



Blockchain foundations

Module 1 (part 1)

Outline

- What is a blockchain? (paper blockchain)
- What is decentralization?
- The technical side
 - Public key cryptography
 - Cryptographic Hash function
 - Digital signature
 - ...

Part 1

What is a blockchain?

- A blockchain is a growing list of records, called blocks, which are linked using **cryptography**. Each block contains a cryptographic **hash** of the previous block, a timestamp, and transaction data run over a P2P network in a **decentralized** manner...

Explain the blockchain to me simply

For instance, if John Smith sells his house at 123 Sunshine Blvd, Arlington, VA 22011 to Mary Anderson on November 5, 2018 for \$100,000.00 and record this transaction on a blockchain, no one would be able to change this fact, and no one would be able to dispute the title transfer to Mary Anderson from John Smith.

And that's why The Economist calls blockchain a "TRUST Machine".

- Why in current technologies is easy to do data tampering?

What is a blockchain?

[Source from ConsenSys]



Satoshi Nakamoto's Bitcoin Whitepaper



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of

```
bitcoin-0.1.0.rar  
bitcoin-0.1.0.tgz
```

[The brief history of blockchain](#)

What is decentralization?

[Source from ConsenSys]

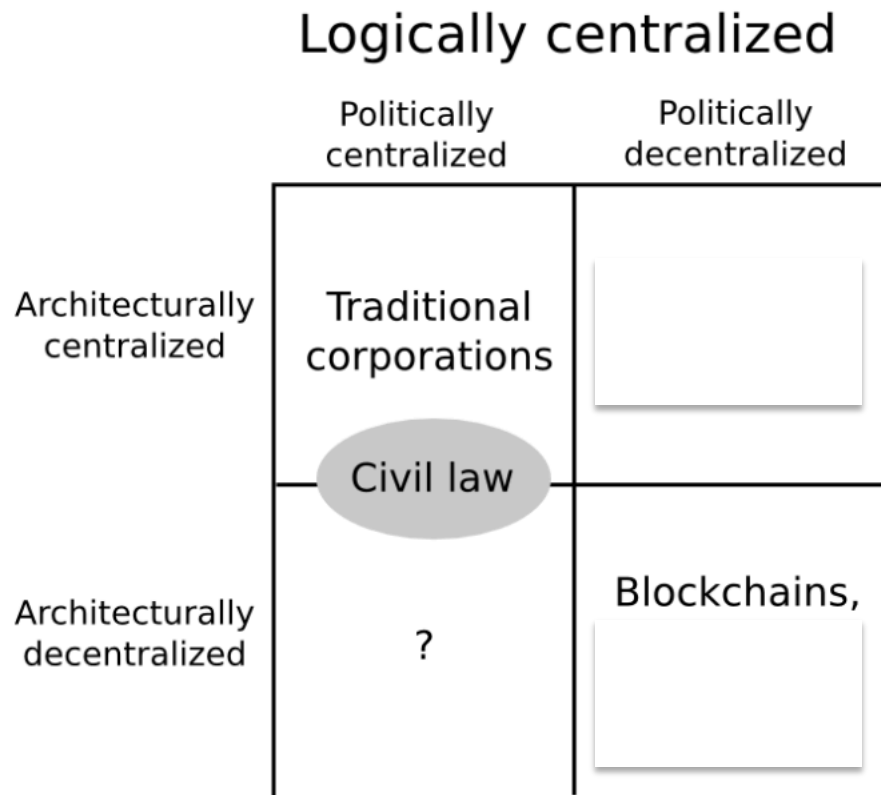


Decentralization has become
Synonymous for Blockchain. **But is it
true?**

Three types of decentralization

- **Architectural (de)centralization** — how many physical computers is a system made up of? How many of those computers can it tolerate breaking down at any single time?
- **Political (de)centralization** — how many individuals or organizations ultimately control the computers that the system is made up of?
- **Logical (de)centralization** — do the interface and data structures that the system presents and maintains look more like a single monolithic object, or an amorphous swarm? One simple heuristic is: if you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?

What type(s) of decentralization blockchain is?



Blockchains are
politically decentralized
(no one controls them)
architecturally decentralized (
no infrastructural central point of failure)
but they are logically centralized
(there is one commonly agreed state and the
system *behaves* like a single computer)

Why should people care about
decentralization?

~10,000 reachable nodes

<http://bitnodes.earn.com/>

GLOBAL BITCOIN NODES DISTRIBUTION

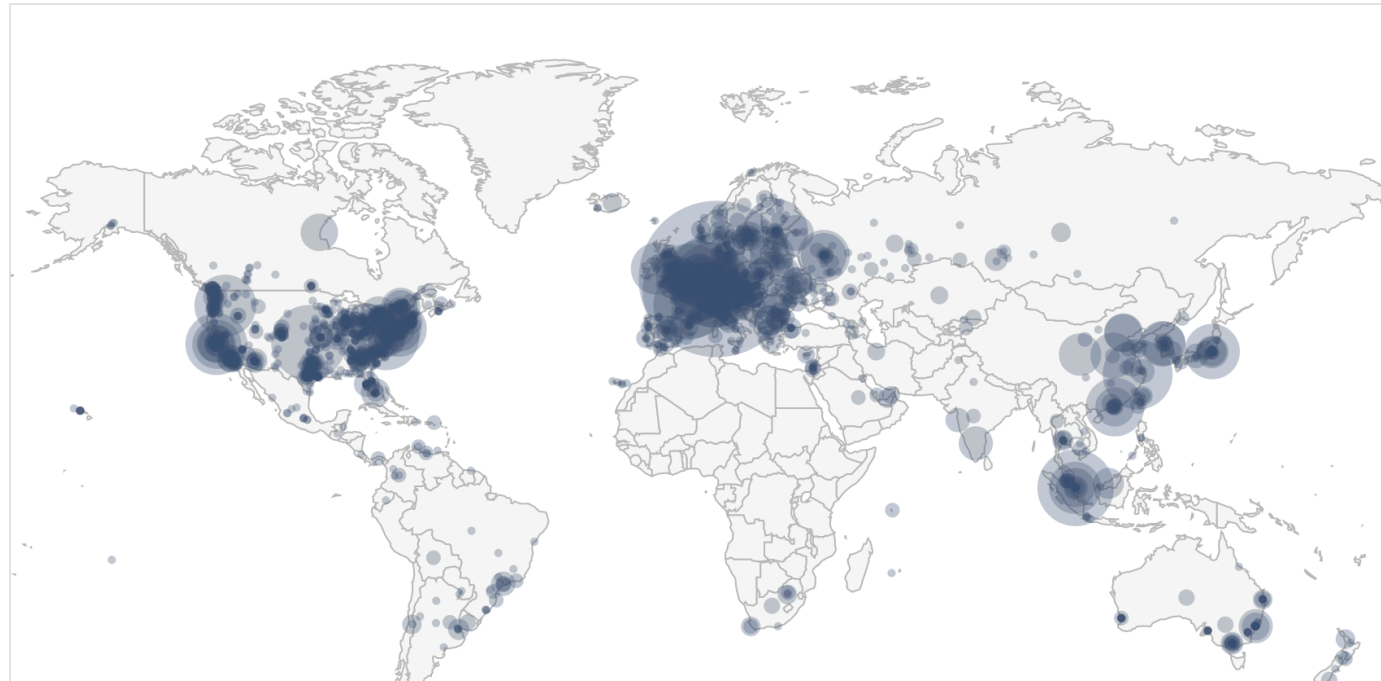
Reachable nodes as of Sat Sep 28 2019 13:51:53
GMT-0400 (Eastern Daylight Time).

9641 NODES

[24-hour charts »](#)

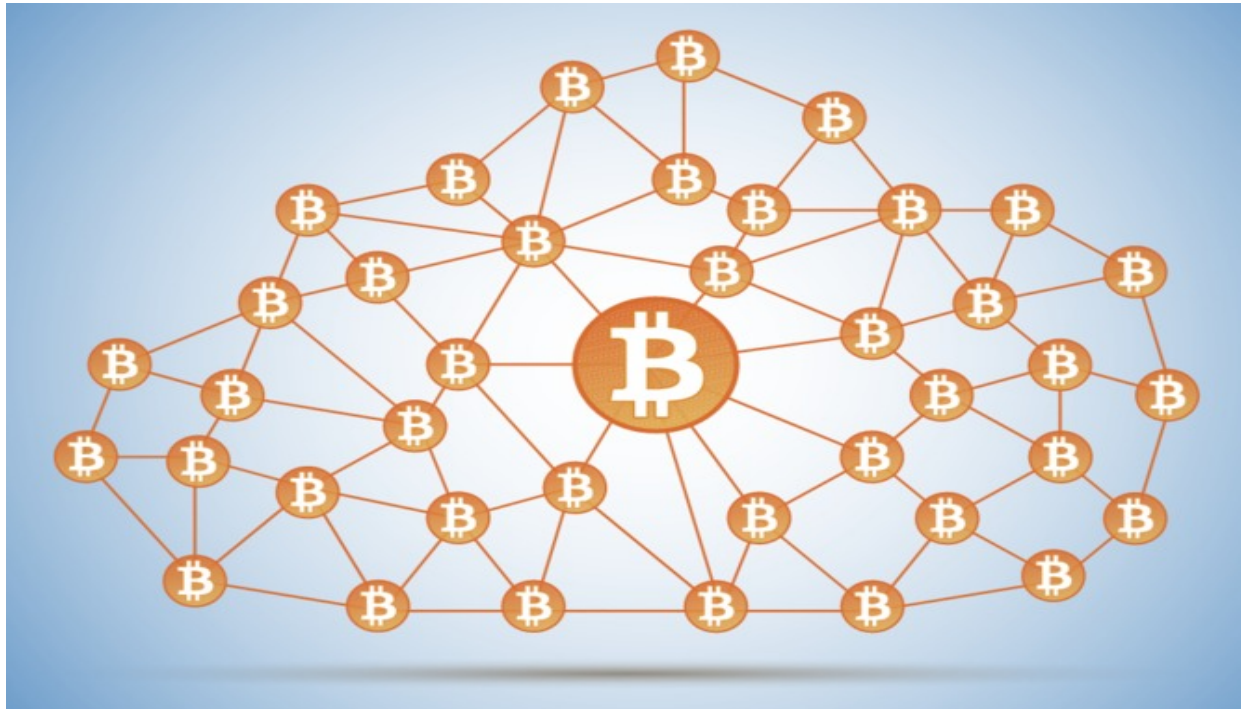
Top 10 countries with their respective number of
reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2433 (25.24%)
2	Germany	1947 (20.20%)
3	France	614 (6.37%)
4	Netherlands	507 (5.26%)
5	China	335 (3.47%)
6	Singapore	331 (3.43%)
7	Canada	325 (3.37%)
8	United Kingdom	323 (3.35%)
9	Russian Federation	252 (2.61%)



How to become a Bitcoin node?

- Running a full node (Bitcoin Core software): [link](#)



That's what makes it decentralized

How to become a Bitcoin miner?

- Running a node is different than [Bitcoin mining](#)
- Learn how to mine Bitcoin: [link](#)

Does blockchain hold the balance?

- no

Blockchain Explorer

BLOCKCHAIN					Products	Data	Q	Login	Sign up
Blocks					Transactions				
Height	Age	Transactions	Miner	Size (KB)					
557229	7 minutes	1212	Unknown	1,105,458					
557228	8 minutes	2754	AntPool	1,334,458					
557227	21 minutes	3674	BTC.com	1,251,623					
557226	25 minutes	3125	BTC.com	1,262,634					
557225	1 hour	2607	BTC.TOP	1,240,323					

<https://www.blockchain.com/explorer>

Why study blockchains and computer security?

- Optimistic: a chance to build security into new platforms from the start
 - Cryptocurrencies are open systems, exciting platforms for experimenting
- Cryptocurrencies encourage DIY security,
“be your own bank”

More Resources

https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

