BITCOIN· DIGITAL DECENTRALIZED PEER TO PEER
1 TROYOZ 999 FINE COPPER MJB MONETARY METALS

The Cryptography behind Cryptocurrency

Lolita Rozenbaum and Christine Yan

What is Cryptocurrency? Why do people use it?

Cryptocurrency is a peer-to-peer digital asset used as a means of exchange. This internet currency uses cryptography to secure the transaction.

- No need to rely on banking institutions or the government
- Not tied to any country or subject to any regulation
- Purchases can be made anonymously

The basic building block for Bitcoin and a blockchain system is cryptography.

How is Bitcoin Acquired?

Direct Purchase

Buying Bitcoin at the current market value

Transaction

Selling products and receiving Bitcoin as payment

Creation

Creating Bitcoin through a computer or machine

Mining

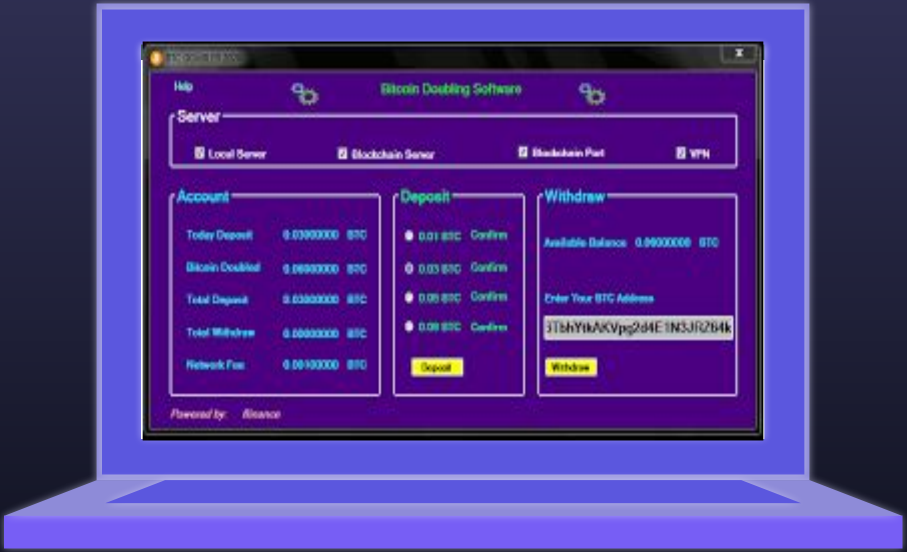
Purposes

1. Verifies transaction records across networks
2. Contributes to blockchains
3. Adds credibility to networks

Users solve complex mathematical puzzles on supercomputers to discover new blocks.

- Limited amount of Bitcoin available to be mined, which allows the system to prevent inflation

Bitcoin Encryption



Server

☑ Local Server ☑ Blockchain Server ☑ Blockchain Port ☑ VPN

Account

Today Deposit 0.03000000 BTC
Bitcoin Doubled 0.06000000 BTC
Total Deposit 0.03000000 BTC
Total Withdraw 0.00000000 BTC
Network Fee 0.00100000 BTC

Deposit

● 0.01 BTC Confirm
○ 0.03 BTC Confirm
● 0.05 BTC Confirm
● 0.08 BTC Confirm

Withdraw

Available Balance 0.06000000 BTC

Enter Your BTC Address

3TbhYtkAKVpg2d4E1N3JRZ84k

Powered by: Binance

Bitcoin token balances are kept using public and private keys.

- ➢ Public key: address published to the world; others may send funds to
  - ○ Analogous to Bank Account Number
- ➢ Private key: authorize Bitcoin transmissions
  - ○ Analogous to ATM PIN

Bitcoin Encryption Cont.

Private keys produce a public key via a one-sided algorithm: **ECDSA** (Elliptical Curve Digital Signature Algorithm)

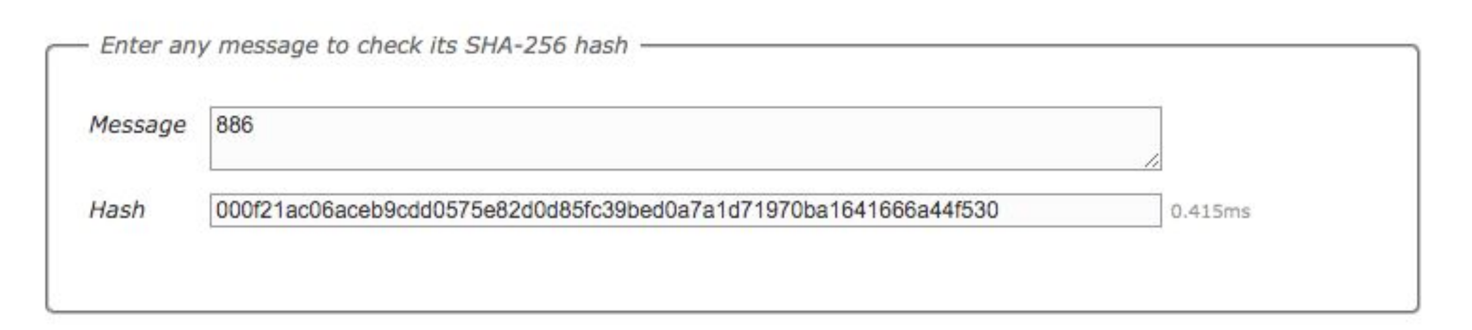
- Public keys can never be reverse-engineered to produce private keys
- A private key is usually a 256-bit number
- Total address space: 2^160

Private Key:
KxeNcRw8mBfyLrnnXQymQkogLjvmn6uJCmSWLRmZ6Mt3Hzfgo1mY

Deposit Address:
1MnU3iyTeej69DKGGKo6vU3H3dKKZ9ZL6u

Proof-of-Work

Demonstrate that the computer completed algorithms to solve the problem



Enter any message to check its SHA-256 hash

Message: 886

Hash: 000f21ac06aceb9cdd0575e82d0d85fc39bed0a7a1d71970ba1641666a44f530 0.415ms

Hash Proof-of-Work Example

If Person A claims “886” produces a hash starting with 000, anyone is able to verify Person A’s statement.

For Bitcoin, the process requires supercomputers.

- Finding a string with the first 40 bits being 0’s could take a trillion attempts.
- The proof string needs to be hashed and matched with desired bits to confirm the proof of work as valid.

Mining from the Block Chain

1 1

Hashed Transactions

Mining software takes the active transactions and double hashes them (applies SHA-256 twice).

2

Chain Creation

Software creates block headers to keep track of blocks and related information.

Mining from the Block Chain Cont.

3

Nonce

The 4-byte field is adjusted and incremented each time a block is mined.

4

End Comparison

Block is compared to the “target”, which is compressed and stored in bits. The hash must be less than or equal to the target.

Example of End/Target Comparison

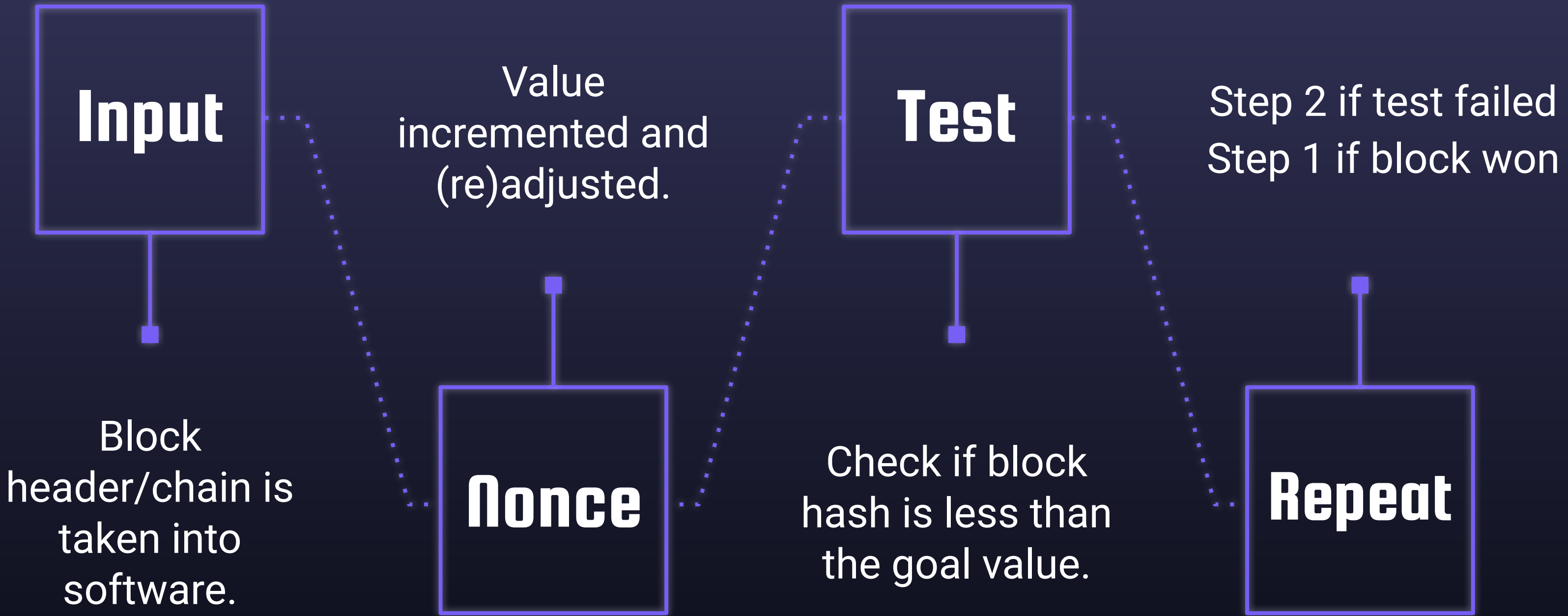
Example of Real Expanded Hash Solved by Miners:
00000000000000000008263**b489**e924db823edbec18b715eed6c53ecabb49a07

Example of Possible Expanded Target Compared Against:
00000000000000000008263**c299**0000000000000000000000000000000000000

The comparison is to check if the SHA-256 Hash Block is less than or equal to the target.

- b489 is less than c299 in the example, so the miner won the block.

Mining Process Summary



Input

Block header/chain is taken into software.

Nonce

Value incremented and (re)adjusted.

Test

Check if block hash is less than the goal value.

Repeat

Step 2 if test failed
Step 1 if block won

Demo

Python Blockchain with Mining

References & Sources

- https://www.blockchain.com/explorer
- https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work
- https://www.pluralsight.com/guides/the-cryptography-of-bitcoin
- https://en.bitcoin.it/wiki/Target
- https://en.bitcoin.it/wiki/Nonce
- https://www.investopedia.com/tech/how-does-bitcoin-mining-work/
- https://www.bitcoinmining.com/