Continuous-Time Analysis of the Bitcoin and Prism Backbone Protocols

Jing Li\textsuperscript{1} and Dongning Guo\textsuperscript{2}

Department of Electrical and Computer Engineering
Northwestern University
Evanston, IL 60208
\textsuperscript{1}jingli2015@u.northwestern.edu,
\textsuperscript{2}dGuo@northwestern.edu

January 17, 2020

Abstract

Bitcoin is a peer-to-peer payment system proposed by Nakamoto in 2008. Based on the Nakamoto consensus, Bagaria, Kannan, Tse, Fanti, and Viswanath proposed the Prism protocol in 2018 and showed that it achieves near-optimal blockchain throughput while maintaining similar level of security as bitcoin. This work provides the probabilistic guarantees for the liveliness and consistency of bitcoin and Prism transactions. Previous analyses of the bitcoin and Prism have been either established under a simplified discrete-time model or expressed in terms of exponential order result. This paper presents a streamlined and strengthened analysis under a more realistic continuous-time model where the block propagation delays are heterogeneous, arbitrary, and upper bounded by some constant. The goal is to show that every valid transaction becomes permanent in all honest miners’ blockchains under a certain “typical event”, which occurs with probability close to 1. To that end, we establish the blockchain growth theorem, the blockchain quality theorem, and the common prefix theorem. In lieu of exponential order result in the literature, the probabilistic guarantees for the desired properties of the bitcoin and Prism protocols take the form of explicit expressions here, which provide improved design references for public transaction ledger protocols.

I. INTRODUCTION

A. The bitcoin backbone protocol

Bitcoin was invented by Nakamoto\textsuperscript{1} in 2008 as an electronic payment system. The system is built on a distributed ledger technology commonly referred to as blockchain. A blockchain is a finite sequence
of transaction-recording blocks which begins with a genesis block, and every subsequent block contains a cryptographic hashing of the previous one (which confirms all preceding blocks). To mine a block requires proof of work: A nonce must be included such that the block’s hash value satisfies a difficulty requirement. Miners join a peer-to-peer network to inform each other of new blocks. An honest miner follows the longest-chain rule, i.e., it always tries to mine a block at the maximum height.

Different blocks may be mined and announced at around the same time. So honest miners may extend different blockchains depending on which blocks they hear first. This phenomenon is called forking, which must be resolved quickly to reach timely consensus about the ledger.

An adversarial miner may wish to sabotage consensus or manipulate the network to a consensus to its own advantage. In particular, forking presents opportunities for double spending, which is only possible if a transaction included in the longest fork at one time is not included in a different fork that overtakes the first one to become the longest blockchain. Nakamoto [1] characterized the race between the honest miners and the adversary 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 as long as the collective mining power of adversarial miners is less than that of honest miners. In this case, a bitcoin transaction becomes (arbitrarily) secure if it is confirmed by enough new blocks.

Garay, Kiayias, and Leonardos [2] first formally described and analyzed the bitcoin backbone protocol under the lockstep synchronous model, where all miners have perfectly synchronized rounds and all miners receive the same block(s) at exactly the end of the round. Under this model, [2] established a blockchain quality theorem, which states the honest miners contribute at least a certain percentage of the blocks with wish probability. Also established in [2] is a common prefix theorem, which states if a block is $k$ blocks deep in an honest miner’s blockchain, then the block is in all other honest miners’ blockchains with high probability (the probability that some honest miner does not extend this block vanishes exponentially with $k$). Kiayias and Panagiotakos [3] established a blockchain growth theorem, which quantifies the number of blocks added to the blockchain during any time interval. The blockchain growth theorem and the blockchain quality theorem guarantee that many honest blocks will eventually become $k$ deep in an honest miner’s blockchain (liveliness). The common prefix theorem then guarantees that an honest miner’s $k$-deep block become permanent consensus of all honest miners (consistency). Thus, every transaction that is recorded in a sufficiently deep block in an honest miner’s blockchain is with high probability guaranteed to remain in the final ledger.

The strictly lockstep synchrony model completely assumes away network delay and failure. Several meaningful analyses have been proposed under the non-lockstep synchrony model, where messages can be delayed arbitrarily but the delay is upper bounded. A complicated analysis with strong assumptions
Reference [5] also reasoned the consistency of bitcoin protocol using the Markov chains, although their result has a non-closed form. Most previous analyses [2], [4], [6], [7] assume the blockchain’s lifespan is finite, i.e., there exists a maximum round when the blockchain ends. In [8], we dropped the finite horizon assumption and proved stronger properties of the bitcoin backbone protocol regardless of whether or not the blockchains have a finite lifespan.

Most previous work [2], [4], [6], [7], [9] expressed the probability of the mentioned properties in exponential order result (big $O$ notation). Our previous work [8] gives the explicit bounds for the liveliness and consistency under the non-lockstep synchronous discrete-time model. The strategies taken by previous works can be described as the following: Intuitively, during any time interval the liveliness and consistency of honest blockchains hold under the following conditions: 1) The number of honest blocks mined during this time interval is larger than the number of adversarial blocks mined, so that the longest blockchain will not be overtaken by the adversarial party. 2) There are enough number of non-reversible honest blocks to guard the honest blockchain, in case the adversarial use strategies (like selfish mining) to introduce disagreement between honest miners and split their hashing power. Technically, with respect to time interval $[s, t]$, a “good event” occurs if the numbers of various blocks mined during the period are close to their respective expected values. A “typical event” with respect to $[s, t]$ occurs if good events occur for all time intervals covering $[s, t]$, so that the consistency of honest blockchains is guaranteed from time $t$ onward. The desired properties hold under the typical events, which are shown to almost certainly occur in the discrete-time model.

The discrete-time model eases analysis but is still a significant departure from reality. In 2019, Ren [9] extended the liveliness and consistency of bitcoin protocol assuming the continuous-time model where mining is modelled as a Poisson point process. The probability bounds are shown to be exponential in a linear order term in the confirmation time.

In this paper, we provide explicit probabilistic guarantees for the liveliness and consistency properties of the bitcoin transactions under the continuous-time model. To this end, we develop a technique to show that the typical event, which is the intersection of uncountably many good events with arbitrary real valued starting and ending points, still occurs with high probability. This treatment enables us to derive explicit probability bounds for the liveliness and consistency of bitcoin blockchains, which are more refined than previous exponential order result.
B. The Prism protocol

The throughput of bitcoin is very limited by design to ensure security [10]. In particular, the average time interval between new blocks is set to be much longer than the block propagation delays so that forking is infrequent [11]. Many ideas have been proposed to improve the blockchain throughput. One way is to construct high-forking blockchains by optimizing the forking rule, which is vulnerable to certain attacks [11]–[17]. Another line of work is to decouple the various functionalities of the blockchain [18], [19], under the spirit of which Bagaria, Kannan, Tse, Fanti, and Viswanath [7] proposed the Prism protocol in 2018. The Prism protocol defines 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. 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 leader sequence they selected. 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 found in [7].

In [7], liveliness and consistency of Prism transactions were proved assuming a finite life span of the blockchains under the lockstep synchrony model [7]. In [8] we have strengthened and extended the results to the non-lockstep synchrony model. This paper establishes the key properties for the continuous-time model. Compared with bitcoin blockchains whose consistency is achieved by the numerical advantage of honest blocks, the Prism blockchains achieve consistency by the permanent voting from voter blockchains.

II. The Bitcoin Backbone Protocol

Let $\Delta$ denote an upper bound for all communication delays. Let $\alpha$ denote the collective mining power of honest miners. Let $\beta$ denote the collective mining power of all other miners, referred to as adversarial miners from now on. The mining process of each honest miner is modelled as an independent homogeneous continuous-time Poisson point process. If a block is mined by some honest miner, we call it an honest block; otherwise the block is called an adversarial block. If a blockchain is adopted by an honest miner at time $t$, we call it an honest blockchain (at time $t$).

Let $H_t$ denote the total number of honest blocks mined up until time $t$. For convenience, it is assumed a genesis block is placed at $t = 0$ with height equal to 0. The genesis block is regarded as honest. Evidently, $(H_t, t \geq 0)$ is a homogeneous Poisson point process with rate $\alpha$. 

Lemma 3. For all real numbers $0 \leq s < t$ and non-negative integer $k$, conditioned on $N[s,t] = k$, $X_1, X_2, \ldots, X_k$ are independent Bernoulli random variables with

$$P(X_i = 1|N[s,t] = k) = e^{-\alpha \Delta}, \quad i = 1, 2, \ldots, k.$$  

Definition 1. An honest block mined at time $t$ is called a lagger if it is mined strictly more than $\Delta$ seconds after the last honest block was mined, i.e., if $H_t = 1 + H_{t-\Delta}$. The lagger is also called a loner if the next block mined is also a lagger, i.e., if $H_{t+\Delta} = H_t$.

By assumption, regardless of what strategy the adversarial miners take, there exists an independent homogeneous Poisson point process $(Z_t, t \geq 0)$ with rate $\beta$ that dominates the mining of adversarial blocks, in the sense that $Z[s,t] = Z_t - Z_s$ is always no less than the number of adversarial blocks mined during interval $(s,t)$. Let $N[s,t] = H_t - H_s$ denote the total number of honest blocks mined during time interval $(s,t)$. Let $X[s,t]$ denote the number of all lagers mined during time interval $(s,t)$. Let $Y[s,t]$ denote the number of all loners mined during time interval $(s,t)$.

Definition 2. For all $0 \leq s < t$ and $0 < \delta < 1$, the $\delta$-good event covering time interval $(s,t)$ is

$$E^\delta[s,t] = E^\delta_1[s,t] \cap E^\delta_2[s,t] \cap E^\delta_3[s,t] \cap E^\delta_4[s,t]$$

where

$$E^\delta_1[s,t] = \{(1 - \delta)\mathbb{E}[N[s,t]] < N[s,t] < (1 + \delta)\mathbb{E}[N[s,t]]\}$$

$$E^\delta_2[s,t] = \{(1 - \delta)\mathbb{E}[X[s,t]] < X[s,t]\}$$

$$E^\delta_3[s,t] = \{(1 - \delta)\mathbb{E}[Y[s,t]] < Y[s,t]\}$$

$$E^\delta_4[s,t] = \{Z[s,t] < \mathbb{E}[Z[s,t]] + \delta\mathbb{E}[Y[s,t]]\}.$$ 

Under event $E^\delta_1[s,t]$, the number honest blocks mined during time interval $(s,t)$ does not deviate from its expected value by more than a fraction of $\delta$. Under event $E^\delta_2[s,t]$, the number of lagers $X[s,t]$ is no less than $1 - \delta$ of its expected value. Under event $E^\delta_3[s,t]$, the number of loners $Y[s,t]$ is no less than $1 - \delta$ of its expected value. Under event $E^\delta_4[s,t]$, the upper bound for the number of adversarial blocks is no more than its expected value plus $\delta$ of the expectation of $Y[s,t]$. Under $E^\delta[s,t]$, we have 1) a “typical” number of honest blocks, 2) “enough” lagers and loners, and 3) the total number of adversarial blocks is unextraordinary.

During time interval $(s,t)$, for $i = 0, 1, \ldots, N[s,t]$, denote $X_i = 1$ if the $i$-th honest block starting from time $s$ is a lagger, and 0 otherwise. Then we have $X[s,t] = \sum_{i=1}^{N[s,t]} X_i$. Likewise, denote $Y_i = 1$ if the $i$-th honest block is a loner and 0 otherwise. Then we have $Y[s,t] = \sum_{i=1}^{N[s,t]} Y_i$. 

Lemma 3. For all real numbers $0 \leq s < t$ and non-negative integer $k$, conditioned on $N[s,t] = k$, $X_1, X_2, \ldots, X_k$ are independent Bernoulli random variables with

$$P(X_i = 1|N[s,t] = k) = e^{-\alpha \Delta}, \quad i = 1, 2, \ldots, k.$$  

Proof. Since the inter-arrival times of the Poisson process \((H_t, t > 0)\) are independent exponential random variables with the same parameter \(\alpha\) (Page 419 in [20]), (6) follows.

For convenience, let
\[
g = e^{-\alpha \Delta}.
\]

Lemma 4. For all real numbers \(0 \leq s < t\) and non-negative integer \(k\), conditioned on \(N[s,t] = k\), \(Y_1, Y_2, \ldots, Y_k\) are Bernoulli random variables with
\[
P(Y_i = 1 | N[s,t] = k) = g^2, \ i = 1, 2, \ldots, k.
\]

Proof. Let \(X_{k+1} = 1\) if the first honest block after time \(t\) is a lagger and \(X_{k+1} = 0\) otherwise. Then for \(i = 0, 1, \ldots, k\), we have \(Y_i = X_i X_{i+1}\). Note that \(X_i\)s are independent of each other, we have
\[
P(Y_i = 1 | N[s,t] = k) = P(X_i = 1 | N[s,t] = k)P(X_{i+1} = 1 | N[s,t] = k) = g^2, \ i = 1, 2, \ldots, k.
\]

Lemma 5. For all real numbers \(0 \leq s < t\),
\[
\mathbb{E}[N[s,t]] = \alpha(t - s).
\]

Proof. The result follows from the fact that \(N[s,t]\) is a Poisson distribution with parameter \(\alpha(t - s)\).

Lemma 6. For all real numbers \(0 \leq s < t\),
\[
\mathbb{E}[X[s,t]] = g \alpha(t - s).
\]

Proof.
\[
\mathbb{E}[X[s,t]] = \mathbb{E}\left[ \sum_{i=1}^{N[s,t]} X_i \right] = \mathbb{E}\left[ \sum_{i=1}^{N[s,t]} X_i | N[s,t] \right] = \mathbb{E}[g N[s,t]] = g \alpha(t - s).
\]
Lemma 7. For all real numbers $0 \leq s < t$,

$$
\mathbb{E}[Y[s,t]] = g^2 \alpha (t - s).
$$

(17)

Proof.

$$
\mathbb{E}[Y[s,t]] = \mathbb{E}\left[ \sum_{i=1}^{N[s,t]} X_i \right]
= \mathbb{E}\left[ \sum_{i=1}^{N[s,t]} Y_i | N[s,t] \right]
= \mathbb{E}[g^2 N[s,t]]
= g^2 \alpha (t - s).
$$

(18) \space (19) \space (20) \space (21)

Lemma 8. For all real numbers $0 \leq s < t$,

$$
\mathbb{E}[Z[s,t]] = \beta (t - s).
$$

(22)

Proof. The result follows from the fact that $Z[s,t]$ is a Poisson distribution with parameter $\beta(t - s)$.

Properties in the following parts of this paper require the parameters satisfy

$$
(1 - 3 \delta) g^2 \alpha > \beta.
$$

(23)

This assumption indicates the mining rate of adversarial blocks must be strictly less than the mining rate of loners multiplied by the square of “propagation discount” to enable a feasible $\delta$. In practice, the difficulty of this requirement depends on the upper bound of propagation delay $\Delta$. For example, if $\Delta = 0.5$ second, an honest mining power of 70% enables $\delta = 0.13$.

Next, we introduce a few preliminaries.

Lemma 9. Let $X$ be a Poisson random variable with parameter $\lambda$. Then for every $\delta \in (0, 1]$,

$$
P(X < (1-\delta)\lambda) < e^{-\frac{\delta^2 \lambda}{2}},
$$

(24)

and

$$
P(X > (1+\delta)\lambda) < e^{-\frac{\delta^2 \lambda}{3}}.
$$

(25)
Proof. To prove (24), we have
\[
P(X < (1 - \delta)\lambda) = P(e^{-tX} > e^{-t(1-\delta)\lambda})
\]
\[
< \frac{\mathbb{E}[e^{-tX}]}{e^{-t(1-\delta)\lambda}}
\]
\[
= e^{(e^{-t}-1)\lambda + t(1-\delta)\lambda}
\]
where (27) is due to Markov inequality and (28) is due to the moment generating function of Poisson random variable. Picking \( t = -\log(1 - \delta) \), we have
\[
P(X < (1 - \delta)\lambda) < e^{\delta - (1-\delta)\log(1-\delta)}
\]
\[
< e^{\frac{\delta^2}{2} \lambda}
\]
where (30) is due to \((1 - \delta)\log(1 - \delta) > -\delta + \frac{\delta^2}{2} \) for \( \delta \in (0, 1) \).

To prove (25), we have
\[
P(X > (1 + \delta)\lambda) = P(e^{tX} > e^{t(1+\delta)\lambda})
\]
\[
< \frac{\mathbb{E}[e^{tX}]}{e^{t(1+\delta)\lambda}}
\]
\[
= e^{(e^t-1)\lambda - t(1+\delta)\lambda}
\]
where (31) is due to Markov inequality and (32) is due to the moment generating function of Poisson random variable. Picking \( t = \log(1 + \delta) \), we have
\[
P(X > (1 + \delta)\lambda) < e^{\delta - (1+\delta)\log(1+\delta)}
\]
\[
< e^{\frac{\delta^2}{2} \lambda}
\]
where (35) is due to \((1 + \delta)\log(1 + \delta) > \delta + \frac{\delta^2}{2} \) for \( \delta \in (0, 1) \).

Proposition 10. (Chernoff bound, page 69 in [21]) Let \( X \sim \text{binomial}(n, p) \). Then for every \( \delta \in (0, 1] \),
\[
P(X < (1 - \delta)pn) < e^{-\frac{\delta^2 pn}{2} },
\]
and
\[
P(X < (1 + \delta)pn) < e^{-\frac{\delta^2 pn}{2} }.
\]

Lemma 11. If \( N \) is a Poisson random variable, then for any \( h \in [0, 1) \),
\[
\mathbb{E}[e^{-hN}] \leq e^{-\frac{1}{2}h\mathbb{E}[N]}.
\]
Proof. Let \( \lambda = \mathbb{E}[N] \). Then,

\[
\mathbb{E}[e^{-hN}] = \sum_{k=0}^{\infty} e^{-hk} P(N = k) = \sum_{k=0}^{\infty} \frac{e^{-hk} \lambda^k}{k!} e^{-\lambda} = \sum_{k=0}^{\infty} \frac{(e^{-h})^k \lambda^k}{k!} e^{-\lambda} = e^{e^{-h}\lambda} e^{-\lambda} \leq e^{-\frac{h}{2}\lambda}
\]

where (42) is due to Taylor expansion and (43) is due to \( e^{-h} \leq 1 - \frac{h}{2} \) for all \( h \in [0, 1) \).

Lemma 12. For all \( 0 < \delta < 1 \) and \( 0 \leq s < t \), we have

\[
P\left(E^\delta_{[s,t]}\right) > 1 - 7e^{-\frac{1}{8}g^2(t-s)}.
\]

Proof. We analyze events \( E^\delta_{1}[s,t] \), \( E^\delta_{2}[s,t] \), \( E^\delta_{3}[s,t] \), and \( E^\delta_{4}[s,t] \) separately.

First, we have

\[
P((E^\delta_{1}[s,t])^c) = P\left(N^\delta_{[s,t]} > \mathbb{E}[N[s,t]] + \delta \mathbb{E}[N[s,t]]\right) + P\left(N[s,t] < \mathbb{E}[N[s,t]] - \delta \mathbb{E}[N[s,t]]\right)
\]

\[
< 2e^{-\frac{1}{8}g^2(t-s)},
\]

where (46) is due to Lemma 9.

We have

\[
P((E^\delta_{3}[s,t])^c) = P\left(X[s,t] < (1-\delta)\mathbb{E}[X[s,t]]\right)
\]

\[
= \sum_{k=0}^{\infty} P\left(X[s,t] < (1-\delta)\mathbb{E}[X[s,t]] | N[s,t] = k\right) P(N[s,t] = k)
\]

\[
= \sum_{k=0}^{\infty} P\left(\sum_{i=1}^{k} X_i < (1-\delta)\mathbb{E}\left[\sum_{i=1}^{k} X_i\right]\right) P(N[s,t] = k)
\]

\[
< \sum_{k=0}^{\infty} e^{-\frac{\delta^2 k^2}{2}} P(N[s,t] = k)
\]

\[
= \mathbb{E}\left[e^{-\frac{\delta^2}{2} N[s,t]}\right]
\]

\[
\leq e^{-\frac{\delta^2}{4} \alpha(t-s)}
\]

where (50) is due to Lemma 6 and Proposition 10, (52) is due to Lemma 11.
Note that although \( Y_i \) and \( Y_{i+1} \) are dependent, \( Y_i \) and \( Y_{i+2} \) are independent. For all random variables \( U \) and \( V \) and constants \( a \) and \( b \), the following holds:

\[
P(U + V \leq a + b) \leq P(U \leq a \text{ or } V \leq b) \tag{53}
\]

\[
\leq P(U \leq a) + P(V \leq b). \tag{54}
\]

We calculate even blocks and odd blocks separately:

\[
P\left(\left( E\left[\delta_{s+\frac{1}{2}t}\right]\right]_{c}\right) = P\left( Y\left[\frac{s}{2}, t\right] \leq (1 - \delta)E[Y\left[\frac{s}{2}, t\right]]\right) \tag{55}
\]

\[
< P\left( \sum_{k=0}^{\left\lfloor \frac{N_{s+t}}{2} \right\rfloor} Y_{2k+1} < (1 - \delta)E\left[ \sum_{k=0}^{\left\lfloor \frac{N_{s+t}}{2} \right\rfloor} Y_{2k+1} \right] \right) + P\left( \sum_{k=1}^{\left\lfloor \frac{N_{s+t}}{2} \right\rfloor} Y_{2k} < (1 - \delta)E\left[ \sum_{k=1}^{\left\lfloor \frac{N_{s+t}}{2} \right\rfloor} Y_{2k} \right] \right) \tag{56}
\]

\[
\leq E\left[ e^{-\frac{\delta^2}{2}g^2\left(\left\lfloor \frac{N_{s+t}}{2}\right\rfloor + 1\right)} \right] + E\left[ e^{-\frac{\delta^2}{2}g^2\left(\left\lfloor \frac{N_{s+t}}{2}\right\rfloor\right)} \right] \tag{57}
\]

\[
\leq 2E\left[ e^{-\frac{\delta^2}{2}g^2\left(\left\lfloor \frac{N_{s+t}}{2}\right\rfloor - 1\right)} \right] \tag{58}
\]

\[
\leq 2e^{\frac{\delta^2}{4}}e^{-\frac{\delta^2}{2}g^2\alpha(t-s)} \tag{59}
\]

\[
< 3e^{\frac{\delta^2}{4}}g^2\alpha(t-s) \tag{60}
\]

where (56) is due to Lemma 4 and Proposition 10. (59) is due to Lemma 11.

Note that the moment generating function for a Poisson random variable with parameter \( \lambda \) is \( e^{\lambda(e^u - 1)} \).

We have

\[
P\left( E_{\frac{1}{2}[s, t]}^c \right) = P\left( Z[s, t] \geq E[Z[s, t]] + \delta E[Y[s, t]] \right) \tag{61}
\]

\[
< E\left[ e^{u(Z[s, t] - E[Z[s, t]] - \delta E[Y[s, t]])} \right] \tag{62}
\]

\[
= \frac{E\left[ e^{u Z[s, t]} \right]}{e^{\beta(t-s)(e^u - 1)}} \tag{63}
\]

\[
= \frac{e^{\beta(t-s)(e^u - 1)}}{e^{\beta(t-s)u + \frac{1}{2}\beta(t-s)u + \frac{1}{2}\delta g^2\alpha(t-s)u}} \tag{64}
\]

\[
\leq \frac{e^{\beta(t-s)u + \frac{1}{2}\beta(t-s)u + \frac{1}{2}\delta g^2\alpha(t-s)u}}{e^{\beta(t-s)(e^u - 1)}} \tag{65}
\]

\[
= e\left( e^u - u(1 + \frac{1}{2}) \right)\beta(t-s) - \frac{1}{2}\delta g^2\alpha(t-s)u, \tag{66}
\]
where (65) is due to $g^2 \alpha \geq \beta$. Picking $u = \log(1 + \frac{\delta}{2})$, we have
\[
P(E_4^c[s, t]) < e^{(e^u - 1 - u(1 + \frac{\delta}{2}))\beta(t-s) - \frac{1}{2}g^2\alpha(t-s)u},
\]
(67)
\[
< e^{-\frac{\delta}{2} \log(1 + \frac{\delta}{2})g^2\alpha(t-s)}
\]
(68)
\[
< e^{-\frac{g^2}{2}\alpha(t-s)}
\]
(69)
where (68) is due to $\frac{\delta}{2} - (1 + \frac{\delta}{2}) \log(1 + \frac{\delta}{2}) < 0$ for all $\delta \in (0, 1)$ and (69) is due to $\log(1 + \frac{\delta}{2}) > \frac{\delta}{3}$ for all $\delta \in (0, 1)$.

By (46), (52), (60), and (69), we have
\[
P\left(E^\delta[s, t]\right) = 1 - P\left((E^\delta[s, t])^c\right)
\]
(70)
\[
\geq 1 - P\left((E_4^\delta[s, t])^c\right) - P\left((E_3^\delta[s, t])^c\right) - P\left((E_2^\delta[s, t])^c\right) - P\left((E_1^\delta[s, t])^c\right)
\]
(71)
\[
> 1 - 7e^{-\frac{1}{2}g^2\alpha(t-s)}
\]
(72)
where (72) is due to $g < 1$.

Note that Lemma [12] reflects the law of large numbers by stating the probability of $(E^\delta[s, t])^c$ vanishes exponentially with $t - s$.

**Definition 13.** (Typical event) The $\delta$-typical event on interval $(s, t]$ is defined as:
\[
G^\delta[s, t] = \cap_{a, b \in \mathbb{R}, 0 \leq a \leq s, 0 \leq b} E^\delta[s - a, t + b].
\]
(73)

**Definition 14.** For $0 \leq s < t$, define
\[
J^\delta[s, t] = \left(\cap_{k, \ell \in \mathbb{Z}, 0 \leq k \leq \lfloor s \rfloor, 0 \leq \ell} E^\delta[\lfloor s \rfloor - k, \lceil t \rceil + \ell]\right).
\]
(74)

**Lemma 15.** For all real numbers $0 \leq s < t - \frac{4}{\delta}$,
\[
J^\delta[s, t] \subset G^\delta[s, t].
\]
(75)

**Proof.** We note that the event $G^\delta[s, t]$ occurs when the events $E^\delta[s - a, t + b]$ simultaneously occurs for all real number $0 \leq a \leq s$ and $b \geq 0$. The $G$ event is defined as the intersection of uncountably many $E$ events, whereas the $J$ event is defined as the intersection of countably many. Bounding the probability of the $G$ event by the $J$ event eases the calculation. For every $0 \leq a \leq s$ and $b \geq 0$, we show that $E^\delta[s - a, t + b]$ occurs if $J^\delta[s, t]$ occurs:

Note that $J^\delta[s, t]$ indicates $E^\delta[\lfloor s \rfloor - k, \lceil t \rceil + \ell]$ for all integers $0 \leq k \leq \lfloor s \rfloor$ and $0 \leq \ell$. For every $0 \leq a \leq s$ and $b \geq 0$, let $k = \lfloor s \rfloor - \lfloor s - a \rfloor$ and $\ell = \lceil t + b \rceil - \lfloor t \rfloor$, we know
\[
E^\delta[\lfloor s \rfloor - k, \lceil t \rceil + \ell] = E^\delta[\lfloor s - a \rfloor, \lceil t + b \rceil]
\]
(76)
occurs. Similarly, let \( k = \lceil s \rceil - \lfloor s - a \rfloor \) and \( \ell = \lceil t + b \rceil - \lfloor t \rfloor \), we know
\[
\mathbb{E}^s_\delta [[s] - k, [t] + \ell] = \mathbb{E}^s_\delta [[s - a], [t + b]]
\]  
(77)
occurs.

To prove \( \mathbb{E}^s_\delta[s - a, t + b] \) occurs, we have

\[
N[s - a, t + b] \geq N\lfloor s - a \rfloor, \lfloor t + b \rfloor \]
(78)
> (1 - \frac{\delta}{3})\mathbb{E}[N\lfloor s - a \rfloor, \lfloor t + b \rfloor] 
(79)
= (1 - \frac{\delta}{3})\alpha([t + b] - \lfloor s - a \rfloor) 
(80)
\geq (1 - \frac{\delta}{3})\alpha(t - s + a + b - 2) 
(81)
= (1 - \frac{\delta}{3})\alpha(t - s + a + b)(1 - \frac{2}{t - s + a + b}) 
(82)
> (1 - \frac{\delta}{3})(1 - \frac{\delta}{2})\alpha(t - s + a + b) 
(83)
> (1 - \delta)\mathbb{E}[N[s - a, t + b]] 
(84)

where (79) is due to (2), (80) is due to Lemma 5, and (82) is due to \( t - s > \frac{4}{\delta} \). Also,

\[
N[s - a, t + b] < N\lfloor s - a \rfloor, \lfloor t + b \rfloor \]
(85)
< (1 + \frac{\delta}{3})\mathbb{E}[N\lfloor s - a \rfloor, \lfloor t + b \rfloor] 
(86)
= (1 + \frac{\delta}{3})\alpha([t + b] - \lfloor s - a \rfloor) 
(87)
\leq (1 + \frac{\delta}{3})\alpha(t - s + a + b + 2) 
(88)
= (1 + \frac{\delta}{3})\alpha(t - s + a + b)(1 + \frac{2}{t - s + a + b}) 
(89)
< (1 + \frac{\delta}{3})(1 + \frac{\delta}{2})\alpha(t - s + a + b) 
(90)
< (1 + \delta)\mathbb{E}[N[s - a, t + b]] 
(91)

where (86) is due to (2), (87) is due to Lemma 5, and (89) is due to \( t - s > \frac{4}{\delta} \).

To prove \( \mathbb{E}^s_\delta[s - a, t + b] \) occurs, we have

\[
X[s - a, t + b] > X\lfloor s - a \rfloor, \lfloor t + b \rfloor 
\]  
(92)
> (1 - \frac{\delta}{3})\mathbb{E}[X\lfloor s - a \rfloor, \lfloor t + b \rfloor] 
(93)
= (1 - \frac{\delta}{3})g\alpha([t + b] - \lfloor s - a \rfloor) 
(94)
> (1 - \frac{\delta}{3})g\alpha(t - s + a + b - 2) 
(95)
\[ g_t(\mathcal{X}) \]

where (93) is due to (3), (94) is due to Lemma 6, and (96) is due to \( t - s > \frac{4}{\delta} \).

To prove \( E_3^\delta[s - a, t + b] \) occurs, we have

\[ Y[s - a, t + b] > Y[[s - a], [t + b]] \]
\[ > (1 - \frac{\delta}{3})\mathbb{E}[Y[[s - a], [t + b]]] \]
\[ = (1 - \frac{\delta}{3})g^2\alpha([t + b] - Y[[s - a]]) \]
\[ > (1 - \frac{\delta}{3})g^2\alpha(t - s + a + b - 2) \]
\[ = (1 - \frac{\delta}{3})g^2\alpha(t - s + a + b)(1 - \frac{2}{t - s + a + b}) \]
\[ > (1 - \frac{\delta}{3})(1 - \frac{\delta}{2})g^2\alpha(t - s + a + b) \]
\[ > (1 - \delta)\mathbb{E}[Y[s - a, t + b]] \]

where (100) is due to (4), (101) is due to Lemma 7 and (103) is due to \( t - s > \frac{4}{\delta} \).

At last, to prove \( E_4^\delta[s - a, t + b] \) occurs, we have

\[ Z[s - a, t + b] < Z[[s - a], [t + b]] \]
\[ < \mathbb{E}[Z[[s - a], [t + b]] + \frac{\delta}{3}\mathbb{E}[Y[[s - a], [t + b]]] \]
\[ = \beta([t + b] - [s - a]) + \frac{\delta}{3}g^2\alpha([t + b] - [s - a]) \]
\[ < \beta(t - s + a + b + 2) + \frac{\delta}{3}g^2\alpha(t - s + a + b + 2) \]
\[ = \beta(t - s + a + b)(1 + \frac{2}{t - s + a + b}) + \frac{\delta}{3}g^2\alpha(t - s + a + b)(1 + \frac{2}{t - s + a + b}) \]
\[ < (1 + \frac{\delta}{2})\beta(t - s + a + b) + (1 + \frac{\delta}{2})\frac{\delta}{3}g^2\alpha(t - s + a + b) \]
\[ < \beta(t - s + a + b) + \frac{\delta^2}{g}\alpha(t - s + a + b) \]
\[ = \mathbb{E}[Z[s - a, t + b]] + \delta\mathbb{E}[Y[s - a, t + b]]. \]

where (107) is due to (5) and (112) is due to (23).
To sum up, under $J_\delta[s,t]$, all real number $0 \leq a \leq s$ and $b \geq 0$, all $E_1^\delta[s-a,t+b]$, $E_2^\delta[s-a,t+b]$, $E_3^\delta[s-a,t+b]$, and $E_4^\delta[s-a,t+b]$ occur. Thus $E_\delta^\delta[s-a,t+b]$ occurs for all valid $a$ and $b$. Thus the occurrence of $G_\delta^\delta[s,t]$. □

For convenience, let
\[ \eta = \frac{1}{72} \delta^2 g^2 \alpha. \] (114)

**Lemma 16.** For all real numbers $0 \leq s < t - \frac{4}{5}$,
\[ P(G_\delta^\delta[s,t]) > 1 - 9\eta^{-2}e^{-\eta(t-s)}. \] (115)

**Proof.**
\[
P(G_\delta^\delta[s,t]) < P(J_\delta^\delta[s,t]) \]
\[
= P \left( \cap_{k,\ell \in \mathbb{Z}, 0 \leq k \leq [s], 0 \leq \ell} E_5^\delta \left[ k, [t] + \ell \right] \right) \]
\[
< \sum_{k,\ell \in \mathbb{Z}, 0 \leq k \leq [s], 0 \leq \ell} 7e^{-\frac{1}{2} \left( \frac{5}{2} \right)^2 g^2 \alpha (|t| - [s] + k + \ell)} \]
\[
< \sum_{k,\ell \in \mathbb{Z}, 0 \leq k \leq [s], 0 \leq \ell} 7e^{-\frac{1}{2} \left( \frac{5}{2} \right)^2 g^2 \alpha (t-s+k+\ell-2)} \]
\[
< \sum_{m=0}^{\infty} 7(m + 1)e^{-\frac{1}{2} \left( \frac{5}{2} \right)^2 g^2 \alpha (t-s+m-2)} \]
\[
= \frac{7e^{\frac{1}{2} \delta^2 g^2 \alpha}}{(1 - e^{-\frac{1}{2} \left( \frac{5}{2} \right)^2 g^2 \alpha})^2} e^{-\frac{1}{2} \left( \frac{5}{2} \right)^2 g^2 \alpha (t-s)} \]
\[
< 9\eta^{-2}e^{-\eta(t-s)} \] (122)

where (122) is due to $1 - e^{-x} > \sqrt{\frac{8}{9}}x$ for $x \in (0, \frac{1}{72})$ and $e^{\frac{1}{72}} < \frac{8}{9}$. □

**Lemma 17.** *(Lemma 4 in [9])* Laggers have different heights.

**Proof.** Suppose two laggers, $B$ and $B'$, have the same height $k$. Let $t$ and $t'$ denote the time $B$ and $B'$ are mined, respectively. Without loss of generality, we assume $t < t'$. Then we have $t' > t + \Delta$ by the assumption that $B'$ is a lagger. On the other hand, all honest miners will extend a blockchain equal or longer than $k$ after time $t + \Delta$. So the height of $B'$ cannot be $k$, contradicting the assumption. □

**Lemma 18.** *(Lemma 4 in [9])* Suppose some honest blockchain’s $k$th block $B$ is a loner, then the $k$th block of every blockchain is either $B$ or an adversarial block.
Proof. Suppose block \( B \) is a loner of height \( k \) in an honest blockchain, and the \( k \)th block of another blockchain is \( B' \neq B \). Assume \( B \) and \( B' \) are mined at time \( t \) and \( t' \), respectively. Since \( B \) is a loner we must have \( t' < t - \Delta \) or \( t' > t + \Delta \). If \( t' < t - \Delta \), all honest blocks mined after \( t' + \Delta \) will extend a blockchain equal or longer than \( k \). If \( t' > t + \Delta \), all honest blocks mined after \( t + \Delta \) will extend a blockchain equal or longer than \( k \). Both contradict the assumption that \( B \) and \( B' \) are both of height \( k \).

\[ \square \]

**Lemma 19.** For all real numbers \( \delta, s, t, \) and integer \( k \) satisfying \( 0 \leq s < t \), \( 0 < \delta < 1 \), and \( k \geq (2 - \delta)\alpha(t - s) \), under event \( G^\delta[s, t] \), every honest miner’s \( k \)-deep block at time \( t \) must be mined no later than \( s \).

**Proof.** The blockchain growth of an honest miner during time interval \((s, t]\) is upper bounded by \( N[s, t] + Z[s, t] \). Note that under \( G^\delta[s, t] \),

\[
N[s, t] + Z[s, t] < (1 + \delta)\alpha(t - s) + \beta(t - s) + \delta g^2\alpha(t - s) \tag{123}
\]

\[
< (1 + \delta)\alpha(t - s) + (1 - 2\delta)g^2\alpha(t - s) \tag{124}
\]

\[
< (1 + \delta)\alpha(t - s) + (1 - 2\delta)\alpha(t - s) \tag{125}
\]

\[
< (2 - \delta)\alpha(t - s) \tag{126}
\]

where (123) is due to (2) and (4), and (124) is due to (23). Thus, the \( k \)-deep block must be mined no later than \( s \). \( \square \)

**Theorem 20.** (Blockchain growth theorem) Let \( 0 \leq r < s < t - \frac{2\Delta}{\delta} \). Then under \( \delta \)-typical event \( G^\delta[s + \Delta, t - \Delta] \), the height of every honest blockchain increases by at least \((1 - \delta)^2g\alpha(t - r)\) during \((r, t]\).

**Proof.** Assume an honest miner adopts a blockchain of height \( \ell \) at time \( r \). Then at time \( r + \Delta \), all honest miners have adopted a blockchain of height at least \( \ell \). Moreover, \( G^\delta[s + \Delta, t - \Delta] \) indicates \( E^\delta[s + \Delta, t - \Delta] \) occurs. Then, during time interval \((r + \Delta, t - \Delta]\), the number of laggers is at least

\[
(1 - \delta)g\alpha(t - r - 2\Delta)
\]

\[
= (1 - \delta)g\alpha \frac{t - r - 2\Delta}{t - r} (t - r) \tag{127}
\]

\[
> (1 - \delta)^2g\alpha(t - r) \tag{128}
\]

where (128) is due to \( \frac{2\Delta}{t - r} < \delta \). According to Lemma 17 these laggers have different heights, and they arrive at all honest miners by time \( t \). Thus, the honest miner must adopt a blockchain whose height is at
least $\ell + (1 - \delta)^2 g \alpha (t - r)$ at time $t$.

\[\square\]

**Theorem 21.** (Blockchain quality theorem) For integer $k \geq \frac{2(2-\delta)\alpha(\Delta+2)}{\delta}$, in any $k$ consecutive blocks, the fraction of honest blocks is at least $1 - (1 - \delta^2)g$ with probability at least $1 - 9\eta e^{-\frac{\beta(1-\delta)k}{(1-\delta)g}}$.

**Proof.** The intuition is that under typical event, an honest miner’s blockchain grow by at least $X[s + \Delta, t - \Delta]$ according to Lemma 17. Meanwhile, the number of adversarial blocks mined is upper bounded by (5). Thus, at least certain fraction of blocks must be honest even in the worst case that all adversarial blocks are included in the blockchain.

To be precise, assume the head and tail of these $k$ blocks are at height $h_0$ and $h_1$, respectively. Let block $h_0'$ be the highest honest block on the same blockchain which is mined before block $h_0$. $h_0'$ can be as high as $h_0 - 1$ and as small as 0. Assume block $h_0'$ is mined at time $t_0$. If this block is the genesis block, then $t_0 = 0$. If there is any honest block mined after $h_1$ on the same blockchain, we denote the lowest as $h_1'$ and denote the time it is mined as $t_1$; otherwise let $t_1$ be the current time and let be $h_1'$ be current height plus 1.

By definition, the blocks at heights $\{h_0' + 1, \ldots, h_0 - 1\}$ and $\{h_1 + 1, \ldots, h_1' - 1\}$ are adversarial. Assume event $G_{t_0 + \Delta, t_1 - \Delta}$ occurs. Therefore,

\[t_1 - t_0 > \frac{k}{(2 - \delta)\alpha} \tag{129}\]
\[> \frac{2\Delta}{\delta} + \frac{4}{\delta}, \tag{130}\]

where (129) is by Lemma 19 and (130) is by $k \geq \frac{2(2-\delta)\alpha(\Delta+2)}{\delta}$.

Denote the number of adversarial blocks between block $h_0$ (inclusive) and block $h_1$ (inclusive) as $z$. We have

\[
\frac{z}{k} \leq \frac{z + (h_0 - h_0' - 1) + (h_1' - h_1 - 1)}{k + (h_0 - h_0' - 1) + (h_1' - h_1 - 1)} \leq \frac{Z[t_0, t_1]}{Z[t_0, t_1]} \leq \frac{Z[t_0, t_1]}{(1 - \delta)^2 g \alpha (t_1 - t_0)} < \frac{\beta(t_1 - t_0) + \delta g^2 \alpha (t_1 - t_0)}{(1 - \delta)^2 g \alpha (t_1 - t_0)} = \frac{1}{(1 - \delta)^2} \left( \frac{\beta}{g \alpha} + \delta g \right) < \frac{1}{(1 - \delta)^2} (1 - 3\delta) g + \delta g < (1 - \delta^2) g, \tag{131}
\]

\[
\leq \frac{k + (h_0 - h_0' - 1) + (h_1' - h_1 - 1)}{Z[t_0, t_1]} \leq \frac{Z[t_0, t_1]}{(1 - \delta)^2 g \alpha (t_1 - t_0)} < \frac{\beta(t_1 - t_0) + \delta g^2 \alpha (t_1 - t_0)}{(1 - \delta)^2 g \alpha (t_1 - t_0)} = \frac{1}{(1 - \delta)^2} \left( \frac{\beta}{g \alpha} + \delta g \right) < \frac{1}{(1 - \delta)^2} (1 - 3\delta) g + \delta g < (1 - \delta^2) g, \tag{132}
\]

\[
\leq \frac{Z[t_0, t_1]}{(1 - \delta)^2 g \alpha (t_1 - t_0)} < \frac{\beta(t_1 - t_0) + \delta g^2 \alpha (t_1 - t_0)}{(1 - \delta)^2 g \alpha (t_1 - t_0)} = \frac{1}{(1 - \delta)^2} \left( \frac{\beta}{g \alpha} + \delta g \right) < \frac{1}{(1 - \delta)^2} (1 - 3\delta) g + \delta g < (1 - \delta^2) g, \tag{133}
\]

\[
< \frac{1}{(1 - \delta)^2} (1 - 3\delta) g + \delta g < (1 - \delta^2) g, \tag{134}
\]
where (131) is due to \( z \leq k \). Since all blocks within height \( \{h'_0 + 1, \ldots, h_0\} \) and \( \{h_1, \ldots, h'_1 - 1\} \) are adversarial, \( z + (h_0 - h'_0 - 1) + (h'_1 - h_1 - 1) \) is the number of adversarial blocks between block \( h'_0 + 1 \) and block \( h'_1 - 1 \). These adversarial blocks are after block \( h'_0 \) so they must be mined within time \((t_0, t_1]\), thus we have (132). On the other hand, during \((t_0, t_1]\) the blockchain’s length increases by at least \( k + (h_0 - h'_0 - 1) + (h'_1 - h_1 - 1) \). This number is no less than \((1 - \delta)^2 g \alpha (t_1 - t_0)\) by Theorem 20. Thus we have (133). (134) is due to (5), (136) is due to (23), and (137) is due to \( \delta \in (0, 1) \).

Note that according to (130), we know \( t_1 - t_0 - 2\Delta > \frac{4}{\delta} \). According to Lemma 16,

\[
P(G^{\delta}[t_0 + \Delta, t_1 - \Delta]) > 1 - 9\eta^{-2} e^{-\eta(t_1 - t_0 - 2\Delta)} \tag{138}
\]
\[
\geq 1 - 9\eta^{-2} e^{-\eta(1-\delta)(t_1 - t_0)} \tag{139}
\]
\[
> 1 - 9\eta^{-2} e^{\frac{-\eta(1-\delta)k}{(2-\delta)\alpha}} \tag{140}
\]

To sum up, with probability at least \( 1 - 9\eta^{-2} e^{\frac{-\eta(1-\delta)k}{(2-\delta)\alpha}} \), event \( G^{\delta}[t_0 + \Delta, t_1 - \Delta] \) occurs, under which the fraction of honest blocks is ensured.

\[
\]

**Definition 22.** Let \( t > 0 \). A block or a sequence (of blocks) is said to be permanent after \( t \) if the block or sequence remains in all honest blockchains starting from \( t \).

**Definition 23.** Let \( t > 0 \). A block or a sequence (of blocks) is said to be \( \epsilon \)-permanent after \( t \) if with probability at least \( 1 - \epsilon \), the block or sequence is permanent after time \( t \).

**Theorem 24.** (Common prefix theorem) Suppose real numbers \( s, t, \delta \) and integer \( k \) satisfy \( 0 \leq s < t - \frac{2\Delta}{\delta} \), \( 0 < \delta < 1 \), and \( k \geq (2 - \delta)\alpha (t - s) \). Suppose an honest blockchain has a \( k \)-deep prefix at time \( t \), then under \( G^{\delta}[s + \Delta, t - \Delta] \), the prefix is permanent after \( t \).

**Proof.** The intuition is based on Lemma 18. If a block is a loner, 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 for every loner after the common prefix. This can not be true under certain typical event because the number of loner is lower bounded and the number of adversarial blocks are upper bounded.

To be precise, we prove the desired result by contradiction. Let \( B^* \) be the last block of this blockchain’s \( k \)-deep prefix. Let \( C_1 \) be the first honest blockchain that does not extend \( B^* \). Assume \( C_1 \) is adopted by some honest miner right after \( t_1 \). Then at time \( t_1 \), an honest miner adopts a blockchain that extends \( B^* \), denote this blockchain as \( C'_1 \). Assume blockchain \( C_1 \) and blockchain \( C'_1 \) end with block \( B_1 \) and \( B'_1 \).
respectively. Assume $B_0$ is the last common ancestor of $C_1$ and $C'_1$. Assume $B'_0$ is the last honest block on the common prefix of $C_1$ and $C'_1$ ($B'_0$ can be the same as $B_0$). Let $t_0$ be the time $B'_0$ is mined.

According to Lemma 19, since $B'_0$ is at least $k$ blocks deep and $k \geq (2 - \delta)\alpha(t - s)$, we know $t_0 < s$. Thus, $G^{\delta}[s + \Delta, t - \Delta]$ indicates $G^{\delta}[t_0 + \Delta, t_1 - \Delta]$ occurs. We have

\begin{align*}
Y[t_0 + \Delta, t_1 - \Delta] &> (1 - \delta)g^2\alpha(t_1 - t_0 - 2\Delta) \\
&= (1 - \delta)\frac{t_1 - t_0 - 2\Delta}{t_1 - t_0}g^2\alpha(t_1 - t_0) \\
&> (1 - \delta)^2g^2\alpha(t_1 - t_0) \\
&> (1 - 3\delta)g^2\alpha(t_1 - t_0) + \delta g^2\alpha(t_1 - t_0) \\
&> \beta(t_1 - t_0) + \delta g^2\alpha(t_1 - t_0) \\
&> Z[t_0, t_1]
\end{align*}

where (141) is due to (4), (143) is due to $t_1 - t_0 > t - s > \frac{2\Delta}{\delta}$, (144) is due to (23), and (146) is due to (5).

On the other hand, we will show $Z[t_0, t_1] > Y[t_0 + \Delta, t_1 - \Delta]$ under the above scenario. Assume the heights of $B_0, B'_0, B_1,$ and $B'_1$ are $h_0, h'_0, h_1,$ and $h'_1$ respectively. Since some honest miner adopts
Consider a loner $B$ which is mined within time interval $(t_0 + \Delta, t_1 - \Delta]$. Assume $B$’s height is $h$. Since $B'_0$ is mined at time $t_0$, every honest miner has received a blockchain of height at least $h'_0$ by time $t_0 + \Delta$, thus $h > h'_0$. What is more, if $h > h'_1$ and $B$ is mined by time $t_1 - \Delta$, blockchain $C'_1$ (with height $h'_1$) will not be the highest blockchain at time $t_1$, and no honest miner will adopt it. Thus, $h \leq h'_1$.

We have $h \in (h'_0, h'_1]$.

If $h'_0 < h \leq h_0$, according to our definition, the blocks at height $h$ of blockchain $C_1$ and blockchain $C'_1$ are adversarial. If $h_0 < h \leq h'_1$, there are at least two different blocks at position $h$ since there are at least two diverging blockchains. According to Lemma 18 at least one of the position $h$ blocks are adversarial. That is to say, for any loner $B$ mined within $(t_0 + \Delta, t_1 - \Delta]$, we can find at least one adversarial block. The adversarial blocks whose height is within $(h'_0, h'_1]$ must be mined within $(t_0, t_1]$, thus, we have $Y[t_0 + \Delta, t_1 - \Delta] \geq Z[t_0, t_1]$. Contradiction arises, hence the proof of the theorem. \qed

**Corollary 25.** For integer $k \geq \frac{2(2-\delta)\alpha(\Delta+2)}{\delta}$, suppose an honest blockchain has a $k$-deep prefix at time $t$, then its $k$-prefix is permanent after $t$ with probability at least $1 - 9\eta^{-2}e^{\frac{-n(1-\delta)k}{(2-\delta)\alpha}}$.

**Proof.** Denote $s = t - \frac{k}{(2-\delta)\alpha}$. Then,

$$s - t = \frac{k}{(2-\delta)\alpha} \geq \frac{2\Delta}{\delta} + \frac{4}{\delta} .$$

According to Theorem 24 the $k$-deep prefix is permanent under event $G^\delta[s + \Delta, t - \Delta]$, whose probability is lower bounded by

$$P(G^\delta[s + \Delta, t - \Delta]) > 1 - 9\eta^{-2}e^{-\eta(t-s-2\Delta)}$$

$$\geq 1 - 9\eta^{-2}e^{-\eta(1-\delta)(t-s)}$$

$$= 1 - 9\eta^{-2}e^{-\frac{n(1-\delta)k}{(2-\delta)\alpha}} .$$

\qed

In this section, we have defined typical events, studied the properties of various blocks under these events, and bound the probability of them. The blockchain growth theorem, the blockchain quality theorems, and the common prefix theorem of bitcoin blockchains are proved for the bitcoin backbone protocol, which guarantee the liveliness and consistency of bitcoin blockchains. In essence, bitcoin transactions deep enough in any honest blockchain are with high probability guaranteed to remain in
the final ledger. This framework can naturally extend to Prism protocol which is based on Nakamoto consensus.

III. THE PRISM BACKBONE PROTOCOL

The Prism protocol is invented and fully described in [7]. 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 at time 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 \([j\gamma, j\gamma + \gamma)\) for \( j = 0, 1, \ldots, m \), the mined block belongs to blockchain \( i \).

To certify its level, a new honest voter block for blockchain \( j \) points to blockchain \( j \)’s maximum-level block by a parent link. In addition, an honest new proposer block 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-chain rule. The miner determines the its main blockchain by votes from the main voter blockchains. By saying block \( B \) 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). 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 \( B_0B_1 \ldots B_l \), 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. 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.

To analyze the Prism protocol, we first define laggers, loners, and typical events for the proposer blockchain or each voter blockchain. For each blockchain \( j (j = 0, 1, \ldots, m) \), let homogeneous Poisson point process \( (H_{t,j}, t \geq 0) \) denote the total number of honest blocks mined up until time \( t \). Also, there exists an homogeneous Poisson point process \( (Z_{t,j}, t \geq 0) \) that dominates the generation of adversarial blocks. The mining difficulty can be adjusted so that \( H_{t,j} \) has parameter \( \alpha \) and \( Z_{t,j} \) has parameter \( \beta \) for
each $j$. Similar to that in the bitcoin protocol, an honest block mined at time $t$ in blockchain $j$ is called a lagger if it is mined strictly more than $\Delta$ seconds after the last honest block on blockchain $j$ is mined. The lagger is also called a loner if the next block mined is also a lagger.

Let $N_j[s, t] = H_{t,j} - H_{s,j}$, $X_j[s, t]$, and $Y_j[s, t]$ denote the number of honest blocks, laggers, and loners on blockchain $j$ mined during time interval $(s, t)$, respectively. Let $Z_j[s, t] = Z_{t,j} - Z_{s,j}$ upper bound the number of adversarial blocks on blockchain $j$ mined during $(s, t)$. As in the bitcoin protocol, we assume

\[(1 - 3\delta)g^2 \alpha > \beta.\]  

**Definition 26.** For all non-negative real numbers $0 \leq s < t$, $0 < \delta < 1$, and integer $0 \leq j \leq m$, define

\[E^\delta_j[s, t] = E^\delta_{1,j}[s, t] \cap E^\delta_{2,j}[s, t] \cap E^\delta_{3,j}[s, t] \cap E^\delta_{4,j}[s, t] \]  

where

\[E^\delta_{1,j}[s, t] = \{(1 - \delta)E[N_j[s, t]] < N_j[s, t] < (1 + \delta)E[N_j[s, t]]\} \]  
\[E^\delta_{2,j}[s, t] = \{(1 - \delta)E[X_j[s, t]] < X_j[s, t]\} \]  
\[E^\delta_{3,j}[s, t] = \{(1 - \delta)E[Y_j[s, t]] < Y_j[s, t]\} \]  
\[E^\delta_{4,j}[s, t] = \{Z_j[s, t] < E[Z_j[s, t]] + \delta E[Y_j[s, t]]\}. \]

**Lemma 27.** For all $0 < \delta < 1$ and $0 \leq s < t$, we have

\[P(E^\delta_j[s, t]) > 1 - 7e^{-\frac{1}{2}g^2 \alpha(t-s)}.\]  

**Definition 28.** *(Typical event for blockchain $j$)* The $\delta$-typical event on time interval $(s, t]$ is defined as:

\[G_j[s, t] = \cap_{a, b \in \mathbb{R}, 0 \leq a \leq s, 0 \leq b} E^\delta_j[a, t + b] \]

**Lemma 29.** For all real numbers $0 \leq s < t - \frac{4}{\delta}$ and integer $0 \leq j \leq m$,

\[P(G_j[s, t]) > 1 - 9\eta^{-2}e^{-\eta(t-s)}.\]  

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. Meanwhile, the blockchain quality theorem and the common prefix theorem only extend to all voter blockchains, since the leader sequence is decided by voting instead of the longest-chain rule.
Lemma 30. For all real numbers $\delta, s, t,$ and integer $k, j$ satisfying $0 \leq s < t$, $0 < \delta < 1$, $k \geq (2 - \delta)\alpha(t - s)$, and $0 \leq j \leq m$, under event $G_j[s, t]$, every honest miner’s $k$-deep block at time $t$ must be mined no later than $s$.

Proof. For $j = 0, \ldots, m$, the lemma admits essentially the same proof at that for Lemma 19.

Theorem 31. (Blockchain growth theorem for proposer and voter blockchains) Let $0 \leq r < s < t - \frac{2\Delta}{\delta}$. Then under $\delta$-typical event $G^\delta[s + \Delta, t - \Delta]$, the height of every honest blockchain increases by at least $(1 - \delta)^2g\alpha(t - r)$ during $(r, t]$.

Proof. For $j = 0, \ldots, m$, the theorem admits essentially the same proof at that for Theorem 20.

Theorem 32. (Blockchain quality theorem for voter blockchains) For integer $k \geq \frac{2(2 - \delta)\alpha(\Delta + 2)}{\delta} \eta \alpha(t - r)$, and $0 \leq j \leq m$, in any $k$ consecutive blocks of blockchain $j$, the fraction of honest blocks is at least $1 - (1 - \delta^2)g$ with probability at least $1 - 9\eta^{-2}e^{-\frac{(t-r-k)}{12-9m}}$.

Proof. For $j = 1, \ldots, m$, the theorem admits essentially the same proof at that for Theorem 21.

Theorem 33. (Common prefix theorem for the voter blockchains) Suppose real numbers $s, t, \delta$ and integer $k, j$ satisfy $0 \leq s < t - \frac{2\Delta}{\delta}$, $0 < \delta < 1$, $k \geq (2 - \delta)\alpha(t - s)$ and $0 \leq j \leq m$. Suppose an honest blockchain $j$ has a $k$-deep prefix at time $t$, then under $G^\delta[s + \Delta, t - \Delta]$, the prefix is permanent after $t$.

Proof. For $j = 1, \ldots, m$, the theorem admits essentially the same proof at that for Theorem 24.

Definition 34. We let $\text{LedSeq}_l(t)$ denote the proposer blockchain’s leader sequence up to level $l$ at time $t$.

Theorem 35. Fix $\epsilon \in (0, 1)$. Let $T_l$ be the time when the first proposer block on level $l$ is mined. For real number

$$t > \frac{3(2 - \delta)}{\eta(1 - \delta)^3g} \log \left(\frac{18m}{\epsilon\eta^2}\right)$$

(161)

$\text{LedSeq}_l(T_l + t)$ is permanent after time $T_l + t$.

Proof. Denote

$$k = \left\lceil \frac{(2 - \delta)\alpha}{\eta(1 - \delta)} \log \left(\frac{18}{\epsilon\eta^2}\right) \right\rceil.$$ 

(162)
Consider voter blockchain 1. According to Theorem 20, under event $G^\delta_1[T_l + \Delta, T_l + t - \Delta]$, voter blockchain 1 grows by at least

\[
(1 - \delta)^2 g_{\alpha t} = \frac{3(2 - \delta)\alpha}{\eta(1 - \delta)} \log \left( \frac{18m}{e\eta^2} \right) > 2k \tag{163}
\]

where (164) is due to \( \frac{(2 - \delta)\alpha}{\eta(1 - \delta)} \log \left( \frac{18}{e\eta^2} \right) \geq 2 \). Note that the probability of $G^\delta_1[T_l + \Delta, T_l + t - \Delta]$ is at least

\[
1 - 9\eta^{-2} e^{-\eta(t - 2\Delta)} > 1 - \frac{e}{3m} \tag{165}
\]

where (165) is due to (161). Also, according to Corollary 25 voter blockchain 1’s $k$-prefix is permanent with probability at least

\[
1 - 9\eta^{-2} e^{-\eta(t - 2\Delta)} > 1 - \frac{e}{3m} \tag{166}
\]

where (166) is due to (161). What is more, according to Theorem 21 the last $k$ blocks of voter blockchain 1’s $k$-prefix contain at least $1 - (1 - \delta^2)g$ fraction of honest blocks with probability at least

\[
1 - 9\eta^{-2} e^{-\eta(t - 2\Delta)} > 1 - \frac{e}{3m} \tag{167}
\]

where (167) is also due to (161). That is to say, there is at least one honest block in the last $k$ blocks of voter blockchain 1’s $k$-prefix.

Combine (165), (166) and (167), with probability at least $1 - \frac{e}{m}$, voter blockchain 1 has at least one honest block which is permanent after time $T_l + t$, and this honest block is mined after $T_l$. This block must have voted for all levels up to level $l$ of the proposer blockchain by the voting rule. By the union rule, with probability at least $1 - \epsilon$, all voter blockchains have their own honest block which is permanent after time $T_l + t$. These honest blocks have finalized their voting to level $l$. Thus, $\text{LedSeq}_l(t)$ is $\epsilon$-permanent.

Theorem 35 is an analogy to the common prefix theorem for the leader sequence. It guarantees the consistency of the proposer blockchain. In addition, we can guarantee the quality of the leader sequence by the following theorem:

**Theorem 36.** (Blockchain quality theorem for proposer blockchain) For integer $k \geq \frac{2(2-\delta)\alpha(\Delta+2)}{\delta}$, any $k$ consecutive leader blocks of the proposer blockchain contain at least $1 - (1 - \delta^2)g$ fraction of honest blocks with probability at least $1 - 9\eta^{-2} e^{-\frac{\eta(t - 2\Delta)}{(2-\delta)m}}$.

**Proof.** Assume the head and tail of these $k$ blocks are at level $h_0$ and $h_1$, respectively. Let $h'_0$ be the highest level strictly before $h_0$ on which the first proposer block is honest. $h'_0$ can be as high as $h_0 - 1$
and as low as 0, which corresponds to the genesis block. Assume the first proposer block on level \( h'_0 \) is mined right before \( t_0 \). If this block is the genesis block, then \( t_0 = 0 \). Let \( h'_1 \) be the lowest level after \( h_1 \) on which the first proposer block is honest. Assume the first proposer block on level \( h'_1 \) is mined right after \( t_1 \). If such an \( h'_1 \) does not exist, let \( t_1 \) be the current time and let \( h'_1 \) be current level plus 1.

From definition, the first proposer block on every level within \( \{ h'_0 + 1, \ldots, h_0 \} \) and \( \{ h_1, \ldots, h'_1 - 1 \} \) is adversarial. From level \( h'_0 \) to level \( h'_1 - 1 \), there must be at least one adversarial block on every level except (possibly) on the levels between \( h_0 \) and \( h_1 \) where the leading block is honest.

Assume event \( G_0^\delta[t_0 + \Delta, t_1 - \Delta] \) occurs. According to Lemma 19, the number of blocks mined during \( (t_0, t_1] \) is at most \((2 - \delta)\alpha(t_1 - t_0)\). We have

\[
(2 - \delta)\alpha(t_1 - t_0) > k
\]

\[
t_1 - t_0 > \frac{k}{(2 - \delta)\alpha}
\]

\[
t_1 - t_0 > \frac{2\Delta}{\delta}.
\]

Let \( z \) be the number of adversarial blocks within \( \{ h_0, \ldots, h_1 \} \). We have

\[
z \leq \frac{z + (h_0 - h'_0 - 1) + (h'_1 - h_1 - 1)}{k + (h_0 - h'_0 - 1) + (h'_1 - h_1 - 1)}
\]

\[
\leq \frac{Z[t_0, t_1]}{X[t_0 + \Delta, t_1 - \Delta]}
\]

\[
< \frac{\beta(t_1 - t_0) + \delta g\alpha(t_1 - t_0)}{(1 - \delta)g\alpha(t_1 - t_0 - 2\Delta)}
\]

\[
= \frac{t_1 - t_0}{t_1 - t_0 - 2\Delta} \frac{1}{1 - \delta} \left( \frac{\beta}{g\alpha} + \delta g \right)
\]

\[
< \frac{1}{(1 - \delta)^2} \left( \frac{\beta}{g\alpha} + \delta g \right)
\]

\[
< \frac{1}{(1 - \delta)^2} ((1 - 3\delta)g + \delta g)
\]

\[
< (1 - \delta^2)g,
\]

where (171) is due to \( z \leq k \), (172) is because at least one block on level \( \{ h'_0 + 1, \ldots, h_0 \} \) and \( \{ h_1, \ldots, h'_1 - 1 \} \) is adversarial, (173) is due to Theorem 20 and (5), (176) is due to (23), and (177) is due to \( \delta \in (0, 1) \).

Also note that

\[
P(G_0^\delta[t_0 + \Delta, t_1 - \Delta]) > 1 - 9\eta^{-2}e^{-\eta(t_1 - t_0 - 2\Delta)}
\]

\[
> 1 - 9\eta^{-2}e^{-\eta(1 - \delta)(t_1 - t_0)}
\]

\[
> 1 - 9\eta^{-2}e^{-\eta\frac{1 - \delta}{(1 - \delta)\alpha}}
\]
To sum up, with probability at least \(1 - 9\eta^{-2}e^{-\frac{\eta(1-\delta)k}{(2-\delta)e}}\), event \(G^e_0|t_0 + \Delta, t_1 - \Delta\) occurs, under which the fraction of honest blocks is ensured.

**Definition 37.** A transaction is honest if it has been broadcast, and no other transaction spending from the same unspent output has been broadcast.

**Definition 38.** A transaction is said to be \(\epsilon\)-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 39.** Suppose right before time \(s\), the leader block on level \(l\) is honest. Suppose this leader block is mined at time \(t\). If an honest transaction enters a block and the block is broadcast before time \(t\), 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 time \(s\). 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.

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.

**Theorem 40.** For every \(\epsilon > 0\) and every real number

\[
t > \frac{5(2 - \delta)}{\eta(1 - \delta)g} \log \left( \frac{54m}{\epsilon\eta^2} \right)
\]

assume an honest transaction enters into a block and the block is broadcast at time \(s\). Then, the transaction is \(\epsilon\)-permanent after time \(s + t\).
Proof. Denote

\[ t_0 = \frac{2(2 - \delta)}{\eta(1 - \delta)^2} \log \left( \frac{54m}{\epsilon \eta^2} \right) \]  
(182)

and

\[ k = \left\lceil \frac{(2 - \delta)\alpha}{\eta(1 - \delta)} \log \left( \frac{54m}{\epsilon \eta^2} \right) \right\rceil. \]  
(183)

Denote the highest level of proposer blockchain right before time \( s \) is \( h \). Denote the highest level of proposer blockchain right before time \( s + t_0 \) is \( h_0 \). Then, the first proposer block on level \( h_0 \) is mined before \( s + t_0 \). According to Theorem 35, since \( t - t_0 \geq \frac{3(2 - \delta)}{\eta(1 - \delta)^2} \log \left( \frac{54m}{\epsilon \eta^2} \right) \), the leader sequence up to level \( h_0 \) is \( \xi \)-permanent after time \( s + t \).

According to Theorem 20, under event \( G_\delta^\Delta[s + \Delta, s + t_0 - \Delta] \), proposer blockchain grows by at least

\[ (1 - \delta)^2 g \alpha t_0 = \frac{2(2 - \delta)\alpha}{\eta(1 - \delta)} \log \left( \frac{54m}{\epsilon \eta^2} \right) \]  
(184)

\[ > k. \]  
(185)

Note that the probability of \( G_\delta^\Delta[s + \Delta, s + t_0 - \Delta] \) is at least

\[ 1 - 9\eta^{-2} e^{-\eta(t_0 - 2\Delta)} > 1 - 9\eta^{-2} e^{-\eta(1 - \delta)t_0} > 1 - \frac{\epsilon}{3} \]  
(186)

where (186) is due to (182). Also, according to Theorem 21, the blocks at the increased height (at least \( k \)) of the proposer proposer blockchain contain at least \( 1 - (1 - \delta)^2 g \) fraction of honest blocks with probability at least

\[ 1 - 9\eta^{-2} e^{-\eta(1 - \delta)k} > 1 - \frac{\epsilon}{3} \]  
(187)

where (187) is due to (183). That is to say, there is at least one honest leader block within levels \( \{h, \ldots, h_0\} \).

To sum up, combine (186) and (187), with probability at least \( 1 - \epsilon \), after time \( s + t \), the leader sequence up to level \( h_0 \) is permanent, and this leader sequence contains at least one honest block. According to Lemma 39, this honest leader block will include the honest transaction to the final ledger. \( \square \)

Theorem 40 illustrates that every honest transaction that is sufficiently deep in an honest blockchain will eventually become permanent. Moreover, the confirmation time is proportional to \( \log \frac{1}{\epsilon} \) when we want to ensure at most \( \epsilon \) probability of failure. Liveliness and consistency of the Prism transactions are justified.
IV. CONCLUSION

In this paper, we have analyzed the bitcoin and the Prism backbone protocols using more general models than in previous analyses. In particular, we assume a continuous-time model with no lifespan limitations and allow the block propagation delays to be arbitrary but bounded. Under the new setting, we have rigorously established a blockchain growth theorem, a blockchain quality theorem, and a common prefix theorem for the bitcoin backbone protocol. We have also proved a blockchain growth theorem and a blockchain quality theorem 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 valid 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 provides explicit security bounds for the bitcoin and the Prism backbone transactions, which improves understanding of both protocols and provides practical guidance to public transaction ledger protocol design.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Available online: http://bitcoin.org/bitcoin.pdf, 2008.
[2] 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.
[3] A. Kiayias and G. Panagiotakos, “Speed-security tradeoffs in blockchain protocols,” IACR Cryptology ePrint Archive, vol. 2015, p. 1019, 2015.
[4] R. Pass, L. Seeman, and A. Shelat, “Analysis of the blockchain protocol in asynchronous networks,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 643–673, Springer, 2017.
[5] L. Kiffer, R. Rajaraman, and S. Abhi, “A better method to analyze blockchain consistency,” in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 729–744, ACM, 2018.
[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] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, “Deconstructing the blockchain to approach physical limits,” arXiv preprint arXiv:1810.08092, 2018.
[8] J. Li and D. Guo, “On analysis of the bitcoin and prism backbone protocols,” arXiv:1907.05016v1, 2019.
[9] L. Ren, “Analysis of nakamoto consensus,” IACR Cryptology ePrint Archive, vol. 2019, p. 943, 2019.
[10] C. Decker and R. Wattenhofer, “Information propagation in the bitcoin network,” in IEEE P2P 2013 Proceedings, pp. 1–10, IEEE, 2013.
[11] 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.
[12] 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.
[13] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, “Spectre: A fast and scalable cryptocurrency protocol,” IACR Cryptology ePrint Archive, vol. 2016, p. 1159, 2016.
[14] Y. Sompolinsky and A. Zohar, “Phantom,” IACR Cryptology ePrint Archive, Report 2018/104, 2018.

[15] 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.

[16] 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.

[17] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[18] 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.

[19] 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.

[20] S. M. Ross, S. M. Ross, S. M. Ross, S. M. Ross, and E.-U. Mathématicien, A first course in probability. Prentice Hall Upper Saddle River, NJ, 1998.

[21] M. Mitzenmacher and E. Upfal, Probability and computing: Randomization and probabilistic techniques in algorithms and data analysis. Cambridge university press, 2017.