The Generals’ Scuttlebutt: Byzantine-Resilient Gossip Protocols

Sandro Coretti
IOG
sandro.coretti@iohk.io

Alexander Russell
University of Connecticut
IOG
acr@uconn.edu

Aggelos Kiayias
University of Edinburgh
IOG
Aggelos.Kiayias@ed.ac.uk

Cristopher Moore
Santa Fe Institute
moore@santafe.edu

ABSTRACT
One of the most successful applications of peer-to-peer communication networks is in the context of blockchain protocols, which—in Satoshi Nakamoto’s own words—rely on the “nature of information being easy to spread and hard to stifle.” Significant efforts were invested in the last decade into analyzing the security of these protocols, and invariably the security arguments known for longest-chain Nakamoto-style consensus use an idealization of this tenet. Unfortunately, the real-world implementations of peer-to-peer gossip-style networks used by blockchain protocols rely on a number of ad-hoc attack mitigation strategies that leave a glaring gap between the idealized communication layer assumed in formal security arguments for blockchains and the real world, where a wide array of attacks have been showcased.

In this work we bridge this gap by presenting a Byzantine-resilient gossip network layer for blockchain protocols. For the first time we quantify the problem of network-layer attacks in the context of blockchain security models, and we develop a design that thwarts resource-restricted adversaries. Importantly, we focus on the proof-of-stake setting due to its vulnerability to Denial-of-Service (DoS) attacks stemming from the well-known deficiency (compared to the proof-of-work setting) known as nothing at stake.

We present a Byzantine-resilient gossip protocol, and we analyze it in the Universal Composition framework. In order to prove security, we show novel results on expander properties of random graphs. Importantly, our gossip protocol can be based on any given bilateral functionality that determines a desired interaction between two “adjacent” peers in the networking layer and demonstrates how it is possible to use application-layer information to make the networking-layer resilient to attacks. Despite the seeming circularity, we demonstrate how to prove the security of a Nakamoto-style longest-chain protocol given our gossip networking functionality, and hence, we demonstrate constructively how it is possible to obtain provable security across protocol layers, given only bare-bone point-to-point networking, majority of honest state, and a verifiable random function.

CCS CONCEPTS
• Security and privacy → Cryptography; Distributed systems security.

KEYWORDS
proof of stake, blockchains, gossiping, Byzantine-resilience, expander graphs, universal composability

ACM Reference Format:

1 INTRODUCTION
1.1 Gossip Protocols and Byzantine Attackers
Gossip protocols. Gossip protocols [12, 18] provide an efficient mechanism to distribute information to a large set of parties. The key feature of such algorithms is their peer-to-peer operation that load balances the effort of information propagation in a way that individual nodes are only investing a modicum of effort when contributing to the delivery of a message network-wide.

As communication infrastructure for multiparty cryptography, gossip protocols have recently found wide-spread application in the context of blockchain protocols, notably with the introduction of the Bitcoin blockchain [26]. Among other things, gossip protocols are used by blockchain participants to diffuse newly found blocks. In the words of Nakamoto, blockchain protocols rely on the “nature of information being easy to spread and hard to stifle,” underscoring the relevance of gossip as the underlying communication layer.1

The “security” of gossip protocols. Deploying gossip protocols as the communication layer of blockchain protocols adds a crucial new dimension to their design: their “security.”

At the very least, gossip protocols underlying blockchains must deal with the fact that the resources (e.g., network bandwidth, computation time and space) of each peer are limited, and exhausting them will lead to denial-of-service (DoS) attacks. As such, the aforementioned consideration of keeping the complexity for each peer

1Note that the security guarantees of gossip protocols are weaker than Byzantine-resilient Broadcast aka the Byzantine Generals problem [23] because they do not guarantee any kind of agreement or consistent ordering of messages gossiped among parties.
small (sublinear, preferably constant, in the number of total participants) is therefore not only relevant for efficiency but also essential for security.

For this reason, gossip protocols currently used in practice incorporate an array of (typically ad-hoc) measures to protect information propagation against DoS attacks. In the setting of blockchain protocols in particular, the most salient feature of such DoS mitigations is the fact that the adversary is resource-bounded (e.g., has limited hashing power, in the context of the Bitcoin protocol, or stake, in the context of proof-of-stake protocols), and peers can exploit this to manage network-wide message propagation. Techniques include rejecting previously seen proof-of-work messages and skipping content downloads that will not result in a local state update (such as skipping the download of a block’s contents when the block header indicates that it cannot be adopted based on the local state of the client).

It should be stressed that such measures are far from perfect, as exemplified by a number of attacks that have been described, including eclipse attacks [17] and routing attacks [2]. Moreover, the proof-of-stake setting poses additional difficulties stemming from the possibility of reusing keys to issue numerous conflicting messages [27] and the fact that the whole stakeholder set should be at hand for proof-of-stake verification to work, in sharp contrast to proof of work, which only needs the current difficulty level.

However, the security issues extend far beyond just the per-peer complexity. Most crucially, the design, setup, and maintenance of the overlay used for gossiping must be such that it resists Byzantine attackers—who make participants actively and maliciously deviate from the prescribed protocol—that command a large number of peers in the network. Despite all of the above shortcomings, in practice the information-propagation guarantees of the deployed networking layers of blockchain protocols are generally postulated to be sufficient for the higher-level protocol to maintain its security and correctness.

On the theory side, blockchain consensus protocols—be they Nakamoto-style (e.g., [11, 26]) or inspired by Byzantine fault-tolerant computing (e.g., [7]), based on proof of work (PoW) or proof of stake (PoS)—all crucially rely on the reliable and timely delivery of protocol messages (blocks, votes, etc.) to achieve liveness and many also to be safe. However, while the consensus layers of all these protocols have received considerable attention, with a number of them achieving provable security against Byzantine attackers, the design and security of the network layer are usually an afterthought at best.

Specifically, all previous formal security analyses of PoS protocols (e.g., [7, 10, 11]) use (over-)idealized message-passing abstractions that essentially promise that honest messages are distributed undisturbed to all honest parties within a reasonable delay window and ignore the fact that these abstractions must be implemented in the real world.

More broadly, there exists surprisingly little published work that considers the problem of extending Byzantine resilience to the communication layer of blockchains or gossip protocols in general.

The above state of affairs highlights serious shortcomings of the approaches taken both in theory and in practice and also suggests a significant gap between the two. Given that gossip is a critical piece of the protocol stack for any permissionless distributed-ledger protocol, the lack of a thorough, formal security treatment of its properties is a critical deficiency in the understanding of the security of these protocols. This the main motivation behind the present paper.

1.2 Our Results

This work takes a systematic and principled approach to alleviating the issues explained above and provides a novel design for Byzantine-resilient gossiping in the context of PoS blockchain protocols. The results are presented in the Universal Composability framework [5].

A Byzantine-resilient network layer for blockchains. The first main contribution of this work is a protocol for “synchronizing chains” globally among participants of PoS blockchain consensus. The protocol is designed to work over a standard, Internet-like network with (bounded-delay) message passing.

Crucially, the security of the network layer is based on the same assumption as that of the consensus layer, namely that the majority of stake in the system is controlled by honest parties. This may seem circular at first, as the proper operation of the network layer is conditioned on agreement on the stake distribution. The way to break this “cycle” is as follows: Commonly, Nakamoto-style PoS blockchains anyway split the execution of the consensus protocol into epochs and use the stake distribution SD1−i as a basis for consensus in epoch i + 1 (under the assumption of bounded stake drift during epochs). The same approach can be taken for the network layer, i.e., SD1−i underpins the execution of the network layer in epoch i + 1. Specifically, in the new protocol parties use a verifiable random function (VRF) to, based on SD1−i, create a stake-weighted random-graph overlay in which the degree of each party is constant in the number of participants. The use of VRFs allows parties to reject connection requests from participants that are not supposed to be in their neighbor set.3

Because the node degrees in the network protocol are constant, it is easy for an (adaptive) attacker to isolate a (bounded) fraction of the stake by corrupting all neighbors of parties making up said stake. To that end, edges in the graph have an expiration time, at which point replacements are sampled. In addition to helping parties recover from eclipses, this also allows the overlay to gradually adapt to changing stake distributions.

It may seem tempting to now simply perform run-of-the-mill block gossiping over the above overlay. Such an approach, however, seems to be unsuitable (at least) for Nakamoto blockchains: For example, it is an impractical and insecure design to ask parties to keep all received blocks around, as many of them could be adversarial in the PoS setting (an attacker may—in principle—generate as many blocks as they like, in particular as slot leader). Therefore, with block gossip, a party should delete blocks unless they extend its current local chain. During a fork event, however, the

---

3This work focuses on synchronizing chains; similar approaches can be taken to synchronize other protocol messages, such as votes, transactions, etc.

3Non-Nakamoto blockchains sometimes do not have the notion of an epoch built into the consensus protocol, e.g., because they finalize blocks and use the stake distribution of the finalized block as a basis for agreeing on the next block. However, for the purpose of equipping them with the network design presented here, such a notion can easily be added to them. Moreover, note that it seems that any reasonable design of a network layer for PoS protocols needs to assume bounded stake drift.
party may require previously deleted blocks for which the gossip is “over.” Similar issues apply if a party misses blocks, e.g., due to an eclipse. In general, which blocks are needed by a particular party to synchronize with the system is highly dependent on the party’s local state.

Therefore, stateless solutions, i.e., solutions in which neighbors do not share state, do not appear to be a good fit and will not yield DoS-resilient and scalable blockchain protocols in practice. A more suitable approach is to have each pair of neighbors run a bilateral chain synchronization (chain sync) protocol, which allows them to keep each other informed about their locally preferred chains. When a party discovers a better chain in one of these chain-sync instances or when it produces a better one, it informs all of its current chain-sync instances of the new chain.

This work abstracts this bilateral chain sync as a functionality \( f_{\text{bilateral}} \). The actual implementation of such a protocol is outside the scope of and irrelevant for this work.\(^4\) It is merely important to note that chain sync is stateful and instances thereof take time to set up in the real world (establishing the connection, initial synchronization of blocks, etc.). Hence, bilateral chain sync is intended to run between two parties for an extended (albeit bounded) amount of time. These facts are captured by \( f_{\text{bilateral}} \) in that there is an initial synchronization delay \( \delta_{\text{init}} \), which may be much larger than the delay \( \delta_{\text{sync}} \) occurring once a chain sync instance has been set up.

Finally, observe that in the blockchain context particularly (but also in general), the attacker must be prevented from interrupting the propagation of any specific message; otherwise, the attacker can, e.g., prevent honest chain updates from spreading through the network. Unfortunately, with an efficient gossip protocol, in which nodes have constant degrees, the (adaptive) attacker can simply corrupt all neighbors of a block leader and thereby halt propagation. It is therefore unavoidable to consider a model in which corruption requests by the attacker only take effect after a certain amount of time.

The ideal global chain-sync functionality. The security guarantees of the protocol above are captured by a functionality \( f_{\text{sync}} \), the second main contribution of this work. Similarly to the network functionalities assumed in prior work, \( f_{\text{sync}} \) provides global chain “propagation” within some time bound \( \Delta_{\text{sync}} \). However, there are several important differences stemming from the fact \( f_{\text{sync}} \) is implemented and not assumed. The two most crucial ones are the following:

- Due to the use of chain sync, \( f_{\text{sync}} \)‘s guarantees are slightly weaker than those offered by the assumed network functionalities in prior work: instead of a particular chain \( C \) “propagating” through the network within \( \Delta \), \( f_{\text{sync}} \) may also instead deliver different chains \( C' \) that are not worse (i.e., equal length or longer) than \( C \).

**Security proof.** In order to show that the new network protocol securely realizes ideal functionality \( f_{\text{sync}} \), this work derives a new result on expander graphs: Consider the stake-weighted random graph formed by parties in the protocol. Then, even after removing all corrupted nodes form the graph, leaving behind some fraction \( \alpha \) of honest stake, there exists a subgraph of honest parties, the backbone, corresponding to at least an \( (\alpha - \beta) \)-fraction of the total stake, for some \( \beta \), and this backbone is an expander graph (with overwhelming probability). Most importantly, the result holds even if the attacker chooses which nodes to remove with full knowledge of the entire graph. The expander property guarantees that the diameter in the backbone is small, and therefore timely chain “propagation” is possible therein.

Fully Byzantine-resilient PoS. As a final contribution, this work demonstrates how to utilize the synchronization functionality in the context of a proof-of-stake protocol. Specifically, \([11]\) is used to illustrate the result. First, note that the original analysis is insufficient: despite the fact that the networking model of \([11]\) allows a Byzantine adversary controlling a minority of stake, \( f_{\text{sync}} \) permits a “mobile” eclipsing strategy that would deplete the adversarial budget of any straightforward reduction to the adversary of \([11]\). To circumvent this issue, a revamped analysis is presented showing that adaptive eclipsing does not disturb the forkable-string analysis of \([11] \), which can be recovered to demonstrate that the protocol remains secure even against an adversary that exploits the enhanced capabilities of the adversarial interface of \( f_{\text{sync}} \). This gives rise to a new analysis of \([11]\) in an adversarial setting where in addition to party corruption, some degree of message suppression is also permitted.

1.3 Related Work

The use of gossip or epidemic algorithms in the context of distributed systems was put forth in \([13]\) and explored at length both in networking systems \([20]\) but also from theoretical angles \([19]\). The study of Byzantine fault tolerance in a network of a bounded degree was initiated in \([14]\) and further refined in \([29]\), where it is shown that if the adversary is bounded by \( O(n/\log n) \) or \( O(n) \), respectively, there exist graphs of bounded degree that facilitate broadcast.

In terms of total communication, it is known that the communication complexity of Byzantine broadcast is \( \Omega(n^2) \), and assuming some type of delay in the corruption model is necessary to break the communication complexity barrier to sublinear \([1]\). In the context of peer-to-peer networking for blockchains, a “structured” approach in the organization of the peer-to-peer network can be used to reduce communication complexity further, but at the expense of adaptive security \([28]\).

Our protocols, viewed from the lens of multiparty computation, exhibit a “communication locality,” which has also been studied

---

\(^4\)Secure and practical implementations of chain sync exist, e.g., \([9]\) and \([8, \text{Section 3.7}]\)
more broadly in the context of general secure multiparty computation [6]. We also remark that message suppression as an enhanced adversarial capability was also studied in the general secure MPC setting in the context of “omission corruptions” [30].

Finally, concurrently and independently of our work, [24, 25] studied the related problem of stateless flooding amongst a set of participants, also motivated in part by the blockchain setting. Their flooding protocol has peers connecting to a bounded-size, randomly chosen neighborhood for each message transmission. This can be seen as creating a separate random graph for every message. However, as mentioned above, stateless flooding is unsuitable in practice for blockchain protocols. Moreover, their protocol does not use any mechanism to resource bound the adversary (e.g., as a VRF) and hence there is no mitigation that can prevent honest parties from being flooded with messages by the adversary.

2 PRELIMINARIES AND NOTATION

UC security. Protocols are described and proven secure in the Universal Composability (UC) framework [5]. In UC, the security of a particular protocol is captured by comparing a real-world execution of the protocol to an ideal-world execution in which the protocol is replaced by an ideal functionality. In rough terms, a protocol \( \pi \) securely realizes a functionality \( F \), if for every real-world attacker \( A \) attacking \( \pi \), there exists an ideal-world simulator \( S \) attacking \( F \) such that the real and ideal experiments become indistinguishable to all environments \( Z \).

A protocol (in the real world) may itself make calls to so-called hybrid functionalities. These hybrid functionalities may serve to either model assumptions (e.g., \( F_{\text{net}} \) below) or are themselves realized by protocols. The UC framework guarantees that the security of a protocol is maintained when hybrids are replaced by the protocols that realize them.

Round structure. All functionalities/protocols proceed in rounds (not made explicit) and are assumed to have access to the current time, denoted \( T \). Generally, the round structure is such that parties first use a fetch-type command to retrieve information, followed by a send/set-type command to distribute information.

Attacker and corruption delay. The attacker considered is polynomially bounded and may corrupt parties, thereby learning their internal state, and make them deviate from the prescribed protocol arbitrarily. The attacker is adaptive, i.e., it may choose whom to corrupt on the fly during the execution of the protocol and based on all the information observed. However, there is a corruption delay of \( \xi_{\text{corr}} \), i.e., a corruption request issued by the attacker takes effect after a delay of \( \xi_{\text{corr}} \) rounds only.

Underlying network. This work considers parties \( P \) with so-called relays, identified by their IP addresses \( IP \). Having the actual node—holding the key material—firewalled by relays is common practice as a first line of defense against intrusion attacks.\(^\text{6}\)

Communication between relays is modeled by functionality \( F_{\text{net}} \) (cf. Figure 1), which captures a simple, Internet-like network. Parties

\[\text{Figure 1: Network/Internet functionality } F_{\text{net}}.\]

\[\begin{align*}
\text{Parameters: } & \delta_{\text{net}}: \text{maximum delay.} \\
\text{Variables: } & \text{The functionality keeps track of the following variables,}\, \text{initialized to the following values: array } IPs[P] := \emptyset; \text{ set of IPs owned by parties } P; \text{ array } M[mid]: \text{message records, indexed by message IDs (MIDs) mid.} \\
\text{IP addresses: } & \text{Upon } (\text{GETIP}) \text{ from } P; \text{ Output } (\text{GETIP}) \text{ to } S \text{ and ask } S \text{ for a unique address IP. Add IP to } IPs[P] \text{ and output } (\text{GETIP}, IP) \text{ to } P. \\
\text{Malicious IPs Registration: } & \text{Upon } (\text{REGIP}, IP) \text{ from } S; \text{ if IP is unique, add it to } IPs[S]. \\
\text{Message send: } & \text{Upon } (\text{SEND}, IP, IP', m) \text{ from } P \text{ with } IP \in IPs[P]; \\
& \text{ (1) Store } M[mid] := (\text{mid, IP, IP', } T, m). \\
& \text{ (2) Output } (\text{SEND}, mid, IP, IP', m) \text{ to } S. \\
\text{Malicious message send: } & \text{Upon } (\text{SEND}, IP, IP', m) \text{ from } S \text{ where } IP \in IPs[S] \text{ or } P \text{ with } IP \in IPs[P] \text{ is corrupted; Pick a unique mid and store } M[mid] := (\text{mid, IP, IP', } \infty, m). \text{ Output } (\text{SEND}, mid) \text{ to } S. \\
\text{Fetching: } & \text{Upon } (\text{FETCH}, IP) \text{ from } P \text{ with } IP \in IPs[P]: \\
& \text{ (1) Output } (\text{FETCH}, P, IP) \text{ to } S \text{ and ask } S \text{ for a set } M \text{ of MIDs.} \\
& \text{ (2) Let } M' \text{ be the set of MIDs corresponding to records } (\cdot, \cdot, IP, T, \cdot) \text{ with } T > T \geq \delta_{\text{net}}. \\
& \text{ (3) Let } \mathcal{M} := M[M \cup M'] \text{ and set } M[M \cup M'] := \bot. \\
& \text{ (4) Output } (\text{FETCH}, M') \text{ to } P, \text{ where } M' \text{ is the set } \mathcal{M} \text{ with MIDs and time stamp removed in each tuple.}
\end{align*}\]

can obtain (unique) IP addresses for their relays. \( F_{\text{net}} \) guarantees bounded-delay message transmission between any two relays. The attacker sees all messages sent and may send messages on behalf of any relay IP owned by a corrupted party; it is, however, not permitted to interfere with message transmission between honest relays (beyond inducing a bounded delay).

Master index. A master index \( M \) is made up of:

- the network directory \( ND \), which consists of tuples \( (P, IP, v) \), where \( P \) is a party ID, \( IP \) is an IP address, and \( v \) is a VRF public key (see below);
- the stake distribution \( SD \), which consists of tuples \( (P, \alpha) \), where \( \alpha \in [0, 1] \) denotes \( P \)’s stake fraction; and
- a seed value \( R \).

A master index is valid if (a) the same parties appear in \( ND \) and \( SD \), and each party appears at most once, (b) values \( IP \) and \( v \) appear only once in \( ND \), and (c) the values \( \alpha \) in \( SD \) sum up to 1. All master indices appearing in this work are tacitly assumed to be valid.

Observe that the MI format defined above restricts each party to having only one IP address. This choice was made for simplicity; the definition of master indices as well as all protocols and functionalities can easily be adapted to allow multiple IP addresses per party, thereby modeling the fact that in practice parties often have multiple relays.

\( ^{6} \)The environment both acts as distinguisher and controls the attacker/simulator as well as the inputs to the parties.

\( ^{\text{Note, however, that for the purposes of this work, the attacker corrupts parties, at which point it gains control over (all of) their relays.}} \)
The above guarantees are abstracted by an idealized functionality $F_{\text{ref}}$ (cf. Figure 2). The main commands offered by $F_{\text{ref}}$ are (i) $(\text{getKey})$, answered by $(\text{getKey}, v)$ for an (adversarially chosen) idealized public key $v$, (ii) $(\text{eval}, v, x)$, answered by $(\text{eval}, y, x, \pi)$, and (iii) $(\text{verify}, v, x, y, \pi)$, answered by $(\text{verify}, \phi)$ with $\phi \in \{0, 1\}$ indicating whether $\pi$ is a valid proof for the input/output pair $(x, y)$ under public key $v$.

### 3 Byzantine-Resilient Networking

#### 3.1 Overview

One of the main contributions of this work is to define and realize a synchronization functionality $F_{\text{sync}}$ that can be used by participants of proof-of-stake (PoS) consensus layers to globally synchronize their blockchains. A most crucial feature of $F_{\text{sync}}$ is that it is realizable under the same assumptions as the consensus protocol that builds on top of it.

In rough terms, the idea underpinning the protocol realizing $F_{\text{sync}}$ is as follows: Each consensus participant $P$ samples $\Theta P \cdot d$ neighbors in a stake-based fashion based on the output of a verifiable random function (VRF); $d$ is a small constant, and $\Theta P$ is a multiplier that depends on the amount of stake of $P$ itself. The use of a VRF guarantees that parties can verify whether they were indeed supposed to be chosen as neighbors by other participants.

Once the neighbors are sampled, chains are synchronized globally by each party engaging in bilateral chain synchronization with all its neighbors. Due to the fact that the resulting communication overlay is essentially a random graph, using expander theory, one can show that even with all adversarial nodes removed, there remains a large connected backbone with small diameter. This enables timely synchronization (TS), which is crucial to the security of many consensus protocols.

Of course, with a constant number of neighbors, it is unavoidable that some parties end up being connected solely to corrupted parties, which means that they are eclipsed. Consequently, $F_{\text{sync}}$ will have to grant eclipsing power to the adversary and can only guarantee TS to non-eclipsed parties.

Functionality $F_{\text{sync}}$ will be realized (cf. Section 3.4) from a functionality $F_{\text{bilateral}}$ (cf. Section 3.2), which models bilateral chain synchronization, as well as from network functionality $F_{\text{net}}$ (cf. Section 2) and (standard) functionality $F_{\text{ref}}$ (cf. Section 2).

#### 3.2 Bilateral Chain Synchronization

Functionality $F_{\text{bilateral}}$ (cf. Figure 3) models bilateral chain synchronization between two parties $A$ and $B$. In $F_{\text{bilateral}}$, each party has a local chain, and the functionality allows them to learn their counterparty’s chain as it evolves. A party’s local chain evolves by use of the setC command, under the restriction that local chains are only replaced by “better” chains as determined by a strict partial order prefer($\cdot, \cdot$), where prefer($C, C'$) (also denoted by $C > C'$) if and only if $C$ is strictly preferable to $C'$;\footnote{Commonly, $C$ is strictly preferable to $C'$ if it is longer.} prefer is a parameter of the functionality.

Both parties are informed about changes to their counterparty’s local chain with a delay of at most $\delta_{\text{sync}}$. However, initially, i.e., until both parties have used setC at least once (thereby indicating that
they are ready to start chain synchronization), the delay may be up to \( \delta_{\text{init}} \); this models the fact that in reality chain synchronization can take significant time between two parties who have just established a connection.

This work leaves the exact mechanism employed to realize \( F_{\text{bilateral}} \) open and simply assumes \( F_{\text{bilateral}} \) as a hybrid. In general, the approach to realizing \( F_{\text{bilateral}} \) is along the following lines: Upon establishing a connection, two parties first determine the point at which their local chains diverge and subsequently, they inform each other about changes to their local chains.

In practice, highly optimized implementations of \( F_{\text{bilateral}} \) are used in order to improve synchronization time even further. For an example of such an implementation, see [9] and [8, Section 3.7].

### 3.3 Synchronization Functionality

Functionality \( F_{\text{sync}} \), whose realization is the main focus of this work, allows parties to synchronize their chains with the rest of the participants. It is parameterized by an initial delay \( \Delta_{\text{init}} \), a synchronization delay \( \Delta_{\text{sync}} \), an eclipse delay \( \xi_{\text{ecl}} \geq \Delta_{\text{sync}} \), a "lookback" parameter

\[ \mu \geq \Delta_{\text{sync}} \text{, as well as an upper bound } \lambda \text{ on the amount of eclipsed honest stake.} \]

Note that parties have to agree on the round number in which they start using \( F_{\text{sync}} \). For convenience, in this section, initialization of \( F_{\text{sync}} \) begins in round \( -\Delta_{\text{init}} \), and parties actually start using \( F_{\text{sync}} \) in round 0.

**IP and key management.** Since \( F_{\text{sync}} \) is realized from \( F_{\text{net}} \) and \( F_{\text{reg}} \), interfaces for IP and key registration are also provided by \( F_{\text{sync}} \). The reason these are not abstracted away is that IPs and VRF keys must be known by the (higher-level) consensus protocol (e.g., to generate the genesis block).

**Master index and setup.** As previously mentioned, in the synchronization protocol parties will sample neighbors based on their stake. The stake distribution, however, is an object that emanates from the consensus layer, which itself relies on the synchronization functionality. This apparent cycle is broken as follows: \( F_{\text{sync}} \) expects each party to input its view on the master index (cf. Section 2) in the beginning via command setup, and \( F_{\text{sync}} \) only provides guarantees if (a) all honest parties (i) agree on the master index and (ii) input chains originating from the same genesis block, and (b) all honest parties are represented in the master index \( \mathcal{M} \) = (ND, SD, R) they input; a party is represented in \( \mathcal{M} \) if one of its IP addresses IP and one of its keys \( \nu \) appear in ND, i.e., \((P, IP, \nu) \in ND\).

When all of the above conditions are satisfied, \( F_{\text{sync}} \) has valid setup. If the setup is not valid, \( F_{\text{sync}} \) shuts down. Note that it is the responsibility of the consensus protocol (i.e., the environment in the diffusion context) to ensure that the setup is valid. This is commonly achieved via the genesis block (which is assumed to be available to all parties) initially and later on based on the epoch-wise consensus properties of the protocol. More details on this relationship are provided in Section 5.

**Eclipsing.** Due to the fact that in practically feasible and scalable protocols for realizing \( F_{\text{sync}} \), each party is connected only to a small subset of all participants, it is unavoidable that the adversary may eclipse certain honest parties by (adaptively) corrupting all of their neighbors. Consequently, \( F_{\text{sync}} \) offers an eclipse command by which the attacker can exclude any honest party from the TS guarantees (see below).

There are two limitations on the attacker’s use of the eclipse command. The first one is that eclipse commands only take effect after a delay of \( \xi_{\text{ecl}} \). The second limitation is based on the following notion of \( t \)-free party:

**Definition 3.1.** A \( t \)-free party is an honest party that was not eclipsed during rounds \( t \sim 1, 1, t - 2, \ldots, t - \mu \).

The eclipse restriction is that at any time \( t \), the fraction of stake corresponding to \( t \)-non-free honest parties may not exceed parameter \( \lambda \).

Formulating an eclipse restriction in this way prevents the attacker from eclipsing a completely different subset of parties in each round since a party eclipsed in round \( t \) essentially blocks a fraction corresponding to its stake in the attacker’s eclipse budget \( \Delta_{\text{sync}} \text{ for } \mu \).

\[ \text{For the sake of offering a concrete description: In order to figure out the common prefix, party A sends block hashes of suffixes of length 1, 2, 4, 8, \ldots \text{ to party B until B finds that one of these hashes corresponds to a block on their chain. Thereafter, the exact point of divergence is located by binary search. In the worst case, this takes } O(\Delta_{\text{init}} \cdot \log k), \text{ where } k \text{ is the common prefix parameter. Note that this is independent of the length of the parties’ chains. Furthermore, on average, in a longest chain protocol, due to the exponential decay in the probability of divergence (as a function of the size of the divergence), synchronization time is much shorter (typically a small constant) between up-to-date peers.} \]

\[ \text{In a BFT-style blockchain like Algorand [7], one local chain is normally a prefix of the other, which simplifies this step.} \]
The functionality keeps track of the following variables, initialized to the values below for all parties \( P \) and rounds \( t \):
1. \( \text{IPs}[P] := \emptyset \): set of IPs owned by \( P \);
2. \( \text{Keys}[P] := \emptyset \): set of keys owned by \( P \);
3. \( C[P, t] := \perp \): local chain of \( P \) in round \( t \);
4. \( E[P, t] := \text{false} \): eclipse status of \( P \) in round \( t \);
5. \( M[P] := \perp \): master index as seen by \( P \); recall that \( M = (\text{ND}, \text{SD}, \text{R}) \) (cf. Section 2).

**Setup:** Upon \( \text{setup}(M', C) \) from \( P \) in round \( t - \Delta_{\text{sys}} \): set \( C'[P', \Delta_{\text{sys}}] = C \) and \( M'[P] := M \).

**IP addresses:** Upon \( \text{getIP}(P) \) from \( P \): Output \( \text{IPs}[P] \) to \( S \) and ask \( S \) for a unique address IP. Add IP to \( \text{IPs}[P] \) and output \( \text{getIP}(P) \) to \( P \).

**Keys:** Upon \( \text{getKeys}(P) \) from \( P \): Output \( \text{getKeys}(P) \) to \( S \) and ask \( S \) for a unique key \( v \). Add \( v \) to \( \text{Keys}[P] \) and output \( \text{getKeys}(v) \) to \( P \).

**Fetch & Set:**
Upon \( \text{fetch}(P) \) from \( P \):
- Output \( \text{fetch}(P) \) to \( S \) and ask \( S \) for a set \( D \) of chains.
- For any \( C \) with \( \text{C}[P', \Delta_{\text{sys}}] = C \) for some \( \Delta_{\text{sys}} \)-core node \( P' \) in round \( t \) as well as \( \text{prefer}(C, P, \Delta_{\text{sys}}) \) for all chains \( C' \) in \( D \), add \( C \) to a set \( D' \).
- Output \( \text{fetch}(D \cup D') \) to \( P \).

**Register IPs:** Upon \( \text{regIP}(IP) \) from \( S \): if IP is unique, add it to \( \text{IPs}[P] \).

**Register keys:** Upon \( \text{regKey}(v) \) from \( S \): if \( v \) is unique, add it to \( \text{Keys}[P] \).

**Notions**
- **Representation:** \( P \) is represented if \( (P, \text{IP}, v) \in \text{ND} \) for IP in \( \text{IPs}[P] \) and \( v \in \text{Keys}[P] \).
- **Eclipsed:** \( P \) is eclipsed in round \( t \) if \( E[P, t] = \text{true} \).
- **Core and free parties:** \( P \) is a core party (resp. \( \text{t-free party} \)) if it was not eclipsed in rounds \( t - \Delta_{\text{sys}}, \ldots, t - 1 \) (resp. \( t - \mu, \ldots, t - 1 \)).
- **Valid setup:** \( \text{Fsync} \) has valid setup if (a) all honest parties use setup with (i) chains originating from the same genesis block and (ii) the same \( M \), and (b) all honest parties are represented. If \( \text{Fsync} \)’s setup is not valid, it halts.

**Adversarial**
- **Eclipsing:** Upon \( \text{eclipse}(P) \) from \( S \)—after all honest parties have set master index in current round \( T \); if eclipsing \( P \) in round \( T \) would result in the fraction of \( (T + \xi_{\text{sync}} + 1) \)-non-free stake remaining below \( \lambda \), set \( E[P, T + \xi_{\text{sync}}] = \text{true} \).

---

**Figure 4:** Functionality \( \text{Fsync} \) for global chain synchronization among participants of PoS consensus.

 slots. Note, however, that it is absolutely possible for the adversary to eclipse a particular party for an unlimited amount of time. This must be dealt with by the higher-level consensus protocol using \( \text{Fsync} \).

**Main operation and timely synchronization (TS).** Similarly to \( \text{Fbilateral} \), a party uses setC to switch their local chain to a strictly better one according to a predicate prefer (cf. Section 3.2). Moreover, parties use fetch in order to receive information about chains of other participants.

The TS guarantee offered by \( \text{Fsync} \) is based on the following notion of \( t \)-core:

**Definition 3.2.** A \( t \)-core party is an honest party that was not eclipsed during rounds \( t - 1, t - 2, \ldots, t - \Delta_{\text{sys}} \).

Thus, the \( t \)-core notion is very similar to that of \( t \)-free parties, except with less “lookback” (as \( \Delta_{\text{sys}} \leq \mu \)).

The TS guarantee is now the following: Suppose an honest party \( P \) sets its local chain to some chain \( C \) at time \( t \). Then, by time \( t + \Delta_{\text{sys}} \), provided \( P \) is in the \( (t + \Delta_{\text{sys}}) \)-core, the following holds for all \( (t + \Delta_{\text{sys}}) \)-core parties \( P' \):
- either \( P' \) has already switched their local chain to \( C' \), or
- the fetch command returns \( C' \).
Independently and based on their stake, where $\Theta_P$ is a multiplier that depends on the stake $\alpha_P$ of $P$ itself; specifically,

$$\Theta_P := \left[ \frac{\alpha_P}{\alpha_{\min}} \right],$$

for some parameter $\alpha_{\min}$.

Connections to neighbors expire after $dr$ slots; thus, in each round that is a multiple of $r$, $\Theta_P$ new neighbors are sampled. Updating the overlay in this fashion helps parties recover from eclipse events in practice; in the context of this work, however, the adaptive attacker considered here may simply corrupt all new neighbors of a party. Hence, with such a powerful adversary, there is no upper bound on the duration of an eclipse for a particular party (short of the adversary exhausting its corruption budget, of course). Furthermore, refreshing neighbors also allows gradual adaptation of the overlay to changing stake distributions.

The actual sampling performed by a party $P$ is described as a procedure $\text{SamCon}(t, j)$ in Figure 5, where $t$ is a time stamp and $j = 1, \ldots, \Theta_P$. The procedure uses a subroutine $\text{pick}(y)$ which, using VRF output $y$ as random coins, chooses a party $P'$ proportionally to its stake in SD. Note that the inputs to the VRF are (apart from $P$'s public key) the random nonce $R$ (part of $M$), $t$, as well as $j$.

Subsequent to the above sampling, $P$ sends a connection request to $P'$ via $F_{\text{net}}$ and immediately begins a corresponding instance of $F_{\text{bilateral}}$. Conversely, $P'$ will start the instance upon receiving the connection request (after performing the obvious checks).

**Chain management.** Upon receiving $(\text{set}C, C)$ from the environment, if $C$ is better than $P$’s current local chain, $P$ updates the corresponding variable and inputs $(\text{set}C, C)$ to all running $F_{\text{bilateral}}$ instances.

Upon receiving $(\text{fetch})$ from the environment, $P$ sends $(\text{fetch})$ to all running $F_{\text{bilateral}}$ instances and collects the answer chains in a set $D$; all chains in $D$ preferable to $P$’s current local chain are returned to the environment.

**Chain validity and switching.** With the application of blockchain consensus in mind, observe that in the context of $\pi_{\text{sync}}$ (or, in the ideal world, of $F_{\text{sync}}$) there is no notion of "chain validity." This is a concept from the higher-level consensus layer. Consequently, $\pi_{\text{sync}}$ ($F_{\text{sync}}$) cannot possibly check a chain for its validity and "automatically" switch to the best valid chain. This task therefore falls upon the environment.

At this point it is also important to observe that successful chain "propagation" through the network crucially depends on the environment—in each round—using $(\text{set}C)$ to make each party

\[ F_{\text{bilateral}} \]

\[ \pi_{\text{sync}} \]
switch to the best valid chain received so far. In order to circumvent the application-specific nature of the notion of “validity,” the following proxy for it is used:

**Definition 3.3.** In an execution of $\pi_{sync}$ (or $F_{sync}$), a chain $C$ is **endorsed** if the environment at some point inputs $(SET, C)$ on behalf of an honest party $P$.

The notion of endorsed chains allows to define the class of environments $Z$ w.r.t. which $\pi_{sync}$ must realize $F_{sync}$:

**Definition 3.4.** An environment $Z$ is **$H$-improving** if in each round $t$, every honest party $P$ inputs $(SET, C)$ for a chain $C$ which is maximal w.r.t. prefer among all endorsed chains received by $P$ via FETCH in rounds up to $t$.

The above finally leads to the following main theorem:

**Theorem 3.5.** Let

- $n \in \mathbb{N}$,
- $\alpha > \beta > 0$, $\delta > 0$, $c_{\min}$, and $c_{\max}$ be constants satisfying $0 < c_{\min} < 1 < c_{\max}$ and $(\alpha - \beta)/2 \geq \beta + c_{\min}/n$, and
- $r \in \mathbb{N}$.

Then, for all sufficiently large $d$, there exists a constant $\gamma > 0$ such that protocol $\pi_{sync}[d + 1, r, c_{\min}/n] r$-securely realizes $F_{sync}[\Delta_{init}, \Delta_{sync}, \mu, \xi_{ccl}, \lambda]$ in the $(\{PoE[\delta_{net}], F_{net}, F_{bilateral}[\delta_{init}, \delta_{sync}]\})$-hybrid model w.r.t. $H$-improving environments that (1) input an $M1$ with $n$ parties in which no party owns more than a $c_{\max}/n$ fraction of stake, (2) corrupt at most an $\alpha$-fraction of stake, (3) run for at most $L$ rounds, where

- $\Delta_{init} = \delta_{net} + \delta_{init}$,
- $\Delta_{sync} = 8\ell$ for $\ell := \lceil - \log_{1+\gamma}(2c_{\min}/n) + 1 \rceil$,
- $\lambda = 2(\beta + c_{\min})$, and
- $\varepsilon = L/r \cdot e^{-\delta n}$.

**Remarks.** A simple Chernoff bound can be used to show that if there are no small-stake nodes (with less than $c_{\min}/n$ stake), the degrees of all parties are constant. In case there are many small-stake nodes, the degrees of large nodes are beyond constant. However, one can show that by having small-stake node pick their peers uniformly (instead of based on stake), all node degrees go back to constant again.

The security error $\varepsilon$ is exponentially small in the number of parties $n$. It is, of course, important in practice to ensure by suitable means that there are sufficiently many parties participating. One possible way to achieve this by having so-called stake-pool operators (SPOs), to which parties can delegate stake, run the blockchain and use incentive mechanisms to control the total number of SPOs.

Furthermore, there are also several ways of enforcing the maximum-stake restriction in Theorem 3.5. In a system with SPOs, one may restrict the maximum delegated stake on the consensus level. Alternatively, one can again set incentives in such a way that SPOs do not attract more than a certain amount of stake. For more information, see [4].

## 4 SECURITY PROOF

This section presents the security proof of the synchronization protocol $\pi_{sync}$ (cf. Section 3.4).

The most crucial part of the security argument is a new result on stake-based expander graphs. Specifically, given a graph $G$ wherein each vertex $v$ has assigned to it some stake $\alpha_v \in (0, 1]$, where $\sum_v \alpha_v = 1$, and each vertex chooses its neighbors in the stake-based fashion adopted by protocol $\pi_{sync}$, the results in Section 4.1 show that even after removing all adversarial nodes from $G$, leaving behind at least some $\alpha$-fraction of honest stake, there exists an honest “backbone” holding at least $\alpha - \beta$ stake, for some $\beta$, such that the backbone is an expander graph.

As shown in Section 4.2, the above translates to $\pi_{sync}$ realizing $F_{sync}$ with roughly a $\beta$-fraction of honest stake being eclipsed, while due to the expander property of the backbone, the remaining “core” of honest parties are at most $O(\log n)$ hops apart from each other, where $n$ is the total number of parties. It should be noted that the this core only approximately corresponds to the backbone above, the reason for this being that (a) the backbone cannot be efficiently computed (and thus, an approximation has to be used), and (b) backbone nodes with less than $c_{\min}/n$ stake need to be excluded from the core (because the expander property cannot be used to bound their distance from other nodes in the backbone).

### 4.1 Expanders Resisting Vertex Deletion

It is a well-known fact that random graphs—with a wide variety of edge distributions—form expanders with high probability and hence have small diameter and other desirable properties. This section shows that the random graphs produced by the protocol possess such strong properties even if an adversary with full knowledge of the graph is permitted to remove a constant fraction of the nodes.

As outlined above, we show that for any two constants $\alpha > \beta > 0$, there is a degree parameter $d$ for which the following holds: so long as an $\alpha$ fraction of nodes remain after adversarial deletion, there is a subset (the “backbone”) consisting of an $\alpha - \beta$ fraction of the nodes that is a strong expander. Typically, one would choose $\beta \ll \alpha$ so that the backbone consists of almost all of the remaining vertices.

These results are motivated by a classical theorem of Upfal [29], which uses different methods to establish a similar property of Ramanujan graphs (which achieved fixed constants) and [27], which established that any constants can be achieved by appropriate choice of $d$. A final remark before transitioning to the technical survey: we also work directly with weighted graphs (with a weight corresponding to stake) so that we can define and treat a natural notion of “stake-weighted” expansion.

Our protocol directly motivates the following family of distributions of random directed graphs.

**Definition 4.1.** Let $\bar{d}$ and $n$ be positive integers and let $\bar{D}$ be a probability distribution on $[n]$ with the property that $d_v = \bar{n} \bar{d}(v)$ is an integer for every vertex $v$. We let $\mathcal{G}_{\bar{n}, \bar{d}(\bar{D})}$ denote the probability law on directed multigraphs with $V = [n]$ obtained by selecting,
for each \( v, d_v \) outgoing neighbors \( w_1, \ldots, w_{d_v} \) independently according to \( D \) and defining the multiset of directed edges to be \( E = \bigcup_{v} d_v^{\to}(v, w_i). \)

We let \( G_{n, d} \) denote the special case when \( D \) is the uniform distribution, in which case \( d_v = d \) for all \( v \).

We wish to show that \( G_{n, d} \) is typically a “stake expander”; that is, that sets \( S \subseteq V \) have a number of neighbors outside them, or edges leaving them, proportional to their total stake.

**Definition 4.2.** Let \( G = (V, E) \) be a directed graph. For a subset \( S \subseteq V \), we define the (outer) boundary of \( S \) as

\[
\partial(S) = \{ w \notin S \mid \exists s \in S : (s, w) \in E \text{ or } (w, s) \in E \}.
\]

Let \( D \) be a distribution on the set \( V \) and \( \gamma > 0 \). We say that \( G \) is a \((D, \gamma)\)-expander if for every subset of vertices \( S \subseteq V \) for which \( D(S) \leq 1/2 \),

\[
D(\partial(S)) \geq \gamma D(S),
\]

where we use the notation \( D(S) \) to denote \( \sum_{v \in S} D(v) \).

**Theorem 4.3.** Let \( \alpha > \beta > 0 \) and \( \delta > 0 \) be positive constants, and let \( c_{\min} \) and \( c_{\max} \) be positive constants satisfying \( c_{\min} < 1 < c_{\max} \). For sufficiently large \( d \) there is a constant \( \gamma > 0 \) for which the following holds: Let \( D \) be a distribution on \( V = [n] \) for which \( c_{\min}/n \leq D(v) \leq c_{\max}/n \) and \( d_v \pm \delta D(v) \) is an integer for each \( v \in V \). Consider \( G = (V, E) \) drawn according to \( G_{n, d, D} \). Then, except with probability \( \Pr_{\text{fail}} \leq e^{-\delta n} \), for every subset \( S \subseteq V \) for which \( D(H) \geq \alpha \), there is a subset \( H' \subseteq H \) for which \( D(H') \geq \alpha - \beta \) and the subgraph induced by \( H' \) is a \((D', \gamma)\)-expander, where \( D' \) is the distribution \( D \) scaled by \( 1/D(H') \).

See Appendix A for the proof.

Remark. The condition in Definition 4.1 and Theorem 4.3 that \( ndD(v) \) is an integer for all \( v \) is a mere convenience so that the out-degree of each vertex will be a fixed integer \( d_v \). We can also define \( d_v = \lfloor ndD(v) \rfloor \). This changes the effective stake of each player by a factor of at most \( 1 \pm O(1/d) \). In fact we only need an upper bound on the stake each vertex has, as we can hand over all the vertices with very low stake to the adversary (cf. Lemma A.5).

### 4.2 Security of the Synchronization Protocol

This section uses the results from Section 4.1 to finally prove the security of protocol \( \sync \).

**Simulation basics.** Simulator \( S \) internally simulates instances of the protocol and of hybrids \( F_{\text{net}}, F_{\text{ref}}, \) and \( F_{\text{bilateral}} \) as well as the adversary \( A \) which acts as the interface to the environment; in the following, this ensemble is referred to as the *simulated real world* (SRW). Specifically, \( S \) reacts as follows when receiving messages from \( F_{\text{sync}} \):

- Upon \((\text{setup}, P, \text{MI}, C)\): in the SRW, input \((\text{setup}, \text{MI}, C)\) on behalf of \( P \).
- Upon \((\text{getIP}, P)\): in the SRW, input \((\text{getIP})\) on behalf of \( P \); wait to receive \((\text{getIP}, \text{IP})\) on behalf of \( P \); return \( \text{IP} \) to \( F_{\text{sync}} \).
- Upon \((\text{regIP}, P)\): in the SRW, input \((\text{regIP}, P)\) to \( F_{\text{sync}} \).
- Upon \((\text{regKey}, P)\): in the SRW, input \((\text{regKey}, P)\) to \( F_{\text{sync}} \).
- Upon \((\text{getKey}, P)\): in the SRW, input \((\text{getKey}, P)\) on behalf of \( P \); wait to receive \((\text{getKey}, \text{v})\) on behalf of \( P \); return \( \text{v} \) to \( F_{\text{sync}} \).
- Upon \((\text{fetch}, P)\): in the SRW, input \((\text{fetch}, \text{ID})\) on behalf of \( P \); wait to receive \((\text{fetch}, \text{ID})\); return \( \text{ID} \) to \( F_{\text{sync}} \).

Messages from \( A \) are handled as follows:

- Upon \((\text{regIP}, P)\): input \((\text{regIP}, P)\) to \( F_{\text{sync}} \).
- Upon \((\text{regKey}, P)\): input \((\text{regKey}, P)\) to \( F_{\text{sync}} \).

**Notation.** Fix the master index \( \text{MI} = (\text{ND}, \text{SD}, \text{R}) \) input by the honest parties at the beginning; recall that \( n \) denotes the number of parties in \( \text{MI} \). In the following, for a subset \( S \) of the parties in \( \text{MI} \), denote by \( a_S := \text{SD}(S) \) the amount of stake held by parties in \( S \).

**Determining whom to eclipse.** A crucial part of \( S \) is to ensure that when handling fetch commands, \( F_{\text{sync}} \) does not enforce delivery guarantees that contradict the SRW. To that end, \( S \) determines which honest parties are “eclipsed” and relays this information to \( F_{\text{sync}} \). Recall that \( F_{\text{sync}} \) will not offer any guarantees to non-core parties, where a party is in the core in round \( t \) if and only if it has not been eclipsed in rounds \( t - 1, t - 2, \ldots, t - \Delta_{\text{sync}} \).

Towards understanding which parties to eclipse at a particular time \( t \), consider the graph \( G \) formed by all parties in \( \text{MI} \) and the connections implied by the use of the VRF at time \( t \), but ignore the edges added to it during the latest refresh (i.e., in the largest round \( t' \leq t \) that is a multiple of \( r \)). This graph follows the distribution \( G_{n, d, \text{SD}} \).

Let \( H \) denote the set of honest parties in at time \( t \). By Theorem 4.3, there exists a set \( H' \subseteq H \) with \( a_{H'} \geq \alpha_{H'}/(1 + \beta) \), such that the subgraph of \( G \) induced by \( H' \) is an \((D', \gamma)\)-expander, where \( D' \) is \( D \) scaled by \( 1/(1 + \beta) \). This expander property allows to bound the diameter between parties in \( H' \) with a certain minimum amount of stake, a fact used to show:

**CLAIM 4.4.** From each party in \( H' \) with stake at least \( c_{\min}/n \) in \( \text{SD} \), one can reach more than \( (\alpha_{H'}/(1 + \beta))/2 \) of honest stake in at most \( \ell \) steps.

Proof. Consider a party \( P \in H' \) with stake \( a_P \geq c_{\min}/n \). Its stake according to \( \text{SD}' \) is equal to

\[
a_P/a_{H'} \geq \frac{c_{\min}}{a_H n}.
\]

By the expander property on \( H' \), one can reach more than \( 1/2 \) of the stake in \( H' \) from \( P \) (according to \( \text{SD}' \)) in \( \ell' \) steps if

\[
\frac{c_{\min}}{a_H n} (1 + \gamma)^{\ell'} > \frac{1}{2}.
\]

This is satisfied for

\[
\ell' := \log_{1+\gamma} \left( \frac{a_H n}{2c_{\min}} \right) + 1 \leq \log_{1+\gamma} \left( \frac{n}{2c_{\min}} \right) + 1 = \ell.
\]

Reaching half of the stake in \( H' \) according to \( \text{SD}' \) translates to reaching

\[
\frac{a_H}{2} \geq \frac{\alpha_{H'} - \beta}{2}
\]

of stake according to \( \text{SD} \).
Since the security argument in Theorem 4.3 is non-constructive, it is unclear whether set $H'$ can be efficiently determined. Instead, consider the set

$$I_1 := \{ h \in H \mid \text{can reach } \beta + c/n \text{ HS in } \ell \text{ steps from } h \},$$

where HS stands for “honest stake.” The subscript is dropped from $I$ whenever clear from the context.

**Claim 4.5.** $a_1 \geq \alpha_H - \beta - c_{\min}$.

**Proof.** First, observe that $(\alpha_H - \beta)/2 \geq (\alpha - \beta)/2 \geq \beta + c_{\min}/n$, where the last inequality is by assumption. By Claim 4.4, all parties in $H'$ with stake at least $c_{\min}/n$ are therefore in $I$. The claim follows by observing that at most $c_{\min}$ of the total stake is held by parties with more than $c_{\min}/n$ stake.

As the subgraph induced by $H'$, that induced by $I$ also has bounded diameter:

**Claim 4.6.** There is a path of length at most $4\ell$ between any two parties in $I$.

**Proof.** By definition of $I$, from any node in $I$, one can reach at least $\beta + c_{\min}/n$ stake in $H$ in $\ell$ steps, and, therefore, $c_{\min}/n$ stake in $H'$. The argument in the proof of Claim 4.4 suggests there is a path of length at most $2\ell$ between any two nodes with stake at least $c_{\min}/n$ in $H'$. One concludes that there must be a path of length at most $4\ell$ between any two nodes in $I$.

Given the above, the eclipse strategy of $S$ is to, in each round $t$, use (ECLIPSE, $P$) to eclipse all parties $P \notin I_1$. However, due to the eclipse-delay property of $F_{\text{sync}}$, $S$ is forced to set eclipsed status based on $I_1$ at or before time $t - \xi_{\text{ecl}}$. This is, however, possible:

- Since $\xi_{\text{ecl}} \leq r$ and the edges added during the latest round $t' \leq t$ that was a multiple of $r$ are ignored, the topology of $G$ in round $t$ is known by round $t - \xi_{\text{ecl}}$.
- Since $\xi_{\text{corr}} \geq \xi_{\text{ecl}}$, which parties are honest/corrupted is also known by round $t - \xi_{\text{ecl}}$.

**Bounding synchronization time.** The next step in the proof consists of arguing that $F_{\text{sync}}$ never has to add any chain $C$ to set $D'$ during a FETCH call by party $P$ in some round $t$.

To that end, assume first that there is no multiple of $r$ in $(t - 4\ell, \ldots, t - 1)$, i.e., the underlying graph $G$ does not change in this period. Consequently, $I_{t-4\ell} \supseteq I_{t-(4\ell-1)} \supseteq \ldots \supseteq I_{t-1}$, where the only reason elements are dropped from $I$ over time is corruption.

Consider now the FETCH command by $P$ in round $t$. Recall that a chain $C$ is added to $D'$ only if

(i) $C$ was held by some honest party $P'$ in round $t - \Delta_{\text{sync}}$, (ii) neither $P$ nor $P'$ were eclipsed in rounds $t - 1, \ldots, t - \Delta_{\text{sync}}$, (iii) $C$ is preferable to the chain held by $P'$ in round $t - 1$ and to all chains in set $D$ (during the FETCH call).

Observe that $\Delta_{\text{sync}} \geq 4\ell$; thus, that the fact that (ii) holds (i.e., $S$ did not issue, in advance, eclipse commands for $P$ or $P'$ for rounds $t - 1, \ldots, t - \Delta_{\text{sync}}$) means that both parties $P$ and $P'$ were in sets $I$ during rounds $t - 1, \ldots, t - 4\ell$.

By the monotonicity of the sets $I$, there has been a path of length at most $4\ell$ between $P'$ and $P$, which, combined with the facts that $Z$ is H-improving and (again) $\Delta_{\text{sync}} \geq 4\ell\Delta_{\text{sync}}$, means that by time $t$, either $P'$'s local chain will already be set to a chain $C' \notin C$ or a chain $C' \notin C$ is in set $D$ at time $t$. In either case, $C$ is not added to $D'$.

Finally, for intervals including changes to $G$, observe that since $\Delta_{\text{sync}} = 8\ell$, there are at least $4\ell$ rounds either before or after the change to $G$.

**Amount of non-free stake.** The fact that the amount of non-free stake remains below $\lambda = 2(\beta + c_{\min})$ follows from Claim 4.5, noting that the extra factor of 2 is required for $\Delta_{\text{sync}}$-sized intervals containing a multiple of $r$.

**Proof (of Theorem 3.5)**. In order to complete the proof based on the above, note that it remains merely to apply a union bound over all refresh periods (which are of length $r$).

## 5 FULLY SECURE POS CONSENSUS

This section discusses the application of running a PoS consensus protocol on top of the chain synchronization functionality $F_{\text{sync}}$. For concreteness, the protocol considered here is Ouroboros Praos [11] which is a longest chain Nakamoto-style blockchain PoS protocol and is described first. This is followed by a comparison of the “diffusion” functionality $F_{\text{diff}}$ used in [11] and $F_{\text{sync}}$. Based on this comparison, the changes to Ouroboros Praos’ security proof are presented and discussed; in particular, as a contribution of possibly independent interest, a generalized version of the so-called forkable-string analysis is provided.

### 5.1 Ouroboros Praos

Ouroboros Praos (or, simply, Praos) proceeds in so-called slots. In each slot, each party $P$ first checks whether it has “received” valid chains that are longer than its current local chain; if so, it switches to a longest one among those. Subsequently, based on the stake distribution used in the current epoch, $P$ checks whether it is the slot leader. This determination is made based on the output $y$ of a VRF evaluated on (in addition to $P$’s key) the slot number and the so-called epoch randomness; if $y$ ends up below a certain threshold, which is a monotonically increasing function of $P$’s stake, $P$ is a slot leader. As such, it creates a new block extending its current local chain $C$; the block consists of the hash of the last block of $C$, the slot number, $P$’s identity, the VRF output and VRF proof, a data payload, as well as a signature. The resulting chain $C'$ is then “sent to everyone.”

### 5.2 Diffusion vs. Synchronization

In [11], parties share a diffusion functionality $F_{\text{diff}}$, parametrized by a value $\Delta$, with the simple intuitive property that any chain an honest party diffuses via $F_{\text{diff}}$ will “arrive” at all other honest parties with a delay of no more than $\Delta$ slots.

Consider now using $F_{\text{sync}}$ in order to “synchronize” rather than “diffuse” chains. Figure 6 contains a description of the (static-stake) Praos protocol using $F_{\text{sync}}$. The protocol additionally uses hybrids $F_{\text{sync}}$ for slot leadership as well as the following two hybrids, which are only described on a high-level sufficient for the context of this section:

- $F_{\text{master}}$ is used for master-index and genesis-block generation.
- more precisely, parties initially send information such as
of leader elections (as determined by a characteristic string) into a single numeric metric of interest called margin and (ii) an analysis of the stochastic process that governs generation of characteristic strings and the resulting behavior of margin. The final result is articulated as a large-deviation bound for margin, which establishes consistency with high probability. In this section, we discuss how that analysis can be adapted to our setting with a finer-grained view of networking and block delivery.

Characteristic strings in Praos have the form \( w = w_1w_2\ldots \) and record information about slot leadership in an execution. Each character in the string is a symbol \( w_i \in \{A, H, \perp\} \), where

\[
\begin{align*}
  w_i &= \begin{cases} 
    A & \text{if slot } i \text{ has an adversarial or multiple leaders}, \\
    H & \text{if slot } i \text{ has a single honest leader}, \\
    \perp & \text{if slot } i \text{ has no leader}.
  \end{cases}
\end{align*}
\]

A \( \Delta \)-fork \( F \) for a characteristic string \( w \) is a directed, rooted tree, intended to represent the topology of all chains observed during an execution of Praos: Each vertex \( v \) of \( F \) corresponds to a block in a particular chain and has a label \( \ell(v) \in \mathbb{N} \), which records the block’s slot number. The genesis block is represented by the root of the tree. The edges of a fork are directed “away from” the root so that there is a unique directed path from the root to any vertex.

Based on the description of Praos, it is easy to see that a fork satisfies the following properties:

(i) The root \( r \in V \) has label \( \ell(r) = 0 \) and is considered honest by fiat.

(ii) The sequence of labels \( \ell() \) along any directed path is strictly increasing. Reason: this is enforced by the protocol.

(iii) If \( w_i = H \), there is a unique vertex \( v \) for which \( \ell(v) = i \).

Reason: honest parties do not create multiple blocks.
(iv) For any pair of honest vertices \( v, v' \) (i.e., \( w_{\ell(v)} = w_{\ell(v')} = H \)) with \( \ell(v) + \Delta \leq \ell(v') \), their lengths (i.e., distance from root) \( \text{len}(v) \) and \( \text{len}(v') \) satisfy \( \text{len}(v) < \text{len}(v') \). Reason: As per the guarantees of \( F_{\text{diff}} \), during the creation of the block corresponding to vertex \( v' \) in slot \( \ell(v') \), the block corresponding to \( v \) was available to build on since it was created in slot \( \ell(v) \), which was at least \( \Delta \) slots before \( v' \); hence, \( \text{len}(v') \) must be strictly larger than \( \text{len}(v) \).

The analysis proceeds by defining a notion of margin for a fork, which reflects the presence of pairs of paths (chains) in the fork that diverge prior to a particular slot and exceed the length of the deepest honest block. Intuitively, such pairs of paths correspond to a consistency failure and, indeed, the precise definition of margin ensures that the quantity is positive exactly when such a consistency failure exists. This notion is extended to characteristic strings by maximizing over all forks consistent with the string. The analysis then shows that margin satisfies a recurrence relation in terms of the characteristic string (corresponding to an execution of the protocol) and, finally, that the probability of observing a positive margin is small.

5.3.2 Accounting for Eclipsed Parties. Clearly, the \( \Delta \)-fork formalism above does not consider cases where (a) the leader is out of sync and potentially fails to build on some longest chain \( C \) whose last block is more than \( \Delta \) slots old or (b) the leader’s block takes longer than \( \Delta \) to reach the next slot leader; naturally, an eclipse event can cause both (a) and (b). In the following, an honest leader not suffering from (a) is called current, and an honest leader not suffering from (b) is called relayed. An honest leader that is both current and relayed is called synchronized.

In order to update the forkable-string analysis to account for non-relayed parties, the following changes are introduced to it. First, the characteristic string is now over an alphabet \( w_i \in \{ A, \ldots, R, \bot \} \), where

\[
 w_i = \begin{cases} 
 A & \text{if slot } i \text{ has an adversarial or multiple leaders}, \\
 \text{CR} & \text{if slot } i \text{ has a single synchronized leader}, \\
 C & \text{if slot } i \text{ has a single current leader}, \\
 R & \text{if slot } i \text{ has a single relayed leader}, \\
 \bot & \text{if slot } i \text{ has no leader}.
\end{cases}
\]

Second, condition (iv) for forks is amended as follows:

(iv) For any pair \( v, v' \) with \( w_{\ell(v)} \in \{ R, \text{CR} \} \) and \( w_{\ell(v')} \in \{ C, \text{CR} \} \) and where \( \ell(v) + \Delta \leq \ell(v') \), their lengths (i.e., distance from root) \( \text{len}(v) \) and \( \text{len}(v') \) satisfy \( \text{len}(v) < \text{len}(v') \).

The definition of margin is essentially unchanged with this new definition of fork. However, the recursive behavior depends on the new semantics of these richer characteristic string symbols and exhibits some rather interesting properties: in particular, the effect of the \( C \) and \( R \) symbols depends on whether the worst-case margin is currently negative or positive. We discuss this in detail in Appendix B.

5.3.3 Alternative chains and H-improving. It is easy to see that (1) condition (iv) of the forks is not violated if instead of a chain \( C \) non-worse chains \( C' \) are delivered after \( \Delta_{\text{sync}} \) slots and (2) Praos is an H-improving environment for \( F_{\text{sync}} \).

5.4 Multi-Epoch Praos

There are two approaches to running Praos with \( F_{\text{sync}} \) in a multi-epoch setting with an evolving state distribution: (a) use a different instance of \( F_{\text{sync}} \) in every epoch or (b) define a version of \( F_{\text{sync}} \) that allows for changing state distributions.

The conceptually simpler approach is, of course, (a). The idea is to, \( \Delta_{\text{init}} \) before the end of each epoch, begin a new instance of \( F_{\text{sync}} \). At that point, the master index (including the network directory, the state distribution, and the randomness) to be used in the new epoch is determined. Taking approach (a) would mean that the random overlay is completely re-sampled for each new epoch. In practice, this may constitute an unacceptable overhead. Using approach (b) avoids this issue, but makes the definition, realization, and proofs of \( F_{\text{sync}} \) somewhat more cumbersome.

Observe that in either case it is important to properly deal with honest parties that have been eclipsed for more than an epoch. The issue with these parties is that once they have been eclipsed long enough for their master index to be out of date, they will face difficulties ever reconnecting to the network since the choice of neighbors via the VRF is based on an up-to-date state distribution.

While in practice such a scenario is unlikely to occur due to the evolving nature of the random-graph overlay, in theory the adaptive attacker can keep corrupting a party’s neighbors until it exhausts its corruption budget, thereby keeping it eclipsed for a long period of time. This issue can be mitigated by assuming a checkpointing functionality (realized, e.g., via some light-client infrastructure) that supplies parties, sufficiently in advance of an epoch’s beginning, with the relevant master index.

6 ACKNOWLEDGEMENTS

Cristopher Moore was partially supported by National Science Foundation grant 1838251. Alexander Russell was partially supported by National Science Foundation grant 1801487.

REFERENCES


Note that there are implementations of the network layer in which the connections to peers are unidirectional. In such cases, it is possible that due to an eclipse event (a) occurs but (b) does not (or vice versa).

15Of course, parameters such as epoch length, common prefix, etc. need to be suitably chosen for this to be the case.
A EXPANDERS RESILIENT AGAINST VERTEX DELETION

We consider the following family of distributions of random directed graphs.

Definition A.1 (Restatement of Definition 4.1.). Let \( \bar{d} \) and \( n \) be positive integers and let \( D \) be a probability distribution on \([n]\) with the property that \( d_v = \bar{d} D(v) \) is an integer for every vertex \( v \). We let \( \mathcal{G}_{n,\bar{d},D} \) denote the probability law on directed multigraphs with \( V = [n] \) obtained by selecting, for each \( v \), outgoing neighbors \( w_1, \ldots, w_{d_v} \) independently according to \( D \) and defining the multiset of directed edges to be \( E = \bigcup_{i=1}^{d_v} (v, w_i) \). In our main application, we are actually interested in the properties of the undirected version of such graphs; however, for analytic purposes it is convenient to distinguish the source and sinks for each edge.

In the definition above, we let \( \mathcal{G}_{n,\bar{d}} \) denote the special case when \( D \) is the uniform distribution, in which case \( d_v = \bar{d} \) for all \( v \).

Notation warning. Note that \( \mathcal{G}_{n,\bar{d}} \) does not denote the random \( \bar{d} \)-regular graph as it often does in the literature. Rather, it is a directed graph where every vertex has out-degree \( \bar{d} \) and in-degree \( \bar{d} \) distributed as Bin(\( \bar{d} n \), 1/\( n \)).

We wish to show that \( \mathcal{G}_{n,\bar{d}} \) is typically a “stake expander”; that is, that sets \( S \subset V \) have a number of neighbors outside them, or edges leaving them, proportional to their total stake.

Definition A.2 (Restatement of Definition 4.2.). Let \( G = (V, E) \) be a directed graph. For a subset \( S \subset V \), we define the (outer) boundary of \( S \) as

\[
\partial(S) = \{ w \not\in S \mid \exists s \in S : (s, w) \in E \text{ or } (w, s) \in E \}.
\]

Let \( D \) be a distribution on the set \( V \) and \( \gamma > 0 \). We say that \( G \) is a \((D, \gamma)\)-expander if for every subset of vertices \( S \subset V \) for which \( D(S) \leq 1/2 \),

\[
D(\partial(S)) \geq \gamma D(S),
\]

where we use the notation \( D(S) \) to denote \( \sum_{s \in S} D(s) \). When \( D \) is the uniform distribution, we say that \( G \) is an \( \gamma \)-expander.

Proposition A.3 (Diameter bound for stake expanders.). Let \( G = (V, E) \) be a \( \gamma \)-stake expander with (stake) distribution \( D \). Let \( m = \min_{v \in V} D(v) \) be the minimum stake of any vertex in \( G \). Let \( \mathcal{T} \) be the undirected counterpart of \( G \), obtained by replacing each directed edge with an undirected edge. Writing \( m = c/n \), where \( n = |V| \), the diameter of \( \mathcal{T} \) is no more than \( 2 \log_{1+c}(2n/m) \).

Proof. Consider two vertices \( u \) and \( v \) of \( G \). Note that the total stake reachable from \( u \) by paths of length \( k \) is at least \((1+c)^k D(v) \geq (1 + \gamma)^k \) if \( k \geq \log_{1+c} (1/\gamma) \). The same can be said of the vertex \( v \). Composing these two paths (and reversing the directions of arrows on the second) yields a path of length \( 2 \log_{1+c}(2n/m) \), as desired. \( \square \)

Theorem A.4 (Restatement of Theorem 4.3.). Let \( \alpha > \beta > 0 \) and \( \delta > 0 \) be positive constants, and let \( c \) and \( C \) be positive constants satisfying \( c < 1 < C \). For sufficiently large \( \bar{d} \) there is a constant \( \gamma > 0 \) for which the following holds. Let \( D \) be a distribution on \( V = [n] \) for which \( c/n \leq D(v) \leq C/n \) and \( d_v \leq D(v) \) is an integer for each \( v \in V \). Consider \( G = (V, E) \) drawn according to \( \mathcal{G}_{n,\bar{d},D} \). Then, except with probability \( \Pr_{\mathcal{G}_{n,\bar{d}}}(\cdot) \leq e^{-\delta n} \), for every subset \( H \subset V \) for which \( D(H) \geq \alpha \), there is a subset \( H' \subset H \) for which \( D(H') \geq \alpha - \beta \) and the subgraph induced by \( H' \) is a \((D', \gamma)\)-expander, where \( D' \) is the distribution \( D \) scaled by \( 1/D(H') \).

Remark. The condition in Definition 4.1 and Theorem 4.3 that \( \bar{d} D(v) \) is an integer for all \( v \) is a mere convenience so that the out-degree of each vertex will be a fixed integer \( d_v \). We can also define \( d_v = \lfloor \bar{d} D(v) \rfloor \). This changes the effective stake of each player by a factor of \( 1 + O(1/\bar{d}) \).

In fact we only need an upper bound on the stake each vertex has, if we are willing to hand over all the vertices with very low stake to the adversary:

Lemma A.5. Let \( c < 1 < C \) and let \( D \) be a distribution on \([n]\) such that \( D(v) \leq C/n \) for all \( v \). Then the fraction \( q \) of vertices \( v \) with \( c/n \leq D(v) \leq C/n \), is bounded below by

\[
q \geq \frac{1-c}{C-c}.
\]

It follows that the total probability mass associated with vertices \( v \) for which \( D(v) \leq c/n \) is no more than \( c(1-q) \leq c(C-1)/(C-c) \leq c \).

Proof. Otherwise, the total stake would be at most \( qC + (1-q)c < 1 \). \( \square \)

A.1 Mixing and expansion

The Expander Mixing Lemma is a classic result asserting that if \( G = (V, E) \) is a \( d \)-regular expander and \( S, T \subset V \) are sufficiently large disjoint sets, the number of edges between \( S \) and \( T \) is close to \( (d/|V|)|S| \cdot |T| \) (which can be interpreted as the expected value if the graph had been drawn randomly). This property is useful to us since it is inherited by any induced subgraph of \( G \), e.g., the subgraph \( H \) induced by the good players, albeit with modified parameters. As a partial converse, this mixing property implies expansion for sufficiently large sets, since we can take \( T \) to be the complement of \( S \).

Here we prove a mixing lemma for graphs in our model. The proof is a simple Chernoff bound with a union bound over all \( S \) and \( T \), and is essentially the same as for random \( d \)-regular graphs or sparse Erdős-Rényi graphs \( G_{n,p,d/n} \). For simplicity, we focus here on the uniform case \( \mathcal{G}_{n,\bar{d}} \) and then generalize to the stake-weighted case. We then use it to establish edge expansion and vertex expansion for sufficiently large sets.

Lemma A.6. Fix disjoint sets \( S, T \subset V \) of size \( |S| = \sigma n \) and \( |T| = \tau n \). Let \( G \in \mathcal{G}_{n,\bar{d}} \) and let \( E(S, T) \) denote the number of edges in either direction between \( S \) and \( T \). For any \( \kappa \leq 1 \),

\[
\Pr \left[ \left| \frac{E(S, T)}{2\sigma \tau n} - 1 \right| > \kappa \right] \leq \exp \left( -\frac{\kappa^2 \sigma \tau n}{3} \right).
\]

Proof. Recall that in \( \mathcal{G}_{n,\bar{d}} \) each vertex in \( S \) chooses \( \bar{d} \) outgoing neighbors uniformly and independently from the graph. Since each of these neighbors falls in \( T \) with probability \( |T|/n \), the number of directed edges from \( S \) to \( T \) is binomially distributed as Bin(\( \bar{d}|S| \cdot |T|/n \)). Similarly, the number of edges from \( T \) to \( S \) is distributed as Bin(\( \bar{d}|T| \cdot |S|/n \)). Since \( E(S, T) \) is the sum of these two random variables, both of which have expectation \( \bar{d}|S||T|/n = \bar{d}\sigma \tau n \),
the event $|E(S, T) - 2\sigma \tau n| > 2t$ implies that at least one of them deviates from its mean by $t$. A standard two-sided Chernoff bound for binomial variables $X$ with mean $\mu$ states that

$$\Pr[|X - \mu| > t] \leq e^{-\frac{t^2}{\mu}}$$

if $t \leq \mu$. Setting $t = \kappa \sigma \tau n$ and $\mu = \sigma \tau n$ completes the proof. \hfill \Box

**Lemma A.7.** Let $0 < \varepsilon < 1/2$, $\kappa > 0$, and $\delta > 0$. Then for sufficiently large $\delta$, with probability $1 - e^{-\delta n}$ in $G \in \mathcal{G}_{n, \frac{\varepsilon}{n}}$, for all pairs of disjoint sets $S, T \subseteq V$, if $|S| = \sigma n$ and $|T| = \tau n$ where $\varepsilon \leq \sigma, \tau \leq 1 - \varepsilon$, then

$$1 - \kappa \leq \frac{E(S, T)}{2\sigma \tau n} \leq 1 + \kappa.$$  \hfill (3)

**Proof.** We use Lemma A.6 and take the union bound over $S$ and $T$. The number of pairs of sets of size $\sigma n$ and $\tau n$, disjoint or not, is

$$\binom{n}{\sigma n} \binom{n}{\tau n} \leq \exp\left((h(\sigma) + h(\tau))n\right),$$

where $h(x) = -x \ln x - (1 - x) \ln(1 - x)$ is the entropy function. Comparing (1), we need to set $\delta$ such that

$$\frac{\kappa^2 \sigma \tau}{3} > \delta + h(\sigma) + h(\tau)$$

for all $\varepsilon < \sigma, \tau < 1 - \varepsilon$. Since $h(x) \leq \ln 2$, setting $\delta > \frac{3(\delta + 2 \ln 2)}{\kappa^2 \sigma \tau}$ suffices to beat the union bound over all pairs of sets $S, T$ for any fixed $\sigma, \tau$. Since the failure probability is exponentially small, it also easily covers the union bound easily covers all $O(n^3)$ possible values of $\sigma$ and $\tau$. \hfill \Box

**A.2 Inferring expansion of induced subgraphs**

Lemma A.7 implies that, with high probability in $G \in \mathcal{G}_{n, \frac{\varepsilon}{n}}$, any sufficiently large set is “edge expanding”, with a large number of edges connecting it to its complement. The same holds in any induced subgraph of $G$. Consider the following definition.

**Definition A.8.** For $\rho > 0$ and a multigraph $G = (V, E)$, we say a subset $S \subseteq V$ is $\rho$-edge-expanding if $E(S, V \setminus S) \geq \rho |S|$. We say $G$ is an $\rho$-edge-expander if all subsets $S \subseteq V$ with $|S| \leq |V|/2$ are $\rho$-edge-expanding.

Then Lemma A.7 states that in an induced subgraph of size $n'$, with high probability any set of size greater than $\varepsilon n$ is $\rho$-edge-expanding where

$$\rho = \frac{\varepsilon n}{\kappa} / n$$

where we took $|T| \geq n'/2$ and thus $\tau \geq n'/2n$ in (3).

Intuitively, a graph where the only non-expanding subsets are small is close to an expander. Here we show that we can obtain an expander simply by removing the largest non-expanding subset.

**Lemma A.9.** Let $G = (V, E)$ be an undirected multi-graph of maximum degree $\delta$. Let $\rho > 0$, and let $S \subseteq V$ be a subset of maximum cardinality such that $|S| \leq |V|/2$ and $S$ is non-$\rho$-edge-expanding. Assume that $|S| \leq \mu |V|$ where $\mu < \varepsilon /4$. Then the subgraph $G'$ induced by $V' = V \setminus S$ is an $\rho'$-edge-expander, where

$$\rho' = \rho - 4\delta \mu.$$  \hfill (4)

**Proof.** To the contrary, assume there is some subset $T \subseteq V'$ with $|T| \leq |V'|/2$ which is not $\rho'$-edge-expanding: that is, $E(T, V' \setminus T) < \rho'|T|$. There are two cases. If $|T| \leq (1/2 - \mu)|V|$ then $|S \cup T| \leq |V|/2$. However, this gives $E(S \cup T, V \setminus (S \cup T)) \leq E(S, V \setminus S) + E(T, V \setminus T) < \rho |S| + \rho' |T| \leq \rho |S \cup T|$.

Thus $|S \cup T|$ is non-$\rho$-edge-expanding in $V$, contradicting the maximality of $|S|$. In the other case, $|T| > (1/2 - \mu)|V|$ and $|S| \leq |T|/|V'|$. Then this implies $E(T, V \setminus T) = E(T, V' \setminus T) + E(S, T) \leq E(T, V' \setminus T) + \sigma |S| \leq E(T, V' \setminus T) + 4\delta \rho |T| \leq \rho |T|.$ Thus $T$ is non-$\rho$-expanding in $V$. But since $|S| \leq \mu |V| < |T| \leq |V'|/2$, this again contradicts the maximality of $|S|$. \hfill \Box

**Remark.** We have chosen to write Lemma A.9 as a purely graph-theoretic result with as few assumptions as possible. In our setting, however, we can be considerably less pessimistic. First, we assumed in (5) that $E(S, T)$ could be as large as $\bar{\delta}|S|$, but the upper bound of Lemma A.7 shows that this is almost certainly not the case. Second, just as Lemma A.7 implies that $|S|/|V|$ is bounded by a small constant $\mu$, the same holds for $|T|/|V'|$. Thus we can in fact exclude the second case where $|S \cup T| > |V|/2$ with high probability.

**A.3 From edge expansion to vertex expansion**

In order to bound the diameter of the subgraph induced by $H'$, we care more about vertex expansion—as in Definition 4.2—than about edge expansion. Even if a set $S$ is edge-expanding, if many vertices outside $S$ have large in-degree, then many of $S$’s outgoing edges could be incident to just a few vertices.

The next lemma shows that if $D(u) \leq C/n$ for all $u$ as in the statement of Theorem 4.3, then the set of vertices $u$ with in-degree more than $2\delta \bar{d}$, and thus total degree more than $d_u + 2\delta \bar{d} \leq 3\delta \bar{d}$, is almost always a small fraction of the graph. By condemning these vertices to spend eternity with the adversary, we are left with a subgraph where no vertex has degree greater than $3\delta \bar{d}$. If $S$ has $m$ edges connecting it to its complement in that subgraph, we have $\delta(S) \geq m/(3\delta \bar{d})$. Thus if that subgraph is an $\alpha$-edge-expander, it is also a $\gamma$-expander where $\gamma = \alpha/(3\delta \bar{d})$.

**Lemma A.10.** Let $\delta > 0$ and $\varepsilon > 0$ and assume that $D(v) \leq C/n$ for all $v$. Then for sufficiently large $\bar{d}$, with probability $1 - e^{-\delta n}$ in $G \in \mathcal{G}_{n, \frac{\varepsilon}{n}}$ at most vertices in in-degree greater than $2\bar{d}$.

**Proof.** Since the outgoing neighbors of each vertex in $\mathcal{G}_{n, \frac{\varepsilon}{n}}$ are chosen independently and the total out-degree is $\bar{d} n$, the in-degree of any given vertex $v$ is distributed as $\text{Bin}(\bar{d} n, D(v))$, which is stochastically dominated by $\text{Bin}(\bar{d} n, C/n)$. Using the Chernoff bound (2) with $t = \mu \leq \bar{d} \delta$, the probability this exceeds $2\bar{d} \delta$ is at most $e^{-\delta \bar{d}^2 / 3}$. Since the total in-degree is fixed, the number of such vertices is stochastically dominated by $\text{Bin}(n, e^{-\delta \bar{d}^2 / 3})$. Using
a crude union bound, the probability that there are more than \(en\) such vertices is at most
\[
\left( \frac{n}{en} \right)^{-(cA/3)en} \leq 2^n e^{-(cA/3)en},
\]
which is less than \(e^{-\delta n}\) whenever \(\tilde{d} > (3/eC)(\delta + \ln 2)\).

\[\square\]

**A.4 Proof of Theorem 4.3**

Now we put these pieces together.

**Proof of Theorem 4.3.** We begin wth the uniform case. Consider \(G \in G_{n,\tilde{d}}\) where \(c = C = 1\). Fix a subset \(H \subseteq V\) such that \(|H| \geq an\). Our task is to find a subset \(H'\) of \(H\) of size at least \((a - \beta)n\) whose induced subgraph is a \(\gamma\)-expander for some \(\gamma > 0\).

First, we remove from \(H\) the vertices whose in-degree exceeds \(2\tilde{d}\). Using Lemma A.10, with high probability there are at most \(en\) of these, and we set \(\tilde{d}\) large enough so that \(e = \beta/2\). Denote the remaining set of vertices \(H''\) and note that \(|H''| \geq (a - \beta)n\).

We now want to find a subset \(H' \subseteq H''\) whose induced subgraph is an edge expander and where \(|H'| \geq (a - \beta)n\). Lemma A.9 tells us that we can do that by removing the largest subset \(S\) of \(H''\) which is non-\(\rho\)-edge-expanding, as long as this set is of size at most \(\mu n\) where \(\mu \leq \beta/2\). In fact we set \(\mu = \beta/16\).

To bound the size of \(S\) we use the fact that \(H''\), like any induced subgraph of \(G\), inherits the mixing property of Lemma A.7. We set \(\tilde{d}\) large enough so that \(e = \mu = \beta/16\) and \(\kappa = 1/2\) in that lemma.

Then with high probability every set of size between \(en\) and \(|H''|/2\) is \(\rho\)-edge-expanding in \(H''\) where from (4)
\[\rho = (1 - \kappa)\tilde{d}|H''|/n \geq \tilde{d}(a - \beta)/2\).

Lemma A.9 then tells us that \(H' = H'' \setminus S\) is a \(\rho\)-edge-expander where
\[\rho' = \rho - 4\mu \tilde{d} \geq \tilde{d}(a - \beta)/2 - 4\mu \tilde{d}/4 = \tilde{d}(a - \beta)/2\).

Since the maximum total degree of any vertex in \(H''\) is at most \(3\tilde{d}\), \(H'\) is a \(\gamma\)-expander where
\[\gamma = \rho'/(3\tilde{d}) = (a - \beta)/6\.

Finally, we set \(\delta\) in both Lemmas A.7 and A.10 to be strictly larger than \(\delta + \ln 2\) where \(\delta\) is the desired parameter for \(p_{\text{fail}}\) in Theorem 4.3. Then the probability either of these lemmas fails is less than \(2^{-\delta n} e^{-\delta n}\). Finally, we take a union bound over all subsets \(H \subseteq V\) with \(|H| \geq an\), of which there are at most \(2^n\).

The nonuniform case of the theorem follows with minor alterations. Specifically, the mixing lemma follows because the number of independent random variables appearing in the Chernoff bounds there depend only on stake. The subgraph removal lemma translates immediately to a stake-weighted version and the remainder of the argument treats individual vertices. \[\square\]

**Remark.** Note that the expansion parameter \(\gamma\) stays constant as \(\tilde{d}\) increases, since the edge expansion parameter \(\alpha\) is proportional to \(\tilde{d}\).

**B. ANALYSIS OF NAKAMOTO CONSENSUS WITH ADVERSARIAL SUPPRESSED MESSAGES.**

Existing work on the analysis of Nakamoto consensus has focused on the setting of \(\Delta\)-synchrony, where all message broadcasts are delivered with adversarially determined delays of no more than \(\Delta\) time steps. In this section, we show how to analyze a setting where the adversary may entirely eliminate messages of his choice from the protocol. We remark that this axis of adversarial activity does not have the same hard threshold at \(1/2\): indeed, there are natural settings where Nakamoto consensus can survive even if a majority of honestly sent messages never arrive.

**B.1 The synchronous setting with message suppression.**

We adopt the framework of characteristic strings and margin, developed in [22], to study the behavior of the longest chain rule under message suppression. Specifically, the analysis divides time into equal length time slots. While these time slots can be chosen to be small enough so that the possibility of multiple proof-of-work successes in a single slot can be neglected, it is convenient for our analysis to permit multiple proof-of-work discoveries in each time slot. We refer to the set of parties that discover proofs-of-work in a particular time slot as the “leaders” of that slot.

In this setting where we wish to explore the effects of message suppression, we identify two properties of interest: \(\Delta\)-current leaders and \(\Delta\)-relayed leaders. In the context of a particular execution of the blockchain protocol these properties—which are only applied to honest parties—have the following meaning: If a party is \(\Delta\)-current at a particular time slot then she holds a chain at least as long as any chain broadcast by a \(\Delta\)-relayed party at time slot \(t - \Delta\) or earlier. If a party is both \(\Delta\)-current and \(\Delta\)-relayed, we say that it is \(\Delta\)-synchronized. When the network delay \(\Delta\) can be inferred from context, we simply say current, relayed, and synchronized. Intuitively, any block produced by a “relayed” leader is successfully transmitted to the network layer; likewise, any “current” leader is aware of all blocks recently transmitted to the network layer.

With any fixed execution, we may associate a characteristic string \(w_1 w_2 \ldots\) indicating certain properties of the sequence of parties elected to be slot leaders (and hence block producers). Specifically, each \(w_i\) is a symbol \(w_i \in \Sigma = \{A, C, R, \mathcal{Q}, \bot\}\). These symbols have the following interpretation:

- A indicates a slot with an adversarial leader, or with more than one leader;
- \(\mathcal{Q}\) indicates a slot with a synchronized leader;
- C indicates a slot with a current leader;
- R indicates a slot with a relayed leader;
- \(\bot\) indicates a slot with no leader.

When \(w_i \in \{\mathcal{Q}, C, R\}\), we say that the index (or, alternatively, “slot”) \(i\) is honest; we further distinguish honest indices according to which of these symbols actually arises: if \(w_i \neq C\), we say that the index is relayed; if \(w_i \neq R\), we say that the index is current; if an index is both current and relayed, we say that it is synchronized. If \(w_i = A\), we say that the index is adversarial.

We remark that this framework is “first order” modeling, in the sense that it simply treats any slot with multiple leaders as adversarial. Generalizing the model to handle more sophisticated
leadership patterns in a single slot is straightforward, but complicates the case analyses of the proofs below. Furthermore, for typical settings where slots are short with respect to network delays the major improvements in analysis arises from careful treatment of the leadership pattern across slots within Δ of each other (rather than careful treatment of the pattern in a single slot).

### B.2 Fork notation, closure.

We adopt the modeling infrastructure developed in [11, 22] for reasoning about the consistency and liveness of Nakamoto consensus algorithms. Specifically, the relevant state of a blockchain algorithm is reflected with the following graph-theoretic object, the Δ-fork.

**Definition B.1 (Δ-fork).** Let Δ be a positive integer and L ∈ N. A Δ-fork for the string w ∈ Σ^L is a directed, rooted tree F = (V, E) with a labeling

\[ ℓ : V \rightarrow \mathbb{N} \]

satisfying the axioms below. Edges are directed “away” from the root so that there is a unique directed path from the root to any vertex. The value \( ℓ(v) \) is referred to as the label of \( v \), and takes values in the set \( \{ i | w_i \neq Δ \} \cup \{ 0 \} \). We apply the same terminology to vertices as to the indices that label them; that is, the vertex \( v \) is respectively adversarial, honest, relayed, current, or synchronized if this is true of \( ℓ(v) \).

(i) the root \( r \in V \) has label \( ℓ(r) = 0 \) and is considered honest and relayed by fiat;
(ii) the sequence of labels \( ℓ() \) along any directed path is strictly increasing;
(iii) if \( w_i \in \{ \mathbb{R}, C, R \} \), there is a unique vertex \( v \) for which \( ℓ(v) = i \);
(iv) for any pair of vertices \( v, w \) for which \( v \) is relayed, \( w \) is current, and \( ℓ(v) + Δ \leq ℓ(w) \), their depths \( len(v) \) and \( len(w) \) satisfy \( len(v) < len(w) \).

We write \( F \vdash w \) to indicate that \( F \) is a Δ-fork for the string \( w \). When \( Δ = 1 \), corresponding to the synchronous case, we may just write \( F \vdash w \). If \( F' \vdash w' \) for a prefix \( w' \) of \( w \), we say that \( F' \) is a subfork of \( F \vdash w \), denoted \( F' \sqsubset F \), if \( F \) contains \( F' \) as a consistently-labeled subgraph. We remark that with any prefix \( w \) of \( w \) there is a unique maximal subfork \( F' \vdash w' \) of a given fork \( F \vdash w \) (given by all vertices labeled with the indices of \( w' \)).

**Tines.** A path in a fork \( F \) originating at the root is called a tine. (Note that tines do not necessarily terminate at a leaf.) For a vertex \( v \in F, F(v) \) denotes the tine in \( F \) terminating in \( v \). Given this one-to-one correspondence between vertices and tines of a fork, we routinely overload notation so that it applies to both tines and vertices. For example, we let \( len(T) \) denote the length of the tine \( T \), equal to the number of edges on the path; recall that \( len(v) \) also indicates the depth of the vertex \( v \). If we must identify the fork from which \( v \) is drawn, we sometimes write \( len_F(v) \). We further overload \( len() \) to apply to forks: \( len(F) \) denotes the length of the longest tine in a fork \( F \). A tine is called honest if it terminates in an honest vertex; we likewise apply the terms adversarial, current, relayed, and synchronized.

For two tines \( T, T' \) of a fork \( F \), we write \( T \sim \ell T' \) if the two tines share a vertex with a label greater or equal to \( \ell \). Intuitively, \( T \sim \ell T' \) guarantees that the respective blockchains agree on the state of the ledger up to time \( \ell \). Observe that \( \sim \ell \) is a "partial equivalence relation": it is symmetric and transitive, but not necessarily reflexive (for example, \( T \not\sim \ell T \) if this tine has no blocks appearing in slots \( \ell \) or larger). Looking ahead, the adversary can only make two parties disagree on the state of the ledger up to time \( \ell \) if she makes them hold two chains corresponding to tines for which \( T \not\sim \ell T' \).

**Fork trimming; dominance.** For a characteristic string \( w = w_1 . . . w_n \in \Sigma^* \) and a positive integer \( k \), we let \( w'_k = w_1 . . . w_{n-k+1} \) denote the string obtained by removing the last \( k - 1 \) symbols. When \( |w| < k \), \( w'_k = \epsilon \). For a fork \( F \vdash w_1 . . . w_n \) we let \( F |_k \vdash w'_k \) denote the fork obtained by retaining only those vertices labeled from the set \( \{ 0 \} \cup \{ 1, \ldots, n-k+1 \} \). Observe that relayed tines appearing in \( F |_n \) are those that are necessarily visible to current players at a round just beyond the last one described by the characteristic string. We say that a tine \( T \in F \) is \( Δ \)-dominant if \( len(T) \geq len(F |_\Delta) \) and simply call it dominant if \( Δ \) is clear from the context.

### B.3 Advantage, reach, and margin

We generally focus our analysis on forks that represent the view(s) of honest parties during the protocol. This places special emphasis on two properties defined next.

**Definition B.2 (Honest and relayed forks and subforks).**

- We say that a fork \( F \) is honest if every leaf is honest. In general, the honest subfork of a fork \( F \) is the maximal honest subfork of \( F \).
- We say that a fork \( F \) is relayed if every leaf is relayed. The relayed subfork of a fork \( F \) is the maximal relayed subfork of \( F \). We let \( T \) denote the relayed subfork of the fork \( F \).

For a Δ-fork \( F \vdash w \), we define the advantage of a tine \( T \in F \) as

\[ α_F(T) = len(T) - len(F |_\Delta) \]

When \( F \) can be inferred from context, we remove the subscripts. Observe that \( α_F(T) \geq 0 \) if and only if \( T \) is \( Δ \)-dominant in \( F \).

We pause to remark that our treatment differs somewhat from that developed in [22]. They consider a notion of "reserve" for a tine, which intuitively adds to that tine’s advantage any yet unused adversarial slots; with this addition, the analysis can focus entirely on honest subforks forks (which are called closed forks in [22]). In our current setting this mechanism is less convenient due to the more complicated role played by the various classes of honest parties. We thus opt for a treatment that considers arbitrary forks, rather than honest subforks—this somewhat complicates the analysis, but permits us to work with a simpler notion of advantage.

For \( ℓ \geq 1 \), we define two quantities of interest

\[ \rho(F) = \max_T α_F(T), \]

\[ μ_F^α(T) = \min_{T \geq T'} \alpha_F(T'), \]

this maximum extended over all pairs of tines \( (T, T') \) for which \( T \not\sim \ell T' \). Note that there might exist multiple such pairs in \( F \), but under the condition \( ℓ \geq 1 \) there will always exist at least one such pair, as the trivial tine \( T_0 \) containing only the root vertex satisfies \( T_0 \sim \ell T_0 \) for any \( T \) and \( ℓ \geq 1 \); in particular \( T_0 \sim \ell T_0 \). For this reason, we will always consider \( μ_F^α \) only for \( ℓ \geq 1 \). Intuitively, \( α_F^\Delta(T) \) captures the length advantage (or deficit) of the tine \( T \) against
the longest relayed time created at least Δ slots before the upcoming slot, and hence known to all current parties. Consequently, \( \mu_B^T(F) \) records the maximal advantage of any pair of times \( F \) that agree only prior to \( \ell \), where “advantage” in this setting is treated as the minimum of the two times.

The quantity \( \rho(F) \) is the reach of \( F \); the quantity \( \mu(F) \) is the margin of \( F \). We say that a time \( T^* \) is a witness for the reach \( \rho(F) \) when it achieves the maximum of definition (6); we use the same terminology for margin: a pair of times \( T \) and \( T' \) witness the margin \( \mu(F) \) if they achieve the maximum of the definition (7).

We remark that one may always choose a pair of times \((T,T')\) that witness \( \mu(F) \) for which one is, additionally, a witness for reach. To see this, consider any witness \( T^* \) of \( \rho(F) \) and a pair \((T,T')\) that witness \( \mu(F) \); as \( T \) \( \not\equiv \) \( T' \), we must have either \( T^* \not\equiv \ell \) \( T \) or \( T^* \not\equiv \ell \) \( T' \) and hence \( T^* \) can replace one of these without reducing the margin quantity.

We overload the notation and let
\[
\mu_{\ell}^A(w) = \max_{w \cap T^*} \mu_{\ell}^A(F).
\]
We again emphasize the difference between this approach and that of \([22]\), which maximizes only over honest forks.

The crucial property motivating these definitions is that \( \mu_{\ell}^A() \) provides explicit control over consistency failure events. This is reflected in the lemma below, which follows directly from the analogous formulation and proof in \([3, 16]\).

**Lemma B.3.** Consider the sequence of forks \( F_1 \uplus w_1, F_2 \uplus w_2, \ldots \) associated with each step of an execution corresponding to a characteristic string \( w = w_1 w_2 \ldots \). Consider a time \( T \) held by a current honest party in round \( s \), which is hence \( \Delta \)-dominant in \( F_s \); let \( \ell \) be a round associated with a vertex (block) \( B \) that appears on \( T \). If \( \mu_{\ell}(w) \) \( \leqslant 0 \) for every \( r \) \( \leqslant s \leqslant t \) then any \( \Delta \)-dominant time \( T^* \) of \( F_t \) contains the vertex \( B \).

Thus, in order to rule out consistency violations it suffices to establish that \( \mu_{\ell}^A(w) < 0 \) for appropriate \( s \) and \( \mu_{\ell}(w_{r+1}) \) (note that this bounds above \( \mu_{\ell}^A(F) \) for any relevant fork). Similar connections were originally established for PoS forks \([22]\) with guaranteed network delivery.

### B.4 An exact analysis in the serialized, synchronous setting.

We begin with an analysis of the quantity \( \mu_{\ell}^A(w) \) in the synchronous setting, corresponding to the case where \( \Delta = 0 \) and block creation is strictly serialized. In this synchronous case we abbreviate \( \alpha_T^f() \) by \( \alpha_T^f \) (and note that \( \alpha_T(T) = \text{len}(T) - \text{len}(\overline{T}) \)). We similarly abbreviate \( \mu_{\ell}^A \) by \( \mu_{\ell} \). In preparation for the statement of the theorem below, one final definition: we say that a characteristic string is silent if it contains no relayed symbols, and relayed otherwise.

**Theorem B.4.** Fix \( \ell \geq 1 \). By definition \( \mu_{\ell}(\epsilon) = \mu_{\ell}(\epsilon) = 0 \). In general,
\[
\rho(wA) = \rho(w) + 1 ,
\rho(wR) = \begin{cases} 
\max(\rho(w) - 1, 0) & \text{if } w \text{ is silent,} \\
\rho(w) & \text{otherwise,}
\end{cases} \\
\rho(wC) \leq \rho(w) + 1 ,
\rho(w\overline{Q}) = \max(0, \rho(w) - 1),
\]
and, turning to margin: \( \mu_{\ell}(w) = \rho(w) \) for \( |w| < \ell \), and, for \( |w| \geq \ell \),
\[
\mu_{\ell}(wA) = \mu_{\ell}(w) + 1 ,
\mu_{\ell}(wR) = \begin{cases} 
\mu_{\ell}(w) + 1 & \text{if } \mu_{\ell}(w) < 0 , \\
\mu_{\ell}(w) & \text{otherwise,}
\end{cases} \\
\mu_{\ell}(wC) = \begin{cases} 
\mu_{\ell}(w) - 1 & \text{if } \mu_{\ell}(w) \geq 0 \text{ and } w \text{ is relayed,} \\
\mu_{\ell}(w) & \text{if } \mu_{\ell}(w) \geq 0 \text{ and } w \text{ is silent,}
\end{cases} \\
\mu_{\ell}(w\overline{Q}) = \begin{cases} 
0 & \text{if } \rho(w) > 0 \text{ and } \mu_{\ell}(w) = 0 , \\
\mu_{\ell}(w) - 1 & \text{otherwise.}
\end{cases}
\]

The proof is presented as a sequence of lemmas, the first establishes the relationship between \( \rho \) and \( \mu_{\ell} \) when \( |x| < \ell \). The remaining lemmas handle each input symbol separately.

**Lemma B.5.** \( \rho(\epsilon) = 0 \) and, for any \( x \in \Sigma^* \) and \( |x| < \ell \), \( \mu_{\ell}(x) = \rho(x) \).

**Proof.** The only possible fork for the empty string \( \epsilon \) contains a single honest vertex; the only time in this fork has advantage zero; hence \( \rho(\epsilon) = 0 \).

Let \( F \uplus x \) be a fork for which \( \rho(F) = \rho(x) \); let \( T^* \) be a time witnessing \( \rho(F) \). Observe that \( T^* \not\equiv \ell \) \( T^* \) because \( \ell \not\equiv |x| \). Therefore, \( \mu_{\ell}(F) \geq \rho(x) \) by considering the pair \((T^*,T^*)\) as a witness for margin. As \( \mu_{\ell}(F) \) can clearly not exceed \( \rho(x) \), it follows that \( \mu_{\ell}(x) = \rho(x) \). \( \square \)

**Lemma B.6.** \( \forall w \in \Sigma^*, \rho(wA) = \rho(w) + 1 \). Additionally, \( \forall w \in \Sigma^*, \mu_{\ell}(wA) = \mu_{\ell}(w) + 1 \).

**Proof.** We first establish the bounds \( \rho(wA) \geq \rho(w) + 1 \) and \( \mu_{\ell}(wA) \geq \mu_{\ell}(w) + 1 \). Consider a fork \( F \uplus w \) and a pair of times, \( T \) and \( T^* \), for which \( \alpha(T^*) = \rho(F) \), \( \alpha(T) = \mu_{\ell}(F) \), and \( T \not\equiv \ell \) \( T^* \). We may construct a new fork \( F' \uplus \overline{w} \) from \( F \) by adding two new adversarial vertices, \( v \) and \( v^* \), both labeled with the index of the additional A symbol. Each of the two times \( T \) and \( T' \) of \( F \) are then extended by adding a directed edge to one of these vertices: \( T \) is extended by the vertex \( v \); \( T^* \) is extended by \( v^* \). Note that \( \overline{F} = \overline{F'} \). Then \( \alpha_{T'}(\text{ext}(\overline{F})) = \alpha_T(T') + 1 \) and \( \alpha_{T'}(\text{ext}(\overline{F})) = \alpha_T(T) + 1 \). Applying this transformation to a fork \( F \) for which \( \rho(F) = \rho(w) \) shows that \( \rho(wA) \geq \rho(w) + 1 \). Similarly, applying this transformation to a fork \( F \) for which \( \mu_{\ell}(F) = \mu_{\ell}(w) \) shows that \( \mu_{\ell}(wA) \geq \mu_{\ell}(w) + 1 \).

To complete the proof we establish the bounds \( \rho(F) \leq \rho(w) + 1 \) and \( \mu_{\ell}(F) \leq \mu_{\ell}(w) + 1 \). Consider a fork \( F \uplus w \) and a pair of times, \( T \) and \( T^* \), for which \( \alpha(T^*) = \rho(F) \), \( \alpha(T) = \mu_{\ell}(F) \), and \( T \not\equiv \ell \) \( T^* \). Let \( \text{res}(T) \uplus \text{res}(T^*) \) be the maximal subfork of \( F \) for the prefix \( w \) and let \( \text{res}(T) \) and \( \text{res}(T^*) \) the restrictions of \( T \) and \( T^* \) to \( F \). Observe that \( \text{res}(\overline{T} = \overline{F}) \). Furthermore, the times \( T \) and \( T' \), when restricted to \( F \), lose at most one vertex: thus \( \text{len}(\text{res}(T)) \geq \text{len}(T) - 1 \) and \( \text{len}(\text{res}(T^*)) \geq \text{len}(T^*) - 1 \). It follows that \( \rho(\text{res}(T) \geq \rho(F) - 1 \) and \( \mu_{\ell}(\text{res}(T)) \geq \mu_{\ell}(F) - 1 \). Applying this transformation to a fork \( F \) for which \( \rho(F) = \rho(wA) \) proves that \( \rho(wA) \geq \rho(F) - 1 \); similarly, applying this transformation to a fork \( F \) for which \( \mu_{\ell}(F) = \mu_{\ell}(wA) \) proves that \( \mu_{\ell}(wA) \geq \mu_{\ell}(F) - 1 \), as desired. \( \square \)
Consider a fork $F \vdash wR$ for which $\mu_F(w) = \mu_F(wR)$; let $T$ and $T^*$ be a pair of tines for which $a(T^*) = F$, and $a(T) = \mu_F(w)$. Let $v$ be the unique vertex labeled by the last symbol (R) and let res $F \vdash w$ be the fork obtained by removal of the vertex $v$. Observe that if $\mu_F(w) > 0$ the vertex $v$ cannot appear on either of the tines $T$ or $T^*$, as $\ell(F) < \ell(T) \leq \ell(T^*)$ (and $v$ is a leaf in the fork $F$).

Noting that the removal of $v$ can only reduce the length of $\text{res} F$, and that the two tines $T$ and $T^*$ appear in res $F$, we conclude that $\mu_F(w) \geq \mu_F(\text{res} F) \geq \alpha_{\text{res} F}(T) \geq \alpha_T(T)$. Observe, moreover, that if $w$ is silent then $\ell(\text{res} F) = 0$ and $\ell(F) > 0$; thus $\alpha_{\text{res} F}(T) \geq \alpha_T(T) + 1$. This establishes (12). We proceed to the last case (13), in which we again consider the construction $\text{res} F \vdash w$ above with the same notation. In this case, however, there is no guarantee that the leaf node $v$ (labeled with the index of the last symbol (R)) does not appear on one of the two times of interest, $T$ and $T^*$. We let res $T$ denote the result of removing the vertex $v$ from $T$, so that res $T = T$ if $v$ does not appear on $T$, and res $T$ is the resulting prefix of $T$ otherwise; we adopt the same notation res $T^*$ for the time $T^*$. Thus, res $T$ and res $T^*$ are times of res $F$. Clearly, the lengths of $T$ and $T^*$ can differ from their restricted counterparts res $T$ and res $T^*$ by no more than one and

$$\min(\text{len}_{\text{res} F}(\text{res} T^*), \text{len}_{\text{res} F}(\text{res} T)) \geq \min(\text{len}_{\text{res} F}(\text{res} T^*), \text{len}_{\text{res} F}(T)) - 1.$$ 

Noting, as above, that $\text{len}(\text{res} F) \leq \ell(F)$, we conclude that $\mu_F(w) \geq \mu_F(\text{res} F) \geq \mu_F(F) - 1$, as desired.

**Lemma B.8 (C).** For any $w \in \Sigma^*$, $\rho(wC) = \rho(w) + 1$. Additionally, for any $w \in \Sigma^*$, with $\ell \leq |w|$, 

$$\mu_F(w) \leq \mu_F(w) + 1, \quad \text{if } \mu_F(w) \geq 0,$$ 

$$\mu_F(w) = \mu_F(w) + 1, \quad \text{if } \mu_F(w) < 0.$$ 

**Proof.** Note that if $F \vdash wC$ then $F \vdash wA$ and it follows that $\rho(wC) \leq \rho(wA) \leq \rho(w) + 1$ by Lemma B.6. To establish $\rho(wC) = \rho(w) + 1$, consider a fork $F \vdash w$ and a tine $T$ that witnesses $\rho(w)$. Construct the fork $\text{ext} F \vdash wC$ by adding a new vertex $v$ to the end of the tine $T$ labeled with the additional symbol (C). This is a legal fork for which $\text{len}(\text{ext} F) = \ell(F)$ as the new vertex in ext $F$ is not relayed. As $\ell(v) = \ell(T) + 1$, we conclude that $\rho(wC) = \rho(\text{ext} F) = \rho(w) + 1$.

To establish inequality (14) consider a fork $F \vdash w$ for which $\mu_F(w) = \mu_F(w)$ and define ext $F \vdash wC$ to be the fork obtained from $F$ by adding a single vertex $v$ labeled by the index of the new symbol (C), so that it extends the longest time of $F$. As the new vertex is not relayed, $\text{len}(\text{ext} F) = \ell(F)$ and it follows that $\mu_F(\text{ext} F) \geq \mu_F(F)$, considering that any pair of tines in $F$ exist in ext $F$. Thus $\mu_F(w) \geq \mu_F(\text{ext} F)$, as desired.
We observe that the case when

\( T \neq \star \)

...it is both left and right isolated. Then consider the transformation

\( \perp \to \perp \)

\( A \to A \)

\( C \to \begin{cases} C & \text{if left isolated,} \\ A & \text{otherwise,} \end{cases} \)

\( R \to \begin{cases} R & \text{if right isolated,} \\ A & \text{otherwise,} \end{cases} \)

\( G_R \to \begin{cases} G_R & \text{if doubly isolated,} \\ R & \text{if right isolated,} \\ C & \text{if left isolated,} \\ A & \text{if not isolated on either side.} \end{cases} \)

It is straightforward to check that any \( \Delta \)-fork for a characteristic string \( w \) is also a 1-fork for the characteristic string \( T(w) \). This reduces the study of \( \Delta \)-forks to the synchronous case as in [11].

\textbf{B.6 The asymptotics}

Finally, we consider the distribution placed on characteristic strings corresponding to the executions of interest: each symbol is i.i.d. with distribution of the form

\[
\begin{align*}
p_R &= \Pr[w_i = R] = p_h \cdot \Pr[\text{send}(1 - \Pr[\text{receive}]), \\
p_C &= \Pr[w_i = C] = p_h \cdot (1 - \Pr[\text{send}]\Pr[\text{receive}] \\
p_{G_R} &= \Pr[w_i = G] = p_h \cdot \Pr[\text{send}]\Pr[\text{receive}] \\
p_\perp &= \Pr[w_i = \perp] = (1 - p_a)(1 - p_h) \\
p_A &= \Pr[w_i = A] = 1 - p_\perp - p_R - p_C - p_{G_R},
\end{align*}
\]

where \( p_h \) is the probability that a slot has an honest slot leader, \( p_h \) is the probability that a slot has a unique honest slot leader, \( p_a \) is the probability that a slot has an adversarial slot leader, \( p_{\text{send}} \) is the probability that a block sent from a stake-weighted random honest party is received by the backbone in \( \Delta \) time, and \( p_{\text{receive}} \) is the probability that a block known to a member of the backbone is received by a stake-weighted random honest party in \( \Delta \) time.

Then the final probabilistic bounds on margin with this distribution follow directly from the analysis of [21], yielding the following consistency result.

\textbf{Lemma B.9.} Let \( w = w_1, \ldots, w_n \) be chosen according to the distribution above with the added assumption that \( p_a < p_{G_R} \). Then for any \( \ell \) and \( k \) for which \( \ell + k \leq n \), \( \Pr[\mu_T(w) \geq 0] \geq \exp(-O(k)) \).