Based on “Bitcoin Tutorial” presentation by Joseph Bonneau, Princeton University

Bonneau slides marked “JB”
Bitcoin Snapshot: October 2, 2015

Bitcoin is a combination of several things: a currency, a payment system, and a collection of algorithms and software implementations.

The goal of bitcoin is to enable payments with low transaction costs. Bitcoin can also sometimes provide anonymity.

One bitcoin (BTC) is worth about $238. (A year ago: $394.)

Approximately 14 million bitcoins have been created (mined) to date, for a total value of approximately $3.5 billion.
Double spending: why ecash is hard

Alice

Bob

Charlie

BANK

Signₐ(Transfer X to Bob)

Redeem X?

Signₐ(Transfer X to Charlie)

Redeem X?

Sign₂(Transfer X to Alice)
Solution: Maintain a global public append-only log

The block chain – a public ledger of all transactions.

(In Bitcoin, the log is extended in increments of blocks, each of which may contain thousands of transactions.)
Getting started

Download software to create a Bitcoin wallet (see https://bitcoin.org/en/choose-your-wallet)

The wallet holds the private keys you use to prove you own specific Bitcoins.

The software creates public/private key pairs for you as needed. For each pair, there is a corresponding bitcoin address, which is a 160-bit hash of the public key. Bitcoins are sent to addresses.

The wallet also contains software that allows you to send and receive bitcoins. You send bitcoins by registering your payments in the block chain, which is bitcoin’s public ledger containing all transactions since the beginning of bitcoin.

bmm
Bitcoin Core (original) wallet on first start-up
Send
Spending a Bitcoin

A transaction is of the form “send these Bitcoins from address Y to address Z”

Specific Bitcoins are described as outputs of previous transactions.

The transaction is signed with the private key of address Y and broadcast, along with the public key of Y, to the payment network.

A transaction might also include a transaction fee, to be described later.
Bitcoin mining

Every ten minutes, one lucky Bitcoin miner earns a reward for extending the block chain by one block.

In 2009, the reward was 50 BTC. Today it is 25 BTC. (See https://blockchain.info/q to issue queries about the block chain.)

Mining is the only mechanism for creating new bitcoins. The total number of Bitcoins will never exceed 21M.

The rewarded miner also receives all (optional) transaction fees in the block.
How is a new block created?

A Bitcoin miner creates a block by

(1) Gathering a set of pending transactions, possibly prioritizing those with transaction fees
(2) Verifying the transactions
(3) Solving a hashing problem

On October 3, 2015, according to https://blockchain.info/q, average number of transactions per block is 411, current number of pending unconfirmed transactions is 2495.
How is a transaction verified?

“send these Bitcoins from address Y to address Z”

The miner first checks the signature using the public key for address Y.
- compute hash of public key for Y, which should be Y
- check signature of transaction using public key for Y

Then the miner checks the public ledger to verify that Y hasn’t already sent these Bitcoins to someone else.
The Hashing Problem

To extend the blockchain, a miner creates a new block, containing:

(1) hash of previous block
(2) new transactions to include in the blockchain, including transactions fees
(3) creation of reward bitcoins (e.g., 25 new BTC)
(4) nonce

Block is valid if hash of (1)-(4) ends in enough zeroes, as determined by current difficulty. Miner has to find the right nonce by trial and error!

Difficulty chosen so that the time until the first miner wins is about ten minutes, on average.
Why use a proof of work scheme to pick the winning miner?

Why not just hold a lottery and choose a miner at random?

Have to solve the Sybil problem: What if one person enters the lottery many times?

The proof of work scheme makes it difficult for one party to “enter the lottery so many times” that they can take control of the block chain.
Difficulty adjustment

Bitcoin Block Generation Time vs Difficulty

- Block Generation Time (2009)
- Block Generation Time (2016)
- Estimated Next Difficulty
- Difficulty

10 minutes

2 weeks
Mining rewards

Graph showing the total Bitcoin (BTC) in existence over time. The graph indicates a logarithmic increase in the number of BTC, with specific points labeled for 50 BTC/block and 25 BTC/block. The x-axis represents blocks and time, starting from 2009 and progressing to +4 years in increments of 8 years. The y-axis represents the total BTC in existence, ranging from 10.5M to 21.0M. The total supply of 21 million BTC is approached but not reached, with the supply gradually decreasing from a peak of 12.5 BTC/block to 0.78125 BTC/block as time progresses.

Courtesy: Brian Warner
Total network capacity

- $9 \times 10^{18}$ hashes per block (every 10 minutes!) on average, based on difficulty level on October 3, 2015
- $2^{75}$ hashes in 2013
  - In exchange for $\sim$US$250M
- Consuming $> 100$ MW
Transaction costs

Assuming one BTC is worth $400, reward (25 BTC) per block is $10,000. (Transaction fees negligible today.)

Today number of transactions per second is about 2, number per block is about 1200.

Reward per transaction is about $8.33 !!!!

Cost of electricity spent mining is probably close to reward.

Fundamental problem: 1MB limit on block size implies at most 10 transactions per second.
Transaction Confirmations

A transaction is said to have received \( k \) confirmations if it has been published in a block that has been added to the blockchain, and \( k-1 \) more blocks have also been added.

A transaction is typically considered “confirmed” once it has 6 confirmations.

Newly minted Bitcoins are typically considered confirmed once they have received 100 confirmations.
## Transaction confirmation (~6 blocks)

### My Wallet

**Be Your Own Bank.**

- **Wallet Home**
- **My Transactions**
- **Send Money**
- **Receive Money**
- **Import / Export**

### Transactions

**Summary of your recent transactions**

<table>
<thead>
<tr>
<th>To / From</th>
<th>Date</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Today 10:27:48</td>
<td>26 Confirmations</td>
</tr>
<tr>
<td></td>
<td>2014-02-13 21:57:14</td>
<td></td>
</tr>
<tr>
<td>1Bhv6XjXBrrlvcATHwwLMscZ5xJm9Fspn</td>
<td>2014-02-13 21:21:57:17</td>
<td>0.00000001 BTC</td>
</tr>
<tr>
<td></td>
<td>2014-02-13 21:24:17</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2014-02-13 21:15:17</td>
<td></td>
</tr>
<tr>
<td>1Enjoy1C4bYBr3tn4sMKxvYDqG8NkdR4Z</td>
<td>2014-02-13 10:15:17</td>
<td>0.00000001 BTC</td>
</tr>
<tr>
<td></td>
<td>2014-02-13 10:17:17</td>
<td></td>
</tr>
<tr>
<td>1SochiWwFFySjQo2biVfXn8NRPCSQC</td>
<td>2014-02-13 10:17:17</td>
<td>0.00000001 BTC</td>
</tr>
</tbody>
</table>
A fork can occur when two miners publish blocks simultaneously. Such blocks are almost always in conflict.
Effort spent on a fork that eventually loses is wasted.

Give reward to X.

Give reward to Y.

Give reward to Z.
To break ties, choose branch with greater number of zeros in hash.

\[
\text{SHA-256}(\text{Block}_{N-1}, n) = 0x00000000000046a3f89...
\]

\[
\text{SHA-256}(\text{Block}_{N-1}, n) = 0x00000000000000008c71...
\]

- Give reward to X.
- Give reward to Y.
- Give reward to Z.
More generally, longest chain wins.

Where length is measured in terms of sum of difficulties (number of zeroes in hashes) of blocks in chain.
Bitcoin mining hardware

TerraMiner™ IV – 2TH/s Networked ASIC Miner
$5,999
Shipping June 2014

300 GH Bitcoin Mining Card
The Monarch BPU 300 C
$1,497.00

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.
Mining pools

A miner creates a new block assigning reward and transaction fees to the pool.

Every miner “proves” to the pool how much effort has been expended by submitting the hash with largest number of zeros.
At times in the past, one pool, Ghash.IO had over 51% of the computing power.

51% attack: If one guild has more power than all others combined, they can extend their fork faster than any other fork, reaping all rewards and transaction fees, and choosing which transactions to confirm.

https://blockchain.info/pools
Why does Bitcoin have value?

Consensus

- Consensus in state (blockchain)
- Consensus in payment
- Consensus in rules
Price during 2013
Black Markets

Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace
Nicolas Christin. WWW 2013
E-commerce

Payment Information

Credit / Debit card
- Visa
- Mastercard
- American Express
- Discover

Card Number *

Expiration Date *
01 Jan 2014

PayPal
The safer, easier way to pay.

Learn More

Learn More

What's this?

Learn More

Why Can't I Use a Gift Card?
Bitcoin exchanges – buy and sell bitcoin using different currencies

Beware the middleman: Empirical analysis of Bitcoin-exchange risk
Tyler Moore and Nicolas Christin, Financial Crypto 2013
Physical Bitcoin (a gimmic?)

private key is embedded in coin and can be accessed (possibly electronically) only by physically breaking the coin.

trust creator to destroy any record of private key.

http://media.coindesk.com/2014/09/casascius-coins.jpg
Anonymity?

A transaction history is recorded for every Bitcoin

Key to anonymity is to avoid tying any personal information to your Bitcoin addresses

Use an address only once

Self-mined Bitcoins, using an anonymizing network to connect to the payment system, are hardest to trace
Mixes
Mixes today

Caution: Mixing services may themselves be operating with anonymity. As such, if the mixing output fails to be delivered or access to funds is denied there is no recourse. Use at your own discretion.

- The Bitcoin Wiki

An inquiry into money laundering tools in the Bitcoin ecosystem Möser, Malte, Rainer Böhme, and Dominic Breuker, ECRIME 2013
Bitcoin in the news

In the news

- BitPay reports a theft of 5,000 BTC and is suing its insurer for declining to pay a $1 million settlement.
- Mark Karpeles (pictured) is charged with embezzling ¥321 million from Mt. Gox customers.
- Shaun Bridges pleads guilty to stealing $820,000 from the Silk Road.
- A flash crash on Bitfinex brings a low of $162 before quickly recovering.
- Bitcoin Core 0.11 is released.

Ongoing: Block size limit controversy

https://en.bitcoin.it/wiki/Main_Page