

CAN304

Computer Systems Security

Lecture 9+. Blockchain

2022-04-29, 14:00-16:00, Friday

Jie Zhang
Department of Communications and Networking
Email: jie.zhang01@xjtlu.edu.cn
Office: EE522

Outline

- Blockchain foundations
- The technical side
- Blockchain in use

Part 1. Blockchain foundations

- The brief history of blockchain
- What is decentralization?
- Distributed ledgers and consensus

The history of blockchain

- It all starts in the 1990s with Stuart Haber and W. Scott Stornetta
- How to keep the past secure, and keep digital information safe and resistant to tampering?
- 1991
- Stuart Haber and W. Scott Stornetta
- Published the first paper to outline the use of a chain of cryptographically secured blocks to preserve the integrity of past information and protect it.

Haber S., Stornetta W.S. (1991) How to Time-Stamp a Digital Document. In: Menezes A.J., Vanstone S.A. (eds) Advances in Cryptology-CRYPTO' 90. CRYPTO 1990. Lecture Notes in Computer Science, vol 537. Springer, Berlin, Heidelberg

The history of blockchain

- 1993
- There's too much spam!
- The concept of proof-of-work was established, seeking to provide countermeasures to spam and other network abuses.

Dwork C., Naor M. (1993) Pricing via Processing or Combatting Junk Mail. In: Brickell E.F. (eds) Advances in Cryptology — CRYPTO' 92. CRYPTO 1992. Lecture Notes in Computer Science, vol 740. Springer, Berlin, Heidelberg

The history of blockchain

- 2008
- Bitcoin is born
- Satoshi Nakamoto, the unknown figure or group behind Bitcoin, publishes the now-famous whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System”
- Note
- Bitcoin is not the only blockchain!
- <https://bitcoin.org/en/>



Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. 2008.

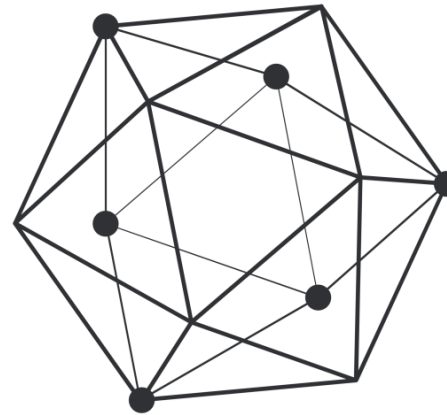
The history of blockchain

- 2014
- Ethereum is born
- Much more than just currency transactions, Ethereum is a blockchain that can also be programmed and run computations. It's a distributed world computer that runs on a blockchain.
- <https://ethereum.org>



The history of blockchain

- 2015
 - Linux Foundation started Hyperledger project to advance cross-industry blockchain technologies.
 - fabric v0.6.0 is released in September 2016
 - fabric v2.0.0-alpha is released in April 2019
 - fabric v2.1.0 is released in April 2020
 - latest version: fabric v2.4
-
- <https://www.hyperledger.org>



The history of blockchain

- Today
- The momentum is growing towards a decentralized future. But why?

Decentralization

- No central authority
- Community members self-sovereign
- Power is shared

- Decentralization benefits
 - Systems are less likely to fail when based on redundant components
 - It's harder to attack a decentralized network, and users aren't all in one place

Decentralization benefits for blockchain

- Decentralization (politically and architecturally) allows blockchains to be:
- Less likely to fail because they rely on many separate components.
- Harder to attack because the networks are spread across many computers.

Distributed ledgers

- Keep copies of the ledger distributed on a network
- There is no one authoritative copy and had specific rules around changing them
- Make the system much more robust and has the added effect of decentralizing the authority



- But, how to make those ledgers work together? How to keep their information and alignment?

Consensus

- In order to keep the distributed ledgers in alignment, protocols must be established for the network to reach consensus on what exactly gets written to those ledgers and if one such ledger it gets changed, these networks should be able to notice the discrepancy and self-correct.

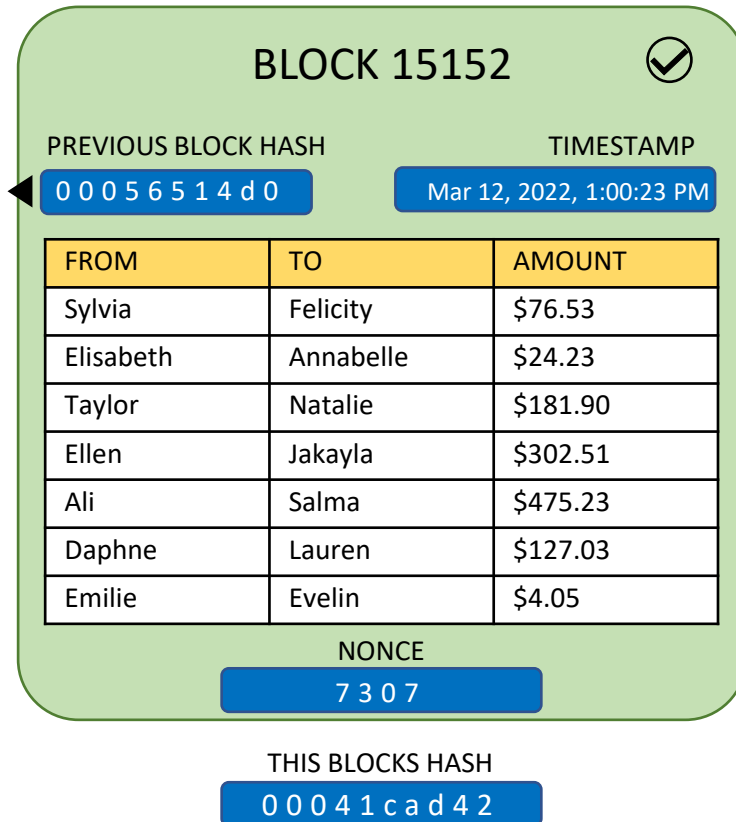


Part 2. The technical side

- Cryptography primitives
- Anatomy of a block
- Nodes and networks

Blocks

- The building blocks of the blockchain.
- The primary purpose of a block is to record transactions.




Bitcoin blocks generally contain around 1500-2000 transactions.

Block sizes are generally limited to prevent network congestion.

Bitcoin blocks are limited to 1MB in size.

Mining

- Block valid if block hash is less than 001000000


BLOCK 15152 

PREVIOUS BLOCK HASH: 0 0 0 9 2 d 1 7 d c
TIMESTAMP: Mar 12, 2022, 1:00:23 PM

FROM	TO	AMOUNT
Emilie	Evelin	\$4.05
Elisabeth	Annabelle	\$24.23
Taylor	Natalie	\$181.90
Ellen	Jakayla	\$302.51
Ali	Salma	\$475.23
Daphne	Lauren	\$127.03
Sylvia	Felicity	\$76.53

NONCE: 8 2 6 3

THIS BLOCKS HASH: 5 3 4 0 f 7 1 5 b c

BLOCK 15152 

PREVIOUS BLOCK HASH: 0 0 0 9 2 d 1 7 d c
TIMESTAMP: Mar 12, 2022, 1:00:23 PM

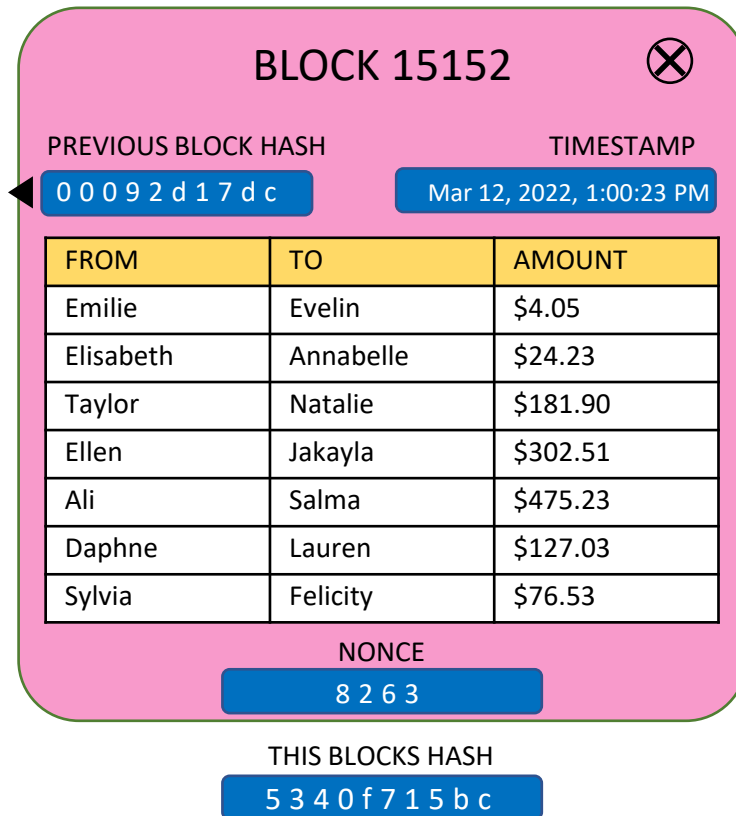
FROM	TO	AMOUNT
Sylvia	Felicity	\$76.53
Elisabeth	Annabelle	\$24.23
Taylor	Natalie	\$181.90
Ellen	Jakayla	\$302.51
Ali	Salma	\$475.23
Daphne	Lauren	\$127.03
Emilie	Evelin	\$4.05

NONCE: 8 2 6 3

THIS BLOCKS HASH: 7 9 0 c 8 e b c 4 9

- A valid block hash would look something like: 000383ec5

Mining

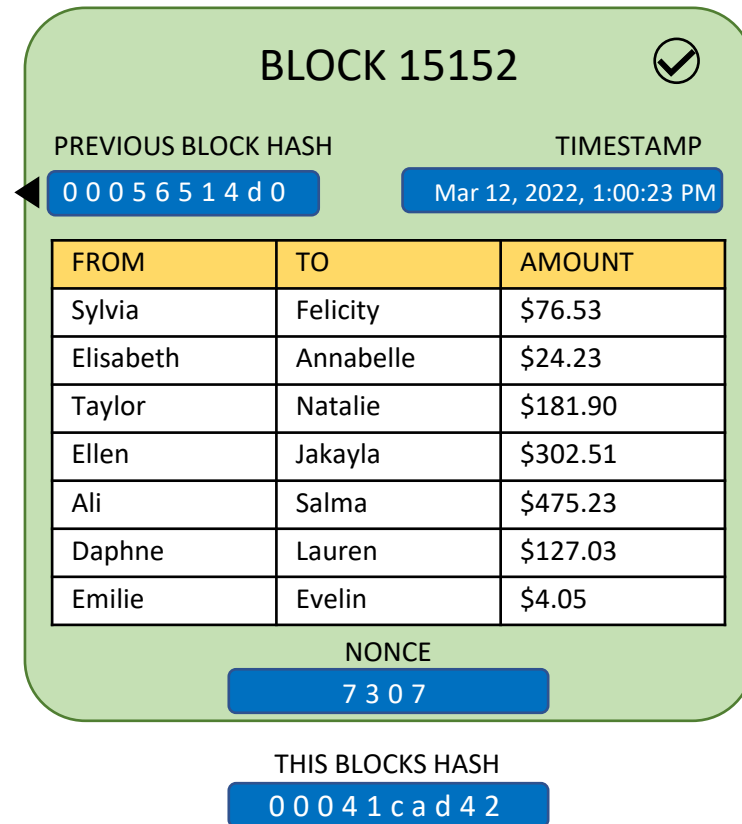


- Hash function outputs are unpredictable. Each digit is like rolling at 16-sided die.
- The odds of our block yielding a hash that starts with three zeroes are the same as rolling three 16-sided dice and getting three 1s. So we'll have to change the data and rehash, over and over again.

- What data can you change in your block?
- This is where the nonce comes in!

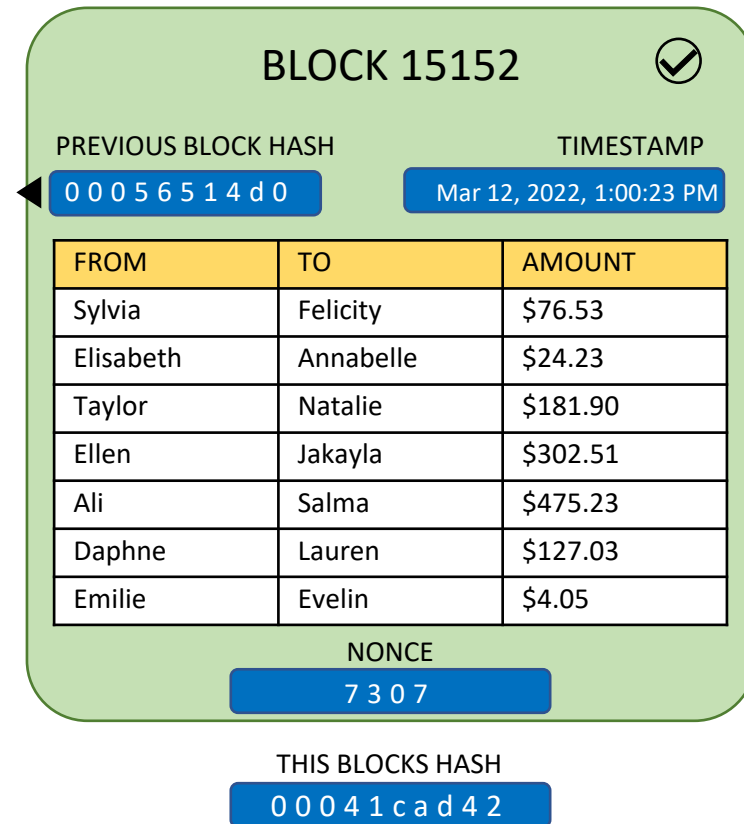
Mining

- This process is purely based on chance!
- But the more computing power you have, the “luckier” you will be.
- We are looking for just 3 zeros at the start of our hash.
- The block hash and matching nonce are in a real sense, “precious”.
- On the bitcoin blockchain, and with the current most powerful mining computer, you could expect to mine a block just once every 40 years.



Mining

- The current reward for finding a block on the bitcoin blockchain is 6.25BTC
- Currently around \$240,000USD!

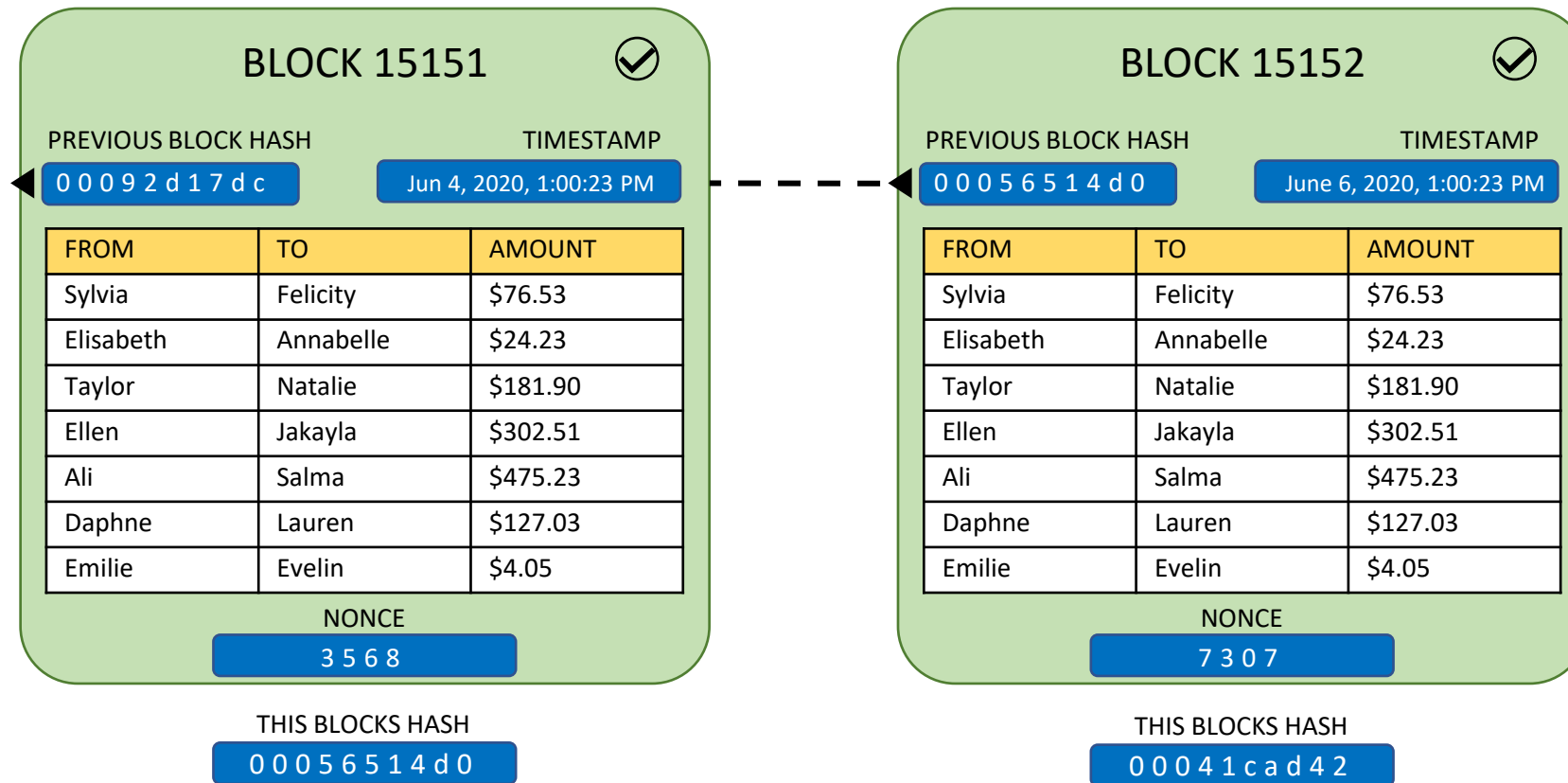


Checking validity

- Checking the validity of a node is easy.
- Other computers on the network just have to hash it. If it's below the difficulty threshold (and all the transactions are valid), they will accept it.

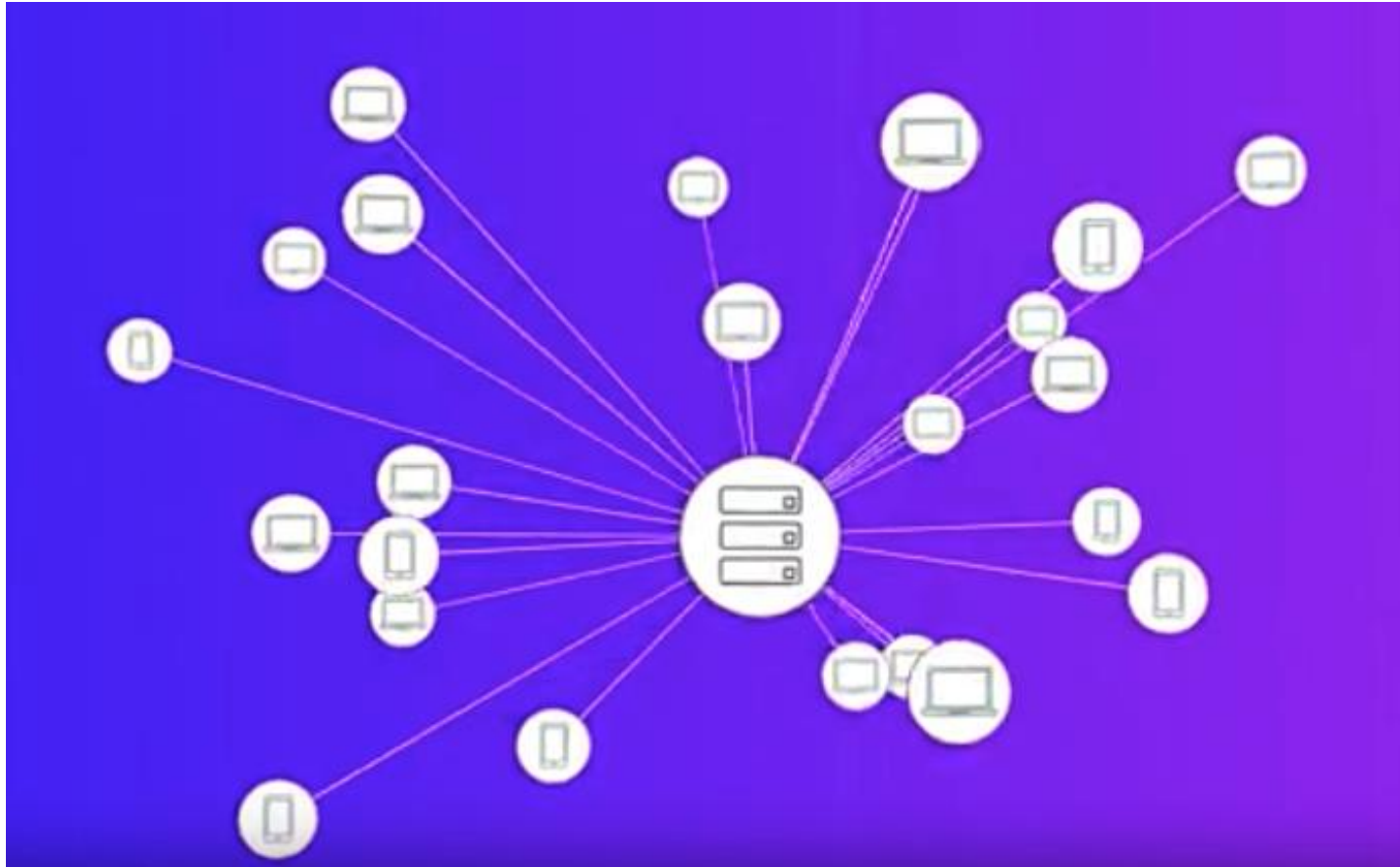
The chain of blocks

- block chain



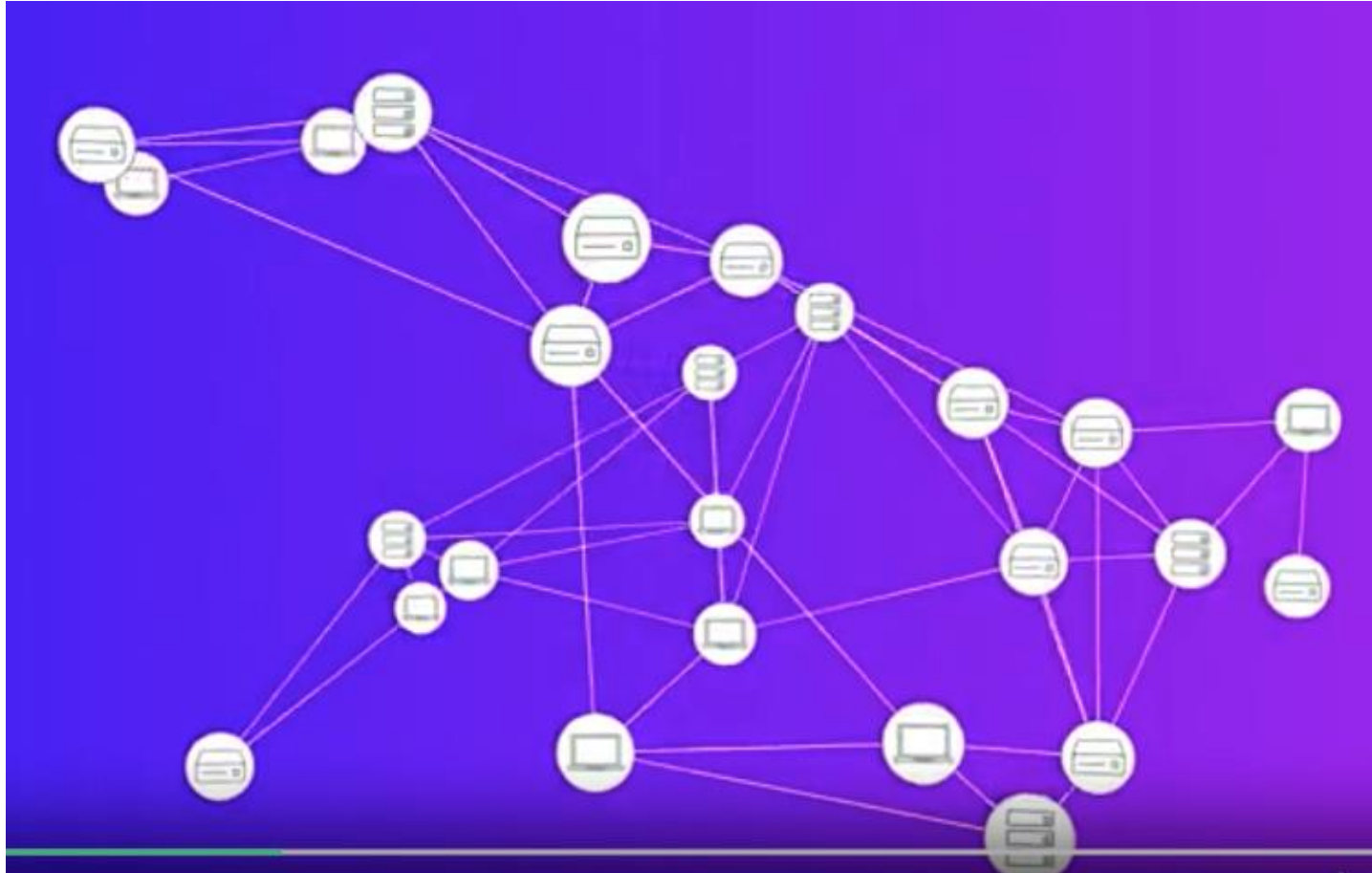
Centralized networks

- Web applications
- client -- server



Distributed networks

- Blockchain



Nodes

- The computers that make up a blockchain network.
- There's nothing special about a node, you could run a node on your computer by downloading and running the software.
- You don't need permission from any authority to take part in the network.

Nodes: gatekeepers

- Nodes are where the data of the blockchain lives. Each node stores a full or partial copy of the blockchain, and communicates with other nodes to verify its accuracy.
- Full nodes
- Full nodes store the entire blockchain and validate every single transaction and block.
- Light nodes
- Light nodes store a recent portion of the blockchain only. They verify blocks and transactions too.

Miners

- Miners are nodes who also do what's called mining.
- They are the ones who are trying to find valid blocks by hashing and rehashing them while changing the nonces. When they find a valid block, they include it in their blockchain and send it to other nodes.

Part 3. Blockchain in use

- Consensus mechanisms and trust frameworks
- Public, private & consortium blockchains

So far

- How blocks are made
 - How blocks are added
 - How nodes communicate
 - How nodes agree, with proof-of-work
 - A valid block
-
- The fact that a block is valid demonstrates proof that work has been done
 - That proof is what nodes use to agree on what makes a valid block.

Consensus mechanisms

- The purpose of a consensus mechanism in a blockchain is to allow a group of separate nodes to distribute the right to update the system according to specific rules, amongst a set of participants, and in a secure way.
- Example
- Proof-of-work

Consensus mechanisms: proof-of-work

- Mining and proof-of-work is a random process. So, each miner is rewarded over time by how much of that random work they do.
- In other words, miners are rewarded in proportion to their share of the network's total computational power.
- Drawbacks
 - This process uses huge amount of energy.
 - Transaction rates and volumes will be lower.
 - Together, those mean higher transaction fees, fees that grow as the network grows.

Consensus alternatives

- Proof of stake
- Delegated proof of stake
- Proof of importance
- PBFT

Proof of stake

- Blocks are forged, not mined.
- Forgers are rewarded for the proportion of stake they have, not proportion of computing power.
- Forgers risk their stake. If they include a bad transaction, they lose it.
- This is a strong incentive to stay honest.

Proof of stake VS proof of work

- Electricity use
- Efficiency
- Speed
- Transaction fees

- Problem of proof of stake
 - Small balance holders
 - With a low balance, it's unlikely this account will ever forge a block.

Kinds of networks

- Bitcoin is public network.
- But there are other kinds!
- Public blockchain
- Consortium (aka shared permissioned) blockchain
- Private (aka permissioned)

Summary

- Blockchain foundations
- The technical side
- Blockchain in use