Bitcoin

What is Bitcoin?

Online Cryptocurrency

Based on Blockchain

Created by Satoshi Nakamoto

Why BitCoin?

Global - usable from any location

Decentralized - not controlled by anyone

Anonymous - not tied to your identity

Cheap - minimal fees

Transparent - every transaction is shared across the network

Free - no government or organizational backing

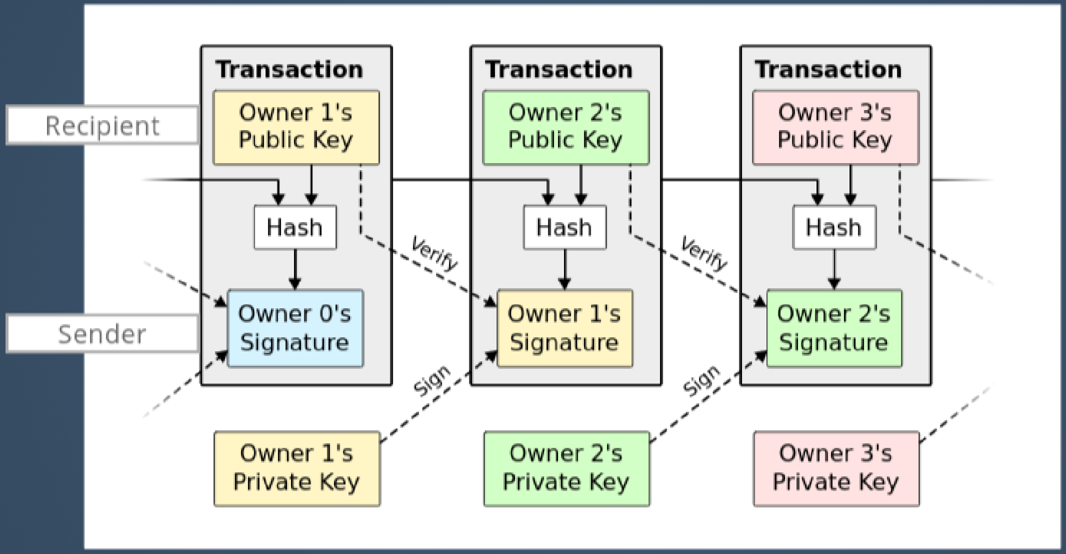
Transaction

Alice can send Bob BTC by sending them to his public key

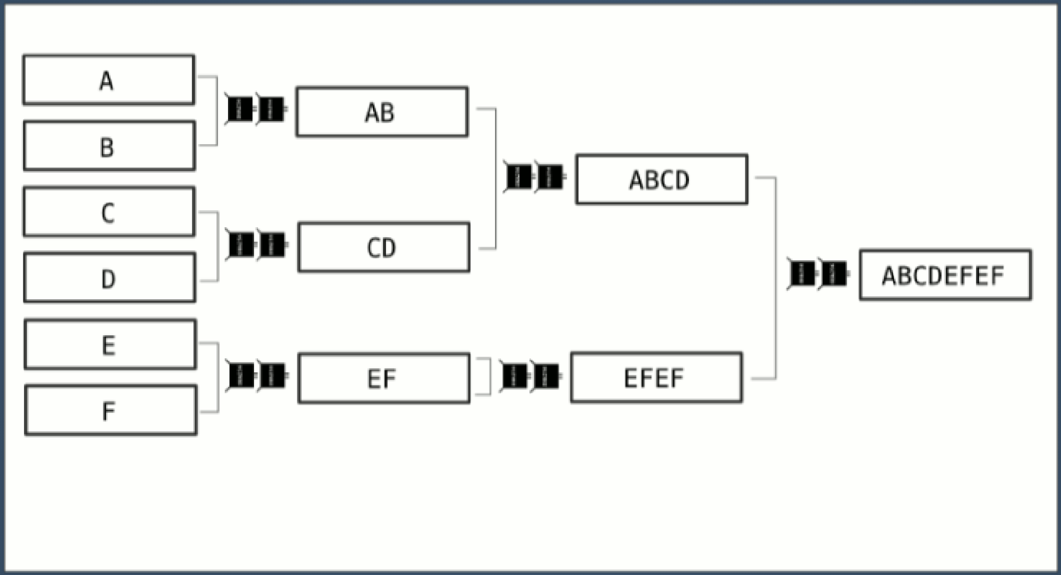
Her transaction is broadcasted to other nodes network, where it is verified

If verified, transaction gets added to the public open ledger on the newest block

Transaction

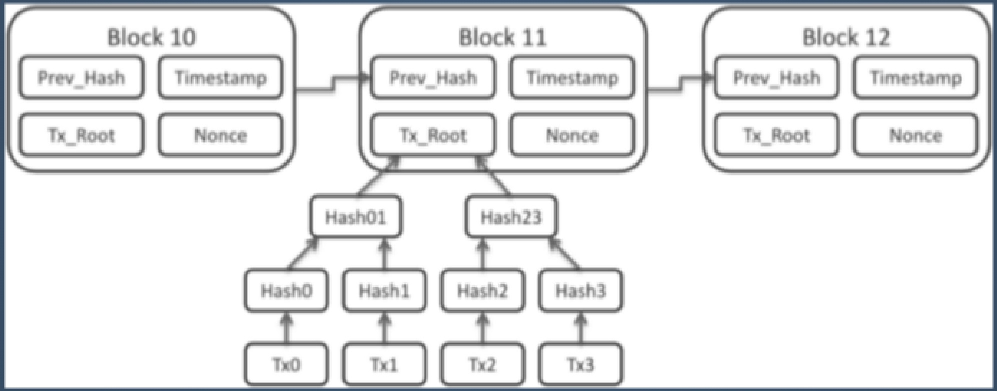


Merkle Tree

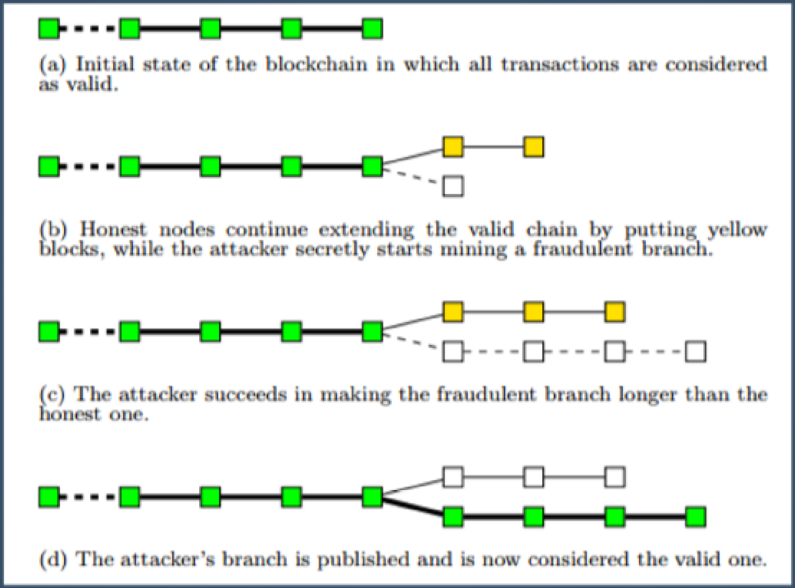


Blockchain

Distributed database



Double Spending



(a) Initial state of the blockchain in which all transactions are considered as valid.

(b) Honest nodes continue extending the valid chain by putting yellow blocks, while the attacker secretly starts mining a fraudulent branch.

(c) The attacker succeeds in making the fraudulent branch longer than the honest one.

(d) The attacker's branch is published and is now considered the valid one.

Gold Mining

It looks easy in cartoons...

It's

a

BIT

hard

It's all electronic

3 options to mine for bitcoins:

A) CPU

Or enhance the performance:

B) CPU + GPU

C) ASICs & FPGAs

Customized devices exclusively for mining.

AntMiner S7

Advertised Capacity:
4.73 Th/s

AntMiner S9

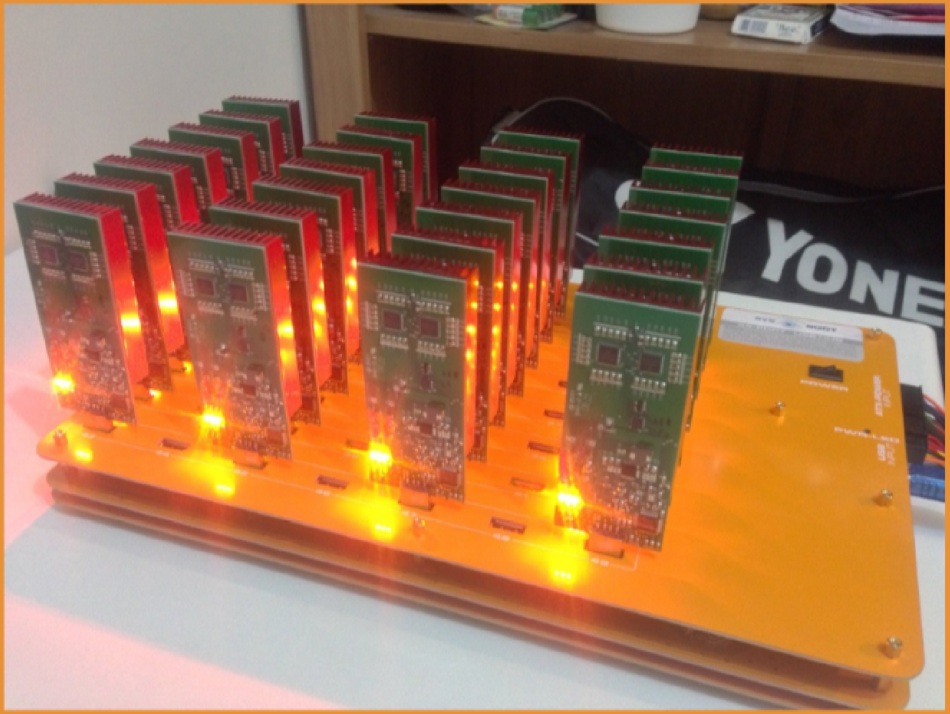
Advertised Capacity:
13.5 Th/s

Avalon6

Advertised Capacity:
3.5 Th/s

TOCK

Start your own cluster



or join a pool

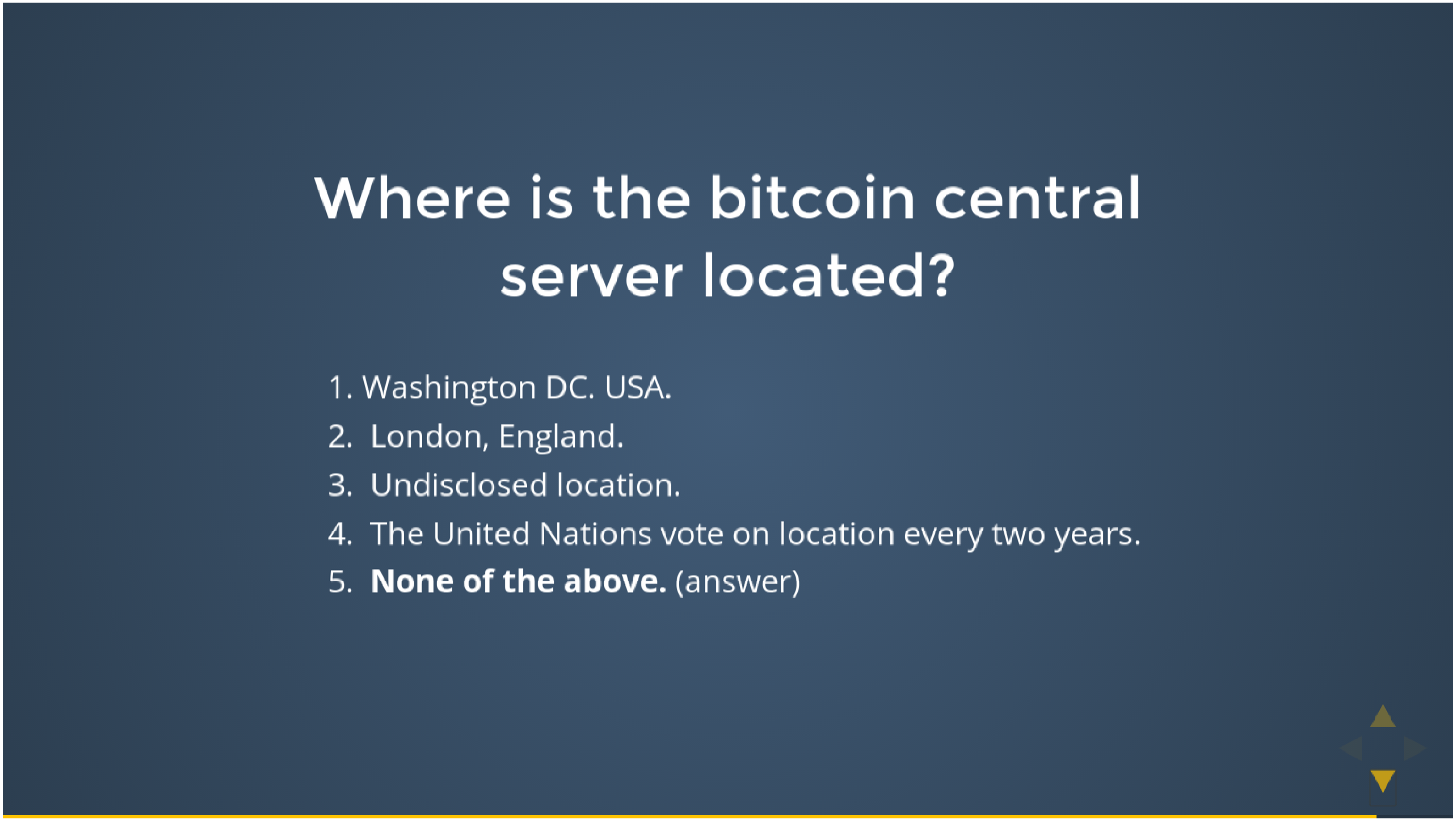
There will be only 21 M of BTC. Why?

- By design and determined by the protocol code.
- Described feature - makes supply of money predictable and independent of human decisions.
- Possible reasons to have exactly 21 M:
    - Volume of the gold mined.
    - 50 BTC as first reward for mining.

Security Challenges

The bitcoin protocol itself can be secure enough, but this doesn't extend to all the sites and services that deal with bitcoin, some examples are:

- BTC wallet service being hacked.
- Attack on BTC exchange services.
- "Pony" Botnet.
- 51% attack.
- Lost password.



Where is the bitcoin central server located?

1. Washington DC. USA.
2. London, England.
3. Undisclosed location.
4. The United Nations vote on location every two years.
5. **None of the above.** (answer)

Does the geographical location matter for bitcoin miners?

Yes, for example it electric bills cost less to run machines in china.

How many bitcoin will ever be created?

1. Unlimited.
2. 77,340,109.
3. 21 million but can be adjusted by the Bitcoin Foundation by majority vote.
4. **21,000,000.**(answer)
5. The Square root of 2^2.