Truncating Blockchains with Tangly Statistics

Nathan Stouffer, Max Digiacomo, and Dr. Mike Wittie – Montana State University

Introduction

Blockchain security increases when mining power is decentralized. Unfortunately, decentralization is limited by the costs of joining a blockchain.

Blockchains grow without bound and new miners must process each block. Chains can be summarized into a state, but the state cannot be trusted.

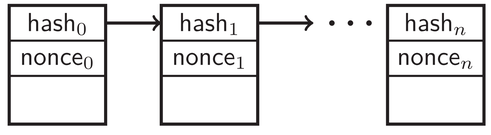

Figure 1: A prototypical blockchain [1]

We host an election to verify a blockchain state. A trusted state reduces bootstrapping costs, making blockchains more accessible.

Background

Properties

- Trust a shared protocol, not a central party
- Honest majority of mining power

Blockchain State

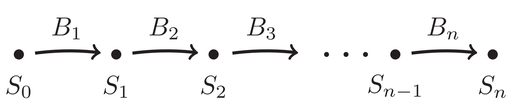

Figure 2: Blocks as transitions between states

Tangle

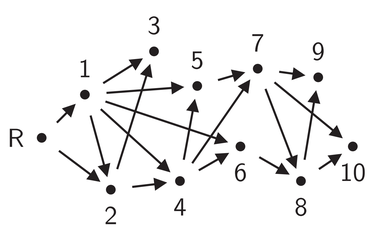

Figure 3: A tangle [2] creating vote dependencies

Solution

Voting Protocol

- Construct a vote v as in Figure 4
- Submit v to two deterministically chosen tangles [2] (this creates a sibling relationship)
- Each tangle manager chooses parents and attaches v to its tangle

public key	block number: i
hash(S_i)	digital signature

Figure 4: Vote structure

Validity Requirements for v

- v is structurally valid
- v has a valid sibling
- Every ancestor of v is valid

Decision Protocol

- Collect all tangles and mark votes as invalid
- Determine majority among valid votes
- Accept or reject majority based on χ^2 test

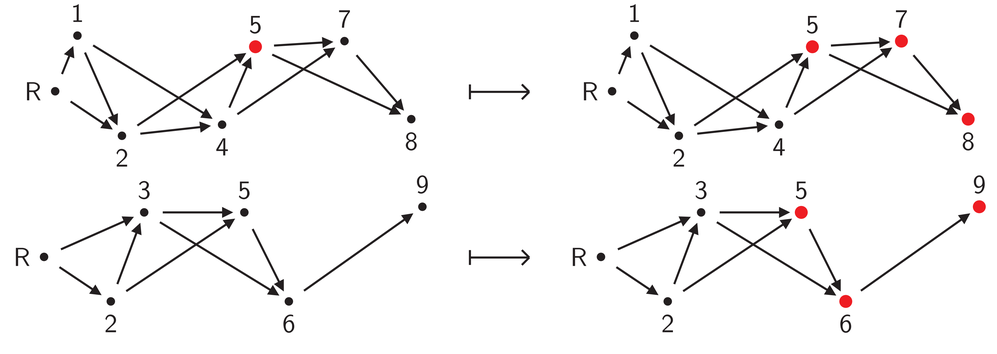

Figure 5: Showing how an invalid vote causes a chain reaction (red is invalid)

Results

- We model a strong, yet stupid, attacker A who controls all but 1 manager
- We wonder if A can gain an unfair share of valid votes
- Figure 6 shows A's proportional gain when A deletes the k^{th} vote in simulated elections
- Experimentally, we find A can only affect the election by deleting one of the first 400 votes

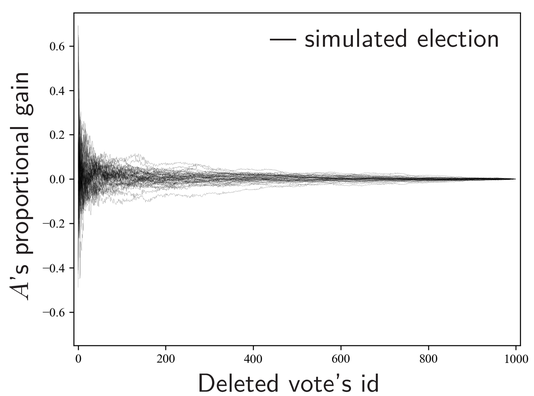

Figure 6: A's proportional gain by deleting the k^{th} vote

- We use the χ^2 test to determine whether a bootstrapping node should accept a state
- We expect at least 90% of votes to agree
- In Figure 7, the red regions show when we accept a state ($p > 0.10$)
- We find that elections with more than 600 votes are resilient against attackers with less than 50% of mining power

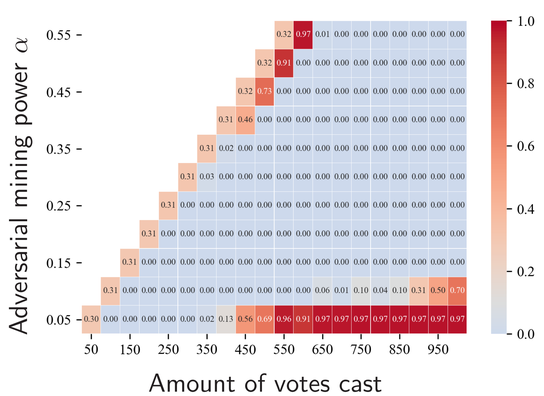

Figure 7: P-value from a χ^2 goodness of fit test

Conclusion

- Vote timing does not depend on new blocks being generated, decreasing the lower bound for consensus time
- If we require at least 600 valid votes, an attacker has a negligible probability of satisfying the χ^2 test
- If there is at least one honest manager, an attacker cannot significantly affect the χ^2 test by deleting votes
- Protocol may increase miner participation, resulting in better blockchain security

Acknowledgments

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.

[2] Serguei Popov. The tangle. *cit. on*, page 131, 2016.

- Summer 2020 funding provided by the National Science Foundation via the REU hosted by the Software Factory
- Subsequent 2020-2021 funding provided by the Undergraduate Scholars Program at MSU