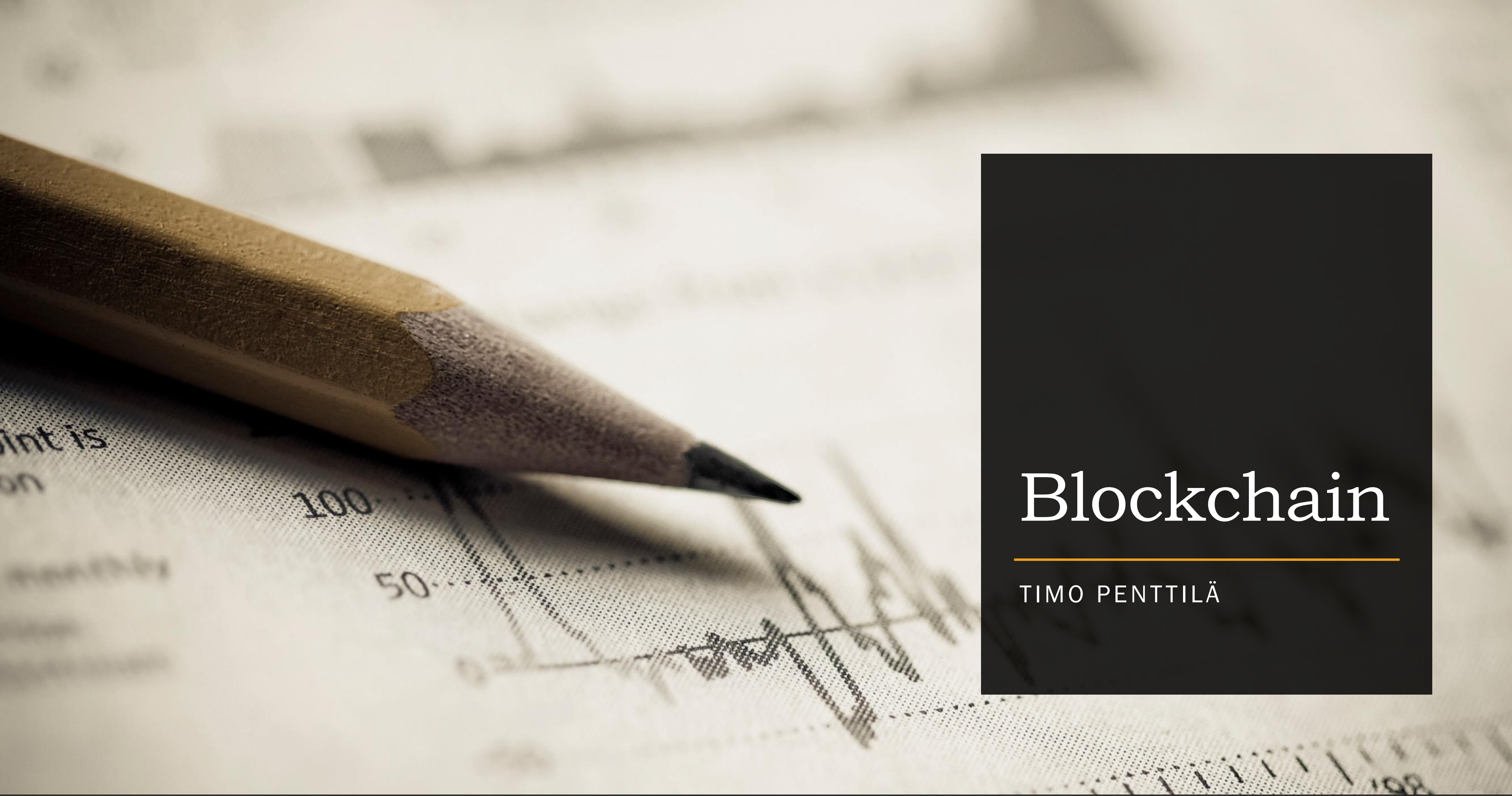


Blockchain

TIMO PENTTILÄ

Blockchain

Originally introduced 1991 by scientist to time stamp data and keep ledger to verify backdated data

Satoshi Nakamoto, Bitcoin 2009

WHY

NFT

Smart Contract

Blockchain <> Cryptocurrencies

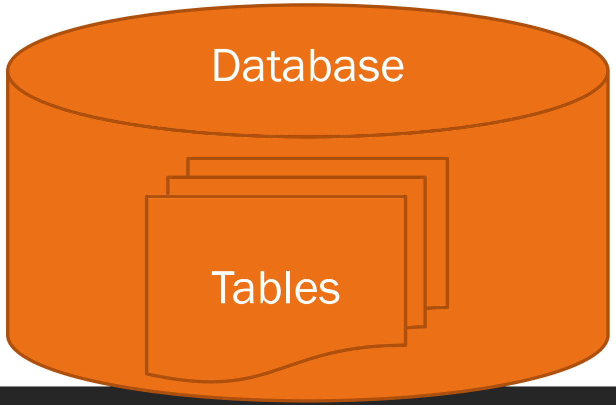
Blockchain is distributed database which is shared with ”blocks” in the network of computers

Blocks are linked by cryptography

Many applications one well known example is Bitcoin (2009) / cryptocurrencies

Information usually transactions in strict order, stored permanently (Distributed ledger)

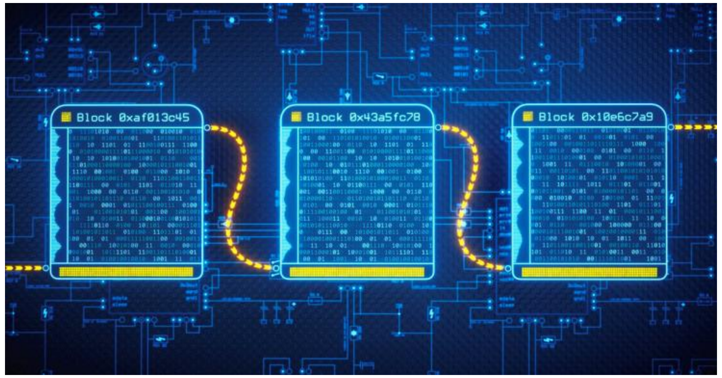
Traditional



Database

Tables

Blockchain



Example

In the class, let’s agree

1. We have network (we can talk and will talk) = “Blocks”
2. We have four people each have identification number each have application to verify cryptographic tokens
3. I have been mining money 100 units and That is verified with “secret token” given to me =stored in “ledger”
4. I transfer money to #1 and with token verify transfer, everyone knows about that =transaction and verification (Verification cryptographic)
5. 1# get token to manage transfered money
6. #2 claims he has the money – that claim can be verified 3 members say they know those tokens belong to #1

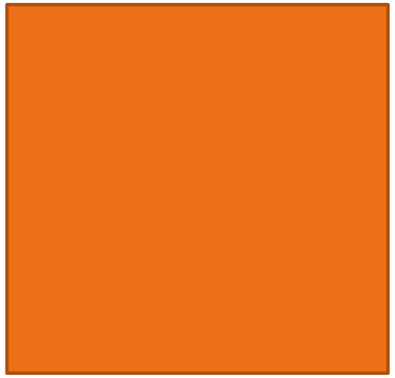
Block

Data (example: transaction from whom – to whom – amount)

Hash jkfd8fdmjkfdf….

Hash of previous block

Hash



Hash: jkfd8fdmjkfdfidie4454t4jkjfdkjkk333jfdk

Hash is unique identifier – hence like fingerprint, pin, password….

Hash will be regenerated if block data changes

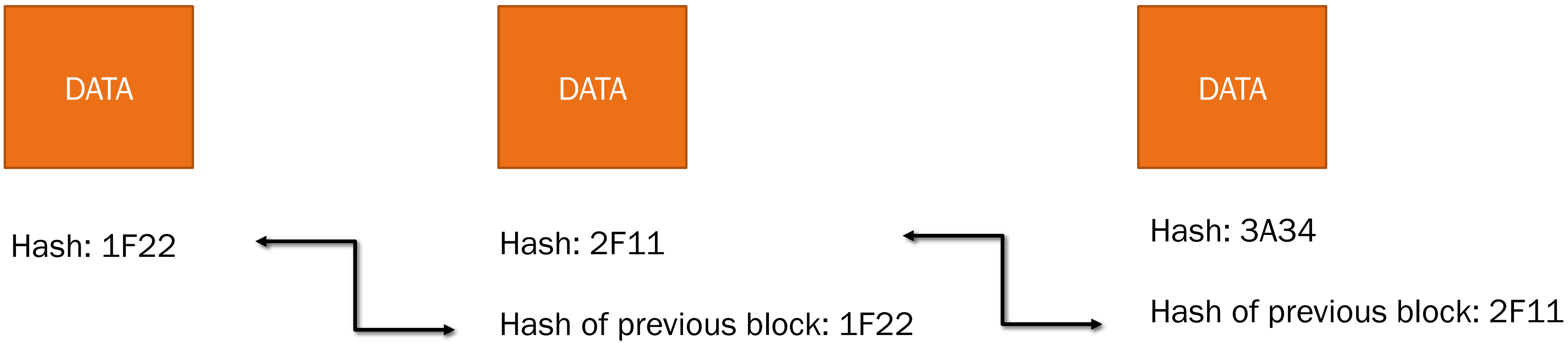
Identifies the Data and content of the block

MyPassword

1234

Blockchain

Genesis Block (First block)



DATA

DATA

DATA

Hash: 1F22

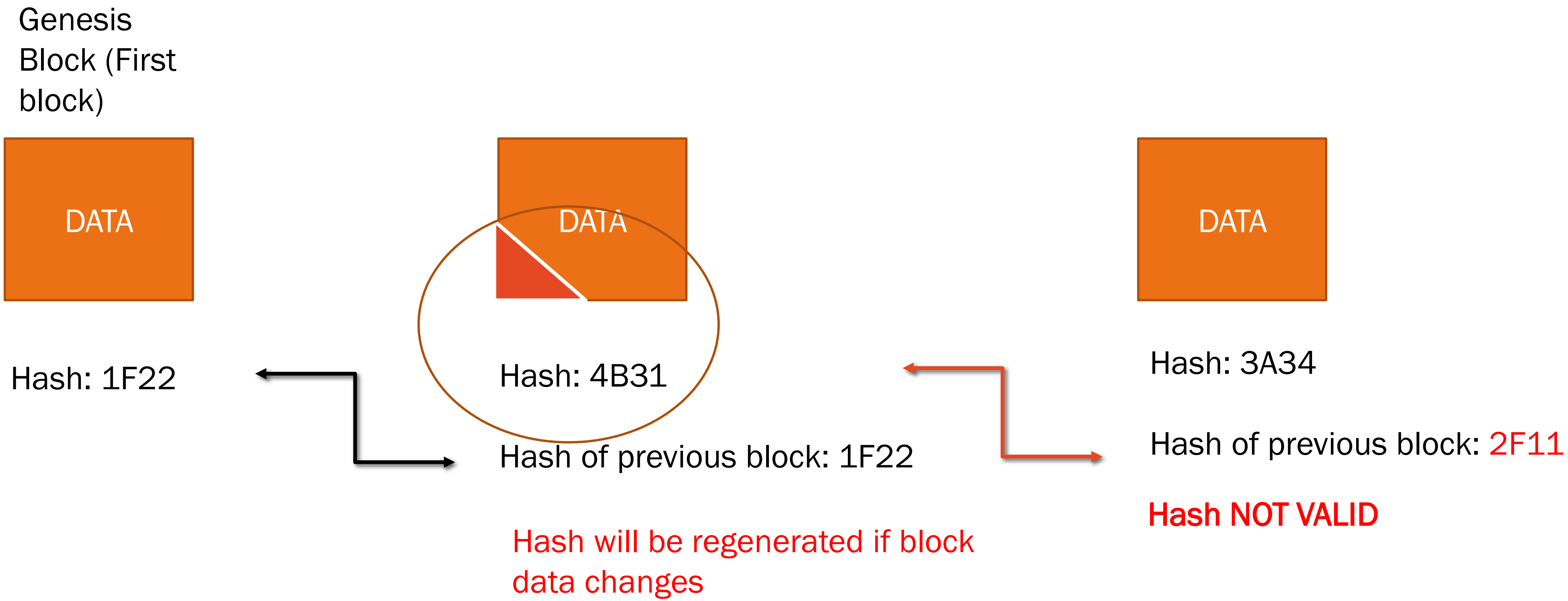
Hash: 2F11

Hash of previous block: 1F22

Hash: 3A34

Hash of previous block: 2F11

Blockchain



Genesis Block (First block)

DATA

Hash: 1F22

DATA

Hash: 4B31

Hash of previous block: 1F22

Hash will be regenerated if block data changes

DATA

Hash: 3A34

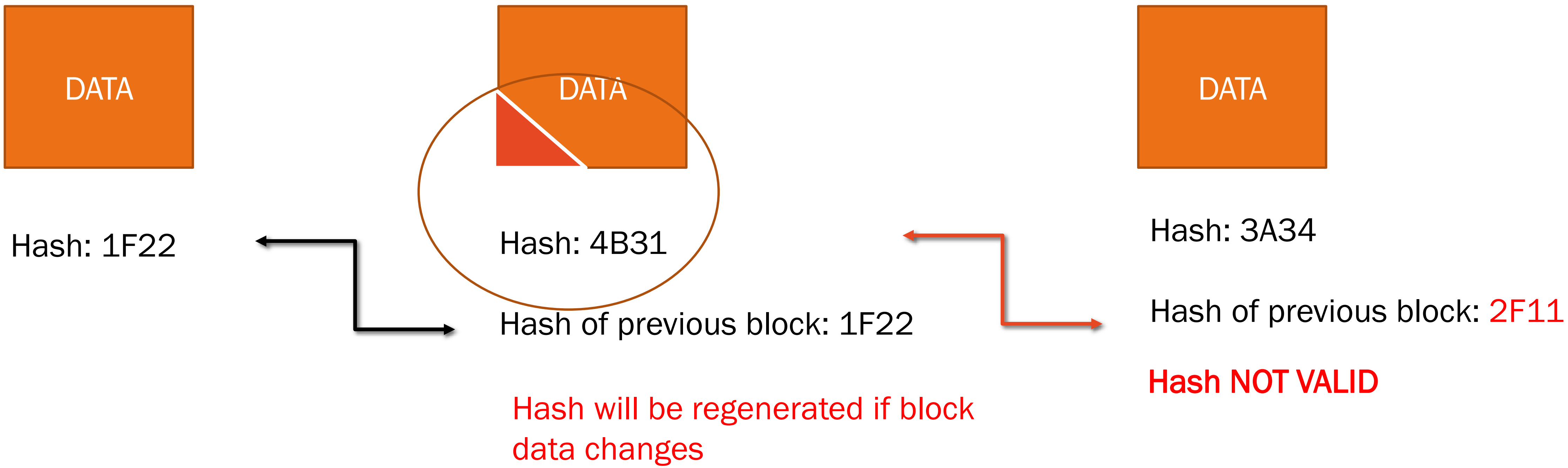
Hash of previous block: 2F11

Hash NOT VALID

Blockchain

Could you recalculate hashes and make blocks valid again??? Yeas but not

Genesis Block (First block)



DATA

Hash: 1F22

DATA

Hash: 4B31

Hash of previous block: 1F22

Hash will be regenerated if block data changes

DATA

Hash: 3A34

Hash of previous block: 2F11

Hash NOT VALID

Proof of work

Slowing down creation of new blocks

decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system

Proof-of-Work requires time to ad new block, Bitcoin 10 minutes

Genesis Block (First block)

DATA

DATA

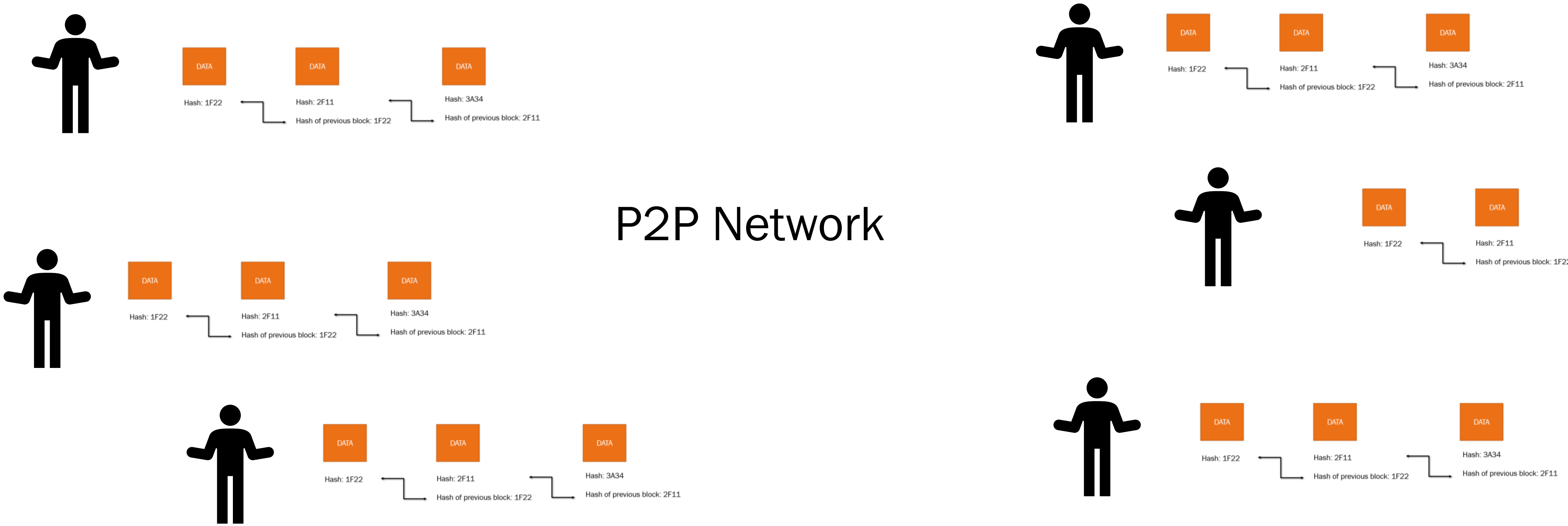
DATA

Proof-of-work
10 minutes

Proof-of-work
10 minutes

If you tamper with one block you need to calculate proof-of-work for all the following blocks

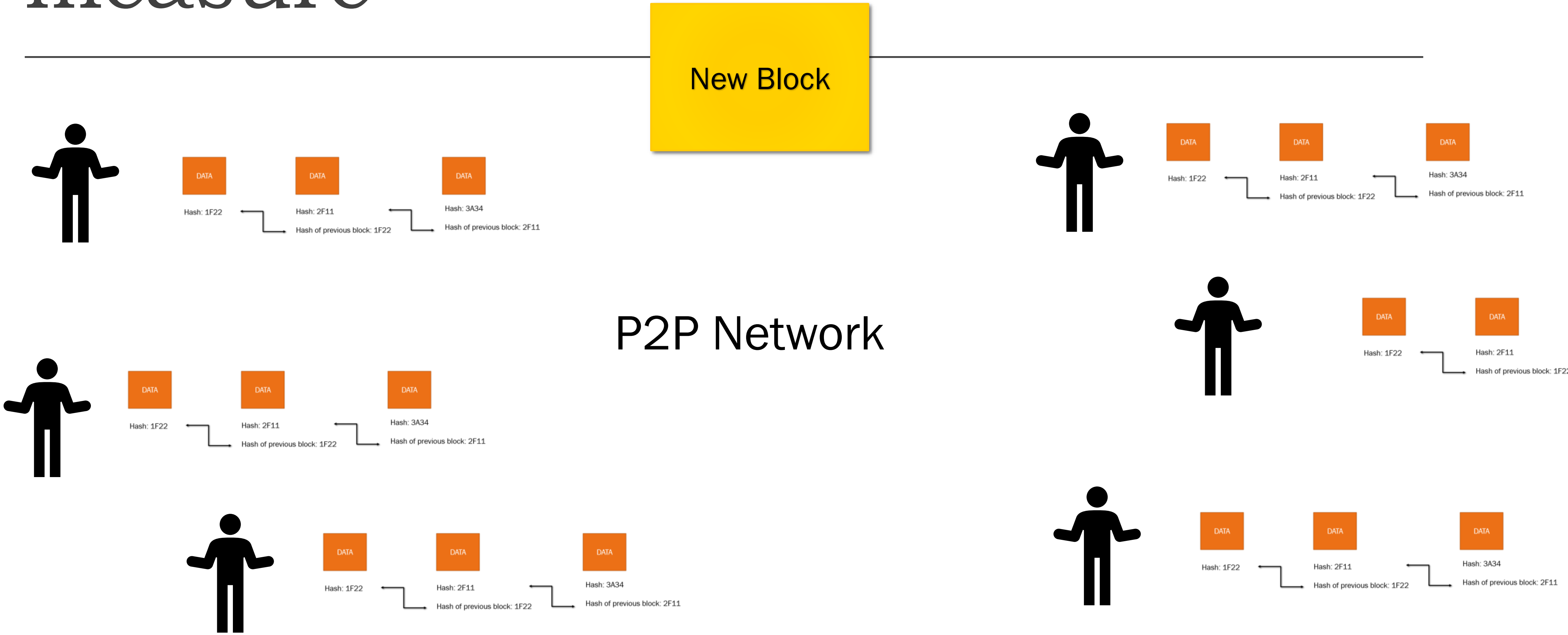
Disributed data – another security measure



P2P Network

DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F2
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11

Disributed data – another security measure

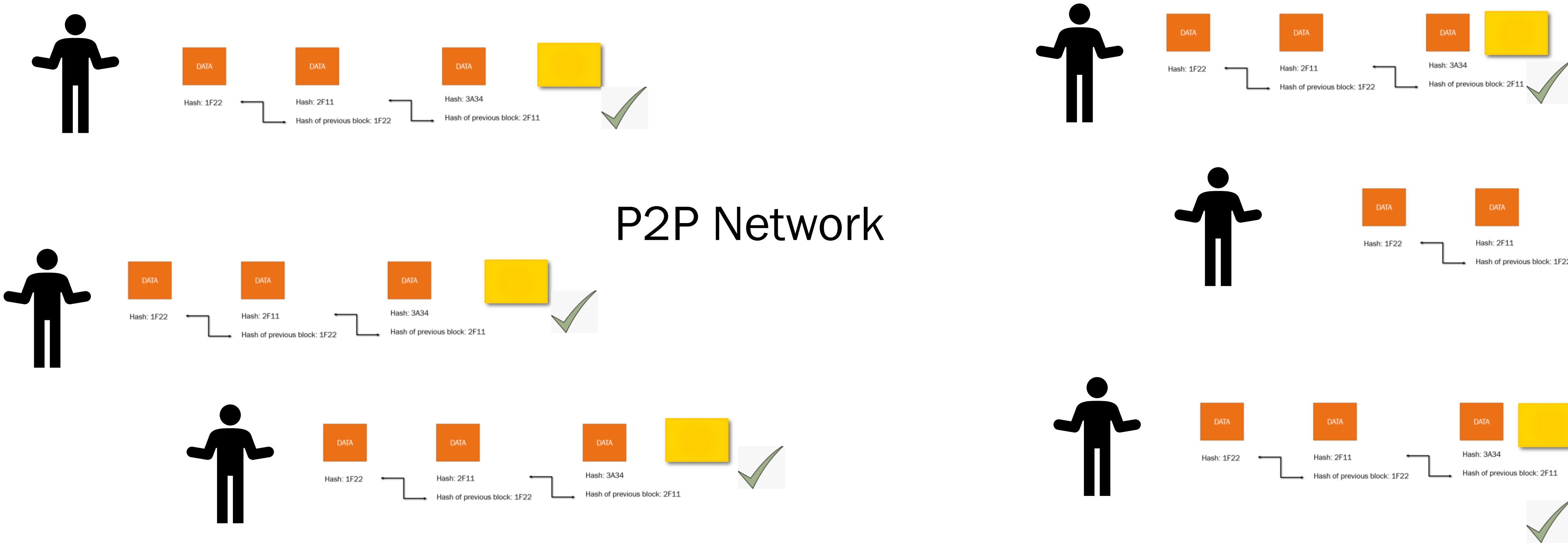


New Block

P2P Network

DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F2
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11

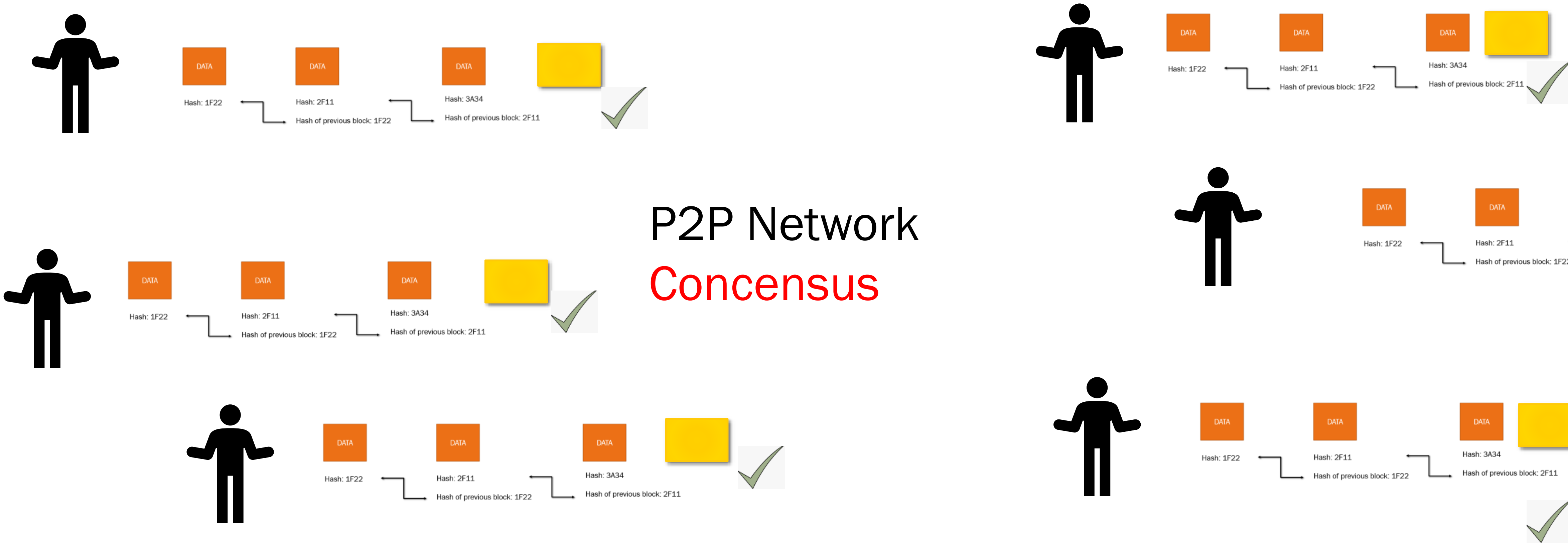
Disributed data



P2P Network

DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F2
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11
DATA
DATA
DATA
Hash: 1F22
Hash: 2F11
Hash of previous block: 1F22
Hash: 3A34
Hash of previous block: 2F11

Disributed data


DATA
Hash: 1F22
DATA
Hash: 2F11
Hash of previous block: 1F22
DATA
Hash: 3A34
Hash of previous block: 2F11
DATA
Hash: 1F22
DATA
Hash: 2F11
Hash of previous block: 1F22
DATA
Hash: 3A34
Hash of previous block: 2F11
DATA
Hash: 1F22
DATA
Hash: 2F11
Hash of previous block: 1F22
DATA
Hash: 3A34
Hash of previous block: 2F11
DATA
Hash: 1F22
DATA
Hash: 2F11
Hash of previous block: 1F22
DATA
Hash: 3A34
Hash of previous block: 2F11
DATA
Hash: 1F22
DATA
Hash: 2F11
Hash of previous block: 1F2
DATA
Hash: 1F22
DATA
Hash: 2F11
Hash of previous block: 1F22
DATA
Hash: 3A34
Hash of previous block: 2F11

P2P Network

Concensus

Proof-of-stake

Originated in 2012 with Peercoin cryptocurrency

Other example Cardano cryptocurrency

Owners of the crypto currence are staking their crypto (while staked can not be used)

More energy efficient

Summary Blockchain Security

In order to change/tamper data

- You need to tamper all the blocks
- Redo the proof-of-work for each block
- Take control of more than 50 % peer-to-peer network

Can not be done

Mining

Why one would let blockchain to use his computer for complex lengthy proofing work

Mining is rewarded by issuing new currency for miners

Clockchain locig

Decentralized information

Information cannot no be altered, deleted, added by ”administrator”

”no owner of database”

No trusted party / administrator needed

Distributed ledger technology (DLT)

Bitcoin transaction in blockchain

1. Seller and Buyers Agree on transaction
   1. Seller send reference to previous transaction, amount and buyers public key
   2. Seller signs message with private key
2. Blockchain alerts miners on pending transaction
3. Transacton is added to group of transactions that has happened the same time to be validated by miners. => blocks unique id number, time of creation, reference to previous block
4. Verifcation requiring miners to solve cryptographic computationlan work (proof of work) => results published in the network

Cryptocurrency Exchanges

Trading usually in Exchanges

ETC........
ETC.......

GEMINI

BINANCE.US

crypto.com

coinbase

FTX

NFT – Non-fungible Token

Non-fungible tokens, often referred to as NFTs

Blockchain-based tokens that each represent a unique asset

- piece of art
- digital content
- or media
- Painting, collectible, music, movie…….

An NFT can be thought of as an irrevocable digital certificate of ownership and authenticity for a given asset, whether **digital or physical**

Smart Contract

Self-executing contract with the terms of the agreement

Executed deterministically in the context of a blockchain network

Primary means by which developers can create and manage tokens on a blockchain

Run when predetermined conditions are met.

Typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome

Programming language examples: Solidity, Vyper

Fuksi/Mursu Passi (Fresman pass)

Goal to collect stamps “other achiments)

Become teekkari or even Superfuksi

Need to have ledger

Must be secure

(Should not be stolen, loss,……….)

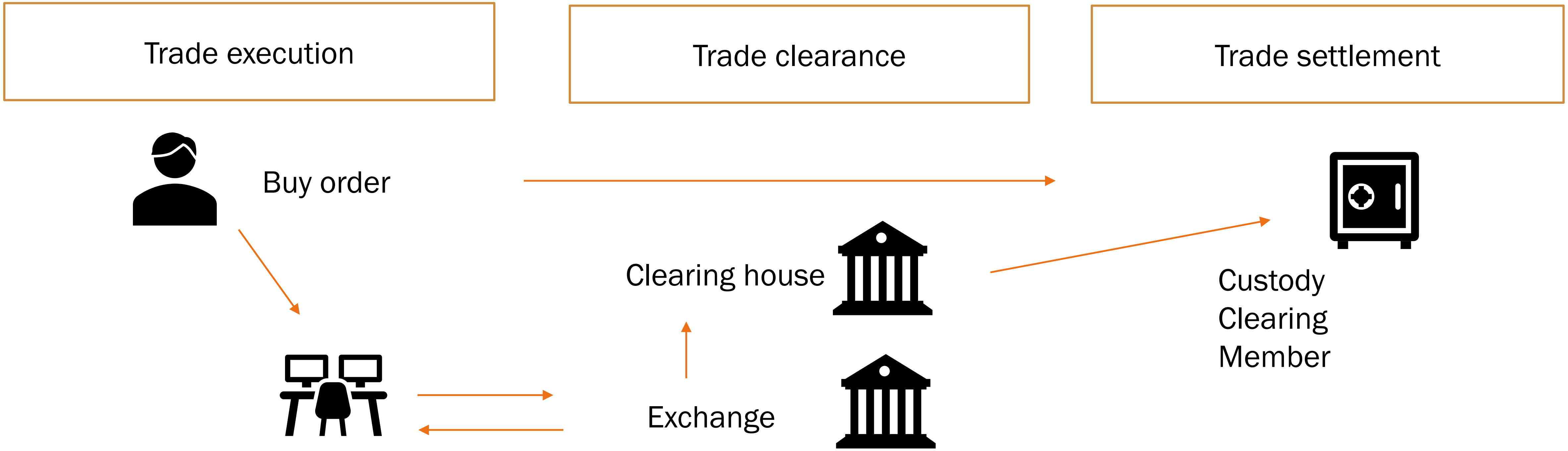
Custody and Exchange

electronic form of securities

maintenance of shareholder, bearer and creditor registers

effective reporting on changes in holdings

Custody and Exchange



Trade execution

Trade clearance

Trade settlement

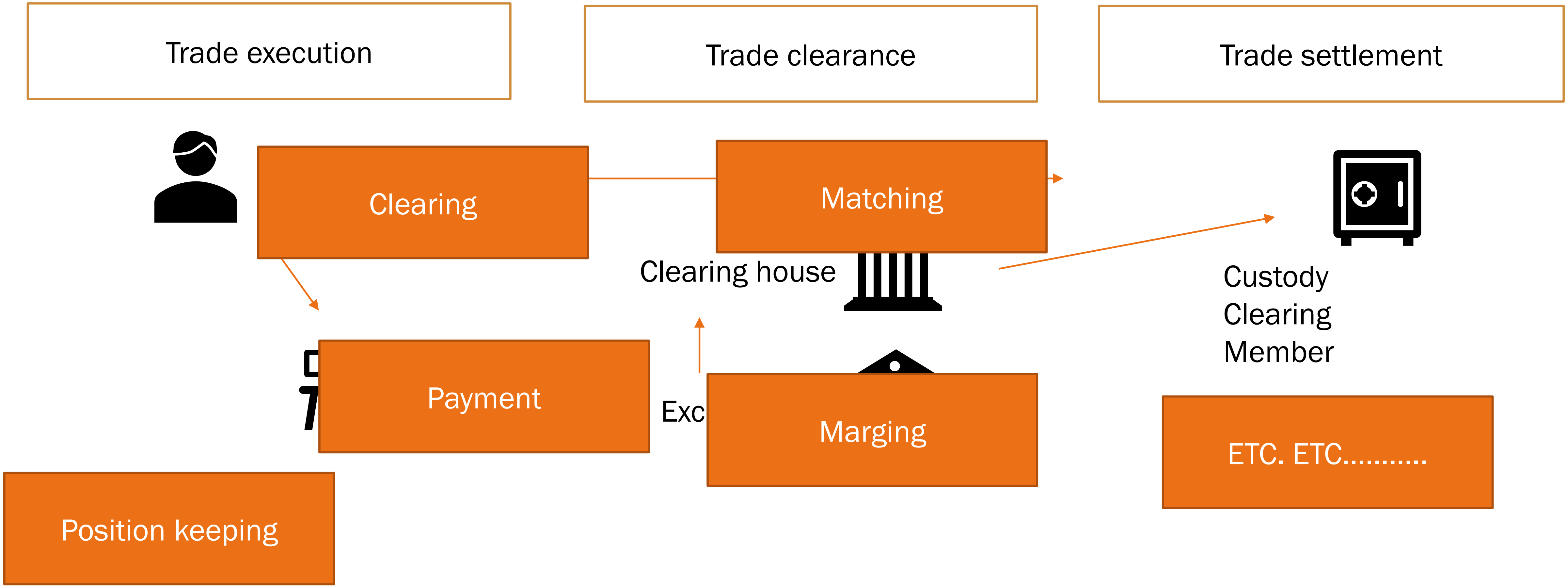
Buy order

Clearing house

Exchange

Custody Clearing Member

Custody and Exchange



Trade execution

Trade clearance

Trade settlement

Clearing

Matching

Clearing house

Custody
Clearing
Member

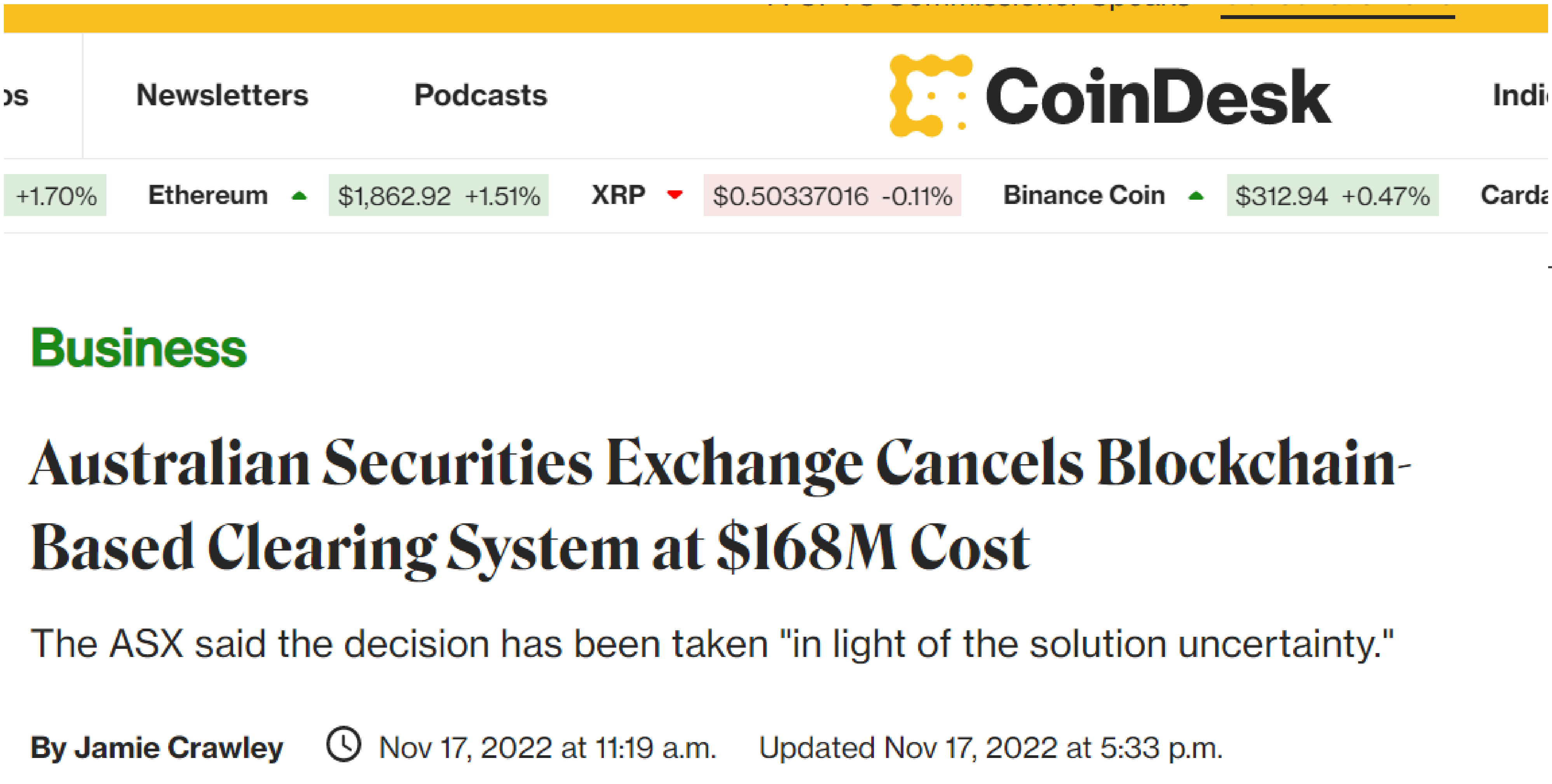
Payment

Exc

Marging

ETC. ETC……….

Position keeping



Business

Australian Securities Exchange Cancels Blockchain-Based Clearing System at $168M Cost

The ASX said the decision has been taken "in light of the solution uncertainty."

By Jamie Crawley Nov 17, 2022 at 11:19 a.m. Updated Nov 17, 2022 at 5:33 p.m.

Exchanges

Deutsche Börse, for example, or Switzerland’s SIX Digital Exchange

Hyperledger

Hyperledger Fabric, an open source project from the Linux Foundation, is the modular blockchain framework and de facto standard for enterprise blockchain platforms. Intended as a foundation for developing enterprise-grade applications and industry solutions, the open, modular architecture uses plug-and-play components to accommodate a wide range of use cases.

With more than 120,000 contributing organizations and more than 15,000 engineer contributors working together, Hyperledger Fabric offers a unique approach to consensus that enables performance at scale while also preserving the data privacy enterprises demand.

adoption by Cloud Service Providers such as AWS, Azure, IBM, Google, and Oracle.

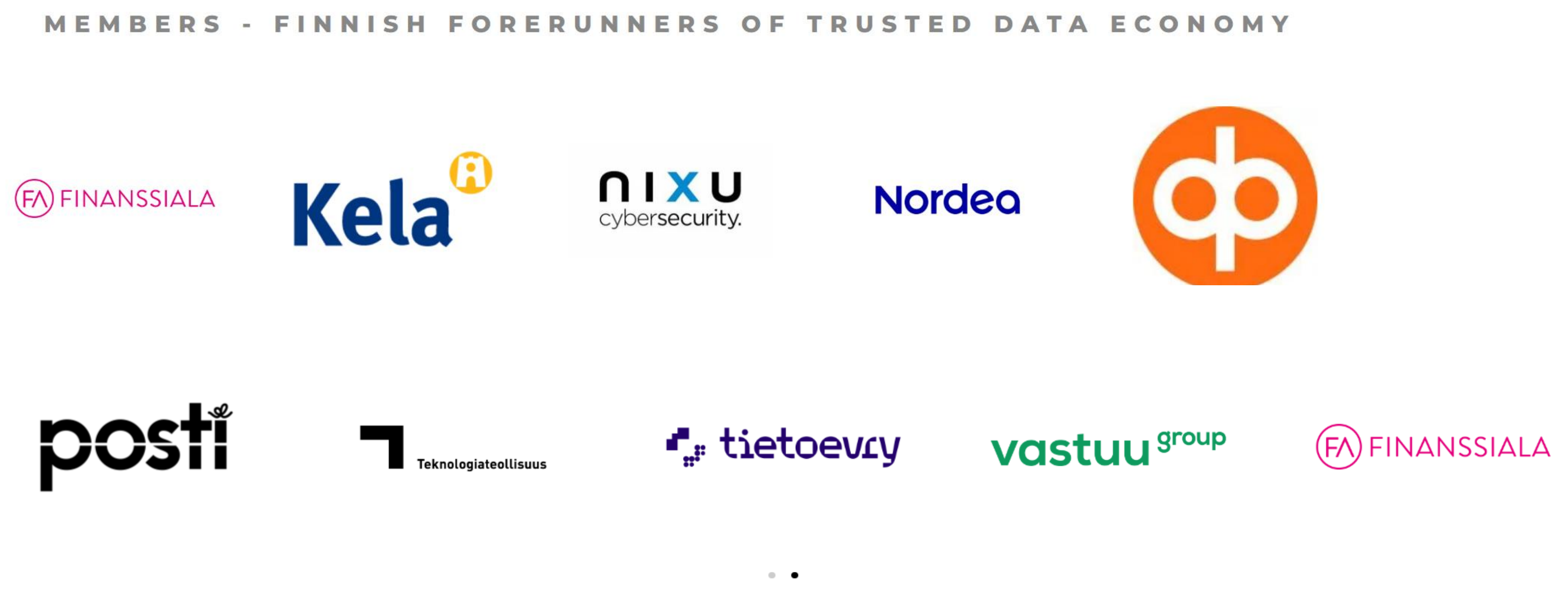
https://www.hyperledger.org/resources/blockchain-showcase

What is hyperledger fabric? | IBM ************

Permissioned architecture • Highly modular • Pluggable consensus • Open smart contract model — flexibility to implement any desired solution model (account model, UTXO model, structured data, unstructured data, etc) • Low latency of finality/confirmation • Flexible approach to data privacy : data isolation using ‘channels’, or share private data on a needto-know basis using private data ‘collections’ • Multi-language smart contract support: Go, Java, Javascript • Support for EVM and Solidity • Designed for continuous operations, including rolling upgrades and asymmetric version sup-port • Governance and versioning of smart contracts • Flexible endorsement model for achieving consensus across required organizations • Queryable data (key-based queries and JSON queries

Findy - Hyperledger

The Findynet Cooperative is Finnish public-private organisation that develops a general-purpose, shared, and secure verfiable data network — a way to ensure the authenticity of information required in e-services.



MEMBERS - FINNISH FORERUNNERS OF TRUSTED DATA ECONOMY

Crypto examples

Bitcoin and Bitcoin Cash (BTC/BCH), Ether (ETC), Ripple Coin (XRP), Litecoin (LTC)

Quadriga CX- whose co-founder then died apparently with the password to his clients' funds

OneCoin—A textbook scam of the multi-level marketing Ponzi scheme variety. $350 million lost and 18 founders jailed by Indian authorities.

Enigma—Poor execution failed this cryptography and security service. The CEO was hacked losing $500k, which killed their security imprimatur.

Droplex—A scam ICO that literally copied another company’s whitepaper (QRL) by doing a global find and replace. Still, they made off with $25k of investors’ cash.

Coindash—A hacker boosted $10 million off this Israeli startup via a phishing site. Rumours of an inside job continue to plague their team.

Veritaseum—YouTube ads pumped up this ICO before $5.4 million in coins were stolen and quickly converted to Ethereum. Claims that the Veritaseum team engineered the hack to pocket funds continue.

Parity—Straight-up hack of the multisignature wallet by exploiting a flaw in the code and two-step verification process. White hat hackers were able to recover most of the stolen Ether.

NFT Examples

MANA, Decentraland (MANA) is a virtual reality real estate platform that allows users to create, experience and monetize content as well as applications.

SAND, the main utility token and medium of exchange in The Sandbox ecosystem, allowing users to own, build and monetize their gaming experiences.

AXS, Axie Infinity is a blockchain-based trading and battling game represented by Axies, the in-game NFT characters.

GALA, the native token of Gala Games, a player-owned blockchain gaming platform of different blockchain games. Players that own NFTs can influence the governance of games within the Gala Games ecosystem. The GALA token is used to buy items, upgrades, and other in-game assets and also functions as the governance token.

ENJ, Enjin coin is a project of Enjin, a company aiming to offer blockchain gaming products that make it easy for everyone to develop, trade, monetize, and market with blockchain. ENJ is a digital store of value used to back the value of blockchain assets like NFTs, giving in-game items real-world liquidity.

Applications

Cryptocurrencys (start via ICO= Initial Coin Offering)

NFTs (NonFungible Token), represent ownership rights to unique digital or real-world assets

NFT coins are fungible, can be traded or exchanged for another NFT coin of the same value

Insurance

Real Estate records

Payments (RippleNet)

National payments/currencies (Dubai, Brazil, Canada,,,,)

Passports, Certificates,,,,,,

Non Financial +++++++++

Some Challenges in Legal Perspective

Legal framework unclear – smart contract are not contracts

Some countries restricting use (Qatar, China, Turkey, Russia (partly), North Macedonia. …

GDPR (General Data Protection Regulation)

Anti Money Laundering

TAX

The Untold Story of Blockchain. Be it investors, startups or corporates… | by Nishant Modi | Medium

Use cases of blockchain technology in business and life (insiderintelligence.com)

Quadriga Fintech Solutions - Wikipedia