NORTHWESTERN UNIVERSITY

Blockchain Models and Latency-Security Guarantees for the Nakamoto Consensus

A DISSERTATION

SUBMITTED TO THE GRADUATE SCHOOL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

for the degree

DOCTOR OF PHILOSOPHY

Field of Electrical Engineering

By

Jing Li

EVANSTON, ILLINOIS

December 2020

ABSTRACT

Blockchain Models and Latency-Security Guarantees for the Nakamoto Consensus

Jing Li

Bitcoin is a decentralized payment system proposed in 2008 by Nakamoto, who remains anonymous to date. It offers an effective alternative to fiat money or centralized payment systems with advantages on privacy, anonymity, and low international remittance fees.

The transactions in Bitcoin payment system are sent through a peer-to-peer network, verified by network nodes, and recorded in a public ledger called blockchain.

The security of the Bitcoin payment system cannot be fully guaranteed without a rigorous mathematical proof. Due to the unpredictability of adversarial miners, it is challenging to characterize the behavior of miners and the synchronization status of blockchains in a concise way.

Unlike classic Byzantine fault tolerant protocols, the Bitcoin protocol only admits probabilistic guarantees. For the sake of security, it is important to derive an explicit formula for the security guarantee as a function of the latency, which will lead to a concrete latency–security trade-off for the Nakamoto consensus. Since Bitcoin's rise to fame, many altcoins and Bitcoin hard forks have adopted the Nakamoto consensus protocol

with very different parameters. Their parameters are mostly determined in an ad-hoc or empirical manner. This calls for theoretical results on parameter selection with the goal of optimizing some performance metrics.

Properties of the Bitcoin blockchain have been investigated in some depth. The liveness property of Bitcoin is reflected by the blockchain growth theorem and blockchain quality theorem: the blockchain growth theorem quantifies the number of blocks added to the blockchain during any time intervals; the blockchain quality theorem ensures the honest miners always contribute at least a certain fraction of the blockchain. The consistency property of Bitcoin is reflected by the common prefix theorem, which states if a block is deep enough, it will eventually be adopted by all honest miners with high probability. The liveness and consistency properties of the Bitcoin backbone protocol have been established by assuming either explicitly or implicitly that the blockchains have finite lifespan. Also, previous probabilistic security guarantees for the Bitcoin were expressed in terms of exponential order results. As such, the asymptotic bounds are very loose for practical use.

This thesis provides a streamlined and strengthened framework to analyze the properties of the Bitcoin protocol under several different models. Under discrete-time model, our results include a blockchain growth theorem, a blockchain quality theorem, and a common prefix theorem of the Bitcoin backbone protocol regardless of whether the blockchains have a finite lifespan. We also express the properties of the Bitcoin protocol in explicit expressions rather than order optimal results. A new notion of "r-credible blockchains" is introduced, which, together with some carefully defined "typical" events concerning block production over time intervals, is crucial to establish probabilisitic security guarantees.

Under continuous-time model, we develop a rigorous analysis of the liveness and consistency of the Bitcoin protocol. Moreover, our analyses yield practical latency and security bounds. For example, when the adversary controls 10% of the total mining power, a Bitcoin block is secured with 10^{-3} error probability after 5 hours 20 minutes of confirmation time, or with 10^{-10} error probability after 12 hours 15 minutes of confirmation time (assuming all block propagation delays are within 10 seconds). To establish the tight analysis, the arrivals of some special blocks are shown to be renewal processes, where the moment generation functions of the inter-arrival times are rigorously derived. The analysis is then applied to several proof-of-work longest-chain cryptocurrencies to bound their latency and security trade-off. Guidance is also provided for parameter selection with the goal of optimizing some performance metrics.

Following the spirit of decoupling various functionalities of the blockchain, the Prism protocol is proposed by Bagaria, Kannan, Tse, Fanti, and Viswanath in 2018 to dramatically improve the throughput while maintaining the same level of security. In addition to Bitcoin, this thesis also extends the analyses to the liveness and consistency of Prism blockchains.

Acknowledgements

Above all, I would like to express my sincere gratitude to my advisor, Professor Dongning Guo. I learned so much from his patience and diligence, his pursue of excellence and the passion to challenge hard problems. I can still remember the weekly meetings with Professor Guo where I felt so thrilled about the beauty of new insights. I can still remember the drafts that Professor Guo revised line by line, word by word. I also remember the conversations where Professor Guo gives me precious life advice. In my heart he is the excellent advisor.

Also, I would like to thank our coauthor Professor Ling Ren. He is sharp-minded and committed. It is really a pleasure working with him. I would like to thank Professor Aleksandar Kuzmanovic, who had discussions with me years ago when I can not find a research direction. He is always warm and supportive. I would like to thank Professor Hai Zhou to be my committee member. I learned a lot from his Bitcoin courses.

I would like to express my gratitude to my friends Yicheng Li, Luyao Tian, Yining Zhu, Mingwei Wei, Zihao Wang, Ziheng Chen, Yuanjing Ma, Jie Yuan, Yeguang Xue, Sylvia Alvino, Hongyi Xiao, Pei Yang, Jiajia Guo, Yingyi Luo, Andi Zhang, Yinsi Qi, Ziqi Zhao, Linxin Chen, Ziyue Xu, and Kevin Wang. Your friendship lights up my life. Special thanks to Zhe Wang and Yang Yu, whose insightful inputs inspired me to solve challenging problems. I would like to say thank you to all the colleagues and friends in the Communications and Networking Laboratory here at Northwestern University, including

Cheng Chen, Xu Chen, Zhiyi Zhou, Chang Liu, Hao Ge, Xu Wang, Hao Zhou, Yasar Sinan Nasir, Ning Yang, and Meng Zhang. With all of you, the Commnet group is like a warm family.

Finally, and most importantly, I want to express my thanks and love to my parents for their unconditional love. To them I dedicate this dissertation.

Table of Contents

List of Tables

List of Figures

CHAPTER 1

Introduction

Bitcoin was invented in 2008 by Nakamoto [**1**]. It is an decentralized payment system where users can send transactions over a peer-to-peer network. Bitcoin offers an alternative to fiat money or centralized payment systems: Bitcoin allows users more autonomy over their own money without trusted intermediaries like a bank or administrator. Bitcoin protects users' anonymity and privacy in the sense that real-world identity is not exposed during Bitcoin acquisitions and transactions. Bitcoin saves users from traditional banking fees, as well as provides timely settlement of international transactions with low cost. It is also helpful in countries suffering from hyperinflation [**2**]. The market capitalization of Bitcoin is more than 200 billion USD as of October, 2020 [**3**], taking 75% market cap of all cryptocurrencies.

Transactions in the Bitcoin system are maintained by miners and recorded in public ledgers referred to as blockchain. Maintainers of the ledger are distributed parties called miners. Producing a new block requires proof-of-work *mining*: a nonce must be included such that the block's hash value satisfies a difficulty requirement. An honest miner follows the longest-chain rule, i.e., it always tries to mine a block at the maximum height. As a distributed ledger technology, the Bitcoin protocol seeks the following two properties: *Liveness*, i.e., the ledger (blockchain) keeps incorporating new transactions. *Consistency*, i.e., all honest miners in the network agree on the same view of the ledger.

To prove the liveness and consistency of the Bitcoin blockchains, proper modelling is required so that the behavior of honest/adversarial miners and the synchronization status of blocks/blockchains are well characterized.

Unlike classic Byzantine fault tolerant protocols, the Bitcoin protocol only admits probabilistic guarantees. The latency (or confirmation time) of a block in Nakamoto-style consensus protocols depends on the desired security level. As a rule of thumb, a transaction is regarded as "confirmed" when it is 6 blocks deep in a longest blockchain. Is a 6-block-deep transaction "secure enough"? Moreover, what is the upper bound on the latency that guarantees a desired security level?

In the Bitcoin protocol, the block size is around 1 MB and the block generation rate is around 6 blocks per hour. Many altcoins and Bitcoin hard forks have adopted the Nakamoto consensus protocol with different parameters. Are these parameters well chosen? What are the trade-offs among different performance metrics (like latency, throughput, and fault-tolerance)? How should designer select parameters to achieve a performance goal?

The objective of this thesis is to resolve the preceding questions. We provide streamlined and strengthened models of the Nakamoto consensus protocol step by step in the discrete-time lockstep synchronous setting, discrete-time non-lockstep synchronous setting, and continuous-time setting, respectively. Under discrete-time model, our results include the liveness property (illustrated by a blockchain growth theorem and a blockchain quality theorem) and the consistency property (reflected by a common prefix theorem) of the Bitcoin backbone protocol regardless of whether the blockchains have a finite lifespan.

Under continuous-time model, we also develop a rigorous analysis of the liveness and consistency of the Bitcoin protocol via typicality. Our analyses yield practical latency and security bounds. The analysis is then applied to several proof-of-work longest-chain cryptocurrencies to bound their latency and security trade-off. Guidance is also provided for parameter selection with the goal of optimizing some performance metrics.

1.1. The Bitcoin backbone protocol

Transactions in Bitcoin system are verified by network nodes and recorded in public ledgers 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. Maintainers of the ledger are distributed parties called miners who generate blocks and maintain their own version of the blockchain. 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. Since miners are anonymous, obviously the collective mining power of adversarial miners must be less than half of the total mining power to ensure security of the blockchain system.

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 [**4**] 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, [**4**] 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 [**4**] 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 [**5**] 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 (liveness). 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 transaction 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 [**6**] showed that the blockchain growth theorem, the blockchain quality theorem, and the common prefix theorem remain valid under the non-lockstep synchrony model. Also, Kiffer, Rajaraman, and Shelat [**7**] gave the non-closed form results of the consistency of the Bitcoin protocol using the Markov chains.

Most previous analyses [**4**, **6**, **8**, **9**] assumed the blockchain's lifespan is finite, i.e., there exists a maximum round when the blockchain system terminates. In this thesis, we drop the finite horizon assumption and prove properties of the Bitcoin backbone protocol regardless of whether or not the blockchains have a finite lifespan. 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 time intervals which are long enough, 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 discrete-time model eases analysis but is still a departure from reality. In 2019, Ren [**10**] extended the liveness and consistency of the 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 thesis, we first build a rigorous (and simple) stochastic model for continuous-time block mining processes and the resulting blockchains. We characterize the liveness and consistency properties of the Bitcoin protocol under the continuous-time model. As numerical results, we discuss the trade-off between performance metrics like latency, security, and throughput. Existing analyses against all possible attacks [**4**, **6**–**9**, **11**] (including a few concurrent and follow-up works [**12**–**15**]) focus on establishing asymptotic bounds using the big $O(\cdot)$ or big $\Omega(\cdot)$ notation. If one works out the constants in these asymptotic results, the latency upper bounds will be several orders of magnitude higher than the best known lower bounds [**16**, **17**]. Thus, despite their theoretical value, existing analyses of the Nakamoto consensus provide little guidance on the actual confirmation time, security guarantees, or parameter selection in practice. In this thesis, we explicitly and closely characterize the trade-off between latency and security for Nakamoto-style proof-of-work consensus protocols. The latency results we prove are within a few hours to simple lower bounds due to the private attack. The gap remains relatively constant at different security levels, and is hence insignificant for high security levels but can be significant at low security levels. For example, with a 10% adversary mining power, a mining rate of one

block every 10 minutes, and a maximum block propagation delay of 10 seconds, a block in the Nakamoto consensus is secured with 10^{-3} error probability after 5 hours 20 minutes, or with 10^{-10} error probability after 12 hours 15 minutes. As a reference, due to the private attack, one must wait for at least 1 hour 30 minutes or 8 hours 5 minutes before confirming for 10^{-3} and 10^{-10} security levels, respectively. The analyses also extend to other Nakamoto-style proof-of-work consensus protocols.

Some new techniques developed in this thesis may be of independent interests. Assuming all block propagation delays are under a fixed amount of time, we show the arrivals of several species of honest blocks form renewal processes. That is, the inter-arrival times of such a process are independent and identically distributed (i.i.d.). We show that the adversary must match the so-called double-laggers in order to succeed in any attack. Then we derive the moment generating functions of the inter-arrival times of double-laggers. This allows us to calculate quite accurately the probability that more double-laggers are mined than adversarial blocks in any time interval, which leads to a close latency–security trade-off.

1.2. The Prism backbone protocol

It is well known that the throughput of Bitcoin is severely restricted by design to ensure security [**18**]. 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 [**19**]. Many ideas have been proposed to improve the blockchain throughput.

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 [**19**]. Inclusive, Spectre, and Phantom construct a directed acyclic graph (DAG) structured blockchain by introducing reference links between blocks in addition to the parent links [**20**–**22**]. However, these protocols are vulnerable to certain attacks [**23**–**25**]. Generally speaking it is difficult to secure a high-forking protocol. Another line of work is to decouple the various functionalities of the blockchain [**26**, **27**]. With this spirit, Bagaria, Kannan, Tse, Fanti, and Viswanath [**9**] 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 vote. 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 transactions. A thorough description and analysis is found in [**9**], where liveness and consistency of Prism transactions were proved assuming a finite life span of the blockchains under the lockstep synchrony model [**9**]. In this thesis, we also prove the liveness and consistency of the Prism protocol with explicit probabilistic bounds under discrete-time model.

1.3. Structure of this thesis

Next, we summarize the major contents of the following part of this thesis.

In Chapter 2, the general modelling of blockchains are introduced. Important concepts which will be used throughout the chapter (like blocks, blockchains, and their prefix) are formally defined.

In Chapter 3, we analyze the Bitcoin backbone protocol using more general discrete-time 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. We have also shown that the leader sequence is permanent with high probability after sufficient amount of wait time. As a consequnce, 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 chapter provide explicit bounds for the properties of Bitcoin backbone protocol, which furthers understanding of the Bitcoin protocol.

In Chapter 4, we briefly introduce the Prism backbone protocol. Under the same discrete-time framework, we prove a blockchain growth property and a blockchain quality property of the leader sequence. Liveness and consistency of the Prism protocol are proved without the finite horizon assumption under both the lock-step synchronous model and the non-lockstep synchronous model.

In Chapter 5, we prove the liveness and consistency of the Bitcoin protocol under the continuous-time model, which is simpler and more realistic than the discrete-time model. We also provide an explicit formula for the security guarantee as a function of the latency, which enable us to derive a concrete latency–security trade-off for the Nakamoto

consensus. By means of numerical analysis, the latency upper bound is shown to be close to a lower bound due to the private attack. We quantify how the block propagation delay bound, mining rates, and other parameters affect the latency–security trade-off. We also apply the results to analyze existing proof-of-work longest-chain cryptocurrencies. When the mining rate is low (compared to the block propagation delay), the obtained upper bounds are close to the lower bounds from private mining. When the block generation rate is high, however, our method does not give very tight results. Recent works [**14**, **15**] have established the tight fault tolerance under high mining rate but tight bounds on latency remain open. Another direction is to analyze the Nakamoto consensus with dynamic participation and/or difficulty adjustment. Only asymptotic bounds exist in this direction [**8**, **28**] and it is interesting future work to establish concrete latency–security bounds.

Chapter 6 concludes the thesis.

CHAPTER 2

Definitions Common to All Models

The Bitcoin blockchain can be regarded as a growing sequence of transaction-recording blocks which begins with a genesis block, and chains every subsequent block to a parent block using a cryptographic hash. Formally, we define blocks and blockchains as the following:

Definition 2.1 (Blocks)**.** *A block in a practical blockchain system is a data structure with an identifier and a reference to its parent block. An honest genesis block is referred to as block* 0*. Subsequent blocks are referred to as block* 1*, block* 2*, and so on, in the order they are mined.*

Definition 2.2 (Blockchain and height)**.** *Every block has a unique parent block that is mined strictly before it. We use* $f_b \in \{0, 1, ..., b-1\}$ *to denote block* b*'s parent block number. The sequence* $(b_0, b_1, \ldots, b_n)$ *defines a blockchain if* $b_0 = 0$ *and* $f_{b_i} = b_{i-1}$ *for* $i = 1, \ldots, n$*. It is also referred to as blockchain* b_n *since* b_n *uniquely identifies it. The height of both block* b_i *and blockchain* b_i *is said to be* i*.*

Because invalid blocks are inconsequential as far as the distributed consensus protocol is concerned, throughout this thesis, by a block we always mean a valid block.

Definition 2.3 (k-deep block, k-deep prefix)**.** *Suppose* $k \in \{1, \ldots, i\}$*. By the* k*-deep block of blockchain* $(b_0, b_1, \ldots, b_i)$ *we mean block* b_{i-k+1}*. By the* k*-deep prefix of blockchain*

$(b_0, b_1, \ldots, b_i)$ we mean blockchain b_{i-k}. By convention, let the k-deep block and k-deep prefix of the blockchain be the genesis block if $k > i$.

By Definition 2.3, a k-deep block extends a k-deep prefix of the same blockchain.

CHAPTER 3

Discrete-time Analysis of the Bitcoin Backbone Protocol

3.1. Introduction

In this chapter, we adopt a discrete model where activities take place in rounds. In the Bitcoin white paper [**1**], Nakamoto 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 [**29**]. Several important properties of the Bitcoin backbone protocol have been proposed in [**1**,**4**,**5**,**8**,**30**]. Garay, Kiayias, and Leonardos [**4**] 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, [**4**] 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, [**5**] 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 [**30**] 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 also gives birth to numerous "robust public transaction ledger" protocols [**26**, **31**, **32**]. 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.

However, many previous analysis on the Bitcoin protocol assumes a blockchain's lifespan is finite, i.e., there exists a maximum round when the blockchain ends. For example, in [**4**, **8**] and [**32**], 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 chapter, 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.

Some previous work [**4**, **8**, **32**] assume 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 lockstep synchronous model. In this chapter, our analyses apply to both the lockstep synchronous model and non-lockstep synchronous model, where 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. In the non-lockstep synchronous model, it is only assumed that the propagation time is bounded by T rounds, which is realistic in practice. A key idea in this chapter 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 lockstep-synchronous synchronous model find their counterparts for this non-lockstep synchronous model.

3.2. General discrete-time model

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). With minor abuse of notation, we use β to denote the percentage of adversarial miners in the following part of this thesis:

$$\beta = \frac{t}{n}. \tag{3.1}$$

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

$$\xi = \frac{1-2\beta}{1-\beta}. \tag{3.2}$$

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

By saying "by round r" we mean all rounds up to and including round $r-1$. We let T_b denote the round during which block b is mined.

Next, we redefine concepts of miner's view, published, credible blockchain, etc. These definitions are similar to that in Chapter 5 but are under the discrete-time scenario.

Definition 3.1 (A miner's view)**.** *A miner's view at round r is a subset of all blocks mined by round r. A miner's view can only increase over time. A block is in its own miner's view from the round it is mined.*

Definition 3.2 (A miner's longest blockchain)**.** *A blockchain is in a miner's view at round r if all blocks of the blockchain are in the miner's view at round r. A miner's longest blockchain at round r is a blockchain with the maximum height in the miner's view at round r. Ties are broken in an arbitrary manner.*[1]

Definition 3.3 (Honest and adversarial miners)**.** *Each miner is either honest or adversarial. A block is said to be honest (resp. adversarial) if it is mined by an honest (resp. adversarial) miner. An honest block mined during round r must extend its miner's longest blockchain at round r.*

Definition 3.4 (Publication)**.** *A block is said to be published at round r if it is included in at least one honest miner's view at round r. A blockchain is said to be published at round r if all of its blocks are published at round r.*

We let P_b denote the round at which block b is published. By definition 3.3, an honest block b is published at the round it is mined. We have $T_b = P_b$.

Next, we introduce a few notations representing the mining process.

For $r \in \{1, 2, \ldots\}$, let H_r denote the number of all honest blocks mined during round r. The mining difficulty and miner' 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 $p \in (0, 1)$.[2] Note that $H_r \sim Binomial(n-t, p)$.

[1]The Bitcoin protocol favors the earliest to enter the view.

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

Define

$$X_r = \begin{cases} 1, & \text{if } H_r \geq 1 \\ 0, & \text{otherwise.} \end{cases} \tag{3.3}$$

X_r indicates if one or more honest blocks are mined during round r or not. Let

$$q = 1 - (1-p)^{n-t}. \tag{3.4}$$

Basically q is the probability that one or more honest blocks are mined during a round. Then $X_r \sim Bernoulli(q)$. Define

$$Y_r = \begin{cases} 1, & \text{if } H_r = 1 \\ 0, & \text{otherwise.} \end{cases} \tag{3.5}$$

Basically Y_r indicates if a single honest block is mined in round r or not. Then $Y_r \sim Bernoulli((n-t)p(1-p)^{n-t-1})$.

Let Z_r denote the number of adversarial blocks mined during round r (the adversarial miners may or may not publish them). Since there are at most t adversarial miners, the number of blocks mined in any rounds is upper bounded probabilistically. Specifically, let S represent an arbitrary set of positive numbers. Then the probability that more than a adversarial blocks are mined during those rounds in S does not exceed the probability that a binomial distribution with parameter $(t|S|, p)$ is greater than a. In other words,

for every $a \geq 0$,

$$P\left(\sum_{r\in S} Z_r \leq a\right) > \sum_{i=0}^{\lfloor a \rfloor} \binom{t|S|}{i} p^i (1-p)^{t|S|-i} \tag{3.6}$$

where $|S|$ is the cardinality of S.

It is important to note that $H_1, H_2, \ldots$ are i.i.d., which form a stationary process. The same can be said of the X and Y sequences.

In the following part of this chapter, we define $a_{s,r}$ as the sum of the subsequence of $a_s, \ldots, a_{r-1}$, i.e.,

$$a_{s,r} = \sum_{i=s}^{r-1} a_i \tag{3.7}$$

for all integers $1 \leq s < r$. To be specific,

$$X_{s,r} = \sum_{i=s}^{r-1} X_i, \tag{3.8}$$

$$Y_{s,r} = \sum_{i=s}^{r-1} Y_i, \tag{3.9}$$

$$Z_{s,r} = \sum_{i=s}^{r-1} Z_i \tag{3.10}$$

for all integers $1 \leq s < r$.

Definition 3.5. *Let r be a positive integer. A block or a sequence (of blocks) is said to be* permanent after round r *if the block or sequence remains in the longest blockchain in all honest miners' views starting from round r.*

3.3. Lockstep synchronous model and analysis

In Lockstep synchronous model, if one or more blocks are published 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. We assume that during round 0, the genesis block is mined and published.

Definition 3.6. *(r-credible blockchain) Blockchain b is said to be* r-credible *if it has been published by round r, and is no shorter than any blockchain published by round r. That is to say,*

$$P_b < r, \tag{3.11}$$

and

$$h(b) \geq h(k), \quad \forall k : P_k < r. \tag{3.12}$$

If there is no need to specify round r explicitly, blockchain b can also be simply called a credible blockchain.

At round r, an honest miner must have seen all blockchains published by round r. It follows that every honest miner's longest blockchain must be r-credible. Similar to Chapter 5, it is unnecessary to keep track of individual miner's views as far as the fundamental security is concerned. Focusing on credible blockchains allows us to develop a simple rigorous proof with minimal notation.

Definition 3.7 (loner)**.** *Block b is called a* loner *if* $Y_{T_b} = 1$.

That is to say, a block is called a loner if it is the only honest block mined during a round.

It is assumed that the mining difficulty is adjusted such that

$$q \leq \frac{\xi}{6}. \tag{3.13}$$

Proposition 3.8. *For* $r = 1, 2, \dots$,

$$q \leq p(n-t) < \frac{q}{1-q}. \tag{3.14}$$

Proof. As $X_r \sim Bernoulli(q)$, we have

$$\begin{aligned} \mathbb{E}[X_r] &= q && (3.15)\\ &= 1 - (1-p)^{n-t} && (3.16)\\ &\leq p(n-t), && (3.17) \end{aligned}$$

where (3.17) is due to Bernoulli's inequality. Moreover,

$$\begin{aligned} \frac{q}{1-q} &= \frac{1-(1-p)^{n-t}}{(1-p)^{n-t}} && (3.18)\\ &= (1-p)^{-(n-t)} - 1 && (3.19)\\ &> (1+p)^{n-t} - 1 && (3.20)\\ &\geq p(n-t), && (3.21) \end{aligned}$$

where (3.20) is due to $(1+p)(1-p) < 1$ and (3.21) is due to Bernoulli's inequality. By (3.17) and (3.21),

$$q \leq p(n-t) < \frac{q}{1-q}. \tag{3.22}$$

□

Proposition 3.9. *For* $r = 1, 2, \dots$,

$$\mathbb{E}[Y_r] > q(1-q). \tag{3.23}$$

Proof. According to Proposition 3.8, $q \leq \frac{1}{6}$ implies $q < p(n-t) < \frac{1}{5}$. Hence,

$$\mathbb{E}[Y_r] = p(n-t)(1-p)^{n-t-1} \tag{3.24}$$

$$\geq p(n-t)(1-p(n-t-1)) \tag{3.25}$$

$$> p(n-t)(1-p(n-t)) \tag{3.26}$$

$$> q(1-q), \tag{3.27}$$

where (3.25) is due to Bernoulli's inequality, and (3.27) holds because the function $x(1-x)$ is increasing on $[0, \frac{1}{2}]$. □

Proposition 3.10. *For* $r = 1, 2, \dots$,

$$\mathbb{E}[Z_r] < \mathbb{E}[X_r]. \tag{3.28}$$

Proof. Let $Z'_r \sim Binomial(t, p)$. Since Z_r is dominated by Z'_r, we have

$$\mathbb{E}[Z_r] \leq \mathbb{E}[Z'_r] \tag{3.29}$$

$$= pt \tag{3.30}$$

$$= \frac{t}{n-t} p(n-t) \tag{3.31}$$

$$< \frac{t}{n-t} \frac{q}{1-q} \tag{3.32}$$

$$= (1-\xi)\frac{1}{1-q} q \tag{3.33}$$

$$\leq \frac{1-\xi}{1-\frac{\xi}{6}} q \tag{3.34}$$

$$< \mathbb{E}[X_r], \tag{3.35}$$

where (3.32) is due to Proposition 3.8 and (3.35) is due to $q \leq \frac{\xi}{6}$. □

Definition 3.11. *For all integers $1 \leq s < r$, define event*

$$D_{s,r} = D^1_{s,r} \cap D^2_{s,r} \cap D^3_{s,r} \tag{3.36}$$

where

$$D^1_{s,r} = \left\{ (1-\frac{\xi}{6})\mathbb{E}[X_{s,r}] < X_{s,r} < (1+\frac{\xi}{6})\mathbb{E}[X_{s,r}] \right\} \tag{3.37}$$

$$D^2_{s,r} = \left\{ (1-\frac{\xi}{6})\mathbb{E}[Y_{s,r}] < Y_{s,r} \right\} \tag{3.38}$$

$$D^3_{s,r} = \left\{ Z_{s,r} < \mathbb{E}[Z_{s,r}] + \frac{\xi}{6}\mathbb{E}[X_{s,r}] \right\}. \tag{3.39}$$

Under event $D^1_{s,r}$, 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 $D^2_{s,r}$, the number of loners $Y_{s,r}$ is no less than $1-\frac{\xi}{6}$ of its expected value. Under event $D^3_{s,r}$, 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 $D_{s,r}$, we have 1) a "typical" number of rounds during which at least one honest block is mined, 2)"enough" loners, and 3) the total number of adversarial blocks is limited.

For convenience, define

$$\eta = \frac{\xi^2}{180} q. \tag{3.40}$$

Theorem 3.12. *(Chernoff bound, [33, page 69]) Let $X \sim binomial(n,p)$. Then for every $\eta \in (0,1]$,*

$$P(X \leq (1-\eta)pn) \leq e^{-\frac{\eta^2 pn}{2}}, \tag{3.41}$$

and

$$P(X \geq (1+\eta)pn) \leq e^{-\frac{\eta^2 pn}{3}}. \tag{3.42}$$

Lemma 3.13. *For all integers $1 \leq s < r$,*

$$P(D_{s,r}) > 1 - 4e^{-\eta(r-s)}, \tag{3.43}$$

where η is given in (3.40).

Proof. We first analyze events D_1, D_2, and D_3 separately. We have

$$P((D^1_{s,r})^c) = P\left(|X_{s,r} - \mathbb{E}[X_{s,r}]| \geq \frac{\xi}{6}\mathbb{E}[X_{s,r}]\right) \tag{3.44}$$

$$= P\left(X_{s,r} \geq \mathbb{E}[X_{s,r}] + \frac{\xi}{6}\mathbb{E}[X_{s,r}]\right) + P\left(X_{s,r} \leq \mathbb{E}[X_{s,r}] - \frac{\xi}{6}\mathbb{E}[X_{s,r}]\right) \tag{3.45}$$

$$\leq 2e^{-\frac{\xi^2}{108}q(r-s)}, \tag{3.46}$$

where (3.46) is due to Theorem 3.12.

Also,

$$P((D^2_{s,r})^c) = P\left(Y_{s,r} \leq (1 - \frac{\xi}{6})\mathbb{E}[Y_{s,r}]\right) \tag{3.47}$$

$$\leq e^{-\frac{\xi^2}{72}\mathbb{E}[Y_{s,r}]} \tag{3.48}$$

$$\leq e^{-\frac{\xi^2}{72}(1-q)q(r-s)} \tag{3.49}$$

$$< e^{-\frac{\xi^2}{72}(1-\frac{\xi}{6})q(r-s)}, \tag{3.50}$$

where (3.48) is due to Theorem 3.12, (3.49) is due to Proposition 3.9, and (3.50) is due to $q \leq \frac{\xi}{6}$.

Note that the moment generating function for binomial random variable $Z_r \sim Binomial(t, p)$ is $(1 - p + pe^u)^t$ (page 39 in **[34]**). We have

$$P((D^3_{s,r})^c) = P\left(Z_{s,r} \geq \mathbb{E}[Z_{s,r}] + \frac{\xi}{6}\mathbb{E}[X_{s,r}]\right) \tag{3.51}$$

$$\leq P\left(Z_{s,r} \geq \mathbb{E}[Z_{s,r}] + \frac{\xi}{12}\mathbb{E}[Z_{s,r}] + \frac{\xi}{12}\mathbb{E}[X_{s,r}]\right) \tag{3.52}$$

$$< \frac{\mathbb{E}\left[e^{Z_{s,r}u}\right]}{e^{(1+\frac{\xi}{12})\mathbb{E}[Z_{s,r}]u + \frac{\xi}{12}\mathbb{E}[X_{s,r}]u}} \tag{3.53}$$

$$= \frac{(1-p+pe^u)^{t(r-s)}}{e^{(1+\frac{\xi}{12})(r-s)tpu+\frac{\xi}{12}(r-s)qu}} \tag{3.54}$$

$$\leq e^{\left(e^u-1-u(1+\frac{\xi}{12})\right)tp(r-s)-\frac{\xi}{12}qu(r-s)}, \tag{3.55}$$

where (3.52) is due to Proposition 3.10, (3.53) holds for all $u \geq 0$ due to Chernoff's inequality, and (3.55) 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

$$P((D^3_{s,r})^c) \leq e^{\left(\frac{\xi}{12}-(1+\frac{\xi}{12})\log(1+\frac{\xi}{12})\right)tp(r-s)-\frac{\xi}{12}\log(1+\frac{\xi}{12})q(r-s)} \tag{3.56}$$

$$< e^{-\frac{\xi}{12}\log(1+\frac{\xi}{12})q(r-s)} \tag{3.57}$$

$$< e^{-\frac{\xi^2}{180}q(r-s)} \tag{3.58}$$

where (3.57) is due to $(1+x)\log(1+x) > x$ for all $x > 0$, and (3.58) is due to $\log(1+\frac{\xi}{12}) > \frac{\xi}{15}$ for all $0 < \xi \leq 1$.

Thus,

$$P(D_{s,r}) = 1 - P((D_{s,r})^c) \tag{3.59}$$

$$\geq 1 - P((D^1_{s,r})^c) - P((D^2_{s,r})^c) - P((D^3_{s,r})^c) \tag{3.60}$$

$$> 1 - 4e^{-\eta(r-s)} \tag{3.61}$$

where η is defined in (3.40), (3.61) is due to $\frac{\xi^2}{72}(1-\frac{\xi}{6}) > \frac{\xi^2}{180}$ and $\frac{\xi^2}{108} > \frac{\xi^2}{180}$. □

Lemma 3.14. *For all integers $1 \leq s < r$, under event $D_{s,r}$, the following holds.*

$$(1-\frac{\xi}{6})q(r-s) < X_{s,r} < (1+\frac{\xi}{6})q(r-s) \tag{3.62}$$

$$Y_{s,r} > (1 - \frac{\xi}{3})q(r-s) \tag{3.63}$$

$$Z_{s,r} < (1 - \frac{2\xi}{3})q(r-s) \tag{3.64}$$

$$Z_{s,r} < (1 - \frac{\xi}{2})X_{s,r} \tag{3.65}$$

$$Z_{s,r} < Y_{s,r}. \tag{3.66}$$

Proof. Under $D_{s,r}$, (3.62) follows directly from (3.37).

To prove (3.63),

$$Y_{s,r} > (1 - \frac{\xi}{6})q(1-q)(r-s) \tag{3.67}$$

$$> (1 - \frac{\xi}{6})^2 q(r-s) \tag{3.68}$$

$$> (1 - \frac{\xi}{3})q(r-s), \tag{3.69}$$

where (3.67) is due to Proposition 3.9 and (3.68) is due to $q \leq \frac{\xi}{6}$.

To prove (3.64), we have

$$Z_{s,r} < E[Z_{s,r}] + \frac{\xi}{6}E[X_{s,r}] \tag{3.70}$$

$$\leq (1-\xi)\frac{q}{1-q}(r-s) + \frac{\xi}{6}q(r-s) \tag{3.71}$$

$$< (1 - \frac{2\xi}{3})q(r-s) \tag{3.72}$$

where (3.70) is due to (3.39), (3.71) is due to (3.33), and (3.72) is due to $q \leq \frac{\xi}{6}$.

To prove (3.65), we have

$$Z_{s,r} < (1 - \frac{2\xi}{3})q(r-s) \tag{3.73}$$

$$< \frac{1 - \frac{2\xi}{3}}{1 - \frac{\xi}{6}} X_{s,r} \tag{3.74}$$

$$< (1 - \frac{\xi}{2}) X_{s,r}, \tag{3.75}$$

where (3.73) is due to (3.72) and (3.74) is due to (3.62).

The inequality (3.66) is straightforward by (3.64) and (3.63). □

Definition 3.15. *For all integers $1 \leq s < r$, define the typical event with respect to $[s, r]$ as*

$$E_{s,r} = \bigcap_{0 \leq a < s, b \geq 0} D_{s-a,r+b}. \tag{3.76}$$

The event $E_{s,r}$ occurs when the events $D_{s-a,r+b}$ simultaneously occurs for all a, b, i.e., the "E" events occur over all intervals that contain time interval $[s, r]$. 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 $E_{s,r}$ to allow the "good" properties mentioned in Lemma 3.14 to extend to all intervals containing $[s, r]$ under the event. It is important to note that the typical events defined in **[4, 32]** 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 thesis to allow for results for infinite horizon.

Lemma 3.16. *For all integers $1 \leq s < r$,*

$$P(E_{s,r}) > 1 - 5\eta^{-2} e^{-\eta(r-s)}. \tag{3.77}$$

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

$$P(E^c_{s,r}) = P(\cup_{0\le a<s, b\ge 0} D^c_{s-a,r+b}) \tag{3.78}$$

$$= P(\cup_{0\le a<s, b\ge 0} (D_{1,r-s+a+b+1})^c) \tag{3.79}$$

$$\le \sum_{0\le a<s, b\ge 0} (D_{1,r-s+a+b+1})^c) \tag{3.80}$$

$$= \sum_{k=0}^{\infty} \sum_{0\le a<s, b\ge 0: a+b=k} P((D_{1,r-s+a+b+1})^c) \tag{3.81}$$

$$< \sum_{k=0}^{\infty} (k+1) P((D_{1,r-s+a+b+1})^c) \tag{3.82}$$

$$< \sum_{k=0}^{\infty} (k+1) 4e^{-\eta(r-s+k)} \tag{3.83}$$

$$= 4e^{-\eta(r-s)} \sum_{k=0}^{\infty} (k+1) e^{-\eta k} \tag{3.84}$$

$$= \frac{4}{(1-e^{-\eta})^2} e^{-\eta(r-s)}. \tag{3.85}$$

According to (3.13) and (3.40), $\eta \le \frac{1}{6} \cdot \frac{1}{180} = \frac{1}{1080}$. The lemma is thus established using the fact that $1 - e^{-x} \ge \sqrt{\frac{4}{5}} x$ for all $0 \le x \le \frac{1}{1080}$. □

Lemma 3.17. *(Lemma 6 in [4]) A loner is the only honest block at its height.*

Proof. Suppose block b is a loner and block d is a different honest block. Then $T_d < T_b$ or $T_d > T_b$ by definition of a loner. If $T_d > T_b$, we have $h(d) \ge h(b) + 1$ since blockchain b is published during round T_b. If $T_d < T_b$, we have $h(d) \le h(b) - 1$ (if $h(d) \ge h(b)$, block b's height would be at least $h(b) + 1$). □

Lemma 3.18. *If block b is honest, then blockchain f_b must be T_b-credible.*

Proof. According to Definition 3.3, if block b is honest, it must extend a T_b-credible blockchain. Thus the proof of Lemma 3.18 □

Although an honest block always extends a credible blockchain, a credible blockchain may not end with an honest block. Moreover, an adversarial block may or may not extend a credible blockchain and may be published anytime after it is mined.

Lemma 3.19. *(Lemma 7 in [4]) Let $1 \leq s < r$ be integers. Suppose an s-credible blockchain has height ℓ. Then all r-credible blockchains have height at least $\ell + X_{s,r}$.*

Proof. By induction: Consider $r = s + 1$. If $X_s = 0$, then $X_{s,s+1} = 0$. All $(s + 1)$-credible blockchains have heights at least $\ell = \ell + X_{s,r}$. If $X_s = 1$, at least one honest block is published during round s with height $\ell + 1$. Then all $(s + 1)$-credible blockchains have heights at least $\ell + 1 = \ell + X_{s,r}$. Lemma 3.19 is established for the cases of $r = s + 1$.

Assume all r_1-credible blockchains have length at least $\ell + X_{s,r_1}$. If $X_{r_1} = 0$, the claim holds trivially for round $r_1 + 1$. If $X_{r_1} = 1$, at least one honest block is published during round r_1 with height $\ell + X_{s,r_1} + 1$. Then all $(r_1 + 1)$-credible blockchains have height at least $\ell + X_{s,r_1+1}$ by Definition 3.6. By induction on r_1, Lemma 3.19 holds. □

Lemma 3.20. *For all integers $1 \leq s < r$ and $k \geq 2q(r - s)$, under typical event $E_{s,r}$, the k-deep block and k-deep prefix of every r-credible blockchain must be mined before round s.*

Proof. The total number of blocks mined by all miners during rounds $\{s, \ldots, r-1\}$ is upper bounded by $X_{s,r} + Z_{s,r}$. Note that

$$X_{s,r} + Z_{s,r} < (1 + \frac{\xi}{6})q(r-s) + (1 - \frac{2\xi}{3})q(r-s) \tag{3.86}$$

$$< 2q(r-s) \tag{3.87}$$

$$\leq k, \tag{3.88}$$

where (3.86) is due to (3.62) and (3.64). Thus, the k-deep block and k-deep prefix must be mined before round s. □

Theorem 3.21 (Blockchain growth theorem under lockstep synchronous model)**.** *Let r, s, s_1 be integers satisfying $1 \leq s_1 \leq s < r$. Then under typical event $E_{s,r}$, the height of an r-credible blockchain must be at least $(1 - \frac{\xi}{6})q(r - s_1)$ larger than the height of an s_1-credible blockchain.*

Proof. Under $E_{s,r}$, we have

$$X_{s_1,r} > (1 - \frac{\xi}{6})\mathbb{E}[X_{s_1,r}] \tag{3.89}$$

$$= (1 - \frac{\xi}{6})q(r - s_1) \tag{3.90}$$

where (3.90) is due to (3.62). According to Lemma 3.19, the height of an r-credible blockchain is at least $X_{s_1,r}$ larger than that of an s_1-credible blockchain. □

Theorem 3.22 (Blockchain quality theorem under lockstep synchronous model)**.** *Let r, s, k be integers satisfying $1 \leq s < r$ and $k \geq 2q(r-s)$. Suppose an r-credible blockchain*

has more than k blocks by round r. Under event $E_{s,r}$, by round r, at least $\frac{\xi}{2}$ fraction of the last k blocks of the blockchain are honest.

Proof. The intuition is that under typical event $E_{s,r}$, an honest miner's blockchain grow by at least $X_{s,r}$ according to Lemma 3.19. Meanwhile, the number of adversarial blocks mined is upper bounded by (3.65). 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, suppose blockchain d is r-credible and $h(d) \geq k$. Denote the k-deep block of blockchain d as block b. Let block e be the highest honest block mined before block b on blockchain b. Then we have $0 \leq h(e) < h(b)$. The relationship between these blocks is illustrated as follows:

$$\boxed{e} - \cdots - \boxed{} - \overbrace{\boxed{b} - \cdots - \boxed{d}}^{k \text{ blocks}} \tag{3.91}$$

round s_1 round r

Let $s_1 = T_e$ for convenience. According to Lemma 3.19, we have $s_1 < s$. Denote the number of honest blocks between block b (inclusive) and block d (inclusive) as x. To prove the theorem, it suffices to show $x > \frac{\xi}{2}k$.

By definition, on blockchain d, all blocks at heights $\{h(e)+1, \ldots, h(b)-1\}$ are adversarial, thus the number of honest blocks between block e (exclusive) and block d (inclusive) is also x. Let $y = h(d) - h(e)$, then the number of adversarial blocks on blockchain d between block e (exclusive) and block d (inclusive) is $y - x$. Then $y - x$ is a lower bound

for the total number of adversarial blocks mined during rounds $\{s_1+1,\ldots,r-1\}$. We have

$$y - x \leq Z_{s_1+1,r}. \tag{3.92}$$

Under event $E_{s,r}$, event $D_{s_1+1,r}$ occurs. Note that an (s_1+1)-credible blockchain has height at least $h(e)$. By Lemma 3.21, we have $h(d) - h(e) = y \geq X_{s_1+1,r}$. Thus,

$$\begin{aligned} y - x &\leq Z_{s_1+1,r} && (3.93)\\ &< (1-\frac{\xi}{2})X_{s_1+1,r} && (3.94)\\ &< (1-\frac{\xi}{2})y && (3.95)\\ &\leq y - \frac{\xi}{2}k, && (3.96) \end{aligned}$$

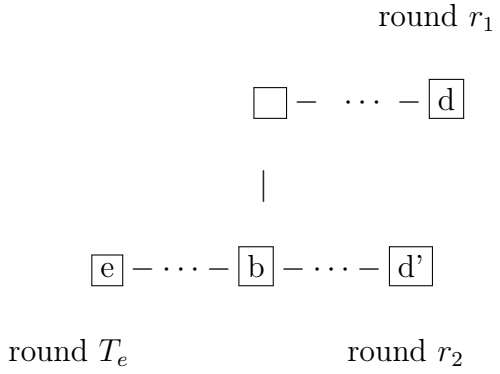
where (3.93) is due to (3.92), (3.94) is due to (3.65), (3.95) is due to Lemma 3.19, and (3.96) is due to $y \geq k$. From (3.96), $x > \frac{\xi}{2}k$ is derived. □

Theorem 3.23 (Common prefix theorem under lockstep synchronous model)**.** *Let r, s, k be integers satisfying $1 \leq s < r$ and $k \geq 2q(r-s)$. Then the k-deep prefix of any r-credible blockchain is permanent after round r under event $E_{s,r}$.*

Proof. The intuition is based on Lemma 3.17: a loner is the only honest block at its height. 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 because according to (3.66): the number of loners must be greater than the number of adversarial blocks under the typical event.

To be precise, we prove the desired result by contradiction. Let blockchain b be the k-deep prefix of an r-credible blockchain. If block b is the genesis block, the theorem is trivial. Otherwise, we will show contradiction if blockchain b is not permanent after r.

Suppose round $r_1 \geq r$ is the smallest integer such that there exists an r_1-credible blockchain (denoted as blockchain d) which does not extend blockchain b. If $r_1 = r$, let $r_2 = r$. If $r_1 > r$, let $r_2 = r_1 - 1$. Then there must exist an r_2-credible blockchain that extends blockchain b (denoted as blockchain d'). Let block e be the highest honest block shared by blockchain d and blockchain d'. Then we have $T_e < s$ by Lemma 3.20. The relationship between these blocks is illustrated as follows:



(3.97)

Next we will show $Y_{T_e+1,r_2} \leq Z_{T_e+1,r_2}$. If $Y_{T_e+1,r_2} = 0$, it is obvious. Otherwise, consider a loner c mined during rounds $\{T_e+1, \ldots, r_2\}$. Since blockchain e is T_e-credible and block c is mined after time $T_e + 1$, we have $h(c) > h(e)$ by Definition 3.6. Since blockchain d is r_1-credible and blockchain d' is r_2-credible, we have $h(c) \leq \min\{h(d), h(d')\}$. Consider the following two only possible cases:

(1) If $h(e) < h(c) \leq h(b)$, there exists at least one adversarial block at height $h(c)$ because all blocks between block e (exclusive) and block b (inclusive) are adversarial by definition.

(2) If $h(b) < h(c) \leq \min\{h(d), h(d')\}$, there is at least one adversarial block at height $h(c)$, because two diverging blockchains exist but loner c is the only honest block at its height by Lemma 3.17.

Thus, for every loner c mined during rounds $\{T_e + 1, \ldots, r_2\}$, at least one adversarial block must be mined during rounds $\{T_e + 1, \ldots, r_2\}$ at the same height. In particular, the adversarial block must be mined before r_2 because it is published by time r_2. Thus, we have $Y_{T_e+1,r_2} \leq Z_{T_e+1,r_2}$.

However, since $T_e + 1 \leq s$ and $r_2 \geq r$, we know D_{T_e+1,r_2} occurs under $E_{s,r}$. So we have $Z_{T_e+1,r_2} < Y_{T_e+1,r_2}$ according to (3.66). Contradiction arises. Hence the proof of the theorem. □

3.4. Non-lockstep synchronous model and analysis

In this section, we consider the non-lockstep synchronous model where there is an upper bound T on the delay for message delivery. That is to say, if a block is published during round r, by round $r + T$, all other miners would have received the block. In this section, the definitions of credible blockchains and typical events are similar but different from that in Section 3.3. In the special case of $T = 1$, this model degenerates to the lockstep synchronous model.

Definition 3.24. *(r-credible blockchain) Blockchain b is said to be* r-credible *if it has been published by round r, and is no shorter than any blockchain published by round*

$r - T + 1$. *That is to say,*

$$P_b < r, \tag{3.98}$$

and

$$h(b) \geq h(k), \quad \forall k : P_k < r - T + 1. \tag{3.99}$$

If there is no need to specify round r explicitly, blockchain b can also be simply called a credible blockchain.

Note that in non-lockstep synchronous networks, there can be multiple r-credible blockchains, which may or may not be of the same height.

Lemma 3.25. *If block b is honest, then blockchain f_b must be T_b credible.*

Proof. Lemma 3.25 is obvious by Definition 3.3: if block b is honest, it must extend a T_b-credible blockchain. □

A block is called a lagger if it is the single honest block mined during a round and no other honest block is mined in the previous $T - 1$ rounds. Accordingly, we define the following indicators for $r = T, T + 1, \ldots$:

$$V_r = \begin{cases} 1, & \text{if } H_r = 1 \text{ and} \\ & H_{r-1} = \ldots = H_{r-T+1} = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{3.100}$$

A block is said to be a loner if it is the only honest block during a round and no other honest block is mined within $T-1$ rounds before or after the round. Accordingly, we define the following indicators for $r = T, T+1, \ldots$:

$$W_r = \begin{cases} 1, & \text{if } H_r = 1, H_{r-1} = \ldots = H_{r-T+1} = 0, \\ & \text{and } H_{r+1} = \ldots = H_{r+T-1} = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{3.101}$$

It is important to note that $H_1, H_2, \ldots$ are identically distributed, which form a stationary process. The same can be said of the V and W sequences.

In non-lockstep synchronous networks, 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

$$q \leq \frac{\xi}{20T} \tag{3.102}$$

where ξ is defined in (3.2).

Theorem 3.26. *(Bernoulli's inequality [**35**, page 55]) For every integer $k \geq 0$ and real number $x > -1$,*

$$(1+x)^k \geq 1 + kx. \tag{3.103}$$

Proposition 3.27. *For every $r = T, T+1, \ldots$,*

$$\mathbb{E}[V_r] > q(1-q)^T \tag{3.104}$$

$$> q(1 - Tq). \tag{3.105}$$

Proof. Here, (3.104) is due to (3.15) and Proposition 3.9 and (3.105) is due to Bernoulli's inequality (3.103). □

Proposition 3.28. *For every* $r = T, T + 1, \ldots,$

$$\mathbb{E}[W_r] > q(1 - q)^{2T-1} \tag{3.106}$$

$$> q(1 - (2T - 1)q). \tag{3.107}$$

Proof. Note that $H[r] = 1$ indicates $Y[r] = 1$, $H[r] = 0$ indicates $X[r] = 0$. Then, (3.106) is due to (3.15) and Proposition 3.9, and (3.107) is due to Bernoulli's inequality (3.103). □

Proposition 3.29. *For every* $r = T, T + 1, \ldots,$

$$\mathbb{E}[Z_r] < \mathbb{E}[V_r]. \tag{3.108}$$

Proof. Let $Z'_r \sim \mathit{Binomial}(t, p)$. Since the adversarial mining power is upper bounded by β, we have

$$\mathbb{E}[Z_r] \leq \mathbb{E}\left[Z'_r\right] \tag{3.109}$$

$$= pt \tag{3.110}$$

$$= \frac{t}{n - t} p(n - t) \tag{3.111}$$

$$= (1 - \xi)p(n - t) \tag{3.112}$$

$$< (1-\xi)\frac{q}{1-q} \tag{3.113}$$

$$< q(1-Tq) \tag{3.114}$$

$$\leq \mathbb{E}[V_r], \tag{3.115}$$

where (3.112) is due to (3.2), (3.113) is due to Proposition 3.8, (3.114) is due to (3.102), and (3.115) is due to Proposition 3.27. □

We define $v_m(\cdot)$ on $\mathcal{R}^m$ by

$$v_m(a_1 \ldots, a_m) = \sum_{i=T}^{m} \mathbb{1}\{a_i = 1, a_{i-1} = \ldots = a_{i-T+1} = 0\}. \tag{3.116}$$

Likewise, we define $w_m(\cdot)$ on $\mathcal{R}^m$ by

$$w_m(a_1, \ldots, a_m) = \sum_{i=T}^{m-T+1} \mathbb{1}\{a_i = 1, a_{i-T+1} = \ldots = a_{i-1} = 0 \text{and } a_{i+1} = \ldots = a_{i+T-1} = 0\}. \tag{3.117}$$

Although a_i is allowed to take arbitrary real values, the indicator functions in (3.116) and (3.117) yield a binary value. For all integers s and r satisfying $T \leq s < r$, we have

$$V_{s,r} = v_{r-s+T-1}(H_{s-T+1}, \ldots, H_{r-1}) \tag{3.118}$$

$$= \sum_{i=s}^{r-1} V_i \tag{3.119}$$

and

$$W_{s,r} = w_{r-s+2T-2}(H_{s-T+1}, \ldots, H_{r+T-2}) \tag{3.120}$$

$$= \sum_{i=s}^{r-1} W_i \tag{3.121}$$

where V_i and W_i are as defined in (3.100) and (3.101), respectively.

Lemma 3.30. *For $T \leq s < r$, $v(\cdot)$ is 1-Lipschitz and $w(\cdot)$ is 2-Lipschitz.*

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

Define $w_i = \mathbb{1}\{h_i = 1, h_{i-T+1} = \ldots = h_{i-1} = h_{i+1} = \ldots = h_{i+T-1} = 0\}$, then $w(h_{s-T+1}, \ldots, h_{r+T-2}) = \sum_{i=s}^{r-1} w_i$. Suppose $h_{s-T+1}, \ldots, h_k, \ldots, h_{r+T-2}$ changes to h_{s-T+1}, $\ldots$, h'_k, $\ldots$, 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 $w_m, \ldots, w_{k-1}, w_k, w_{k+1}, \ldots, w_n$ are possibly affected by this change. By definition, at most two elements of $w_m, \ldots, w_n$ can be non-zero, and they must be on different sides of w_k. Then there are two cases: 1) There are no more than one none-zero elements in $w_m, \ldots, w_n$, 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 $w_p = 1$ and $w_q = 1$. In this case, we must have $h_k = 0$ and $h'_k \neq 0$ according to the definition of w_p, w_q. Thus w_p and w_q change from 1 to 0. Meanwhile, w_k may change from 0 to 1 or remain unchanged, and $w_p + w_k + w_q$ can change by 1 or 2, but not more than 2 from of its original value. So $w(\cdot)$ is 2-Lipschitz. □

Following (3.7), we define

$$V_{s,r} = \sum_{i=s}^{r-1} V_i, \tag{3.122}$$

$$W_{s,r} = \sum_{i=s}^{r-1} W_i \tag{3.123}$$

for all integers $1 \leq s < r$.

For convenience, we define

$$\mu = \frac{\xi^2}{4000T^2} q^2 (1-q)^{4T-2}. \tag{3.124}$$

Definition 3.31. *For all integers $T \leq s < r$, define event*

$$F_{s,r} = F^1_{s,r} \cap F^2_{s,r} \cap F^3_{s,r} \cap F^4_{s,r} \tag{3.125}$$

where

$$F^1_{s,r} = \left\{ (1 - \frac{\xi}{20}) \mathbb{E}[V_{s,r}] < V_{s,r} \right\}, \tag{3.126}$$

$$F^2_{s,r} = \left\{ X_{s,r} < (1 + \frac{\xi}{20}) \mathbb{E}[X_{s,r}] \right\}, \tag{3.127}$$

$$F_{s,r}^3 = \left\{ (1 - \frac{\xi}{20})\mathbb{E}[W_{s,r}] < W_{s,r} \right\}, \tag{3.128}$$

$$F_{s,r}^4 = \left\{ Z_{s,r} < \mathbb{E}[Z_{s,r}] + \frac{\xi}{20}\mathbb{E}[V_{s,r}] \right\}. \tag{3.129}$$

Definition 3.32. *Let f be a function on $\mathcal{R}^n$. Let $x, x' \in \mathcal{R}^n$. A function $f(x_1, \ldots, x_n)$ is k-Lipschitz if $|f(x) - f(x')| \leq k$ whenever x and x' differ in at most one coordinate.*

Theorem 3.33. *(McDiarmid's inequality, [**36**, page 40]) If f on $\mathcal{R}^n$ is k-Lipschitz and $X_1, \ldots, X_n$ are independent random variables, then for every $t > 0$,*

$$P(f(X_1, \ldots, X_n) > \mathbb{E}[f(X_1, \ldots, X_n)] + t) \leq e^{-\frac{2t^2}{nk^2}}, \tag{3.130}$$

$$P(f(X_1, \ldots, X_n) < \mathbb{E}[f(X_1, \ldots, X_n)] - t) \leq e^{-\frac{2t^2}{nk^2}}. \tag{3.131}$$

Lemma 3.34. *For all integers $T \leq s < r$,*

$$P(F_{s,r}) > 1 - 4e^{-\mu(r-s)}, \tag{3.132}$$

where μ is given in (3.124).

Proof. Because V_r and V_s are dependent, standard Chernoff bound does not apply. Similarly for W_r and W_r. However, due to Lemma 3.30, we have

$$P((F_{s,r}^1)^c) = P\left(V_{s,r} \leq \mathbb{E}[V_{s,r}] - \frac{\xi}{20}\mathbb{E}[V_{s,r}] \right) \tag{3.133}$$

$$\leq e^{-\frac{\xi^2}{200(r-s+T-1)}\mathbb{E}[V_{s,r}]^2} \tag{3.134}$$

$$\leq e^{-\frac{\xi^2}{200}q^2(1-q)^{2T}(r-s+T-1)} \tag{3.135}$$

$$\leq e^{-\frac{\xi^2}{200}q^2(1-q)^{2T}(r-s)} \tag{3.136}$$

where (3.134) is due to Theorem 3.33, (3.135) is due to Proposition 3.27, and (3.136) is due to $T \geq 1$.

Similarly,

$$P((F^3_{s,r})^c) = P\left(W_{s,r} \leq \mathbb{E}[W_{s,r}] - \frac{\xi}{20}\mathbb{E}[W_{s,r}]\right) \tag{3.137}$$

$$\leq e^{-\frac{\xi^2}{200(r-s+2T-2)}(\mathbb{E}[W_{s,r}])^2} \tag{3.138}$$

$$\leq e^{-\frac{\xi^2}{200}q^2(1-q)^{4T-2}(r-s+2T-2)} \tag{3.139}$$

$$\leq e^{-\frac{\xi^2}{200}q^2(1-q)^{4T-2}(r-s)} \tag{3.140}$$

where (3.138) is due to Theorem (3.33), (3.139) is due to (3.106), and (3.140) is due to $T \geq 1$.

By Theorem 3.12,

$$P((F^2_{s,r})^c) = P\left(X_{s,r} \geq (1+\frac{\xi}{20})\mathbb{E}[X_{s,r}]\right) \tag{3.141}$$

$$\leq e^{-\frac{\xi^2}{1200}q(r-s)}. \tag{3.142}$$

According to (3.115), $E[Z_{s,r}] < E[V_{s,r}]$. Note that the moment generating function for binomial random variable $Z_r \sim Binomial(t,p)$ is $(1-p+pe^u)^t$ **[34]**. Pick arbitrary $u > 0$. We have

$$P((F^4_{s,r})^c) = P\left(Z_{s,r} \geq \mathbb{E}[Z_{s,r}] + \frac{\xi}{20T}\mathbb{E}[V_{s,r}]\right) \tag{3.143}$$

$$\leq P\left(Z_{s,r} \geq \mathbb{E}[Z_{s,r}] + \frac{\xi}{40T}\mathbb{E}[Z_{s,r}] + \frac{\xi}{40T}\mathbb{E}[V_{s,r}]\right) \tag{3.144}$$

$$< \frac{\mathbb{E}[e^{Z_{s,r}u}]}{e^{(1+\frac{\xi}{40T})\mathbb{E}[Z_{s,r}]u+\frac{\xi}{40T}\mathbb{E}[V_{s,r}]u}} \tag{3.145}$$

$$= \frac{(1-p+pe^u)^{t(r-s)}}{e^{(1+\frac{\xi}{40T})(r-s)tpu+\frac{\xi}{40T}q(1-q)^T u(r-s)}} \tag{3.146}$$

$$\leq e^{(e^u-1-u(1+\frac{\xi}{40T}))tp(r-s)-\frac{\xi}{40T}uq(1-q)^T(r-s)}, \tag{3.147}$$

where (3.145) is by the Chernoff inequality and (3.147) 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

$$P((F^4_{s,r})^c) \leq e^{(\frac{\xi}{40T}-(1+\frac{\xi}{40T})\log(1+\frac{\xi}{40T}))tp(r-s)-\frac{\xi}{40T}\log(1+\frac{\xi}{40T})q(1-q)^T(r-s)} \tag{3.148}$$

$$< e^{-\frac{\xi}{40T}\log(1+\frac{\xi}{40T})q(1-q)^T(r-s)} \tag{3.149}$$

$$< e^{-\frac{\xi^2}{4000T^2}q(1-q)^T(r-s)}, \tag{3.150}$$

where (3.149) is due to $(1+x)\log(1+x) > x$ for all $x > 0$ and (3.150) is due to $\log(1+\frac{\xi}{40T}) > \frac{\xi}{100T}$ for all $\xi \in (0,1]$ and $T \geq 1$.

Since μ defined in (3.124) dominates the corresponding exponential coefficients in (3.136), (3.140), (3.142), and (3.150), we have

$$P(F_{s,r}) = 1 - P((F_{s,r})^c) \tag{3.151}$$

$$\geq 1 - P((F^1_{s,r})^c) - P((F^2_{s,r})^c) - P((F^3_{s,r})^c) - P((F^4_{s,r})^c) \tag{3.152}$$

$$> 1 - 4e^{-\mu(r-s)}. \tag{3.153}$$

□

Lemma 3.35. *For all integers $T \leq s < r - \frac{2}{q}$, the following inequalities hold under event $F_{s,r}$:*

$$(1 - \frac{\xi}{20})q(1-q)^T(r-s) < V_{s,r} \tag{3.154}$$

$$X_{s,r} < (1 + \frac{\xi}{20})q(r-s) \tag{3.155}$$

$$(1 - \frac{\xi}{3})q(r-s) < W_{s,r} \tag{3.156}$$

$$Z_{s,r} < (1 - \frac{2\xi}{3})q(r-s). \tag{3.157}$$

The following inequalities hold under event $F_{s+T,r-T}$:

$$Z_{s,r} < (1 - \frac{\xi}{2})V_{s+T,r-T} \tag{3.158}$$

$$Z_{s,r} < W_{s+T,r-T}. \tag{3.159}$$

Proof. Under $F_{s,r}$, (3.154) follows directly from (3.126). (3.155) follows directly from (3.127).

To prove (3.156), we write

$$W_{s,r} > (1 - \frac{\xi}{20})E[W_{s,r}] \tag{3.160}$$

$$> (1 - \frac{\xi}{20})(1 - (2T-1)q)q(r-s) \tag{3.161}$$

$$> (1 - \frac{\xi}{20})(1 - \frac{\xi}{10})q(r-s) \tag{3.162}$$

$$> (1 - \frac{\xi}{3})q(r-s), \tag{3.163}$$

where (3.160) is due to (3.128), (3.161) is due to Proposition 3.28, (3.162) is due to (3.102), and (3.163) is due to $\xi \in [0, 1)$ and $T \geq 1$.

To prove (3.157),

$$Z_{s,r} < \mathbb{E}[Z_{s,r}] + \frac{\xi}{20}\mathbb{E}[V_{s,r}] \tag{3.164}$$

$$= pt(r-s) + \frac{\xi}{20}q(1-q)^T(r-s) \tag{3.165}$$

$$= \frac{t}{n-t}(n-t)p(r-s) + \frac{\xi}{20}q(1-q)^T(r-s) \tag{3.166}$$

$$\leq (1-\xi)\frac{q}{1-q}(r-s) + \frac{\xi}{20}q(1-q)^T(r-s) \tag{3.167}$$

$$\leq (1-\xi)\frac{q}{1-\frac{\xi}{20T}}(r-s) + \frac{\xi}{20}q(r-s) \tag{3.168}$$

$$< \left(1 - \frac{2\xi}{3}\right) q(r-s), \tag{3.169}$$

where (3.164) is due to (3.129), (3.167) is due to Proposition 3.8, (3.168) is due to (3.102), and (3.169) is due to $\xi \in (0, 1]$.

By assumption (3.102),

$$T \leq \frac{\xi}{20q} \tag{3.170}$$

$$< \frac{\xi}{40}(r-s) \tag{3.171}$$

where (3.171) is by the assumption of this lemma: $r - s > \frac{2}{q}$. Thus,

$$r - s < \frac{r-s-T}{1-\frac{\xi}{40}} \tag{3.172}$$

and

$$r - s < \frac{r - s - 2T}{1 - \frac{\xi}{20}} \tag{3.173}$$

To prove (3.158), we begin with (3.167):

$$\begin{aligned}
Z_{s,r} &< (1-\xi)\frac{q}{1-q}(r-s) + \frac{\xi}{20}q(1-q)^T(r-s) && (3.174)\\
&< \left(\frac{1-\xi}{(1-q)^{T+1}} + \frac{\xi}{20}\right) q(1-q)^T \frac{r-s-T}{1-\frac{\xi}{40}} && (3.175)\\
&< \left(\frac{1-\xi}{1-(T+1)q} + \frac{\xi}{20}\right) q(1-q)^T \frac{r-s-T}{1-\frac{\xi}{40}} && (3.176)\\
&< \left(\frac{1-\xi}{1-(T+1)q} + \frac{\xi}{20}\right) \frac{V_{s,r-T}}{(1-\frac{\xi}{20})(1-\frac{\xi}{40})} && (3.177)\\
&< \left(\frac{1-\xi}{1-\frac{\xi}{10}} + \frac{\xi}{20}\right) \frac{1}{(1-\frac{\xi}{20})(1-\frac{\xi}{40})} V_{s,r-T} && (3.178)\\
&< (1-\frac{\xi}{2})V_{s,r} && (3.179)
\end{aligned}$$

where (3.175) is due to (3.172), (3.176) is due to (3.103), (3.177) is due to (3.154), (3.178) is due to $q < \frac{\xi}{10(T+1)}$, (3.179) is due to $\xi \in [0, 1)$.

To prove (3.159),

$$\begin{aligned}
Z_{s,r} &< (1-\frac{2\xi}{3})q(r-s) && (3.180)\\
&< (1-\frac{2\xi}{3})q\frac{r-s-2T}{1-\frac{\xi}{20}} && (3.181)\\
&< (1-\frac{\xi}{3})q(r-s-2T) && (3.182)\\
&< W_{s+T,r-T}, && (3.183)
\end{aligned}$$

where (3.180) is due to (3.157), (3.181) is due to (3.173), (3.182) is due to $\xi \in [0, 1)$, and (3.183) is due to (3.156). □

Definition 3.36. *For all integers $T \leq s < r - \frac{2}{q}$, define typical event*

$$G_{s,r} = \bigcap_{0 \leq a \leq s-T, b \geq 0} F_{s-a,r+b}. \tag{3.184}$$

$G_{s,r}$ occurs when events $F_{k,\ell}$ simultaneously occurs for all k, ℓ, i.e., the "F" event occur over all consecutive rounds containing $\{s, \ldots, r\}$. The event J represents a collection of outcomes that constrain the number of blocks mined in all those rounds, including arbitrarily large intervals that end in the arbitrarily far future. The "good" properties in Lemma 3.35 to extend to all those rounds under the event $G_{s,r}$.

Lemma 3.37. *For all integers $T \leq s < r - \frac{2}{q}$,*

$$P(G_{s,r}) > 1 - 5\mu^{-2}e^{-\mu(r-s)}. \tag{3.185}$$

Proof. Due to the stationarity of processes X, Y, Z, V, and W, $P(F_{s,r}) = P(F_{T,T+r-s})$ for all s, r. Evidently the probability depends on r and s only through the interval length $r - s$:

$$P((G_{s,r})^c) = P\left(\bigcup_{0 \leq a \leq s-T, b \geq 0} (F_{s-a,r+b})^c\right) \tag{3.186}$$

$$= P\left(\bigcup_{0 \leq a \leq s-T, b \geq 0} (F_{T,r-s+a+b+T})^c\right) \tag{3.187}$$

$$\leq \sum_{0 \leq a \leq s-T, b \geq 0} P((F_{T,r-s+a+b+T})^c) \tag{3.188}$$

$$= \sum_{k=0}^{\infty} \sum_{0 \le a \le s-T, b \ge 0, a+b=k} P((F_{T,r-s+k+T})^c) \tag{3.189}$$

$$< \sum_{k=0}^{\infty} (k+1) P((F_{T,r-s+k+T})^c) \tag{3.190}$$

$$< \sum_{k=0}^{\infty} (k+1) 4e^{-\mu(r-s+k)} \tag{3.191}$$

$$= 4e^{-\mu(r-s)} \sum_{k=0}^{\infty} (k+1) e^{-\mu k} \tag{3.192}$$

$$= \frac{4}{(1-e^{-\mu})^2} e^{-\mu(r-s)}. \tag{3.193}$$

According to (3.102) and (3.124), $\mu < \frac{1}{4000}$. Thus, (3.185) is established using the fact that $1 - e^{-x} > \frac{4}{\sqrt{5}} x$ for all $x \in [0, \frac{1}{4000}]$. □

Lemma 3.38. *If an r-credible blockchain has height h, then the heights of all $(r+T)$-credible blockchains are at least h.*

Proof. Lemma 3.38 is obvious by the Definition 3.24. □

Lemma 3.39. *Laggers have different heights.*

Proof. Suppose two laggers block b and block d with $T_d \ge T_b$ have the same height k. Because block d is a lagger, we must have $T_d \ge T_b + T$. According to Lemma 3.38, the heights of all (T_b+T)-credible blocks are at least k. Since blockchain f_d is T_d-credible and $T_d \ge T_b + T$, the height of block d is at least $k+1$, which contradicts the assumption. □

Lemma 3.40. *Let $T \le s \le r - \frac{2}{q}$ be integers. Suppose an s-credible blockchain has height ℓ. Then all r-credible blockchains have heights at least $\ell + V_{s,r-T}$.*

Proof. We will prove the lemma by induction on r: Consider $r = s + T$. Since an s-credible blockchain has height ℓ, the height of an $(s + T)$-credible blockchain must be at least ℓ.

We next assume the claim holds for $r = s + T, \ldots, s + T + u$ and show that it also holds for $s + T + u + 1$. 1) If $V_{s+u+1} = 0$, the claim holds trivially. 2) If $V_{s+u+1} = 1$, then by definition of V, $H_{s+u} = \cdots = H_{s+u-T+2} = 0$. By induction, all $(s + u + 1)$-credible blockchains have heights at least $\ell' = \ell + V_{s,s+u-T+1} = \ell + V_{s,s+u+1}$. Since $V_{s+u+1} = 1$, during round $s + u + 1$ at least one honest block with height $\ell' + 1$ is broadcast. Then all $(s+T+u+1)$-credible blockchains have heights at least $\ell'+1 = \ell+V_{s,s+u+1}$ by Definition 3.24.

By induction on r, Lemma 3.40 holds. □

Lemma 3.41. *A loner is the only honest block at its height.*

Proof. Suppose block b is a loner and block d is a different honest block. Then $T_d \leq T_b - T$ or $T_d \geq T_b + T$ by definition of a loner. If $T_d \geq T_b + T$, we have $h(d) \geq h(b) + 1$ since blockchain b is published during round T_b. If $T_d < T_b$, we have $h(d) \leq h(b) - 1$ (if $h(d) \geq h(b)$, block b's height would be at least $h(b) + 1$). Thus the proof of Lemma 3.41. □

Lemma 3.42. *For all integers $T \leq s < r - \frac{2}{q}$ and $k \geq 2q(r - s)$, under typical event $G_{s,r}$, the k-deep block and k-deep prefix of every r-credible blockchain must be mined before round s.*

Proof. The number of blockchain growth during rounds $\{s, \ldots, r-1\}$ is upper bounded by $X_{s-T,r} + Z_{s-T,r}$. Under event $G_{s,r}$, event $G_{s-T,r}$ occurs. Note that

$$X_{s-T,r} + Z_{s-T,r} < (1 + \frac{\xi}{20})q(r-s+T) + (1 - \frac{2\xi}{3})q(r-s+T) \tag{3.194}$$

$$< (2 - \frac{\xi}{2})q(r-s+T) \tag{3.195}$$

$$< 2q(r-s) \tag{3.196}$$

$$\leq k, \tag{3.197}$$

where (3.194) is due to (3.155) and (3.157), (3.196) is due to (3.102) and $r - s > \frac{2}{q}$. Then, the k-deep block and k-deep prefix must be mined before round s. □

Theorem 3.43 (Blockchain growth theorem under non-lockstep synchronous model)**.** *Let r, s, s_1 be integers satisfying $T \leq s_1 \leq s < r - \frac{2}{q}$. Under typical event $G_{s,r-T}$, the height of every r-credible blockchain must be at least $(1 - \frac{\xi}{10})(1-q)^T(r-s_1)q$ more than the maximum height of all s_1-credible blockchains.*

Proof. Assume the maximum height of s_1-credible blockchains is ℓ. If event $G_{s,r-T}$ occurs, event $G_{s_1,r-T}$ occurs. We have

$$V_{s_1,r-T} > (1 - \frac{\xi}{20})(1-q)^T q(r - s_1 - T) \tag{3.198}$$

$$= (1 - \frac{\xi}{20})(1-q)^T q(1 - \frac{T}{r-s_1})(r-s_1) \tag{3.199}$$

$$> (1 - \frac{\xi}{20})(1 - \frac{T}{r-s_1})(1-q)^T(r-s_1)q \tag{3.200}$$

$$\geq (1 - \frac{\xi}{20})(1 - \frac{\xi}{40})(1-q)^T(r-s_1)q \tag{3.201}$$

$$> (1 - \frac{\xi}{10})(1-q)^T(r-s_1)q, \tag{3.202}$$

where (3.198) is due to (3.154), (3.201) is due to $r - s_1 \geq \frac{2}{q}$ and (3.102), and (3.202) is due to $\xi \in [0, 1)$. By Lemma 3.40, the height of any r-credible blockchain is at least $\ell + (1 - \frac{\xi}{10})(1-q)^T(r-s_1)q$. □

Theorem 3.44 (Blockchain quality theorem under non-lockstep synchronous model)**.** *Let r, s, k be integers satisfying $T \leq s < r - \frac{2}{q}$ and $k \geq 2(r-s)q$. Suppose an r-credible blockchain has more than k blocks, then under event $G_{s+T,r-T}$, at least $\frac{\xi}{2}k$ of the last k blocks of this blockchain are honest.*

Proof. Suppose blockchain d is r-credible and $h(d) \geq k$. Denote the k-deep block of blockchain d as block b. Let block e be the highest honest block mined before block b on blockchain b. Then we have $0 \leq h(e) < h(b)$. The relationship between these blocks is illustrated as follows:

$$\boxed{e} - \cdots - \boxed{} - \overbrace{\boxed{b} - \cdots - \boxed{d}}^{k \text{ blocks}} \tag{3.203}$$

round s_1 round r

Let $s_1 = T_e$ for convenience. According to Lemma 3.42, we have $s_1 < s$. Denote the number of honest blocks between block b (inclusive) and block d (inclusive) as x. To prove the theorem, it suffices to show $x > \frac{\xi}{2}k$.

By definition, on blockchain d, all blocks at heights $\{h(e)+1, \ldots, h(b)-1\}$ are adversarial, thus the number of honest blocks between block e (exclusive) and block d (inclusive)

is also x. Let $y = h(d) - h(e)$, then the number of adversarial blocks on blockchain b between block e (exclusive) and block d (inclusive) is $y - x$. Then $y - x$ is a lower bound for the total number of adversarial blocks generated during round $\{s_1, \ldots, r-1\}$. We have

$$y - x \leq Z_{s_1,r}. \tag{3.204}$$

Note that an $(s_1 + T)$-credible blockchain has height at least $h(e)$. Since blockchain d is r-credible, by Lemma 3.40 we have

$$h(d) - h(e) = y \geq V_{s_1+T,r-T}. \tag{3.205}$$

Under event $G_{s+T,r-T}$, event $F_{s_1+T,r-T}$ occurs. Thus,

$$y - x \leq Z_{s_1,r} \tag{3.206}$$

$$< (1 - \frac{\xi}{2}) V_{s_1+T,r-T} \tag{3.207}$$

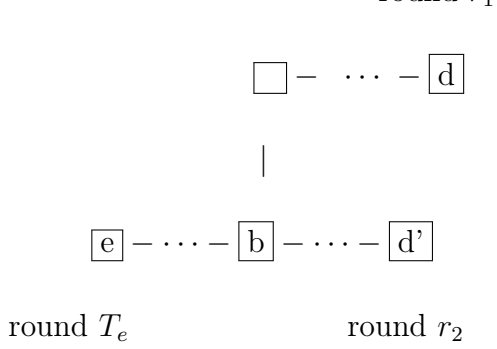
$$< (1 - \frac{\xi}{2}) y, \tag{3.208}$$

where (3.207) is due to (3.158). From (3.208), $x > \frac{\xi}{2}k$ is derived. □

Theorem 3.45 (Common prefix property under non-lockstep synchronous model)**.** *Let r, s, k be integers satisfying $T \leq s < r - \frac{2}{q}$ and $k > 2(r-s)q$. If an r-credible blockchain has a k-deep prefix, then the prefix is permanent after round r under $G_{s+T,r-T}$.*

Proof. We prove the desired result by contradiction. Let blockchain b be the k-deep prefix of an r-credible blockchain. If block b is the genesis block, the theorem is trivial. Otherwise, we will show contradiction if blockchain b is not permanent after r.

Suppose round $r_1 \geq r$ is the smallest integer such that there exists an r_1-credible blockchain (denoted as blockchain d) which does not extend blockchain b. If $r_1 = r$, let $r_2 = r$. If $r_1 > r$, let $r_2 = r_1 - 1$. Then there must exist an r_2-credible blockchain that extends blockchain b (denoted as blockchain d'). Let block e be the highest honest block shared by blockchain d and blockchain d'. Then we have $T_e < s$ by Lemma 3.20. The relationship between these blocks is illustrated as follows:



(3.209)

Next we will show $Y_{T_e+T+1,r_2-T} \leq Z_{T_e+1,r_2}$. If $Y_{T_e+T+1,r_2-T} = 0$, it is obvious. Otherwise, consider a loner c mined during rounds $\{T_e + 1 + T, \ldots, r_2 - T - 1\}$. Since block e is mined during round T_e, every $(T_e + T)$-credible blockchain has height at least $h(e)$. Since block c is honest, its height must be larger than a T_c-credible blockchain. Since $T_c \geq T_e + T + 1$, we know $h(c) > h(e)$. Since $T_c \leq r_2 - T - 1$ and $r_1 \geq r_2$, every r_1-credible blockchain and r_2-credible blockchain has height at least $h(c)$. We have $h(c) \leq \min\{h(d), h(d')\}$. Consider the following two only possible cases:

(1) If $h(e) < h(c) \leq h(b)$, there exists at least one adversarial block at height $h(c)$ because all blocks between block e (exclusive) and block b (inclusive) are adversarial by definition.

(2) If $h(b) < h(c) \leq \min\{h(d), h(d')\}$, there is at least one adversarial block at height $h(c)$, because two diverging blockchains exist but loner c is the only honest block at its height by Lemma 3.17.

Thus, for every loner c mined during rounds $\{T_e + T + 1, \ldots, r_2 - T - 1\}$, at least one adversarial block must be mined at the same height. In particular, the adversarial blocks must be mined before r_2 because it is published by time r_2. Thus, we have $Y_{T_e+T+1,r_2-T} \leq Z_{T_e+1,r_2}$.

However, since $s > T_e$ and $r \leq r_2$, F_{T_e+1,r_2} occurs under event $G_{s,r}$. So we have $Z_{T_e+1,r_2} < Y_{T_e+T+1,r_2-T}$ according to (3.159). Contradiction arises. Hence the proof of the theorem. □

So far, we have analyzed the Bitcoin backbone protocol assuming unlimited lifespan under both the lockstep synchronous model and non-lockstep synchronous model, allowing 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. This framework also serves as a basis for the following analysis of the Prism backbone protocol.

CHAPTER 4

Analyses of the Prism Backbone Protocol

4.1. Introduction

The throughput of Bitcoin is very limited by design to ensure security [**18**]. 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 [**19**]. 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 [**19**–**25**]. Another line of work is to decouple the various functionalities of the blockchain [**26**, **27**], under the spirit of which Bagaria, Kannan, Tse, Fanti, and Viswanath [**32**] 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 [**32**].

In [**32**], liveliness and consistency of Prism transactions were proved assuming a finite life span of the blockchains under the lockstep synchrony model [**32**]. In this chapter, we strengthen and extend the results to the non-lockstep synchrony model. This chapter 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.

The Prism protocol was invented and fully described in [**9**]. Here we describe the Prism backbone protocol with just enough details to facilitate its analysis.

4.2. General model of the Prism protocol

Blocks are generated in a peer-to-peer network where honest and adversarial miners mine and publish blocks over time. The blocks are classified into $m+1$ categories, referred to as 0-blocks, 1-blocks, ..., m-blocks. A block is mined before knowing which kind of block it is, so it contains enough information for all $(m+1)$ kinds of blocks. Sortition relies on the range the new block's hash lands in: If a miner constructs a new block whose hash is within $[j\gamma, j\gamma+\gamma)$ for $j \in \{0,\ldots,m\}$, the mined block is a j-block. Parameter γ can be adjusted to control the mining rate.

Definition 4.1 (j-blocks)**.** *For $j \in \{0,\ldots,m\}$, we assume a genesis j-block, referred to as j-block 0, is mined at time 0. Subsequent j-blocks are referred to as j-block 1, j-block 2, and so on, in the order they are mined in time after time 0.*

Definition 4.2 (j-blockchain and height)**.** *For $j \in \{0,\ldots,m\}$, every non-genesis j-block must contain the hash value of a unique parent j-block which is mined strictly earlier. We use $f_i^j \in \{0,1,...,i-1\}$ to denote j-block i's parent j-block number. The sequence*

$(b_0, \ldots, b_n)$ defines a j-blockchain if $b_0 = 0$ and $f^j_{b_k} = b_{i-1}$ for $i = 1, \ldots, n$. It is also referred to as j-blockchain b_n since b_n uniquely identifies it. The height of both j-block b_i and j-blockchain b_i is said to be i.

Definition 4.3 (A miner's longest j-blockchain)**.** *Let $j \in \{0, 1, \ldots, m\}$. A j-blockchain is in a miner's view at round r if all blocks of the j-blockchain are in the miner's view at round r. A miner's longest j-blockchain at round r is a j-blockchain with the maximum height in the miner's view at round r. Ties are broken in an arbitrary manner.*

Definition 4.4 (Honest and adversarial miners)**.** *Each miner is either honest or adversarial. Let $j \in \{0, 1, \ldots, m\}$. A j-block is said to be honest (resp. adversarial) if it is mined by an honest (resp. adversarial) miner. An honest j-block mined during round r must extend its miner's longest j-blockchain at round r.*

Definition 4.5 (Publication)**.** *Let $j \in \{0, 1, \ldots, m\}$. A j-block is said to be published at round r if it is included in at least one honest miner's view at round r. A j-blockchain is said to be published at round r if all of its j-blocks are published at round r.*

We let T^j_b denote the round when j-block b is mined. We let P^j_b denote the round at which block b is published. By definition 4.4, an honest j-block b is published at the round it is mined. We have $T^j_b = P^j_b$.

For $j = 0, 1, \ldots, m$ and $r = 1, 2, \ldots$, let H^j_r denote the total number of honest j-blocks mined during round r. Following the definitions in the Bitcoin protocol, for $j = 0, 1, \ldots, m$

and $r = 1, 2, \ldots$, we also define

$$X_r^j = \begin{cases} 1, & \text{if } H_r^j \geq 1 \\ 0, & \text{otherwise,} \end{cases} \tag{4.1}$$

$$Y_r^j = \begin{cases} 1, & \text{if } H_r^j = 1 \\ 0, & \text{otherwise,} \end{cases} \tag{4.2}$$

and let Z_r^j be the total number adversarial j-blocks mined during round r.

However, it does not suffice to generate a high-throughput transaction ledger by simply putting $(m + 1)$ Bitcoin blockchains in parallel. In particular, while all transactions in each blockchain itself are consistent, transactions on different blockchains may contradict each other, e.g., there may be double spending across different blockchains. In the Prism protocol, these $(m + 1)$ Bitcoin blockchains are building blocks. An additional process, referred to as voting, is executed to resolve conflicts and achieve global consensus. To be specific, block are classified into proposer blocks (0-blocks) and voter blocks (all j-blocks with $j \in \{1, \ldots, m\}$). Blockchains are classified into proposer blockchains (0-blockchains) and voter blockchains (all j-blockchains with $j \in \{1, \ldots, m\}$). The voting by credible voter blockchains elects a series of proposer blocks called a credible leader sequence, which is responsible for generating a final transaction ledger. A credible leader sequence may or may not be a credible 0-blockchain. While the properties of Bitcoin blockchains ensure the liveness and consistency of voter blockchains, the voting process ensures the

liveness and consistency of credible leader sequences. Below we briefly describe voting and transaction ledger generation.

By saying a voter j-block b votes on a height h, we mean the voter block chooses one proposer block among all proposer blocks at height h and points to the proposer block with a reference link. The reference link is part of the content of voter j-block b, thus it is immutable. Obviously voter j-block b can not vote on height where the first block on this height is mined after it.

According to the Prism protocol, when voting on a height, an honest voter block always chooses the first observed proposer block of this height. An honest voter j-block b votes on all heights h as long as 1) it has observed blocks on height h and 2) height h has not been voted on by the voter block's ancestors. An adversarial voter block may not choose the first observed proposer block when voting. An adversarial voter block may refuse to vote on some height or repeatedly vote on some height that has already been voted by its ancestors.

At each height, the vote(s) from one voter blockchain is counted only once (only the first vote is valid if there exist several). In other words, proposer blocks on the same height receive up to m votes from m voter blockchains in total.

Definition 4.6. *For positive integer h, we let R_h denote the round when the first proposer block on height h is published.*

Definition 4.7. *(Reachable) By saying block d is reachable from block b (or block b reaches block d), we mean block b points to block d by a sequence of reference links.*

Given a credible leader sequence $(0, b_1, \ldots, b_n)$, each credible leader block b_h defines an epoch. Added to the ledger are the blocks which are pointed to by b_h, as well as other blocks reachable from b_h 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. A transaction ledger is created by keeping only the first transaction among double spends or redundant transactions.

Definition 4.8. *(h-high prefix) For every $h \in \{0, \ldots, n\}$, by the h-high prefix of t-credible leader sequence $(0, b_1, \ldots, b_n)$ we mean the sequence of proposer blocks $(0, \ldots, b_h)$.*

4.3. Lockstep synchronous model and analysis

Definition 4.9. *(r-credible j-blockchain) For $j \in \{0, \ldots, m\}$, we say j-blockchain b is r-*credible *if it has been published by round r, and is no shorter than any j-blockchain published by round r. That is to say,*

$$P_b^j < r, \tag{4.3}$$

and

$$h^j(b) \geq h^j(b), \quad \forall k : P_k^j < r. \tag{4.4}$$

If there is no need to specify round r explicitly, j-blockchain b can also be simply called a credible blockchain.

Definition 4.10. *(r-credible leader sequence) Let proposer block $b_1, \ldots, b_n$ be proposer blocks at heights $1, \ldots, n$, respectively, where n is greater or equal to the maximum height of all proposer blockchains published by round r. We say $(0, b_1, \ldots, b_n)$ is an r-credible leader sequence if it is elected by a collection of m r-credible voter blockchains including one j-blockchain for every $j \in \{1, \ldots, m\}$. That is, for every $\ell \in \{1, \ldots, n\}$, proposer block b_ℓ receives the most votes among all proposer blocks of height ℓ at round r from that collection of voter blockchains. In particular, we have $n \geq h$ if height h satisfies $R_h \leq r - 1$. Block b_ℓ is called an r-credible leader block. If there is no need to specify r explicitly, an r-credible leader sequence (block) can also be simply referred to as a credible leader sequence (block).*

Note that even if all proposer blocks of height h have received zero vote, a credible leader block of height h can still exist according to the tie breaking rule. Moreover, as an r-credible leader sequence is defined with respect to a collection of r-credible voter blockchains, in general there can be multiple r-credible leader sequences.

Lemma 4.11. *If proposer blocks $(0, b_1, \ldots, b_n)$ is an r-credible leader sequence, then 0-blockchain b_n is an r-credible 0-blockchain.*

Proof. By definition, n is greater or equal to the maximum height of all proposer blockchains (0-blockchains) published by round r. Thus the proof of Lemma 4.11. □

Every r-credible leader sequence determines a transaction ledger for round r. According to the Prism protocol, as part of its content, an honest proposer block b includes a reference link to every proposer and voter block that is observable from it and has not been pointed to by other reference links.

Lemma 4.12. *If j-block b is honest, then j-blockchain f_b^j must be T_k^j credible.*

Proof. Lemma 4.12 is obvious since an honest j-block must extend a credible j-blockchain. □

Definition 4.13. *For all integers $1 \leq s < r$ and $0 \leq j \leq m$, define event*

$$D_{s,r}^j = D_{s,r}^{1,j} \cap D_{s,r}^{2,j} \cap D_{s,r}^{3,j} \tag{4.5}$$

where

$$D_{s,r}^{1,j} = \left\{ (1 - \frac{\xi}{6})\mathbb{E}[X_{s,r}^j] < X_{s,r}^j < (1 + \frac{\xi}{6})\mathbb{E}[X_{s,r}^j] \right\} \tag{4.6}$$

$$D_{s,r}^{2,j} = \left\{ (1 - \frac{\xi}{6})\mathbb{E}[Y_{s,r}^j] < Y_{s,r}^j \right\} \tag{4.7}$$

$$D_{s,r}^{3,j} = \left\{ Z_{s,r}^j < \mathbb{E}[Z_{s,r}^j] + \frac{\xi}{6}\mathbb{E}[X_{s,r}^j] \right\}. \tag{4.8}$$

We note that for integers $j \in \{0, 1, \ldots, m\}$ and $r \geq 1$, H_r^j, X_r^j, Y_r^j, and Z_r^j here are identically distributed as H_r, X_r, Y_r, and Z_r defined in Section 3.3. Also, for $1 \leq s < r$, $D_{s,r}^j$ is defined in the same manner as $D_{s,r}$. Thus, the proposer blockchain and all voter blockchains satisfy similar properties as in Lemma 3.14:

Lemma 4.14. *(Typical properties lemma for proposer and voter blockchain) For all integers $1 \leq s < r$ and $j \in \{0, 1, \ldots, m\}$, under event $D_{s,r}^j$, the following holds:*

$$(1 - \frac{\xi}{6})q(r-s) < X_{s,r}^j < (1 + \frac{\xi}{6})q(r-s) \tag{4.9}$$

$$Y_{s,r}^j > (1 - \frac{\xi}{3})q(r-s) \tag{4.10}$$

$$Z_{s,r}^j < (1 - \frac{2\xi}{3})q(r-s) \tag{4.11}$$

$$Z_{s,r}^j < (1 - \frac{\xi}{2})X_{s,r}^j \tag{4.12}$$

$$Z_{s,r}^j < Y_{s,r}^j. \tag{4.13}$$

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.14. □

Definition 4.15. *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*

$$E_{s,r}^j = \bigcap_{0 \leq a < s, b \geq 0} D_{s-a,r+b}^j. \tag{4.14}$$

Lemma 4.16. *For all integers $1 \leq s < r$ and $0 \leq j \leq m$,*

$$P(E_{s,r}^j) > 1 - 5\eta^{-2}e^{-\eta(r-s)} \tag{4.15}$$

where η is defined in (3.40).

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.16. □

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 4.17. *Let $1 \leq s < r$ and $j \in \{0, 1, \ldots, m\}$ be integers. Suppose an s-credible j-blockchain has height ℓ. Then all r-credible j-blockchains have height at least $\ell + X^j_{s,r}$.*

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.19. □

Lemma 4.18. *For all integers $1 \leq s < r$, $k \geq 2q(r-s)$ and $j \in \{0, 1, \ldots, m\}$, under typical event $E^j_{s,r}$, the k-deep block and k-deep prefix of every r-credible j-blockchain must be mined before round s.*

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.20. □

Theorem 4.19 (Blockchain growth theorem for voter and proposer blockchain under lockstep synchronous model)**.** *Let r, s, s_1, j be integers satisfying $1 \leq s_1 \leq s < r$ and $0 \leq j \leq m$. Then under typical event $E^j_{s,r}$, the height of an r-credible j-blockchain must be at least $(1 - \frac{\xi}{6})q(r - s_1)$ larger than the height of an s_1-credible j-blockchain.*

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Theorem 3.21. □

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 4.20 (Common prefix theorem for voter blockchain under lockstep synchronous model)**.** *Let r, s, k, j be integers satisfying $1 \leq s < r$, $k \geq 2q(r-s)$ and $j \in \{1, \ldots, m\}$. Then the k-deep prefix of any r-credible j-blockchain is permanent after round r under event $E^j_{s,r}$.*

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Theorem 3.23. □

Theorem 4.21 (Blockchain quality theorem for voter blockchain under lockstep synchronous model)**.** *Let r, s, k, j be integers satisfying $1 \leq s < r$, $k \geq 2q(r-s)$ and $j \in \{1, \ldots, m\}$. Suppose an r-credible j-blockchain has more than k blocks by round r. Under event $E^j_{s,r}$, by round r, at least $\frac{\xi}{2}$ fraction of the last k j-blocks of the j-blockchain are honest.*

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Theorem 3.22. □

Theorem 4.22 (Leader sequence growth theorem under lockstep synchronous model)**.** *Suppose integers s_1, s, r satisfy $1 \leq s_1 \leq s < r$. Under event $E^0_{s,r}$, the height of every r-credible leader sequence is at least $(1 - \frac{\xi}{6})(r - s_1)q$ larger than the maximum height of all s_1-credible leader sequences and all s_1-credible 0-blockchains. As a consequence, the probability that some r-credible leader sequence is less than $(1 - \frac{\xi}{6})(t - s_1)q$ higher than some s_1-credible leader sequence or some s_1-credible 0-blockchain does not exceed $5\eta^{-2}e^{-\eta(r-s)}$.*

Proof. Suppose proposer blocks $(0, b_1, \ldots, b_\ell)$ is an s_1-credible leader sequence, and proposer blocks $(0, d_1, \ldots, d_n)$ is an r-credible leader sequence. Then by Lemma 4.11,

0-blockchain b_ℓ is an s_1-credible and 0-blockchain d_n is r-credible. By Lemma 4.19, n is greater than ℓ by at least $\ell + (1 - \frac{\xi}{6})(r - s_1)q$ under event $E^0_{s,r}$. Thus the proof of Theorem 4.22. □

Theorem 4.23 (Leader sequence quality theorem under lockstep synchronous model)**.** *Let r, s, k be integers satisfying $1 \leq s < r$ and $k \geq 2q(r - s)$. Suppose an r-credible leader sequence has more than k blocks. Then under event $E^0_{s,r}$, at least $\frac{\xi}{2}k$ of the last k blocks of the r-credible leader sequence are honest. As a consequence, the probability that more than $(1 - \frac{\xi}{2})k$ of the last k blocks of some r-credible leader sequence are adversarial does not exceed $5\eta^{-2}e^{-\eta(r-s)}$.*

Proof. Suppose proposer blocks $(0, b_1, \ldots, b_n)$ is an r-credible leader sequence with $n \geq k$. Let h be the maximum height strictly less than $n - k + 1$ such that the earliest proposer block mined on height h is honest. We have $0 \leq h \leq n - k$. Denote the earliest proposer block on height h as block d, then we have $T^0_d = R_h < s$ by Lemma 4.18. Let

$$y = n - k - h. \tag{4.16}$$

Then y lower bounds the number of adversarial blocks on heights $\{h+1, \ldots, n-k\}$ because the earliest proposer blocks on these heights are adversarial by definition. Denote the number of adversarial blocks in proposer blocks $\{b_{n-k+1}, \ldots, b_n\}$ as z. Then $z + y$ lower bounds the number of adversarial proposer blocks generated during rounds $\{R_h+1, \ldots, r\}$. We have

$$z + y \leq Z^0_{R_h+1,r} \tag{4.17}$$

$$< (1 - \frac{\xi}{2}) X^0_{R_h+1,r} \tag{4.18}$$

where (4.18) is due to (4.12).

Note that proposer block d is honest by definition. Then 0-blockchain d is R_h-credible. According to Lemma 3.19, the minimum height of r-credible 0-blockchains is $h + X^0_{R_h,r}$, which lower bounds the height of all r-credible leader sequences by Lemma 4.11. Thus we have

$$n \geq h + X^0_{R_h,r}. \tag{4.19}$$

Thus, under event $E^0_{s,r}$, we have

$$\frac{z}{k} \leq \frac{z+y}{k+y} \tag{4.20}$$

$$= \frac{z+y}{n-h} \tag{4.21}$$

$$< \frac{(1 - \frac{\xi}{2}) X^0_{R_h,r}}{X^0_{R_h,r}} \tag{4.22}$$

$$= 1 - \frac{\xi}{2} \tag{4.23}$$

where (4.20) is due to $z \leq k$ and (4.22) is due to (4.18) and (4.19). □

Lemma 4.24. *Suppose positive integers s, r, and j satisfy $1 \leq s < r$ and $j \in \{0, 1, \ldots, m\}$. Let $\ell = (1 - \frac{\xi}{6})(r - s)q$. Suppose j-blockchain b is r-credible. Under event $E^j_{s,r}$, an honest j-block whose height is no less than $h^j(b) - \ell + 1$ must be mined after round s.*

Proof. Suppose honest j-block d satisfies $T_d^j \le s$. Since j-blockchain d is T_d^j-credible, the heights of all r-credible j-blockchains must be at least $h^j(d) + (1 - \frac{\xi}{6})(r-s)q$. Since j-blockchain b with height $h^j(b)$ is r-credible, we have

$$h^j(d) \le h^j(b) - (1 - \frac{\xi}{6})(r - T_d^j)q \tag{4.24}$$

$$\le h^j(b) - (1 - \frac{\xi}{6})(r-s)q \tag{4.25}$$

$$< h^j(b) - \ell + 1 \tag{4.26}$$

where (4.26) is by definition of ℓ. Thus, an honest j-block with height greater or equal to $h^j(b) - \ell + 1$ must be mined after round s. □

Theorem 4.25 (Leader sequence common prefix theorem under lockstep synchronous model)**.** *Suppose positive integers k, h, s, and r satisfy $k \ge 2q(r-s)$ and*

$$r \ge R_h + \frac{2k}{\xi(1 - \frac{\xi}{6})q}. \tag{4.27}$$

Let

$$G = \bigcap_{j \in \{1,\dots,m\}} E_{s,r}^j. \tag{4.28}$$

Then under event G, all r-credible leader sequences share the same h-high prefix, and the prefix is permanent after around r. As a consequence, with probability at least $1 - 5mn\eta^{-2}e^{-\eta(r-s)}$, the h-high prefix of all r-credible leader sequences is permanent after round r.

Proof. Consider an r-credible voter j-blockchain b.

For convenience, let $\ell = \lceil \frac{2k}{\xi} \rceil$. By $k \geq 2q(r-s)$ we know $s \geq r - \frac{k}{2q} > r - \frac{2k}{\xi(1-\frac{\xi}{6})} \geq R_h$. If event G occurs, event $E^j_{R_h,r}$ occurs. By Lemma 4.19, the height of j-blockchain b is higher than an R_h-credible j-blockchain by at least

$$(1 - \frac{\xi}{6})(r - R_h)q \geq \frac{2k}{\xi} \tag{4.29}$$

where (4.29) is due to (4.27). Then $h^j(b) \geq \ell$ because the height is an integer.

Obviously $\ell > k$. Thus $\ell > 2q(r-s)$. According to Lemma 4.21, under event $E^j_{s,r}$, in the last ℓ blocks of j-blockchain b, the number of honest ones is at least

$$\frac{\xi}{2}\ell \geq k. \tag{4.30}$$

Thus, the lowest of these j-blocks, denoted as j-block d, must be on the k-deep prefix of j-blockchain b. That is to say,

$$h^j(b) - \ell + 1 \leq h^j(d) \leq h^j(b) - k + 1. \tag{4.31}$$

By Lemma 4.24, j-block d must be mined after round R_h. By the voting rule, j-blockchain d must have voted on all heights less or equal to height h. Moreover, if event G occurs, event $E^j_{s,r}$ occurs. By Theorem 4.20, j-blockchain d and its votes (which are on the $(k-1)$-deep prefix of j-blockchain b) must be permanent after round r since.

Such claims can be said for all voter blockchains. That is to say, under event G, for all $j \in \{1, \ldots, m\}$ there exists a permanent honest j-blockchain which has voted on all heights less or equal to h. Thus, the h-high prefix of all r-credible leader sequences is permanent after round r.

According to Lemma 4.16,

$$P(G^c) = P\left(\bigcup_{j\in\{1,\ldots,m\}} \left(E^j_{s,r}\right)^c\right) \tag{4.32}$$

$$\leq mP\left((E^j_{s,r})^c\right) \tag{4.33}$$

$$< 5m\eta^{-2}e^{-\eta(r-s)}. \tag{4.34}$$

As a consequence, with probability at least $1 - 5m\eta^{-2}e^{-\eta(r-s)}$, the h-high prefix of r-credible leader sequences is permanent after time r. □

Corollary 4.26. *Fix positive integer h. For any $\epsilon \in (0,1)$, let*

$$r = R_h + \frac{2}{(1-\frac{\xi}{6})\xi q}\left(2q\left(\frac{1}{\eta}\log\frac{5m}{\epsilon\eta^2}+1\right)+1\right). \tag{4.35}$$

Then with probability at least $1-\epsilon$, the h-high prefix of an r-credible leader sequence is permanent after round r.

Proof. Let

$$k = \left\lceil 2q\left(\frac{1}{\eta}\log\frac{5m}{\epsilon\eta^2}+1\right)\right\rceil. \tag{4.36}$$

Obviously

$$r \geq R_h + \frac{2k}{(1-\frac{\xi}{6})\xi q} \tag{4.37}$$

is satisfied. Let

$$s = r - \left\lceil \frac{1}{\eta} \log \frac{5m}{\epsilon \eta^2} \right\rceil . \tag{4.38}$$

Then $k \geq 2q(r-s)$ is satisfied. Moreover,

$$5m\eta^{-2}e^{-\eta(r-s)} = 5m\eta^{-2}e^{-\eta\left\lceil \frac{1}{\eta} \log \frac{5m}{\epsilon\eta^2} \right\rceil} \tag{4.39}$$

$$\leq \epsilon. \tag{4.40}$$

Apply Theorem 4.25 with k and s given by (4.36) and (4.38), with probability at least $1-5\eta^{-2}e^{-\eta(r-s)} > 1-\epsilon$, the h-high prefix of an r-credible leader sequence is permanent. □

4.4. Non-lockstep synchronous model and analysis

In this model, we consider the non-lockstep synchronous model where 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.

Definition 4.27 (r-credible j-blockchain)**.** *For $j \in \{0, \ldots, m\}$, we say j-blockchain b is* r-credible *if it has been published by round r, and is no shorter than any blockchain published by round $r-T$. That is to say,*

$$P_b^j < r, \tag{4.41}$$

and

$$h^j(b) \geq h^j(b), \quad \forall k : P_k^j < r - T. \tag{4.42}$$

If there is no need to specify round r explicitly, j-blockchain b can also be simply called a credible blockchain.

Definition 4.28 (r-credible leader sequence under non-lockstep synchronous model)**.** *Let proposer block $b_1, \ldots, b_n$ be proposer blocks at heights $1, \ldots, n$, respectively, where n is greater or equal to the maximum height of all proposer blockchains published by round $r-T$. We say $(0, b_1, \ldots, b_n)$ is an r-credible leader sequence if it is elected by a collection of m r-credible voter blockchains including one j-blockchain for every $j \in \{1, \ldots, m\}$. That is, for every $\ell \in \{1, \ldots, n\}$, proposer block b_ℓ receives the most votes among all proposer blocks of height ℓ at round r from that collection of voter blockchains. In particular, we have $n \geq h$ if height h satisfies $R_h \leq r - T - 1$. Block b_ℓ is called an r-credible leader block. If there is no need to specify r explicitly, an r-credible leader sequence (block) can also be simply referred to as a credible leader sequence (block).*

Lemma 4.29. *If proposer blocks $(0, b_1, \ldots, b_n)$ is an r-credible leader sequence, then 0-blockchain b_n is an r-credible 0-blockchain.*

Proof. By definition, n is greater or equal to the maximum height of all proposer blockchains (0-blockchains) published by round $r-T$. Thus the proof of Lemma 4.29. □

Lemma 4.30. *If j-block b is honest, then j-blockchain f_b^j must be T_k^j credible.*

Proof. Lemma 4.30 is obvious since an honest j-block must also extend a credible j-blockchain under the non-lockstep synchronous model. □

Although an honest j-block always extends a credible j-blockchain, a credible j-blockchain may not end with an honest j-block. Moreover, an adversarial j-block may or may not extend a credible j-blockchain and may be published anytime after it is mined.

Suppose $j \in \{0, 1, \ldots, m\}$. A j-block is called a j-lagger if it is the single honest j-block mined during a round and no other honest block is mined in the previous $T-1$ rounds. Accordingly, we define the following indicators for $r = T, T+1, \ldots$:

$$V_r^j = \begin{cases} 1, & \text{if } H_r^j = 1 \text{ and} \\ & H_{r-1}^j = \ldots = H_{r-T+1}^j = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{4.43}$$

A j-block is said to be a j-loner if it is the only honest j-block during a round and no other honest j-block is mined within $T-1$ rounds before or after the round. Accordingly, we define the following indicators for $r = T, T+1, \ldots$:

$$W_r^j = \begin{cases} 1, & \text{if } H_r^j = 1, H_{r-1}^j = \cdots = H_{r-T+1}^j = 0, \\ & \text{and } H_{r+1}^j = \ldots = H_{r+T-1}^j = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{4.44}$$

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

$$q \leq \frac{\xi}{20T} \tag{4.45}$$

where ξ is defined in (3.2) and q is the probability that one or more honest blocks are mined during a round.

Definition 4.31. *For all integers $T \leq s < r$ and $j \in \{0, 1, \ldots, m\}$, define event*

$$F_{s,r} = F_{s,r}^1 \cap F_{s,r}^2 \cap F_{s,r}^3 \cap F_{s,r}^4 \tag{4.46}$$

where

$$F_{s,r}^1 = \left\{ (1 - \frac{\xi}{20})\mathbb{E}[V_{s,r}^j] < V_{s,r}^j \right\}, \tag{4.47}$$

$$F_{s,r}^2 = \left\{ X_{s,r}^j < (1 + \frac{\xi}{20})\mathbb{E}[X_{s,r}^j] \right\}, \tag{4.48}$$

$$F_{s,r}^3 = \left\{ (1 - \frac{\xi}{20})\mathbb{E}[W_{s,r}^j] < W_{s,r}^j \right\}, \tag{4.49}$$

$$F_{s,r}^4 = \left\{ Z_{s,r}^j < \mathbb{E}[Z_{s,r}^j] + \frac{\xi}{20}\mathbb{E}[V_{s,r}^j] \right\}. \tag{4.50}$$

We note that for integers $j \in \{0, 1, \ldots, m\}$ and $r \geq 1$, X_r^j, V_r^j, W_r^j, and Z_r^j here are identically distributed as X_r, V_r, W_r, and Z_r defined in Section 3.4. Also, for $1 \leq s < r$, $F_{s,r}^j$ is defined in the same manner as $F_{s,r}$. Thus, the proposer blockchain and all voter blockchains satisfy similar properties as in Lemma 3.34 and Lemma 3.35:

Lemma 4.32. *For all integers $T \leq s < r$ and $j \in \{0, 1, \ldots, m\}$,*

$$P(F_{s,r}^j) > 1 - 4e^{-\mu(r-s)}, \tag{4.51}$$

where μ is given in (3.124).

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.34. □

Lemma 4.33. *For all integers $T \leq s < r - \frac{2}{q}$, the following inequalities hold under event $F_{s,r}$:*

$$(1 - \frac{\xi}{20})q(1-q)^T(r-s) < V_{s,r}^j \tag{4.52}$$

$$X_{s,r}^j < (1 + \frac{\xi}{20})q(r-s) \tag{4.53}$$

$$(1 - \frac{\xi}{3})q(r-s) < W_{s,r}^j \tag{4.54}$$

$$Z_{s,r}^j < (1 - \frac{2\xi}{3})q(r-s). \tag{4.55}$$

The following inequalities hold under event $F_{s+T,r-T}$:

$$Z_{s,r}^j < (1 - \frac{\xi}{2})V_{s+T,r-T}^j \tag{4.56}$$

$$Z_{s,r}^j < W_{s+T,r-T}^j. \tag{4.57}$$

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.35. □

Definition 4.34. *For all integers $T \leq s < r - \frac{2}{q}$ and $j \in \{0, 1, \ldots, m\}$, define typical event*

$$G^j_{s,r} = \bigcap_{0 \leq a \leq s-T, b \geq 0} F^j_{s-a,r+b}. \tag{4.58}$$

$G^j_{s,r}$ occurs when events $F^j_{k,\ell}$ simultaneously occurs for all k, ℓ, i.e., the "F" event occur over all consecutive rounds containing $\{s, \ldots, r\}$.

Lemma 4.35. *For all integers $T \leq s < r - \frac{2}{q}$ and $j \in \{0, 1, \ldots, m\}$,*

$$P(G^j_{s,r}) > 1 - 5\mu^{-2}e^{-\mu(r-s)}. \tag{4.59}$$

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.37. □

Since the proposer blockchain and all voter blockchains follows essentially the same rules as a Bitcoin blockchain, the following lemmas remain valid:

Lemma 4.36. *For $j \in \{0, 1, \ldots, m\}$, j-laggers have different heights.*

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.39. □

Lemma 4.37. *A j-loner is the only honest j-block at its height.*

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.41. □

Lemma 4.38. *For all integers $T \leq s < r - \frac{2}{q}$, $k \geq 2q(r-s)$, and $0 \leq j \leq m$, under typical event $G^j_{s,r}$, the k-deep block and k-deep prefix of every r-credible j-blockchain must be mined before round s.*

Proof. For $j = 0, 1, \ldots, m$, the lemma admits essentially the same proof as that for Lemma 3.42. □

Theorem 4.39. *Let r, s, s_1, j be integers satisfying $T \leq s_1 \leq s < r - \frac{2}{q}$ and $j \in \{0, 1, \ldots, m\}$. Under typical event $G^j_{s+T,r-T}$, the height of every r-credible j-blockchain must be at least $(1 - \frac{\xi}{10})(1-q)^T(r-s_1)q$ more than the maximum height of all s_1-credible j-blockchains.*

Proof. For $j = 0, 1, \ldots, m$, the theorem admits essentially the same proof as that for Lemma 3.43. □

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 4.40. *Let r, s, k, j be integers satisfying $T \leq s < r - \frac{2}{q}$, $k \geq 2(r-s)q$ and $j \in \{1, \ldots, m\}$. Suppose an r-credible j-blockchain has more than k blocks, then under event $G^j_{s,r-T}$, at least $\frac{\xi}{2}k$ of the last k blocks of this j-blockchain are honest.*

Proof. For $j = 1, \ldots, m$, the theorem admits essentially the same proof as that for Lemma 3.44. □

Theorem 4.41. *Let r, s, k, j be integers satisfying $T \leq s < r - \frac{2}{q}$, $k > 2(r-s)q$, and $j \in \{1, \ldots, m\}$. If an r-credible j-blockchain has a k-deep prefix, then the prefix is permanent after round r under $G^j_{s+T,r-T}$.*

Proof. For $j = 1, \ldots, m$, the theorem admits essentially the same proof as that for Lemma 3.45. □

Theorem 4.42 (Leader sequence growth theorem under non-lockstep synchronous model)**.** *Suppose integers s_1, s, r satisfy $T \leq s_1 \leq s < r - \frac{2}{q}$. Under event $G^0_{s,r-T}$, the height of every r-credible leader sequence is at least $(1-\frac{\xi}{10})(1-q)^T(r-s_1)q$ larger than the maximum height of all s_1-credible leader sequences and all s_1-credible 0-blockchains. As a consequence, the probability that some r-credible leader sequence is less than $(1-\frac{\xi}{10})(1-q)^T(r-s_1)q$ higher than some s_1-credible leader sequence or some s_1-credible 0-blockchain does not exceed $5\mu^{-2}e^{-\mu(r-s-T)}$.*

Proof. Suppose proposer blocks $(0, b_1, \ldots, b_\ell)$ is an s_1-credible leader sequence, and proposer blocks $(0, d_1, \ldots, d_n)$ is an r-credible leader sequence. Then by Lemma 4.29, 0-blockchain b_ℓ is an s_1-credible and 0-blockchain d_n is r-credible. By Lemma 4.39, n is greater than ℓ by at least $\ell + (1-\frac{\xi}{6})(r-s_1)q$ under event $G^0_{s,r-T}$. Thus the proof of Theorem 4.22. □

Theorem 4.43 (Leader sequence quality theorem under non-lockstep synchronous model)**.** *Let r, s, k be integers satisfying $T \leq s < r - \frac{2}{q}$ and $k \geq 2q(r-s)$. Suppose an r-credible leader sequence has more than k blocks. Then under event $G^0_{s+T,r-T}$, at least $\frac{\xi}{2}k$ of the last k blocks of the r-credible leader sequence are honest. As a consequence, the*

probability that more than $(1-\frac{\xi}{2})k$ *of the last* k *blocks of some* r*-credible leader sequence are adversarial does not exceed* $5\mu^{-2}e^{-\mu(r-s-2T)}$.

Proof. Suppose proposer blocks $(0, b_1, \ldots, b_n)$ is an r-credible leader sequence with $n \geq k$. Let h be the maximum height strictly less than $n-k+1$ such that the earliest proposer block mined on height h is honest. We have $0 \leq h \leq n-k$. Denote the earliest proposer block on height h as block d, then we have $T_d^0 = R_h < s$ by Lemma 4.38. 4.18. Let

$$y = n - k - h. \tag{4.60}$$

Then y lower bounds the number of adversarial blocks on heights $\{h+1, \ldots, n-k\}$ because the earliest proposer blocks on these heights are adversarial by definition. Denote the number of adversarial blocks in proposer blocks $\{b_{n-k+1}, \ldots, b_n\}$ as z. Then $z+y$ lower bounds the number of adversarial proposer blocks generated during rounds $\{R_h+1, \ldots, r\}$. We have

$$\begin{aligned} z + y &\leq Z^0_{R_h, r} && (4.61) \\ &< (1-\frac{\xi}{2}) V^0_{R_h+T, r-T} && (4.62) \end{aligned}$$

where (4.62) is due to (4.12).

Note that since proposer block d is mined during round R_h, then the height of an (R_h+T)-credible blockchain is at least h. According to Lemma 3.19, the minimum height of r-credible 0-blockchains is $h+V^0_{R_h+T, r-T}$, which lower bounds the height of all r-credible

leader sequences by Lemma 4.29. Thus we have

$$n \geq h + V^0_{R_h,r}. \tag{4.63}$$

Thus, under event $G^0_{s+T,r-T}$, we have

$$\begin{aligned}
\frac{z}{k} &\leq \frac{z+y}{k+y} && (4.64)\\
&= \frac{z+y}{n-h} && (4.65)\\
&< \frac{(1-\frac{\xi}{2})V^0_{R_h+T,r-T}}{V^0_{R_h+T,r-T}} && (4.66)\\
&= 1-\frac{\xi}{2} && (4.67)
\end{aligned}$$

where (4.64) is due to $z \leq k$ and (4.66) is due to (4.62) and (4.63). □

Lemma 4.44. *Suppose positive integers s, r, and j satisfy $T \leq s < r - \frac{2}{q}$ and $j \in \{0, 1, \ldots, m\}$. Let $\ell = (1-\frac{\xi}{10})(1-q)^T(r-s)q$. Suppose j-blockchain b is r-credible. Under event $G^j_{s,r}$, an honest j-block whose height is no less than $h^j(b) - \ell + 1$ must be mined after round s.*

Proof. Suppose honest j-block d satisfies $T^j_d \leq s$. Since j-blockchain d is T^j_d-credible, the heights of all r-credible j-blockchains must be at least $h^j(d) + (1-\frac{\xi}{10})(1-q)^T(r-s)q$. Since j-blockchain b with height $h^j(b)$ is r-credible, we have

$$\begin{aligned}
h^j(d) &\leq h^j(b) - (1-\frac{\xi}{10})(1-q)^T(r-T^j_d)q && (4.68)\\
&\leq h^j(b) - (1-\frac{\xi}{10})(1-q)^T(r-s)q && (4.69)
\end{aligned}$$

$$< h^j(b) - \ell + 1 \tag{4.70}$$

where (4.70) is by definition of ℓ. Thus, an honest j-block with height greater or equal to $h^j(b) - \ell + 1$ must be mined after round s. □

Theorem 4.45 (Leader sequence common prefix theorem under non-lockstep synchronous model)**.** *Suppose positive integers k, h, s, and r satisfy $k \geq 2q(r-s)$ and*

$$r \geq R_h + \frac{2k}{(1-\frac{\xi}{10})(1-q)^T q\xi}. \tag{4.71}$$

Let

$$G = \bigcap_{j\in\{1,\ldots,m\}} G^j_{s+T,r-T}. \tag{4.72}$$

Then under event G, all r-credible leader sequences share the same h-high prefix, and the prefix is permanent after around r. As a consequence, with probability at least $1 - 5m\mu^{-2}e^{-\mu(r-s-2T)}$, the h-high prefix of all r-credible leader sequences is permanent after round r.

Proof. Consider an r-credible voter j-blockchain b.

For convenience, let $\ell = \lceil \frac{2k}{\xi} \rceil$. By $k \geq 2q(r-s)$ we know $s \geq r - \frac{k}{2q} > R_h$. If event G occurs, event $G^j_{R_h,r-T}$ occurs. By Lemma 4.39, the height of j-blockchain b is higher than an R_h-credible j-blockchain by at least

$$(1-\frac{\xi}{10})(1-q)^T(r-R_h)q \geq \frac{2k}{\xi} \tag{4.73}$$

where (4.73) is due to (4.71). Then $h^j(b) \geq \ell$ because the height is an integer.

Obviously $\ell > k$. Thus $\ell > 2q(r-s)$. According to Lemma 4.40, under event $G^j_{s+T,r-T}$, in the last ℓ blocks of j-blockchain b, the number of honest ones is at least

$$\frac{\xi}{2}\ell \geq k. \tag{4.74}$$

Thus, the lowest of these j-blocks, denoted as j-block d, must be on the k-deep prefix of j-blockchain b. That is to say,

$$h^j(b) - \ell + 1 \leq h^j(d) \leq h^j(b) - k + 1. \tag{4.75}$$

By Lemma 4.44, j-block d must be mined after round R_h. By the voting rule, j-blockchain d must have voted on all heights less or equal to height h. Moreover, if event G occurs, event $G^j_{s+T,r-T}$ occurs. By Theorem 4.41, j-blockchain d and its votes (which are on the $(k-1)$-deep prefix of j-blockchain b) must be permanent after round r since.

Such claims can be said for all voter blockchains. That is to say, under event G, for all $j \in \{1, \ldots, m\}$ there exists a permanent honest j-blockchain which has voted on all heights less or equal to h. Thus, the h-high prefix of all r-credible leader sequences is permanent after round r.

According to Lemma 4.34,

$$P(G^c) = P\left(\bigcup_{j\in\{1,\ldots,m\}} \left(G^j_{s+T,r-T}\right)^c\right) \tag{4.76}$$

$$\leq mP\left((G^j_{s+T,r-T})^c\right) \tag{4.77}$$

$$< 5m\mu^{-2}e^{-\mu(r-s-2T)}. \tag{4.78}$$

As a consequence, with probability at least $1 - 5m\mu^{-2}e^{-\mu(r-s-2T)}$, the h-high prefix of r-credible leader sequences is permanent after time r. □

Corollary 4.46. *Fix positive integer h. For any $\epsilon \in (0,1)$, let*

$$r = R_h + \frac{2}{(1-\frac{\xi}{10})(1-q)^T \xi q}\left(2q\left(\frac{1}{\mu}\log\frac{5m}{\epsilon\mu^2} + 1 + 2T\right) + 1\right). \tag{4.79}$$

Then with probability at least $1-\epsilon$, the h-high prefix of an r-credible leader sequence is permanent after round r.

Proof. Let

$$k = \left\lceil 2q\left(\frac{1}{\mu}\log\frac{5m}{\epsilon\mu^2} + 1 + 2T\right)\right\rceil. \tag{4.80}$$

Obviously

$$r \geq R_h + \frac{2k}{\xi(1-\frac{\xi}{10})(1-q)^T q} \tag{4.81}$$

is satisfied. Let

$$s = r - \left\lceil \frac{1}{\mu}\log\frac{5m}{\epsilon\mu^2}\right\rceil - 2T. \tag{4.82}$$

Then $k \geq 2q(r-s)$ is satisfied. Moreover,

$$5m\eta^{-2}e^{-\mu(r-s-2T)} = 5m\eta^{-2}e^{-\eta\left\lceil\frac{1}{\eta}\log\frac{5m}{\epsilon\eta^2}\right\rceil} \tag{4.83}$$

$$\leq \epsilon. \tag{4.84}$$

Apply Theorem 4.25 with k and s given by (4.36) and (4.82), with probability at least $1 - 5\mu^{-2}e^{-\mu(r-s-2T)} > 1 - \epsilon$, the h-high prefix of an r-credible leader sequence is permanent. □

So far, we have shown that in the Prism blockchains, the leader sequence is permanent with high probability after sufficient amount of wait time. To be more specific, 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 $\log \frac{1}{\epsilon}$.

CHAPTER 5

Continuous-time Analysis of the Bitcoin Backbone Protocol

5.1. Introduction

While the Nakamoto consensus protocol is simple and elegant, a rigorous analysis for the latency–security trade-off is very challenging. As mentioned in Chapter 3, the original Bitcoin white paper [**1**] only analyzed a single specific attack, called *private mining attack*, which is to mine an adversarial fork in private. Nakamoto showed that the probability the adversary's private fork overtakes the main blockchain vanishes exponentially with the latency.

It is not until six years later that Garay et al. [**4**] provided the first proof that the Nakamoto consensus is secure against all possible attacks. One major limitation of [**4**] is that their round-based lock-step synchrony model essentially abstracts away block propagation delays. Several follow-up works [**6**, **7**, **9**, **11**] have extended the analysis to the Δ-synchrony model in which the rounds in which different honest miners observe the same block may differ by up to a known upper bound Δ.

So far, existing analyses against all possible attacks [**4**, **6**–**9**, **11**] (including a few concurrent and follow-up works [**12**–**15**]) focus on establishing asymptotic bounds using the big $O(\cdot)$ or big $\Omega(\cdot)$ notation. If one works out the constants in these asymptotic results, the latency upper bounds will be several orders of magnitude higher than the best known lower bounds [**16**, **17**]. Thus, despite their theoretical value, existing analyses of

the Nakamoto consensus provide little guidance on the actual confirmation time, security guarantees, or parameter selection in practice.

In this chapter, we explicitly and closely characterize the trade-off between latency and security for Nakamoto-style proof-of-work consensus protocols. The latency results we prove are within a few hours to simple lower bounds due to the private attack. The gap remains relatively constant at different security levels, and is hence insignificant for high security levels but can be significant at low security levels. For example, with a 10% adversary mining power, a mining rate of one block every 10 minutes, and a maximum block propagation delay of 10 seconds, a block in the Nakamoto consensus is secured with 10^{-3} error probability after 5 hours 20 minutes, or with 10^{-10} error probability after 12 hours 15 minutes. As a reference, due to the private attack, one must wait for at least 1 hour 30 minutes or 8 hours 5 minutes before confirming for 10^{-3} and 10^{-10} security levels, respectively.

Since Bitcoin's rise to fame, numerous altcoins and Bitcoin hard forks have adopted the Nakamoto consensus protocol with very different parameters. Those parameters are mostly determined in an ad-hoc or empirical manner. This chapter provides theoretical and quantitative tools to reason about the effects and trade-offs of these parameters on different metrics in the Nakamoto consensus including confirmation time, throughput, and fault tolerance. We use these new tools to analyze and compare various altcoins and offer new insights and recommendations for setting parameters.

Some new techniques developed in this chapter may be of independent interests. Assuming all block propagation delays are under Δ units of time, we show the arrivals of several species of honest blocks form renewal processes. That is, the inter-arrival times

of such a process are i.i.d. We show that the adversary must match the so-called double-laggers in order to succeed in any attack. We derive the moment generating functions of the inter-arrival times. This allows us to calculate quite accurately the probability that more double-laggers are mined than adversarial blocks in any time interval, which leads to a close latency–security trade-off.

We note that several existing proofs in the literature are flawed. A recurrent subtle mistake is to presume memorylessness of the mining process over a time interval defined according to some miners' views and actions. The boundaries of such an interval are in fact complicated *stopping times*. In general, when conditioned on a stopping time, the mining processes are no longer distributed as the original ones without conditioning. In this chapter, we carefully circumvent this issue to develop a fully rigorous analysis.

Specifically, we provide an explicit formula for the security guarantee as a function of the latency. This is equivalent to an upper bound on the latency that guarantees any desired security level. By means of numerical analysis, the latency upper bound is shown to be close to a lower bound due to the private attack. We also quantify how the block propagation delay bound, mining rates, and other parameters affect the latency–security trade-off. At last, we analyze and compare the performance and security of several prominent proof-of-work longest-chain protocols.

Main results of this chapter are reported in [**37**]

5.2. Continuous-time model

Throughout this thesis, "by time t" means "during $(0, t]$".

Definition 5.1 (A miner's view)**.** *A miner's view at time t is a subset of all blocks mined by time t. A miner's view can only increase over time. A block is in its own miner's view from the time it is mined.*

Definition 5.2 (A miner's longest blockchain)**.** *A blockchain is in a miner's view at time t if all blocks of the blockchain are in the miner's view at time t. A miner's longest blockchain at time t is a blockchain with the maximum height in the miner's view at time t. Ties are broken in an arbitrary manner.*[1]

Definition 5.3 (Honest and adversarial miners)**.** *Each miner is either honest or adversarial. A block is said to be honest (resp. adversarial) if it is mined by an honest (resp. adversarial) miner. An honest block mined at time t must extend its miner's longest blockchain immediately before t.*

Definition 5.4 (Publication)**.** *A block is said to be published by time t if it is included in at least one honest miner's view by time t. A blockchain is said to be published by time t if all of its blocks are published by time t.*

We let T_b denote the time when block b is mined. By Definition 5.2 and 5.3, an honest block b is published from time T_b.

We assume all block propagation delays are upper bounded by Δ units of time in the following sense:

Definition 5.5 (Block propagation delay bound Δ)**.** *If a block is in any honest miner's view by time t, then it is in all miners' views by time $t + \Delta$.*

[1]The Bitcoin protocol favors the earliest to enter the view.

The adversary is allowed to use arbitrary strategy subject to the preceding constraints. Specifically, an adversary can choose to extend any existing blockchain. Once an adversarial block is mined, its miner can determine when it enters each individual honest miner's view subject to the delay bound Δ (Definition 5.5).

This treatment cannot be fully rigorous without a well-defined probability space. At first it appears to be intricate to fully described blockchains and its probability space. One option (adopted in **[14]**) is to define blockchains as branches of a random tree that depend on the adversary's strategies as well as the network topology and delays. Other authors include in their probability space the random hashing outcomes, which also depend on the adversary strategies. For our purposes it turns out to be sufficient (and most convenient) to include no more than the mining times of the honest and adversarial blocks in the probability space. Under a typical event in this probability space, blockchain consistency is guaranteed under all adversarial strategies and network schedules (under Δ-synchrony). Thus, the adversary's strategies and the network schedules do not have to be included in the probability space.

Definition 5.6 (Mining processes)**.** *Let H_t (resp. A_t) denote the total number of honest (resp. adversarial) blocks mined during $(0, t]$. We assume $(H_t, t \geq 0)$ and $(A_t, t \geq 0)$ to be independent homogeneous Poisson point processes with rate α and β, respectively. The total mining rate of honest (resp. adversarial) miners is thus α (resp. β) blocks per unit of time.*

Note that the adversary can in principle regulate their mining effort at will (i.e., mine at reduced rates). But such strategies can be modeled as discarding selected adversarial blocks. Hence, Definition 5.6 is without loss of generality.

In lieu of specifying the number of honest and adversarial miners, the proposed model only defines their respective aggregate mining rates (they remain constant in time). This is in the same spirit as the permissionless nature of the Nakamoto consensus.

5.3. Proof of consistency

The proof of consistency is done in two main steps: First, we identify a typical event, which is a sufficient condition for a block to be *permanent* (or irreversible) once confirmed. That is, the block will be included in all honest miners' local longest blockchains infinitely into the future. Second, we upper bound the probability that the typical event does not occur. Combining the two yields an upper bound on the probability of consistency violation.

In slightly more detail, the typical event involves a special type of honest blocks called *loners*. A loner is an honest block that is not mined within Δ units of time of other honest blocks. Let b be a block mined at time s and included in some honest miner's longest blockchain at time $s + t$. We then prove that, if for all $a \leq s$ and $b \geq s + t$, more loners than adversarial blocks are mined in the time interval $(a, b]$ (this is the typical event), then block b is permanent. After that, we upper bound the probability that the typical event does not occur. The probability of distribution of loners is difficult to analyze. We define another specie of honest blocks called *double-laggers*. Double laggers have one-to-one correspondence with loners but are easier to analyze since they can be shown to

form a renewal process. We derive the moment generating function of double-laggers' inter-arrival times. This allows to tightly bound the probability of the typical event.

For convenience and better intuition, we specifically choose the time unit to be equal to the block propagation delay bound in this proof. Hence Δ units of time becomes one (new) unit of time here. This obviously normalizes the block propagation delay bound to 1 under the new unit. Consequently, the mining rate, aka the expected number of blocks mined *per new unit of time*, is equal to the expected number of blocks mined per maximum delay. With slight abuse of notion, we still use α and β as the mining rates under the new time unit. At the end of the analysis we will recover Δ to arbitrary time unit.

Definition 5.7 (t-credibility)**.** *A blockchain is said to be* t-credible *if it is published by time* t *and its height is no less than the height of any blockchain published by time* $t-1$*. If there is no need to specify* t *explicitly, the blockchain is simply said to be credible (in context).*

Once a block is published, it takes no more than 1 unit of time to propagate to all miners. Hence at time t, an honest miner must have seen all blockchains published by $t-1$. It follows that every honest miner's longest blockchain must be t-credible. As we shall see, it is unnecessary to keep tabs of individual miner's views as far as the fundamental security is concerned. Focusing on credible blockchains allows us to develop a simple rigorous proof with minimal notation.

There can be multiple t-credible blockchains, which may or may not be of the same height.

Definition 5.8 (Lagger)**.** *An honest block mined at time t is called a* lagger *if it is the only honest block mined during $[t-1, t]$. By convention, the genesis block is honest and is regarded as the 0-th lagger.*

Definition 5.9 (Loner)**.** *An honest block mined at time t is called a* loner *if it is the only honest block mined during $[t-1, t+1]$.*

Lemma 5.10. *A loner is the only honest block at its height.*

Proof. Suppose block b mined at time t is a loner. By definition, no other honest block is mined during $[t-1, t+1]$. By Definitions 5.1 and 5.5, block b is in all honest miners' views by time $t+1$. Thus, all honest blocks mined after $t+1$ must have heights at least $h(b)+1$. Similarly, if an honest block is mined before $t-1$, its height must be smaller than $h(b)$; otherwise, block b's height would be at least $h(b)+1$. Hence, no other honest block is at the same height as block b. □

Suppose $0 \leq s < t$. Let $H_{s,t} = H_t - H_s$ denote the total number of honest blocks mined during time interval $(s, t]$. Let $X_{s,t}$ denote the total number of laggers mined during $(s, t]$. Let $Y_{s,t}$ denote the total number of loners mined during $(s, t]$. Let $A_{s,t}$ denote the total number of adversarial blocks mined during $(s, t]$. By convention, $H_{s,t} = X_{s,t} = Y_{s,t} = A_{s,t} = 0$ for all $s \geq t$. Table 5.1 illustrates frequently used notations.

Although symbols like H, X, Y are reused in Chapter 3, they can be easily distinguished because their footnote are defined to be integers in the previous Chapter.

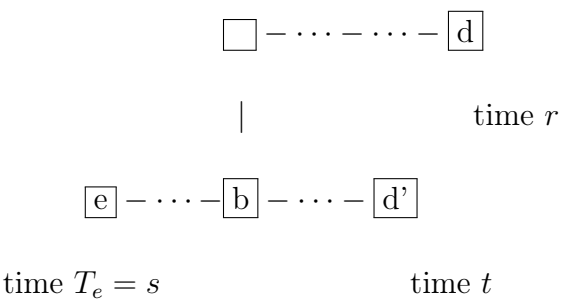
α	collective honest mining rate
β	collective adversarial mining rate
Δ	upper bound on network delay
f_b	the block number of block b's parent
T_b	the time block b is mined
$A_{s,t}$	total number of adversarial blocks mined during time $(s,t]$
$H_{s,t}$	total number of honest blocks mined during time interval $(s,t]$
$X_{s,t}$	total number of laggers mined during time interval $(s,t]$
$Y_{s,t}$	total number of loners mined during time interval $(s,t]$

Table 5.1. Notations

Lemma 5.11. *Suppose $t \leq r$. Let s denote the mining time of the highest honest block shared by a t-credible blockchain and an r-credible blockchain. Then*

$$Y_{s+1,t-1} \leq A_{s,r}. \tag{5.1}$$

Proof. Let block e denote the highest honest block shared by r-credible blockchain d and t-credible blockchain d' with $T_e = s$. Let block b denote the highest block shared by blockchains d and d'. Blocks b and e may or may not be the same block. The relationship between these blocks is illustrated as follows:



(5.2)

If $t - s \leq 2$ or no loner is mined during $(s+1, t-1]$, obviously $Y_{s+1,t-1} = 0 \leq A_{s,r}$. Otherwise, consider loner c mined during $(s+1, t-1]$. We next show that c can be paired with an adversary block mined during $(s, r]$.

Since blockchain e is s-credible and block c is mined after time $s+1$, we have $h(c) \geq h(e)$. Since blockchain d is r-credible and blockchain d' is t-credible, we have $h(c) \leq \min\{h(d), h(d')\}$. Consider the following two only possible cases:

(1) If $h(e) < h(c) \leq h(b)$, there exists at least one adversarial block at height $h(c)$ because all blocks between block e (exclusive) and block b (inclusive) are adversarial by definition.

(2) If $h(b) < h(c) \leq \min\{h(d), h(d')\}$, there is at least one adversarial block at height $h(c)$, because two diverging blockchains exist but loner c is the only honest block at its height by Lemma 5.10.

Thus, for every loner mined during $(s+1, t-1]$, at least one adversarial block must be mined during $(s, r]$ at the same height. In particular, the adversarial block must be mined before r because it is published by r. Hence (5.1) must hold. □

We now define some "typical events" alluded to at the beginning of this section.

Definition 5.12. *For all $s, t \geq 0$ and $\epsilon \in (0,1)$, let*

$$F^{\epsilon}_{s,t} = \bigcap_{a \in [0,s], b \in [t,\infty)} \{Y_{a+1,b-1-\epsilon} > A_{a,b}\} \tag{5.3}$$

We fix arbitrary $\epsilon \in (0,1)$ for now. We will send $\epsilon \to 0$ later.

Lemma 5.13. *Suppose block b is mined by time s and is included in a t-credible blockchain. Then, under event $F^{\epsilon}_{s,t}$, block b is included in all r-credible blockchains for all $r \geq t$.*

Proof. We first establish the result for $r \in [t, t+\epsilon]$ and then prove the lemma by induction.

Fix arbitrary $r \in [t, t+\epsilon]$. Let block e denote the highest honest block shared by an r-credible blockchain and a t-credible blockchain that includes block b. We have

$$Y_{T_e+1,r-1-\epsilon} \leq Y_{T_e+1,t-1} \tag{5.4}$$

$$\leq A_{T_e,r} \tag{5.5}$$

where (5.5) is due to Lemma 5.11. Under $F^{\epsilon}_{s,t}$,

$$Y_{a+1,r-1-\epsilon} > A_{s,r} \tag{5.6}$$

holds for all $a \in [0, s]$. Hence for (5.5) to hold, we must have $T_e > s$. Since $s \geq T_b$ by assumption, block b must be included in blockchain e, which implies that block b must also be included in the r-credible blockchain.

Suppose the lemma holds for $r \in [t, t+n\epsilon]$ for some positive integer n. We show the lemma also holds for $r \in [r, t+(n+1)\epsilon]$ as follows: Let $t' = t + n\epsilon$. Because $F^{\epsilon}_{s,t'}$ occurs under $F^{\epsilon}_{s,t}$ and that block b is included in a t'-credible blockchain, a repetition of the $r \in [t, t+\epsilon]$ case with t replaced by t' implies that block b is included in all r-credible blockchains with $r \in [t', t'+\epsilon]$. Hence lemma holds also for $r \in [t, t+(n+1)\epsilon]$.

The lemma is then established by induction on n. □

Lemma 5.13 guarantees that a block with some confirmation time is permanent/irreversible under the typical event $F^{\epsilon}_{s,t}$. It remains to lower bound the probability of $F^{\epsilon}_{s,t}$ as a function of the confirmation time $t - s$.

We then derive the moment generating functions (MGF) of several types of inter-arrival times. These will be useful in the analysis of $P\left(F_{s,t}^{\epsilon}\right)$.

Lemma 5.14. *Let W be an exponential random variable with mean $1/\alpha$. Let the MGF of W conditioned on $W \leq 1$ be denoted as $\Phi_0(u)$. Then*

$$\Phi_0(u) = \begin{cases} \frac{\alpha(1-e^{u-\alpha})}{(1-e^{-\alpha})(\alpha-u)} & \text{if } u \neq \alpha \\ \frac{\alpha}{1-e^{-\alpha}} & \text{if } u = \alpha. \end{cases} \tag{5.7}$$

Proof. The probability density function (pdf) of W conditioned on $W \leq 1$ is simply

$$\frac{\alpha}{1-e^{-\alpha}} e^{-\alpha w} 1_{\{0<w<1\}} \tag{5.8}$$

where $1_{\{\cdot\}}$ represents the indicator function which takes the values of 1 or 0 depending on whether the condition in the braces holds or not. The conditional MGF is thus

$$\Phi_0(u) = \mathbb{E}\left[e^{uW} | W \leq 1\right] \tag{5.9}$$

$$= \int_0^1 \frac{\alpha}{1-e^{-\alpha}} e^{-\alpha w} e^{uw} \mathrm{d}w \tag{5.10}$$

which becomes (5.7). □

Lemma 5.15. *Let W be an exponential random variable with mean $1/\alpha$. Let the MGF of W conditioned on $W > 1$ be denoted as $\Phi_1(u)$. Then*

$$\Phi_1(u) = \frac{\alpha e^u}{\alpha - u} \tag{5.11}$$

where the region of convergence is $u \in (-\infty, \alpha)$.

Proof. Conditioned on $W > 1$, the pdf of W is given by

$$e^{\alpha(-w+1)} 1_{\{w>1\}}. \tag{5.12}$$

The conditional MGF is thus:

$$\Phi_1(u) = \mathbb{E}\left[e^{uW} | W > 1\right] \tag{5.13}$$

$$= \int_1^{+\infty} e^{\alpha(-w+1)} e^{uw} \mathrm{d}w. \tag{5.14}$$

The integral converges if and only if $u < \alpha$, where the result is given by (5.11). □

Recall the genesis block is the 0-th lagger. For $i = 1, 2, \ldots$, let X_i denote the time elapsed between the mining times of the $(i-1)$-st and the i-th lagger. Let K_i denote the number of honest blocks mined between the $(i-1)$-st lagger (excluded) and the i-th lagger (included).

Lemma 5.16. *$(X_1, K_1), (X_2, K_2), \ldots$ are i.i.d.*

Proof. For convenience, for $n = 1, 2, \ldots$, let

$$L_n = K_1 + \cdots + K_n, \tag{5.15}$$

$$l_n = k_1 + \cdots + l_n. \tag{5.16}$$

It is easy to see that

$$X_i = W_{L_{i-1}+1} + \cdots + W_{L_i} \tag{5.17}$$

holds for $i = 1, 2, \ldots$. Also, the event that $K_i = k_i$ is equivalent to the event that

$$W_{L_{i-1}+1} \leq 1, \ldots, W_{L_{i-1}+k_i-1} \leq 1, W_{L_{i-1}+k_i} > 1. \tag{5.18}$$

Given $K_1 = k_1, \ldots, K_i = k_i$, the event $X_i \leq x$ is equivalent to the event that

$$W_{l_{i-1}+1} + \cdots + W_{l_i} \leq x. \tag{5.19}$$

For all positive integers $n, k_1, k_2, \ldots, k_n$ and real numbers $x_1, x_2, \ldots, x_n$, we have

$$\begin{aligned}
&P(X_1 \leq x_1, K_1 = k_1, \ldots, X_n \leq x_n, K_n = k_n) \\
&\quad = P(W_1 + \cdots + W_{l_1} \leq x_1, W_1 \leq 1, \ldots, W_{l_1-1} \leq 1, W_{l_1} > 1, && (5.20) \\
&\qquad \cdots, \\
&\qquad W_{l_{n-1}+1} + \cdots + W_{l_n} \leq x_n, W_{l_{n-1}+1} \leq 1, \ldots, W_{l_n-1} \leq 1, dW_{l_n} > 1) && (5.21) \\
&\quad = P(W_1 + \cdots + W_{k_1} \leq x_1, W_1 \leq 1, \ldots, W_{k_1-1} \leq 1, W_{k_1} > 1) \\
&\qquad \times \cdots \\
&\qquad \times P(W_{l_{n-1}+1} + \cdots + W_{l_n} \leq x_n, W_{l_{n-1}+1} \leq 1, \ldots, W_{l_n-1} \leq 1, W_{l_n} > 1) && (5.22)
\end{aligned}$$

which is a product of n probabilities, where (5.22) is because $W_1, W_2, \ldots$ are i.i.d. Moreover, the i-th probability on the right hand side of (5.22) can be reduced as follows:

$$\begin{aligned}
&P(W_{l_{i-1}+1} + \cdots + W_{l_i} \leq x, W_{l_{i-1}+1} \leq 1, \ldots, W_{l_i-1} \leq 1, W_{l_i} > 1) \\
&\quad = P(W_1 + \cdots + W_{k_i} \leq x, W_1 \leq 1, \ldots, W_{k_i-1} \leq 1, W_{k_i} > 1) && (5.23)
\end{aligned}$$

for all $i = 1, \ldots, n$. Applying (5.23) to (5.22) yields

$$P(X_1 \leq x_1, K_1 = k_1, \ldots, X_n \leq x_n, K_n = k_n)$$

$$= P(X_1 \leq x_1, K_1 = k_1) \cdots P(X_1 \leq x_n, K_1 = k_n).$$

Hence the joint probability distribution of $(X_i, K_i)_{i=1}^n$ decomposes and each term takes exactly the same form. Thus Lemma 5.16 is established. □

The loner process is not easy to characterize since whether a block mined at time t is a loner depends not only on the past but also on future blocks (in $(t, t+1]$). In order to count loners, we examine a tightly-related specie of honest blocks defined as follows.

Definition 5.17 (Double-lagger)**.** *The first honest block mined after a loner is called a double-lagger.*

Note that a loner is also a lagger. So whenever two laggers are mined in a row, the former one is a lagger and the latter one is a double-lagger. As such, there is a one-to-one correspondence between loners and double-laggers. We prove the independence of inter-double-lagger times, and derive their MGFs, thus establishing the arrivals of double-laggers as a renewal process.

Let $V_{s,t}$ denote the total number of double-laggers mined during $(s, t]$. Let V_1 denote the time the first double-lagger arrives. Let J_1 be the number of laggers after the genesis block until the first double-lagger (included). For $i > 1$, let V_i denote the time elapsed between the $(i-1)$-st and the i-th double-lagger. Let J_i be the number of laggers between the $(i-1)$-st double-lagger to the i-th double-lagger.

Lemma 5.18. *For all* $0 \leq s \leq t$,

$$Y_{s,t} \geq V_{s,t} - 1. \tag{5.24}$$

Proof. Because loners and double-laggers appear in consecutive pairs, all but the first double-lagger mined during $(s,t]$ corresponds to a loner mined during $(s,t]$. □

Lemma 5.19. $(V_1, J_1), (V_2, J_2), \ldots$ *are i.i.d.*

Proof. For convenience, for $n = 1, 2, \ldots$, let

$$M_n = J_1 + \cdots + J_n, \tag{5.25}$$

$$m_n = m_n. \tag{5.26}$$

This proof takes the same form as the proof of Lemma 5.16. It is easy to see that

$$L_i = X_{M_{i-1}+1} + \cdots + X_{M_i} \tag{5.27}$$

holds for $i = 1, 2, \ldots$. Also, the event $J_i = j_i$ is equivalent to the event that

$$K_{M_{i-1}+1} > 1, \ldots, K_{M_{i-1}+j_i-1} > 1, K_{M_{i-1}+j_i} = 1. \tag{5.28}$$

Given $J_1 = j_1, \ldots, J_i = j_i$, the event $L_i \leq \ell$ is equivalent to

$$X_{m_{i-1}+1} + \cdots + X_{m_i} \leq \ell. \tag{5.29}$$

For all positive integers $n, j_1, \ldots, j_n$ and real numbers $\ell_1, \ldots, \ell_n$, we have

$$\begin{aligned}
&P(V_1 \le \ell_1, J_1 = j_1, \ldots, L_n \le \ell_n, J_n = j_n) \\
&\quad = P(X_1 + \cdots + X_{j_1} \le \ell_1, K_1 > 1, \ldots, K_{j_1-1} > 1, K_{j_1} = 1, \\
&\qquad \ldots, \\
&\qquad X_{m_{n-1}+1} + \cdots + X_{m_n} \le \ell_n, K_{m_{n-1}+1} > 1, \ldots, K_{m_n-1} > 1, K_{m_n} = 1) \qquad (5.30) \\
&\quad = P(X_1 + \cdots + X_{j_1} \le \ell_1, K_1 > 1, \ldots, K_{j_1-1} > 1, K_{j_1} = 1) \\
&\qquad \times \cdots \\
&\qquad \times P(X_{m_{n-1}+1} + \cdots + X_{m_n} \le \ell_n, K_{m_{n-1}+1} > 1, \ldots, K_{m_n-1} > 1, K_{m_n} = 1) \qquad (5.31)
\end{aligned}$$

which is the product of n probabilities, where (5.31) is due to Lemma 5.16, i.e., $(X_1, K_1), (X_2, K_2), \ldots$ are i.i.d. Moreover, the i-th probability on the right hand side of (5.31) can be reduced as:

$$\begin{aligned}
&P(X_{m_{i-1}+1} + \cdots + X_{m_i} \le \ell, K_{m_{i-1}+1} > 1, \ldots, K_{m_i-1} > 1, K_{m_i} = 1) \\
&\quad = P(X_1 + \cdots + X_{j_i} \le \ell, K_1 > 1, \ldots, K_{j_i-1} > 1, K_{j_i} = 1)
\end{aligned} \qquad (5.32)$$

for all $i = 1, \ldots, n$. Applying (5.32) to (5.31) yields

$$P(V_1 \le \ell_1, J_1 = j_1, \ldots, L_n \le \ell_n, J_n = j_n) = P(V_1 \le \ell_1, J_1 = j_1) \cdots P(V_1 \le \ell_n, J_1 = j_n). \qquad (5.33)$$

Hence the joint probability distribution of $(L_i, J_i)_{i=1}^n$ decomposes and each term takes exactly the same form. Thus Lemma 5.19 is established. □

Lemma 5.20. *The time from a lagger to the next double-lagger follows the same distribution as the inter-double-lagger time.*

Proof. Let blocks b, c, d be consecutive honest blocks. Evidently, $T_c - T_b$ and $T_d - T_c$ are i.i.d. exponential random variables. Let Q be the time elapsed from block d to the next double-lagger. If d is a lagger, then Q does not depend on whether c is a lagger. Thus, for all x,

$$P(Q \leq x | T_d - T_c > 1) = P(Q \leq x | T_d - T_c > 1, T_c - T_b > 1).$$

The left hand side is the cdf of the time between a lagger and the next double-lagger; the right hand side is the cdf of inter-double-lagger time. Hence, the lemma is proved. □

For convenience we define the following function $h_\alpha(u)$:

$$h_\alpha(u) = u^2 - \alpha u - \alpha u e^{u-\alpha} + \alpha^2 e^{2(u-\alpha)}. \tag{5.34}$$

Evidently $h_\alpha(u) > 0$ if $u \leq 0$ and $h_\alpha(\alpha) = 0$. Also, $h_\alpha(u)$ is differentiable with bounded derivative on $[0, \alpha]$. From now on, let u_0 denote the smallest zero of $h_\alpha(\cdot)$, i.e.,

$$h_\alpha(u_0) = 0 \tag{5.35}$$

and $h_\alpha(u) \neq 0$ for all $u \in [0, u_0)$. We must have

$$0 < u_0 \leq \alpha. \tag{5.36}$$

Lemma 5.21. *Let V denote an inter-double-lagger time. The MGF of V is*

$$\Phi(u) = 1 + \frac{\alpha u - u^2}{u^2 - \alpha u - \alpha u e^{(u-\alpha)} + \alpha^2 e^{2(u-\alpha)}} \tag{5.37}$$

where the region of convergence is $(-\infty, u_0)$.

Proof. The key is to study a Markov process: The initial state is a lagger. With a known probability a double-lagger follows immediately to terminate the process. With the remaining probability we visit a non-lagger state a geometric number of times until we return to the initial lagger state. This allows us to write a recursion for the MGF of the inter-double-lagger time (aka the time till the double-lagger terminal state), the solution of which is (5.37).

By Lemma 5.19, it suffices to consider V_1, the arrival time of the first double-lagger starting from time 0. Let K denote the number of honest blocks until (including) the first lagger and let $b_1, \ldots, b_K$ denote that sequence of blocks. Then blocks $b_1, \ldots, b_{K-1}$ are non-laggers, and block b_K is a lagger (it may or may not be a double-lagger).

With probability $e^{-\alpha}$, $W_1 > 1$. In this case, block b_1 is a double-lagger since the genesis block is a lagger. We know $K = 1$ and $V_1 = W_1$.

With probability $1 - e^{-\alpha}$, $W_1 \leq 1$. Then block b_1 is not a lagger. We have $W_1 \leq 1, \ldots, W_{K-1} \leq 1, W_K > 1$. Let V' denote the time from lagger b_K to the next double-lagger. Then we can write

$$V_1 = \begin{cases} W_1 & \text{if } W_1 > 1 \\ W_1 + \cdots + W_K + V' & \text{if } W_1 \leq 1 \end{cases} \tag{5.38}$$

where V' follows the same distribution as V_1 by Lemma 5.20. Thus the MGF of V_1 can be calculated as

$$\mathbb{E}\left[e^{uV_1}\right] = (1-e^{-\alpha})\mathbb{E}\left[e^{u(W_1+\cdots+W_K+V')}\middle|W_1 \le 1\right] + e^{-\alpha}\mathbb{E}\left[e^{uW_1}\middle|W_1 > 1\right] \tag{5.39}$$

$$= (1-e^{-\alpha})\mathbb{E}\left[e^{u(W_1+\cdots+W_K)}\middle|W_1 \le 1\right]\mathbb{E}\left[e^{uV'}\right] + e^{-\alpha}\mathbb{E}\left[e^{uW_1}\middle|W_1 > 1\right] \tag{5.40}$$

$$= (1-e^{-\alpha})\mathbb{E}\left[e^{u(W_1+\cdots+W_K)}\middle|W_1 \le 1\right]\mathbb{E}\left[e^{uV_1}\right] + e^{-\alpha}\mathbb{E}\left[e^{uW_1}\middle|W_1 > 1\right] \tag{5.41}$$

where (5.40) is because V' and W_is are independent, and the fixed-point equation (5.41) is because V' is identically distributed as V_1.

If

$$(1-e^{-\alpha})\mathbb{E}\left[e^{u(W_1+\cdots+W_K)}\middle|W_1 \le 1\right] < 1 \tag{5.42}$$

rearranging (5.41) yields

$$\mathbb{E}\left[e^{uV_1}\right] = \frac{e^{-\alpha}\mathbb{E}\left[e^{uW_1}\middle|W_1 > 1\right]}{1-(1-e^{-\alpha})\mathbb{E}\left[e^{u(W_1+\cdots+W_K)}\middle|W_1 \le 1\right]}. \tag{5.43}$$

We shall revisit the condition (5.42) shortly.

Note that

$$P(K=k|W_1 \le 1) = (1-e^{-\alpha})^{k-2}e^{-\alpha}, k = 2,3,\ldots. \tag{5.44}$$

Hence

$$\mathbb{E}\left[e^{u(W_1+\cdots+W_K)}\middle|W_1 \le 1\right]$$

$$= \sum_{k=2}^{\infty} P(K=k|W_1 \leq 1) \times \mathbb{E}\left[e^{u(W_1+\cdots+W_k)}\middle| K=k, W_1 \leq 1\right] \tag{5.45}$$

$$= \sum_{k=2}^{\infty} (1-e^{-\alpha})^{k-2} e^{-\alpha} \times \mathbb{E}\left[e^{u(W_1+\cdots+W_k)}\middle| W_1 \leq 1, \ldots, W_{k-1} \leq 1, W_k > 1\right] \tag{5.46}$$

$$= \sum_{k=2}^{\infty} (1-e^{-\alpha})^{k-2} e^{-\alpha} \times \mathbb{E}\left[e^{uW_1}|W_1 \leq 1\right] \times \cdots \times$$

$$\mathbb{E}\left[e^{uW_{k-1}}|W_{k-1} \leq 1\right] \times \mathbb{E}\left[e^{uW_k}|W_k > 1\right] \tag{5.47}$$

$$= \sum_{k=2}^{\infty} (1-e^{-\alpha})^{k-2} e^{-\alpha}\, \Phi_0^{k-1}(u)\Phi_1(u) \tag{5.48}$$

$$= e^{-\alpha}\Phi_0(u)\Phi_1(u) \sum_{k=0}^{\infty} (1-e^{-\alpha})^k \Phi_0^k(u) \tag{5.49}$$

where (5.47) is due to mutual independence of inter-arrival times and (5.48) is due to Lemmas 5.14 and 5.15.

If

$$(1-e^{-\alpha})\Phi_0(u) < 1, \tag{5.50}$$

then the series sum converges to yield

$$\mathbb{E}\left[e^{u(W_1+\cdots+W_K)}\middle| W_1 \leq 1\right] = \frac{e^{-\alpha}\Phi_0(u)\Phi_1(u)}{1-(1-e^{-\alpha})\Phi_0(u)}. \tag{5.51}$$

Let us examine the conditions (5.42) and (5.50). Note that

$$(1-e^{-\alpha})\Phi_0(u) = \begin{cases} \frac{1-\frac{e^u}{e^\alpha}}{1-\frac{u}{\alpha}} & \text{if } u \neq \alpha, \\ \alpha & \text{if } u = \alpha. \end{cases} \tag{5.52}$$

It is clear that (5.52) is less than 1 for $u \leq 0$. For $u > 0$, because e^u/u is monotone decreasing on $(0,1)$ and monotone increasing on $(1,+\infty)$, there must exist $u \leq \alpha$ that satisfies $(1-e^{-\alpha})\Phi_0(u) = 1$. Hence the region of convergence must be a subset of $(-\infty, \alpha)$.

Let $h_\alpha(u)$ be defined as in (5.34). Using (5.51), it is straightforward to show that $(1-e^{-\alpha})\mathbb{E}\left[e^{u(W_1+\cdots+W_K)}\middle| W_1 \leq 1\right] = 1$ is equivalent to $h_\alpha(u) = 0$. Let $u_0 > 0$ be the smallest number that satisfies $h_\alpha(u_0) = 0$. Then u_0 exists and $0 < u_0 \leq \alpha$ according to (5.36). Also, $u < u_0$ implies (5.42). Therefore, the region of convergence for the MGF is $(-\infty, u_0)$.

For $u < u_0$, we have by (5.51) and Lemma 5.15:

$$\mathbb{E}\left[e^{uV_1}\right] = \frac{e^{-\alpha}\Phi_1(u)(1-(1-e^{-\alpha})\Phi_0(u))}{1-(1-e^{-\alpha})\Phi_0(u) - e^{-\alpha}(1-e^{-\alpha})\Phi_0(u)\Phi_1(u)} \tag{5.53}$$

which becomes (5.37).

□

Next, we bound the probability of typical events. It is hard to directly calculate the probability of the event $F^\epsilon_{s,t}$, which is defined as the intersection of uncountably many events. To circumvent this difficulty, we lower bound the probability of a "smaller" event $G^{\epsilon,q}_{s,t}$, which is the intersection of a countable number of simple events.

Definition 5.22. *For all $\epsilon \in (0,1)$, $q > 0$, and $0 \leq s < t$, let*

$$G^{\epsilon,q}_{s,t} = \bigcap_{\substack{m\in\{0,1,\ldots,\lceil\frac{s}{q}\rceil\},\\ n\in\{0,1,\ldots\}}} \{Y_{s-mq+q+1,t+nq-q-1-\epsilon} > A_{s-mq,t+nq}\}. \tag{5.54}$$

Lemma 5.23. *For all* $\epsilon \in (0,1)$*,* $q > 0$*, and* $0 \le s < t$*,*

$$G^{\epsilon,q}_{s,t} \subset F^{\epsilon}_{s,t}. \tag{5.55}$$

Proof. Without loss of generality, we assume $G^{\epsilon,q}_{s,t}$ is not empty. For every $0 \le a \le s < t \le b$, let m be the smallest integer satisfying $s - mq \le a$ and n be the smallest integer satisfying $t + nq \ge b$. Evidently $m, n \ge 0$. Then we have,

$$Y_{a+1,b-1-\epsilon} \ge Y_{s-mq+q+1,t+nq-q-1-\epsilon} \tag{5.56}$$

$$> A_{s-mq,t+nq} \tag{5.57}$$

$$\ge A_{a,b} \tag{5.58}$$

where (5.57) is because $G^{\epsilon,q}_{s,t}$ occurs. As a consequence, $F^{\epsilon}_{s,t}$ occurs. Hence the proof of this Lemma. □

With some foresight, we define

$$f(u) = e^{(2q+2+\epsilon)u}\Phi^2(u) \tag{5.59}$$

and

$$\Psi(u) = \frac{1}{u}(\beta + u - \beta\Phi(u)) \tag{5.60}$$

for $u \in [0, u_0)$. By convention, we let $\Psi(0) = 1$, so that Ψ is continuous on $[0, u_0)$.

Lemma 5.24. *For all $\epsilon \in (0,1)$, $q > 0$, and $0 \le s < t$,*

$$P(Y_{s+q+1,t-q-1-\epsilon} \le A_{s,t}) \le f(u)e^{-u\Psi(u)(t-s)} \tag{5.61}$$

for all $u \in (0, u_0)$.

Proof. Suppose $u \in (0, u_0)$. By independence of the Y and Z processes, we have

$$P(Y_{s+q+1,t-q-1-\epsilon} \le A_{s,t}) \le \sum_{j=0}^{\infty} P(A_{s,t} = j) \cdot P(Y_{s+q+1,t-q-1-\epsilon} \le j) \tag{5.62}$$

$$\le \sum_{j=0}^{\infty} P(A_{s,t} = j) \cdot P(V_{s+q+1,t-q-1-\epsilon} \le j+1) \tag{5.63}$$

where (5.63) is due to Lemma 5.18.

If no more than $j+1$ double-laggers are mined during time interval $(s+q+1, t-q-1-\epsilon]$, then counting from time $s+q+1$, the $(j+2)$-nd double-lagger must be mined after time $t-q-1-\epsilon$. Due to Lemma 5.19, we have

$$P(V_{s+q+1,t-q-1-\epsilon} \le j+1) \le P\left(\sum_{m=1}^{j+2} V_m \ge t-s-2q-2-\epsilon\right) \tag{5.64}$$

where $V_1, V_2, \ldots$ are i.i.d. inter-double-lagger times. Using Markov's inequality and Lemma 5.19, for all $u \in (0, u_0)$:

$$P\left(\sum_{m=1}^{j+2} V_m \ge t-s-2q-2-\epsilon\right) \le \mathbb{E}\left[\exp\left(u\Big(\sum_{m=1}^{j+2} V_m - (t-s-2q-2-\epsilon)\Big)\right)\right] \tag{5.65}$$

$$= e^{-u(t-s-2q-2-\epsilon)}\Phi^{j+2}(u). \tag{5.66}$$

Using (5.63)–(5.66), we have for $u \in (0, u_0)$

$$P(Y_{s+q+1,t-q-1-\epsilon} \le A_{s,t}) \le \sum_{j=0}^{\infty} e^{-(t-s)\beta} \frac{((t-s)\beta)^j}{j!} e^{-u(t-s-2q-2-\epsilon)} \Phi^{j+2}(u) \tag{5.67}$$

$$= e^{-(\beta+u)(t-s)+(2q+2+\epsilon)u} \Phi^2(u) \sum_{j=0}^{\infty} \frac{((t-s)\beta\Phi(u))^j}{j!} \tag{5.68}$$

$$= e^{(2q+2+\epsilon)u} \Phi^2(u) e^{-(t-s)(\beta+u-\beta\Phi(u))} \tag{5.69}$$

which becomes (5.61). □

Lemma 5.25. *If $\beta < \alpha e^{-2\alpha}$, then there exists some positive number $u^* < u_0$ such that $u\Psi(u) > 0$ for all $u \in (0, u^*]$.*

Proof. By definition, $u\Psi(0) = 0$ and the right derivative

$$(u\Psi(u))'_+|_{u=0} = 1 - \beta(\Phi(u))'_+|_{u=0} \tag{5.70}$$

$$= -\left[\frac{-\alpha - \alpha e^{-\alpha+u} + 2u^2 e^{2(u-\alpha)} + 2u - \alpha u e^{u-\alpha}}{(\alpha^2 e^{2(u-a)} - \alpha u - \alpha u e^{u-a} + u^2)^2} \cdot \beta(-\alpha u + u^2) \right.$$

$$\left. + \frac{\beta(-\alpha + 2u)}{\alpha^2 e^{2(u-a)} - \alpha u - \alpha u e^{u-a} + u^2} + 1 \right] \Bigg|_{u=0} \tag{5.71}$$

$$= 1 - \frac{\beta}{\alpha e^{-2\alpha}}. \tag{5.72}$$

If $\beta < \alpha e^{-2\alpha}$, we have $(u\Psi(u))'_+|_{u=0} > 0$. By continuity, there must exist a $u^* < u_0$ such that $(u\Psi(u))' > 0$ and $u\Psi(u) > 0$ for all $u \in (0, u^*]$. □

Let $u_1 > 0$ be the smallest positive number such that $\Psi(u) = 0$. Note that as $u \to u_0$, we have $\Phi(u) \to \infty$ and $u\Psi(u) \to -\infty$. By Lemma 5.25, u_1 exists and $u^* < u_1 < u_0$.

Lemma 5.26. *For all $\epsilon \in (0,1)$, $q > 0$, and $0 \le s < t$,*

$$P\left((F_{s,t}^{\epsilon})^c\right) \le \min_{0<u<u_1} \left(1 + \frac{u + \beta - u\Psi^2(u)}{\beta\Psi(u)}\right)^2 \times (1+\Psi(u))^{\frac{2}{\Psi(u)}} e^{(2+\epsilon)u - \Psi(u)u(t-s)} \tag{5.73}$$

where u_1 is the smallest number such that $u_1\Psi(u_1) = 0$.

Proof. Let $k = \lceil \frac{s}{q} \rceil$. By Lemmas 5.23 and 5.24 and using the union bound, we have for $u \in (0, u_1)$:

$$\begin{aligned}
P\left((F_{s,t}^{\epsilon})^c\right) &\le P\left((G_{s,t}^{\epsilon,q})^c\right) && (5.74)\\
&\le P\left(\bigcup_{\substack{m\in\{0,1,\ldots,k\},\\ n\in\{0,1,\ldots\}}} \{Y_{s-mq+q+1,t+nq-q-1-\epsilon} \le A_{s-mq,t+nq}\}\right) && (5.75)\\
&< \sum_{\substack{m\in\{0,1,\ldots,k\},\\ n\in\{0,1,\ldots\}}} f(u) e^{-u\Psi(u)(t+nq-s+mq)} && (5.76)\\
&= f(u)e^{-u\Psi(u)(t-s)} \left(\sum_{m=0}^{k} e^{-u\Psi(u)mq}\right)\left(\sum_{n=0}^{\infty} e^{-u\Psi(u)nq}\right) && (5.77)\\
&< \frac{f(u)}{\left(1-e^{-u\Psi(u)q}\right)^2} e^{-u\Psi(u)(t-s)}. && (5.78)
\end{aligned}$$

For a given u, to minimize (5.78), we set the derivative with respect to q to zero to obtain the optimal choice:

$$q^* = \frac{\log\left(1+\Psi(u)\right)}{u\Psi(u)}. \tag{5.79}$$

Note that by (5.60), we have

$$\Phi(u) = 1 + \frac{u - u\Psi(u)}{\beta}. \tag{5.80}$$

We set q to q^*, plug (5.59), (5.79), and (5.80) into (5.78). Then for $u \in (0, u_1)$

$$P\left((F^{\epsilon}_{s,t})^c\right) \leq \frac{e^{(2q^*+2+\epsilon)u}\Phi^2(u)}{\left(1 - \frac{1}{1+\Psi(u)}\right)^2} e^{-u\Psi(u)(t-s)}. \tag{5.81}$$

$$= \frac{\left(1 + \frac{u-u\Psi(u)}{\beta}\right)^2}{\left(\frac{\Psi(u)}{1+\Psi(u)}\right)^2} e^{2q^*} e^{-u\Psi(u)(t-s)+(2+\epsilon)u} \tag{5.82}$$

$$= \left(1 + \frac{u + \beta - u\Psi^2(u)}{\beta\Psi(u)}\right)^2 (1 + \Psi(u))^{\frac{2}{\Psi(u)}} e^{(2+\epsilon)u - \Psi(u)u(t-s)}. \tag{5.83}$$

This completes the proof of Lemma 5.26. □

Lastly, we recover the result for the original arbitrary time unit where the block propagation delays are bounded by Δ time units in lieu of 1 time unit.

Theorem 5.27 (Blockchain consistency theorem)**.** *Let α and β denote the total mining rates (in blocks per unit time) of all honest and adversarial miners, respectively. Let network delays be upper bounded by Δ units of time. Suppose*

$$\beta < \alpha e^{-2\alpha\Delta}. \tag{5.84}$$

For every $s > 0$, barring an event $E_{s,t}$ with probability $P(E_{s,t}) \leq e^{-\Theta(t-s)}$, a block that is mined by time s and included in some honest miner's longest blockchain at time t is also

included in all honest miners' longest blockchains at all later times. To be precise, let

$$\psi(v) = 1 - \frac{\beta\,(\alpha - v)}{v^2 - \alpha v - \alpha v e^{(v-\alpha)\Delta} + \alpha^2 e^{2(v-\alpha)\Delta}}. \tag{5.85}$$

Let θ be the smallest positive number that satisfies $\psi(\theta) = 0$. Then $P\,(E_{s,t})$ is upper bounded by

$$\min_{v\in(0,\theta)} \left(1 + \frac{v + \beta - v\psi^2(v)}{\beta\psi(v)}\right)^2 (1 + \psi(v))^{\frac{2}{\psi(v)}} e^{2\Delta v - \psi(v)v(t-s)}. \tag{5.86}$$

Proof. To reintroduce Δ into the result, we let $\tau = t\Delta$, $\sigma = s\Delta$, $a = \alpha/\Delta$, $b = \beta/\Delta$, and $v = u/\Delta$. These new variables and parameters are then defined under the original time unit. We define

$$\phi(v) = \Phi(\Delta v) \tag{5.87}$$

$$\psi(v) = \Psi(\Delta v). \tag{5.88}$$

Plugging in (5.37) and (5.60), we have

$$\phi(v) = 1 + \frac{av - v^2}{v^2 - av - ave^{(v-a)\Delta} + a^2 e^{2(v-a)\Delta}} \tag{5.89}$$

$$\psi(v) = \frac{b + v - b\phi(v)}{v} \tag{5.90}$$

$$= 1 - \frac{b\,(a - v)}{v^2 - av - ave^{(v-a)\Delta} + a^2 e^{2(v-a)\Delta}}. \tag{5.91}$$

Suppose a block is mined at time σ and is included in a τ-credible blockchain. Applying Lemma 5.13, the block is included in all future credible blockchains under event $F^{\epsilon}_{\frac{\sigma}{\Delta},\frac{\tau}{\Delta}}$.

We then apply Lemma 5.26 with the conversion. For $0 \leq \sigma < \tau$, we define

$$E_{\sigma,\tau} = \left(\bigcup_{0<\epsilon<1} F^{\epsilon}_{\frac{\sigma}{\Delta},\frac{\tau}{\Delta}} \right)^{\mathrm{c}}. \tag{5.92}$$

Using Lemma 5.26 and letting $\epsilon \to 0$, an upper bound of $E_{\sigma,\tau}$ is given by

$$\min_{v\in(0,v_1)} \left(1 + \frac{v + b - v\psi^2(v)}{b\psi(v)}\right)^2 (1+\psi(u))^{\frac{2}{\psi(v)}} e^{2v\Delta - \psi(v)(\tau-\sigma)v} \tag{5.93}$$

where v_1 is the smallest positive number such that $\psi(v_1) = 0$. Then every block mined before σ and is in a τ-credible blockchain must be included in all credible blockchains thereafter barring event $E_{\sigma,\tau}$, whose probability is upper bounded by (5.93). This conclusion is equivalent to Theorem 5.27 (with minor abuse of notation we still use α, β, s, and t to replace a, b, σ, and τ, respectively, to follow some convention). Thus, Theorem 5.27 is proved. □

5.4. Proof of Liveness

Definition 5.28 (Jumper)**.** *A block is called a jumper if it is the first honest block mined at its height.*[2]

For $i = 1, 2, \ldots$, let M_i denote the time elapsed between the $(i-1)$-st jumper and the i-th jumper. As in Section 5.3, we use Δ as the time unit for convenience. Let $M_{s,t}$ denote the number of jumpers mined during time interval $(s, t]$. For simplicity, we also assume that individual honest miners have infinitesimal mining power, so that almost surely no individual miner mines two consecutive jumpers in a row.

[2]Ties are broken in a deterministic manner.

Lemma 5.29. *The inter-jumper times $M_1, M_2, \ldots$ are i.i.d. and $M_i - 1$ follows an exponential distribution with mean $1/\alpha$.*

Proof. Let $b_0 = b$ be the 0-th jumper and and let block b_i denote the i-th jumper after block b. Until $T_{b_i} + 1$ when block b_i is in all honest miners' views, all honest miners except block b_i's miner (who is negligible) are mining at heights no higher than $h(b_i)$. From $T_{b_i} + 1$, it takes exponential time with mean $1/\alpha$ to mine the next jumper. Due to the memoryless nature of the honest mining process, $M_1, M_2, \ldots$ are i.i.d. (the jumpers form a renewal process). □

Using Lemma 5.29, it is straightforward to establish the following result concerning the height of longest (or credible) blockchains over time.

Definition 5.30. *Let $F(\cdot, k, \alpha)$ be the cumulative distribution function (cdf) of the Erlang distribution with shape parameter k and scale parameter α.*

Lemma 5.31 (Blockchain Growth Lemma)**.** *For all $0 \leq s < t$, every honest miner's longest blockchain at time t must be at least n higher than every honest miner's longest blockchain at time s with probability no less than*

$$F(t - s - 1 - n, n, \alpha). \tag{5.94}$$

Proof. If $t - s < 1$ then $F(t - s - 1 - n, n, \alpha) = 0$, so the lemma holds trivially. We assume $t - s > 1$. All jumpers mined during $(s, t - 1]$ must be in every honest miner's views by t, where the first jumper is higher than the miner's longest blockchain at time s and the last jumper is no higher than the miner's longest blockchain at time t. Hence the

probability of interest is no less than $P(M_{s,t-1} \geq n)$. The event that n or more jumpers are mined on $(s, t-1]$ is the same as that n inter-jumper times can fit in a duration of $t-1-s$, i.e.,

$$P(M_{s,t-1} \geq n) = P(M_1 + \cdots + M_n \leq t-s-1) \tag{5.95}$$

where $M_1, \ldots, M_n$ are i.i.d. inter-jumper times. This probability is equal to

$$\begin{aligned} &P((M_1-1) + \cdots + (M_n-1) < t-s-1-n) \\ &\qquad = F(t-s-1-n, n, \alpha) \end{aligned} \tag{5.96}$$

where (5.96) is because $M_1 - 1, \ldots, M_n - 1$ are i.i.d. exponential random variables whose sum has the Erlang distribution with shape parameter n and rate α. □

With the preceding techniques, we can establish the following probabilistic bound for blockchain quality or liveness.

Lemma 5.32 (Blockchain Liveness Theorem)**.** *Let $0 \leq s < t-1$. In every honest miner's longest blockchain at time t, the probability that n or more of those blocks are honest blocks mined during (s, t) is lower bounded by*

$$\sum_{i=0}^{\infty} e^{-\beta(t-s)} \frac{(\beta(t-s))^i}{i!} F(t-s-i-n-1, i+n, \alpha). \tag{5.97}$$

Proof. Since $M_{s,t-1}$ jumpers are mined during $(s, t-1]$ (with different heights), and at most $A_{s,t}$ of them are matched by adversarial blocks, the number of surplus jumper blocks lower bounds the number of honest blocks in any honest miner's longest blockchain

that are mined during $(s,t]$. The said probability is thus lower bounded by

$$P\left(M_{s,t-1} - A_{s,t} \geq n\right) = \sum_{i=0}^{\infty} P(A_{s,t} = i) P(M_{s,t-1} \geq i + n) \tag{5.98}$$

$$= \sum_{i=0}^{\infty} e^{-\beta(t-s)} \frac{(\beta(t-s))^i}{i!} P(M_1 + \cdots + M_{i+n} \leq t - s - 1) \tag{5.99}$$

which is equal to (5.97). □

5.5. Latency-Security tradeoff of the Bitcoin protocol

Given a desired security level, Theorem 5.27 provides an upper bound of the confirmation time needed to achieve it. In this section, we analyze a private attack which establishes a minimum confirmation time needed for the security level.

With the lower bound and upper bound of confirmation time, we provide practical numerical results on the latency-security tradeoff of the Bitcoin blockchain in this section. The effect of block generation rate is also discussed.

5.5.1. Private attack

Definition 5.33 (Private attack)**.** *A private attack strategy on block b, denoted as ζ_b, is described as follows:*

- *As soon as b is mined, the adversary starts to mine a private adversarial blockchain that extends block f_b.*
- *Starting from (including) block b, every newly mined honest block enters all other honest miners' view exactly Δ units of time thereafter.*

As alluded to in Section 5.2, the adversary is given the advantage of manipulating block propagation times subject to the delay bound (Definition 5.5). We say the private attack on block b is successful at time t if the privately mined adversarial blockchain at time t is at least as long as one t-credible blockchain (so that the adversarial blockchain can be published to make some honest miners reverse block b).

Without loss of generality, we assume that honest miners always mine on top of the earliest longest blockchain in case multiple longest blockchains are in an honest miner's view. If an honest block is not a jumper, then once its propagation is subject to the maximum delay, it loses to some other honest block at the same height and hence does not make into any later credible blockchain even if the adversary takes no action at all. Hence, without loss of generality, we assume the adversary attacks a jumper block b which is referred to as the 0-th jumper in this subsection.

Lemma 5.34. *If the adversary performs the private attack ζ_b on a jumper b and publishes no block during $[T_b - \Delta, T_b + t]$ with $t > 0$, then the height of the i-th jumper mined during $(T_b, T_b + t)$ is $h(b) + i$. Also, the height of all $(T_b + t)$-credible blockchains is no greater than $h(b) + M_{T_b, T_b + t}$.*

Proof. By the private attack strategy in Definition 5.33, starting from block b, no adversarial blocks are published on those heights by $T_b + t$. Thus, the jumpers mined during $[T_b, T_b + t)$ have consecutive heights, and the height of a $(T_b + t)$-credible blockchain is no higher than that of the last jumper mined before $T_b + t$. Hence the proof of the lemma. □

Theorem 5.35 (Latency–security lower bound)**.** *Given* $0 \leq s < t-\Delta$*, under an event* $B_{s,t}$*, a block* b *mined at time* s *that is included in an honest miner's longest blockchain at time* t *will not be in some honest miner's longest blockchains at some later time under the private attack* ζ_b*, where*

$$P\left(B_{s,t}\right) = \sum_{i=1}^{\infty} e^{-\beta(t-s)} \frac{(\beta(t-s))^i}{i!} \left(1 - F\left(\frac{t-s}{\Delta} - i - 1, i, \alpha\Delta\right)\right) \tag{5.100}$$

where $F(\cdot, n, a)$ *is defined in Definition 5.30.*

Proof. Using the normalized time unit, we convert the original condition $t - s > \Delta$ to $t - s > 1$. If block b is not a jumper, it will not be included in any honest miner's longest blockchain at t when the adversary takes no action, so there is nothing to prove in this case.

If block b is a jumper, the adversary performs the private attack ζ_b and begins to mine blocks from height $h(b)$. The private attack is successful at time t if the adversary mines more blocks than the number of competing jumpers. Because jumpers are subject to one unit of propagation delay, only jumpers mined until time $t-1$ are competitive. Specifically, the private attack is successful under this event:

$$B_{s,t} = \{A_{s,t} \geq M_{s,t-1} + 1\}. \tag{5.101}$$

Again, let $M_1, M_2, \ldots$ denote i.i.d. inter-jumper times. The probability of success can be lower bounded by

$$P\left(B_{s,t}\right) = \sum_{i=1}^{\infty} P(A_{s,t} = i) P(M_{s,t-1} \leq i - 1) \tag{5.102}$$

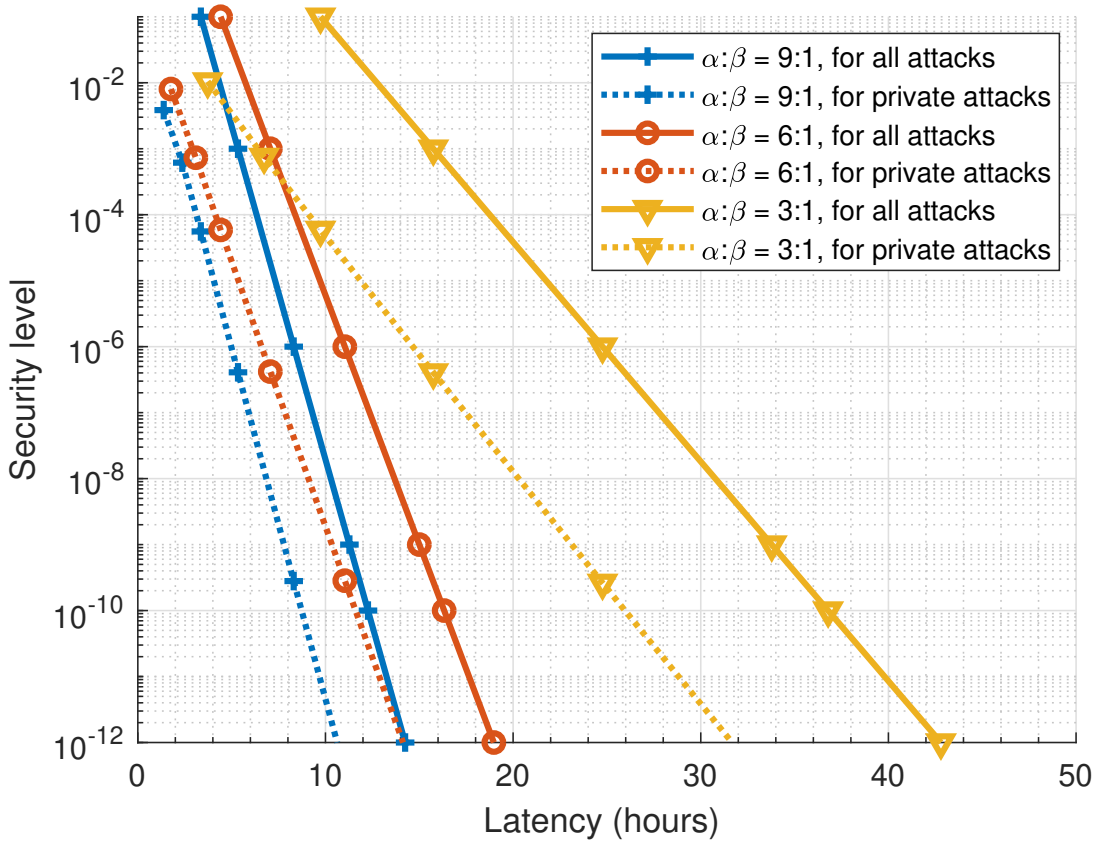


Figure 5.1. Bitcoin's latency–security trade-off with $\alpha + \beta = 1/600$ blocks per second and $\Delta = 10$ seconds.

$$= \sum_{i=1}^{\infty} e^{-\beta(t-s)} \frac{(\beta(t-s))^i}{i!} P(M_1 + \cdots + M_i > t - s - 1) \tag{5.103}$$

$$= \sum_{i=1}^{\infty} e^{-\beta(t-s)} \frac{(\beta(t-s))^i}{i!} (1 - F(t - s - i - 1, i, \alpha)). \tag{5.104}$$

Once converted to the original time unit, i.e., with α, β, s and t replaced by $\alpha\Delta$, $\beta\Delta$, s/Δ, and t/Δ, respectively, this result becomes (5.100). □

5.5.2. Numerical results

The latency–security trade-off under several different sets of parameters is plotted in Figure 5.1. The mining rate is set to Bitcoin's one block per 600 seconds, or $\alpha+\beta = 1/600$ blocks/second. In Bitcoin, the block size is about 1 MB. The propagation delay of Bitcoin blocks fluctuates over the years with an overall decreasing trend [**38**]; the 90th percentile of block propagation is 4 seconds on average as of July 2020. Since Δ in our model needs to be an upper bound on propagation delay, we assume $\Delta = 10$ seconds for a 1 MB Bitcoin block. The latency upper (resp. lower) bounds are computed using Theorem 5.27 (resp. Theorem 5.35). In Figure 5.1, all bounds appear to be exponential in latency (this is also rigorously established by Theorem 5.27.)

It is instructive to examine concrete data points in Figure 5.1: If the adversarial share of the total network mining rate is 10%, then a confirmation time of 5 hours 20 minutes is sufficient to achieve 10^{-3} security level, and 12 hours 15 minutes achieve 10^{-10} security level. These results are within 4 hours of the corresponding lower bounds due to the private attack. If the adversarial share of the mining rate increases to 25%, then 16 hours 20 minutes and 37 hours 20 minutes of confirmation times achieve 10^{-3} and 10^{-10} security levels, respectively, and the gap between the upper and lower bounds is about 12 hours. The gap is essentially constant under at security levels (a pair of corresponding curves are almost parallel in the figure). The gap is relatively insignificant at high security levels but can be significant at low security levels.

5.5.3. Remarks

First, we note that most previous analyses on the Nakamoto consensus assume a finite lifespan of the protocol [**4**, **32**], that is, a maximum round number is defined, at which round the protocol terminates. The probability of consistency depends on the maximum round number.

In contrast, this thesis does not assume a finite lifespan. Theorem 5.27 states that, barring a small probability event, a confirmed block remains permanently in all miners' longest blockchains into the arbitrary future.

Second, for technical convenience, we regard a block in a miner's longest blockchain to be confirmed after a certain amount of *time* elapses since the block is mined or enters the miner's view. Nakamoto [**1**] originally proposed confirming a block after it is sufficiently *deep* in an honest miner's longest blockchain. We believe both confirmation rules are easy to use in practice. But the two confirmation rules imply each other in probability:

Let

$$\kappa(\lambda, \epsilon) = \min \left\{ k : \ e^{-\lambda} \sum_{i=k}^{\infty} \frac{\lambda^i}{i!} \leq \epsilon \right\}. \tag{5.105}$$

Then for every $\tau > 0$, the probability that $\kappa((\alpha + \beta)\tau, \epsilon)$ or more blocks are mined in τ units of time is no greater than ϵ. For example, we learn from Figure 5.1 that 5.58 hours of latency guarantees a security level of 0.0005. Using (5.105), we obtain that $\kappa(5.58 \times 6, 0.0005) = 55$. Hence if one counts 55 confirmation blocks, it implies that at least 5.58 hours have elapsed with error probability 0.0005. In all, 55 confirmation blocks

guarantees 10^{-3} security level, assuming that at most 10% of the total mining power is adversarial.

At 10% adversarial mining power, Nakamoto [**1**] estimated that confirming after six blocks beats private attack at least 99.9% of the time. In contrast, 55 confirmation blocks guarantees the same security level regardless of what attack the adversary chooses to employ. We also note that while on average six blocks take only one hour to mine, with probability 10^{-3} it takes 2.75 hours or more to mine.

5.5.4. Effect of block generation rate

The latency–security trade-off has already been shown in Figure 5.1 for the Bitcoin protocol parameters. Figure 5.2 illustrates how the trade-off changes if the block generation rate increases by 10 folds (to 1 block per minute), with everything else held the same. It is not surprising to see that the latency is much shorter under the higher block generation rate in this particular case.

Figure 5.3 illustrates the confirmation time needed for different security levels, block generation rates, and block propagation delays. As expected, the latency is larger with longer block propagation delay and/or stronger security level requirement. Interestingly, increasing the block generation rate first reduces latency but eventually causes the latency to rise without bound. The intuition is as the block generation rate keeps increasing, more confirmation time is needed due to heavy forking From the graph, with the Bitcoin block propagation delay around 10 seconds, a sweet spot for block generation rate is between 40 and 100 blocks per hour in terms of optimizing latency.

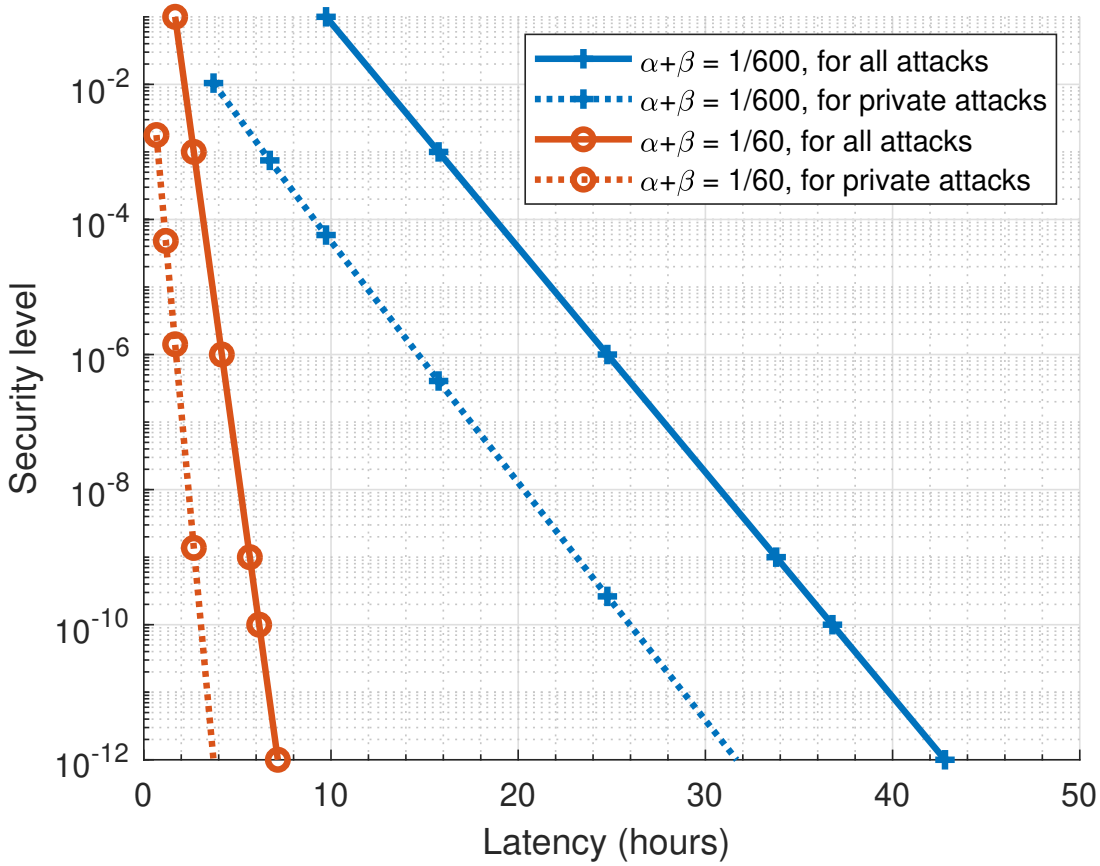


Figure 5.2. Latency–security trade-off with $\Delta = 10$ seconds and 25% percentage of adversarial mining.

We recall that Theorem 5.27 requires the honest-to-adversarial mining ratio to be bounded by

$$\frac{\beta}{\alpha} < e^{-2\alpha\Delta}. \tag{5.106}$$

This is because $\alpha e^{-2\alpha\Delta}$ is the exact rate that loners are mined. Beyond the ratio in (5.106), this thesis provides no security guarantee. This is marked as the "calculation bound" in Figure 5.3. Note that (5.106) is a sufficient but not necessary condition for the consistency

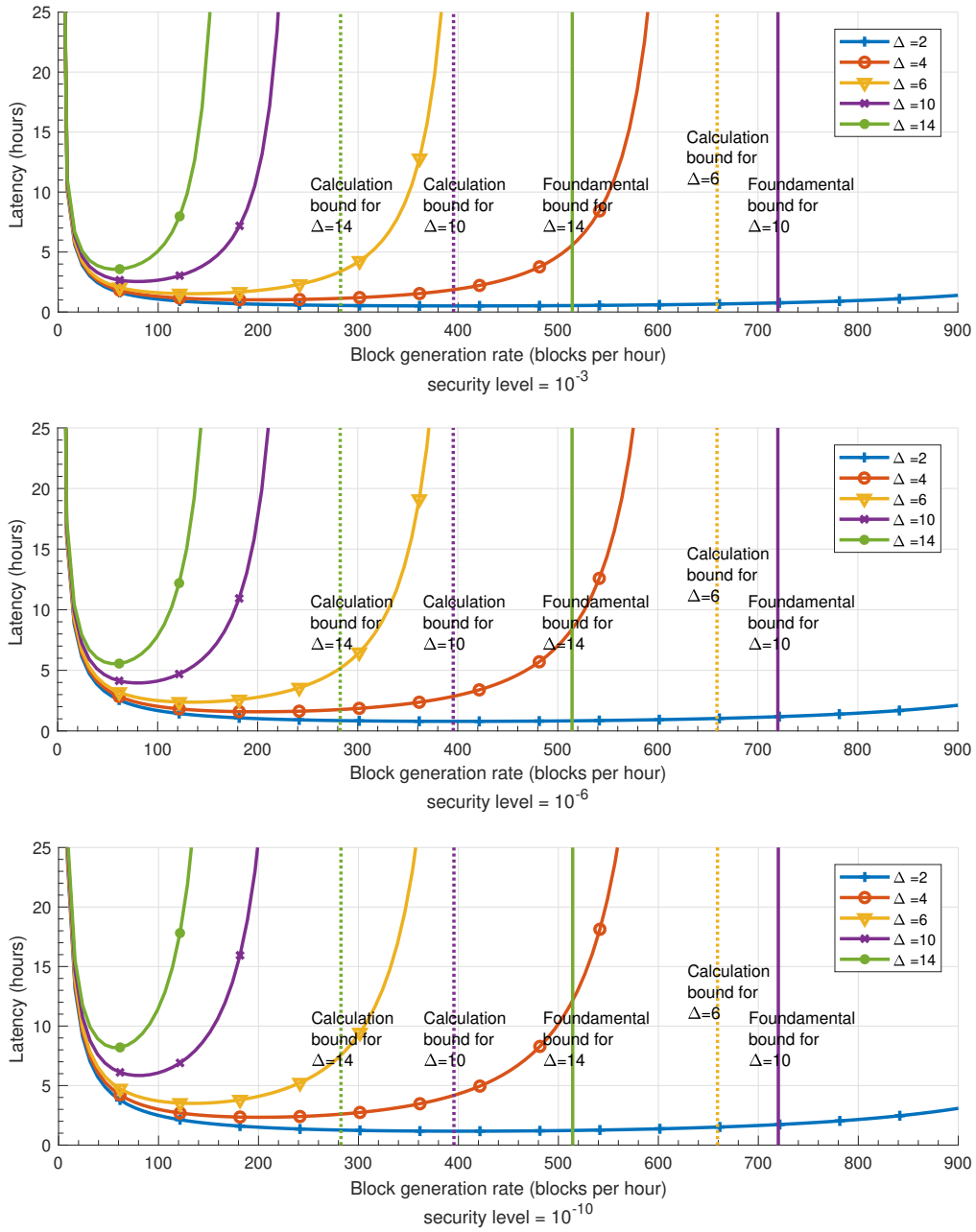


Figure 5.3. Latency required for different propagation delays. The percentage of adversarial mining is 25%.

of the Nakamoto consensus. The sufficient and necessary condition is given in [**14**, **15**]:

$$\frac{\beta}{\alpha} < \frac{1}{1+\alpha\Delta}. \tag{5.107}$$

This is marked as the fundamental bounds in Figure 5.3.

5.6. Analysis of existing systems

5.6.1. Methodology

5.6.1.1. Metrics. The performance metrics of a Nakamoto-style protocol include latency for a given security level, throughput, and fault tolerance (the upper limit of the fraction of adversarial mining in a secure system). This section numerically computes the trade-off between different performance metrics of popular Nakamoto-style systems (Bitcoin Cash, Ethereum, etc.) and discuss their parameter selections.

We remark that the throughput metric can be defined in a few different ways, ranging from the "best-case" throughput where the adversarial miners follow the protocol, to the "worst-case" throughput where the adversarial miners not only mine empty blocks but also use a selfish mining type of attack [**4**,**39**] to push honest blocks out of longest blockchains. In this thesis, we choose to focus on the "best-case" throughput, which is the throughput under normal operation and is perhaps what protocol designers have in mind when setting parameters.

5.6.1.2. Block propagation delay. The above metrics crucially depend on the block generation rate (or the total mining rate in the system), maximum block size, and block propagation delay. The former two are explicitly specified in the protocol. The block propagation delay, however, depends on network conditions. Block propagation delays

in the Bitcoin network have been measured in [**18**, **40**, **41**]. Such measurements are in general lacking for other systems. It is observed in [**18**] that there is a linear relationship between propagation delays and block size.

In this section, we let the maximum block propagation delay be determined by the block size S (in KB) according to the following formula:

$$\Delta = aS + b. \tag{5.108}$$

We determine the coefficients a and b using propagation delay data from Bitcoin and Ethereum monitoring websites. In Bitcoin, the block size is about 1 MB. We assume $\Delta = 10$ seconds for a 1 MB Bitcoin block as illustrated in subsection 5.5.2. According to [**42**], the 90th percentile of Ethereum block propagation is 1.75 seconds for an average block size of 25 KB. We round it up to 2 seconds for an upper bound. Using these data points, we estimate $a = 0.008$ and $b = 1.79$.

5.6.2. The latency–throughput trade-off

A larger block size may benefit throughput by carrying more transactions. On the other hand, the larger block size increases the propagation delay, which causes longer latency. A protocol designer may want to find a sweet spot that leads to the most desirable latency and throughput.

Figure 5.4 illustrates the minimum latency required to achieve given throughput according to Theorem 5.27 (it is actually a latency upper bound). For several target throughput numbers (20, 30, 40, 50, and 60 KB per second), we also mark the corresponding block

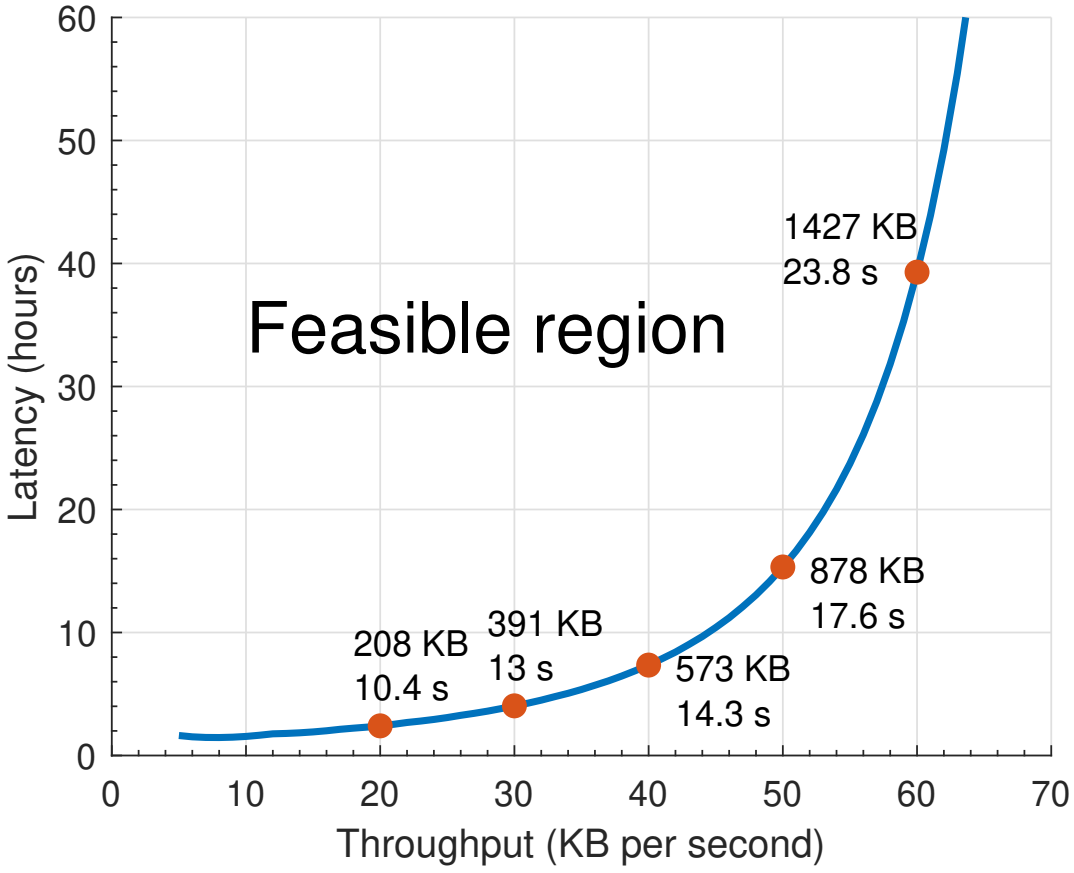


Figure 5.4. Feasible latency for different throughput. The security level is 10^{-10}. The percentage of adversarial mining power is 25%.

sizes (in KB) and block generation rates (in seconds per block) to achieve the best latency bound. For example, the best latency bound is 2 hours and 25 minutes for a target throughput of 20 KB per second (at 10^{-10} security level, 25% percentage adversarial mining). This latency can be achieved by setting the block size to 208 KB and the block generation rate to one block every 10.4 seconds.

Protocol	Maximum block size	Generation rate	Propagation delay (seconds)	Latency: 10^{-3} security level	Latency:10^{-6} security level	Latency: 10^{-10} security level	Throughput (KB/second)	Fault tolerance
Bitcoin	1 MB	6	10	< 15h 45m	< 24h 45m	< 37h 50m	1.7	49.7%
BCH	8 MB	6	67.4	< 21h 55m	< 34h 10m	< 50h 30m	13.3	48.0%
BSV	2000 MB	6	1.6×10^4	N/A	N/A	N/A	N/A	3.6%
Litecoin	1 MB	24	10	< 4h 40m	< 7h 15m	< 10h 55m	6.7	48.8%
Zcash	2 MB	48	18.2	< 4h 40m	< 7h 15m	< 10h 40m	26.7	45.8%
Ethereum	0.183 MB	240	3.3	< 50m	< 1h 20m	< 1h 55m	12.2	46.2%

Table 5.2. Parameters and performances of Nakamoto-style Protocols. The percentage of adversarial mining power is 25%. In formula (5.108), a = 0.008 and b = 1.79.

5.6.3. Case Studies in the Current Ecosystem

Some proof-of-work protocols attempt to better Bitcoin by inflating the block size (Bitcoin Cash, Bitcoin SV) or increasing the block generation rate (Litecoin). This subsection discusses the performance of these Bitcoin-like protocols. Table 5.2 describes the parameters, estimated propagation delay, and performances of the aforementioned protocols.

5.6.3.1. BCH. Bitcoin Cash (BCH) is a hard fork of Bitcoin from 2017. BCH aims to increase the throughput by increasing the maximum block size to 8 MB while remaining the same block generation rate as Bitcoin [**43**]. As a result, the latency is increased from around 37 hours to 50 hours for 10^{-10} security level. Had BCH increase the block generation rate (instead of the block size) by eight times, it would have obtained the same eight fold throughput improvement while at the same time shortened the latency by a factor of eight or so.

5.6.3.2. BSV. Bitcoin SV (BSV) was created in 2018 by forking BCH. BSV intended to reduce transaction fees by adjusting the protocol with even larger block sizes upper bounded by 2 GB [**44**]. However, the 2 GB block size will cause very long propagation delay. According to the fundamental fault tolerance bound (5.107), we see that BSV's security can not be guaranteed unless the adversary controls less than 3.6% of the total

mining power. In reality, the only reason BSV has not observed a problem because it has low interests and the blocks its miners produce are nowhere close to 2 GB. However, when BSV starts to operate at its intended capacity, its 3.6% fault tolerance will become a major issue.

5.6.3.3. Litecoin. Litecoin is also a fork of the Bitcoin Core client that dates back to 2011. Litecoin decreases the block generation time from 10 minutes to 2.5 minutes per block [**45**]. For Litecoin, the latency is 10 hours 55 minutes, and the current throughput is 6.7 KB per second (for 10^{-10} security level and 25% percentage of adversarial mining power). From Figure 5.4, one can see that a latency less than 2 hours can be achieved with a throughput of 6.7 KB per second. This can be achieved by increasing the block generation rate and decreasing the block size.

5.6.3.4. Zcash. Proposed in 2016, Zcash is aims to provide enhanced privacy features. In 2017, Zcash doubled the maximum block size from 1 MB to 2 MB [**46**]. Zcash also decreased the block interval from 10 minutes to 1.25 minutes [**47**]. Similar to Litecoin, ZCash can be improved by increasing the block generation rate (higher throughput) and/or decreasing block size (shorter latency).

5.6.3.5. Ethereum. The second largest cryptocurrency platform Ethereum has the block generation rate of 15 seconds per block [**48**, **49**]. The maximum gas consumption for each Ethereum block is 12.5×10^6. Given that 21000 gas must be paid for each transaction and 68 gas must be paid for each non-zero byte of the transaction [**31**], we estimate the maximum block size of an Ethereum block is 183 KB. Ethereum increases the block generation rate and decrease the block size. From Figure 5.4, for the throughput of around 12 KB per second, the latency bound is around 1 hour and 40 minutes, which is close to

the current confirmation time of 1 hour and 55 minutes. The parameters of Ethereum seem to be well-chosen.

5.6.3.6. Summary. In general, most of Nakamoto-style cryptocurrencies start with Bitcoin as the baseline and aim to improve its throughput. Since Bitcoin has a very low block generation rate, the best option according to a principled method is to increase its block generation rate. Additional improvements can be obtained by *decreasing* the block size and *further increasing* the block generation rate. This will not only increases throughput but also shortens the latency. Unfortunately, almost all the systems we looked at went in the opposite direction to increase the block size, partly due to a lack of principled methodology. The only exception is Etheruem; Etheruem's parameters are very close to the optimal ones recommended in Figure 5.3.

CHAPTER 6

Conclusion and Future Work

In this thesis, we have analyzed the Bitcoin backbone protocol and the Prism backbone protocol using more general models than previously seen in the literature. Under discrete-time model, 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 consequnce, 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 thesis provides explicit bounds for the Bitcoin and the Prism backbone protocols.

Under the continuous-time model, we rigorously establish the liveness and consistency properties of the Bitcoin blockchains. We also derive both upper bound and lower bound of confirmation time given a desired security level. Concrete latency–security trade-off for the Nakamoto consensus is derived and applied to analyze existing proof-of-work longest-chain cryptocurrencies.

When the mining rate is low (compared to the block propagation delay), the obtained upper bounds are close to the lower bounds from private mining. When the block

generation rate is high, however, our method does not give very tight results. Recent works [**14**, **15**] have established the tight fault tolerance under high mining rate but tight bounds on latency remain open. Another direction is to analyze the Nakamoto consensus with dynamic participation and/or difficulty adjustment. Only asymptotic bounds exist in this direction [**8**, **28**] and it is interesting future work to establish concrete latency–security bounds.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Available online: http://bitcoin.org/bitcoin.pdf*, 2008.

[2] "Countries suffering from rapid inflation show significant demand for cryptos." `https://news.bitcoin.com/countries-suffering-from-rapid-inflation-show-significant-demand-for-cryptos/`.

[3] "Market capitalization." `https://www.blockchain.com/charts/market-cap`.

[4] 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.

[5] A. Kiayias and G. Panagiotakos, "Speed-security tradeoffs in blockchain protocols.," *IACR Cryptology ePrint Archive*, vol. 2015, p. 1019, 2015.

[6] 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.

[7] 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.

[8] 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.

[9] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, "Prism: Deconstructing the blockchain to approach physical limits," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 585–602, 2019.

[10] L. Ren, "Analysis of nakamoto consensus," *IACR Cryptology ePrint Archive*, vol. 2019, p. 943, 2019.

[11] R. Pass and E. Shi, "Rethinking large-scale consensus," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pp. 115–129, IEEE, 2017.

[12] V. Bagaria, A. Dembo, S. Kannan, S. Oh, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni, "Proof-of-stake longest chain protocols: Security vs predictability," *arXiv preprint arXiv:1910.02218*, 2019.

[13] J. Niu, C. Feng, H. Dau, Y.-C. Huang, and J. Zhu, "Analysis of nakamoto consensus, revisited," *arXiv preprint arXiv:1910.08510*, 2019.

[14] A. Dembo, S. Kannan, E. N. Tas, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni, "Everything is a race and Nakamoto always wins," *The ACM Conference on Computer and Communications Security*, 2020.

[15] P. Gazi, A. Kiayias, and A. Russell, "Tight consistency bounds for bitcoin," *IACR Cryptology ePrint Archive*, vol. 2020, 2020.

[16] J. Li and D. Guo, "On analysis of the bitcoin and prism backbone protocols in synchronous networks," in *Proceedings of the 57th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2019.

[17] J. Li and D. Guo, "Liveness and consistency of bitcoin and prism blockchains: The non-lockstep synchronous case," in *IEEE International Conference on Blockchain and Cryptocurrency*, Online, 2020.

[18] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, pp. 1–10, IEEE, 2013.

[19] 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.

[20] 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.

[21] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Spectre: A fast and scalable cryptocurrency protocol.," *IACR Cryptology ePrint Archive*, vol. 2016, p. 1159, 2016.

[22] Y. Sompolinsky and A. Zohar, "Phantom," *IACR Cryptology ePrint Archive*, vol. 2018, p. 104, 2018.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] T. H. Chan, N. Ephraim, A. Marcedone, A. Morgan, R. Pass, and E. Shi, "Blockchain with varying number of players," 2017.

[29] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press, 2016.

[30] A. Sapirshtein, 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.

[31] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, 2014.

[32] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, "Deconstructing the blockchain to approach physical limits," *arXiv preprint arXiv:1810.08092*, 2018.

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

[34] M. N. Das, *Statistical methods and concepts*. New Age International, 1989.

[35] D. S. Stirling, *Mathematical analysis and proof*. Elsevier, 2009.

[36] R. Vershynin, *High-dimensional probability: An introduction with applications in data science*, vol. 47. Cambridge University Press, 2018.

[37] J. Li, D. Guo, and L. Ren, "Close latency–security trade-off for the nakamoto consensus," in *42nd IEEE Symposium on Security and Privacy*, submitted.

[38] "Propagation evolution." `http://bitcoinstats.com/network/propagation/`.

[39] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *International conference on financial cryptography and data security*, pp. 436–454, Springer, 2014.

[40] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, *et al.*, "On scaling decentralized blockchains," in *International conference on financial cryptography and data security*, pp. 106–125, Springer, 2016.

[41] A. E. Gencer, S. Basu, I. Eyal, R. Van Renesse, and E. G. Sirer, "Decentralization in bitcoin and ethereum networks," in *International Conference on Financial Cryptography and Data Security*, pp. 439–457, Springer, 2018.

[42] "Block propagation." `https://ethstats.net/`.

[43] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. bitcoin cash: Coexistence or downfall of bitcoin cash?," in *2019 IEEE Symposium on Security and Privacy*, pp. 935–951, 2019.

[44] "Bitcoin sv removes block sizes limits via its 'genesis' hard fork." `https://www.cryptoglobe.com/latest/2020/02/bitcoin-sv-removes-block-sizes-limits-via-its-genesis-hard-fork/`.

[45] "Litecoin mining: A helpful guide." `https://www.genesis-mining.com/litecoin-mining-guide`.

[46] "Zcash protocol specification." `https://github.com/zcash/zips/blob/b34edb5e4090e9abb20825a7891dba33d8a6ddb2/protocol/protocol.pdf`.

[47] "Network information." `https://z.cash/upgrade/`.

[48] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *2018 17th international symposium infoteh-jahorina*, pp. 1–6, IEEE, 2018.

[49] "Ethereum average block time chart." `https://etherscan.io/chart/blocktime`.