Distributed Ledger Technology:
An introduction to interoperability
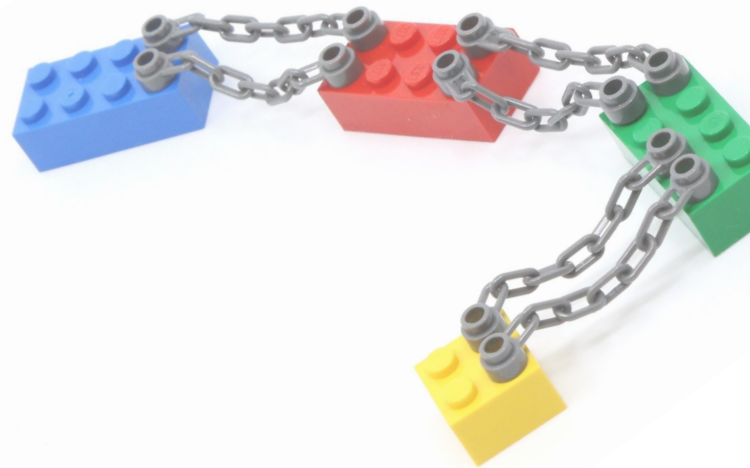
Andrea Lisi, Paolo Mori

Università degli studi di Pisa
02/03/20

2009

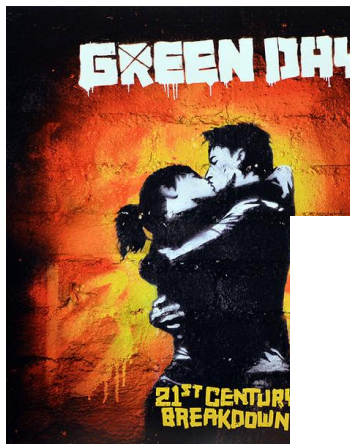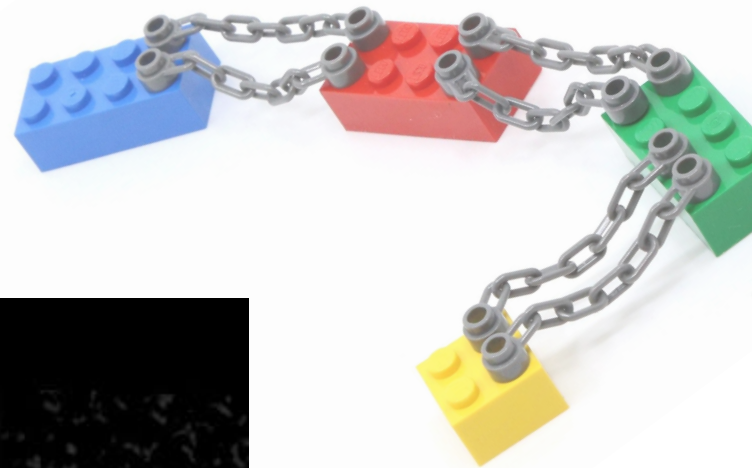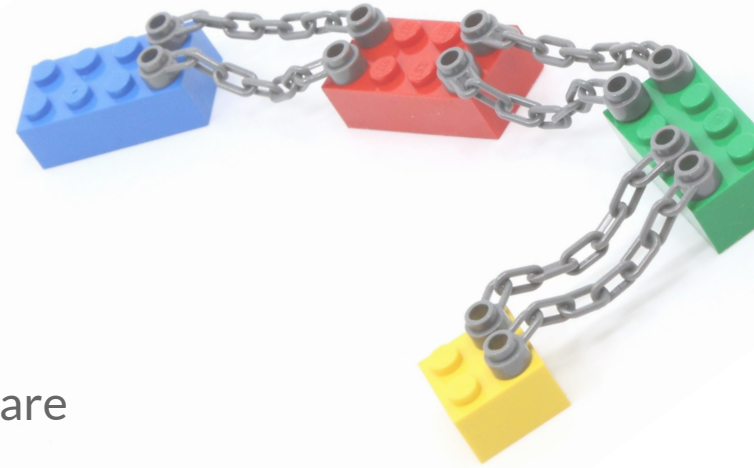# 2009

2009

Bitcoin is a P2P payment system where nodes share the ledger of money Transactions, the Blockchain

The ledger is updated by the first node solving a hash search puzzle, Proof-of-Work (PoW), and gets rewarded with new coins
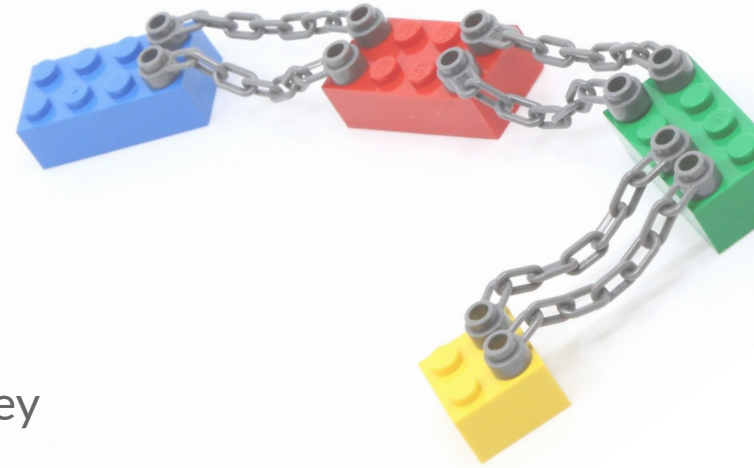
Bitcoin

Transactions are secured by cryptography, i.e. they cannot be (easily) modified: **Immutability**

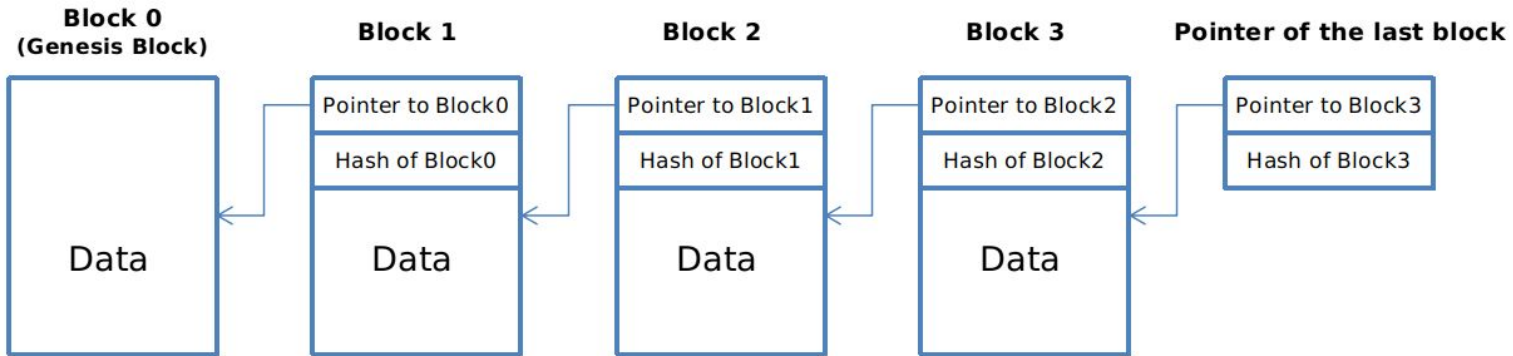Transactions are visible by design: **Transparency**

Transactions are **ordered**, i.e. it is possible to rebuild the current state of the ledger

User are **pseudo-anonym**

Bitcoin

Block 0 (Genesis Block)	Block 1	Block 2	Block 3	Pointer of the last block
	Pointer to Block0	Pointer to Block1	Pointer to Block2	Pointer to Block3
	Hash of Block0	Hash of Block1	Hash of Block2	Hash of Block3
Data	Data	Data	Data	

Bitcoin

It is not intuitive for end users: it is easy to lose coins

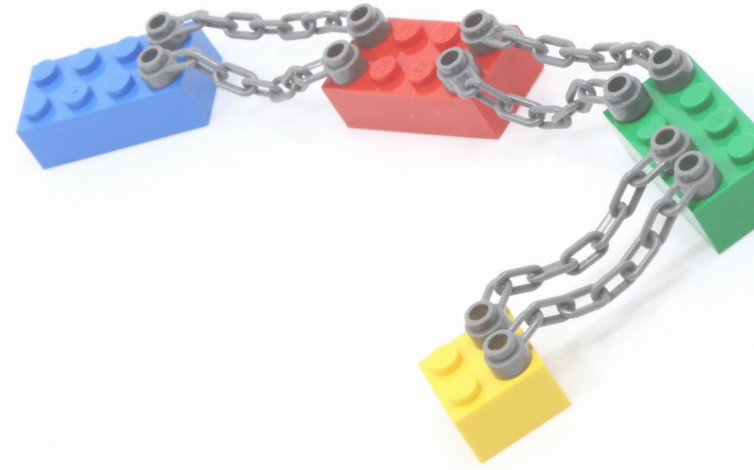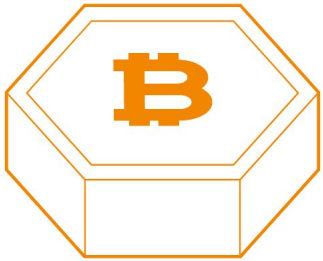Slow processing power: around 7 Txs / s

Bitcoin is a good protocol as a decentralized payment system, but not much more
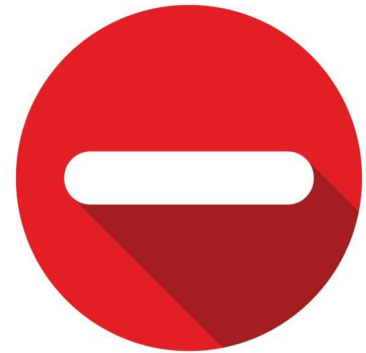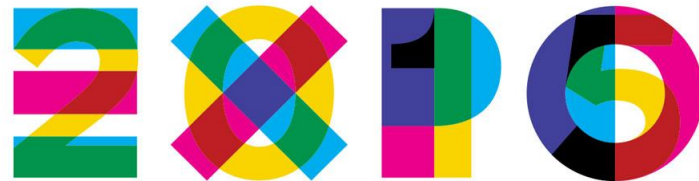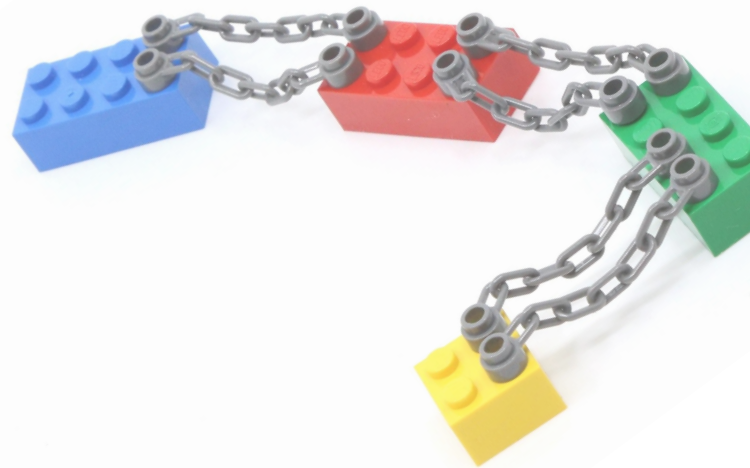
Bitcoin - Monolithic

2015

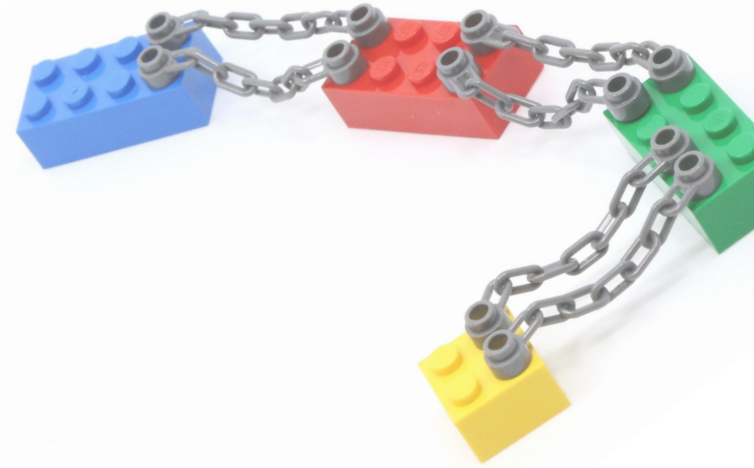PARIS2015
UN CLIMATE CHANGE CONFERENCE
COP21·CMP11

EXPO
MILANO 2015

2015

Ethereum is a global, open-source platform for decentralized applications

Ethereum nodes run a virtual machine (EVM) that allows the execution of Turing-complete software called Smart Contracts
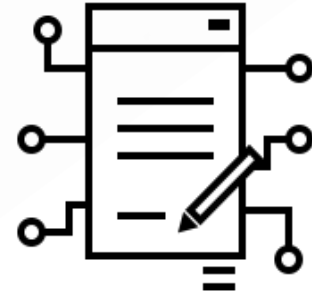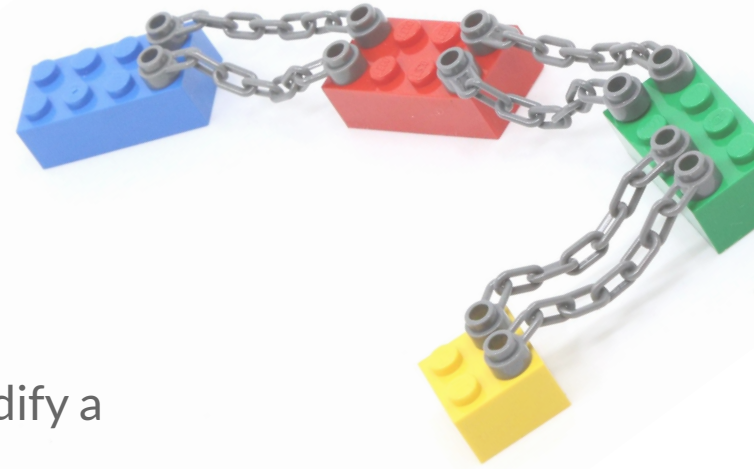
Ethereum

Smart contracts expose Functions which can modify a State stored in such contracts

With respect to Bitcoin, is possible to create more complex applications, also known as Decentralized Applications (DApp)

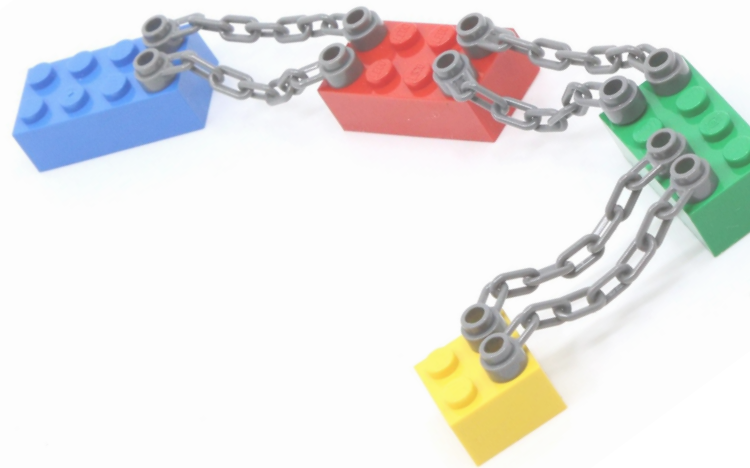- Because Smart contracts are executed by the whole network

Ethereum

A very popular DApp is called Cryptokitties, a
marketplace of digital cats with unique traits

- Its popularity caused a network slowdown in
  December 2017

Cryptokitties smart contract:
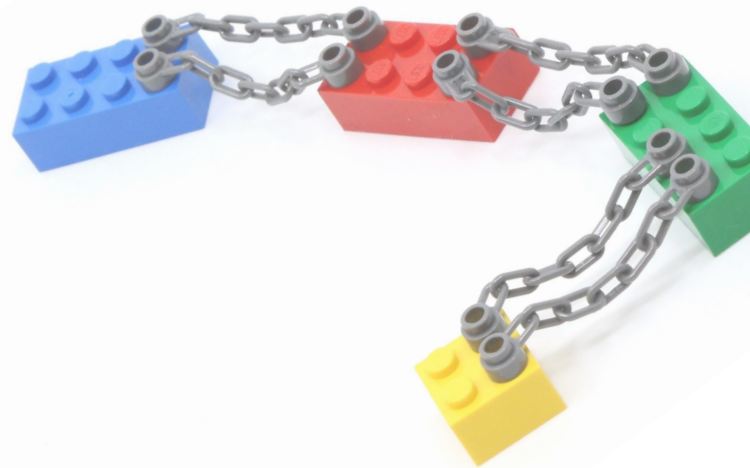https://etherscan.io/token/0x06012c8cf97bead5deae237070f9587f8e7a266d

Ethereum

Slow processing power, around 15 Txs / s

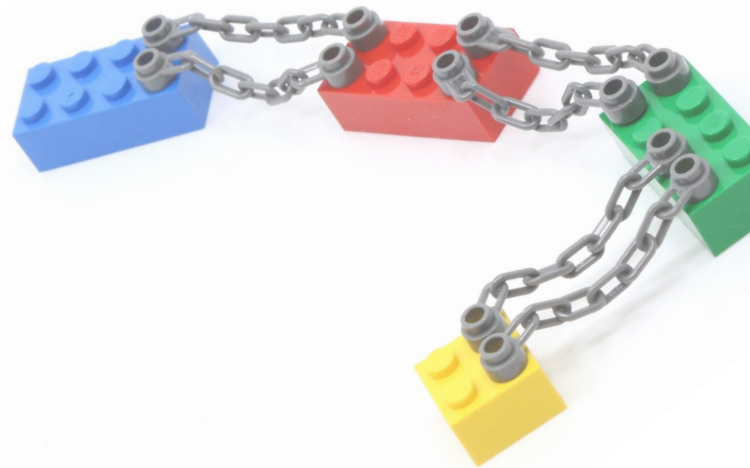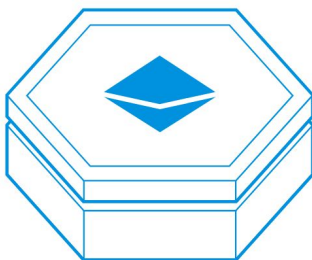Smart contracts bugs cannot be fixed and can lead to big money loss

- In 2016 3.6M ETH were stolen, the equivalent of 70M $ (DAO attack)

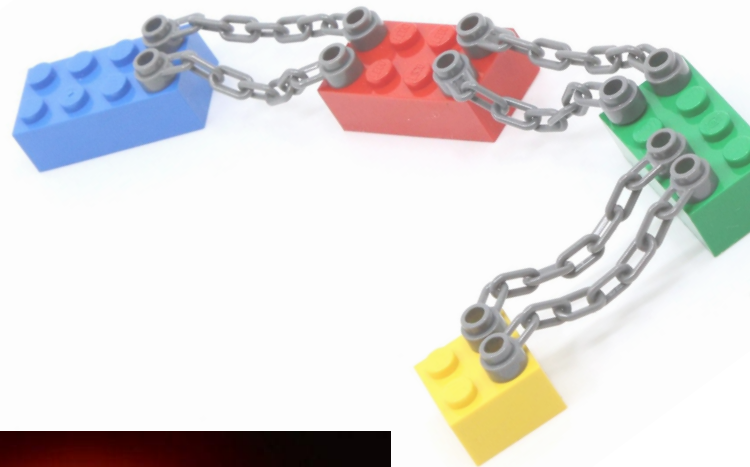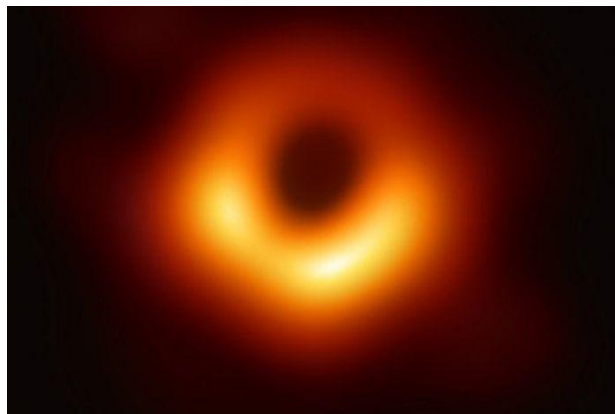Less specialized than Bitcoin, but all DApps share the same resources

Ethereum - A top layer

Images from:

https://cosmos.network/intro

2019

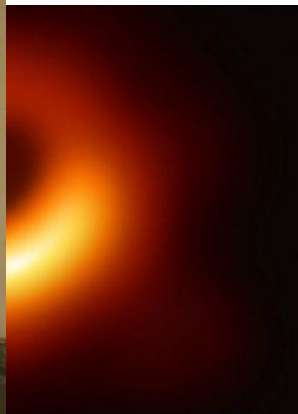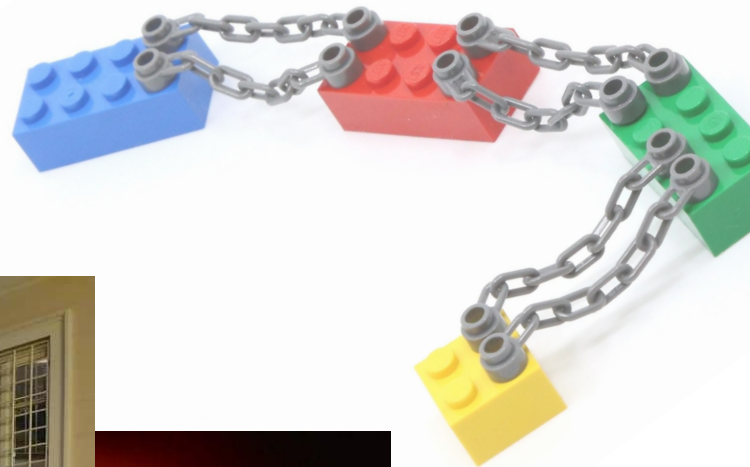# 2019

2019

Blockchain applications are self-contained

- Bitcoin is specialized in digital payments

- Ethereum allows general DApps, but with shared resources

- And more...

Can they interact?
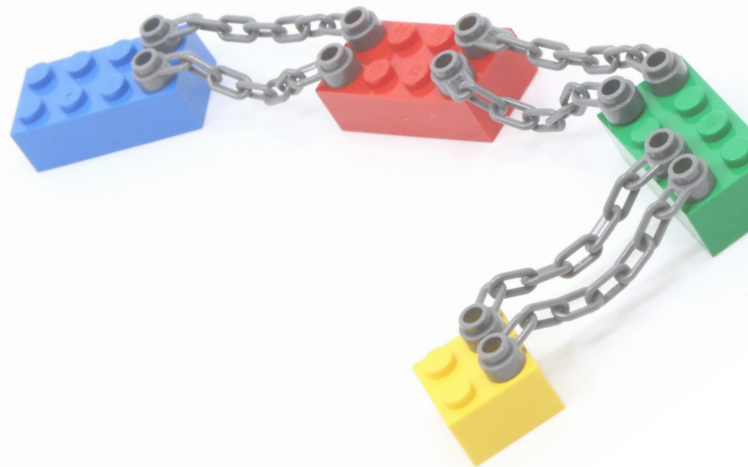
Use cases

Cross-chain asset exchange

- Without relying on trusted third parties

Cross-chain asset portability

- Move an asset between chains

Cross-chain smart contract interaction

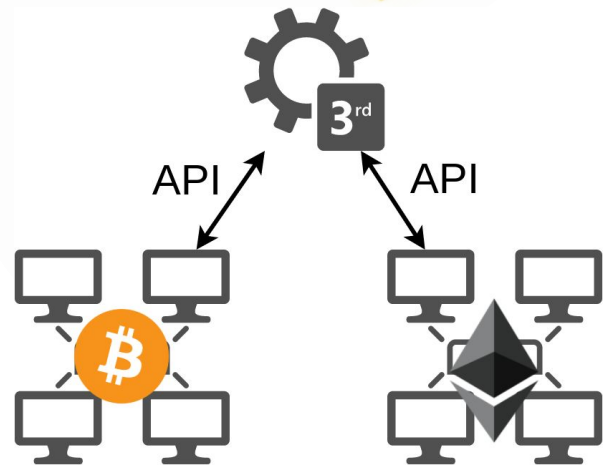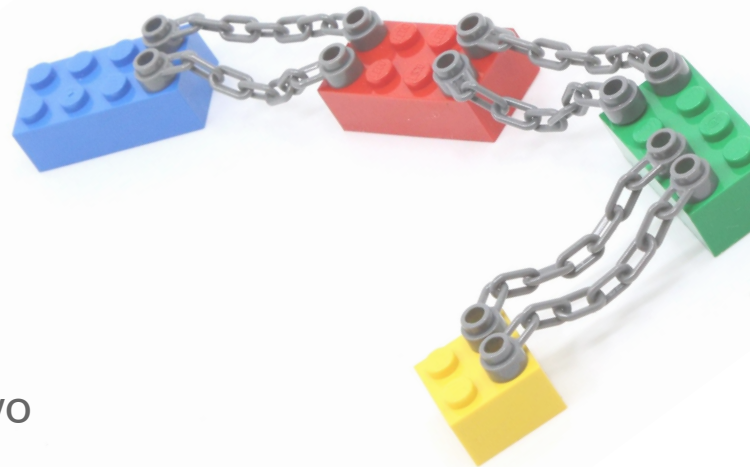- Smart contracts can trigger operations on other chains

Notary schemes

A trusted party, notary, is able to interact with two chains, X and Y

- Example: a listener fires a callback on X when detects a particular event on Y

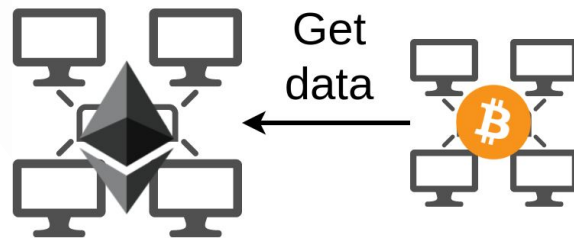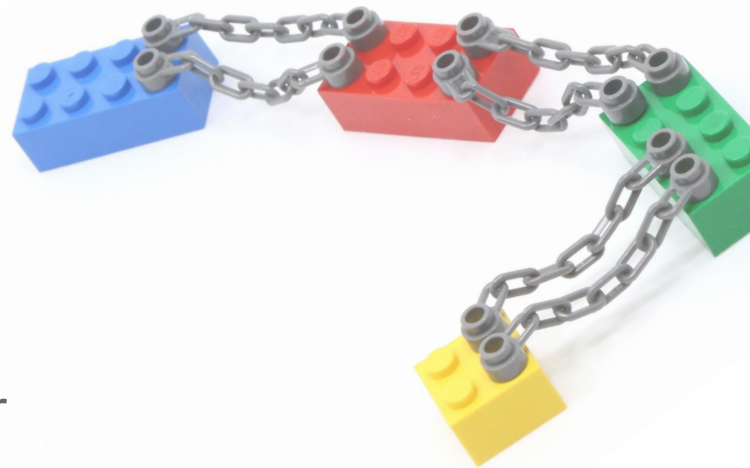Most intuitive approach, but introduces a single point of failure

Side-chains

A chain can validate the state transitions of other chains

This approach is hard to achieve: it requires a blockchain, a self-contained system, to access to the outside world
- Otherwise, the input data must be provided by an external user
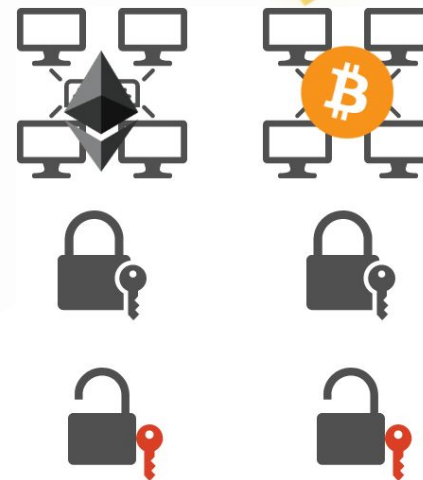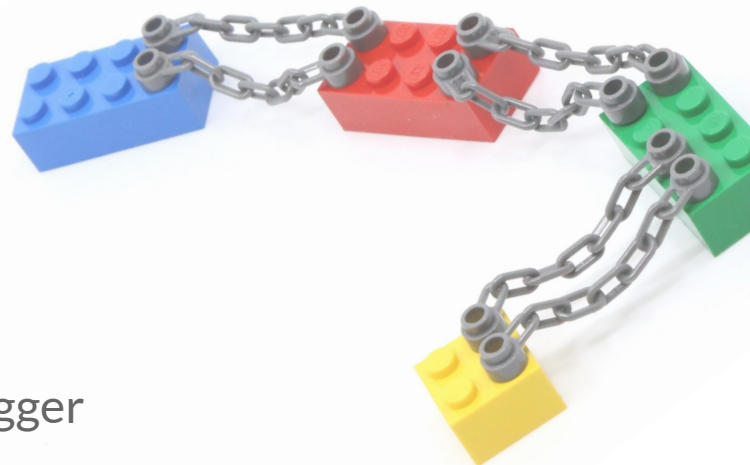
Get data

Hash locking

Operations on different chains have the same trigger
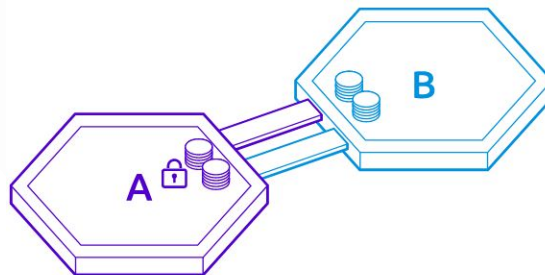
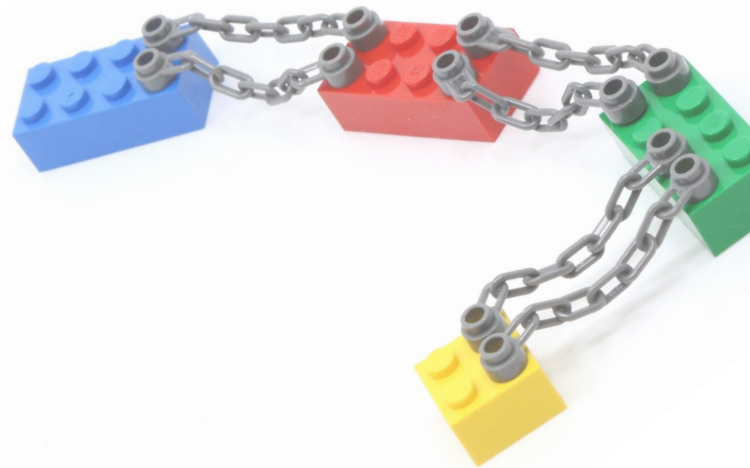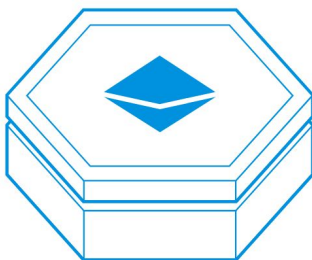- Typically, the preimage of an hash value

This approach is easy to implement and does not require external data

- But its applicability is limited with respect to the other approaches

Connecting chains

Images from:

https://cosmos.network/intro
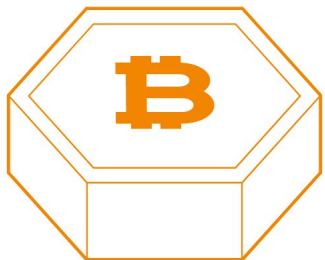
Future steps

Investigate more in depth the approaches and the use cases

Propose an interoperability solution for a particular use case, either modifying an existing technology (if feasible) or provide an original proof of concept
- In the past I worked on a notary scheme solution
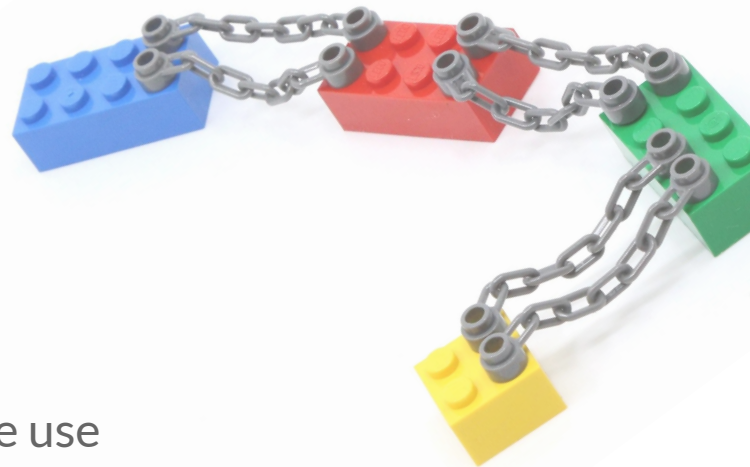
Thank you!
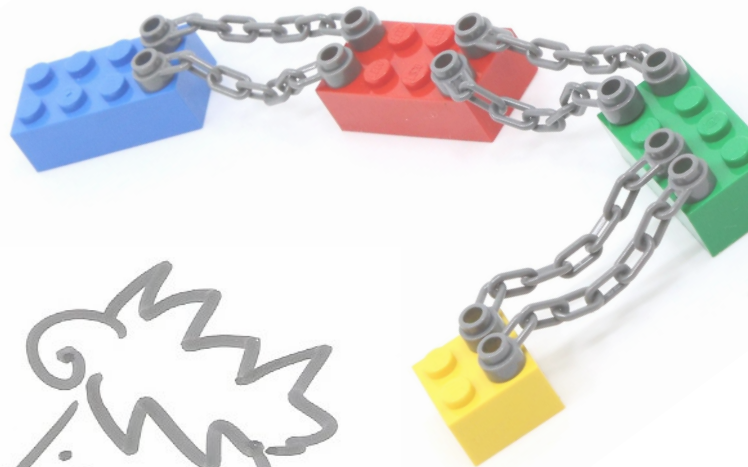
References - Bitcoin

Bitcoin: A peer-to-peer electronic cash system, S Nakamoto

https://bitcoin.org/en/blockchain-guide

Mastering Bitcoin, M. Antonopoulos
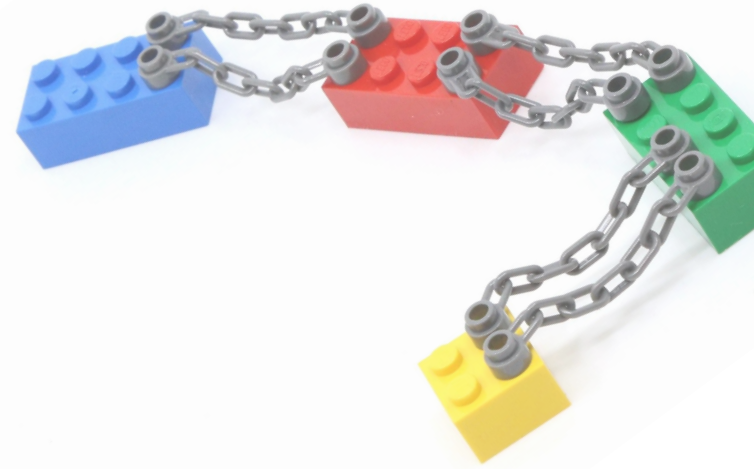
References - Ethereum

Ethereum: A secure decentralised generalised transaction ledger, G Wood

https://blog.openzeppelin.com/ethereum-in-depth-part-1-968981e6f833/

A survey of attacks on ethereum smart contracts, N. Atzei, M. Bartoletti T. Cimoli

References - Interoperability

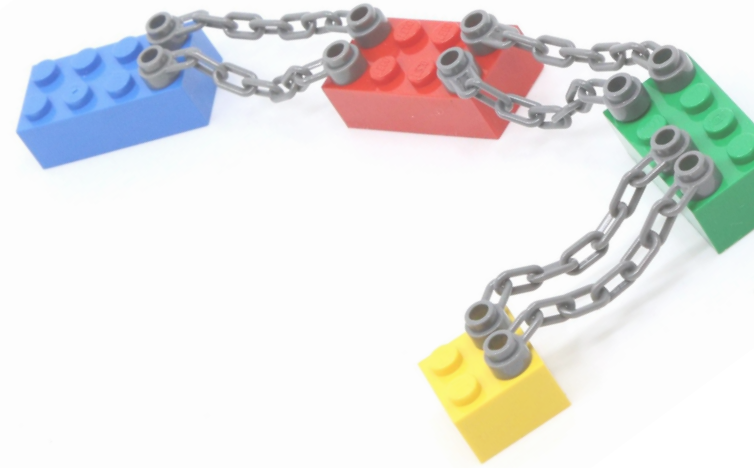**Chain Interoperability**, V. Buterin

Assessing interoperability solutions for distributed ledgers, T. Koens , E. Poll

Anonymous Multi-Hop Locks for Blockchain, G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, M. Maffei

Interledger Approaches, V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, G. C. Polyzos

Atomic Cross-Chain Swaps, M. Herlihy

References - Technology

Bitcoin Lightning Network: https://lightning.network/

BTCRelay (deprecated): http://btcrelay.org/

Cosmos: https://cosmos.network/

Polkadot: https://polkadot.network/

Interledger: https://interledger.org/