
# Introduction to Blockchain and Smart Contracts

# A Technical Perspective

*presented by*

**Yi LI**
*Associate Professor*
*College of Computing and Data Science*
*Nanyang Technological University*

# About Me

- A Brief History
  - 2007: B.Comp. (hons) in Computer Science, NUS, Singapore
  - 2011: M.Sc. & Ph.D. in Computer Science, University of Toronto, Canada
  - 2018: School of Computer Science and Engineering, NTU, Singapore

- Research Interests
  - Program analysis, automated reasoning
  - Software verification
  - Software reuse
  - Software security

# Today's Agenda

- Bitcoin Revolution
- Blockchain Primer
- How does blockchain work?
- Blockchain 2.0: decentralized applications

# The Bitcoin Revolution

# What is Money?

**A medium of exchange**
for buying things

**A unit of account**
for pricing

**A store of value**
for saving

**MONEY = VALUE = TRUST**

# Fiat Money

(*Latin fiat - 'let it be done' or 'so it be')*

- **Fiat money**
  - The dollars, or euros, or any other currency for that matter have value because the government orders it to.
- **Drawbacks**
  - It is centralised.
  - It is not limited in quantity (e.g., unlimited QE).

Beigel, O. (2022, January 13). *What is bitcoin? A complete beginner's guide*. 99Bitcoins. Retrieved July 20, 2022 from https://99bitcoins.com/bitcoin/#centralization

# Digital Money and “Double-Spending” Problem

- Digital money is a type of currency available in digital form in contrast to physical, such as banknotes and coins.
  - Allow for instantaneous transactions and borderless transfer-of-ownership
- **Double-spending:** A potential flaw in a digital cash scheme in which the same single digital token can be spent more than once.
- This is possible because a digital token consists of a digital file that can be **duplicated or falsified**.
- Banks’ solution:
  - Keep a computer ledger to keep track of who owns what
    ⟶ **Centralised computer system**

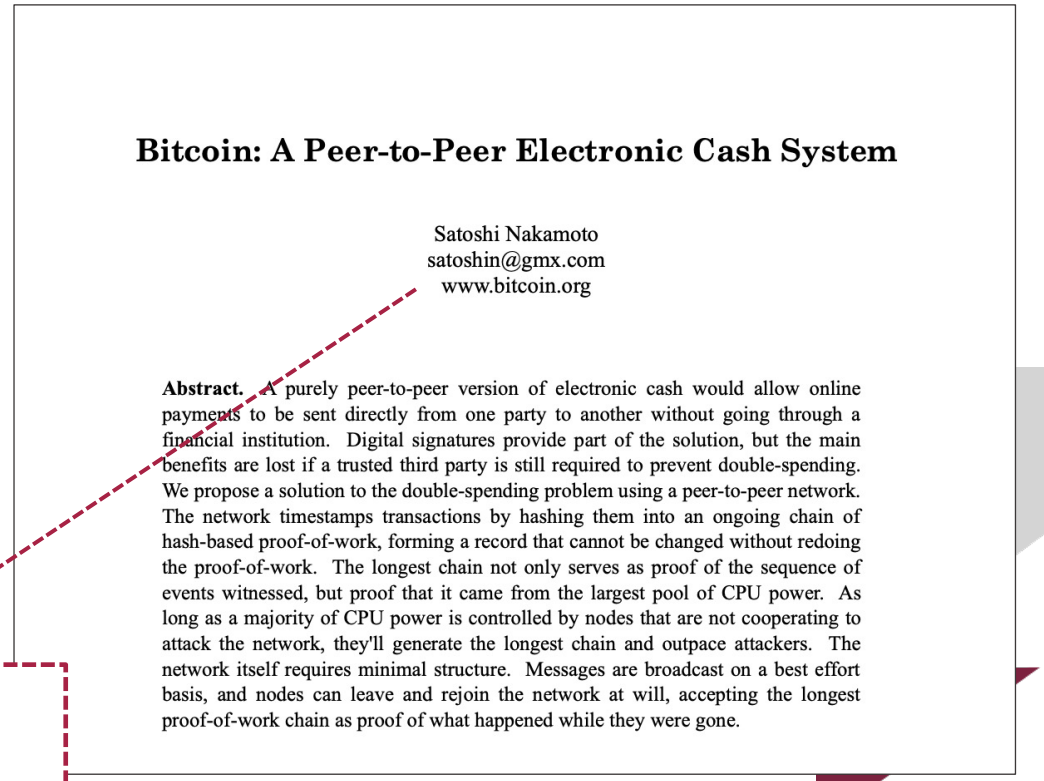


Double-spending. (2022, June 19). In *Wikipedia*. Retrieved July 20, 2022 from https://en.wikipedia.org/wiki/Double-spending

# Hello Bitcoin! (Oct 2008)

Proposed by Satoshi Nakamoto

- A **peer-to-peer (P2P)** electronic cash system
- This system claimed to create **digital money** that solves the **double-spending problem** without the **need for a central authority**.

**Bitcoin: A Peer-to-Peer Electronic Cash System**

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

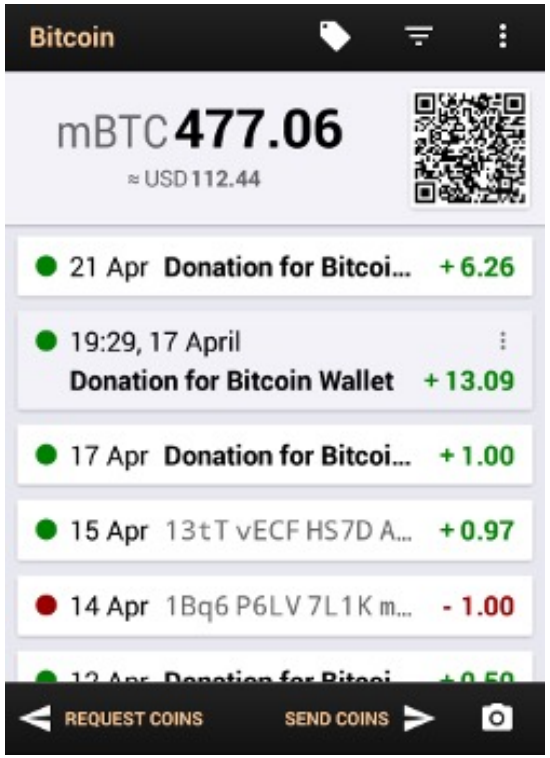
**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

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

Nakamoto, S. (2009). *Bitcoin: A peer-to-peer electronic cash system* [White paper]. Bitcoin. Retrieved July 20, 2022 from https://bitcoin.org/bitcoin.pdf

# Bitcoin Quick Facts

- Bitcoin is a Digital currency (Cryptocurrency) in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central Bank.
- Bitcoin is the first decentralized digital currency.
- Bitcoins are digital coins you can send over the Internet
- Bitcoins are stored in a digital wallet (address)
- Transactions are permanently and anonymously stored over the network



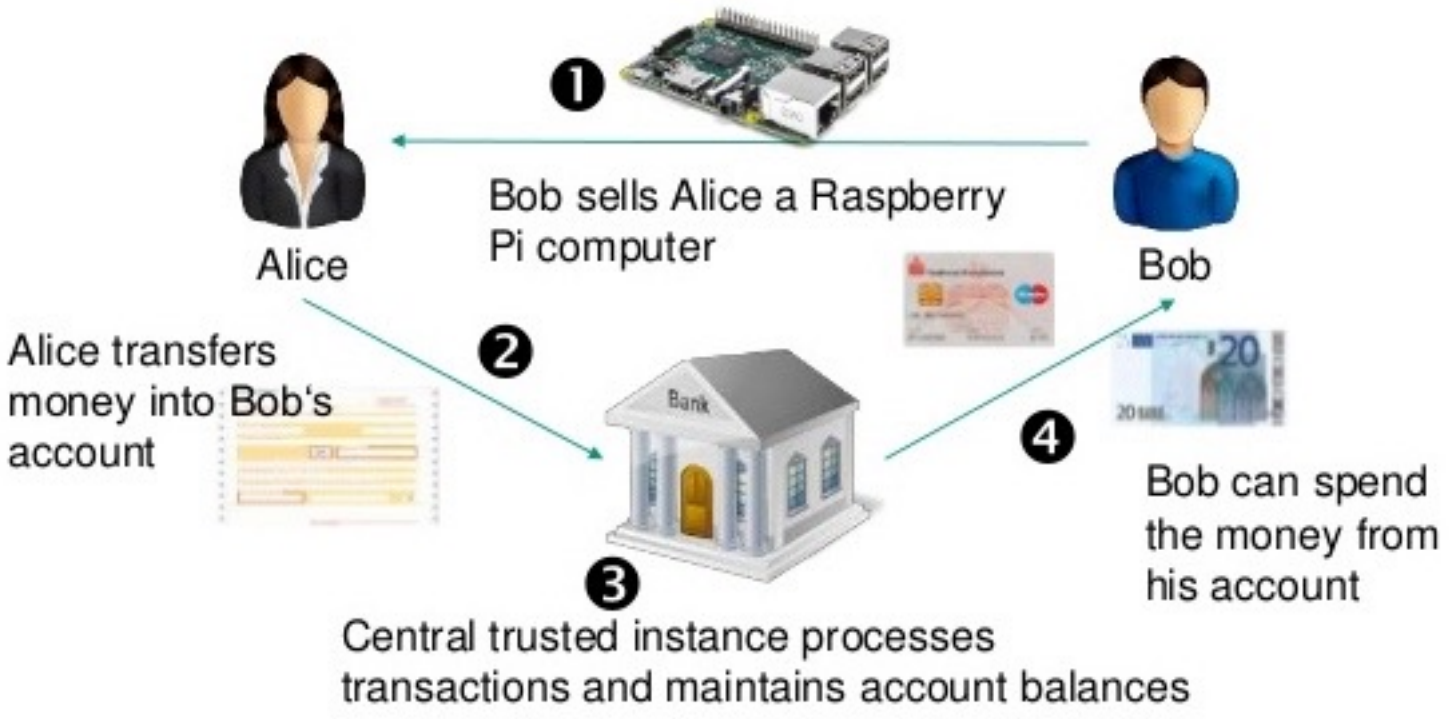
# Bitcoin vs. Bank

Transparent vs. Non-transparent
Decentralized vs. Centralized

# Centralized Ledger

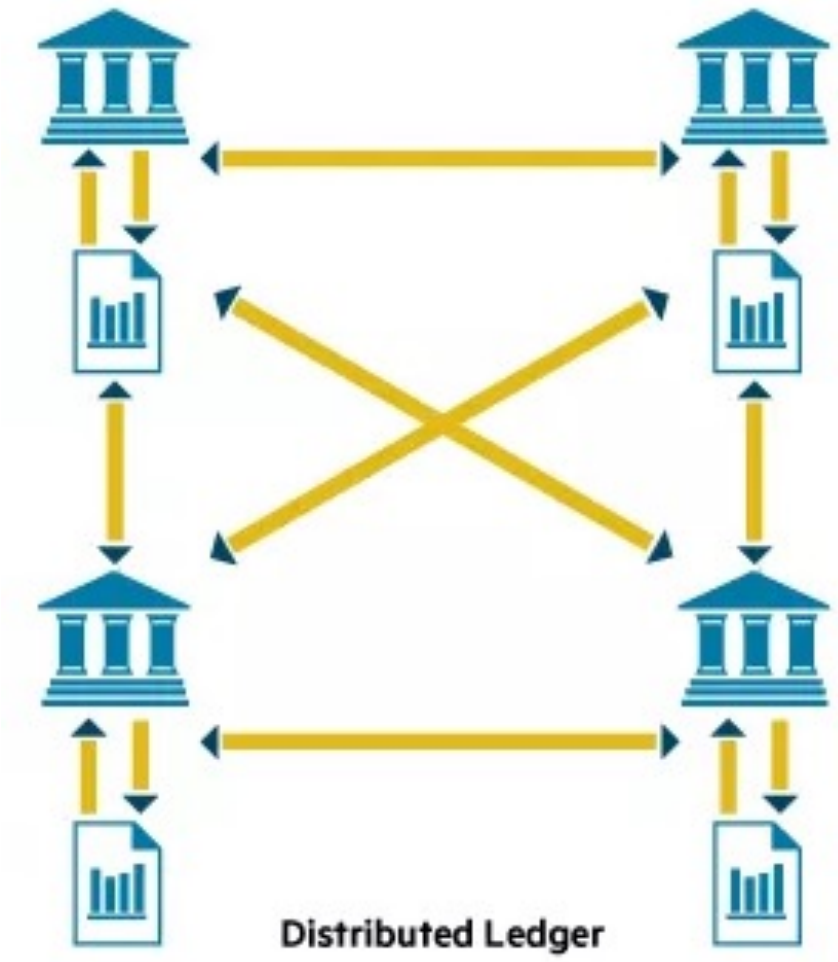
- Record each transaction in a **Ledger**
- Bookkeeper needed

# Centralized Transaction

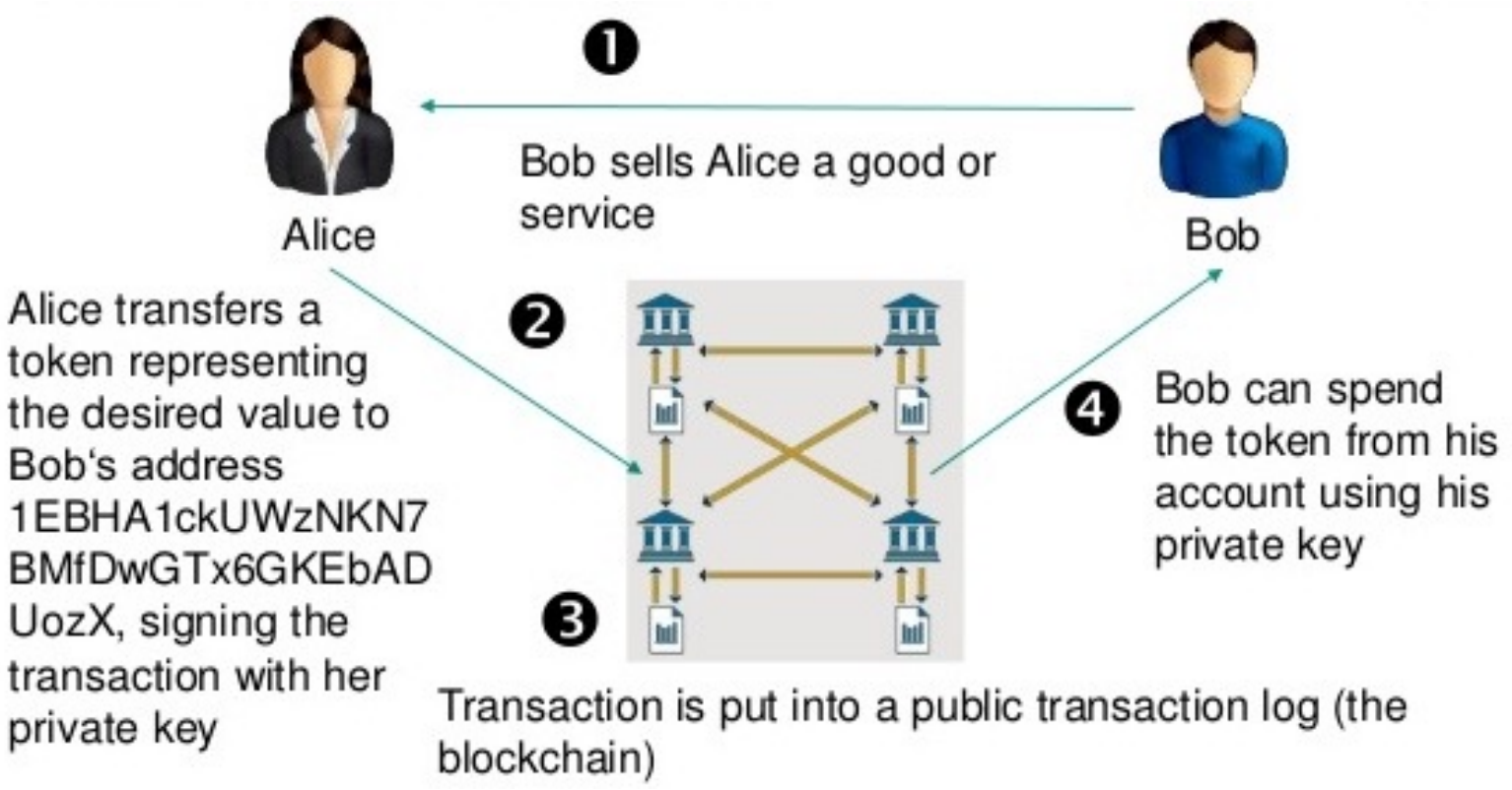


# Decentralized Ledger

- A new way of handling transactions
- Every individual maintains its own copy of the ledger



# Decentralized Transaction



# Problems of a centralized monetary system

Corruption

CNN Money Companies Markets Tech Media U.S.

Wells Fargo uncovers up to 1.4 million more fake accounts

by Matt Egan @MattEganCNN

August 31, 2017: 12:34 PM ET

Recommend 39

Mismanagement


Control

Business

**India Abolishes 500 and 1,000 Rupee Notes to Fight Corruption**

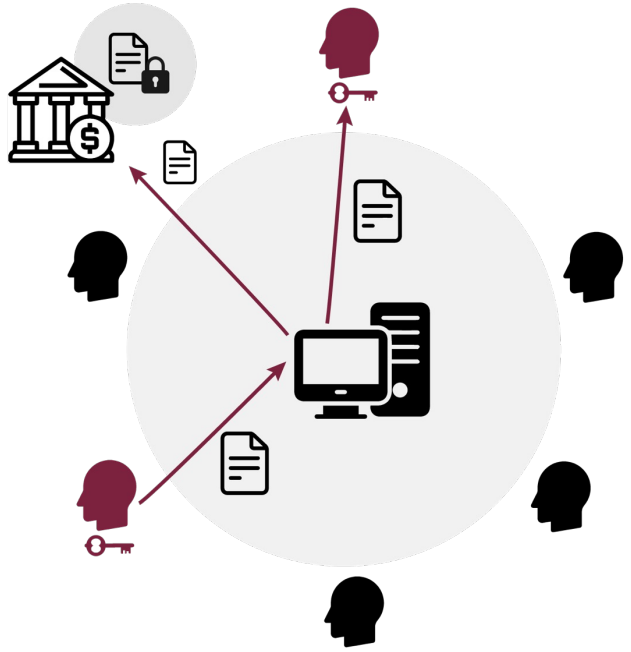
By Rajesh Kumar Singh and Iain Marlow

November 8, 2016, 10:59 PM GMT+8 *Updated on November 9, 2016, 1:49 PM GMT+8*

# Centralised or Decentralised

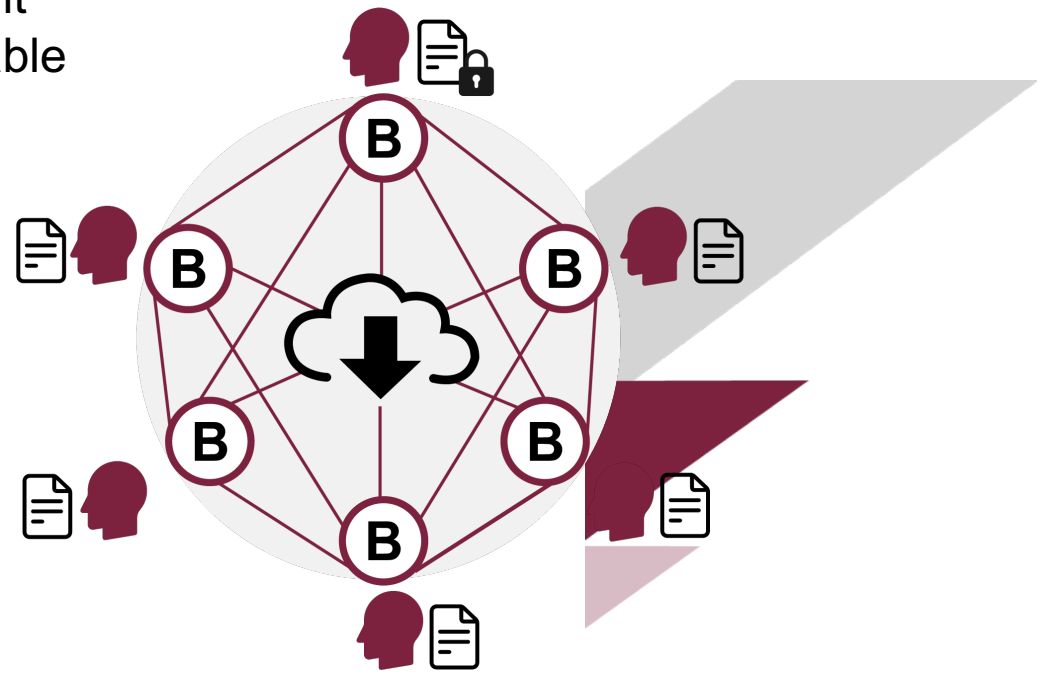
## Centralised system:

- Bookkeeper fee
- Availability
- Power corruption
- Single point of failure
- Non-resilient



## Decentralised system:

- Trusted
- Transparent
- Shared
- Resilient
- Immutable



# Why is Bitcoin a Big Thing?

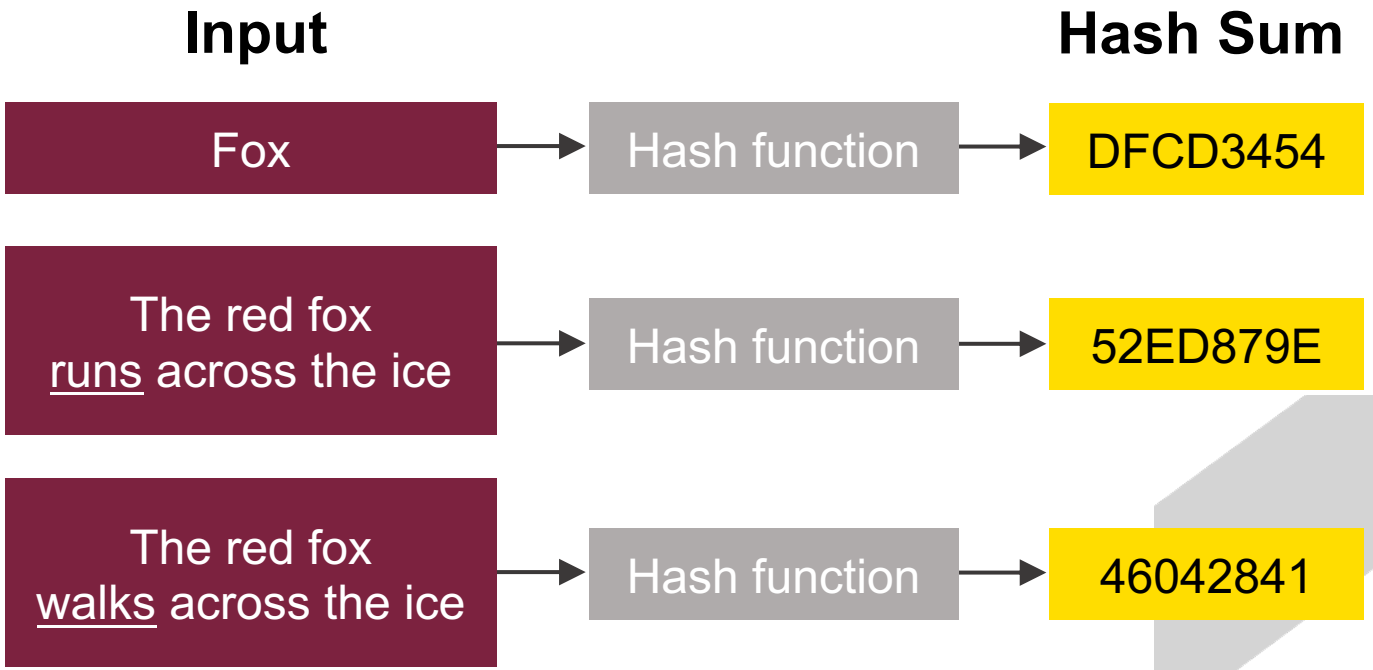
**Internet is the information superhighway**


**is the Internet of Value (Trust)**

# Blockchain Primer

# Hash Function

- A **hash function** is a mathematical function that converts a variable-length string of characters into a **fixed-size** numerical value
- **Cryptographic hash function:** one-way function – easy to compute, hard to invert

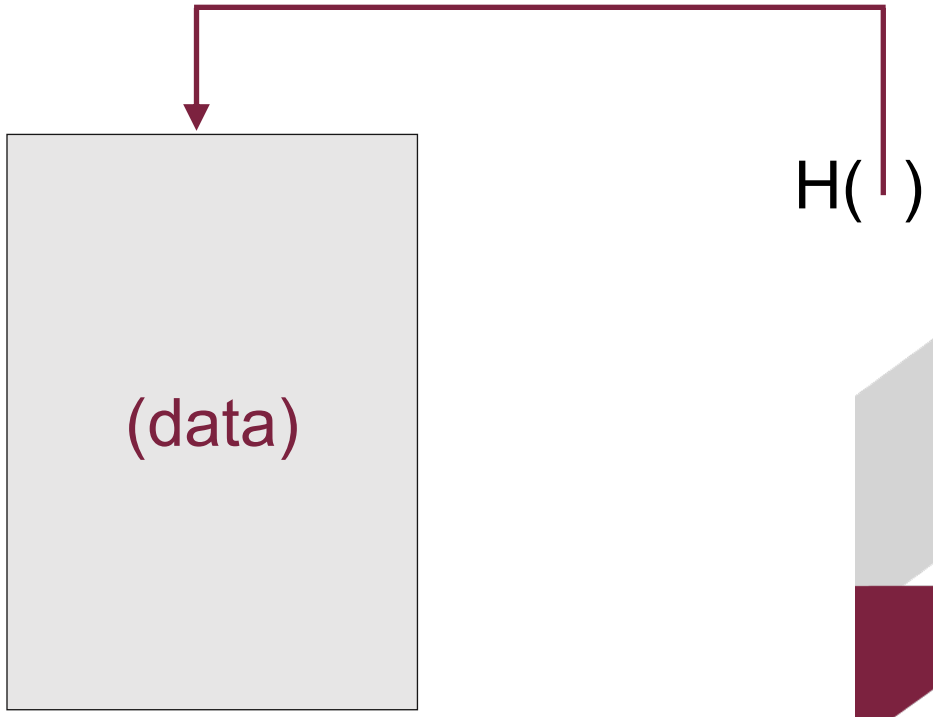



E.g., MD5, SHA-1, SHA-256, …

Lowery, J. M. (2020). *MD5 vs SHA-1 vs SHA-2 - Which is the most secure encryption hash and how to check them*. freeCodeCamp. https://www.freecodecamp.org/news/md5-vs-sha-1-vs-sha-2-which-is-the-most-secure-encryption-hash-and-how-to-check-them/

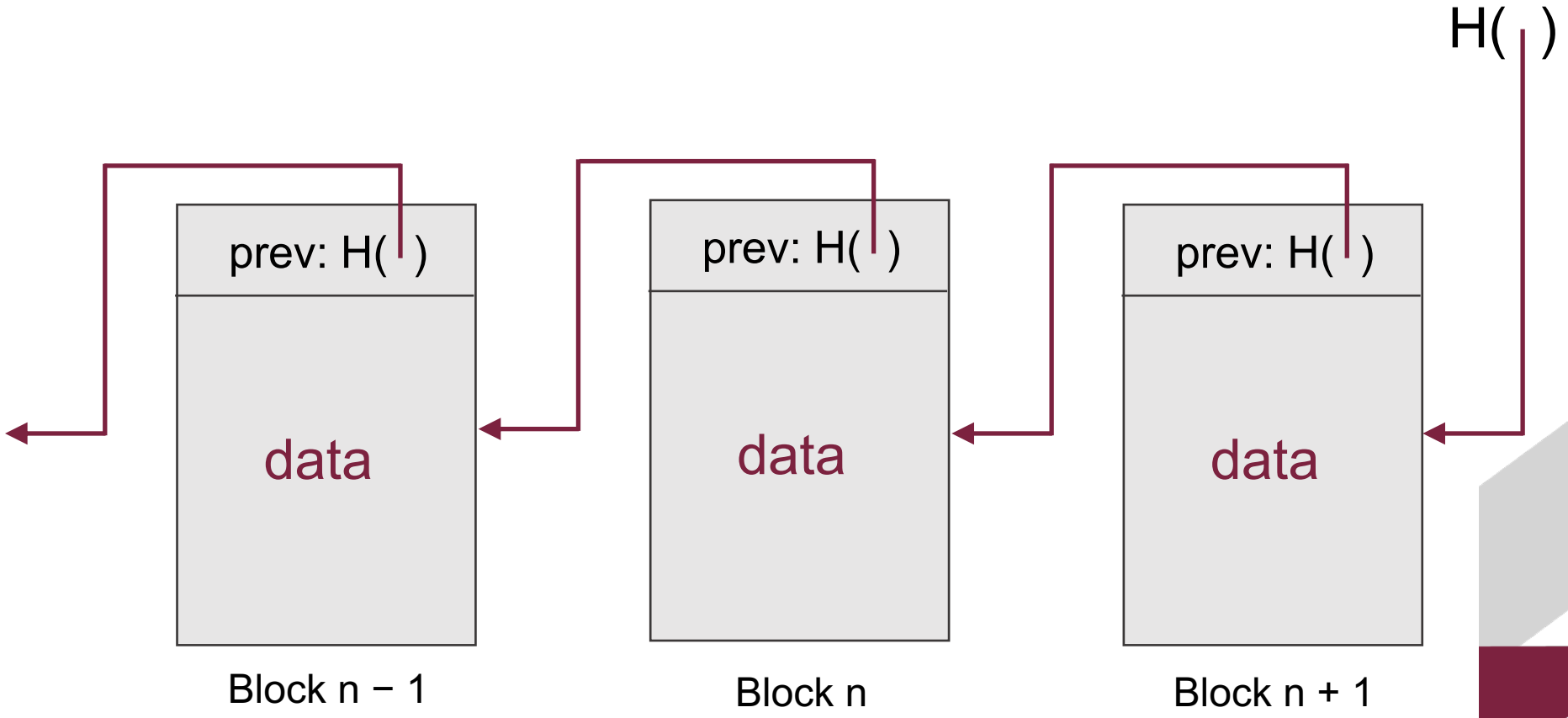
# Hash Pointer

- A pointer to where data is stored together with a cryptographic hash of the value of that data at some fixed point in time
- Difference from a regular pointer: This also gives you a way to **verify that the information hasn't been changed**.



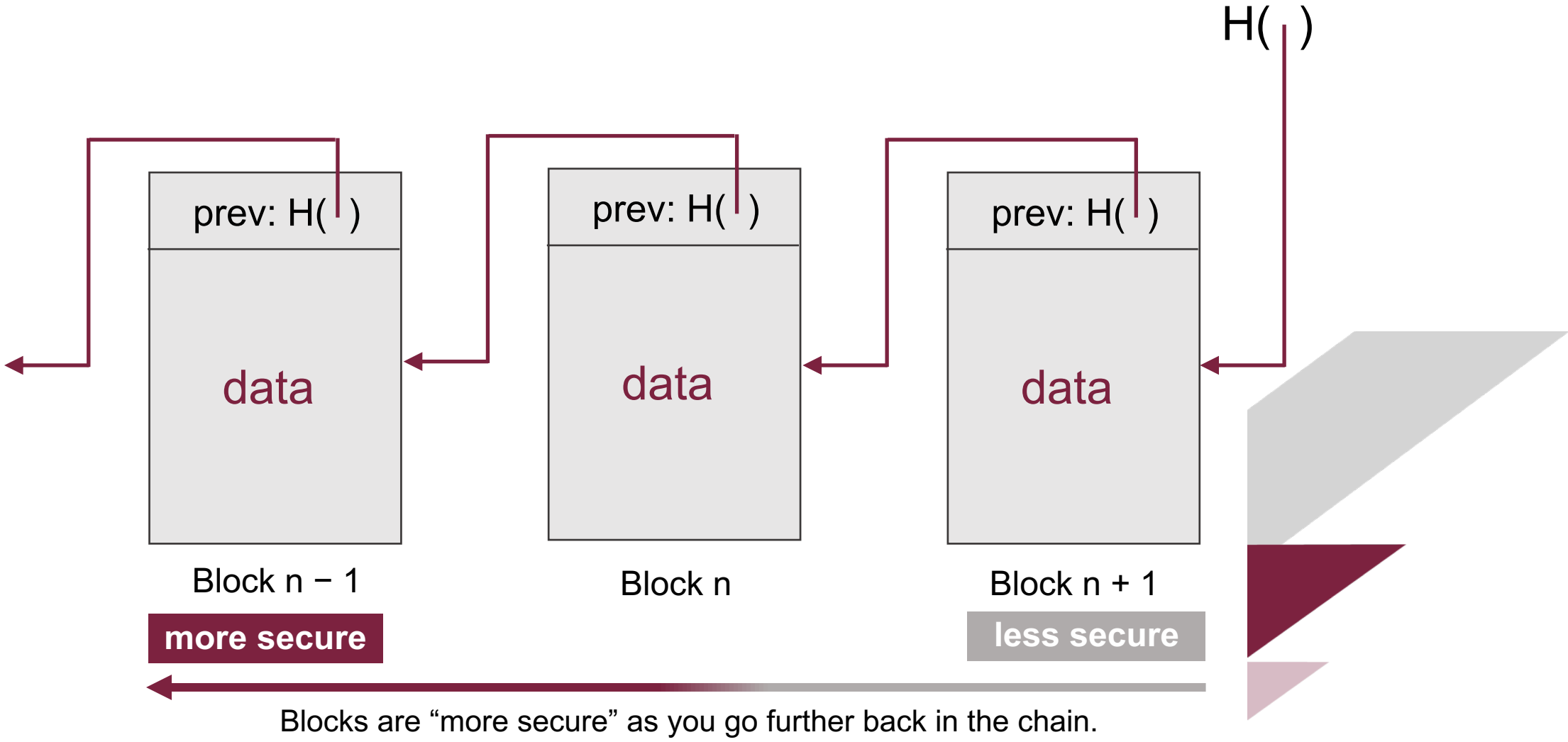

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

# Blockchain




Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

# Blockchain

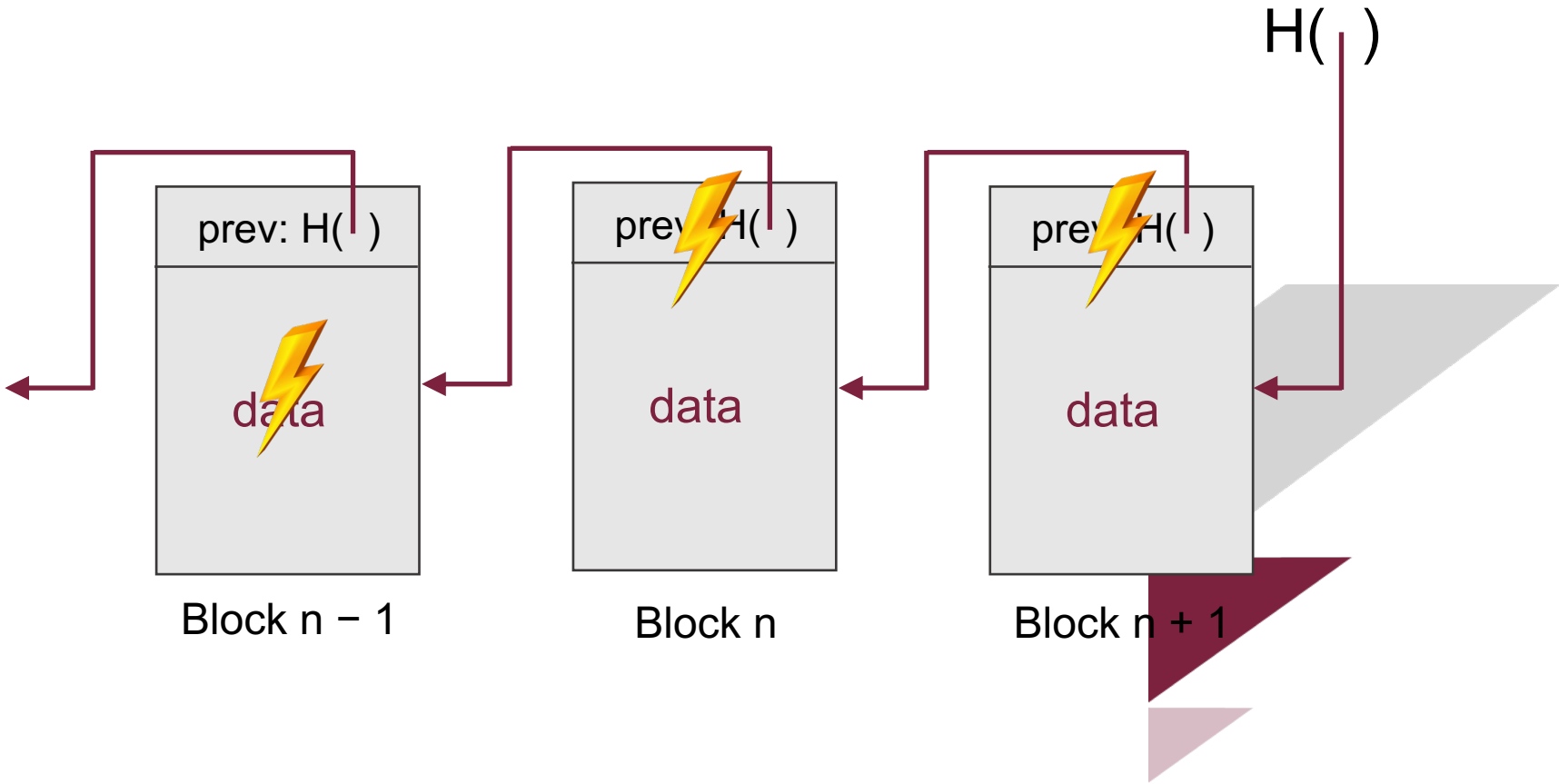



Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

# Blockchain as a Tamper-Evident Log

If an adversary modifies data in block n − 1:

- The hash in block n, which is a hash of the entire block n − 1, is not going to match up.
- We will detect the **inconsistency**.

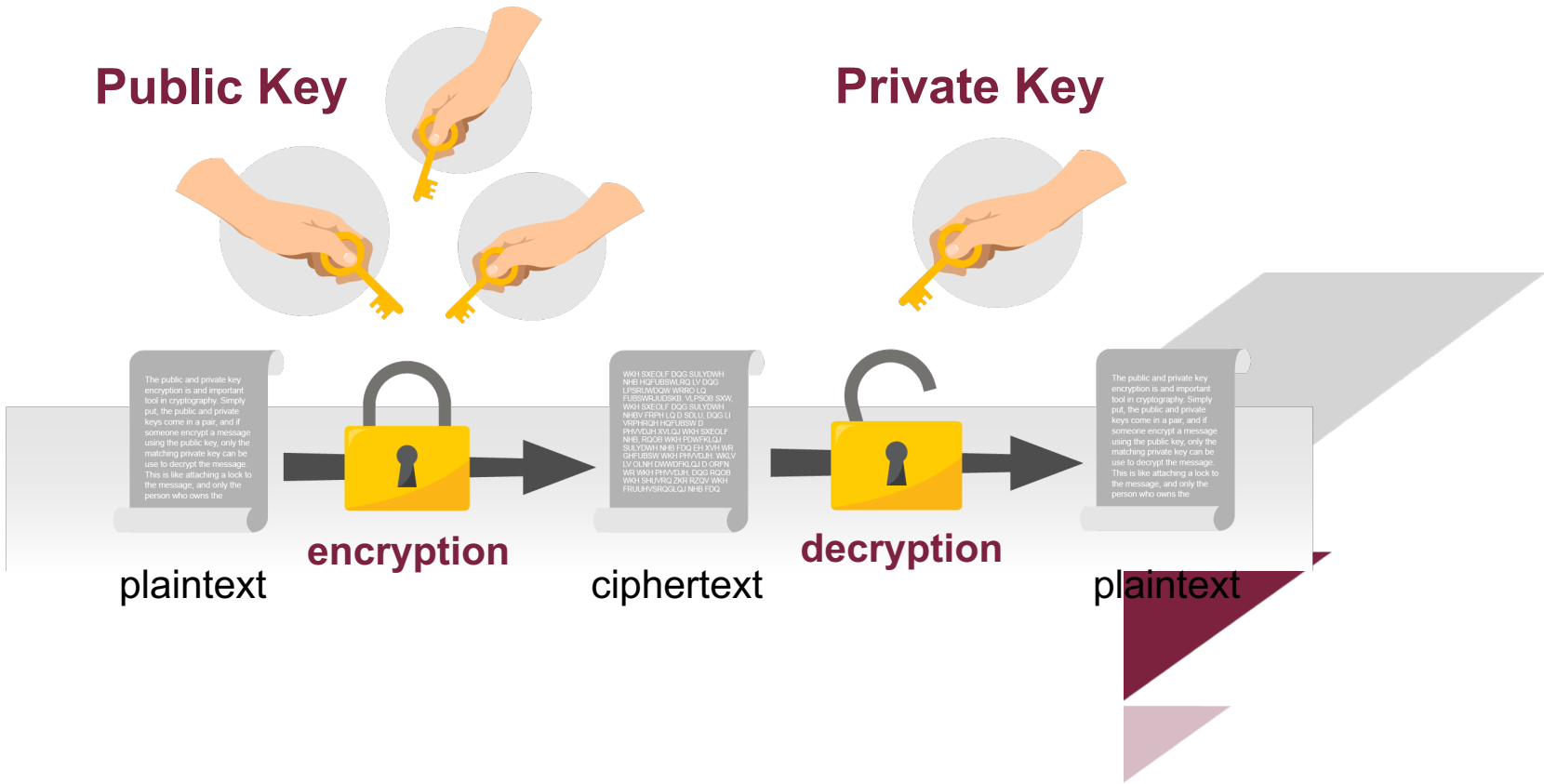



Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

# Public and Private Keys

In cryptography:

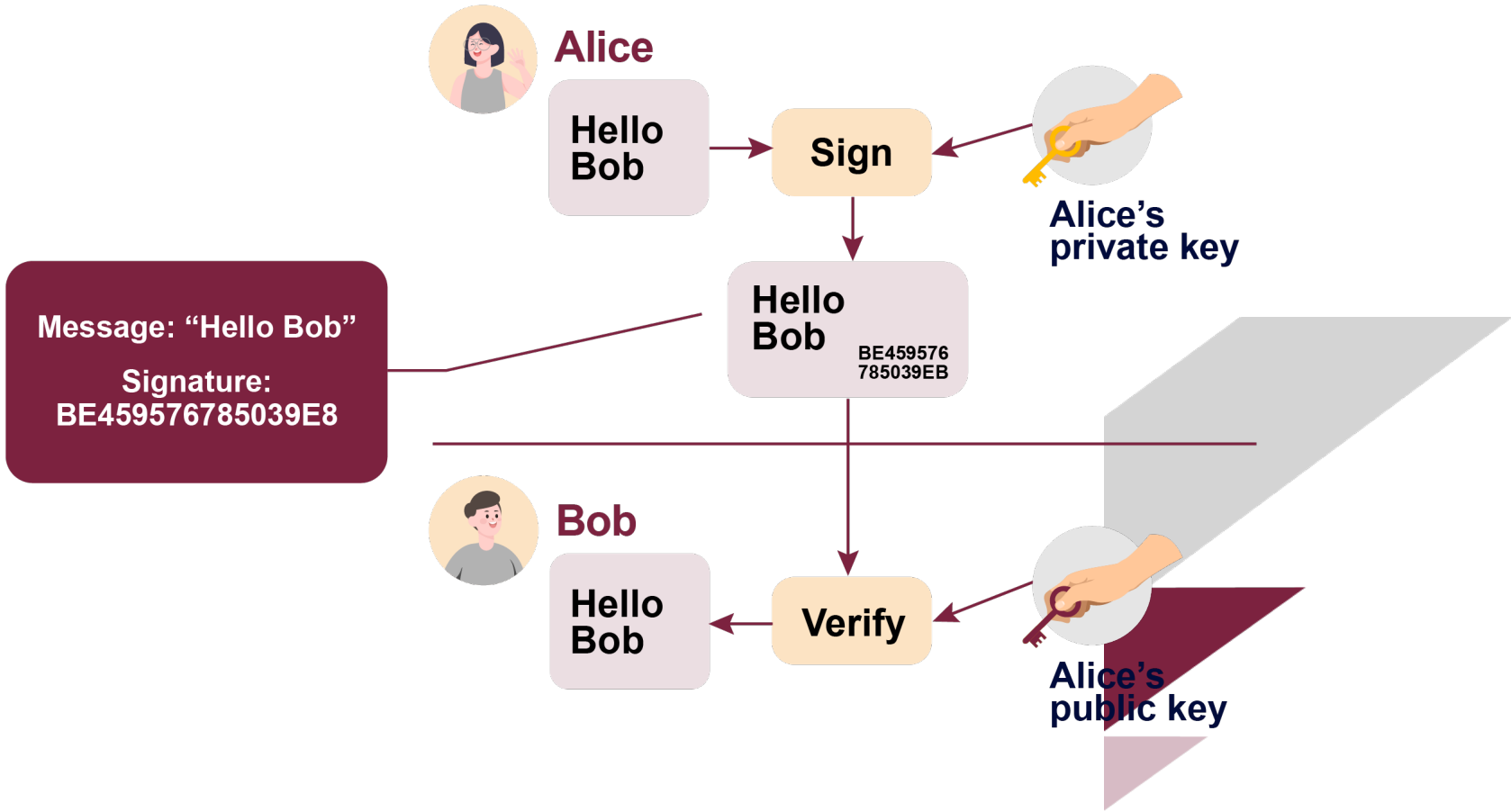
- The public key is used to encrypt, and the private key is used to decrypt.
- It is computationally infeasible to compute the private key based on the public key.




GlobalSign. (n.d.). *What is public-key cryptography?* Retrieved July 20, 2022 from https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography

# Digital Signatures

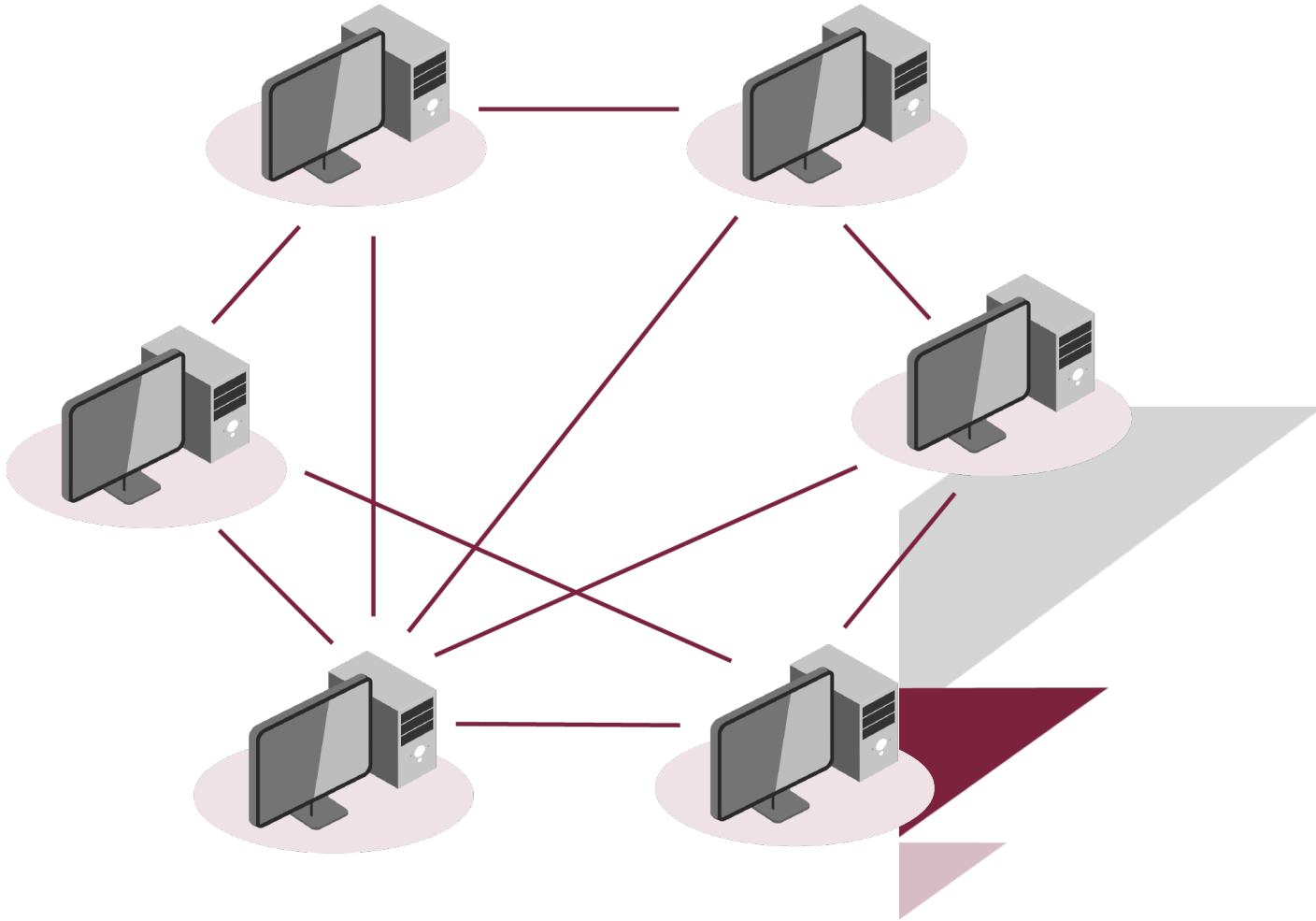
- The digital analog to a handwritten signature on paper.
- **Properties:**
  - Only you can make your signature, but anyone who sees it can verify that it's valid.
  - The signature to be tied to a particular document.




Adapted from FlippyFlink. (2019). *Example showing digital signing* [Illustration]. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Private_key_signing.svg. CC BY-SA 4.0.

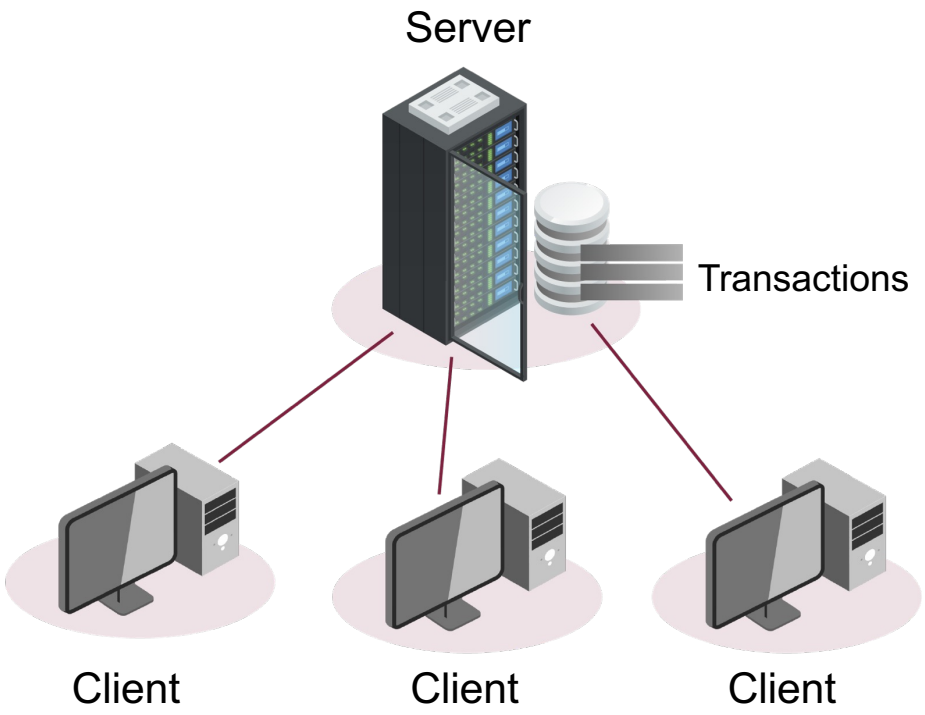
# Peer-to-Peer (P2P) Network

- Identical information in each server/node
- Allow the participants of the market to trade directly with each other without any trusted third party to process all trades
- Offer high resistance to transaction censorship
- Cheap to use; private and secure, at least when realized properly

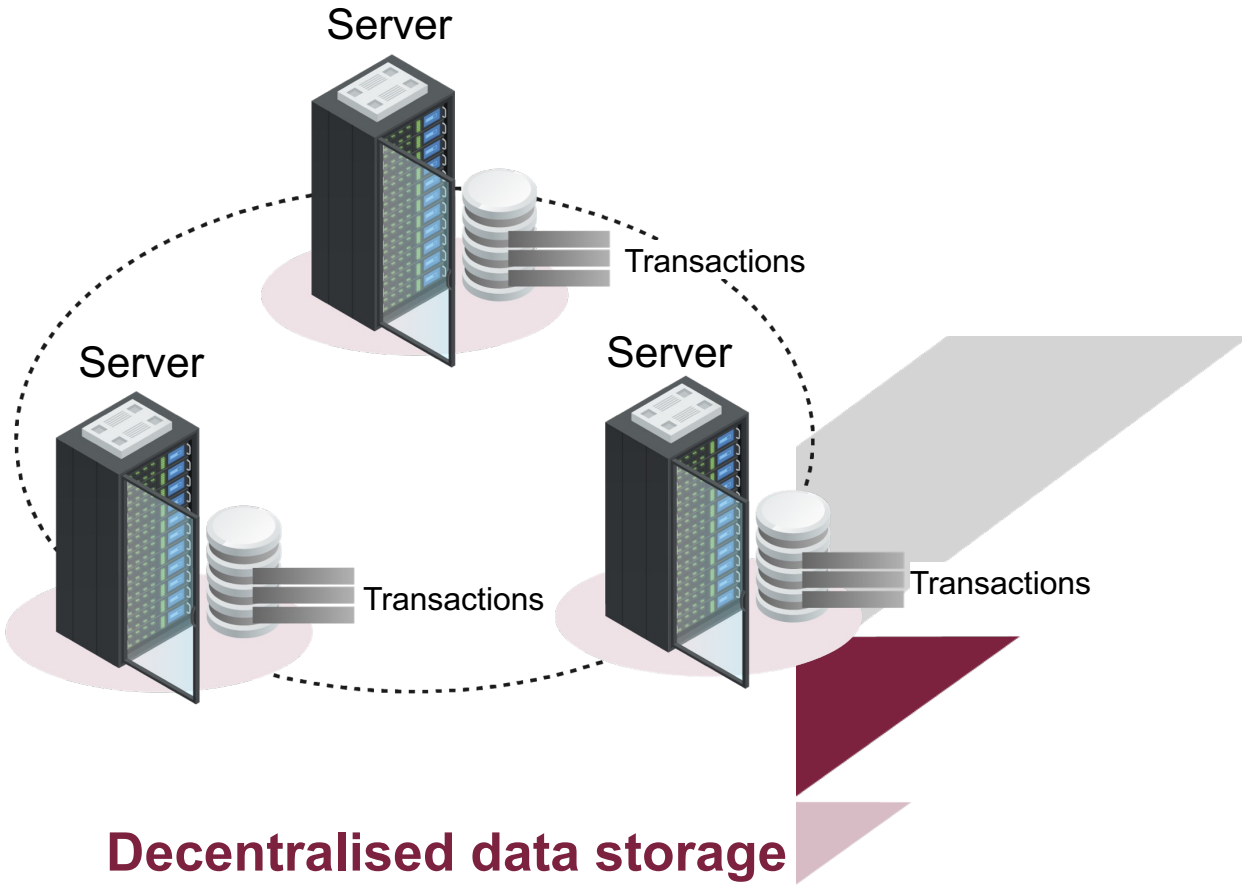


Marshall, A. (2017). *P2P cryptocurrency exchanges, explained*. Cointelegraph. Retrieved July 20, 2022 from https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained

# Centralised vs. Decentralised Data Storage

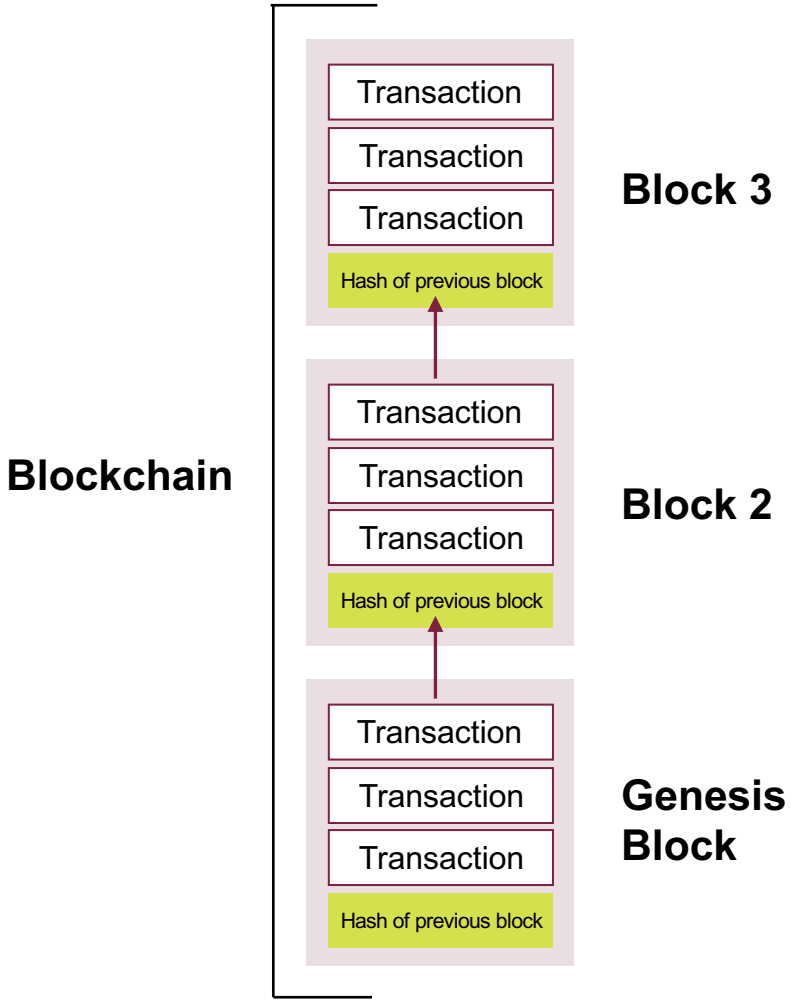


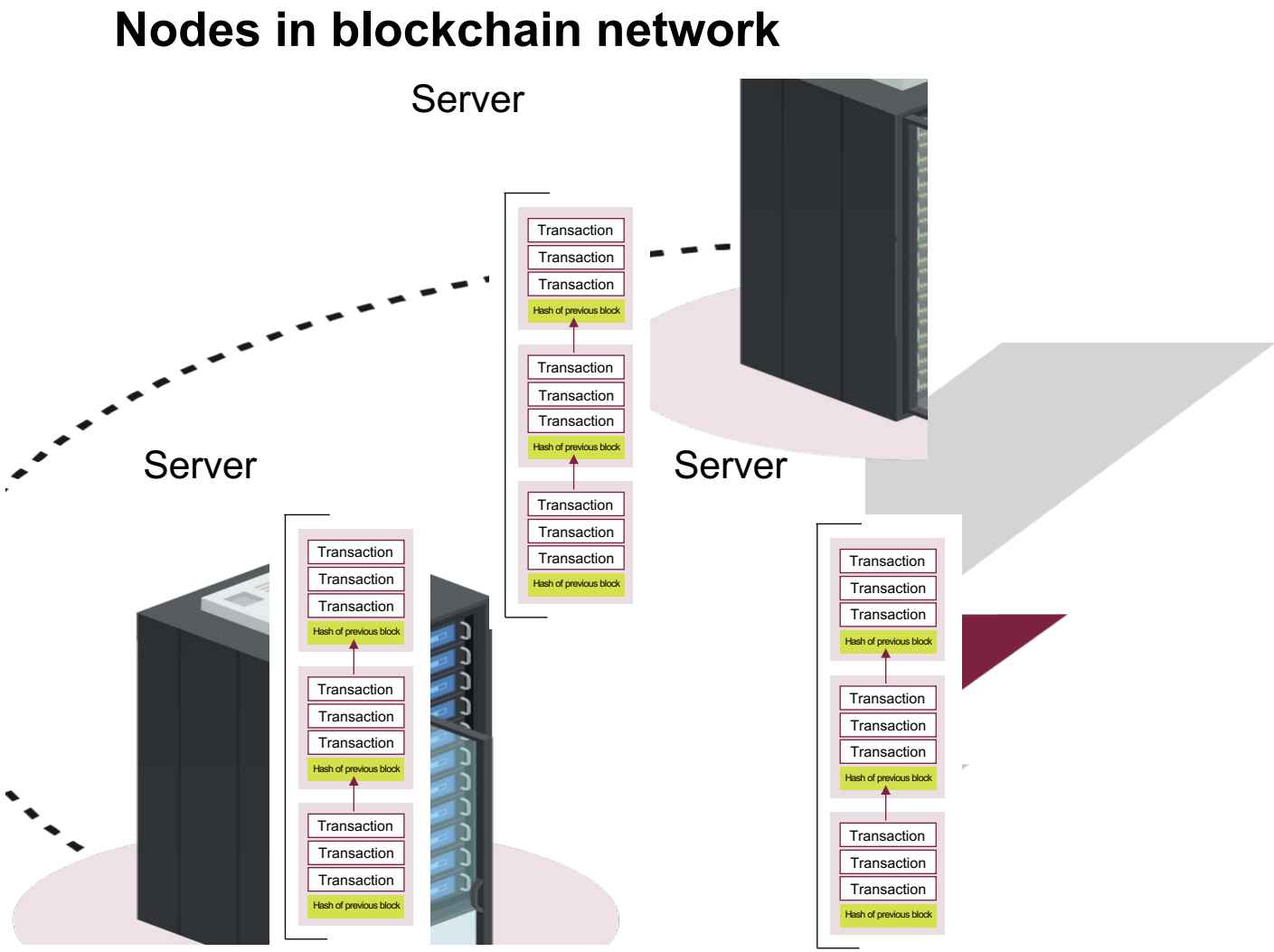

**Centralised data storage**




**Decentralised data storage**

# Linking Blocks to Form a Blockchain



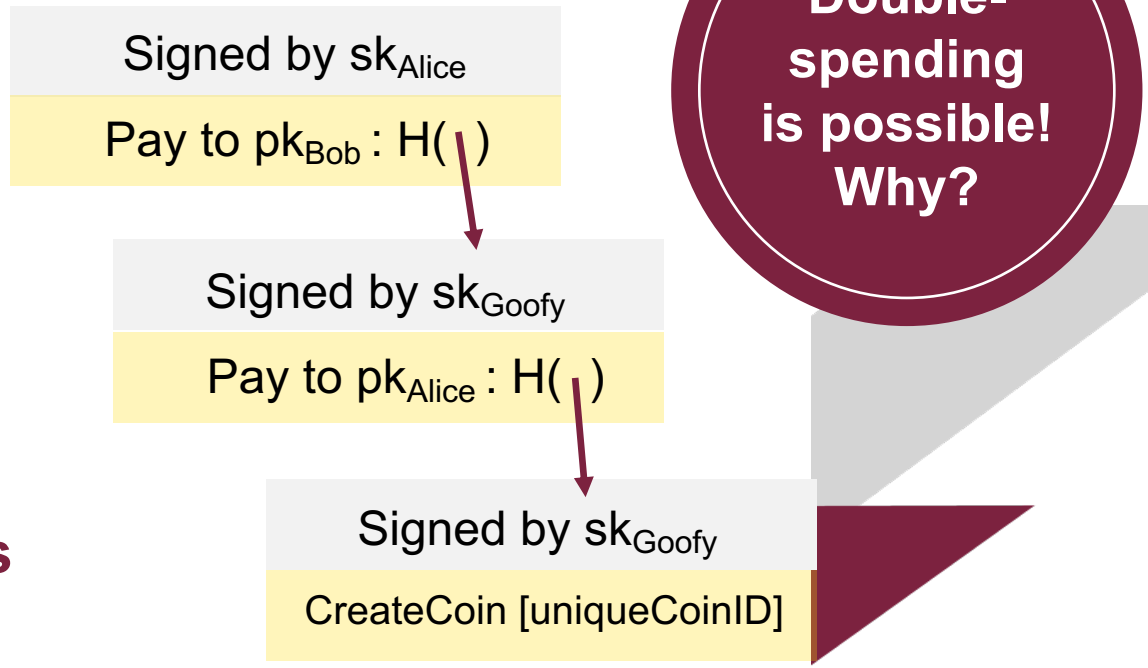



# How Does Blockchain Work?

# A Simple Cryptocurrency: GoofyCoin

**GoofyCoin Rules:**

1. Goofy can create new coins: "**CreateCoin[uniqueCoinID]**"
2. Whoever owns a coin can pass it on to someone else by signing a statement that saying, "**Pass on this coin to X**" (where X is specified as a public key)
3. Anyone can **verify the validity of a coin by following the chain of hash pointers** back to its creation by Goofy, verifying all signatures along the way

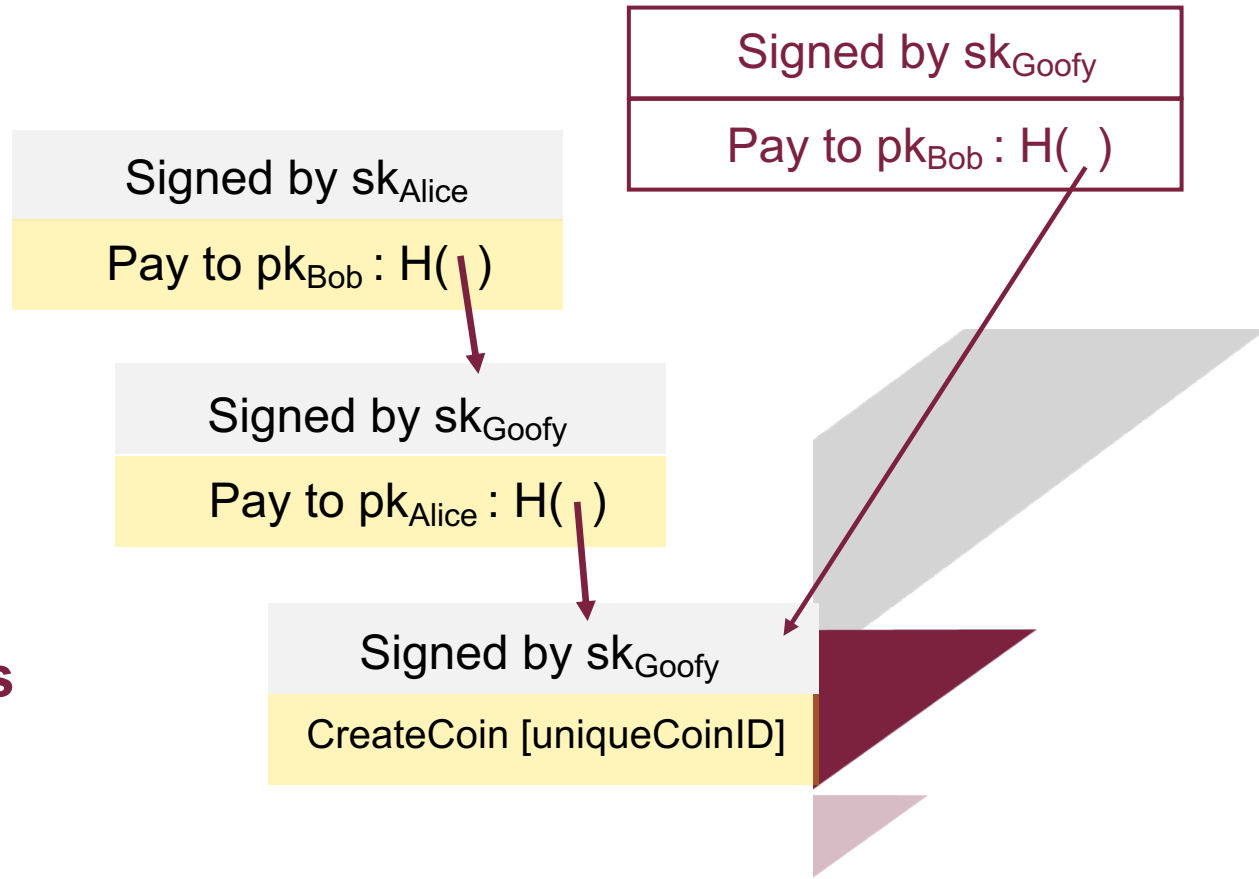



Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

# A Simple Cryptocurrency: GoofyCoin

**GoofyCoin Rules:**

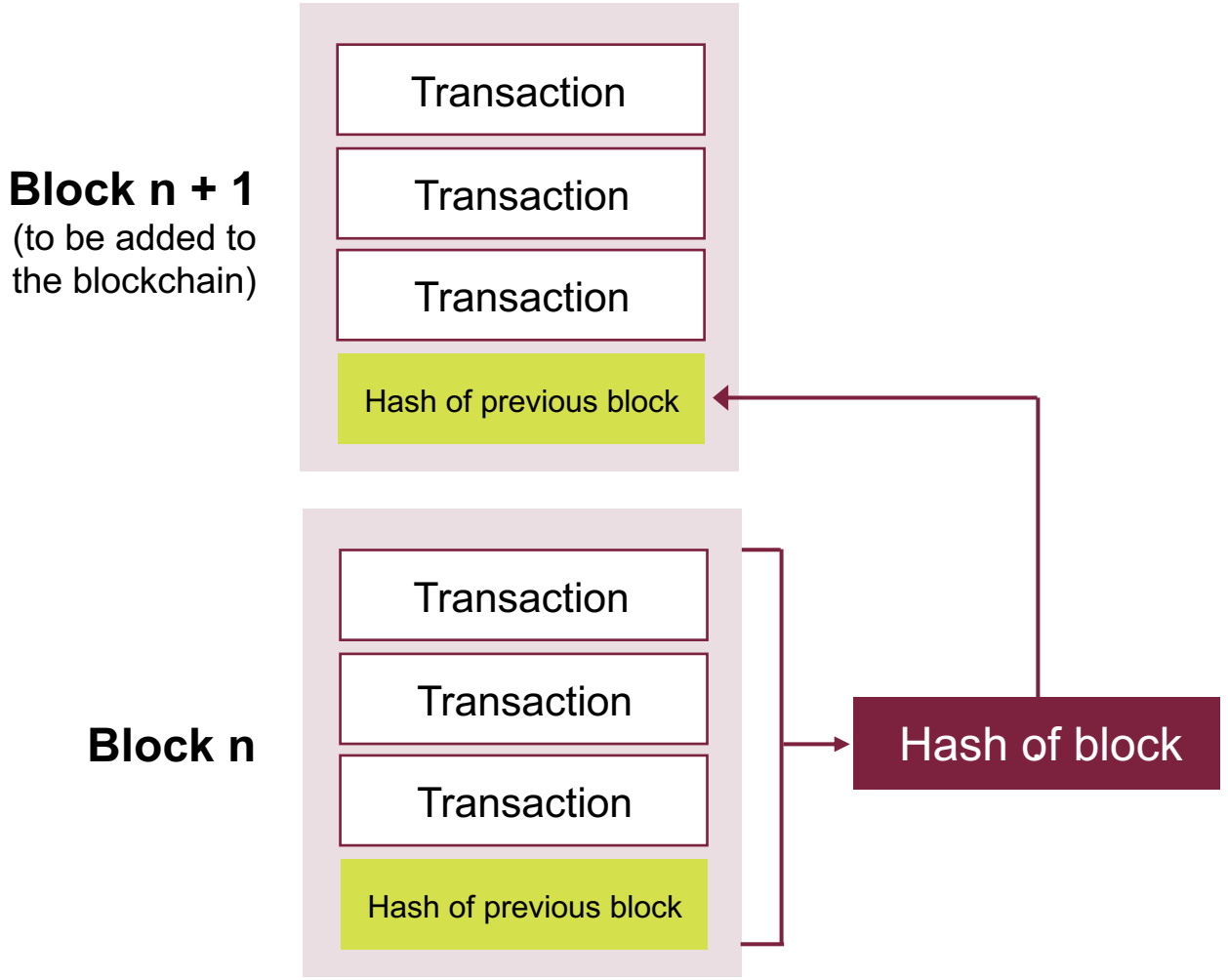
1. Goofy can create new coins: "**CreateCoin[uniqueCoinID]**"
2. Whoever owns a coin can pass it on to someone else by signing a statement that saying, "**Pass on this coin to X**" (where X is specified as a public key)
3. Anyone can **verify the validity of a coin by following the chain of hash pointers** back to its creation by Goofy, verifying all signatures along the way




Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

# Solving the "Double-Spending" Problem

- **Who gets to add the next block?**
- Some nodes are known as **miners**. Miners add blocks to the blockchain.
- In order to add a block to the blockchain, a miner needs to do the following:
  - Take the transactions in the previous block and combine it with the hash of the previous block to derive its hash.
  - Store the derived hash into the current block.




Lee, W-M. (2018). *Understanding how blockchain works*. NDC Conferences. Retrieved July 20, 2022 from https://blog.ndcconferences.com/understanding-blockchain/

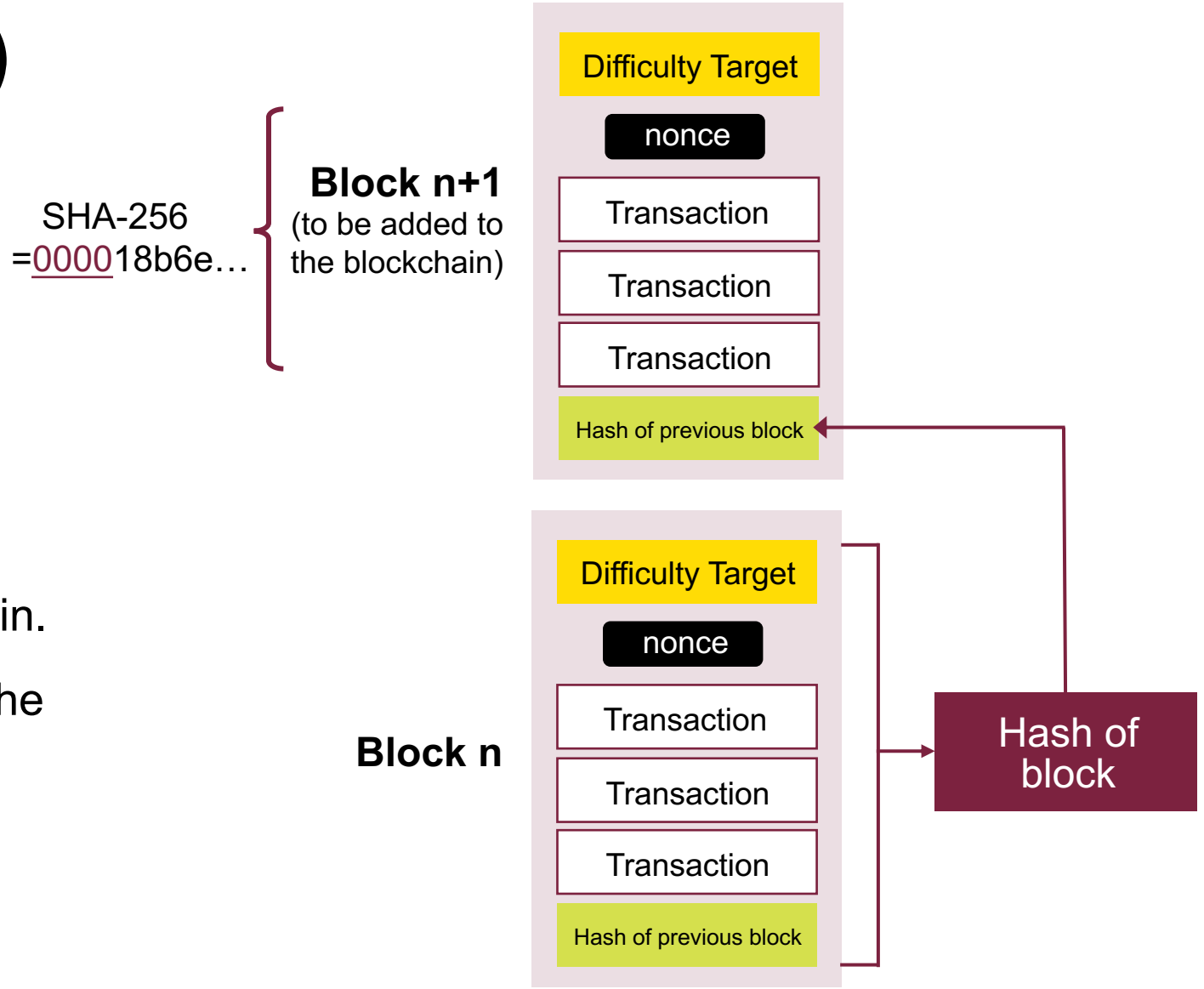
# Proof of Work (PoW)

- A mechanism to help reach consensus on the state of the blockchain.
- PoW requires the nodes to demonstrate they have burned CPU in order to win the right to create the next block.
  - A piece of data which was difficult (costly, time-consuming) to produce so as to satisfy certain requirements.
  - It must be trivial to check whether data satisfies said requirements.
  - Hashcash (SHA-256) is the PoW function used to solve difficult mathematics problems.
  - **Mining** is usually the process in which this proof occurs.

WeUseCoins. (n.d.). *What is bitcoin mining?* Retrieved July 20, 2022 from https://www.weusecoins.com/en/mining-guide/

# Proof of Work (PoW)

- Miners work hard to find the value of **nonce**.
  - Once the nonce is found, the entire block and the nonce is broadcasted to other nodes.
  - The block has been mined and ready to be added to the blockchain.
  - Other miners can now verify that the nonce does indeed satisfy the difficult target.
  - The miner earns the mining fees and transaction fees.




Lee, W-M. (2018). *Understanding how blockchain works*. NDC Conferences. Retrieved July 20, 2022 from https://blog.ndcconferences.com/understanding-blockchain/

# Building a Blockchain for Students' Grades

## Students

- Student identities are concealed.
- Each student has a public key that matches a private key that only the student knows.


| | Public Key | Private Key |
|---|---|---|
| Student 1 | ad59da | c8fc47b6fe |
| Student 2 | bd9ebc | 4382af3398 |
| Student 3 | c67445 | 56164d905c |

## Faculties

- Miners
- Other participating nodes
- Miners mine blocks, all nodes verify and vote

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

# Pool of Grade Records

**Block 1**
Course: Parks 320
Student: ad59da
Grade: F

**Block 2**
Course: Engineering 300
Student: bd9ebc
Grade: B

**Block 3**
Course: Business 200
Student: c67445
Grade: C


Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

# Go Miners, Go

**Hash = Nonce + a + b + c − Value of last two digits of previous hash**

a = Value of the first letter of the course

b = Value of the first letter of the student's public key

c = Value of the grade

Nonce = Value between 1 and 3 that you will adjust to calculate a hash that can be evenly divisible by 3

Table

| | | | |
|---|---|---|---|
| A | 65 | N | 78 |
| B | 66 | O | 79 |
| C | 67 | P | 80 |
| D | 68 | Q | 81 |
| E | 69 | R | 82 |
| F | 70 | S | 83 |
| G | 71 | T | 84 |
| H | 72 | U | 85 |
| I | 73 | V | 86 |
| J | 74 | W | 87 |
| K | 75 | X | 88 |
| L | 76 | Y | 89 |
| M | 77 | Z | 90 |

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

# Our First Block

**Hash: 212**

**Genesis Block**
Course: -
Student: -
Grade: -

**Block 1**
Course: Parks 320
Student: ad59da
Grade: F

| Block | Course | Student | Grade | Nonce (1-3) | Prev Hash | a | b | c | Hash |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 212 |
| 1 | Parks 320 | ad59da | F | | 12 | 80 | 65 | 70 | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**Hash = Nonce + a + b + c – Value of last two digits of previous hash**

# Finishing the Block: Hashing

**Hash: 212**

**Genesis Block**
Course: -
Student: -
Grade: -

**Hash: 204**

**Block 1**
Course: Parks 320
Student: ad59da
Grade: F

| Block | Course | Student | Grade | Nonce (1-3) | Prev Hash | a | b | c | Hash |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 212 |
| 1 | Parks 320 | ad59da | F | I | 12 | 80 | 65 | 70 | 204 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**Hash = Nonce + a + b + c – Value of last two digits of previous hash**

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

# Finishing the Block: Verifying and Voting

**Hash: 212**

**Genesis Block**
Course: -
Student: -
Grade: -

**Hash: 204**

**Block 1**
Course: Parks 320
Student: ad59da
Grade: F


| Block | Course | Student | Grade | Nonce (1-3) | Prev Hash | a | b | c | Hash |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 212 |
| 1 | Parks 320 | ad59da | F | I | 12 | 80 | 65 | 70 | 204 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**Hash = Nonce + a + b + c – Value of last two digits of previous hash**

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

# Second Block

**Hash: 212**

**Genesis Block**
Course: -
Student: -
Grade: -

**Hash: 204**

**Block 1**
Course: Parks 320
Student: ad59da
Grade: F

**Hash: 198**

**Block 2**
Course: Engineering 300
Student: bd9ebc
Grade: B

...

| Block | Course | Student | Grade | Nonce (1-3) | Prev Hash | a | b | c | Hash |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 212 |
| 1 | Parks 320 | ad59da | F | I | 12 | 80 | 65 | 70 | 204 |
| 2 | Engineering 300 | bd9ebc | B | I | 4 | 69 | 66 | 66 | 198 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**Hash = Nonce + a + b + c – Value of last two digits of previous hash**

Christianson, J. S. (2022, February 10). *How to teach blockchain with "The Blockchain Game!".* Medium. https://medium.com/predict/how-to-teach-blockchain-with-the-blockchain-game-44360c542c81. CC BY-NC-SA 4.0.

# Discussion

- What if "Student 1" loses his/her private key?
- What if a student pays off a node to change the score stored in "Block 1"?

| Block | Course | Student | Grade | Nonce (1-3) | Prev Hash | a | b | c | Hash |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 212 |
| 1 | Parks 320 | ad59da | F | I | 12 | 80 | 65 | 70 | 204 |
| 2 | Engineering 300 | bd9ebc | B | I | 4 | 69 | 66 | 66 | 198 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

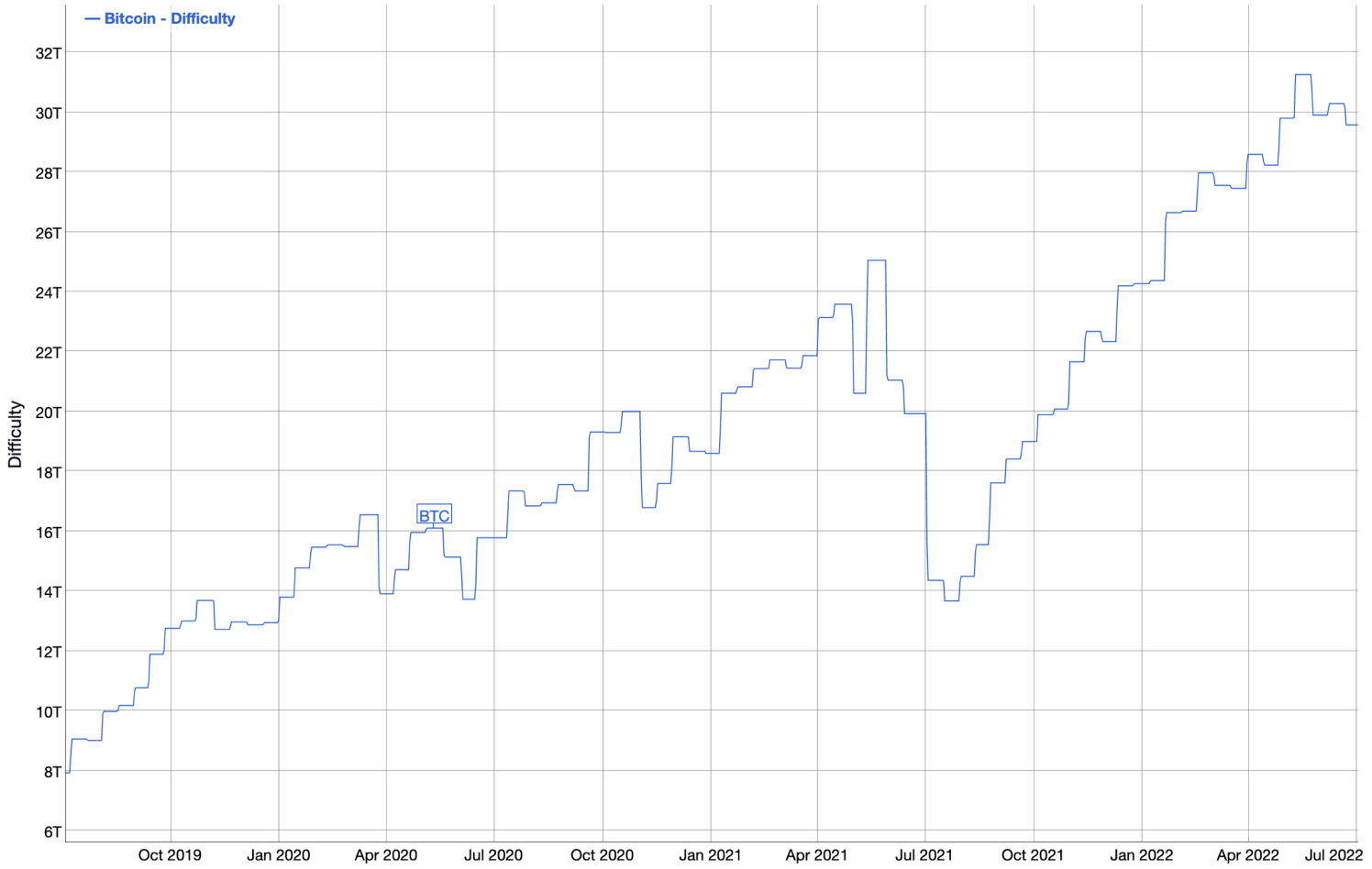
# Discussion

- Is it a good idea to store student grades on a blockchain? Why?
- Come up with an example which you think is a suitable application of blockchain

# Mining Difficulty

- Satoshi Nakamoto: “The more mining power the network has, the harder it is to guess the answer to the mining math problem”
- **Self-adjusting** to the accumulated mining power the network possesses.
- Why did Satoshi do this?
  - **On average**, a new block will be added every **10 minutes** (i.e., the nonce will be guessed every 10 minutes on average).
  - A sort of “arms race” to get the most efficient and powerful miners.

# Mining Difficulty



# Mining Revolution

CPU mining

GPU mining

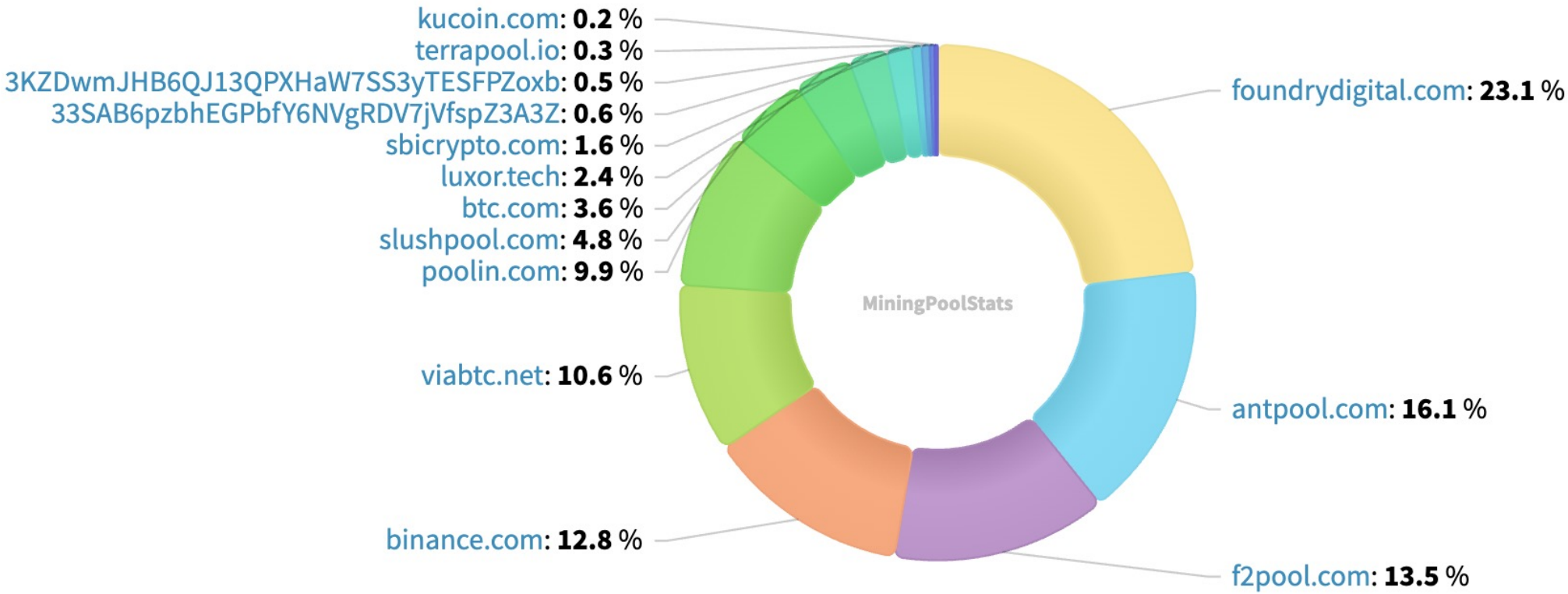

FPGA mining

ASIC mining

# Mining Pools

- **Idea:** Miners group together to form a “pool” (i.e., combine their mining power to compete more effectively).
- Once the pool wins, the reward is divided among the pool members based on their contributed mining power.
  - **Pros:** Reduce the variance of mining rewards; easy to upgrade the network
  - **Cons:** Pool manager must be trusted; centralised

# Mining Pool Distribution



# Is Bitcoin mining profitable?

- Things should be taken into consideration
  - Bitcoin reward per block: 50 BTC in 2009, now is 6.25
  - Mining difficulty
  - Electricity cost (going up …)
  - Power consumption
  - Pool fees
  - Bitcoin's price
  - Difficulty increase per year
  - Regulations

The Bitcoin block mining reward halves every 210,000 BLOCKs (~4 years). The most recent coin reward has decreased from 6.25 to 3.125 coins in 2024.

# PoW


- Effort is investment
- Uses computer cycle time to validate transactions
- Costly – hardware, energy wastage

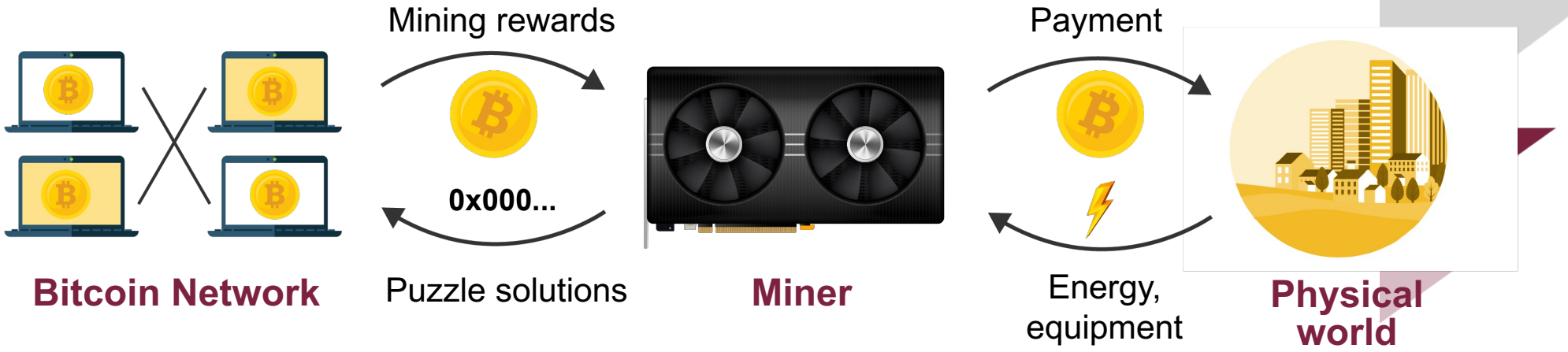
# PoW Problems?

# Alternatives to “PoW”

- Proof of Stake: the creator of a new block depends on his wealth in a deterministic way, also defined as stake
- Proof of Space: computation is replaced by storage
- Measure of Trust: most trustworthy miner wins
- Minimum Block Hash: (rather than faster) miner wins → More random
- …

# Proof-of-Stake and Virtual Mining

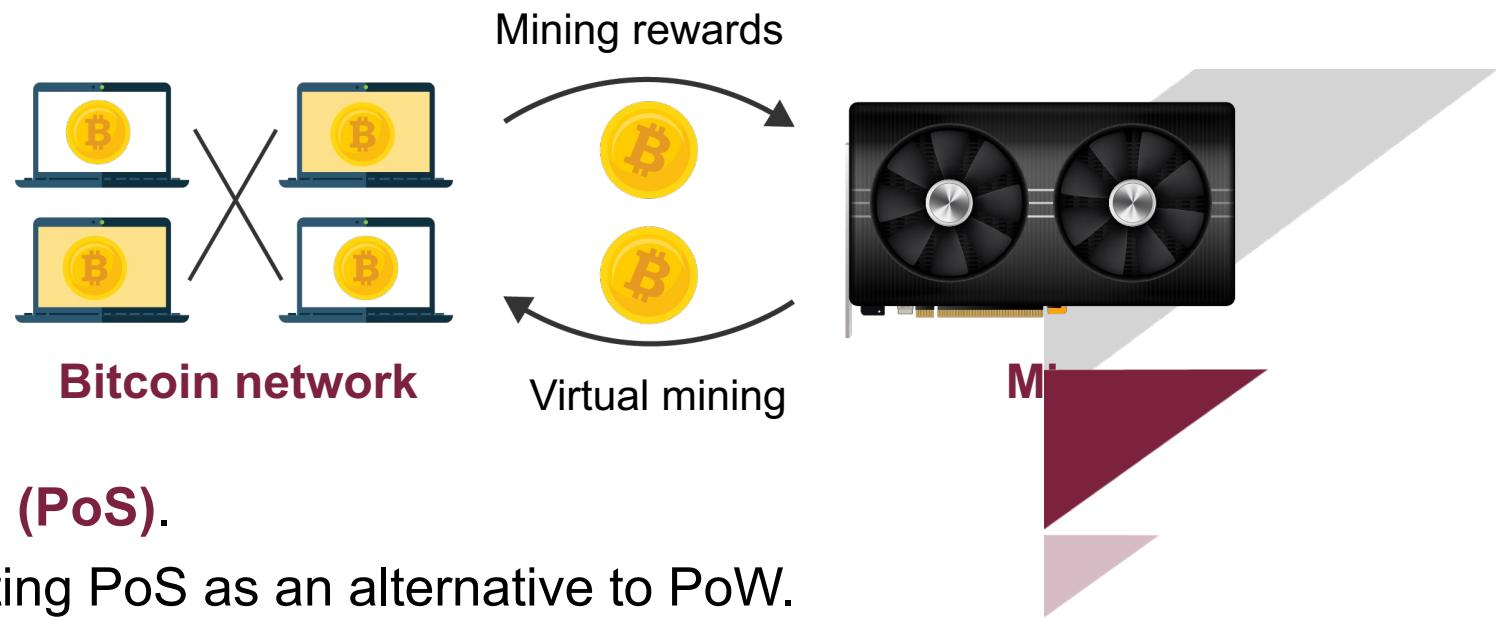
- Goal of mining is to enable a form of voting on the state of the blockchain
  - Miners invest in computer cycles
  - Computing power is translated to votes
- Mining in PoW is costly
  - Hardware equipment
  - Energy




Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

# Proof-of-Stake and Virtual Mining

- Can we remove the step of spending money on energy and equipment?
  - After all, this is only to prove who has invested more in mining.
  - Votes come directly from the proportion of the currency they hold.
- Advantages of virtual mining
  - It reduces the environmental footprint of PoW.
  - Large shareholders have an incentive to do things that would benefit the system as a whole.
  - This is essentially **Proof-of-Stake (PoS)**.
  - Ethereum and Algorand are adopting PoS as an alternative to PoW.




Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

# Alt Coins

- Follow same design as Bitcoin, but with separate blockchain and network
  - Hundreds alt coins, most of them are not very successful
  - Different proof of work or consensus mechanism
  - Specific features, such as strong anonymity

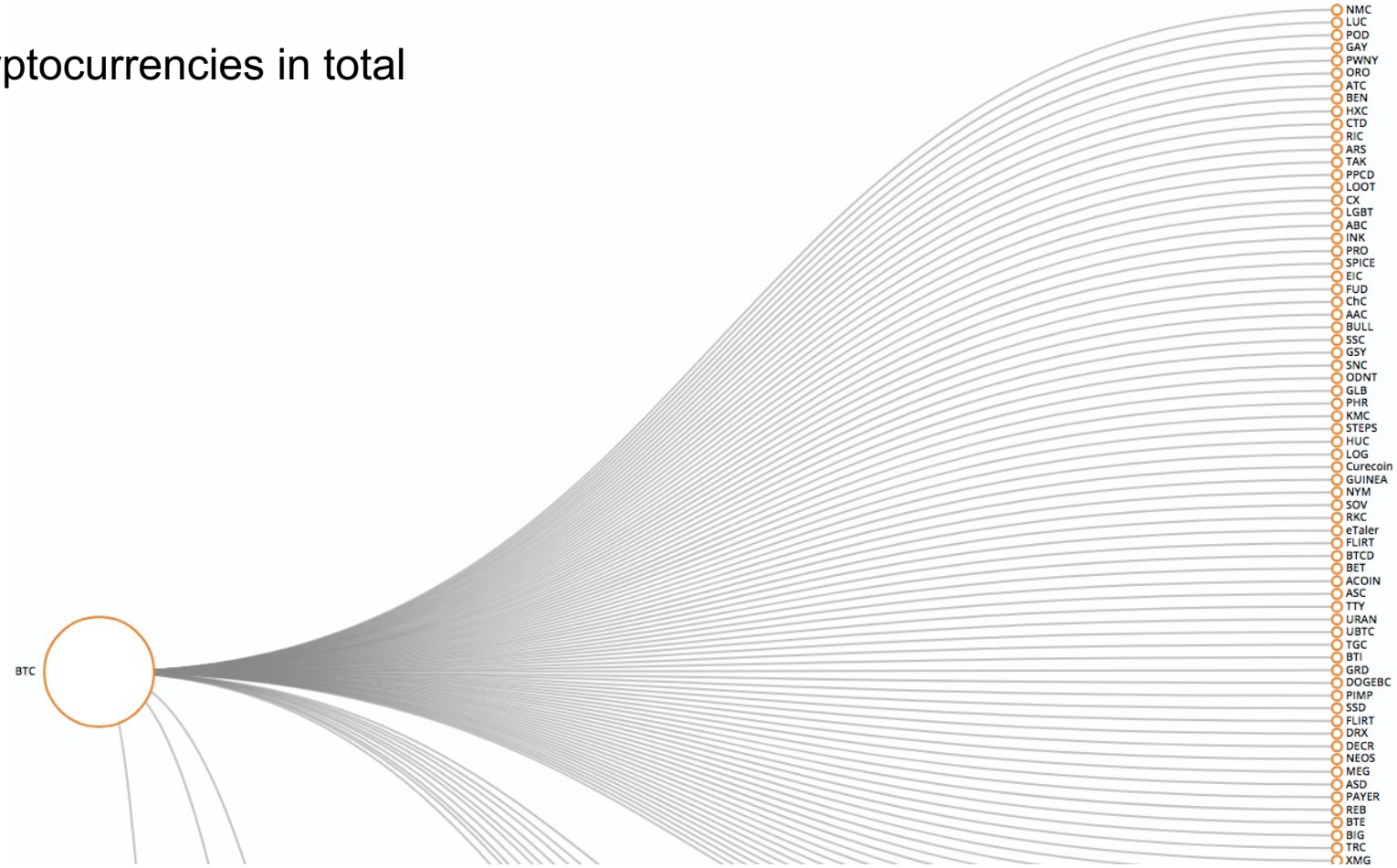

- 2011.08: IXCoin is Bitcoin with increased reward


- 2011.09: Tenebrix changed proof of work algorithm to **Scrypt**


- 2011.10: LiteCoin uses **Scrypt** as proof of work and faster block generation


# Alt Coins Today: 1000+ currencies derived from Bitcoin

2000+ cryptocurrencies in total




Source: http://mapofcoins.com/bitcoin

| # | Name | Market Cap | Price | Volume (24h) | Circulating Supply | Change (24h) | Price Graph (7d) |
|---|---|---|---|---|---|---|---|
| 1 | Bitcoin | $91,001,625,910 | $5,161.05 | $17,730,330,208 | 17,632,400 BTC | 3.11% |  |
| 2 | Ethereum | $17,794,858,793 | $168.58 | $7,586,734,884 | 105,558,231 ETH | 3.31% |  |
| 3 | XRP | $15,149,467,799 | $0.362916 | $1,530,695,312 | 41,743,765,071 XRP * | 2.42% |  |
| 4 | Litecoin | $5,725,718,989 | $93.51 | $4,069,048,904 | 61,233,211 LTC | 7.49% |  |
| 5 | Bitcoin Cash | $5,702,732,934 | $321.91 | $2,574,053,158 | 17,715,238 BCH | 11.98% |  |
| 6 | EOS | $4,939,315,216 | $5.45 | $3,100,759,496 | 906,245,118 EOS * | 3.50% |  |
| 7 | Binance Coin | $2,710,322,050 | $19.20 | $156,786,655 | 141,175,490 BNB * | -0.45% |  |
| 8 | Stellar | $2,470,233,594 | $0.128193 | $339,059,198 | 19,269,667,026 XLM * | 3.40% |  |
| 9 | Cardano | $2,352,205,947 | $0.090724 | $114,789,274 | 25,927,070,538 ADA | 2.32% |  |
| 10 | Tether | $2,089,389,879 | $1.00 | $18,361,678,180 | 2,079,324,324 USDT * | -0.11% |  |





Source: https://coinmarketcap.com/

# Types of Blockchain

**Public blockchain**

**Private blockchain**

**Consortium blockchain**

# Public Blockchain

- Anyone can run the public code, start mining, make a transaction, explore and validate the blockchain.
- Each transaction is verified by every node before it is written to the system.
- **Examples: Bitcoin, Ethereum, Algorand**

# Private Blockchain

- R/W permissions are kept centralised by one organisation.
- **Examples: Ripple, Multichain, Corda**

# Consortium Blockchain

**Also known as federated blockchain**

- Controlled by a set of pre-selected nodes, members of the consortium can run code, start mining and make transactions.
- **Examples: R3, HyperLedger Fabric**

# Blockchain 2.0: Decentralized Applications

# Decentralised Applications (DApps)

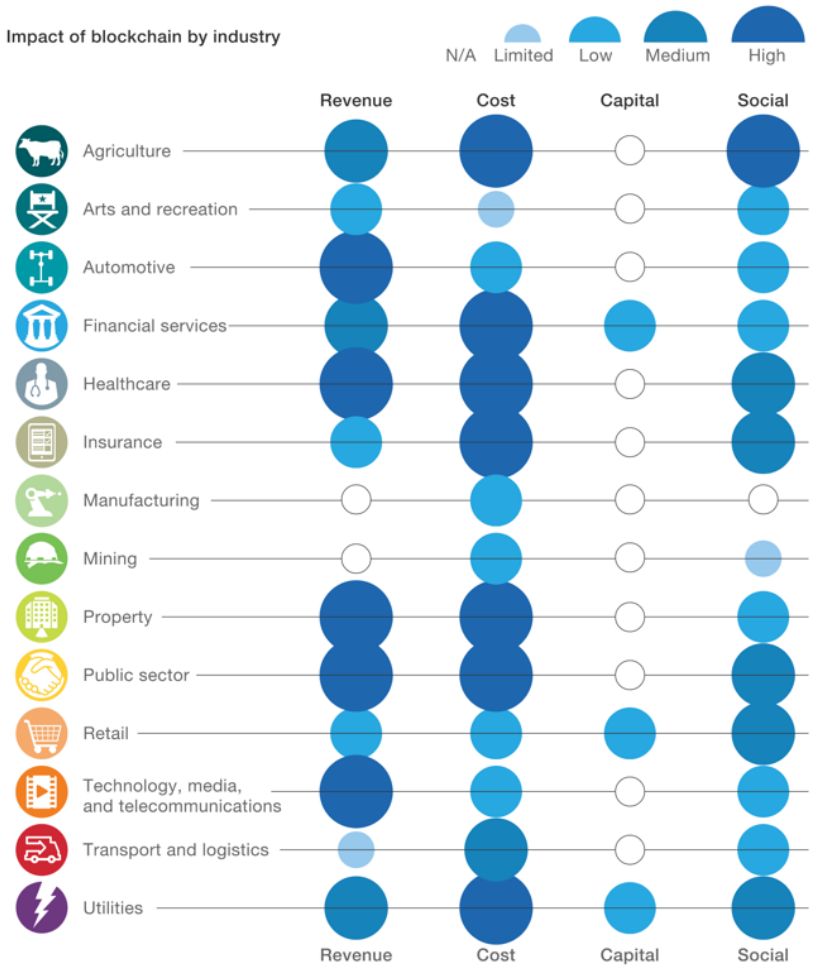
- The Do-It-Yourself platform for decentralised programs is also known as **Decentralised Applications**
- The infrastructure for running DApps worldwide
- First proposed in 2013 and then brought to life in 2014 by Vitalik Buterin, the co-founder of Bitcoin Magazine
- Goal: Ro truly decentralise the internet


- **Ethereum** in 2022:
  - **48 million** smart contracts
  - **2,970** DApps deployed
  - **49.38K** active users/day
  - **102.18K** transactions/day

State of the DApps. (n.d.). *DApp statistics*. Retrieved July 20, 2022 from https://www.stateofthedapps.com/stats

# Smart Contracts

- User-defined self-executing computer programs running on top of blockchain
- Managing exchange of digital assets
- Applications across many different sectors



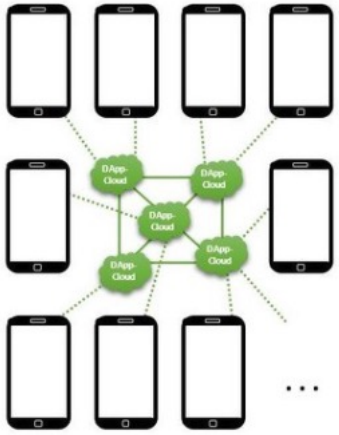

McKinsey&Company

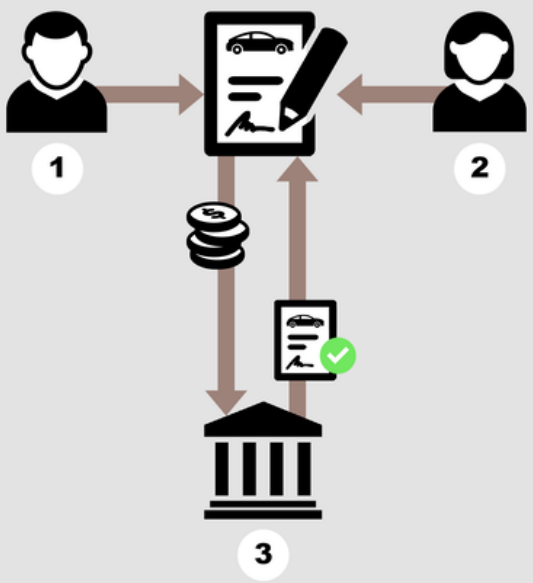
# Decentralized Applications and Smart Contracts

Apps

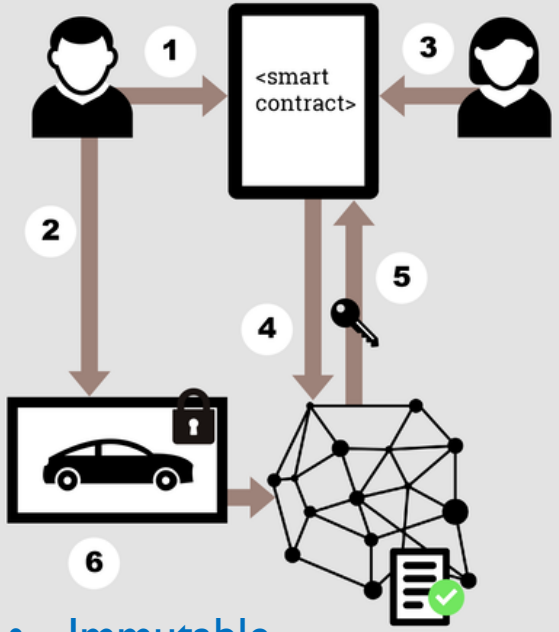
(Centralized)


DApps



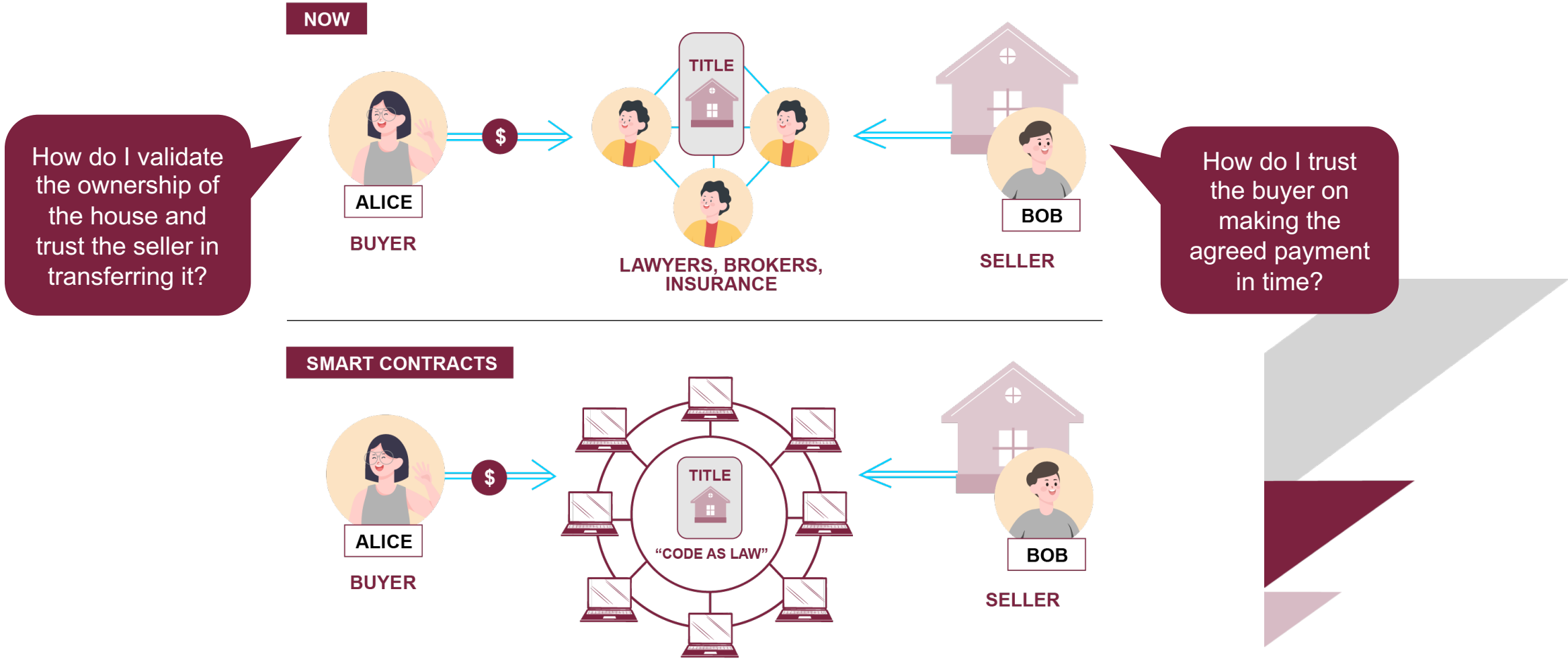



- Relying on intermediaries
- Non-transparent
- Slow and costly

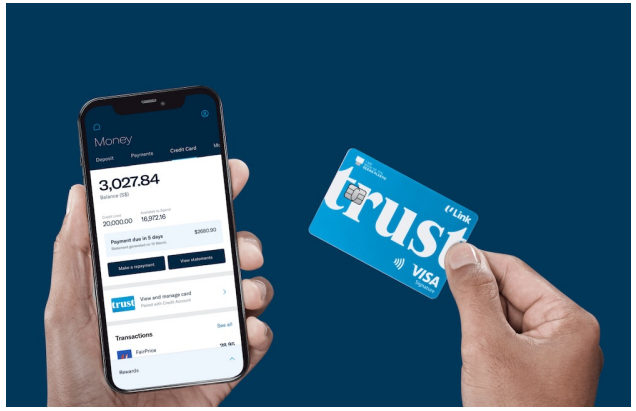



- Immutable
- Self-enforcing
- Affordable and accessible

# Buying a House on Ethereum



# Why is DApp a big thing?




Decentralized finance

- Banking, insurance, decentralized exchange, …
- Nearly $30 billion locked inside
- 4.4 million wallets

- Direct peer-to-peer exchange of surplus electricity
- Reduce transaction costs

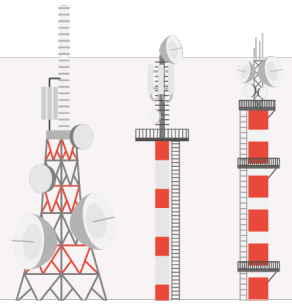
Energy trading

Supply chain management

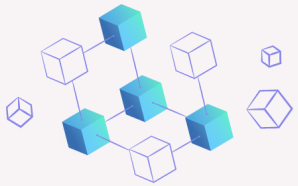
- Better visibility and traceability
- Improve financing, contracting, and international transactions

Internet is the information superhighway, blockchain is the Internet of value

# Blockchain/Bitcoin/Ethereum



Core Tech



Gen 1:
Special Purpose
Apps

Next Gen:
Platform for Apps