Truncating Blockchain with Tangly Statistics

Nathan Stouffer advised by Dr. Mike Wittie

Blockchains provide a way to decentralize ledger-keeping systems. They are best known for their use in cryptocurrencies, but blockchains also have applications in supply chain tracking, providing data integrity, and any situation where immutable data is useful. To provide immutability, some blockchains use Proof of Work to construct an ever growing chain of blocks in a peer to peer network. Miners are expected to expend computational work to create a new block. Since blocks are intentionally difficult to create, users of a blockchain can trust the information held in the longest blockchain.

Miners have collective control over a blockchain. If miners are sufficiently decentralized, then only a large coalition of miners could gain explicit control of a blockchain. Explicit control allows the coalition to decide which blocks are added to the chain, reducing the integrity of the system. Thus a blockchain perform better when control of the chain is decentralized. Decentralized mining can be difficult to achieve when blockchains grow to an unmanageable length. To begin mining, one must download and process the entire chain. This is not problem when the chain is relatively small, but a larger chain (such as Bitcoin) can take days to process.

Excessively long chains limit decentralization in two ways. First, lightweight devices are prevented from becoming miners. Soon, many desktops and laptops will not be able to become a Bitcoin miner. Second, incredibly long bootstrapping time deters participation from users who do have sufficient space. Together, these issues decrease decentralization which reduces the effectiveness of a blockchain.

Over the summer, I worked with collaborators to devise a protocol that prunes blocks while preserving the chain's integrity. We ended the summer with a solution sketch that has potential but still needs significant work. At a high level, our solution has miners of recent blocks vote for a blockchain summary. If sufficiently many votes agree, bootstrapping nodes can trust the blockchain summary, which drastically reduces onboarding times.

For my capstone project, I will extend the solution sketch from this summer. There are still issues to resolve and I must provide formal security proofs. Following this, I will implement a model of our solution. Using the model, I will run simulations and extract experimental results.