Analyzing the Security and Privacy of Bitcoin

Max Grice

Purpose

- Online transactions have previously relied on trusted third parties such as governments and banks to ensure reliability, security, and privacy
- A growing lack of trust in financial institutions has helped to promote cryptocurrencies like bitcoin which function without third party authentication

❖ ***To what extent is Bitcoin a solution to the vulnerabilities of current online transaction methods?***

Background

- Critical features that separate cryptocurrencies like Bitcoin from normal third party transaction schemes are listed and described below:

➢ **Asymmetric Cryptography:** Public keys identify users while private keys encrypted in a hash of transactional information to validate transactions. A user can generate multiple public keys using deterministic wallets to make keys easier to remember and maximize anonymity

➢ **Digital Signatures:** Users must sign a transactional message with their private key in order to confirm ensure secure validation

➢ **Proof of Work Protocol (PoW)** : Once signed, transactions are sent into the node network and bundled into blocks by miners who use computational power to solve a crypto-puzzle, creating a decentralized distributed consensus model

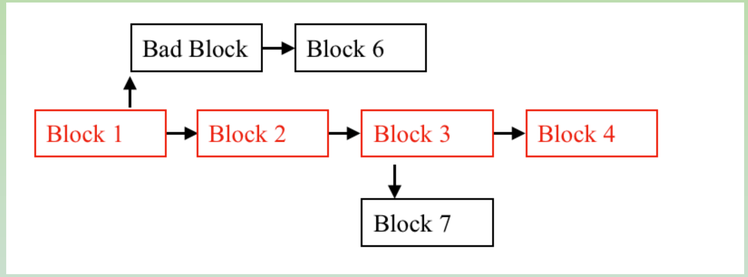
➢ **Block-Chain**: Validated blocks are broadcasted to the network to be accepted by other miners and chained together as a shared public ledger.

Implementation + Evaluation

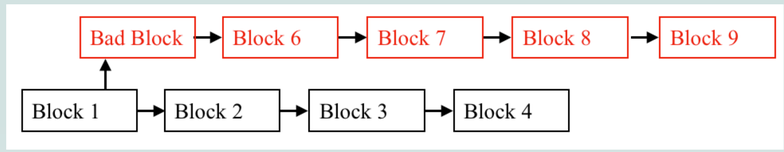
- **Block-Chain Implementation**: Created Transactions, Blocks, Public/Private keys, and Wallets
- Validated transactions by creating and moving coins between wallets
- Tested Points of Vulnerability in block validation
  - Double Spending
  - Invalid Coin Ownership
  - Malicious Modification of Blocks
  - **Majority Attack (51%) – Illustrated Below:**

**** Accepted Chain is Denoted by Red***

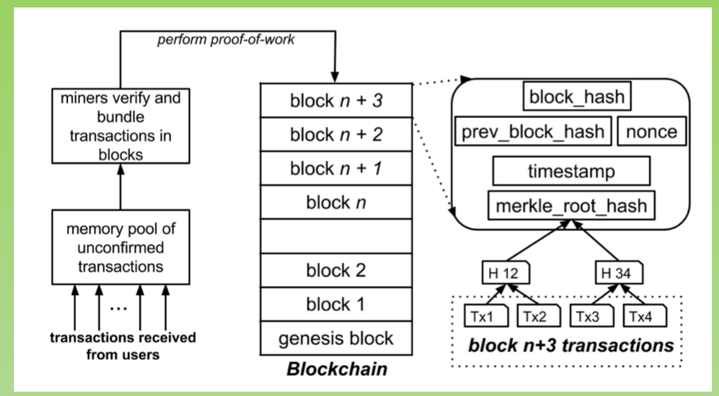
Majority Attack is Unsuccessful: The bad block is in the shorter forked chain so it is not accepted by node network.



Majority Attack is Successful: Miners mine blocks on top of the bad block so that the forked chain becomes longer than the original, making the attack successful.



Block Chain Diagram



Conclusions

Strengths

- Asymmetric cryptography provides privacy and security
- Distributed consensus model creates decentralized network, protecting from inflation and malicious manipulations
- Transaction fees are low and processing time is faster when transferring large sums of money (eg internationally)

Weaknesses

- The PoW protocol often leads to computational waste and slow transaction validation times
- Growth in popularity has lead to higher transaction fees and slower processing for many smaller transactions
- Private keys and seed words cannot be recovered if lost
- While rare, 51% and net-split attacks are possible

Current Solutions

- **BIP39**: Mnemonic code allows for generation of deterministic wallets with seed words that are much easier to recall and store than private keys
- **Lightning Network**: Second layer technology that uses micropayment channels to decongest and reduce fees
- **Shamir's Secret:** Cryptographic algorithm used to divide seed words among parties so that only a user majority can combine parts to reconstruct the original secret (potential solution to security issues in seed word storage).