

# Introducción a Blockchain y Criptomonedas

GFT

Esteban Chiner

EDEM - MDA

Fecha 19/12/2020

# About me

- Working in GFT as a **Senior Architect** specialized in Big Data and Blockchain
- Part of the technological **Business Development** team
- Leading the “**Data**” and “**DLT & Crypto**” domains
- **Certified Bitcoin Professional** 
- **Certified Blockchain Architect**  Blockchain Council

- **Lecturer**

- Big Data & Analytics Master (**UPV**) – “Big Data Architectures in Financial Services”
- Data Analytics for Enterprises (**EDEM**) – Seminar on Blockchain
- Seminars d’Empresa (**UPC**) – “Developing decentralized apps with Ethereum”

- **Distributed Ledger Technologies Courses:**

- Bitcoin and Cryptocurrency Technologies
- Ethereum Developer: Build A Decentralised Blockchain App
- Ethereum Blockchain Developer: Build Projects Using Solidity
- Game Theory

- **Traveller, “Photographer”, Geek and Fan** of cryptos and decentralization



## My Bio:

0xD732650550dF069B7C25cbf1c701b678ccE35e24

(Rinkeby)



[@echiner](#)



[echiner](#)



[esteban.chiner@gft.com](mailto:esteban.chiner@gft.com)

# Why GFT

**“We provide enterprise grade blockchain services you can trust”**



## OUR CLIENTS



## OUR PARTNERS



## GLOBALLY RECOGNIZED

*One of the top financial services providers worldwide*



*“Market Guide for Blockchain Services”*



*“Major Contenders”*



**DISCLAIMER**



**DISCLAIMER**

**I am not a financial advisor  
Educational purposes  
Evaluations based on technology  
DYOR**



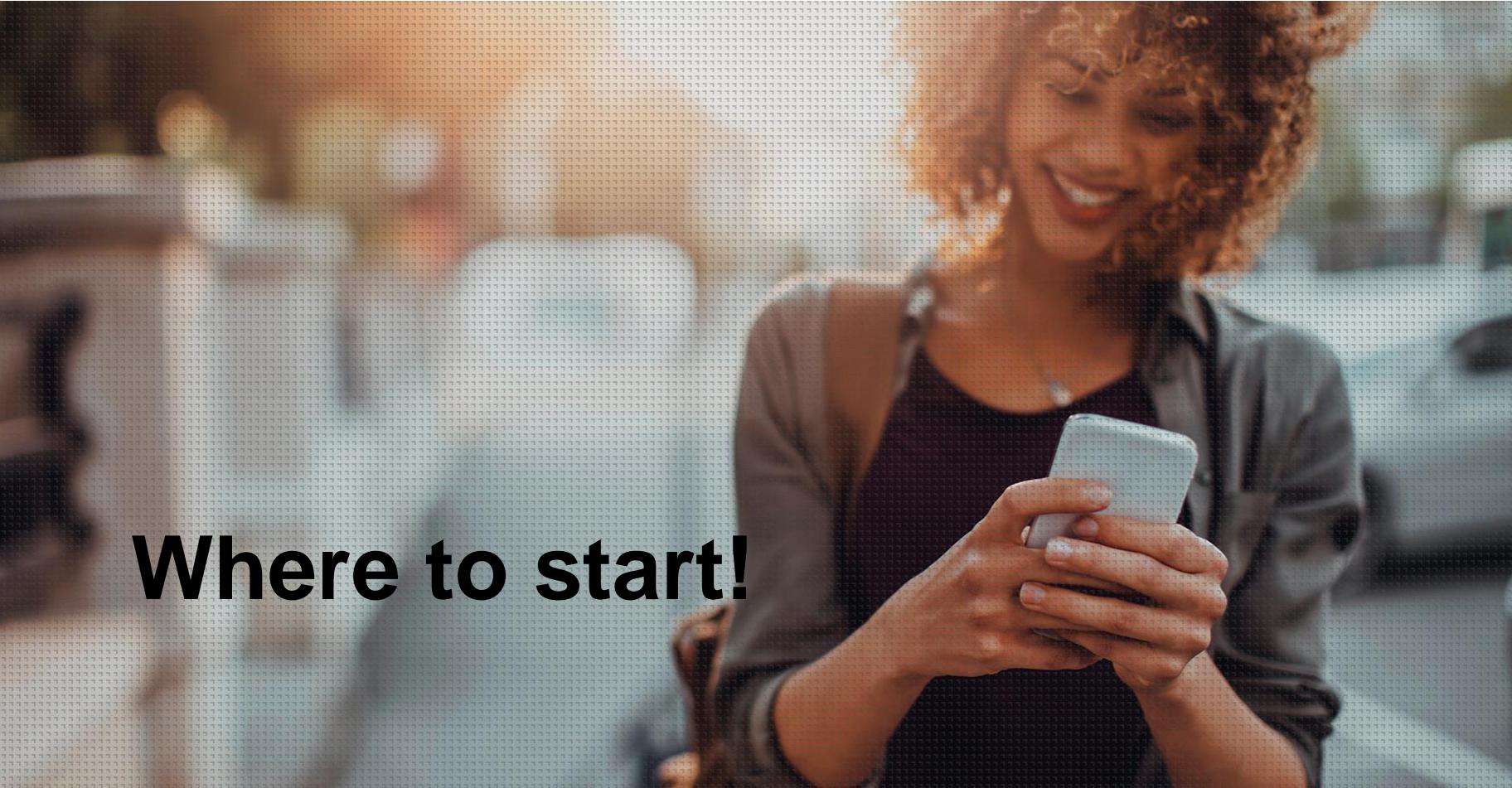
**DISCLAIMER**



**DISCLAIMER**

# Agenda

- 1. The basics**
- 2. A little bit of history**
- 3. Cryptocurrencies**
- 4. How does Blockchain work? Smart Contracts**
- 5. Tokenization & Decentralized Finance**
- 6. Benefits & Challenges**
- 7. Real use cases**
- 8. DLT Implementations**
- 9. More on decentralization**

A woman with curly hair is smiling and looking down at her smartphone. She is wearing a dark long-sleeved shirt. The background is blurred, showing what appears to be an office environment.

# Where to start!

# Let's start with the basics

# Basic concepts

- **bitcoin**: Popular virtual decentralized currency
- **Cryptocurrencies**: Digital asset used as a medium of exchange, i.e. decentralized currency, in which transactions are verified using cryptography
- **Bitcoin**: Protocol used by the “bitcoin” cryptocurrency
- **Blockchain**: Underlying technology used by cryptos (e.g. bitcoin) or other technologies (e.g. Ethereum)
- **DLT**: Distributed Ledger Technologies

## Cryptocurrencies



and **many** others!

## DLT

### Blockchain



### Tangle



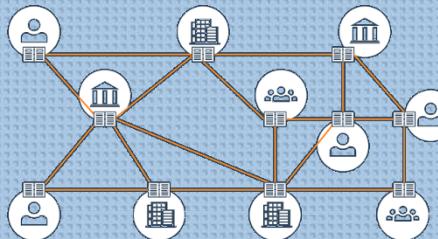
### Hashgraph



# Introduction to Distributed Ledger Technologies

What is a **Distributed Ledger Technology?**

«**Consensus of replicated,  
shared, and synchronized  
digital data**



# What is a DLT?



## Data repository

*Used for storage*



## Decentralized

*No central authority*



## Secure

*By the use of cryptography*



## Transparent

*All data is public*



## Immutable

*Unable to change history*



## Autonomous

*Using Smart Contracts*

# What is NOT a DLT (today)



## Big Data

*Not for big data volumes*



## Bitcoin

*At least “not only”*



## Real-time

*Latency related to mining*



## Mature

*Still evolving*



## Relational database

*There is not “transactionality”*



## A product

*Many implementations*

# So, what is the difference between DLT and Blockchain?

- “A distributed ledger technology (or DLT) is **a consensus of replicated, shared, and synchronized digital data** geographically spread across multiple sites, countries, or institutions. There is no central administrator or centralized data storage.”

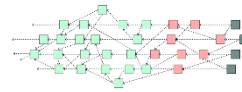
[Wikipedia](#)

## Distributed Ledger Technologies

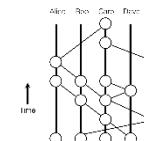
Blockchain



Tangle



Hashgraph



# A little bit of history

## Early days



“We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence.”

“We the Cypherpunks are dedicated to building **anonymous** systems. We are defending our privacy with **cryptography**”

“Privacy is necessary for an open society in the electronic age.”

“Privacy in an open society also requires cryptography”

“...privacy in an open society requires anonymous transaction systems”

# Early days

## Cyphernomicon

### Table of Contents

1. [Introduction](#)
2. [MFAQ -- Most Frequently Asked Questions](#)
3. [Cypherpunks -- History, Organization, Agenda](#)
4. [Goals and Ideology -- Privacy, Freedom, New Approaches](#)
5. [Cryptology](#)
6. [The Need For Strong Crypto](#)
7. [PGP -- Pretty Good Privacy](#)
8. [Anonymity, Digital Mixes, and Remailers](#)
9. [Policy: Clipper, Key Escrow, and Digital Telephony](#)
10. [Legal Issues](#)
  1. [Surveillance, Privacy, And Intelligence Agencies](#)
  2. [Digital Cash and Net Commerce](#)
13. [Activism and Projects](#)
14. [Other Advanced Crypto Applications](#)
15. [Reputations and Credentials](#)
16. [Crypto Anarchy](#)
17. [The Future](#)
18. [Loose Ends and Miscellaneous Topics](#)
19. [Appendices](#)
20. [README](#)

### 12. Digital Cash and Net Commerce

- [12.1 - copyright](#)
- [12.2 - SUMMARY: Digital Cash and Net Commerce](#)
- [12.3 - The Nature of Money](#)
- [12.4 - Smart Cards](#)
- [12.5 - David Chaum's "DigiCash"](#)
- [12.6 - Online and Offline Clearing, Double Spending](#)
- [12.7 - Uses for Digital Cash](#)
- [12.8 - Other Digital Money Systems](#)
- [12.9 - Legal Issues with Digital Cash](#)
- [12.10 - Prospects for Digital Cash Use](#)
- [12.11 - Commerce on the Internet](#)
- [12.12 - Cypherpunks Experiments \("Magic Money"\)](#)
- [12.13 - Practical Issues and Concerns with Digital Cash](#)
- [12.14 - Cyberspace and Digital Money](#)
- [12.15 - Outlawing of Cash](#)
- [12.16 - Novel Opportunities](#)
- [12.17 - Loose Ends](#)

# Bitcoin beginnings

## 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.

## CoinBase

04ffff001d0104455468652054696d65732030332f4a616e2f32302039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73  
(decodificado) ☐☐☐☐☐☐EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks



**Génesis block:** <https://www.blockchain.com/es/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>

# BITCOIN PIZZA DAY



## First crash: Mt.Gox & Silk Road



A screenshot of the Silk Road anonymous marketplace website. At the top, there's a navigation bar with "messages 0", "orders 0", and "account \$0.00". Below that is a search bar and a "Go" button. The main area shows a grid of product listings. On the left, a sidebar lists categories: Drugs (7,052), Cannabis (1,275), Dissociatives (185), Ecstasy (787), Opioids (474), Other (439), Precursors (69), Prescription (1,585), Psychedelics (875), Stimulants (1,044), Apparel (259), Art (114), Biotic materials (1), Books (856), Computer equipment (39), Custom Orders (65), Digital goods (519), Drug paraphernalia (239), Flentamine (69), ICE / 1 POINT (0.1G), 20x 1MG Alprazolam, and 50x MDMA / 1gr pure. Each listing includes a small image of the product and its price.

# Banking on Bitcoin (Documentary)



**BANKING  
ON BITCOIN  
TRAILER**



*Gavitas  
Ventures*



Video: <https://www.youtube.com/watch?v=tmxqlSevtkQ>

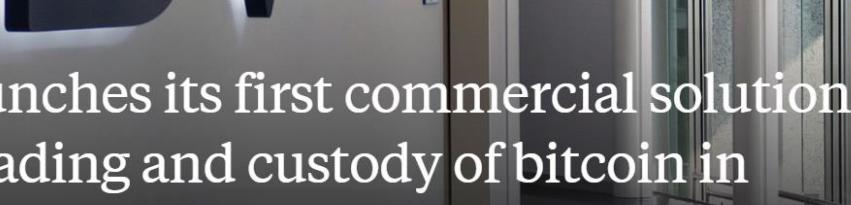
# Blockchain and crypto boom!



# Mainstream

BLOCKCHAIN | 09 Dec 2020

## BBVA launches its first commercial solution for the trading and custody of bitcoin in Switzerland



HELEN PARTZ

DEC 08, 2020

### Facebook hopes to launch its crypto and wallet in 2021, top exec says

News • Technology

## Europe's blockchain infrastructure starts to go live

10 months ago • by Ledger Ins

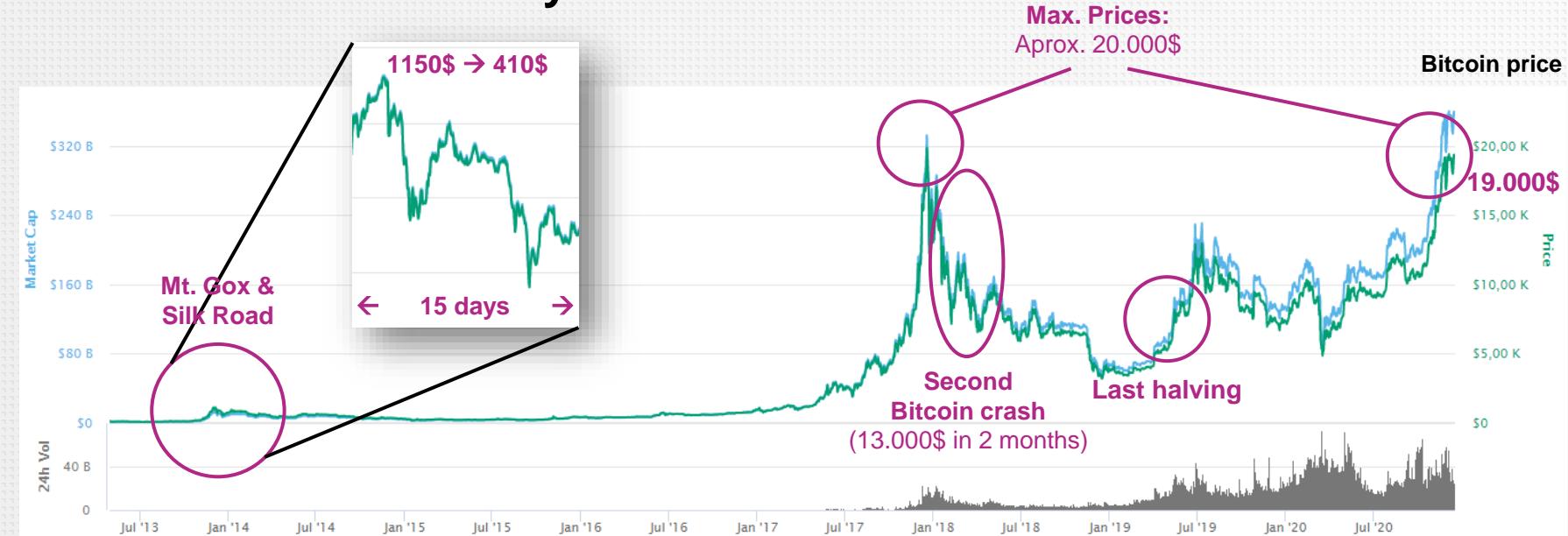


ADRIAN ZMUDZINSKI

JUL 20, 2020

### PayPal to Reportedly Offer Crypto Trading Through Paxos Partnership

# Where we are today

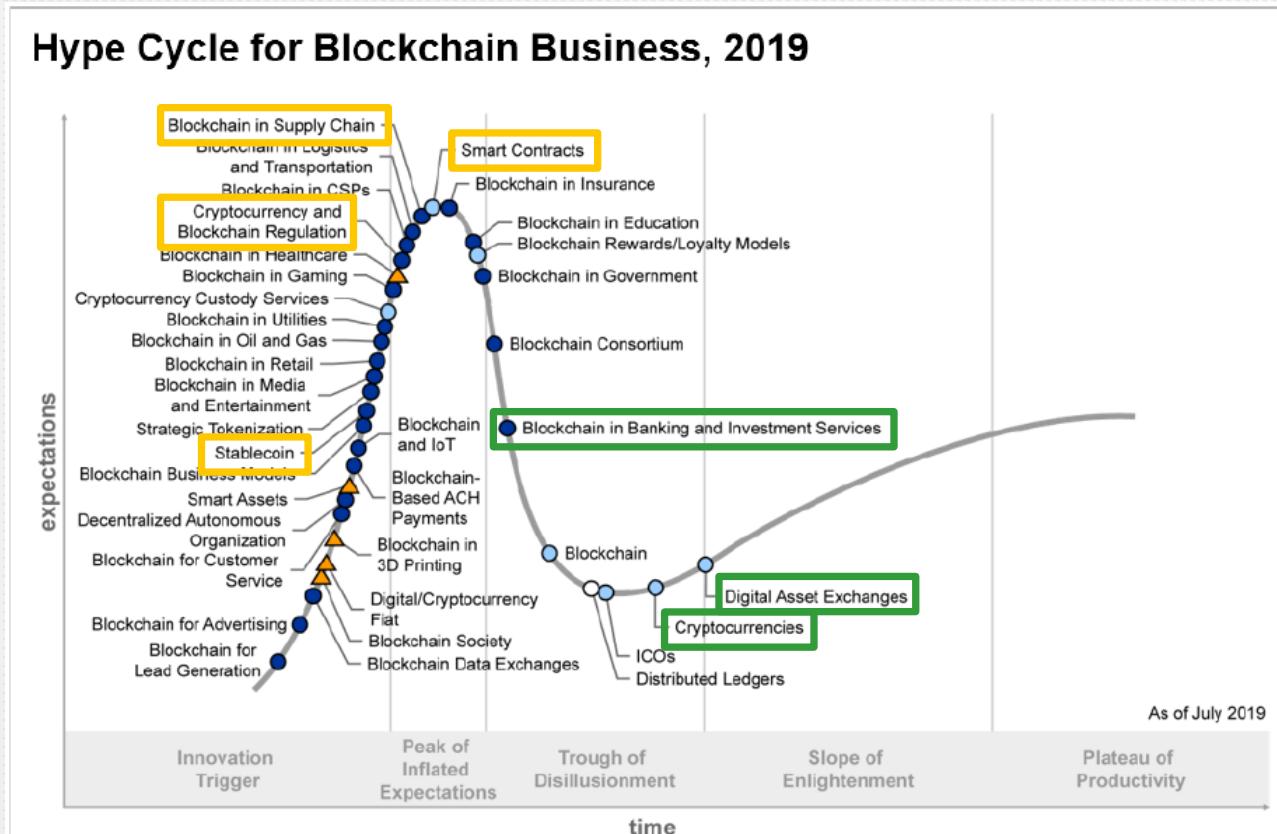


Dozens of **blockchain**  
**implementations**

(Corda, Hyperledger, Quorum, IOTA, DAH, Cardano...)

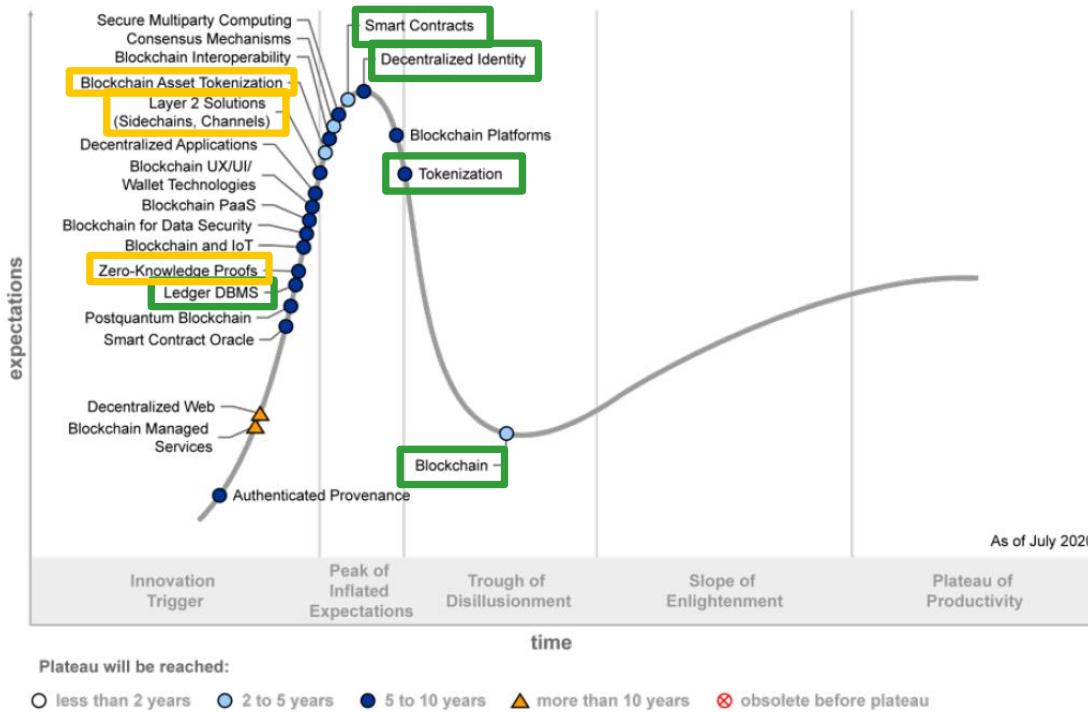
Over 2600 **cryptocurrencies**  
(<https://coinmarketcap.com/all/views/all/>)

# Where we are in 2019 - Business



# Where we are in 2020 - Technology

## Hype Cycle for Blockchain Technologies, 2020



Source: Gartner

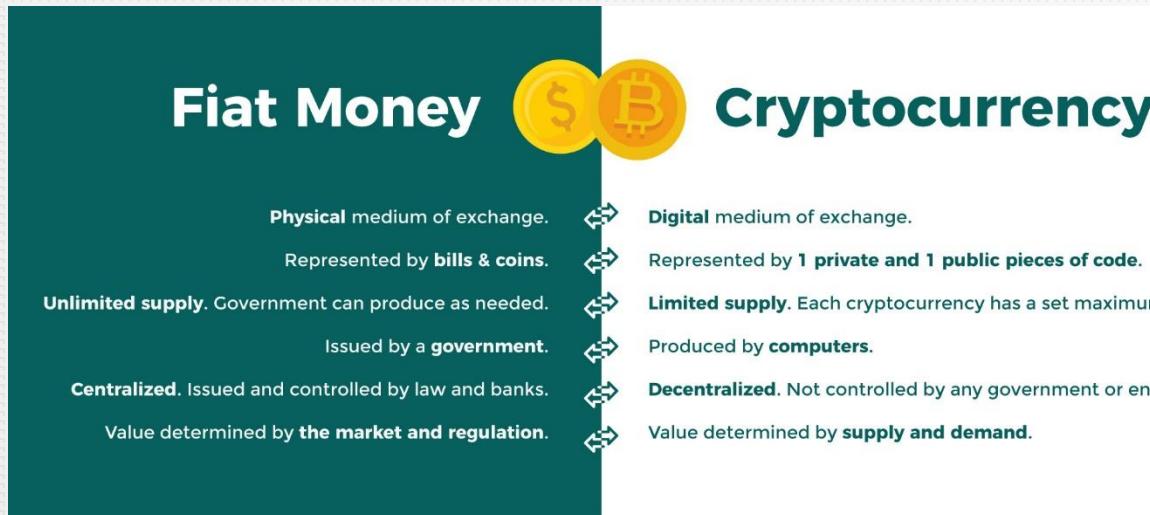
A woman with curly hair is smiling and looking down at her smartphone. She is wearing a dark t-shirt. The background is blurred, suggesting an indoor setting.

Quiz time!

# Cryptocurrencies

# What is a cryptocurrency?

“Digital **currency** 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.” – **Oxford Dictionary**



# Role of money

As discussed in McLeay, Radia and Thomas (2014) **money** is fundamentally a special kind of IOU (or promise to pay) that **performs certain key roles in society**, serving as the following.

**Store of value**



A store of value with which to transfer purchasing power from today to the future.

**Medium of exchange**



A medium of exchange with which to make payments for goods and services.

**Unit of account**



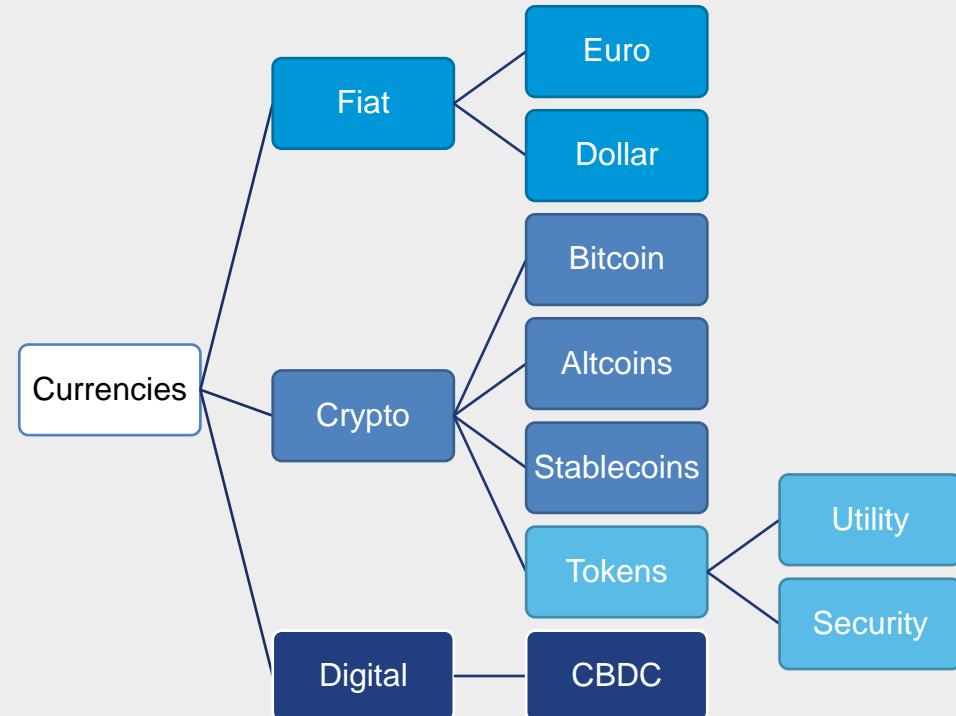
A unit of account with which to measure the value of a particular good, service, savings product or loan.

# Formal definition

- The system **does not require a central authority**, its state is maintained through distributed consensus.
- The **system** keeps an overview of cryptocurrency **units and their ownership**.
- The system **defines whether new cryptocurrency units can be created**. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
- **Ownership** of cryptocurrency units can be proved exclusively **cryptographically**.
- The system allows transactions to be performed in which ownership of the cryptographic units is changed. A **transaction statement** can only be **issued by an entity proving the current ownership** of these units.
- If two different **instructions** for changing the ownership of the same cryptographic units are **simultaneously entered**, the system performs at most **one of them**.



# Types of (crypto)currencies



# Types or sub-types

## Altcoins



**Altcoins** are alternative digital currencies but more often refer to any cryptocurrency other than Bitcoin.

### Examples:

- Litecoin
- Dogecoin
- Bitcoin Cash
- Namecoin

## Stablecoins



**Stablecoins** are cryptocurrencies designed to minimize the volatility of the price of the stablecoin, relative to some "stable" asset or basket of assets (e.g. USD).

### Examples:

- USD Tether
- Diem (f.k.a. Libra)
- DAI
- Paxos

## Tokens



**Crypto tokens**, which are also called crypto assets, are special kinds of virtual currency tokens that reside on their own blockchains and represent an asset or utility.

### Examples:

- Maker
- Augur
- Wrapped BTC
- GFT Coin

# Examples



| #  | Name             | Price       | 24h     | 7d       | Market Cap        | Volume                                  | Circulating Supply  | Last 7 Days |
|----|------------------|-------------|---------|----------|-------------------|---|---------------------|-------------|
| 1  | Bitcoin BTC      | \$19,343.15 | ▲ 1.47% | ▲ 2.77%  | \$359,679,695,607 | \$25,657,607,709<br>1,324,805 BTC       | 18,571,700 BTC      |             |
| 2  | Ethereum ETH     | \$587.72    | ▲ 1.65% | ▲ 2.02%  | \$66,908,070,492  | \$9,371,495,195<br>15,945,454 ETH       | 113,843,044 ETH     |             |
| 3  | XRP XRP          | \$0.475641  | ▼ 3.73% | ▼ 19.19% | \$21,651,533,478  | \$8,703,443,036<br>18,251,426,730 XRP   | 45,404,028,640 XRP  |             |
| 4  | Tether USDT      | \$1.00      | ▲ 0.04% | ▲ 0.01%  | \$19,768,815,218  | \$40,415,619,319<br>40,407,372,080 USDT | 19,764,781,180 USDT |             |
| 5  | Litecoin LTC     | \$81.45     | ▲ 2.52% | ▲ 1.50%  | \$5,412,950,888   | \$3,953,651,765<br>48,275,014 LTC       | 66,093,398 LTC      |             |
| 6  | Bitcoin Cash BCH | \$289.65    | ▲ 7.97% | ▲ 6.13%  | \$5,402,494,009   | \$2,503,611,833<br>8,619,620 BCH        | 18,600,106 BCH      |             |
| 7  | Chainlink LINK   | \$12.68     | ▲ 2.06% | ▲ 0.74%  | \$5,041,812,929   | \$907,932,528<br>71,403,665 LINK        | 396,509,556 LINK    |             |
| 8  | Cardano ADA      | \$0.153982  | ▲ 2.61% | ▲ 5.44%  | \$4,798,111,140   | \$621,721,189<br>4,031,438,706 ADA      | 31,112,484,646 ADA  |             |
| 9  | Polkadot DOT     | \$5.11      | ▲ 5.33% | ▲ 5.73%  | \$4,542,517,074   | \$298,049,354<br>58,248,976 DOT         | 887,762,257 DOT     |             |
| 10 | Binance Coin BNB | \$29.78     | ▲ 3.20% | ▲ 4.63%  | \$4,299,704,393   | \$353,793,363<br>11,882,231 BNB         | 144,406,561 BNB     |             |

# Exchanges

**Exchanges** are businesses that allows customers to **trade cryptocurrencies** or digital currencies for other assets, such as conventional fiat money or other digital currencies (including crypto currencies).

## Features:

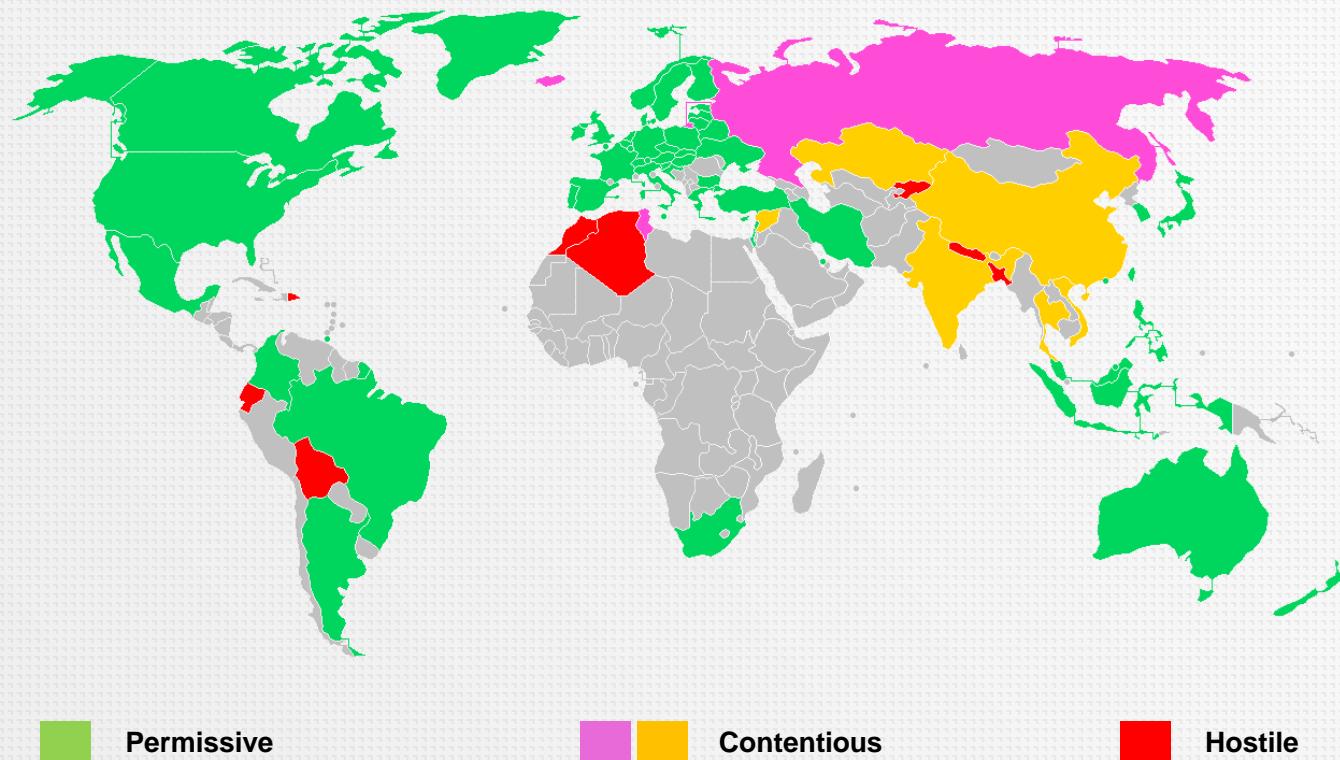
- They hold your wallet
- Allow buying (using credit card or transfer) cryptos, usually charging a fee
  - Fiat to crypto
- Allow withdrawing , usually charging a fee
  - Crypto to fiat
- Allow trading between cryptocurrencies
- Nowadays, many others!!!
  - Deposit, Futures, credit card, staking...



Demo  
(Binance)



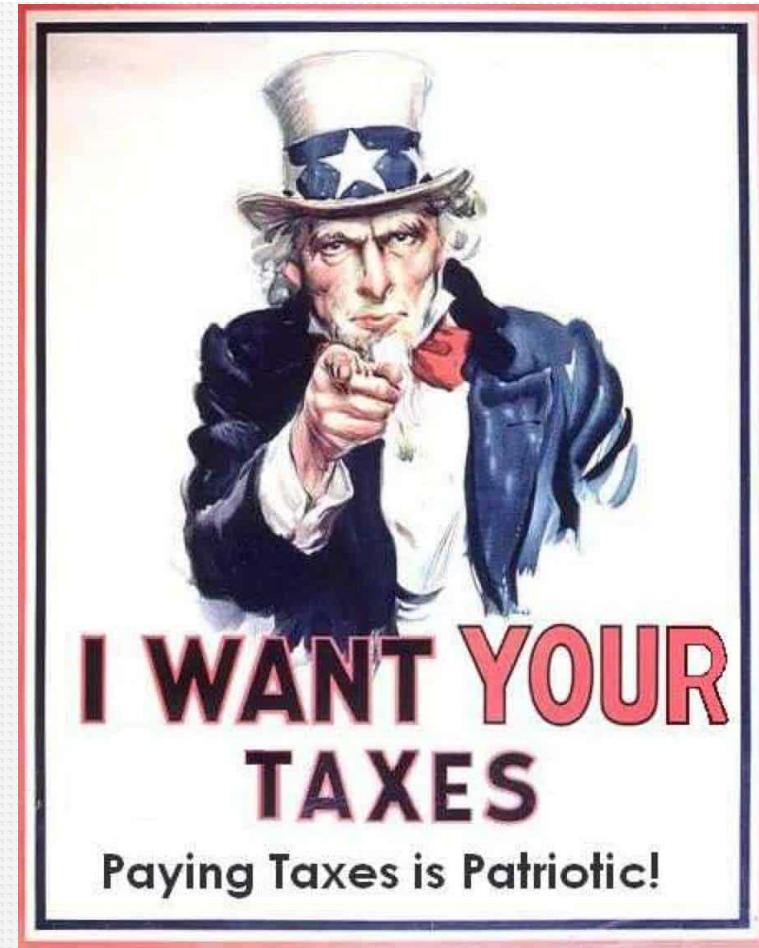
# Legality



# Taxation (in Spain)

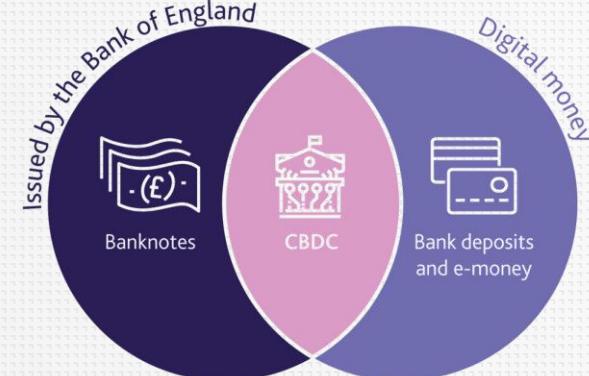
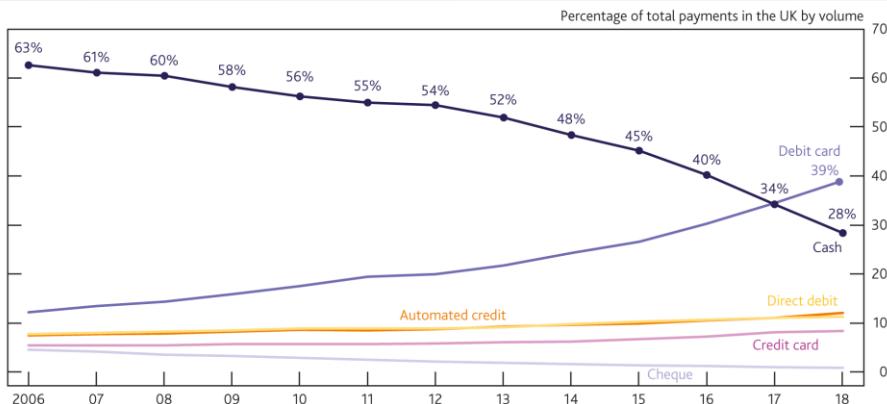
- **Trade** (crypto/crypto or crypto/fiat)
  - Patrimony increase (buy price – sell price)
- **Derivatives** (Futures & Options)
  - Patrimony increase (price difference)
- **Staking**
  - Interests (same as bank account)
- **Mining** (PoW)
  - Economic activity
- **Airdrops & Hardforks**
  - Patrimony increase (not due to transmission)

Source (Binance/Seico): <https://www.youtube.com/watch?v=AblcfSvuwAY>



# Central Bank Digital Currencies (CBDC)

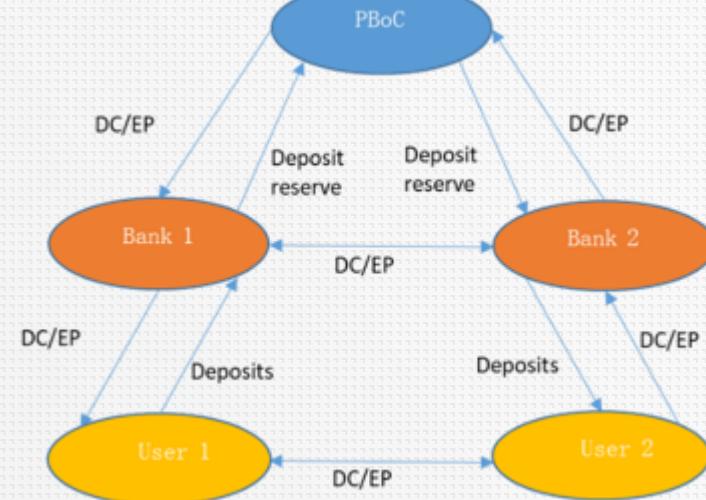
A Central Bank Digital Currency (CBDC) is a digital asset **issued by a central bank** for the purpose of **payment and settlement**, in either retail or wholesale transactions.



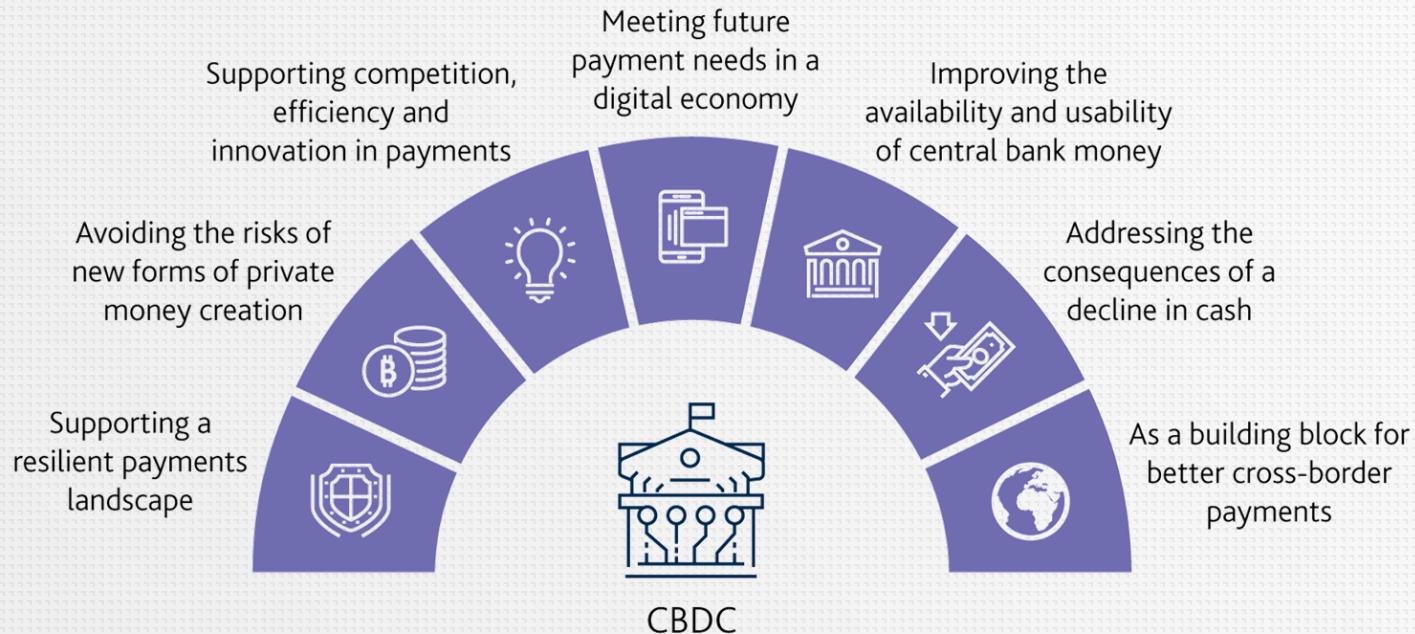
A '**retail**' CBDC would be used like a digital extension of cash by all people and companies, whereas a '**wholesale**' CBDC could be used only by permitted institutions as a settlement asset in the interbank market.

# CBDC

- **Central Bank Digital Currency** (CBDC) is the digital form of fiat money (a currency established as money by government regulation, monetary authority or law)
- Although directly inspired by Bitcoin, CBDC is **different from cryptocurrency**, which are not issued by the state and lack the legal tender status declared by the government
- Proposed implementations **may not even use** any sort of **distributed ledger**
- CBDCs are presently in the hypothetical stage, with some proof-of-concept programmes:
  - China (**Digital Currency Electronic Payment – DCEP**)
  - Sweden (using Corda)
  - Thailand (using Corda)



# Uses



## Crypto Jargon

DYOR

HODL

FOMO

ATH

JOMO

BEAR

WHALE

A woman with curly hair is smiling and looking down at her smartphone. She is wearing a dark top. The background is blurred, suggesting an indoor setting.

Quiz time!

# How does Blockchain work?

## Deep dive into Blockchain

# What is Ethereum

*“Ethereum is an **open-source, public, blockchain-based distributed** computing platform and operating system featuring **smart contract** (scripting) functionality”*

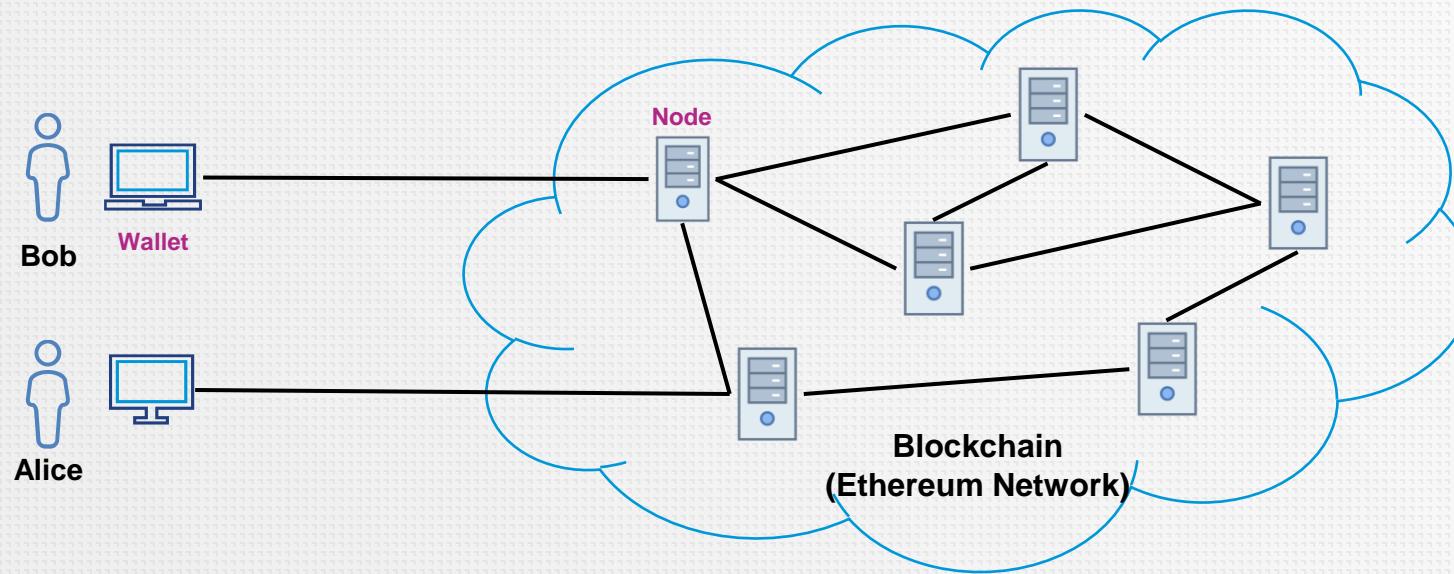


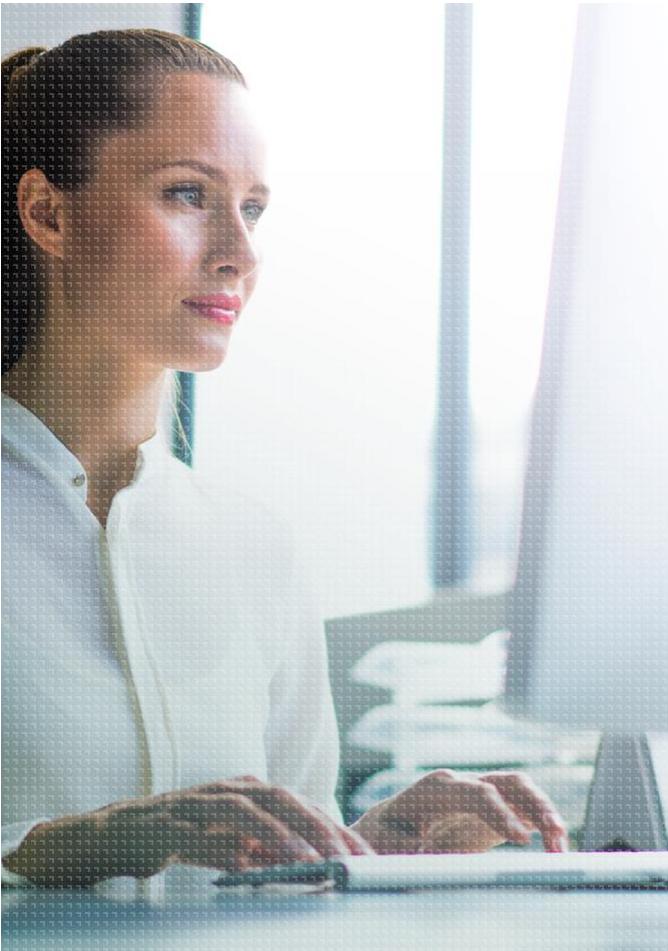
ethereum



# Basic concepts

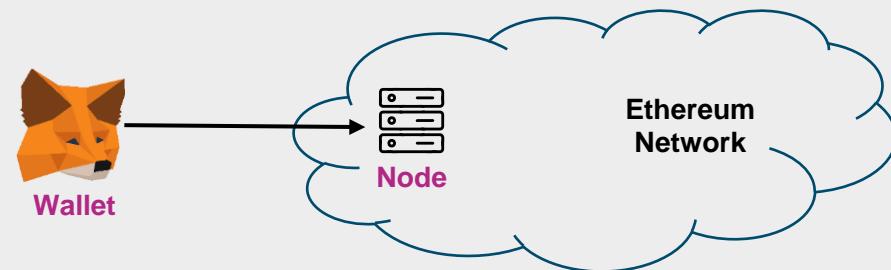
- **Nodes** implement the Ethereum protocol and run on the client side
- **Wallets** hold the users account





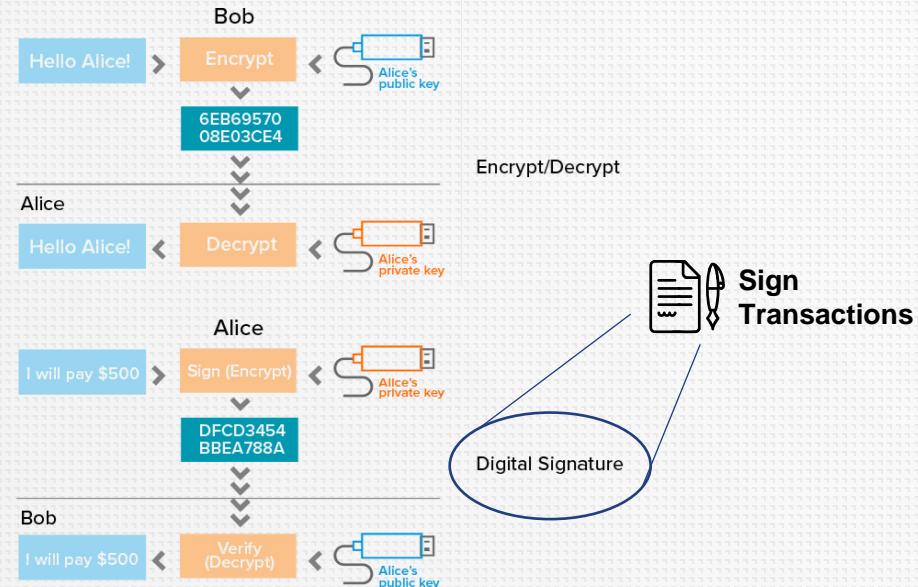
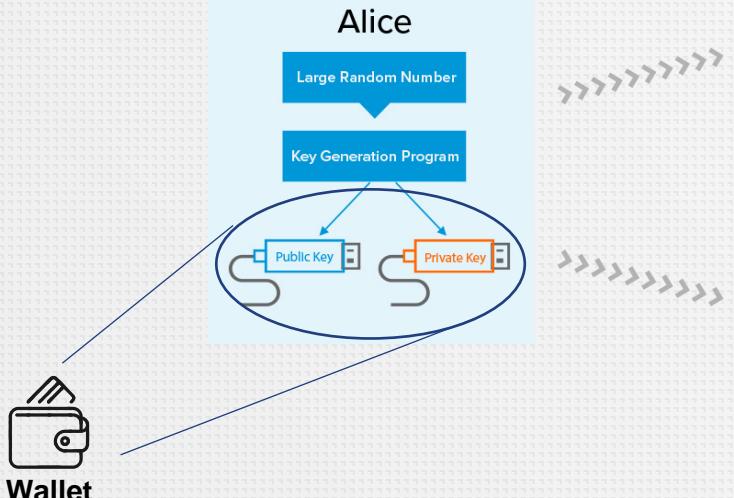
# Exercise 1: Setup an Ethereum Wallet

- **Requirement:** Google Chrome or Firefox installed
- Go to **MetaMask** site: <https://metamask.io/download.html>
- Install the Chrome extension
- Create a new wallet
- Select the “Rinkeby” network (top right)
- Follow the steps in “Rinkeby’s faucet” in order to get some Ether
  - <https://www.rinkeby.io/#faucet>
  - **TIP:** if you don’t have Twitter or Facebook, feel free to ask the teacher for some ether
- Send some Ether to your colleagues!!!



<https://github.com/echiner/edem-mdm-blockchain>

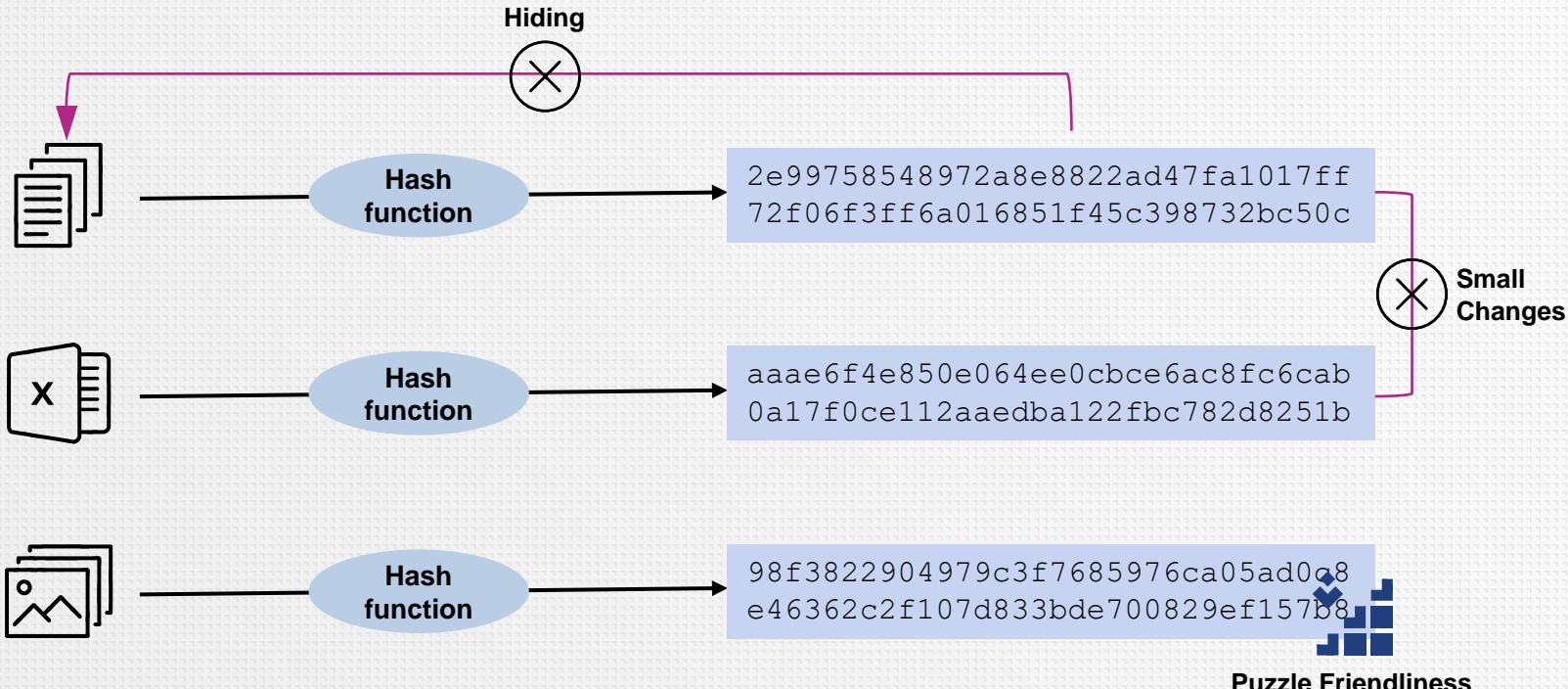
# Some basic concepts – Public Keys



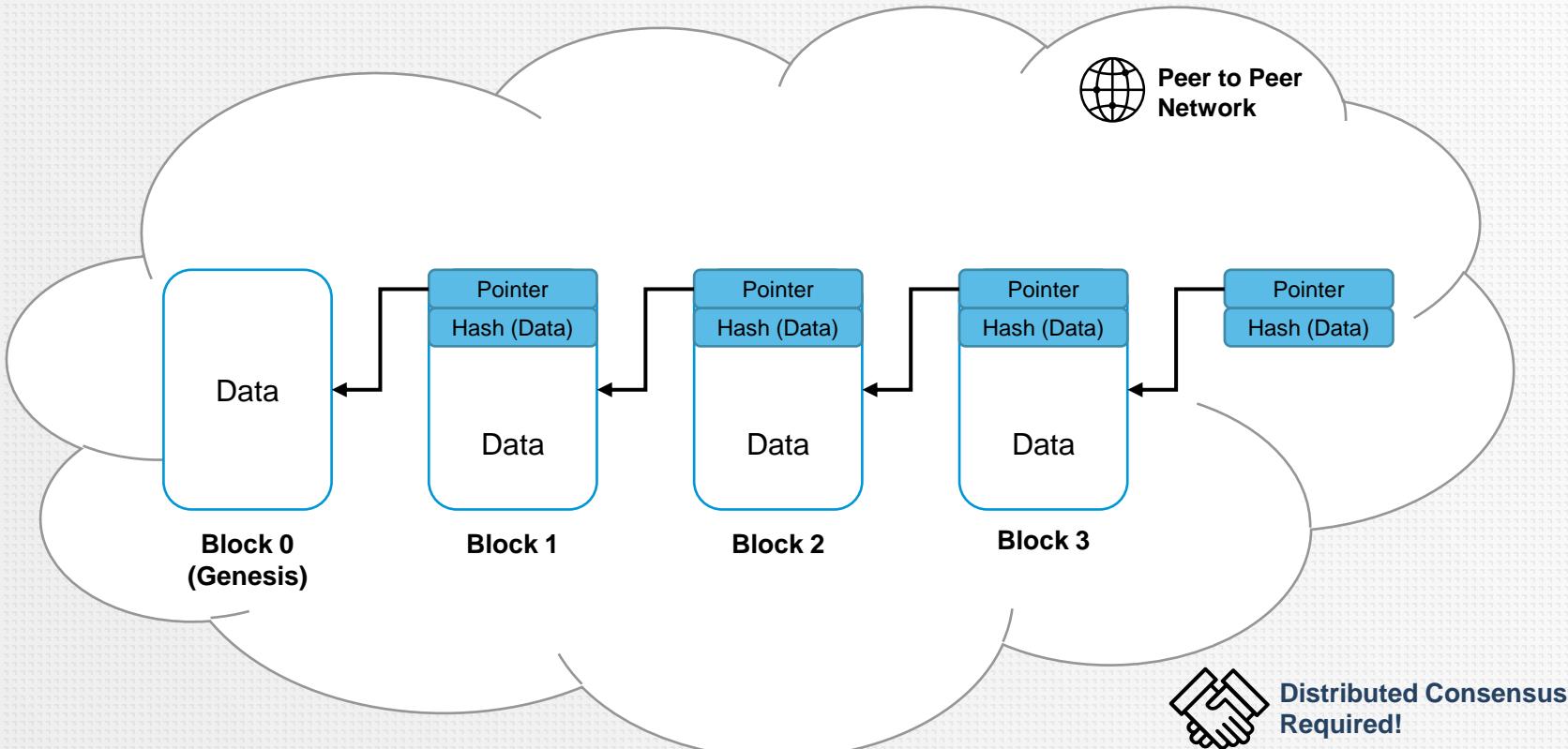
Properties: (1) authentication ▷ (2) non-repudiation ▷ (3) Integrity

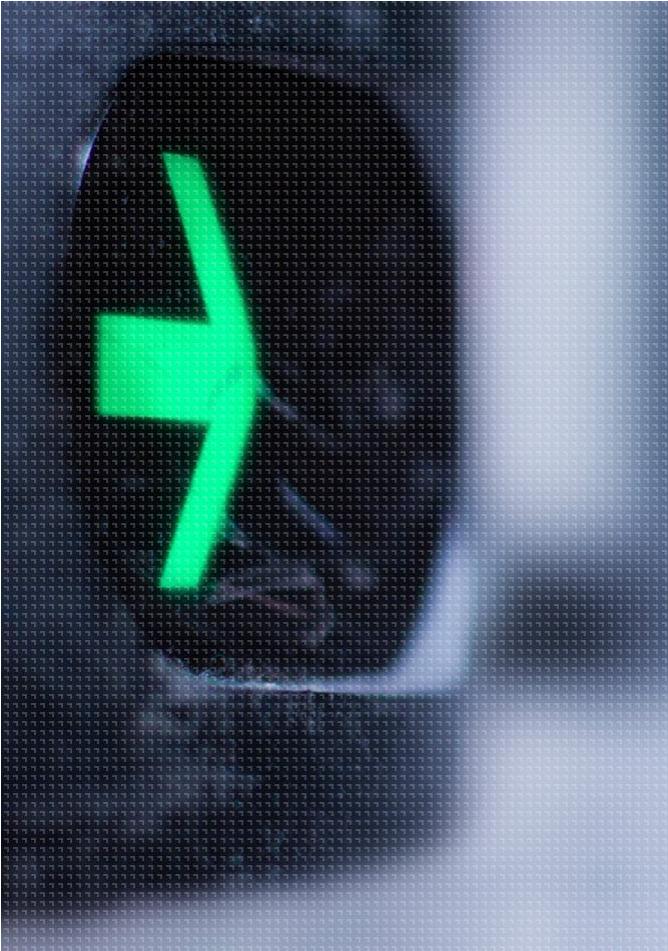
**Public-Key Cryptography (a.k.a. Assymetric Cryptography)**

# Some basic concepts – Hash functions



# What is the Blockchain?





## Distributed consensus

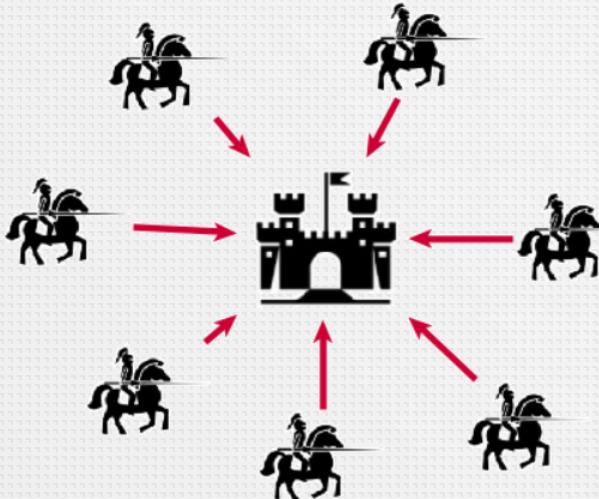
- **Nodes** may experience **downtime** at any time
- The **network** may be **interrupted** at any time
- A sent **message** may be **lost** during delivery
- A sent **message** may be **delayed**
- **Messages** may experience the **out-of-order** problem
- The **network** may be **divided**



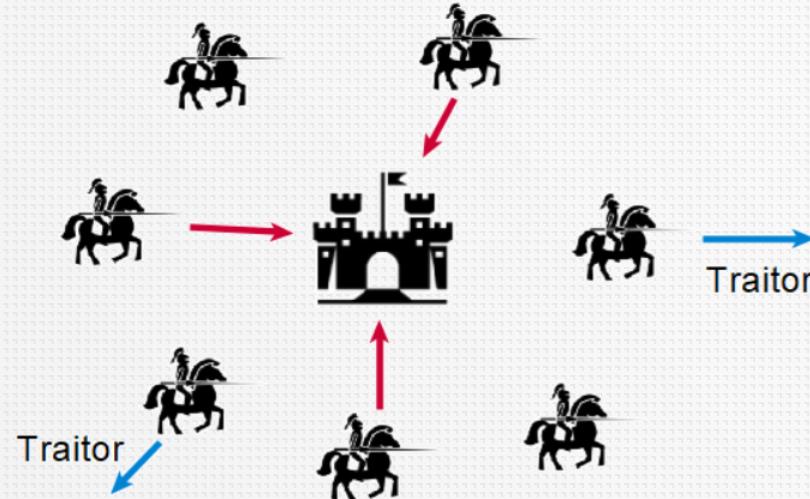
# Byzantines general problem



# Byzantine generals problem

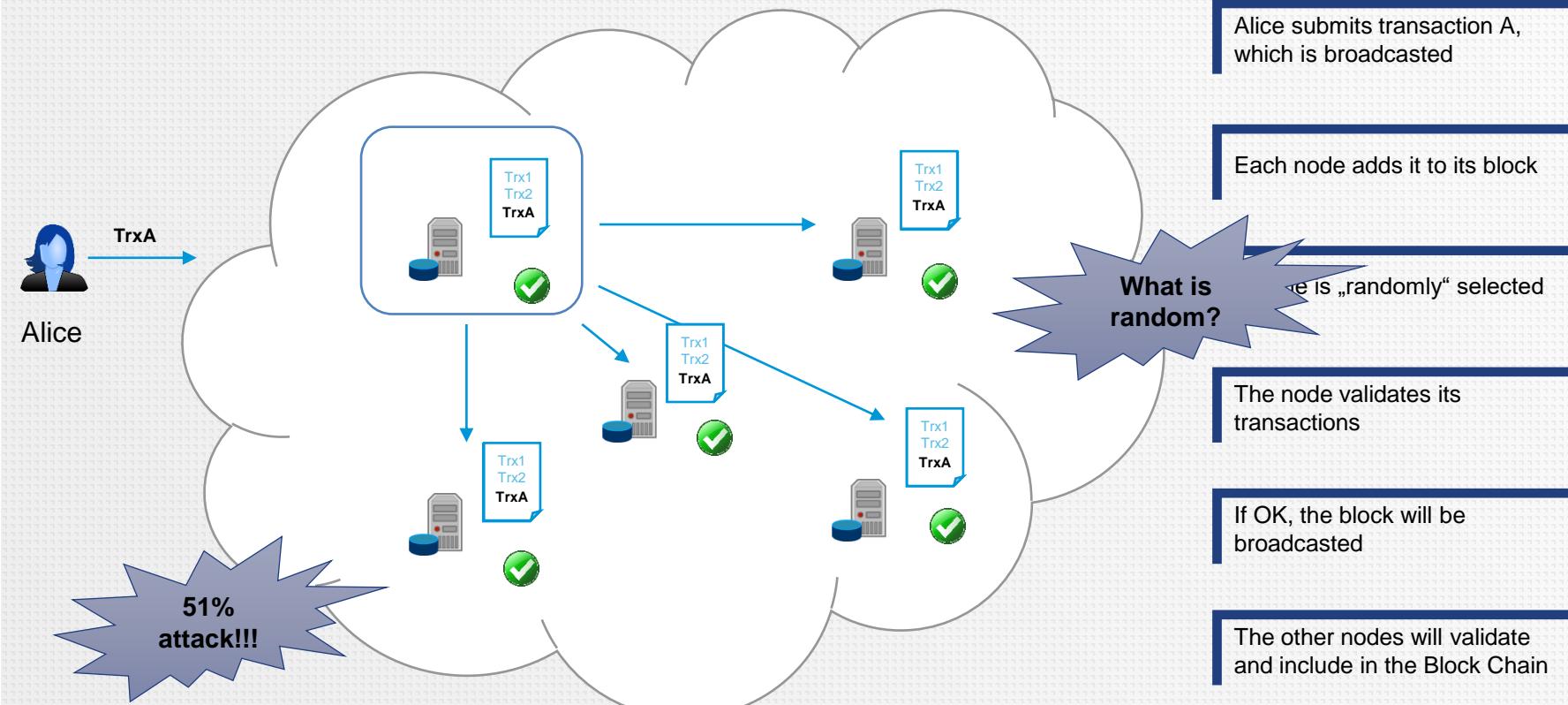


**Coordinated attack  
leading to victory**



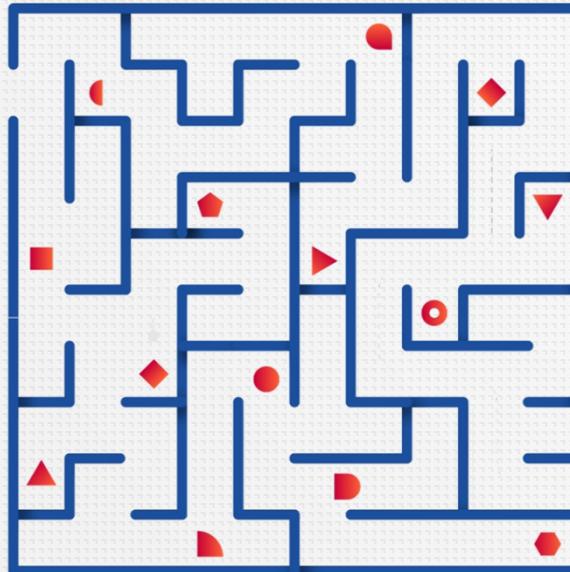
**Uncoordinated attack  
leading to defeat**

# Distributed consensus



# Proof of Work

**1** A very complex mathematical challenge is proposed to the blockchain network



**2** The miners have to compete to find the solution, which takes time and resources, making it costly for the contestants.

**3** The first miner to solve the problem has the ability to validate transactions and create a new block, receiving a reward afterwards.



The system is called **proof of work** because the probability of mining the block is increased with the amount of work that is put in.

# Mining

- This is what we call **mining**, i.e. use of **high power computers** in order to solve complex computational **math problems** which, once solved, will grant you the ability to **release a new block**.



# Mining – PC



Approx. 4 MH/s

# Mining – GPU



50-100x

# Mining – FPGA



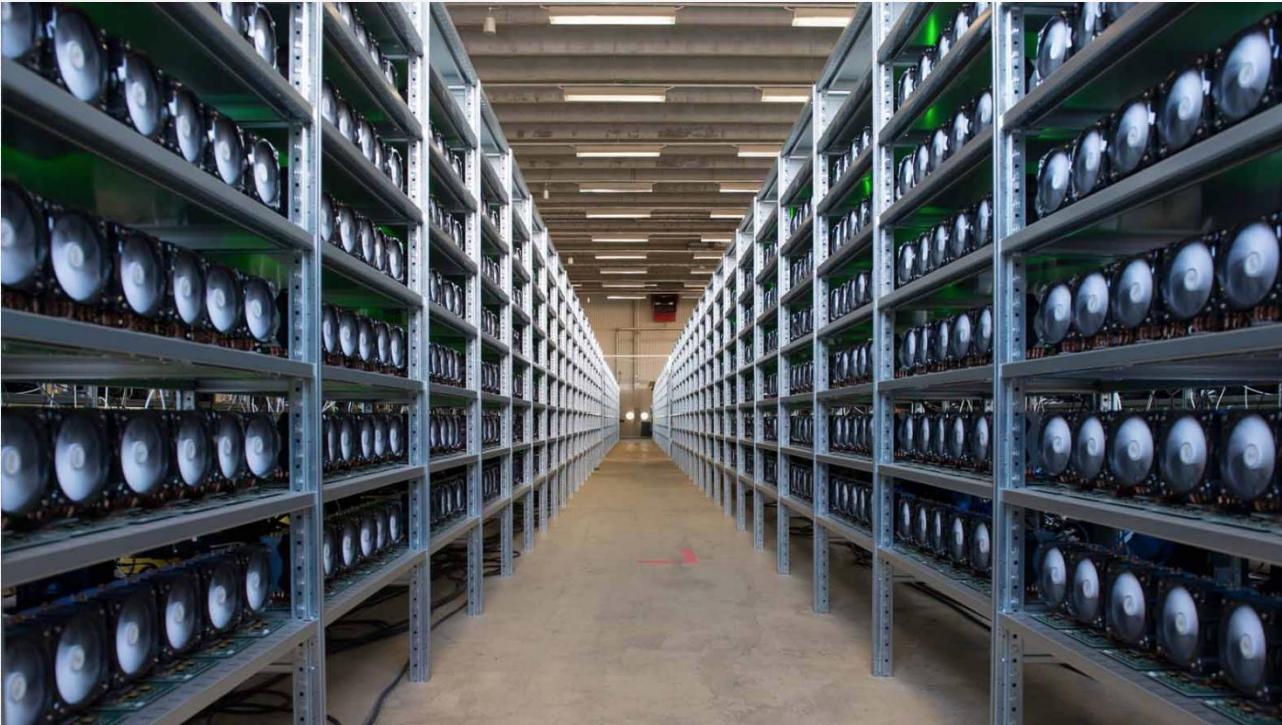
# Mining – ASIC



7 million  
times faster  
than PC!!!

**BITTECH One Miner – 28 TH/s**

# Mining - Pools



AntPool – 7.13 EH/s

# Mining



Between 4 - 200 MH/s

Fugaku (Top 1 Supercomputer)

415.5 petaflops (13k flops/hash)  
32 TH/s

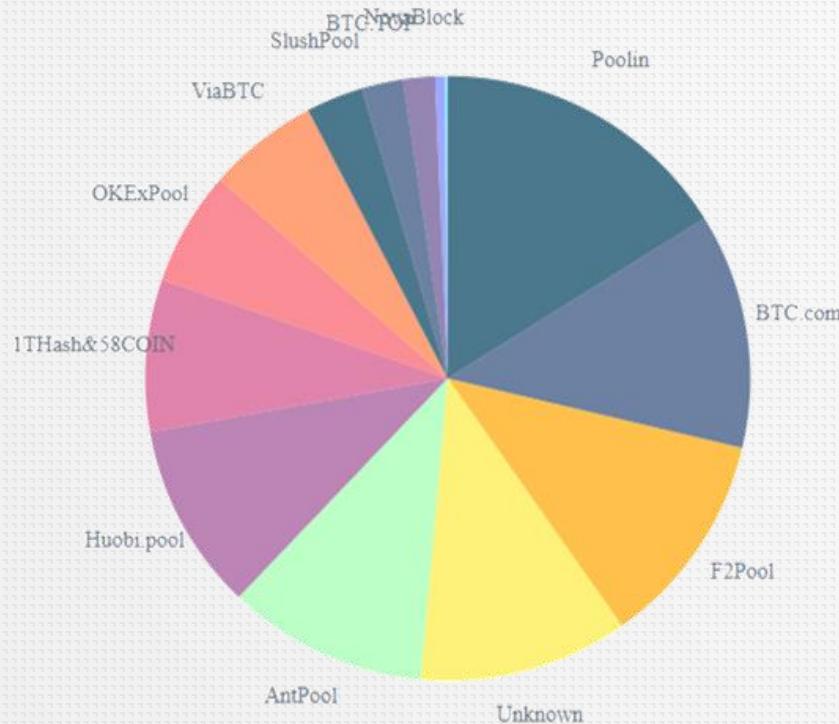
## Reminder

Mega → Giga → Tera → Peta → Exa

Around 20 EH/s



# Satoshi's nightmare



Hashrate distribution (blocks mined) in the last 4 days – **Source:** Blockchain.info

# Consensus algorithms



## Proof of Work

- ➔ Bitcoin, Ethereum\*, Litecoin...
- ✓ It works!
- ✗ Slow throughput; killing the planet



## Proof of Stake

- ➔ Cardano, Ethereum (soon), Tezos...
- ✓ Attacks expensive; decentralized; Energy efficient
- ✗ Nothing at stake



## Proof of Authority

- ➔ Hyperledger BESU, Ethereum Kovan...
- ✓ High throughput; scalable
- ✗ Centralized system



## Others

- ✓ Proof of Weight
- ✓ Proof of Burn
- ✓ Proof of Capacity

# Bitcoin block details



Block 632632 ⓘ

|                              |   |   |
|------------------------------|---|---|
| Hash                         | 000000000000000000000000b069efb51a390724e3f035509d5bf2b93e34760fc0bc0 | → Hash pointer                              |
| Confirmaciones               | 1   |   |
| Fecha y Hora                 | 2020-06-01 19:38  |   |
| Altura                       | 632632  |   |
| Minero                       | SlushPool   | → Who mined the block (solved the puzzle!!) |
| Número de transacciones      | 2888  |   |
| Dificultad                   | 15.138.043.247.082,88   |   |
| Raíz Merkle                  | 9f8a109b32859ee932a084d5a82d8f3221df59badec069bc8d3d6c56ddf11a1d      | → Link to transactions                      |
| Versión                      | 0x20000000  |   |
| Bits                         | 387.094.518   |   |
| Peso                         | 3.993.347 WU  |   |
| Tamaño                       | 1.334.783 bytes   |   |
| Nonce                        | 2.072.399.510   |   |
| Volumen de la transacción    | 8807.65882017 BTC   |   |
| Recompensa de Bloque         | 6.25000000 BTC  | → Reward (new money!)                       |
| Remuneración por la comisión | 0.89381915 BTC  | → Fees                                      |

# Ethereum block details

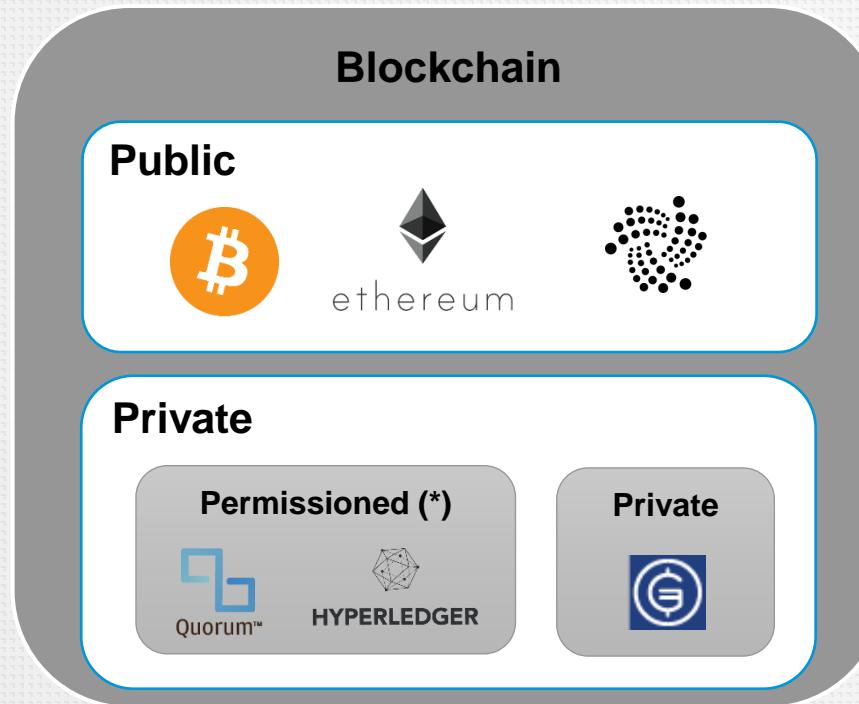


Block #10194249

[Overview](#) [Comments](#)

|                                     |  |  |
|-------------------------------------|--|--|
| ⑦ Block Height:                     | 10194249   | < >  |
| ⑦ Timestamp:                        | ⌚ 22 secs ago (Jun-03-2020 05:39:56 PM +UTC)   |  |
| ⑦ Transactions:                     | 149 transactions and 33 contract internal transactions in this block                   | → <b>Link to transactions (and contract execs)</b> |
| ⑦ Mined by:                         | 0x84a0d77c693adabe0ebc48f88b3ffff010577051 in 19 secs                                  | → <b>Who mined the block (solved the puzzle!!)</b> |
| ⑦ Block Reward:                     | 2.245068484316597582 Ether (2 + 0.245068484316597582)                                  | → <b>Reward (new money!)</b>                       |
| ⑦ Uncles Reward:                    | 0  |  |
| ⑦ Difficulty:                       | 2,361,189,893,362,840  |  |
| ⑦ Total Difficulty:                 | 15,717,023,273,021,800,529,449   |  |
| ⑦ Size:                             | 26,377 bytes   |  |
| ⑦ Gas Used:                         | 9,906,253 (99.79%)   | → <b>Cost (kind of like fees)</b>                  |
| ⑦ Gas Limit:                        | 9,927,010  |  |
| ⑦ Extra Data:                       | 01090d/geth/go1.14.2/linux (Hex: 0xd88301090d846765746888676f312e31342e32856c696e7578) |  |
| <a href="#">Click to see more ↓</a> |  |  |

# Types for blockchains networks



## Same

- Peer-to-peer
- Byzantine fault tolerance
- Public key cryptography
- Transaction constraints
- Distributed consensus

## Differences

- Permission model
- Transaction censorship
- Native cryptocurrency
- Consensus algorithm
- Speed

(\*) Also known as federated or consortium

# Consortium example - EBSI

- **European Blockchain Services Infrastructure (EBSI)** aims to deliver EU-wide cross-border public services using blockchain technology with the highest standards of security and privacy. Other strategic aims of EBSI are to enhance cross border government services. Main examples today being:
  - Notarisation
  - Diplomas
  - European Self-Sovereign Identity
  - Trusted Data Sharing



## IDENTITY & CREDENTIALS

European health insurance card  
Upgraded diplomas  
Sovereign identity in immunization  
Unique European social security number  
Immigration control  
Asylum procedures coordination



## DISTRIBUTED REGISTRY

DLT for the tourism sector  
Network of trust for SMEs  
eHealth – Digital Service Infrastructure  
Supply Chain Visibility  
360° vehicle lifecycle management  
IMZ – electronic markets for media assets



## ENERGY & ENVIRONMENT

BLICK – sustainable cities  
Unique Building Identity (UBI) or Unique  
Object Identifier (UOI)  
Green product portfolio



## LAW & COMPLIANCE

Compliance by design  
Fraud & supply chain integrity



## FINANCING & PROCUREMENT

DLT for debt & equity financing  
DLT in procurement

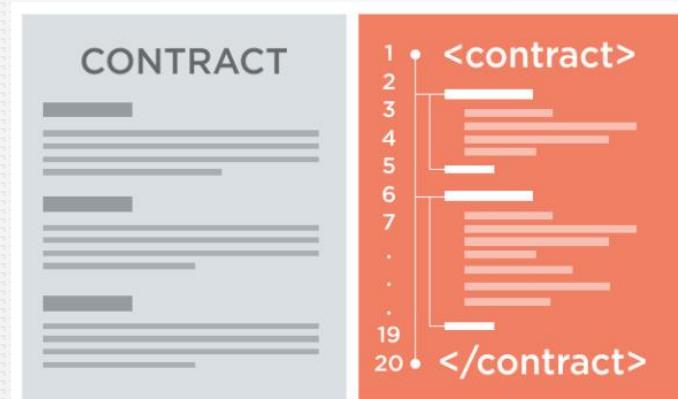
# Smart Contracts

# Differences between Bitcoin and Ethereum

|                       |  Bitcoin |  Ethereum |
|-----------------------|---|--|
| <b>Founder</b>        | Satoshi Nakamoto  | Vitalik Buterin  |
| <b>Release Date</b>   | 2008  | 2015   |
| <b>Release Method</b> | Genesis Block   | Pre-sale   |
| <b>Consensus</b>      | Proof of Work   | Proof of Work*   |
| <b>Main Usage</b>     | Cryptocurrency  | Smart Contracts  |
| <b>Currency</b>       | Bitcoin (Satoshi)   | Ether (Wei)  |
| <b>Algorithm</b>      | SHA-256   | Ethash   |
| <b>Block Time</b>     | 10 minutes  | 15 seconds   |

# Smart Contracts

*“A smart contract is a **program** which execution is **autonomous** and totally **transparent**. In particular this execution cannot be reverted and its trace is **public** and **immutable**.”*





# bitcoin

## Is a Smart Contract!!

|           |  |          |                |
|-----------|--|----------|----------------|
| Índice    | 0  | Detalles | No gastado     |
| Dirección | 147SwRQdpCfj5p8PnfsXV2SsVVpVcz3aPq   | Valor    | 6.31042232 BTC |
| Pkscript  | <pre>OP_DUP<br/>OP_HASH160<br/>2220867b1e79c403fafe339a809a65ed01cb6979<br/>OP_EQUALVERIFY<br/>OP_CHECKSIG</pre> |          |                |

# Anatomy of a Smart Contract (Solidity)

Solidity  
version

```
pragma solidity ^0.4.0;
```

Contract  
definition

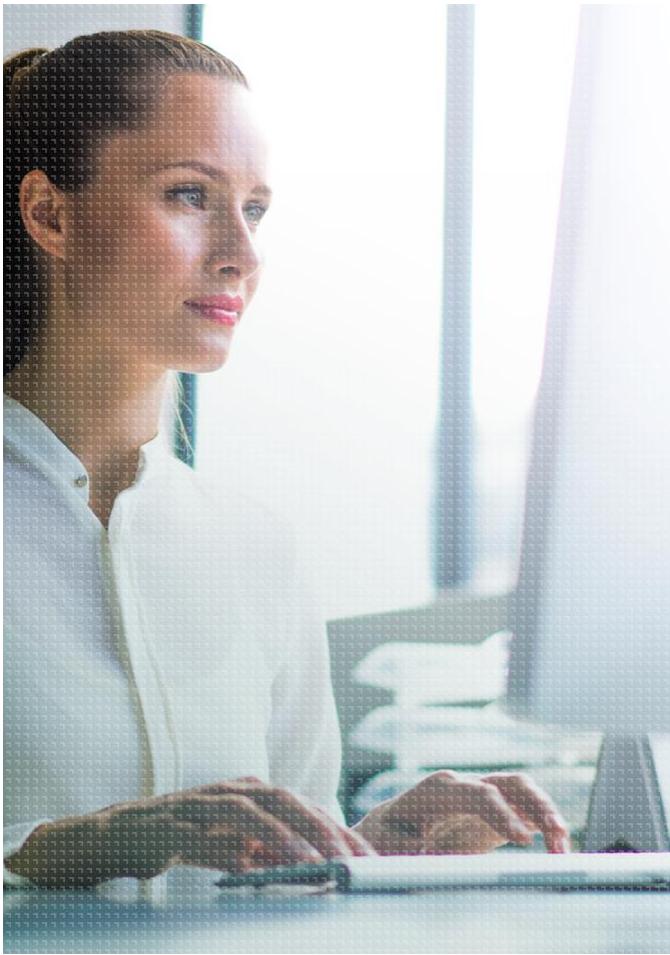
```
contract SimpleStorage {  
    uint storedData;
```

```
        function set(uint x) public {  
            storedData = x;  
        }
```

```
        function get() public constant returns (uint) {  
            return storedData;  
        }
```

State  
variables

Functions



## Exercise 2: Interact with a Smart Contract

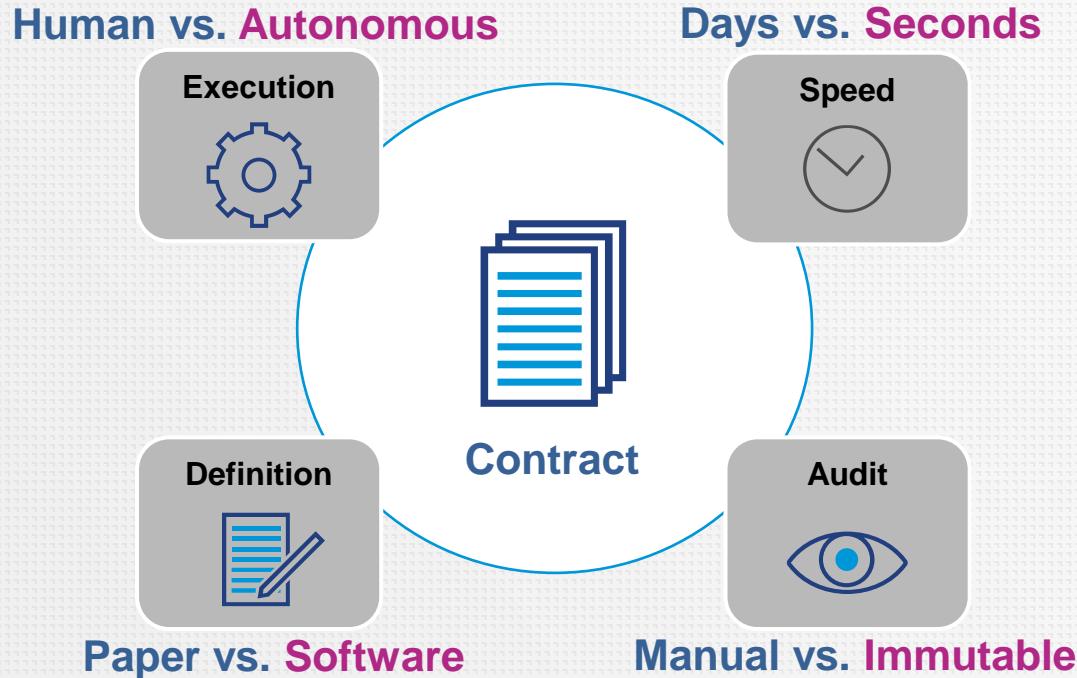
In this exercise we will **interact with an existing Smart Contract** in Ethereum (Rinkeby test network).

We will be using **MyCrypto** to do so.

Follow the steps of exercise 2 in the **Github repository** below.

<https://github.com/echiner/edem-mdm-blockchain>

# Traditional vs Smart Contracts



# Smart Contract Benefits

## ACCURACY

Not prone to human error.

## SPEED

Compared to legal contracts.

## SAVINGS

By removing intermediaries.

## AUTONOMY

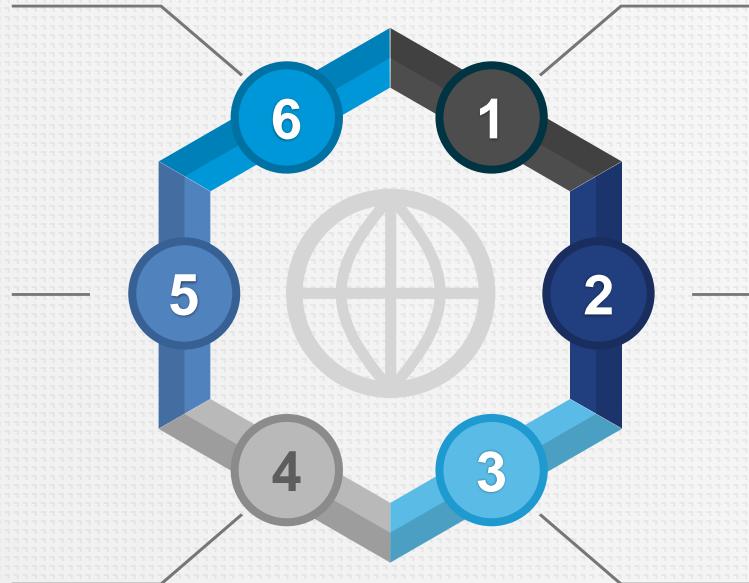
No third parties or extra steps required.

## TRUST & SAFETY

Encrypted on a shared ledger (blockchain) and secured by the power of cryptography.

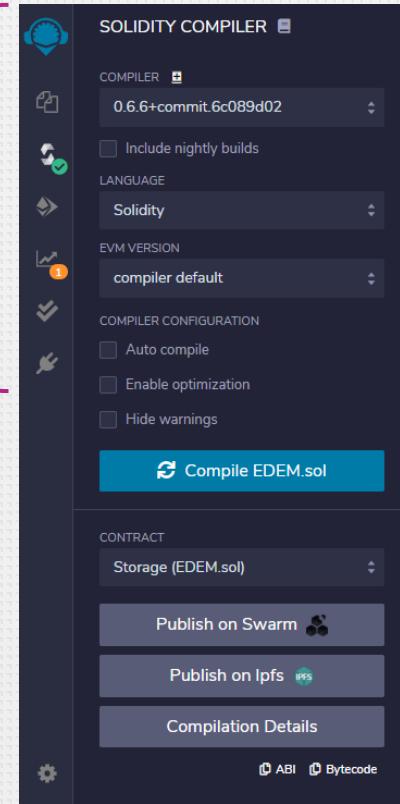
## BACK-UPS

Data is replicated in all nodes.



# Smart Contract Development – Remix

Tools



```
pragma solidity >=0.4.22 <0.7.0;

/*
 * @title EDEM - MDA
 * @dev Store & retrieve value in a variable
 */
contract Storage {
    int pokeCount;

    /**
     * @dev Store value in variable
     */
    function poke() public {
        pokeCount = pokeCount + 1;
    }

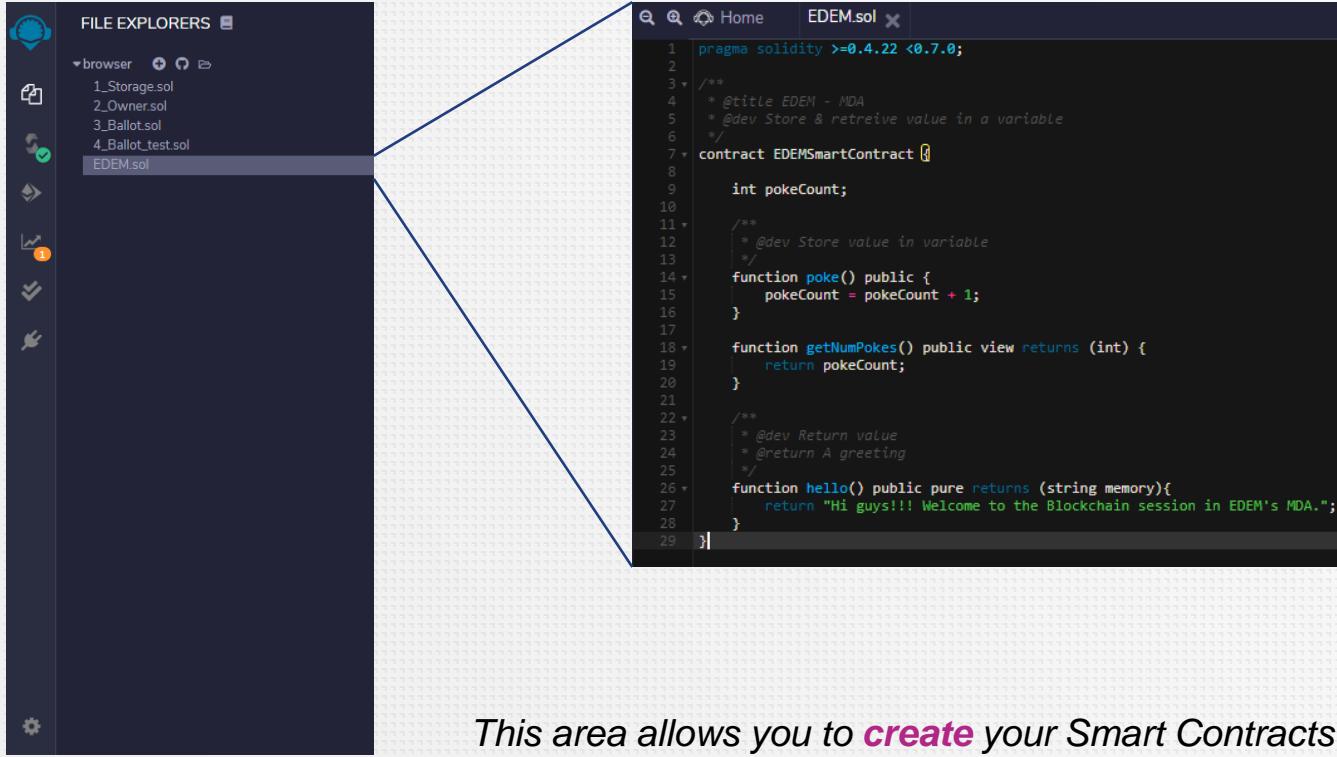
    function getNumPokes() public view returns (int) {
        return pokeCount;
    }

    /**
     * @dev Return value
     * @return A greeting
     */
    function hello() public pure returns (string memory){
        return "Hi guys!!! Welcome to the Blockchain session in EDEM's MDA.";
    }
}
```

Editor

Logs

# Remix – Editor



The image shows the Remix Ethereum IDE interface. On the left is a sidebar titled "FILE EXPLORERS" containing a tree view of Solidity files: browser, 1\_Storage.sol, 2\_Owner.sol, 3\_Ballot.sol, 4\_Ballot\_test.sol, and EDEM.sol. The EDEM.sol file is selected, highlighted with a blue bar at the bottom of the sidebar. A large blue arrow points from the "FILE EXPLORERS" section towards the central code editor area. The central area is titled "EDEM.sol" and contains the following Solidity code:

```
pragma solidity >=0.4.22 <0.7.0;

/*
 * @title EDEM - MDA
 * @dev Store & retrieve value in a variable
 */
contract EDEMSmartContract {

    int pokeCount;

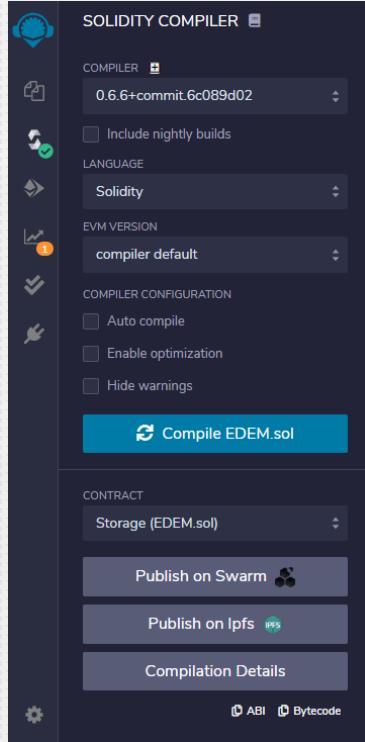
    /**
     * @dev Store value in variable
     */
    function poke() public {
        pokeCount = pokeCount + 1;
    }

    function getNumPokes() public view returns (int) {
        return pokeCount;
    }

    /**
     * @dev Return value
     * @return A greeting
     */
    function hello() public pure returns (string memory){
        return "Hi guys!!! Welcome to the Blockchain session in EDEM's MDA.";
    }
}
```

*This area allows you to **create** your Smart Contracts*

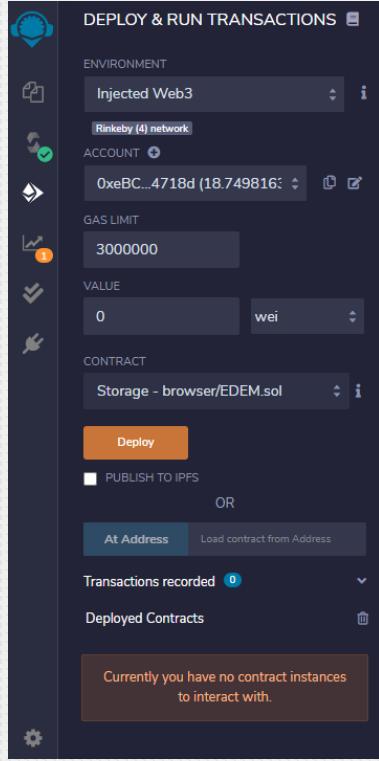
# Remix – Compiler



→ This is all you need for this course ☺

*This area allows you to **compile** your Smart Contracts*

# Remix – Test & Deploy



Select where you want to run/deploy the Smart Contract:

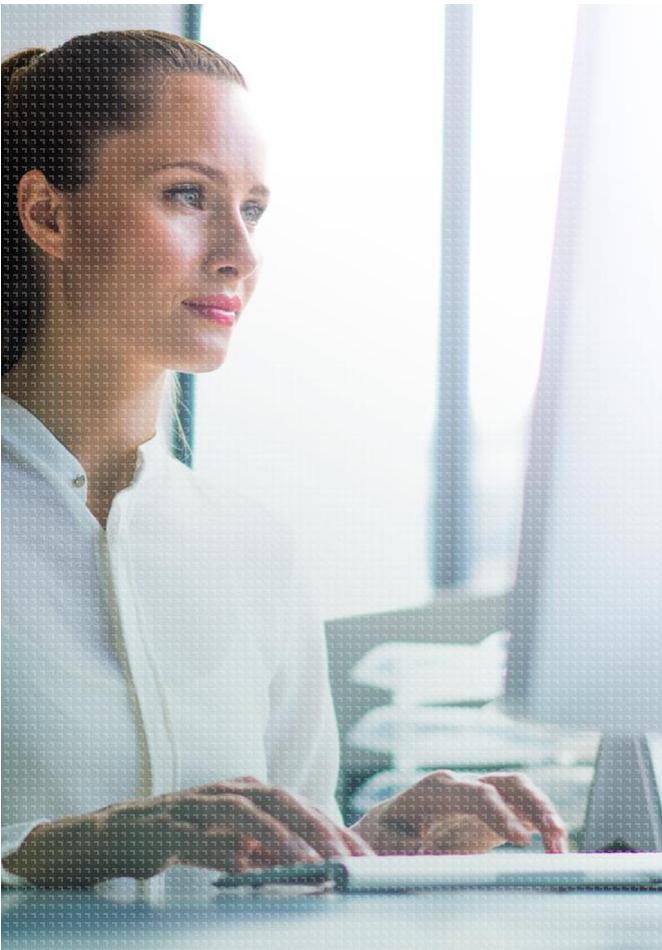
- **JavaScript VM**: run in your browser
- **Injected Web3**: run in the network using MetaMask
- **Web3 Provider**: run directly against a node (local or remote)

Smart Contract you want to run/deploy

Click to deploy!!

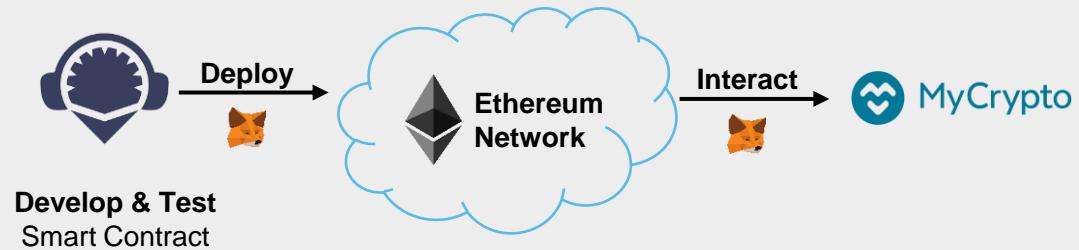
This is where you will test your Smart Contract functions

*This area allows you to **run**, **deploy** and **test** your Smart Contracts*

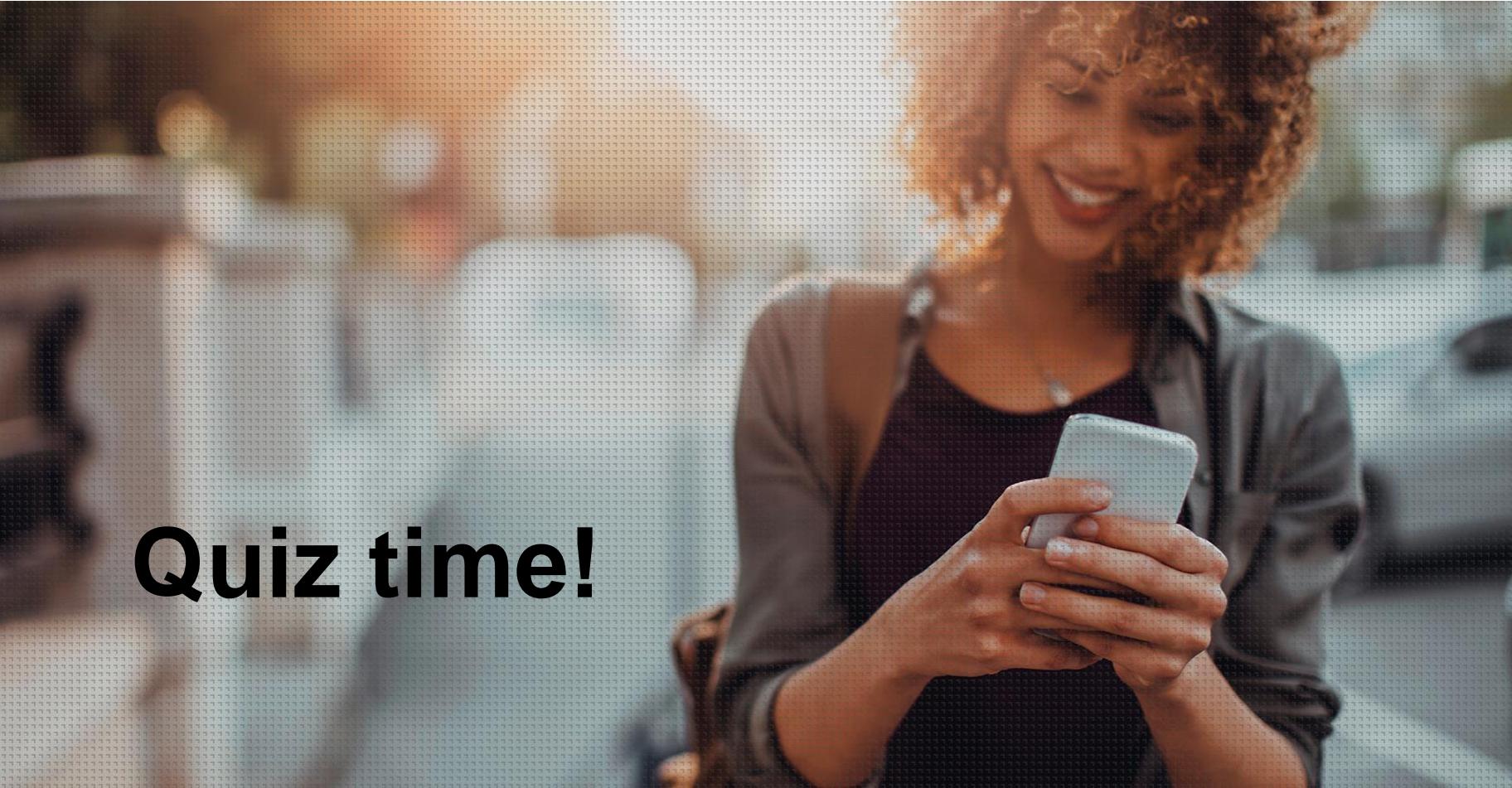


## Exercise 3: Create a Smart Contract

- Create Smart Contract with **Remix**
- Test the contract locally
- Deploy into a real Ethereum network
- Interact using **MyCrypto** (through **MetaMask**)



<https://github.com/echiner/edem-mda-blockchain>

A woman with curly hair is smiling and looking down at her smartphone. She is wearing a dark t-shirt. The background is blurred, suggesting an indoor setting.

Quiz time!

# Tokenization

# Introduction

**“Crypto tokens**, which are also called **crypto assets**, are special kinds of virtual currency tokens that reside on their own blockchains and **represent an asset or utility**. Most often, they are **used to fundraise for crowd sales**, but they can also be used as a **substitute for other things**.“

- “Investopedia”



# Types of tokens



## Utility tokens

*Provides access to the goods & services of the project.*



## Security tokens

*Assets such as participation in real physical underlying, companies, goods or earning streams.*



<https://medium.com/swlh/types-of-tokens-the-four-mistakes-beginner-crypto-investors-make-a76b53be5406>

## Token Standards



<https://research.binance.com/en/analysis/tokenization>

# Sample ERC-20 Token

Token GFT Test Token ⓘ

## Overview [ERC-20]

Total Supply: 1,000,000 GFT ⓘ

Holders: 5 addresses

Transfers: 7

## Profile Summary

Contract: 0x09da9b7a133057e4df17c503cf4589bc096da964

Decimals: 2

Transfers Holders Read Contract Write Contract



Token Holders Chart

(Last Updated 10/19/2020 3:50:51 PM)

A total of 5 token holders

First < Page 1 of 1 > Last

| Rank | Address                                    | Quantity | Percentage |
|------|--|----------|------------|
| 1    | 0xf73536fe9a35751a42ddd7a56177e5814ce0b76b | 500,000  | 50.0000%   |
| 2    | 0xebc5efa7442143c5da1c48ea6cbaaa1e7784718d | 389,900  | 38.9900%   |
| 3    | 0x94c6a2b5c73f74bc7050168e3a593a177f450ac4 | 98,000   | 9.8000%    |
| 4    | 0x99cbaef1283c1a38a140cb5f87bac0345e743c7  | 10,000   | 1.0000%    |
| 5    | 0xc93596765891bbbdbe7fadеead503e7d03dc7f8c | 2,100    | 0.2100%    |

<https://rinkeby.etherscan.io/token/0x09da9b7a133057e4df17c503cf4589bc096da964>

# Initial Coin Offerings (ICOs)

An **Initial Coin Offering (ICO)** is the cryptocurrency industry's **equivalent to an Initial Public Offering (IPO)**. ICOs act as **a way to raise funds**, where a company looking to raise money to create a new coin, app, or service launches an ICO.

## Pros



- Easy to create a new token
- Easy to raise money
- Higher „coverage“
- Easily traded (secondary market)

## Figures from 2017

**435** successful ICOs

**\$12.7 million** raised per ICO

**\$5.6 billion** total raised

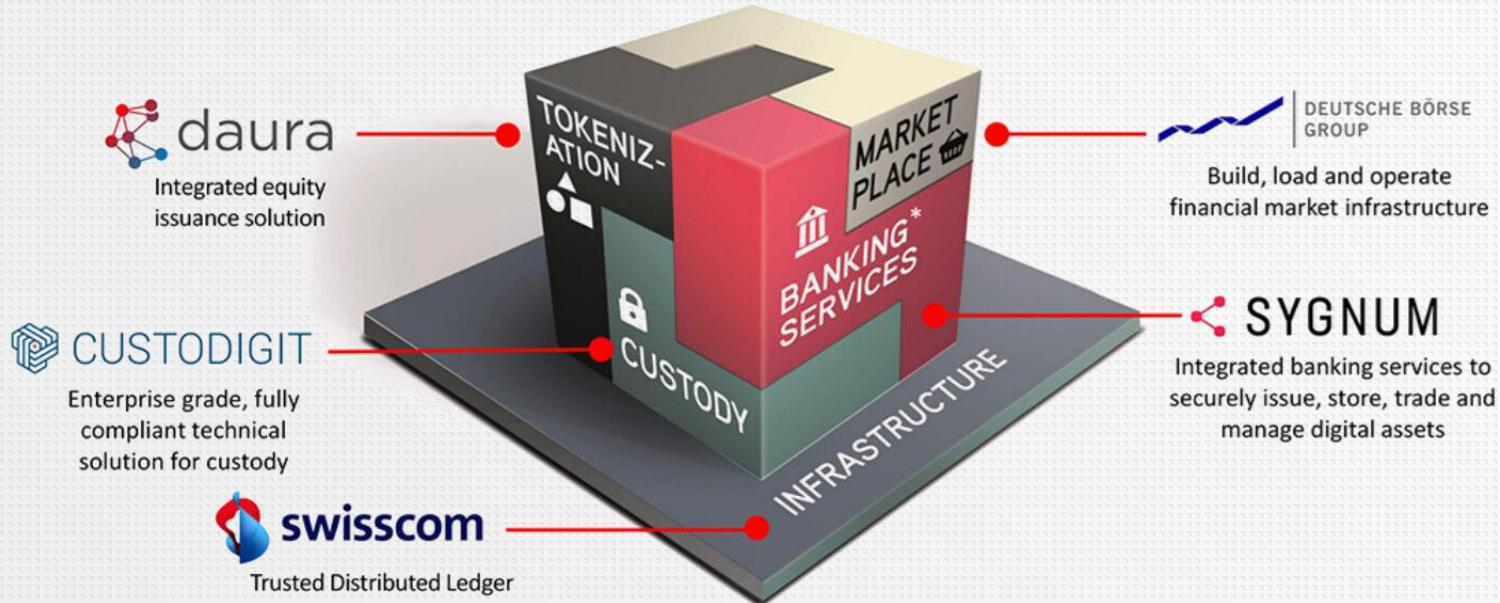
**12.8x** average return

## Cons



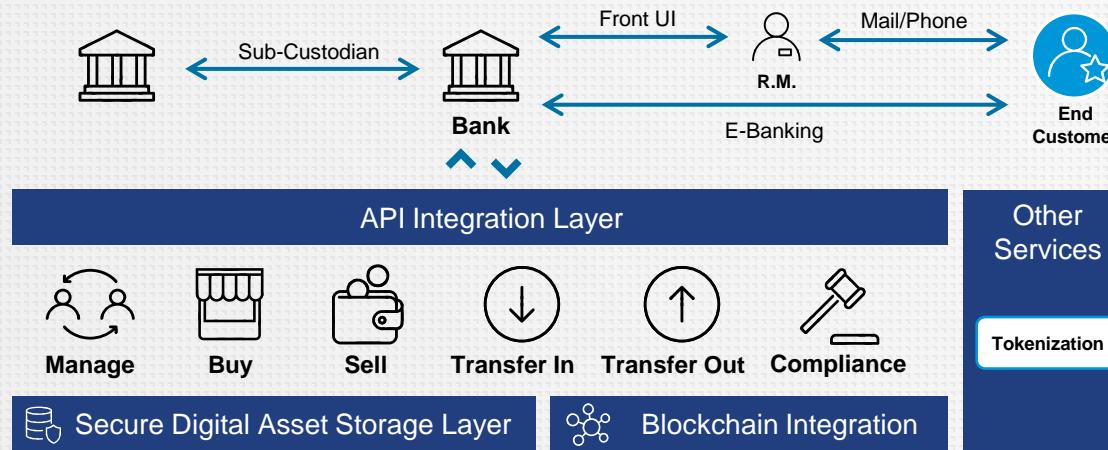
- Largely unregulated
- Fraud and scam
- Not really a share
- Banned in some countries (e.g. China)
- ROI vs Money Raised

# Swiss Digital Asset Custody



# Crypto & Digital Asset Management

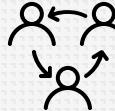
A turn-key ready **Digital Assets Platform** for regulated financial institutions (Banks, CSDs, Exchanges), providing all the required business functionality to provide a Digital Asset market service offering.



# Tokenization



**Decentralized ownership**  
no borders/barriers



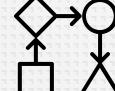
**No middlemen**  
Cost-effective



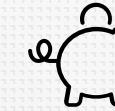
**Greater liquidity**



**Frictionless transfer  
of ownership**

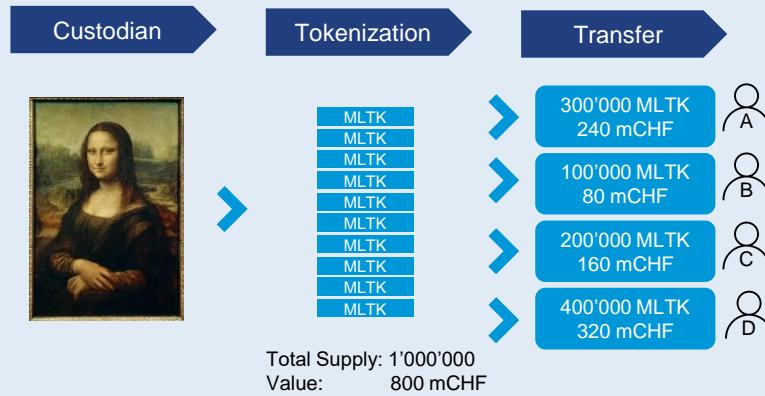


**Traceability**  
Immutable & transparent



**Fungible & non-fungibles**

# Asset Tokenization for a Private Wealth Bank



## Goals

- Tokenization of utilities and investments funds with a standard token
- This standard token must be transferable to other owners
- Compliance with all regulatory requirements
- Fast market introduction with low initial investment and agile further development
- Integrated in bank's target operating model

## Use cases:

- Tokenization of utilities and non-liquid objects
- Tokenization of inherited objects (work of art, real estates, etc.) and distribute among the heirs
- Quickly set up and transfer (private equity) investment funds

# Summary Tokenization solution

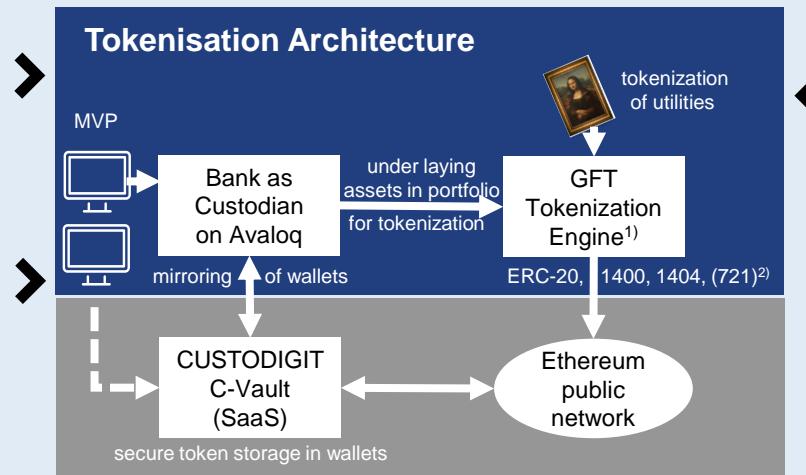
F

## Tokenization features

- Token Issuance
- Token Management
- Solidity smart contract creation
- User Interface
- Import interfaces

## GFT expertise

- Founded 1987 in Germany
- ~6'000 experts in 15 countries
- 70+ DLT experts and 30+ DLT projects since 2015
- Established partnership with Avaloq and CUSTODIGIT
- Listed on TecDAX, 36% owned by founder family



## C-Vault features

- Highly secure storage of wallets
- SaaS Model operated by Swisscom in Tier 4 data centres
- Settlement functionality
- Enterprise Business Functionality
- AML & Reporting Functionality
- Blockchain agnostic and connected to different chains
- Broker Module (optional)
- Key Management PwC audited
- IASE 3000 and ISO 27001 & 22000 certified

## CUSTODIGIT security

- Spin-off company of Swisscom
- Founded 2018 in Switzerland
- Platform live since August 2019 with a FINMA regulated customer
- Owned by Swisscom 75% and Sygnum 25%

1) on premise by the Bank

2) supported in a later state

# Decentralized Finance

**“We are a stone’s throw away from the global financial industry running on a common software infrastructure.”**

–Lex Sokolin, Global Fintech Co-Head of  CONSENSYS

**“In the next five to 10 years, you could see a financial system where all assets and liabilities are native to a blockchain, with all transactions natively happening on chain”**

– Matthew McDermott, head of digital assets,



**“The foundations of new economies start with borrowing and lending. In 2019, the blockchain industry enabled these necessary primitives in what has become DeFi.”**

–Collin Myers, Global DeFi Product Strategy Lead,  CONSENSYS Codefi

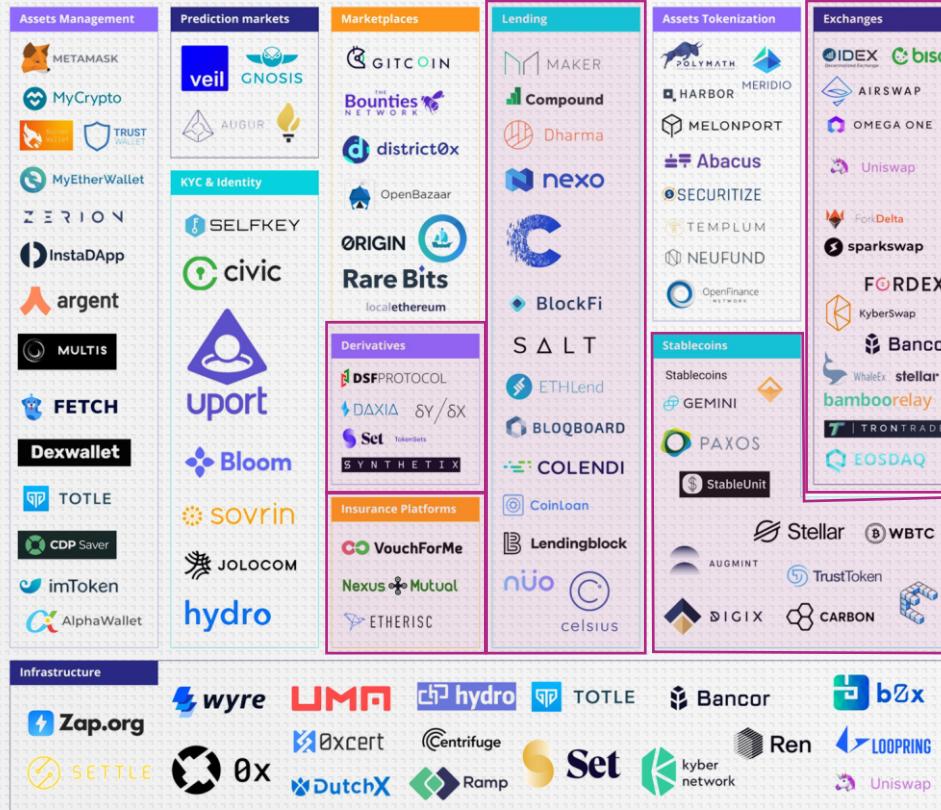
**“I think the financial institutions should understand DeFi because it has the potential to eventually sort of take over and subside the business elements of existing business models.”**

–Nitin Gaur, director of IBM financial services and digital assets, 

# Key steps in evolution of Blockchain for finance



# DeFi landscape today



Source: <https://defiprime.com/>



## Stablecoins

- Linked to a fiat currency
- Avoid volatility
- Algorithmic or non-algorithmic





## Decentralized Exchanges

- Fully decentralized
- Permissionless
- No custody of coins
- Liquidity pools





## Lending & Borrowing

- Usually crypto assets
- Autonomous interest rates
- Making interest
- Collateral for borrowing

 Compound

 AAVE

 MAKER



## Derivatives & Margin Trading

- Price based on an underlying asset
- On-chain exposure to assets
- Synthetic assets

SYNTHETIX

$\delta Y / \delta X$





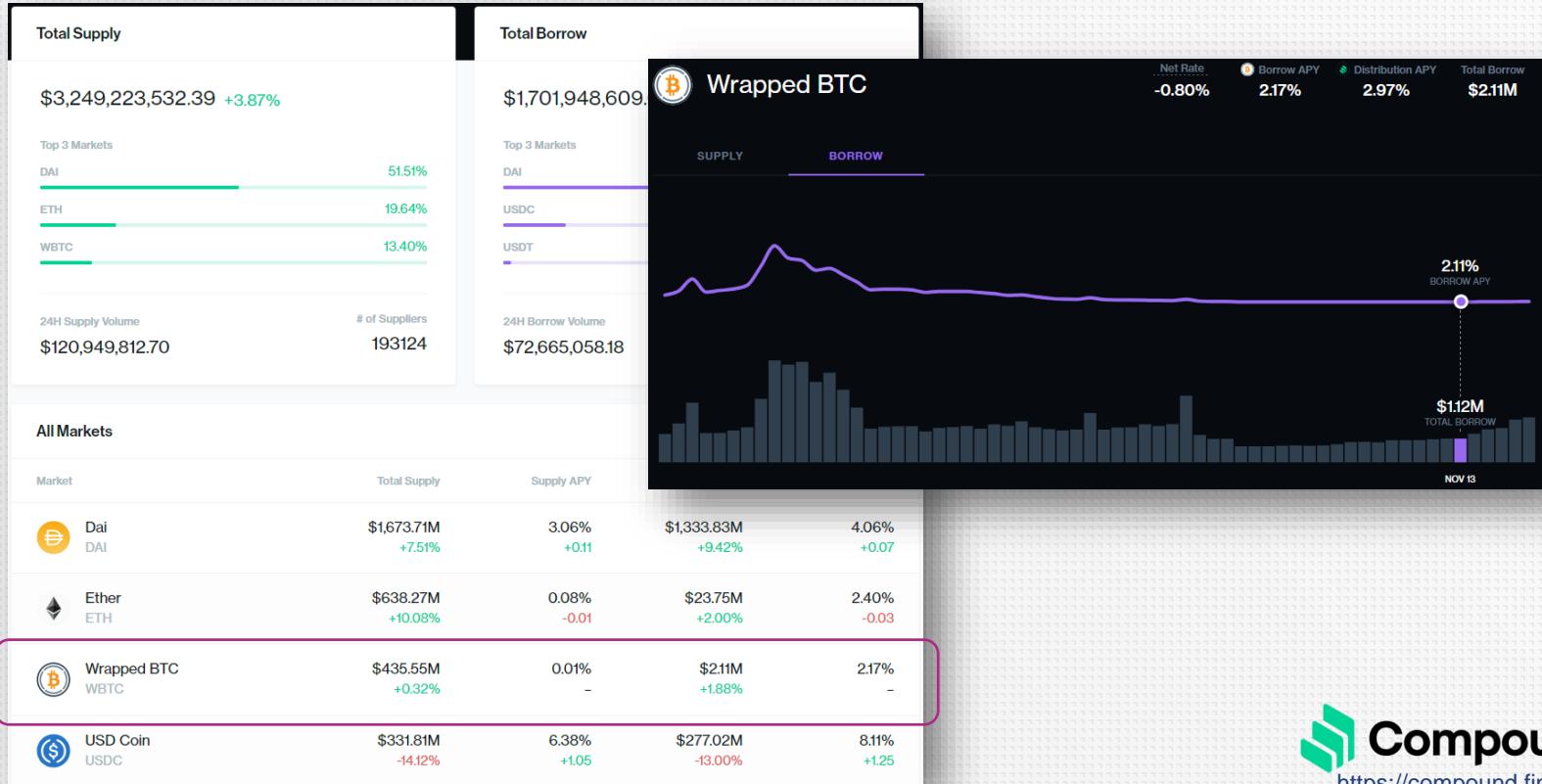
## Insurance

- Guarantee of compensation
- Payment of a premium
- Protection against SC failures or deposits

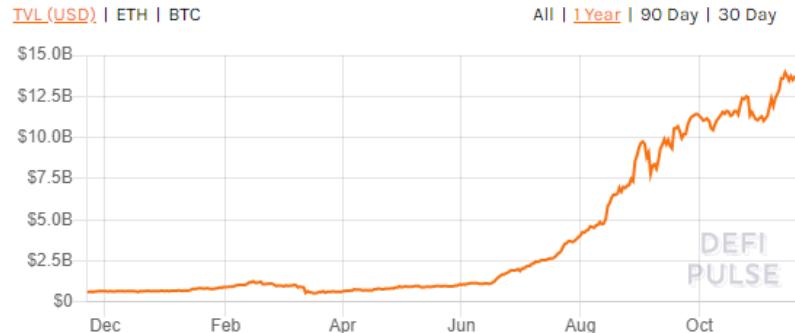
Nexus  Mutual

 opyn

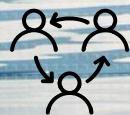
# Lending & Borrowing



## Total Value Locked (USD) in DeFi



Source: <https://defipulse.com/>



COMBINE  
DEFI



INTEROPERABILITY



PROGRAMMABLE  
MONEY

Possibilities are endless!!!

# Benefits & Use Cases

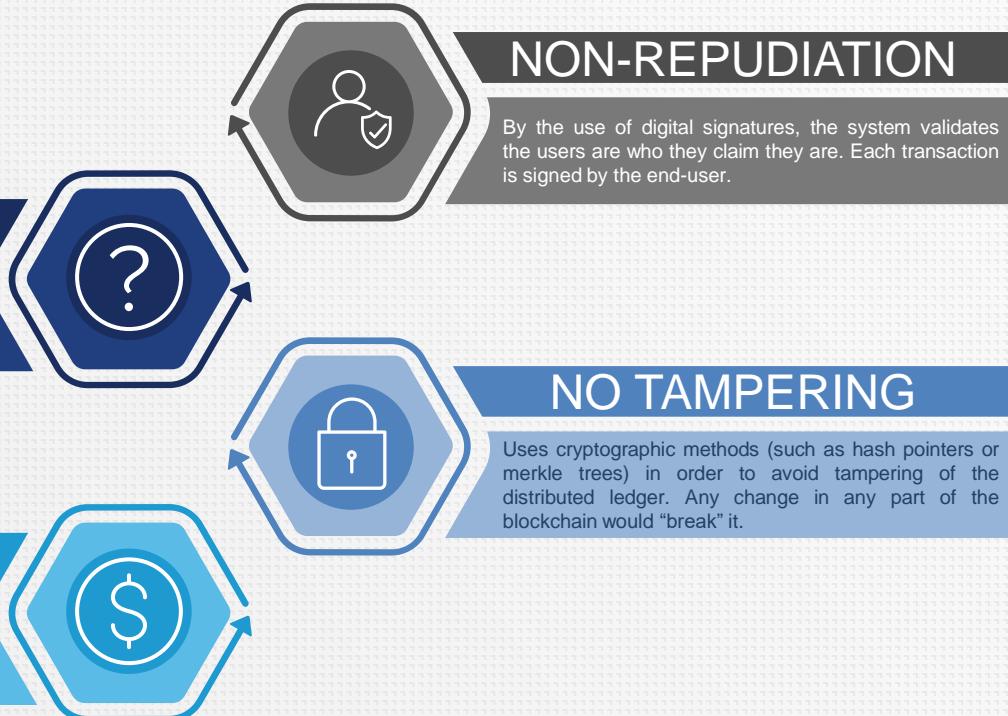
# Security

## “ANONYMITY”

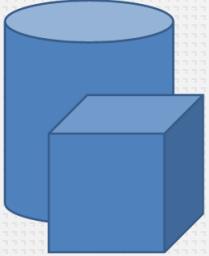
Blockchain accounts are just IDs which cannot be linked to a final user. Beware that in most cases there is no real anonymity, but pseudonymity.

## AUDIT

Given that all data is public and there is no possibility of data tampering, it can be considered as an auditable public ledger.

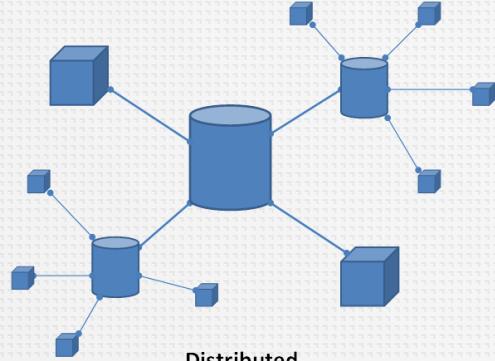


# Decentralization



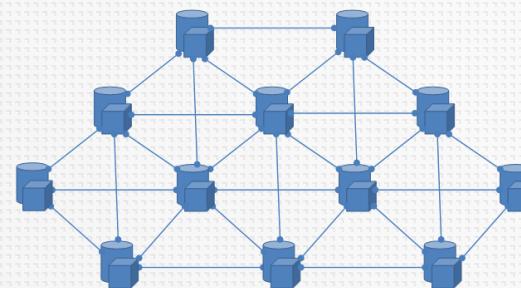
**Centralized**

*one node does everything*



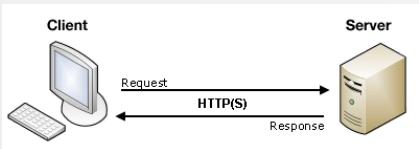
**Distributed**

*nodes distribute work to sub-nodes*



**Decentralized**

*nodes are only connected to peers*



**Side note:** Great article on the “Meaning of Decentralization”:

<https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>

# Why use Blockchain? – Blockchain's Core USPs

## Harmonised data and transactions

Through a secure shared database to be written on by multiple parties



## Untrusted parties

Parties do not know/trust each other or do not have unified interests



## Automated Processing

Parties want to automate agreements and transactions using 'smart contracts'



## Disintermediation

Remove intermediaries which produce none or little value in the chain



# Towards “The Enterprise as Code”

F

## THE FIRM AS CODE

“A firm is just a ‘nexus of contracts.’ Payroll contracts with employees, profit contracts with shareholders, debt contracts with lenders, delivery contracts with customers, tax contracts with the state. Blockchain-based ‘smart’ contracts will eventually reinvent the firm.”



Naval Ravikant, founder of AngelList

## In the news



*Leading Spanish banks achieve  
“blockchain-based payments” in just 2.5  
seconds*



*First international payments using Ripple, for  
retail customers*



*A \$134 Million Building in Zurich Has Sold  
Via Cryptocurrency*



*Porsche has successfully closed a loan with BBVA for  
\$170 million using distributed ledger technology*

# Current challenges

# Current challenges

01



## Fragmentation

There is currently no “one size fits all” blockchain implementation. Each one covers specific needs and has its own requirements.

02



## Privacy

Pseudonymity and traceability as opposed to full anonymity.

03



## Scalability

Bitcoin is only able to process around 4 trx/sec. and Ethereum around 20 trx/sec. Visa handles thousands.

04



## Latency

Current implementations take seconds or even minutes to validate a transaction, but areas such as IoT require much lower (sub-sec) latencies.

05



## Fee costs

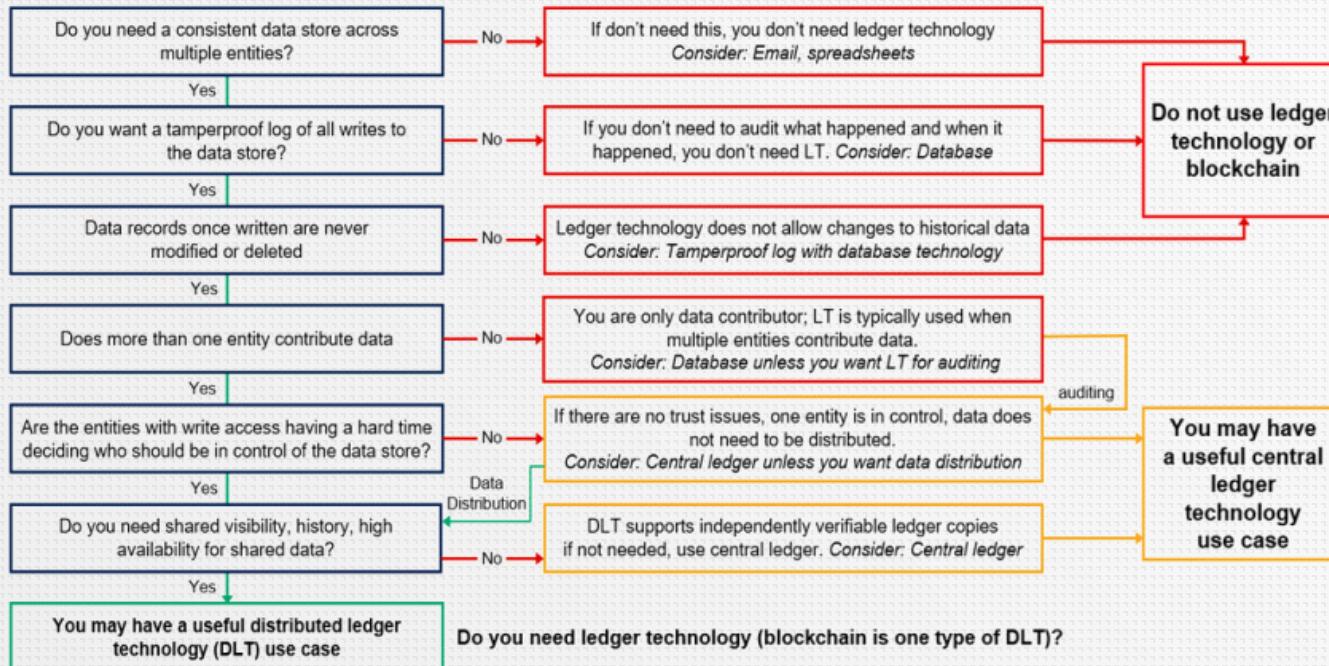
Fee costs (required by the proof of work consensus) is not viable for many use cases, such as IoT or micropayments.

# Blockchain and DLT are often not the answer



# When is blockchain and DLT the correct solution?

## Decision Tree for Ledger Technology Use Cases



# Real use cases

# Helping our clients in the complex DLT/Crypto world

**ANTI-FRAUD**

**CRYPTO BANK**

**TRACEABILITY**

**CAPITAL MARKETS**

**CUSTODY**

**FRAUD ALERT**

**CONFIRM**

**Click here for more information**

**Anti-fraud system from banks**  
Invoice de-duplication for anti-fraud management.

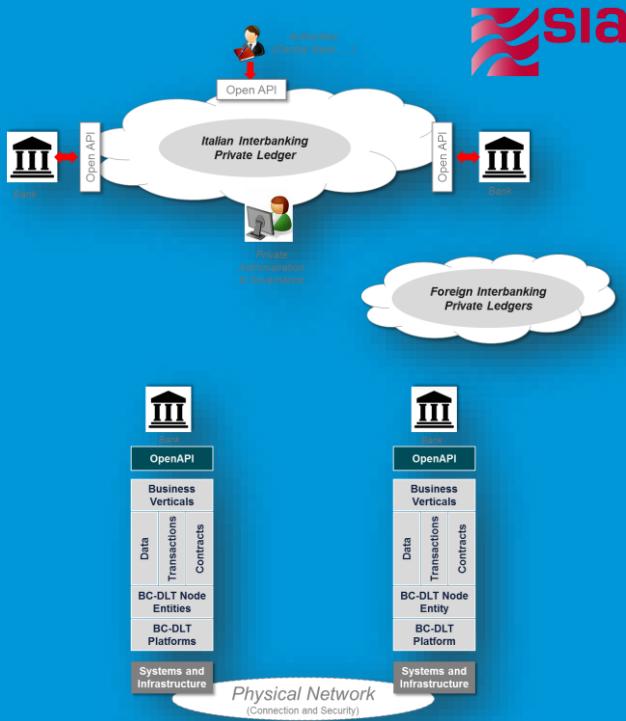
**Secure cryptocurrency trading**  
This major bank offers a unique B2B solution for other financial institutions acting as custodians of their clients' digital assets.

**Position maintenance for sub-custodian**  
Create Beneficial Owner identities for all positions (including all from Omnibus Accounts), enhancing SRDII compliance.

**Bond issuance platform**  
Design and build bond issuance platform based on DLT using DAML's Smart Contracts.

**Custody of digital assets**  
Development of a holistic solution for the custody and management of digital assets.

# Advance Invoice Lending: Interbanking utilization control



## Use Case

- Distributed ledger solution that prevents fraud when clients use the same invoice more times with different bank to get a lending
- A bank needs to be alerted when client tries to obtain credit for an invoice that has already been submitted (partially or fully)

## The Initial Project

- GFT developed the Use Case and created a panel of 10 Italian banks to test the feasibility/acceptance criteria
- POC has been completed by GFT in 3 months jointly with SIA, international financial processor provider of the blockchain infrastructure

## Outcome

- Use Case development and testing through multi-disciplinary workshops and POC
- Scalable architecture to host new Use Cases, in a multi-industry fashion (Finance, Manufacturing, Pharma, ...)
- Development of the production system now complete and running with 4 Italian banks

## Next steps

- Ongoing scale up to a secure, interoperable, multi-platform Blockchain-DLT network at European level as a collection of more than 500 nodes, to provide BC/DLT services through different technologies

# Secure cryptocurrency trading for a tier-one bank



## Success story

Designing and implementing a secure, cloud-based trading and custody platform for digital assets



New revenue opportunities



Leadership and innovation



Cybersecurity

CLOUD



BLOCKCHAIN & DLT



### THE CHALLENGE

In a market with many cryptocurrency trading solutions, this major bank offers a unique B2B solution for other financial institutions acting as custodians of their clients' digital assets

- Achieve the right balance between security and flexibility to meet evolving regulatory compliance requirements
- Integrate all trading and custody operations seamlessly
- Embrace cybersecurity and secure coding while enabling the use of hardware wallets and the latest cloud tools
- Reside in the cloud to fit in with the bank's technology strategy

### THE ENGAGEMENT

**Design and implementation of a back-end system for the custody and trading**

- GFT assembled a world-class team working across several geographies
- The technical landscape comprised a mix of modern technologies: Amazon Aurora, Java, Kubernetes, Solace VMR, Javalin, Guice, Liquibase, Gradle, Protractor, Terraform
- To accelerate progress the team adopted Agile methods and deconstructed tasks into manageable deliverables
- With cybersecurity paramount, it was decided to host customer wallets in a physical data centre with all communication secured using the latest standards

### THE BENEFIT

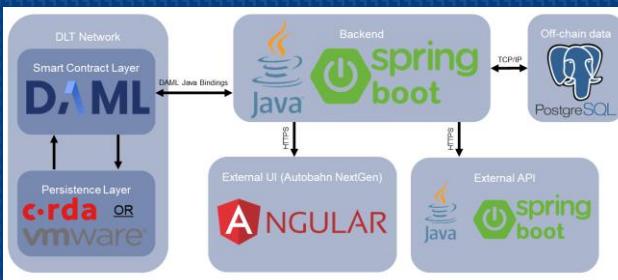
**New revenue opportunities for the bank in the cryptocurrency custody and trading space**

- With a secure, integrated solution the bank can participate confidently in the expanding cryptocurrency trading market
- The current solution combines the advantages of a decentralised market with tighter controls over transactions (such as antifraud and knowing the real beneficiary of a transfer) and the solution running checks before the transactions reach the relevant blockchain
- The bank has maintained its position as both a leader and innovator in distributed ledger technology
- The project's success is attracting other financial institutions and spurring interest in cryptocurrencies within financial markets

# DLT Based Beneficial Owner Management for Position Maintenance



Success story



BLOCKCHAIN & DLT



## PRINCIPAL OBJECTIVES

- Create a central location for position maintenance
- Create Beneficial Owner identities for all positions (including those that come from Omnibus Accounts) and therefore enhancing SRDII compliance
- Integration via EAP/Kafka Topics to core bank systems
- Create an External facing API and intuitive UI
- Design a highly secure and stable system designed for production environment (~12k TxPS, 14 participants)

## FUNDAMENTAL BENEFITS

- SRDII compliance mechanism (avoid high value charges)
- Easier tracking of fund owner information that needs to be updated (B.O view)
- Make the tracking of position tax compliance easier by offering a holistic positions view
- No system currently tracks the B.O status of positions (this is an entirely new/exclusive service)
- Improve transparency to the Global Custodians whilst maintaining privacy within the network

## WHY DLT FOR POSITION MAINTENANCE

- DLT provides a secure network where transactions between peers are audited immutably. This provides prove of provenance and breaks down trust boundaries between participant nodes in the network.
- Smart contracts provide a way of automating transactions between peers in a programmatic way to execute rules defined by the business.
- Data can (but is not always obliged to) be shared between network participants in a transparent and trustable manner.
- Golden source of data improves reconciliation in multi-system workflows

# SGX Project #HASH MVP0

## Success story

DLT: Bond issuance platform



CLOUD



BLOCKCHAIN & DLT



### THE CHALLENGE

#### Design and build bond issuance platform based on DLT using DAML's Smart Contracts

- Provide SGX Business, Technology, Operations, and Regulatory team with experience in digitalization of security issuance and lifecycle events
- Harness the capability of DAML smart contracts to build a re-imagined workflow required for issuance and custody of asset-backed tokens as well as enable real-time DvP settlement of these asset vs recording of cash transfers on ledger automatically
- Assess the current regulatory landscape and identify the changes needed to support development of smart contract and DLT infrastructure for the securities market in Singapore
- Identify the financial products that are likely to achieve the most benefits from a DAML smart contract DLT-enabled platform and have the greatest potential for commercialization
- Validate and quantify the benefits that smart contracts and DLT brings for the specific product(s). Validate the benefits with users and get their feedback/receptiveness to the MVP

### THE ENGAGEMENT

- Design: Market setup, Bond Issuance, Settlement, Coupon Payment, Redemption
- Development: DAML model reflecting bond issuance processes, Java backend application integrating with ledger, Angular frontend application
- End to end testing
- DevOps / IaC support

### THE BENEFIT

#### Streamline the currently fragmented processes; enable straight-through processing between Participants

- Permission-based visibility to the golden source of bond issuance, coupon payment, and redemption information
- Security provided by p2p network
- Reduce long lead times, risk, human errors and high investor costs

# Technical solution for custody of digital assets



Success story



BLOCKCHAIN & DLT



## THE CHALLENGE

### Holistic solution for the custody and management of digital assets

- Provide a technical solution for custody of digital assets for regulated financial services institutions
- Provide a platform with a rich set of features including integration to core banking systems, key management, tax reporting, compliance services and other value-added services
- Openness for a wider range of crypto assets

## THE ENGAGEMENT

### Takeover of the platform after the PoC for expansion and further development

- Provide blockchain knowledge for use case development
- Support of the ambitious roadmap to grow the platform
- General software development and support with technology and sector expertise

## THE BENEFIT

### Successfully settle securities transactions via tokens

- The platform allows bank customers to manage the entire lifecycle of their digital assets
- The platform will offer a new level of speed and efficiency in the financial services sector
- Enables regulated financial service institutions to provide their customers full access to Crypto Asset Classes covering major crypto currencies as well as digital assets
- Settlement of securities transactions using different DLT protocols
- Provides the necessary Tax information to end customers demanded from the different tax authorities

# DLT implementations

# There are many...



## Ethereum

Blockchain 2.0.  
De facto standard.



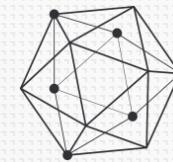
## Quorum

Based on Ethereum.  
Good for consortiums.



## Corda

Focus on finance.  
Interoperability with  
legacy systems.



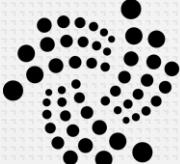
## Hyperledger

Pluggable consensus.  
Permissioned & scalable.



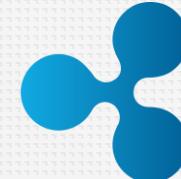
## Digital Assets

DSL for finance (DAML).  
Runs on many DLTs.



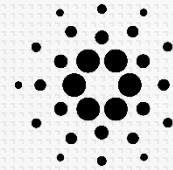
## IOTA

Best for IoT.  
No fees, high throughput.



## Ripple

Used for payments.  
Not fully decentralized.



## Cardano

Blockchain 3.0.  
Under development.

# Ethereum



## Description

*Ethereum is an **open-source, public**, blockchain-based distributed computing platform and operating system featuring **smart contract** (scripting) functionality.*



## Key aspects

- De facto standard
- Public & private blockchains
- Smart Contracts with Solidity
- Many tools available



## References

- Jupiter PoC
- GFT Coin v1
- Internal developer training

# Quorum



## Description

Quorum is an **enterprise-focused** version of Ethereum. Quorum is ideal for any application requiring **high speed** and **high throughput** processing of private transactions within a permissioned group of known participants.



## Key aspects

- Based on Ethereum (language & tools)
- Improves privacy, performance & permissions
- Configurable consensus
- Private transactions
- Good for permissioned blockchains (consortiums)
- Created by JP Morgan



## References

- GFT Coin v2 (PROD)
- Mytigate (Pharma Project)
- Alastria Consortium

# Corda



## Description

*Corda is a Distributed Ledger Technology to be used by businesses, such as **financial institutions**, to keep a **shared ledger of transactions** and thus removing the need for the involved parties to constantly check that each of their books are in line after interacting with each other.*



## Key aspects

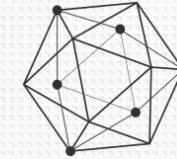
- Focus on financial industry
- Privacy and security
- Not really Blockchain (DAG)
- Permissioned network
- Smart Contracts with Kotlin, executed in Java Virtual Machine
- Interoperability with legacy systems



## References

- SIA Project (Italy)

# Hyperledger Fabric



## Description

*Hyperledger Fabric is a blockchain framework implementation hosted by The Linux Foundation. Intended for developing applications or solutions with a modular plug-and-play architecture.*



## Key aspects

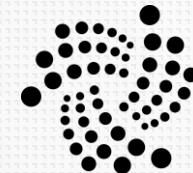
- Permissioned system
- Pluggable consensus protocol
- Prog. Languages: Go, Java, JS, Python...
- Better scalability
- Good cloud support
- Owned by the Linux Foundation



## References

- Introduction Course
- Automotive PoC (Poland)
- SPIE (Facility Management)
- KYC as a Service (Poland)

# IOTA



## Description

*IOTA is the first use case of the Tangle protocol which surpass Blockchain protocol in three key aspects: **transactions per second** (TPS), **scalability** and **zero fees**.*



## Key aspects

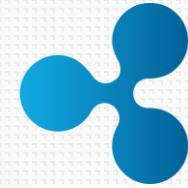
- Good for IoT
- No fees
- High throughput
- No smart contracts (yet)
- Immature
- Only public network
- Support nano payments (m2m)



## References

- Internal research

# Ripple



## Description

*Ripple connects banks and payment providers via RippleNet to provide one frictionless experience for **sending and receiving money globally**. Supports tokens representing fiat currency, cryptocurrency, commodities, or other units of value.*



## Key aspects

- Best for payments (faster and global)
- Not truly decentralized
- Important customers (UBS, Santander, MoneyGram...)
- Faster than current interbank payment systems



## References

- N/A



# Cardano

## Blockchain Third Generation

# Bitcoin: The crypto that changed everything





# The Power of Smart Contracts

# etherum

# Cardano vs. Ethereum

|                      | Cardano   | Ethereum            |
|----------------------|---|---------------------|
| Start Date           | September, 2017   | January, 2014       |
| Figurehead/Leader    | Charles Hoskinson   | Vitalik Buterin     |
| Consensus Mechanism  | PoS   | PoW (moving to PoS) |
| Programming Language | Haskell   | Solidity            |
| Architecture         | 2-layers (Cardano Settlement Layer and Cardano Computational Layer) | 1-layer             |

# Cardano: The Third Generation!



Scalability



Layered architecture



Cryptocurrency



Interoperability



Ecosystem



Multi Asset Ledger



# Cardano Roadmap

BYRON

Foundation



01

SHELLEY

Decentralization



02

GOGUEN

Smart contracts



03

BASHO

Scaling



04

VOLTAIRE

Governance



05

2017

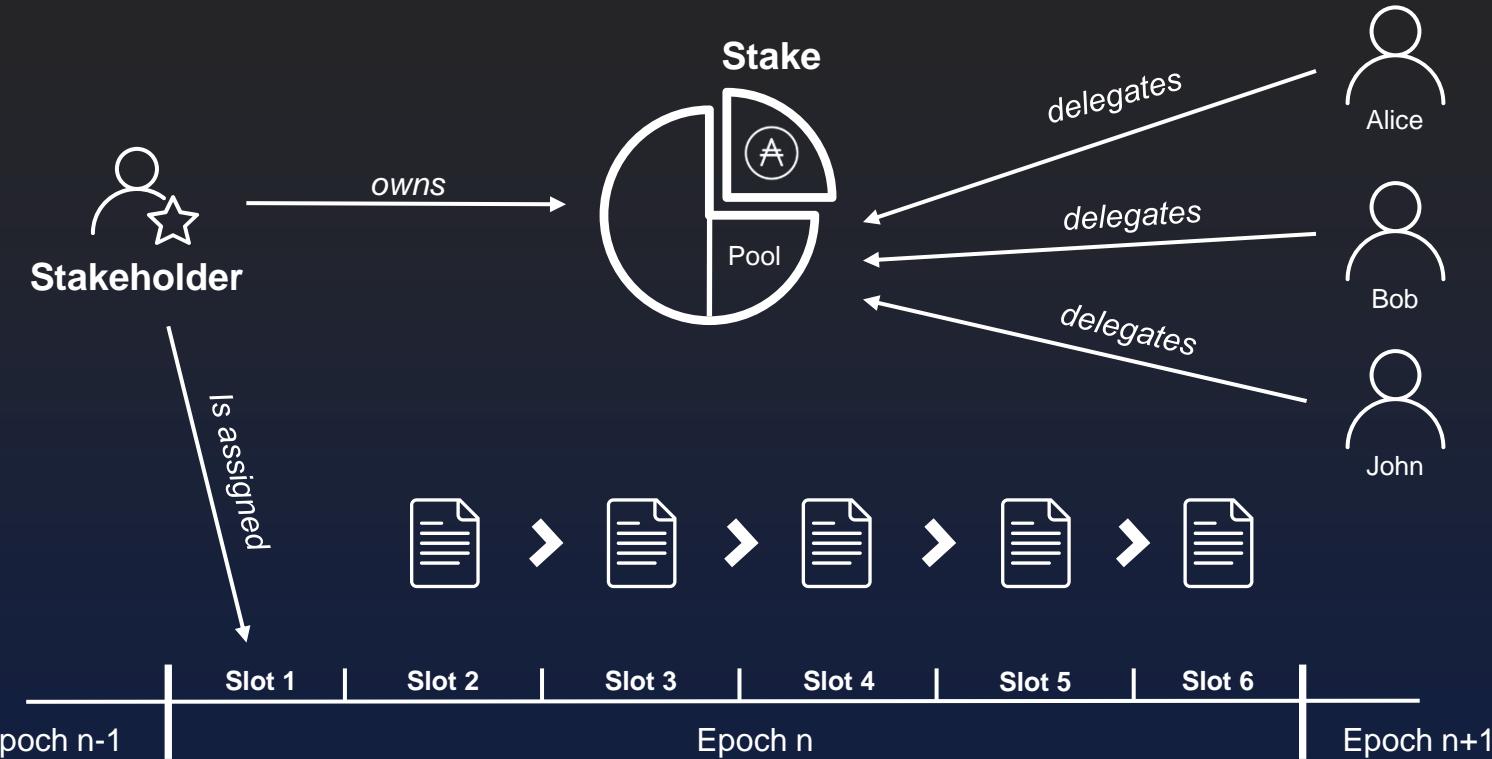
2018

2019

2020



## PoS – How it works



# Demo



**Money Transfer**



**Transaction details**  
(using Cardano Explorer)



**Delegation**

A woman with curly hair is smiling and looking down at her smartphone. She is wearing a dark t-shirt. The background is blurred, suggesting an indoor setting.

Quiz time!

# More on decentralization

# More on decentralization



Architecturally decentralized



Politically decentralized



Logically decentralized

|                               |                          | Logically centralized   |                           | Logically decentralized                 |                              |
|-------------------------------|--------------------------|-------------------------|---------------------------|---|------------------------------|
|                               |                          | Politically centralized | Politically decentralized | Politically centralized                 | Politically decentralized    |
| Architecturally centralized   | Traditional corporations | Direct democracy        |                           | ?                                       | ?                            |
|                               | Civil law                | Blockchains, Common law |                           |   |                              |
| Architecturally decentralized | ?                        | ?                       |                           | Traditional CDNs, Esperanto (initially) | BitTorrent, English language |
|                               | ?                        | ?                       |                           |   |                              |

<https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>

# Fully decentralized applications



## Storage

- **IPFS:** InterPlanetary FileSystem
- **Swarm:** Ethereum's dezentralized storage



## Communication

- **Whisper:** Ethereum's P2P communication protocol.



whisper



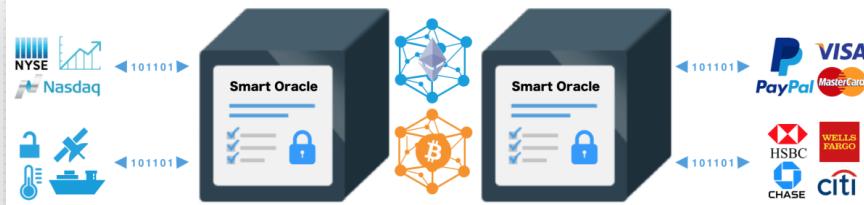
## Naming

- **ENS:** Ethereum naming system



# Oracles

An agent that finds and **verifies real-world occurrences and submits this information to a Blockchain** to be used by smart contracts, given that they cannot access data outside their network.



## Types

- Software Oracles
- Hardware Wallets
- Inbound Oracles
- Outbound Oracles
- Consensus Based Oracles

# DApps

- **Decentralized Apps (DApps)** are **like normal apps**, and offer similar functions, but the key difference is, they are **run on a peer-to-peer network**, such as a blockchain
- There are other **key features**, such as:
  - It must be open-source and operate on its own without anyone entity controlling it.
  - Its data and records must be public.
  - It must use a cryptographic token to help keep the network secure.

## Pros



- Censorship-resistant
- No downtime
- Blockchain-based
- Open-source

## Cons



- Hacks
- Usability
- Users (network effect)

<https://decrypt.co/resources/dapps>

# Decentralized Autonomous Organization (DAO)

- A Decentralized Autonomous Organization (DAO) is an organization represented by **rules encoded as a computer program** that is **transparent**, controlled by shareholders and not influenced by a central government
- A DAO's financial transaction record and program rules are **maintained on a blockchain**



AUGUR



STEEM

A woman with curly hair is smiling and looking down at her smartphone. She is wearing a dark t-shirt. The background is blurred, suggesting an indoor setting.

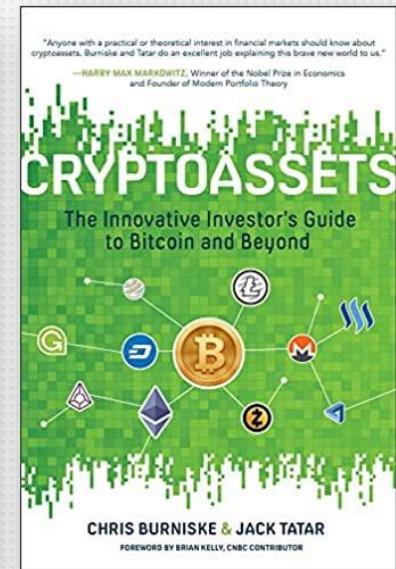
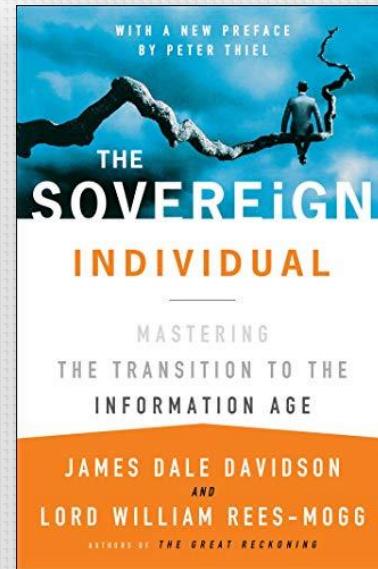
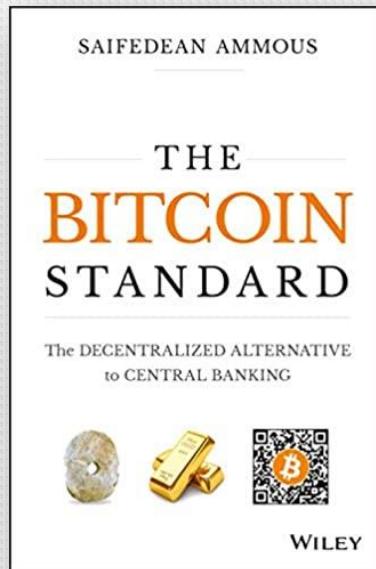
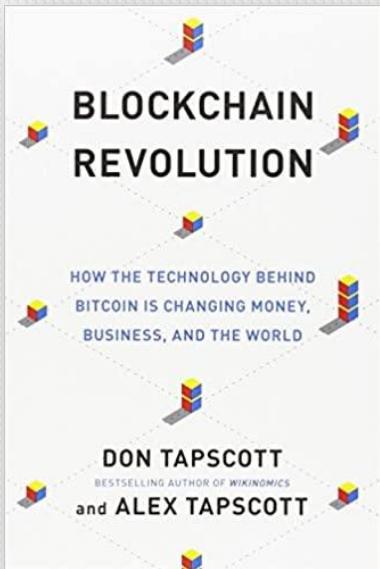
Quiz time!

# Summary & Resources

A circular word cloud composed of various blockchain-related terms, including:

- Blockchain
- Cryptography
- DLT
- Exchange
- Corda
- Consensus
- Hyperledger
- Decentralization
- Smart Contract
- Transaction
- IOTA
- Ethereum
- Bitcoin
- Mining
- Tokens
- Wallet
- Node
- Consortium
- Cardano
- Quorum

# Resources – Books



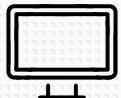
A lot more!!! <https://www.funontheride.com/libros-recomendados>



# Resources – Courses

- **Blockchain for dummies (Intro article)**
  - <https://cryptomaniaks.com/guides/blockchain-for-dummies-ultimate-blockchain-101-guide>
- **Beyond the Bitcoin Bubble (New York Times Article)**
  - <https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html>
- **Bitcoin and Cryptocurrency Technologies**
  - <https://www.coursera.org/learn/cryptocurrency>
- **Blockchain Revolution Specialization**
  - <https://www.coursera.org/specializations/blockchain-revolution-enterprise>
- **Blockchain Specialization**
  - <https://coursera.org/share/8e6bb883ee41d04d5b08ac48984d9d03>

# Resources – YouTube



FunOntheRide

63.100 suscriptores



Simply Explained

203.000 suscriptores



Boxmining ✓

217.000 suscriptores



Binance

62.700 suscriptores



Daniel Muvdi

101.000 suscriptores



David Battaglia

94.300 suscriptores



Chico Crypto ✓

161.000 suscriptores

# Shaping the future of digital business

**Esteban Chiner - GFT**

Senior Architect & Head of the “Blockchain & DLT” Offering Development  
GFT IT Consulting