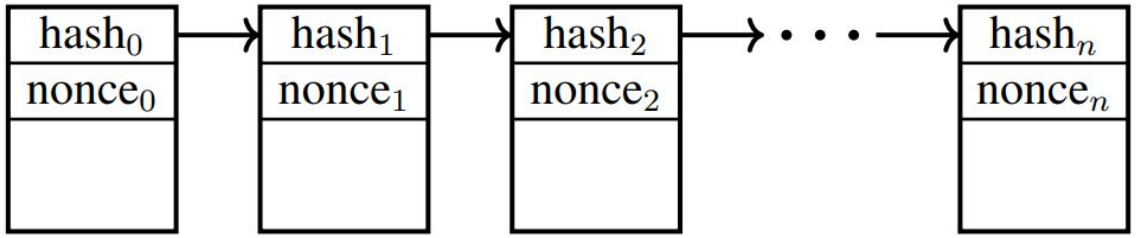
Truncating Blockchains with Tangly Statistics

Nathan Stouffer
Advised by Dr. Mike Wittie

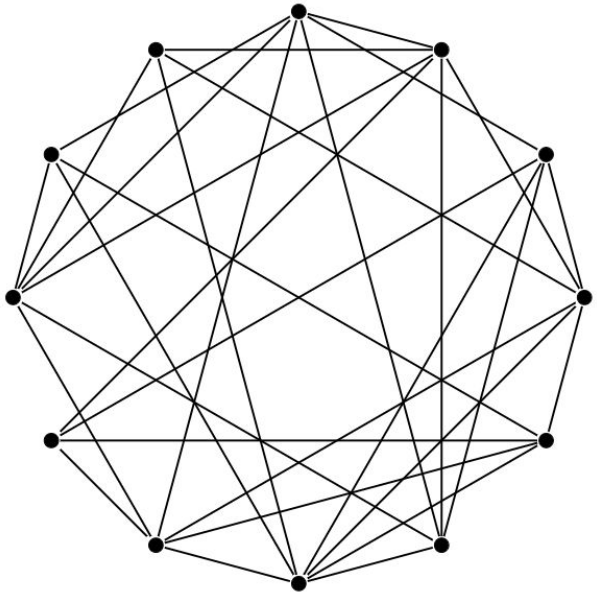
Blockchain

- Relies on cryptographic proof of work
- Provides data immutability
- Applications in cryptocurrencies, securing medical records, and online contracts



Problem

- Blockchains grow without bound
- Bitcoin can take days to download and process
- Current blockchain protocol can exclude small devices
- Computation can tend towards centralization
- Distributed computing makes blockchain more secure



Goal Question Metric

- “Specification of a measurement system… and a set of rules for the interpretation and measurement of data” - Basili
- Conceptual level: Goal
- Operational level: Questions to characterize the goal
- Quantitative level: Data to answer the questions
    - Data can be qualitative or quantitative

Goal Question Metric

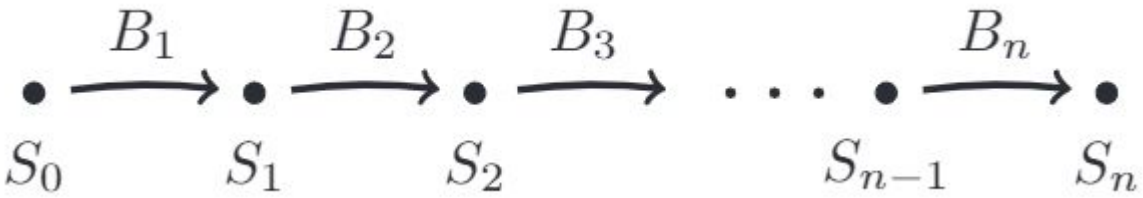
Goal	Purpose Issue Process Viewpoint	Decrease required time and space bootstrap a node to a blockchain network the bootstrapping node
Question	Q1	Is the solution off-chain?
Metrics	M1	Number of changes to blockchain protocol (must be 0)
Question	Q2	Is the solution efficient?
Metrics	M2 M3	Asymptotic analysis of time and space requirements as the chain grows Bytes of network traffic generated
Question	Q3	Is the solution secure?
Metrics	M4 M5	Theoretical probability that a malicious actor fools a bootstrapping node Empirical probability that a malicious actor fools a bootstrapping node

Goal Question Metric

Goal	Purpose Issue Process Viewpoint	Decrease required time and space bootstrap a node to a blockchain network the bootstrapping node
Question	Q1	Is the solution off-chain?
Metrics	M1	Number of changes to blockchain protocol (must be 0)
Question	Q2	Is the solution efficient?
Metrics	M2 M3	Asymptotic analysis of time and space requirements as the chain grows Bytes of network traffic generated
Question	Q3	Is the solution secure?
Metrics	M4 M5	Theoretical probability that a malicious actor fools a bootstrapping node Empirical probability that a malicious actor fools a bootstrapping node

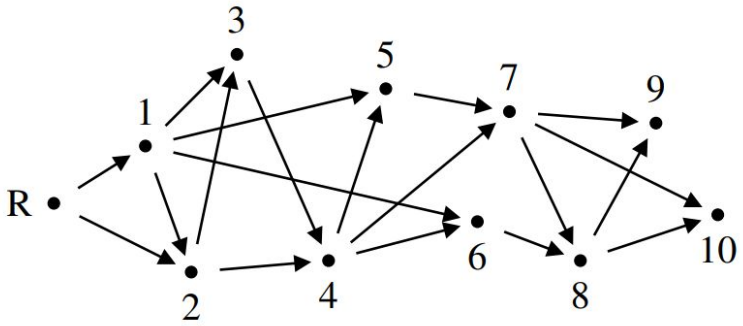
Blockchain State

- Consider blockchain to be a finite state machine
- Blocks are transitions between states
- When you have state k, the first k blocks are obsolete
- Analogous to a deterministic finite automaton

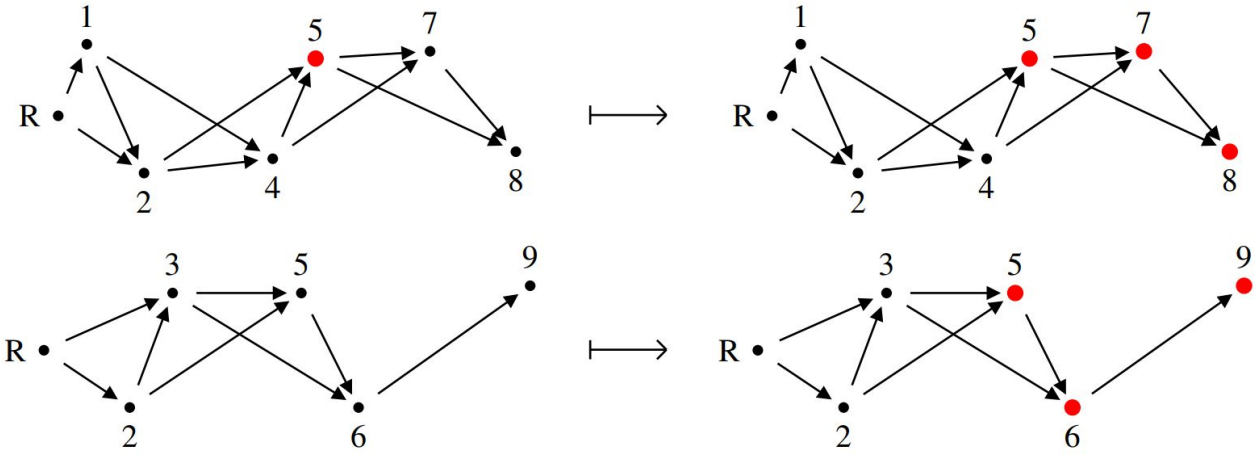


Solution

- Blockchain properties
  - Honest majority of mining power
  - Trust in a shared protocol, not any one entity
- Idea: host an election
  - Miners vote
  - Decide based on vote ratio (statistical test)
- Potential issue: who collects/stores votes
- Solution: create vote dependencies with tangles



Solution



Simulation

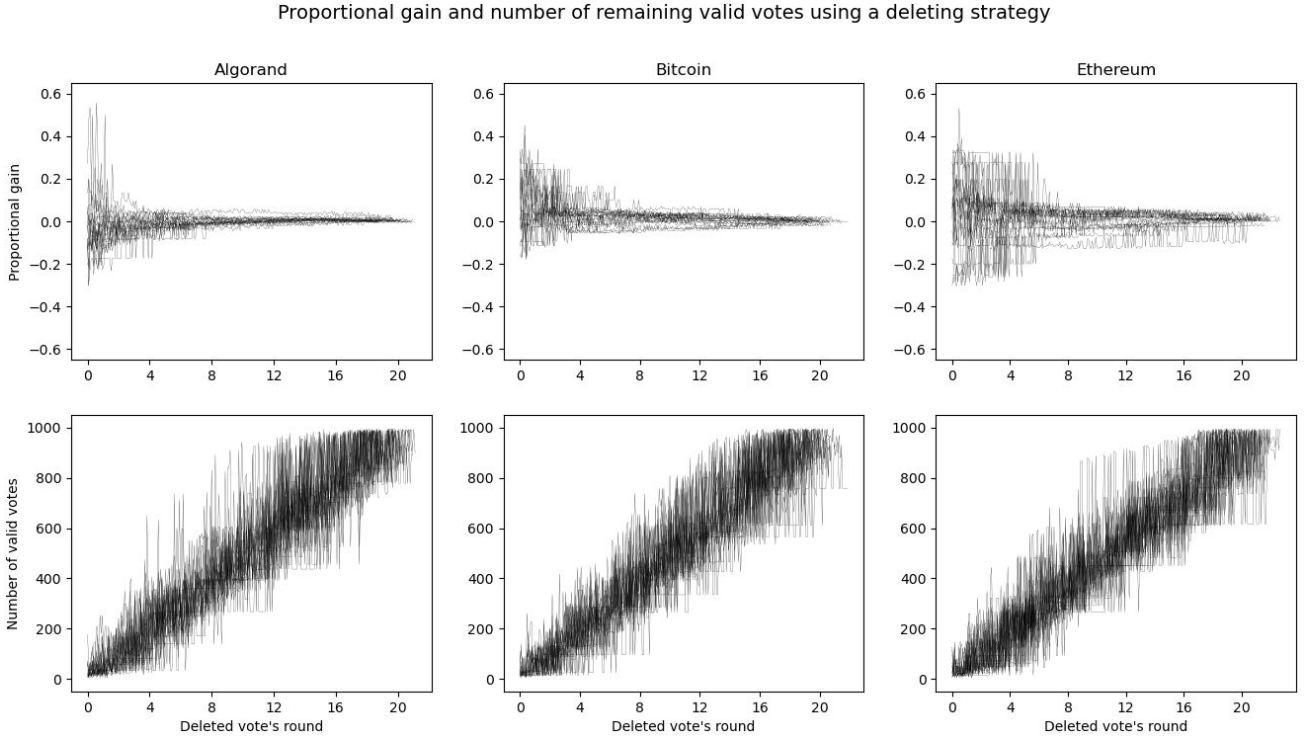
```
root@mininet-vm:~/TanglyConsensus/sim-scripts# python single-sim.py
Beg task: compile tangly package
End task: compile tangly package
Beg task: init simulation class
    Beg task: init mininet network
    End task: init mininet network
End task: init simulation class
Beg task: run simulation
    Beg task: init DHT
    End task: init DHT
    Beg task: cast votes
    End task: cast votes
    Beg task: collect tangles
    End task: collect tangles
    Beg task: shut down dht
    End task: shut down dht
    Beg task: prune tangles
    End task: prune tangles
End task: run simulation
Beg task: stop simulation
End task: stop simulation

No errors found
Simulation took 1504.0 seconds
root@mininet-vm:~/TanglyConsensus/sim-scripts#
```

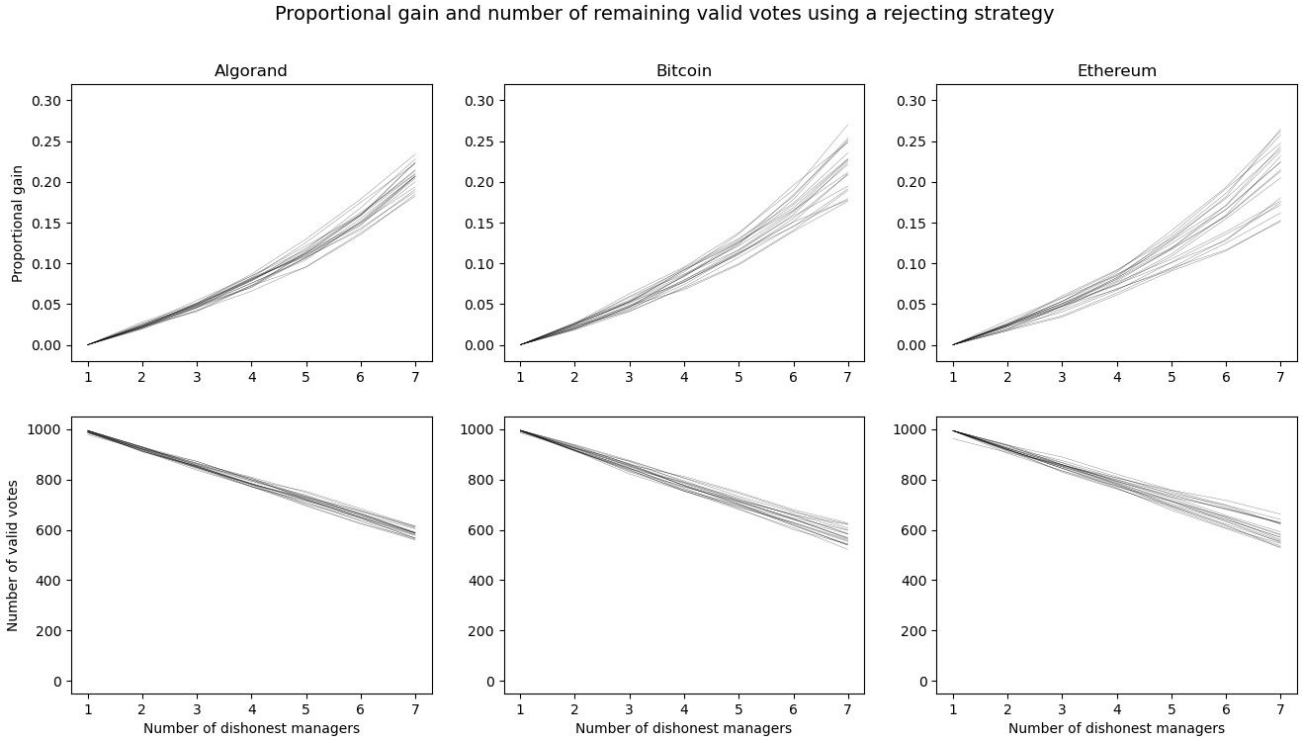
Results

- Q: Is the solution secure?
- M: Empirical probability that a malicious actor fools a bootstrapping node
- Reduction: How much can a malicious actor affect the vote distribution?
    - Two strategies: Deleting and Rejecting

Results


Proportional gain and number of remaining valid votes using a deleting strategy
Algorand
Bitcoin
Ethereum
Proportional gain
Number of valid votes
Deleted vote's round
Deleted vote's round
Deleted vote's round

Results


Proportional gain and number of remaining valid votes using a rejecting strategy
Algorand
Bitcoin
Ethereum
Proportional gain
Number of valid votes
Number of dishonest managers
Number of dishonest managers
Number of dishonest managers

Discussion

- Protocol is way faster than current join time
  - Simulation takes about 1000 seconds on average
  - Note that this is just a lower bound
- Security is questionable
  - Rejecting poses a threat
- Future work
  - Playing with system parameters
  - Collect/analyze network data
  - Nail down details on statistics

References

- Serguei Popov. The tangle. cit. on, page 131, 2016.
- Roman Matzutt, Benedikt Kalde, Jan Pennekamp, Arthur Drichel, Martin Henze, and Klaus Wehrle. How to securely prune bitcoin's blockchain. ArXiv, abs/2004.06911, 2020.
- Victor R Basili, Gianluigi Caldiera, and H Dieter Rombach. The goal question metric approach. Encyclopedia of software engineering, pages 528–532, 1994.