The Longest-Chain Protocol Under Random Delays

Suryanarayana Sankagiri, Shreyas Gandlur*, Bruce Hajek

ECE Department, University of Illinois, Urbana-Champaign

*currently at Princeton

1. Introduction

1.1 Background

Blockchains
- Bitcoin, other cryptocurrencies are blockchain systems
- Longest-chain protocol: method to update blockchains
- Governed by a randomized leader election mechanism
- Leaders arrive as a Poisson process of rate \( \lambda \)
- Each leader creates a new block, broadcasts it to all other peers
- Peers adopt the longest chain heard so far

Factors Affecting Security
- Adversarial peers as well as communication delays can create forks, imply loss of consensus among peers
- Forks with conflicting transactions: security violation!
- Higher fraction of adversarial peers and larger delays \( \rightarrow \) increase forking
- Heuristic: confirm blocks were created \( k \) time units ago
- Intuition: Latency allows random factors to settle

Prior Work

Figure 1. Maximum tolerable adversarial fraction as a function of \( \Delta \) from [2]

\( f^* : \) mining rate, \( \Delta : \) delay

Many papers with formal security analysis, e.g., [1]
Synchronous assumption: all messages delayed by \( \Delta \)

Figure 2. Upper and lower bounds on settlement failure probabilities for Ethereum for fixed \( \beta, f, \Delta \) from [3]

Communication Model
Every message suffers a random delay \( \Delta \)
- I.I.D. delays for each message
- \( \Delta \) dominated by exponential distribution
- Adversary suffers no delay, can deliver messages ahead of time

Novel Tools for Random Delays
Special Honest Blocks.
A sequence of blocks that hear of each other \( \rightarrow \) successive blocks are at increasing heights

\( P( \text{block is special honest | past} ) \geq \alpha P( \Delta \in G) \)
\( \alpha: \) honest fraction, \( G: \) gap between blocks

Figure 3. Comparing the security threshold obtained from our work versus prior work, in a network with random, exponentially distributed delays. Different cut-offs for max delay shown.

Security Analysis Under Random Delays

Main Result

Security Requirements. Given a set of honest peers \( \mathcal{H} \) and latency parameter \( k \),
- every honest peer \( h \in \mathcal{H} \) incorporates at least one honest block every \( k \) time units,
- every pair of honest users \( h_1, h_2 \in \mathcal{H} \) must have in common all blocks, except possibly the blocks mined in the last \( k \) time units

Theorem. Suppose each new block is special honest with prob. \( \frac{1}{2} + \epsilon \). Then, for a fixed \( k \) and \( \mathcal{H} \), the security requirements are violated with probability at most

\[
4 \exp\left(-\frac{3}{32} \epsilon^2 f k \right) + \frac{\epsilon^2}{\epsilon} \exp\left(-\frac{1}{32} \epsilon f k \right)
\]

2. Main Result

Step 1. Obtain a necessary event for security breach

\[
\exists t: N_{\text{adv}}[t] - (N_{\text{sp1}}[t] - \text{Unheard}_h[t]) \geq 0
\]

A security violation event

- \( N_{\text{adv}}[t] \): number of adversarial blocks
- \( N_{\text{sp}}[t] \): number of special honest blocks
- \( \text{Unheard}_h[t] \): number of unheard blocks by peer \( h \)

Step 2. Bound the probability of insecure event

- \( N_{\text{adv}}[t] - N_{\text{sp}}[t] \leq \text{simple random walk with negative drift} \)
- under appropriate bound on adv. fraction
- With high prob., \( N_{\text{adv}}[t] - N_{\text{sp}}[t] < -y \)
- forever after \( t \geq k \), for \( y \) small enough

- \( \text{Unheard}_h[t] \): geometric rand. variable
- With high prob., \( \text{Unheard}_h[t] < y \)
- forever after \( t \geq k \), for any \( y \)
- \( N_{\text{adv}}[t] - (N_{\text{sp}}[t] - \text{Unheard}_h[t]) < 0 \)
- forever after \( t \geq k \), with high prob.

3. Discussion

Gap in the Literature
- Many factors that can cause random communication delays, e.g., message size, P2P network topology, noise and packet drops.
- Maximum possible delay can be much greater than typical delay
- In such a scenario, the analysis under the synchronous model yields poor security guarantees as well as poor throughput.

Key Takeaway
- We show that the security guarantees depend on the probability of atypically large delay, rather than the worst-case delay itself.
- The protocol has an inherent robustness to sporadic large delays.

References

This work: The Longest-Chain Protocol Under Random Delays. arXiv:2102.00973

Directions for Future Work
- A more accurate analysis of the growth process of honest blocks
- Tighter security bounds, extending the analysis of [2] and [3]
- Analysis of other consensus protocols (PBFT) under random delays