

# Capstone Abstract

Nathan Stouffer

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 information needs to be immutable. To provide immutability, 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 technically have complete control over a blockchain, but if the miners are sufficiently decentralized, they cannot make a substantial impact on the blockchain by deviating from the protocol. Thus a blockchain performs better when control of the chain is decentralized. However, decentralized mining can become difficult to achieve when blockchains grow to an unmanageable length. To begin mining, one must download and process the entire chain. For Bitcoin (the most popular blockchain), it can take days to become a full fledged miner. This decreases decentralization in two ways. First, lightweight devices are prevented from becoming miners. Even desktops and laptops will soon not be able to become a Bitcoin miner. Second, people are less likely to become a miner because of the incredibly long bootstrapping time. Together, these issues decrease decentralization in a blockchain which reduces the effectiveness of a blockchain.