Security Analysis of Bitcoin

- Dibyojyoti Mukherjee
- Jaswant Katragadda
- Yashwant Gazula
Security Analysis of Bitcoin

- **Introduction**
- How Bitcoin works?
- Similar peer-to-peer systems
- Vulnerabilities and solutions
Crypto-currency

- It is a digital currency that uses cryptology for security

- Anonymous:
  - (more or less) Transactions are not tied to your identity

- Decentralized:
  - Not issued by any central authority
  - Trust based on peer-to-peer consensus

- Bitcoin was the first cryptocurrency created in 2009
Bitcoin

- An open source P2P digital currency
- Bitcoin is a digital currency, a protocol and a software that enables:
  - Instant peer-to-peer transactions; Worldwide payments
  - Irreversible by design; Almost no processing fee
  - Relies on cryptography and p2p network – no central authority
  - Finite - 21 million Bitcoins issued
  - 12.5 million (60%) ‘mined’ to date
Security Analysis of Bitcoin

- Introduction
- **How Bitcoin works?**
- Similar peer-to-peer systems
- Vulnerabilities and solutions
Bitcoin Transactions

- A network of computers

- Every computer can send messages to some other computers
Bitcoin Transactions

- Every computer maintains a table: “who owns what?”

- All computers have the same table

Remark: The public keys are just bit strings.
Bitcoin Transactions

- Electronic coin is a chain of digital signatures
Bitcoin Transactions

In “short”:

Transfer 0.1 BTC from Alice (Public) to Bob (Public)
**Bitcoin Transactions**

I’LL send 0.1 Bitcoin to Bob.

**Protocol: sending BTC**
1. Craft a transaction.
2. Give it to your computer.

**Protocol: participating**
On valid transactions:
1. Update ledger
2. Relay transaction
Bitcoin Mining

- Collects transactions from the network
- Validates them, and doesn't allow conflicting ones
- Puts them into large bundles called blocks
- Computes cryptographic hashes over and over until if finds one "good enough to count"
- Then submits the block to the network, adding it to the block chain and earning a reward in return
Hardware Acceleration

- Initially miners used their **central processing unit (CPU)** to mine. It blogged down because of its low speed.
- Then **GPU and FPGA** accelerators are used due to increase in complexity in Bitcoin Community.
- FPGA miners made concentrated mining farms possible for the first time.
- 50 to 100 times faster and consumed much less power per unit of work.
Today's modern Bitcoin mining hardware

- **Application-specific integrated circuit** (ASIC) miners have taken over completely.
- ASIC machines mine at unprecedented speeds while consuming much less power than FPGA or GPU miners.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Hashes/Second</th>
<th>Power Consumed</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPU</td>
<td>600M</td>
<td>400W</td>
</tr>
<tr>
<td>FPGA</td>
<td>826M</td>
<td>80W</td>
</tr>
<tr>
<td>ASIC</td>
<td>600G</td>
<td>350W</td>
</tr>
</tbody>
</table>
Mining Software

- Special software is needed to connect miners to the block chain and your mining pool as well, if you are part of a mining pool.
- Software delivers the work to the miners and receives back the completed work and relays that information back to the blockchain and mining pools.
- Examples: CGMINER, BFGMINER
Security Analysis of Bitcoin

- Introduction
- How Bitcoin works?
- Similar peer-to-peer systems
- Vulnerabilities and solutions
Lite-coin is a crypto-currency which was created with the sole motivation of improving upon the existing gold standard of crypto-currency i.e. Bitcoin.

- Bitcoin uses the SHA-256 hashing.
- Litecoin uses the S-Crypt algorithm. S-Crypt favors large amounts of high-speed RAM, rather than raw processing power alone.
Bitcoin vs Ripple

- Ripple is a payment system which is built upon an open source internet protocol and native currency called ripples (XRP).
- Ripple uses the same underlying cryptography as Bitcoin and it employs multi-signature support like Bitcoin.
- Just like Bitcoin, Ripple has low to no transaction fees and also Ripple servers can be run by anyone.
How does ripple solve double spending problem of bitcoin?

- Ripple solves the double-spend problem by consensus.
- Consensus is the process by which the entire network agrees on the same Ledger.
- The Ledger contains a list of all the accounts and the balance of each account (and similar data).
Bitcoin vs MintChip

- MintChip is the brainchild of The Royal Canadian Mint which decided to jump into the digital currency world after witnessing the success of Bitcoin.

- MintChip is very similar to Bitcoin because it shares the core algorithms which run both of these peer to peer systems. However there are a couple of contrasting characteristics.
Security Analysis of Bitcoin

- Introduction
- How Bitcoin works?
- Similar peer-to-peer systems
- Vulnerabilities and solutions
Double-spending

Black Hat prepares two transactions:

- Give BTC from Black Hat to Alice
- Give BTC from Black Hat to Bob

These transactions spend previously spent bitcoins!
Double-spending

- The bad guy spends the \textit{same} Bitcoins with two different transactions \textcolor{red}{\textit{SFT}} and \textcolor{blue}{\textit{SFT}}.

- Computers receiving transaction \textcolor{red}{\textit{SFT}} will have a \textit{different} ledger than computers receiving transaction \textcolor{blue}{\textit{SFT}}.
Existing Solution for double-spending

- Miners collect the transactions on the network into large bundles called **blocks**
- These blocks are strung together into one continuous, authoritative record called the **block chain**
  - *lets you know for sure exactly which transactions count and can be trusted*
- The **block chain** prevents the double spend attack by giving other nodes the power to verify that transaction inputs were not already spent somewhere else
Better Solution for Double-spending

- A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash.

- The timestamp proves that the data must have existed at the time.
Brute force attack applied on Bitcoin

- Brute force attack can be used to attack keys generated by improperly-configured random number generators
- Brute force attack can also be chosen to attack poorly-chosen brain wallets
- The algorithm used for the computation of the private and public (which is the associated address) keys is ECDSA (Elliptic Curve Digital Signature Algorithm)
Why does brute force attack not work?

- Theoretically, a brute force attack should work.
- We have to brute force the ECDSA, which requires solving $2^{256}$ (as the private key is 256 bits) operations to find the private key.
- It's computationally unfeasible.
- To speak in orders of magnitude, brute forcing 50 bits of entropy would cost $1000 of CPU time.
- A bitcoin private key has 256 bits of entropy, so that would be roughly a 60-digit number times $1000.
Finney Attack

- The Finney attack is named after Hal Finney

It is a double spending attack with the following features:

- It only works if the merchant accepts unconfirmed transactions

- It still works, however, if the merchant waits a few seconds to verify that everyone in the network agrees he was paid

- It requires the attacker to be mining and controlling the content of his blocks; however, he can in theory do this with any hashrate, in particular significantly less than 50% of the network hashrate
Possible Solution for a Finney attack

- The only way to protect oneself against such an attack is to require at least one confirmation for transaction before giving out purchased goods, and requiring more confirmations for transactions worth more
Recent Finney attack

- Some illegal miners were regularly using this against gaming websites like Satoshi-Dice. Essentially, they created a block with a transaction crediting themselves.

- They sent a conflicting transaction to SD that can net you more than the block reward. If you lose, you release the block and get your money back. If you win, you discard the block and keep the winnings.

- To avoid this, Satoshi-Dice switched over to only processing bets with 1+ confirmations.
Conclusions

- Current measures adopted by Bitcoin are not enough to protect the privacy of users
- Existing vulnerabilities might severely harm the growth of Bitcoin
- BitCoin combined techniques from crypto and the right incentives
- BitCoin is becoming industrialized
  - Miners form a pool
  - Mining hardware becomes sophisticated
  - Government agencies are keeping an eye on them
THANK YOU
References


