1 INTRODUCTION

1.1 Background

In 2008, Satoshi Nakamoto invented the concept of blockchains as a technology for maintaining decentralized ledgers [Nak08]. A core contribution of this work is the longest chain protocol, a deceptively simple consensus algorithm. Although invented in the context of Bitcoin and its Proof-of-Work (PoW) setting, the longest chain protocol has been adopted in many blockchain projects, as well as extended to other more energy-efficient settings such as Proof-of-Stake (PoS) (eg. [BPS16], [KRD017],[DGKR18],[BGK18],[FZ18]) and Proof-of-Space (PoSpace) (eg. [AAC17, CP19, PKF18]).

Used to maintain a ledger for a valued asset in a permissionless environment, the most important property of the longest chain protocol is its security; how much resource does an adversary need to attack the protocol and revert transactions already confirmed? Nakamoto analyzed this property by proposing a specific attack: the private double-spend attack (Figure 2(a)). The adversary grows a private chain of blocks in a race to outpace the public longest chain and thereby replacing it after a block in the public chain becomes k-deep. Let $\lambda_h$ and $\lambda_a$ be the rate at which the honest nodes and the adversary mine blocks, proportional to their respective hashing powers. Then it is clear from a law of large numbers argument that if $\lambda_a > \lambda_h$, then the adversary will succeed with high probability no matter how large k is. Conversely, if $\lambda_a < \lambda_h$, the probability of the adversary succeeding decreases exponentially with k. When there is a network delay of $\Delta$ between honest nodes, this condition for security becomes:

$$\lambda_a < \lambda_{growth}(\lambda_h, \Delta),$$  

(1)

where $\lambda_{growth}(\lambda_h, \Delta)$ is the growth rate of the honest chain under worst-case forking. In a fully decentralized setting with many honest nodes each having small mining power, [SZ15] calculates this to be $\lambda_{growth} = \lambda_h/(1 + \lambda_h \Delta)$. If we let $\beta$ to be the adversary fraction of power, then (1) yields the following condition:

$$\beta < \frac{1 - \beta}{1 + (1 - \beta) \Delta \lambda}.$$  

(2)

Here, $\lambda$ is the total mining rate, and $\lambda\Delta$ is the number of blocks mined per network delay. $1/(\Delta \lambda)$ is the block speed normalized by the network delay. Solving (2) at equality gives a security threshold $\beta_{pa}(\lambda\Delta)$. When $\lambda\Delta$ is small, $\beta_{pa}(\lambda\Delta) \approx 0.5$, and this leads to Nakamoto’s main claim in [Nak08]: the longest chain protocol is secure as long as the adversary has less than 50% of the total hashing power and the mining rate is set to be low. A more aggressive mining rate to speed up the blockchain reduces the security threshold. Hence (2) can be viewed as a tradeoff between security and block speed.

The private double-spend attack is a specific attack, and Nakamoto claimed security based on the analysis of this attack alone. But what about other attacks? Are there other worse attacks? A pertinent question after Nakamoto’s work is the identification of the true security threshold $\beta^*(\lambda\Delta)$ in the face of the worst attack. The groundbreaking work [GKL15] first addressed this question by formulating and performing a formal security analysis of the Poof-work longest chain protocol. They used a lock-step round-by-round synchronous model, and the analysis was later extended to the more realistic $\Delta$-synchronous model [PSS17]. The results show that when $\lambda\Delta \to 0$, indeed $\beta^*(\lambda\Delta) \to 50\%$, thus validating Nakamoto’s intuition. However, for $\lambda\Delta > 0$, there is a gap between their bounds and the private attack security threshold, and this gap grows when $\lambda\Delta$ grows.

1.2 Main contribution

The main contribution of this work is a new approach to the security analysis of longest chain protocols. This approach is driven by the question of whether the private attack is the worst attack for longest chain protocols in a broad sense. Applying this approach to analyze three classes of longest chain protocols in the $\Delta$-synchronous model [PSS17], we answer this question in the affirmative in all cases: the true security threshold is the same as the private attack threshold:

$$\beta^*(\lambda\Delta) = \beta_{pa}(\lambda\Delta) \quad \text{for all } \lambda\Delta \geq 0.$$  

(3)

(Figure 1). The three classes are: 1) the original Nakamoto PoW protocol; 2) Ouroboros Praos [DGKR18] and SnowWhite [PS17, BPS16] PoS protocols; 3) Chia PoSpace protocol [CP19]. They all use the longest chain rule but differ in how the lotteries for proposing blocks are run. (Figure 4) In the first two protocols, we close the

The authors are listed alphabetically. Amir Dembo and Ofer Zeitouni were partially supported by a US-Israel BSF grant.
winning the lottery. It was not known to be secure for (although the private attack threshold is smaller for Chia than for the other two classes of protocols due to the increased power of the adversary.)

The entire blocktree, consisting of both honest and adversary blocks, public or private, is particularly simple under a private attack: it can be partitioned into two chains, one honest and one adversary (Figure 2(a)). In contrast, under a general attack where the adversary can make public blocks at multiple time instances, a much more complex blocktree can emerge (Figure 2(b)). However, what we observe is that by partitioning this more complex tree into sub-trees, each rooted at a honest block and consisting otherwise entirely of adversary blocks, one can view the general attack as initiating multiple adversary sub-trees to race with a single fictitious chain consisting of only honest blocks (Figure 3). The growth rate of each of these adversary sub-trees is upper bounded by the growth rate of the adversary chain used in the private attack. Therefore, if the private attack is unsuccessful, we know that the growth rate of each of the adversary trees must be less than that of the fictitious honest chain. What we show, for each of the three classes of protocols, is that under that condition, there must exist honest blocks, which we call Nakamoto blocks, each having the property that none of the past adversary trees can ever catch up after the honest chain reaches the block. These Nakamoto blocks serve to stabilize the blockchain: when each such block enters the blocktree, complex as it may be, we are guaranteed that the entire prefix of the longest chain up to that block remains immutable in the future. When Nakamoto blocks occur and occur frequently, the persistence and liveness of the blockchain is guaranteed.

1.3 Related works
There have been several significant ideas that have emerged from the security analysis of blockchains in the past few years, and below we put our contribution in the perspective of these ideas. [GKL15] initiated blockchain security analysis through defining key backbone properties of chain common prefix, chain quality and chain growth. Applying this framework to analyse the PoW longest chain protocol in the lock-step round-by-round model, it is shown that the common prefix property, the most difficult property to analyze, is satisfied if the number of adversary blocks over a long window is less than the number of uniquely successful honest blocks. A similar block counting analysis is conducted by [PSS17] in the Δ- synchronous model, with the notion of uniquely successful blocks replaced by the notion of convergence opportunities. The resulting bound is tight when Δ is small but loose in general. Moreover, the block-counting technique completely breaks down for analyzing PoS longest chain protocols because of the notorious Nothing-at-Stake problem: winning one lottery can yield a very large number of blocks for the adversary. To overcome this

1Thus, Nakamoto blocks have a god-like permanence, they exist, but nobody knows which block is a Nakamoto block.

2Properties of the blocktree, independent of the content of the blocks.

3A uniquely successful honest block is one that is the only honest block mined in a round.
Figure 2: (a) Nakamoto’s private attack as a race between a single adversary chain and the honest chain. (b) By blocktree partitioning, a general attack is represented as multiple adversary chains simultaneously racing with a fictitious honest chain. Note that this fictitious chain is formed by only the honest blocks, and may not correspond to the longest chain in the actual system. However, the longest chain in the actual system must grow no slower than this fictitious chain.

Figure 3: Race between the adversary trees and the fictitious honest chain. While there may be multiple adversary trees simultaneously racing with the honest chain, the growth rate of each tree is bounded by the growth rate of the adversary chain in the private attack. An honest block is a Nakamoto block when all the previous adversary trees never catch up with the honest chain past that block.
issue, two new ideas were invented. In the Ouroboros line of work [KRDO17, DGKR18, BK+18], a new notion of forking strings was invented and a Markov chain analysis was performed to show convergence of the longest chain regardless of adversary action if the adversary stake is below a certain threshold. Sleepy Consensus and SnowWhite [PS17, BPS16] took a different approach and defined a notion of \textit{a pivot}, which is a time instance \( t \) such that in all time intervals around \( t \), there are more honest convergence opportunities than the number of adversary slots. They showed that a pivot forces convergence of the longest chain up to that time, and moreover if the adversary stake is less than a certain threshold, then these pivots must occur and they must occur often.

Despite this impressive stream of ideas, the true security threshold was still unknown for both the PoW and PoS longest chain protocols. Moreover, the analysis techniques seem very tied to the specific longest chain protocol under study. The definition of a pivot in [PS17], for example, is tied to the specific longest chain protocol, SnowWhite, they designed. In contrast, the notion of Nakamoto blocks in our approach can be viewed as a more general notion of pivots, but defined for general longest chain protocols and designed to tie the problem back to the private attack. Even though the analysis method in [PS17] has already evolved (or, shall we say, pivoted) from the analysis method in [GKL15], the influence of the block counting method is still felt in the definition of a pivot. We depart from this method by defining a Nakamoto block directly in terms of structural properties of the evolving blocktree itself. In fact, our approach was motivated from analyzing a protocol like Chia, where the rate of adversary winning slots grows exponentially over time and hence a condition like the one used in [PS17] does not give non-trivial bounds.

The present paper is an extension of an earlier version [BDK+19], where we introduced and applied this approach to analyze a PoS longest chain protocol [FZ18] similar to the Chia protocol. Since we released that early version, we became aware of an independent work [KQR20], which obtains the true security threshold as well as linear consistency for the Ouroboros Praos protocol in the lock-step round-by-round model. They achieved this by tightening the definition of a pivot in [PS17] to count all honest slots, including concurrent ones, not only uniquely successful ones. Like the original definition of pivots, however, this definition is tied to the specific protocol. The approach would not give non-trivial bounds for the Chia protocol, for example. Moreover, their result on the Praos protocol under the \( \Lambda \)-synchronous model is not tight (Figure 1(b)). We believe this is due to their analysis technique of mapping the \( \Lambda \)-synchronous model back to the lock-step round-by-round model. In contrast, our analysis is directly in the \( \Lambda \)-synchronous model and yields tight results in that model.

### 1.4 Outline

In Section 2, we introduce a unified model for all three classes of protocols. In Section 3, we introduce the central concepts of this work: blocktree partitioning and Nakamoto blocks. These concepts are applicable to any longest chain protocol. In Section 4, we use these concepts in the security analysis of the three classes of protocol attaining the private attack security threshold of each.

Section 5 we explore the question of whether the private attack is worst case in a stronger sense for longest chain protocols.

## 2 Models

A key goal of this paper is to provide a common framework to analyze the security properties of various longest chain protocols. We focus here primarily on the graph theoretic and the stochastic aspects of the problem: some resource-dependent randomness is utilized by these protocols to select which node is eligible to create a block. The modality in which the randomness is generated leads to different stochastic processes describing the blocktree growth. Understanding these stochastic processes and the ability of the adversary to manipulate these processes to its advantage is the primary focus of the paper.

Different longest chain protocols use different cryptographic means to generate the randomness needed. We specifically exclude here the cryptographic aspects of the protocols, whose analysis is necessary to guarantee the full security of these protocols. In most of the protocols we consider (for example [GKL15, KRDO17]), the cryptographic aspects have already been carefully studied in the original papers and are not the primary bottleneck. In others, further work may be necessary to guarantee the full cryptographic security. In all of these protocols, we assume ideal sources of randomness to create a model that can then be analyzed independently.

We will adopt a continuous-time model, following the tradition set by Nakamoto [Nak08] and also used in several subsequent influential works (eg. [SZ15]) as well as more recent works (eg. [Ren19]). The continuous-time model affords analytical simplicity and allows us to focus on the essence of the problem without being cluttered by too many parameters. Our model corresponds roughly to the \( \Lambda \)-synchronous network model introduced in [PSS17] in the limit of a large number of lottery rounds over the duration of the network delay. This assumption seems quite reasonable. For example, the total hash rate in today’s Bitcoin network is about 100 ExaHash/s, i.e. solving 10^24 puzzles per second. Nevertheless, we believe our results can be extended to the discrete setting.

We first explain the model in the specific context of Nakamoto’s Proof-of-Work longest chain protocol, and then generalize it to a unified model for all three classes of protocols we study in this paper.

### 2.1 Modeling proof-of-work longest chain

The blockchain is run on a network of \( n \) honest nodes and a set of malicious nodes. Each honest node mines blocks, adds them to the tip of the longest chain in its current view of the blocktree and broadcasts the blocks to other nodes. Malicious nodes also mine blocks, but they can be mined elsewhere on the blocktree, and they can also be made public at arbitrary times. Due to the memoryless nature of the puzzle solving and the fact that many attempts are tried per second, we model the block mining processes as Poisson with rates proportional to the hashing power of the miner.

Because of network delay, different nodes may have different views of the blockchain. Like the \( \Lambda \)-synchronous model in [PSS17], we assume there is a bounded communication delay \( \Delta \) seconds between the \( n \) honest nodes. We assume malicious nodes have zero communication delay among each other, and they can always act

---

4
in collusion, which in aggregate is referred as the adversary. Also
the adversary can delay the delivery of all broadcast blocks by up
to Λ time. Hence, the adversary has the ability to have one message
delivered to honest nodes at different times, all of which has to be
within Λ time of each other.

More formally, the evolution of the blockchain can be modeled
as a process \((T(t), C(t), T^p(t), C^p(t)) : t \geq 0, 1 \leq p \leq n\), \(n\)
being the number of honest miners, where:

- \(T(t)\) is a tree, and is interpreted as the mother tree consist-
ing of all the blocks that are mined by both the adversary
and the honest nodes up until time \(t\), including blocks that
are kept in private by the adversary and including blocks
that are mined by the honest nodes but not yet heard by
other honest nodes in the network.
- \(T^p(t)\) is an induced (public) sub-tree of the mother tree
\(T(t)\) in the view of the \(p\)-th honest node at time \(t\). It is
the collection of all the blocks that are mined by node \(p\) or
received from other nodes up to time \(t\).
- \(C^p(t)\) is a longest chain in the tree \(T^p(t)\), and is inter-
preted as the longest chain in the local view of the \(p\)-th
honest node on which it is mining at time \(t\). Let \(L^p(t)\)
denote the depth, i.e. the number of blocks in \(C^p(t)\) at
time \(t\).
- \(C(t)\) is the common prefix of all the local chains \(C^p(t)\) for
\(1 \leq p \leq n\).

The process evolution is as follows:

- **M0**: \(T(0) = T^p(0) = C^p(0) = 1 \leq p \leq n\) is a single root
block, the genesis block.
- **M1**: Adversary blocks are mined following a Poisson pro-
cess at rate \(\lambda_a\). When a block is mined by the adversary,
the mother tree \(T(t)\) is updated. The adversary can choose
which block in \(T(t)\) to be the parent of the adversary block
(i.e. the adversary can mine anywhere in the tree \(T(t)\).
- **M2**: Honest blocks are mined at a total rate of \(\lambda_h\) across
all the honest nodes. When a block is mined by the honest
node \(p\), the sub-tree \(T^p(t)\) and the longest chain \(C^p(t)\) is
updated. According to the longest chain rule, this honest
block is appended to the tip of \(C^p(t)\). The mother tree
\(T(t)\) is updated accordingly.
- **M3**: \(T^p(t)\) and \(C^p(t)\) can also be updated by the adver-
sary, in two ways: i) a block (whether is honest or adver-
sary) must be added to \(T^p(t)\) within time \(\Lambda\) once it has
appeared in \(T^p(t)\) for some \(q \neq p\), and the longest chain
\(C^p(t)\) is extended if the block is at its tip; ii) the adver-
sary can replace \(T^p(t^-)\) by another sub-tree \(T^p(t)\) from
\(T(t)\) as long as the new sub-tree \(T^p(t)\) is an induced sub-
tree of the new tree \(T^p(t)\), and can update \(C^p(t^-)\) to a
longest chain in \(T^p(t)\).

We highlight the capabilities of the adversary in this model:

- **A1**: Can choose to mine on any one block of the tree \(T(t)\)
at any time.
- **A2**: Can delay the communication of blocks between the
honest nodes, but no more than \(\Lambda\) time.

- **A3**: Can broadcast privately mined blocks at times of its
own choosing: when private blocks are made public at
time \(t\) to node \(p\), then these nodes are added to \(T^p(t^-)\) to
obtain \(T^p(t)\). Note that by property M3(i), when private
blocks appear in the view of some honest node \(p\), they will
also appear in the view of all other honest nodes by time
\(t + \Lambda\).
- **A4**: Can switch the \(p\)-th honest node’s mining from one
longest chain to another of equal length at any time, even
when its view of the tree does not change. In this case,
\(T^p(t) = T^p(t^-)\) but \(C^p(t) \neq C^p(t^-)\).

The question is on what information can the adversary base
in making these decisions? We will assume a very powerful non-
causal adversary which has full knowledge of all past and future
mining times of the honest blocks and the adversary blocks.

Proving the security (persistence and liveness) of the protocol
boils down to providing a guarantee that the chain \(C(t)\) converges
fast as \(t \to \infty\) and that honest blocks enter regularly into \(C(t)\)
regardless of the adversary’s strategy.

### 2.2 From PoW to a unified model

The model introduced in the last section can serve as a unified
model for all three classes of protocols we study in this paper. The
difference between these classes of protocols is how the lottery
in winning block proposal slots is conducted. This difference can
be encapsulated by changing only one modeling assumption: M1,
the assumption on the adversary mining process (Figure 4). In
particular, the assumption on the honest behavior (M2) remains
the same.

- **M1-PoW (Proof-of-Work)**: The original assumption we
already had: Adversary blocks are mined according to a
Poisson process at rate \(\lambda_a\), and the mined block can be
 appended to any parent block but only one, of the adversary’s
choosing, in the current mother tree \(T(t)\). This models the
random attempts at solving the hash puzzle on one of the
existing blocks.
- **M1-PS (Praos/SourceWhite Proof-of-Stake model)**: The
adversary blocks are mined\(^5\) according to a Poisson process
at rate \(\lambda_a\) (similar to PoW), but the adversary is allowed to
append a version of each mined block simultaneously at
all the blocks in the current tree \(T(t)\).
- **M1-Chia (Chia Proof-of-Space model)**: The adversary blocks
are mined according to multiple independent Poisson pro-
cesses of rate \(\lambda_a\), one at each block of the current tree
\(T(t)\). A new block is appended to the tree at a certain block when
a mining event happens.

Under M1-PoW, miners can only mine on one parent block at
a time, a consequence of conservation of work. Hence, the mined
block can only be appended to one of the parent blocks. In M1-PS
and M1-Chia, the adversary is able to mine new blocks on all
of the existing blocks of the blocktree. This is a consequence of the
phenomenon of **Nothing-at-stake**: the same resource (stake in PoS,

\[^5\]In these Proof-of-Stake protocols, block proposal slots are won by conducting lotteries
using the keys of the stake holders rather than by solving difficult computational
puzzles as in Proof-of-Work protocols. However, for convenience, we use the term
"mining" to denote the winning of any type of lotteries.
Figure 4: Three models for adversary block mining. In all models, adversary blocks are visualized as arriving via Poisson queues, and the focus is on how the block at the head of each queue is appended to the blocktree. In the PoW model, each adversary block can be appended to exactly one of the parent blocks of the existing blocktree. In the Ouroboros/SnowWhite model, each adversary block can be appended to all possible parent blocks. In the Chia PoSpace model, the adversary blocks are mined independently on the parent blocks of the existing tree.

We note that it may appear that the capability $A_1$ of the adversary (choosing where to mine), which is present in $M_1$-PoW, is gone under $M_1$-PS and $M_1$-Chia. However, the reason is that the adversary does not have to choose because it can mine everywhere simultaneously. Thus the adversary is actually more powerful under the $M_1$-PS and $M_1$-Chia conditions because the adversary has at its disposal much larger number of adversary blocks to attack the protocol. Somewhat surprisingly, our security threshold results show that this extra power is not useful in Ouroboros/SnowWhite but useful in Chia.

The modeling assumptions for these protocols will be justified in more details in the following two subsections. The reader who is comfortable with these assumptions can go directly to Section 3.

2.3 Ouroboros Praos and Snow White Proof-of-Stake model

This section shows how Ouroboros Praos [DGKR18] and Snow White [BPS16] Proof-of-Stake protocols can be modeled using assumption $M_1$-PS as mentioned earlier. Both of these are Proof-of-Stake protocols, which means nodes get selected to create blocks in proportion to the number of coins (=stake) that they hold rather than the computation power held by the nodes. While the two protocols are similar at the level required for the analysis here, for concreteness, we will describe here the relation with Ouroboros Praos, which can handle adaptive corruption of nodes.

We consider here only the static stake scenario - the stake of various nodes is fixed during the genesis block and assume that there is a single epoch (the composition of epochs into a dynamic stake protocol can be done using the original approach in [DGKR18]). The common randomness as well as the stake of various users is fixed at genesis (more generally, these are fixed at the beginning of each epoch for the entire duration of the epoch). For this protocol, we will assume that all nodes have a common clock (synchronous execution). At each time $t$, every node computes a verifiable random function (VRF) of the current time, the common randomness and the secret key. If the output value of the VRF is less than a certain threshold, then that node is allowed to propose a block at that time, to which it appends its signature. The key property of the VRF is that any node with knowledge only of the public key can validate that it was obtained with a node possessing the corresponding secret key. An honest node will follow the prescribed protocol and thus only create one block which it will append to the longest chain in its view. However, a winning dishonest node can create many different blocks mining on top of distinct chains. Blocks which are well-embedded into the longest-chain are considered confirmed.

Now, we explain the connection of the protocol to our modeling in the earlier section. The first assumption is that time is quantized so finely that the continuous time modeling makes sense - this assumes that there is no simultaneous mining at any time point. However, if nodes mine blocks close to each other in time, they can be forked due to the delay $\Delta$ in the propagation time (thus we model concurrent mining through the effect of the propagation delay rather than through discrete time). Second, the honest action is to grow the longest chain through mining a new block at the tip - this justifies $M_2$ (here $\lambda_h$ is proportional to the total honest stake). The adversaries can mine blocks which can be appended to many
different positions in the blockchain. We assume that in the worst case, every adversary arrival contributes to a block extending every single block in the tree. We note that furthermore, there is another action, which is that the adversary can create many different blocks at any given position of the blockchain. Since this action does not increase the length of any chain or increase future mining opportunities, we do not need to model this explicitly. However, we point out that, since we show that a certain prefix of the blockchain ending at a honest block remains fixed for all future, that statement continues to hold even under this expanded adversary action space.

2.4 Chia Proof-of-Space model

Chia consensus [CP19] incorporates a combination of Proof of Space (PoSpace) and Proof of time, and is another energy efficient alternative to Bitcoin. PoSpace [AAC17, DFKP15] is a cryptographic technique where provers can efficiently generate proofs to show that they allocate unused hard drive space for storage space. Proof of time is implemented by a Verifiable Delay Function (VDF) [BBBF18, Pie18] that requires a certain amount of sequential time is block time in Chia consensus would be there are $N$ puts a value that is uniformly distributed over its range. Suppose the depth of the block from Genesis) as follows:

$[PKF]$ing synchronized clocks as well as preventing long-range attacks than$)ing input, and produces a output $\tau$ $c$ $H$: this is because the hash function $H$ is a cryptographic hash function.

In Chia, each valid block $B$ contains a PoSpace $\sigma$ and a VDF output $\tau$. A Chia full node mines a new block ($B_i$, with $i$ denoting the depth of the block from Genesis) as follows:

1. It first picks the block $B_{i-1}$, at the tip of the longest chain in its local view of the blocktree, as the parent block that the newly generated block $B_i$ will be appended to.
2. It draws a challenge $c_i$ deterministically from $B_{i-1}$ and generates a valid PoSpace $\sigma_i$ based on $c_i$ and a large file of size at least $M$ bits it stores.
3. It computes a valid VDF output $t_i$ based on a challenge $c_i$ and a time parameter $t$, where $c_i$ is also drawn deterministically from $B_{i-1}$ and $t$ is the hash of $\sigma_i$ multiplied by a difficulty parameter $T$ (i.e. $t = 0.H(\sigma_i) \times T$ where $H$ is a cryptographic hash function).
4. A new block $B_i$ comprised of $\sigma_i$, $t_i$ and some payload (example: transactions) is appended to $B_{i-1}$ in the blocktree.

For each node, the “mining” time of a new block follows a uniform distribution in $(0, T)$: this is because the hash function $H$ outputs a value that is uniformly distributed over its range. Suppose there are $N$ full nodes in the Chia network, then the inter-arrival block time in Chia consensus would be $\min(U_1, U_2, \ldots, U_N)$, where $U_i \sim \text{Unif}(0, T)$ for $1 \leq i \leq N$. Then the expected inter-arrival block time is

$$E[\min(U_1, U_2, \ldots, U_N)] = \int_0^T (1 - t/T)^N dt = \frac{T}{N + 1}.$$ 

So to maintain a fixed inter-arrival block time (example: 10 minutes in Bitcoin), the difficulty parameter $T$ needs to be adjusted linearly as number of full nodes $N$ grows. We also observe that the chance for a node storing two large files each of size at least $M$ bits to find the first block is exactly doubled compared with a node storing one file, which provides Sybil resistance to Chia. Further we can model the mining process in Chia as a Poisson point process for large $N$. Fixing a parent block in the block tree, the number of new blocks mined in time $t$ follows a binomial distribution $\text{bin}(N, t/T)$, which approaches a Poisson distribution $\text{Poi}(Nt/T)$ when $N \rightarrow \infty$ and $N/t \rightarrow C$ for some constant $C$.

Assume there are $n$ honest nodes each controlling $M$ bits of space, and the adversary has $a \cdot M$ bits of space, then the mining processes of honest blocks and adversary blocks are Poisson point processes with rate $\lambda_h$ and $\lambda_a$ respectively, where $\lambda_h$ and $\lambda_a$ are proportional to total size of disk space controlled by honest nodes ($n \cdot M$) and the adversary ($a \cdot M$) respectively. Also while the honest nodes are following the longest chain rule, the adversary can work on multiple blocks or even all blocks in the block tree as a valid PoSpace is easy to generate and the adversary can compute an unlimited amount of VDF outputs in parallel; a similar phenomenon occurs in Proof-of-Stake blockchains where it is termed as the Nothing-at-Stake (NaS) attack [BDK+19]. Hence, we can model the adversary blocks as generated according to multiple independent Poisson processes of rate $\lambda_a$, one at each block of the current tree $T(t)$. A new block is appended to the tree at a certain block when a generation event happens. Like in the model for Ouroboros Proofs and Snow White, the total rate of adversary block generation increases as the tree grows; however the generation events across different blocks are independent rather than fully dependent.

3 BLOCKTREE PARTITIONING AND NAKAMOTO BLOCKS

In this section, we will introduce the concept of blocktree partitioning to represent a general adversary attack as a collection of adversary trees racing against a fictitious honest chain. Using this representation, we define the key notion of Nakamoto blocks as honest blocks that are the winners of the race against all the past trees, and show that if a block is a Nakamoto block, then the block will forever remain in the longest chain. The results in this section apply to all three models. In fact, they are valid for any assumption on the adversary mining process in $M1$ in the model in Section 2.1, because no statistical assumptions are made. In Section 4, we will perform security analysis in all three backbone models using the tool of Nakamoto blocks, by showing that they occur frequently with high probability whenever the adversary power is not sufficient to mount a successful private attack. This proves the liveness and persistency of the protocols.

First, we introduce the concept of blocktree partitioning and define Nakamoto blocks in the simpler case when $\Delta = 0$, and then we extend to general $\Delta$. The unrealistic but pedagogically useful zero-delay case allows us to focus on the capability of the adversary to mine and publish blocks, while the general case brings in its capability to delay the delivery of blocks by the honest nodes as well.
3.1 Network delay $\Delta = 0$

3.1.1 Blocktree partitioning

Let $r^h_i$ and $r^a_i$ be the mining time of the i-th honest and adversary blocks respectively; $r^h_0 = 0$ is the mining time of the genesis block, which we consider as the 0-th honest block.

**Definition 3.1. Blocktree partitioning** Given the mother tree $T(t)$, define for the i-th honest block $b_i$, the adversary tree $T_i(t)$ to be the sub-tree of the mother tree $T(t)$ rooted at $b_i$ and consists of all the adversary blocks that can be reached from $b_i$ without going through another honest block. The mother tree $T(t)$ is partitioned into sub-trees $T_0(t), T_1(t), \ldots T_j(t)$, where the j-th honest block is the last honest block that was mined before time $t$. See Figure 2(b) for an example.

The sub-tree $T_i(t)$ is born at time $r^h_i$ as a single block $b_i$ and then grows each time an adversary block is appended to a chain of adversary blocks from $b_i$. Let $D_i(t)$ denote the depth of $T_i(t)$; $D_i(r^h_i) = 0$.

3.1.2 Nakamoto blocks

Let $A_k(t)$ be the number of honest blocks mined from time 0 to $t$. $A_k(t)$ increases by 1 at each time $r^h_i$. We make the following important definition.

**Definition 3.2. (Nakamoto block for $\Delta = 0$)** Define

$$P^0_{ij} = \text{event that } D_i(t) < A_k(t) - A_k(r^h_i) \text{ for all } t > r^h_i$$

for some $i < j$. The j-th honest block is called a Nakamoto block if

$$P^0_j = \bigcap_{i=0}^{j-1} P^0_{ij}$$

occurs.

We can interpret the definition of a Nakamoto block in terms of a fictitious system, having the same block mining times as the actual system, where there is a growing chain consisting of only honest blocks and the adversary trees are racing against this honest chain. (Figure 3). The event $P^0_{ij}$ is the event that the adversary tree rooted at the i-th honest block does not catch with the fictitious honest chain any time after the mining of the j-th honest block. When the fictitious honest chain reaches a Nakamoto block, it has won the race against all adversary trees rooted at the past honest blocks.

Even though the events are about a fictitious system with a purely honest chain and the longest chain in the actual system may consist of a mixture of adversary and honest blocks, the actual chain can only grow faster than the fictitious honest chain, and so we have the following key lemma showing that a Nakamoto block will stabilize and remain in the actual chain forever.

**Lemma 3.1. (Nakamoto blocks stabilize, $\Delta = 0$)** If the j-th honest block is a Nakamoto block, then it will be in the longest chain $C(t)$ for all $t > r^h_j$. Equivalently, $C(r^h_j)$ will be a prefix of $C(t)$ for all $t > r^h_j$.

**Proof.** Note that although honest nodes may have different views of the longest chain because of the adversary capability $A_4$, $T^p(t) = T^q(t)$ and hence $L^p(t) = L^q(t)$ always hold for any $q \neq p$ at any time $t$ when $\Delta = 0$. Let $L(t)$ be the length of the longest chain in the view of honest nodes. $L(0) = 0$. Note that since the length of the chain $C^p(t)$ increments by 1 immediately at each honest block mining event (this is a consequence of $\Delta = 0$), it follows that for all i and for all $t > r^h_i$:

$$L(t) - L(r^h_i) \geq A_k(t) - A_k(r^h_i).$$

(6)

We now proceed to the proof of the lemma.

We will argue by contradiction. Suppose $F^0_j$ occurs and let $t^* > r^h_j$ be the smallest $t$ such that $C(t^j)$ is not a prefix of $C^p(t)$ for some $1 \leq p \leq n$. Let $b_i$ be the last honest block on $C^p(t^*)$ (which must exist, because the genesis block is by definition honest.) If $b_i$ is generated at some time $t_l > t^h_j$, then $C^p(t^*)$ is the prefix of $C^p(t^*)$ before block $b_i$, and does not contain $C(t^j)$ as a prefix, contradicting the minimality of $t^*$.

So $b_i$ must be generated before $t^h_j$, and hence $b_i$ is the i-th honest block for some $i < j$. The part of $C^p(t^*)$ after block $b_i$ must lie entirely in the adversary tree $T_i(t^*)$ rooted at $b_i$. Hence,

$$L(t^*) \leq L(r^h_i) + D_i(t^*)$$

However we know that

$$D_i(t^*) < A_k(t^*) - A_k(r^h_i) \leq L(t^*) - L(r^h_i),$$

(7)

where the first inequality follows from the fact that $F^0_j$ holds, and the second inequality follows from the longest chain policy (eqn. (6)). From this we obtain that

$$L(r^h_i) + D_i(t^*) < L(t^*)$$

(8)

which is a contradiction since $L(t^*) \leq L(r^h_i) + D_i(t^*)$. □

Lemma 3.1 justifies the name Nakamoto block: just like its namesake, a Nakamoto block has a godlike permanency. Also like its namesake, no one knows for sure whether a given block is a Nakamoto block: it is defined in terms of what happens in the indefinite future. However, the concept is useful because as long as a Nakamoto block appears in the last k blocks of the current longest chain, then the prefix before these k blocks will stabilize. Hence, the problem is reduced to showing under what conditions Nakamoto blocks exist and they enter the blockchain frequently.

Since Nakamoto blocks are defined in terms of a race between adversary trees and the honest chain, and the growth rate of each adversary tree is bounded by the growth rate of the private attack adversary chain no matter what the attack is, one can intuitively expect that if the private attack is not successful, i.e. the growth rate of the private adversary chain is less than that of the honest chain, then once in a while Nakamoto blocks will occur because the adversary trees cannot win all the time. This intuition is made precise in Section 4 for the three models of interest. The current task at hand is to extend the notion of Nakamoto blocks to the $\Delta > 0$ case.

3.2 General network delay $\Delta$

Definition 3.2 of a Nakamoto block is tailored for the zero network delay case. When the network delay $\Delta > 0$, there is forking in the
blockchain even without adversary blocks, and two complexities arise:

1. Even when a honest block $b$ has won the race against all the previous adversary trees, there can still be multiple honest blocks on the same level as $b$ in the mother tree $T(t)$ due to forking. Hence there is no guarantee that $b$ will remain in the longest chain.
2. Even when the honest block $b$ is the only block in its level, the condition in Equation (4) is not sufficient to guarantee the stabilization of $b$: the number of honest blocks mined is an over-estimation of the amount of growth in the honest chain due to forking.

The first complexity is a consequence of the fact that when the network delay is non-zero, the adversary has the additional power to delay delivery of honest blocks to create split view among the honest nodes. In the context of the formal security analysis of Nakamoto’s PoW protocol, the limit of this power is quantified by the notion of uniquely successful rounds in [GKL15] in the lock-step synchronous round-by-round model, and extended to the notion of convergence opportunities in [PPS17] in the $\Delta$-synchronous model. The honest blocks encountering the convergence opportunities are called loners in [Ren19].

**Definition 3.3.** The $j$-th honest block mined at time $t_i^j$ is called a loner if there are no other honest blocks mined in the time interval $[t_i^j - \Delta, t_i^j + \Delta]$.

It is shown in [PPS17, Ren19] that a loner must be the only honest block in its depth in $T(t)$ at any time $t$ after the block is mined. Thus, to deal with the first complexity, we simply strengthen the definition of a Nakamoto block to restrict it to also be a loner block. Since loner blocks occur frequently, this is not an onerous restriction.

To deal with the second complexity, we define the race of the adversary trees not against a fictitious honest chain without forking as in definition 3.2, but against a fictitious honest tree with worst-case forking. This tree is defined as follows.

**Definition 3.4.** Given honest block mining times $\tau_i^h$, define a honest fictitious tree $T_h(t)$ as a tree which evolves as follows:

1. $T_h(0)$ is the genesis block.
2. The first mined honest block and all honest blocks within $\Delta$ are all appended to the genesis block at their respective mining times to form the first level.
3. The next honest block mined and all honest blocks mined within time $\Delta$ of that are added to form the second level (which first level blocks are parents to which new blocks is immaterial).
4. The process repeats.

Let $D_h(t)$ be the depth of $T_h(t)$.

We are now ready to put everything together to define Nakamoto blocks in general.

**Definition 3.5.** (Nakamoto block for general $\Delta$) Let us define:

$E_{ij} = \text{event that } D_i(t) < D_h(t - \Delta) - D_h(\tau_i^h + \Delta) \text{ for all } t > \tau_i^h + \Delta. \quad (9)$

The $j$-th honest block is called a Nakamoto block if it is a loner and

$$F_j = \sum_{i=0}^{j-1} E_{ij} \quad (10)$$

occurs.

Note that when $\Delta = 0$, $D_h(t) = A_h(t)$, the number of honest blocks mined in $[0, t]$. Hence $E_{ij} = E_{ij}^0$. Also, every block is a loner. Here Definition 3.5 degenerates to Definition 3.2. Moreover, it is not difficult to see that

$$D_h(t - \Delta) - D_h(\tau_i^h + \Delta) \leq A_h(t) - A_h(\tau_i^h)$$

so Definition 3.5 is indeed a strengthening of Definition 3.2. This strengthening allows us to show that Nakamoto blocks stabilize for all $\Delta > 0$.

**Theorem 3.2. (Nakamoto blocks stabilize, general $\Delta$)** If the $j$-th honest block is a Nakamoto block, then it will be in the chain $C(t)$ for all $t > \tau_i^h + \Delta$. This implies that the longest chain until the $j$-th honest block has stabilized.

For the proof of the stabilization property of a Nakamoto block, it is crucial to show that $D_h(t)$ gives a conservative bound on the growth of the chains $C(t)$ from time $s$ to $t$. For this purpose, we prove the following proposition:

**Proposition 3.3.** For any given $s$, $t$ such that $s + \Delta < t - \Delta$,

$$D_h(t - \Delta) - D_h(s + \Delta) \leq L^P(t) - L^P(s)$$

for any honest miner $p$.

**Proof.** Assume that the increase in $L^P$ within the interval $[s, t]$ is solely due to the arrival of honest blocks to some miner in the interval $[s - \Delta, t]$. Then, we first show that delaying every block that arrives within this interval by $\Delta$ minimizes the increase in $L^P$ from $s$ to $t$ for any $t > s + \Delta$. To prove this, first observe that minimizing the increase in $L^P$ is equivalent to maximizing the time it takes for $C^P$ to reach any depth $d$. Now, let $h_i$ be the block at the tip of $C^P$ when it reaches depth $d$, and, assume that it took $\delta_i \leq \Delta$ time for $p$ to learn about $h_i$ after it was mined. Then, $C^P$ reaches depth $d$ at time $\tau_i^h + \delta_i$. However, if the message for $h_i$ was delayed for $\delta'_i > \delta_i$ time, then, either $C^P$ would have reached depth $d$ at time $\tau_i^h + \delta'_i \geq \tau_i^h + \delta_i$ with block $h_i$ at its tip, or, another block $h_j$, with index $j \neq i$ would have brought $C^P$ to depth $d$ at some time $t$, $\tau_i^h + \delta'_i > t > \tau_i^h + \delta_i$. Hence, delaying the transmission of $h_i$ increases the time it takes for $C^P$ to reach depth $d$. This implies that $h_i$ should be delayed as long as possible, which is $\Delta$. Since this argument also applies to any other block $h_j$ that might also bring $C^P$ to depth $d$ when $h_i$ is delayed, every block should be delayed by $\Delta$ to maximize the time for $C^P$ to reach any depth $d$. This, in turn, minimizes the increase in $L^P$ by any time $t > s$.

Next, define the following random variable:

$$L_{\max}(t) = \max_{p=1, \ldots, n} (L^P(t)).$$

Then, we can assert that:

$$L_{\max}(t - \Delta) \leq L^P(t) \leq L_{\max}(t)$$
for any honest miner $p$. Then,
\[
L^{(p)}(t) - L^{(p)}(s) \geq L_{\text{max}}(t - \Delta) - L_{\text{max}}(s).
\]

From the paragraph above, we know that delaying every honest block by $\Delta$ minimizes $L^{(p)}(t)$ for any $t$. Hence, this action also minimizes $L^{(p)}(t) - L^{(p)}(s)$ for any $t > s + 2\Delta$. Now, assume that no honest miner hears about any adversary block in the interval $[s, t]$ and every honest block is delayed by $\Delta$. Then, the difference $L_{\text{max}}(t - \Delta) - L_{\text{max}}(s)$ will be solely due to the honest blocks that arrive within the period $[s, t - \Delta]$. However, in this case, depth of $L_{\text{max}}$ changes via the same process as $D_h$ (when each miner has infinitesimal power), which implies the following inequality:
\[
L_{\text{max}}(t - \Delta) - L_{\text{max}}(s) \geq D_h(t - \Delta) - D_h(s + \Delta).
\]

Hence, we see that when every block is delayed by $\Delta$ and there are no adversary blocks heard by $p$ in the time interval $[s, t]$,
\[
L^{(p)}(t) - L^{(p)}(s) \geq D_h(t - \Delta) - D_h(s + \Delta).
\]

However, delaying honest blocks less than $\Delta$ time or the arrival of adversary blocks to $p$ in the period $[s, t]$ only increases the difference $L^{(p)}(t) - L^{(p)}(s)$. Consequently,
\[
D_h(t - \Delta) - D_h(s + \Delta) \leq L^{(p)}(t) - L^{(p)}(s)
\]
for any honest miner $p$.

Now we are ready to prove Theorem 3.2.

**Proof.** We prove that the $j$-th honest block will be included in any future chain $C(t)$ for $t > t_j^h + \Delta$, by contradiction. Suppose $\hat{F}_j$ occurs and let $t^* > t_j^h + \Delta$ be the smallest $t$ such that the $j$-th honest block is not contained in $C^{(p)}(t)$ for some $1 \leq p \leq n$. Let $h_i$ be the last honest block on $C^{(p)}(t^*)$, which must exist, because the genesis block is by definition honest. If $t_j^h > t_j^h + \Delta$ for $h_i$, then, $C^{(p)}(t_j^h)$ is the prefix of $C^{(p)}(t^*)$ before block $h_i$, and, does not contain the $j$-th honest block, contradicting the minimality of $t^*$. Therefore, $h_i$ must be mined before time $t_j^h + \Delta$. Since the $j$-th honest block is a loner, we further know that $h_i$ must be mined before time $t_j^h$, implying that $h_i$ is the $i$-th honest block for some $i < j$. In this case, part of $C^{(p)}(t^*)$ after block $h_i$ must lie entirely in the tree $T_i(t^*)$ rooted at $h_i$. Hence,
\[
L^{(p)}(t^*) \leq L^{(p)}(t_j^h) + D_i(t^*).
\]

However, we know that;
\[
D_i(t^*) < D_h(t^* - \Delta) - D_h(t_j^h + \Delta) \leq L^{(p)}(t^*) - L^{(p)}(t_j^h) \ 
\]
(12)
where the first inequality follows from the fact that $\hat{F}_j$ holds and the second inequality follows from proposition 3.3. From this we obtain that
\[
L^{(p)}(t_j^h) + D_i(t^*) < L^{(p)}(t^*) \ 
\]
(13)
which is a contradiction since $L^{(p)}(t^*) \leq L^{(p)}(t_j^h) + D_i(t^*)$. This concludes the proof.

- Nakamoto blocks are defined for general longest chain protocols. When applied to the Praos/SnowWhite protocols, the definition of Nakamoto blocks is a weakening of the definition of pivots in [PS17]. Although [PS17] did not define pivots explicitly in terms of races, one can re-interpret the definition as a race between the adversary and a fictitious honest chain consisting of only loner honest blocks. This fictitious chain can never occur in the actual system even when no adversary blocks are made public, because there are other honest blocks which are not loners but can make it into the main chain. On the other hand, Nakamoto blocks are defined directly as a race between the adversary and the fictitious honest chain which would arise if there were no public adversary blocks. This is why the definition of Nakamoto blocks leads to a tight characterization of the security threshold in the Praos/SnowWhite protocols, matching the private attack threshold, while the definition of pivots in [PS17] cannot. (Theorem 4.2). This tightening is similar to the tightening done in the recent work [KQR20] for the lock-step round-by-round model.

**4 SECURITY ANALYSIS**

The goal of this section is to show that the private attack is the worst attack for the three models defined in Section 2. More precisely, we want to show that security threshold, i.e. the maximum adversary power tolerable for any adversary strategy, is the same as that of Nakamoto’s private attack. This is true for any total mining rate $\lambda$ and for any $\Delta$. (In fact, the threshold depends only on the product $\lambda \Delta$.) We will use the notion of Nakamoto blocks to establish these results.

**4.1 Statement of results**

Our goal is to generate a transaction ledger that satisfies persistence and liveness as defined in [GKL15]. Together, persistence and liveness guarantee robust transaction ledger; honest transactions will be adopted to the ledger and be immutable.

**Definition 4.1 (from [GKL15]).** A protocol $\Pi$ maintains a robust public transaction ledger if it organizes the ledger as a blockchain of transactions and it satisfies the following two properties:

- **(Persistence)** Parameterized by $\tau \in \mathbb{R}$, if at a certain time a transaction $tx$ appears in a block which is mined more than $\tau$ time away from the mining time of the tip of the main chain of an honest node (such transaction will be called confirmed), then $tx$ will be confirmed by all honest nodes in the same position in the ledger.

- **(Liveness)** Parameterized by $u \in \mathbb{R}$, if a transaction $tx$ is received by all honest nodes for more than time $u$, then all honest nodes will contain $tx$ in the same place in the ledger forever.

As discussed in the introduction, the condition for the private attack on Nakamoto’s Proof-of-Work protocol to be successful is
\[
\lambda_a > \lambda_{\text{growth}}(\lambda_h, \Delta) = \frac{\lambda_h}{1 + \lambda_h \Delta}
\]
(14)
in the fully decentralized regime. In terms of $\beta$, the fraction of adversary power, and $\lambda$, the total block mining rate,
\[
\beta > \frac{1 - \beta}{1 + (1 - \beta) \lambda \Delta}
\]
(15)
The parameter $\lambda \Delta$ is the number of blocks generated per network delay, and determines the latency and throughput of the blockchain. If this condition is satisfied, then clearly the ledger does not have persistency or liveness. Hence, the above condition can be interpreted as a tradeoff between latency/throughput and the security (under private attack).

In the Praos/SnowWhite protocol, the honest growth rate is the same as in the PoW system. Consider now the adversary blocks. They are mined according to a Poisson process at rate $\lambda_a$. When a block is mined, the adversary gets to append that block to all the blocks in the current adversary chain (cf. Figure 4(b)). This leads to an exponential increase in the number of adversary blocks. However, the depth of that chain increases by exactly 1. Hence the growth of the adversary chain is exactly the same as the adversary chain under PoW. Hence, we get exactly the same private attack threshold (15) in both the PoW and the Praos/SnowWhite PoS protocols.

The theorem below shows that the the private attack threshold yields the true security threshold for both classes of protocols.

**Theorem 4.2.** If
\[
\beta < \frac{1 - \beta}{1 + (1 - \beta)\lambda \Delta}
\]  
then the Nakamoto PoW and the Ouroboros/SnowWhite PoS protocols generate transaction ledgers such that each transaction $tx^A$ satisfies persistence (parameterized by $\tau = \sigma$) and liveness (parameterized by $u = \sigma$) in Definition 4.1 with probability at least $1 - e^{-\Omega(\sigma^{1/\epsilon})}$, for any $\epsilon > 0$.

For the Chia Proof-of-Space model, the private attack is analyzed in [CP19, FZ18]. The growth rate of the private adversary chain is $e\lambda_a$. The magnification by a factor of $e$ is due to the Nothing-at-Stake nature of the protocol; more on that in Section 4.4.). Hence the condition for success for the private attack is:
\[
e\lambda_a > \frac{\lambda_h}{1 + \lambda \Delta\Lambda}
\]
in the fully decentralized setting. This implies the following condition on $\beta$, the adversary fraction of space resources:
\[
e\beta > \frac{1 - \beta}{1 + (1 - \beta)\lambda \Delta}
\]

For the Chia model, this threshold yields the true threshold as well.

**Theorem 4.3.** If
\[
e\beta < \frac{1 - \beta}{1 + (1 - \beta)\lambda \Delta}
\]  
then the Chia Proof-of-Space protocol generate transaction ledgers satisfying persistence (parameterized by $\tau = \sigma$) and liveness (parameterized by $u = \sigma$) in Definition 4.1 with probability at least $1 - e^{-\Omega(\sigma^{1/\epsilon})}$, for any $\epsilon > 0$.

The security thresholds for the different models are plotted in Figure 1, comparing to existing lower bounds in the literature.

### 4.2 Approach

To prove Theorems 4.2 and 4.3, we use the technique of Nakamoto blocks developed in Section 3. Theorem 3.2 states that Nakamoto blocks remain in the longest chain forever. The question is whether they exist and appear frequently regardless of the adversary strategy. If they do, then the protocol has liveness and persistency: honest transactions can enter the ledger frequently through the Nakamoto blocks, and once they enter, they remain at a fixed location in the ledger. More formally, we have the following result.

**Lemma 4.4.** Define $B_{s,s+t}$ as the event that there is no Nakamoto blocks in the time interval $[s, s + t]$. If
\[
P(B_{s,s+t}) < q_t < 1
\]  
for some $q_t$ independent of $s$ and the adversary strategy, then the protocol generates transaction ledgers satisfying persistence (parameterized by $\tau = \sigma$) and liveness (parameterized by $u = \sigma$) in Definition 4.1 with probability at least 1 $- q_a$.

The proof of Lemma 4.4 can be found in §D. This reduces the problem to that of bounding the probability that there are no Nakamoto blocks in a long duration. Here we follow a similar style of reasoning as in the analysis of occurrence of pivots in the Sleepy Consensus protocol [PS17]:

1. Show that the probability that the $j$-th honest block is a Nakamoto block is lower bounded by some $p > 0$ for all $j$ and for all adversary strategy, in the parameter regime when the private attack growth rate is less than the honest chain growth rate.

2. Bootstrap from (1) to bound the probability of the event $B_{s,t}$, an event of no occurrence of Nakamoto blocks for a long time.

Intuitively, if (1) holds, then one would expect that the chance that Nakamoto blocks do not occur over a long time is low, provided that a block being Nakamoto is close to independent of another block being Nakamoto if the mining times of the two blocks are far apart. We perform the bootstrapping by exploiting this fact for the various models under consideration.

In [PS17], the bootstrapping yields a bound $\exp(-\epsilon \sqrt{t})$ on $P(B_{s,s+t})$. By recursively applying the bootstrapping procedure, we are able to get a bound $\exp(-\Omega(1^\epsilon))$ on $P(B_{s,s+t})$, for any $\epsilon > 0$. We apply this general analysis strategy to the three models in the next two subsections.

### 4.3 Nakamoto PoW and Praos/SnowWhite PoS Models

This subsection is dedicated to proving Theorem 4.2. We will show that if
\[
\lambda_a < \frac{\lambda_h}{1 + \lambda \Delta\Lambda}
\]
then Nakamoto blocks occur frequently and regularly under both the PoW and the Praos/SnowWhite PoS models. Since the adversary in the Praos/SnowWhite PoS model is stronger, it suffices for us to prove the statement in that model.
As outlined in the section above, to prove theorem 4.2, we need to show that there exists constants \( A_r, a_r > 0 \) such that
\[
P(B_{s,t}) < A_r \exp(−a_r t^{1−\varepsilon})
\]
for all \( s, t > 0 \). In this context, we first establish that the probability of occurrence of a Nakamoto block is bounded away from 0.

**Lemma 4.5.** If
\[
\lambda_a < \frac{\lambda_h}{1 + \Delta \lambda_h},
\]
there exists a constant \( p > 0 \) such that the probability that the \( j \)-th honest block is a Nakamoto block is at least \( p \) for all \( j \).

We present a proof sketch below:

First, in the Praos/SnowWhite model, each arrival of an adversary block can increment the depth of each adversary tree by exactly one, although many copies of this block are mined. Hence, the adversary trees grow with the same rate as the adversary’s mining rate, namely \( \lambda_a \). Second, we observe that in the long run, the honest tree \( T_h \) grows with rate \( \lambda_h/(1 + \lambda_a \Delta) \). See Figure 3 for the relation between adversary trees and the honest tree. Then, if \( \lambda_a < \lambda_h/(1 + \lambda_a \Delta) \), the gap between the depths of the honest tree and an adversary tree is expected to increase over time. This implies that the adversary trees built on blocks far from the tip of the honest tree will fall behind and not be able to catch-up with the honest tree. Hence, in order to analyze the probability that the \( j \)-th honest block \( h_j \) is a Nakamoto block for any \( j \), it is sufficient to focus on the adversary trees that have been built on honest blocks immediately preceding \( h_j \). However, as there is only a small number of honest blocks immediately preceding \( h_j \), there is a non-zero probability that none of the adversary trees built on them will be able to catch-up with the honest tree. Hence, when \( \lambda_a < \lambda_h/(1 + \lambda_a \Delta) \), \( h_j \) becomes a Nakamoto block with non-zero probability for any \( j \).

The complete proof of Lemma 4.5 is given in §B.1 of the Appendix. An alternative proof, based on connecting the event of being a Nakamoto block to the event of a random walk never returning to the starting point, is presented in B.2 of the Appendix.

We next obtain a bound on \( P(B_{s,t}) \).

**Lemma 4.6.** If
\[
\lambda_a < \frac{\lambda_h}{1 + \Delta \lambda_h},
\]
then for any \( \varepsilon > 0 \), there exists constants \( a_r, A_r > 0 \), and \( \tilde{a}_r, \tilde{A}_r > 0 \) such that
\[
P(B_{s,t}) < A_r \exp(−a_r t^{1−\varepsilon}).
\]

Proof of Lemma 4.6 is given in §B.3 of the Appendix. Then combining Lemma 4.6 with Lemma 4.4 implies Theorem 4.2.

### 4.4 Chia Proof-of-Space Model

This subsection is dedicated to proving Theorem 4.3. We will show that if
\[
e\lambda_a < \frac{\lambda_h}{1 + \Delta \lambda_h}.
\]
then Nakamoto blocks occur frequently and regularly under the Chia Proof-of-Space model.

Since the occurrence of a Nakamoto block depends on whether the adversary trees from the previous honest blocks can catch up with the (fictional) honest tree, we next turn to an analysis of the growth rate of an adversary tree. Note that under assumption M1 – Chia, adversary blocks are mined at rate \( \lambda \) independently at each block of the mother tree \( T(t) \). Hence, each adversary tree \( T_\lambda(t) \) grows statistically in the same way (and independent of each other). Without loss of generality, let us focus on the adversary tree \( T_\lambda(t) \), rooted at genesis, is the tree \( T(t) \). The depth of the tree \( T_\lambda(t) \) is \( D_\lambda(t) \) and defined as the maximum depth of its blocks. The genesis block is always at depth 0 and hence \( T_\lambda(0) \) has depth zero.

With the machinery of branching random walks, we can show that the growth rate of depth of \( T_\lambda(t) \) is \( \varepsilon \lambda_a \) while the total number of adversary blocks in \( T_\lambda(t) \) grows exponentially with time \( t \). Hence, compared to the Praos/SnowWhite model we just analyzed, the growth rate of each adversary tree is magnified by a factor of \( \varepsilon \). Thus, the Nothing-at-Stake phenomenon is more significant in the Chia model compared to the Praos/SnowWhite model, due to the independence of mining opportunities at different blocks.

We will also need a tail bound on \( D_\lambda(t) \). While such estimates can be read from [Shi15], we bring instead a quantitative statement suited for our needs.

**Lemma 4.7.** For \( m \geq 1 \),
\[
P(D_\lambda(t) \geq m) \leq \left( \frac{e \lambda_a}{m} \right)^m.
\]

Details on the analysis of \( T_\lambda(t) \) and the proof of Lemma 4.7 are in §C.1 in the Appendix.

With Lemma 4.7, we show below that in the regime \( \varepsilon \lambda_a < \frac{\lambda_h}{1 + \Delta \lambda_h} \), Nakamoto blocks has a non-zero probability of occurrence.

**Lemma 4.8.** If
\[
e\lambda_a < \frac{\lambda_h}{1 + \Delta \lambda_h},
\]
then there is a \( p > 0 \) such that that probability the \( j \)-th honest block is a Nakamoto block is greater than \( p \) for all \( j \).

The proof of this result can be found in §C.2. Having established the fact that Nakamoto blocks occurs with non-zero frequency, we can bootstrap on Lemma 4.8 to get a bound on the probability that in a time interval \([s, s + t]\), there are no Nakamoto blocks, i.e. a bound on
\[
P(B_{s,t}) \leq \tilde{A}_2 \exp(−a_2 \tilde{V}_t).
\]

**Lemma 4.9.** If
\[
e\lambda_a < \frac{\lambda_h}{1 + \Delta \lambda_h},
\]
then there exist constants \( \tilde{a}_2, \tilde{A}_2 \) so that for all \( s, t \geq 0 \),
\[
P(B_{s,t}) \leq \tilde{A}_2 \exp(−\tilde{a}_2 \tilde{V}_t).
\]

The proof of this result can be found in §C.3. We can recursively bootstrap and get even better bounds.

**Lemma 4.10.** If
\[
e\lambda_a < \frac{\lambda_h}{1 + \Delta \lambda_h},
\]
then for any \( \varepsilon > 0 \) there exist constants \( \tilde{a}_r, \tilde{A}_r \) so that for all \( s, t \geq 0 \),
\[
P(B_{s,t}) \leq \tilde{A}_r \exp(−\tilde{a}_r t^{1−\varepsilon}).
\]

The proof of this result can be found in §C.4 in the Appendix. Then combining Lemma 4.10 with Lemma 4.4 implies Theorem 4.3.
5 DOES NAKAMOTO REALLY ALWAYS WIN?

We have shown that the threshold for the adversary power beyond which the private attack succeeds is in fact the tight threshold for the security of the three models M1-PoW, M1-PS and M1-Chia. However, security threshold is a statistical concept. Can we say that the private attack is the worst attack in a stronger, deterministic, sense?

Indeed, it turns out that one can, with a slight strengthening of the private attack, in a special case: the PoW model with network delay \( \Delta = 0 \). In this setting, we can indeed make a stronger statement.

In the PoW model, any attack strategy \( \pi \) consists of two components: where to place each new adversary arrival and when to release the adversary blocks. Consider a specific attack \( \pi_{SZ} \) the Sopolinsky and Zohar’s strategy of private attack with pre-mining [SZ16]. This attack focuses on a block \( b \): it builds up a private chain with the maximum lead over the public chain when block \( b \) is mined, and then starts a private attack from that lead. We have the following result.

**Theorem 5.1.** Let \( \tau_1^b, \tau_2^b, \ldots, \tau^n_b \) be a given sequence of mining times of the honest and adversary blocks. Let \( b \) be a specific block. (i) Suppose \( \pi \) violates the persistence of \( b \) with parameter \( k \), i.e. \( b \) leaves the longest chain after becoming \( k \)-deep. Then the \( \pi_{SZ} \) attack on \( b \) also forces \( b \) to leave the longest chain after becoming \( k \)-deep, under the same mining times. (ii) Suppose \( b \) is an honest block and \( \pi \) violates liveness for the \( k \) consecutive honest blocks starting with \( b \), i.e. none of the \( k \) consecutive honest blocks staying with \( b \) stay in the longest chain indefinitely. Then the \( \pi_{SZ} \) attack on \( b \) also forces these \( k \) consecutive honest blocks to leave the longest chain indefinitely under the same mining times.

The proof of 5.1 is given in §E.1 of the Appendix, together with a counter-example in the case of \( \Delta > 0 \).

In contrast to the PoW setting, a beautiful example from [Shi19] indicates that private attack is no longer the worst attack for every sequence of arrival times under the Praos/SnowWhite model, even for \( \Delta = 0 \). Figure 5 explains this example, and exhibits the blocktree partitioning for this example. With only \( 1/3 \) as many mining times opportunities to \( 2/3 \) for the honest players, the protocol can lose persistence. A private attack would not be able to accomplish the same, because the adversary has less mining opportunities than the honest nodes. This is somewhat surprising, given that the security threshold is \( 1/2 \) for this model (at \( \Delta = 0 \)). This also suggests that although the two settings, PoW and Praos/SnowWhite have identical security thresholds, their "true" worst case behaviors, taken over all mining time sequences, are different. The larger number of blocks available to the adversary in the Praos/SnowWhite protocol does have some effect in the true worst-case sense, and this allows the mounting of a more serious attack than a private attack. However, these are very atypical mining time sequences, and this difference does not show up in the security threshold.

So perhaps Nakamoto almost always wins.

![Figure 5](image_url)

**Figure 5:** On the top is the blocktree for the example above. Colors black and white represent adversary and honest blocks respectively. The mining time of each block is stated on it. On the bottom is the partition of the blocktree into honest blocks and adversary chains, verifying that indeed there are no Nakamoto blocks. The adversary mines two blocks every third mining time and gets two copies of it. By publishing the shallower block and keeping the deeper block in private and having the honest nodes mine on the shallower block, it can continue the balance attack indefinitely. This attacks relies on a periodic arrival pattern of the blocks. In a random environment, this pattern cannot hold indefinitely and the attack is not sustainable. So randomness saves Praos/SnowWhite.

**REFERENCES**

[AAC+17] Hamza Abusalah, Joël Abiven, Bram Cohen, Danylo Khilko, Krzysztof Pietrzak, and Leonid Reyzin. Beyond hellman’s time-memory trade-offs with applications to proofs of space. In International Conference on the Theory and Application of Cryptology and Information Security, pages 357–379. Springer, 2017.

[Aid13] Elie Aïdékon. Convergence in law of the minimum of a branching random walk. *The Annals of Probability*, 41(3A):1362–1426, 2013.

[BBBF18] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In Annual international cryptography conference, pages 757–788. Springer, 2018.

[BDK+19] Vivek Bagaria, Amir Dembo, Sreeram Kannan, Sewoong Oh, David Tse, Pramod Viswanath, Xuezhao Wang, and Ofer Zeitouni. Proof-of-stake longest chain protocols: Security vs predictability. arXiv preprint arXiv:1910.02218, 2019.

[BGK+18] Christian Badertscher, Peter Gazi, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ourboros genesis: Composable proof-of-stake blockchains with dynamic availability. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pages 913–930. ACM, 2018.

[BP16] Iddo Bentov, Rafael Pass, and Elaine Shi. Snow white: Provably secure proofs of stake. *IACR Cryptology ePrint Archive*, 2016:919, 2016.

[CP19] Bram Cohen and Krzysztof Pietrzak. The chia network blockchain. https://www.chia.net/assets/ChiaGreenPaper.pdf, 2019.

[DFKP15] Stefan Dziembowski, Sebastian Faust, Vladimir Koltunogorov, and Krzysztof Pietrzak. Proofs of space. In Annual Cryptology Conference, pages 585–605. Springer, 2015.

[DGKR18] Bernardo David, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Ourboros prao: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 66–98. Springer, 2018.

[Drm09] Michael Drmota. The height of increasing trees. *Annals of Combinatorics*, 12(4):373–402, 2009.

[FZ18] Lei Fan and Hong-Sheng Zhou. A scalable proof-of-stake blockchain in the open setting (or, how to mimic nakamoto’s design via proof-of-stake). 2018. Cryptology ePrint Archive, Report 2017/656, Version 20180425:201821.

[GKL15] Juan Guray, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Annual International Conference on
where $b$ can define the following catch up event: Let $D$ appear frequently in the analysis and provide some useful lemmas.

**LEMMA A.1.** For each $j$, 
\[
\hat{E}_j^c = E_j^c \cup U_j^c \cup \bigcup_{(i,k) \mid 0 \leq i < j < k} \hat{B}_{ik}^c \cup U_j^c.
\] (27)

**Proof.**
\[
U_j \cap E_{ij} = U_j \cap \{D_t(t) < D_h(t - \Delta) - D_h(t^h + \Delta) \text{ for all } t > t^h_j + \Delta\}
\]
\[
= U_j \cap \{D_t(t + \Delta) < D_h(t) - D_h(t^h + \Delta) \text{ for all } t > t^h_j\}
\]
\[
= U_j \cap \{D_t(t^h_j + \Delta) < D_h(t^h_j + \Delta) - D_h(t^h_j + \Delta) \text{ for all } k > j\}
\]
\[
= U_j \cap \{D_t(t^h_j + \Delta) < D_h(t^h_j - 1) - D_h(t^h_j + \Delta) \text{ for all } k > j\}
\]
Since $\hat{F}_j = F_j \cap U_j = \bigcap_{0 \leq i < j} E_{ij} \cap U_j$, by the definition of $\hat{B}_{ik}$ we have $\hat{F}_j = \left(\bigcap_{(i,k) \mid 0 \leq i < j < k} \hat{B}_{ik}^c\right) \cap U_j$. Taking complement on both sides, we can conclude the proof.

Finally, define the parameter $\tau$ as follows:
\[
\tau := \frac{1}{\lambda h} \left(1 + \Delta \lambda h\right),
\]
for which $\tau < 1$ holds whenever
\[
\lambda < \frac{\delta_h}{1 + \Delta \lambda h}.
\]

**B PROOFS FOR SECTION 4.3**
Notations used in this section are defined in §A.

**B.1 Proof for Lemma 4.5**
The proof relies on the following propositions.

**Proposition B.1.** Let $Y_d$, $d \geq 1$, be i.i.d random variables, exponentially distributed with rate $\lambda h$. Then, each random variable $X_d$ can be expressed as $\Lambda + Y_d$.

**Proof.** Let $h_1$ be the first block that comes to some depth $d - 1$ within $T_d$. Then, every honest block that arrives within the interval $[t^h_1, t^h + \Delta]$ will be mapped to the same depth as $h_1$, i.e. $d - 1$. Hence, $T_d$ will reach depth $d$ only when an honest block arrives after time $t^h + \Delta$. Now, we know that the difference between $t^h + \Delta$ and the arrival time of the first block after $t^h + \Delta$ is exponentially distributed with rate $\lambda h$ due to the memoryless property of the exponential distribution. This implies that for each depth $d$, $X_d$ is equal to $\Lambda + Y_d$ for some random variable $Y_d$ such that $Y_d$, $d \geq 1$, are i.i.d and exponentially distributed with rate $\lambda h$. Then, $X_d$ are also i.i.d random variables with mean $\Lambda + \frac{1}{\lambda h}$.

**Proportion B.2.** For any constant $a$,
\[
P\left(\sum_{d=a}^{n+a} X_d > n\left(\Lambda + \frac{1}{\lambda h}\right)(1 + \delta)\right) \leq e^{-n\Omega(\delta^2(1+\Delta\lambda_h)^2)}
\]

Proposition B.2 is proven using a Chernoff bound analysis and proposition B.1.
Proposition B.3. Probability that there are less than
\[ \frac{\lambda a(1 - \delta)}{\lambda_h} \]
arrival events from time \( t_0^h \) to \( h_{n+1}^* \) is upper bounded by;
\[ e^{-n\Omega(2\Delta / \lambda_h)} \]
Proposition B.3 is proven using the Poisson tail bounds.

Proposition B.4. Define \( B_n \) as the event that there are at least \( n \) adversary arrivals while \( D_h \) grows from depth 0 to \( n \):
\[ B_n = \{ \sum_{i=1}^{n} X_i \geq \sum_{i=0}^{n} \delta_i^n \} \]
If
\[ \lambda_a < \frac{\lambda_h}{1 + \lambda_a \Delta} \]
then,
\[ P(B_n) \leq e^{-A_0 n} \]
where,
\[ A_0 = s \Delta + \ln\left( \frac{\lambda a \lambda_h}{(\lambda_h - s)(\lambda_a + s)} \right) > 0 \]
and,
\[ s = \frac{\lambda_h - \lambda_a}{2} + \frac{2 - \sqrt{4 + 2\Delta(\lambda_a + \lambda_h)^2}}{2\Delta} \]
Proof is by using Chernoff bound, and, optimizing for the value of \( s \). It also uses proposition B.1.

We now proceed with the proof of lemma 4.5.

Proof. We first observe that \( (F_j \cap U_j) \text{ is the event that at least } b - a \text{ adversary arrival events have occurred during the time interval } [T_j, T_j + \Delta] \), \( h_j \) is a loner. \( P(F_j) \) happens if at least \( b - a \) adversary arrival events have occurred during the time interval \( [T_j, T_j + \Delta] \).

\[ P(F_j) = P(U_j) + P(F_j \cap U_j) \quad (28) \]
Now, since there exists a constant \( c_1 \) such that \( 0 < c_1 \leq P(U_j) \) for any \( j \), to prove the lemma, it is sufficient to find an upper bound \( c_2 \) on \( P(F_j \cap U_j) \) such that \( P(F_j \cap U_j) \leq c_1 < 2 \). Hence, from now on, we assume that \( h_j \) is a loner, and, \( F_j \) happens.

Note that the ‘catch-up’ event \( F_j \) implies the existence of a minimum time \( t_j \geq t_j^h + \Delta \) such that there exists an adversary tree \( T_j \) extending from some honest block \( h_i, i < j \), for which, the following holds:
\[ D(t_j) \geq D_h(t_j - \Delta) - D_h(t_j - h_i + \Delta) \]
Define \( l_j = D_h(t_j - h_i + \Delta) + D_h(t_j - \Delta) \), and, \( r_j = D_h(t_j - h_i + \Delta) \). Since \( D_h \) is monotonically increasing and \( t_j \geq t_j^h + \Delta \), and, \( D(t_j^h) < D(t_j^h) \) as \( h_j \) is a loner, \( r_j = D_h(t_j - h_i + \Delta) \geq D_h(t_j - h_i + \Delta) \) and, \( l_j = D_h(t_j - h_i + \Delta) \). Combining these facts, we infer that \( l_j \leq r_j \) for all \( j \). Consequently, at each depth within the interval \([l_j, r_j] \), there exists at least two blocks, at least one of which is an honest block in \( T_j \) and one of which is an attacker block in \( T_j \).

We next focus on the depth interval \([l_j, r_j] \), and, fix some constant and large integer \( B \). Let \( B_1 \) and \( B_2 \) be the disjoint events that the ‘catch-up’ event happens before and after depth \( d_j^h + B \)
\[ B_1 = \{ r_j > d_j^h + B \} \]
Let \( B_2 \) denote the event that there exists a time \( t \) such that \( D_l(t) \geq D_h(t - \Delta) - D_h(t - \Delta) \) and \( D_h(t - \Delta) \geq d_j^h + B \) for this \( t \). Let \( r_j^* = D_h(t - \Delta) \). Then, we observe that \( B_2 \cap B_2^c = B_2 \)

Using this, we can upper bound \( P(F_j \cap U_j) \) in the following way:
\[ P(F_j \cap U_j) = P(B_1) + P(B_2) \]
\[ = P(B_1) + P(B_2 \cap B_2^c) \]
\[ = P(B_1) + P(B_2)P(B_2^c) \]
\[ = P(B_1) + P(B_2^c)(1 - P(B_1)) \]
\[ \leq P(B_1) + P(B_2^c)(1 - P(B_1)) \]
Assume that \( P(B_1) < 1 \) for all \( j \). We will later prove that this is indeed true. Moreover, note that conditioning on \( B_2^c \) decreases the probability of the event \( B_2^c \) since, (i) \( B_2^c \) requires \( \ell_j \) to be behind \( T_h \) while \( T_h \) increases through depths \( d_j^h \) to \( d_j^h + B \). (ii) Given any initial depths for \( T_j \) and \( T_h \), catch-up events are ergodic. Then, proving that \( P(F_j \cap U_j) \) implies \( c_2 \) for some \( c_2 < 1 \) reduces to proving that \( P(B_2^c) \) \( c_2 \) for some \( c_2 < 1 \) for a fixed \( B \).

We next calculate an upper bound for \( P(B_2^c) \). For this purpose, we first define \( B_{a,b}^c \) as the event that at least \( b - a \) adversary arrival events have occurred during the time interval \([l_j, r_j] \). Via the ergodicity of the processes \( X_n \), using proposition B.4, we can write the following upper bound for \( P(B_{a,b}^c) \) for \( b - a \) sufficiently large:
\[ P(B_{a,b}^c) = P(\sum_{n=0}^{l_j} X_n = 2\Delta \geq \sum_{n=0}^{l_j} \delta_i^h) \leq A_21 e^{-A_0(b-a)} \]
where \( A_1 \) is a constant that is a function of \( \Delta \) and, \( A_0 \) is the constant given in proposition B.4. Now, \( B_2^c \) requires at least \( r_j - l_j \) adversary blocks to be mined at the tip of \( T_j \) from time \( t_j^h + \Delta \) until some time \( t - \Delta \), during which the depth of \( T_j \) grows by exactly \( r_j - l_j \). However, this is only possible if the adversary has at least \( r_j - l_j \) arrival events during this time interval. Hence, we can express \( B_2^c \) as a subset of the union of the events \( B_{a,b}^c \) in the following way:
\[ B_2^c \subseteq \bigcup_{a < d_j^h, b \geq d_j^h + B} B_{a,b}^c \]
Then, via union bound, its probability is upper bounded as shown below:
\[ P(B_2^c) \leq \sum_{a < d_j^h} \sum_{b \geq d_j^h + B} P(B_{a,b}^c) \]
\[ \leq A_21 e^{-A_0(b-a)+b} \]
\[ \leq A_1 \frac{1}{(1 - e^{-\Delta})^2} e^{-A_0(b-a)} \]
\[ = A_1 \frac{1}{(1 - e^{-\Delta})^2} e^{-A_0(b-a)} \]
Finally, for the $B$ fixed above, we prove that there exists a constant $c_3 < 1$ such that $P(B_1) < c_3$ for all $j$. Note that if $l_j \geq d_j^h - B$, there is a non-zero probability that no adversary block is mined from time $\tau_j^h$ to the time $B_k$ reaches depth $d_j^h + B$. Then there exists a constant $c_31 < 1$ such that $P(B_1 | l_j \geq d_j^h - B) \leq c_31$ for all $j$. On the other hand, if $l_j < d_j^h - B$, we know from the calculations above that

$$P(B_1 | l_j < d_j^h - B) \leq \frac{1}{(1 - e^{-\lambda_3 A})^2} e^{-\lambda_3 B}$$

for all $j$. We further know that, for the large $B$ fixed above, there exists a constant $c_4 < 1$ such that this expression is below $c_4$. Consequently, for any $j$,

$$P(B_1) \leq P(l_j \geq d_j^h - B) + (1 - P(l_j \geq d_j^h - B))c_4$$

(38)

$$\leq \max(c_31, c_4) = c_3 < 1$$

(39)

Then, for any $j$,

$$P(F_j^* | U_j) \leq c_3 + c_4(1 - c_3) < 1$$

This concludes the proof. \hfill \Box

### B.2 Alternative Proof of Lemma 4.5

This alternative proof is based on random walk theory.

**Proof.** We would like to lower bound the probability that the $j$-th honest block is a loner and $F_j^*$ happens. Since the $j$-th honest block is a loner with probability $e^{-2\lambda_3 A} > 0$ for all $j$, the probability that it is a Nakamoto block can be expressed as

$$P(F_j^* \mid \text{j-th honest block is a loner}) \cdot e^{-2\lambda_3 A}$$

Then, the proof is reduced to obtaining a lower bound on

$$P(F_j^* \mid \text{j-th honest block is a loner})$$

For this purpose, we assume that the $j$-th honest block is a loner, and, proceed to obtain a lower bound on the probability of the event $F_j^*$:

For any adversary tree $T_i$, $i < j$,

$$D_i(t) < D_h(t - \Delta) - D_h(\tau_j^h + \Delta)$$

for all times $t > \tau_j^h + \Delta$, which is equivalent to

$$D_i(t + \Delta) < D_h(t) - D_h(\tau_j^h + \Delta)$$

for all times $t > \tau_j^h$.

Let $U_j$ be the event that the $j$-th honest block is a loner. Let $G_j$ be the event that no adversary block is mined within the time period $[\tau_j^h, \tau_j^h + \Delta]$. Then, $P(G_j) = e^{-\lambda_3 A}$, and, we can lower bound $P(F_j^* \mid U_j)$ in the following way:

$$P(F_j^* \mid U_j) \geq P(F_j^* \cap G_j \mid U_j) = e^{-\lambda_3 A} P(F_j^* \mid U_j, G_j)$$

Since the events $G_j$, $j = 1, 2, ..$ are shift invariant, the probability $P(F_j^* \mid U_j, G_j)$ is equal to the probability of the following event $F_j^*$:

For any adversary tree $T_i$, $i < j$,

$$D_i(t) < D_h(t) - D_h(\tau_j^h + \Delta)$$

for all times $t > \tau_j^h$. Now, define $D'(t)$ as the depth of the deepest adversary tree at time $t$ for $t \geq \tau_j^h$:

$$D'(t) := \max_{0 \leq i < j} D_i(t) + D_h(\tau_j^h + \Delta)$$

Then, $F_j^*$ basically represents the event that $D'$ is behind $D_h$ for all times $t \geq \tau_j^h$.

We next express $F_j^*$ in terms of the following events:

$$E_1 := \{D'(\tau_j^h) < D_h(\tau_j^h)\}$$

$E_1$ is the event that the tip of the deepest adversary tree, $D'$, is behind the tip of the honest tree, $D_h$ at the arrival time of the $j$-th honest block.

$E_2$ is the event that $D_h(t) - D_h(\tau_j^h)$ is greater than the number of adversary arrivals during the time period $[\tau_j^h, t]$ for all $t, t > \tau_j^h$.

$E_3$ is the event that $D_h(\tau_j^h) - D_h(\tau_j^h + \Delta)$ is greater than the number of adversary arrivals during the time period $[\tau_j^h, \tau_j^h + \Delta]$ for all $i, 0 \leq i < j$.

We can now express $F_j^*$ in terms of $E_1$ and $E_2$:

$$E_1 \cap E_2 \subseteq F_j^*$$

Moreover, when a new adversary block is mined, depth of any of the trees $T_i, i < j$, increases by at most 1. Hence, $E_3$ implies that none of the trees $T_i, i < j$, has depth greater than or equal to $D_h(\tau_j^h)$ at time $\tau_j^h$. Consequently,

$$E_3 \subseteq E_1,$$

which further implies

$$E_3 \cap E_2 \subseteq F_j^*$$

Observing that $E_3$ and $E_2$ are independent events, we can express the probability of $F_j^*$ as:

$$P(F_j^*) \geq P(E_1) P(E_2)$$

Now, define $E_3'$ as the event that $D_h(t - \Delta) - D_h(\tau_j^h)$ is greater than the number of adversary arrivals during the time period $[\tau_j^h, t]$ for all $t, t > \tau_j^h + \Delta$. Let $G_j'$ be the event that there is no adversary arrival during the time interval $[\tau_j^h, \tau_j^h + \Delta]$. Observe that again, $P(G_j') = e^{-\lambda_3 A}$, and, the events $G_j', j = 1, 2, ..$ are shift invariant. Hence, we can do a similar trick as was done for the probabilities of $F_j$ and $G_j$ to obtain

$$P(E_3') \geq e^{-\lambda_3 A} P(E_3)$$

Since the increase times of $D_h$ and the inter-arrival times of adversary arrivals are i.i.d, the growth processes of $D_h$ and the number of adversary blocks are time reversible. Hence, probability of $E_3$ approaches that of $E_3'$ from above as $j \to \infty$. Then, for all $j$, we can write

$$P(F_j^*) \geq P(E_1) P(E_2) \geq P(E_3') P(E_2) \geq e^{-\lambda_3 A} P(E_2)^2$$

We now calculate the probability of the event $E_2$. To aid us in the calculation of $P(E_2)$, we construct a random walk $S[t]$. Here,
We first state the following lemma which will be used in the proof of Proposition 4.6. Recall that we have defined event \( B_i \) for all \( i \in [0, \ldots, p] \).

**Lemma B.5.** There exists a constant \( c > 0 \) such that

\[
P(\hat{B}_{ik}) \leq e^{-c(k-i-1)}
\]

**Proof.** We know from proposition B.3 that there are more than \((1-\delta)(k-i)\lambda_a/\lambda_h\) adversary arrival events in the time period \([t_i^h, t_k^h + \Delta]\) except with probability \(e^{-\Omega((k-i)\delta^2\lambda_a/\lambda_h)}\). Moreover, proposition B.4 states that

\[
P(\sum_{i=1}^{n} X_i \geq \sum_{i=0}^{n} \delta_{ij}) \leq e^{-A_0 n}
\]

for large \(n\). Then, using the union bound, we observe that for any fixed \(\delta\), probability of \(\hat{B}_{ik}\) when there are more than \((1-\delta)(k-i)\lambda_a/\lambda_h\) adversary arrival events in the time period \([t_i^h, t_k^h + \Delta]\) is upper bounded by the following expression:

\[
\frac{1}{1 - e^{-c_i}} e^{-C_i(k-i)}
\]

where

\[
C_1 = \frac{A_0(1-\delta)\lambda_a}{\lambda_h}.
\]

Hence,

\[
P(\hat{B}_{ik}) < \frac{1}{1 - e^{-c_i}} e^{-C_i(k-i)} + e^{-\Omega((k-i)\delta^2\lambda_a/\lambda_h)} \leq C_2 e^{-C_i(k-i)}
\]

for any \(k, i, k > i+1\), and appropriately chosen constants \(C_2, C_3 > 0\) as functions of the fixed \(\delta\). Finally, since \(P(\hat{B}_{ik})\) decreases as \(k-i\) grows and is smaller than 1 for all \(k > i + 1\), we obtain the desired inequality for a sufficiently small \(c \leq C_3\).

We can now proceed with the main proof.

We divide the proof in to two steps. In the first step, we prove for \(\varepsilon = 1/2\). By Lemma A.1, we have

\[
\hat{F}_j = F_j^c \cup U_j^c \subseteq \bigcup_{(i,k):i \neq j < k} \hat{B}_{ik} \cup U_j^c.
\]

Divide \([s, s + t]\) into \(\sqrt{t}\) sub-intervals of length \(\sqrt{t}\), so that the \(r\)th sub-interval is:

\[
J_r := [s + (r-1)\sqrt{t}, s + r\sqrt{t}].
\]

Now look at the first, fourth, seventh, etc sub-intervals, i.e. all the \(r = 1 \mod 3\) sub-intervals. Introduce the event that in the \(1\)st \(3\)th sub-interval, an adversary tree that is rooted at a honest block arriving in that sub-interval or in the previous (0 mod 3) sub-interval catches up with a honest block in that sub-interval or in the next (2 mod 3) sub-interval. Formally,

\[
C_{\ell} = \bigcup_{j: \ell \equiv 0 \mod 3} U_j^c \cup \bigcup_{i,k: i \neq j < k} J_r \cap \hat{B}_{ik}.
\]

Note that for distinct \(\ell\), the events \(C_{\ell}\)'s are independent. Also, we have

\[
P(C_{\ell}) \leq P(\text{no arrival in } J_{(\ell+1)}) + 1 - p < 1
\]

for large enough \(t\), where \(p\) is a uniform lower bound such that \(P(\hat{F}_j) \geq p\) for all \(j\) provided by Lemma 4.5.

Introduce the atypical events:

\[
\hat{B} = \bigcup_{(i,k): \ell \equiv 0 \mod 3} \hat{B}_{ik},
\]

and

\[
\hat{B} = \bigcup_{(i,k): \ell \equiv 0 \mod 3} \hat{B}_{ik}.
\]
The events $B$ and $\hat{B}$ are the events that an adversary tree catches up with an honest block far ahead. Then we have

$$P(B_{s+s+t}) \leq P\left( \bigcap_{j=1}^{\infty} U_j^{c} \right) + P(B) + P(\hat{B}) + \sum_{t=0}^{\sqrt{t}/3} C_t$$

$$= P\left( \bigcap_{j=1}^{\infty} U_j^{c} \right) + P(B) + P(\hat{B}) + (P(C_t))^{\sqrt{t}/3}$$

$$\leq e^{-c_2 t} + P(B) + P(\hat{B}) + (P(C_t))^{\sqrt{t}}$$

(43)

for some positive constant $c_2$ when $t$ is large, where the equality is due to independence. Next we will bound the atypical events $B$ and $\hat{B}$. Consider the following events

$$D_1 = \{ \#\{i:j_i^h \in (s-\sqrt{t} - \Delta, s + t + \sqrt{t} + \Delta)\} > 2\lambda_h t \}$$

$$D_2 = \{ \exists i,k: r_i^h \in (s+t,+t), (k-i) < \frac{\sqrt{t}}{2\lambda_h}, r_i^h - r_i^h + \Delta > \sqrt{t} \}$$

$$D_3 = \{ \exists i,k: r_i^h + \Delta \in (s+t,+t), (k-i) < \frac{\sqrt{t}}{2\lambda_h}, r_i^h - r_i^h + \Delta > \sqrt{t} \}$$

In words, $D_1$ is the event of atypically many honest arrivals in $(s-\sqrt{t} - \Delta, s + t + \sqrt{t} + \Delta)$ while $D_2$ and $D_3$ are the events that there exists an interval of length $\sqrt{t}$ with at least one endpoint inside $(s+t,+t)$ with atypically small number of arrivals. Since the number of honest arrivals in $(s+t,+t)$ is Poisson with parameter $\lambda_h t$, we have from the memoryless property of the Poisson process that $P(D_1) \leq e^{-c_3 t}$ for some constant $c_3 = c_0(\lambda_a, \lambda_h) > 0$ when $t$ is large. On the other hand, using the memoryless property and a union bound, and decreasing $c_0$ if needed, we have that $P(D_2) \leq e^{-c_0 \sqrt{t}}$.

Similarly, using time reversal, $P(D_3) \leq e^{-c_0 \sqrt{t}}$. Therefore, again using the memoryless property of the Poisson process,

$$P(B) \leq P(D_1 \cup D_2 \cup D_3) + P(B \cap D_1^c \cap D_2^c \cap D_3^c)$$

$$\leq e^{-c_0 t} + 2e^{-c_0 \sqrt{t}} + \sum_{t=1}^{2\lambda_h t} \sum_{k,k-i > \sqrt{t}/2\lambda_h} P(\hat{B}_{ik})$$

(44)

$$\leq e^{-c_3 \sqrt{t}}$$

(45)

for large $t$, where $c_3 > 0$ are constants that may depend on $\lambda_a, \lambda_h$ and the last inequality is due to Lemma B.5. We next claim that there exists a constant $\alpha > 0$ such that, for all $t$ large,

$$P(\hat{B}) \leq e^{-\alpha t}$$

(46)

Indeed, we have that

$$P(\hat{B}) = \sum_{i,k} \int_{0}^{s} P(\tau_i^h \in d\theta)P(\hat{B}_{ik}, \tau_i^h - \tau_i^h + \Delta > s + t - \theta)$$

$$\leq \sum_{i,k} \int_{0}^{s} P(\tau_i^h \in d\theta) \sum_{k,k-i > \sqrt{t}/2\lambda_h} P(\hat{B}_{ik})^{1/2} P(\tau_i^h - \tau_i^h + \Delta > s + t - \theta)^{1/2}$$

$$\leq \int_{0}^{s} P(\tau_i^h \in d\theta) e^{-\alpha(\tau_i^h - \tau_i^h + \Delta > s + t - \theta)}$$

(47)

The tails of the Poisson distribution yield the existence of constants $c, c' > 0$ so that

$$P(\tau_i^h - \tau_i^h + \Delta > s + t - \theta) \leq \left\{ \begin{array}{ll}
1, & (k-i) > c(s+t-\theta-\Delta) \\
e^{-c'(s+t-\theta-\Delta)}, & (k-i) \leq c(s+t-\theta-\Delta).
\end{array} \right.$$  

(48)

Lemma B.5 and (48) yield that there exists a constant $\alpha > 0$ so that

$$\sum_{k,k-i > \sqrt{t}/2\lambda_h} P(\hat{B}_{ik})^{1/2} P(\tau_i^h - \tau_i^h + \Delta > s + t - \theta)^{1/2} \leq e^{-2\alpha(s+t-\theta-\Delta)}$$

(49)

$$\sum_{k,k-i > \sqrt{t}/2\lambda_h} P(\hat{B}_{ik}) \leq \int_{0}^{s} e^{-2\alpha(s+t-\theta-\Delta)}d\theta \leq \frac{1}{2\alpha} e^{-2\alpha(s+t-\theta-\Delta)} \leq e^{-\alpha t}$$

(50)

Substituting this bound in (47) and using that $\sum_{i} P(\tau_i^h \in d\theta) = d\theta$ gives

for $t$ large, proving (46).

Combining (45), (51) and (43) concludes the proof of step 1.

In step two, we prove for any $\gamma > 0$ by recursively applying the bootstrapping procedure in step 1. Assume the following statement is true: for any $\theta \geq m$ there exist constants $\hat{a}_0, \hat{a}_0$ so that for all $s, t \geq 0$,

$$\hat{q}(s, s + t) \leq \hat{a}_0 \exp(-\hat{a}_0 t^{\theta - \Delta}).$$

(52)

By step 1, it holds for $m = 2$.

Divide $[s, s + t]$ into $\frac{m}{2\lambda_h}$ sub-intervals of length $\frac{m}{2\lambda_h}$, so that the $r$ th sub-interval is:

$$J_r := [s + (r-1)t, s + rt] \subseteq [s, s + t]$$

Now look at the first, fourth, seventh, etc sub-intervals, i.e. all the $r = 1 \mod 3$ sub-intervals. Introduce the event that in the $\ell$-th $1 \mod 3$th sub-interval, an adversary tree that is rooted at a honest block arriving in that sub-interval or in the previous $0 \mod 3$ sub-interval catches up with a honest block in that sub-interval or in the next $2 \mod 3$ sub-interval. Formally,

$$C_{\ell} = \bigcap_{j=1}^{t_{\ell+i}} U_j \bigcup_{j=1}^{t_{\ell+i}} \bigcup_{j=1}^{t_{\ell+i}} (i,k) \tau_i^h - \tau_i^h > \frac{m}{2\lambda_h}$$

Note that for distinct $\ell$, the events $C_{\ell}$ are independent. Also by (52), we have

$$P(C_{\ell}) \leq A_m \exp(-\hat{a}_m t^{1/2m-1})$$

(53)

Introduce the atypical events:

$$B = \bigcup_{(i,k) \tau_i^h \in [s, s+t]} \hat{B}_{ik}$$

and

$$\hat{B} = \bigcup_{(i,k) \tau_i^h \in [s, s+t]} \hat{B}_{ik}$$

The events $B$ and $\hat{B}$ are the events that an adversary tree catches up with an honest block far ahead. Following the calculations in
We first give a description of the (dual of the) adversary tree in

\[ m_k = \frac{\log \log k}{\log \log \log k} \]

is the appearance already in \[ \text{Pit94, Drm09} \], but we use here the standard

and thus

\[ \lim_{k \to \infty} m_k = 1 \]

for large \( t \), where \( c_1 \) and \( \alpha \) are some positive constant.

Then we have

\[ \tilde{q}(s, s + t) \leq P \left( \bigcup_{\ell=0}^{m_3-1} U_{j,\ell}^t \right) + P(B) + P(\hat{B}) + P \left( \bigcup_{\ell=0}^{m_3-1} C_{\ell} \right) \]

\[ \leq e^{-c_1 t \frac{m_3}{\log \log \log k}} + E \left( -\tilde{a}_m \frac{m_3}{\log \log \log k} \right) \]

\[ \leq \tilde{A}_m \exp \left( -\tilde{a}_m \frac{m_3}{\log \log \log k} \right) \]

(56)

for large \( t \), where \( \tilde{A}_m \) and \( \tilde{a}_m \) are some positive constant.

So we know the statement in (52) holds for all \( \theta \geq \frac{2m_3 - 1}{m_3} \). Start

with \( m_1 = 2 \), we have a recursion equation \( m_k = \frac{2m_3 - 1}{m_3} \) and we

know (52) holds for all \( \theta \geq m_k \). It is not hard to see that \( m_k \approx \frac{k+1}{k} \)

and therefore \( \lim_{k \to \infty} m_k = 1 \), which concludes the lemma.

C PROOFS FOR SECTION 4.4

Notations used in this section are defined in §A.

C.1 The adversary tree via branching random walks

We first give a description of the (dual of the) adversary tree in

\[ \text{terms of a Branching Random Walk (BRW). Such a representation}
\]

appears already in [Pit94, Drm09], but we use here the standard

language from, e.g., [Aid13, Shi15].

Consider the collection of \( k \) tuples of positive integers, \( I_k \)

\( = \{(i_1, \ldots, i_k)\} \), and set \( I = U_{k \geq 0} I_k \). We consider \( I \) as

labelling the vertices of a rooted infinite tree, with \( I_k \) labelling the vertices at generation \( k \) as follows: the vertex \( v = (i_1, \ldots, i_k) \in I_k \)

is the \( k \)-th child of vertex \( (i_1, \ldots, i_{k-1}) \) at level \( k - 1 \). An example

of labelling is given in Fig. 6. For such \( v \) we also let \( v' = (i_1, \ldots, i_j) \),

\( j = 1, \ldots, k \), denote the ancestor of \( v \) at level \( j \), with \( v^k = v \). For

notation convenience, we set \( v^0 = 0 \) as the root of the tree.

Next, let \( \{E_v\}_{v \in I} \) be an i.i.d. family of exponential random

variables of parameter \( \lambda_k \). For \( v = (i_1, \ldots, i_k) \in I_k \), let \( W_v = \sum_{j \leq k} E_{(i_1, \ldots, i_{j-1}, i_j)} \) and let \( S_v = \sum_{j \leq k} W_j \). This creates a labelled
tree, with the following interpretation: for \( v = (i_1, \ldots, i_j) \), the \( W_j \)

are the waiting for \( v^j \) to appear, measured from the appearance of \( v^j \), and \( S_v \) is the appearance time of \( v \). A moment thought

ought to convince the reader that the tree \( S_v \) is a description of the

adversary tree, sorted by depth.

Let \( S_k^* = \min_{v \in I_k} S_v \). Note that \( S_k^* \) is the time of appearance of

a block at level \( k \) and therefore we have

\[ \{D_0(t) \leq k \} = \{S_k^* \geq t\} \]

(57)

\( S_k^* \) is the minimum of a standard BRW. Introduce, for \( \theta < 0 \), the

moment generating function

\[ \Lambda(\theta) = \log \sum_{v \in I_1} E(e^{\theta S_v}) = \log \sum_{j=1}^{\infty} E(e^{\sum_{i=1}^{j} \theta E_i}) \]

\[ = \log \sum_{j=1}^{\infty} (E(e^{\theta E_1}))^j = \log \frac{E(e^{\theta E_1})}{1 - E(e^{\theta E_1})} \]

Due to the exponential law of \( E_1 \), \( E(e^{\theta E_1}) = \frac{\lambda - \theta}{\lambda - \theta} \) and therefore

\[ \Lambda(\theta) = \log \frac{\lambda}{\lambda - \theta} . \]

An important role is played by \( \theta^* = -e \lambda_a \), for which \( \Lambda(\theta^*) = -1 \)

\[ \sup_{\theta < 0} \left( \frac{\Lambda(\theta)}{\theta} \right) = \frac{\Lambda(\theta^*)}{\theta^*} = \frac{1}{\lambda_a e} = \frac{1}{|\theta^*|} . \]

Indeed, see e.g. [Shi15, Theorem 1.3], we have the following.

\[ \text{Lemma C.1.} \]

\[ \lim_{k \to \infty} S_k^*/k = \sup_{\theta < 0} \left( \frac{\Lambda(\theta)}{\theta} \right) = \frac{1}{|\theta^*|} , \text{ a.s.} \]

In fact, much more is known, see e.g. [HS09].

\[ \text{Lemma C.2. There exist explicit constants } c_1 > c_2 > 0 \text{ so that the sequence } S_k^* - k/\lambda \lambda_a e - c_1 \log k \text{ is tight, and} \]

\[ \lim \inf_{k \to \infty} S_k^* - k/\lambda \lambda_a e - c_2 \log k = \infty , \text{ a.s.} \]

Note that Lemmas C.1, C.2 and (57) imply in particular that

\[ D_0(t) \leq e \lambda_a t \text{ for all large } t, \text{ a.s., and also that} \]

\[ e \lambda_a > \lambda_h \text{ then } D_0(t) > \lambda_h t \text{ for all large } t, \text{ a.s.} \] (58)

With all these preparations, we can give a simple proof for

Lemma 4.7.

\[ \text{Proof.} \text{ We use a simple upper bound. Note that by (57),} \]

\[ P(D_0(t) \geq m) = P(S_m^* \leq t) \leq \sum_{v \in I_m} P(S_v \leq t) \]

(59)

For \( v = (i_1, \ldots, i_k) \), set \( |v| = i_1 + \cdots + i_k \). Then, we have that \( S_v \)

has the same law as \( \sum_{j=1}^{|v|} E_j \). Thus, by Chebycheff’s inequality, for \( v \in I_m \),

\[ P(S_v \leq t) \leq E(e^{\theta S_v}) e^{-\theta t} = \left( \frac{\lambda_e}{\lambda - \theta} \right)^{|v|} e^{-\theta t} . \] (60)
But
\[
\sum_{v \in \mathcal{I}_m} \left( \frac{\lambda_v}{\lambda_v - \theta} \right)^{|v|} = \sum_{i_1, \ldots, i_m \geq 1} \left( \frac{\lambda_a}{\lambda_a - \theta} \right)^{\sum_{j=1}^m i_j} = \left( \sum_{i \geq 1} \left( \frac{\lambda_a}{\lambda_a - \theta} \right)^i \right)^m = \left( \frac{\theta}{\lambda_a} \right)^{-m}. \tag{62}
\]
Combining (60), (61), we have
\[
P(D_0(t) \geq m) \leq \left( \frac{-\theta}{\lambda_a} \right)^{-m} e^{-\theta t},
\]
and optimizing over \( \theta \) we have when \( \theta = m/t \),
\[
P(D_0(t) \geq m) \leq \left( \frac{\epsilon \lambda_a t}{m} \right)^m.
\]
\( \square \)

### C.2 Proof of Lemma 4.8

In this proof, let \( r_k := \frac{\lambda_k}{T_k \lambda_k} \).

The random processes of interest start from time 0. To look at the system in stationarity, let us extend them to \( -\infty < t < \infty \). More specifically, define \( \tau_{i-1}^h, \tau_{i-1}^\ast, \ldots \) such that together with \( \tau_0^h, \tau_1^h, \ldots \), we have a double-sided infinite Poisson process of rate \( \lambda_k \). Also, for each \( i < 0 \), we define an independent copy of a random adversary tree \( T_i \) with the same distribution as \( T_0 \). And we extend the definition of \( T_0(t) \) and \( D_k(t) \) to \( t < 0 \): the last honest block mined at \( \tau_n^h < 0 \) and all honest blocks mined within \( (\tau_{i-1}^h - \Delta, \tau_i^h) \) appear in \( T_0(t) \) at their respective mining times to form the level \( -1 \), and the process repeats for level less than \( -1 \); let \( D_k(t) \) be the level of the last honest arrival before \( t \) in \( T_0(t) \), i.e., \( D_k(t) = \ell \) if \( \tau_i^h \leq t < \tau_{i+1}^h \) and the \( i \)-th honest block appears at level \( \ell \) of \( T_0(t) \).

These extensions allow us to extend the definition of \( E_{ij} \) to all \( i, j, -\infty < i < j < \infty \), and define \( \hat{E}_j \) and \( \tilde{E}_j \) to be:
\[
E_j = \bigcap_{i} E_{ij}
\]
and
\[
\hat{E}_j = E_j \cup U_j.
\]

Note that \( \hat{E}_j \subset \tilde{E}_j \), so to prove that \( \hat{E}_j \) has a probability bounded away from 0 for all \( j \), all we need is to prove that \( \tilde{E}_j \) has a non-zero probability.

Recall that we have defined the event \( \hat{B}_{ik} \) in §A as:
\[
\hat{B}_{ik} = \text{event that } D_k(\sum_{m=k}^{k-1} \sum_{n=1}^{\lambda_k} R_m + \Delta + \tau_i^h) \geq D_k(\tau_{i-1}^h) - D_k(\iota^h + \Delta).
\]

Following the idea in Lemma A.1, we have
\[
E_j \cap U_j = \bigcap_{i < j} E_{ij} \cap U_j = \bigcap_{i < j < k} \hat{B}^c_{ik} \cup U_j.
\]
Hence \( E_j \cap U_j \) has a time-invariant dependence on \( \{ Z_i \} \), which means that \( \rho = P(\hat{E}_j) \) does not depend on \( j \). Then we can just focus on \( P(\hat{E}_0) \). This is the last step to prove.

\[
P(\hat{E}_0) = P(E_0|U_0)P(U_0) = P(E_0|U_0)P(R_0 > \Delta)P(R_{-1} > \Delta) = e^{-2\lambda_h} P(E_0|U_0).
\]

It remains to show that \( P(E_0|U_0) > 0 \). We have
\[
E_0 = \text{event that } D_k(\sum_{m=1}^{k-1} \sum_{n=1}^{\lambda_k} R_m + \Delta + \tau_i^h) < D_k(\tau_{i-1}^h) - D_k(\iota^h + \Delta)
\]
for all \( k > 0 \) and \( i < 0 \), then
\[
E_0 = \bigcup_{k > 0, i < 0} \hat{B}_{ik}.
\]

Let us fix a particular \( n > 2\lambda_h \Delta > 0 \), and define:
\[
G_n = \text{event that } D_m(3n/\lambda_h + \tau_m^h) = 0
\]
for \( m = -n, -n+1, \ldots , -1, 0, +1, \ldots , n-1, n \).

Then
\[
P(E_0|U_0) \geq P(E_0|U_0, G_n)P(G_n|U_0)
\]
\[
= (1 - P(\cup_{k > 0, i < 0} \hat{B}_{ik}|U_0, G_n))P(G_n|U_0)
\]
\[
\geq (1 - \sum_{\ell > i, t < 0} P(\hat{B}_{ik}|U_0, G_n))P(G_n|U_0)
\]
\[
\geq (1 - a_n - \tilde{b}_n)P(G_n|U_0)
\]
where
\[
a_n := \sum_{(i,k) : -n < i < k < n} P(\hat{B}_{ik}|U_0, G_n)
\]
\[
\tilde{b}_n := \sum_{(i,k) : i < -n \text{ or } k > n} P(\hat{B}_{ik}|U_0, G_n).
\]

Using (23), we can bound \( P(\hat{B}_{ik}|U_0, G_n) \). Consider two cases:

**Case 1:** \( -n \leq i < 0 < k \leq n \):
\[
P(\hat{B}_{ik}|U_0, G_n) = P(\hat{B}_{ik}|U_0, G_n, \sum_{m=1}^{k-1} \sum_{n=1}^{\lambda_k} R_m + \Delta + \tau_i^h + \Delta)
\]
\[
+ P(\hat{B}_{ik}|U_0, G_n, \sum_{m=k}^{k-1} \sum_{n=1}^{\lambda_k} R_m + \Delta > 3n/\lambda_h)
\]
\[
\leq \sum_{m=1}^{k-1} \sum_{n=1}^{\lambda_k} P(R_m + \Delta > 3n/\lambda_h|U_0, G_n)
\]
\[
\leq \sum_{m=1}^{k-1} \sum_{n=1}^{\lambda_k} P(R_m > 5n/(2\lambda_h)|U_0)
\]
\[
\leq \sum_{m=1}^{k-1} \sum_{n=1}^{\lambda_k} P(R_m > 5n/(2\lambda_h))P(U_0)
\]
\[
\leq \sum_{m=1}^{k-1} \sum_{n=1}^{\lambda_k} A_1 e^{-\alpha_1 n}.
\]

for some positive constants \( A_1, \alpha_1 \) independent of \( n, k, i \). The last inequality follows from the fact that \( R_i \)'s are iid exponential random variables of mean \( 1/\lambda_k \). Summing these terms, we have:
\[
a_n = \sum_{(i,k) : -n \leq i < k \leq n} P(\hat{B}_{ik}|U_0, G_n)
\]
\[
\leq \sum_{(i,k) : -n \leq i < k \leq n} A_1 e^{-\alpha_1 n} := \bar{a}_n,
\]
which is bounded and moreover \( \bar{a}_n \to 0 \) as \( n \to \infty \).

**Case 2:** \( k > n \) or \( i < -n \):

For $0 < \epsilon < 1$, let us define event $W_{ik}^\epsilon$ to be:

$$W_{ik}^\epsilon = \text{event that } D_h(r_{i-1}^h) - D_h(r_i^h + \Delta) \geq (1 - \epsilon)\frac{r_h}{\lambda_h}(k - i - 1).$$

Then we have

$$P(\hat{B}_{ik}|U_0, G_n) \leq P(\hat{B}_{ik}|U_0, G_n, W_{ik}^\epsilon) + P(W_{ik}^\epsilon|U_0, G_n).$$

We first bound $P(W_{ik}^\epsilon|U_0, G_n)$:

$$P(W_{ik}^\epsilon|U_0, G_n) \leq P(W_{ik}^\epsilon|\tau_{k-1}^h - \tau_i^h - \Delta \leq \frac{k - i - 1}{1 + \epsilon}\lambda_h) + P(\tau_{k-1}^h - \tau_i^h - \Delta \leq \frac{k - i - 1}{1 + \epsilon}\lambda_h)
\leq P(W_{ik}^\epsilon|\tau_{k-1}^h - \tau_i^h - \Delta \leq \frac{k - i - 1}{1 + \epsilon}\lambda_h)
\leq e^{-\Omega(\epsilon^2(k - i - 1))} + e^{-\Omega(\epsilon^2(k - i - 1))}
\leq A_2e^{-a_2(k - i - 1)} \quad (69)$$

for some positive constants $A_2, a_2$ independent of $n, k, i$, where the second inequality follows from the Erlang tail bound and the third inequality follows from Proposition B.2.

Meanwhile, we have

$$P(\hat{B}_{ik}|U_0, G_n, W_{ik}^\epsilon)
\leq P(D_i \sum_{m=1}^{k-1} R_m + \Delta + \tau_i^h \geq (1 - \epsilon)\frac{r_h}{\lambda_h}(k - i - 1)|U_0, G_n, W_{ik}^\epsilon)
\leq P(D_i \sum_{m=1}^{k-1} R_m + \Delta + \tau_i^h \geq (1 - \epsilon)\frac{r_h}{\lambda_h}(k - i - 1)
\ub{U_0, G_n, W_{ik}^\epsilon})
\leq \frac{1}{\lambda_h} \left( \sum_{m=1}^{k-1} R_m + \Delta \leq (k - i - 1)\frac{r_h + \lambda a e}{2\lambda_h} \right)
\leq P(\tau_{k-1}^h - \tau_i^h - \Delta \leq \frac{k - i - 1}{1 + \epsilon}\lambda_h)
\leq e^{-\Omega(\epsilon^2(k - i - 1))} + e^{-\Omega(\epsilon^2(k - i - 1))}
\leq A_2e^{-a_2(k - i - 1)} \quad (70)$$

where the first term in the last inequality follows from (23), and the second term can also be bounded:

$$P(\tau_{k-1}^h - \tau_i^h - \Delta \leq \frac{k - i - 1}{1 + \epsilon}\lambda_h)
\leq \sum_{i=1}^{k-1} P(\tau_{k-1}^h - \tau_i^h - \Delta \leq \frac{k - i - 1}{1 + \epsilon}\lambda_h)
\leq A_2e^{-a_2(k - i - 1)} \quad (71)$$

for some positive constants $A_2, a_2$ independent of $n, k, i$. The last inequality follows from the fact that $(r_h + \lambda a e)/(2\lambda a e) > 1$ and the $R_i$’s have mean $1/\lambda_h$, while $P(U_0, W_{ik}^\epsilon)$ is an event with high probability as we showed in (69).

Then we have

$$P(\hat{B}_{ik}|U_0, G_n) \leq A_2e^{-a_2(k - i - 1)} \quad (72)$$

Summing these terms, we have:

$$b_n = \sum_{(i,k):i<n \text{ or } k>n} P(\hat{B}_{ik}|U_0, G_n)
\leq \sum_{(i,k):i<n \text{ or } k>n} A_2e^{-a_2(k - i - 1)}
+ \frac{r_h + \lambda a e}{2(1 - \epsilon)r_h} e^{-\Omega(\epsilon^2(k - i - 1))}
\leq \hat{b}_n$$

which is bounded and moreover $\hat{b}_n \to 0$ as $n \to \infty$ when we set $\epsilon$ to be small enough such that $\frac{r_h + \lambda a e}{2(1 - \epsilon)r_h} < 1$.

Substituting these bounds in (65) we finally get:

$$P(E_0|U_0) > 1 - (\hat{a}_n + \hat{b}_n)P(G_n|U_0) \quad (73)$$

By setting $n$ sufficiently large such that $\hat{a}_n$ and $\hat{b}_n$ are sufficiently small, we conclude that $P(E_0|U_0) > 0$.

### C.3 Proof of Lemma 4.9

Recall that we have defined event $\hat{B}_{ik}$ in §A as:

$$\hat{B}_{ik} = \text{event that } D_i(\sum_{m=1}^{k-1} R_m + \Delta + \tau_i^h) \geq D_h(r_{k-1}^h) - D_h(\tau_i^h + \Delta).$$

Note that from Lemma 4.8 and similar to inequality (70), we have $P(\hat{B}_{ik}) \leq e^{-c_i(k - i - 1)} \quad (74)$

for some positive constants $c_i$.

And by Lemma A.1, we have

$$\hat{P}_j^\epsilon = P_j^\epsilon \cup U_j^\epsilon = \left( \bigcup_{(i,k):i<j<k} \hat{B}_{ik} \right) \cup U_j^\epsilon. \quad (75)$$

Divide $[s, t] + t$ into $\sqrt{t}$ sub-intervals of length $\sqrt{t}$, so that the $r$ th sub-interval is:

$$J_r := [s + (r - 1)\sqrt{t}, s + r\sqrt{t}].$$

Now look at the first, fourth, seventh, etc sub-intervals, i.e. all the $r = 1 \mod 3$ sub-intervals. Introduce the event that in the $l$-th 1 mod 3th sub-interval, an adversary tree that is rooted at a honest block arriving in that sub-interval or in the previous (0 mod 3) sub-interval catches up with a honest block in that sub-interval or in the next (2 mod 3) sub-interval. Formally,

$$C_l = \bigcap_{j: r^\leq_h \in J_{l+1}} U_j^\epsilon \cup \left( \bigcup_{(i,k):i<j<k} \hat{B}_{ik} \right).$$

Note that for distinct $l$, the events $C_l$’s are independent. Also, we have $P(C_l) \leq P(\text{no arrival in } J_{l+1}) + 1 - p < 1 \quad (76)$
for large enough $t$, where $p$ is a uniform lower bound such that $P(\hat{F}_t) \geq p$ for all $j$ provided by Lemma 4.8.

Introduce the atypical events:

$$B = \bigcup_{(i,k): r^h_k \in [s,s+t]} B_{ik},$$

and

$$\tilde{B} = \bigcup_{(i,k): r^h_k < s, s+t < r^h_k + \Delta} \tilde{B}_{ik}.$$ 

The events $B$ and $\tilde{B}$ are the events that an adversary tree catches up with an honest block far ahead. Then we have

$$P(B_{k,s+t}) \leq P\left( \bigcap_{j:y_i,s+t} U_j^c \right) + P(B) + P\left( \bigcap_{t=0}^{\sqrt{t}/3} C_t \right) \leq P\left( \bigcap_{j:y_i,s+t} U_j^c \right) + P(B) + P\left( (C_t) \right)^{\sqrt{t}/3} \leq e^{-c_2 t} + P(B) + P(\tilde{B}) \leq e^{-c_2 t} + P(B) + (P(\tilde{B}) + P(C_t))^{\sqrt{t}/3} (75)$$

for some positive constant $c_2$ when $t$ is large, where the equality is due to independence. Next, we will bound the atypical events $B$ and $\tilde{B}$. Consider the following events:

$$D_1 = \{ \#(j: r^h_k \in (s - \sqrt{t} - \Delta, s + t - \sqrt{t} + \Delta)]) > 2\lambda_k t \}$$

$$D_2 = \{ \exists i, k: r^h_k \in (s, s+t), (k-i) < \frac{\sqrt{t}}{2\lambda_k}, r^h_k - r^h_i + \Delta > \sqrt{t} \}$$

$$D_3 = \{ \exists i, k: r^h_k + \Delta \in (s, s+t), (k-i) < \frac{\sqrt{t}}{2\lambda_k}, r^h_k - r^h_i + \Delta > \sqrt{t} \}$$

In words, $D_1$ is the event of atypically many honest arrivals in $(s - \sqrt{t} - \Delta, s + t - \sqrt{t} + \Delta)$ while $D_2$ and $D_3$ are the events that there exists an interval of length $\sqrt{t}$ with at least one endpoint inside $(s, s+t)$ with atypically small number of arrivals. Since the number of honest arrivals in $(s, s+t)$ is Poisson with parameter $\lambda_k t$, we have from the memoryless property of the Poisson process that $P(D_1) \leq e^{-c_0 t}$ for some constant $c_0 = c_0(\lambda_a, \lambda_k) > 0$ when $t$ is large. On the other hand, using the memoryless property and a union bound, and decreasing $c_0$ if needed, we have that $P(D_2) \leq e^{-c_0 t}\sqrt{t}$.

Similarly, using time reversal, $P(D_3) \leq e^{-c_0 \sqrt{t}}$. Therefore, again using the memoryless property of the Poisson process,

$$P(\tilde{B}) \leq P(D_1 \cup D_2 \cup D_3) \leq P(B \cap D_1^c \cap D_2^c \cap D_3^c) \leq e^{-c_0 t} + 2e^{-c_0 \sqrt{t}} + \sum_{i=1}^{2\lambda_k t} P(\tilde{B}_{ik}) \leq e^{-c_0 t} \sqrt{t}, (77)$$

for large $t$, where $c_0 > 0$ are constants that may depend on $\lambda_a, \lambda_k$ and the last inequality is due to (72). We next claim that there exists a constant $\alpha > 0$ such that, for all $t$ large,

$$P(\tilde{B}) \leq e^{-\alpha t}. (78)$$

Indeed, we have that

$$P(\tilde{B}) = \sum_{i=0}^{t} \int_0^t P(\tau^h_i \in d\theta)P(\tilde{B}_{ik}, \tau^h_i - \tau^h_k + \Delta > s + t - \theta) \leq \int_0^t P(\tau^h_i \in d\theta) \sum_{k: k > i} P(\tilde{B}_{ik})^{1/2}P(\tau^h_k - \tau^h_i - \Delta > s + t - \theta)^{1/2}. (79)$$

The tails of the Poisson distribution yield the existence of constants $c, c' > 0$ so that

$$P(\tau^h_k - \tau^h_i - \Delta > s + t - \theta) \leq e^{-c\theta} (s + t - \theta - \Delta), (80)$$

and

$$P(\tilde{B}_{ik})^{1/2} \leq e^{-c'\theta} (s + t - \theta - \Delta), (81)$$

Substituting this bound in (79) and using that $\sum_i P(\tau^h_i \in d\theta) = d\theta$ gives

$$P(\tilde{B}) \leq \int_0^t e^{-c\theta} (s + t - \theta - \Delta) \leq \frac{1}{2\alpha} e^{-c\theta} (s + t - \theta - \Delta), (82)$$

for $t$ large, proving (78).

Combining (77), (83) and (75) yields (24).

### C.4 Proof of Lemma 4.10

Assume the following statement is true: for any $\theta \geq m$ there exist constants $\bar{a}_m, \bar{A}_\theta$ so that for all $s, t \geq 0$,

$$\mathcal{G}[s, s+t] \leq \bar{A}_\theta \exp(-\bar{a}_m \theta). (84)$$

By Lemma 4.9, it holds for $m = 2$.

Divide $[s, s+t]$ into $t \mathcal{m}$ sub-intervals of length $t \mathcal{m}$, so that the $r$ th sub-interval is:

$$[s, s+t \mathcal{m}]: [s + (r-1)t \mathcal{m}, s + rt \mathcal{m}].$$

Now look at the first, fourth, seventh, etc sub-intervals, i.e. all the $r = 1 \mod 3$ sub-intervals. Introduce the event that in the $l$-th 1 mod 3 sub-interval, an adversary tree that is rooted at a honest block arriving in that sub-interval or in the previous (0 mod 3) sub-interval catches up with a honest block in that sub-interval or in the next (2 mod 3) sub-interval. Formally,

$$C'' = \bigcup_{j: r^h_k < s < r^h_k + \Delta \in [s + (r-1)t \mathcal{m}, s + rt \mathcal{m}]} U_j^c \bigcup_{i: r^h_i \in [s + (r-1)t \mathcal{m}, s + rt \mathcal{m}]} U_i^c \bigcup_{(i,k): r^h_k + \Delta < s < r^h_k + \Delta \in [s + (r-1)t \mathcal{m}, s + rt \mathcal{m}]} B_{ik}.$$ 

Note that for distinct $\ell$, the events $C''$'s are independent. Also by (84), we have

$$P(C'') \leq A_m \exp(-\bar{a}_m^{1/2m} - 1). (85)$$

22
Introduce the atypical events:

\[ B = \bigcup_{i,k} \tilde{B}_{ik}, \]

\[ \tilde{B} = \bigcup_{i,k} \tilde{B}_{ik}. \]

And the last block mined at time \( t \) is placed at the tip of chain \( \tau \).

The events \( B \) and \( \tilde{B} \) are the events that an adversary tree catches up with an honest block far ahead. Following the calculations in Lemma 4.9, we have

\[ P(B) \leq e^{-c_1t \frac{m-1}{3}} \quad \text{(86)} \]

\[ P(\tilde{B}) \leq e^{-\alpha t}. \quad \text{(87)} \]

for large \( t \), where \( c_1 \) and \( \alpha \) are some positive constant.

Then we have

\[ \tilde{q}(s,s+t) \leq P(\bigcup_{j: t^h_j \in [s,s+t]} U_j^f) + P(\tilde{B}) + P(B) + P(\bigcup_{t=0}^{t\frac{m-1}{3}} C_t). \]

\[ \leq e^{-c_1t} e^{-\alpha t} + e^{-c_1t \frac{m-1}{3}} + e^{-\alpha t} \]

\[ + (A_m \exp(-\hat{a}_t)) \frac{m-1}{3} \]

\[ \leq A'_m \exp(-\hat{a}_t \frac{m-1}{3}) \quad \text{(88)} \]

for large \( t \), where \( A'_m \) and \( \hat{a}_m \) are some positive constant.

So we know the statement in (84) holds for all \( \theta \geq \frac{2m-1}{m} \). Start with \( m_1 = 2 \), we have a recursion equation \( m_k = \frac{2m-k-1}{m-1} \) and we know (84) holds for all \( \theta \geq m_k \). It is not hard to see that \( m_k = \frac{k+1}{k} \) and thus \( \lim_{k \to \infty} m_k = 1 \), which concludes the lemma.

**D PROOF OF PERSISTENCE AND LIVENESS**

This subsection, we will prove Lemma 4.4. Our goal is to generate a transaction ledger that satisfies persistence and liveness as defined in section 4.1. Together, persistence and liveness guarantees robust transaction ledger [GKL15]; honest transactions will be adopted to the ledger and be immutable.

Proof. We first prove persistence by contradiction. For a chain \( C \) with the last block mined at time \( t \), let \( C_t^{[\sigma]} \) be the chain resulting from pruning a chain \( C_t \) up to \( \sigma \), by removing the last blocks at the end of the chain that were mined after time \( t - \sigma \). Note that \( C_t^{[\sigma]} \) is a prefix of \( C \), which we denote by \( C^{[\sigma]} \leq C \).

Let \( C_t \) denote the longest chain adopted by an honest node with the last block mined at time \( t \). Suppose there exists a longest chain \( C_t' \) adopted by some honest node with the last block mined at time \( t' > t \) and \( C_t'^{[\sigma]} \neq C_t^{[\sigma]} \). There are a number of honest blocks mined in the time interval \( [t-\sigma, t] \), each of which can be in \( C_t, C_t' \), or neither. We partition the set of honest blocks generated in that interval with three sets: \( \mathcal{H}_t \equiv \{ H_t \in C_t : t_j \in [t-\sigma, t] \}, \mathcal{H}_t' \equiv \{ H_t \in C_t' : t_j \in [t-\sigma, t] \}, \) and \( \mathcal{H}_{\text{rest}} \equiv \{ H_t \in C_t \cup C_t' : t_j \in [t-\sigma, t] \}, \) depending on which chain they belong to.

Then we claim that \( C_t^{[\sigma]} \neq C_t' \) implies that \( \tilde{t}_j^f \) holds for all \( j \) such that \( t_j \in [t-\sigma, t] \). This in turn implies that \( P(C_t^{[\sigma]} \neq C_t') \leq P(t_j \in [t-\sigma, t] | \tilde{t}_j^f \) ). However, we know that the probability of this happening is as low as \( q_\# \). This follows from the following facts.

(i) the honest blocks in \( C_t \) does not make it to the longest chain at happening time \( t' \); \( H_t \notin C_t' \) for all \( H_t \in \mathcal{H}_t \), which follows from \( C_t^{[\sigma]} \neq C_t' \).

(ii) the honest blocks in \( C_t \) does not make it to the longest chain \( C_t \) at time \( t' \); \( H_t \notin C_t' \) for all \( H_t \in \mathcal{H}_t \), which also follows from \( C_t^{[\sigma]} \neq C_t' \).

(iii) the rest of the honest blocks did not make it to either of the above: \( H_t \notin C_t \cup C_t' \) for all \( H_t \in \mathcal{H}_{\text{rest}} \).

We prove next liveness. Assume a transaction \( tx \) is received by all honest nodes at time \( t \), then we know that with probability at least \( 1 - q_\# \), there exists one honest block \( b_t \) mined at time \( t \) event \( \tilde{t}_j^f \) occurs, i.e., the block \( b_t \) and its ancestor blocks will be contained in any future longest chain. Therefore, \( tx \) must be contained in block \( b_t \) or one ancestor block of \( b_t \) since \( tx \) is seen by all honest nodes at time \( t' > t \). In either way, \( tx \) is stabilized forever. Thus, liveness holds.

**E PROOFS FOR SECTION 5**

**E.1 Proof of theorem 5.1**

Before presenting the proof for theorem 5.1, which covers the \( \Delta = 0 \) case, we first describe \( \pi_{SZ} \), Sompolinsky and Zohar’s strategy of private attack with pre-mining, focusing on some block \( b \). We know that if \( b = h_j \) is an honest block with index \( j \), it will be mined at the tip of the public longest chain \( C \) when \( \Delta = 0 \). In this case, \( \pi_{SZ} \) consists of two phases:

- **Pre-mining phase:** Starting from the genesis block, the attacker starts mining blocks in private to build a private chain. When the first honest block \( h_j \) is mined on the genesis block, the attacker does one of two things: i) If the private chain is longer than the public chain at that moment, then the adversary continues mining on the private chain; if the private chain is shorter than the public chain, the attacker abandons the private chain it has been mining on and starts a new private chain on \( h_j \) instead.

The attacker repeats this process with all honest blocks \( h_2, h_3, \ldots, h_{j-1} \).

- **Private attack phase:** After block \( h_{j-1} \) is mined, the attacker starts Nakamotoâ€”Zs private attack from the current private chain it is working on, whether it is off \( h_{j-1} \) or the one it has been working on before \( h_{j-1} \) depending on which is longer.

Note that it is possible for the adversary to attack one of its own blocks. In this case, \( b \) is placed at the tip of \( C \), and, kept private until an honest block \( h_{j-1} \) is mined at the same depth as \( b \). Then, the adversary denotes the chain including \( b \) as the longest chain for all honest miners. Hence, we can treat \( b \) as if it is an honest block with index \( j \), and, the strategy proceeds as described above for all other adversary blocks.

Having presented an algorithmic description for \( \pi_{SZ} \) above, we now identify certain features of \( \pi_{SZ} \), which will be used in the proof of theorem 5.1:
(1) All of the adversary blocks (except \(b\) when it is an adversary block) mined after the genesis block are placed at distinct depths in increasing order of their arrival times.

(2) If an adversary block (except \(b\) when it is an adversary block) arrives after an honest block \(h_i\) for \(i < j\), it is placed at a depth larger than the depth of \(h_j\).

(3) None of the paths from adversary blocks to the genesis includes block \(b\).

(4) No adversary block (except \(b\) when it is an adversary block) is revealed until the attack is successful.

We now proceed with the proof:

**Proof.** We first prove part (i) of the theorem, namely the fact that \(\pi_{SZ}\) is the worst-attack for preventing persistence with parameter \(k\). Consider a sequence of mining times for the honest and adversary blocks such that the persistence of \(b\) with parameter \(k\) is violated by an adversary following some arbitrary attack strategy \(\pi\). Let \(\tau_b\) be the mining time of block \(b\). Define \(t > \tau_b\) as the first time block \(b\) disappears from the public longest chain \(C\) after it becomes \(k\) deep within \(C\) at some previous time. We will prove this part of the theorem by showing that \(\pi_{SZ}\) also succeeds in removing \(b\) from \(C\) after it becomes \(k\) deep, for the same sequence of block mining times.

Let \(T\) be the blocktree built under \(\pi\), and observe that the public longest chain, \(C(t)\), contains block \(b\) at time \(t\). By our assumption, we know that at time \(t\), there exists a parallel chain \(C'\) with depth greater than or equal to the depth of \(b\) at time \(t\), and, \(C'\) does not include \(b\). Hence, it also does not include any of the blocks that came to \(C\) after \(b\). See Figure 7 for a visual example of the chains \(C\) and \(C'\). Let \(h_i\) be the last honest block in \(C'\) that is also on \(C\). Such a block \(h_i\) must exist; otherwise, these chains could not have grown from the same genesis block. Then, \(h_i\) has depth smaller than the depth of \(b\). In this context, let \(d_i^h\) and \(d_i^b\), \(d_i^h < d_i^b\), denote the depths of \(h_i\) and \(b\) respectively. Define \(H\) as the number of honest blocks mined in the time interval \((\tau_i^h, t]\), and observe that all of these honest blocks lay in the depth interval \([d_i^h, L(t)]\) of the blocktree \(T(t)\) as there can be no honest blocks at depths larger than \(L(t)\) at time \(t\).

Next, consider the portion of \(T(t)\) deeper than \(d_i^h\). Let \(d := L(t) - d_i^h\), and, define \(A\) as the number of adversary blocks mined in the time interval \((\tau_i^h, t]\). Note that since \(C\) and \(C'\) both include \(h_i\), the adversary blocks that are within these chains and have depths greater than \(d_i^h\) should have been mined after time \(\tau_i^h\). Now, as there can be at most one honest block at every depth due to \(\Delta = 0\); \(H \leq d\). Moreover, at each depth after \(d_i^h\), either \(C\) and \(C'\) have two distinct blocks, or, they share the same block, which by definition is an adversary block. Hence, the number of the adversary blocks that are within these chains and have depths greater than \(d_i^h\) is at least \(d\), which implies \(A \geq d\). Hence,

\[A \geq d \geq H.\]

Finally, we know from the definition of persistence that block \(b\) has been at least \(k\) deep in \(C\) before time \(t\), and, there are \(d_i^b - d_i^h\) blocks of distinct depths from \(h_i\) to \(b\). Consequently, \(d \geq (k - 1) + (d_i^b - d_i^h)\).

Figure 7 displays the interplay between these parameters in the context of an example attack.

We now consider an adversary that follows strategy \(\pi_{SZ}\). Again, let \(T^*\) be the blocktree built under \(\pi_{SZ}\), and, define \(d_i^b + d_i^h\) as the depths of the blocks \(h_i\) and \(b\) within \(T^*\). Let \(C^*\) denote the public longest chain under strategy \(\pi_{SZ}\). See Figure 8 for a visual example of the \(\pi_{SZ}\) attack. We next make the following observations using the properties of \(\pi_{SZ}\): Via property (2) of \(\pi_{SZ}\), every adversary block mined after time \(\tau_i^h\) is placed at a depth higher than \(d_i^h\). Via property (1), every one of these adversary blocks mined after time \(\tau_i^h\) is placed at a distinct depth. Hence, at time \(t\), the deepest adversary block has depth at least \(d_i^b + A\). Via property (3), the path from this deepest adversary block to the genesis does not include \(b\). Consequently, at time \(t\), the adversary following \(\pi_{SZ}\) has a private chain that does not include \(b\) and is at depth at least \(d_i^b + A\).

Finally, we observe via property (4) of \(\pi_{SZ}\) that \(C^*\) contains no adversary blocks (except \(b\) when it is an adversary block). Then, at time \(t > \tau_b\), \(C^*\) contains \(b\), and, it is exactly at depth \(L^*(t) = d_i^b + H\) as \(\Delta = 0\). Finally, to prove that the adversary succeeds under \(\pi_{SZ}\), we consider the following two cases:

- \(b\) is at least \(k\)-deep in \(C^*\) at time \(t\), i.e., \(L^*(t) \geq (k - 1) + d_i^b\). However, since the adversary has a private chain that does not include \(b\) and has depth at least \(d_i^b + A \geq d_i^b + H = L^*(t)\), the attack is successful.
• $b$ is not $k$-deep yet, i.e. $L^*(t) < (k - 1) + d_{h}^k$. (Figure 8 corresponds to this case.) However, the adversary has a private chain that does not include $b$ and is at depth at least,

$$d_{h}^k + A \geq d_{h}^b + d \geq (k - 1) + d_{b} + d_{h}^k - d_{h}^b.$$ Moreover, as $C^*$ does not contain any adversary blocks under $\pi_{SZ}$ (except $b$), $d_{b} - d_{h}^k \geq d_{h}^b - d_{h}^k$. Hence, $d_{h}^k + A \geq (k - 1) + d_{h}^b$, implying that the adversary would eventually succeed once $b$ becomes $k$-deep in $C^*$.

This concludes the proof of part (i) of the theorem.

Second, we prove part (ii) of the theorem, namely the fact that $\pi_{SZ}$ is the worst-attack for preventing liveness with parameter $k$.

Consider a sequence of mining times for the honest and adversary blocks such that the liveness of the $k$ consecutive honest blocks starting with $b$ is violated by an adversary following some arbitrary attack strategy $\pi$. Since $b$ is an honest block by assumption, let $b = h_j$ without loss of generality. For each of the $k$ consecutive honest blocks $h_m, m = j, \ldots, j + k - 1$; define $t_m \geq t_m^{h} = \tau_{\pi}^m$ as the first time block $h_m$ disappeared from the public longest chain $C$. Let $t^*$ denote the maximum of $t_m, m = j, \ldots, j + k - 1$. We will prove this part of the theorem by showing that $\pi_{SZ}$ also succeeds in removing each $h_m, m = j, \ldots, j + k - 1$ from $C$ by time $t^*$, for the sequence of block mining times.

Let $T$ be the blocktree built under $\pi$, and, observe that at time $t_m, (i)$ $C(t_m)$ contains the block $h_m$, (ii) there is a parallel chain $C_m$ with depth greater than or equal to $L(t_m)$, depth of $C$ at time $t_m$, and, $C_m$ does not include $h_m$. See Figure 9 for a visual example of the attack $\pi$. Let $e(m)$ be the index of the last honest block in $C_m$ that also on $C$. Such a block must exist for each $m$; otherwise, the chains $C_m$ could not have grown from the same genesis block. Let $d^e$ denote the minimum depth of the honest blocks $h_{e(m)}$:

$$d^e = \min_{m=j,\ldots,j+k-1} (d_{h}^{e(m)} < d_{h}^{j})$$

Let $e^*$ denote the index of the honest block at depth $d^e$. Define $H$ as the number of honest blocks mined in the time interval $(\tau_{h}^{e^*}, t^*)$, and observe that all of these honest blocks lay in the depth interval $(d^e, L(t^*))$ as there cannot be honest blocks at depths larger than $L(t^*)$ at time $t^*$.

Next, consider the portion of $T(t^*)$ deeper than $d^e$. Let $d := L(t^*) - d^e$, and, define $A$ as the number of adversary blocks mined in the time interval $(\tau_{h}^{e^*}, t^*)$. Note that all of the adversary blocks within the chains $C_m(t^*), m = j, \ldots, j + k - 1$, and $C(t^*)$ at time $t^*$ that lay in the depth interval $(d^e, L(t^*))$, should have been mined after time $\tau_{h}^{e^*}$. Hence, these adversary blocks constitute a subset of the adversary blocks mined in the time interval $(\tau_{h}^{e^*}, t^*)$. As there can be at most one honest block at every depth as $\Delta = 0, d \geq H$. Moreover, at each depth after $d^e = d_{h}^{e^*}$, for any given $m$, either $C$ and $C_m$ have two distinct blocks, or, they share the same block, which by definition is an adversary block. Hence, the number of the adversary blocks within the chains $C_m(t^*), m = j, \ldots, j + k - 1$, and $C(t^*)$ at time $t^*$ that lay in the depth interval $(d^e, L(t^*))$, is at least $d$, implying that $A \geq d$. Hence,

$$A \geq d \geq H.$$
there does not exist a sample path worst attack. This is shown by the following lemma:

**Lemma E.1.** Consider attacks for preventing the persistence, with some parameter k, of some block h_j, and, define the worst attack as the strategy π^* satisfying the following condition: If some strategy π ≠ π^* succeeds under a sequence of mining times, then π^* also succeeds under the same sequence except on a measure-zero set of sequences. Then, when Δ > 0, and, λ_a < λ_b/(1 + Δλ_h), there does not exist a worst attack.

**Proof.** Proof is by contradiction. First, let S_1 be the set of mining time sequences for the blocks preceding h_j such that h_j−1 is a loner, no adversary block is mined during the time interval [t^h_j−1, t^h_j], and, for any i, 0 ≤ i < j − 1, D_h^b(t^h_{j−1} − Δ) − D_h^p(t^h_j + Δ) is greater than the number of adversary arrivals during the time period [t^h_j−1, t^h_{j−1}]. (D_h^b was defined previously in section 3.2.) Note that since this is a necessary condition for h_j−1 to be a Nakamoto block, and, h_j−1 is a Nakamoto block with positive probability when λ_a < λ_b/(1 + Δλ_h), there exists a constant c > 0 such that P(S_1) ≥ c for all j.

Second, consider the following set of mining times for the next three blocks that arrive after h_j:

- Let h_{j+1}, and h_{j+2}' denote these blocks in order of their mining times.
- b is an adversary block and h_{j+1} is an honest block.
- Mining time of b satisfies the following equation:

\[ t^b_j < t^h_j < t^h_{j+1} + Δ. \]

- b' is mined after time t^h_{j+1} + Δ.

Now, depending on the mining time of t^h_{j+1}, we have two different sets of mining time sequences, S_2 and S_2'. The condition on h_{j+1} which differentiates these two sets is given below:

- S_2: \( t^h_{j+1} < t^h_j + Δ \)
- S_2': \( t^h_j + Δ < t^h_{j+1} \)

We next consider the sets S_1xS_2 and S_1xS_2'. For the sake of simplicity, let’s call any arbitrary sequence from S_1xS_2, sequence 1, and, any arbitrary sequence from S_1xS_2', sequence 2.

Now, for the sake of contradiction, assume that there exists a worst attack π^* that aims to prevent the persistence of block h_j. Consider an arbitrary sequence of mining times from the set S_1xS_2 ∪ S_1xS_2'. Via the definition of the set S_1, no matter what π^* does, the deepest adversary block at time t^h_j has depth smaller than t^h_{j+1}. Then, to prevent the persistence of h_j, π^* builds two parallel chains starting at block h_{j+1}, only one of which contains h_j. Let C be the chain containing h_j and let C' be the other parallel chain. It also delays the broadcast of block h_j by Δ so that if h_{j+1} is mined within Δ time of h_j, it is placed within the chain C', at the same depth as h_j. However, when block b is mined, there are two distinct actions that π^* might follow:

1. **Action 1:** Choose h_j as b's parent. Keep b private until at least time t^h_{j+1} + Δ.
2. **Action 2:** Choose h_{j+1} as b's parent. (Note that a worst attack will not mine b on a block preceding h_{j−1}.)

See Figure 11 for the effects of these actions on the blocktree under the sequences 1 and 2.

Now, assume that π^* follows action 1. Then, under sequence 1, the optimal behavior for π^* is to broadcast h_{j+1} before h_j becomes public at time t^h_j + Δ, and, to prompt the honest miners to keep mining on h_{j+1}. Then, C' becomes the public longest chain, and, the adversary can balance the chains C and C' in the future using the private block b. However, if π^* follows action 2, then, under sequence 1, C would not be leading C' via the private block, thus, making it harder for the adversary to maintain a balance between these two chains in the future. Hence, under sequence 1, for any sequence of mining times for the blocks after h_{j+1}, if π^* following action 2 prevents the persistence of block h_j, so does π^* following action 1. On the other hand, there exists a set S_3 of mining time sequences for the blocks after h_{j+1} such that P(S_3) > 0, and, under the sequences in S_3, following action 1 prevents the persistence of block h_j whereas following action 2 does not. Since P(S_1) ≥ c > 0 for all j, the set S_1xS_2xS_3 has positive probability. Consequently, the worst attack π^* does not follow action 2, implying that it follows action 1.
Next, observe that under sequence 2, \( h_{j+1} \) comes to a higher depth than \( h_j \). Hence, the optimal action for \( \pi^* \) under sequence 2 is to follow action 2 as it enables the adversary to extend \( C' \) by one block using \( b \). Action 1, on the other hand, does not help the adversary in its endeavor to maintain two parallel chains from block \( h_{j-1} \) as demonstrated by Figure 11. Then, under sequence 2, for any sequence of mining times for the blocks after \( h_{j+1} \), if \( \pi^* \) following action 1 prevents the persistence of block \( h_j \), so does \( \pi^* \) following action 2. On the other hand, there exists a set \( S'_3 \) of mining time sequences for the blocks after \( h_{j+1} \) such that \( P(S'_3) > 0 \), and, under the sequences in \( S'_3 \), following action 2 prevents the persistence of block \( h_j \) whereas following action 1 does not. Since \( P(S_1) \geq c > 0 \) for all \( j \), the set \( S_1 \times S'_2 \times S'_3 \) has positive probability. Consequently, the worst attack \( \pi^* \) does not follow action 1, implying that it follows action 2. However, this is a contradiction as the worst attack \( \pi^* \) can choose only one of the actions 1 and 2. Hence, there does not exist a worst attack \( \pi^* \).

\[ \square \]

Finally, via the lemma E.1, we observe that, for any given attack strategy \( \pi \), there exists a set of mining time sequences with positive probability (which can be very small) under which \( \pi \) is dominated by some other attack strategy. However, it is important to note that if we fix \( \Delta \) to be some finite value and \( \pi \) to be the private attack, probability of such atypical sets of mining time sequences go to zero as the parameter for persistence, \( k \), goes to infinity. This is because, as we have seen in the previous sections, the private attack is the worst attack in terms of achieving the security threshold.