists a positive γ such that

$$\Pr\left[\phi(x)-\phi(y) > \frac{\Gamma}{\varphi(\kappa)}\middle|\begin{matrix}x\leftarrow_{\$}\mathcal{H}_{\min}^{\alpha\widehat{\Omega}}\\ y\leftarrow_{\$}\mathcal{H}_{\min}^{(1-\alpha)\widehat{\Omega}}\end{matrix}\right] > \kappa^{-\gamma},$$

we show that Γ is not a secure convergence gap in the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$-model. Consider a view trace $\mathsf{view}\leftarrow_{\$}\mathrm{EXEC}^{\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}}_{\mathcal{A},\mathcal{Z}}(1^{\kappa})$ with $T=(\boldsymbol{B},\mathsf{h},\mathsf{pre},\mathsf{w})=\mathsf{tree}(\mathsf{view})$ that

1. $\boldsymbol{B}=\{B_0,B_1,\ldots,B_{\ell},\widetilde{B}\}$,

2. $\mathsf{pre}(B_i) = B_{i-1}$ for each $i \in [\ell]$, and $\mathsf{pre}(\widetilde{B}) = B_0$,
3. $\sum_{i=1}^{\ell} \mathsf{w}(B_i) - \mathsf{w}(\widetilde{B}) = \Gamma$.

It is easy to verify that

$$\mathsf{weight}\left(\mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}\right)\Big|_{B_1}\right)\right) - \mathsf{weight}\left(\mathsf{MC}\left(\mathsf{tree}\left(\mathsf{view}\right)\Big|_{\widetilde{B}}\right)\right) = \Gamma.$$

However, an adversary $\mathcal{A}$ that continuously mines after $\widetilde{B}$ has the change of reaching a branch with a greater weight after $\widetilde{B}$ in $\kappa^{\mathsf{ord}(\rho)}\varphi(\kappa)$ rounds by at least

$$(\kappa^{-\gamma})^{\varphi(\kappa)}$$

which is asymptotically the inverse of a polynomial of κ. This contradicts the negligible probability of having the branch after $\widetilde{B}$ enter the main chain.

4.2 Applications of Convergence Results

Lemma 1. *If $\widehat{\phi} : \mathcal{R} \to \mathbb{R}_0^+$ is a monotonically non-increasing function, We define $\widehat{\phi}^{-1}(y)$ as the maximal $x \in \mathcal{R} \cup \{0\}$ that $\widehat{\phi}(x) \geq y$ for any $y \in \mathbb{R}_0^+$ (let $\widehat{\phi}(0) := +\infty$). If*

$$\widehat{\phi}^{-1}(Z) = \mathit{negl}(\kappa) \cdot |\mathcal{R}|$$

for a negligible function $\mathit{negl}(\kappa)$, then $\Pr\left[\widehat{\phi}(x) \geq Z \middle| x \leftarrow_{\$} \mathcal{H}_{min}^{\alpha\Omega}\right]$ is negligible in κ.

Proof. Since $x \leq \widehat{\phi}^{-1}(Z)$ implies $\widehat{\phi}(x) \geq Z$, we need only to have

$$\begin{aligned}\Pr\left[x \leq \widehat{\phi}^{-1}(Z) \middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{\alpha\Omega}\right] &= 1 - (1 - \frac{\widehat{\phi}^{-1}(Z)}{|\mathcal{R}|})^{\alpha\Omega} \\ &< (1+\varepsilon)(1 - e^{-\frac{\alpha\Omega}{|\mathcal{R}|}\widehat{\phi}^{-1}(Z)})\end{aligned}$$

negligible for a constant ε, which by Lemma. 5 (in the appendix) asks only that $\frac{\alpha\Omega}{|\mathcal{R}|}\widehat{\phi}^{-1}(Z)$ is a negligible function in κ. This is satisfied if $\widehat{\phi}^{-1}(Z) = \mathsf{negl}(\kappa) \cdot |\mathcal{R}|$ for a negligible function $\mathsf{negl}(\kappa)$.

Theorem 3. *Any sound $\mathcal{F}_{\mathit{trigger}}^{\Omega,\phi,\rho}$-model with a polynomial $1 \leq \Phi_{\Omega,\phi,\rho}^{1} = \varphi(\kappa)$ and $\max_{x\in\mathcal{R}} \widehat{\phi}(x) = u(\kappa)$ for polynomials $\varphi(\kappa), u(\kappa)$ has a practical secure convergence gap.*

Proof. By both Thm. 1 and Lemma. 1, we only need to show that there exists a Γ polynomial in κ, a certain $\epsilon > 0$ and a negligible function $\mathsf{negl}(\cdot)$ such that

$$\widehat{\phi}^{-1}(\frac{\Gamma}{\kappa^{\epsilon}} + 1) = \mathsf{negl}(\kappa) \cdot |\mathcal{R}|$$

and

$$\Gamma \leq \kappa^{\mathsf{ord}(\rho)} \cdot u(\kappa) \cdot \Phi^1_{\Omega,\phi,\rho}$$

Suppose that $\varphi(\kappa) = \tilde{\Theta}(\kappa^c)$, let $\epsilon = \mathsf{ord}(\rho)+c$, $\Gamma = \kappa^\epsilon \cdot u(\kappa)$, Obviously, $\widehat{\phi}^{-1}(\frac{\Gamma}{\kappa^\epsilon}+1) = 0$ and 0 is a negligible function.

One intuitional implementation of the consensus of Tang et al. is to set $\phi(x) := \frac{M}{x}$ with a $M = \Theta(|\mathcal{R}|)$. Indeed, the consensus with this ϕ function has no practical convergence gap.

Theorem 4. *The $\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}$-model with $(\Omega,\phi,\rho) = \left(T(\kappa), \lambda x.\frac{M}{x}, \lambda x.1\right)$ has no practical convergence gap for any $T(\kappa) = \tilde{\Theta}(\kappa)$ and $M = \Theta(|\mathcal{R}|)$.*

Proof. By Thm. 2, it suffices to show that any Γ, either it is not a practical gap or

$$\Pr\left[\phi(x) - \phi(y) > \frac{\Gamma}{\varphi(\kappa)} \middle| \begin{matrix} x \leftarrow_\$ \mathcal{H}^{\alpha\Omega}_{\min} \\ y \leftarrow_\$ \mathcal{H}^{(1-\alpha)\Omega}_{\min} \end{matrix}\right] = \Pr\left[\frac{xy}{y-x} < \frac{\varphi(\kappa)M}{\Gamma} \middle| \begin{matrix} x \leftarrow_\$ \mathcal{H}^{\alpha\Omega}_{\min} \\ y \leftarrow_\$ \mathcal{H}^{(1-\alpha)\Omega}_{\min} \end{matrix}\right] \tag{6}$$

is not negligible in κ to a certain $\varphi(\kappa)$=O(1). In fact, (6) is no smaller than

$$\Pr\left[x < x_0 \middle| x \leftarrow_\$ \mathcal{H}^{\alpha t\Omega}_{\min}\right] \cdot \Pr\left[y \geq y_0 \middle| y \leftarrow_\$ \mathcal{H}^{(1-\alpha)t\Omega}_{\min}\right] \tag{7}$$

where $x_0 = \frac{M}{\Omega+\frac{\Gamma}{\varphi(\kappa)}}$ and $y_0 = \frac{M}{\Omega}$ since $x < x_0$ and $y \geq y_0 > x_0$ implies that $\frac{xy}{y-x} < x_0 \cdot \frac{y}{y-x_0} \leq x_0 \cdot \frac{y_0}{y_0-x_0} = \frac{\varphi(\kappa)M}{\Gamma}$. Similarly to the proof for Lemma. 1, (7) is greater than a positive constant times

$$\left(1 - \exp\left(-\frac{\alpha\Omega}{|\mathcal{R}|}\frac{M}{\Omega+\Gamma}\right)\right)\exp\left(-\frac{\alpha M}{|\mathcal{R}|}\right),$$

which is asymptotically no smaller than the inverse of a polynomial if $M = O(|\mathcal{R}|)$ and Γ is polynomial in κ. Next, we show that if Γ is greater than any polynomial, then it is not a practical convergence gap. To this end, we only need to show that $\Phi^1_{\Omega,\phi,\rho}$ is polynomial. Actually,

$$\Phi^1_{\Omega,\phi,\rho} = \mathrm{E}\left[\frac{M}{x}\middle| x \leftarrow_\$ \mathcal{H}^{\Omega}_{\min}\right] = \frac{M}{|\mathcal{R}|}\Omega \ln\frac{|\mathcal{R}|}{\Omega} + O\left(\left(\frac{\Omega}{|\mathcal{R}|}\right)^2\right) = \tilde{O}(\kappa^2)$$

according to the derivations of the same formula in Sec. D.

Moreover, according to our convergence theorem, any polynomial is asymptotically a secure convergence gap for the bitcoin blockchain.

Theorem 5 (Convergence of the Bitcoin Case). *Any $\Gamma = \kappa^\varepsilon$ with a constant $\varepsilon > 0$ is a secure convergence gap of the $\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}$-model with*

$$(\Omega,\phi,\rho) = \left(c, \quad \lambda x.1, \quad \lambda x.\begin{cases} 1, x < \frac{|\mathcal{R}|}{\varphi(\kappa)} \\ 0, o.w. \end{cases}\right),$$

where c is a constant and $\varphi(\kappa) = \Theta(\kappa)$.

Proof. As $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$ is a sound trigger functionality (proved in Lemma. 9) and

$$\Pr\left[\widehat{\phi}(x) > \frac{\kappa^{\epsilon}}{\kappa^{\epsilon/2}} \middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{\alpha\Omega}\right] = 0$$

for $\kappa > 1$. From Thm. 1, $\Gamma = \kappa^{\epsilon}$ is a secure convergence gap.

5 Realizing Triggers in $\mathscr{F}_g$

5.1 The Necessity of Event-Trigger

In this part, we explain in principle that we have to adopt an "event-trigger" to securely realize any giant-step functionalities in $\mathscr{F}_g$. This explains why [1] has to adopt another blockchain to attain a weak synchronization and also why realizing functionalities in $\mathscr{F}_s$ (including the bitcoin case) needs no event-trigger. This is shown from the lemma.

Lemma 2. *We assume a sound trigger functionality $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$. Let $C \in \mathbb{N}^+$ be a natural number sub-polynomial in κ, let $w := \beta\Omega$ for a $0 < \beta < 1$,*

$$M_1(C) := \mathrm{E}\left[\widehat{\phi}(z) \middle| z \leftarrow_{\$} \mathcal{H}_{min}^{Cw}\right],$$

$$M_2(C) := C \cdot \mathrm{E}\left[\widehat{\phi}(x) \middle| x \leftarrow_{\$} \mathcal{H}_{min}^{w}\right].$$

Generally, $M_1(C) \leq M_2(C)$. Specifically, if $\mathsf{ord}(\rho) \neq 0$, then $M_1(C) \approx_{\kappa} M_2(C)$, else $\frac{M_2(C)}{M_1(C)} > 1 + r$ for a substantial constant r.

The proof is shown in the appendix. D. From the lemma, we can see that giant-step consensus faces severe power-splitting attacks if the length of adversary branches is not restricted by an explicit event-trigger. However, such an issue is negligible to small-step consensus. That's why such an event-trigger is never seen in the classical Nakamoto consensus.

5.2 Methods of Realizing An Event-Trigger

We have shown that event triggers are necessary to realize any giant-step model of our framework. There are a few ways of constructing such event triggers.

Leveraging An Existing Blockchain. One way is to adopt the construction of Tang et al. by introducing an existing blockchain like the bitcoin blockchain. Each growth of the bitcoin main chain corresponds to one round of the trigger functionality. This is a fine way of realizing the trigger if we are allowed to regard that bitcoin blockchain grows at a steady rate and the interval between two block generations is regarded as a constant. However, the interval varies greatly between the generation of different adjacent blocks and hence not well corresponds to an Ω global hash assumption of the ideal framework. Therefore, this is not the best way.

A Global Clock. The best way is to leverage a trusted global clock. However, such a global clock is never tolerated in the distributed consensus literature since it does not comply with the decentralization principle. However, this can be considered when implemented in the layer-one of consortium chain schemes.

Proofs of Sequential Work. Proofs of sequential work [19] allows universally verifiable CPU benchmarks which cannot be cheated by parallelism (and GPU). We may assume that miners have CPUs of roughly the same computational power and ask that all miners should propose a proof of sequential work according to the previous block for each block proposal. In this way, a weak synchronization is also attained. Although it is hard to describe an event-trigger in this case, we believe that the security of this scheme can be reduced to one protocol with an explicit event-trigger.

5.3 Reward Issues

Intuitionally, for the sake of fairness and hence security, rewards should be sent to the proposer of each block of the main chain with the amount proportional to the block weight. However, we find that it is sufficient only to provide the same reward to the proposer of each block of the main chain. In case that $\rho(x) = 1$ is easy to satisfy and many blocks might be proposed in one round, miners will still devote all their hash power to attain the smallest hash to compete for the block finally on the main chain. As long as $\phi(\cdot)$ is monotonous, each participant has the probability of proposing the most competitive block proportional to its hash power. This is the *basic fairness* in Appendix. A.

5.4 Communication Complexity

One natural question is that in case that $\rho(x) = 1$ is easy to satisfy, probably many valid blocks will be proposed for each round and cause network issues. Tang et al. have shown in [1] that the communication complexity in this case is still bounded by $O(N \log N)$ where N is the number of network nodes.

6 Conclusion

This article develops the consensus model of Tang et al. by introducing the trigger-functionality-based framework comprising both the consensus of Tang et al. (giant-step consensus) and the classical Nakamoto consensus (small-step consensus). Useful convergence results are presented in an asymptotical level. Also, the necessity of the event-trigger, which is another blockchain in the original construction, is formally explained. This work opens up a great variety of potential future works shown in Appendix. B.

References

1. Shuyang Tang, Sherman S. M. Chow, Zhiqiang Liu, and Joseph K. Liu. Fast-to-finalize Nakamoto-like consensus. In *Information Security and Privacy - 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3-5, 2019, Proceedings*, pages 271–288, 2019.
2. Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf, 2016.
3. Marko Vukolic. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *Open Problems in Network Security - IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers*, pages 112–125, 2015.
4. Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 17–30, 2016.
5. Rafael Pass and Elaine Shi. Hybrid consensus: Efficient consensus in the permissionless model. In *31st International Symposium on Distributed Computing, DISC 2017, October 16-20, 2017, Vienna, Austria*, pages 39:1–39:16, 2017.
6. Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing bitcoin security and performance with strong consistency via collective signing. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 279–296, 2016.
7. Mahdi Zamani, Mahnush Movahedi, and Mariana Raykova. Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 931–948, 2018.
8. Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28-31, 2017*, pages 51–68, 2017.
9. QuantumMechanic. Proof of stake instead of proof of work, 2011. https://bitcointalk.org/index.php?topic=27787.0.
10. Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, pages 436–454, 2014.
11. Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, pages 281–310, 2015.
12. Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol with chains of variable difficulty. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 291–323, 2017.
13. Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic*

Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II, pages 643–673, 2017.
14. Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In *Proceedings of the ACM Symposium on Principles of Distributed Computing, PODC 2017, Washington, DC, USA, July 25-27, 2017*, pages 315–324, 2017.
15. Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert van Renesse. Bitcoin-NG: A scalable blockchain protocol. In *13th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2016, Santa Clara, CA, USA, March 16-18, 2016*, pages 45–59, 2016.
16. Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers*, pages 507–527, 2015.
17. Sunoo Park, Albert Kwon, Georg Fuchsbauer, Peter Gazi, Joël Alwen, and Krzysztof Pietrzak. SpaceMint: A cryptocurrency based on proofs of space. In *Financial Cryptography and Data Security - 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26 - March 2, 2018, Revised Selected Papers*, pages 480–499, 2018.
18. George Bissias and Brian Neil Levine. Bobtail: A proof-of-work target that minimizes blockchain mining variance (draft). arXiv CoRR abs/1709.08750, 2017.
19. Mohammad Mahmoody, Tal Moran, and Salil P. Vadhan. Publicly verifiable proofs of sequential work. In *Innovations in Theoretical Computer Science, ITCS '13, Berkeley, CA, USA, January 9-12, 2013*, pages 373–388, 2013.
20. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
21. Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, pages 139–147, 1992.
22. Markus Jakobsson and Ari Juels. Proofs of work and bread pudding protocols. In *Secure Information Networks: Communications and Multimedia Security, IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS '99), September 20-21, 1999, Leuven, Belgium*, pages 258–272, 1999.
23. Cynthia Dwork, Moni Naor, and Hoeteck Wee. Pebbling and proofs of work. In *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, pages 37–54, 2005.

A Fairness Results

Without considering block withholding or power splitting attacks, the fairness (and hence the security from chain quality) is already proved in [1]. Such a fairness in the definition of their work in called *one-round fairness* in our work.

Theorem 6 (One-Round Fairness). *If* $\widehat{\phi}(\cdot) : \mathcal{R} \to \mathbb{R}_0^+$ *is a monotonically non-increasing function, then*

$$\Pr\left[\widehat{\phi}(x) > \widehat{\phi}(y) \middle| x \leftarrow_{\$} \mathcal{H}_{min}^{\alpha\Omega}, y \leftarrow_{\$} \mathcal{H}_{min}^{(1-\alpha)\Omega}\right] - \alpha < 1/q(\kappa)$$

for a polynomial $q(\cdot)$.

The definition of general fairness is more complicated. It is the least fraction of total blocks of the main chain (w.h.p.) with the best adversary strategy including any block withholding and selfish mining under the execution model. We have a bound for fairness (suppose $\rho = \lambda x.1$ for simplicity).

Theorem 7 (The General Fairness Bound for $\rho = \lambda x.1$). *In the $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$ model, for any adversary $\mathcal{A}$, its general fairness has a lower bound of*

$$1 - \frac{1}{1 + \Psi_{\Omega,\phi,\rho}}$$

where

$$\Psi_{\Omega,\phi,\rho} := \mathrm{E}\left[\max_{\ell}\left\{\sum_{i=1}^{\ell}\widehat{\phi}(x_i) - \sum_{i=1}^{\ell}\widehat{\phi}(y_i) \geq 0\right\} \middle| \begin{array}{l} x_1, x_2, \ldots \leftarrow_{\$} \mathcal{H}_{min}^{\alpha\Omega} \\ y_1, y_2, \ldots \leftarrow_{\$} \mathcal{H}_{min}^{(1-\alpha)\Omega} \end{array}\right].$$

Proof. We consider an omniscient adversary $\mathcal{A}_o$ with unbounded computing power having access to all information and the randomness of all participants. In another world, $\mathcal{A}_o$ is a "future teller" that knows the minimal hash of other participants of every round anytime. Obviously, the fairness in the face of such an adversary is a fairness bound to all bounded adversaries with any strategy including block withholding of the selfish mining. We assume that $\mathcal{A}_o$ has known the minimal hash attained by it ($\{x_R\}_{R\in\mathbb{N}^+}$) and honest participants ($\{y_R\}_{R\in\mathbb{N}^+}$) of each round R. Clearly the optimal strategy for $\mathcal{A}_o$ is iterated as follows.

(i) It sets $R \leftarrow 0$,
(ii) Let $R \leftarrow R + 1$,
(iii) If $\sum_{i=R}^{\ell}\widehat{\phi}(x_i) < \sum_{i=R}^{\ell}\widehat{\phi}(y_i)$ for any $\ell \geq R$, do nothing to round R, and go back to (ii),
(iv) Else, let

$$K_R := \max_{K\in\mathbb{N}^+}\left\{\sum_{i=R}^{R+K-1}\widehat{\phi}(x_i) - \sum_{i=R}^{R+K-1}\widehat{\phi}(y_i) \geq 0\right\},$$

start a selfish mining by withholding newly mined blocks (if $K_R > 1$) till round $R + K_R - 1$ and propose all withhold blocks afterwards,
(v) Go back to (ii).

Thereby, we can derive that $\mathcal{A}_o$ could have its blocks on the main chain with a fraction of

$$\frac{\Psi_{\Omega,\phi,\rho}}{1 + \Psi_{\Omega,\phi,\rho}}.$$

B Future Works

This work opens up a variety of future works.

Fairness Bounds. Fairness is measured by the least fraction (w.h.p.) of total blocks of the main chain mined by honest participants with an adversary with the best mining strategy (including all hybrid strategies of selfish mining and block withholdings). Actually, fairness is a crucial property to the security basis known as *chain quality*. However, we did not put our existing fairness result to the main content for the following reasons (it is moved to the appendix). Firstly, our current fairness bound is not useful enough to qualify a $\widehat{\phi}$ without numerical and statistical methods. Intuitionally, a fair framework should have $\Phi^{\beta}_{\Omega,\phi,\rho} \propto \beta$. However, our existing fairness result is not yet explicitly linked to $\Phi^{\beta}_{\Omega,\phi,\rho}$. Secondly, our fairness bound is not tight since a "future-telling" omniscient adversary is too strong an assumption.

Consistency and Liveness in An Asynchronous Network. The consistency consists of common prefix and chain quality whose analysis strongly depends on fairness. Thereby, it is expected to formally prove the consistency after having a better fairness bound. Also, the liveness in an asynchronous network is worthy of further research.

Unifying the Necessity and Sufficiency Theorem. There is a gap between necessity and sufficiency theorem of our convergence results. It is expected to narrow the gap or even make two theorems meet, i.e., finding a necessary and sufficient condition for secure convergence.

Applying The Functional Nakamoto Consensus to More Protocols. The methodology of functional Nakamoto consensus is expected to be applied to more distributed consensus schemes other than naive blockchains. For example, the GHOST protocol [16] or other DAG-based consensus. Also, consensus frameworks other than proof-of-work (like proof-of-space) may adopt such a methodology for a fairer evaluation of the resource of participants and potentially improve the fairness and convergence rate. Also, the methodology might be used to improve the fairness of leader elections in committee-based consensus schemes. Moreover, the functional Nakamoto consensus can be potentially combined with blockchains with novel structures like fruitchain [14] or bitcoin-NG [15].

Alternative Proofs. Some of our proofs have leveraged the approximation from Gaussian distribution which is rarely considered in cryptographic proofs, though it is asymptotically correct according to the central limit theorem. Still, alternative proofs without approximating with Gaussian distributions are expected.

C Analytic Search Towards Faster Convergence

Few "potential functions" (which is the way $\widehat{\phi}$ function is referred to by Tang et al.) with outstanding convergence rate were listed in the paper of [1]. A natural question is whether we can try to find a potential function by linearly combining these given functions. To this end, we write these functions as a sequence of base

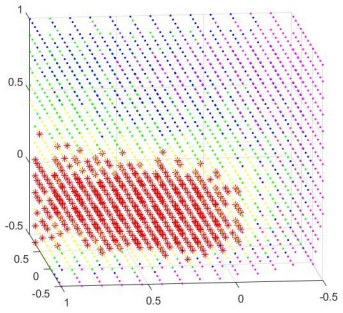

Fig. 1. The Function Space (the color of each point (u, v, w) of the graph corresponds to the convergence rate of the potential function $\widehat{\phi} = f_1 + uf_2 + vf_3 + wf_4$)

functions $\boldsymbol{f} = (f_1, f_2, f_3, f_4) \in (\mathcal{R} \to \mathbb{R})^\ell$ that

$$\begin{aligned} f_1(x) =& \frac{\pi}{2} - \arctan\left(\frac{x-D}{2D}\right), \\ f_2(x) =& \min\left\{\frac{\Omega}{x}, \frac{\Omega}{D}\right\}, \\ f_3(x) =& 2\sqrt{D} - \mathsf{sgn}(x-D)\cdot\sqrt{|x-D|}, \\ f_4(x) =& [x \le 2D]_b + [x \le D]_b, \end{aligned}$$

with $D = \frac{|\mathcal{R}|}{\Omega}$ and try to search for a list of coefficients $\boldsymbol{c} = (c_1, c_2, c_3, c_4) \in \mathbb{R}^4$ in the space of $\mathbb{R}^4$ for a potential function corresponding to a giant-step protocol with faster convergence rate. Clearly, each tuple of $\boldsymbol{c}$ determines a potential function

$$\widehat{\phi} := \mathsf{rectify}(\sum_{i=1}^{\ell} c_i f_i),$$

where $\mathsf{rectify} \in (\mathcal{R} \to \mathbb{R}) \to (\mathcal{R} \to \mathbb{R}_0^+)$ is a functor that "rectifies" a function into an admissible potential function by

$$\mathsf{rectify}(f)(x) := \max\left\{0, \min\left\{f(x), \min_{u=1}^{x-1} f(u)\right\}\right\}.$$

An intuitional way is to search for a better tuple of $\boldsymbol{c}$ with Newton-based approaches and random samplings. This was our first experiment. However, we failed to find a convergence better than f_1 which is the best provided function in [1]. Inspired by failed Newton-based approaches, the following experiment tells us that the linear combination method fails since the best linear combination is merely sticking on f_1. Simply put, we sample throughput the whole space of $\boldsymbol{c} \in \{1\} \times [0,1] \times [0,1] \times [0,1]$ and mark on fig. 1 with a color according to the convergence rate of $\widehat{\phi} = \boldsymbol{c} \cdot \boldsymbol{f}$ (we have neglected the rectify part in the second experiment). As shown in the figure, the result turns out to be more

"monotonous" than we expected and the optimum is attain around $(0, 0, 0)$ which corresponds to $\widehat{\phi} = f_1$.

D Proofs

The following two lemmas are implicitly implemented for several times throughout this paper without an explicit reference to the appendix since they are obvious from the definition of limitations.

Lemma 3. *For two functions $p(x)$ and $q(x)$ over $\mathbb{R}_0^+$, if $\lim_{x\to 0} \frac{p(x)}{q(x)} = 1$, then for any marginal $\epsilon > 0$, there exists a $x' \in \mathbb{R}_0^+$ such that $1 - \epsilon < \frac{p(x)}{q(x)} < 1 + \epsilon$ holds for all $0 \leq x \leq x'$.*

Lemma 4. *For two functions $p(n)$ and $q(n)$ over $\mathbb{N}$, if $\lim_{n\to+\infty} \frac{p(n)}{q(n)} = 1$, then for any marginal $\epsilon > 0$, there exists a $n' \in \mathbb{N}$ such that $1-\epsilon < \frac{p(n)}{q(n)} < 1+\epsilon$ holds for all $n \geq n'$.*

Lemma 5. *For any negligible $p(\cdot)$ over $\mathbb{R}_0^+$, the function $f(x) = 1 - e^{-p(x)}$ is also a negligible function.*

Proof. Suppose that $f(x)$ is not a negligible function and hence there is a polynomial $q(x)$ such that for any small x' there always exists a $0 \leq x \leq x'$ that $f(x) > q(x)$. $f(x) > q(x)$ is equivalent to

$$p(x) > \ln\left(1 + \frac{q(x)}{1 - q(x)}\right)$$

and thereby $p(x) > (1-\epsilon)\frac{q(x)}{1-q(x)} > \frac{1}{2}q(x)$ for a marginal $\epsilon > 0$. This contradicts to the condition of a negligible $p(x)$.

Lemma 6. *For any $1 < k < n$, $n, k \in \mathbb{N}^+$:*

$$\frac{1}{k}\binom{n}{k} = \sum_{i=k}^{n} \frac{1}{i}\binom{i}{k}$$

Proof.

$$\begin{aligned}
\frac{1}{k}\binom{n}{k} &= \frac{1}{k}\left(\binom{n-1}{k-1} + \binom{n}{k-1} + \ldots + \binom{k}{k-1} + 1\right) \\
&= \frac{1}{k}\left(1 + \binom{k}{1} + \binom{k+1}{2} + \ldots + \binom{n-1}{n-k}\right) \\
&= \sum_{i=0}^{n-k} \frac{1}{k}\binom{k+i-1}{i} = \sum_{i=0}^{n-k} \frac{1}{k+i}\binom{k+i}{k} = \sum_{i=k}^{n} \frac{1}{i}\binom{i}{k}.
\end{aligned}$$

Lemma 7. *For any $n \in \mathbb{N}^+$:*

$$\sum_{i=1}^{n} \frac{(-1)^{i-1}\binom{n}{i}}{i} = \sum_{i=1}^{n} \frac{1}{i}$$

Proof. On the left-hand side (LHS) of this formula,

$$LHS = \sum_{i=1}^{n}(-1)^{i-1}\frac{\binom{n}{i}}{i} = \sum_{i=1}^{n}(-1)^{i-1}\sum_{j=i}^{n}\frac{\binom{j}{i}}{j},$$

this step is taken following lemma 6, then, on the right-hand side (RHS) of this formula,

$$LHS = \sum_{i=1}^{n}\frac{\sum_{j=1}^{i}(-1)^{j-1}\binom{i}{j}}{i} = \sum_{i=1}^{n}\frac{1}{i} = RHS.$$

Theorem 8. *For any great integer T polynomial in κ,*

$$\mathrm{E}\left[h \leftarrow \mathcal{H}_{min}^{T}\middle|\frac{|\mathcal{R}|}{h}\right] = T\ln\frac{|\mathcal{R}|}{T} + O\left((\frac{T}{|\mathcal{R}|})^2\right)$$

holds.

Proof. It can be directly derived that

$$\mathrm{E}\left[h \leftarrow \mathcal{H}_{\min}^{T}\middle|\frac{|\mathcal{R}|}{h}\right] = |\mathcal{R}|\cdot\sum_{i=1}^{|\mathcal{R}|}\frac{T}{|\mathcal{R}|}(1-\frac{i}{|\mathcal{R}|})^{T-1}/i = T\sum_{i=1}^{|\mathcal{R}|}(1-\frac{i}{|\mathcal{R}|})^{T}/i,$$

where

$$\begin{aligned}
&\sum_{i=1}^{|\mathcal{R}|}(1-\frac{i}{|\mathcal{R}|})^{T}/i \\
&= \sum_{i=1}^{|\mathcal{R}|}\left[\frac{1}{i} + \sum_{k=1}^{T}(-1)^k\binom{T}{k}(\frac{i}{|\mathcal{R}|})^k/i\right] \\
&= \left(\sum_{i=1}^{|\mathcal{R}|}1/i\right) + \sum_{k=1}^{T}\left[(-1)^k\sum_{i=1}^{|\mathcal{R}|}\binom{T}{k}\frac{i^{k-1}}{|\mathcal{R}|^k}\right] \\
&= \left(\sum_{i=1}^{|\mathcal{R}|}1/i\right) + \sum_{k=1}^{T}\left[(-1)^k\frac{\binom{T}{k}}{|\mathcal{R}|^k}\left(\int_0^{|\mathcal{R}|}x^{k-1}\mathrm{d}x + \left|O(k|\mathcal{R}|^{k-2})\right|\right)\right] \\
&= \left(\sum_{i=1}^{|\mathcal{R}|}1/i\right) + \left(\sum_{k=1}^{T}(-1)^k\binom{T}{k}/k\right) + \left(\sum_{k=1}^{T}(-1)^k\binom{T}{k}\left|O(T/|\mathcal{R}|^2)\right|\right) \\
&= (\ln|\mathcal{R}| + \gamma) - (\ln T + \gamma) + O(T/|\mathcal{R}|^2) \\
&= \ln\frac{|\mathcal{R}|}{T} + O(T/|\mathcal{R}|^2).
\end{aligned}$$

So forth, we have proved

$$\mathrm{E}\left[h \leftarrow \mathcal{H}_{\min}^{T}\middle|\frac{|\mathcal{R}|}{h}\right] = T\ln\frac{|\mathcal{R}|}{T} + O\left((\frac{T}{|\mathcal{R}|})^2\right).$$

Lemma 8. *We assume a sound trigger functionality $\mathcal{F}_{\mathsf{trigger}}^{\Omega,\phi,\rho}$. Let $C \in \mathbb{N}^+$ be a natural number sub-polynomial in κ, let $w := \beta\Omega$ for a $0 < \beta < 1$, let*

$$M_1(C) := \mathrm{E}\left[\widehat{\phi}(z)\middle| z \leftarrow_{\$} \mathcal{H}_{min}^{Cw}\right],$$

$$M_2(C) := C \cdot \mathrm{E}\left[\widehat{\phi}(x)\middle| x \leftarrow_{\$} \mathcal{H}_{min}^{w}\right].$$

Generally, $M_1(C) \leq M_2(C)$. Specifically, if $\mathsf{ord}(\rho) \neq 0$, then $M_1(C) \approx_\kappa M_2(C)$, else $\frac{M_2(C)}{M_1(C)} > 1 + r$ for a substantial constant r for sufficiently large constant C.

Proof. We first show a simple deformation.

$$\begin{aligned} M_1(C) &= \mathrm{E}\left[\max\left\{\widehat{\phi}(y_1), \widehat{\phi}(y_2), \ldots, \widehat{\phi}(y_C)\right\}\middle| y_1, y_2, \ldots \leftarrow_{\$} \mathcal{H}_{\min}^{w}\right] && (8)\\ &\leq \mathrm{E}\left[\sum_{i=1}^{C}\widehat{\phi}(y_i)\middle| y_1, y_2, \ldots \leftarrow_{\$} \mathcal{H}_{\min}^{w}\right] && (9)\\ &= M_2(C). \end{aligned}$$

In the $\mathsf{ord}(\rho) = 0$ case, (9) equals $C \cdot \Phi_{\Omega,\phi,\rho}^{\beta}$, therefore

$$\begin{aligned} \frac{M_2(C)}{M_1(C)} &= \frac{C \cdot \Phi_{\Omega,\phi,\rho}^{\beta}}{\mathrm{E}\left[\max\left\{\widehat{\phi}(y_1), \widehat{\phi}(y_2), \ldots, \widehat{\phi}(y_C)\right\}\middle| y_1, y_2, \ldots \leftarrow_{\$} \mathcal{H}_{\min}^{w}\right]}\\ &\geq \frac{(1-\chi)\beta C \cdot \Phi_{\Omega,\phi,\rho}^{1}}{\mathsf{ext}(\kappa) \cdot \Phi_{\Omega,\phi,\rho}^{1}}. \end{aligned}$$

Let $C > \frac{2}{(1-\chi)\beta}\mathsf{ext}(\kappa)$, $\frac{M_2(C)}{M_1(C)} \geq 2$. In the $\mathsf{ord}(\rho) \geq 1$ case,

$$M_2(C) = C \cdot \Pr\left[x \leftarrow_{\$} \mathcal{H}_{\min}^{w} : \rho(x) = 1\right] \cdot \mathrm{E}\left[\phi(x)\middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge \rho(x) = 1\right],$$

$$M_1(C) = \Pr\left[x \leftarrow_{\$} \mathcal{H}_{\min}^{Cw} : \rho(x) = 1\right] \cdot \mathrm{E}\left[\phi(x)\middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{Cw} \wedge \rho(x) = 1\right].$$

In fact,

$$
\begin{aligned}
&\mathrm{E}\left[\phi(x)\middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{Cw} \wedge \rho(x)=1\right] \\
&= \mathrm{E}\left[\phi\left(\min_{i\in[C]}\{x_i\}\right)\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge |\{i\in[C]:\rho(x_i)=1\}|=1\right] \\
&\qquad \times \Pr\left[|\{i\in[C]:\rho(x_i)=1\}|=1\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge \phi\left(\min_{i\in[C]}\{x_i\}\right)=1\right] \\
&\quad + \mathrm{E}\left[\phi\left(\min_{i\in[C]}\{x_i\}\right)\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge |\{i\in[C]:\rho(x_i)=1\}|\geq 2\right] \\
&\qquad \times \Pr\left[|\{i\in[C]:\rho(x_i)=1\}|\geq 2\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge \phi\left(\min_{i\in[C]}\{x_i\}\right)=1\right] \\
&= \mathrm{E}\left[\phi(x)\middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge \rho(x)=1\right] \\
&\qquad \times \frac{\Pr\left[|\{i\in[C]:\rho(x_i)=1\}|=1 \wedge \phi\left(\min_{i\in[C]}\{x_i\}\right)=1\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w}\right]}{\Pr\left[\phi\left(\min_{i\in[C]}\{x_i\}\right)=1\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w}\right]} \\
&\quad + \mathrm{E}\left[\phi\left(\min_{i\in[C]}\{x_i\}\right)\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge |\{i\in[C]:\rho(x_i)=1\}|\geq 2\right] \\
&\qquad \times \frac{\Pr\left[|\{i\in[C]:\rho(x_i)=1\}|\geq 2 \wedge \phi\left(\min_{i\in[C]}\{x_i\}\right)=1\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w}\right]}{\Pr\left[\phi\left(\min_{i\in[C]}\{x_i\}\right)=1\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w}\right]}
\end{aligned}
$$

$$
\begin{aligned}
&\approx_{\kappa} \mathrm{E}\left[\phi(x)\middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge \rho(x)=1\right] \times \frac{\binom{C}{1}p(1-p)^{C-1}}{pC} \\
&\quad + \mathrm{E}\left[\phi\left(\min_{i\in[C]}\{x_i\}\right)\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge |\{i\in[C]:\rho(x_i)=1\}|\geq 2\right] \\
&\qquad \times \frac{\binom{C}{2}p^2(1-p)^{C-2}}{pC} \\
&\approx_{\kappa} \mathrm{E}\left[\phi(x)\middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge \rho(x)=1\right] \\
&\quad + \mathrm{E}\left[\phi\left(\min_{i\in[C]}\{x_i\}\right)\middle| x_1,x_2,\ldots,x_C \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge |\{i\in[C]:\rho(x_i)=1\}|\geq 2\right] \times \frac{(pC)^2}{2pC} \\
&\approx_{\kappa} \mathrm{E}\left[\phi(x)\middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{w} \wedge \rho(x)=1\right],
\end{aligned}
$$

where $p = \Pr\left[\rho(x)=1\middle| x \leftarrow_{\$} \mathcal{H}_{\min}^{w}\right]$, obviously $pC = o(\frac{1}{\kappa})$ and

$$
\Pr\left[x \leftarrow_{\$} \mathcal{H}_{\min}^{Cw} : \rho(x)=1\right] \approx_{\kappa} C \cdot \Pr\left[x \leftarrow_{\$} \mathcal{H}_{\min}^{w} : \rho(x)=1\right].
$$

Thereby,

$$\frac{M_2(C)}{M_1(C)} = \frac{C \cdot \Pr\left[x \leftarrow_{\$} \mathcal{H}^{w}_{\min} : \rho(x) = 1\right]}{\Pr\left[x \leftarrow_{\$} \mathcal{H}^{Cw}_{\min} : \rho(x) = 1\right]} \cdot \frac{\mathrm{E}\left[\phi(x) \middle| x \leftarrow_{\$} \mathcal{H}^{w}_{\min} \wedge \rho(x) = 1\right]}{\mathrm{E}\left[\phi(x) \middle| x \leftarrow_{\$} \mathcal{H}^{Cw}_{\min} \wedge \rho(x) = 1\right]} = 1 \pm o(1/\kappa).$$

Lemma 9. *$\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}$ with*

$$(\Omega, \phi, \rho) = \left(c, \quad \lambda x.1, \quad \lambda x. \begin{cases} 1, x < \frac{|\mathcal{R}|}{\varphi(\kappa)} \\ 0, o.w. \end{cases}\right),$$

is a sound trigger functionality where c is a constant and $\varphi(\kappa) = \Theta(\kappa)$.

Proof. Since $\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}$ obviously satisfies the properties of admissible tuples, finitely-order functionality (with order 0) and bounded maximal weight, we only show that there exists a constant $0 < \chi < 1-2\alpha$ such that for any constant $0 < \beta < 1$,

$$(1-\chi)\beta \leq \frac{\Phi^{\beta}_{\Omega,\phi,\rho}}{\Phi^{1}_{\Omega,\phi,\rho}} \leq (1+\chi)\beta.$$

In fact, let p be the probability of having a x returned from a single query to $\mathcal{H}$ that $\rho(x) = 1$ (easy to observe that actually $p = \varphi(\kappa)$), we have

$$\frac{\Phi^{\beta}_{\Omega,\phi,\rho}}{\Phi^{1}_{\Omega,\phi,\rho}} = \frac{1-(1-p)^{\beta c}}{1-(1-p)^{c}}.$$

As p as also a function of κ approaches 0 asymptotically, according to Lemma. 3, there exists marginal constants ϵ_1, ϵ_2 such that

$$(1-\epsilon_1)\frac{1-e^{\beta pc}}{1-e^{pc}} \leq \frac{1-(1-p)^{\beta c}}{1-(1-p)^{c}} \leq (1+\epsilon_1)\frac{1-e^{\beta pc}}{1-e^{pc}},$$

and

$$(1-\epsilon_2)\frac{\beta pc}{pc} \leq \frac{1-e^{\beta pc}}{1-e^{pc}} \leq (1+\epsilon_2)\frac{\beta pc}{pc}.$$

Finally, $\chi = \epsilon_1 + \epsilon_2 + \epsilon_1\epsilon_2$ is a satisfiable constant for our proof.

E Classical Nakamoto Consensus

In this part, we briefly introduce the classical Nakamoto consensus (the abstracted consensus of bitcoin). The classical Nakamoto consensus is also referred to as bitcoin consensus in this paper since it starts from the bitcoin whitepaper of Nakamoto in 2008 [20]. Blockchain is an append-only distributed ledger in the form of a chain of blocks, each containing certain transactions. The ledger of blockchain is essentially a linear log of transactions which is formed by concatenating all transactions of each block of the chain (the model of a linearly

ordered log of transactions is known as *state machine republica*). To append new transactions into the log and hence update the ledger, a new block is proposed to be appended to the rear of the blockchain. Proposing a block requires participants (*miners*) to solve a computational puzzle from "moderately hard functions" (known as *proof-of-work*, [21–23]). That is to find a nonce value by brute-force to make the hash of the nonce (concatenating the block head comprising the Merkle tree root of newly appended transactions and the previous block hash along with necessary auxiliary information) as small as possible. Such a hash value is called *block hash*. A block can be proposed and appended to the blockchain if the block hash is smaller than a predetermined target (or the *difficulty*). The procedure of finding such a nonce is *mining*. We describe the power of mining of each participant with *hash power*, which is defined as the total number of hash attempts done every time unit.

In case of an accident like malicious block proposal or multiple blocks proposed almost simultaneous due to network delays, a chain fork happens. Namely, two blocks are proposed with the same previous block. Honest participants always mine after the longest valid chain branch (we call it *main chain*). To make sure that a newly proposed block will remain always on the main chain without the risk of being replaced by a branch fork, it has to wait till the block is followed by a significant amount of consecutive newer blocks such that this block will remain on the main chain with an overwhelming probability even in case of adversary attacks. This amount of new blocks to wait is called the *secure convergence gap* or just *convergence gap* in this paper. For example, the secure convergence gap to bitcoin is often regarded as 6 (it guarantees the security with the probability of $1 - 10^{-3}$ from [20]). The convergence rate is measured with *finality time* which is defined as the expected time to meet the secure convergence gap.

Table 1. Notations

κ	the security parameter
α	the upper-bound of the adversary portion of total hash power, open to all participants and functionalities ($\alpha < 1/2$)
$[M]$	for an natural number M, $[M] = \{1, 2, \ldots, M\}$
$[A]_b$	for an assertion A, $[A]_b$ equals 1 (or else 0) if A is satisfied
$\lvert S \rvert$	the cardinality of the set S
$[\![\mathcal{X} \to \mathcal{Y}]\!]$	the space of functions from $\mathcal{X}$ to $\mathcal{Y}$
H	a cryptographic hash function
$\mathcal{R}$	the range of the hash function H with $\lvert\mathcal{R}\rvert = O(2^{2\kappa})$
$\mathcal{H}$	the oracle that returns a hash value from H with a random input for each query
$\mathcal{H}^t_{\min}$	the least-hash oracle that outputs the least output among t queries to $\mathcal{H}$
$\mathsf{ord}(\rho)$	the order of a trigger $\mathcal{F}^{\Omega,\phi,\rho}_{\mathsf{trigger}}$
$\lambda x.p(x)$	the notation for λ-calculus, can be regarded as a function that returns $p(x)$ for any input x
$P_1, P_2, \ldots, P_N$	ideal participants sharing the same hash power, $P_1, P_2, \ldots, P_{\alpha N}$ are controlled by the adversary $\mathcal{A}$

Table of Contents