Consistency in Proof-of-Stake Blockchains with Concurrent Honest Slot Leaders

Aggelos Kiayias[1,3], Saad Quader[2], and Alexander Russell[2,3]

[1]University of Edinburgh [2]University of Connecticut [3]IOHK

January 14, 2020

Abstract

We improve the fundamental security threshold of Proof-of-Stake (PoS) blockchain protocols, reflecting for the first time the positive effect of rounds with multiple honest leaders. Current analyses of the longest-chain rule in PoS blockchain protocols reduce consistency to the dynamics of an abstract, round-based block creation process that is determined by three probabilities:

- $p_{\mathtt{A}}$, the probability that a round has at least one adversarial leader;
- $p_{\mathtt{h}}$, the probability that a round has a single honest leader; and
- $p_{\mathtt{H}}$, the probability that a round has multiple, but honest, leaders.

We present a consistency analysis that achieves the optimal threshold $p_{\mathtt{h}} + p_{\mathtt{H}} > p_{\mathtt{A}}$. This is a first in the literature and can be applied to both the simple synchronous setting and the setting with bounded delays. Moreover, we achieve the optimal consistency error $e^{-\Theta(k)}$ where k is the confirmation time.

The consistency analyses in Ouroboros Praos (Eurocrypt 2018) and Genesis (CCS 2018) assume that the probability of a uniquely honest round exceeds that of the other two events combined (i.e., $p_{\mathtt{h}} - p_{\mathtt{H}} > p_{\mathtt{A}}$); the analyses in Sleepy Consensus (Asiacrypt 2017) and Snow White (Fin. Crypto 2019) assume that a uniquely honest round is more likely than an adversarial round (i.e., $p_{\mathtt{h}} > p_{\mathtt{A}}$). Thus existing analyses either incur a penalty for multiply honest rounds, or treat them neutrally. In addition, previous analyses completely break down when uniquely honest rounds become less frequent, i.e., $p_{\mathtt{h}} < p_{\mathtt{A}}$. Our new results can be directly applied to improve consistency of these existing protocols. We emphasize that these thresholds determine the critical tradeoff between honest majority, network delays, and consistency error.

We complement our results with a consistency analysis in the setting where uniquely honest slots are rare, event letting $p_{\mathtt{h}} = 0$, under the added assumption that honest players adopt a consistent chain selection rule. Our analysis provides a direct connection between the Ouroboros analysis by Blum et al. (SODA 2020) focusing on "relative margin" and the Sleepy consensus analysis focusing on "strong pivots."

1 Introduction

Proof-of-Stake (PoS) blockchain protocols have emerged as a viable alternative to resource-intensive Proof-of-Work (PoW) blockchain protocols such as Bitcoin and Ethereum. These PoS protocols are organized in rounds (which we call *slots* in this paper); their most critical algorithmic component is a leader election procedure which determines—for each slot—a subset of participants with the authority to add a block to the blockchain. Existing security analyses of these protocols are logically divided into two components: the first reasons about the properties of the leader election process, the second reasons about the combinatorial properties of the blockchains that can be produced by an *idealized* leader schedule in the face of adaptive adversarial control of some participants. An attractive side effect of this structure is that the combinatorial considerations can be treated independently of other aspects of the protocol. A recent article of Blum et al. [3] gave an axiomatic treatment of this combinatorial portion of the analysis which we extend in this paper.

These common combinatorial arguments can be formulated with very little information about the leader election process. Specifically, current analyses focus on three parameters:

- $p_{\mathtt{h}}$, the probability that a slot has a unique honest leader;
- $p_{\mathtt{H}}$, the probability that a slot has multiple, but honest, leaders; and
- $p_{\mathtt{A}}$, the probability that a slot has at least one adversarial leader.

Our major contribution is a generic, rigorous guarantee of consistency under the most desirable assumption[1] $p_{\mathtt{h}} + p_{\mathtt{H}} > p_{\mathtt{A}}$ that achieves optimal consistency error $\exp(-\Theta(k))$ as a function of confirmation time k. Our analysis can be directly applied to existing protocols to improve their consistency guarantees.

To contrast this with existing literature, the analysis of Ouroboros Praos [5] and Ouroboros Genesis [1] require the threshold assumption $p_{\mathtt{h}} - p_{\mathtt{H}} > p_{\mathtt{A}}$ to achieve the optimal consistency error of $e^{-\Theta(k)}$. Note how multiply honest slots actually *detract* from security, appearing negatively in the basic security threshold. The consistency analyses in Snow White [2] and Sleepy Consensus [12] assume an improved threshold $p_{\mathtt{h}} > p_{\mathtt{A}}$; however, they only establish a consistency error bound of $e^{-\Theta(\sqrt{k})}$. Note here that multiple honest slots appear neutrally. All existing analyses break down if $p_{\mathtt{h}} < p_{\mathtt{A}}$, i.e., when the uniquely honest slots are less probable than the adversarial slots.

Multiply-honest slots may arise by design, e.g., when each player checks privately whether he is a leader. They may also occur as a side-effect if the chain broadcast speed is relatively slow compared to the average chain growth rate in the network. The role of these slots is rather delicate: while it is good for the system to have many honest blocks, *concurrent* blocks can help the adversary in creating two long, diverging blockchains that might jeopardize the consistency property. Our new analysis shows that this second effect can be mitigated, achieving consistency error bound of $e^{-\Theta(k)}$ under the (tight) assumption $p_{\mathtt{h}} + p_{\mathtt{H}} > p_{\mathtt{A}}$.

Our results and contributions. As described above, we show for the first time that PoS blockchain protocols using the longest-chain rule can achieve a consistency error of $e^{-\Theta(k)}$ under the desirable condition $p_{\mathtt{h}} + p_{\mathtt{H}} > p_{\mathtt{A}}$. This improves the security guarantee of all "longest chain rule" PoS protocols such as Praos [5], Genesis [1], and Snow White [2] (we remark that other PoS protocols such as Algorand [10] operate in a different setting where explicit participation bounds are assumed and forks can be prevented). We discuss our results in more detail before turning to the model and proofs.

Our analysis in the simple synchronous model achieves the same asymptotic error bound as in [4]—the tightest result in the literature—under a much weaker assumption, namely $p_{\mathtt{h}} + p_{\mathtt{H}} > p_{\mathtt{A}}$. Thus PoS protocols can in fact achieve consistency with $0 < p_{\mathtt{h}} < p_{\mathtt{A}}$, a regime beyond reach of all previous analyses. When $p_{\mathtt{H}} = 0$ (i.e., all honest slots are in fact uniquely honest), we exactly recover the bound in [4]. Finally, when $p_{\mathtt{h}} \ll 1$ (i.e., when uniquely honest slots are rare), our bound has the right dependence on $p_{\mathtt{h}}$; in contrast, no existing analysis works in this regime.

Next, we consider a variant model where the honest players use a consistent tie-breaking rule when selecting the longest chain. (I.e., when a fixed set of blockchains of equal length are presented to a collection of honest players, they all select the same chain. In previous models, the adversary had the right to break such ties by influencing network delivery.) Assuming $p_{\mathtt{h}} + p_{\mathtt{H}} > p_{\mathtt{A}}$, we prove that the consistency error bound in this model is identical to the $e^{-\Theta(k)}$ bound in [4] *even when* $p_{\mathtt{h}} = 0$. No existing analysis survives in this regime.

Finally, we analyze the Δ-synchronous setting (i.e., all messages are delivered with at most a Δ delay) using the same general principle developed by the Praos analysis [5], achieving a consistency error probability of $e^{-\Theta(k)}$ in this setting as well. This analysis is presented in Section 7.

A technical overview. We initially work in the synchronous communication model and extend the synchronous combinatorial framework of [4] to accommodate multiply-honest slots. Many of the important constructs and

[1] Note that the case $p_{\mathtt{h}} + p_{\mathtt{H}} = p_{\mathtt{A}}$ leaves little room for consistency since in this case the adversary can create a private protocol execution identically distributed to that of the honest parties and by selectively disclosing it, it can break consistency. See [7] for more details on the necessity of an honest majority assumption.

proofs from their development break down, however: In particular, the critical notions of "relative margin" and "balanced forks" do not retain their direct significance in the multi-leader setting. Thus we need new tools with the right expressive properties.

Our analysis focuses on a combinatorial event called a "Catalan slot."[2] Catalan slots are honest slots c so that any interval containing c possesses strictly more honest slots—with any number of honest leaders—than adversarial ones. The analysis of [2] and [12] introduced this basic concept, though they counted only uniquely honest slots. In comparison with their analysis, then, our treatment has two important advantages: first of all, we let multiply honest slots count in the analysis and, additionally, we achieve strikingly stronger error bounds: specifically, we achieve optimal settlement error of $\exp(-\theta(k))$ rather then $\exp(-\theta(\sqrt{k}))$. Catalan slots are immediately connected to the notion of "relative margin" in [3]; more on this below.

A Catalan slot c acts as a barrier for the adversary in that if an honest blockchain from a slot $h < c$ is padded with adversarial blocks and presented to an honest observer at slot $c + 1$, the observer will never adopt this blockchain. As a result, the chains adopted by this honest observer must contain *some* block from slot c. Note that this is true *even if c is multiply-honest*.

A critical observation is that *a slot is Catalan if and only if all competitive blockhains in future slots, contain at least one block from this slot*. Thus if a Catalan slot c is uniquely honest, all blockchains that are eligible to be adopted by future honest players, must contain the (only) honest block issued from slot c. We call this the "Unique Vertex Property" (UVP). Note how the UVP is reminiscent of the "Common Prefix Property" (CP) in the literature.

This explains why both analyses produce similar bounds; we explore these connections in Section 9. In the analysis in [3], "balanced forks" and "relative margin" machinery act as a conduit between consistency violations and underlying stochastic process. The same role is played by the UVP and Catalan slots in this paper. In fact, UVP makes the characterization of consistency violations (and respective proofs) *much* simpler in comparison. This is a testament to the expressive power of Catalan slots in analyzing PoS dynamics.

With this in place, the major challenge is to bound the probability that Catalan slots are infrequent. Here we break away entirely from the analysis of [2] and approach the question using the theory of generating functions and stochastic dominance. We find an exact generating function for a related event and use this, by dominance, to control the undesirable event that a long window of slots is devoid of Catalan slots. This permits us to achieve asymptotically optimal settlement bounds.

Finally, it follows from the discussion above that if two consecutive slots are Catalan then any subsequent honest block must contain, in its prefix, a block from each of these slots. In a setting where all honest players use a consistent longest-chain selection rule, we show that both slots have UVP as well. Since Catalan slots can be multiply-honest, PoS protocols can achieve a consistency error bound of $e^{-\Theta(k)}$ in this model even if $p_{\mathrm{h}} = 0$. Recall that no existing analysis can handle this parameter regime.

Consistency violations and PoS dynamics. The analysis in [3] characterizes PoS dynamics via a non-simple biased random walk (called the *relative margin walk*) on integers; specifically, the walk may stick at zero from time to time. This was in contrast with the PoW setting where the dynamics is captured by a simple random walk; see [11, 8, 6]. However, we argue that the distinction between the PoS and the PoW dynamics stems *not* from the intricacy of the random walks involved, but rather from the relevant combinatorial events defined on those walks. Specifically, in the present analysis, we have a simple random walk (similar to the PoW setting) although our stopping time (e.g., the first occurrence of a Catalan slot) resembles the event analyzed in [3], namely, the last time the relative margin walk is non-negative. Thus it appears that the combinatorial nature of a consistency violation—*not* the random walk(s) per se—is more complex in PoS than that in PoW.

Outline. We specify our model in Section 2 and focus on a specific consistency property called "k-settelement." This section also contains our main theorems although the proofs are deferred to Section 5. In Section 3, we describe further necessary elements of the fork framework of [3] so that we can explore the relationship between Catalan slots and the UVP in Section 4. In Section 5, we present two bounds on the stochastic events of interest, e.g.,

[2]The name is a nod to the *Catalan number* in combinatorics: The nth Catalan number C_n is the number of strings $w \in \{0, 1\}^{2n}$ so that every prefix x of w satisfies $\#_0(x) \geq \#_1(x)$.

the rarity of a Catalan slot; these bounds lead to short proofs of the main theorems. The proofs of these bounds are presented next in Section 6 which contains all of our stochastic arguments. Our treatment of the Δ-synchronous setting is presented in Section 7. In Section 8, we treat the traditional Common Prefix (CP) violations using our bounds on the UVP. Section 9 explores the connections between the Catalan slots and the relative margin and thus establish a conceptual bridge between the Snow White analysis and the Ouroboros-family analysis. Finally, Section 10 imitates [3] and explores an alternative connection between a CP violation and balanced forks in our extended fork framework, without using Catalan slots.

2 The model; statement of the main theorems

We study the behavior of the elementary *longest-chain rule* algorithm, carried out by a collection of participants:

- In each round, each participant collects all valid blockchains from the network; if a participant is a leader in the round, he adds a block to the longest chain and broadcasts the result.

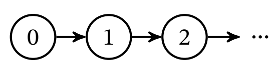
Here, "valid" indicates that any block appearing in the chain was indeed issued by a leader from the associated slot; in the PoS setting, this property is guaranteed with digital signatures.

We begin by studying this algorithm in the simple, synchronous model posited by Blum et. al [3]. The model adopts a synchronous communication network in the presence of a *rushing* adversary: in particular,

A0. Any message broadcast by an honest participant at the beginning of a particular slot is received by the adversary first, who may decide strategically and individually for each recipient in the network whether to inject additional messages and in which order all messages are to be delivered prior to the conclusion of the slot.

(See before Section 2.1 for our comments on this network assumption. A variant of this adversarial message-ordering is presented in Section 2.3. The Δ-synchronous communication model is handled in Section 7.

Given this, it is easy to describe the behavior of the longest-chain rule when carried out by a group of honest participants with the extra guarantee that exactly one is elected as leader in a slot: Assuming that the system is initialized with a common "genesis block" corresponding to sl_0, the players observe a common, linearly growing blockchain:



Here node i represents the block broadcast by the leader of slot i and the arrows represent the direction of increasing time.

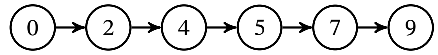
The blockchain axioms: Informal discussion. The introduction of adversarial participants or multiple slot leaders complicates the family of possible blockchains that could emerge from this process. To explore this in the context of our protocols, we work with an abstract notion of a blockchain which ignores all internal structure. We consider a fixed assignment of leaders to time slots, and assume that the blockchain uses a proof mechanism to ensure that any block labeled with slot sl_t was indeed produced by a leader of slot sl_t; this is guaranteed in practice by appropriate use of a secure digital signature scheme.

Specifically, we treat a *blockchain* as a sequence of abstract blocks, each labeled with a slot number, so that:

A1. The blockchain begins with a fixed "genesis" block, assigned to slot sl_0.

A2. The (slot) labels of the blocks are in strictly increasing order.

It is further convenient to introduce the structure of a directed graph on our presentation, where each block is treated as a vertex; in light of the first two axioms above, a blockchain is a path beginning with a special "genesis" vertex, labeled 0, followed by vertices with strictly increasing labels that indicate which slot is associated with the block.

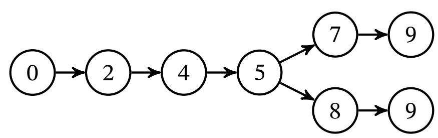


The protocols of interest call for honest players to add a *single* block during any slot. In particular:

A3. Let $k \geq 1$ be an integer. If a slot sl_t was assigned to k honest players but no adversarial players, then k blocks are created—during the entire protocol—each having the label sl_t.

Recall that blockchains are *immutable* in the sense that any block in the chain commits to the entire previous history of the chain; this is achieved in practice by including with each block a collision-free hash of the previous block. These properties imply that any chain that includes a block issued by an honest player must also include that block's associated prefix in its entirety.

As we analyze the dynamics of blockchain algorithms, it is convenient to maintain an entire family of blockchains at once. As a matter of bookkeeping, when two blockchains agree on a common prefix, we can glue together the associated paths to reflect this, as indicated below.



When we glue together many chains to form such a diagram, we call it a "fork"—the precise definition appears below. Observe that while these two blockchains agree through the vertex (block) labeled 5, they contain (distinct) vertices labeled 9; this reflects two distinct blocks associated with slot 9 which, in light of the axiom above, may be produced by either an adversarial participant assigned to slot 9 or two honest participants, both assigned to slot 9.

Finally, as we assume that messages from honest players are delivered without delay, we note a direct consequence of the longest chain rule:

A4. If two honestly generated blocks B_1 and B_2 are labeled with slots sl_1 and sl_2 for which $sl_1 < sl_2$, then the length of the unique blockchain terminating at B_1 is strictly less than the length of the unique blockchain terminating at B_2.

Recall that the honest participant(s) assigned to slot sl_2 will be aware of the blockchain terminating at B_1 that was broadcast by an honest player in slot sl_1 as a result of synchronicity; according to the longest-chain rule, B_2 must have been placed on a chain that was at least this long. In contrast, not all participants are necessarily aware of all blocks generated by dishonest players, and indeed dishonest players may often want to delay the delivery of an adversarial block to a participant or show one block to some participants and show a completely different block to others.

Characteristic strings, forks, and the formal axioms. Note that with the axioms we have discussed above, whether or not a particular fork diagram (such as the one just above) corresponds to a valid execution of the protocol depends on how the slots have been awarded to the parties by the leader election mechanism. We introduce the notion of a "characteristic" string as a convenient means of representing information about slot leaders in a given execution.

Definition 1 (Characteristic string). *Let $sl_1, \ldots, sl_n$ be a sequence of slots. A* characteristic string *w is an element of $\{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^n$ defined for a particular execution of a blockchain protocol on these slots so that for $t \in [n]$, $w_t = \mathtt{A}$ if sl_t is assigned to an adversarial participant; otherwise, $w_t = \mathtt{h}$ if sl_t is assigned to a single honest participant; otherwise, $w_t = \mathtt{H}$.*

For two strings x and w on the same alphabet, we write $x \prec w$ iff x is a strict prefix of w. Similarly, we write $x \preceq w$ iff either $x = w$ or $x \prec w$. The empty string ε is a prefix to any string. If $w_t \in \{\mathtt{h}, \mathtt{H}\}$, we say that "$sl_t$ is honest" and otherwise, we say that "sl_t is adversarial." With this discussion behind us, we set down the formal object we use to reflect the various blockchains adopted by honest players during the execution of a blockchain protocol. This definition formalizes the blockchains axioms discussed above.

Definition 2 (Fork)**.** *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^n$, $P = \{i : w_i = \mathtt{h}\}$, and $Q = \{j : w_j = \mathtt{H}\}$. A* fork *for the string w consists of a directed and rooted tree $F = (V, E)$ with a labeling $\ell : V \to \{0, 1, \ldots, n\}$. We insist that each edge of F is directed away from the root vertex and further require that*

(F1.) the root vertex r has label $\ell(r) = 0$;

(F2.) the labels of vertices along any directed path are strictly increasing;

(F3.) each index $i \in P$ is the label of exactly one vertex of F and, in addition, each index $j \in Q$ is the label of at least two vertices of F; and

(F4.) for any indices $i, j \in P \cup Q$, if $i < j$ then the depth of a vertex with label i is strictly less than the depth of a vertex with label j.

If F is a fork for the characteristic string w, we write $F \vdash w$. Note that the conditions (F1)–(F4) are direct analogues of the axioms **A1**– **A4** above. See Fig. 1 for an example fork. A final notational convention: If $F \vdash x$

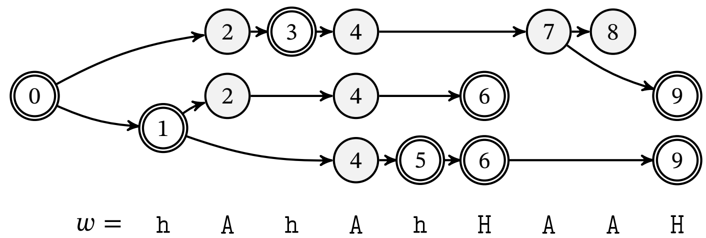


Figure 1: A fork F for the characteristic string $w = \mathtt{hAhAhHAAH}$; vertices appear with their labels and honest vertices are highlighted with double borders. Note that the depths of the (honest) vertices associated with the honest indices of w are strictly increasing. Note, also, that this fork has three disjoint paths of maximum depth. In addition, two honest vertices have label 6 and two more have label 9, indicating the fact that two honest leaders are associated with each of the (honest) slots 6 and 9.

and $\hat{F} \vdash w$, we say that F is a *prefix* of $\hat{F}$, written $F \sqsubseteq \hat{F}$, if $x \preceq w$ and F appears as a consistently-labeled subgraph of $\hat{F}$. (Specifically, each path of F appears, with identical labels, in $\hat{F}$.)

Let w be a characteristic string. The directed paths in the fork $F \vdash w$ originating from the root are called *tines*; these are abstract representations of blockchains. (Note that a tine may not terminate at a leaf of the fork.) We naturally extend the label function ℓ for tines: i.e., $\ell(t) \triangleq \ell(v)$ where the tine t terminates at vertex v. The length of a tine t is denoted by length(t).

Viable tines. The longest-chain rule dictates that honest players build on chains that are at least as long as all previously broadcast honest chains. It is convenient to distinguish such tines in the analysis: specifically, a tine t of F is called *viable* if its length is no smaller than the depth of any honest vertex v for which $\ell(v) \leq \ell(t)$. A tine t is *viable at slot s* if the length of the portion of t appearing over slots $0, \ldots, s$ is no smaller than the depths of any honest vertices labeled from these slots. (As noted, the properties (F3) and (F4) together imply that an honest observer at slot s will only adopt a viable tine.) The *honest depth* function $\mathbf{d} : P \cup Q \to [n]$, defined as $\mathbf{d}(i) = \max_{t \in F} \{\text{length}(t) : \ell(t) = i\}$, gives the largest depth of the (honest) vertices associated with an honest slot; by (F4), $\mathbf{d}(\cdot)$ is strictly increasing.

2.1 Slot settlement and the Unique Vertex Property

We are now ready to explore the power of an adversary in this setting who has corrupted a (perhaps evolving) coalition of the players. We focus on the possibility that such an adversary can violate the consistency of the honest players' blockchains. In particular, we consider the possibility that, at some time t, the adversary conspires to produce two blockchains of maximal length that diverge prior to a previous slot $s \leq t$; in this case honest players

The $(\mathcal{D}, T; s, k)$-settlement game

1. A characteristic string $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ is drawn from $\mathcal{D}$. (This reflects the results of the leader election mechanism.)
2. Let $A_0 \vdash \varepsilon$ denote the initial fork for the empty string ε consisting of a single node corresponding to the genesis block.
3. For each slot $sl_t, t = 1, \ldots, T$ in increasing order:
   (a) (Honest slot.) This case pertains to $w_t \in \{\mathtt{h}, \mathtt{H}\}$. If $w_t = \mathtt{h}$ then $\mathcal{A}$ sets $k = 1$. If $w_t = \mathtt{H}$ then $\mathcal{A}$ chooses an arbitrary integer $k \geq 2$. The challenger is then given k and the fork $A_{t-1} \vdash w_1 \ldots w_{t-1}$. He must determine a new fork $F_t \vdash w_1 \ldots w_t$ by adding k new vertices (all labeled with t) to A_{t-1}. Each new vertex is added at the end of a maximally long path in A_{t-1}. If there are multiple candidates[a] for this path, $\mathcal{A}$ may break the tie. If $k \geq 2$, multiple vertices (all with label k) may be added at the end of the same path.
   (b) (Adversarial slot.) If $w_t = 1$, this is an adversarial slot. $\mathcal{A}$ may set $F_t \vdash w_1 \ldots w_t$ to be an arbitrary fork for which $A_{t-1} \sqsubseteq F_t$.
   (c) (Adversarial augmentation.) $\mathcal{A}$ determines an arbitrary fork $A_t \vdash w_1 \ldots, w_t$ for which $F_t \sqsubseteq A_t$.

   Recall that $F \sqsubseteq F'$ indicates that F' contains, as a consistently-labeled subgraph, the fork F.

$\mathcal{A}$ wins the settlement game if slot s is not k-settled in some fork $A_t, t \geq s + k$.

[a] It is possible that all maximally long paths are honest. In the settlement game considered in [4], at least one of these paths was adversarial.

adopting the longest-chain rule may clearly disagree about the history of the blockchain after slot s. We call such a circumstance a *settlement violation*.

To reflect this in our abstract language, let $F \vdash w$ be a fork corresponding to an execution with characteristic string w. Such a settlement violation induces two viable tines t_1, t_2 with the same length that diverge prior to a particular slot of interest. We record this below.

Definition 3 (Settlement with parameters $s, k \in \mathbb{N}$)**.** *Let $n \in \mathbb{N}$ and let w be a characteristic string of length n. Let $t \in [s + k, n]$ be an integer, $\hat{w} \preceq w$, $|\hat{w}| = t$, and let F be any fork for $\hat{w}$. We say that a slot s is* not k-settled *in F if F contains two maximally long tines $\mathcal{C}_1, \mathcal{C}_2$ that "diverge prior to s," i.e., they either contain different vertices labeled with s, or one contains a vertex labeled with s while the other does not. Otherwise, we say that* slot s is k-settled in F. *We say that* slot s is k-settled in w *if, for each $t \geq s + k$, it is k-settled in every fork $F \vdash \hat{w}$ where $\hat{w} \preceq w$, $|\hat{w}| = t$.*

Definition 4 (Bottleneck Property (BP) and Unique Vertex Property (UVP))**.** *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string. A slot $s \in [T]$ is said to have the* bottleneck property in w with parameter k *if, for any fork $F \vdash w$ and any $k \geq s + 1$, every tine viable at the onset of slot k contains, as its prefix, some vertex with label s. Slot s is said to have the* Unique Vertex Property *if, for any fork $F \vdash w$, there is a unique vertex $u \in F$ with label s so that for any $k \geq s + 1$, all tines viable at the onset of slot k contain, as their common prefix, the vertex u.*

Thus if a uniquely honest slot in w has the bottleneck property, it has the UVP as well. As a consistency property, UVP has several advantages over slot settlement. First, it easily implies the slot settlement property: let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$, $s \in [T]$, and $k \in [T - s]$.

$$\text{If } s + k \text{ has UVP in } w \text{ then } s \text{ is } k\text{-settled in } w. \tag{1}$$

In addition, UVP has a straightforward characterization using "Catalan slots" (see Theorem 3) which is amenable to stochastic analysis. Finally, since UVP is structurally reminiscent of the traditional common prefix (CP) violations, UVP easily implies CP. The analogous statement "settlement implies CP," however, requires a lengthy proof both in [3] and our framework. See Section 10 for details.

2.2 Adversarial attacks on settlement time; the settlement game

To clarify the relationship between forks and the chains at play in a canonical blockchain protocol, we define a game-based model below that explicitly describes the relationship between forks and executions. By design, the probability that the adversary wins this game is at most the probability that a slot s is not k-settled.

Consider the $(\mathcal{D}, T; s, k)$-*settlement game* (presented in the box), played between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ with a leader election mechanism modeled by an ideal distribution $\mathcal{D}$. Intuitively, the game should reflect the ability of the adversary to achieve a settlement violation; that is, to present two maximally-long viable blockchains to a future honest observer, thus forcing them to choose between two alternate histories which disagree on slot s. The challenger plays the role(s) of the honest players during the protocol.

It is important to note that the game bestows the player $\mathcal{A}$ with the power to choose the number of honest vertices in a multiply-honest slot. Note that this setting makes the player strictly more powerful and, importantly, implies that the game is completely determined by the choices made by $\mathcal{A}$ (i.e., the actions of the challenger are deterministic). Consequently, in Definition 5, we can use a single, implicit universal quantifier over all strategies $\mathcal{A}$; no choices of the challenger are actually necessary to fully describe the game.

Definition 5 (Settlement insecurity)**.** *Let $\mathcal{D}$ be a distribution on $\{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$. Let $w \sim \mathcal{D}$ be the string used in the first step of a $(\mathcal{D}, T; s, k)$-settlement game G. The (s, k)-*settlement insecurity *of $\mathcal{D}$ is defined as*

$$\mathbf{S}^{s,k}[\mathcal{D}] \triangleq \max_{\substack{\hat{w} \preceq w \\ |\hat{w}| \geq s+k}} \max_{F \vdash \hat{w}} \Pr\left[\begin{array}{c} F \text{ has two maximally long tines} \\ \text{that diverge prior to slot } s \end{array} \right].$$

Note that the probability in the right-hand side is the same as the probability that the player wins G.

Note that in typical PoS settings the distribution $\mathcal{D}$ is determined by the combined stake held by the adversarial players, the leader election mechanism, and the dynamics of the protocol. The most common case (as seen in Snow White [2], Ouroboros [9], and Ouroboros Praos [5]) guarantees that the characteristic string $w = w_1 \dots w_T$ is drawn from an i.i.d. distribution for which $\Pr[w_i = 1] \leq (1 - \epsilon)/2$ for some $\epsilon \in (0, 1)$; here the constant $(1 - \epsilon)/2$ is directly related to the stake held by the adversary. Some settings involving adaptive adversaries (e.g., Ouroboros Genesis [1]) yield a weaker martingale-type guarantee that $\Pr[w_i = 1 \mid w_1, \dots, w_{i-1}] \leq (1 - \epsilon)/2$. We can easily handle both types of distributions in our analysis since the former distribution "stochastically dominates" the latter. As a rule, we denote the probability distribution associated with a random variable using uppercase script letters.

Definition 6 (Stochastic dominance)**.** *Let X and Y be random variables taking values in some set Ω endowed with a partial order $\leq$. We say that X* stochastically dominates *Y, written $Y \preceq X$, if $\mathcal{X}(A) \geq \mathcal{Y}(A)$ for all* monotone sets *$A \subseteq \Omega$, where a set $A \subseteq \Omega$ is called monotone if $x \in A$ implies $y \in A$ for all $x \leq y$. As a special case, when $\Omega = \mathbb{R}$, $Y \preceq X$ if $\Pr[X \geq \Lambda] \geq \Pr[Y \geq \Lambda]$ for every $\Lambda \in \mathbb{R}$. We extend this notion to probability distributions in the natural way.*

Let w be a characteristic string, $|w| = T$. We investigate a family of distributions that stipulate that w has i.i.d. coordinates; specifically, for $\epsilon \in (0, 1)$, let $B_\epsilon = (B_1, \dots, B_T)$ denote a list of independent and identically distributed random variables $B_i \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}, i \in [T]$ where $\Pr[B_i = \mathtt{A}] = (1 - \epsilon)/2$ and $\Pr[B_i = \mathtt{h}] > 0$. Let $\mathcal{B}_\epsilon$ be the distribution associated with B_ϵ.

Theorem 1 (Main theorem)**.** *Let $\epsilon \in (0, 1), s, k, T \in \mathbb{N}$. Considering the random variable B_ϵ above, let $p_\mathtt{h} = \Pr[B_1 = \mathtt{h}] > 0$. Then $\mathbf{S}^{s,k}[\mathcal{B}_\epsilon] \leq \exp\left(-k \cdot \Omega(\min(\epsilon^3, \epsilon^2 p_\mathtt{h}))\right)$ for large k. Furthermore, let $\mathcal{W}$ be a distribution on $\{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ so that $\mathcal{W} \preceq \mathcal{B}_\epsilon$. Then $\mathbf{S}^{s,k}[\mathcal{W}] \leq \mathbf{S}^{s,k}[\mathcal{B}_\epsilon]$. (Here, the asymptotic notation hides constants that do not depend on ϵ or k.)*

The proof is deferred to Section 5.

Analysis in the Δ-synchronous setting. The security game above most naturally models a blockchain protocol over a synchronous network with immediate delivery (because each "honest" play of the challenger always builds on a fork that contains the fork generated by previous honest plays). However, the model can be easily adapted to protocols in the Δ-synchronous model by applying the Δ-reduction mapping of [5] (which is specifically designed to lift the synchronous analysis to the Δ-synchronous setting). These details appear in Section 7.

Public leader schedules. One attractive feature of this model is that it gives the adversary full information about the future schedule of leaders. The analysis of some protocols indeed demand this (e.g., Ouroboros, Snow White). Other protocols—especially those designed to offer security against adaptive adversaries (Praos, Genesis)—in fact contrive to keep the leader schedule private. Of course, as our analysis is in the more difficult "full information" model, it applies to all of these systems.

Bootstrapping multi-phase algorithms; stake shift. We remark that several existing proof-of-stake blockchain protocols proceed in phases, each of which is obligated to generate the randomness (for leader election, say) for the next phase based on the current stake distribution. The blockchain security properties of each phase are then individually analyzed—assuming clean randomness—which yields a recursive security argument; in this context the game outlined above precisely reflects the single phase analysis.

2.3 A consistent longest-chain selection rule

The rushing adversary described at the outset of Section 2 can always reorder messages before delivering to a recipient. Let us modify this threat model by modifying axiom **A0** as follows:

A0′. Assume axiom **A0**. Suppose two honest recipients receive the same set L of maximally long blockchains. If all chains in L end in honest blocks then the adversary delivers the elements of L to these honest recipients in an arbitrary but consistent order.

Note that the adversary is free to deliver adversarial blockchains in any order, interleaving the honest chains if he so wishes. Moreover, if there is no competitive adversarial blockchain when devlivering to an honest recipient, he relinquishes his right to reorder the maximally long honest blockchains. When an execution satisfies this axiom, we say that *the honest players use a cosnsistent longest-chain tie-breaking rule*.

Definition 7 (Bivalent characteristic string). *Let $sl_1, \ldots, sl_n$ be a sequence of slots. A* bivalent characteristic string *w is an element of $\{\mathtt{H}, \mathtt{A}\}^n$ defined for a particular execution of a blockchain protocol on these slots so that for $t \in [n]$, $w_t = \mathtt{A}$ if sl_t is assigned to an adversarial participant, and $w_t = \mathtt{H}$ otherwise.*

The definition of a fork F for a bivalent characteristic string is identical to Definition 2 except the following:

(F3.) each index in $\{j : w_j = \mathtt{H}\}$ is the label of at least one vertex of F.

Let w a bivalent characteristic string, F a fork for w, and F' a fork for $w\mathtt{H}$ so that $F \sqsubseteq F'$ and any honest vertex in $F' \setminus F$ has label $|w| + 1$. Considering F', let C be the set of all maximally long tines in F seen by an honest slot leader associated with the honest slot $|w| + 1$. (In particular, if a maximally long tine has an honest label, it is in C.) There can be two scenarios: If C contains an adversarial tine, we say that *F has a tie for the longest-chain rule*—or, in short, that *F has an LCR tie*. In this case, axiom **A0′** above states that every honest slot leader at slot $|w| + 1$ selects a tine $t \in C$ chosen by the adversary. Otherwise, every tine in C is honest and, in this case, every slot leader at slot $|w| + 1$ selects a unique chain determined by the consistent longest-chain tie-breaking rule. Therefore, if F does not have an LCR tie, all honest tines in F' with label $|w| + 1$ build upon a unique honest tine in F.

Let w be a bivalent characteristic string and consider distributions for w so that w has i.i.d. slots; specifically, for $T \in \mathbb{N}$ and $\epsilon \in (0, 1)$, let $\tilde{B}_\epsilon = (B_1, \ldots, B_T)$ denote a list of independent and identically distributed random variables $B_i \in \{\mathtt{H}, \mathtt{A}\}$, $i \in [T]$ so that $\Pr[B_i = \mathtt{A}] = (1 - \epsilon)/2$. Let $\tilde{\mathcal{B}}_\epsilon$ be the distribution associated with $\tilde{B}_\epsilon$.

Theorem 2 (Main theorem; consistent tie-breaking). *Let $\epsilon \in (0, 1)$, $s, k, T \in \mathbb{N}$. Let $\mathcal{W}$ and $\tilde{\mathcal{B}}_\epsilon$ be two distributions on $\{\mathtt{H}, \mathtt{A}\}^T$ where $\tilde{\mathcal{B}}_\epsilon$ is defined above and $\mathcal{W} \preceq \tilde{\mathcal{B}}_\epsilon$. Then $\mathbf{S}^{s,k}[\mathcal{W}] \leq \mathbf{S}^{s,k}[\tilde{\mathcal{B}}_\epsilon] \leq \exp\bigl(-k \cdot \Omega(\epsilon^3(1 + O(\epsilon)))\bigr)$ for large k. (Here, the asymptotic notation hides constants that do not depend on ϵ or k.)*

The proof is deferred to Section 5. We can interpret the random variables B_i (defined above the theorem) as taking values in the set $\{\mathtt{h}, \mathtt{H}, \mathtt{A}\}$ but with $\Pr[B_i = \mathtt{h}] = 0$. Thus the theorem above allows a leader election scheme to produce no uniquely honest slot and yet achieve optimal consistency error. (Recall that Theorem 1 requires $\Pr[B_i = \mathtt{h}] > 0$.)

3 Structure of forks

Let us lay down the elements from the fork framework of [4]. For completeness, we restate and briefly discuss the pertinent definitions below. A vertex of a fork is said to be *honest* if it is labeled with an index i such that $w_i \in \{\mathtt{h}, \mathtt{H}\}$; otherwise, it is said to be *adversarial*.

Definition 8 (Tines, length, and height). *Let $F \vdash w$ be a fork for a characteristic string. A* tine *of F is a directed path starting from the root. For any tine t we define its* length *to be the number of edges in the path, and for any vertex v we define its* depth *to be the length of the unique tine that ends at v. If a tine t_1 is a strict prefix of another tine t_2, we write $t_1 \prec t_2$. Similarly, if t_1 is a non-strict prefix of t_2, we write $t_1 \preceq t_2$. The longest common prefix of two tines t_1, t_2 is denoted by $t_1 \cap t_2$. That is, $\ell(t_1 \cap t_2) = \max\{\ell(u) : u \preceq t_1 \text{ and } u \preceq t_2\}$. The* height *of a fork (as is usual for a tree) is the length of the longest tine, denoted by* $\text{height}(F)$.

When an adversary builds a fork, it is natural to imagine that he "grows" an existing fork by adding new vertices and edges.

Definition 9 (Fork prefixes). *Let $w, x \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ so that $x \preceq w$. Let F, F' be two forks for x and w, respectively. We say that F is a* prefix *of F' if F is a consistently labeled subgraph of F'. That is, all vertices and edges of F also appear in F' and the label of any vertex appearing in both F and F' is identical. We denote this relationship by $F \sqsubseteq F'$.*

When speaking about a tine that appears in both F and F', we place the fork in the subscript of relevant properties.

For any string x (on any alphabet) and a symbol σ in that alphabet, define $\#_\sigma(x)$ as the number of appearances of σ in x. When a characteristic string $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ is fixed from the context, we extend this notation to sub-intervals of $[T]$ in a natural way: For integers $i, j \in [T], i \le j$, let $I = [i, j] \subset [T]$ be a closed interval and define $\#_\sigma(I) = \#_\sigma(w_i \dots w_j)$ for $\sigma \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}$. A characteristic string w is called hH-heavy if $\#_{\mathtt{h}}(w) + \#_{\mathtt{H}}(w) > \#_1(x)$; otherwise, it is called A-heavy. For a given characteristic string w of length T, an interval $I = [i, j] \subseteq [T]$ is called A-heavy if the substring $w_i \dots w_j$ is A-heavy.

Let F be a fork for w and let B be an honest tine in F. We say that B has an *adversarial extension t* if B can be extended to an adversarial tine t using only adversarial vertices from the interval $I = [\ell(B) + 1, \ell(t)]$ so that $B \prec t$ and the last honest vertex on t is B. Note that t can be made disjoint with any F-tine over the interval I. If $w = xy$ and two tines t_1, t_2 are disjoint over y, we call these tines *y-disjoint*. We also equivalently say that t_1 *is y-disjoint with t_2*.

Fact 1. *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string, $s \in [T+1]$ be an integer, $x \preceq w, |x| = s - 1$. Let F be a fork for w, B an honest vertex in F, $h = \ell(B)$, and $I = [h+1, s-1]$. Let $F_x \vdash x$ be a fork prefix of F so that F_x contains all honest tines from F with labels at most $s - 1$. The following statements are equivalent: (a) I is A-heavy; and (b) B has an adversarial extension $t, \ell(t) \in I$ so that t is viable at the onset of slot s.*

Proof. First let us prove that (a) implies (b). Let t^* be a maximally long honest tine in F so that $\ell(t^*) \in I$. There can be two cases. If B is on t^*, the adversarial slots in I can be used to create an adversarial tine t so that i) B is the last honest vertex on t, ii) B is the last common vertex between t and t^*, and iii) $\text{length}(t) \ge \text{length}(t^*)$ so that t is viable at the onset of slot s. Now suppose B is not on t^*. Let B^* be the first honest vertex on t^* so that $\ell(B^*) \le \ell(B)$. If the interval $I' = [\ell(B^*) + 1, \ell(B) - 1]$ is non-empty, t^* must contain only adversarial vertices in I'. We can build the adversarial tine t as follows: Extend B^* by duplicating the vertices on t^* in the interval $[\ell(B^*) + 1, \ell(B) - 1]$, put B on t and finally, extend B using only adversarial slots from I so that B^* is the last common vertex between t and t^*, and $\text{length}(t) \ge \text{length}(t^*)$. Hence t is viable at the onset of slot s.

It remains to prove that (b) implies (a). Since t is an adversarial extension of B, it contains only adversarial vertices from I. By assumption, t is viable at the onset of slot s. It follows that $\#_{\mathtt{A}}(I) \ge \#_{\mathtt{h}}(I) + \#_{\mathtt{H}}(I)$ since the longest tine grows by at least one vertex for each honest slot in I. □

Corollary 1. *Let w be a characteristic string, F be any fork for w, and let t be any tine in F. Let B_1 and B_2 be two honest vertices on t such that (i) $\ell(B_1) < \ell(B_2)$, (ii) t contains only adversarial vertices from $I = [\ell(B_1)+1, \ell(B_2)-1]$, and (iii) t contains at least one vertex from I. Then I is A-heavy.*

Proof. By assumption, the honest vertex B_2 builds on some adversarial tine t' that is viable at the onset of slot $\ell(B_2)$ and, importantly, contains B_1 as its last honest vertex. By Fact 1, the interval I is A-heavy. □

4 Catalan slots and the UVP

Definition 10 (Catalan slot)**.** *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string and let $s \in [T]$ be an integer. s is called a* left-Catalan slot in w *if, for any integer $\ell \in [s]$, the interval $[\ell, s]$ is $\mathtt{hH}$-heavy in w. s is called a* right-Catalan slot in w *if, for any integer $r \in [s, T]$, the interval $[s, r]$ is $\mathtt{hH}$-heavy in w. Finally, s is called a* Catalan slot in w *if it is both left- and right-Catalan in w.*

Observe that a left- or right-Catalan slot must be honest. In addition, the slot before a left-Catalan (resp. after a right-Catalan) slot must be honest as well. Thus the slots adjacent to a Catalan slot must be honest. A Catalan slot c acts as a barrier for adversarial tine extensions in that in any fork, every tine viable at the onset of slot $c+1$ must be honest.

Fact 2. *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string and s a left-Catalan slot in w. In any fork for w, every viable tine at the onset of slot $s+1$ is an honest tine from slot s.*

Proof. Let τ be the longest tine with label s. (τ is an honest tine. If s is a uniquely honest slot, τ is unique. Otherwise, τ is unique up to tie-breaking among equally-long tines.) We claim that all adversarial tines $t \in F, \ell(t) \leq s-1$ are strictly shorter than τ. Suppose, towards a contradiction, that t is a viable adversarial tine at the onset of slot $s+1$, i.e., $\ell(t) \leq s-1$ and $\text{length}(t) \geq \text{length}(\tau)$. Let B be the last honest vertex on t; necessarily, $\ell(B) < s$. According to Fact 1, the interval $[\ell(B)+1, s]$ is $\mathtt{A}$-heavy. But this contradicts the assumption that s is a left-Catalan slot. Hence the adversarial tine t cannot be viable. ☐

Observation 1. If s is a Catalan slot for w, Fact 2 implies that in every fork for w, an honest slot leader at slot $s+1$ always builds on top of an honest tine with label s; this tine, in fact, will be maximally long among all tines with label s.

Fact 3 (Bottleneck property implies a Catalan slot)**.** *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string. If an honest slot in w has the bottleneck property then it is a Catalan slot.*

Proof. Let $s \in [T]$ be an honest slot in w. We will prove the contrapositive: namely, that if s is not Catalan then s does not have the bottleneck property. Suppose s is not a Catalan slot. Then there must be some $a, b \in [T]$ so that $I = [a, b]$ is the largest $\mathtt{A}$-heavy interval which includes s. Necessarily, either $b = T$, or $b+1$ must be an honest slot. Likewise, either $a = 1$, or $a-1$ must be an honest slot. Let $u \in F, \ell(u) = a-1$ be an honest tine. (If $a = 1$, we can take u as the root vertex.) Since I is $\mathtt{A}$-heavy, Fact 1 states that it is possible to augment F with an adversarial extension $t, u \prec t$ so that t is viable at the onset of slot $b+1$. In particular, the extension will use only adversarial vertices from the interval I and, in particular, t will not contain any vertex from the honest slot s. Thus s does not have the bottleneck property. ☐

4.1 UVP from a uniquely honest Catalan slot

Theorem 3. *Let $w \in \{h, H, A\}^T$ be a characteristic string. Let $s \in [T]$ be a uniquely honest slot in w. Slot s is Catalan in w if and only if it has the UVP in w.*

Proof. (The $\Longleftarrow$ direction.) Since s has the UVP it satisfies the (weaker) bottleneck property. By Fact 3, the honest slot s must be Catalan.

(The $\Longrightarrow$ direction.) By assumption, slot s has a unique honest leader. Let τ be the unique honest tine at slot s. By Fact 2, the honest tine τ is the only viable tine at the onset of slot $s+1$. If $s = T$ then τ is the only viable tine at the onset of slot $T+1$. Now suppose $s \leq T-1$. As s is a Catalan slot, slots s and $s+1$ must be honest. Let t be a viable tine at the onset of some slot $k, k \geq s+2$. We claim that τ must be a prefix of t.

Suppose, for a contradiction, that t does not contain τ as its prefix. Let B_1 be the last honest vertex on t such that $\ell(B_1) \leq s-1$. (If $s = 1$ or no such vertex can be found, take B_1 as the root vertex.) Likewise, let B_2 be the first honest vertex on t such that $\ell(B_2) \in [s+1, k-1]$.

Suppose B_2 exists. If $\ell(B_2) = s+1$ then, by Observation 1, B_2 builds on τ, contradicting our assumption that τ is not a prefix of t. Otherwise, suppose $\ell(B_2) \in [s+2, k-1]$. let I be the interval $[\ell(B_1)+1, \ell(B_2)-1]$. Clearly, I

contains s. If t contains any adversarial vertex between B_1 and B_2 then, by Corollary 1, I must be A-heavy; but this contradicts the assumption that s is a Catatan slot. Otherwise, B_2 builds on top of B_1 and, in particular, B_1 must be viable at the onset of slot $\ell(B_2) \geq s+1$. Since $\ell(\tau) = s$, this means length(B_1) $\geq$ length(τ). However, since $\ell(B_1) < s$, by the monotonicity of the honest-depth function $\mathbf{d}(\cdot)$, length(τ) $\geq 1 +$ length(B_1). This contradicts the inequality above.

Now suppose B_2 does not exist. We claim that t is an adversarial tine. To see why, note that if t were honest and $\ell(t) \geq s+1$ then there would have been a B_2. Since s is a uniquely honest slot and τ is not a prefix of t by assumption, $\ell(t) \neq s$ if t is honest.

Finally, if t is honest and $\ell(t) \leq s-1$ then, by Fact 2, t cannot be viable at the onset of slot $s+1$ since s is Catalan. Since $s+1$ is an honest slot, honest tines with label $s+1$ will be strictly longer than t and, therefore, t cannot be viable at the onset of slot $k \geq s+2$ either. We conclude that t must be an adversarial tine viable at the onset of slot k. By Fact 1, the interval $I = [\ell(B_1)+1, k-1]$ must be A-heavy. However, since I contains s, it contradicts the fact that s is a Catalan slot.

It follows that every viable tine $t \in F, \ell(t) \geq s+1$ must contain τ as its prefix. □

4.2 UVP from consecutive Catalan slots and axiom A0′

Theorem 4. *Let $w \in \{\mathtt{H}, \mathtt{A}\}^T$ be a bivalent characteristic string and axiom **A0′** is satisfied. Let $s \in [2, T]$ be an integer such that s and $s-1$ are two honest slots in w. The following statements are equivalent: (i) Slots $s, s-1$ are Catalan. (ii) If $s \leq T-1$, both s and $s-1$ have the UVP. Otherwise, slot $T-1$ has the UVP but slot T has the bottleneck property.*

Proof. Since the slots $s, s-1$ satisfy the (weaker) bottleneck property, Fact 3 implies that they must be Catalan slots. This proves (*ii*) implies (*i*).

Now let us prove that (*i*) implies (*ii*). Slots $s, s-1$ are Catalan. Let V_s (resp. V_{s+1}) be the set of all viable tines at the onset of slot s (resp. slot $s+1$). Since $s-1$ (resp. s) is a Catalan slots, we use Fact 2 and conclude that V_s (resp. V_{s+1}) can contain only maximally long honest tines $t, \ell(t) = s-1$ (resp. $\ell(t) = s$). Let $u_s \in V_s$ be the unique vertex determined by the consistent tie-breaking rule when applied to the set V_s. Define $u_{s+1} \in V_{s+1}$ in an analogous way for the set V_{s+1}.

Let $k \in [s+1, T+1]$ be an integer. We wish tho show that for every tine t viable at the onset of slot k, the following holds: (i) if $s \leq T-1$ then $u_s \prec u_{s+1} \preceq t$, and (ii) if $s = T$ then $u_{T-1} \prec t$ where $\ell(t) = T$.

All tines at the honest slot s build upon u_s. If $s = T$, we are done. Otherwise, i.e., if $s \leq T-1$, let $\tau = u_{s+1}$ and note that $u_s \prec u_{s+1} = \tau$. If $k = s+1$, we are done since by Fact 2, every tine at the honest slot k will build upon τ.

It remains to reason about the case $s \leq T-2$ and $k \geq s+2$. Consider a tine t which is viable at the onset of slot k. (All we know about t's label is that $\ell(t) \leq k-1$.) We claim that $\tau \prec t$. Suppose, towards a contradiction, that τ is not a prefix of t. Let B_1 be the last honest vertex on t such that $\ell(B_1) \leq s-1$. (If no such vertex can be found, take B_1 as the root vertex.) Likewise, let B_2 be the first honest vertex on t such that $\ell(B_2) \in [s+1, k-1]$.

Below, we show that every choice for B_1, B_2 leads to a contradiction and, therefore, τ must be a prefix of t. If B_2 exists then, by construction, $\ell(B_1) < s < \ell(B_2) \leq k-1$. If $\ell(B_2) = s+1$ then, as we have argued earler, B_2 must have built on τ. This contradicts our assumption that τ is not a prefix of t. Otherwise, suppose $\ell(B_2) \geq s+2$. Let I be the interval $[\ell(B_1)+1, \ell(B_2)-1]$ and note that I contains s. There can be two scenarios. If t contains an adversarial vertex between B_1 and B_2 then, by Corollary 1, I must be A-heavy; but this contradicts the assumption that s is a Catatan slot. Otherwise, B_2 builds on top of B_1 and, in particular, B_1 must be viable at the onset of slot $\ell(B_2) \geq s+1$. Since $\ell(\tau) = s$, this means length(B_1) $\geq$ length(τ). However, since $\ell(B_1) < s$, by the monotonicity of the honest-depth function $\mathbf{d}(\cdot)$, length(τ) $\geq 1 +$ length(B_1). This contradicts the inequality above.

If B_2 does not exist then we claim that t is an adversarial tine. To see why, note that if t were honest and $\ell(t) \geq s+1$ then there would have been a B_2. If t were honest with $\ell(t) = s, t \neq \tau$ then t would not be viable at the onset of slot $s+2$. This is because s is a Catalan slot and as such, each vertex from slot $s+1$ builds on τ, length(τ) $\geq$ length(t). Hence tines viable at the onset of slot $s+2$ must have length at least $1 +$ length(τ) $>$ length(t). Finally, if t is honest and $\ell(t) \leq s-1$ then, by Fact 2, t cannot be viable at the onset of slot $s+1$ since s is Catalan. Since $s+1$ is an honest slot, honest tines with label $s+1$ will be strictly longer than t and, therefore, t cannot be viable at the onset of slot $k \geq s+2$ either. We conclude that t must be an adversarial tine viable at the onset of slot k. By Fact 1, the interval $I = [\ell(B_1) + 1, k - 1]$ must be $\mathtt{A}$-heavy. However, since I contains s, it contradicts the fact that s is a Catalan slot. □

5 Proofs of main theorems

We start with two bounds on the event that Catalan slots are rare; the proofs are deferred till the next section. Bound 1 conerns uniquely honest Catalan slots and complements Theorem 3 while Bound 2 concerns two consecutive Catalan slots and complements Theorem 4.

Bound 1. *Let $\epsilon, q_{\mathtt{h}} \in (0,1)$ and $q_{\mathtt{H}} \in [0,1)$ so that $q_{\mathtt{h}} + q_{\mathtt{H}} = (1+\epsilon)/2$. Let $w \in \{\mathtt{h},\mathtt{H},\mathtt{A}\}^*$ be a characteristic string, written $w = xyz$, where both $|x|$ and $|z|$ are allowed to go to ∞ and the w_is are i.i.d. random variables with $\Pr[w_i = \mathtt{h}] = q_{\mathtt{h}} > 0$ and $\Pr[w_i = \mathtt{H}] = q_{\mathtt{H}}$. Let $k = |y|$. Let H denote the event that y does not contain a uniquely honest Catalan slot. Then for large k, $\Pr[H] \leq \exp\left(-k \cdot \Omega(\min(\epsilon^3, \epsilon^2 q_{\mathtt{h}}))\right)$.*

In particular, when $q_{\mathtt{H}} = 0$, the bound above coincides with the bound in [3]; thus the current analysis subsumes their result.

Bound 2. *Let $\epsilon \in (0,1)$ and let $w \in \{\mathtt{H},\mathtt{A}\}^*$ be a bivalent characteristic string, written $w = xyz$, where both $|x|$ and $|z|$ are allowed to go to ∞ and the w_is are i.i.d. random variables with $\Pr[w_i = \mathtt{H}] = (1+\epsilon)/2$. Let $k = |y|$. Let H denote the event that y does not contain two consecutive Catalan slots. Then for large k, $\Pr[H] \leq \exp\left(-k \cdot \Omega(\epsilon^3(1 + O(\epsilon)))\right)$.*

Proof of Theorem 1. We consider the distribution $\mathcal{B}_\epsilon$ first. Write $w = xyz$, $|x| = s - 1$. Recall that $\mathbf{S}^{s,k}[\mathcal{B}_\epsilon] = \Pr_{w \sim \mathcal{B}_\epsilon}[s \text{ is not } k\text{-settled in } w]$. Theorem 3 and Equation (1) implies that if w contains a uniquely honest Catalan slot $c \in [s, s+k]$ then slot s must be k-settled in w. In fact, by virtue of Fact 2, it suffices to take $c \in [s, s+k-1]$, i.e., $|x| \leq c \leq |xy|$. Thus the probability above is bounded by Bound 1 which renames $p_{\mathtt{h}} = q_{\mathtt{h}}$ and $p_{\mathtt{H}} = q_{\mathtt{H}}$. This proves the first inequality.

Now let us prove the second inequality. Let $a, b \in \{\mathtt{h},\mathtt{H},\mathtt{A}\}^*$, $|a| = |b|$. Define the partial order $\leq$ on equal-length characteristic strings as follows: $a \leq b$ if and only if for all $i = 1, \ldots, |a|$, $a_i = 1$ implies $b_i = 1$. For any player playing the settlement game, let C be the set of strings on which the player wins. Clearly, C is monotone with respect to the partial order $\leq$. To see why, note that if the player wins on a specific string w, he can certainly win on any string w' so that $w \leq w'$. By assumption, $\mathcal{W} \preceq \mathcal{B}_\epsilon$. It follows from Definition 6 that $\Pr_{\mathcal{W}}[w] \leq \Pr_{\mathcal{B}_\epsilon}[w]$ for any w in the monotone set C. By referring to the definition of settlement insecurity (see Definition 5), we conclude that $\mathbf{S}^{s,k}[\mathcal{W}] \leq \mathbf{S}^{s,k}[\mathcal{B}_\epsilon]$. □

Proof of Theorem 2. This proof is identical to the proof of Theorem 1 except that we need to refer to Theorem 4 in lieu of Theorem 3 and Bound 2 in lieu of Bound 1. □

6 Proofs of Bounds 1 and 2

As a rule, we denote the probability distribution associated with a random variable using uppercase script letters. Observe that if $Y \preceq X$ and Z is independent of both X and Y, then $Z + Y \preceq Z + X$. In addition, for any non-decreasing function u defined on Ω, $Y \preceq X$ implies $u(Y) \preceq u(X)$.

Generating functions. We reserve the term *generating function* to refer to an "ordinary" generating function which represents a sequence $a_0, a_1, \ldots$ of non-negative real numbers by the formal power series $\mathsf{A}(Z) = \sum_{t=0}^{\infty} a_t Z^t$. We denote the above correspondence as $\{a_t\} \stackrel{\text{gf}}{\longleftrightarrow} \mathsf{A}(Z)$. When $\mathsf{A}(1) = \sum_t a_t = 1$ we say that the generating function is a *probability generating function*; in this case, the generating function A can naturally be associated with the integer-valued random variable A for which $\Pr[A = k] = a_k$. If the probability generating functions A and B are associated with the random variables A and B, it is easy to check that $\mathsf{A} \cdot \mathsf{B}$ is the generating function associated with the convolution $A + B$ (where A and B are assumed to be independent). Translating the notion of stochastic dominance to the setting with generating functions, we say that the generating function A *stochastically dominates* B if $\sum_{t\le T} a_t \le \sum_{t\le T} b_t$ for all $T \ge 0$; we write $\mathsf{B} \preceq \mathsf{A}$ to denote this state of affairs. If $\mathsf{B}_1 \preceq \mathsf{A}_1$ and $\mathsf{B}_2 \preceq \mathsf{A}_2$ then $\mathsf{B}_1 \cdot \mathsf{B}_2 \preceq \mathsf{A}_1 \cdot \mathsf{A}_2$ and $\alpha\mathsf{B}_1 + \beta\mathsf{B}_2 \preceq \alpha\mathsf{A}_1 + \beta\mathsf{A}_2$ (for any $\alpha, \beta \ge 0$). Moreover, if $\mathsf{B} \preceq \mathsf{A}$ then it can be checked that $\mathsf{B}(\mathsf{C}) \preceq \mathsf{A}(\mathsf{C})$ for any probability generating function $\mathsf{C}(Z)$, where we write $\mathsf{A}(\mathsf{C})$ to denote the composition $\mathsf{A}(\mathsf{C}(Z))$.

Finally, we remark that if $\mathsf{A}(Z)$ is a generating function which converges as a function of a complex Z for $|Z| < R$ for some non-negative R, R is called the *radius of convergence* of A. It follows from Theorem 2.19 in [13] that $\lim_{k\to\infty} |a_k|R^k = 0$ and that $|a_k| = O(R^{-k})$. In addition, if A is a probability generating function associated with the random variable A then it follows that $\Pr[A \ge T] = O(R^{-T})$.

6.1 Proof of Bound 1

Let $p = (1-\epsilon)/2$ and $q = 1-p = q_{\mathtt{h}} + q_{\mathtt{H}}$; thus $q - p = \epsilon$. Define the process $W = (W_t : t \in \mathbb{N}), W_t \in \{\pm 1\}$ as $W_t = 1$ if and only if $w_t = \mathtt{A}$. Let $S = (S_t : t \in \mathbb{N}), S_t = \sum_{i\le t} W_i$ be the position of the particle at time t. Thus S is a random walk on $\mathbb{Z}$ with ϵ negative (i.e., downward) bias. By convention, set $W_0 = S_0 = 0$.

Case 1: x is an empty string. In this case, we write $w = yz$ so that $|y| = k$. Let c_t be the probability that t is the first uniquely honest Catalan slot in w with $c_0 = 0$, and consider the probability generating function $\{c_t\} \overset{\text{gf}}{\longleftrightarrow} \mathsf{C}(Z) = \sum_{t=0}^{\infty} c_t Z^t$. Controlling the decay of the coefficients c_t suffices to give a bound on $\Pr[H]$, i.e., the probability that y *does not* contain a Catalan slot, because this probability is at most $1 - \sum_{t=0}^{k-1} c_t = \sum_{t=k}^{\infty} c_t$. To this end, we develop a closed-form expression for a related probability generating function $\hat{\mathsf{C}}(Z) = \sum_t \hat{c}_t Z^t$ which stochastically dominates $\mathsf{C}(Z)$. Recall that this means that for any k, $\sum_{t\ge k} c_k \le \sum_{t\ge k} \hat{c}_k$. Finally, bound the latter sum by using the analytic properties of $\hat{\mathsf{C}}(Z)$.

Treating the random variables $W_1, \ldots$ as defining a (negatively) biased random walk, define D (resp. A) to be the generating function for the *descent stopping time* (resp. the *ascent stopping time*) of the walk; this is the first time the random walk, starting at 0, visits -1 (resp. $+1$). The natural recursive formulation of these descent time yield simple algebraic equations for the descent generating function, $\mathsf{D}(Z) = qZ + pZ\mathsf{D}(Z)^2$ and $\mathsf{A}(Z) = pZ + qZ\mathsf{A}(Z)^2$, and from this we may conclude

$$\mathsf{D}(Z) = (1 - \sqrt{1 - 4pqZ^2})/2pZ\,,$$

$$\mathsf{A}(Z) = (1 - \sqrt{1 - 4pqZ^2})/2qZ\,.$$

Note that while D is a probability generating function, A is not: according to the classical "gambler's ruin" analysis, the probability that a negatively-biased random walk starting at 0 ever rises to 1 is exactly p/q; thus $\mathsf{A}(1) = p/q$.

Recall that a slot is Catalan in w if and only if it is both left-Catalan and right-Catalan. A slot is left-Catalan if the walk S descends to a new low at that slot. In addition, the same slot (say s) is right-Catalan if the walk never reaches to that level in future, i.e., $S_s \ge S_i, i \ge s+1$. The probability of this event is $1 - \mathsf{A}(1) = 1 - p/q = \epsilon/q$, conditioned on the fact that $W_s = -1$.

Assume that the walk is now at its historical minimum. We can think of the generating function $\mathsf{C}(Z)$ as a search procedure for finding the first uniquely honest Catalan slot. Let v be the first symbol we observe. Noting that $1 - \epsilon/q = p/q$, we claim that

$$\mathsf{C}(Z) = pZ\mathsf{D}(Z)\mathsf{C}(Z) + q_{\mathtt{h}}Z \cdot \epsilon/q + q_{\mathtt{h}}Z \cdot p/q \cdot \mathsf{E}(Z)\mathsf{C}(Z) + q_{\mathtt{H}}Z\mathsf{C}(Z)\,.$$

Here is the explanation: (*i*) With probability p, $v = \mathtt{A}$ and the walk moves up. then we wait till the walk makes a first descent and restart. (*ii*) With probability $q_{\mathtt{H}}$, $v = \mathtt{H}$ and the walk moves down. Since we will reach a new minimum, we restart. (*iii*) With probability $q_{\mathtt{h}} \cdot \epsilon/q$, $v = \mathtt{h}$ *and* the walk diverges below. Hence our search has succeded and we stop. (*iv*) Otherwise, i.e., with probability $q_{\mathtt{h}} \cdot p/q$, $v = \mathtt{h}$ *but* the walk returns to the origin from below. Then we wait for the walk to match its minimum again before we can restart. We use $\mathsf{E}(Z)$ to denote the generating function for this "guaranteed ascent then match minimum" walk. After rearranging, we get

$$\mathsf{C}(Z) = \frac{(q_{\mathrm{h}}\epsilon/q)Z}{1-\left(pZ\mathsf{D}(Z) + (q_{\mathrm{h}}p/q)Z\mathsf{E}(Z) + q_{\mathrm{H}}Z\right)}\,, \tag{2}$$

Since $\mathsf{E}(1) = 1$ by assumption, $p + (q_{\mathrm{h}}p/q) + q_{\mathrm{H}} = 1 - q_{\mathrm{h}}(1-p/q) = 1 - q_{\mathrm{h}}\epsilon/q$. It follows that $\mathsf{C}(1) = (q_{\mathrm{h}}\epsilon/q)/(1-(1-q_{\mathrm{h}}\epsilon/q)) = 1$; hence $\mathsf{C}(Z)$ is a probability generating function.

Instead of working directly with $\mathsf{E}(Z)$, we can work with a generating function $\hat{\mathsf{E}}(Z)$ which is identical to $\mathsf{E}(Z)$ for the initial ascending part but differs in the descending part. Specifically, in the descending part, the walk represented by $\hat{\mathsf{E}}(Z)$ descends as many levels as the number of steps it took to return to the origin. Clearly, $\mathsf{E}(Z) \preceq \hat{\mathsf{E}}(Z) \triangleq \mathsf{A}(Z\mathsf{D}(Z))/\mathsf{A}(1)$. Here, an individual term in $\mathsf{A}(Z\mathsf{D}(Z)) = \sum_i a_i Z^i \mathsf{D}(Z)^i$ has the interpretation "if the first ascent took i steps then immediately descend i levels." Since $\mathsf{A}(Z)$ is not a probability generating function, we have to normalize it by $\mathsf{A}(1)$ to make sure that the ascent happens with certainty. Writing

$$\mathsf{F}(Z) \triangleq pZ\mathsf{D}(Z) + q_{\mathrm{h}}Z\mathsf{A}(Z\mathsf{D}(Z)) + q_{\mathrm{H}}Z\,,$$

note that

$$\mathsf{C}(Z) \preceq \hat{\mathsf{C}}(Z) \triangleq (q_{\mathrm{h}}\epsilon/q)Z/(1-\mathsf{F}(Z))\,. \tag{3}$$

Since $\mathsf{F}(1) = p + q_{\mathrm{h}}p/q + q_{\mathrm{H}} = 1 - q_{\mathrm{h}}(1-p/q) = 1 - q_{\mathrm{h}}\epsilon/q$, we have $\hat{\mathsf{C}}(1) = 1$, i.e., $\hat{\mathsf{C}}(Z)$ is a probability generating function. It remains to establish a bound on the radius of convergence of $\hat{\mathsf{C}}$. A sufficient condition for the convergence of $\hat{\mathsf{C}}(z)$ for some $z \in \mathbb{R}$ is that all generating functions appearing in the definition of $\hat{\mathsf{C}}(z)$ converge at z and that $\mathsf{F}(z) \neq 1$.

The generating functions $\mathsf{D}(z)$ and $\mathsf{A}(z)$ converge when the discriminant $1-4pqz^2$ is positive; equivalently $|z| < 1/\sqrt{1-\epsilon^2} = 1+\epsilon^2/2 + O(\epsilon^4)$. In addition, conditioned on the convergence of $\mathsf{A}(z)$ and $\mathsf{D}(z)$, we can check that

$$\mathsf{A}(z) < 1/2qz \quad \text{and} \quad \mathsf{D}(z) < 1/2pz\,. \tag{4}$$

On the other hand, the convergence of $\mathsf{F}(z)$ depends on the convergence of $\mathsf{D}(z)$ and $\mathsf{A}(z\mathsf{D}(z))$. The convergence of $\mathsf{A}(z\mathsf{D}(z))$ is likewise determined by the positivity of its discriminant, i.e.,

$$1-(1-\epsilon^2)\left(z\cdot\frac{1-\sqrt{1-(1-\epsilon^2)z^2}}{(1-\epsilon)z}\right)^2 > 0\,.$$

The inequality above implies that if $\mathsf{A}(z\mathsf{D}(z))$ converges when

$$|z| < R_1 \triangleq \left(\left(2/\sqrt{1-\epsilon^2} - 1/(1+\epsilon)\right)/(1+\epsilon)\right)^{1/2}\,,$$

where

$$R_1 = 1+\epsilon^3/2 + O(\epsilon^4) \approx \exp\left(\epsilon^3(1+O(\epsilon))/2\right)\,. \tag{5}$$

Note that the radius of convergence of $\mathsf{A}(Z\mathsf{D}(Z))$ is smaller than that of $\mathsf{A}(Z)$ or $\mathsf{D}(Z)$.

It is easy to check that when $\mathsf{F}(z)$ converges, it satisfies

$$\mathsf{F}(z) \le \mathsf{F}(|z|)\,.$$

The claim is trivial for $z = 0$. Otherwise, note that $\mathsf{D}(z)$ is an odd function and hence, $z\mathsf{D}(z) = |z|\,\mathsf{D}(|z|)$. Thus, for the claim to hold, we need only show that $z\,(q_{\mathrm{h}}\mathsf{A}(z\mathsf{D}(z)) + q_{\mathrm{H}}) \le |z|\,(q_{\mathrm{h}}\mathsf{A}(|z|\mathsf{D}(|z|)) + q_{\mathrm{H}})$. But the right-hand side equals $|z|\,(q_{\mathrm{h}}\mathsf{A}(z\mathsf{D}(z)) + q_{\mathrm{H}})$ and $\mathsf{A}(x) > 0$ for real $x > 0$, we can divide both sides by $q_{\mathrm{h}}\mathsf{A}(z\mathsf{D}(z)) + q_{\mathrm{H}}$. The reduced inequality becomes $z/|z| \le 1$. However, $z/|z| = \pm 1$ for any non-zero real z. Therefore, it suffices for us to require that $F(z) \neq 1$ for $z > 0$.

We can also check that

$$F(z) \text{ is convex and increasing for } z \in [0, R_1)\,. \tag{6}$$

To see why, note that since z^2 is convex in z, $(1-4pqz^2)$ is concave. Since square root is non-decreasing and convex for positive z, $\sqrt{1-4pqz^2}$ is concave and consequently, $-\sqrt{1-4pqz^2}$ is convex. Since $1/z^2$ is convex, it follows that $\mathsf{D}(z)$ and, by a simliar reasoning, $\mathsf{A}(z)$ are convex. Next, observe that $\mathsf{A}(z\mathsf{D}(z))$ converges for $z \in [0, R_1)$ and hence it is also convex in z. Thus $\mathsf{F}(z)$ turns out to be a convex combination of convex functions; it follows that $F(z)$ is convex for $z \in (0, R_1)$. In addition, since $\mathsf{F}(0) = 0$ and $\mathsf{F}(1) > 0$, $\mathsf{F}(z)$ must be increasing as well.

Let

$$R_2 \text{ be the solution to the equation } \mathsf{F}(z) = 1, z > 0\,.$$

Then $\hat{\mathsf{C}}(z)$ would converge for $|z| < R \triangleq \min(R_1, R_2)$. It remains to characterize R_2 in terms of ϵ and q_{h}. Note that $R_1 < 2$ as long as $\epsilon \leq 0.97$. Since the final bounds will be only asymptotic in ϵ, it suffices for us to consider small ϵ. That is to say, we consider the case where $0 < z < R_1 < 2$, i.e., $z - 1 < 1$.

If we express $\mathsf{F}(z)$ as its power series around $z = 1$, we can check that

$$\begin{aligned}
\mathsf{F}(1) &= 1 - \epsilon q_{\mathrm{h}}/q\,,\\
\mathsf{F}''(1) &= \frac{1-\epsilon}{\epsilon^5}\left(q_{\mathrm{h}}(1+3\epsilon) + q_{\mathrm{H}}\epsilon^2\right)\,, \quad \text{and}\\
\mathsf{F}'(1) &= p(1+1/\epsilon) + q_{\mathrm{h}}(p/q)\big(1 + (1+1/\epsilon)/\epsilon\big) + q_{\mathrm{H}}\,.
\end{aligned}$$

Since $\mathsf{F}''(1) > 0$ and $\mathsf{F}(z)$ is convex and increasing, the first-order approximation

$$f(z) = (1 - \epsilon q_{\mathrm{h}}/q) + \mathsf{F}'(1)(z-1) \tag{7}$$

is a lower bound for $\mathsf{F}(z)$ when $1 \leq z < R_1$. The approximation error at any $z \in (1,2)$ is $\mathsf{F}(z) - f(z) = O(h(z))$ where we define

$$h(z) \triangleq \mathsf{F}''(1)(z-1)^2\,.$$

Since the bounds we develop will have the asymptotic notation $\Theta(\cdot)$ in the exponent, it suffices to ensure that $R_2 = \Theta(R_2^*)$. In the exposition below, we will only develop approximations R_2^* satisfying $R_2 = (1-\theta)R_2^*$ for a small positive constant $\theta \in (0,1)$.

In the special case $q_{\mathrm{H}} = 0$, $\mathsf{F}(Z)$ simplifies as $\mathsf{F}(Z) = pZ\mathsf{D}(Z) + qZ\mathsf{A}(Z\mathsf{D}(Z))$. Note that $\mathsf{F}(Z)$ converges when $\mathsf{A}(Z\mathsf{D}(Z))$ does and it is not hard to check that $\mathsf{F}(z) < 1$. Specifically, we know that $\mathsf{F}(z)$ converges when $z \in [0, R_1)$ and when it does, we claim that $\mathsf{F}(z) < 1$. Specifically, when $z \in [0,1]$, $\mathsf{F}(z) \leq \mathsf{F}(1) = 1 - \epsilon q_{\mathrm{h}}/q = 1 - \epsilon < 1$ since $\epsilon < 1$. On the other hand, we can check that $\mathsf{D}(z)$ is convex for $z \geq 0$ and, in particular, the first order approximation $1 + (z-1)/\epsilon$ around $z = 1$ is a lower bound for $\mathsf{D}(z), z \geq 1$. It follows that $\mathsf{D}(z) \geq 1$ for $z \in [1, R_1)$. Consequently, $\mathsf{F}(z) \leq pZ\mathsf{D}(Z) + qz\mathsf{A}(z\mathsf{D}(z)) \cdot \mathsf{D}(z) = pz\mathsf{D}(z) + qx\mathsf{A}(x) < 1/2 + 1/2 = 1$ where we write $x = z\mathsf{D}(z)$ and use (4). Thus the radius of convergence of $\hat{\mathsf{C}}$ is R_1 if $q_{\mathrm{H}} = 0$.

The remainder of the exposition considers the general case $0 < q_{\mathrm{h}} < q$. Let the solution to the equation $f(z) = 1$ be denoted by

$$R_2^* \triangleq 1 + \epsilon(q_{\mathrm{h}}/q)/\mathsf{F}'(1)\,.$$

If q_{h} is small, $q = (1+\epsilon)/2$, $p + \epsilon = q$ and $p/q^3 \in [1,4]$, we can check that

$$h(R_2^*) = O\left(\frac{pq}{\epsilon^3} \cdot \left(\frac{\epsilon^2 q_h/q}{p(1+\epsilon)+\epsilon q}\right)^2\right) = O\left(\frac{\epsilon q_{\mathrm{h}}^2 \cdot pq}{q^2\,(p+\epsilon)^2}\right) = O\left(\frac{\epsilon q_{\mathrm{h}}^2 \cdot p}{q^3}\right) = O(\epsilon q_{\mathrm{h}}^2)\,,$$

i.e., it vanishes. Thus $f(z)$ is a good approximation for $\mathsf{F}(z)$. It follows that $\mathsf{F}'(1) \approx p(1+1/\epsilon) + q = q/\epsilon$ and, therefore,

$$R_2^* \approx 1 + (\epsilon q_{\mathrm{h}}/q)/(q/\epsilon) = 1 + q_{\mathrm{h}}(\epsilon/q)^2 \approx \exp(\epsilon^2 q_{\mathrm{h}}/q^2) = e^{O(\epsilon^2 q_{\mathrm{h}})}$$

since $q \in (1/2, 1)$. (Although we have an asymptotic notation, it is important that we have the right exponenet on q_{h}.)

If, on the contrary, $q_{\mathtt{h}} = O(1)$ but ϵ vanishes then $\mathsf{F}'(1)$ will be dominated by its second term; that is to say, $\mathsf{F}'(1) \approx q_{\mathtt{h}}(p/q)(1 + (1 + 1/\epsilon)/\epsilon) = O(q_{\mathtt{h}}/\epsilon^2)$ and, therefore,

$$R_2^* \approx 1 + O\left((\epsilon q_{\mathtt{h}}/q)/(q_{\mathtt{h}}/\epsilon^2)\right) = 1 + O(\epsilon^3) = e^{O(\epsilon^3)}$$

since $q \approx 1/2$.

Recall that $R_1 = \exp\left(O(\epsilon^3(1 + O(\epsilon)))\right)$. It follows that $\hat{\mathsf{C}}(z)$ converges for $|z|$ less than

$$R = \exp\left(O(\min(\epsilon^3, \epsilon^2 q_{\mathtt{h}}))\right) . \tag{8}$$

Recall that if the radius of convergence of $\hat{\mathsf{C}}$ is $\exp(\delta)$ then $\Pr[H]$—which is a geometric sum—is at most $O(1) \cdot \exp(-\delta k)$. We conclude that for large k,

$$\Pr[H] \le O(1) \cdot e^{-k \ln R} = \exp\left(-k \cdot \Omega(\min(\epsilon^3, \epsilon^2 q_{\mathtt{h}}))\right) .$$

Case 2: x is non-empty. Next, let us consider the case when $x \neq \varepsilon$, i.e., $|x| \ge 1$. Let $m = |x|$ and write $w = xyz$ where $|y| = k$. Recall the processes (W_t) and (S_t) defined on w and, in addition, define $M = (M_t : t \in \mathbb{N}), M_t = \min_{0 \le i \le t} S_i$ and $X = (X_t : t \in \mathbb{N}), X_t = S_t - M_t$. By convention, set $M_0 = X_0 = 0$. Thus X_t denotes the height of the walk S, at time t, with respect to its minimum M_t.

For a fixed value $h = X_m$, the relevant generating function would be $\mathsf{D}(Z)^h \hat{\mathsf{C}}$. Hence the final generating function we seek is

$$\tilde{\mathsf{C}}(Z) \triangleq \sum_{h=0}^{\infty} \Pr[X_m = h] \cdot \mathsf{D}(Z)^h \hat{\mathsf{C}}(Z)$$

whose tth coefficient is the probability that t is a Catalan slot in y.

Note that $X = (X_t)$ is an ϵ-downward biased random walk on non-negative integers with a reflective barrier at -1. Specifically, for any $h \in \mathbb{N}$, $\Pr[X_t = h \mid X_{t-1} = h - 1] = p$ and $\Pr[X_t = h - 1 \mid X_{t-1} = h] = \Pr[X_t = 0 \mid X_{t-1} = 0] = q$. In [4, Lemma 6.1], it is proved that the distribution of X_m is stochastically dominated by the distribution of X_∞, written $\mathcal{X}_\infty$ and defined, for $k = 0, 1, 2, \ldots$, as

$$\mathcal{X}_\infty(k) = \Pr[X_\infty = k] \triangleq \left(\frac{2\epsilon}{1+\epsilon}\right) \cdot \left(\frac{1-\epsilon}{1+\epsilon}\right)^k = (1-\beta)\beta^k \tag{9}$$

where $\beta \triangleq (1-\epsilon)/(1+\epsilon)$. Let

$$\{\mathcal{X}_\infty(k)\} \overset{\text{gf}}{\longleftrightarrow} \mathsf{X}_\infty(Z) = \frac{1-\beta}{1-\beta Z} .$$

It follows that $\tilde{\mathsf{C}}(Z)$ is dominated by

$$\sum_{h=0}^{\infty} \mathcal{X}_\infty(h) \mathsf{D}(Z)^h \hat{\mathsf{C}}(Z) = \mathsf{X}_\infty(\mathsf{D}(Z)) \hat{\mathsf{C}}(Z) = \frac{(1-\beta)\hat{\mathsf{C}}(Z)}{1 - \beta \mathsf{D}(Z)} .$$

Let $\star$ denote the quantity above. For it to converge, we need to check that $\mathsf{D}(Z)$ should never converge to $1/\beta$. Since the radius of convergence of $\mathsf{D}(Z)$—which is $(1-\epsilon^2)^{-1/2}$—is strictly less than $(1+\epsilon)/(1-\epsilon)$ for $\epsilon > 0$, we conclude that $\star$ converges if both $\mathsf{D}(Z)$ and $\hat{\mathsf{C}}(Z)$ converge. The radius of convergence of $\star$ would be the smaller of the radii of convergence of $\mathsf{D}(Z)$ and $\hat{\mathsf{C}}(Z)$. We already know from the previous analysis that $\hat{\mathsf{C}}(Z)$ has the smaller radius of convergence of these two; therefore, the bound on $\Pr[H]$ from the previous case holds for $|x| \ge 0$. □

6.2 Proof of Bound 2

Let $p = (1-\epsilon)/2$ and $q = 1 - p$; thus $q - p = \epsilon$. Define the process $W = (W_t : t \in \mathbb{N}), W_t \in \{\pm 1\}$ as $W_t = 1$ if and only if $w_t = \mathtt{A}$. Let $S = (S_t : t \in \mathbb{N}), S_t = \sum_{i \le t} W_i$ be the position of the particle at time t. Thus S is a random walk on $\mathbb{Z}$ with ϵ negative (i.e., downward) bias. By convention, set $W_0 = S_0 = 0$.

Case 1: x is an empty string. In this case, we write $w = yz$ so that $|y| = k$. Let m_t denote the probability that t is the first index so that both t and $t+1$ are Catalan slots in w, with $m_0 = 0$, and consider the probability generating function $\{m_t\} \stackrel{\text{gf}}{\longleftrightarrow} \mathsf{M}(Z) = \sum_{t=0}^{\infty} m_t Z^t$. Controlling the decay of the coefficients m_t suffices to give a bound on $\Pr[H]$, i.e., the probability that y *does not* contain two consecutive Catalan slots, because this probability is at most $1 - \sum_{t=0}^{k-1} m_t = \sum_{t=k}^{\infty} m_t$. To this end, we develop a closed-form expression for a related probability generating function $\hat{\mathsf{M}}(Z) = \sum_t \hat{m}_t Z^t$ which stochastically dominates $\mathsf{M}(Z)$. Recall that this means that for any k, $\sum_{t \geq k} m_k \leq \sum_{t \geq k} \hat{m}_k$. Finally, bound the latter sum by using the analytic properties of $\hat{\mathsf{M}}(Z)$.

Recall the "first ascent" and "first descent" generating functions $\mathsf{A}(Z)$ and $\mathsf{D}(Z)$ from the proof of Bound 1. We wish to devise the generating function for the first occurrence of a left-Catalan slot immediately followed by a right-Catalan slot. To that end, note that $\mathsf{D}(Z)$ is the generating function for the first left-Catalan slot. The generating function for the first right-Catalan slot can be devised as follows. Consider the walk S starting at the origin. With probability $q(1 - p/q) = \epsilon$, the walk will immediately descend a step and never return to the origin. But this means $S_1 \leq S_t, t \geq 2$ and hence the first slot is a right-Catalan slot and we are done. Otherwise, i.e., with probability $1 - \epsilon$, the walk makes a (guaranteed) return to the origin in future. In this case, we will have to restart our search for the next consecutive Catalan slots but, before that, we will have to ensure that we are in a "safe position." In particular, we can safely restart our search if Specifically, if the current position (i.e., level) of the walk is at its historical minimum, we can restart our search by applying $\mathsf{D}(Z)$ to find the next left-Catalan slot. Thus an "epoch" begins with a guaranteed return and ends when the walk descends to a new level for the first time. Let $\mathsf{E}(Z)$ be the generating function of an epoch. Thus we can write

$$\begin{aligned} \mathsf{M}(Z) &= \mathsf{D}(Z) \cdot \{\epsilon + (1-\epsilon)\mathsf{E}(Z)\mathsf{M}(Z)\} \\ &= \frac{\epsilon \mathsf{D}(Z)}{1 - (1-\epsilon)\mathsf{E}(Z)} \,. \end{aligned} \tag{10}$$

An epoch can have two shapes. If an epoch starts with an up-step (i.e., an "up" shape), it is easy to see that the epoch ends as soon as the walk returns to the origin from above and, importantly, that the walk will (eventually) return to the origin with probability one. However, if the epoch starts with a down-step (i.e., a "down" shape), we have to "remember" the lowest level ℓ touched by the walk in its way to its (sure) ascent to the origin and then descend ℓ levels to end the epoch. In particular, we have to ensure that we return to the origin with probability one.

A generating function of a stopping time of a random walk is ill suited to "remember" its historical minimum/maximum. However, it can remember the length of the walk for free. Thus, instead of working directly with $\mathsf{E}(Z)$, we work with a generating function $\hat{\mathsf{E}}(Z)$ which is identical to $\mathsf{E}(Z)$ for the up shape but differs in the down shape. Specifically, in the down shape, the walk represented by $\hat{\mathsf{E}}(Z)$ descends as many levels as the number of steps it took to return to the origin. Clearly, $\mathsf{E} \preceq \hat{\mathsf{E}}$ where

$$\hat{\mathsf{E}}(Z) \triangleq pZ\mathsf{D}(Z) + qZ\mathsf{A}(Z\mathsf{D}(Z))/\mathsf{A}(1)\,.$$

Here, the first term denotes the "return to origin from above" shape. An individual term in $\mathsf{A}(Z\mathsf{D}(Z)) = \sum_t a_t Z^t \mathsf{D}(Z)^t$ has the interpretation "if the first ascent took t steps then follow it by descending t levels." Since $\mathsf{A}(Z)$ is not a probability generating function, we have to normalize it by $\mathsf{A}(1)$ to denote that the ascent happens with certainty. This implies,

$$\mathsf{M}(Z) \preceq \hat{\mathsf{M}}(Z) \triangleq \frac{\epsilon \mathsf{D}(Z)}{1 - (1-\epsilon)\hat{\mathsf{E}}(Z)}$$

It remains to establish a bound on the radius of convergence of $\hat{\mathsf{M}}$. A sufficient condition for the convergence of $\hat{\mathsf{M}}(z)$ for some $z \in \mathbb{R}$ is that all generating functions appearing in the definition of $\hat{\mathsf{M}}$ converge at z and that $(1-\epsilon)\hat{\mathsf{E}}(Z) \neq 1$.

By retracing our footsteps as in the proof of Bound 1, we can see that $\mathsf{D}(z)$, $\mathsf{A}(z)$, and $\mathsf{A}(z\mathsf{D}(z))$ converge when $|z|$ satisfies (5). Moreover, since $\mathsf{D}(Z)$ is a probability generating function, it follows that $\hat{\mathsf{E}}(Z)$ is stochastically dominated by $pZ\mathsf{D}(Z) + qZ\mathsf{A}(Z\mathsf{D}(Z))/\mathsf{A}(1) \cdot \mathsf{D}(Z)$. Therefore, when $\hat{\mathsf{E}}(z)$ converges for some z, it satisfies

$$\begin{aligned}\hat{\mathsf{E}}(z) &\le pz\mathsf{D}(z) + (q/p)(qz\mathsf{D}(z))\mathsf{A}(z\mathsf{D}(z)) \\ &< 1/2 + (q/p)/2\end{aligned}$$

since $\mathsf{A}(1) = p/q$, $pz\mathsf{D}(z) < 1/2$, and $qx\mathsf{A}(x) < 1/2$ for any z, x so that $\mathsf{A}(x)$ and $\mathsf{D}(z)$ converge, respectively. Therefore, $(1-\epsilon)\hat{\mathsf{E}}(z) = 2p\hat{\mathsf{E}}(z) < p + q = 1$. It follows that $\hat{\mathsf{M}}(z)$ converges for $|z| < 1 + \epsilon^3/2 + O(\epsilon^4) \le \exp(\epsilon^3/2 + O(\epsilon^4))$. Recall that if the radius of convergence of $\hat{\mathsf{M}}$ is $\exp(\delta)$ then $\Pr[H]$ is at most $O(1) \cdot \exp(-\delta k)$. We conclude that

$$\Pr[H] \le O(1) \cdot e^{-\epsilon^3(1+O(\epsilon))k/2} . \tag{11}$$

Case 2: x is non-empty. This part of the proof is the same as the $|x| \ge 1$ case in the proof of Bound 1. The only difference is that $\hat{\mathsf{C}}(Z)$ and $\tilde{\mathsf{C}}(Z)$ would be replaced by $\hat{\mathsf{M}}(Z)$ and $\tilde{\mathsf{M}}(Z)$, respectively, where

$$\tilde{\mathsf{M}}(Z) \le \sum_{h=0}^{\infty} \mathcal{X}_\infty(h)\mathsf{D}(Z)^h \hat{\mathsf{M}}(Z) .$$

We conclude that the bound in (11) holds when $|x| \ge 0$. □

7 The semisynchronous setting

We set the stage by stating the Δ-synchronous model.

Definition 11 (Semisynchronous characteristic string)**.** *Let $sl_1, \dots, sl_n$ be a sequence of slots. A* semisynchronous characteristic string *w is an element of $\{\mathtt{h}, \mathtt{H}, \mathtt{A}, \perp\}^n$ defined for a particular execution of a blockchain protocol on these slots so that for $t \in [n]$, $w_t = \perp$ if sl_t was assigned to no participants; otherwise, $w_t = \mathtt{A}$ if sl_t was assigned to an adversarial participant; otherwise, $w_t = \mathtt{h}$ if sl_t was assigned to a single honest participant; otherwise $w_t = \mathtt{H}$.*

In the Δ-synchronous setting, axiom **A4** is replaced by

A4$_\Delta$. In a Δ-synchronous execution, if two honestly generated blocks B_1 and B_2 are labeled with slots sl_1 and sl_2 for which $sl_1 + \Delta < sl_2$, then the length of the unique blockchain terminating at B_1 is strictly less than the length of the unique blockchain terminating at B_2.

Definition 12 (Δ-Fork)**.** *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}, \perp\}^n$, $\Delta \in \{0, 1, 2, \dots\}$, $P = \{i : w_i = \mathtt{h}\}$, and $Q = \{j : w_j = \mathtt{H}\}$. A* Δ-fork *for the semisynchronous string w consists of a directed and rooted tree $F = (V, E)$ with a labeling $\ell : V \to \{0, 1, \dots, n\}$. We insist that each edge of F is directed away from the root vertex and further require that*

(F1.) the root vertex r has label $\ell(r) = 0$;

(F2.) the labels of vertices along any directed path are strictly increasing;

(F3.) each index $i \in P$ is the label of exactly one vertex of F and, in addition, each index $j \in Q$ is the label of at least two vertices of F; and

(F4.) for any indices $i, j \in P \cup Q$, if $i + \Delta < j$ then the depth of a vertex with label i is strictly less than the depth of a vertex with label j.

If F is a Δ-fork for the semisynchronous characteristic string w, we write $F \vdash_\Delta w$. Note that the conditions (F1)–(F4) above are direct analogues of the axioms **A1**– **A3** and axiom **A4$_\Delta$** above. Note that the synchronous fork in Definition 2 is a Δ-fork with $\Delta = 0$. We sometimes emphasize this fact by writing $F' \vdash_0 w'$ where w' is a synchronous characteristic string and F' is a synchronous fork.

Definition 13 (Reduction map). *For $\Delta \in \mathbb{N}$, we define the function $\rho_\Delta : \{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^* \to \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ inductively as follows: $\rho_\Delta(\varepsilon) = \varepsilon$ and for $w \in \{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$,*

$$\rho_\Delta(bw) = \begin{cases} \rho_\Delta(w) & \text{if } b = \perp\,, \\ b\rho_\Delta(w) & \text{if } b \in \{\mathtt{h}, \mathtt{H}\} \text{ and } \{\perp, \mathtt{A}\}^\Delta \preceq w\,, \\ \mathtt{A}\rho_\Delta(w) & \text{otherwise}\,. \end{cases} \tag{12}$$

In the above definition, if $w' = \rho_\Delta(w)$ and $A = \{i : w_i \neq \perp\}$ then note that $|A| = |w'|$. Also note that the reduction ρ_Δ implicitly defines a bijective, increasing function $\pi : A \to |w'|$.

Definition 14 (Δ-settlement with parameters $s, k \in \mathbb{N}$). *Let $n \in \mathbb{N}$ and let $w \in \{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^n$. Let $t \in [s + k, n]$ be an integer, $\hat{w} \preceq w$, $|\hat{w}| = t$, and let F be any Δ-fork for $\hat{w}$. We say that a slot s is* not (k, Δ)-settled in F *if F contains two maximally long tines $\mathcal{C}_1, \mathcal{C}_2$ so that at least one of these tines contains a vertex with label s, both tines contain at least k vertices after slot s, and the label of their last common vertex is at most $s - 1$. Otherwise, we say that* slot s is (k, Δ)-settled in F. *We say that* slot s is (k, Δ)-settled in w *if, for each $t \geq s + k$, it is (k, Δ)-settled in every Δ-fork $F \vdash \hat{w}$ where $\hat{w} \preceq w$, $|\hat{w}| = t$.*

Note that in the above definition, we truncated k trailing blocks from a tine whereas in Definition 3, we truncated from a tine all trailing blocks corresponding to the last k slots. Note that this change of perspective is necessary since w may contain $\perp$ symbols, i.e., empty slots.

Let $f \in (0, 1)$, $\Delta \in \mathbb{N}$ and write $\alpha = (1 - f)^\Delta$. Let $p_\perp, p_\mathtt{h}, p_\mathtt{H}, p_\mathtt{A} \in (0, 1)$ so that $p_\perp = 1 - f$ and $p_\mathtt{h} + p_\mathtt{H} + p_\mathtt{A} = f$. Let $B = B_{f,\Delta,T}$ denote a list of independent and identically distributed random variables B_i, $i \in [T]$, $B_i \in \{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}$ so that $\Pr[B_i = \sigma] = p_\sigma$ for $\sigma \in \{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}$.

Theorem 5 (Main theorem; Δ-synchronous setting). *Let $s, k, T, \Delta \in \mathbb{N}$, $T \geq s + k + \Delta$, $w \in \{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$. Let $f, \epsilon \in (0, 1)$ and suppose that the random variable B defined above (using parameters f, Δ, and T) additionally satisfies*

$$p_\mathtt{A} \cdot \alpha / f = (1 - \epsilon)/2 - (1 - \alpha)\,. \tag{13}$$

Let $\mathcal{B}$ be the distribution of B. Let S be the event that slot s is not (k, Δ)-settled in w. Then $\Pr_{w \sim \mathcal{B}}[S] \leq e^{-k \cdot \Theta(\min(\epsilon^3, \epsilon^2 p_\mathtt{h})) + \Delta}$. (Here, the asymptotic notation hides constants that do not depend on ϵ or k.) Let $\mathcal{W}$ be a distribution on $\{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ so that $\mathcal{W} \preceq \mathcal{B}$. Then $\Pr_{w \sim \mathcal{W}}[S] \leq \Pr_{w \sim \mathcal{B}}[S]$.

The condition (13) reflects (and quantifies) the fact that the adversarial probability is amplified by the reduction map ρ_Δ but we still want it to be bounded from above by $1/2$. The amplification is inevitable since the map ρ_Δ turns an $\mathtt{h}$ or $\mathtt{H}$ symbol into an $\mathtt{A}$ symbol with a constant probability.

The main observation for proving the theorem above is that a Δ-settlement violation in w, implies a certain combinatorial event (parameterized by Δ) in a prefix of $\rho_\Delta(w)$ that can be analyzed using techniques similar to those used in proving Theorem 1.

7.1 Some structural and stochastic ingredients

Let $w \in \{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$, $w' = \rho_\Delta(w)$, $n = |w|$, and $m = |\rho_\Delta|$. Our roadmap forward is as follows:

1. Show that there is a bijection between Δ-forks for w and synchronous forks for w'. In particular, for each Δ-fork $F \vdash_\Delta w$ there is an isomorphic synchronous fork $F' \vdash_0 w'$ and a bijective map $\{i \in [n] : w_i \neq \perp\} \to [m]$. This is shown in Proposition 1.

2. Since the decisions made by ρ_Δ at each slot depends on the Δ future slots, the distribution of the last few symbols of $\rho_\Delta(w)$ will be "distorted" no matter how w is distributed. Assuming w has i.i.d. symbols, we need to identify a prefix $b \prec \rho_\Delta(w)$ whose symbols are i.i.d. as well. This is done in Lemma 2.

3. Show that if w violates Δ-settlement then the aforementioned prefix b violates *some* combinatorial event. It is important that we can analyze this event using the techniques and results we have already established. This is done in Lemma 1.

4. Obtain a bound on this probability. This is done in Bound 3.

5. Prove Theorem 5.

Proposition 1. *Let $w \in \{\bot, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ and $w' = \rho_\Delta(w)$. Then, for every Δ-fork $F \vdash w$ there is a synchronous fork $F' \vdash_0 w'$ which is isomorphic to F. F' is called the* image of F under ρ_Δ.

Proof sketch. Let F' be a copy of F. Establish the natural bijection $m : V(F) \to V(F')$ given by the copying proess, i.e., $u \mapsto m(u)$, and relabel the vertices as

$$\ell(m(u)) = \pi(\ell(u)) \text{ for each vertex } u \in F\,. \tag{14}$$

Set $r(F') = m(r(F))$ and $\ell(r(F')) = 0$. It suffices to check that $F' \vdash_0 w'$, i.e., F' is a valid (synchronous) fork for w'. Specifically, if there are two honest slots h_1, h_2 in w within a distance Δ of each other, then the former honest slot is mapped to an adversarial slot in w'. Therefore, in F', an honest vertex is aware of all honest vertices with smaller labels. □

For any string $x = x_1 x_2 \ldots, n = |x|$ on any alphabet and any $k \in \mathbb{N}$, define $x^{\lceil k} \triangleq x_1 \ldots x_{n-k}$.

Proposition 2. *Let $T \in \mathbb{N}$, $w = w_1 \ldots w_T \in \{\bot, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a sequence of i.i.d. symbols, and define $p_\sigma \triangleq \Pr[w_1 = \sigma]$ for each $\sigma \in \{\bot, \mathtt{h}, \mathtt{H}, \mathtt{A}\}$. Let $x = \rho_\Delta(w)$ and let $\ell = |x|$. Write $f = 1 - p_\bot$ and $\alpha = (1-f)^\Delta$. Then the symbols in the string $x^{\lceil \Delta}$ are i.i.d. with*

$$\begin{aligned} \Pr[x_i = \mathtt{h}] &= p_\mathtt{h} \cdot \alpha / f\,, \\ \Pr[x_i = \mathtt{H}] &= p_\mathtt{H} \cdot \alpha / f\,, \quad \textit{and} \\ \Pr[x_i = \mathtt{A}] &= 1 - \alpha + p_\mathtt{A} \cdot \alpha / f \end{aligned} \tag{15}$$

for each $i \in [\ell - \Delta]$.

Proof. First let us pretend for a moment that $T = \infty$; then $\ell = \infty$ as well. Let us write the infinite sequence w as a concatenation of segments of $\bot$s punctuated by a single non-$\bot$ symbol. That is, write $w = b_0 e_1 b_1 e_2 b_2 \ldots$ where, for $i = 0, 1, \ldots, b_i = \bot^*$ and $e_i \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}$. The reduction map ρ_Δ translates a segment $e_i b_i$ into a symbol z_i as follows:

$$z_i = \begin{cases} \mathtt{A} & \text{if } e_i = \mathtt{A} \text{ or } |b_i| \le \Delta - 1 \\ e_i & \text{if } e_i \in \{\mathtt{h}, \mathtt{H}\} \text{ and } |b_i| \ge \Delta\,. \end{cases}$$

In particular, the segments $e_i b_i$ as well as the events that determine the value of an z_i are disjoint. Therefore, the symbols in the infinite sequence $z_1 z_2 \ldots = \rho_\Delta(w_1 w_w \ldots)$ are independent and identically distributed.

If T is finite, however, the last Δ symbols of $x = \rho_\Delta(w)$ are "distorted" in that the translated symbols in this region will be more favored to be As. However, since the last Δ symbols of x must correspond to at least Δ trailing symbols of w, it follows that $x_1 \ldots x_{\ell-\Delta}$ is a prefix of $z_1 z_2 \ldots$.

It remains to compute the probabilities. Let $q_\sigma = \Pr[z_i = \sigma]$ for any i and $\sigma \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}$. Then $q_\mathtt{h} = p_\mathtt{h}/(1-p_\bot)p_\bot^\Delta = p_\mathtt{h}\alpha/f, q_\mathtt{H} = p_\mathtt{H}\alpha/f$, and $q_\mathtt{A} = 1 - (q_\mathtt{h} + q_\mathtt{H}) = 1 - (p_\mathtt{h} + p_\mathtt{H})\alpha/f = 1 - (f - p_\mathtt{A})\alpha/f = 1 - \alpha + p_\mathtt{A}\alpha/f$. □

The following lemma connects a Δ-settlement violation in $w \in \{\bot, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ to a combinatorial event in $\rho_\Delta(w)^{\lceil \Delta} \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$.

Lemma 1. *Let $w \in \{\bot, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^*, \Delta, s, k \in \mathbb{N}$ so that $|x| = s$ and $x_s \neq \bot$. Let $w' = \rho_\Delta(w)$ and write $w' = x'y'z'a'$ so that $|a'| = \Delta$ and $|y'| \ge 1 + \Delta$. Let E_y be the event that there are at least $1 + \Delta$ slots in y' that are Catalan in $x'y'z'$ and, in addition, that the earliest one of these slots is uniquely honest. Then E_y implies that s is $(|y'|, \Delta)$-settled in w.*

We insist that the event E_y in the lemma is sufficient, but not necessary, for the conclusion to hold.[3]

[3] In fact, there are other combinatorial events that lead to tighter tail bounds; we defer the relevant analysis for a future version of this manuscript.

Proof. Let π be the bijection described after Definition 13. Note that $|x'| = \pi(s)$. Let the slots $c_i', i \in [1+\Delta]$ be Catalan in $x'y'z'$ so that $|x'| < c_1 < \cdots < c_{1+\Delta} \le |x'y'|$. By assumption, c_1' is uniquely honest. Note that c_i' may not be Catalan in w'. However, the suffix a' can "destroy" at most Δ of the Catalan slots $c_2', \ldots, c_{1+\Delta}'$—starting from $c_{1+\Delta}'$ and moving backwards. In particular, the slot c_1' will remain a uniquely honest Catalan slot in w'. Therefore, by Theorem 3, c_1' has the UVP in w'. Let c be the integer satisfying $c_1' = \pi(c)$.

Let $b \preceq xyz, |b| \ge |xy|$ and $b' = \rho_\Delta(b) \preceq x'y'z'$. (Necessarily, $|b'| \ge |x'y'|$.) Since the reduction map gives an isomorphism between every Δ-fork for b and its unique image (which is a synchronous fork for b') under the reduction ρ_Δ, it follows that c has the UVP in w.

For any Δ-fork $F \vdash_\Delta b$, let $u \in F, \ell(u) = c$ be the unique vertex contained by every tine $t \in F$ viable at the onset of any slot after c. Consider all tines $\tau \in F$ so that τ has at least $|y'|$ vertices with label at least $s+1$. and τ is viable at the onset of slot $\ell(\tau)+1$. Since $\ell(\tau) \ge |xy| \ge c$, it follows that $u \preceq \tau$. Thus all these tines τ agree about slot s since $s < c = \ell(u)$. In particular, if F contains two maximally long tines τ_1, τ_2, each with at least $|y'|$ vertices after slot s, then they would agree about slot s. In fact, $\ell(\tau_1 \cap \tau_2) \ge c > s$. Hence s must be $(|y'|, \Delta)$-settled in F and, since F was arbitrary, s must be $(|y'|, \Delta)$-settled in w. □

Bound 3. *Let $\epsilon, q_{\mathtt{h}}, q_{\mathtt{H}} \in (0,1)$ so that $q_{\mathtt{h}} + q_{\mathtt{H}} = (1+\epsilon)/2$. Let $w' \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ be a characteristic string, written $w' = x'y'z'$, where both $|x'|$ and $|z'|$ are allowed to go to ∞ and the w_i's are i.i.d. random variables with $\Pr[w_i' = \mathtt{A}] = (1-\epsilon)/2, \Pr[w_i' = \mathtt{h}] = q_{\mathtt{h}}$, and $\Pr[w_i' = \mathtt{H}] = q_{\mathtt{H}}$. Let $k = |y'|$. Let $\Delta \in \mathbb{N}$ and let E be the event that y' contains $1+\Delta$ slots, each Catalan in w', and the first of these Catalan slots is uniquely honest. Then $\Pr[E$ does not happen$]$ is at most $O\left(k^\Delta b(k,\epsilon)\right)$ where $b(k,\epsilon)$ is the right-hand side in the probability in Bound 1.*

Proof.

Case: $|x'| = 0$. The generating function of interest is $\mathsf{L}(Z) \triangleq \mathsf{C}(Z)^{1+\Delta}$ where $\mathsf{C}(Z)$ is defined in (2). Recall that $\mathsf{C}(Z)$ is stochastically dominated by $\hat{\mathsf{C}}(Z)$; see (3). The radius of convergence of $\hat{\mathsf{L}}(Z) \triangleq \hat{\mathsf{C}}(Z)^{1+\Delta}$ is the same as that of $\hat{\mathsf{C}}(Z)$, i.e., R defined in (8). Since $\mathsf{L}(Z)$ is the convolution of $m = 1+\Delta$ identical generating functions, its kth coefficient is

$$\ell_n = \sum_{\substack{k_1,\ldots,k_m \\ k_1+\cdots+k_m = k}} O(1) \cdot R^{-k}\,.$$

But this equals $O(1) \binom{k}{k_1,\ldots,k_m} R^{-k}$ which is at most $O(1)\, k^{m-1} \cdot R^{-k} = e^{-k \ln R + \Delta \ln k}$. Since this decreases geometrically for large k, We conclude that

$$\Pr[E \text{ does not happen} \mid x' \text{ is empty}] \le O(1)\, e^{-k \ln R + \Delta \ln k}\,. \tag{16}$$

Case: $|x'| \ge 1$. This part of the proof is the same as the $|x| \ge 1$ case in the proof of Bound 1. The only difference is that $\hat{\mathsf{C}}(Z)$ and $\tilde{\mathsf{C}}(Z)$ would be replaced by $\hat{\mathsf{L}}(Z)$ and $\tilde{\mathsf{L}}(Z)$, respectively, where

$$\tilde{\mathsf{L}}(Z) \preceq \sum_{h=0}^{\infty} \mathcal{X}_\infty(h) \mathsf{D}(Z)^h \hat{\mathsf{L}}(Z)\,.$$

As we did in that proof, we conclude that $\Pr[E$ does not occur$]$ is no more than the probability at the right-hand side in (11). □

7.2 Proof of Theorem 5

The symbols in w are independent and identically distributed. Write $w' = \rho_\Delta(w), w' = x'y'z'a', |a'| = \Delta$ and $|y'| \ge 1+\Delta$. Let $k = |y'|$. Let E be the event that there are at least $1+\Delta$ slots in y' that are Catalan in $x'y'z'$ and, in addition, that the earliest one of these slots is uniquely honest.

Lemma 1 states that the $\Pr[S]$ is no more than the probability that E does not occur. This latter probability can be bounded from above using Bound 3 provided the symbols in $x'y'z'$ are i.i.d. and $\Pr[x_1' = \mathtt{A}] = (1-\epsilon)/2$.

We have $f = 1 - p_\perp$ and $\alpha = (1-f)^\Delta$. Proposition 2 states that the symbols of $x'y'z'$ are i.i.d. with distribution given by (15). For each $\sigma \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}$ we write $p'_\sigma = \Pr[x'_1 = \sigma]$.

The condition (13) can be equivalently stated as $1-(1-p_\mathtt{A}/f)\alpha = (1-\epsilon)/2$. We check that $p'_\mathtt{A} = 1-(p'_\mathtt{h}+p'_\mathtt{H}) = 1-(p_\mathtt{h}+p_\mathtt{H})\alpha/f = 1-(f-p_\mathtt{A})\alpha/f = 1-(1-p_\mathtt{A}/f)\alpha = (1-\epsilon)/2$ and, consequently, $p'_\mathtt{h}+p'_\mathtt{H} = (1+\epsilon)/2$. Hence we can directly apply Bound 3 to bound $\Pr[E]$. This completes the proof of Theorem 5. □

8 The common prefix property

For the sake of simplicity, assume the synchronous communication model from Section 2.2; the Δ-synchronous setting can be handled in the same way as delineated in Sections 7 and 7.

The common prefix property with parameter k asserts that, for any slot index s, if an honest observer at slot $s+k$ adopts a blockchain $\mathcal{C}$, the prefix $\mathcal{C}[0:s]$ will be present in every honestly-held blockchain at or after slot $s+k$. (Here, $\mathcal{C}[0:s]$ denotes the prefix of the blockchain $\mathcal{C}$ containing only the blocks issued from slots $0, 1, \ldots, s$.)

We translate this property into the framework of forks. Consider a tine t of a fork $F \vdash w$. The *trimmed* tine $t^{\lfloor k}$ is defined as the portion of t labeled with slots $\{0, \ldots, \ell(t)-k\}$. For two tines, we use the notation $t_1 \preceq t_2$ to indicate that the tine t_1 is a prefix of tine t_2.

Definition 15 (Common Prefix Property with parameter $k \in \mathbb{N}$)**.** *Let w be a characteristic string. A fork $F \vdash w$ satisfies k-CP$^{\text{slot}}$ if, for all pairs (t_1, t_2) of viable tines F for which $\ell(t_1) \le \ell(t_2)$, we have $t_1^{\lfloor k} \preceq t_2$. Otherwise, we say that the tine-pair (t_1, t_2) is a witness to a k-CP$^{\text{slot}}$ violation. Finally, w* satisfies *k-CP$^{\text{slot}}$ if every fork $F \vdash w$ satisfies k-CP$^{\text{slot}}$.*

If a string w does not possess the k-CP$^{\text{slot}}$ property, we say that w *violates* k-CP$^{\text{slot}}$. Observe that traditionally (cf. [6]), the truncated chain is defined in terms of deleting a suffix of (block-)length k from $\mathcal{C}$. We denote this traditional version of the common prefix property as the k-CP property. Note, however, that a k-CP violation immediately implies a k-CP$^{\text{slot}}$ violation; hence, bounding the probability of a k-CP$^{\text{slot}}$ violation is sufficient to rule out both events.

Connection with the UVP. Note that if w admits a k-CP$^{\text{slot}}$ violation, then there must be a fork F containing two distinct viable tines $t_1, t_2, \ell(t_1) \le \ell(t_2)$ so that $\ell(t_1) - \ell(t_1 \cap t_2) \ge k+1$. Then t_1 must contain a vertex $v, \ell(t_1 \cap t_2) < \ell(v) \le \ell(t_1) - k$ so that v does not belong to t_2. If every substring x of w with $|x| \ge k$, contained a slot with the UVP then we would never have a k-CP$^{\text{slot}}$ violation. Therefore,

$$\begin{array}{c} w \text{ violates} \\ k\text{-CP}^{\text{slot}} \end{array} \implies \begin{array}{c} w \text{ has a substring } y, |y| \ge k \text{ so} \\ \text{that no slot indexed by } y \text{ has} \\ \text{the UVP in } w. \end{array} \tag{17}$$

Recall that a uniquely honest Catalan slot has the UVP. This fact allows us to bound the probability of common prefix violations by reasoning only about Catalan slots.[4]

Theorem 6 (Main theorem; CP version)**.** *Let $\epsilon \in (0,1)$ and $T \in \mathbb{N}$. Recall the distribution $\mathcal{W}$ on $\{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ from Theorem 1 and the distribution $\tilde{\mathcal{W}}$ on $\{\mathtt{H}, \mathtt{A}\}^T$ from Theorem 2. Then*

$$\Pr_{w\sim\mathcal{W}}[w \text{ violates } k\text{-CP}] \le \Pr_{w\sim\mathcal{W}}[w \text{ violates } k\text{-CP}^{\text{slot}}] \le T \cdot \exp\bigl(-k \cdot \Omega(\min(\epsilon^3, \epsilon^2 q_\mathtt{h}))\bigr)\,.$$

*Furthermore, if axiom **A0′** is satisfied then*

$$\Pr_{w\sim\tilde{\mathcal{W}}}[w \text{ violates } k\text{-CP}] \le \Pr_{w\sim\tilde{\mathcal{W}}}[w \text{ violates } k\text{-CP}^{\text{slot}}] \le T \cdot \exp\bigl(-\Omega(\epsilon^3(1+O(\epsilon))k)\bigr)\,.$$

[4] One can also prove Theorem 6 by directly showing—as in [3]—that a k-CP$^{\text{slot}}$ violation implies a k-settlement violation and then appealing to Theorem 1. However, the proof of the implication (see Section 10) is several pages long and far complicated compared to the short proof yielded by the Catalan slots and UVP. Nevertheless, the proof shows how arguments in [3] can be adapted to our generalized fork framework.

Proof. (The first claim.) Write $w = xyz$ and let ε_k be the probability that y contains no slot with the UVP in w, conditioned on the fact that $|y| = k$. Then, recalling (17), we can apply a union bound over all substrings of w of length at least k to get $\Pr[w \text{ violates } k\text{-CP}^{\text{slot}}] \leq T \sum_{r \geq k} \varepsilon_r$ where the factor T represents a summation over all $x \prec w$. By Theorem 3, if a substring y of w does not contain a slot with the unique vertex proeprty in w, y cannot contain a uniquely honest slot that is Catalan in w. Therefore, ε_k is at most the error probability from Bound 1. Since ε_k decreases exponentially in k, we can write

$$\Pr[w \text{ violates } k\text{-CP}^{\text{slot}}] \leq T \cdot O(1) \cdot \varepsilon_k\,.$$

This proves the second inequality. The first inequality follows since in a given characteristic string, a k-CP violation implies a k-CP$^{\text{slot}}$ violation.

(The second claim.) The proof in this case is identical to the preceding argument except that we need to refer to Theorem 4 in lieu of Theorem 3 and Bound 2 in lieu of Bound 1. ☐

The Δ-synchronous setting. A k-CP violation in a Δ-fork for a string $w \in \{\perp, \mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ would imply a k-CP violation in the corresponding synchronous fork in the string $\rho_\Delta(w) \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ and, consequently, a k-CP$^{\text{slot}}$ violation in $\rho_\Delta(w)$. We omit further details.

9 Catalan slots and relative margin

We set the stage by defining additional elements of the fork framework.

Definition 16 (Closed fork). *A fork F is* closed *if every leaf is honest. For convenience, we say the trivial fork is closed.*

Closed forks have two nice properties that make them especially useful in reasoning about the view of honest parties. First, all honest observers will select a unique longest tine from this fork (since all longest tines in a closed fork are honest, honest parties are aware of all previous honest blocks, they observe the longest chain rule, and they employ the same consistent tie-breaking rule). Second, closed forks intuitively capture decision points for the adversary. The adversary can potentially show many tines to many honest parties, but once an honest node has been placed on top of a tine, any adversarial blocks beneath it are part of the public record and are visible to all honest parties. For these reasons, we will often find it easier to reason about closed forks than arbitrary forks.

The next few definitions are the start of a general toolkit for reasoning about an adversary's capacity to build highly diverging paths in forks, based on the underlying characteristic string.

Definition 17 (Gap, reserve, and reach). *For a closed fork $F \vdash w$ and its unique longest tine $\hat{t}$, we define the* gap *of a tine t to be* $\text{gap}(t) = \text{length}(\hat{t}) - \text{length}(t)$. *Furthermore, we define the* reserve *of t, denoted* $\text{reserve}(t)$*, to be the number of adversarial indices in w that appear after the terminating vertex of t. More precisely, if v is the last vertex of t, then*

$$\text{reserve}(t) = |\{\, i \mid w_i = 1 \textit{ and } i > \ell(v)\}|\,.$$

These quantities together define the reach *of a tine:* $\text{reach}(t) = \text{reserve}(t) - \text{gap}(t)$.

The notion of reach can be intuitively understood as a measure of the resources available to our adversary in the settlement game. Reserve tracks the number of slots in which the adversary has the right to issue new blocks. When reserve exceeds gap (or equivalently, when reach is nonnegative), such a tine could be extended—using a sequence of dishonest blocks—until it is as long as the longest tine. Such a tine could be offered to an honest player who would prefer it over, e.g., the current longest tine in the fork. In contrast, a tine with negative reach is too far behind to be directly useful to the adversary at that time.

Definition 18 (Maximum reach). *For a closed fork $F \vdash w$, we define $\rho(F)$ to be the largest reach attained by any tine of F, i.e.,*

$$\rho(F) = \max_t \ \text{reach}(t)\,.$$

Note that $\rho(F)$ is never negative (as the longest tine of any fork always has reach at least 0). We overload this notation to denote the maximum reach over all forks for a given characteristic string:

$$\rho(w) = \max_{\substack{F \vdash w \\ F \text{ closed}}} \left[\max_{t} \ \mathrm{reach}(t)\right].$$

Reach of vertices is always non-increasing as we move down a tine. That is, if $B_1, B_2, \ldots$ are vertices on the same tine in the root-to-leaf order, then $\mathrm{reach}(B_i) \leq \mathrm{reach}(B_{i+1})$. The inequality is strict if B_{i+1} is honest. Consequently, the reach of an adversarial tine is no more than the reach of the last honest vertex in that tine. In any fork, the reach of a maximally long tine is always non-negative. Hence, an honest tine with the maximal length over all honest tines will always have a non-negative reach. Thanks to the monotonicity of the honest-depth function $\mathbf{d}(\cdot)$, if there are multiple honest tines having the (same) maximal length among all honest tines, they must have the same label. Therefore, if h is the last honest slot in w and t a maximally long honest tine with label h, then $\mathrm{reach}(t) \geq 0$.

Fact 4. *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string, $s \in [T+1]$ be an integer, $x \preceq w, |x| = s-1$. Let F be a fork for w, B an honest vertex in F, $h = \ell(B)$, and $I = [h+1, s-1]$. Let $F_x \vdash x$ be a fork prefix of F so that F_x contains all honest tines from F with labels at most $s-1$. The following statements are equivalent: (i) $\mathrm{reach}_{F_x}(B) \geq 0$; (ii) I is $\mathtt{A}$-heavy; and (iii) B has an adversarial extension $t, \ell(t) \in I$ so that t is viable at the onset of slot s.*

Proof. The equivalence between items (ii) and (iii) has already been shown in Fact 1.

(i) implies (ii). By assumption, $\mathrm{reach}_{F_x}(B) = \mathrm{reserve}_{F_x}(B) - \mathrm{gap}_{F_x}(B) \geq 0$. Since $\mathrm{reserve}_{F_x}(B) = \#_{\mathtt{A}}(I)$ and $\mathrm{gap}_{F_x}(B) \geq \#_{\mathtt{h}}(I) + \#_{\mathtt{H}}(I)$, it follows that $\#_{\mathtt{A}}(I) \geq \#_{\mathtt{h}}(I) + \#_{\mathtt{H}}(I)$.

(iii) implies (i). Since t is an adversarial extension of B, it contains only adversarial vertices from I. By assumption, t is viable at the onset of slot s. It follows that $\#_{\mathtt{A}}(I) \geq \mathrm{gap}_{F_x}(B)$. Since $\mathrm{reserve}_{F_x}(B) = \#_{\mathtt{A}}(I)$, we have $\mathrm{reach}_{F_x}(B) = \mathrm{reserve}_{F_x}(B) - \mathrm{gap}_{F_x}(B) \geq 0$.

□

Observe that for any characteristic string x, one can *extend* (i.e., augment) a closed fork prefix $F \vdash x$ into a larger closed fork $F' \vdash x0$ so that $F \sqsubseteq F'$. A *conservative extension* is a minimal extension in that it consumes the least amount of reserve (cf. Definition 17), leaving the remaining reserve to be used in future. Extensions and, in particular, conservative extensions play a critical role in the exposition that follows.

Definition 19 (Extensions)**.** *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ be a characteristic string and F a closed fork for w. Let F' be a closed fork for $wb, b \in \{\mathtt{h}, \mathtt{H}\}$ so that $F \sqsubseteq F'$. We say that F'* is an extension of *F if every honest vertex in F' either belongs to F or has label $|w|+1$. Let $\sigma \in F'$ be an honest vertex with $\ell(\sigma) = |w|+1$ and let s be the longest honest prefix of σ. (Necessarily, $s \in F$.) We say that σ* is an extension of *s. The new tine σ is a* conservative extension *if* $\mathrm{height}(F') = \mathrm{height}(F) + 1$.

Since F' is closed, all longest tines in F' are honest and they have label $|w|+1$. Let $\hat{t}$ be the unique longest honest tine in F' under the consistent longest-chain selection rule in Axiom $\mathbf{A0'}$. Now consider a tine $\sigma \in S$. Since σ is honest, it follows that $\mathrm{length}(\sigma) \geq 1 + \mathrm{height}(F) = 1 + \mathrm{length}(s) + \mathrm{gap}_F(s)$ where $s \in F$ is the longest honst prefix of σ. The root-to-leaf path in F' that ends at σ contains at least $\mathrm{gap}_F(s)$ adversarial vertices $u \in F'$ so that $\ell(u) \in [\ell(s)+1, |w|]$ and $u \notin F$. If σ is a conservative extension, the number of such vertices is exactly $\mathrm{gap}_F(s)$.

9.1 Relative margin and balanced forks

Definition 20 (The $\sim_x$ relations)**.** *For two tines t_1 and t_2 of a fork F, we write $t_1 \sim t_2$ when t_1 and t_2 share an edge; otherwise we write $t_1 \nsim t_2$. We generalize this equivalence relation to reflect whether tines share an edge over a particular suffix of w: for $w = xy$ we define $t_1 \sim_x t_2$ if t_1 and t_2 share an edge that terminates at some node labeled with an index in y; otherwise, we write $t_1 \nsim_x t_2$ (observe that in this case the paths share no vertex labeled by a slot associated with y). We sometimes call such pairs of tines* disjoint *(or, if $t_1 \nsim_x t_2$ for a string $w = xy$,* disjoint over *y). Note that $\sim$ and $\sim_\varepsilon$ are the same relation.*

The basic structure we use to use to reason about settlement times is that of a "balanced fork."

Definition 21 (Balanced fork)**.** *A fork F is* balanced *if it contains a pair of tines t_1 and t_2 for which $t_1 \nsim t_2$ and* $\mathrm{length}(t_1) = \mathrm{length}(t_2) = \mathrm{height}(F)$*. We define a relative notion of balance as follows: a fork $F \vdash xy$ is x-*balanced *if it contains a pair of tines t_1 and t_2 for which $t_1 \nsim_x t_2$ and* $\mathrm{length}(t_1) = \mathrm{length}(t_2) = \mathrm{height}(F)$*.*

Thus, balanced forks contain two completely disjoint, maximum-length tines, while x-balanced forks contain two maximum-length tines that may share edges in x but must be disjoint over the rest of the string. See Figures 2 and 3 for examples of balanced forks.

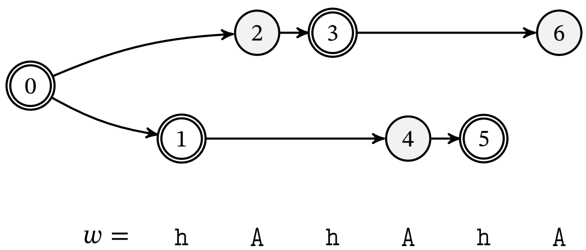


Figure 2: A balanced fork

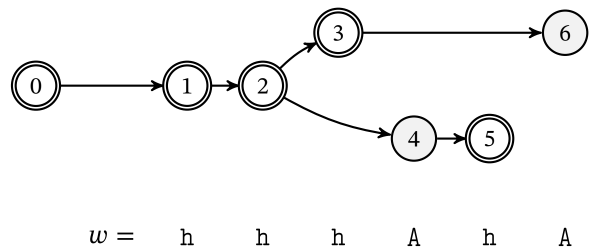


Figure 3: An x-balanced fork, where $x = \mathtt{hh}$

Balanced forks and settlement time. A fundamental question arising in typical blockchain settings is how to determine *settlement time*, the delay after which the contents of a particular block of a blockchain can be considered stable. The existence of a balanced fork is a precise indicator for "settlement violations" in this sense. Specifically, consider a characteristic string xy and a transaction appearing in a block associated with the first slot of y (that is, slot $|x|+1$). One clear violation of settlement at this point of the execution is the existence of two chains—each of maximum length—which diverge *prior to* y; in particular, this indicates that there is an x-balanced fork F for xy. Let us record this observation below.[5]

Observation 2. Let $s, k \in \mathbb{N}$ be given and let w be a characteristic string. Slot s is not k-settled for the characteristic string w if there exist a decomposition $w = xyz$, where $|x| = s - 1$ and $|y| \geq k + 1$, and an x-balanced fork for xy.

In particular, to provide a rigorous k-slot settlement guarantee—which is to say that the transaction can be considered settled once k slots have gone by—it suffices to show that with overwhelming probability in choice of the characteristic string determined by the leader election process (of a full execution of the protocol), no such forks are possible. Specifically, if the protocol runs for a total of T time steps yielding the characteristics string $w = xy$ (where $w \in \{0,1\}^T$ and the transaction of interest appears in slot $|x|+1$ as above) then it suffices to ensure that there is no x-balanced fork for $x\hat{y}$, where $\hat{y}$ is an arbitrary prefix of y of length at least $k+1$. Note that for systems adopting the longest chain rule, this condition must necessarily involve the *entire future dynamics* of the blockchain. We remark that our analysis below will in fact let us take $T = \infty$.

Definition 22 (Margin)**.** *The* margin *of a fork $F \vdash w$, denoted $\mu(F)$, is defined as*

$$\mu(F) = \max_{t_1 \nsim t_2} \bigl(\min\{\mathrm{reach}(t_1), \mathrm{reach}(t_2)\}\bigr)\,, \tag{18}$$

where this maximum is extended over all pairs of disjoint tines of F; thus margin reflects the "second best" reach obtained over all disjoint tines. In order to study splits in the chain over particular portions of a string, we generalize this to define a "relative" notion of margin: If $w = xy$ for two strings x and y and, as above, $F \vdash w$, we define

$$\mu_x(F) = \max_{t_1 \nsim_x t_2} \bigl(\min\{\mathrm{reach}(t_1), \mathrm{reach}(t_2)\}\bigr)\,.$$

[5] A balanced fork in [3] had the property that at least one maximally long tine was adversarial. But this is not true in our setting since we allow multiply-honest slots.

Note that $\mu_\varepsilon(F) = \mu(F)$.

For convenience, we once again overload this notation to denote the margin of a string. $\mu(w)$ refers to the maximum value of $\mu(F)$ over all possible closed forks F for a characteristic string w:

$$\mu(w) = \max_{\substack{F \vdash w, \\ F \text{ closed}}} \mu(F)\,.$$

Likewise, if $w = xy$ for two strings x and y we define

$$\mu_x(y) = \max_{\substack{F \vdash w, \\ F \text{ closed}}} \mu_x(F)\,.$$

Note that, at least informally, tines with the "second-best" reach are of natural interest to an adversary who wants to build an x-balanced fork, since such a fork contains two (partially disjoint) long tines.

Finally, writing $w = xy$, consider any tine-pair (t_x, t_ρ) in a fork $F \vdash w$ so that $\text{reach}_F(t_\rho) = \rho(F)$ and t_x is y-disjoint with t_ρ. Observe that if $\mu_x(y) < 0$ then $\text{reach}_F(t_x) < 0$.

Fact 5 (see Fact 1 in [4])**.** *Let $xy \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ be a characteristic string. Then there is an x-balanced fork $F \vdash xy$ if and only if $\mu_x(y) \geq 0$.*

Let $w = xy$. If $\mu_x(y)$ is negative, there can be no x-balanced fork for w. However, this also means that there can be no fork for w which contains two maximally long tines that diverge prior to *any* slot $s \leq |x| + 1$.

Corollary 2. *Let w be a characteristic string and let $w = xx'y$ be an arbitrary decomposition. If $\mu_{xx'}(y) < 0$ then $\mu_x(x'y) < 0$.*

Note that if a slot $s > |x|$ has the UVP then there can be no x-balanced fork for xy. An appeal to Corollary 5 immediately gives:

Corollary 3. *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string, $s \in [T]$ be an integer, and $w = xy$ be an arbitrary decomposition where $|x| < s$. If s is a uniquely honest Catalan slot in w then $\mu_x(y) < 0$.*

9.2 Catalan slots and relative margin

Below, we lay down the connection between Catalan slots and relative margin. Note, however, that the exposition below is not essential in proving the main theorems.

Definition 23 (Margin-critical slot)**.** *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string, $s \in [T]$ be a slot in w, and x be a prefix of w so that $|x| = s - 1$. Slot s is called* margin-critical *if, for all decompositions $w = xyz$ so that $|y| \geq 1$ and $|z| \geq 0$, we have $\mu_x(y) < 0$.*

Since $\mu_x(\varepsilon) \geq 0$ and $|y| \geq 1$ in the above definition, it follows that a margin-critical slot (i.e., the first slot in y) must be honest.

Lemma 2. *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string. A a uniquely honest slot is margin-critical if and only if it has the UVP.*

Proof.

The $\Longrightarrow$ direction. Let $s \in [T]$ be a uniquely honest margin-critical slot in w. This means, for every prefix $xy \preceq w, |x| = s - 1, |y| \geq 1$, we have $\mu_x(y) < 0$. Let F be any fork for xy and let $t \in F, \ell(t) \leq s - 1$ be an honest tine. Since it is disjoint with any tine in F over the suffix y, $\text{reach}(t) < 0$ and, by Fact 1, t does not have an adversarial extension $t' \in F, t \prec t'$ that is viable at the onset of slot $|xy| + 1$. Therefore, if a tine in F is viable at the onset of slot $|xy| + 1$, it must contain an honest vertex with label at least s. However, since an honest vertex builds only on top of a viable tine, it follows that any viable tine must contain the unique honest vertex with label s.

The $\Longleftarrow$ direction. Let $s \in [T]$ be a uniquely honest slot in w so that s has the UVP in xy. Let $k \in \mathbb{N}, s \leq k \leq T$; Write $w = xyz$ with $|x| = s - 1$ and $|xy| = k$. (Thus $|y| \geq 1$ and $y_1 = w_s$.) Let F be any fork for xy. Since slot s belongs to y, F cannot contain two tines such that i) both tines are viable at the onset of slot $|xy| + 1$ and, at the same time, ii) disjoint over the length of y since they must contain the unique vertex with label s. In particular, F cannot be x-balanced. As F was an arbitrary fork for xy, no fork for xy can be x-balanced for our choice of m and k. We use Fact 5 to conclude that the relative margin $\mu_x(y)$ must be negative. Since our $k \in [s, T]$ is arbitrary, the above conclusion applies to all decompositions $w = xyz$ where $|x| = s - 1$ and $|xy| \geq s$. Therefore, slot s is margin-critical in w.

□

Corollary 4. *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string. A uniquely honest slot in w is Catalan if and only if it is margin-critical.*

10 CP violations and balanced forks with concurrent honest leaders

Balanced forks played a critical role in the analysis of [3]. Specifically, a balanced fork was equivalent to a settlement violation in their setting and a CP violation would also imply a balanced fork. In the current analysis, we have analyzed settlement and CP violations through their connections with the UVP and Catalan slots; thus balanced forks are not necessary in our analysis. However, it is instructive to see whether the statement "a CP violation implies a balanced fork" still holds in our model and, importantly, how the existing proof needs to be modified.

Thus the the goal of this section is to prove Theorem 7 below which would yield an alternative proof of Theorem 6 without using the Catalan slots. However, the simplicity of the proof of Theorem 6 in Section 8 demonstrates the expressive power of the UVP and Catalan slots compared to relative margin and balanced forks.

A k-CP$^{\mathsf{slot}}$ violation implies a k-settlement violation. Let w be a characteristic string, written $w = xy$, and let F be a fork for w. Recall that a slot $s = |x| + 1$ is not k-settled if and only if F contains two maximally long tines that diverge prior to s, i.e., F is x-balanced (see Definition 21).

Definition 24 (Slot divergence)**.** *Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$ and let F be a fork for w. Define the* slot divergence *of two tines $t_1, t_2 \in F$ as*

$$\mathrm{div}_{\mathsf{slot}}(t_1, t_2) \triangleq \ell(t_1) - \ell(t_1 \cap t_2) \quad \textit{where } \ell(t_1) \leq \ell(t_2)\,. \tag{19}$$

We can generalize this notion for forks and characteristic strings as follows: $\mathrm{div}_{\mathsf{slot}}(F) \triangleq \max_{t_1, t_2 \in F} \mathrm{div}_{\mathsf{slot}}(t_1, t_2)$ *and* $\mathrm{div}_{\mathsf{slot}}(w) \triangleq \max_{F \vdash w} \mathrm{div}_{\mathsf{slot}}(F)$.

By definition, a k-CP$^{\mathsf{slot}}$ violation implies the existence of a fork with a slot divergence at least $k+1$. Theorem 7 below shows that a if a fork has a slot divergence at least $k+1$ then there is a balanced fork for a prefix of the same characteristic string so that two maximally long tine diverge prior to last k slots. Therefore, a k-CP$^{\mathsf{slot}}$ violation implies an (s, k)-settlement violation for some slot s.

Theorem 7. *Let $k, T \in \mathbb{N}$. Let $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^T$ be a characteristic string so that* $\mathrm{div}_{\mathsf{slot}}(w) \geq k + 1$. *Then there is a decomposition $w = xyz$ and a fork $\hat{F} \vdash xy$, where $|y| \geq k$, so that $\hat{F}$ is x-balanced.*

Recall that $\ell(t)$ is the slot index of the last vertex of tine t. Define $A \triangleq \bigcup_{F \vdash w} A_F$ where, for a given fork $F \vdash w$, define

$$A_F \triangleq \left\{ (\tau_1, \tau_2) : \begin{array}{l} \tau_1, \tau_2 \text{ are two viable tines in the fork } F, \\ \ell(\tau_1) \leq \ell(\tau_2), \text{ and } \mathrm{div}_{\mathsf{slot}}(\tau_1, \tau_2) \geq k+1 \end{array} \right\}.$$

Notice that there must be a tine-pair $(t_1, t_2) \in A$ which satisfies the following two conditions:

$$\mathrm{div}_{\mathsf{slot}}(t_1, t_2) \text{ is maximal over } A\,, \tag{20}$$

$$|\ell(t_2) - \ell(t_1)| \text{ is minimal among all tine-pairs in } A \text{ for which (20) holds}\,, \tag{21}$$

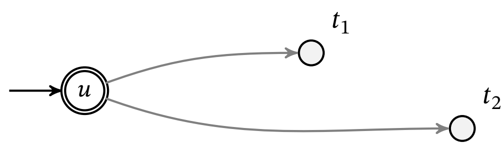
and

$$\text{For a fixed } t_2\text{, the tine } t_1 \text{ has the maximal length over all tines } t_1', \ell(t_1') = \ell(t_1) \text{ such that } (t_1', t_2) \text{ satisfies (20) and (21)}. \tag{22}$$

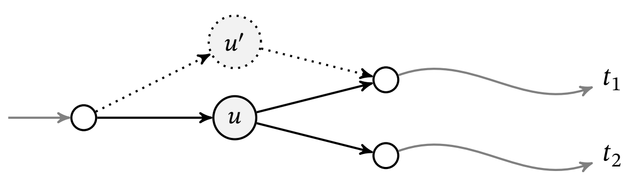
(Note that t_1, t_2 are not uniquely identified.) The tines t_1, t_2 will play a special role in our proof; let F be a fork containing these tines.

Recall given a characteristic string $w \in \{\mathtt{h}, \mathtt{H}, \mathtt{A}\}^*$, a uniquely honest slot contains the symbold h, a multiply-honest slot contains the symbold H, and an adversarial slot contains the symbold A. We call a slot honest if it contains either an h or an H; otherwise, we call it an adversarial slot.

The prefix x, fork F_x, and vertex u. Let u denote the last vertex on the tine $t_1 \cap t_2$, as shown in the diagram below, and let $\alpha \triangleq \ell(u) = \ell(t_1 \cap t_2)$. Let $x \triangleq w_1, \dots, w_\alpha$ and let F_x be the fork-prefix of F supported on x. We will argue that α must be a uniquely honest slot and, in addition, that F_x must contain a unique longest tine t_u terminating at the vertex u. We will also identify a substring y, $|y| \geq k$ such that w can be written as $w = xyz$. Then we will construct a balanced fork $\tilde{F}_y \vdash y$ by modifying the subgraph of F supported on y. We will finish the proof by constructing an x-balanced fork by suitably appending $\tilde{F}_y$ to F_x.



α must be a uniquely honest slot. We observe, first of all, that the slot α can neither be adversarial nor multiply honest: otherwise it is easy to construct a fork $F' \vdash w$ and a pair of tines in F' that violate (20). Specifically, construct F' from F by adding a new vertex u' to F for which $\ell(u') = \ell(u)$, adding an edge to u' from the vertex preceding u, and replacing the edge of t_1 following u with one from u'; then the other relevant properties of the fork are maintained, but the slot divergence of the resulting tines has increased by at least one. (See the diagram below.)



F_x has a unique, longest (and honest) tine t_u. A similar argument implies that the fork F_x has a unique vertex of depth depth(u): namely, u itself. In the presence of another vertex u' (of F_x) with depth depth(u), "redirecting" t_1 through u' (as in the argument above) would likewise result in a fork with a larger slot divergence. To see this, notice that $\ell(u')$ must be strictly less than $\ell(u)$ since $\ell(u)$ is an honest slot (which means u is the only vertex at that slot). Thus $\ell(\cdot)$ would indeed be increasing along this new tine (resulting from redirecting t_1). As α is the last index of the string x, this additionally implies that F_x has no vertices of depth exceeding depth(u). Let $t_u \in F_x$ be the tine with $\ell(t_u) = \alpha$.

$$\text{The honest tine } t_u \text{ is the unique longest tine in } F_x\,. \tag{23}$$

Identifying y. Let β denote the smallest honest index of w for which $\beta \geq \ell(t_2)$, with the convention that if there is no such index we define $\beta = T + 1$. Thus $\beta \geq \ell(t_2) \geq \ell(t_1)$. These indices, α and β, distinguish the substrings $y = w_{\alpha+1} \dots w_{\beta-1}$ and $z = w_\beta \dots w_T$; we will focus on y in the remainder of the proof. Since the function $\ell(\cdot)$ is strictly increasing along any tine, observe that

$$|y| = (\beta - 1) - (\alpha + 1) + 1 = \beta - \alpha - 1 \geq (\ell(t_1) - \ell(u)) - 1 \geq (k+1) - 1 = k\,.$$

Hence y has the desired length and it suffices to establish that it is forkable.[6]

Honest indices in xy have small depths. The minimality assumption (21) implies that any honest index h for which $h < \beta$ has depth no more than min(length(t_1), length(t_2)): specifically, we claim that

$$h < \beta \quad \Longrightarrow \quad \mathbf{d}(h) \leq \min(\text{length}(t_1), \text{length}(t_2)) . \tag{24}$$

To see this, consider an honest index h, $h < \beta$ and a tine t_h for which $\ell(t_h) = h$. If $\ell(t_2)$ is honest then $h < \beta = \ell(t_2)$. Otherwise, $h < \ell(t_2) < \beta$ since $\ell(t_2)$ is adversarial. In any case, $h < \ell(t_2)$ and, since t_2 is viable, it follows immediately that $\mathbf{d}(h) \leq \text{length}(t_2)$. Similarly, if $h < \ell(t_1)$ then $\mathbf{d}(h) \leq \text{length}(t_1)$ since t_1 is viable as well.

Now consider the case $h = \ell(t_1)$. We claim that

$$\text{If } h = \ell(t_1) < \beta \text{ then } \mathbf{d}(h) = \text{length}(t_1) \ . \tag{25}$$

We can rule out the case $h = \ell(t_1) = \ell(t_2)$ since if this happens, $\ell(t_2)$ is honest and $\beta = \ell(t_2)$, contradicting our assumption that $h < \beta$. Thus, it must be the case that $h = \ell(t_1) < \ell(t_2)$. In this case, the claim follows trivially if $\ell(t_1)$ is a uniquely honest slot. Otherwise, let t be a tine with maximal length among all tines labeled with the multiply-honest slot $h = \ell(t_1) < \ell(t_2)$. We wish to show that length(t_1) = length(t). There are four contingencies to consider; the first three of these lead to contradictions and for the last one, we get length(t_1) = $\mathbf{d}(h)$ = length(t).

- If $(t, t_2) \notin A$, $\text{div}_{\text{slot}}(t, t_2)$ is at most k. Since $\text{div}_{\text{slot}}(t_1, t_2)$ is at least $k + 1$, t must share a vertex with t_2 after slot $\ell(u)$. But this means $\ell(t \cap t_1) = \ell(u)$ and $\text{div}_{\text{slot}}(t, t_1) = \text{div}_{\text{slot}}(t_1, t_2) \geq k + 1$. As a result, $(t, t_1) \in A$. However, this violates (21) since $|\ell(t) - \ell(t_1)| = 0 < |\ell(t_2) - \ell(t_1)|$ by assumption.
- If (t, t_2) is in A and $\ell(t \cap t_1) < \ell(u)$, then $\text{div}_{\text{slot}}(t, t_1) > \text{div}_{\text{slot}}(t_1, t_2)$, violating (20).
- If (t, t_2) is in A and $\ell(t \cap t_1) = \ell(u)$, this means t is disjoint with t_1 after $\ell(u)$. Then (21) is violated since $\text{div}_{\text{slot}}(t, t_1) = \text{div}_{\text{slot}}(t_1, t_2)$ but $|\ell(t) - \ell(t_1)| = 0 < |\ell(t_2) - \ell(t_1)|$ by assumption.
- If (t, t_2) is in A and $\ell(t \cap t_1) > \ell(u)$, this means t shares a vertex with t_1 after $\ell(u)$. Then $\text{div}_{\text{slot}}(t, t_2) = \text{div}_{\text{slot}}(t_1, t_2)$ and $|\ell(t_2) - \ell(t_1)| = |\ell(t_2) - \ell(t)|$. By (22), length($t_1$) $\geq$ length(t); hence length(t_1) = length(t) since by assumption, t has the maximal length among all tines with label $\ell(t_1)$. Hence length(t_1) = $\mathbf{d}(h)$.

The remaining case for proving (24), i.e., when $\ell(t_1) < h < \ell(t_2)$, can be ruled out by the argument below.

There is no honest index between $\ell(t_1)$ and $\ell(t_2)$. We claim that

$$\text{There is no honest index } h \text{ satisfying } \ell(t_1) < h < \ell(t_2) . \tag{26}$$

The claim above is trivially true if $\ell(t_1) = \ell(t_2)$. Otherwise, suppose (toward a contradiction) that h is an honest index satisfying $\ell(t_1) < h < \ell(t_2)$. Let t_h be an honest tine at slot h. The tine-pair (t_1, t_h) may or may not be in A. We will show that both cases lead to contradictions.

- If (t_1, t_h) is in A and $\ell(t_1 \cap t_h) \leq \ell(u)$, $\text{div}_{\text{slot}}(t_1, t_h)$ is at least $\text{div}_{\text{slot}}(t_1, t_2)$. In fact, due to (20), this inequality must be an equality. However, the assumption $\ell(t_1) < h < \ell(t_2)$ contradicts (21).
- If (t_1, t_h) is in A and $\ell(t_1 \cap t_h) > \ell(u)$, it follows that $\text{div}_{\text{slot}}(t_h, t_2) > \text{div}_{\text{slot}}(t_1, t_2)$. As the latter quantity is at least $k + 1$, (t_h, t_2) must be in A. The preceding inequality, however, contradicts (20).
- If $(t_1, t_h) \notin A$, $\text{div}_{\text{slot}}(t_1, t_h)$ is at most k. As $\text{div}_{\text{slot}}(t_1, t_2)$ is at least $k + 1$, t_h and t_1 must share a vertex after slot $\ell(u)$. Since $\ell(t_1) < h < \ell(t_2)$ by assumption, $\text{div}_{\text{slot}}(t_h, t_2) > \text{div}_{\text{slot}}(t_1, t_2) \geq k + 1$ and, as a result, $(t_h, t_2) \in A$. However, the strict inequality above violates (20).

We conclude that (26)—and thus (24)—is true. (Note that in the above argument, all we needed was that t_h is a viable tine since in all cases, t_h appears in a tine-pair in A. Thus (26) can be generalized as saying "there is no fork for w with a viable tine t so that $\ell(t_1) < \ell(t) < \ell(t_2)$.")

[6] In Blum et al. [3], $|y|$ was at least $k + 1$. The difference is due to the fact that in their analysis, a slot with multiple vertices was necessarily adversarial.

A fork $F^{\rhd u \lhd}$ where all long tines go through u. In light of the remarks above, we observe that the fork F may be "pinched" at u to yield an essentially identical fork $F^{\rhd u \lhd} \vdash w$ with the exception that all tines of length exceeding depth(u) pass through the vertex u. Specifically, the fork $F^{\rhd u \lhd} \vdash w$ is defined to be the graph obtained from F by changing every edge of F directed towards a vertex of depth depth(u) + 1 so that it originates from u. To see that the resulting tree is a well-defined fork, it suffices to check that $\ell(\cdot)$ is still increasing along all tines of $F^{\rhd u \lhd}$. For this purpose, consider the effect of this pinching on an individual tine t terminating at a particular vertex v—it is replaced with a tine $t^{\rhd u \lhd}$ defined so that:

- If $\text{length}(t) \leq \text{depth}(u)$, the tine t is unchanged: $t^{\rhd u \lhd} = t$.
- Otherwise, $\text{length}(t) > \text{depth}(u)$ and t has a vertex v of depth $\text{depth}(u) + 1$; note that $\ell(v) > \ell(u)$ because F_x contains no vertices of depth exceeding depth(u). Then $t^{\rhd u \lhd}$ is defined to be the path given by the tine terminating at u, a (new) edge from u to v, and the suffix of t beginning at z. (As $\ell(v) > \ell(u)$ this has the increasing label property.)

Thus the tree $F^{\rhd u \lhd}$ is a legal fork on the same vertex set; note that the depths of vertices in F and $F^{\rhd u \lhd}$ are identical.

Constructing a fork $F_y \vdash y$ containing two long tines. By excising the tree rooted at u from this pinched fork $F^{\rhd u \lhd}$, we may extract a fork for the string $w_{\alpha+1} \dots w_T$. Specifically, consider the induced subgraph $F^{u \lhd}$ of $F^{\rhd u \lhd}$ given by the vertices $\{u\} \cup \{v : \text{depth}(v) > \text{depth}(u)\}$. By treating u as a root vertex and suitably defining the labels $\ell^{u \lhd}$ of $F^{u \lhd}$ so that $\ell^{u \lhd}(v) = \ell(v) - \ell(u)$, this subgraph has the defining properties of a fork for $w_{\alpha+1} \dots w_T$. In particular, considering that α is honest, it follows that each honest index $h > \alpha$ has depth $\mathbf{d}(h) > \text{length}(u)$ and hence any vertex with label h is also present in $F^{u \lhd}$. For a tine t of $F^{\rhd u \lhd}$, we let $t^{u \lhd}$ denote the suffix of this tine beginning at u, which forms a tine in $F^{u \lhd}$. (If $\text{length}(t) \leq \text{depth}(u)$, we define $t^{u \lhd}$ to consist solely of the vertex u.) Considering ${t_1}^{u \lhd}$ and ${t_2}^{u \lhd}$, let $\check{t}_i, i \in \{1,2\}$ be the longest prefix of ${t_i}^{u \lhd}$ so that $\check{t}_i$ is labeled by a slot in y. Since the tines ${t_1}^{u \lhd}, {t_2}^{u \lhd}$ are disjoint in $F^{u \lhd}$, so are $\check{t}_1, \check{t}_2$.

Recall that that y is as a prefix of $w_{\alpha+1} \dots w_T$. Let h^* be the largest honest index in y. Let F_y denote the subtree of $F^{u \lhd}$, with the same root as $F^{u \lhd}$, containing the following tines: $\check{t}_1, \check{t}_2$, and all tines $t^{u \lhd} \in F^{u \lhd} \setminus \{\check{t}_1, \check{t}_2\}$ so that $\ell(t^{u \lhd})$ is drawn from y and

$$\text{length}(t^{u \lhd}) \leq \mathbf{d}(h^*)\,. \tag{27}$$

Note that the length of every honest tine labeled by y is at most $\mathbf{d}(h^*)$; hence, thanks to (24), F_y contains all honest tines from $F^{u \lhd}$ that have labels in y. Note, in addition, that the tines $\check{t}_1$ and $\check{t}_2$ are consistently labeled in F_y. Thus F_y satisfies all properties of a legal fork.

Having defined F_y, we claim that

$$\min\left(\text{length}(\check{t}_1), \text{length}(\check{t}_2)\right) \geq \mathbf{d}(h^*)\,. \tag{28}$$

Let $i \in \{1,2\}$. If $\ell(t_i) < \beta$ then $\check{t}_i = {t_i}^{u \lhd}$ and, by (24), $\text{length}(\check{t}_i) = \text{length}({t_i}^{u \lhd}) \geq \mathbf{d}(h^*)$. Othereise, we have $\ell(t_i) = \beta$ which means $\ell(t_i)$ is an honest slot. Thus ${t_i}^{u \lhd}$ must be an honest tine, building directly on top of the viable tine $\check{t}_i$. Therefore, we have $\text{length}(\check{t}_i) \geq \mathbf{d}(h^*)$.

Constructing a balanced fork $\tilde{F}_y \vdash y$. If $\text{length}(\check{t}_1) = \text{length}(\check{t}_2)$, set $\tilde{F}_y = F_y$ and, due to (27) and (28), the fork $\tilde{F}_y \vdash y$ must be balanced. Otherwise, let $a, b \in \{1,2\}, a \neq b$ be two integers so that $\text{length}(\check{t}_a) > \text{length}(\check{t}_b)$. We modify F_y by deleting some trailing nodes from $\check{t}_a$ so that the surviving prefix—let it be denoted by $\tilde{t}_a$—has the same length as $\check{t}_b$. That is, we achieve

$$\text{length}(\tilde{t}_a) = \text{length}(\check{t}_b) = \min\left(\text{length}(\check{t}_1), \text{length}(\check{t}_2)\right)\,.$$

Let $\tilde{F}_y$ be the resulting fork. Equations (27) and (28) imply that $\tilde{F}_y$ has at least two maximally long tines (i.e., $\tilde{t}_a$ and $\check{t}_b$) and therefore, it is balanced. It remains to show that the longer tine, $\check{t}_a$, has sufficiently many trailing adversarial vertices so that after deleting them, we obtain $\text{length}(\tilde{t}_a) = \text{length}(\check{t}_b)$. (If we had to delete an honest vertex in this process, $\tilde{F}_y$ may have violated property (F3) in the definition of a fork.) Let h_a be the label of the last honest vertex on $\check{t}_a$. Thanks to (28), we have $\text{length}(\check{t}_a) > \text{length}(\check{t}_b) \geq \mathbf{d}(h^*) \geq \mathbf{d}(h_a)$. Hence all vertices in $\check{t}_a$ with labels in $[h_a + 1, \ell(\check{t}_a)]$ must be adversarial; we can safely delete $|\,\text{length}(\check{t}_a) - \text{length}(\check{t}_b)|$ of these adversarial vertices.

An x-balanced fork $\hat{F} \sqsubseteq F$. Let us identify the root of the fork $\tilde{F}_y$ with the vertex u of F_x and let $\hat{F}$ be the resulting graph (after "gluing" the root of $\tilde{F}_y$ to u). By (23), it is easy to see that the fork $\hat{F} \sqsubseteq F$ is indeed a valid fork on the string xy. Moreover, $\hat{F}$ is x-balanced since $\tilde{F}_y$ is balanced. The claim in Theorem 7 follows immediately since $|y| \geq k$.

□

References

[1] Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 913–930, 2018.

[2] Iddo Bentov, Rafael Pass, and Elaine Shi. Snow white: Provably secure proofs of stake. page 919, 2016. URL `http://eprint.iacr.org/2016/919`.

[3] Erica Blum, Aggelos Kiayias, Cristopher Moore, Saad Quader, and Alexander Russell. Linear consistency for proof-of-stake blockchains. Technical report, Cryptology ePrint Archive, Report 2017/241, 2018. URL `https://eprint.iacr.org/2017/241`.

[4] Erica Blum, Aggelos Kiayias, Cristopher Moore, Saad Quader, and Alexander Russell. The combinatorics of the longest-chain rule: Linear consistency for proof-of-stake blockchains. In *Proceedings of the 2020 ACM Symposium on Discrete Algorithms*, SODA '20, 2020.

[5] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Advances in Cryptology – EUROCRYPT 2018*, pages 66–98, 2018.

[6] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol with chains of variable difficulty. In *Annual International Cryptology Conference*, pages 291–323. Springer, 2017.

[7] Juan A. Garay and Aggelos Kiayias. Sok: A consensus taxonomy in the blockchain era. *IACR Cryptology ePrint Archive*, 2018:754, 2018. URL `https://eprint.iacr.org/2018/754`.

[8] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology - EUROCRYPT 2015*, pages 281–310, 2015. URL `https://doi.org/10.1007/978-3-662-46803-6_10`.

[9] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference*, volume 10401 of *Lecture Notes in Computer Science*, pages 357–388, 2017.

[10] Silvio Micali. ALGORAND: the efficient and democratic ledger. *CoRR*, abs/1607.01341, 2016. URL `http://arxiv.org/abs/1607.01341`.

[11] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf, 2008.

[12] Rafael Pass and Elaine Shi. The sleepy model of consensus. In *Advances in Cryptology - ASIACRYPT 2017*, pages 380–409, 2017. URL `https://doi.org/10.1007/978-3-319-70697-9_14`.

[13] Herbert S Wilf. *generatingfunctionology*. AK Peters/CRC Press, 3 edition, 2005.