Solana: High-Performance Blockchain

A Technical Exploration into Solana’s Architecture

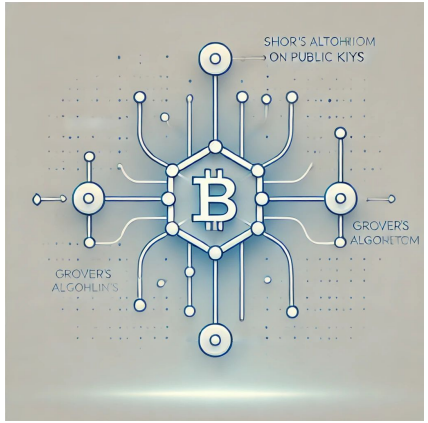
Pooya Sharifi

Agenda

1. Weaknesses of Classic Blockchains
2. Solana’s Architecture
   - Proof of History (PoH)
   - Proof of Stake (PoS) Consensus
   - High-Performance Design
3. How Solana Blockchain Works – Real-World Example
4. Solana’s Adaptability to Quantum Threats
5. Conclusion and Discussion

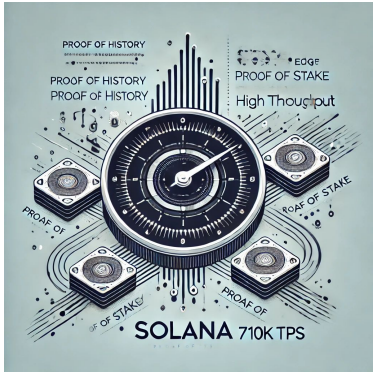
Weaknesses of Classic Blockchains

- Low Scalability
- High Energy Consumption
- Vulnerabilities to Quantum Attacks
- Slow Transaction Finality



Solana – Introduction and Goals

- Goal: High throughput, low fees, scalability
- Technical Edge:
  - Proof of History (PoH): Cryptographic clock
  - Proof of Stake (PoS): Consensus
- Why Solana? Over 710K TPS achievable on modern networks



Network Design

- Components:
  - Leader: Generates PoH sequence
  - Verifiers: Confirm state and validate blocks
- Flow: Leader → PoH → Verifiers → Finality
- CAP Theorem: Consistency prioritized

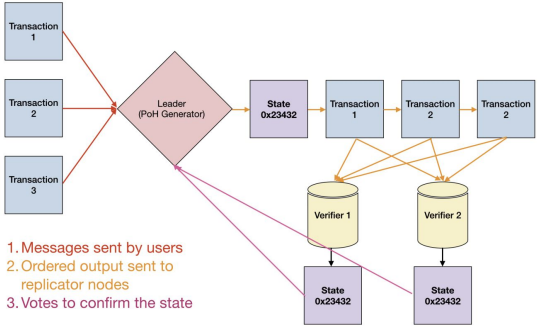


Figure 1: Transaction flow throughout the network.

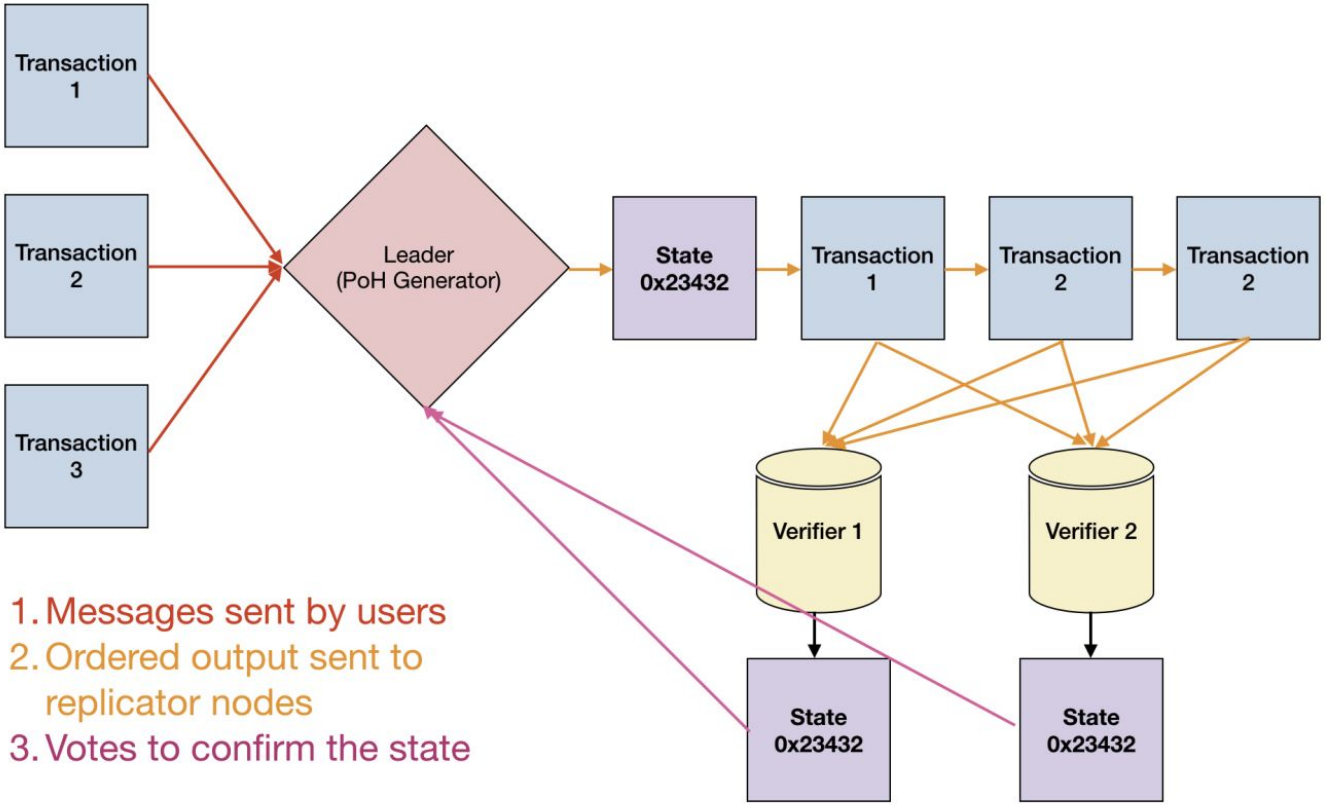
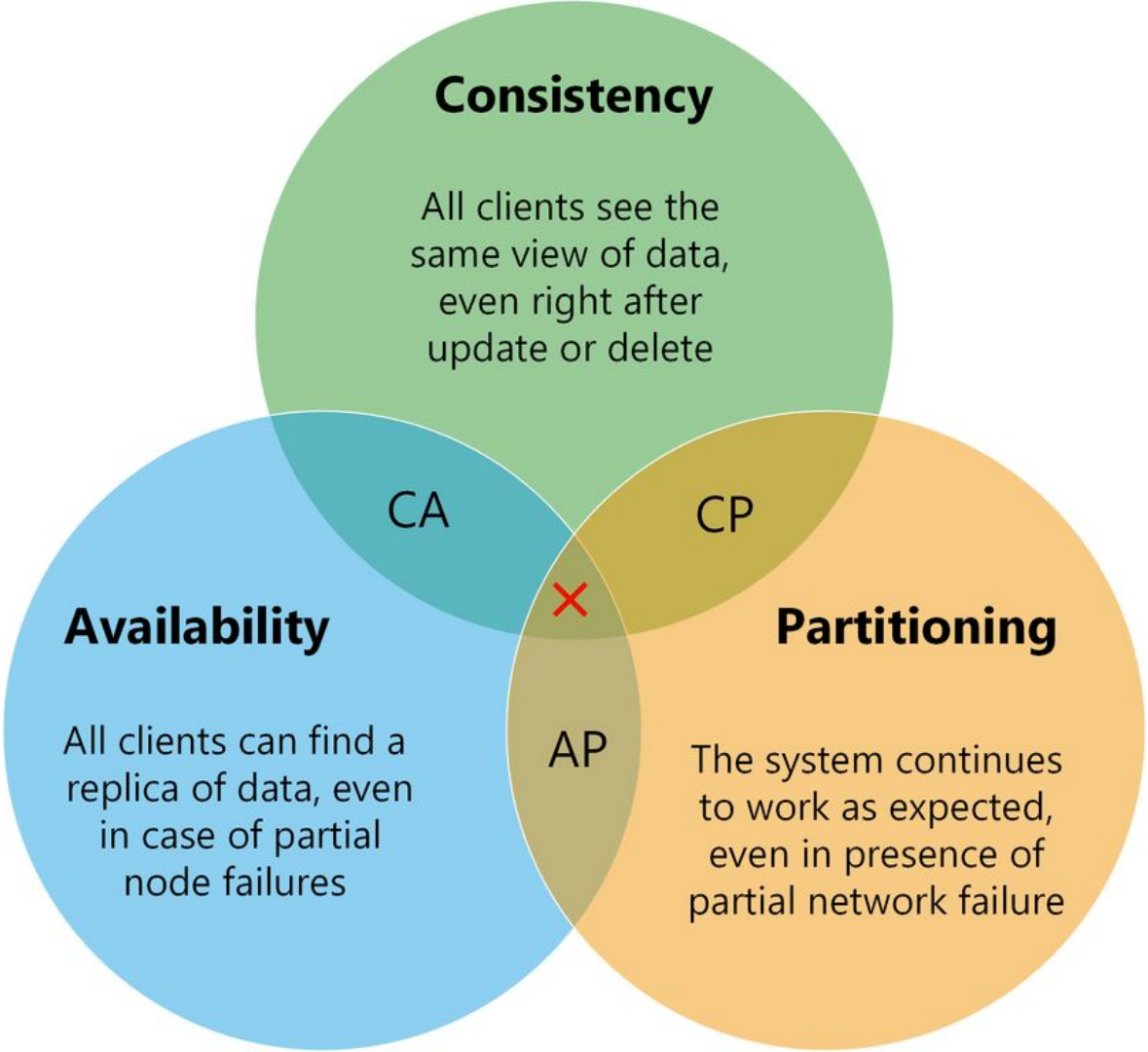


Figure 1: Transaction flow throughout the network.


Consistency
All clients see the same view of data, even right after update or delete
CA
CP
Availability
All clients can find a replica of data, even in case of partial node failures
AP
Partitioning
The system continues to work as expected, even in presence of partial network failure

Proof of History (PoH)

- Problem: Time-ordering without messaging overhead
- Solution:
  - Sequential hash chain (SHA-256)
  - Events added at intervals: Guaranteed order
- Verification: Parallelizable using GPUs

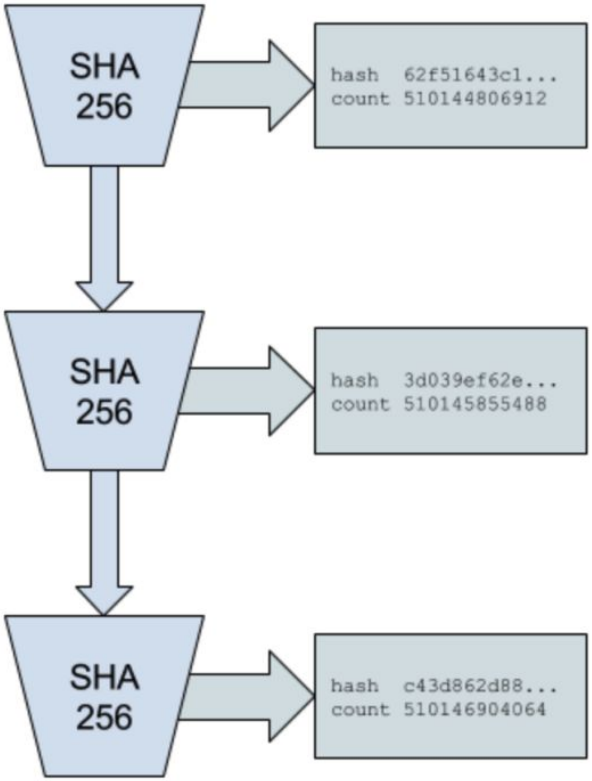


Figure 2: Proof of History sequence

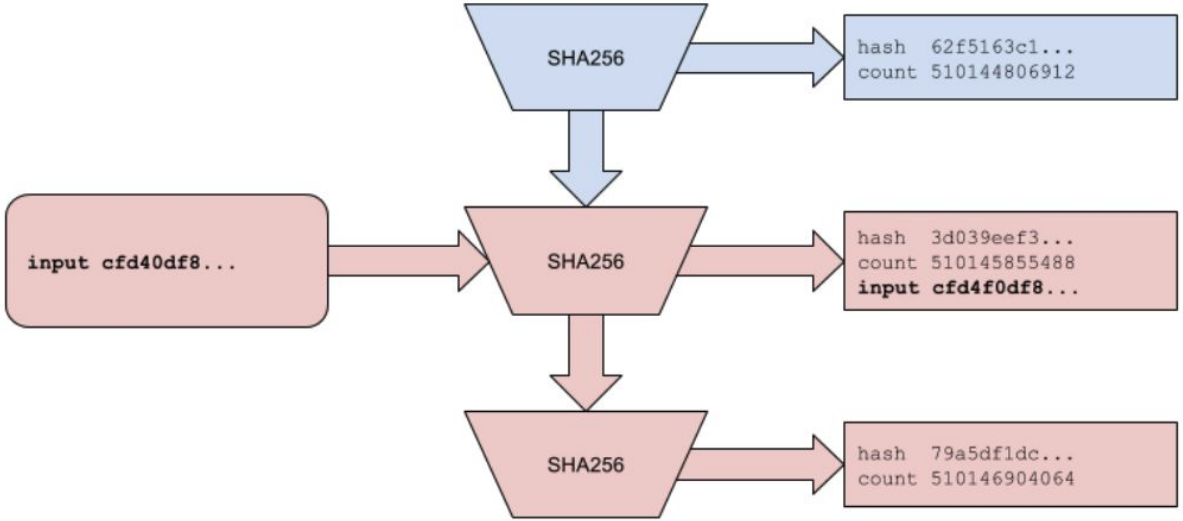


Figure 3: Inserting data into Proof of History

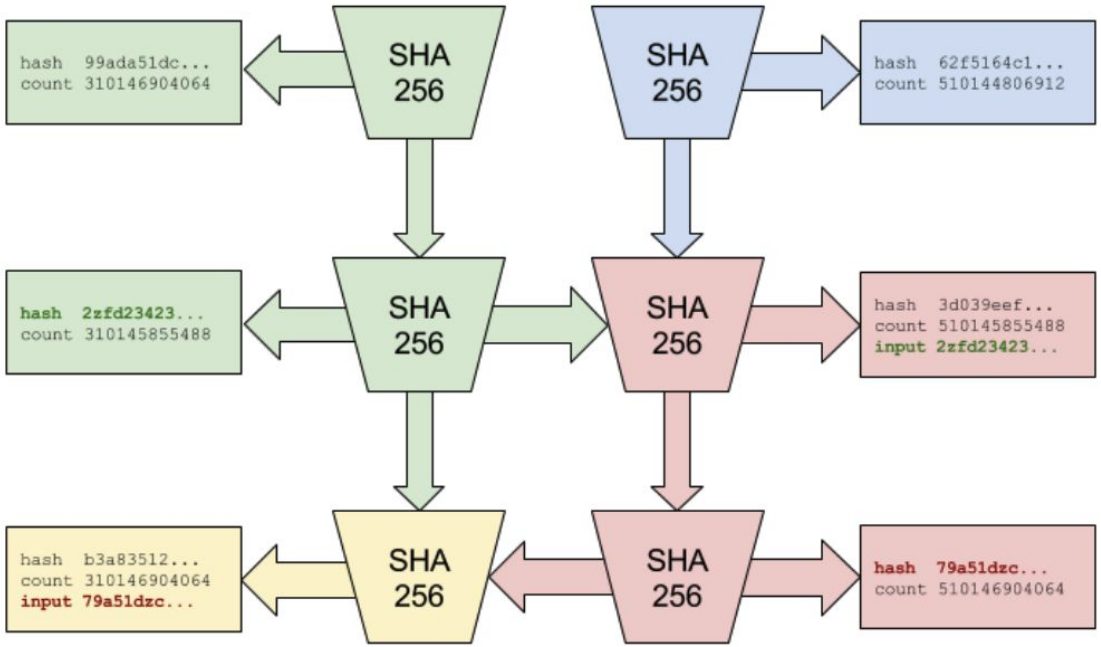


Figure 5: Two generators synchronizing

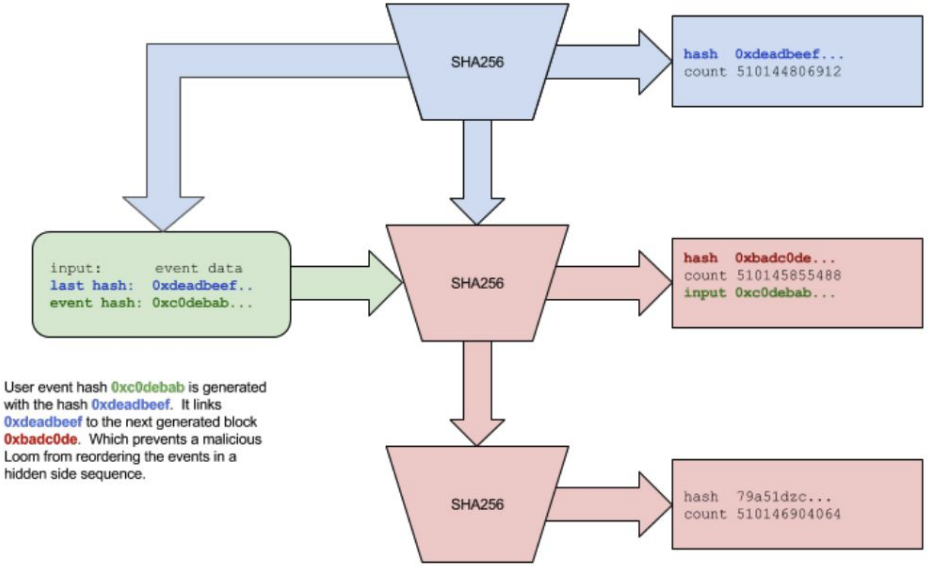


Figure 6: Input with a back reference.

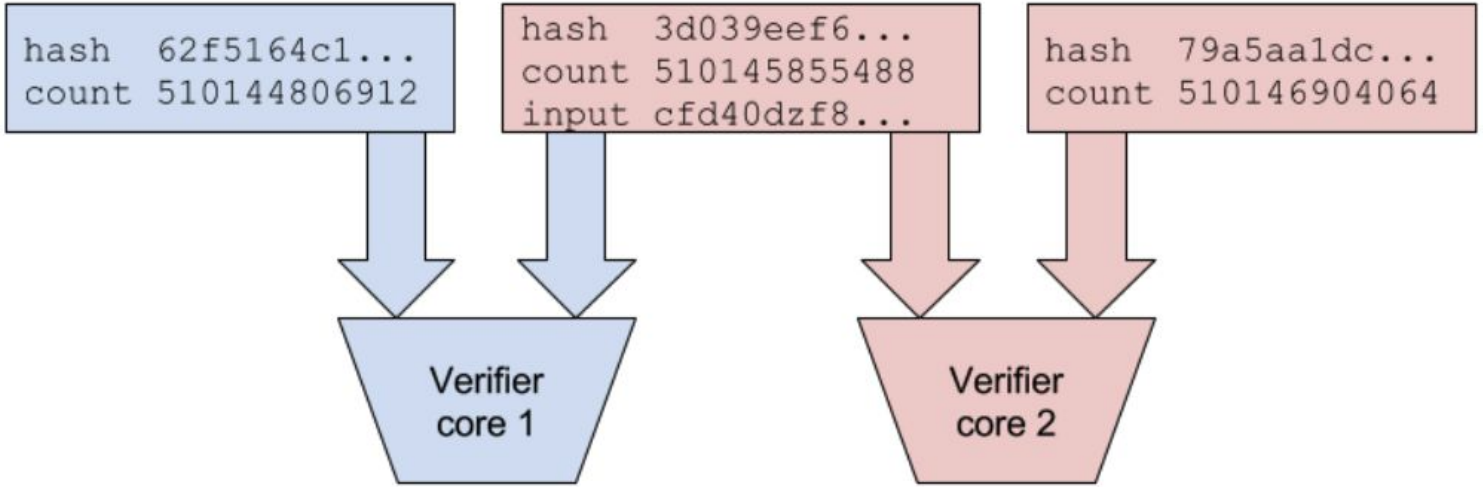


Figure 4: Verification using multiple cores

$$\frac{\text{Total number of hashes}}{\text{Hashes per second for 1 core}}$$

The expected time to verify that the sequence is correct is going to be:

$$\frac{\text{Total number of hashes}}{(\text{Hashes per second per core} * \text{Number of cores available to verify})}$$

Proof of Stake Consensus

- PoS Details:
  - Validators stake tokens
  - Supermajority (⅔) finalizes state
- Slashing Mechanism: Punishes malicious validators
- Finality in ~500 ms: Sub-second confirmation

High-Performance Features

- 710K transactions/second with 1 Gbps network
- GPU-based parallel ECDSA verification (~900K/s)
- Memory-efficient state storage: 10B accounts on 640GB RAM

How Solana Blockchain Works – Real-World Example

Inspect Live Data:
Use Solana Explorer to view live blocks and transactions.
Example Block:

- **Slot**: 223,456,789
- **Transactions**: 1,234 processed in 400ms

Key Highlights:

- Transactions are time-ordered with Proof of History (PoH).
- Fast validation using GPUs.
- Sub-second finality (~500ms).

Solana’s Quantum-Resilience Potential

It's not immediately obvious how PoH affects quantum's ability to break Solana. Do you mind elaborating?

4 Reply Award Share ···

[deleted] • 3y ago •

I suspect that a decently sized quantum computer could outperform the current calculation of the PoH chain.

I do not know whether this is really possible and if it were, would it be an attack vector.

Sorry for the vague answer, I just wanted to mention it bc I was thinking about it recently.

2 Reply Award Share ···

ZantetsuLastBlade2 • 3y ago •

PoH is based on iterative SHA-256. If loinj is correct about SHA-256 being quantum resistant, then PoH is as well.

Solana also uses ed25519 encryption, and when asked this question in Discord, the Solana devs stated pretty bluntly that they'd just swap the encryption algorithm out should it be necessary.

However, quantum attacks are basically science fiction and in my opinion, will be for a very, very, VERY long time.

4 Reply Award Share ···

[deleted] • 3y ago •

r/solana Join

Solana

Welcome to the official Solana subreddit. This is a place to post any information, news, or questions about the Solana...

Show more

Created Mar 27, 2018

Public

333K	198	Top 1%
Members	Online	Rank by size

COMMUNITY BOOKMARKS

Network Analysis

Staking Resources

Dev Community

Dev Resources

GET STARTED WITH SOLANA

It's not immediately obvious how PoH affects quantum's ability to break Solana. Do you mind elaborating?

4 Reply Award Share ···

[deleted] • 3y ago •

I suspect that a decently sized quantum computer could outperform the current calculation of the PoH chain.

I do not know whether this is really possible and if it were, would it be an attack vector.

Sorry for the vague answer, I just wanted to mention it bc I was thinking about it recently.

2 Reply Award Share ···

ZantetsuLastBlade2 • 3y ago •

PoH is based on iterative SHA-256. If loinj is correct about SHA-256 being quantum resistant, then PoH is as well.

Solana also uses ed25519 encryption, and when asked this question in Discord, the Solana devs stated pretty bluntly that they'd just swap the encryption algorithm out should it be necessary.

However, quantum attacks are basically science fiction and in my opinion, will be for a very, very, VERY long time.

4 Reply Award Share ···

[deleted] • 3y ago •

r/solana

Join

Solana

Welcome to the official Solana subreddit. This is a place to post any information, news, or questions about the Solana...

Show more

Created Mar 27, 2018

Public

333K Members

198 Online

Top 1% Rank by size

COMMUNITY BOOKMARKS

Network Analysis

Staking Resources

Dev Community

Dev Resources

GET STARTED WITH SOLANA

ZantetsuLastBlade2 · 3y ago ·

Yes, in a sense it would be. What it would allow is "censorship", where one node produces a block in a slot that should be for another node. There would be a competition for the slot between the valid node and the cheating node, and the cheating node may or may not win depending on alot of factors, but the faster it can run PoH, the better chance it has of winning. Also it gets harder and harder for the cheating node the more slots it tries to skip in this way. The easiest cheat would be to try to produce a block in the slot directly before yours. You need to run PoH twice as fast as the previous leader to compete for their slot. You need to run PoH 3x as fast as the leader before that one to compete for the slot two prior to yours. Etc. 10 slots prior to yours requires 10x PoH speed.

In the end, the network still functions, and only valid transactions are produced (the cheating validator cannot fabricate invalid transactions this way). It's just that the validator who is doing it may be not the one who "should" gave gone in that slot, and this may benefit a cheating validator a little bit -- allowing them to get a specific transaction onto the chain earlier than it might have otherwise.

It's a very marginal payoff for a cheater though. And the cheater may not win despite having faster PoH because of network latencies and other things beyond their control, and if they lose, they lose the ability to produce a block in their own slot without being slashed (since they already submitted a cheating block that claimed to be for their slot during someone else's slot, and thus cannot produce another one during their own actual slot), so there is a real cost to failure.

Also I should mention that this would be a way to produce forks very readily, so if you wanted to attack Solana itself by making it much slower with many more forks, you could do this kind of PoH cheating. But really it would be very hard to do it more often than once in a while, because a leader only has so many slots to work with.

Conclusion

- Solana’s Key Innovations:
  - Proof of History: Scalable, verifiable time
  - Proof of Stake: Efficient consensus
- Future-Proof Design: Modular cryptography for quantum safety

Questions and Discussion

Thank you for your attention!