Bitter to Better: How to make Bitcoin a Better Currency

Authors: Simon Barber, Xavier Boyen, Elaine Shi, Ersin Uzun

Presentation by Aroon Sharma
April 23, 2014
What is Bitcoin?

• P2P online payment system introduced in 2009
• Developed by Satoshi Nakamoto
• Uses many cryptographic techniques to support the protocol
Bitcoin’s Appealing Characteristics

- Decentralized
  - No central bank or entity controlling the currency
- Privacy and Anonymity
  - Transactions are difficult to tie to a particular individual
- Currency divisibility
  - 1 satoshi = 0.00000001 BTC
- Transaction irreversibility
  - By construction, transactions become final within 10 minutes
Bitcoin’s Appealing Characteristics

- **Low transaction fees**
  - Fees included at discretion of payer
  - Fees for credit card processing usually total to 2-5%

- **Incentives to participate**
  - Coinbase transactions
  - Transaction fees

- **Open source**
  - Anyone with an Internet connection can open up a wallet and start transacting
  - Anyone can modify the client code and protocol
Transaction Example

- Inputs (green)
- Outputs (red)

Alice’s Digital Signature (ECDSA)

Broadcast to network
Bitcoin Wallet

- A wallet is a file that contains a series of valid Bitcoin addresses
- Each address can contain its own balance of Bitcoins
- Loss of the Bitcoin wallet results in permanent loss of Bitcoins tied to those addresses!
Bitcoin Address Generation

- Bitcoin transactions use Elliptic Curve Digital Signature Algorithm (ECDSA)

- Public and private keys generated per address
  - Private key is signing key
  - Public key is verifying key

- Actual Bitcoin address is a series of hashes of the ECDSA public key
Bitcoin Address Generation

Elliptic-Curve Public Key to BTC Address conversion

Public Key:

\[ X_{\text{integer}} \quad Y_{\text{integer}} \]

1. 32 bytes (BE) 32 bytes (BE)

0x04

\text{ripemd160(sha256( } \begin{array}{c} 1 \quad 32 \text{ bytes (BE)} \quad 32 \text{ bytes (BE)} \end{array} ) \text{ )}}

Network ID Byte:

Main Network: 0x00
Test Network: 0x07
Namecoin Net: 0x34

1. 20 bytes

\text{sha256(sha256( } \begin{array}{c} 1 \quad 20 \text{ bytes} \end{array} ) \text{ )}}

32 bytes

25-byte binary address

1. 20 bytes 4

Base256-to-Base58 conversion*

(treat both quantities like big-endian)

1AGRxqDa5WjUKBwHB9XYEjmknv1uc0UUsy1s

*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing "0052" instead of just "52"), but in the BTC network the left-most zero byte is carried through the conversion. So for every valid byte on the left end of the binary address, we will attach one \( 1 \) character to the Base58 address. This is why main network addresses all start with \( 1 \).
Bitcoin Block Chain

- Transactions are grouped together in bundles called *blocks*.
  - Also contains the hash of the previous block

- The collective history of transactions and blocks is known as the *block chain*

- Parameters of the protocol make it so a new block is created every 10 minutes

- Bitcoin miners race to compute a cryptographic hash of the current block
  - Coinbase transactions
  - Transaction fees
Block Details

- Transactions within a block are organized as a Merkle hash tree structure
  - Transactions $t_1$, $t_2$, $t_3$
  - Previous block hash $H$
  - $F(\ . \ ) = \text{SHA256(\text{SHA256}(\ . \ )))$ – double hash

```
\begin{align*}
  h_7 &= F(h_5 \ || \ h_6) \\
  h_5 &= F(h_1 \ || \ h_2) \\
  h_6 &= F(h_3 \ || \ h_4) \\
  h_1 &= F(t_1) \\
  h_2 &= F(t_2) \\
  h_3 &= F(t_3) \\
  h_4 &= F(H) \\
  t_1 \
  t_2 \
  t_3 \
  H
\end{align*}
```
Money Supply

• 21 million Bitcoins to ever be in circulation
  • Deflationary currency
  • Currently about 12.5 million BTC in circulation
  • Expected to reach 21 million BTC by 2140

• How are new Bitcoins created?
  • Coinbase transactions – rewards for miners that correctly create a new block
  • Reward is currently 25 coins per block
  • Reward halves every four years
Transaction verification and mining

- If there is no central authority, how can the network agree on a single history of transactions?
  - Once a block is confirmed, it is sent out across the network and all transactions within the block are considered final.
  - Other nodes on the network now use this block to extend the chain and produce the next block.
  - Protocol works under the assumption that the majority of the nodes and computational power are honest.
Transaction verification and mining

- Bitcoin Miner
  - A node on the network that races to compute a new transaction block
  - Solves a cryptographic puzzle based on a proof of work protocol
  - Proof of work protocol’s difficulty is adjusted based on the total computational power on the network in order to maintain a new block every 10 minutes
Proof of Work Protocol

- A cryptographic puzzle that takes substantial computational power to solve
- A correct solution to the puzzle can be easily verified
- In Bitcoin
  - Given a challenge string \( c \)
  - Produce a proof string \( p \) such that the hash of \( c \) concatenated with \( p \) has \( n \) leading 0’s.

\[
\begin{align*}
&c & p \\
\downarrow & \downarrow \\
\text{SHA256} \\
\downarrow \\
00000…xxxxxxx…
\end{align*}
\]
Proof of Work Protocol

• Why is the protocol set up this way?
  • Answer: The hash function is one-way pseudorandom. The only way to produce the required output is to try many inputs

• The difficulty in solving the puzzle is tuned by n, the number of leading 0’s
  • Remember, a block must be solved every 10 minutes
  • Change in difficulty accounts for changes in total computational power on the network
Proof of Work Protocol

• Complicated hardware configurations dedicated solely to mining

• ASICs – Application Specific Integrated Circuits
  • Hardware designs specifically designed to computed hashes at higher throughput and lower power

• Mining Pools
  • Nodes pool their computational power together and share the block reward payouts
Potential Problems with Bitcoin – Loss of Bitcoins

• If a wallet file is lost, all bitcoins associated with that wallet are lost forever

  • Possible solution – generate bitcoin addresses for a wallet using a deterministic pseudo-random generator

  • Only need to store the seed of the generator to retrieve wallet addresses
Potential Problems with Bitcoin – History Revision Attack

- Bitcoin transactions are generally valid once they are added to the block chain.

- What happens if two nodes solve the same block simultaneously?
  - The node with the higher computational effort in solving the block wins.

- A group of malicious nodes having the majority of the computational power could produce a valid but incorrect transaction history.

- It would be accepted if the computational effort to produce the incorrect history exceeded the true branch’s effort.
Potential Problems with Bitcoin – Quantum Attack

- Bitcoin transactions use ECDSA for signing and verifying.

- This signature scheme is vulnerable to Shor’s algorithm, a quantum algorithm that can efficiently determine the signing key from the verifying key.

- Possible solution: Replace ECDSA with a quantum resistant signature scheme such as NTRU (Nth Degree Truncated Polynomials).