EDEM
Escuela de Empresarios

# Introducción a **Blockchain y Criptomonedas**

GFT

Esteban Chiner

EDEM - MDA

Fecha 06/11/2021

# About me

- Working in GFT as a **Senior Architect** specialized in Big Data and Blockchain

- Part of the technological **Offering Development** team
- Leading the **"Data" and "DLT & Crypto" domains**
- **Certified Bitcoin Professional**
- **Certified Blockchain Architect**
- **Certified Ethereum Expert**

- **Lecturer**
  - Big Data & Analytics Master (**UPV**) – "Big Data Architectures in Financial Services"
  - Data Analytics for Enterprises (**EDEM**) – Seminar on Blockchain

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

- **Traveler**, **"Photographer", Geek** and **Fan** of cryptos and decentralization

**My Bio:**

0xD732650550dF069B7C25cbf1c701b678ccE35e24

(**Rinkeby**)

@echiner

echiner

esteban.chiner@gft.com

# Why GFT

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

## OUR CLIENTS

SGX
RBS
SYGNUM
sia
scventures by Standard Chartered
CUSTODIGIT
Deutsche Bank
BBVA
VPBANK

## OUR PARTNERS

CUSTODIGIT
r3
Digital Asset
vmware
ALASTRIA
CONSENSYS
Hedera Hashgraph

## GLOBALLY RECOGNIZED

***One of the top financial services providers worldwide***

Gartner
**“Market Guide for Blockchain Services”**

Everest Group
**“Major Contenders”**

FORRESTER
**“Invent The Future With Asset Tokenization”**



# I am not a financial advisor

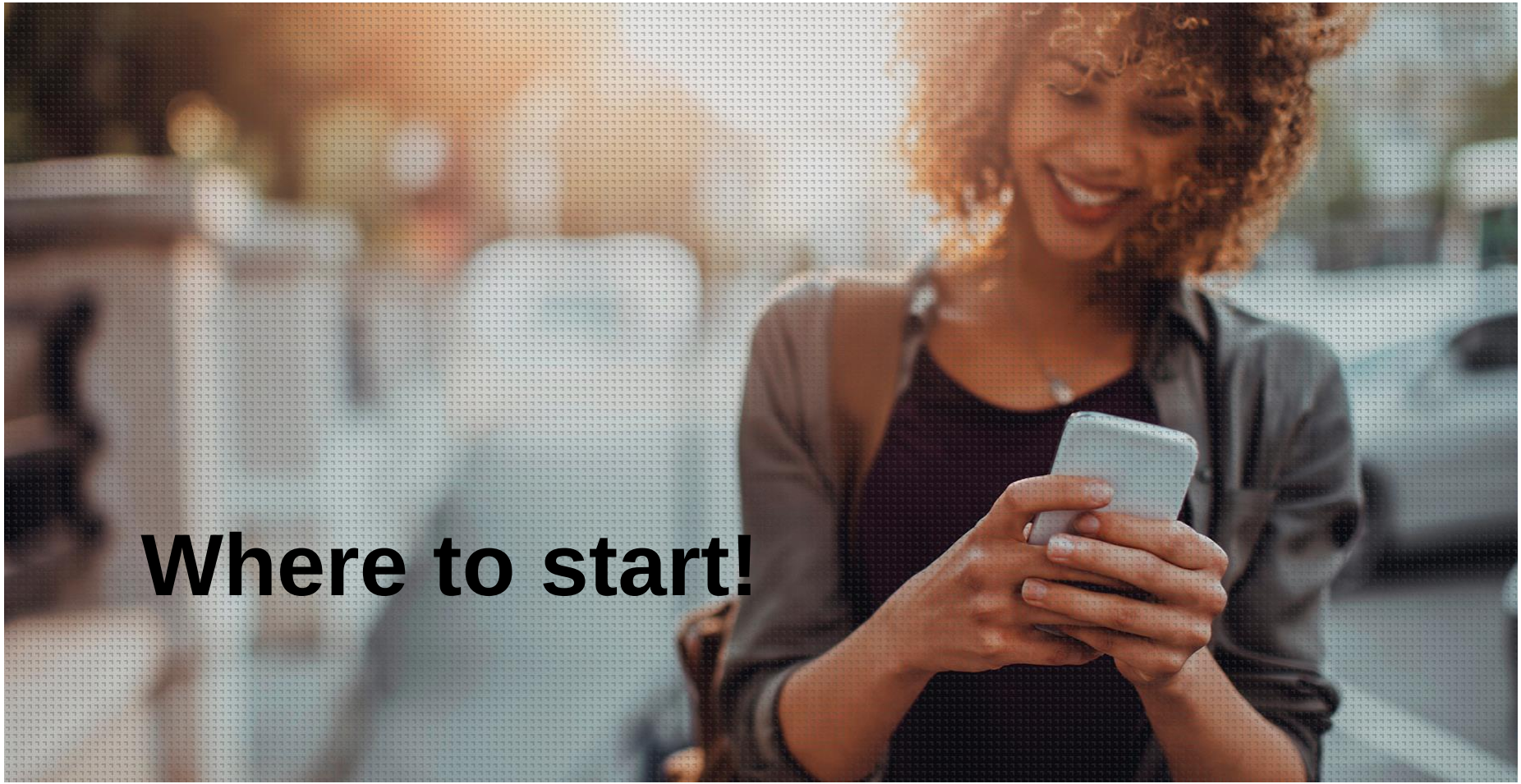
# Educational purposes

# Evaluations based on technology

# DYOR


# 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



# Where to start!

# Let’s start with the basics


Bitwala

# Basic concepts

- **bitcoin**: Popular virtual decentralized currency
- **Cryptocurrencies**: Digital asset used as a medium of exchange, i.e. decentralized currency
- **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
- **Smart Contracts**: Autonomous programs running on a DLT
- **DApps**: Decentralized Applications

## Applications


## Other Implementations

## Cryptocurrencies

and **many** others!

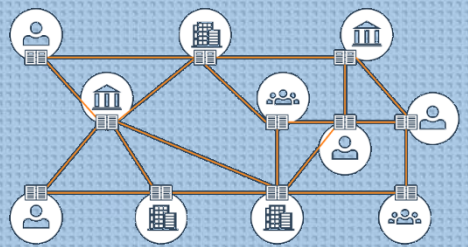
## DLT

- **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.”*

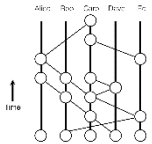
Wikipedia

**Distributed Ledger Technologies**

**Blockchain**

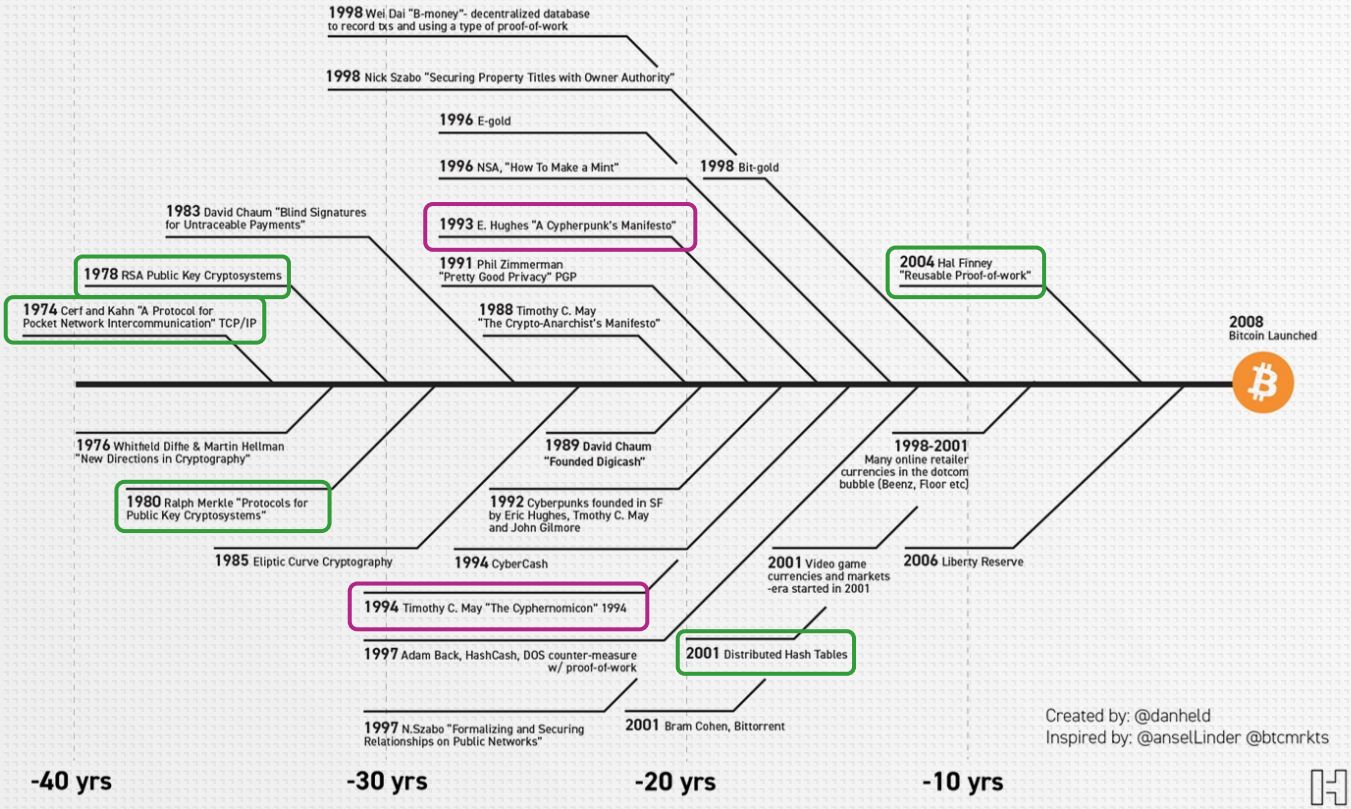
**Tangle**

**Hashgraph**



# A little bit of history

# Bitcoin prehistory



# Early days


"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"

"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**"

# 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
11. Surveillance, Privacy, And Intelligence Agencies
12. 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.


THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout Inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I Won't Marry Again

Giant Killing? Guide to the FA Cup Third Round

CoinBase

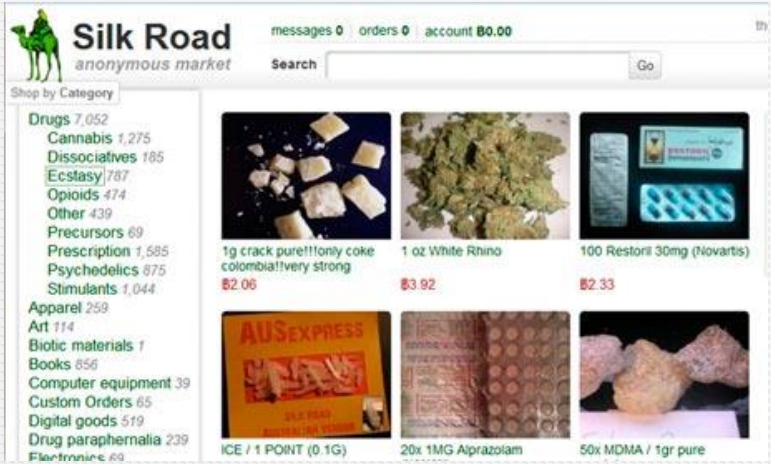
04ffff001d0104455468652054696d65732030332f4a616e2f323030392043686616e63656c6c6f72206f6e206272696e6b206f66207365636f6e642061696c6f757420666f722062616e6b73

**(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

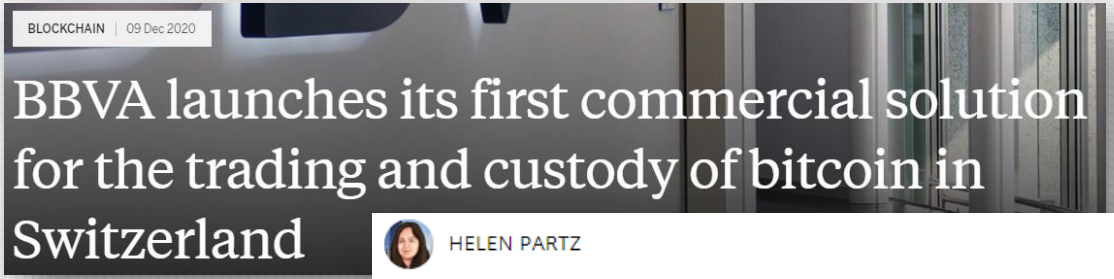



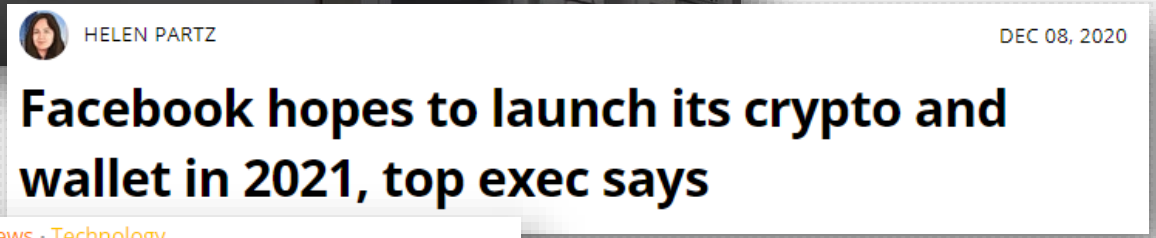
# Banking on Bitcoin (Documentary)


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

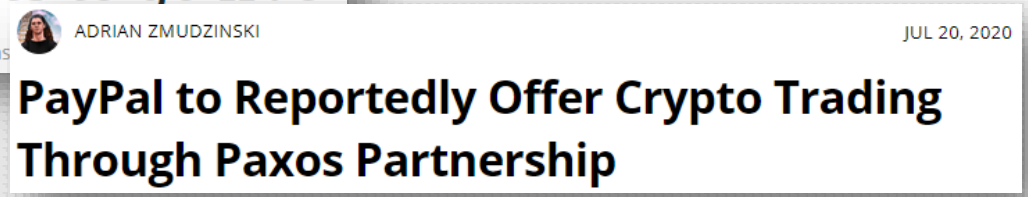
# Blockchain and crypto boom!

# 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

# Mainstream


Mastercard Will Let Merchants Accept Payments in Crypto This Year
The payments giant plans to support digital currency transactions di
on network.


TECH
Tesla buys $1.5 billion in bitcoin, plans to accept it as payment
PUBLISHED MON, FEB 8 2021•7:48 AM EST | UPDATED MON, FEB 8 2021•1:43 PM EST
Steve Kovach
@STEVEKOVACH
SHARE


euronews.
Ethereum jumps to record high after reports the EIB will issue digital bonds


PayPal CEO says the payments giant wants to be 'the digital wallet for global CBDCs'
by Aislinn Keely
Download PDF / Print
February 11, 2021, 5:58PM EST · 2 min read

# Where we are today

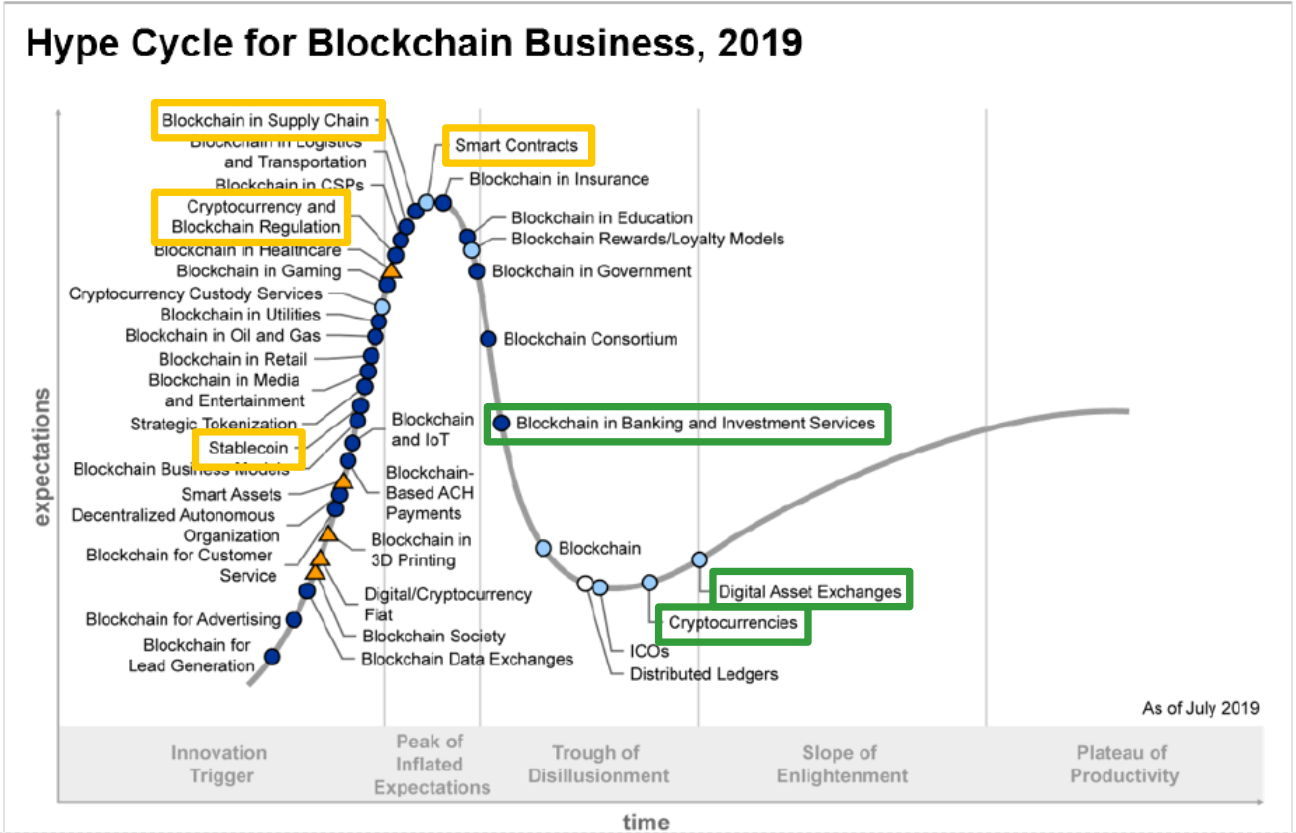

Dozens of **blockchain technologies**

*(Corda, Hyperledger, Quorum, IOTA, DAH, Cardano…)*

Over 4000 **cryptocurrencies**

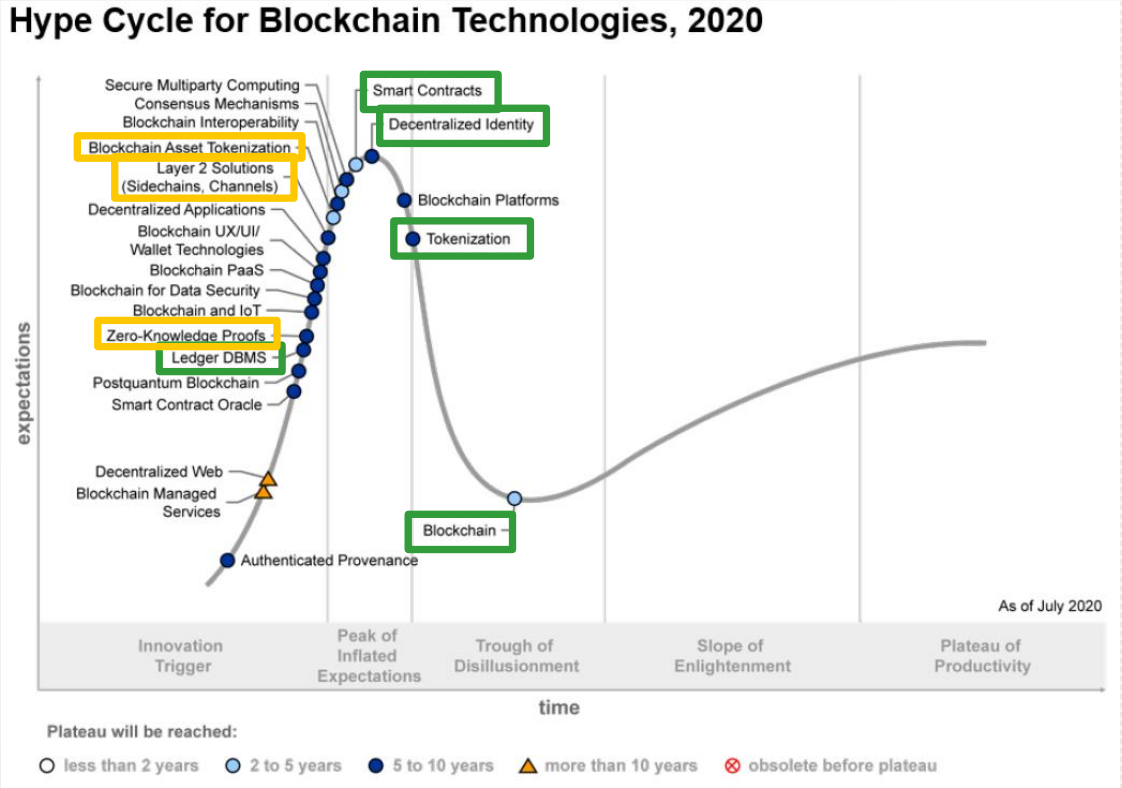
*(https://coinmarketcap.com/all/views/all/)*

# Where we are in 2019 - Business




**Source**: Gartner

# Where we are in 2020 - Technology



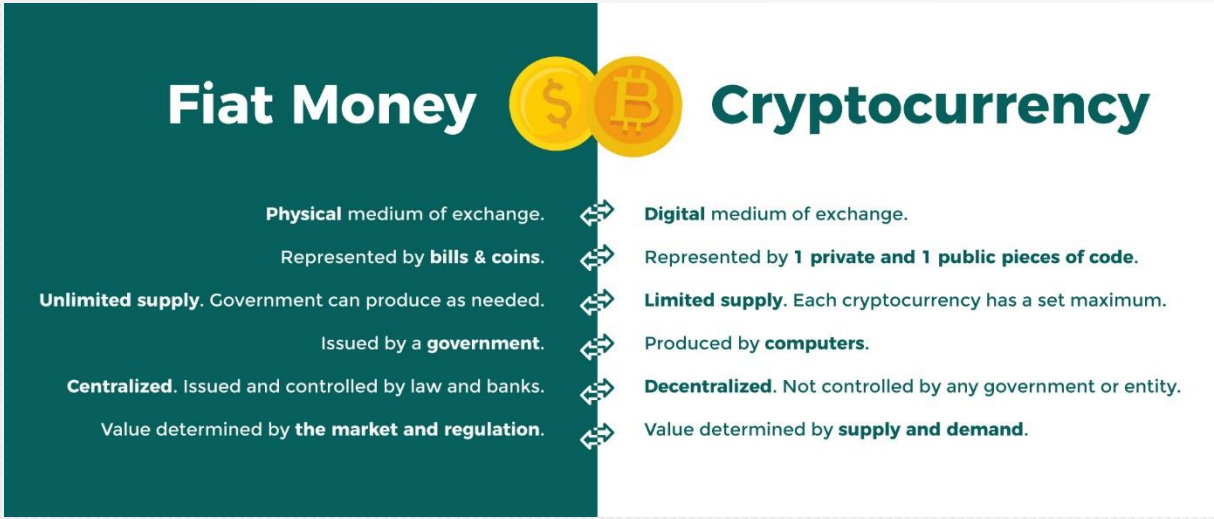

**Source**: Gartner

# 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.

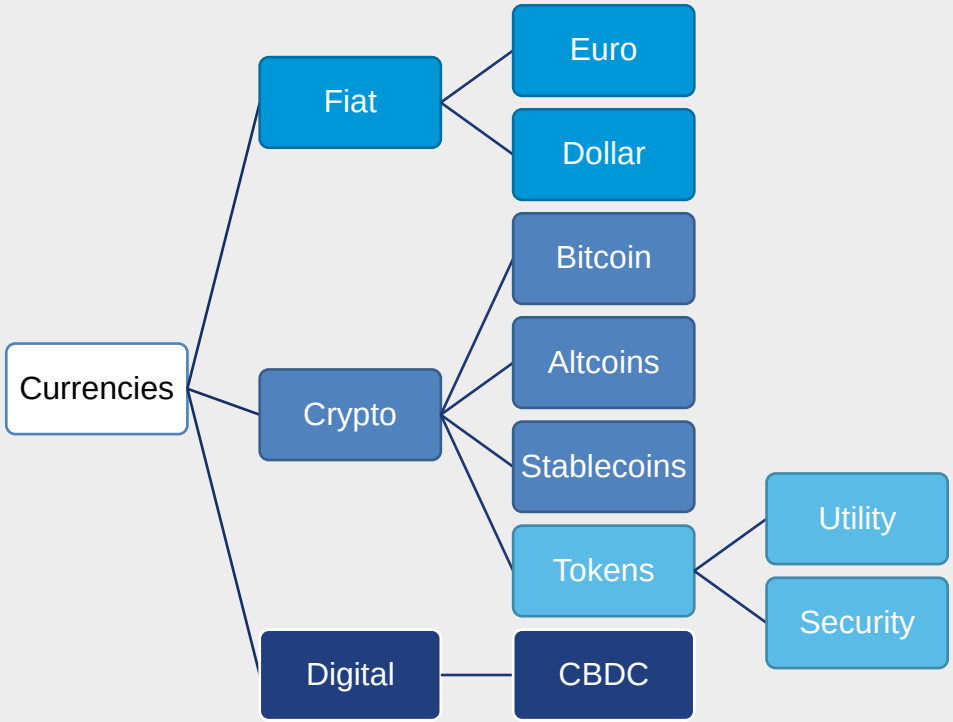

Let’s vote!

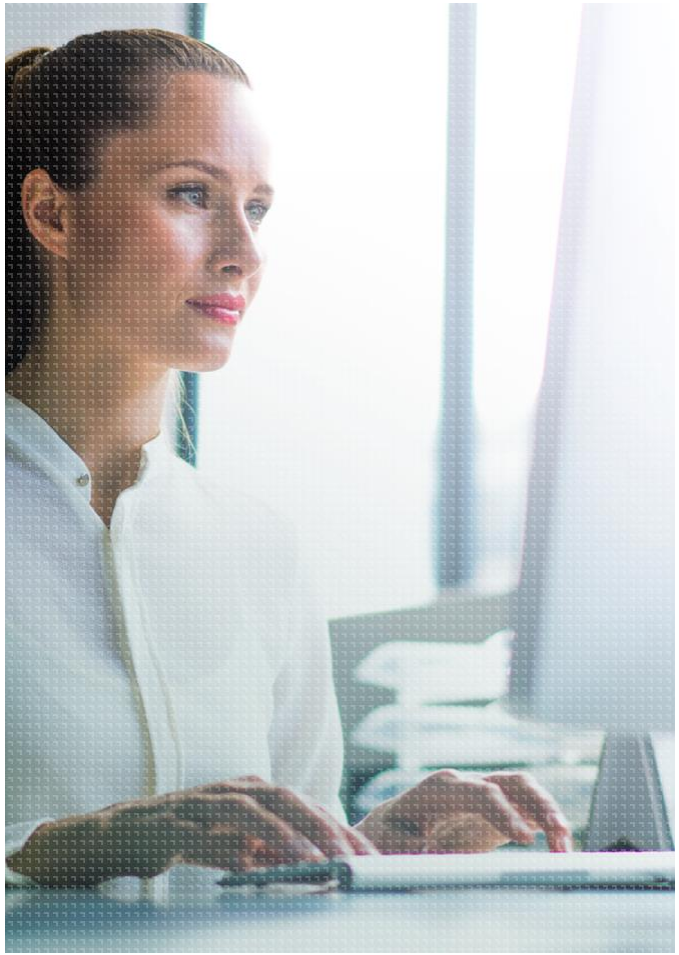
# Formal definition

- 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**.

**Possible State Approaches to Cryptocurrencies - Jan Lansky**

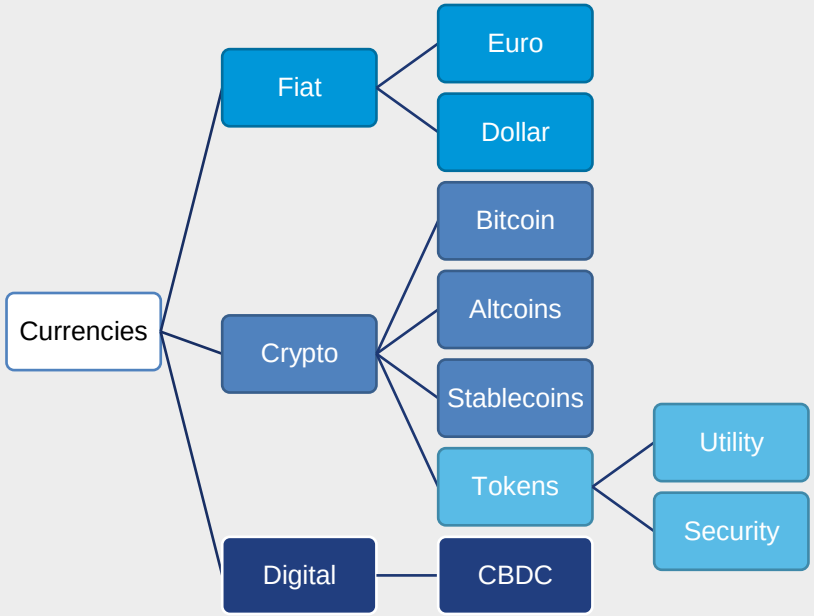

# Types of (crypto)currencies





# **Exercise:** Cryptocurrencies

Search for different currencies and classify them into the following categories:



# Types or sub-types

## Altcoins

**Altoins** 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

CoinMarketCap

| # | Name | Price | 24h % | 7d % | Market Cap | Volume(24h) | Circulating Supply | Last 7 Days |
|---|---|---|---|---|---|---|---|---|
| 1 | Bitcoin BTC Buy | $63,061.97 | 0.04% | 7.24% | $1,189,537,406,505 | $36,310,441,974<br>575,790 BTC | 18,862,993 BTC | |
| 2 | Ethereum ETH Buy | $4,603.13 | 1.65% | 15.17% | $544,069,725,386 | $21,555,664,805<br>4,682,830 ETH | 118,195,649 ETH | |
| 3 | Binance Coin BNB Buy | $567.99 | 1.68% | 25.03% | $94,740,669,360 | $2,526,128,954<br>4,447,522 BNB | 166,801,148 BNB | |
| 4 | Solana SOL | $240.50 | 12.43% | 26.71% | $72,409,191,106 | $5,936,001,295<br>24,681,734 SOL | 301,075,474 SOL | |
| 5 | Tether USDT Buy | $1.00 | 0.03% | 0.01% | $71,094,902,172 | $88,904,643,857<br>88,843,192,199 USDT | 71,045,760,761 USDT | |
| 6 | Cardano ADA | $2.07 | 5.55% | 5.98% | $68,961,713,539 | $4,681,573,762<br>2,258,606,692 ADA | 33,270,305,168 ADA | |
| 7 | XRP XRP | $1.21 | 7.42% | 19.07% | $56,933,254,183 | $6,333,425,587<br>5,237,506,985 XRP | 47,081,679,946 XRP | |
| 8 | Polkadot DOT | $53.97 | 4.42% | 31.23% | $53,299,387,659 | $3,367,983,906<br>62,405,055 DOT | 987,579,315 DOT | |
| 9 | Dogecoin DOGE | $0.2696 | 1.96% | 11.52% | $35,580,805,001 | $2,096,382,468<br>7,775,563,908 DOGE | 131,970,586,164 DOGE | |
| 10 | USD Coin USDC | $1.00 | 0.07% | 0.02% | $33,596,356,697 | $4,822,800,509<br>4,821,575,433 USDC | 33,587,822,633 USDC | |

# 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).

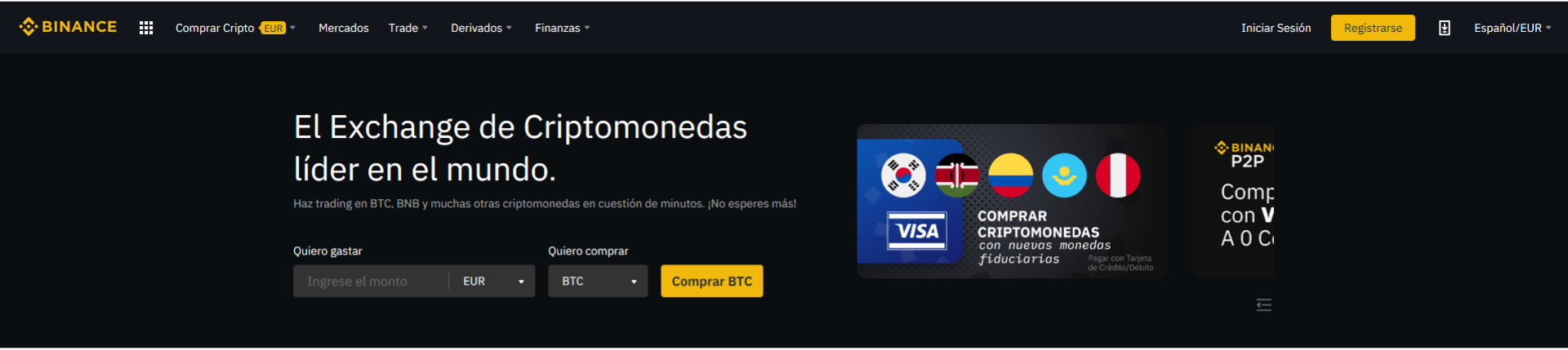
## Features:

- 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…

BINANCE

coinbase

kraken

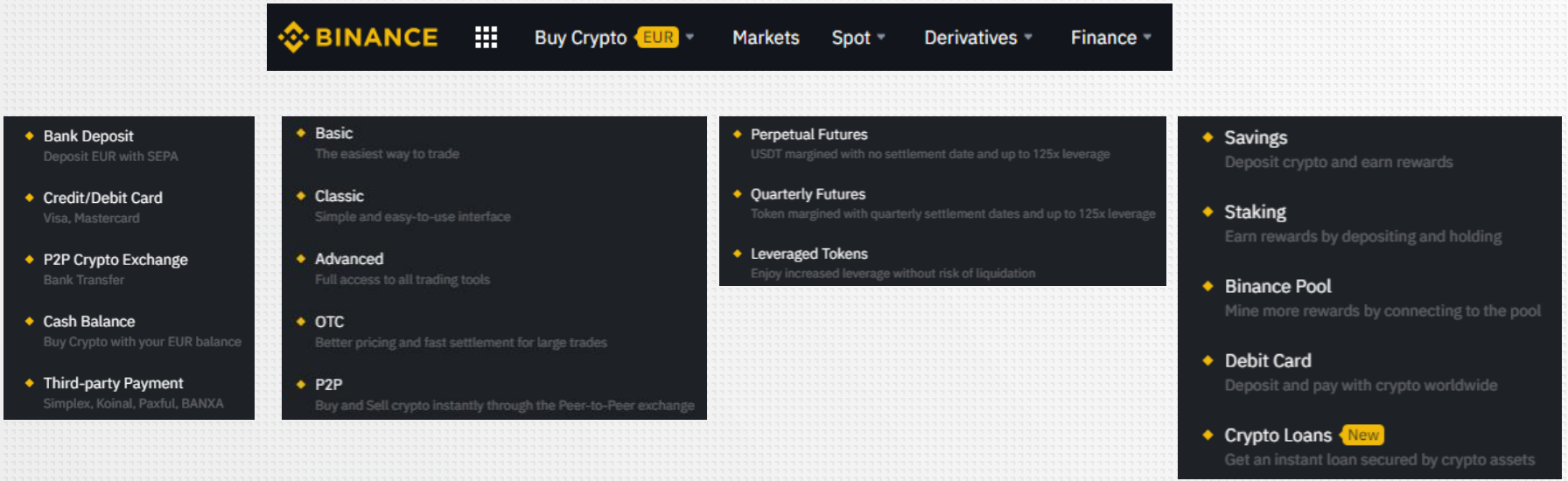



La actividad de trading de MATIC ha finalizado 06-16 | Más >

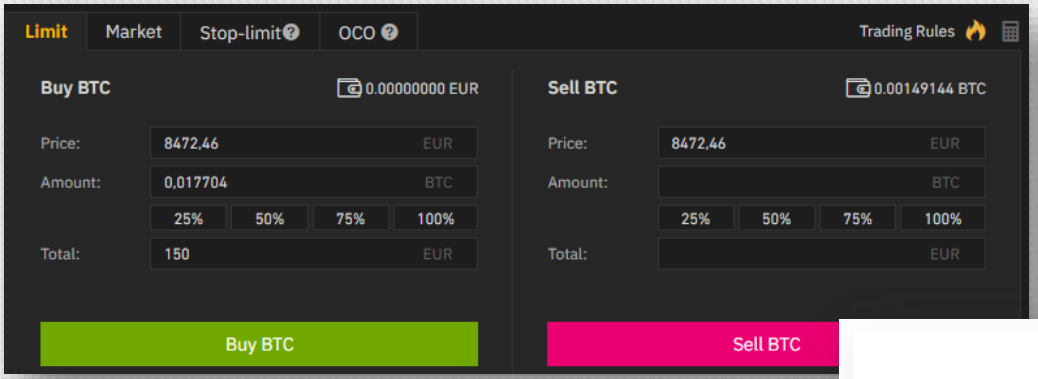
| Nombre completo | Último precio | 24h cambio | Mercados |
|---|---|---|---|
| BNB BNB | € 14.60 | +0.63% | |
| BTC Bitcoin | € 8,430.01 | +0.11% | |
| ETH Ethereum | € 208.27 | +0.88% | |
| XRP Ripple | € 0.173230 | +1.79% | |
| BCH Bitcoin Cash | € 213.90 | +1.77% | |
| LTC Litecoin | € 39.68 | +2.31% | |

# Exchanges nowadays

- Exchanges nowadays are **closer to the existing banks**, and offer features usually providedº by them.
- **Example**:

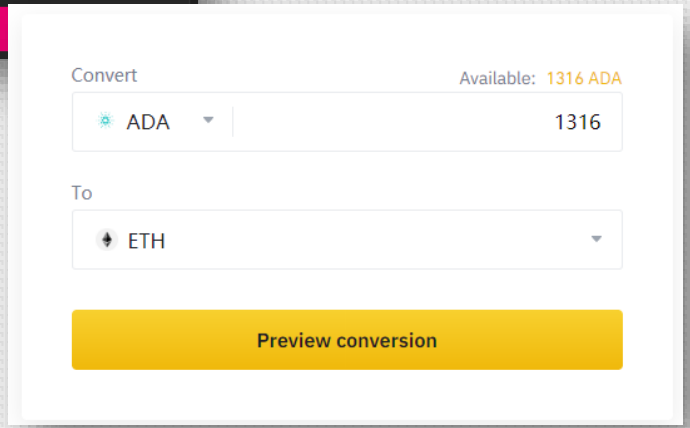


# Crypto trading

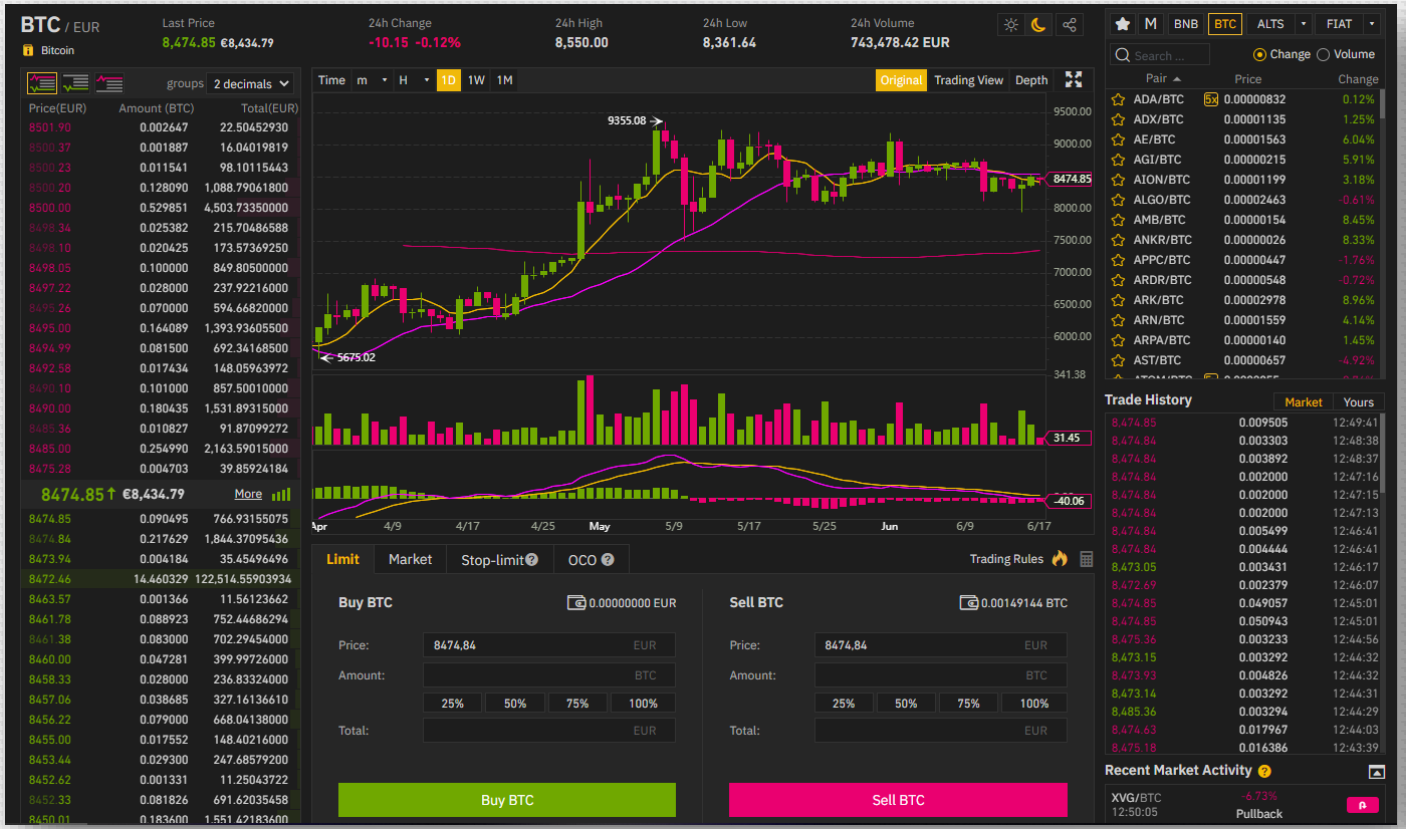



Fiat to crypto

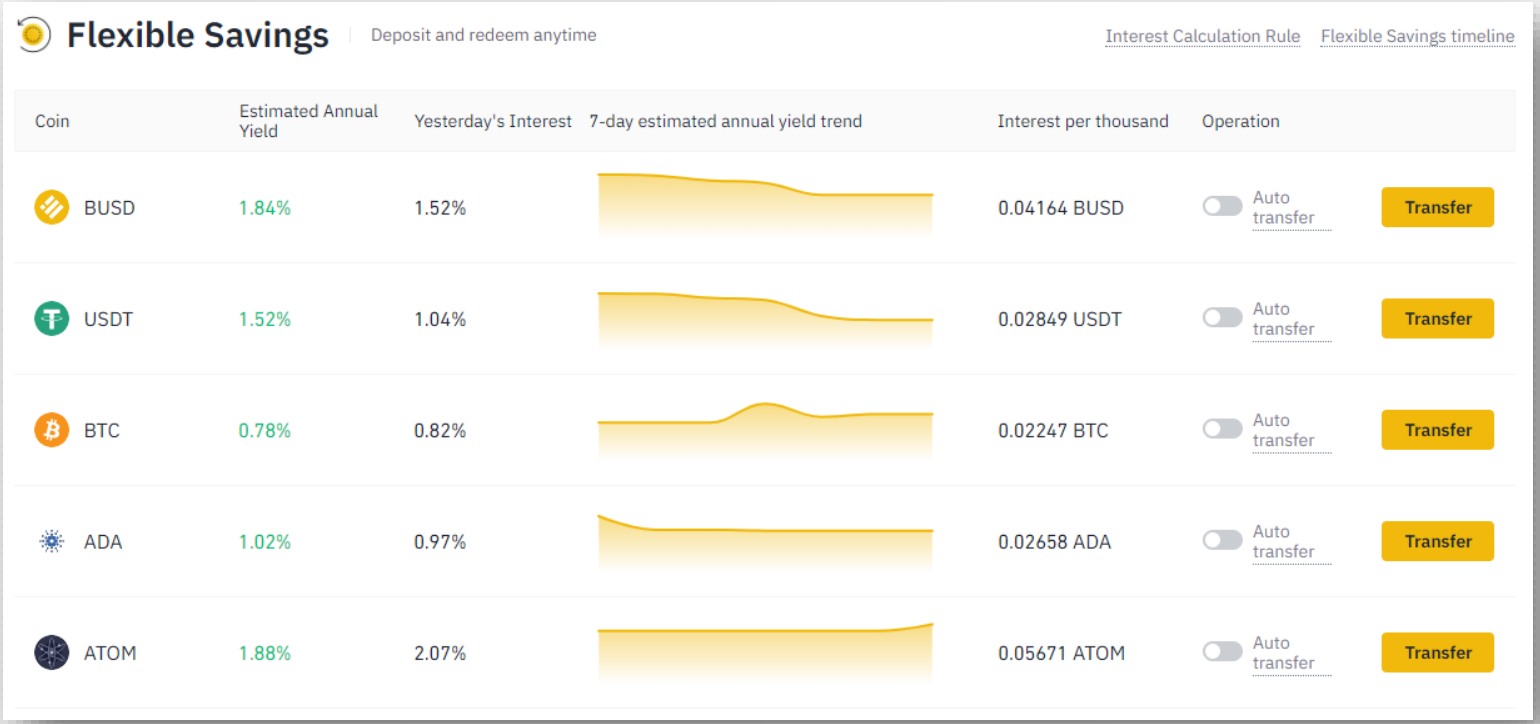
Crypto to crypto



# Trading


BTC / EUR
Bitcoin
Last Price
8,474.85 €8,434.79
24h Change
-10.15 -0.12%
24h High
8,550.00
24h Low
8,361.64
24h Volume
743,478.42 EUR
groups 2 decimals
Price(EUR) Amount (BTC) Total(EUR)
8474.85 €8,434.79 More
Time m H 1D 1W 1M
Original Trading View Depth
9355.08
5675.02
Limit Market Stop-limit OCO
Trading Rules
Buy BTC
0.00000000 EUR
Price: 8474,84 EUR
Amount: BTC
25% 50% 75% 100%
Total: EUR
Buy BTC
Sell BTC
0.00149144 BTC
Price: 8474,84 EUR
Amount: BTC
25% 50% 75% 100%
Total: EUR
Sell BTC
BNB BTC ALTS FIAT
Search ...
Change Volume
Pair Price Change
Trade History
Market Yours
Recent Market Activity
XVG/BTC
12:50:05
-6.73%
Pullback

# Savings


Flexible Savings
Deposit and redeem anytime
Interest Calculation Rule
Flexible Savings timeline
Coin
Estimated Annual Yield
Yesterday's Interest
7-day estimated annual yield trend
Interest per thousand
Operation
BUSD
1.84%
1.52%
0.04164 BUSD
Auto transfer
Transfer
USDT
1.52%
1.04%
0.02849 USDT
Auto transfer
Transfer
BTC
0.78%
0.82%
0.02247 BTC
Auto transfer
Transfer
ADA
1.02%
0.97%
0.02658 ADA
Auto transfer
Transfer
ATOM
1.88%
2.07%
0.05671 ATOM
Auto transfer
Transfer

# Loans & Credit Card

I want to borrow

USDT

Collateral Amount

Only show my asset

BTC

Initial LTV 65% Margin Call 75% Liquidation LTV 83%

Loan Term

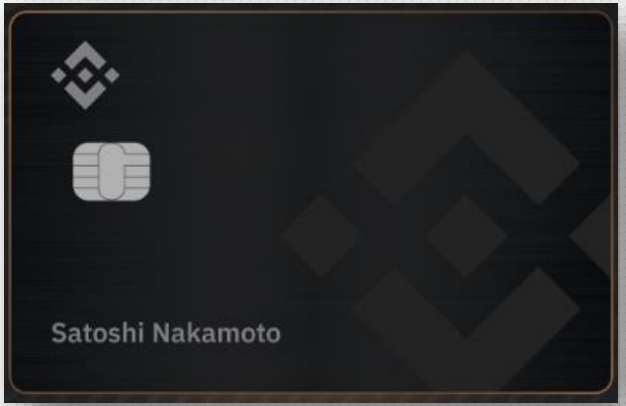
7 Days | 14 Days | 30 Days | 90 Days

Interest

| | |
|---|---|
| Annual Interest Rate | 11.13% |
| Daily Interest Rate | 0.0305% |
| Total Interest Amount | - USDT |

Repayment Amount - USDT

Start borrowing now



# Crypto specific: Pool & Staking

## Proof of Work

| Coin | Algo | Active Workers | Hashrate | Network | Tutorial |
|---|---|---|---|---|---|
| | SHA256 | 108727 | 6.76 EH/s | 101.71/2.95/1.90 EH/s | View tutorial |

Hashrate EH/s


Mining URL stratum+tcp://sha256.poolbinance.com:8888

Mining URL stratum+tcp://bs.poolbinance.com:3333

( Supported ports 8888、3333、1800、443 )

Calculation 1 TH/s → 0.00000839 BTC, 0.00030188 BCH, 0.00048253 BSV

Mining Fee 2.50%

Settlement Method FPPS

Payment Method The settlement period is from 08:00 the previous day to 08:00 the current day.

## Staking

**EOS Staking**

Projected annual earnings: 1%-3%

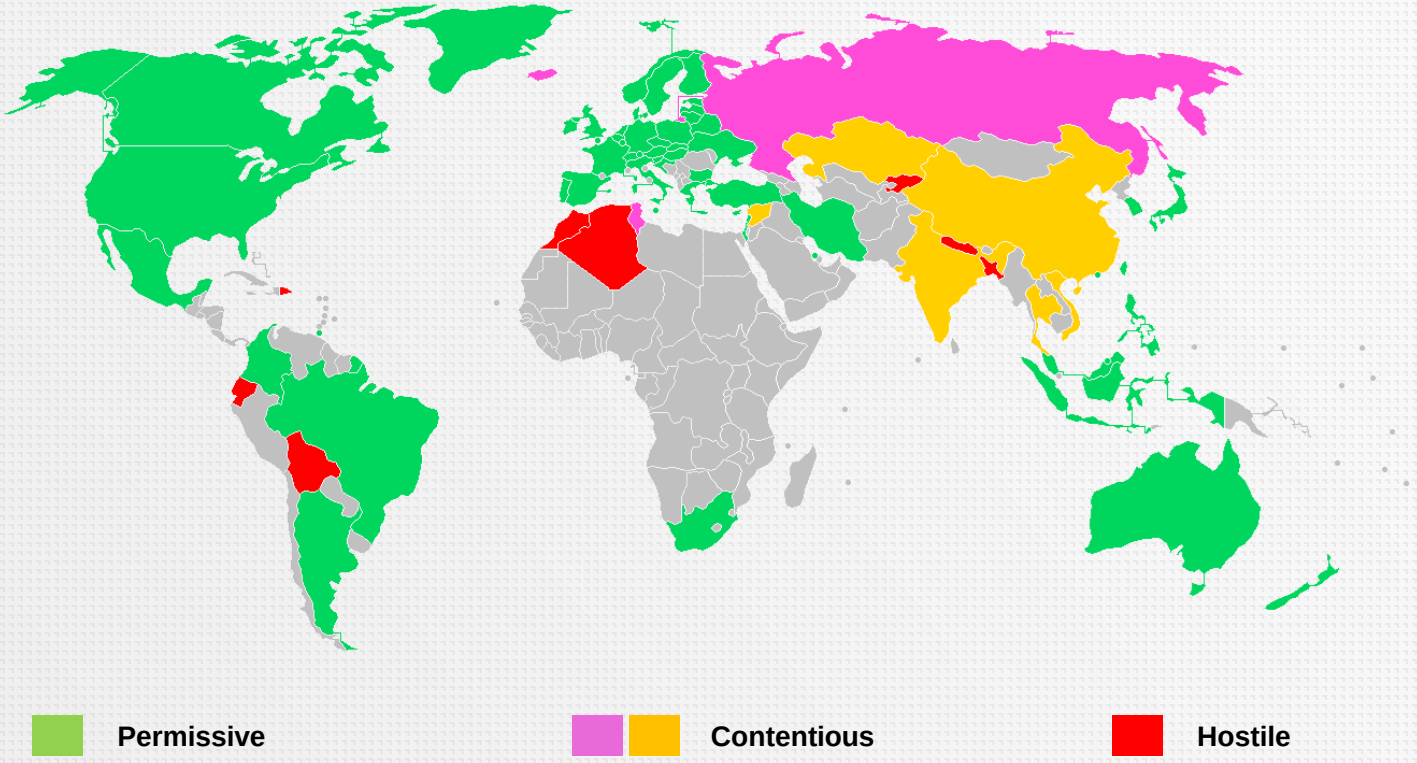
**GXS Staking 5x Initial Reward Multiplier**

Projected annual earnings: 11%-22%

**Tezos Staking**

Projected annual earnings: 6%-9%

# Legality



# Taxation (in Spain)

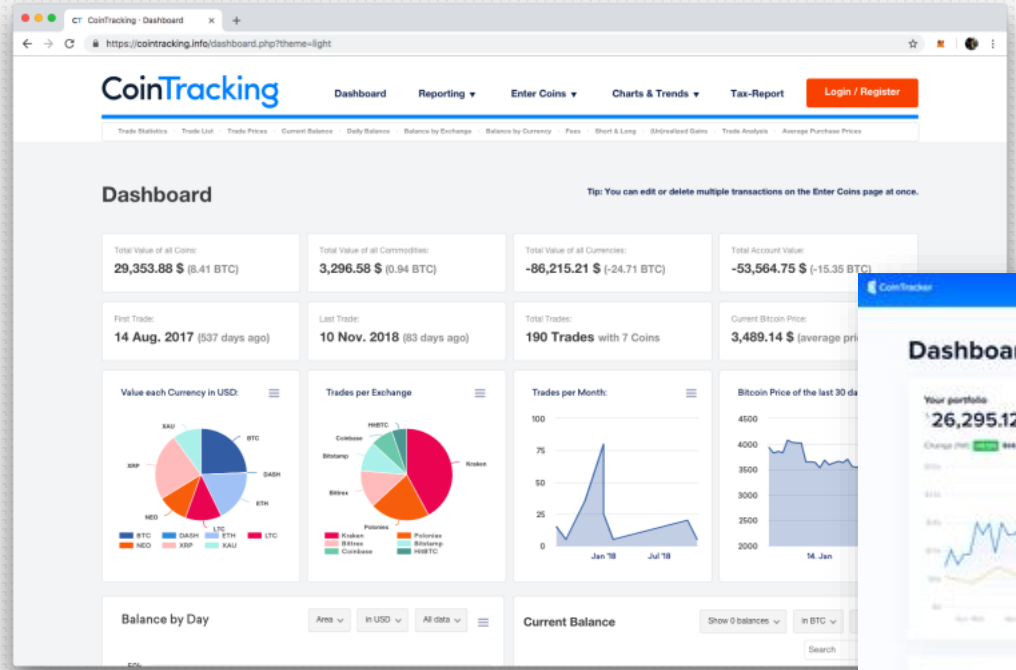
- **Trade** (crypto/crypto or crypto/fiat)
  - Patrimony increase (buy price – sell price)
- **Derivatives** (Futures & Options)
  - Patrimony increase (price difference)
- **Staking**
  - Interests (same as bank account)
- **Mining** (PoW)
  - Economic activity
- **Airdrops & Hardforks**
  - Patrimony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

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

# Taxes in Spain


**Video**: https://www.youtube.com/watch?v=6h4GO4tldX0

# Manage your crypto and prepare for taxes




CoinTracking


CoinTracker

# CBDC
## Central Bank Digital Currencies

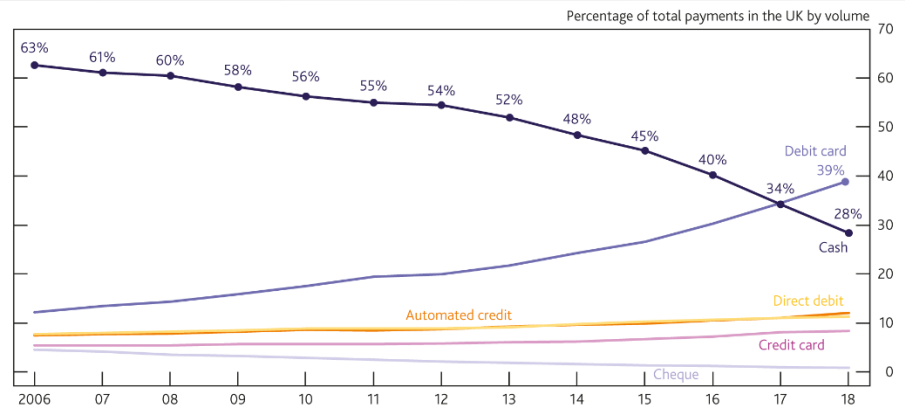
# Crypto vs. Fiat

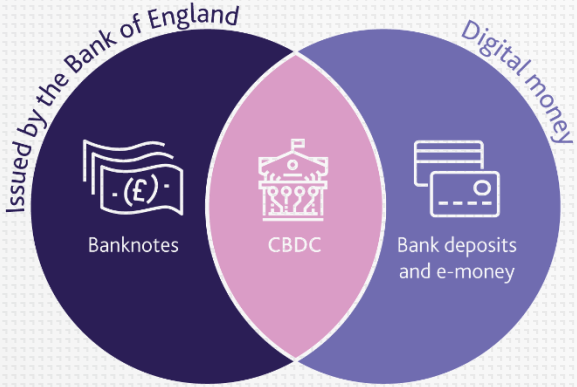
+ Peer-to-peer
+ Programable money

| Fiat Money | | Cryptocurrency |
|---|---|---|
| **Physical** medium of exchange. | ⇔ | **Digital** medium of exchange. |
| Represented by **bills & coins**. | ⇔ | Represented by **1 private and 1 public pieces of code**. |
| **Unlimited supply**. Government can produce as needed. | ⇔ | **Limited supply**. Each cryptocurrency has a set maximum. |
| Issued by a **government**. | ⇔ | Produced by **computers**. |
| **Centralized**. Issued and controlled by law and banks. | ⇔ | **Decentralized**. Not controlled by any government or entity. |
| Value determined by **the market and regulation**. | ⇔ | Value determined by **supply and demand**. |

# Central Bank Digital Currencies (CBDC)

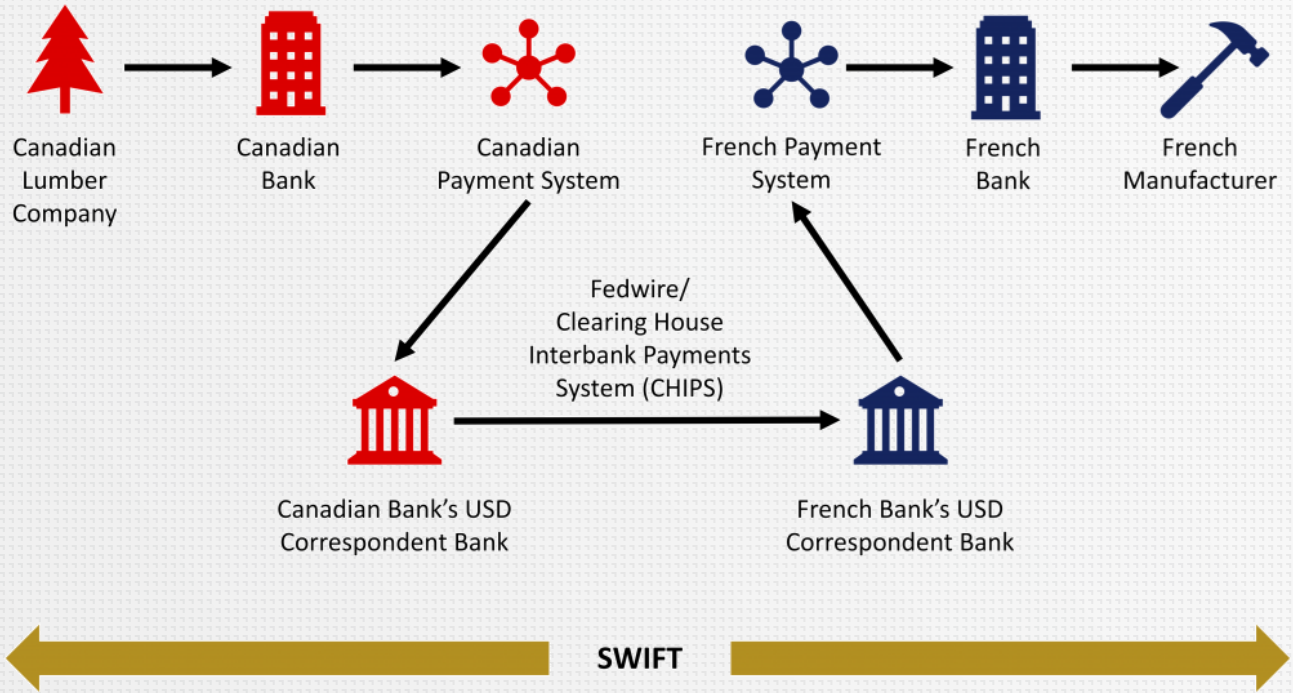
A **Central Bank Digital Currency (CBDC)** is a digital asset **issued by a central bank** for the purpose of **payment and settlement**, in either retail or wholesale transactions.




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.

# Payment systems today

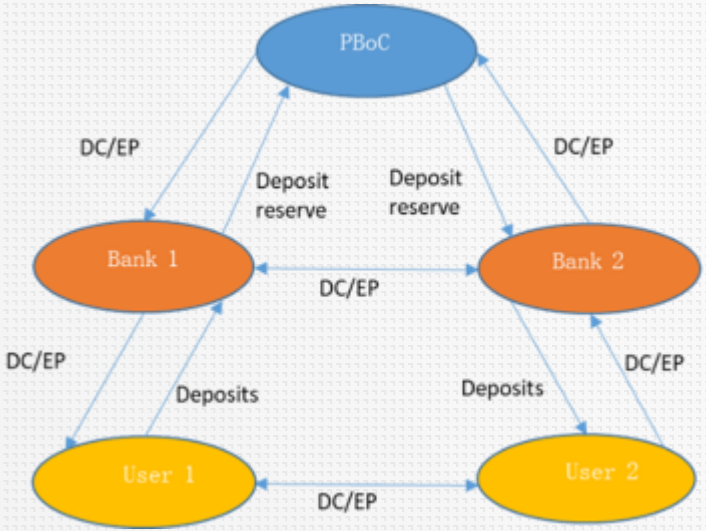


# Introduction

*“Central Bank Digital Currencies (CBDCs) and the transformation of global payments”*
**Source**: ConsenSysMedia

# 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)



# CBDC – The Money of Tomorrow

## Replace Cash

Should replace cash (eventually);

All transactions at all points of sale and between individuals and organizations will be digital.

## Same Value

Will have the same value as cash of today and be exchanged at a rate of 1:1

## Distributed Ledger Technologies

Using Distributed Ledger Technology, the ‘journey’ of money earned and spent will be trackable/ traceable; difficult to lose/ steal; peer-to-peer;

## Cost reduction

Will eliminate costs attributable to the production, distribution/transport , storage and protection of cash

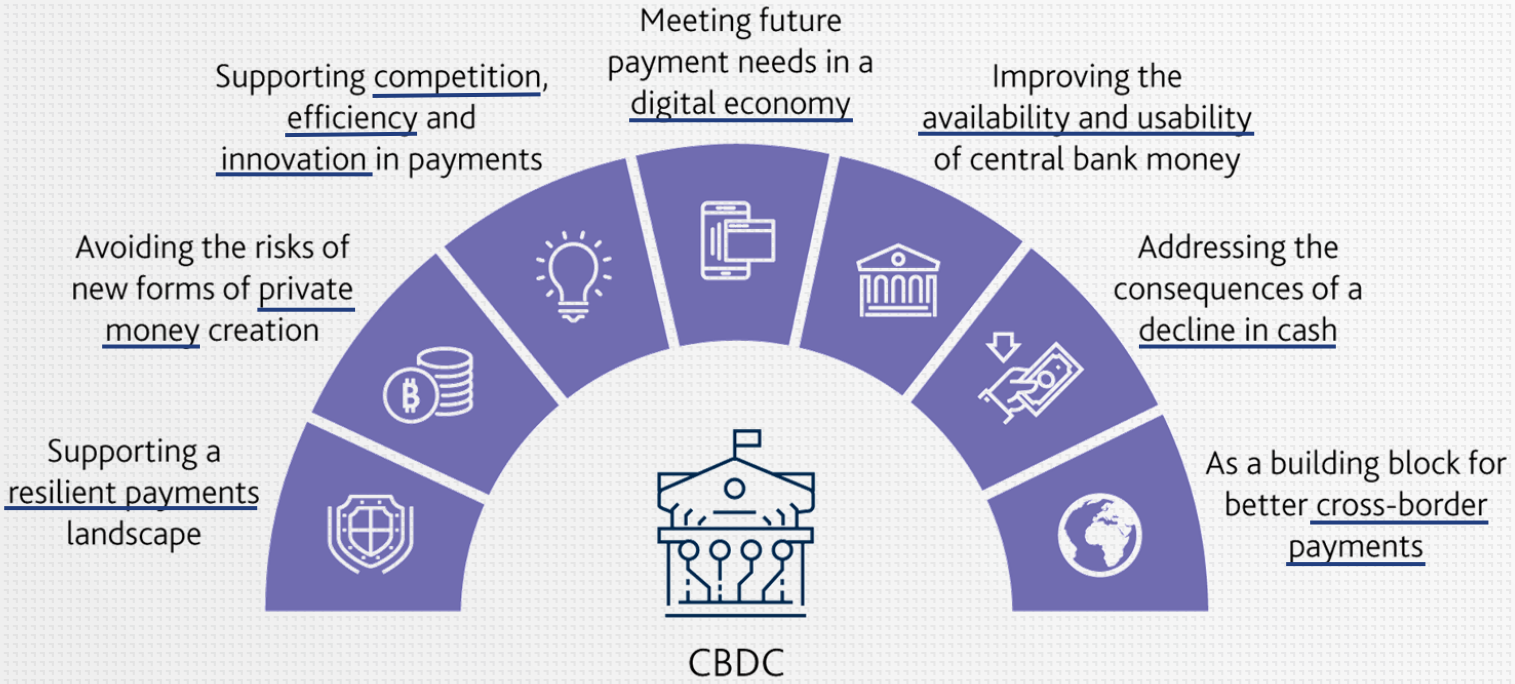
## Reduce fraud

Will eliminate the effects of counterfeiting and forgery

## Traceability

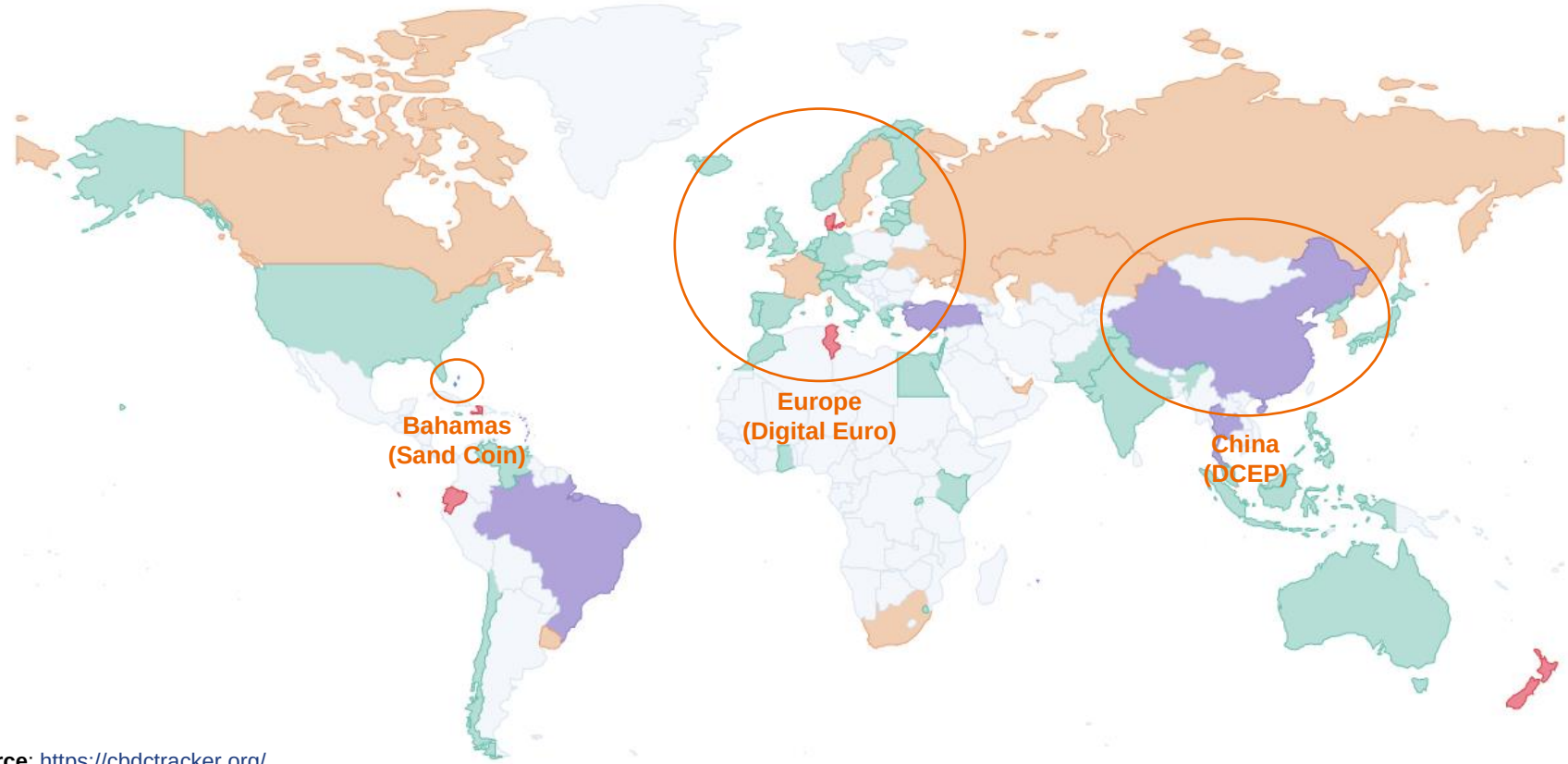
Will enable enhanced tracking and tracing of monies earned by business and individuals for the purposes of tax collection; dissolving of black/ grey market economies; real-time monetary policies…

# Uses & Benefits



## Central Bank Digital Currencies Status

update: March 2021 • News update: Apr, 15 21




**Source**: https://cbdctracker.org/

# Crypto Jargon

DYOR

HODL

ATH

FOMO

JOMO

BEAR

WHALE

# Quiz time!

# How does Blockchain work?

## Deep dive into Blockchain

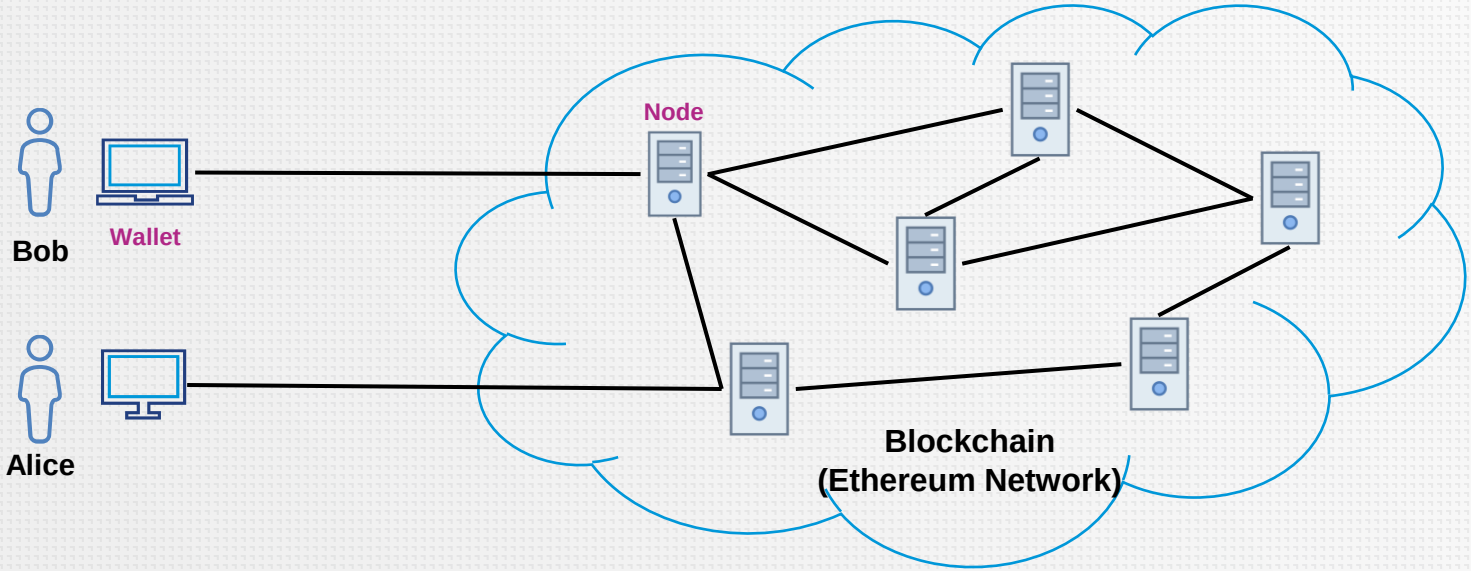
# What is Ethereum

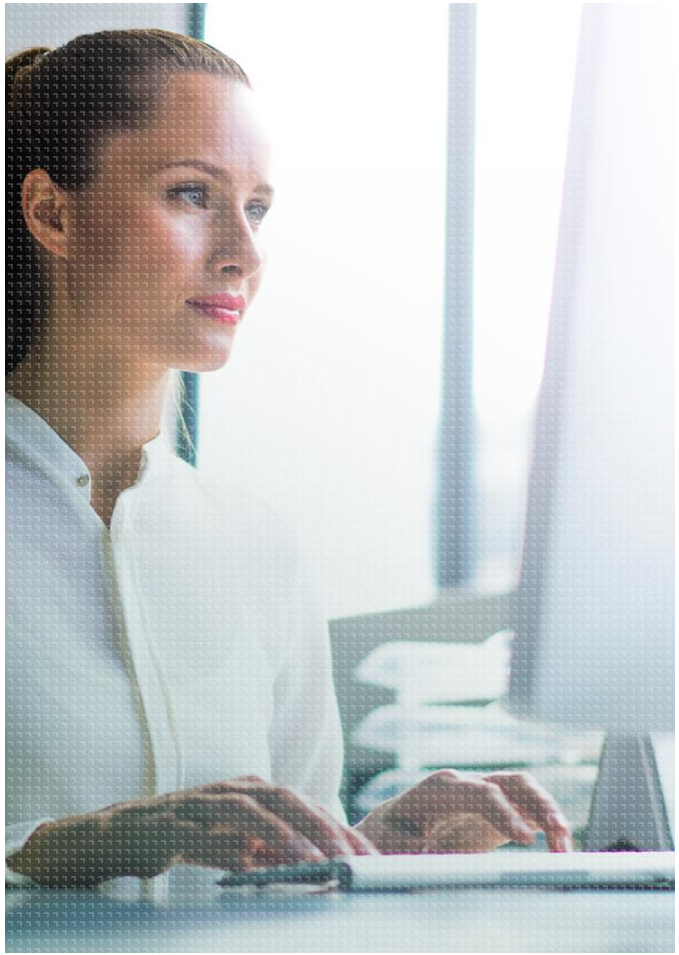
*"Ethereum is an **open-source**, **public**, **blockchain-based** **distributed** computing platform and operating system featuring **smart contract** (scripting) functionality"*

ethereum

# Basic concepts

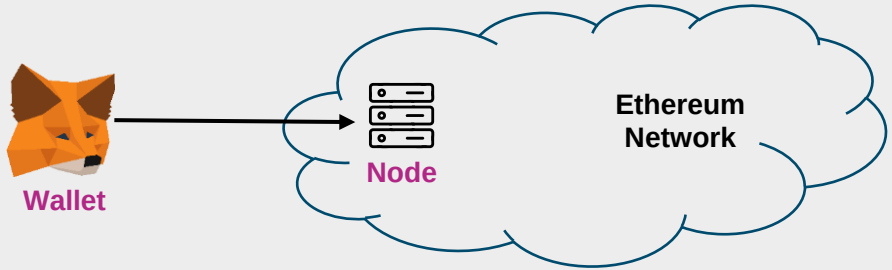
- **Nodes** implement the Ethereum protocol and run on the client side
- **Wallets** hold the users account



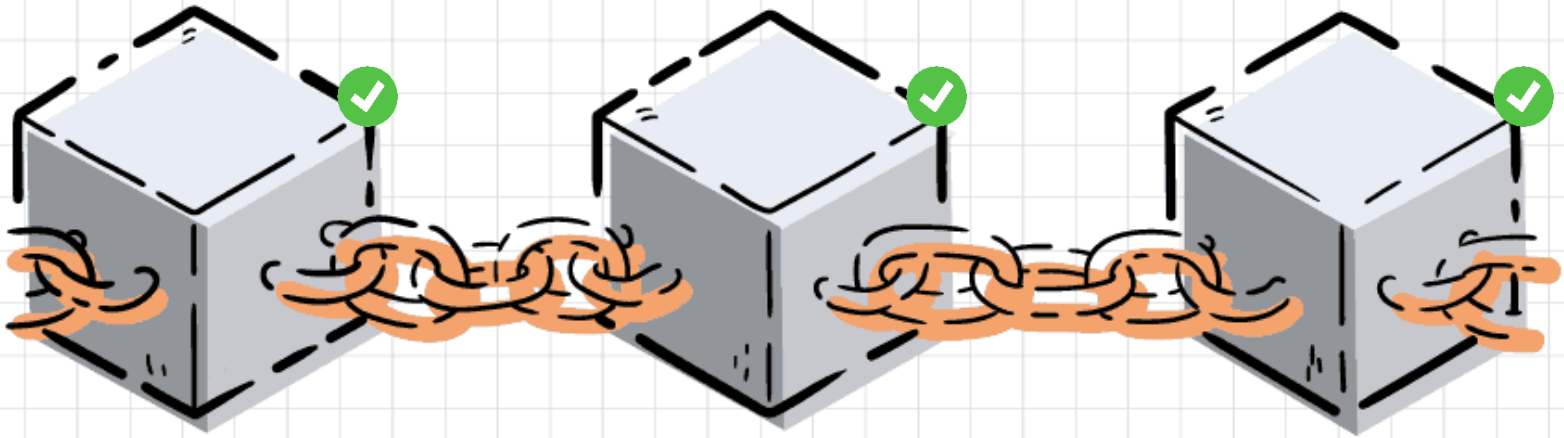


# **Exercise 1:** Setup an Ethereum Wallet

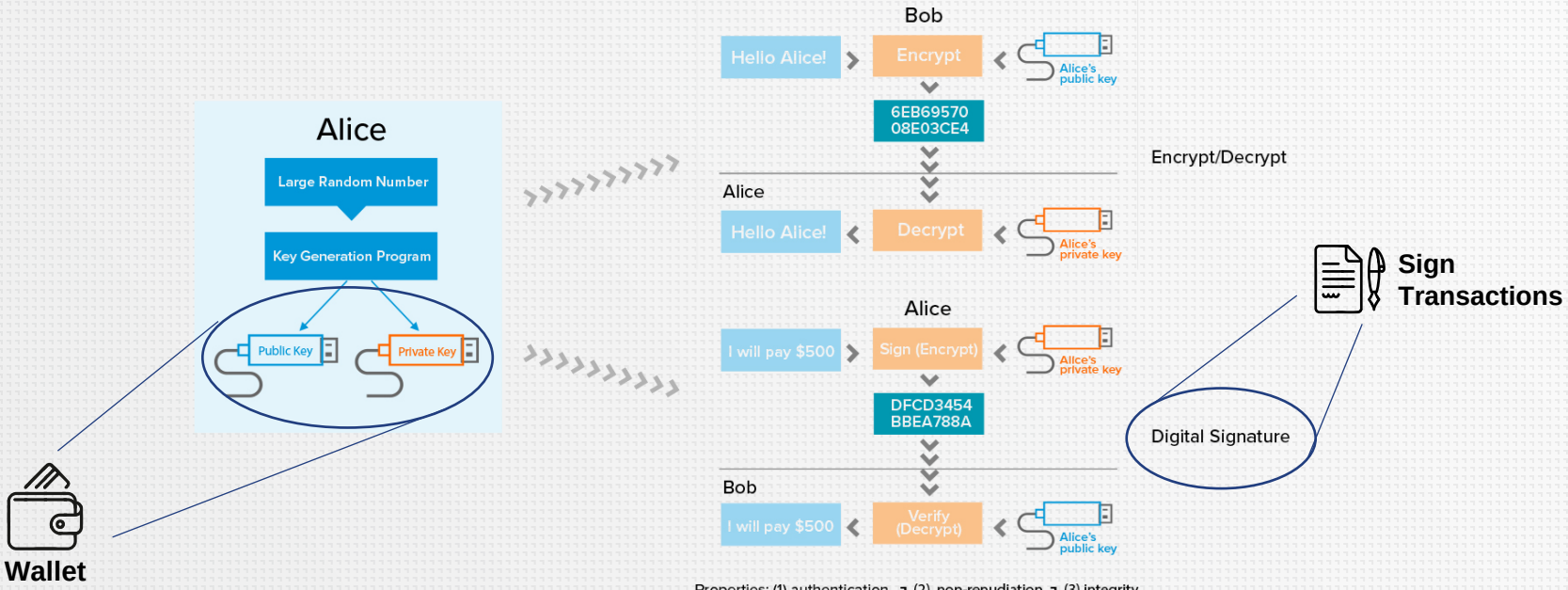
- **Requirement**: Google Chrome or Firefox installed
- Go to **MetaMask** site: https://metamask.io/download.html
- Install the Chrome extension
- Create a new wallet
- Select the “Rinkeby” network (top right)
- Follow the steps in “Rinkeby’s faucet” in order to get some Ether
  - https://www.rinkeby.io/#faucet
  - **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-mda-blockchain

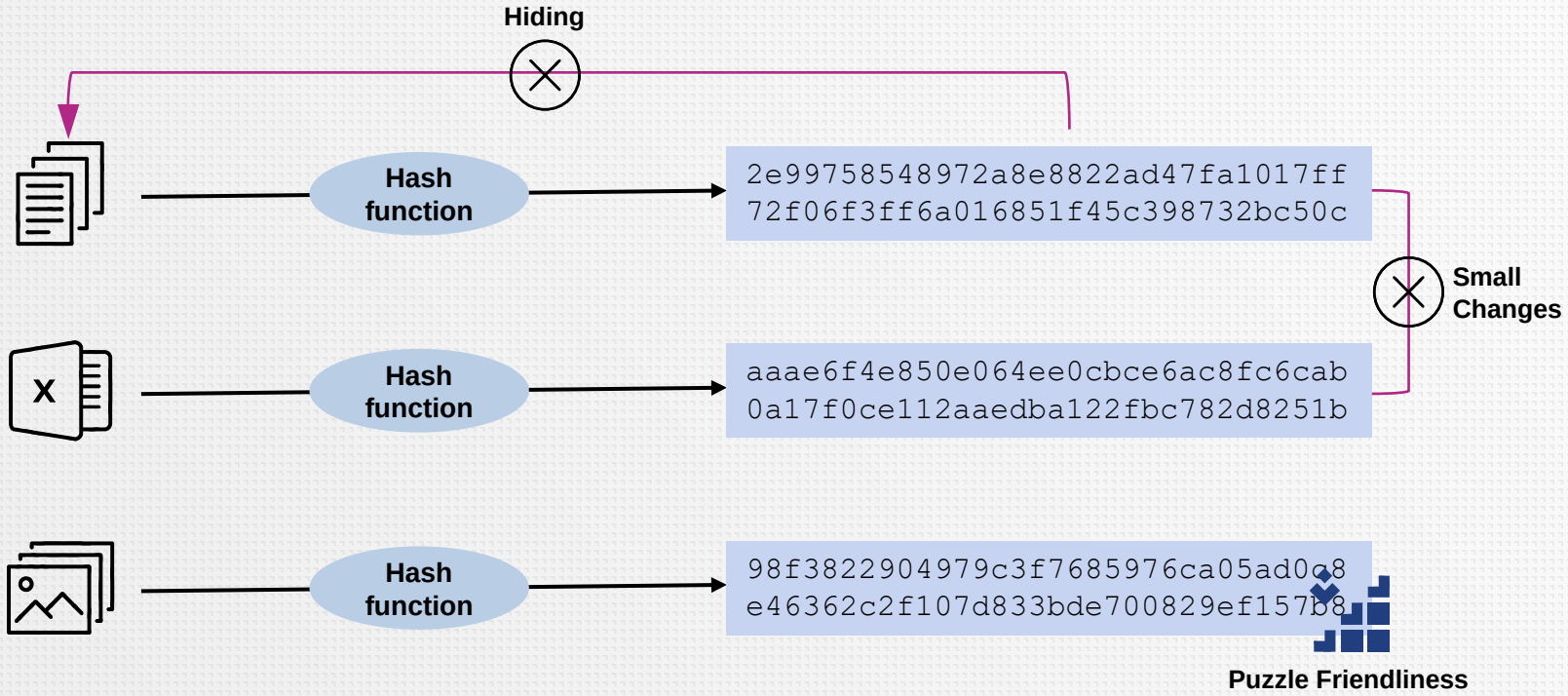


# Some basic concepts – Public Keys

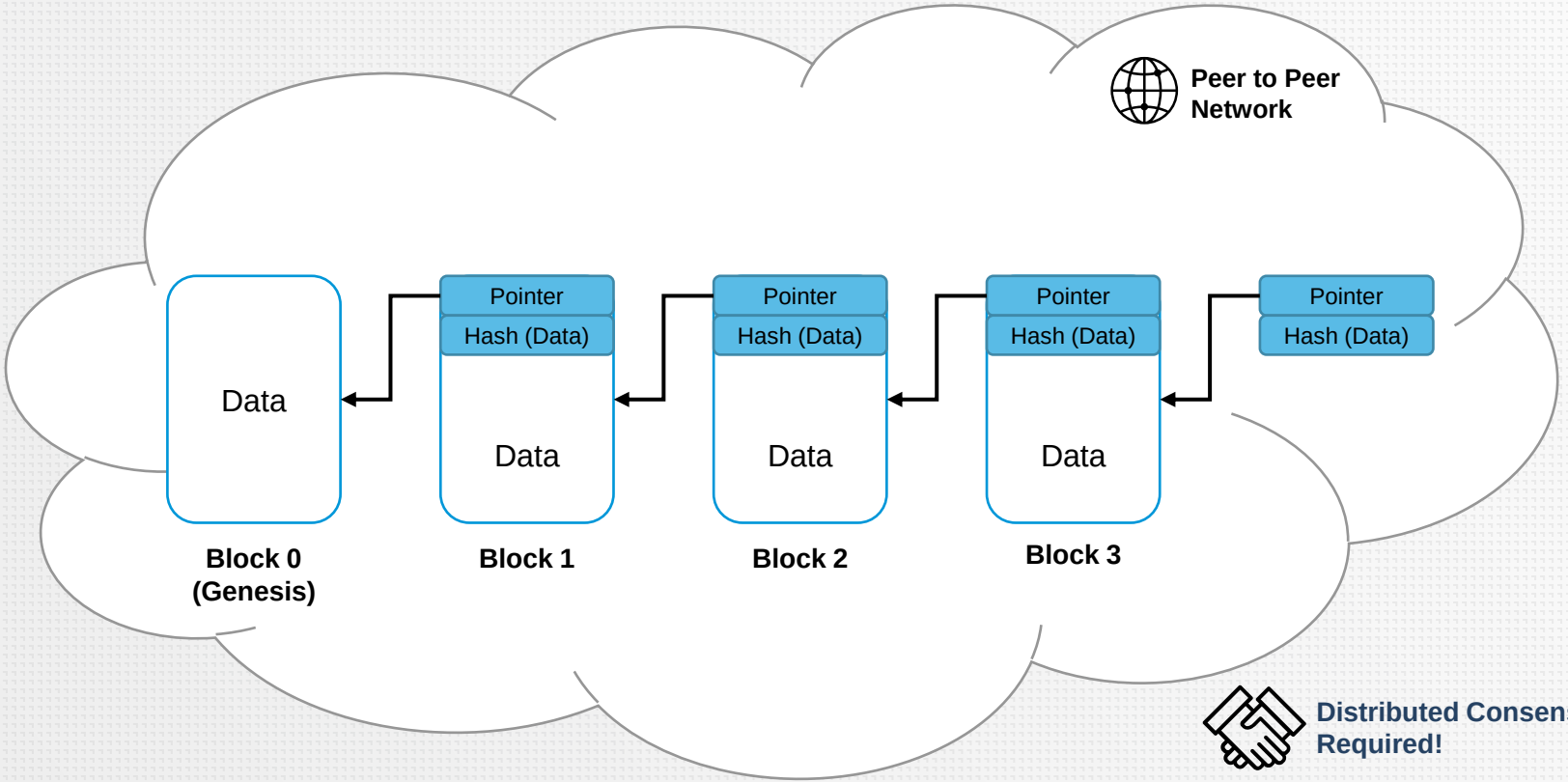


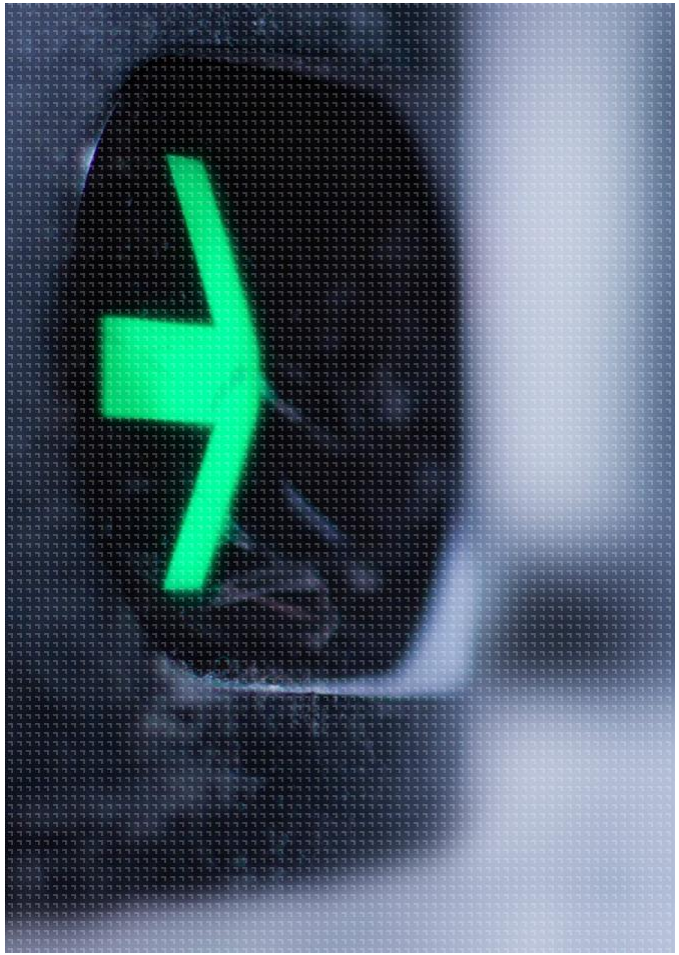

## Public-Key Cryptography (a.k.a. Assymetric Cryptography)

# Some basic concepts – Hash functions



# What is the Blockchain?





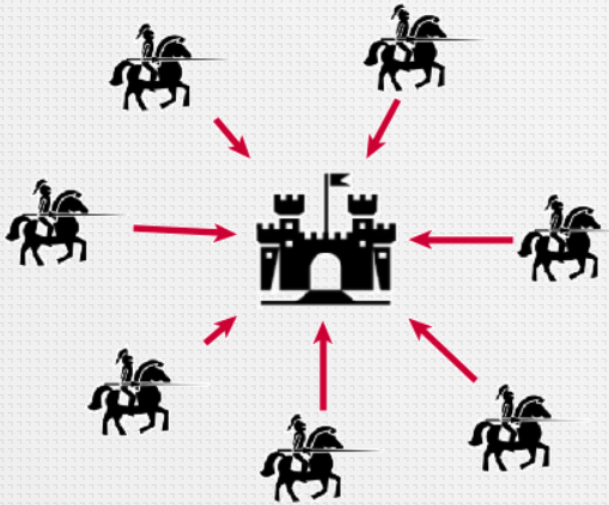
# Distributed consensus

- **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**

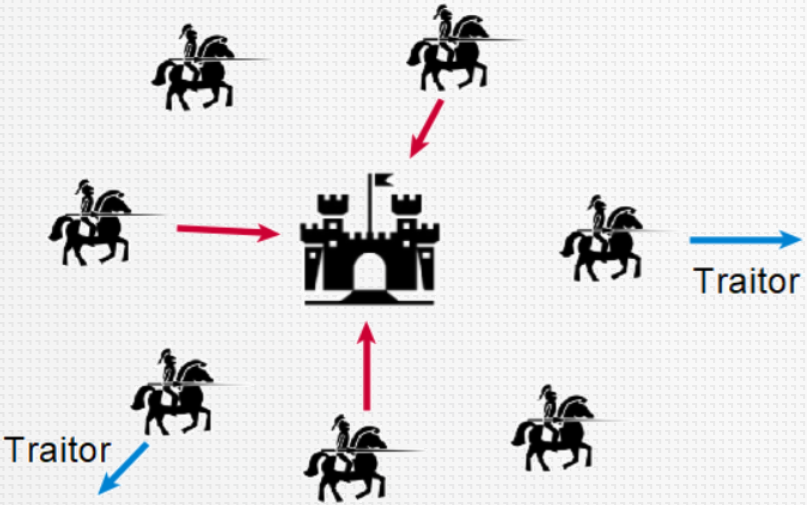
# Byzantines general problem

**Video**: https://www.youtube.com/watch?v=_MwqAaVweJ8

# Byzantine generals problem

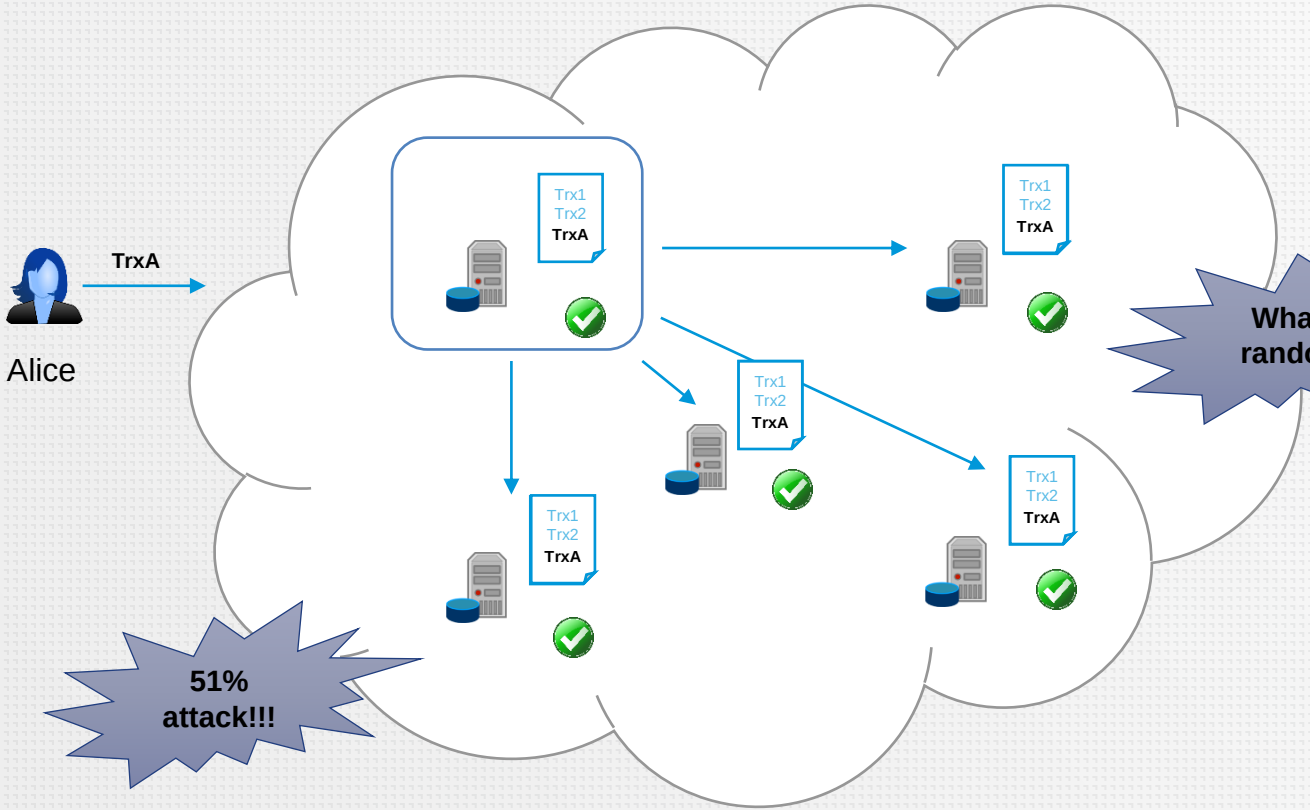


Coordinated attack
leading to victory




Uncoordinated attack
leading to defeat

# Distributed consensus




Alice submits transaction A, which is broadcasted

Each node adds it to its block

e is „randomly“ selected

The node validates its transactions

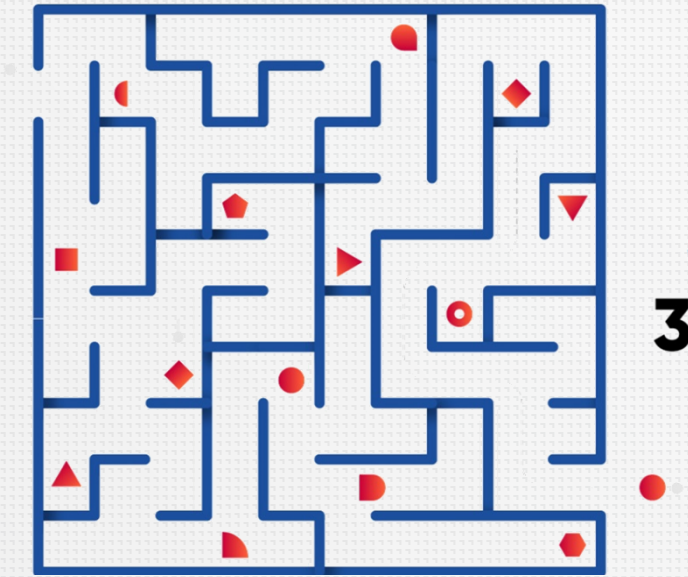
If OK, the block will be broadcasted

The other nodes will validate and include in the Block Chain

# 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**

**Reminder**

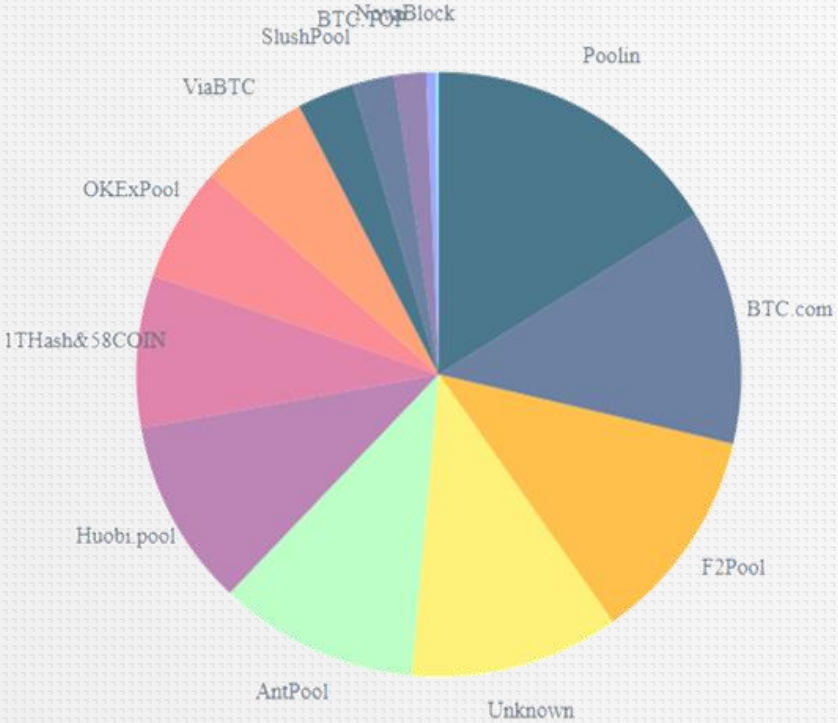
Mega → Giga → Tera → Peta → Exa

**Around 20 EH/s**

**Fugaku** (Top 1 Supercomputer)

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

# Satoshi's nightmare




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

# Consensus algorithms

## Proof of Work

- Bitcoin, Etherum*, 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

# Demo – Sending money with Bitcoin

BLOCKCHAIN


37YdZhA4CVnVHSStFcKSwnfXZTGbciUpfx

1NZt1WyhhyimfuBFWhSYoEAcCtgPn4jUYH

| | | | | | |
|---|---|---|---|---|---|
| Hash | c2c5709689cc2a107234979e1e539c0c1c4f1ddd044c3f309072f86... | | | | 2020-07-27 09:00 |
| | 37YdZhA4CVnVHSStFcKSwnfXZTGbciUpfx | 0.00043444 BTC | → | 1NZt1WyhhyimfuBFWhSYoEAcCtgPn4jUYH | 0.00003807 BTC |
| | | | | 1CKNonLGxwrxrnrVePYEUnimjZr3Zcmy45 | 0.00002637 BTC |
| Comisión | 0.00037000 BTC (147.410 sat/B - 54.653 sat/WU - 251 bytes) | | | | 0.00006444 BTC |

https://www.blockchain.com/btc/block/000000000000000000008a97a6badf545c27592de79a83c343aaab789e5b1c913?page=3

# Bitcoin block details


## Block 632632

| | |
|---|---|
| Hash | 00000000000000000000b069efb51a390724e3f035509d5bf2b93e34760fc0bc0 |
| Confirmaciones | 1 |
| Fecha y Hora | 2020-06-01 19:38 |
| Altura | 632632 |
| Minero | SlushPool |
| Número de transacciones | 2888 |
| Dificultad | 15.138.043.247.082,88 |
| Raíz Merkle | 9f8a109b32859ee932a084d5a82d8f3221df59badec069bc8d3d6c56ddf11a1d |
| Versión | 0×20000000 |
| 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 |
| Remuneración por la comisión | 0.89381915 BTC |

→ **Hash pointer**

→ **Who mined the block (solved the puzzle!!)**

→ **Link to transactions**

→ **Reward (new money!)**

→ **Fees**

# Ethereum block details

Etherscan

Block #10194249

Overview | Comments

| | |
|---|---|
| Block Height: | 10194249 |
| Timestamp: | 22 secs ago (Jun-03-2020 05:39:56 PM +UTC) |
| Transactions: | 149 transactions and 33 contract internal transactions in this block |
| Mined by: | 0x84a0d77c693adabe0ebc48f88b3ffff010577051 in 19 secs |
| Block Reward: | 2.245068484316597582 Ether (2 + 0.245068484316597582) |
| Uncles Reward: | 0 |
| Difficulty: | 2,361,189,893,362,840 |
| Total Difficulty: | 15,717,023,273,021,800,529,449 |
| Size: | 26,377 bytes |
| Gas Used: | 9,906,253 (99.79%) |
| Gas Limit: | 9,927,010 |
| Extra Data: | 01090d/geth/go1.14.2/linux (Hex:0xd88301090d846765746888676f312e31342e32856c696e7578) |

Click to see more

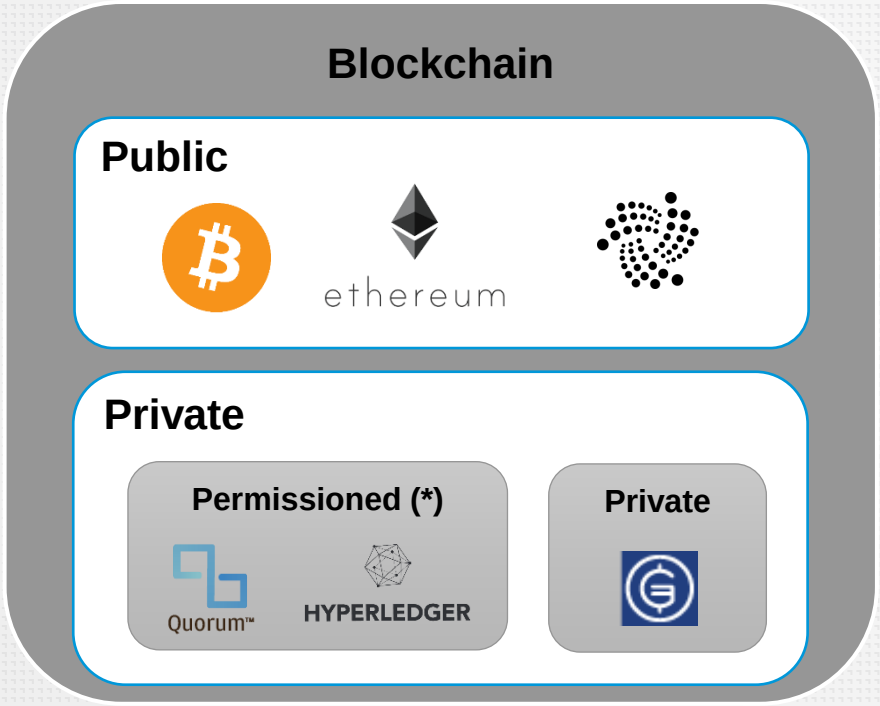
→ **Link to transactions (and contract execs)**

→ **Who mined the block (solved the puzzle!!)**

→ **Reward (new money!)**

→ **Cost (kind of like fees)**

# 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

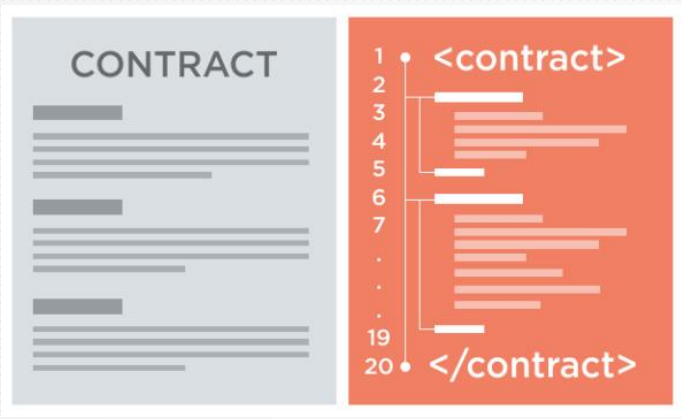
# Smart Contracts

# Differences between Bitcoin and Ethereum

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

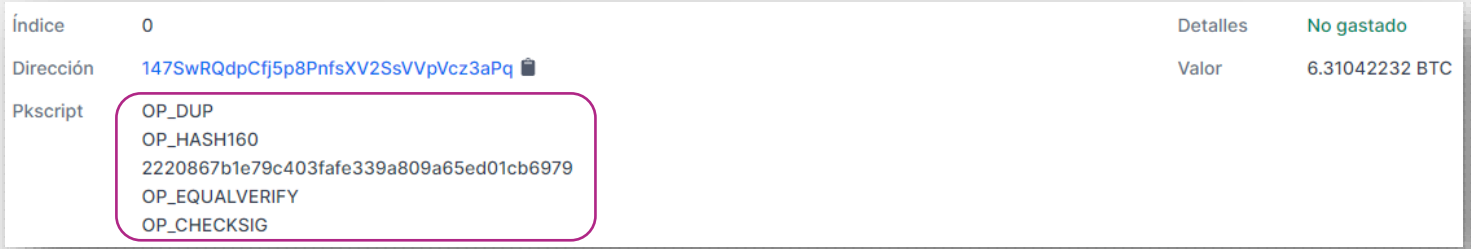
# Smart Contracts

*“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!!



# **Anatomy of a Smart Contract** (Solidity)

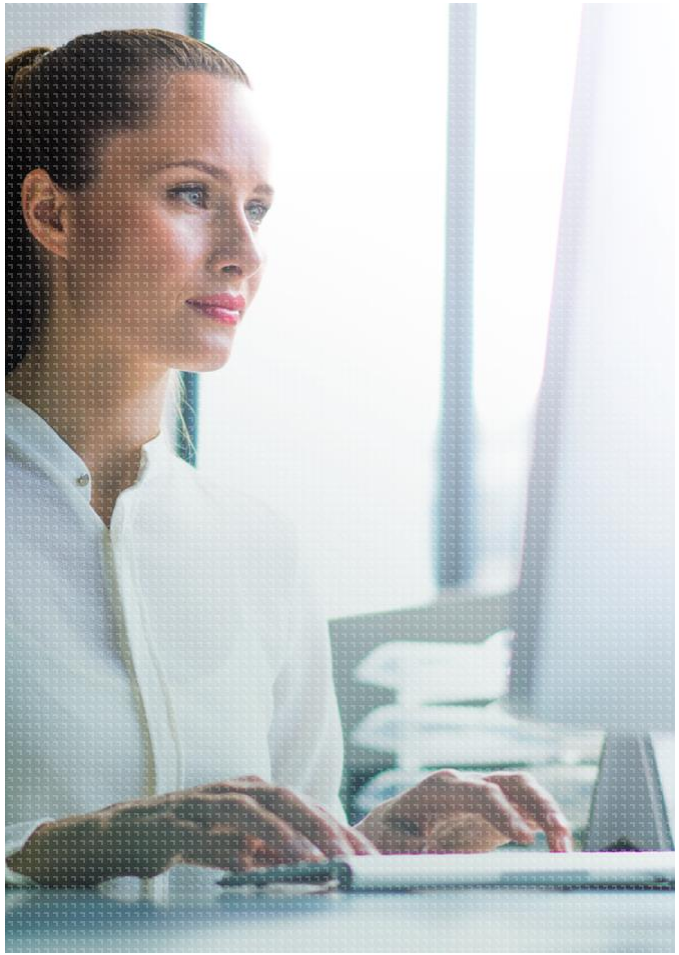
Solidity version

Contract definition

```
pragma solidity ^0.4.0;

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

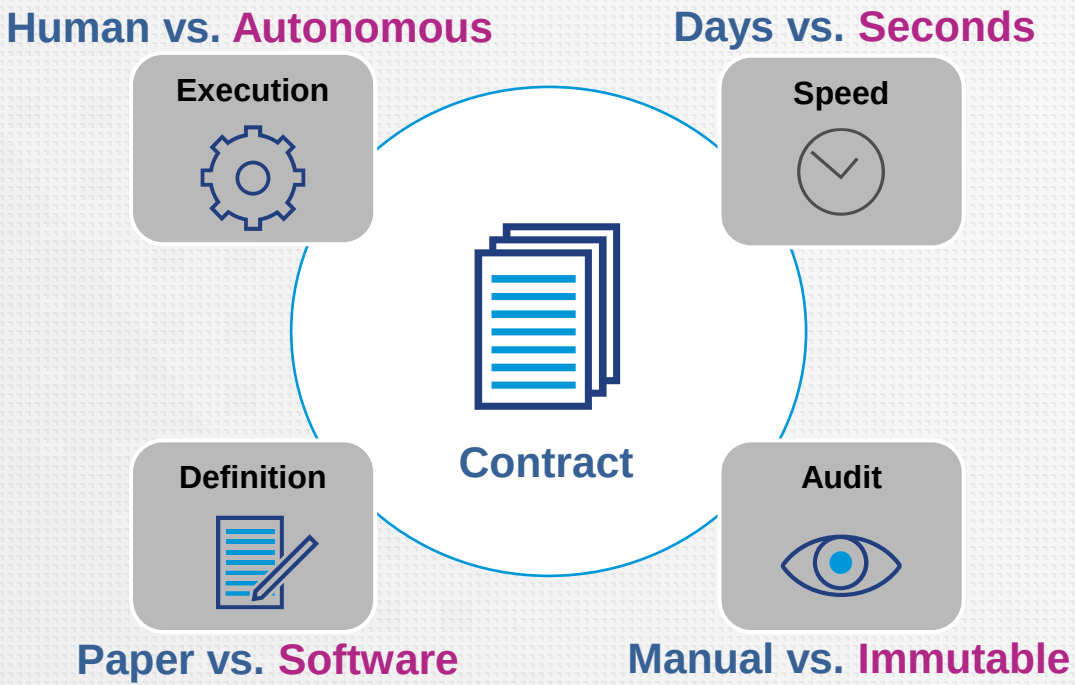
In this exercise we will **interact with an existing Smart Contract** in Ethereum (Rinkeby test network).

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

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

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

# Traditional vs Smart Contracts



# Smart Contract Benefits

## ACCURACY

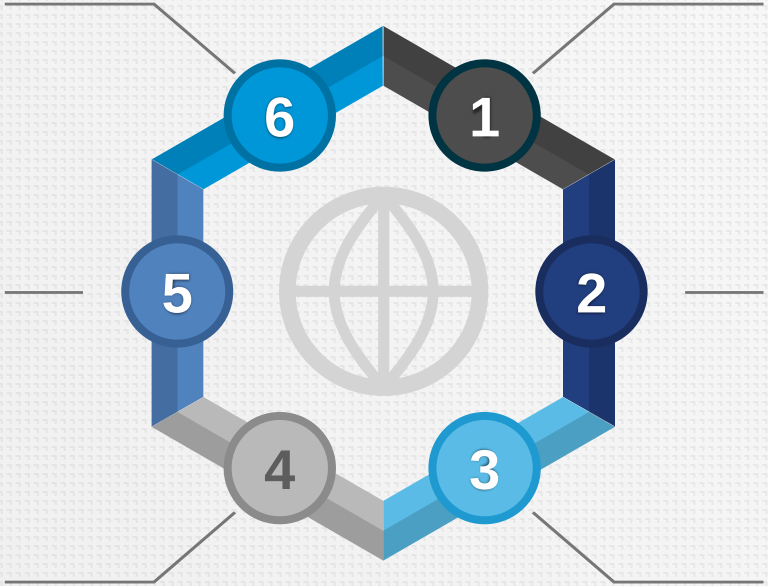
Not prone to human error.

## SPEED

Compared to legal contracts.

## SAVINGS

By removing intermediaries.




## AUTONOMY

No third parties or extra steps required.

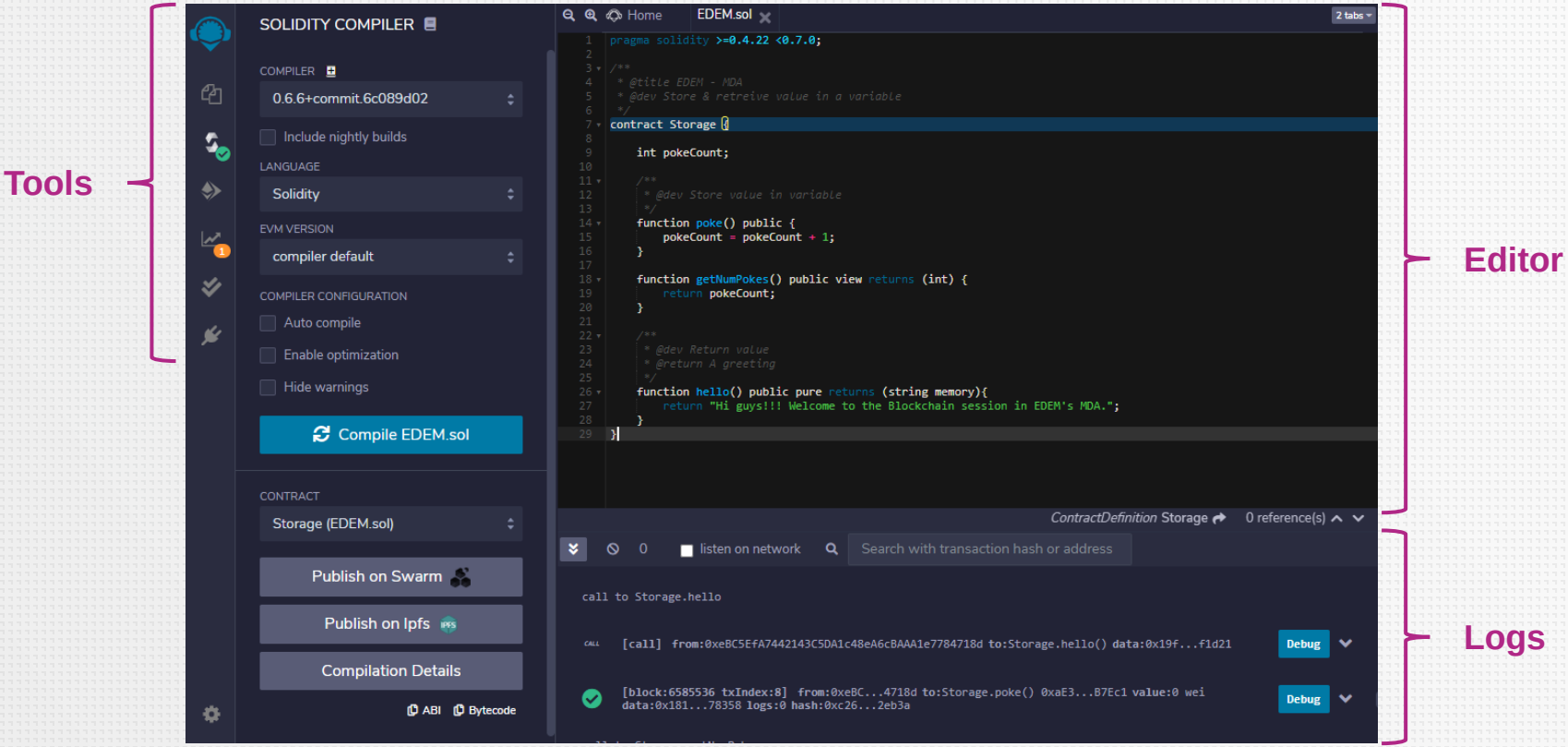
## TRUST & SAFETY

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

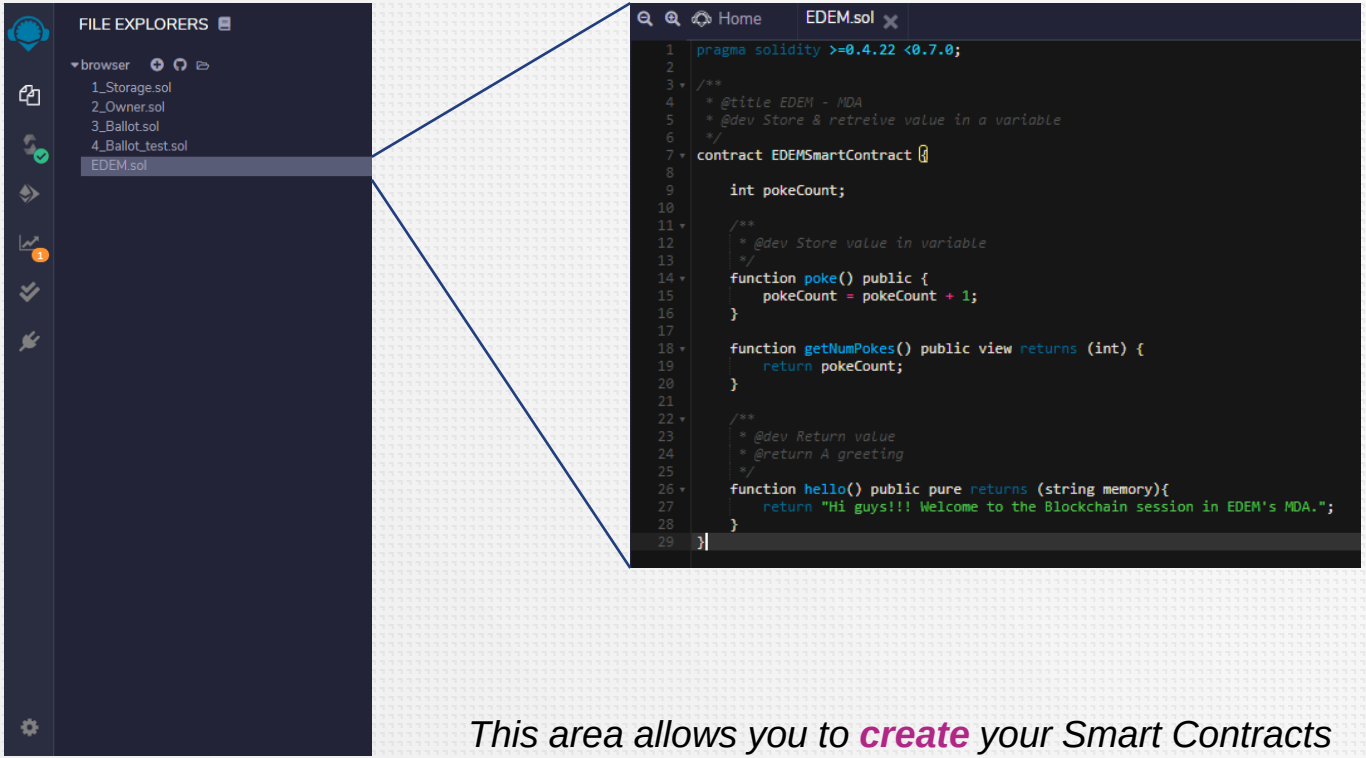
## BACK-UPS

Data is replicated in all nodes.

# Smart Contract Development – Remix

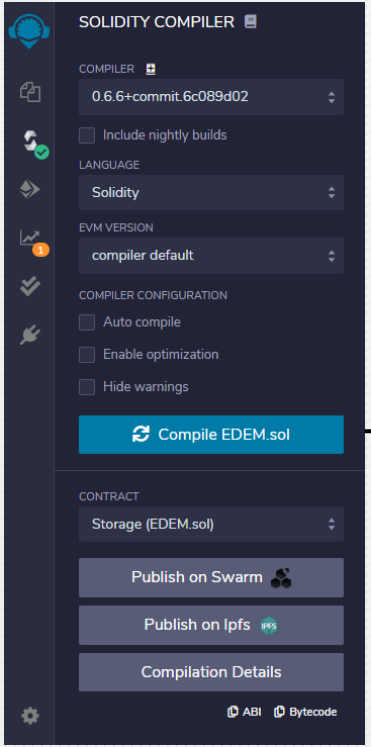


# Remix – Editor




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

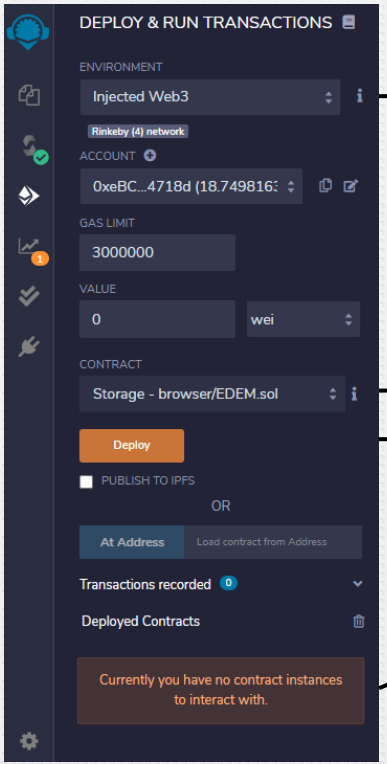
# Remix – Compiler




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:

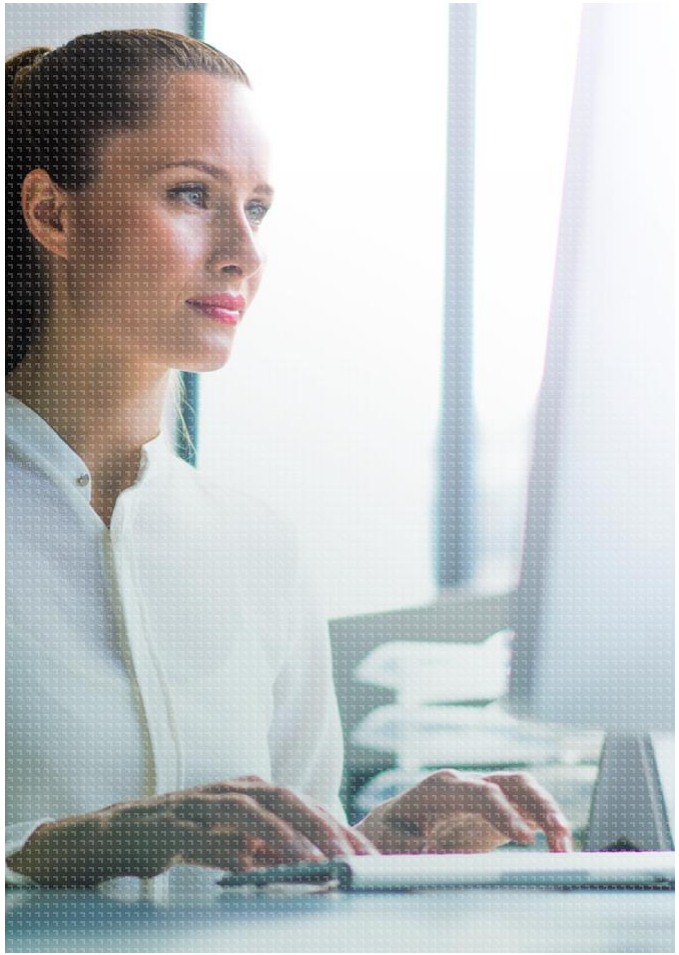
- **JavaScript VM**: run in your browser
- **Injected Web3**: run in the network using MetaMask
- **Web3 Provider**: run directly against a node (local or remote)

Smart Contract you want to run/deploy

Click to deploy!!

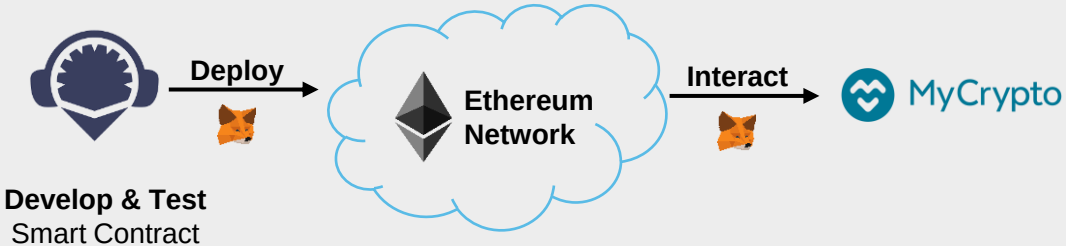
This is where you will test you Smart Contract functions

*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

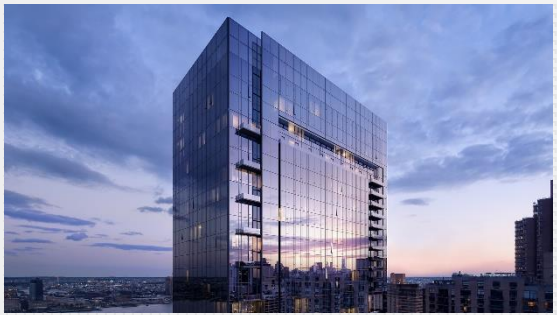
# Quiz time!

# 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

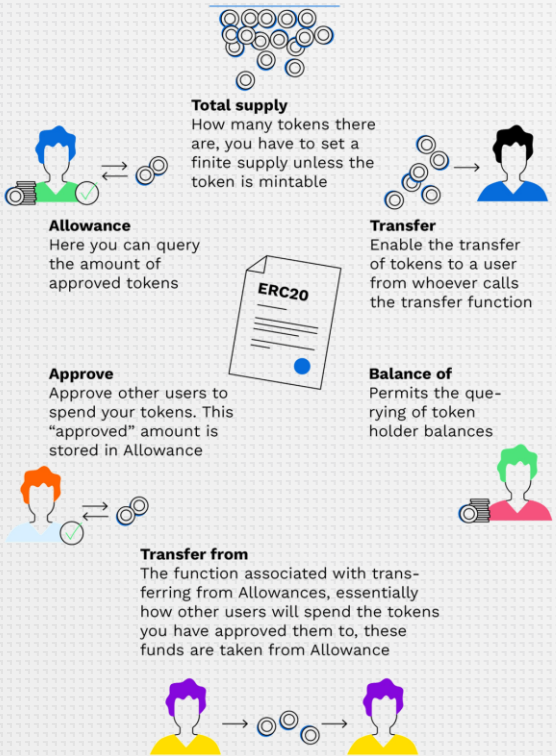
# Token Standards


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

# ERC token examples

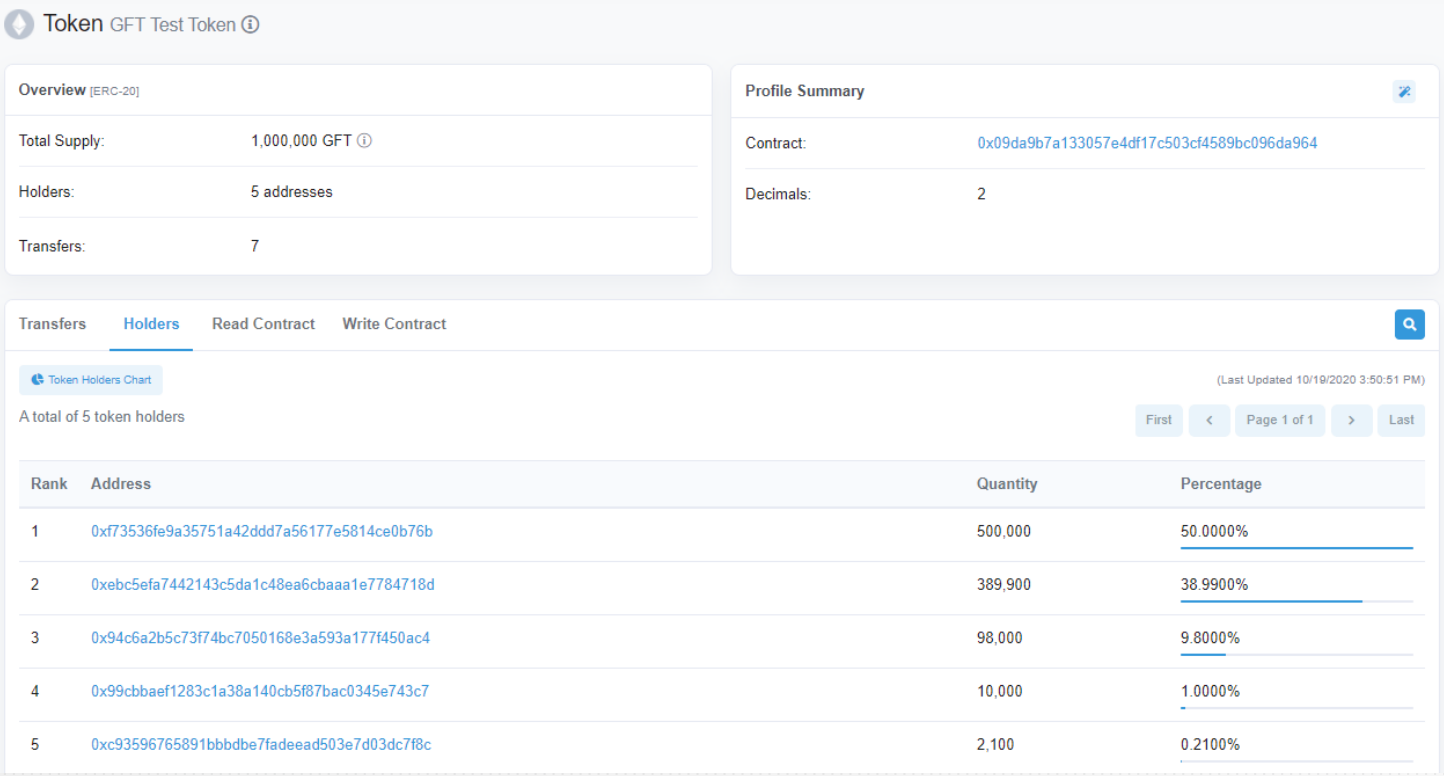
| Standard | ERC-20 compatible | Description |
|---|---|---|
| **ERC-20** | Yes | Simplest use of **fungible tokens**. Most common standard. |
| **ERC-223** | Yes | ERC-20 compatible. Adds functions to prevent accidentally sending of tokens to contract addresses. |
| **ERC-721** | No | Describes how to construct **non-fungible tokens**, unique tokens or collectibles. |
| **ERC-1155** | No | Interface for contracts that manage **multiple token** types (fungible, non-fungible and partially fungible). |
| **ERC-1400** | Yes | Library of standards for **security tokens** on Ethereum: Partially fungible (ERC-1410), core security token (ERC-1594), document and legend (ERC-1643), controller (ERC-1644), etc. |

# ERC-20: Fungible Token




```
function name() public view returns (string)
function symbol() public view returns (string)
function decimals() public view returns (uint8)
function totalSupply() public view returns (uint256)
function balanceOf(address _owner) public view returns (uint256 balance)
function transfer(address _to, uint256 _value) public returns (bool
success)
function transferFrom(address _from, address _to, uint256 _value) public
returns (bool success)
function approve(address _spender, uint256 _value) public returns (bool
success)
function allowance(address _owner, address _spender) public view returns
(uint256 remaining)
```

# 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

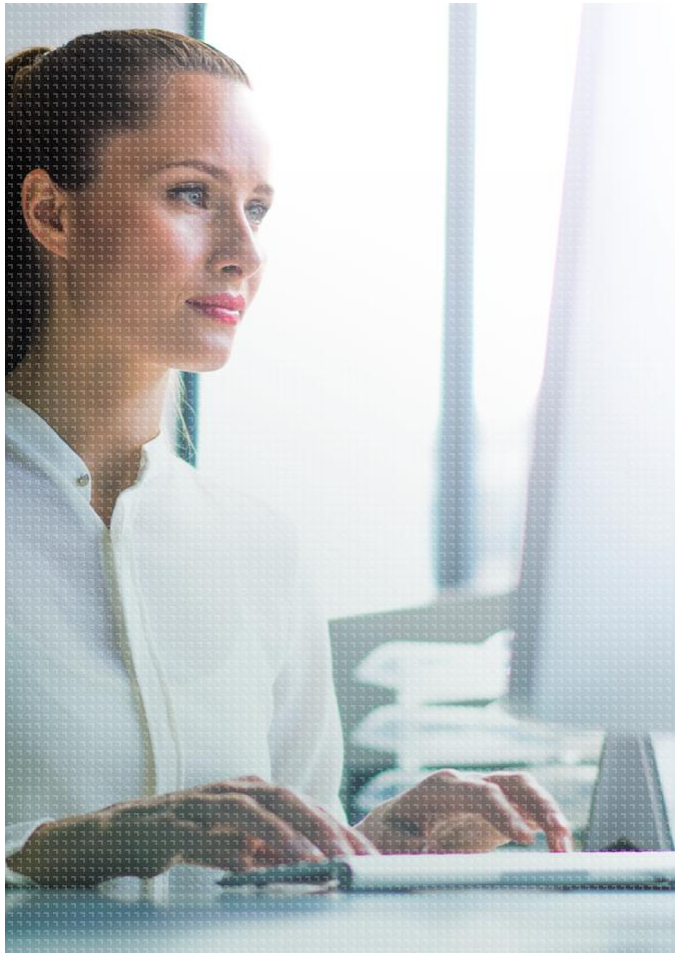
First | Page 1 of 1 | Last

| Rank | Address | Quantity | Percentage |
|---|---|---|---|
| 1 | 0xf73536fe9a35751a42ddd7a56177e5814ce0b76b | 500,000 | 50.0000% |
| 2 | 0xebc5efa7442143c5da1c48ea6cbaaa1e7784718d | 389,900 | 38.9900% |
| 3 | 0x94c6a2b5c73f74bc7050168e3a593a177f450ac4 | 98,000 | 9.8000% |
| 4 | 0x99cbbaef1283c1a38a140cb5f87bac0345e743c7 | 10,000 | 1.0000% |
| 5 | 0xc93596765891bbbdbe7fadeead503e7d03dc7f8c | 2,100 | 0.2100% |

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

# ERC-20 Tokens

| # | Token | Price | Change (%) | Volume (24H) | Market Cap | Holders |
|---|---|---|---|---|---|---|
| 1 | Tether USD (USDT)<br>Tether gives you the joint benefits of open blockchain technology and traditional currency by converting your cash into a stable digital currency equivalent. | $0.9968<br>0.000721 Eth | ▲ 0.08% | $89,135,255,288 | $26,262,939,279 | 2,373,040<br>▲ 0.313% |
| 2 | ChainLink Token (LINK)<br>A blockchain-based middleware, acting as a bridge between cryptocurrency smart contracts, data feeds, APIs and traditional bank account payments. | $23.4900<br>0.017002 Eth | ▲ 2.74% | $1,837,248,561 | $9,508,023,656 | 380,511<br>▲ 0.661% |
| 3 | BNB (BNB)<br>Binance aims to build a world-class crypto exchange, powering the future of crypto finance. | $44.8000<br>0.032426 Eth | ▲ 6.11% | $614,291,440 | $6,653,569,428 | 314,966<br>▲ 0.002% |
| 4 | USD Coin (USDC)<br>USDC is a fully collateralized US Dollar stablecoin developed by CENTRE, the open source project with Circle being the first of several forthcoming issuers. | $0.9961<br>0.000721 Eth | ▼ -0.33% | $1,475,528,470 | $5,824,310,808 | 606,527<br>▲ 0.398% |
| 5 | Uniswap (UNI)<br>UNI token served as governance token for Uniswap protocol with 1 billion UNI have been minted at genesis. 60% of the UNI genesis supply is allocated to Uniswap community members and remaining for team, investors and advisors. | $18.6100<br>0.013470 Eth | ▲ 24.81% | $1,904,130,093 | $5,282,951,237 | 137,591<br>▲ 1.459% |
| 6 | Wrapped BTC (WBTC)<br>Wrapped Bitcoin (WBTC) is an ERC20 token backed 1:1 with Bitcoin. Completely transparent. 100% verifiable. Community led. | $34,266.0000<br>24.801859 Eth | ▼ -0.93% | $319,335,479 | $3,995,763,171 | 24,799<br>▲ 0.089% |
| 7 | Synthetix Network Token (SNX)<br>The Synthetix Network Token (SNX) is the native token of Synthetix, a synthetic asset (Synth) issuance protocol built on Ethereum. The SNX token is used as collateral to issue Synths, ERC-20 tokens that track the price of assets like Gold, Silver, Oil and Bitcoin. | $18.0700<br>0.013079 Eth | ▲ 9.12% | $248,569,578 | $2,585,198,296 | 55,939<br>▲ 1.144% |



# **Exercise 4:** Adding tokens to your wallet

- We will be adding the following tokens to the MetaMask wallet:
  - Tether USD
  - GFT Test Token

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

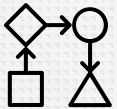
# Tokenization benefits

**Decentralized ownership**
no borders/barriers

**No middlemen**
Cost-effective

**Greater liquidity**

Frictionless **transfer of ownership**



**Traceability**
Immutable & transparent

**Fungible & non-fungibles**

# 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

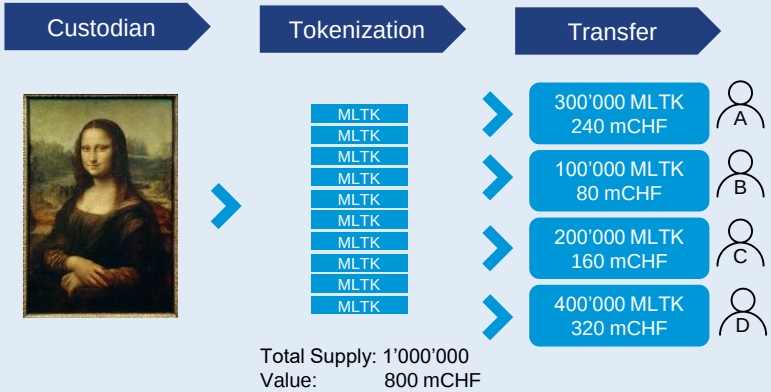
## Cons

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

# Tokenizing Green Bonds – Project Genesis


**Video**: https://www.youtube.com/watch?v=9XMN_2oq2a8

# Asset Tokenization for a Private Wealth Bank



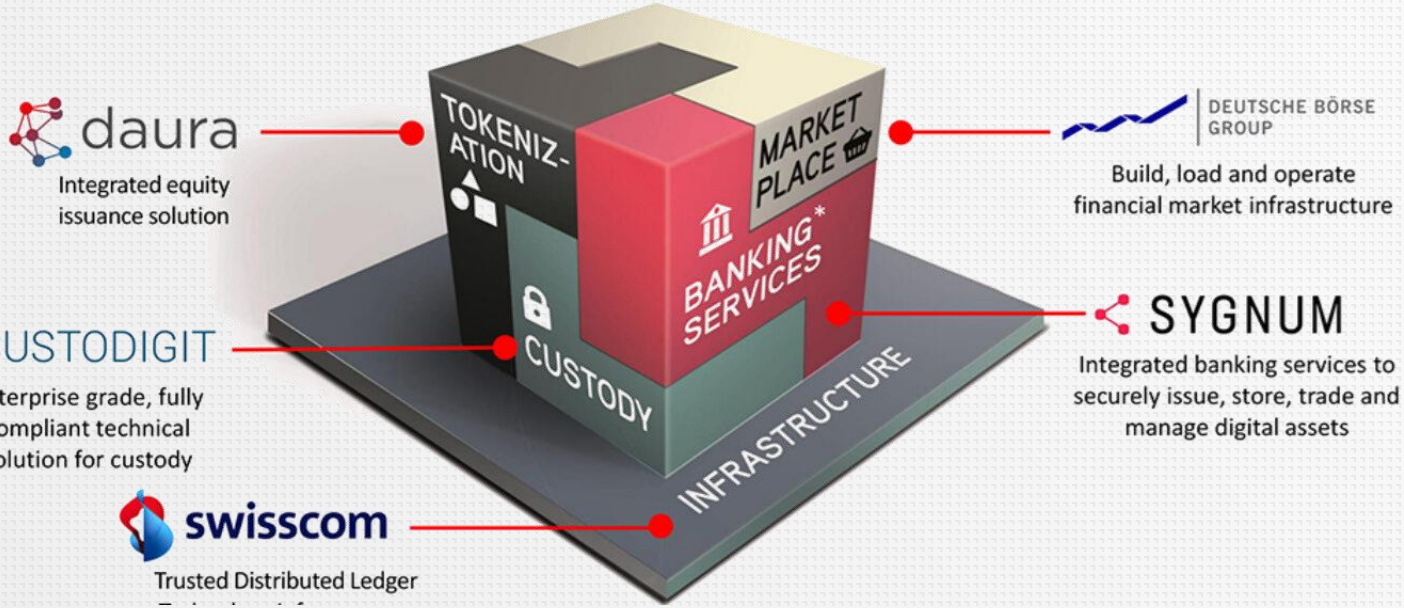

## Goals

- 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:

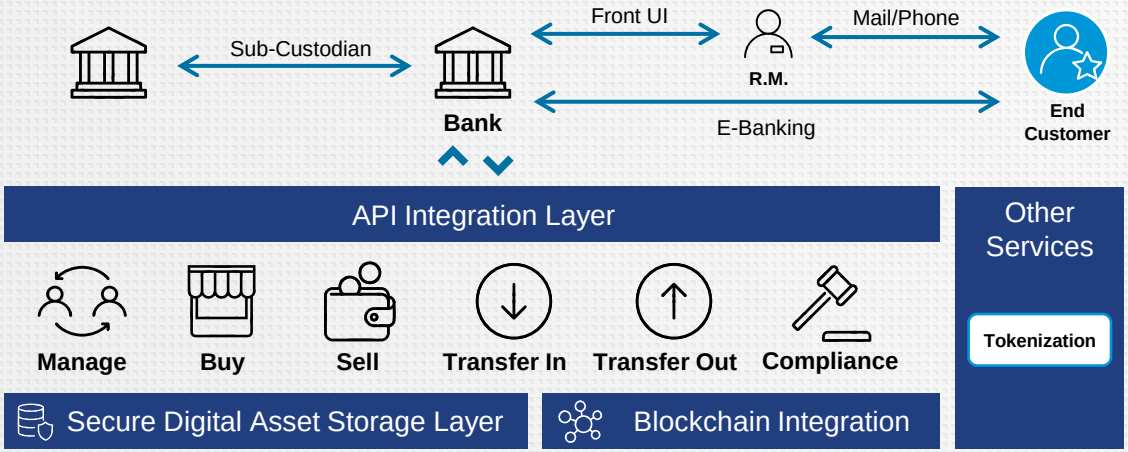
- Tokenization of utilities and non-liquid objects
- Tokenization of inherited objects (work of art, real estates, etc.) and distribute among the heirs
- Quickly set up and transfer (private equity) investment funds

# 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.



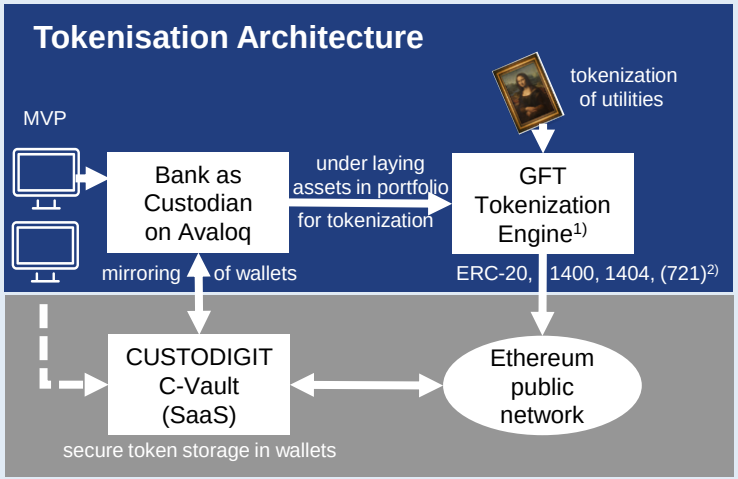
# Summary Tokenization solution

## 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, Goldman Sachs

**“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, IBM

# Key steps in evolution of Blockchain for finance

## Blockchain

Value store and transactions

## Smart Contracts

Programability, tokenisation

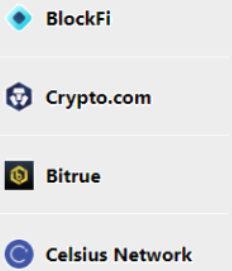
## Altcoins, Tokens ICOs


Experiment with investing, trading

## Stablecoins

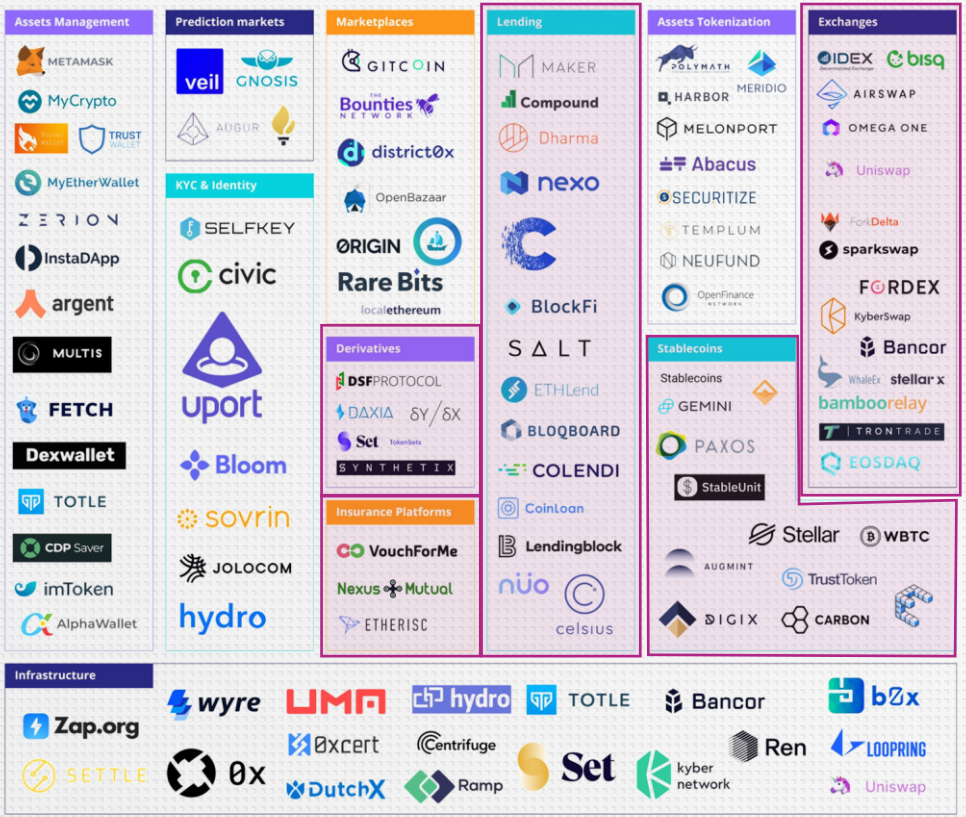

Crypto with money-like attributes

## Decentralised Finance




Borrowing, lending & other services

# DeFi landscape today




**Source**: https://defiprime.com/


# Stablecoins

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

libra

tether

PAXOS


# 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

δY/δX

UMA

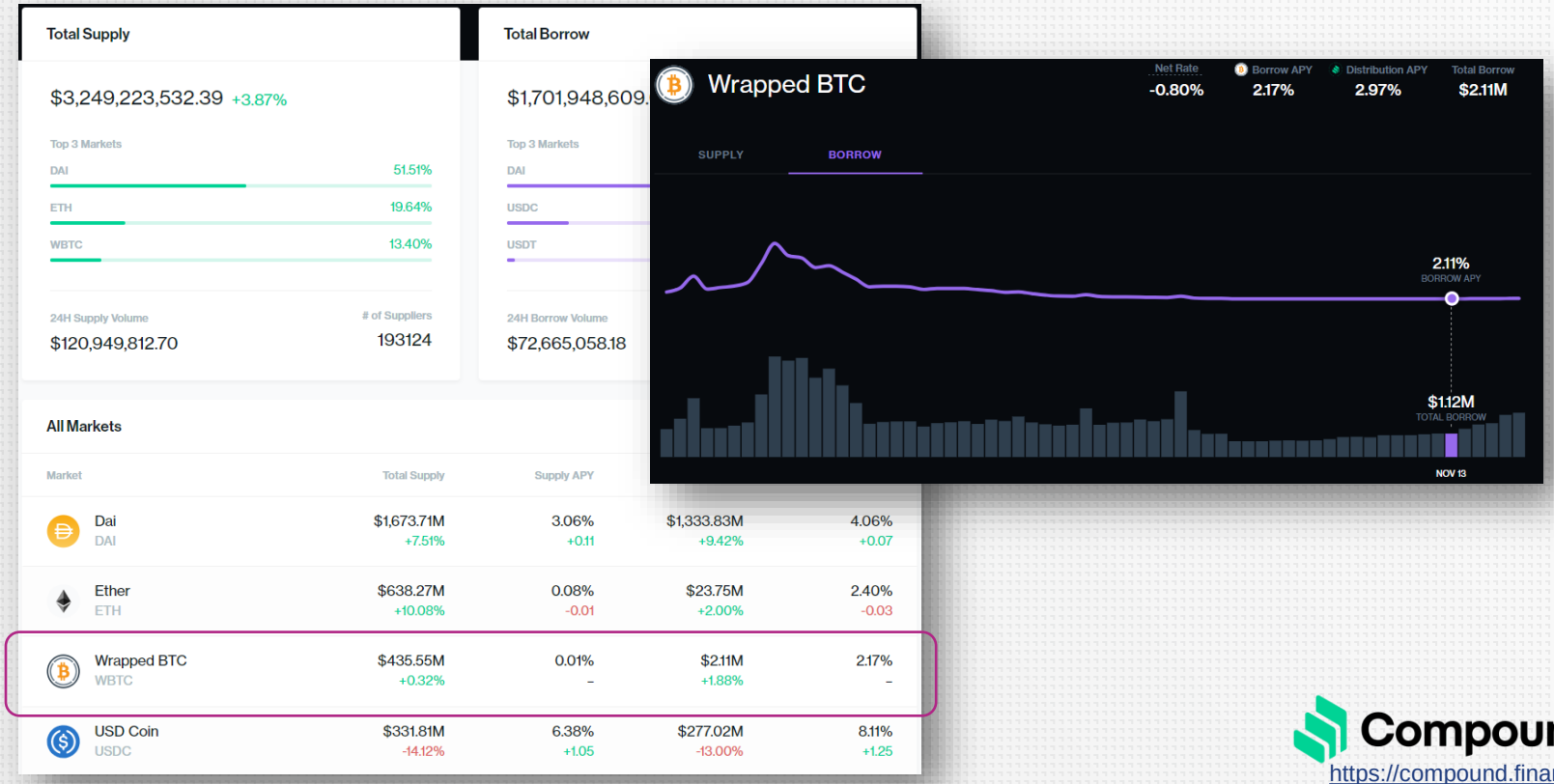

# Insurance

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

Nexus Mutual

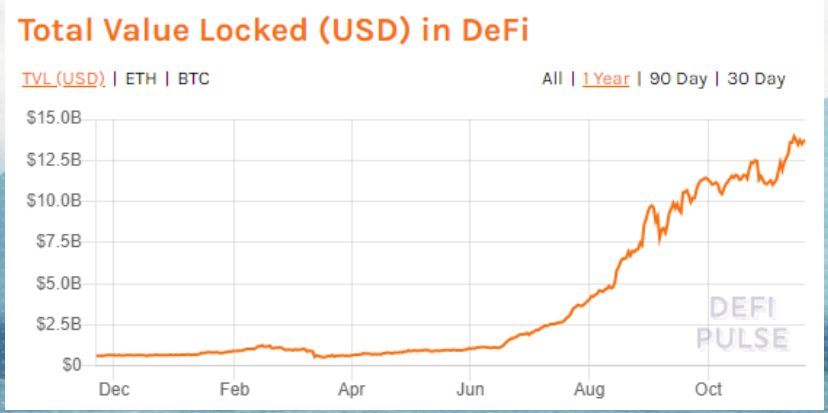
opyn

# Lending & Borrowing




Compound

https://compound.finance/




**Source**: https://defipulse.com/

**COMBINE DEFI**

**INTEROPERABILITY**

**PROGRAMABLE MONEY**

# Possibilities are endless!!!

# Benefits & Use Cases

# Security

## NON-REPUDIATION

By the use of digital signatures, the system validates the users are who they claim they are. Each transaction is signed by the end-user.

## “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 pseudonimity.

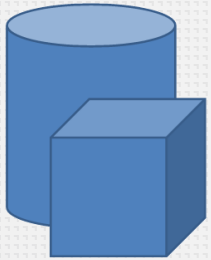
## NO TAMPERING

Uses cryptographic methods (such as hash pointers or merkle trees) in order to avoid tampering of the distributed ledger. Any change in any part of the blockchain would “break” it.

## AUDIT

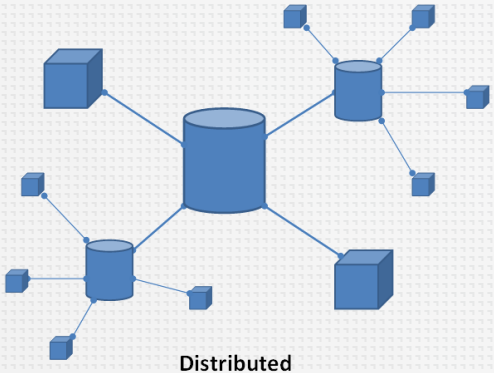
Given that all data is public and there is no possibility of data tampering, it can be considered as an auditable public ledger.

# Decentralization



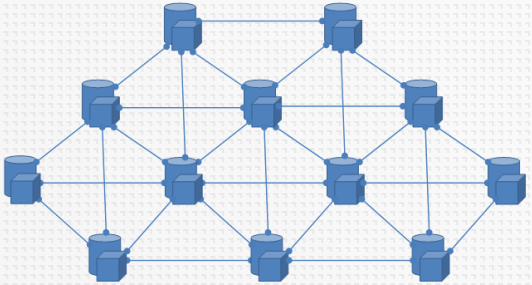
**Centralized**

*one node does everything*



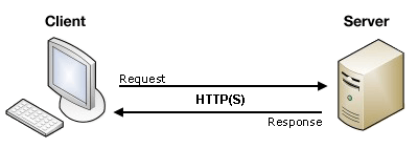
**Distributed**

*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

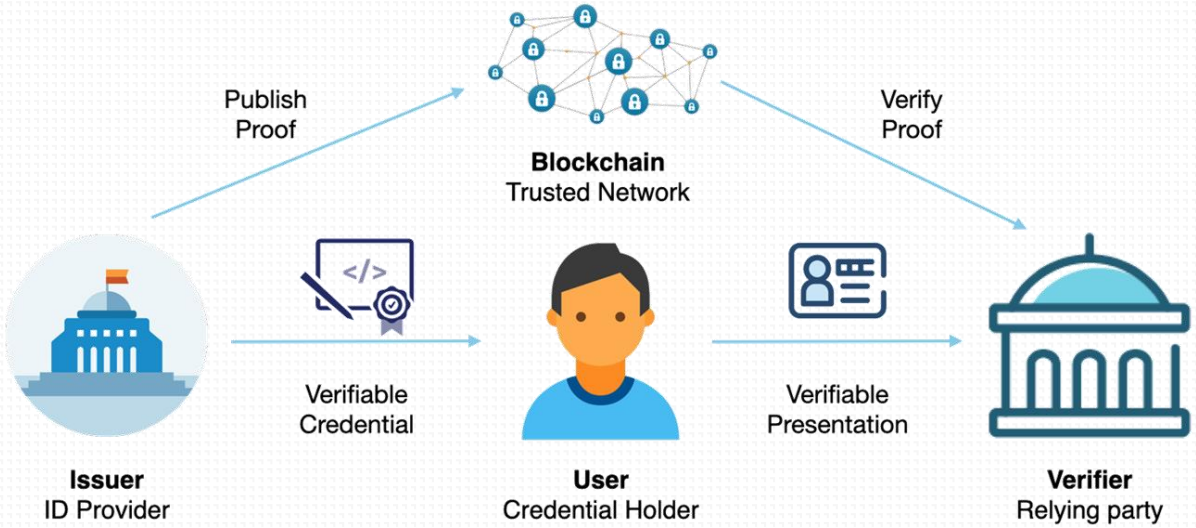
Parties want to automate agreements and transactions using 'smart contracts'

## Disintermediation

Remove intermediaries which produce none or little value in the chain

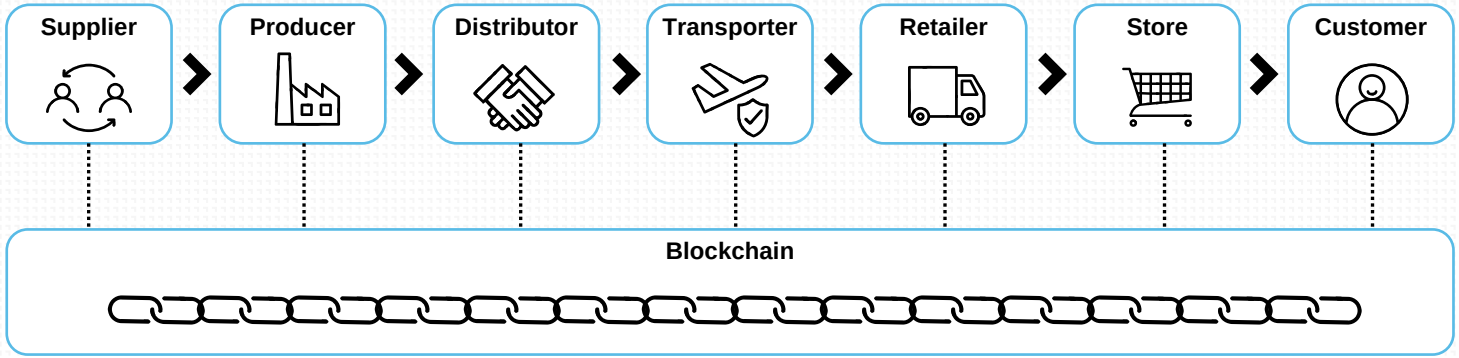
# Casos de uso – Identidad Soberana

- La identidad soberana es una **forma de identidad digital** en la que el usuario tiene **pleno control de sus datos**. Además de permitirle manejar **quién puede acceder** a ellos y en qué términos.



# Casos de uso – Cadena de Distribución

La **inmutabilidad** y **trazabilidad** del blockchain aporta beneficios en sectores como la gestión de la cadena de distribución (*Supply Chain*).



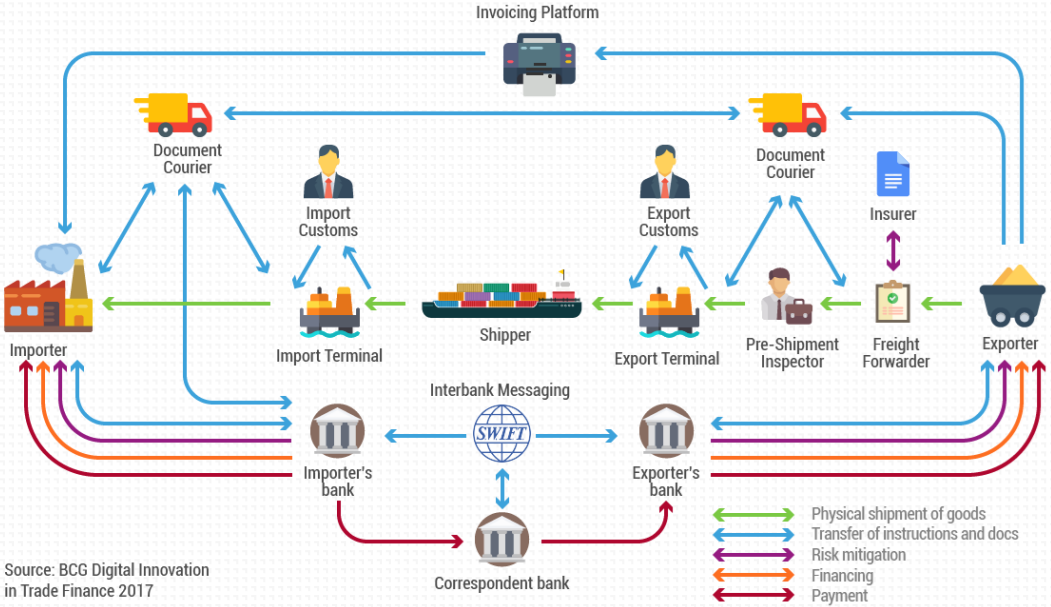

Nespresso uses blockchain to track coffee from Zimbabwe

4 weeks ago • by Ledger Insights

MYTIGATE

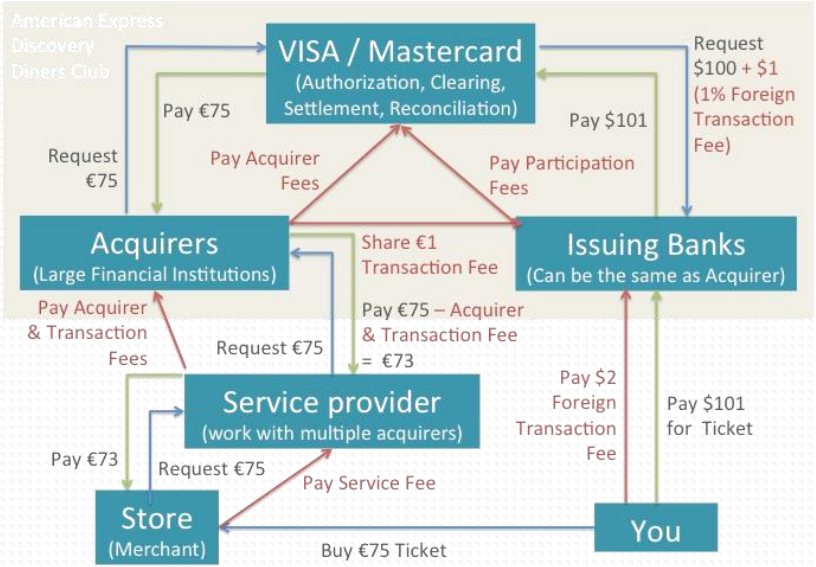
# Casos de uso – Trade Finance

Trade Finance es un caso de uso donde intervienen **muchos agentes** y donde el uso de una "**capa común de datos**" (blockchain) mejoraría mucho la eficiencia, especialmente en la transparencia y reducción de fallos.



# Casos de uso – Desintermediación

En general, siempre que exista un **intermediario** donde su “único” valor añadido sea la **confianza** que depositamos en ellos puede ser susceptible de ser sustituido por blockchain y Smart Contracts.



# Towards “The Enterprise as Code”

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

CBINSIGHTS 41

# In the news

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

*First international payments using Ripple, for retail customers*

BRICKMARK™
THE BLOCKCHAIN REAL ESTATE COMPANY

*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*

07/11/2021

# 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.

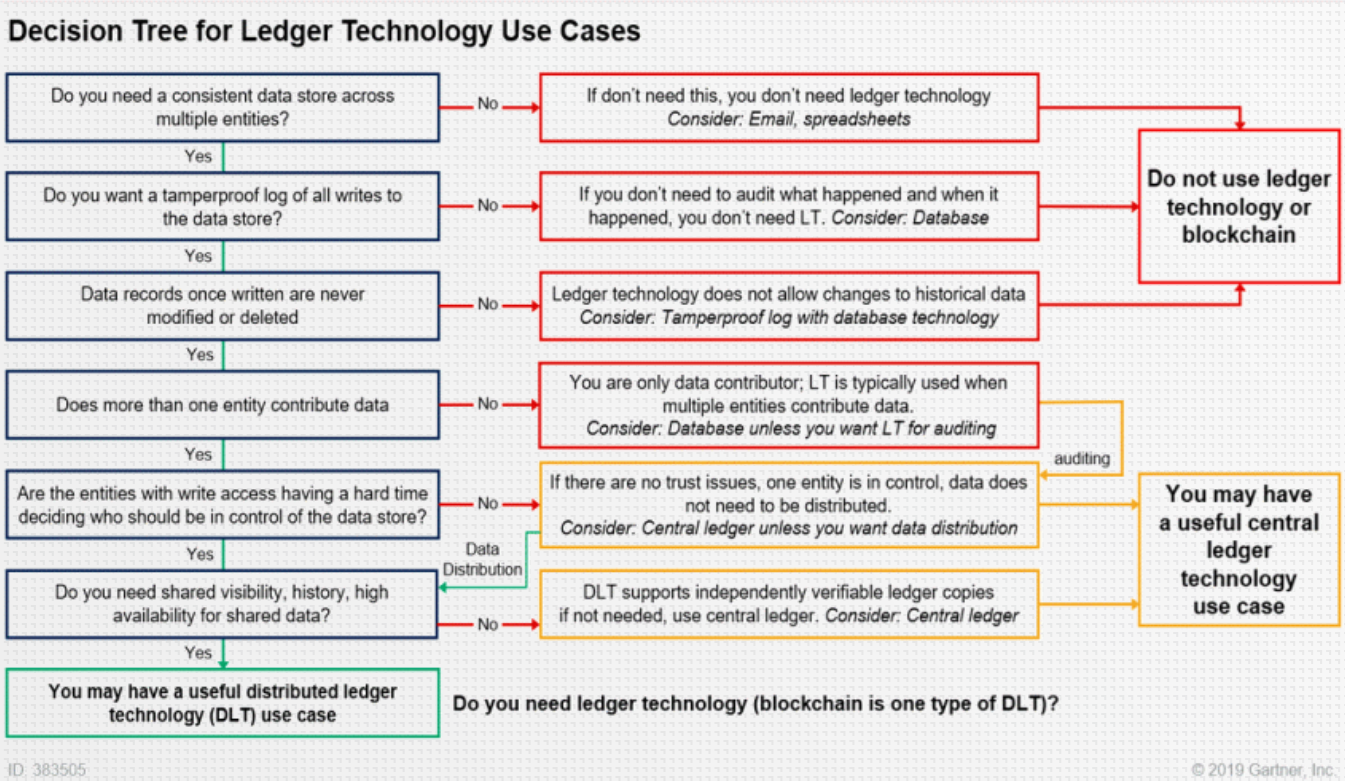
## 05

### 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?



# Real use cases

# Helping our clients in the complex DLT/Crypto world


**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.

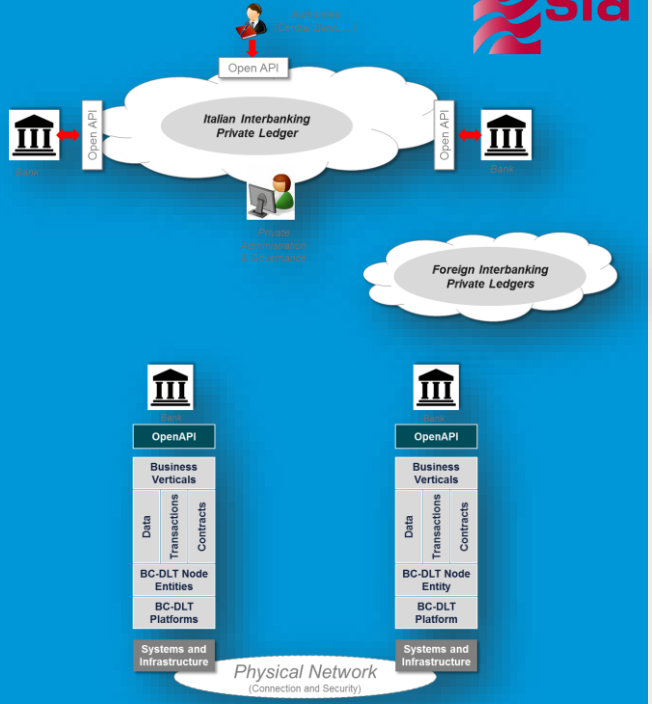
**Bond issuance platform**

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

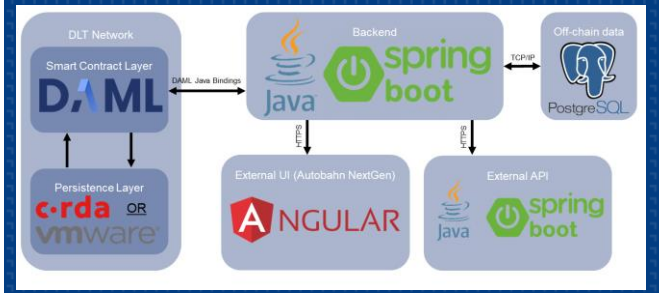
THE BENEFIT

**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

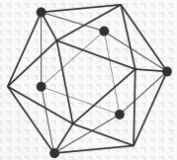
Blockchain 2.0.
De facto standard.

## Quorum

Based on Ethereum.
Good for consortiums.

## Corda

Focus on finance.
Interoperability with
legacy systems.

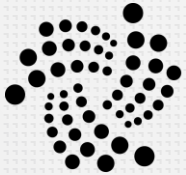


## Hyperledger

Pluggable consensus.
Permissioned & scalable.

## Digital Assets

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

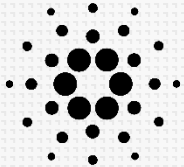


## IOTA

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****.*

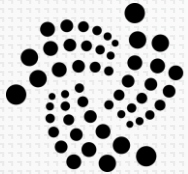
## Key aspects

- 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
ethereum

# 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 (Caradno Settlement Layer and Cardano Computational Layer) | 1-layer |

# **Cardano:** The Third Generation!

**Scalability**

**Layered architecture**

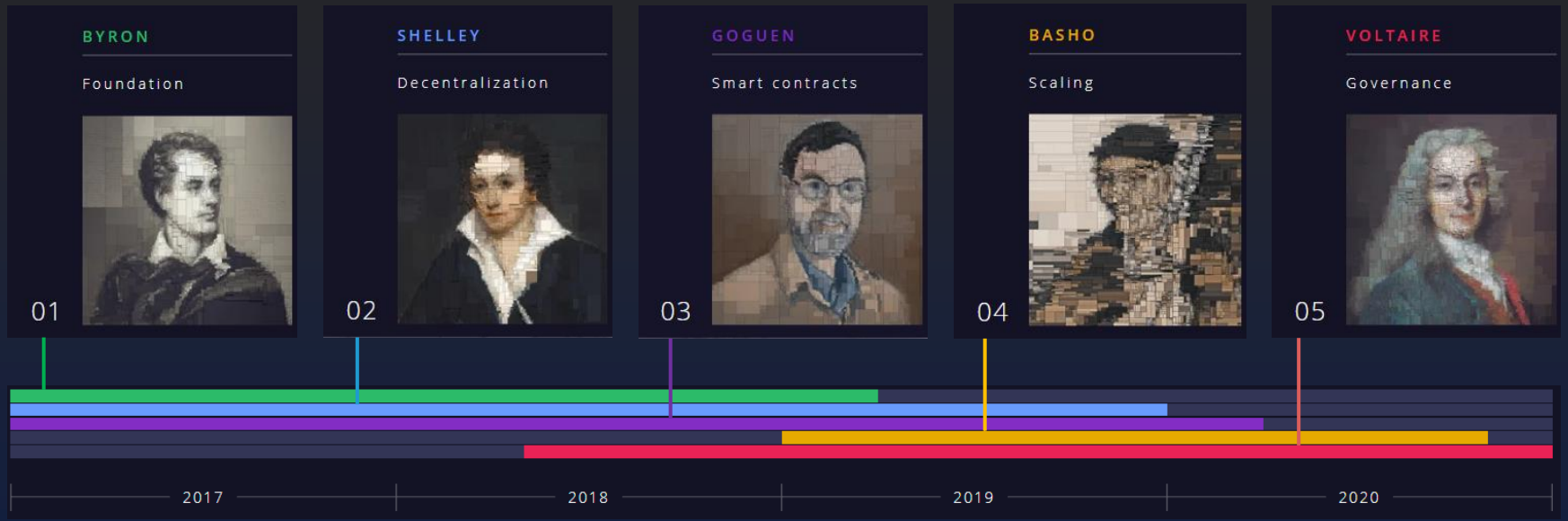
**Cryptocurrency**

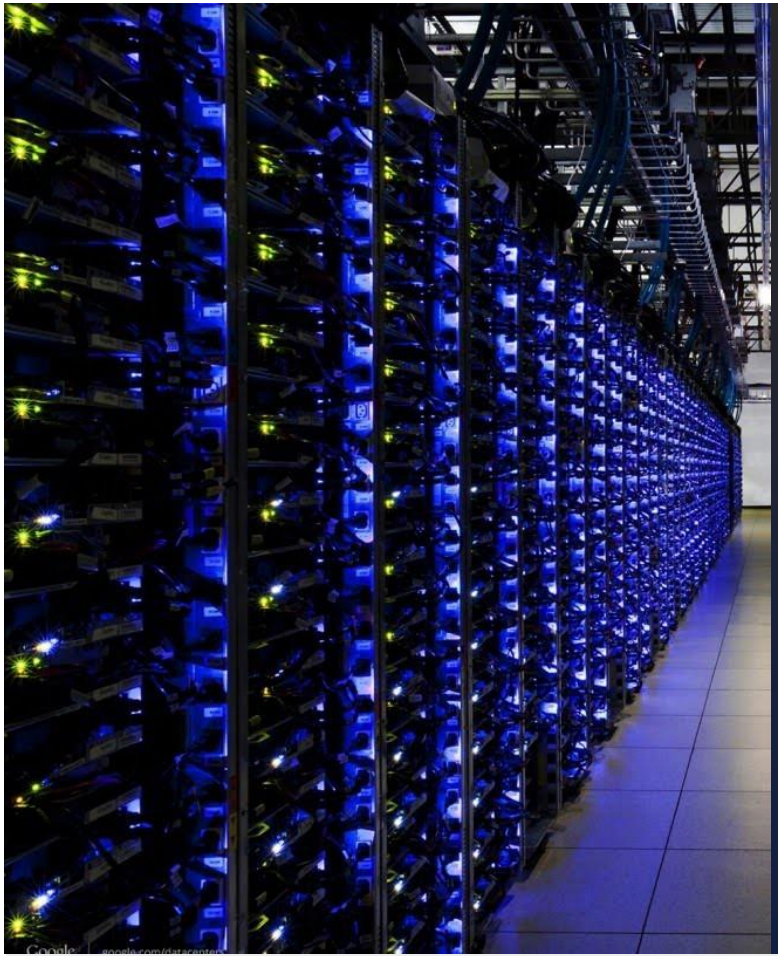
**Interoperability**

**Ecosystem**

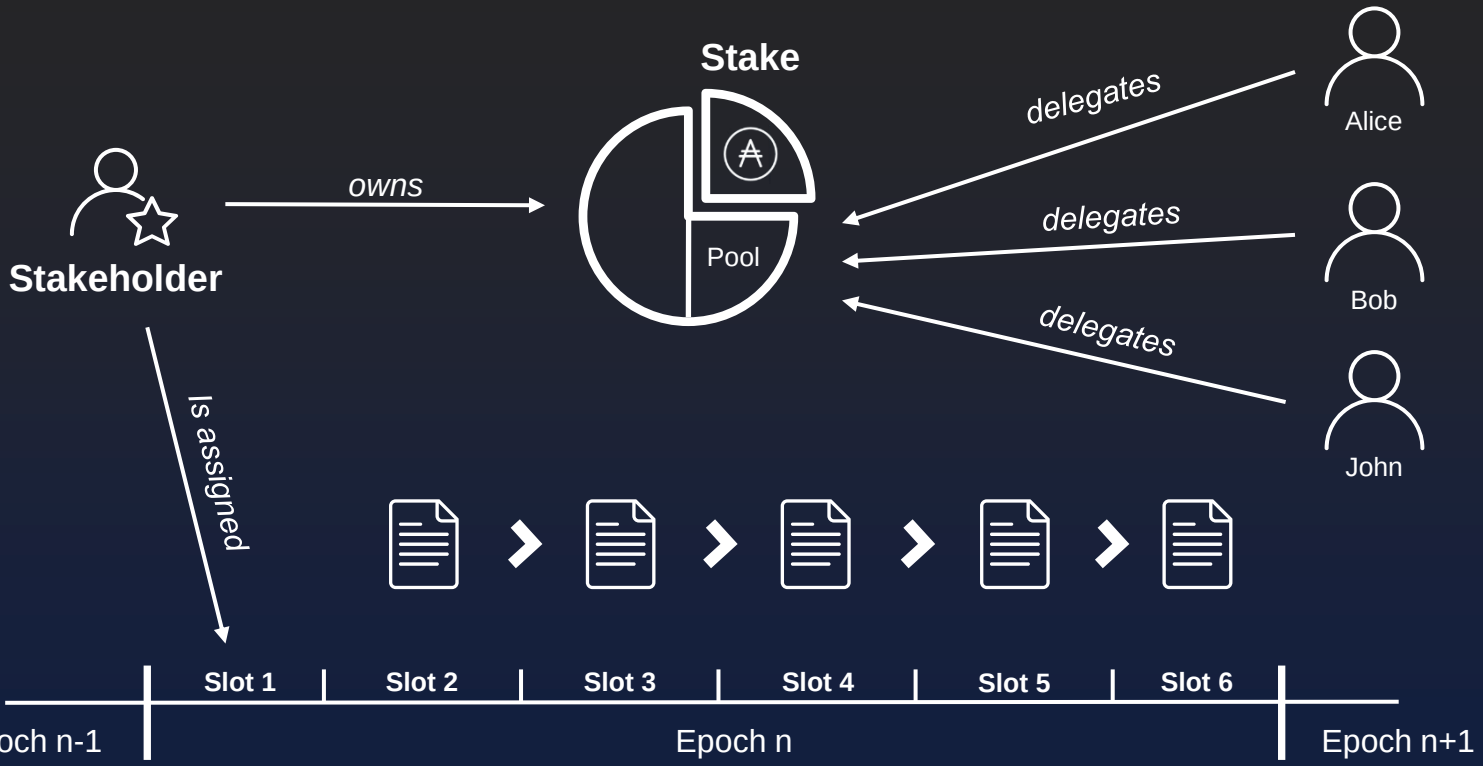
**Multi Asset Ledger**

# Cardano Roadmap





# PoS – How it works



# Demo

YOROI
wallet

**Money Transfer**

**Transaction details**
(using Cardano Explorer)

**Delegation**

# Quiz time!

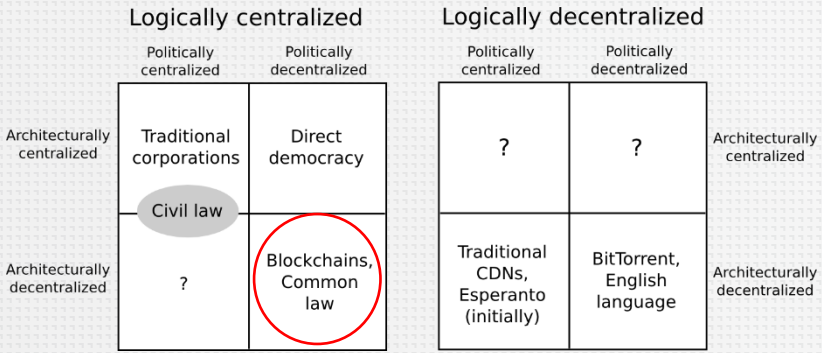
# More on decentralization

# More on decentralization

**Architecturally decentralized**

**Politically decentralized**

**Logically decentralized**




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.


## 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

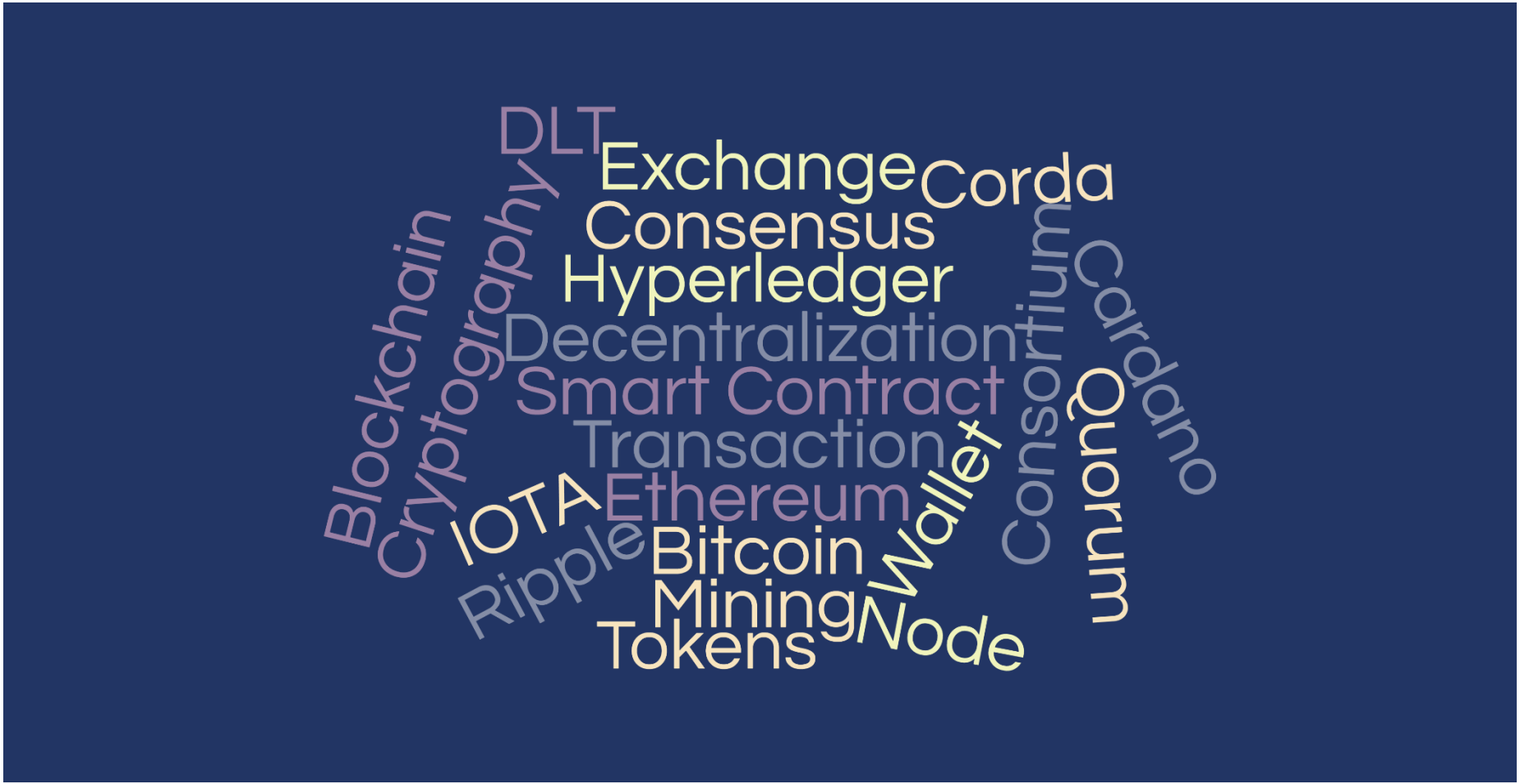
# Decentralized Autonomous Organization (DAO)

- 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**

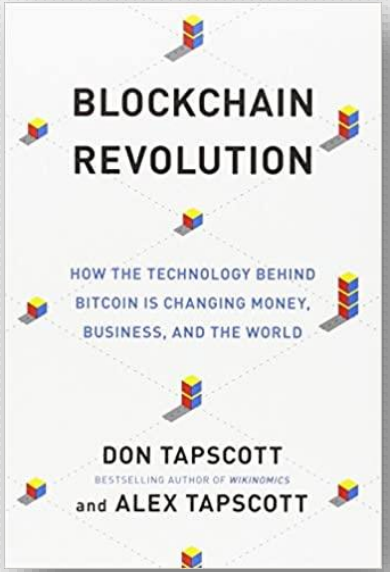


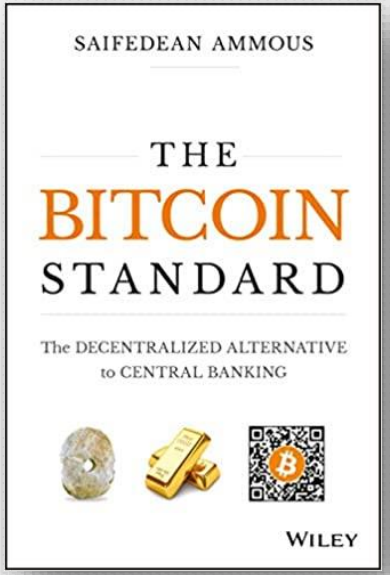
# Quiz time!

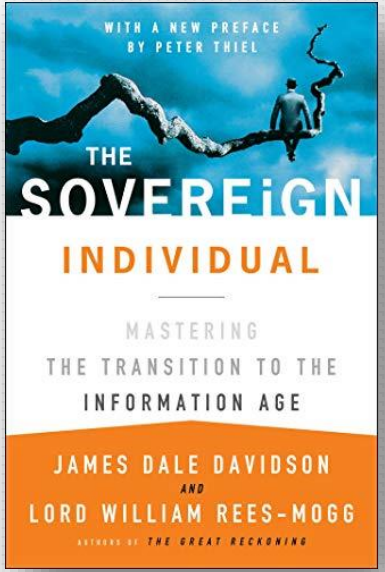
# Summary & Resources

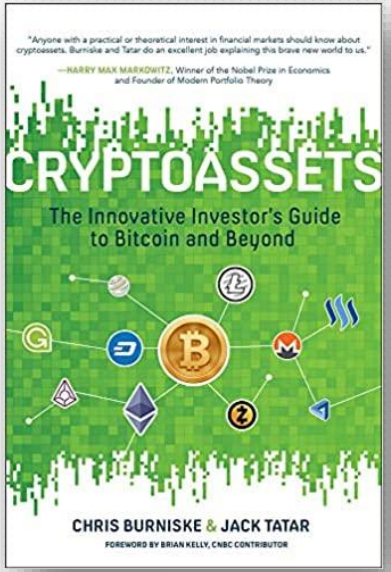

DLT
Exchange
Corda
Consensus
Hyperledger
Blockchain
Cryptography
Decentralization
Smart Contract
Transaction
Cardano
Consortium
Quorum
IOTA
Ethereum
Wallet
Ripple
Bitcoin
Mining
Node
Tokens

# 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

GFT

# Shaping the future of digital business

**Esteban Chiner - GFT**

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

GFT IT Consulting