

On Analysis of the Bitcoin and Prism Backbone Protocols

Jing Li and Dongning Guo

Northwestern University

jingli2015@u.northwestern.edu, dGuo@Northwestern.edu

October 22, 2019

Abstract

Bitcoin is a peer-to-peer payment system proposed by Nakamoto in 2008. Properties of the bitcoin backbone protocol have been investigated in some depth: the blockchain growth property quantifies the number of blocks added to the blockchain during any time intervals; the blockchain quality property ensures the honest miners always contribute at least a certain fraction of the blockchain; the common prefix property ensures if a block is deep enough, it will eventually be adopted by all honest miners with high probability. Following the spirit of decoupling various functionalities of the blockchain, Bagaria, Kannan, Tse, Fanti, and Viswanath (2018) proposed the Prism protocol to dramatically improve the transaction rate while maintaining the same level of security. Most prior analyses of the bitcoin and the Prism backbone protocols provide performance guarantees up until a finite number of rounds (equivalent to finite lifespan) and that all miners have identical information by the end of each round (referred to as the synchronous model). This paper presents a streamlined and strengthened analysis without the finite lifespan assumption. Also, both the synchronous model and a more general model with arbitrary but bounded block propagation delays are studied. The results include a blockchain growth property, a blockchain quality property, and a common prefix property of the bitcoin backbone protocol, as well as the liveness and persistence of the Prism backbone protocol. An explicit probabilistic guarantee is provided for every transaction found in an honest blockchain to become permanent in the final ledger. The properties of the bitcoin and the Prism backbone protocols are given as explicit expressions rather than order optimal results, which lead to improved references for public transaction ledger protocol design.

I. INTRODUCTION

A. The bitcoin backbone protocol

Bitcoin is an electronic payment system introduced by Nakamoto [1] in 2008. The system is built on a distributed ledger technology commonly referred to as blockchain. Miners are distributed parties who

generate blocks and maintain their own version of the blockchain. A blockchain is a finite sequence of blocks adopted by some miner at some point in time. It begins with a genesis block, and every subsequent block contains a cryptographic hashing of the previous block. In order to generate a valid new block, a miner need to find a nonce whose hash values satisfies a difficulty requirement. The process of finding such a nonce is called mining. An honest miner follows the honest chain rule, i.e., it always adopts the longest blockchain it heard about and mines on top of the longest blockchain. Since all miners work simultaneously, it is possible that two or more different blocks are mined and announced at around the same time. Then different honest miners may extend different blockchains depending on which longest one they hear first. This phenomenon is called forking. Forking of a blockchain challenges network consensus and presents opportunities for double spending attack, namely, a transaction included in the longest fork is not included in a different fork that overtakes the first fork to become the longest one.

Nakamoto [1] characterized the race between the honest miners and an adversary with less than half of the total mining power as a random walk with a drift. Nakamoto showed that the probability the adversary blockchain overtakes the honest miner's consensus blockchain vanishes exponentially over time. Nakamoto argued that the bitcoin protocol is safe under double spending attack as long as one considers a transaction confirmed only after enough new blocks are mined to extend the honest blockchain. An in-depth analysis of the bitcoin protocol was given in [2]. Several important properties of the bitcoin backbone protocol have been proposed in [1], [3]–[6]. Garay, Kiayias, and Leonardos [3] gave a formal description and analysis of the bitcoin backbone protocol assuming a fully synchronous network, namely, mining takes place in rounds and at the end of each round, all miners see all published blocks. Under this model, [3] introduced a common prefix property and a blockchain quality property. The common prefix property states if a block is k blocks deep in an honest miner's blockchain, then the probability that the block is not included by all other honest miners' blockchain decreases exponentially with k . The blockchain quality property states the honest miners always contribute at least a certain percentage of the blockchain regardless of the strategy of adversarial parties. Then, [4] introduced a blockchain growth property, which quantifies the number of blocks added to the blockchain during any time intervals.

Moreover, Nakamoto's analysis was improved in [5] to address selfish mining. In this case, selfish miners can introduce disagreement between honest miners and split their hashing power. Selfish miners thus enhance their relative hashing power to win disproportionate rewards. This strategy, however, is not designed for double spending purposes.

The bitcoin backbone protocol gives birth to numerous "robust public transaction ledger" protocols [7]–[9]. The preceding properties guarantee two fundamental properties of a robust public transaction ledger: liveness and persistence. Due to the blockchain growth property and the blockchain quality property,

blocks originating from honest miners will eventually end up at a level of more than k blocks of an honest miner's blockchain. Due to the common prefix property, an honest miner's k -deep block remains permanent.

The bitcoin backbone protocol can also be leveraged to solve other problems. For example, the bitcoin backbone protocol ensures some basic properties for some randomized Byzantine agreement protocols [10]–[14].

B. The Prism protocol

The throughput of bitcoin is limited by design to ensure security [15]. As mining rate increases, blocks are more likely to be mined and announced simultaneously, i.e., forking is more likely to occur. Due to the longest blockchain rule, only the blocks on the longest blockchain will eventually be adopted by honest miners, and other honest blocks are wasted. Then the adversarial miners compete with fewer honest miners. To avoid forking, the average time interval between new blocks is set to be much longer than the latency for propagating a block to most miners in the network [16].

Many ideas have been proposed to improve the blockchain throughput while maintaining its security. One way is to deal with high-forking blockchains by optimizing the forking rule. For example, GHOST chooses the main blockchain according to the heaviest tree rule instead of the longest blockchain rule [16]. Inclusive, Spectre, and Phantom construct a directed acyclic graph (DAG) structured blockchain by introducing reference links between blocks in addition to the parent links [17]–[19]. However, these protocols are vulnerable to certain attacks [20]–[22]. Generally speaking it is very challenging to make high-forking protocols secure.

Another line of work is to decouple the various functionalities of the blockchain. For example, BitcoinNG divides the bitcoin blockchain's operations into leader selection and transaction serialization [7]. In BitcoinNG, time is divided into epochs. During each epoch, a leader is chosen to order the transaction blocks of that epoch. However, this protocol is vulnerable to bribery or targeted attacks to leaders. In Fruitchain, transactions (fruits) are also decoupled from proposer blocks. However, fruitchain focuses on enhancing fairness instead of improving throughput [23].

Following the spirit of decoupling blocks' functionalities, Bagaria, Kannan, Tse, Fanti, and Viswanath [9] proposed the Prism protocol, which is a structured-DAG blockchain with one proposer blockchain and many voter blockchains. The voter blocks elect a leader block at each level of the proposer blockchain by voting. The sequence of leader blocks concludes the contents of all voter blocks, and finalizes the ledger. Each voter blockchain mines independently at a low mining rate. A voter blockchain follows the bitcoin protocol to provide security to leader election process.

With this design, the throughput (containing the content of *all* voter blocks) is decoupled from the mining rate of each voter blockchain. Slow mining rate guarantees the security of each voter blockchain as well as the proposer blockchain. Prism achieves security against up to 50% adversarial hashing power, optimal throughput up to the capacity of the network, and fast confirmation latency for honest transactions. A thorough description and analysis is shown in [9].

C. Our results

Previous analysis on the backbone of bitcoin and Prism assumes a blockchain’s lifespan is finite, i.e., there exists a maximum round when the blockchain ends. For example, in [3], [6] and [9], the good properties of blockchain hold only under typical events, i.e., the number of honest and adversarial blocks mined must not deviate too much from their expected value over all long enough time intervals. The probability of typical events was shown to depend on the blockchain’s maximum round parameter. Indeed, the probability of the blockchain growth property, the blockchain quality property, and the common prefix property are all expressed implicitly in terms of the blockchain’s maximum round.

In this paper, we drop the finite horizon assumption and prove strong properties of the bitcoin backbone protocol. We define the typical events with respect to each interval: instead of requiring the number of honest and adversarial blocks to be typical over all long enough time intervals, we only require them to be typical over all time intervals that contain a certain interval that includes the transaction of interest. Since the probability that the number of honest and adversarial blocks are “atypical” decreases exponentially with interval length, the sum of the probabilities over all those intervals remains vanishingly small. Thus we provide performance guarantees that are truly *permanent* whether or not the blockchain have a finite lifespan. Moreover, without the finite horizon assumption, we express the properties of the bitcoin backbone protocol in explicit expressions in lieu of order optimality results in some previous analysis. The explicit expressions provide tighter bounds and more practical references to public transaction ledger protocol design.

In [9], liveness and consistency properties of the Prism protocol were proved assuming a finite life span of the blockchains [9]. In this paper, we also prove the liveness and consistency of the Prism protocol without the finite horizon assumption.

Another crucial assumption in [3], [6], [9] is that all blocks broadcast during a protocol round reach all miners by the end of that round, i.e., all miners have complete up-to-date information by the end of each round. This is referred to as the synchronous model. In this paper, we generalize the analysis to a much more challenging model in which a block may reach different miners after arbitrary different delays, so that even the honest miners are never guaranteed to have identical view of the system. It is only assumed

that the propagation time is bounded by T rounds, which is realistic in practice. A key idea in this paper is to exploit honest miners' common information about those rounds in which a single honest block is mined and that no other honest blocks are mined within $T - 1$ rounds before and after. Essentially all the properties developed for the synchronous model find their counterparts for this bounded-delay model.

II. MODEL AND DEFINITIONS

We assume the total number of miners is n , among which t miners are adversarial and the remaining miners are honest. Assume all miners have equal hash powers (if not, we assume they can be split into equal-power pieces). Let

$$\beta = \frac{t}{n} \quad (1)$$

denote the percentage of adversarial miners. We assume adversarial miners collectively have less than $\frac{1}{2}$ of the total mining power in the blockchain network, so $\beta \in [0, \frac{1}{2})$.

We adopt a discrete model where activities take place in rounds. If a miner publishes one or more blocks in a round, all miners receive the block(s) at exactly the end of the round (a miner can only react to round r blocks in round $r + 1$). Evidently, by the end of each round, all honest miners are fully synchronized. If a block is mined by an honest miner, we call it an *honest block*; otherwise the block is called an *adversarial block*. We assume that during round 0, a single honest block, called the genesis block, is mined and broadcast to all miners. For $r \in \{1, 2, \dots\}$, let $H[r]$ denote the number of all honest blocks mined during round r . The mining difficulty and miner's mining powers are adjusted to be constant in all rounds $r \geq 1$.

Without loss of generality, the mining power of all miners are and the mining difficulty are assumed to remain constant, such that the probability that an honest miner mines a new block in every round $r \geq 1$ is equal to $p \in (0, 1)$.¹ Note that $H[r] \sim \text{Binomial}(n - t, p)$. Define

$$X[r] = \begin{cases} 1, & \text{if } H[r] \geq 1 \\ 0, & \text{otherwise.} \end{cases} \quad (2)$$

$X[r]$ indicates if one or more honest blocks are mined during round r or not. Let

$$q = 1 - (1 - p)^{n-t}. \quad (3)$$

¹This probability is held constant by adjusting the mining difficulty in case the mining power fluctuate over rounds.

Then $X[r] \sim \text{Bernoulli}(q)$. Define

$$Y[r] = \begin{cases} 1, & \text{if } H[r] = 1 \\ 0, & \text{otherwise.} \end{cases} \quad (4)$$

Basically $Y[r]$ indicates if a single honest block is mined in round r or not. Then $Y[r] \sim \text{Bernoulli}((n-t)p(1-p)^{n-t-1})$. A round r is called a uniquely successful round if $Y[r] = 1$. Let $Z[r]$ upper bound the number of adversarial blocks mined during round r (the adversarial miners may or may not publish them). Then $Z[r] \sim \text{Binomial}(t, p)$.

It is important to note that $H[1], H[2], \dots$ are independently and identically distributed (i.i.d.), which form a stationary process. The same can be said of the X , Y , and Z sequences. Define

$$\xi = \frac{1 - 2\beta}{1 - \beta}. \quad (5)$$

Then $\xi \in (0, 1]$.

For all integers s and r satisfying $1 \leq s < r$, let

$$H[s, r] = \sum_{i=s}^{r-1} H[i], \quad (6)$$

which represents the total number of honest blocks mined during rounds $s, \dots, r-1$. To be consistent with this notation, we mean all rounds up to and including $r-1$ when we say “by round r ”. Likewise, we define

$$X[s, r] = \sum_{i=s}^{r-1} X[i] \quad (7)$$

$$Y[s, r] = \sum_{i=s}^{r-1} Y[i] \quad (8)$$

$$Z[s, r] = \sum_{i=s}^{r-1} Z[i]. \quad (9)$$

Definition 1. By a blockchain we mean a finite sequence of blocks adopted by some miner at some point in time which begins with a genesis block and that every subsequent block contains a cryptographic hashing of the previous block. It is assumed that no block can be mined in an earlier round than its immediate predecessor.

A blockchain’s prefix is also a blockchain. A blockchain must have the following properties: 1) Its blocks must be mined in order; 2) it is immutable in the sense that it is computationally impossible for any miner to mine a different blockchain that has the same genesis block and the same final block.

Definition 2. If a blockchain is adopted by an honest miner by some round, it is said to be honest.

III. THE BITCOIN BACKBONE PROTOCOL

In Section III and IV , it is assumed that, the mining difficulty is adjusted such that

$$q \leq \frac{\xi}{6}. \quad (10)$$

We will make heavy use of Bernoulli's inequality:

Proposition 3. (*Bernoulli's inequality*) For every integer $k \geq 0$ and real number $x > -1$,

$$(1 + x)^k \geq 1 + kx. \quad (11)$$

Proposition 4. For $r = 1, 2, \dots$,

$$q \leq p(n - t) < \frac{q}{1 - q}. \quad (12)$$

Proof. As $X[r] \sim \text{Bernoulli}(q)$, we have

$$\mathbb{E}[X[r]] = q \quad (13)$$

$$= 1 - (1 - p)^{n-t} \quad (14)$$

$$\leq p(n - t), \quad (15)$$

where (15) is due to Bernoulli's inequality. Moreover,

$$\frac{q}{1 - q} = \frac{1 - (1 - p)^{n-t}}{(1 - p)^{n-t}} \quad (16)$$

$$= (1 - p)^{-(n-t)} - 1 \quad (17)$$

$$> (1 + p)^{n-t} - 1 \quad (18)$$

$$\geq p(n - t), \quad (19)$$

where (18) is due to $(1 + p)(1 - p) < 1$ and (19) is due to Bernoulli's inequality. By (15) and (19),

$$q \leq p(n - t) < \frac{q}{1 - q}. \quad (20)$$

□

Proposition 5. For $r = 1, 2, \dots$,

$$\mathbb{E}[Y[r]] > q(1 - q). \quad (21)$$

Proof. According to Proposition 4, $q \leq \frac{1}{6}$ implies $q < p(n-t) < \frac{1}{5}$. Hence,

$$\mathbb{E}[Y[r]] = p(n-t)(1-p)^{n-t-1} \quad (22)$$

$$\geq p(n-t)(1-p(n-t-1)) \quad (23)$$

$$> p(n-t)(1-p(n-t)) \quad (24)$$

$$> q(1-q), \quad (25)$$

where (23) is due to Bernoulli's inequality, and (25) holds because the function $x(1-x)$ is increasing on $[0, \frac{1}{2}]$. \square

Proposition 6. For $r = 1, 2, \dots$,

$$\mathbb{E}[Z[r]] < \mathbb{E}[X[r]]. \quad (26)$$

Proof. Since $Z[r] \sim \text{Binomial}(t, p)$,

$$\mathbb{E}[Z[r]] = pt \quad (27)$$

$$= \frac{t}{n-t} p(n-t) \quad (28)$$

$$< \frac{t}{n-t} \frac{q}{1-q} \quad (29)$$

$$= (1-\xi) \frac{1}{1-q} q \quad (30)$$

$$\leq \frac{1-\xi}{1-\frac{\xi}{6}} q \quad (31)$$

$$< \mathbb{E}[X[r]], \quad (32)$$

where (29) is due to Proposition 4 and (32) is due to $q \leq \frac{\xi}{6}$. \square

Definition 7. For all integers $1 \leq s < r$, define event

$$E[s, r] := E_1[s, r] \cap E_2[s, r] \cap E_3[s, r] \quad (33)$$

where

$$E_1[s, r] := \left\{ \left(1 - \frac{\xi}{6}\right) \mathbb{E}[X[s, r]] < X[s, r] < \left(1 + \frac{\xi}{6}\right) \mathbb{E}[X[s, r]] \right\} \quad (34)$$

$$E_2[s, r] := \left\{ \left(1 - \frac{\xi}{6}\right) \mathbb{E}[Y[s, r]] < Y[s, r] \right\} \quad (35)$$

$$E_3[s, r] := \left\{ Z[s, r] < \mathbb{E}[Z[s, r]] + \frac{\xi}{6} \mathbb{E}[X[s, r]] \right\}. \quad (36)$$

Under event $E_1[s, r]$, the number of rounds with honest block mined, $X[s, r]$, does not deviate from its expected value by more than a fraction of $\frac{\xi}{6}$. Under event $E_2[s, r]$, the number of uniquely successful rounds $Y[s, r]$ is no less than $1 - \frac{\xi}{6}$ of its expected value. Under event $E_3[s, r]$, the upper bound for the number of adversarial blocks is no more than its expected value plus $\frac{\xi}{6}$ of the expectation of $X[s, r]$. Intuitively, under $E[s, r]$, we have 1) a “typical” number of rounds during which at least one honest block is mined, 2) “enough” uniquely successful rounds, and 3) the total number of adversarial blocks is limited.

Proposition 8. (Chernoff bound, [24, page 69]) Let $X \sim \text{binomial}(n, p)$. Then for every $\eta \in (0, 1]$,

$$P(X \leq (1 - \eta)pn) \leq e^{-\frac{\eta^2 pn}{2}}, \quad (37)$$

and

$$P(X \geq (1 + \eta)pn) \leq e^{-\frac{\eta^2 pn}{3}}. \quad (38)$$

Define

$$\eta = \frac{\xi^2}{180}q. \quad (39)$$

Lemma 9. For all integers $1 \leq s < r$,

$$P(E[s, r]) > 1 - 4e^{-\eta(r-s)}, \quad (40)$$

where η is given in (39).

Proof. We first analyze events E_1 , E_2 , and E_3 separately. We have

$$P(E_1[s, r]^c) = P\left(|X[s, r] - \mathbb{E}[X[s, r]]| \geq \frac{\xi}{6}\mathbb{E}[X[s, r]]\right) \quad (41)$$

$$= P\left(X[s, r] \geq \mathbb{E}[X[s, r]] + \frac{\xi}{6}\mathbb{E}[X[s, r]]\right) + P\left(X[s, r] \leq \mathbb{E}[X[s, r]] - \frac{\xi}{6}\mathbb{E}[X[s, r]]\right) \quad (42)$$

$$\leq 2e^{-\frac{\xi^2}{108}q(r-s)}, \quad (43)$$

where (43) is due to Proposition 8.

Also,

$$P(E_2^c[s, r]) = P\left(Y[s, r] \leq \left(1 - \frac{\xi}{6}\right)\mathbb{E}[Y[s, r]]\right) \quad (44)$$

$$\leq e^{-\frac{\xi^2}{72}\mathbb{E}[Y[s, r]]} \quad (45)$$

$$\leq e^{-\frac{\xi^2}{72}(1-q)q(r-s)} \quad (46)$$

$$< e^{-\frac{\xi^2}{72}(1-\frac{\xi}{6})q(r-s)}, \quad (47)$$

where (45) is due to Proposition 8, (46) is due to Proposition 5, and (47) is due to $q \leq \frac{\xi}{6}$.

Note that the moment generating function for binomial random variable $Z[r] \sim \text{Binomial}(t, p)$ is $(1 - p + pe^u)^t$ (page 39 in [25]). We have

$$P(E_3^c[s, r]) = P\left(Z[s, r] \geq \mathbb{E}[Z[s, r]] + \frac{\xi}{6}\mathbb{E}[X[s, r]]\right) \quad (48)$$

$$\leq P\left(Z[s, r] \geq \mathbb{E}[Z[s, r]] + \frac{\xi}{12}\mathbb{E}[Z[s, r]] + \frac{\xi}{12}\mathbb{E}[X[s, r]]\right) \quad (49)$$

$$< \frac{\mathbb{E}[e^{Z[s, r]u}]}{e^{(1+\frac{\xi}{12})\mathbb{E}[Z[s, r]]u + \frac{\xi}{12}\mathbb{E}[X[s, r]]u}} \quad (50)$$

$$= \frac{(1 - p + pe^u)^{t(r-s)}}{e^{(1+\frac{\xi}{12})(r-s)tpu + \frac{\xi}{12}(r-s)qu}} \quad (51)$$

$$\leq e^{(e^u - 1 - u(1+\frac{\xi}{12}))tp(r-s) - \frac{\xi}{12}qu(r-s)}, \quad (52)$$

where (49) is due to Proposition 6, (50) holds for all $u \geq 0$ due to Chernoff's inequality, and (52) is due to $1 + x \leq e^x$ for every $x \geq 0$ (here $x = p(e^u - 1)$). Pick $u = \log(1 + \frac{\xi}{12})$. Then

$$P(E_3^c[s, r]) \leq e^{(\frac{\xi}{12} - (1+\frac{\xi}{12})\log(1+\frac{\xi}{12}))tp(r-s) - \frac{\xi}{12}\log(1+\frac{\xi}{12})q(r-s)} \quad (53)$$

$$< e^{-\frac{\xi}{12}\log(1+\frac{\xi}{12})q(r-s)} \quad (54)$$

$$< e^{-\frac{\xi^2}{180}q(r-s)} \quad (55)$$

where (54) is due to $(1+x)\log(1+x) > x$ for all $x > 0$, and (55) is due to $\log(1 + \frac{\xi}{12}) > \frac{\xi}{15}$ for all $0 < \xi \leq 1$.

Thus,

$$P(E[s, r]) = 1 - P(E^c[s, r]) \quad (56)$$

$$\geq 1 - P(E_1^c[s, r]) - P(E_2^c[s, r]) - P(E_3^c[s, r]) \quad (57)$$

$$> 1 - 4e^{-\eta(r-s)} \quad (58)$$

where η is defined in (39), (58) is due to $\frac{\xi^2}{72}(1 - \frac{\xi}{6}) > \frac{\xi^2}{180}$ and $\frac{\xi^2}{108} > \frac{\xi^2}{180}$. \square

Lemma 10. (*Typical properties lemma*) For all integers $1 \leq s < r$, under event $E[s, r]$, the following holds.

$$(1 - \frac{\xi}{6})q(r - s) < X[s, r] < (1 + \frac{\xi}{6})q(r - s) \quad (59)$$

$$Y[s, r] > (1 - \frac{\xi}{3})q(r - s) \quad (60)$$

$$Z[s, r] < (1 - \frac{2\xi}{3})q(r - s) \quad (61)$$

$$Z[s, r] < (1 - \frac{\xi}{2})X[s, r] \quad (62)$$

$$Z[s, r] < Y[s, r]. \quad (63)$$

Proof. Under $E[s, r]$, (59) follows directly from (34).

To prove (60),

$$Y[s, r] > (1 - \frac{\xi}{6})q(1 - q)(r - s) \quad (64)$$

$$> (1 - \frac{\xi}{6})^2 q(r - s) \quad (65)$$

$$> (1 - \frac{\xi}{3})q(r - s), \quad (66)$$

where (64) is due to Proposition 5 and (65) is due to $q \leq \frac{\xi}{6}$.

To prove (61), we have

$$Z[s, r] < E[Z[s, r]] + \frac{\xi}{6}E[X[s, r]] \quad (67)$$

$$\leq (1 - \xi)\frac{q}{1 - q}(r - s) + \frac{\xi}{6}q(r - s) \quad (68)$$

$$< (1 - \frac{2\xi}{3})q(r - s) \quad (69)$$

where (67) is due to (36), (68) is due to (30), and (69) is due to $q \leq \frac{\xi}{6}$.

To prove (62), we have

$$Z[s, r] < (1 - \frac{2\xi}{3})q(r - s) \quad (70)$$

$$< \frac{1 - \frac{2\xi}{3}}{1 - \frac{\xi}{6}}X[s, r] \quad (71)$$

$$< (1 - \frac{\xi}{2})X[s, r], \quad (72)$$

where (70) is due to (69) and (71) is due to (59).

The inequality (63) is straightforward by (61) and (60). \square

Definition 11. (*Typical event*) For all integers $1 \leq s < r$, define the typical event with respect to $[s, r]$ as

$$G[s, r] := \cap_{0 \leq a < s, b \geq 0} E[s - a, r + b]. \quad (73)$$

The event $G[s, r]$ occurs when the events $E[s - a, r + b]$ simultaneously occurs for all a, b , i.e., the “ E ” events occur over all intervals that contain $[s, r]$. The event G represents a collection of outcomes that constrain the number of blocks mined in all intervals that contain $[s, r]$, including arbitrarily large intervals that terminate in the arbitrarily far future. Intuitively, we have defined $G[s, r]$ to allow the “good” properties mentioned in Lemma 10 to extend to all intervals containing $[s, r]$ under the event. It is important to note that the typical events defined in [3], [9] requires the interval to be bounded by $b < r_{\max}$ where r_{\max} denotes a finite *execution horizon*. In contrast, the typical event is defined in this paper to allow for results for infinite horizon.

Lemma 12. For all integers $1 \leq s < r$,

$$P(G[s, r]) > 1 - 5\eta^{-2}e^{-\eta(r-s)}. \quad (74)$$

Proof. Due to the stationarity of X , Y and Z processes, $P(E[s, r]) = P(E[1, r - s + 1])$ for all s, r . Evidently the probability only depends on the length of the interval $r - s$.

$$P(G^c[s, r]) = P(\cup_{0 \leq a < s, b \geq 0} E^c[s - a, r + b]) \quad (75)$$

$$= P(\cup_{0 \leq a < s, b \geq 0} E^c[1, r - s + a + b + 1]) \quad (76)$$

$$\leq \sum_{0 \leq a < s, b \geq 0} P(E^c[1, r - s + a + b + 1]) \quad (77)$$

$$= \sum_{k=0}^{\infty} \sum_{0 \leq a < s, b \geq 0: a+b=k} P(E^c[1, r - s + k + 1]) \quad (78)$$

$$< \sum_{k=0}^{\infty} (k+1) P(E^c[1, r - s + k + 1]) \quad (79)$$

$$< \sum_{k=0}^{\infty} (k+1) 4e^{-\eta(r-s+k)} \quad (80)$$

$$= 4e^{-\eta(r-s)} \sum_{k=0}^{\infty} (k+1) e^{-\eta k} \quad (81)$$

$$= \frac{4}{(1 - e^{-\eta})^2} e^{-\eta(r-s)}. \quad (82)$$

According to (10) and (39), $\eta \leq \frac{1}{6} \cdot \frac{1}{180} = \frac{1}{1080}$. The lemma is thus established using the fact that $1 - e^{-x} \geq \sqrt{\frac{4}{5}}x$ for all $0 \leq x \leq \frac{1}{1080}$. \square

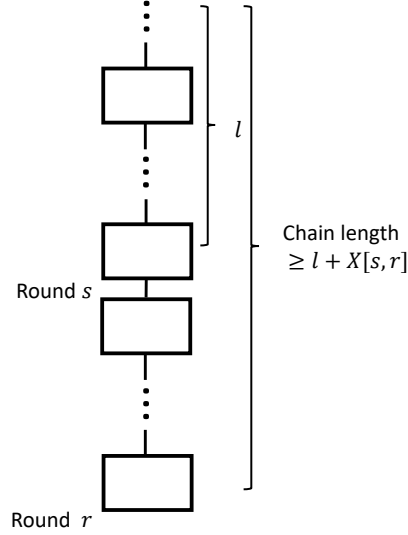


Fig. 1. Illustration for Lemma 15.

Lemma 13. *All honest blockchains must have identical length by every round.*

Proof. This is a simple consequence of the fact that all honest miners have seen the same blocks and every honest miner adopts the longest blockchain at the end of every round. \square

Lemma 14. (Lemma 6 in [3]) *Suppose some blockchain's k th block B is mined by an honest miner in a uniquely successful round. Then the k th block of every blockchain is either B or an adversarial block.*

Proof. Suppose the k th block of another blockchain is an honest block $B' \neq B$. Let r and r' denote the rounds in which B and B' are mined, respectively. Then we must have $r \neq r'$ by assumption that B is mined in a uniquely successful round. Since both B and B' are mined and adopted as the k th block by some honest miners, all other honest miners must have adopted a blockchain of length at least k by round $r^* = \min\{r+1, r'+1\}$. Hence, all honest blocks mined after round r^* will extend a blockchain longer than k . This contradicts the assumption that B and B' are both at position k of some miner's blockchain. Hence the proof of Lemma 14. \square

Lemma 15. (Lemma 7 in [3]) *Let $1 \leq s < r$ be integers. Suppose an honest blockchain is of length l by round s . Then by round r , the length of every honest blockchain is at least $l + X[s, r]$.*

Proof. By induction: Consider $r = s + 1$. All honest miners' blockchains are of identical length l by round s according to Lemma 13. If $X[s] = 0$, then $X[s, s + 1] = 0$. If $X[s] = 1$, at least one honest

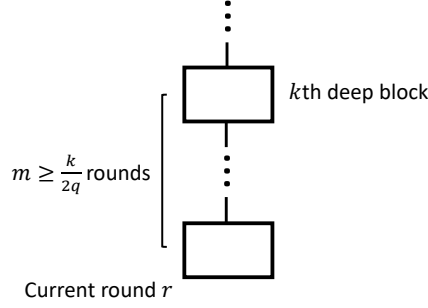


Fig. 2. Illustration for Lemma 16.

block is broadcast to all miners during round s . Then by round $s + 1$, each honest miner will adopt a blockchain of at least $l + 1$ blocks. Thus Lemma 15 is established for the cases of $r = s + 1$.

Assume by round r_1 , each honest miner's blockchain length is at least $l + X[s, r_1]$. If $X[r_1] = 0$, the claim holds trivially for round $r_1 + 1$. If $X[r_1] = 1$, at least one honest miner will have a blockchain of length no shorter than $l + X[s, r_1] + 1$ by round r_1 . Then according to Lemma 13, each honest miner will adopt a blockchain of length at least $l + X[s, r_1 + 1]$ by round $r_1 + 1$. By induction on r_1 , Lemma 15 holds. \square

Lemma 16. (*Blockchain growth lemma*) For all integers $1 \leq s < r$ and $k \geq 2q(r - s)$, under typical event $G[s, r]$, every honest miner's k -deep block by round r must be mined before round s .

Proof. The blockchain growth of an honest miner during rounds $\{s, \dots, r - 1\}$ is upper bounded by $X[s, r] + Z[s, r]$. Note that

$$X[s, r] + Z[s, r] < (1 + \frac{\xi}{6})q(r - s) + (1 - \frac{2\xi}{3})q(r - s) \quad (83)$$

$$< 2q(r - s) \quad (84)$$

$$\leq k, \quad (85)$$

where (83) is due to (59) and (61). Thus, the k -deep block must be mined before round s . \square

Theorem 17. (*Blockchain growth theorem*) Let r, s, s_1 be integers satisfying $1 \leq s_1 \leq s < r$. Then under typical event $G[s, r]$, the length of every honest blockchain must increase by at least $(1 - \frac{\xi}{6})q(r - s_1)$ during rounds $\{s_1, \dots, r\}$.

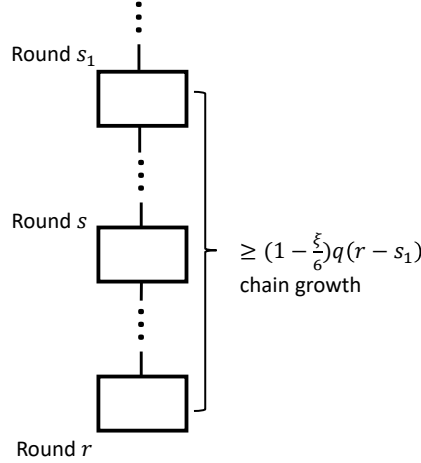


Fig. 3. Illustration for blockchain growth theorem.

Proof. Under $G[s, r]$,

$$X[s_1, r] > (1 - \frac{\xi}{6})\mathbb{E}[X[s_1, r]] \quad (86)$$

$$= (1 - \frac{\xi}{6})q(r - s_1) \quad (87)$$

where (87) is due to (59). According to Lemma 15, the blockchain growth for any honest miner is at least $X[s_1, r]$ during $[s_1, r]$. \square

Let $\text{len}(C)$ denote the length of a blockchain C .

Theorem 18. (*Blockchain quality theorem*) Let r, s, k be integers satisfying $1 \leq s < r$ and $k \geq 2q(r - s)$. Suppose an honest miner's blockchain has more than k blocks by round r . Under event $G[s, r]$, by round r , at least $\frac{\xi}{2}$ fraction of the last k blocks of this miner's blockchain are honest.

Proof. The intuition is that under typical event $G[s, r]$, an honest miner's blockchain grow by at least $X[s, r]$ according to Lemma 15. Meanwhile, the number of adversarial blocks mined is upper bounded by (62). Thus, at least $\frac{\xi}{2}$ fraction of blocks must be honest even in the worst case that all adversarial blocks are included in the blockchain.

To be precise, assume an honest miner adopts blockchain C by round r . Denote B_i as the i th block of blockchain C ($C = B_0 B_1 \dots B_{\text{len}(C)-1}$, where B_0 is the genesis block). By assumption, $\text{len}(C) > k$. Let $u = \text{len}(C) - k$. Then the last k blocks of C are $B_u \dots B_{\text{len}(C)-1}$. Let $B_{u'}$ be the last honest block before B_u . That is to say, $u' = \max\{u' | u' \leq u - 1, B_{u'} \text{ is honest}\}$ (u' is always well defined as B_0 is regarded

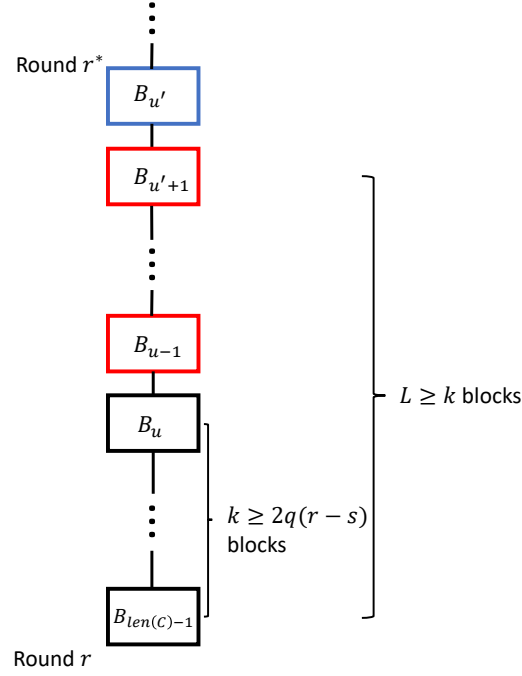


Fig. 4. Illustration to prove blockchain quality theorem.

as honest). Let r^* be the round when $B_{u'}$ is mined. By Lemma 16, $r^* < s$. Let $L = \text{len}(C) - u' - 1$. Note that $L \geq k$. These definitions are illustrated in Figure 4.

Let x be the number of honest blocks in $B_u \dots B_{\text{len}(C)-1}$. To prove the theorem, it suffices to show $x > \frac{\xi}{2}k$. Since all blocks in $B_{u'+1} \dots B_{u-1}$ are adversarial, the number of honest blocks in $B_{u'+1} \dots B_{\text{len}(C)-1}$ is also x . Thus, the number of adversarial blocks in $B_{u'+1} \dots B_{\text{len}(C)-1}$ is $L - x$. Under $G[s, r]$, which implies that $E[r^* + 1, r]$ also occurs, we have

$$L - x \leq Z[r^* + 1, r] \quad (88)$$

$$< (1 - \frac{\xi}{2})X[r^* + 1, r] \quad (89)$$

$$\leq (1 - \frac{\xi}{2})L \quad (90)$$

$$\leq L - \frac{\xi}{2}k, \quad (91)$$

where (89) is due to (62), (90) is due to Lemma 15, and (91) is due to $L \geq k$. From (91), $x > \frac{\xi}{2}k$ is derived. \square

Let $C^{\lceil k}$ denote the k -deep prefix of blockchain C . If $\text{len}(C) \leq k$, let $C^{\lceil k}$ be the genesis block.

Definition 19. Let G be an event and r be a positive integer. A block or a sequence (of blocks) is said to be permanent after round r under G if, under event G , the block or sequence remains in all honest blockchains starting from round r .

Definition 20. Let r be a positive integer. A block or a sequence (of blocks) is said to be ϵ -permanent after round r if, there exists an event G with $P(G) > 1 - \epsilon$ such that the block or sequence is permanent after round r under G .

Lemma 21. If a block or a sequence is ϵ -permanent after round r , then it is also ϵ -permanent after round s for every $s > r$.

Theorem 22. (Common prefix theorem) Let r, s, k be integers satisfying $1 \leq s < r$ and $k \geq 2q(r - s)$. If by round r an honest blockchain has a k -deep prefix, then the prefix is permanent after round r under $G[s, r]$.

Proof. The intuition is based on Lemma 14: Once a block is mined in a uniquely successful round, a different block on any other blockchain at the same position must be adversarial. If some adversarial miners wish to fork the blockchain, they must generate at least one adversarial block during every uniquely successful round after the common prefix. This can not be true because according to (63), the number of uniquely successful rounds must be greater than the number of adversarial blocks under the typical event.

To be precise, we prove the desired result by contradiction. Suppose blockchain C_1 whose length is great than k is adopted by an honest miner P_1 by round r . Contrary to the claim, assume $r_2 > r$ is the smallest round by which an honest miner P_2 adopts a blockchain C_2 such that $C_1^{[k]} \not\subseteq C_2$. Let C'_2 be the blockchain P_2 adopted by round $r_2 - 1$. Note that $C_1^{[k]} \subseteq C'_2$.

Assume the last honest block on the common prefix of C'_2 and C_2 is mined during round r^* . If $r^* > 0$, this common block of C'_2 and C_2 must be more than k deep in C_1 by round r . According to Lemma 16, we have $r^* < s$, so that

$$[s, r] \subset [r^* + 1, r_2 - 1]. \quad (92)$$

On the other hand, if $r^* = 0$, the last common block is the genesis block. Since $s \geq 1$, (92) also holds. An illustration of these chains and parameters is given in Figure 5.

By assumption $G[s, r]$, $E_2[s, r]$ also occurs, so that $Y[s, r] > 0$ according to (35). Hence, there must be at least one uniquely successful round $u \in \{r^* + 1, \dots, r_2 - 2\}$. According to Lemma 13, all honest miners have the same chain length. Let l_u denote one plus the length of the honest miners' blockchains

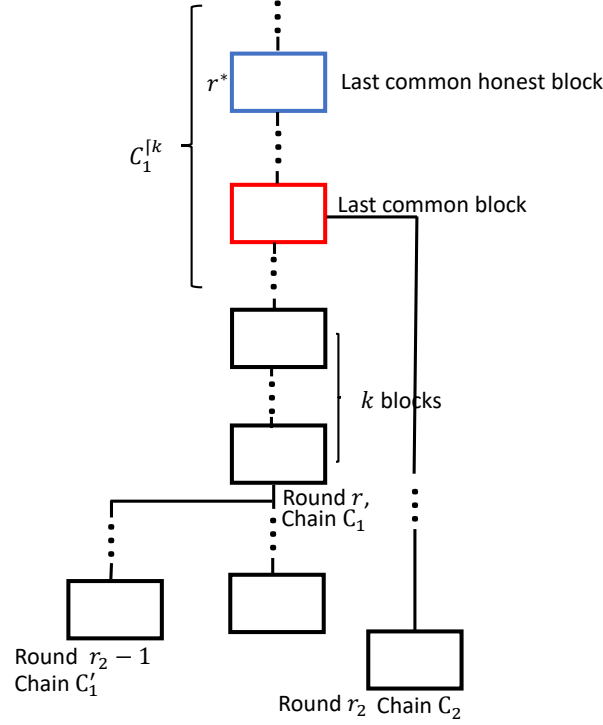


Fig. 5. Illustration to prove common prefix theorem.

by round u . Suppose honest miner P mines B_u during round u . According to Lemma 14, the l_u th block of every blockchain is either B_u or an adversarial block. Because C_2 and C'_2 are adopted by an honest miner after round $r_2 - 2$, they must be no shorter than $\max\{l_u : u \text{ is a uniquely successful round in } \{r^* + 1, \dots, r_2 - 2\}\}$.

For every uniquely successful round u in $\{r^* + 1, \dots, r_2 - 2\}$, if the l_u th blocks of C_2 and C'_2 are different, then at least one of them must be adversarial according to Lemma 14. On the other hand, if the l_u th block of C_2 and C'_2 are identical, the block must be in their common prefix, which must be adversarial by definition of r^* . Thus, at least one adversarial block is mined during each uniquely successful round, so that $Z[r^* + 1, r_2 - 1] \geq Y[r^* + 1, r_2 - 1]$. However, since $[s, r] \subset [r^* + 1, r_2 - 1]$, $E[r^* + 1, r_2 - 1]$ occurs under $G[s, r]$, so that $Z[r^* + 1, r_2 - 1] < Y[r^* + 1, r_2 - 1]$ according to (63). Contradiction arises. Hence the proof of the theorem. \square

IV. THE PRISM BACKBONE PROTOCOL

The Prism protocol is invented and fully described in [9]. Here we describe the Prism backbone with just enough details to facilitate its analysis. We assume $m + 1$ genesis blocks are generated for the same number of blockchains during round 0 by honest miners. Blockchain 0 is referred to as the proposer

blockchain. The remaining blockchains are voter blockchains. A block is mined before knowing which blockchain it will be part of. Sortition relies on the range the nonce's hash lands in: If a miner find a nonce whose hash is within $[j\alpha, j\alpha + \alpha)$ for $j = 0, 1, \dots, m$, the mined block belongs to blockchain i . Mining difficulty can be adjusted by changing parameter α . This sortition scheme ensures the mining power of both honest and adversarial miners are evenly distributed across different voting blockchains and the proposer blockchain.

To certify its level, a new honest voter block for blockchain j ($j = 1, 2, \dots, m$) points to blockchain j 's maximum-level block by a *parent link* (ties are broken by predefined rules). To certify its level, an honest new proposer block includes the hash of a maximum-level block in the proposer blockchain and point to it by a *reference link*. In addition, an honest new proposer includes one reference link to every existing block in both proposer and voter blockchains that has not been pointed to by other reference links.

Following the bitcoin protocol, an honest miner decides each main voter blockchain by the longest blockchain rule. The miner determines the its main blockchain by votes from the main voter blockchains. Let B be an honest block on a voter blockchain j . By B 's ancestors we mean all blocks on B 's path to the blockchain genesis block following parent links. By saying B votes for a level l , we mean B chooses one proposer block among all proposer blocks at level l according to a predefined rule, and points to its choice with a reference link. An honest voter block votes for all levels which have not been voted by its ancestors.

A voter blockchain is allowed to vote only once for each level (more votes from the same voter blockchain are discarded). That is to say, proposer blocks on the same level receive m votes in total. At each level, the proposer block with most votes is elected as a leader block, with ties broken by a predefined rule. The sequence of leader blocks over all levels is called the leader sequence.

A miner generates its final ledger based on its leader sequence. Given a leader sequence $B_0 B_1 \dots B_l$, each leader block B_i defines an epoch. Added to the ledger are the blocks which are pointed to by B_i , as well as other blocks reachable from B_i but have not been included in previous epochs. The list of blocks are sorted topologically, with ties broken by their contents. Since the blocks referenced are mined independently, there can be double spends or redundant transactions. An end user can create a valid ledger by keeping only the first transaction among double spends or redundant transactions.

For $j = 0, 1, \dots, m$ and $r = 1, 2, \dots$, let $H_j[r]$ denote the total number of honest blocks mined during round r for blockchain j . Following the definitions in Section III, for $j = 0, 1, \dots, m$ and $r = 1, 2, \dots$,

we also define

$$X_j[r] = \begin{cases} 1, & \text{if } H_j[r] \geq 1 \\ 0, & \text{otherwise,} \end{cases} \quad (93)$$

$$Y_j[r] = \begin{cases} 1, & \text{if } H_j[r] = 1 \\ 0, & \text{otherwise,} \end{cases} \quad (94)$$

and let $Z_j[r]$ be the total number adversarial blocks mined for blockchain j during round r .

Definition 23. For all integers $1 \leq s < r$ and $0 \leq j \leq m$, define event

$$E_j[s, r] := E_{1,j}[s, r] \cap E_{2,j}[s, r] \cap E_{3,j}[s, r] \quad (95)$$

where

$$E_{1,j}[s, r] := \left\{ \left(1 - \frac{\xi}{6}\right)\mathbb{E}[X_j[s, r]] < X_j[s, r] < \left(1 + \frac{\xi}{6}\right)\mathbb{E}[X_j[s, r]] \right\} \quad (96)$$

$$E_{2,j}[s, r] := \left\{ \left(1 - \frac{\xi}{6}\right)\mathbb{E}[Y_j[s, r]] < Y_j[s, r] \right\} \quad (97)$$

$$E_{3,j}[s, r] := \left\{ Z_j[s, r] < \mathbb{E}[Z_j[s, r]] + \frac{\xi}{6}\mathbb{E}[X_j[s, r]] \right\}. \quad (98)$$

We note that for integers $0 \leq j \leq m$ and $r \geq 1$, $H_j[r]$, $X_j[r]$, $Y_j[r]$, and $Z_j[r]$ here are identically distributed as $H[r]$, $X[r]$, $Y[r]$, and $Z[r]$ defined in Section III. Also, for $1 \leq s < r$, $E_j[s, r]$ is defined in the same manner as $E[s, r]$. Thus, the proposer blockchain and all voter blockchains satisfy similar properties as in Lemma 10:

Lemma 24. (Typical properties lemma for proposer and voter blockchain) For all integers $1 \leq s < r$ and $0 \leq j \leq m$, under event $E_j[s, r]$, the following holds:

$$\left(1 - \frac{\xi}{6}\right)q(r - s) < X_j[s, r] < \left(1 + \frac{\xi}{6}\right)q(r - s) \quad (99)$$

$$Y_j[s, r] > \left(1 - \frac{\xi}{3}\right)q(r - s) \quad (100)$$

$$Z_j[s, r] < \left(1 - \frac{2\xi}{3}\right)q(r - s) \quad (101)$$

$$Z_j[s, r] < \left(1 - \frac{\xi}{2}\right)X_j[s, r] \quad (102)$$

$$Z_j[s, r] < Y_j[s, r]. \quad (103)$$

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof as that for Lemma 10. \square

Definition 25. For all integers $1 \leq s < r$ and $0 \leq j \leq m$, define blockchain j 's typical event with respect to $[s, r]$ as

$$G_j[s, r] := \cap_{0 \leq a < s, b \geq 0} E_j[s - a, r + b]. \quad (104)$$

Lemma 26. For all integers $1 \leq s < r$ and $0 \leq j \leq m$,

$$P(G_j[s, r]) > 1 - 5\eta^{-2}e^{-\eta(r-s)} \quad (105)$$

where η is defined in (39).

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof as that for Lemma 12. \square

Since the proposer blockchain and all voter blockchains grow in the same manner as how a bitcoin blockchain grows, the blockchain growth lemma and blockchain growth theorem remain valid:

Lemma 27. Let $1 \leq s < r$ and $0 \leq j \leq m$ be integers. Suppose an honest voter blockchain j is of length l by round s . Then by round r , the length of every honest voter blockchain j is at least $l + X_j[s, r]$.

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof as that for Lemma 15. \square

Lemma 28. (Blockchain growth lemma for voter and proposer blockchain) For all integers $1 \leq s < r$, $k \geq 2q(r - s)$ and $0 \leq j \leq m$, under typical event $G_j[s, r]$, every honest miner's k -deep block of blockchain j by round r must be mined before round s .

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof as that for Lemma 16. \square

Theorem 29. (Blockchain growth theorem for voter and proposer blockchain) Let r, s, s_1 be integers satisfying $1 \leq s_1 \leq s < r$. Let j be an integer satisfying $0 \leq j \leq m$. Then under typical event $G_j[s, r]$, the length of every honest miner's blockchain j must grow by at least $(1 - \frac{\xi}{6})q(r - s_1)$ during rounds $\{s_1, \dots, r\}$.

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof as that for Theorem 17. \square

Since the protocol for voter blockchains is identical to that of bitcoin, the blockchain quality theorem and the common prefix theorem hold for all voter blockchains.

Theorem 30. (*Blockchain quality theorem for voter blockchain*) Let r, s, k, j be integers satisfying $1 \leq s < r$, $k \geq 2q(r - s)$ and $1 \leq j \leq m$. Suppose an honest blockchain has more than k blocks by round r . Under event $G_j[s, r]$, at least $\frac{\xi}{2}$ fraction of the last k blocks of this blockchain j are honest.

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof as that for Theorem 18. \square

Theorem 31. (*Common prefix theorem for voter blockchain*) Let r, s, k, j be integers satisfying $1 \leq s < r$, $k \geq 2q(r - s)$ and $1 \leq j \leq m$. If by round r an honest voter blockchain j has a k prefix, then the prefix is permanent after round r under $G_j[s, r]$.

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof as that for Theorem 22. \square

Since the leader sequence of the proposer blockchain is decided by votes instead of the longest blockchain rule, the blockchain quality theorem and common prefix theorem do not immediately extend to the leader sequence of the proposer blockchain.

Definition 32. We define R_l as the round in which the first proposer block on level l is mined. We also define

$$\epsilon_k = 6m\eta^{-2}e^{-\eta\frac{k}{2q}}, \quad k = 1, 2, \dots \quad (106)$$

where η is given by (39).

Definition 33. We let $\mathbf{LedSeq}_l(r)$ denote the proposer blockchain's leader sequence up to level l by round r .

Lemma 34. Consider a given level l . Let k be a positive integer. If by some round $r > \max\left\{\frac{k}{2q}, R_l + 1\right\}$, every voter blockchain contains at least one honest block mined after round R_l which is at least k -deep, then $\mathbf{LedSeq}_l(r)$ is ϵ_k -permanent after round r .

Proof. Let

$$s = r - \left\lfloor \frac{k}{2q} \right\rfloor, \quad (107)$$

which must be a positive integer because $2qr > k$. Define

$$G = \cap_{j=1,2,\dots,m} G_j[s, r]. \quad (108)$$

For $j = 1, \dots, m$, let B_j denote an honest block on an honest voter blockchain j which is mined after round R_l and is at least k -deep by round r . According to Theorem 31, B_j and its ancestors are permanent after round r under $G_j[s, r]$. Hence, B_1, \dots, B_m and all their ancestors must be permanent

after round r under G . Thus, all voter blockchains' voting are permanent. Since B_1, \dots, B_m are honest, they would have voted for all levels up to level l of the proposer blockchain by the voting rule. Hence, the leader block sequence up to level l is permanent after round r under G . Note that

$$P(G) = 1 - P(\cup_{j=1,2,\dots,m} G_j^c[s, r]) \quad (109)$$

$$\geq 1 - \sum_{j=1}^m P(G_j^c[s, r]) \quad (110)$$

$$= 1 - mP(G_1^c[s, r]) \quad (111)$$

$$> 1 - 5m\eta^{-2}e^{-\eta(r-s)}, \quad (112)$$

where (110) is due to the union bound, (111) is due to symmetry of all voter blockchains, (112) is due to Lemma 26. By (107), we have $2q(r-s+1) > k$, so that (112) becomes

$$P(G) > 1 - 5m\eta^{-2}e^{-\eta\frac{k}{q}+\eta} \quad (113)$$

$$> 1 - 6m\eta^{-2}e^{-\eta\frac{k}{2q}} \quad (114)$$

$$= 1 - \epsilon_k \quad (115)$$

where (114) is due to $e^\eta < \frac{6}{5}$. Thus, the leader block sequence up to level l is ϵ_k -permanent after round r . \square

Lemma 35. *If positive integers R , r , and k satisfy*

$$r \geq \frac{2(k+1)}{(1-\frac{\xi}{6})\xi q} + 1, \quad (116)$$

then right before round $R+r$, with probability at least $1 - \epsilon_k$, all honest voter blockchains have an honest block mined after round R which is at least k deep.

Proof. Let

$$\ell = \left\lceil \frac{2k}{\xi} \right\rceil. \quad (117)$$

Let

$$s_1 = \left\lfloor \frac{k}{q\xi} \right\rfloor. \quad (118)$$

Then

$$\ell \geq \frac{2k}{\xi} \quad (119)$$

$$\geq 2q \left\lfloor \frac{k}{q\xi} \right\rfloor \quad (120)$$

$$= 2qs_1. \quad (121)$$

According to the Theorem 29, under event $G_j[R, R+r]$, an honest voter blockchain j 's growth during $\{R, R+1, \dots, R+r-1\}$ is at least

$$(1 - \frac{\xi}{6})qr \geq \frac{2k}{\xi} + 1 \quad (122)$$

$$> \ell, \quad (123)$$

where (122) is due to (116) and (123) is due to (117).

According to Theorem 30 and (121), under event $G_j[R+r-s_1, R+r]$, at least $\frac{\xi}{2}$ fraction of the last ℓ blocks of this voter blockchain j are honest. Because $\frac{\xi}{2}\ell \geq k$, the earliest of these honest blocks must be at least k deep.

By (116) and (118), it is easy to see that $s_1 \leq r$. Hence $G_j[R+r-s_1, R+r] \subset G_j[R, R+r]$. Define

$$G = \cap_{j=1,2,\dots,m} G_j[R+r-s_1, R+r]. \quad (124)$$

Under event G , by round $R+r$, every honest voter blockchain has an honest block mined after round R which is at least k deep. The probability of the typical event can be lower bounded:

$$P(G) = P(\cap_{j=1,2,\dots,m} G_j[R+r-s_1, R+r]) \quad (125)$$

$$= 1 - P(\cup_{j=1,2,\dots,m} G_j^c[R+r-s_1, R+r]) \quad (126)$$

$$\geq 1 - mP(G_1^c[R+r-s_1, R+r]) \quad (127)$$

$$> 1 - 5m\eta^{-2}e^{-\eta s_1} \quad (128)$$

$$> 1 - 6m\eta^{-2}e^{-\eta s_1}, \quad (129)$$

where (127) is due to the union bound and symmetry of all voter blockchains and (128) is due to Lemma 26. Moreover,

$$qs_1 > q \left(\frac{k}{q\xi} - 1 \right) \quad (130)$$

$$= \frac{k}{\xi} - q \quad (131)$$

$$> k - \frac{1}{6} \quad (132)$$

$$> \frac{k}{2}, \quad (133)$$

where (130) is due to (118). Therefore,

$$P(G) > 1 - 6m\eta^{-2}e^{-\eta \frac{k}{2q}} \quad (134)$$

$$= 1 - \epsilon_k, \quad (135)$$

In summary, by round $R + r$, with probability at least $1 - \epsilon_k$, all honest voter blockchains have an honest block mined after round R which is at least k deep. \square

Theorem 36. Fix $\epsilon \in (0, 1)$. Let R_l be the round during which the first proposer block on level l is mined. For every integer

$$r \geq \frac{5}{(1 - \frac{\xi}{6})\xi\eta} \log \frac{12m\eta^{-2}}{\epsilon}, \quad (136)$$

the leader sequence up to level l is ϵ -permanent after round $R_l + r$.

Proof. Let

$$k = \left\lceil \frac{2q}{\eta} \log \frac{12m\eta^{-2}}{\epsilon} \right\rceil, \quad (137)$$

and

$$s = \left\lceil \frac{2(k+1)}{(1 - \frac{\xi}{6})\xi q} + 1 \right\rceil. \quad (138)$$

Let ϵ_k be as defined as in (106).

According to Lemma 35 and (138), by round $R_l + s$, all honest voter blockchains have an honest block which is mined after R_l and is at least k deep with probability at least $1 - \epsilon_k$. Under this event, according to Lemma 34 (evidently, $R_l + s > \frac{k}{2q}$), the leader sequence up to level l is ϵ_k -permanent after round $R_l + s$. Therefore, the leader sequence up to level l is $2\epsilon_k$ -permanent after round $R_l + s$. Note that

$$\epsilon_k = 6m\eta^{-2} e^{-\eta \frac{k}{2q}} \quad (139)$$

$$\leq 6m\eta^{-2} e^{-\log \frac{12m\eta^{-2}}{\epsilon}} \quad (140)$$

$$= \frac{\epsilon}{2}. \quad (141)$$

the leader sequence up to level l is ϵ -permanent after round $R_l + s$.

From (137), it is easy to verify that $k > 10$. As a consequence, we have

$$s < \frac{2(k+1)}{(1 - \frac{\xi}{6})\xi q} + 2 \quad (142)$$

$$= \frac{2k + 2 + 2(1 - \frac{\xi}{6})\xi q}{(1 - \frac{\xi}{6})\xi q} \quad (143)$$

$$< \frac{\frac{5}{2}(k-1)}{(1 - \frac{\xi}{6})\xi q} \quad (144)$$

$$< \frac{5}{(1 - \frac{\xi}{6})\xi\eta} \log \frac{12m\eta^{-2}}{\epsilon} \quad (145)$$

$$\leq r, \quad (146)$$

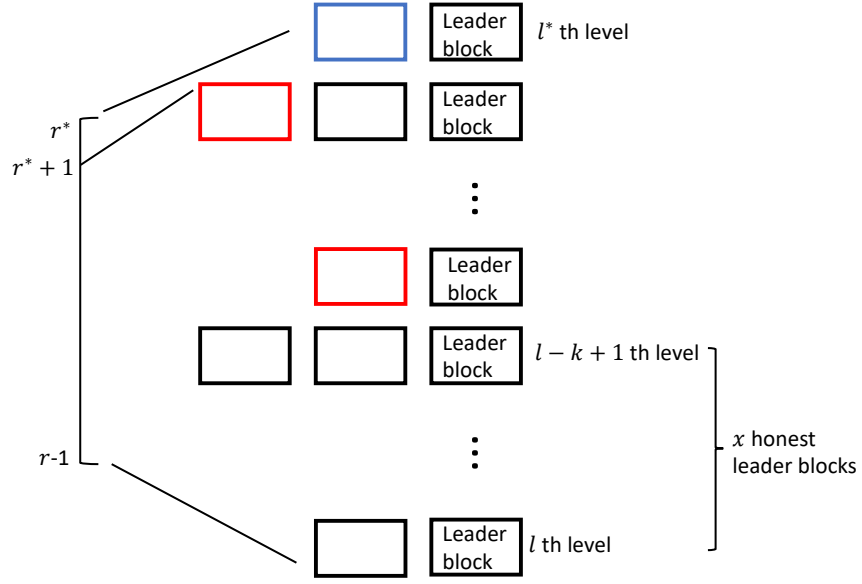


Fig. 6. Illustration to prove blockchain quality theorem for proposer blockchain.

where (142) is due to (137), (144) is due to $k > 10$, (145) is due to (137), and (146) is by (136).

Since $r > s$, the leader sequence up to level l is ϵ -permanent after round $R_l + r$ by Lemma 21. \square

Theorem 37. (*Blockchain quality theorem for proposer blockchain*) Let r, s, k be integers satisfying $1 \leq s < r$ and $k \geq 2q(r-s)$. Suppose an honest proposer blockchain has more than k leader blocks by round r . Under event $G_0[s, r]$, by round r , at least $\frac{\xi}{2}$ fraction of the last k leader blocks of the proposer blockchain are honest.

Proof. Let l denote the highest level of the proposer blockchain by round r . Evidently $l > k$. Let l^* be the highest level before $l-k+1$ on which the first proposer block is honest. l^* may be as high as $l-k$ and as low as 0, which corresponds to the genesis block. Let r^* be the round when the first block on level l^* is mined. If this block is the genesis block, then $r^* = 0$. If $r^* > 0$, since blocks on level l^* are more than k blocks away from the last level by round r , we have $r^* < s$ according to Lemma 28. In any cases, we have $[s, r] \subset [r^*+1, r]$. An illustration of the said proposer blocks and blockchain is given in Figure 6.

Since the first proposer block on every level within $\{l^*+1, \dots, l-k\}$ is adversarial, from level l^*+1 to level l , there must be at least one adversarial block on every level except (possibly) on the levels between $l-k+1$ and l where the leading block is honest. Let x be the number of honest leader blocks on levels $\{l-k+1, \dots, l\}$. Then during rounds $\{r^*+1, \dots, r-1\}$, the total number of adversarial

proposer blocks is no fewer than $l - l^* - x$, i.e.,

$$Z_0[r^* + 1, r] \geq l - l^* - x. \quad (147)$$

Under $G_0[s, r]$, $E_0[r^* + 1, r]$ occurs. Thus,

$$x \geq l - l^* - Z_0[r^* + 1, r] \quad (148)$$

$$> l - l^* - (1 - \frac{\xi}{2})X_0[r^* + 1, r] \quad (149)$$

$$\geq \frac{\xi}{2}(l - l^*) \quad (150)$$

$$\geq \frac{\xi}{2}k, \quad (151)$$

where (149) is due to (102), (150) is due to Lemma 27, and (151) is due to $l - l^* \geq k$. To sum up, we have $x > \frac{\xi}{2}k$ and the proof is complete. \square

Definition 38. A transaction tx is honest if it has been broadcast, and no other transaction spending from the same unspent output has been broadcast.

Note that the notion of honesty is applicable only to transactions which have been broadcast.

Definition 39. A transaction is said to be ϵ -permanent after round r if, with probability at least $1 - \epsilon$, it remains on the final ledger of every honest miner after round r .

Lemma 40. Suppose right before round r , the leader block on level l is honest. Suppose this leader block is mined during round R . If an honest transaction enters a block and the block is broadcast by round R , then every honest miner's final ledger generated by $\text{LedSeq}_l(r)$ will include this honest transaction.

Proof. Suppose the honest transaction tx enters block B which is broadcast by round R . Note that B may be honest or adversarial, a voter block or a leader block, and it can be on the main blockchain or an orphan block. Denote the honest leader block on level l as B_l .

By saying block B is reachable from block A , we mean A can points to B by a sequence of reference links. According to the Prism protocol, all blocks which are reachable from an honest leader block will be included in the final ledger. By round R , one of the following three cases must be true:

1) B is not reachable by any blocks. According to the Prism protocol, B_l will reference B , so B will be included in the final ledger.

2) B is reachable from an honest leader block whose level is smaller than l , then B must already be included in the final ledger.

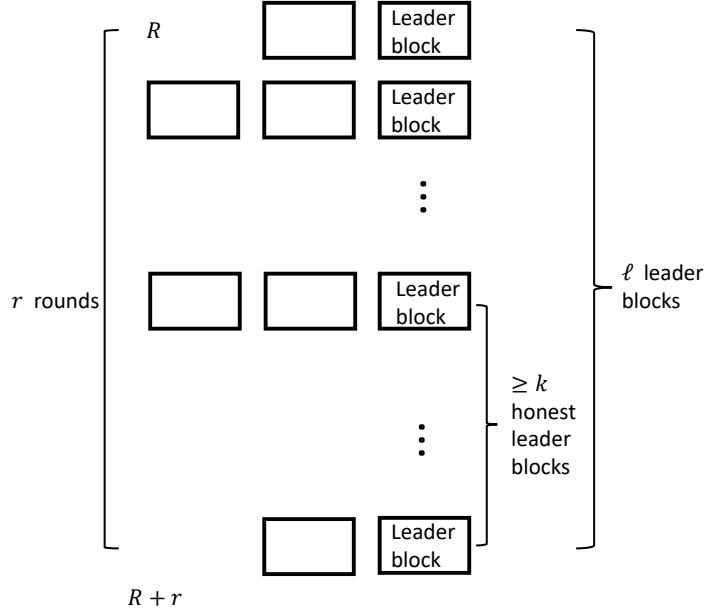


Fig. 7. Illustration to prove Theorem 41

3) B is reachable from some block(s), but none of these block(s) is an honest leader block whose level is smaller than l . Note that the number of proposer blocks by round R is finite, and that reference links cannot form a circle. Thus, among all the proposer blocks which can reach B , there must be at least one proposer block which is not referenced by any other block by round R . Denote such a block as B_r . Then according to the Prism protocol, B_l will reference B_r . As a sequence, B will be included in the final ledger.

Once B is included in the ledger, the honest transaction tx will not be discarded. \square

Theorem 41. For every $\epsilon > 0$ and every integer

$$r \geq \frac{25}{(1 - \frac{\xi}{6})^2 \xi^2 \eta} \log \frac{24m\eta^{-2}}{\epsilon}, \quad (152)$$

every transaction that is on an honest blockchain r rounds after its block is broadcast is ϵ -permanent.

Proof. Let

$$\ell = \left\lceil \left(1 - \frac{\xi}{6}\right)qr \right\rceil \quad (153)$$

$$k = \left\lfloor \frac{\xi}{2}\ell \right\rfloor \quad (154)$$

$$w = \left\lfloor \frac{\ell}{2q} \right\rfloor \quad (155)$$

$$u = \left\lfloor \frac{k}{2q} \right\rfloor. \quad (156)$$

Let R be the round during which the block including the honest transaction is broadcast. Define

$$G = G_0[R + r - u, R + r] \cap G_0[R + r - w, R + r] \cap G_0[R, R + r]. \quad (157)$$

Note that 1) According to Theorem 29 and (153), under $G_0[R, R + r]$, the proposer blockchain grows by at least ℓ leader blocks during rounds $\{R, \dots, R + r\}$. 2) According to Theorem 37, under event $G_0[R + r - w, R + r]$, by round $R + r$ the last ℓ leader blocks includes at least $\frac{\xi}{2}$ fraction of honest ones. Since $k \leq \frac{\xi}{2}\ell$, at least k out of the last ℓ leader blocks are honest. 3) According to Lemma 28, under event $G_0[R + r - u, R + r]$, the deepest one of these k honest leader blocks is mined at least $\frac{k}{2q}$ rounds before round $R + r$. 4) We have

$$\frac{k}{2q} \geq \frac{1}{2q} \left\lfloor \frac{\xi}{2}\ell \right\rfloor \quad (158)$$

$$\geq \frac{1}{2q} \left\lfloor \frac{\xi}{2} \left(1 - \frac{\xi}{6}\right)qr \right\rfloor \quad (159)$$

$$\geq \frac{1}{2q} \left\lfloor \frac{\xi}{2} \left(1 - \frac{\xi}{6}\right)q \frac{25}{(1 - \frac{\xi}{6})^2 \xi^2 \eta} \log \frac{24m\eta^{-2}}{\epsilon} \right\rfloor \quad (160)$$

$$\geq \frac{1}{2q} \left\lfloor \frac{25q}{2(1 - \frac{\xi}{6})\xi\eta} \log \frac{24m\eta^{-2}}{\epsilon} \right\rfloor \quad (161)$$

$$> \frac{1}{2q} \left(\frac{25q}{2(1 - \frac{\xi}{6})\xi\eta} \log \frac{24m\eta^{-2}}{\epsilon} - 1 \right) \quad (162)$$

$$> \frac{1}{2q} \left(\frac{10q}{(1 - \frac{\xi}{6})\xi\eta} \log \frac{24m\eta^{-2}}{\epsilon} \right) \quad (163)$$

$$= \frac{5}{(1 - \frac{\xi}{6})\xi\eta} \log \frac{12m\eta^{-2}}{\frac{\epsilon}{2}}, \quad (164)$$

where (158) is due to (154), (159) is due to (153), and (163) is obvious due to $\xi \in (0, 1]$. According to Theorem 36 and (164), the deepest honest leader block is $\frac{\epsilon}{2}$ -permanent after round $R + r$ under event G . Next, we will lower bound probability of G .

Note that

$$u \leq \frac{k}{2q} \quad (165)$$

$$\leq \frac{\xi \ell}{4q} \quad (166)$$

$$< \frac{\ell}{2q} - 1 \quad (167)$$

$$< w, \quad (168)$$

where (166) is due to (154), (167) is due to $q \leq \frac{\xi}{6}$, and (168) is due to (155). Also,

$$w \leq \frac{\ell}{2q} \quad (169)$$

$$\leq r, \quad (170)$$

where (169) is due to (155) and (170) is due to (153). We have $u < w < s$. According to definition, $G_0[R + r - u, R + r] \subset G_0[R + r - w, R + r] \subset G_0[R, R + r]$. Then,

$$P(G) = P(G_0[R + r - u, R + r]) \quad (171)$$

$$> 1 - 5\eta^{-2}e^{-\eta u} \quad (172)$$

$$> 1 - 5\eta^{-2}e^{-\eta(\frac{k}{2q}-1)} \quad (173)$$

$$\geq 1 - 5\eta^{-2}e^{-\frac{5}{(1-\frac{\xi}{6})\xi} \log \frac{24m\eta^{-2}}{\epsilon} + \eta} \quad (174)$$

$$> 1 - 5\eta^{-2}e^{-\log \frac{10m\eta^{-2}}{\epsilon}} \quad (175)$$

$$\geq 1 - 5\eta^{-2}e^{-\log \frac{10\eta^{-2}}{\epsilon}} \quad (176)$$

$$= 1 - \frac{\epsilon}{2}, \quad (177)$$

where (172) is due to Lemma 26, (173) is due to (156), (174) is due to (164), (175) is due to $0 < \xi \leq 1$, and (176) is due to $m \geq 1$. According to the union rule, the deepest honest leader block is ϵ -permanent after round $R + r$. According to Lemma 40, the honest transaction will become a ϵ -permanent transaction after round $R + r$. \square

V. BOUNDED-DELAY MODEL

A. The bitcoin protocol in bounded-delay model

In this section we generalize the results to the bounded-delay model, in which there is an upper bound T on the delay for message delivery. That is to say, if a block is broadcast to the network during round

r , by round $r + T$, all other miners would have received the block. In the special case of $T = 1$, this model degenerates to the synchronous model described in Section II.

Let $H[r]$, $X[r]$, $Y[r]$ and $Z[r]$ be defined in the same way as that in synchronized model. In particular, $H[r]$ stands for the number of honest blocks mined during round r for $r = 1, 2, \dots$. A round is said to be a T -left-isolated successful round if a single honest block is mined during this round and no other honest block is mined in the previous $T - 1$ rounds. Accordingly, we define the following indicators for $r = T, T + 1, T + 2, \dots$:

$$X'[r] = \begin{cases} 1, & \text{if } H[r] = 1 \text{ and } H[r - 1] = H[r - 2] = \dots = H[r - T + 1] = 0, \\ 0, & \text{otherwise.} \end{cases} \quad (178)$$

Proposition 42. For every $r = T, T + 1, \dots$,

$$\mathbb{E}[X'[r]] > q(1 - q)^T \quad (179)$$

$$> q(1 - Tq). \quad (180)$$

Proof. (179) is due to (13) and Proposition 5 and (180) is due to Bernoulli's inequality (11). \square

A round is said to be a T -doubly-isolated successful round if a single honest block is mined during this round and no other honest block is mined within $T - 1$ rounds before or after the round. Accordingly, we define the following indicators for $r = T, T + 1, T + 2, \dots$:

$$Y'[r] = \begin{cases} 1, & \text{if } H[r] = 1, H[r - 1] = H[r - 2] = \dots = H[r - T + 1] = 0, \\ & \text{and } H[r + 1] = H[r + 2] = \dots = H[r + T - 1] = 0, \\ 0, & \text{otherwise.} \end{cases} \quad (181)$$

Proposition 43. For every $r = T, T + 1, \dots$,

$$\mathbb{E}[Y'[r]] > q(1 - q)^{2T-1} \quad (182)$$

$$> q(1 - (2T - 1)q). \quad (183)$$

Proof. Note that $H[r] = 1$ indicates $Y[r] = 1$, $H[r] = 0$ indicates $X[r] = 0$. Then, (182) is due to (13) and Proposition 5, and (183) is due to Bernoulli's inequality (11). \square

From this point onward, it is assumed that the mining difficulty is adjusted to be sufficiently low such that the probability that one or more honest blocks are mined in a slot satisfies

$$q \leq \frac{\xi}{20T}. \quad (184)$$

Proposition 44. For every $r = T, T + 1, \dots$,

$$\mathbb{E}[Z[r]] < \mathbb{E}[X'[r]]. \quad (185)$$

Proof.

$$\mathbb{E}[Z[r]] = pt \quad (186)$$

$$= \frac{t}{n-t} p(n-t) \quad (187)$$

$$= (1-\xi)p(n-t) \quad (188)$$

$$< (1-\xi) \frac{q}{1-q} \quad (189)$$

$$< q(1-Tq) \quad (190)$$

$$\leq \mathbb{E}[X'[r]], \quad (191)$$

where (188) is due to (5), (189) is due to Proposition 4, (190) is due to (184), and (191) is due to Proposition 42. \square

For $T \leq s < r$, we define $x(\cdot)$ on $\mathcal{R}^{r-s+T-1}$ by

$$x(h_{s-T+1}, \dots, h_{r-1}) = \sum_{i=s}^{r-1} \mathbb{1}\{h_i = 1, h_{i-1} = \dots = h_{i-T+1} = 0\}. \quad (192)$$

Likewise, we define $y(\cdot)$ on $\mathcal{R}^{r-s+2T-2}$ by

$$y(h_{s-T+1}, \dots, h_{r+T-2}) = \sum_{i=s}^{r-1} \mathbb{1}\{h_i = 1, h_{i-T+1} = \dots = h_{i-1} = h_{i+1} = \dots = h_{i+T-1} = 0\}. \quad (193)$$

Although h_i is allowed to take arbitrary real values, the indicator function yields binary value.

For all integers s and r satisfying $T \leq s < r$, we define

$$X'[s, r] = x(H[s-T+1], \dots, H[r-1]) \quad (194)$$

$$= \sum_{i=s}^{r-1} X'[i] \quad (195)$$

and

$$Y'[s, r] = y(H[s-T+1], \dots, H[r+T-2]) \quad (196)$$

$$= \sum_{i=s}^{r-1} Y'[i]. \quad (197)$$

Definition 45. For all integers $T \leq s < r$, define event

$$F[s, r] := F_1[s, r] \cap F_2[s, r] \cap F_3[s, r] \cap F_4[s, r] \quad (198)$$

where

$$F_1[s, r] := \left\{ \left(1 - \frac{\xi}{20}\right) \mathbb{E}[X'[s, r]] < X'[s, r] \right\}, \quad (199)$$

$$F_2[s, r] := \left\{ X[s, r] < \left(1 + \frac{\xi}{20}\right) \mathbb{E}[X[s, r]] \right\}, \quad (200)$$

$$F_3[s, r] := \left\{ \left(1 - \frac{\xi}{20}\right) \mathbb{E}[Y'[s, r]] < Y'[s, r] \right\}, \quad (201)$$

$$F_4[s, r] := \left\{ Z[s, r] < \mathbb{E}[Z[s, r]] + \frac{\xi}{20} \mathbb{E}[X'[s, r]] \right\}. \quad (202)$$

Definition 46. Let f be a function on \mathcal{R}^n . Let $x, x' \in \mathcal{R}^n$. A function $f(x_1, x_2, \dots, x_n)$ is k -Lipschitz if $|f(x) - f(x')| \leq k$ whenever x and x' differ in at most one coordinate.

Theorem 47. (McDiarmids inequality, [26, page 40]) If f on \mathcal{R}^n is k -Lipschitz and X_1, \dots, X_n are independent random variables, then for every $t > 0$,

$$P(f(X_1, X_2, \dots, X_n) > \mathbb{E}(f(X_1, X_2, \dots, X_n)) + t) \leq e^{-\frac{2t^2}{nk^2}}, \quad (203)$$

$$P(f(X_1, X_2, \dots, X_n) < \mathbb{E}(f(X_1, X_2, \dots, X_n)) - t) \leq e^{-\frac{2t^2}{nk^2}}. \quad (204)$$

Lemma 48. For $T \leq s < r$, $x(\cdot)$ is 1-Lipschitz and $y(\cdot)$ is 2-Lipschitz.

Proof. Define $x_i = \mathbb{1}\{h_i = 1, h_{i-1} = \dots = h_{i-T+1} = 0\}$, then $x(h_{s-T+1}, \dots, h_{r-1}) = \sum_{i=s}^{r-1} x_i$. Suppose $h_{s-T+1}, \dots, h_k, \dots, h_{r-1}$ changes to $h_{s-T+1}, \dots, h'_k, \dots, h_{r-1}$. Let ℓ be equal to the smaller one of $k+T-1$ and $r-1$. Only $x_k, x_{k+1}, \dots, x_\ell$ may be affected by this change. By definition, at most one of x_{k+1}, \dots, x_ℓ can be non-zero. Then there are two cases before the change: 1) All of x_{k+1}, \dots, x_ℓ are equal to 0. In this case, the change of h_k can change (increase or decrease) the value of x_k by at most 1, but has no impact on x_{k+1}, \dots, x_ℓ . 2) There exists a j between $k+1$ and ℓ . In this case, h_k must be zero according to the definition of x_j . Thus, $h'_k \neq 0$, x_j changes from 1 to 0. Meanwhile, x_k may change from 0 to 1 or remain zero, so $x_k + x_j$ is not going to differ by more than 1 from of its original value. In either case, $x(h_{s-T+1}, \dots, h_{r-1})$ can change by no more than 1, so $x(\cdot)$ is 1-Lipschitz.

Define $y_i = \mathbb{1}\{h_i = 1, h_{i-T+1} = \dots = h_{i-1} = h_{i+1} = \dots = h_{i+T-1} = 0\}$, then $y(h_{s-T+1}, \dots, h_{r+T-2}) = \sum_{i=s}^{r-1} y_i$. Suppose $h_{s-T+1}, \dots, h_k, \dots, h_{r+T-2}$ changes to $h_{s-T+1}, \dots, h'_k, \dots, h_{r+T-2}$. Let m be the larger one of $k-T+1$ and $s-T+1$, let n be the smaller one of $k+T-1$ and $r+T-2$. Only $y_m, \dots, y_{k-1}, y_k, y_{k+1}, \dots, y_n$ are possibly affected by this change. By definition, at most two elements of y_m, \dots, y_n can be non-zero, and they must be on different sides of y_k . Then there are two cases: 1) There are no more than one none-zero elements in y_m, \dots, y_n , in this case changing h_k can not change the value of g by more than 2. 2) There exists an p and q satisfying $m \leq p \leq k-1, k+1 \leq q \leq n$ such

that $y_p = 1$ and $y_q = 1$. In this case, we must have $h_k = 0$ and $h'_k \neq 0$ according to the definition of y_p, y_q . Thus y_p and y_q change from 1 to 0. Meanwhile, y_k may change from 0 to 1 or remain unchanged, and $y_p + y_k + y_q$ can change by 1 or 2, but not more than 2 from of its original value. So $y(\cdot)$ is 2-Lipschitz. \square

We define

$$\eta' = \frac{\xi^2}{4000T^2} q^2 (1-q)^{4T-2}. \quad (205)$$

Lemma 49. *For all integers $T \leq s < r$,*

$$P(F[s, r]) > 1 - 4e^{-\eta'(r-s)}, \quad (206)$$

where η' is given in (205).

Proof. Because $X'[r]$ and $X'[s]$ are dependent, standard Chernoff bound does not apply. Similarly for $Y'[r]$ and $Y'[s]$. However, due to Lemma 48, we have

$$P(F_1^c[s, r]) = P\left(X'[s, r] \leq \mathbb{E}[X'[s, r]] - \frac{\xi}{20} \mathbb{E}[X'[s, r]]\right) \quad (207)$$

$$\leq e^{-\frac{\xi^2}{200(r-s+T-1)} \mathbb{E}[X'[s, r]]^2} \quad (208)$$

$$\leq e^{-\frac{\xi^2}{200} q^2 (1-q)^{2T} (r-s+T-1)} \quad (209)$$

$$\leq e^{-\frac{\xi^2}{200} q^2 (1-q)^{2T} (r-s)} \quad (210)$$

where (208) is due to Theorem 47, (209) is due to Proposition 42, and (210) is due to $T \geq 1$.

Similarly,

$$P(F_3^c[s, r]) = P\left(Y'[s, r] \leq \mathbb{E}[Y'[s, r]] - \frac{\xi}{20} \mathbb{E}[Y'[s, r]]\right) \quad (211)$$

$$\leq e^{-\frac{\xi^2}{200(r-s+2T-2)} \mathbb{E}[Y'[s, r]]^2} \quad (212)$$

$$\leq e^{-\frac{\xi^2}{200} q^2 (1-q)^{4T-2} (r-s+2T-2)} \quad (213)$$

$$\leq e^{-\frac{\xi^2}{200} q^2 (1-q)^{4T-2} (r-s)} \quad (214)$$

where (212) is due to Theorem (47), (213) is due to (182), and (214) is due to $T \geq 1$.

By Proposition 8,

$$P(F_2^c[s, r]) = P\left(X[s, r] \geq \left(1 + \frac{\xi}{20}\right) \mathbb{E}[X[s, r]]\right) \quad (215)$$

$$\leq e^{-\frac{\xi^2}{1200} q(r-s)}. \quad (216)$$

According to (191), $E[Z[s, r]] < E[X'[s, r]]$. Note that the moment generating function for binomial random variable $Z[r] \sim \text{Binomial}(t, p)$ is $(1 - p + pe^u)^t$ [25]. Pick arbitrary $u > 0$. We have

$$P(F_4^c[s, r]) = P\left(Z[s, r] \geq \mathbb{E}[Z[s, r]] + \frac{\xi}{20T} \mathbb{E}[X'[s, r]]\right) \quad (217)$$

$$\leq P\left(Z[s, r] \geq \mathbb{E}[Z[s, r]] + \frac{\xi}{40T} \mathbb{E}[Z[s, r]] + \frac{\xi}{40T} \mathbb{E}[X'[s, r]]\right) \quad (218)$$

$$< \frac{\mathbb{E}[e^{Z[s, r]u}]}{e^{(1 + \frac{\xi}{40T})\mathbb{E}[Z[s, r]]u + \frac{\xi}{40T}\mathbb{E}[X'[s, r]]u}} \quad (219)$$

$$= \frac{(1 - p + pe^u)^{t(r-s)}}{e^{(1 + \frac{\xi}{40T})(r-s)tpu + \frac{\xi}{40T}q(1-q)^T u(r-s)}} \quad (220)$$

$$\leq e^{(e^u - 1 - u(1 + \frac{\xi}{40T}))tp(r-s) - \frac{\xi}{40T}uq(1-q)^T(r-s)}, \quad (221)$$

where (219) is by the Chernoff inequality and (221) is due to $1 + x \leq e^x$ for every $x \geq 0$ (here $x = p(e^u - 1)$). Let $u = \log(1 + \frac{\xi}{40T})$. Then

$$P(F_4^c[s, r]) \leq e^{(\frac{\xi}{40T} - (1 + \frac{\xi}{40T})\log(1 + \frac{\xi}{40T}))tp(r-s) - \frac{\xi}{40T}\log(1 + \frac{\xi}{40T})q(1-q)^T(r-s)} \quad (222)$$

$$< e^{-\frac{\xi}{40T}\log(1 + \frac{\xi}{40T})q(1-q)^T(r-s)} \quad (223)$$

$$< e^{-\frac{\xi^2}{4000T^2}q(1-q)^T(r-s)}, \quad (224)$$

where (223) is due to $(1 + x)\log(1 + x) > x$ for all $x > 0$ and (224) is due to $\log(1 + \frac{\xi}{40T}) > \frac{\xi}{100T}$ for all $\xi \in (0, 1]$ and $T \geq 1$.

Since η' defined in (205) dominates the corresponding exponential coefficients in (210), (214), (216), and (224), we have

$$P(F[s, r]) = 1 - P(F^c[s, r]) \quad (225)$$

$$\geq 1 - P(F_1^c[s, r]) - P(F_2^c[s, r]) - P(F_3^c[s, r]) - P(F_4^c[s, r]) \quad (226)$$

$$> 1 - 4e^{-\eta'(r-s)}. \quad (227)$$

□

Lemma 50. *For all integers $T \leq s < r - \frac{2}{q}$, the following inequalities hold under event $F[s, r]$:*

$$(1 - \frac{\xi}{20})q(1 - q)^T(r - s) < X'[s, r] \quad (228)$$

$$X[s, r] < (1 + \frac{\xi}{20})q(r - s) \quad (229)$$

$$(1 - \frac{\xi}{3})q(r - s) < Y'[s, r] \quad (230)$$

$$Z[s, r] < (1 - \frac{2\xi}{3})q(r - s) \quad (231)$$

$$Z[s, r + T] < (1 - \frac{\xi}{2})X'[s, r] \quad (232)$$

$$Z[s - T, r + T] < Y'[s, r]. \quad (233)$$

Proof. Under $F[s, r]$, (228) follows directly from (199). (229) follows directly from (200).

To prove (230), we write

$$Y'[s, r] > (1 - \frac{\xi}{20})E[Y'[s, r]] \quad (234)$$

$$> (1 - \frac{\xi}{20})(1 - (2T - 1)q)q(r - s) \quad (235)$$

$$> (1 - \frac{\xi}{20})(1 - \frac{\xi}{10})q(r - s) \quad (236)$$

$$> (1 - \frac{\xi}{3})q(r - s), \quad (237)$$

where (234) is due to (201), (235) is due to Proposition 43, (236) is due to (184), and (237) is due to $\xi \in [0, 1)$ and $T \geq 1$.

To prove (231),

$$Z[s, r] < \mathbb{E}[Z[s, r]] + \frac{\xi}{20}\mathbb{E}[X'[s, r]] \quad (238)$$

$$= pt(r - s) + \frac{\xi}{20}q(1 - q)^T(r - s) \quad (239)$$

$$= \frac{t}{n - t}(n - t)p(r - s) + \frac{\xi}{20}q(1 - q)^T(r - s) \quad (240)$$

$$\leq (1 - \xi)\frac{q}{1 - q}(r - s) + \frac{\xi}{20}q(1 - q)^T(r - s) \quad (241)$$

$$\leq (1 - \xi)\frac{q}{1 - \frac{\xi}{20T}}(r - s) + \frac{\xi}{20}q(r - s) \quad (242)$$

$$< \left(1 - \frac{2\xi}{3}\right)q(r - s), \quad (243)$$

where (238) is due to (202), (241) is due to Proposition 4, (242) is due to (184), and (243) is due to $\xi \in (0, 1]$.

By assumption (184),

$$T \leq \frac{\xi}{20q} \quad (244)$$

$$< \frac{\xi}{40}(r - s) \quad (245)$$

where (245) is by the assumption of this lemma. Thus,

$$r - s + T < (1 + \frac{\xi}{20})(r - s). \quad (246)$$

To prove (232), we begin with (241) with r replaced by $r + T$:

$$Z[s, r + T] < (1 - \xi) \frac{q}{1 - q} (r - s + T) + \frac{\xi}{20} q (1 - q)^T (r - s + T) \quad (247)$$

$$< \left(\frac{1 - \xi}{(1 - q)^{T+1}} + \frac{\xi}{20} \right) (1 + \frac{\xi}{40}) q (1 - q)^T (r - s) \quad (248)$$

$$< \left(\frac{1 - \xi}{1 - (T + 1)q} + \frac{\xi}{20} \right) (1 + \frac{\xi}{40}) q (1 - q)^T (r - s) \quad (249)$$

$$< \left(\frac{1 - \xi}{1 - (T + 1)q} + \frac{\xi}{20} \right) (1 + \frac{\xi}{40}) \frac{X'[s, r]}{1 - \frac{\xi}{20}} \quad (250)$$

$$< \left(\frac{1 - \xi}{1 - \frac{\xi}{10}} + \frac{\xi}{20} \right) (1 + \frac{\xi}{40}) \frac{1}{1 - \frac{\xi}{20}} X'[s, r] \quad (251)$$

$$< (1 - \frac{\xi}{2}) X'[s, r] \quad (252)$$

where (248) is due to (246), (249) is due to (11), (250) is due to (228), (251) is due to $q < \frac{\xi}{10(T+1)}$, (252) is due to $\xi \in [0, 1)$.

To prove (233),

$$Z[s - T, r + T] < (1 - \frac{2\xi}{3}) q (r - s + 2T) \quad (253)$$

$$< (1 - \frac{2\xi}{3}) (1 + \frac{\xi}{20}) q (r - s) \quad (254)$$

$$< (1 - \frac{\xi}{3}) q (r - s) \quad (255)$$

$$< Y'[s, r], \quad (256)$$

where (253) is due to (231), (254) is due to (246), (255) is due to $\xi \in [0, 1)$, and (256) is due to (230). \square

Definition 51. For all integers $T \leq s < r - \frac{2}{q}$, define typical event

$$J[s, r] := \cap_{0 \leq a \leq s-T, b \geq 0} F[s - a, r + b]. \quad (257)$$

$J[s, r]$ occurs when events $F[s - a, r + b]$ simultaneously occurs for all a, b , i.e., the “ F ” event occurs over all intervals containing $[s, r]$. Like event G , the event F represents a collection of outcomes that constrain the number of blocks mined in all intervals that contain $[s, r]$, including arbitrarily large intervals that end in the arbitrarily far future. Intuitively, we define $J[s, r]$ to allow the “good” properties in Lemma 50 to extend to all intervals containing $[s, r]$ under the event.

Lemma 52. For all integers $T \leq s < r - \frac{2}{q}$,

$$P(J[s, r]) > 1 - 5\eta'^{-2}e^{-\eta'(r-s)}. \quad (258)$$

Proof. Due to the stationarity of processes X, Y, Z, X' , and Y' , $P(F[s, r]) = P(F[T, T + r - s])$ for all s, r . Evidently the probability depends on r and s only through the interval length $r - s$:

$$P(J^c[s, r]) = P(\cup_{0 \leq a \leq s-T, b \geq 0} F^c[s - a, r + b]) \quad (259)$$

$$= P(\cup_{0 \leq a \leq s-T, b \geq 0} F^c[T, r - s + a + b + T]) \quad (260)$$

$$\leq \sum_{0 \leq a \leq s-T, b \geq 0} P(F^c[T, r - s + a + b + T]) \quad (261)$$

$$= \sum_{k=0}^{\infty} \sum_{0 \leq a \leq s-T, b \geq 0, a+b=k} P(F^c[T, r - s + k + T]) \quad (262)$$

$$< \sum_{k=0}^{\infty} (k+1) P(F^c[T, r - s + k + T]) \quad (263)$$

$$< \sum_{k=0}^{\infty} (k+1) 4e^{-\eta'(r-s+k)} \quad (264)$$

$$= 4e^{-\eta'(r-s)} \sum_{k=0}^{\infty} (k+1) e^{-\eta'k} \quad (265)$$

$$= \frac{4}{(1 - e^{-\eta'})^2} e^{-\eta'(r-s)}. \quad (266)$$

$$(267)$$

According to (184) and (205), $\eta' < \frac{1}{4000}$. Thus, (258) is established using the fact that $1 - e^{-x} > \frac{4}{\sqrt{5}}x$ for all $x \in [0, \frac{1}{4000}]$. \square

Lemma 53. Suppose some blockchain's k th block B is mined by an honest miner during round $r > T$ in a T -doubly-isolated successful round. Then, after round $r + T$, the k th block of every blockchain is either B or an adversarial block.

Proof. Suppose, contrary to the claim, the k th block of another blockchain is an honest block $B' \neq B$. Let \underline{r} (respectively, \bar{r}) denote the round number that earlier (respectively, later) of B and B' is mined. Then we have $\bar{r} > \underline{r} + T$ by assumption that B is mined in a uniquely successful round. Because the propagation delay is bounded by T , then by round \bar{r} all miners have seen a block of height k , so no other honest block of height k will be mined. This contradicts the assumption that B and B' are both at position k . Hence the proof of Lemma 53. \square

Lemma 54. (Lemma 29 in [3]) Let $T \leq s \leq r - T$ be integers. Suppose an honest blockchain is of length l by round s . Then by round r , the length of every honest blockchain is at least $l + X'[s, r - T + 1]$.

Proof. By induction on r : Consider $r = s + T$. If $X'[s] = 0$, then $X'[s, s + 1] = 0$. Since propagation delays are upper bounded by T rounds, all miners have seen a block of height l by round $s + T$, so all honest blockchains' height is at least l . If $X'[s] = 1$, $X'[s, s + 1] = 1$. By round $s + 1$, at least one honest miner would have broadcast a block of height $l + 1$. Then by round $r + T$, each honest miner will adopt a blockchain of at least $l + 1 = l + X[s, r - T + 1]$ blocks.

We next assume the claim holds for $r = s + T, s + T + 1, \dots, s + T + u$ and show that it also holds for $s + T + u + 1$. There are two cases. 1) $X'[s + u + 1] = 0$, the claim holds trivially. 2) $X'[s + u + 1] = 1$, then by definition of X' , $X'[s + u] = \dots = X'[s + u - T + 2] = 0$. By induction, by round $s + u + 1$, any honest miner's blockchain length is at least $l' = l + X'[s, s + u - T + 2] = l + X'[s, s + u + 1]$. Since $X'[s + u + 1] = 1$, by round $s + u + 2$ at least one honest miner would have broadcast a blockchain of length $l' + 1 = X'[s, s + u + 2] + 1$. Then each honest miner will adopt a blockchain of length at least $l + X[s + u + 2]$ by round $s + u + T + 1$.

By induction on r , Lemma 54 holds. \square

Lemma 55. For all integers $T \leq s < r - \frac{2}{q}$ and $k \geq 2q(r - s)$, under typical event $J[s, r]$, every honest miner's k -deep block by round r must be mined before round s .

Proof. The blockchain growth of an honest miner during rounds $\{s, \dots, r - 1\}$ is upper bounded by $X[s - T, r] + Z[s - T, r]$. Under $J[s, r]$, $F[s - T, r]$ also occurs. Note that

$$X[s - T, r] + Z[s - T, r] < (1 + \frac{\xi}{20})q(r - s + T) + (1 - \frac{2\xi}{3})q(r - s + T) \quad (268)$$

$$< (2 - \frac{\xi}{2})q(r - s + T) \quad (269)$$

$$< 2q(r - s) \quad (270)$$

$$\leq k, \quad (271)$$

where (268) is due to (229) and (231), (270) is due to (184) and $r - s > \frac{2}{q}$. Then, the k -deep block must be adopted before round s , thus mined before round s . \square

Theorem 56. (Blockchain growth property for bounded-delay model) Let r, s, s_1 be integers satisfying $T \leq s_1 \leq s < r - \frac{2}{q}$. Then under typical event $J[s, r - T]$, the length of every honest blockchain must increase by at least $(1 - \frac{\xi}{10})(1 - q)^T q(r - s_1)$ during rounds $\{s_1, \dots, r\}$.

Proof. Note that $\frac{2}{q} \geq \frac{40T}{\xi} > T$ by (184). Since $[s, r - T] \subset [s_1, r - T + 1]$, we have

$$X'[s_1, r - T + 1] > (1 - \frac{\xi}{20})q(1 - q)^T(r - s_1 - T + 1) \quad (272)$$

$$= (1 - \frac{\xi}{20})q(1 - q)^T(1 - \frac{T - 1}{r - s_1})(r - s_1) \quad (273)$$

$$> (1 - \frac{\xi}{20})(1 - \frac{T}{r - s_1})q(1 - q)^T(r - s_1) \quad (274)$$

$$\geq (1 - \frac{\xi}{20})(1 - \frac{\xi}{40})q(1 - q)^T(r - s_1) \quad (275)$$

$$> (1 - \frac{\xi}{10})q(1 - q)^T(r - s_1), \quad (276)$$

where (272) is due to (228), (275) is due to $r - s_1 \geq \frac{2}{q}$ and (184) $q \leq \frac{\xi}{20T}$, (276) is due to $\xi \in [0, 1)$. By Lemma 54, the length of every honest blockchain must increase by at least $(1 - \frac{\xi}{10})(1 - q)^T q(r - s_1)$ during rounds $\{s_1, \dots, r\}$. \square

Theorem 57. (*Blockchain quality theorem for bounded-delay model*) Let r, s, k be integers satisfying $T \leq s < r - \frac{2}{q}$ and $k \geq 2q(r - s)$. Suppose an honest miner's blockchain j has more than k blocks by round r . By round r , at least $\frac{\xi}{2}$ fraction of the last k blocks of this miner's blockchain are honest under event $J[s, r - T]$.

Proof. Assume an honest miner adopts blockchain $C = B_0 B_1 \dots B_{\text{len}(C)-1}$ by round r , where B_0 is the genesis block and $\text{len}(C) > k$. Let $u = \text{len}(C) - k$. Then the last k blocks of C are $B_u \dots B_{\text{len}(C)-1}$. Let $B_{u'}$ be the last honest block before B_u . That is to say, $u' = \max\{u' | u' \leq u - 1, B_{u'} \text{ is honest}\}$ (u' is always well defined as B_0 is regarded as honest). Let r^* be the round when $B_{u'}$ is mined. By Lemma 55 and the fact that $J[s, r - T] \subset J[s, r]$, we have $r^* < s$. Let $L = \text{len}(C) - u' - 1$. Note that $L \geq \text{len}(C) - u \geq k$.

Let x be the number of honest blocks in $B_u \dots B_{\text{len}(C)-1}$. To prove the theorem, it suffices to show $x > \frac{\xi}{2}k$. Since all blocks in $B_{u'+1} \dots B_{u-1}$ are adversarial, the number of honest blocks in $B_{u'+1} \dots B_{\text{len}(C)}$ is also x . Thus, the number of adversarial blocks in $B_{u'+1} \dots B_{\text{len}(C)-1}$ is $L - x$. Under $J[s, r - T]$, which implies $F[r^* + 1, r - T]$ also occurs, we have

$$L - x \leq Z[r^* + 1, r] \quad (277)$$

$$< (1 - \frac{\xi}{2})X'[r^* + 1, r - T] \quad (278)$$

$$\leq (1 - \frac{\xi}{2})L \quad (279)$$

$$\leq L - \frac{\xi}{2}k, \quad (280)$$

where (278) is due to (232), (279) is due to Lemma 54, (280) is due to $L \geq k$. From (280), $x > \frac{\xi}{2}k$ is derived. \square

Theorem 58. (*Common prefix property for bounded-delay model*) Let r, s, k be integers satisfying $T \leq s < r - \frac{2}{q}$ and $k > 2q(r - s)$. If by round r an honest blockchain has a k -deep prefix, then the prefix is permanent after round r under $J[s + T, r - T]$.

Proof. By assumption,

$$r - s > \frac{2}{q} \tag{281}$$

$$> \frac{40T}{\xi} \tag{282}$$

$$> 2T + 1. \tag{283}$$

Hence $J[s + T, r - T]$ is well defined.

We prove the desired result by contradiction. Suppose blockchain C_1 is adopted by an honest miner P_1 by round r . Suppose, contrary to claimed, an honest miner P_2 first deviates from the prefix $C_1^{\lceil k}$ from some round number $r_2 \geq r$. Specifically, P_2 adopts C'_2 by round $r_2 - 1$ which satisfies $C_1^{\lceil k} \preceq C'_2$ and then adopts C_2 by round r_2 which satisfies $C_1^{\lceil k} \not\preceq C_2$.

Assume the last honest block on the common prefix of C_2 and C'_2 is mined during round r^* . If $r^* > 0$, this common block of C_2 and C'_2 must be more than k deep in C_1 by round r . According to Lemma 55, we have $r^* < s$, so that

$$[s + T, r - T] \subset [r^* + T + 1, r_2 - T]. \tag{284}$$

On the other hand, if $r^* = 0$, the last common block is the genesis block. Since $s \geq T$, (284) also holds.

Under $J[s + T, r - T]$, $F[r^* + T + 1, r_2 - T]$ also occurs, so that $Y'[r^* + T + 1, r_2 - T] > 0$ according to (230). Hence, there must be at least one T -doubly-isolated successful round $u \in \{r^* + T + 1, \dots, r_2 - T - 1\}$. Suppose honest miner P mines B_u during round u with height l_u . According to Lemma 53, the l_u th block of every blockchain by round r_2 is either B_u or adversarial block.

If the l_u th block of C_2 and C'_2 are different, then at least one of them must be adversarial according to Lemma 53. On the other hand, if the l_u th block of C_2 and C'_2 are identical, the block must be in their common prefix, which must be adversarial by the definition of r^* . Thus, for each T -doubly-isolated successful round u , there is at least one adversarial block at height l_u . Since these adversarial blocks are mined after the last common honest block of C'_2 and C_2 , they are mined after round r^* . Since C'_2 and C_2 are adopted by round r_2 , their blocks must be mined before round r_2 . Thus, the

adversarial blocks that match the T -doubly-isolated successful rounds are mined within $[r^* + 1, r_2]$. Thus, $Z[r^* + 1, r_2] \geq Y'[r^* + T + 1, r_2 - T]$. However, since $[s + T, r - T] \in [r^* + T + 1, r_2 - T]$, $F[r^* + T + 1, r_2 - T]$ occurs under $J[s + T, r - T]$, so that $Z[r^* + 1, r_2] < Y'[r^* + T + 1, r_2 - T]$ according to (233). Contradiction arises, hence the proof of the theorem. \square

B. Prism under bounded-delay model

Recall $H_j[r]$ denotes the total number of honest blocks mined during round r for blockchain j . Following the definitions in Section V-A, for $j = 0, 1, \dots, m$ and $r = T, T + 1, \dots$, we define

$$Y'_j[r] = \begin{cases} 1, & \text{if } H_j[r] = 1 \text{ and } H_j[s] = 0 \text{ for } s = r - T + 1, \dots, r - 1, r + 1, \dots, r + T - 1 \\ 0, & \text{otherwise} \end{cases} \quad (285)$$

and

$$X'_j[r] = \begin{cases} 1, & \text{if } H_j[r] = 1 \text{ and } H_j[s] = 0 \text{ for } s = r - T + 1, \dots, r - 1 \\ 0, & \text{otherwise.} \end{cases} \quad (286)$$

Basically $Y'_j[r]$ indicates whether r is a T -doubly-isolated successful round for blockchain j , whereas $X'_j[r]$ indicates whether r is a T -left-isolated uniquely successful round for blockchain j .

Definition 59. For all integers $T \leq s < r - \frac{2}{q}$ and $0 \leq j \leq m$, define event

$$F_j[s, r] := F_{1,j}[s, r] \cap F_{2,j}[s, r] \cap F_{3,j}[s, r] \cap F_{4,j}[s, r] \quad (287)$$

where

$$F_{1,j}[s, r] := \left\{ \left(1 - \frac{\xi}{20}\right) \mathbb{E}[X'_j[s, r]] < X'_j[s, r] \right\}, \quad (288)$$

$$F_{2,j}[s, r] := \left\{ X_j[s, r] < \left(1 + \frac{\xi}{20}\right) \mathbb{E}[X_j[s, r]] \right\}, \quad (289)$$

$$F_{3,j}[s, r] := \left\{ \left(1 - \frac{\xi}{20}\right) \mathbb{E}[Y'_j[s, r]] < Y'_j[s, r] \right\}, \quad (290)$$

$$F_{4,j}[s, r] := \left\{ Z_j[s, r] < \mathbb{E}[Z_j[s, r]] + \frac{\xi}{20} \mathbb{E}[X'_j[s, r]] \right\}. \quad (291)$$

Note that for $0 \leq j \leq m$ and $r \geq T$, $X_j[r]$, $Y_j[r]$, $X'_j[r]$, $Y'_j[r]$ and $Z_j[r]$ are identically distributed as $X[r]$, $Y[r]$, $X'[r]$, $Y'[r]$ and $Z[r]$ in bitcoin protocol. Also, $F_j[s, r]$ is defined in the same manner as $F[s, r]$. Thus the proposer blockchain and all voter blockchains satisfy similar properties as those of the bitcoin blockchains.

Definition 60. For all integers $T \leq s < r - \frac{2}{q}$ and $0 \leq j \leq m$, define blockchain j 's typical event with respect to $[s, r]$ as

$$J_j[s, r] := \cap_{0 \leq a \leq s-T, b \geq 0} F_j[s-a, r+b]. \quad (292)$$

Lemma 61. For all integers $T \leq s < r - \frac{2}{q}$ and $0 \leq j \leq m$,

$$P(J_j[s, r]) > 1 - 5\eta'^{-2}e^{-\eta'(r-s)} \quad (293)$$

where η' is defined in (205).

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof at that for Lemma 52. \square

Lemma 62. Let $T \leq s \leq r - T$ and $0 \leq j \leq m$ be integers. Suppose an honest blockchain is of length l by round s . Then by round r , the length of every honest voter blockchain is at least $l + X'_j[s, r - T + 1]$.

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof at that for Lemma 54. \square

Lemma 63. For all integers $T \leq s < r - \frac{2}{q}$, $k \geq 2q(r - s)$ and $0 \leq j \leq m$, under typical event $J_j[s, r]$, every honest miner's k -deep block of blockchain j by round r must be mined before round s .

Proof. For $j = 0, 1, \dots, m$, the lemma admits essentially the same proof at that for Lemma 55. \square

Theorem 64. Let r, s, s_1, j be integers satisfying $T \leq s_1 \leq s < r - \frac{2}{q}$ and $0 \leq j \leq m$. Then under typical event $J_j[s, r - T]$, the length of every honest miner's blockchain j must increase by at least $(1 - \frac{\xi}{10})(1 - q)^T q(r - s_1)$ during rounds $\{s_1, \dots, r\}$.

Proof. For $j = 0, 1, \dots, m$, the theorem admits essentially the same proof at that for Theorem 56. \square

Theorem 65. Let r, s, k, j be integers satisfying $T \leq s < r - \frac{2}{q}$, $k \geq 2q(r - s)$ and $1 \leq j \leq m$. Suppose an honest miner's blockchain j has more than k blocks by round r . Under event $J_j[s, r - T]$, by round r , at least $\frac{\xi}{2}$ fraction of the last k blocks of this miner's blockchain j are honest.

Proof. For $j = 1, \dots, m$, the theorem admits essentially the same proof at that for Theorem 57. \square

Theorem 66. Let r, s, k, j be integers satisfying $T \leq s < r - \frac{2}{q}$, $k > 2q(r - s)$ and $1 \leq j \leq m$. If by round r an honest miner's blockchain j has a k -deep prefix, then the prefix is permanent after round r under $J_j[s + T, r - T]$.

Proof. For $j = 1, \dots, m$, the theorem admits essentially the same proof at that for Theorem 58. \square

Define

$$\delta_k = 5m(\eta')^{-2}e^{-\eta'\frac{k}{2q}+(2T+1)\eta'}. \quad (294)$$

Recall that R_l denotes the round in which the first proposer block on level l is mined (Definition 32).

Lemma 67. *Consider a given level l . Let k be a positive integer satisfying $k \geq 5$. If by some round $r > \max\left\{\frac{k}{2q}, R_l + T\right\}$, every voter blockchain contains at least one honest block mined after round R_l which is at least k -deep, then $\mathbf{LedSeq}_l(r)$ is δ_k -permanent after round r .*

Proof. Let

$$s = r - \left\lfloor \frac{k}{2q} \right\rfloor, \quad (295)$$

which must be a positive integer because $2qr > k$. Define

$$J = \cap_{j=1,2,\dots,m} J_j[s+T, r-T]. \quad (296)$$

For $j = 1, \dots, m$, let B_j denote an honest block on an honest voter blockchain j which is mined after round R_l and is at least k -deep by round r . Since $r - s = \left\lfloor \frac{k}{2q} \right\rfloor > \frac{2}{q}$, according to Theorem 66, B_j and its ancestors are permanent after round r under $J_j[s+T, r-T]$. Hence, B_1, \dots, B_m and all their ancestors must be permanent after round r under J . Thus, all voter blockchains' voting are permanent. Since B_1, \dots, B_m are honest, they would have voted for all levels up to level l of the proposer blockchain by the voting rule. Hence, the leader block sequence up to level l is permanent after round r under J . Note that

$$P(J) = 1 - P(\cup_{j=1,2,\dots,m} J_j^c[s+T, r-T]) \quad (297)$$

$$\geq 1 - \sum_{j=1}^m P(J_j^c[s+T, r-T]) \quad (298)$$

$$= 1 - mP(J_1^c[s+T, r-T]) \quad (299)$$

$$> 1 - 5m\eta'^{-2}e^{-\eta'(r-s-2T)}, \quad (300)$$

where (298) is due to the union bound, (299) is due to symmetry of all voter blockchains, (300) is due to Lemma 61. By (295), we have $2q(r-s+1) > k$, so that (300) becomes

$$P(G) > 1 - 5m\eta'^{-2}e^{-\eta'\frac{k}{2q}+\eta'(2T+1)} \quad (301)$$

$$= 1 - \delta_k. \quad (302)$$

Thus, the leader block sequence up to level l is δ_k -permanent after round r . \square

Lemma 68. *If positive integers R , r , and k satisfy $k \geq 5$ and*

$$r \geq \frac{2(k+1)}{(1 - \frac{\xi}{10})\xi q(1-q)^T} + 1, \quad (303)$$

then by round $R + r$, with probability of at least $1 - \delta_k$, all honest voter blockchains have an honest block mined after R which is at least k deep.

Proof. Let

$$\ell = \left\lceil \frac{2k}{\xi} \right\rceil. \quad (304)$$

Let

$$s_1 = \left\lfloor \frac{k}{q\xi} \right\rfloor. \quad (305)$$

Then

$$\ell \geq \frac{2k}{\xi} \quad (306)$$

$$\geq 2q \left\lfloor \frac{k}{q\xi} \right\rfloor \quad (307)$$

$$= 2qs_1. \quad (308)$$

Obviously $r > \frac{2}{q}$. According to the Theorem 64, under event $J_j[R, R+r-T]$, an honest voter blockchain j 's growth during $\{R, R+1, \dots, R+r-1\}$ is at least

$$(1 - \frac{\xi}{10})q(1-q)^T r \geq \frac{2(k+1)}{\xi} \quad (309)$$

$$> \ell, \quad (310)$$

where (309) is due to (303) and (310) is due to (304).

Note that $s_1 = \left\lfloor \frac{k}{q\xi} \right\rfloor > \frac{2}{q}$. According to Theorem 65 and (308), under event $J_j[R+r-s_1, R+r-T]$, at least $\frac{\xi}{2}$ fraction of the last ℓ blocks of this voter blockchain j are honest. Because $\frac{\xi}{2}\ell \geq k$, the earliest of these honest blocks must be at least k deep.

By (303) and (305), it is easy to see that $s_1 \leq r$. Hence $J_j[R+r-s_1, R+r-T] \subset J_j[R, R+r-T]$. We define

$$J = \cap_{j=1,2,\dots,m} J_j[R+r-s_1, R+r-T]. \quad (311)$$

Under event J , by round $R + r$, every honest voter blockchain has an honest block mined after round R which is at least k deep. The probability of the typical event can be lower bounded:

$$P(J) = P(\cap_{j=1,2,\dots,m} J_j[R + r - s_1, R + r - T]) \quad (312)$$

$$= 1 - P(\cup_{j=1,2,\dots,m} J_j^c[R + r - s_1, R + r - T]) \quad (313)$$

$$\geq 1 - mP(J_1^c[R + r - s_1, R + r - T]) \quad (314)$$

$$> 1 - 5m\eta'^{-2}e^{-\eta'(s_1-T)} \quad (315)$$

where (314) is due to the union bound and symmetry of all voter blockchains and (315) is due to Lemma 61. Moreover,

$$s_1 - T = \lfloor \frac{k}{q\xi} \rfloor - T \quad (316)$$

$$> \frac{k}{2q} - 1 - 2T. \quad (317)$$

Therefore,

$$P(J) > 1 - \delta_k. \quad (318)$$

In summary, by round $R + r$, with probability at least $1 - \delta_k$, all honest voter blockchains have an honest block mined after round R which is at least k deep. \square

Theorem 69. Fix $\epsilon \in (0, 1)$. Let R_l be the round during which the first proposer block on level l is mined. For every integer

$$r \geq \frac{5}{(1 - \frac{\xi}{10})\xi\eta'(1-q)^T} \left(\log \frac{10m\eta'^{-2}}{\epsilon} + \eta'(2T + 1) \right), \quad (319)$$

the leader sequence up to level l is ϵ -permanent after round $R_l + r$.

Proof. Let

$$k = \left\lceil \frac{2}{\eta'} \log \frac{10m\eta'^{-2}}{\epsilon} + 2(2T + 1)q \right\rceil, \quad (320)$$

and

$$s = \left\lceil \frac{2(k + 1)}{(1 - \frac{\xi}{10})\xi q(1-q)^T} + 1 \right\rceil. \quad (321)$$

Let δ_k be as defined as in (294).

According to Lemma 68 and (321), by round $R_l + s$, all honest voter blockchains have an honest block which is mined after R_l and is at least k deep with probability at least $1 - \delta_k$. Under this event, according

to Lemma 67 (evidently, $R_l + s > \frac{k}{2q}$ and $s > \frac{2}{q}$), the leader sequence up to level l is δ_k -permanent after round $R_l + s$. Therefore, the leader sequence up to level l is $2\delta_k$ -permanent after round $R_l + s$. Note that

$$\delta_k = 5m\eta'^{-2}e^{-\eta'\frac{k}{2} + \eta'(2T+1)} \quad (322)$$

$$\leq 5m\eta'^{-2}e^{-\log \frac{12m\eta'^{-2}}{\epsilon}} \quad (323)$$

$$= \frac{\epsilon}{2}. \quad (324)$$

the leader sequence up to level l is ϵ -permanent after round $R_l + s$.

From (320), it is easy to verify that $k > 10$. As a consequence, we have

$$s < \frac{2(k+1)}{(1 - \frac{\xi}{10})\xi q(1-q)^T} + 2 \quad (325)$$

$$= \frac{2k + 2 + 2(1 - \frac{\xi}{10})\xi q(1-q)^T}{(1 - \frac{\xi}{10})\xi q(1-q)^T} \quad (326)$$

$$< \frac{\frac{5}{2}(k-1)}{(1 - \frac{\xi}{10})\xi q(1-q)^T} \quad (327)$$

$$< \frac{5}{(1 - \frac{\xi}{10})\xi \eta'(1-q)^T} \left(\log \frac{10m\eta'^{-2}}{\epsilon} + \eta'(2T+1) \right) \quad (328)$$

$$\leq r, \quad (329)$$

where (325) is due to (320), (327) is due to $k > 10$, (328) is due to (320), and (329) is by (319).

Since $r > s$, is ϵ -permanent after round $R_l + r$ by Lemma 21. \square

Theorem 70. (*Blockchain quality theorem for proposer block for bounded-delay model*) Let r, s, k be integers satisfying $T \leq s < r - \frac{2}{q}$ and $k \geq 2q(r-s)$. Suppose an honest proposer blockchain has more than k leader blocks by round r . Under event $J_0[s, r-T]$, by round r , at least $\frac{\xi}{2}$ fraction of the last k leader blocks of the proposer blockchain are honest.

Proof. Let l denote the highest level of the proposer blockchain by round r . Evidently $l > k$. Let l^* be the highest level before $l - k + 1$ on which the first proposer block is honest. l^* may be as high as $l - k$ and as low as 0, which corresponds to the genesis block. Let r^* be the round when the first block on level l^* is mined. If this block is the genesis block, then $r^* = 0$. If $r^* > 0$, since blocks on level l^* are more than k blocks away from the last level by round r , we have $r^* < s$ according to Lemma 63. In any cases, we have $[s, r] \subset [r^* + 1, r]$.

Since the first proposer block on every level within $\{l^* + 1, \dots, l - k\}$ is adversarial, from level $l^* + 1$ to level l , there must be at least one adversarial block on every level except (possibly) on the levels between $l - k + 1$ and l where the leading block is honest. Let x be the number of honest leader blocks

on levels $\{l - k + 1, \dots, l\}$. Then during rounds $\{r^* + 1, \dots, r - 1\}$, the total number of adversarial proposer blocks is no fewer than $l - l^* - x$, i.e.,

$$Z_0[r^* + 1, r] \geq l - l^* - x. \quad (330)$$

Under $J_0[s, r - T]$, $E_0[r^* + 1, r - T]$ also occurs. Thus,

$$x \geq l - l^* - Z_0[r^* + 1, r] \quad (331)$$

$$> l - l^* - (1 - \frac{\xi}{2})X'_0[r^* + 1, r - T] \quad (332)$$

$$\geq \frac{\xi}{2}(l - l^*) \quad (333)$$

$$\geq \frac{\xi}{2}k, \quad (334)$$

where (332) is due to (232), (333) is due to Lemma 62, and (334) is due to $l - l^* \geq k$. To sum up, we have $x > \frac{\xi}{2}k$ and the proof is complete. \square

Theorem 71. *For every $\epsilon > 0$ and every integer*

$$r \geq \frac{25}{(1 - \frac{\xi}{10})^2 \xi^2 \eta' (1 - q)^{2T}} \left(\log \frac{20m\eta'^{-2}}{\epsilon} + \eta'(2T + 1) \right), \quad (335)$$

an honest transaction that enters into a block is ϵ -permanent r rounds after the block is broadcast.

Proof. Let

$$\ell = \left\lceil (1 - \frac{\xi}{10})q(1 - q)^T r \right\rceil \quad (336)$$

$$k = \left\lfloor \frac{\xi}{2} \ell \right\rfloor \quad (337)$$

$$w = \left\lfloor \frac{\ell}{2q} \right\rfloor \quad (338)$$

$$u = \left\lfloor \frac{k}{2q} \right\rfloor. \quad (339)$$

Let R be the round during which the block including the honest transaction is broadcast. Define

$$J = J_0[R + r - u, R + r - T] \cap J_0[R + r - w, R + r - T] \cap J_0[R, R + r - T]. \quad (340)$$

Note that 1) According to Theorem 64 and (336), under $G_0[R, R + r - T]$, the proposer blockchain grows by at least ℓ leader blocks during rounds $\{R, \dots, R + r\}$. 2) According to Theorem 70, under event $G_0[R + r - w, R + r - T]$, by round $R + r$ the last ℓ leader blocks includes at least $\frac{\xi}{2}$ fraction of honest ones. Since $k \leq \frac{\xi}{2}\ell$, at least k out of the last ℓ leader blocks are honest. 3) According to Lemma

63, under event $G_0[R + r - u, R + r - T]$, the deepest one of these k honest leader blocks is mined at least $\frac{k}{2q}$ rounds before round $R + r$. 4) We have

$$\frac{k}{2q} \geq \frac{1}{2q} \left\lfloor \frac{\xi}{2} \ell \right\rfloor \quad (341)$$

$$\geq \frac{1}{2q} \left\lfloor \frac{\xi}{2} \left(1 - \frac{\xi}{10}\right) q (1 - q)^T r \right\rfloor \quad (342)$$

$$\geq \frac{1}{2q} \left\lfloor \frac{25}{2(1 - \frac{\xi}{10}) \xi \eta' (1 - q)^T} \left(\log \frac{20m\eta'^{-2}}{\epsilon} + \eta'(2T + 1) \right) \right\rfloor \quad (343)$$

$$> \frac{1}{2q} \left(\frac{25}{2(1 - \frac{\xi}{10}) \xi \eta' (1 - q)^T} \left(\log \frac{20m\eta'^{-2}}{\epsilon} + \eta'(2T + 1) \right) - 1 \right) \quad (344)$$

$$> \frac{1}{2q} \left(\frac{10}{(1 - \frac{\xi}{10}) \xi \eta' (1 - q)^T} \left(\log \frac{20m\eta'^{-2}}{\epsilon} + \eta'(2T + 1) \right) \right) \quad (345)$$

$$= \frac{5}{(1 - \frac{\xi}{10}) \xi \eta' (1 - q)^T} \left(\log \frac{10m\eta'^{-2}}{\frac{\epsilon}{2}} + \eta'(2T + 1) \right), \quad (346)$$

where (341) is due to (337), (342) is due to (336), and (345) is obvious due to $\xi \in (0, 1]$. According to Theorem 69 and (346), the deepest honest leader block is $\frac{\xi}{2}$ -permanent after round $R + r$ under event J . Next, we will lower bound probability of J . Note that

$$u \leq \frac{k}{2q} \quad (347)$$

$$\leq \frac{\xi \ell}{4q} \quad (348)$$

$$< \frac{\ell}{2q} - 1 \quad (349)$$

$$< w, \quad (350)$$

where (348) is due to (337), (349) is due to $q \leq \frac{\xi}{6}$, and (350) is due to (338). Also,

$$w \leq \frac{\ell}{2q} \quad (351)$$

$$\leq r, \quad (352)$$

where (351) is due to (338) and (352) is due to (336). We have $u < w < s$. According to definition,

$G_0[R + r - u, R + r - T] \subset G_0[R + r - w, R + r - T] \subset G_0[R, R + r - T]$. Then,

$$P(J) = P(J_0[R + r - u, R + r - T]) \quad (353)$$

$$> 1 - 5\eta'^{-2}e^{-\eta'u} \quad (354)$$

$$> 1 - 5\eta'^{-2}e^{-\eta'(\frac{k}{2q}-1)} \quad (355)$$

$$> 1 - 5\eta'^{-2}e^{-\log \frac{10\eta'^{-2}}{\epsilon}} \quad (356)$$

$$= 1 - \frac{\epsilon}{2}, \quad (357)$$

where (354) is due to Lemma 61, (355) is due to (339), (356) is due to (346). According to the union rule, the deepest honest leader block is ϵ -permanent after round $R + r$. According to Lemma 40, the honest transaction will become a ϵ -permanent transaction after round $R + r$. \square

VI. CONCLUSION

In this paper, we have analyzed the bitcoin backbone protocol and the Prism backbone protocol using more general models than previously seen in the literature. In particular, we allow the blockchains to have unlimited lifespan and allow the block propagation delays to be arbitrary but bounded. Under the new setting, we rigorously establish a blockchain growth property, a blockchain quality property, and a common prefix property for the bitcoin backbone protocol. Under this framework, we have also proved a blockchain growth property and a blockchain quality property of the leader sequence in the Prism protocol. We have also shown that the leader sequence is permanent with high probability after sufficient amount of wait time. As a consequence, every honest transaction will eventually enter the final ledger and become permanent with probability higher than $1 - \epsilon$ after a confirmation time proportional to security parameter $\log \frac{1}{\epsilon}$. This paper provide explicit bounds for the bitcoin and the Prism backbone protocols, which furthers understanding of both protocols and provides practical guidance to public transaction ledger protocol design.

REFERENCES

- [1] S. Nakamoto *et al.*, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [2] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press, 2016.
- [3] J. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: Analysis and applications,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 281–310, Springer, 2015.
- [4] A. Kiayias and G. Panagiotakos, “Speed-security tradeoffs in blockchain protocols,” *IACR Cryptology ePrint Archive*, vol. 2015, p. 1019, 2015.

- [5] A. Sapirshstein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 515–532, Springer, 2016.
- [6] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol with chains of variable difficulty," in *Annual International Cryptology Conference*, pp. 291–323, Springer, 2017.
- [7] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, pp. 45–59, 2016.
- [8] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
- [9] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, "Deconstructing the blockchain to approach physical limits," *arXiv preprint arXiv:1810.08092*, 2018.
- [10] V. Gramoli, "From blockchain consensus back to byzantine consensus," *Future Generation Computer Systems*, 2017.
- [11] A. Miller and J. J. LaViola Jr, "Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin," Available on line: <http://nakamotoinstitute.org/research/anonymous-byzantine-consensus>, 2014.
- [12] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in *Proceedings of the 17th International Conference on Distributed Computing and Networking*, p. 13, ACM, 2016.
- [13] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.
- [14] P. Feldman and S. Micali, "Optimal algorithms for byzantine agreement," in *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pp. 148–161, ACM, 1988.
- [15] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, pp. 1–10, IEEE, 2013.
- [16] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 507–527, Springer, 2015.
- [17] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *International Conference on Financial Cryptography and Data Security*, pp. 528–547, Springer, 2015.
- [18] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Spectre: A fast and scalable cryptocurrency protocol.," *IACR Cryptology ePrint Archive*, vol. 2016, p. 1159, 2016.
- [19] Y. Sompolinsky and A. Zohar, "Phantom," *IACR Cryptology ePrint Archive, Report 2018/104*, 2018.
- [20] C. Natoli and V. Gramoli, "The balance attack against proof-of-work blockchains: The r3 testbed as an example," *arXiv preprint arXiv:1612.09426*, 2016.
- [21] C. Li, P. Li, W. Xu, F. Long, and A. C.-c. Yao, "Scaling nakamoto consensus to thousands of transactions per second," *arXiv preprint arXiv:1805.03870*, 2018.
- [22] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Work Pap.–2016*, 2016.
- [23] R. Pass and E. Shi, "Fruitchains: A fair blockchain," in *Proceedings of the ACM Symposium on Principles of Distributed Computing*, pp. 315–324, ACM, 2017.
- [24] M. Mitzenmacher and E. Upfal, *Probability and computing: Randomization and probabilistic techniques in algorithms and data analysis*. Cambridge university press, 2017.
- [25] M. N. Das, *Statistical methods and concepts*. New Age International, 1989.
- [26] R. Vershynin, *High-dimensional probability: An introduction with applications in data science*, vol. 47. Cambridge University Press, 2018.