



What is Cryptocurrency?

- Digital Currency
- Secure Anonymous Transactions

Benefits of a Decentralized Cryptocurrency

- No government or financial institution control
- Portability
 - Can be sent across the world quickly
- Trust
 - Impossible to “cook the books” or steal your coins



Bitcoin

- \$65 billion dollars market cap
 - Larger than many well known companies
- ~300,000 transactions per day
- Processing power of 7,295,097,599 GH/s or ~7.3 EH/s

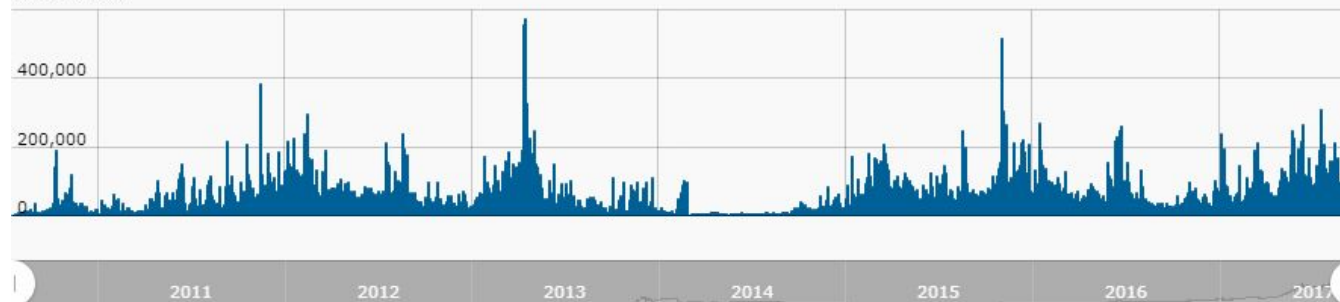
Bitcoin's History

- 2008
 - Satoshi Nakamoto writes the paper “Bitcoin: A Peer-to-Peer Electronic Cash System”
- 2009
 - Nakamoto deploys the Bitcoin network and mines the first Bitcoin
- 2010
 - Mt.Gox launched
- 2011
 - Silk Road launched
- 2013
 - Coinbase and other exchanges take off
 - Silk Road shut down
 - Bitcoin reaches \$1000/BTC
- 2014
 - Mt.Gox shuts down due to fraud

CryptoCompare Index : BTC



Volume BTC



Bitcoin Structure

- Addresses with Private keys
- Transactions
- Blockchain
- Mining

Public Address

- Destination or Source of Bitcoins
- Publically available
- Can be created offline
- Single Use
- First Public Address
 - [1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa](#)

Bitcoin Address



SHARE

181i4mWBmcXfwYjGPH7SxJuCUcF5mAHcqN

Private Key

- Secret number that allows Bitcoins in a paired address to be sent
- Algorithmically related to its public address
- Every transaction will be digitally signed by the sender's private key, where the network can verify with sender's public key.
- With control of the private key, an address can be imported to any wallet

SECRET



Private Key

L52t1JLZKNUPHN4a61myccDyG3KyssqsLBtUwQHhb713Cu5gGyS

Wallets

- Collection of addresses and private keys
- Hot Storage
 - Stored online
- Cold Storage
 - Created and stored without access to the Internet

Advanced Wallets

- Software Wallets
 - Exodus
 - Cryptocurrency Exchanges
- Paper Wallets
 - <https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html>
- Hardware Wallets
 - Trezor
 - USB

Blockchain

- Bitcoin's Ledger containing every transaction ever made
- Every client connected to the Bitcoin network subscribes to the blockchain and stores a local copy.
- Transactions are grouped into *Blocks*
- Every 10 minutes, a new block is appended to the blockchain
- Blocks are arranged into a single long chain, with new blocks being appended to the end of the original chain.
- Blocks are 1 MB Size
- Every block contains a block hash of the previous block.

Transactions from
about 40 minutes ago

```
transaction ID: 100
address 1aaaa -2.0 BTC
address 1bbbb +2.0 BTC
transaction ID: 101
address 1cccc -3.0 BTC
address 1aaaa +2.0 BTC
address 1dddd +1.0 BTC
transaction ID: 102
address 1aaaa -2.0 BTC
address 1bbbb +2.0 BTC
⋮
```

Transactions from
about 30 minutes ago

```
transaction ID: 520
address 1eeee -5.0 BTC
address 1cccc +4.8 BTC
address 1ffff +0.1 BTC
address 1aaaa +0.1 BTC
transaction ID: 521
address 1eeee -5.0 BTC
address 1cccc +4.8 BTC
address 1ffff +0.1 BTC
address 1aaaa +0.1 BTC
⋮
```

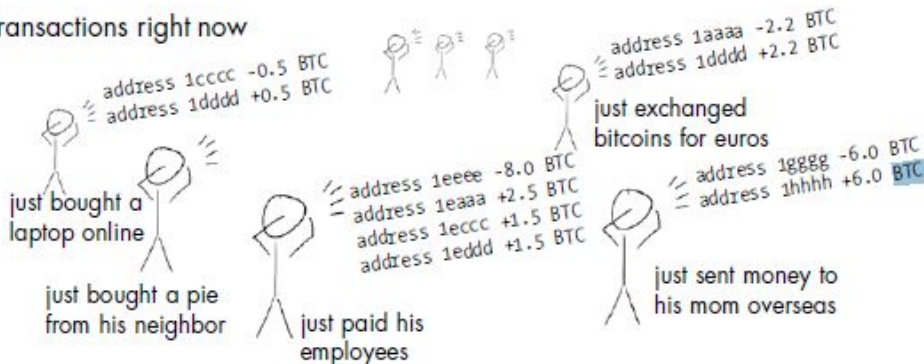
Transactions from
about 20 minutes ago

```
transaction ID: 734
address 1bbbb -0.2 BTC
address 1aaaa +0.1 BTC
address 1ffff +0.1 BTC
transaction ID: 735
address 1gggg -0.1 BTC
address 1hhhh +0.1 BTC
transaction ID: 736
address 1aaaa -1.0 BTC
address 1abcd +1.0 BTC
⋮
```

Transactions from
about 10 minutes ago

```
transaction ID: 1100
address 1eeee -9.0 BTC
address 1cccc +4.8 BTC
address 1ffff +0.1 BTC
address 1aaaa +0.1 BTC
address 1abcd +4.0 BTC
transaction ID: 1101
address 1gggg -0.1 BTC
address 1hhhh +0.1 BTC
⋮
```

Transactions right now



Block will be added
to the chain soon

```
transaction ID: 1544
address 1gggg -6.0 BTC
address 1hhhh +6.0 BTC
```

Mining

- Mining is the process of collecting transactions and adding them to the blockchain
- Verify transactions
 - Prevents double spending
- Create new currency

Bitcoin Mining Process

1. Miner gathers transactions into a 1MB block
2. The Miner attempts to solve a difficult cryptographic hash function
 - a. Result of the hash must have a certain number of 0's
 - b. Nonce
 - i. Field input into the SHA256 hash function in order to get the required # of 0's
 - c. Includes using hash of the previous block
3. If solved, the miner gets to add their block to the blockchain
4. If someone else solves it first, you start over.
5. All other nodes/miners are notified, and they verify that the block has the correct "nonce" and its transactions have valid digital signatures
6. If all is good, the block is added to the blockchain and the miner will be rewarded.

Bitcoin Mining Rewards

- Reward for adding a new block
 - Transaction fees
 - Currently 12.5 BTC
 - Every 210,000 mined, the reward will be halved
- Currently 16,574,963 of 21,000,000 mined

Mining (Proof of Work)

- A miner completes a computationally intensive task
- Only the first miner to complete the task will be rewarded
- Easy to verify that the miner solved the task

Mining (Proof of Stake)

- The supply of currency already exists
 - Only transaction fees are rewarded
- Miners must deposit some coins as collateral
- The miners bet on the block that they think is valid
- The block with the most coins wins
- Easier to compute than POW

How To Mine Bitcoin



How To Mine Bitcoin

- Fun Fact: Need at least a device with 4.4×10^6 GH/s to mine 1BTC/day
 - Average computer has about 0.2 GH/s
- Personal Desktop Mining
- ASICS
- Mining Pools
- Cloud Mining
 - Mining Contracts
 - <https://www.genesis-mining.com/>

Buying & Selling Bitcoins

- Wallets
 - Coinbase
- Exchanges
 - Gemini
 - Gdax
 - Bittrex
- Peer-to-Peer

How to Keep Your Coins Safe





1. Never leave any large amount of cryptocurrency in online exchanges
2. Always use the highest security options available
 - a. 2FA
 - b. SMS
3. Use desktop wallets for medium term storage
4. Use paper/hardware wallets for long term storage
5. Never trust that your address can be used more than once

Alt Currencies: Ethereum

- Blockchain Platform
- Turing Complete Language
 - Build new Ether based blockchains easily
- Smart Contracts
 - Code to facilitate and enforce contracts
 - ICO
- Fast Transactions



Other Alt Currencies

1. Litecoin 
2. Ripple 
3. Monero 
4. Lisk 

Thanks!