ISEG

LISBON
SCHOOL OF
ECONOMICS &
MANAGEMENT

UNIVERSIDADE DE LISBOA

Carlos J. Costa (ISEG)
Manuela Aparicio (NovaIMS)

BLOCKCHAIN

Version 2020

Blockchain

- Blockchain is a **technology**.
- Blockchain is part of the **implementation layer** of distributed software systems.
- The **purpose** of the blockchain is to achieve and **maintain integrity** in **distributed systems**.

Software Systems’ Integrity

- **Data integrity**: The data used and maintained by the system are complete, correct, and free of contradictions.
- **Behavioural integrity**: The system behaves as intended and it is free of logical errors.
- **Security**: The system is able to restrict access to its data and functionality to authorized users only.

(Boritz, 2005)

Blockchain Architecture

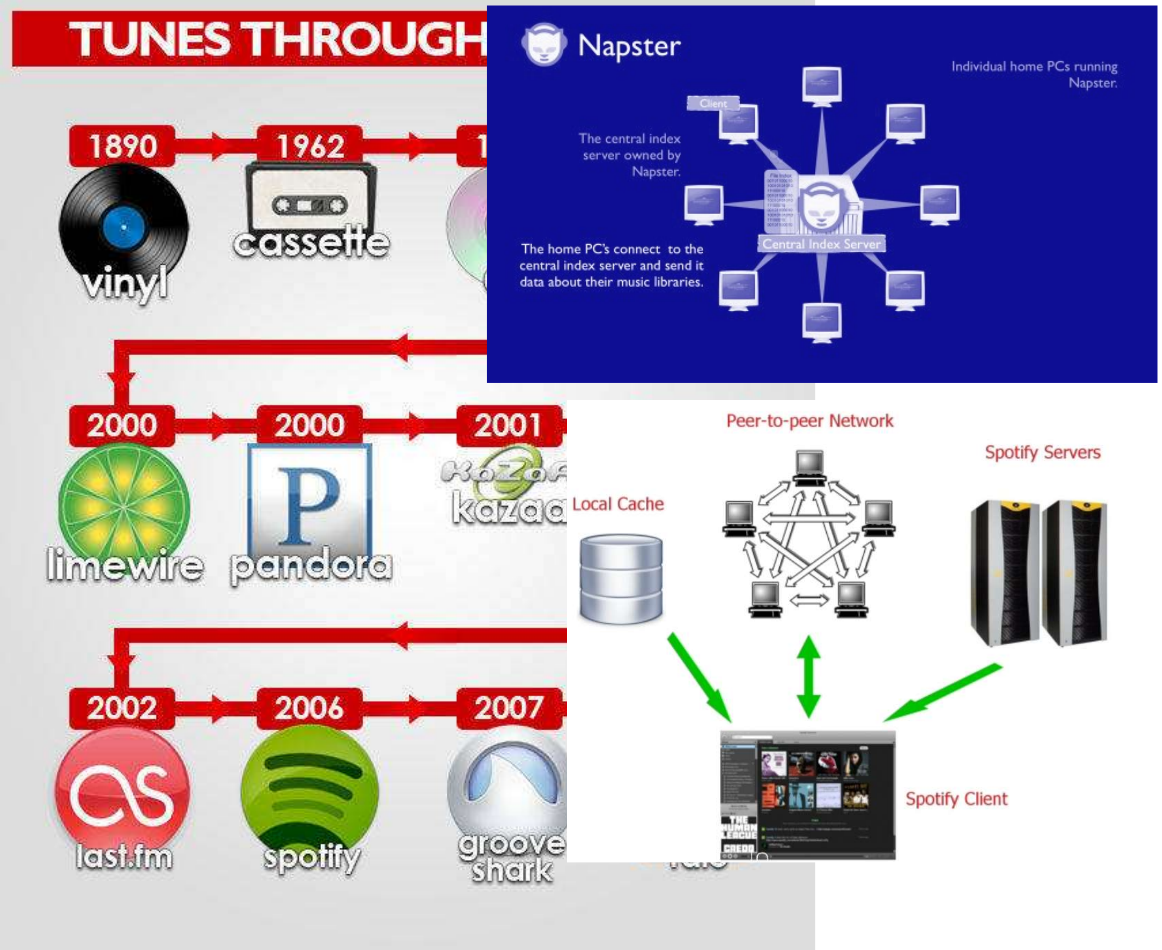
- The **architecture** of a software system **determines** how its **components are organized and related to one another**;

- A distributed system consists of a number of **independent computers**, that **cooperate** with one another by using a communication medium, **without having any centralized element** of control or coordination;
- Blockchain is part of the **implementation layer** of a **distributed software system**;

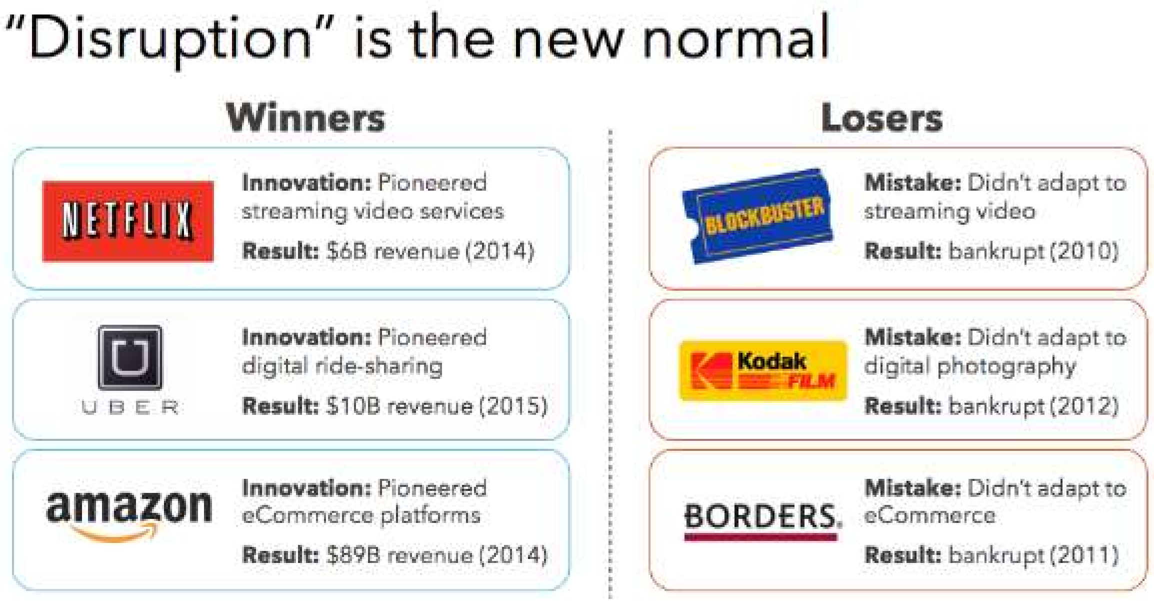
- Blockchain **objective** is to **ensure** a specific non-functional aspect of a distributed software system that achieves and maintains its **integrity**.

(Dresher, 2017)

How peer-to-peer changed business (Blockchain Metaphor)



How peer-to-peer changed business



“Disruption” is the new normal

Winners

NETFLIX
Innovation: Pioneered streaming video services
Result: $6B revenue (2014)

UBER
Innovation: Pioneered digital ride-sharing
Result: $10B revenue (2015)

amazon
Innovation: Pioneered eCommerce platforms
Result: $89B revenue (2014)

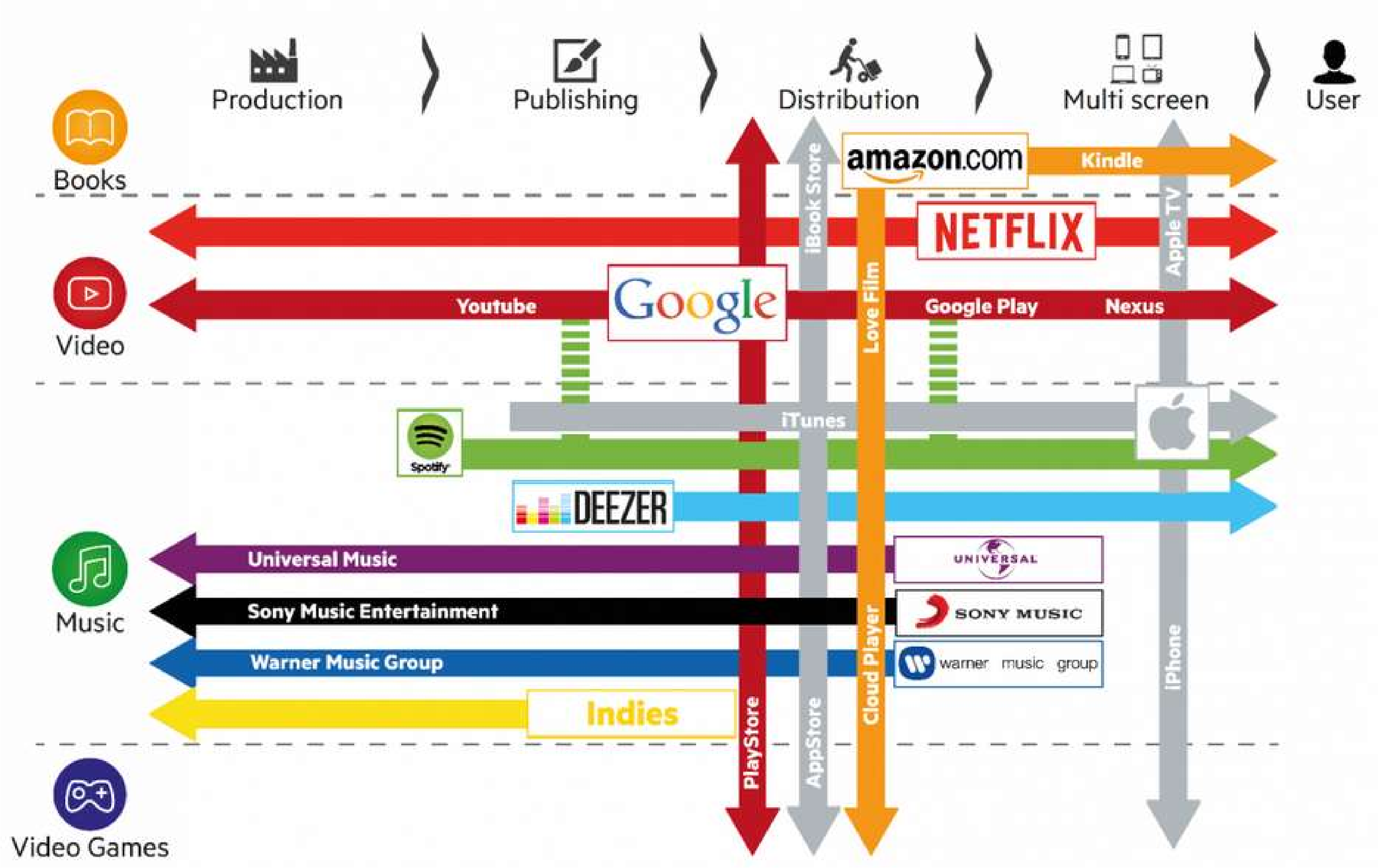
Losers

BLOCKBUSTER
Mistake: Didn’t adapt to streaming video
Result: bankrupt (2010)

Kodak FILM
Mistake: Didn’t adapt to digital photography
Result: bankrupt (2012)

BORDERS.
Mistake: Didn’t adapt to eCommerce
Result: bankrupt (2011)

Various businesses operate the same way

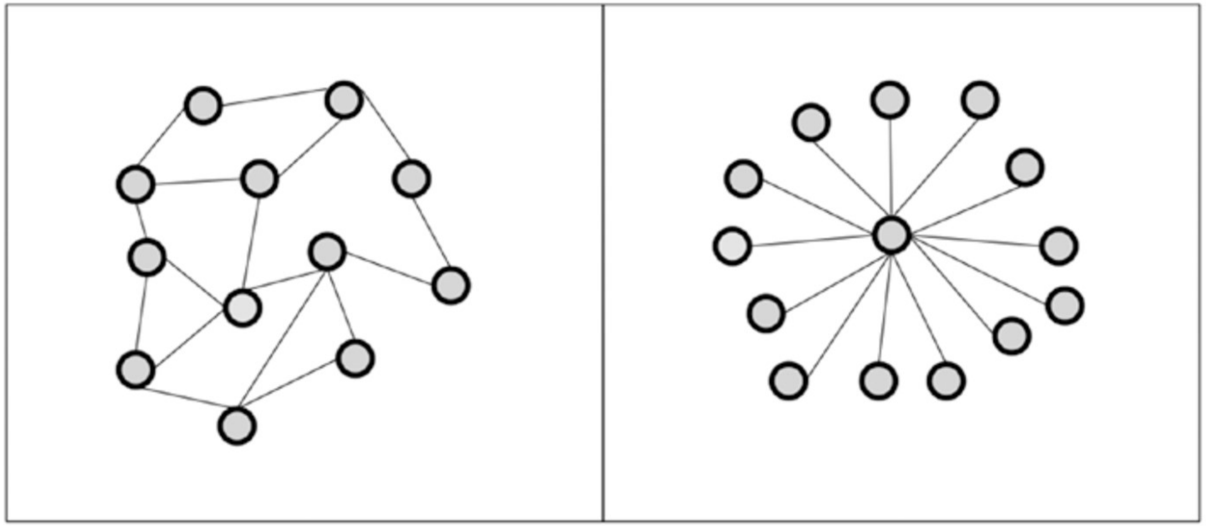


Peer-to-peer system

- **Peer-to-peer** systems are **distributed software** systems that consist of nodes (individual computers), which make their **computational resources** (e.g., processing power, storage capacity, or information distribution) **directly available to another**.

- **Centralized peer-to-peer** systems **maintain central nodes** to facilitate the interaction between peers, to maintain directories that describe the services offered by the peer nodes, or to perform look-ups and identification of the nodes.

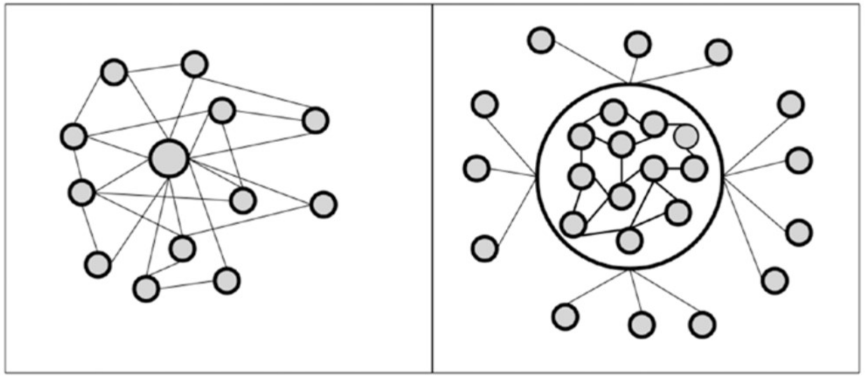
Software Architecture Types



Distributed architecture system

Centralized architecture system

Mixing Centralized & Distributed Systems



Blockchain & Peer-to-Peer Systems

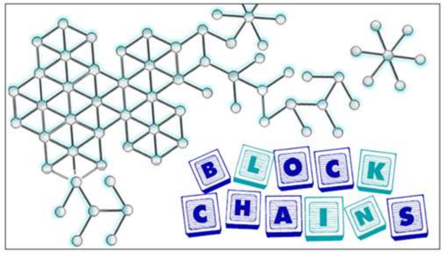
- Purely peer-to-peer distributed systems, may use blockchain for achieving and maintaining integrity;

- **Blockchain** can be considered a tool for achieving and maintaining **integrity in distributed systems**. Purely distributed peer-to-peer systems may use the blockchain in order to achieve and to maintain system integrity

(Drescher, 2017)

Blockchain

- “What is the Blockchain technology? Think of the ability to transfer ownership without an intermediary. Then think of a system that records the correlation of these transfers as time goes by, and it does so every 30 seconds (block) while ensuring correlation with the next block, and so on. This is what is meant by a “blockchain.”



http://www.huffingtonpost.com/entry/591dac73e4b07617ae4cb9ba

Blockchain

- "*Blockchain* owes its name to the way it stores transaction data —in *blocks* that are linked together to form a *chain*"

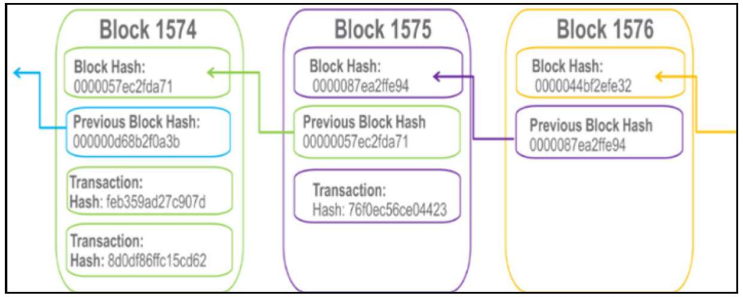
- "As the number of transactions grows, so does the blockchain. Blocks record and confirm the time and sequence of transactions, which are then logged into the blockchain, within a discrete network governed by rules agreed on by the network participants."

(Gupta, 2018)

Blockchain

- "*Blockchain* owes its name to the way it stores transaction data —in *blocks* that are linked together to form a *chain*"

- "As the number of transactions grows, so does the blockchain. Blocks record and confirm the time and sequence of transactions, which are then logged into the blockchain, within a discrete network governed by rules agreed on by the network participants."



(Gupta, 2018)

Blockchain: concept disambiguation

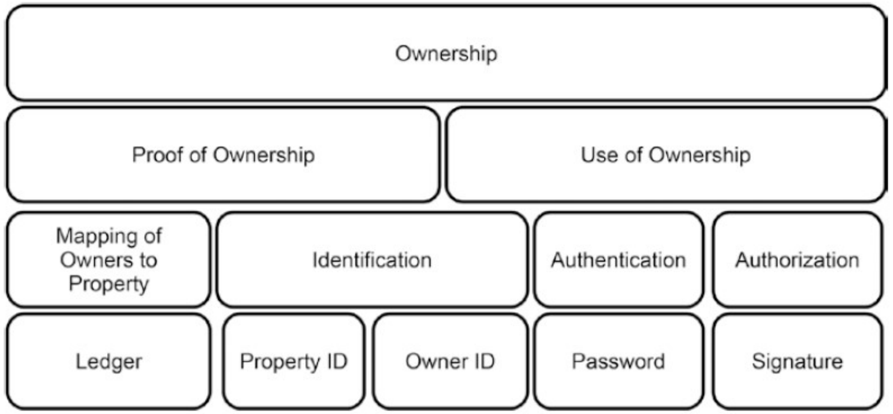
- The term blockchain is ambiguous; it has different meanings for different people depending on the context.

- Blockchain can refer to:
  - A data structure
  - An algorithm
  - A suite of technologies
  - A group of purely distributed peer-to-peer systems with a common application area

(Drescher, 2017)

Blockchain & Ownership

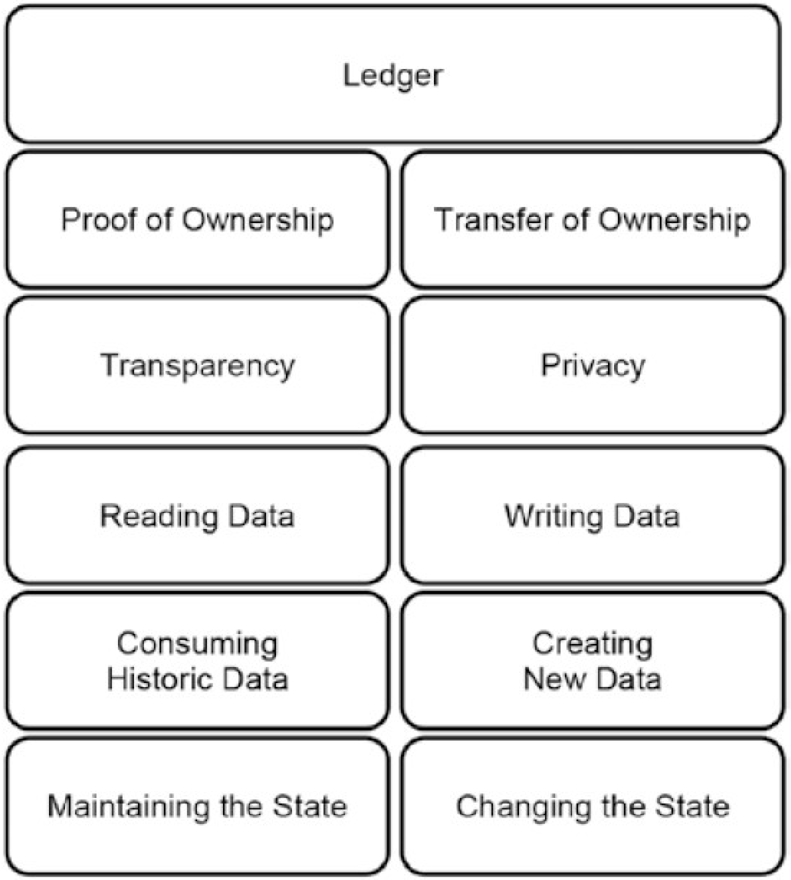
- Ownership is composed by 3 elements:
  - Owner identification
  - Owned object identification
  - Owner object mapping



- **Identification** means claiming
- **Authentication** means proving
- **Authorization** means getting access to something due to the previously authenticated identity.

Blockchain & Ledger

- Proving ownership is done with a ledger, which is open to anyone.
- Transparency is the basis of proving ownership, this transparency makes information public
- Each blockchain-data-structure represents one ledger
- The ledger is maintained by and replicated by every node of the distributed system.



Ledger

Proof of Ownership

Transfer of Ownership

Transparency

Privacy

Reading Data

Writing Data

Consuming Historic Data

Creating New Data

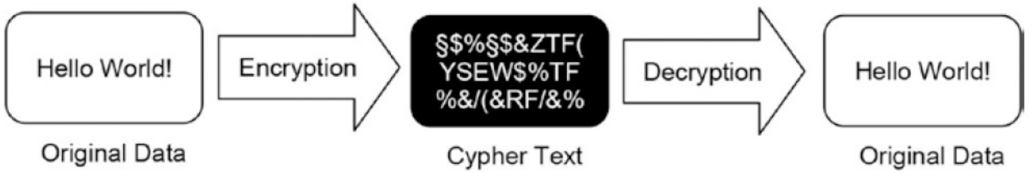
Maintaining the State

Changing the State

Ownership Access

- Information owner access is maintained through the usage of asymmetric cryptography during the data transaction.
- The asymmetric cryptography is composed by two complementary keys: private key & public key:
  - The private key protects data by cypher text
    - (a function which transforms any kind of data into a number of fixed length (hash), this process is named encryption)
  - The public key turns cyphered text back into useful data
    - (this part of the process is named decryption. In each of these processes, and for every one of them, blockchain produces a hash, so that data is linked with the produced hashes that link each piece of data with another piece of data, a chain)
  - Blockchain use asymmetric cryptography to identify accounts (user accounts correspond to the public cryptographic key), and to authorize transactions. All these transactions are kept.

(Abreu et al., 2018; Drescher, 2017)



Blockchain

“*Each block contains a hash (a digital fingerprint or unique identifier), timestamped batches of recent valid transactions, and the hash of the previous block. The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks.*”

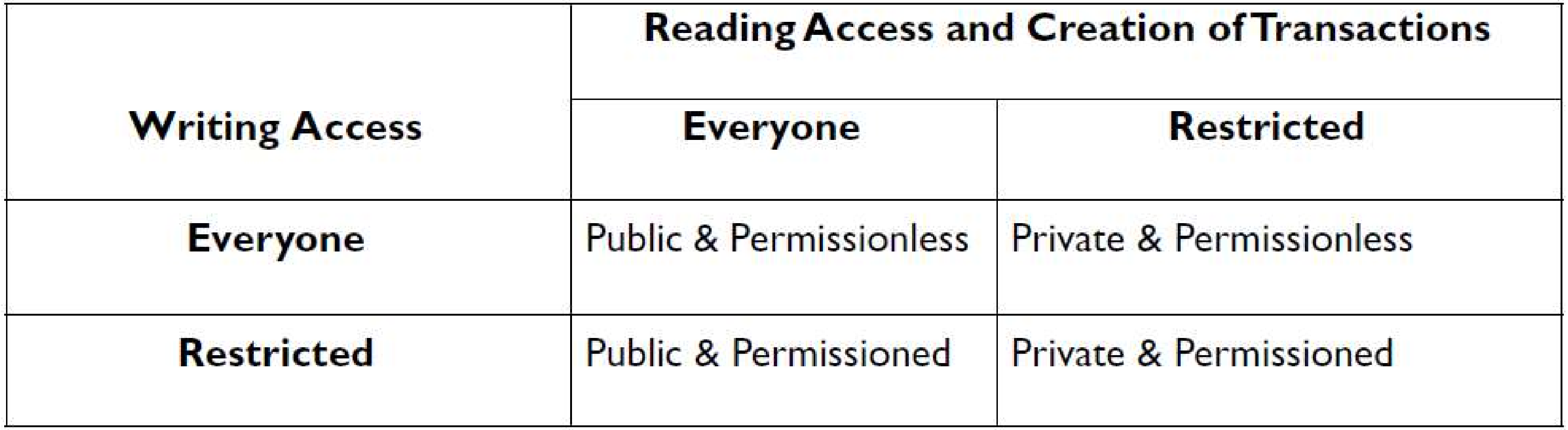
(Gupta, 2018)

HYPERLEDGER

“Hyperledger Fabric provides a framework for developing blockchain solutions with a modular architecture, pluggable implementations, and container technology. While leveraging open-source best practices, Hyperledger Fabric enables confidentiality, scalability, and security in business environments.”

https://www.hyperledger.org/
https://github.com/hyperledger

Blockchain Types



Writing Access	Reading Access and Creation of Transactions	
	Everyone	Restricted
Everyone	Public & Permissionless	Private & Permissionless
Restricted	Public & Permissioned	Private & Permissioned

Where Blockchain can be used (1/2):

- Payments:
  Managing ownership and transfer of digital fiat currencies.

- Cryptocurrencies:
  Managing ownership and creation of digital instruments of payment that exist independently from any government, central bank, or other central institution.

- Micropayments:
  Transfer of small amounts of money that would be too costly by using traditional means of transfer.

- Digital assets:
  Managing creation, ownership, and transfer of digital items that have value in their own right or represent valuable goods in the real world.

Where Blockchain can be used (2/2):

- Digital identity:
  Proving identity and authentication based on unique digital items.

- Notary services:
  Digitizing, storing, and verifying documents or contracts and proof of ownership or transfer.

- Compliance and audit:
  Auditing business activities of people or organizations in regulated industries in an audit track.

- Tax:
  Calculating and collecting taxes based on transactions or on sole ownership, reducing tax avoidance, 2 or double taxation.

- Voting:
  Creating, distributing, and counting digital ballot papers.

- Record management: Creation and storing of medical records.

Blockchain & Smart Contracts

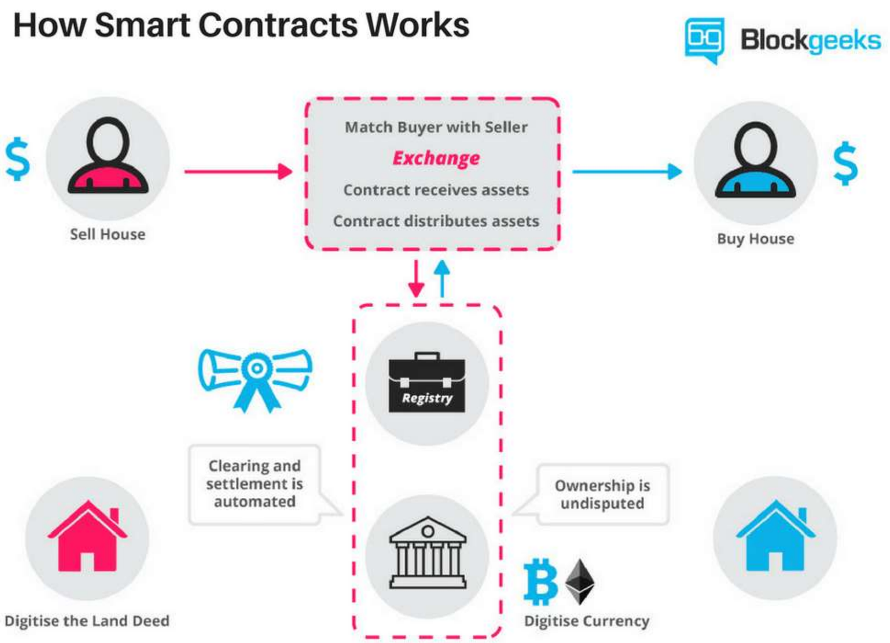
https://youtu.be/ZE2HxTmxfrI

"A smart contract is an agreement or set of rules that govern a business transaction; it's stored on the blockchain and is executed automatically as part of a transaction. Smart contracts may have many contractual clauses that could be made partially or fully self-executing, self-enforcing, or both. Their purpose is to provide security superior to traditional contract law while reducing the costs and delays associated with traditional contracts."

(Gupta, 2018)

Blockchain & Smart Contracts

https://blockgeeks.com/guides/smart-contracts/



Blockchain

https://youtu.be/l9jOJk30eQs

Bitcoin & Blockchain

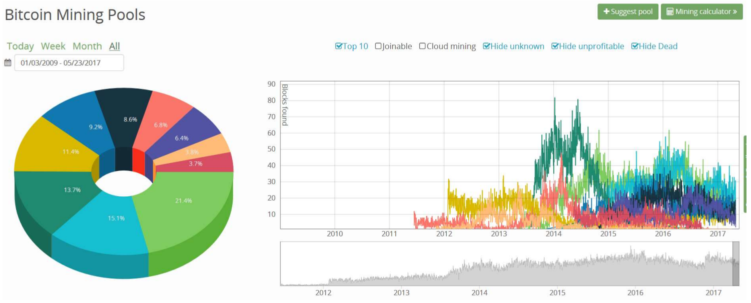
Blockchain Expert Explains One Concept in 5 Levels of Difficulty

https://youtu.be/hYip_Vuv8J0

Bitcoin

- Created by Satoshi Nakamoto in 2009 network and peer-to-peer based
  - With no central authority responsible
  - No reserves for compensation
  - Users create the money “bitcoin miners”
  - Miners work usually in pools to solve very complex crypto puzzles blocks
  - Once the crypto puzzles are deciphered a reward is credited into a bitcoin account

- https://bitcoinchain.com/pools
- http://preev.com/btc/eur



Bitcoin Mining Pools

Today Week Month All

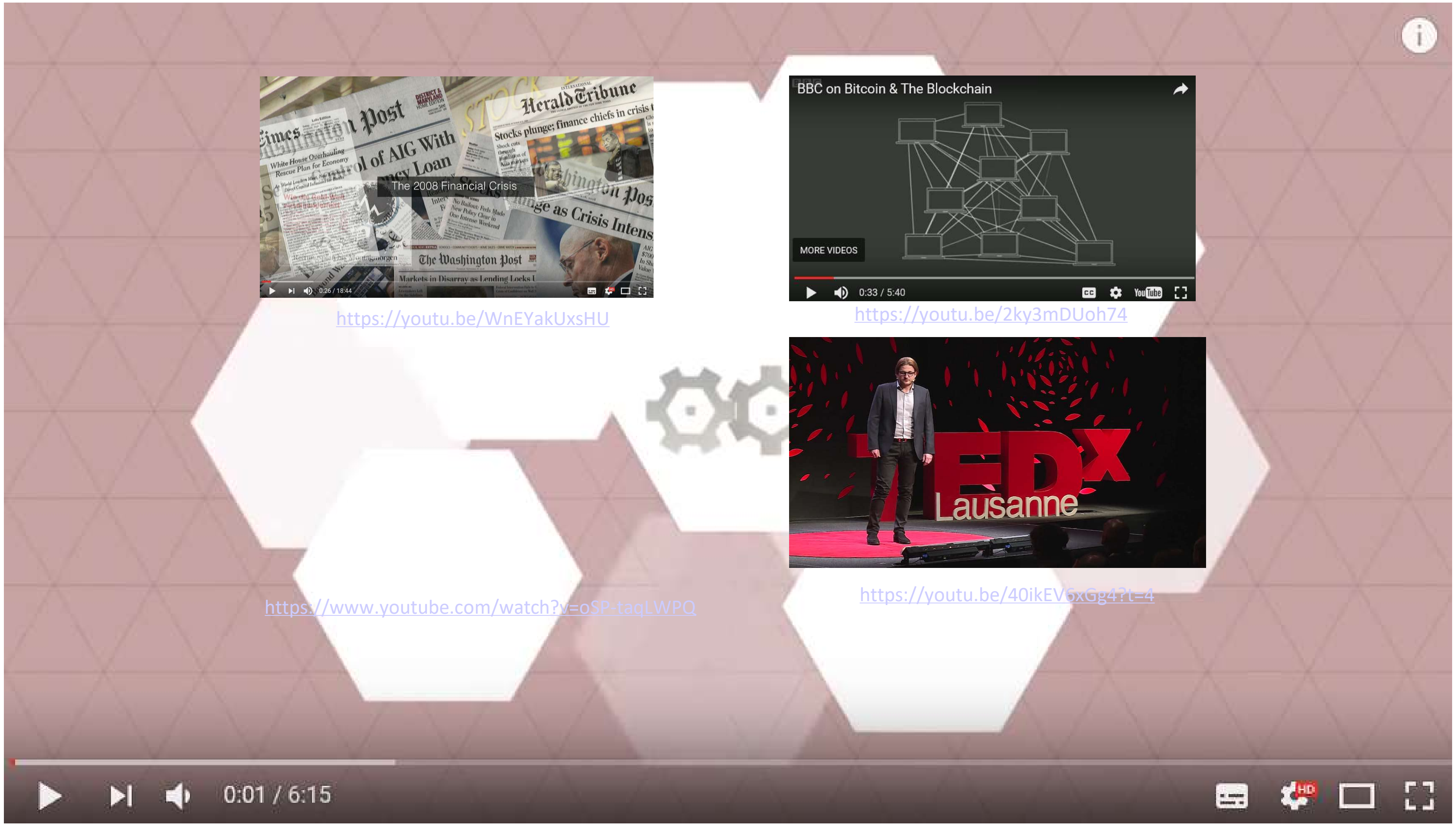
01/03/2009 - 05/23/2017

☑Top 10 □Joinable □Cloud mining ☑Hide unknown ☑Hide unprofitable ☑Hide Dead

Bitcoin

https://bitcoin.org/en/

Blockchain Explained



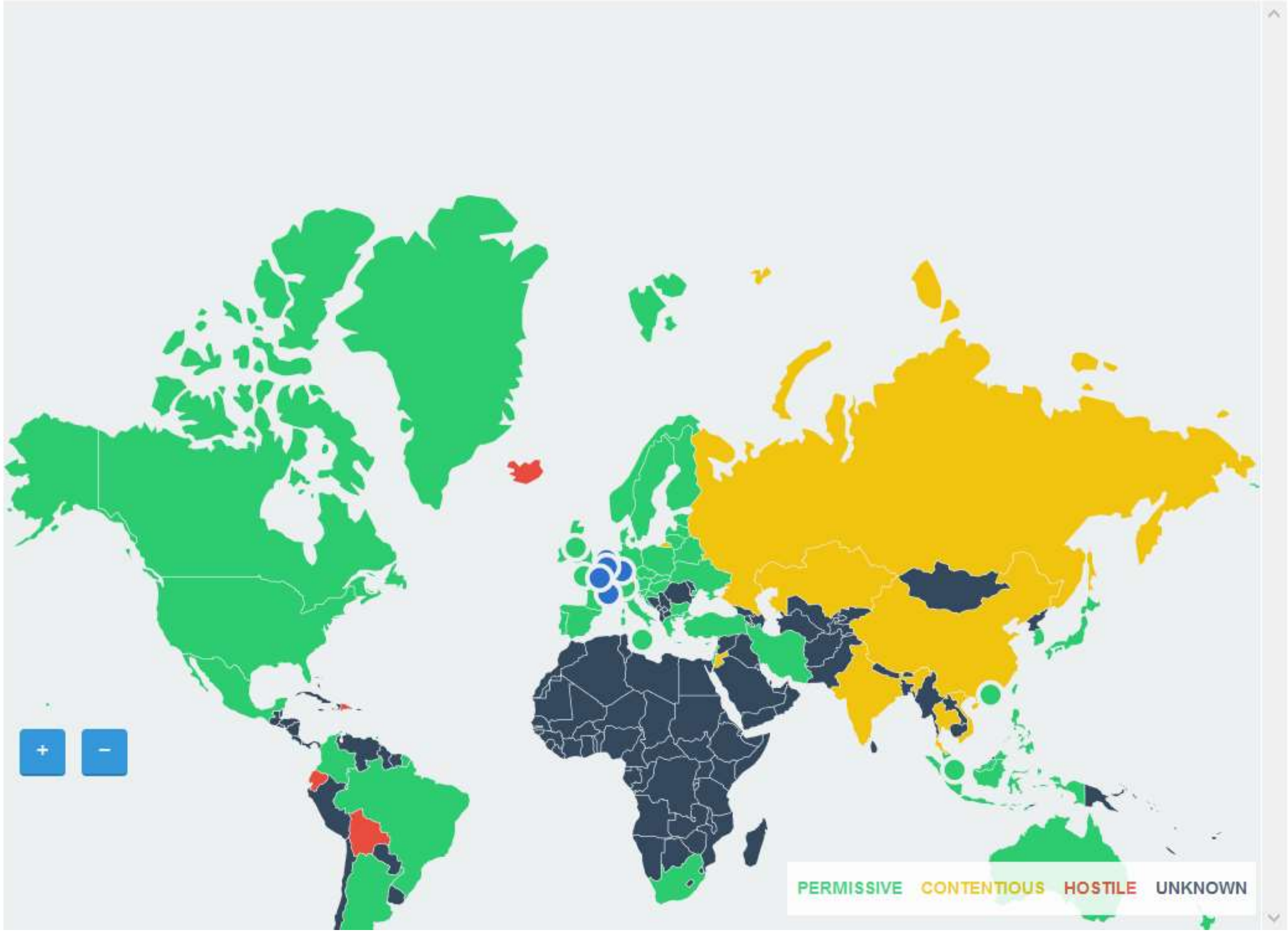
https://youtu.be/WnEYakUxsHU

https://youtu.be/2ky3mDUoh74

https://www.youtube.com/watch?v=oSP-taqLWPQ

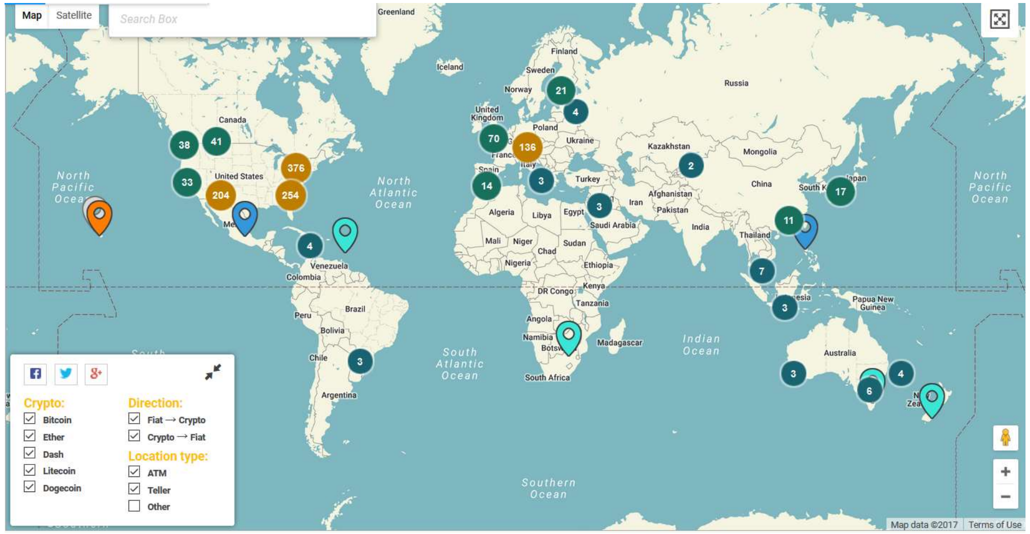
https://youtu.be/40ikEV6xGg4?t=4

Where Bitcoin is regulated



http://www.coindesk.com/bitcoin-legal-map/

ATM Machines



Crypto:

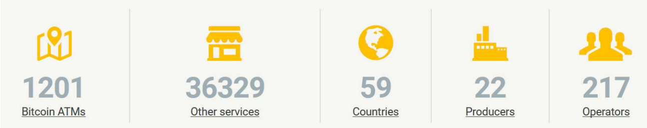
- ☑ Bitcoin
- ☑ Ether
- ☑ Dash
- ☑ Litecoin
- ☑ Dogecoin

Direction:

- ☑ Fiat → Crypto
- ☑ Crypto → Fiat

Location type:

- ☑ ATM
- ☑ Teller
- ☐ Other



1201	36329	59	22	217
Bitcoin ATMs	Other services	Countries	Producers	Operators

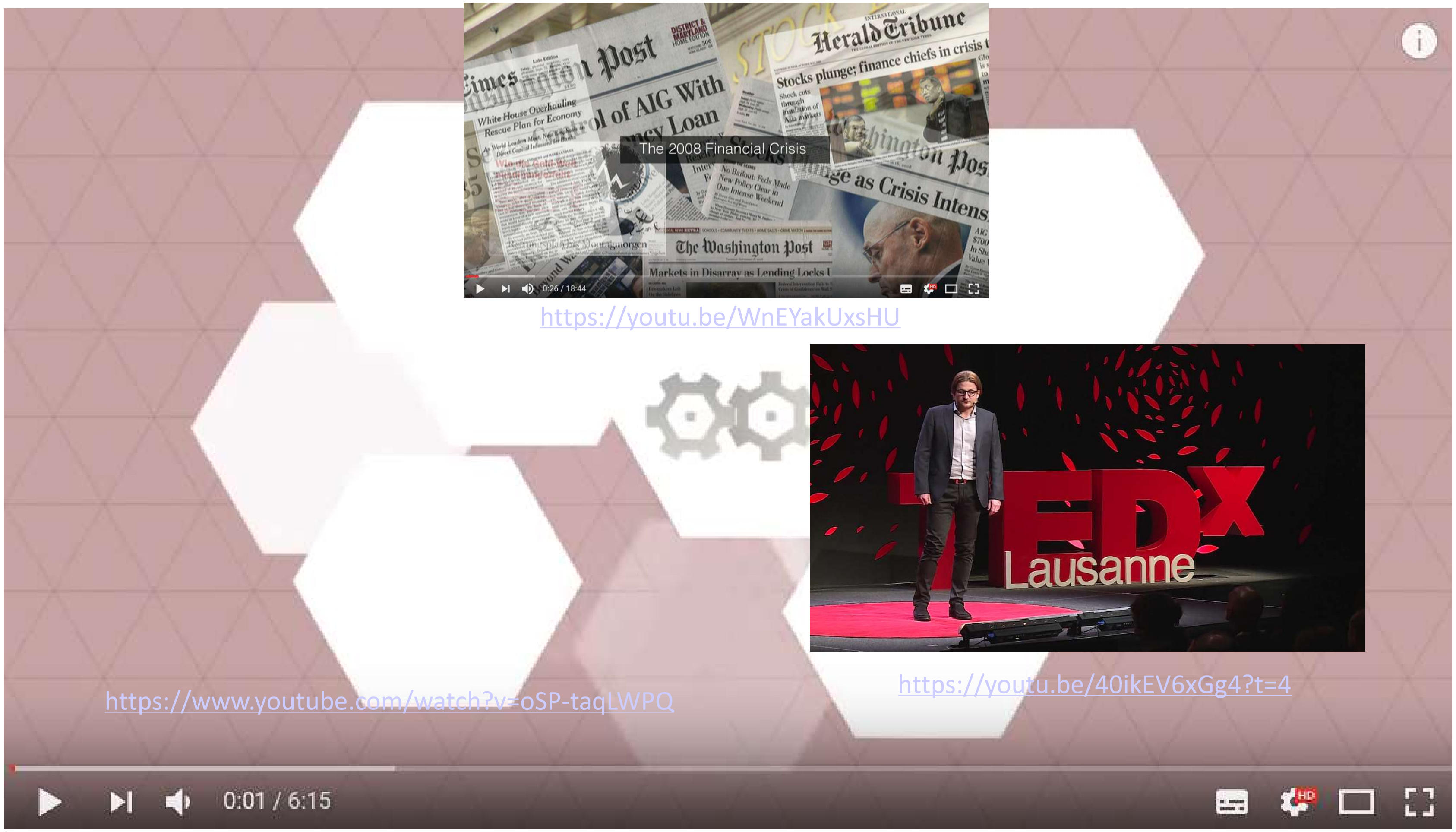
https://coinatmradar.com/

19 Industries The Blockchain Will Disrupt

THE BLOCKCHAIN
IS ONE OF THE MOST PROMISING
NEW TECHNOLOGIES FOR THE FUTURE

https://youtu.be/G3psxs3gyf8

Blockchain Explained



https://youtu.be/WnEYakUxsHU

https://youtu.be/40ikEV6xGg4?t=4

https://www.youtube.com/watch?v=oSP-taqLWPQ

New Market Innovations: Cryptocurrency

- Closed virtual currency systems
  - Can be used only in one specific environment

- Virtual currency with unidierctional flow
  - “real money” can be changed into virtual currency, not otherwise

SECOND LIFE
LINDEN DOLLAR
AUTHORIZED RESELLER

- Bidirectional flow
  - Both currencies are interchangeble (currenc change rate)

MONERO

https://poloniex.com/exchange#btc_eth

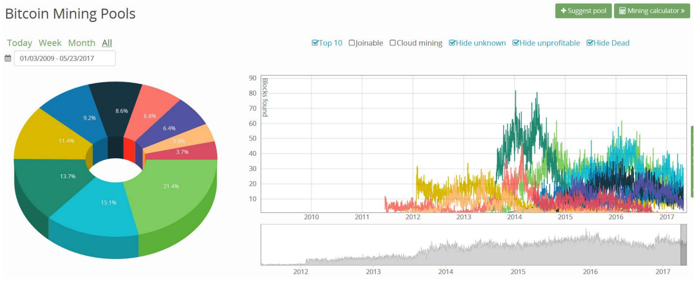
Crypto Escudo

- Created 1000 000 000 coins
- Created through block algorithms resolution
- Used in:
  - ubid.pt
  - Pure Green
  - FP Knots
  - Mercado crypto
  - Mais útil

  - Ver site do Banco de Portugal sobre Moedas virtuais:
  - https://www.bportugal.pt/comunicado/autoridade-bancaria-europeia-alerta-para-os-riscos-das-moedas-virtuais

Bitcoin

- Created by Satoshi Nakamoto in 2009 network and peer-to-peer based
  - With no central authority responsible
  - No reserves for compensation
  - Users create the money “bitcoin miners”
  - Miners work usually in pools to solve very complex crypto puzzles blocks
  - Once the crypto puzzles are deciphered a reward is credited into a bitcoin account



Bitcoin Mining Pools

Today Week Month All

01/03/2009 - 05/23/2017

☑Top 10 □Joinable □Cloud mining ☑Hide unknown ☑Hide unprofitable ☑Hide Dead

- https://bitcoinchain.com/pools

Example of application of Blockchain

https://execed.economist.com/blog/industry-trends/5-applications-blockchain-your-business

Bibliography

.

Abreu, P. W., Aparicio, M., & Costa, C. J. (2018). Blockchain technology in the auditing environment. In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.

Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. International Journal of Accounting Information Systems, 6(4), 260-279.

Christensen, C. M., Bohmer, R., & Kenagy, J. (2000). Will disruptive innovations cure health care?. *Harvard business review*, *78*(5), 102-112.

Christensen, C. M., Raynor, M. E., & McDonald, R. (2015). Disruptive innovation. *Harvard Business Review*, *93*(12), 44-53

Nagy, D., Schuessler, J., & Dubinsky, A. (2016). Defining and identifying disruptive innovations. *Industrial Marketing Management*, *57*, 119-126.

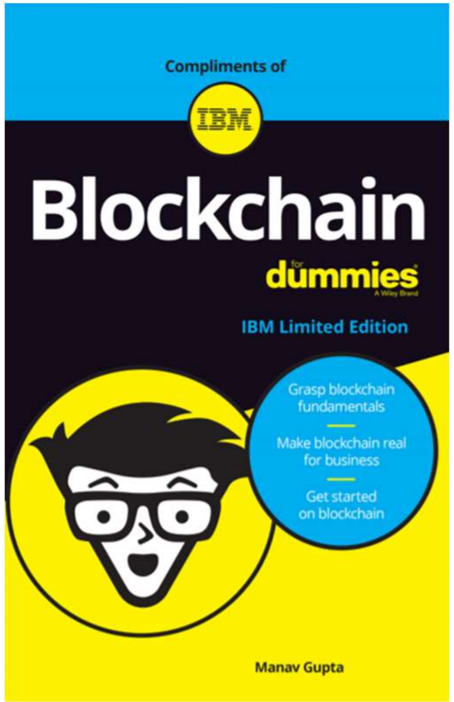
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Raymond, E. (1999). The cathedral and the bazaar. *Philosophy & Technology*, *12*(3), 23.

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable* (Vol. 2). Random house.

Tomlinson, B. ,Donald J. Patterson, and Bonnie Nardi. 2016. Teaching global disruption and information technology online. *interactions* 23, 6 (October 2016), 40-43. DOI: http://dx.doi.org/10.1145/3003818

Blockchain IBM Treat ;)


Compliments of
IBM
Blockchain
for dummies
A Wiley Brand
IBM Limited Edition
Grasp blockchain fundamentals
Make blockchain real for business
Get started on blockchain
Manav Gupta

https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN