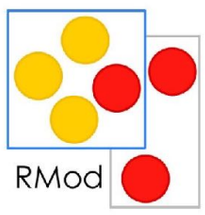
Blockchain & Smart Contracts Crash Course

Santiago Bragagnolo (santiago.bragagnolo@inria.fr)



About Me

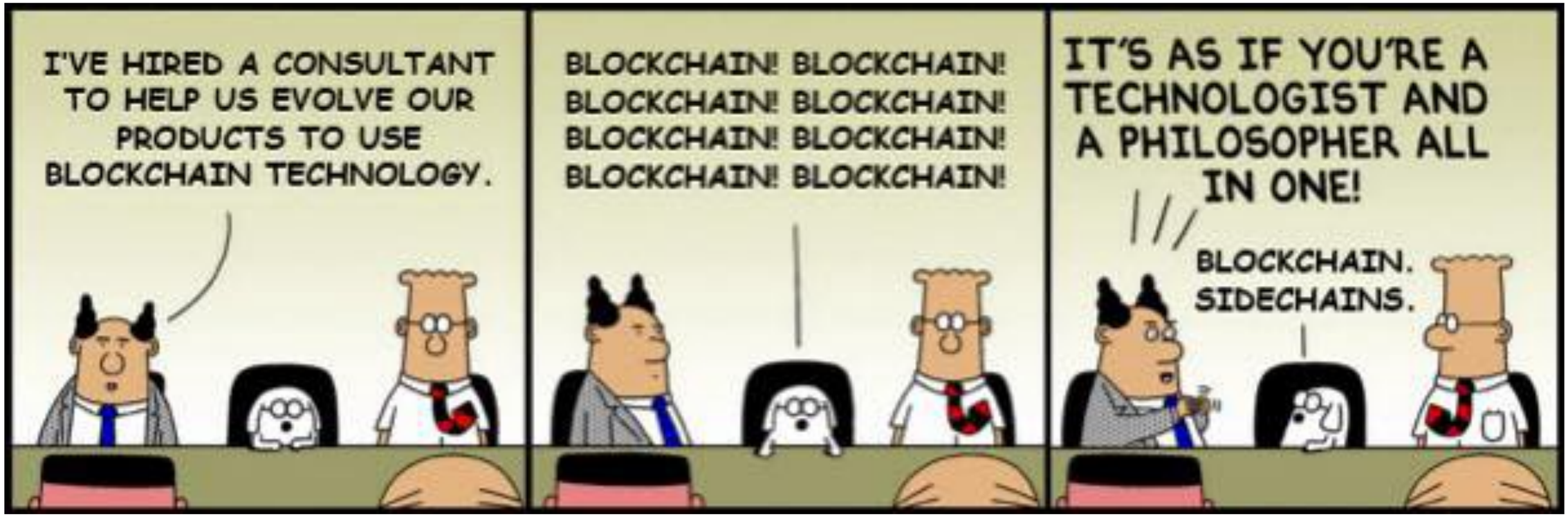
- Santiago Bragagnolo(santiago.bragagnolo@inria.fr)
- Ph.D. Student on Software Migration
- Research Engineer at Inria Lille (France, 2015 – 2020)
- Working on blockchain since 2016
- Working in engineering since 2002

Summary (1st part)

- Introduction
- General Structure
- Mining
- Smart Contracts
- Some contributions from our team

Introduction


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
S. Adams E-mail: SCOTTADAMS@AOL.COM
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.
© 1995 United Feature Syndicate, Inc.(NYC)


I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN. SIDECHAINS.

What is Blockchain?

Examples of Blockchain Technologies

What is Blockchain?
From an User's Perspective

- An open distributed Ledger

GENERAL LEDGER

ACCOUNT NAME: Cash

ACCOUNT NUMBER: 001

DATE	DESCRIPTION	JOURNAL #	DEBIT	CREDIT	BALANCE
4/20/2015	Check from friend	J1	$ 500.00		$500.00
4/21/2015	*Paying a friend*	J1		$ 200.00	$300.00

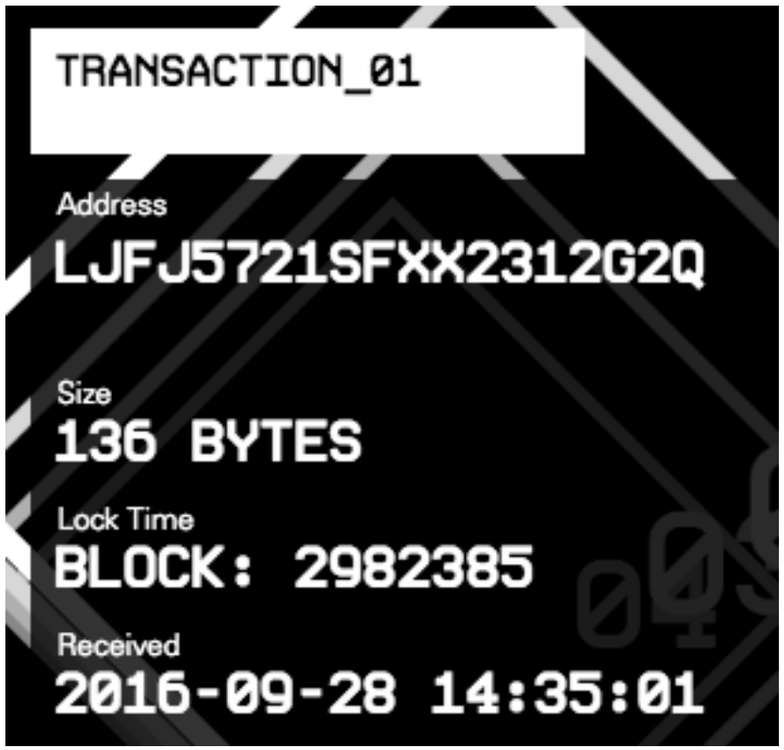
What is Blockchain?
From an User's Perspective

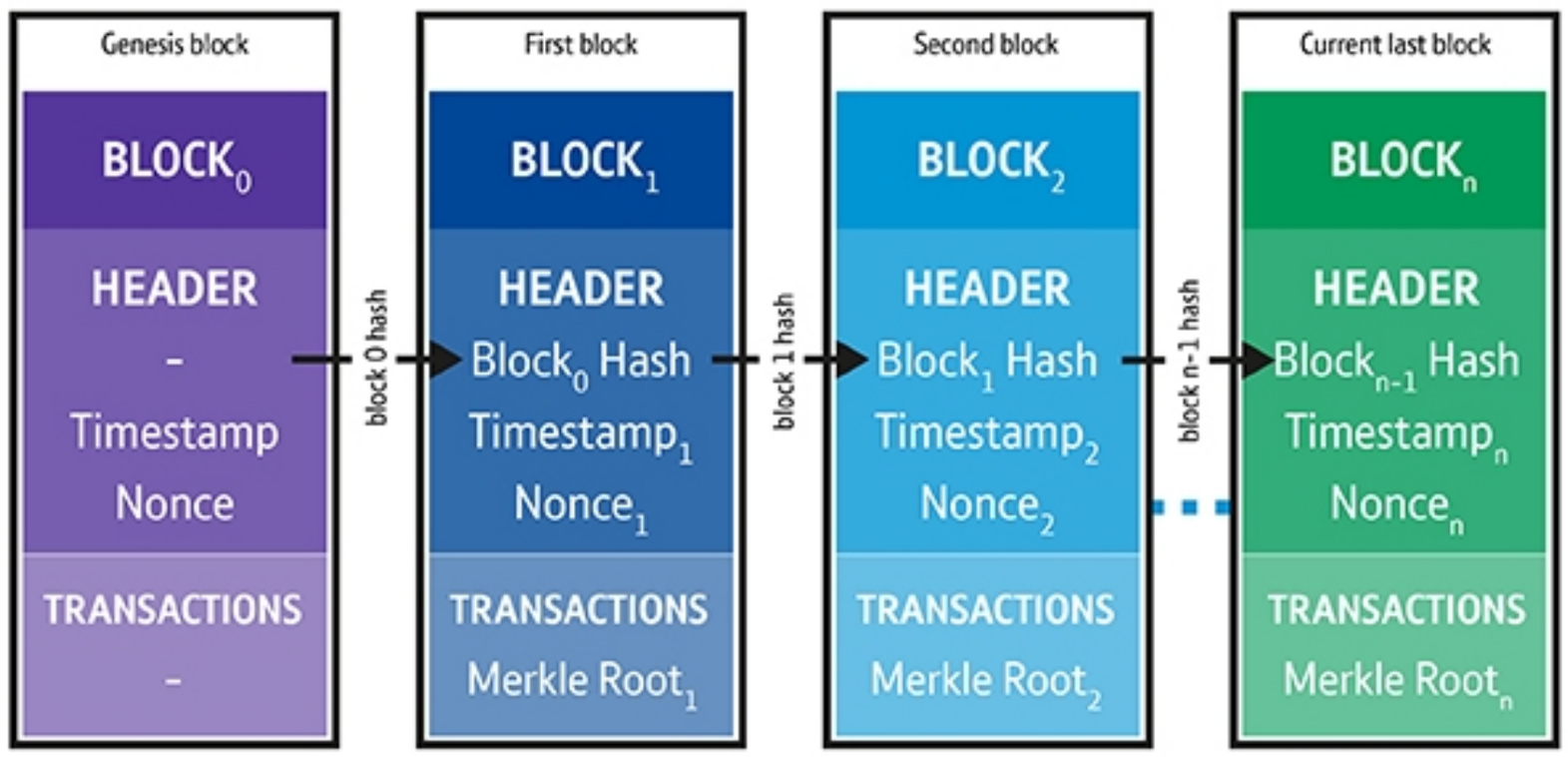
- An open distributed Ledger
- Ledger - Records transactions (BitCoin, Ether).
- Open - anyone can participate
- Distributed - shared and synchronized among several "people"

What is Blockchain?

From a Developer's Perspective

- Roughly, an append-only distributed transactional database





What is Blockchain?
From a Developer's Perspective

- Roughly, an append-only distributed transactional database
  - Database
  - Transaction
  - Append-only
  - Distributed

Structure

Account

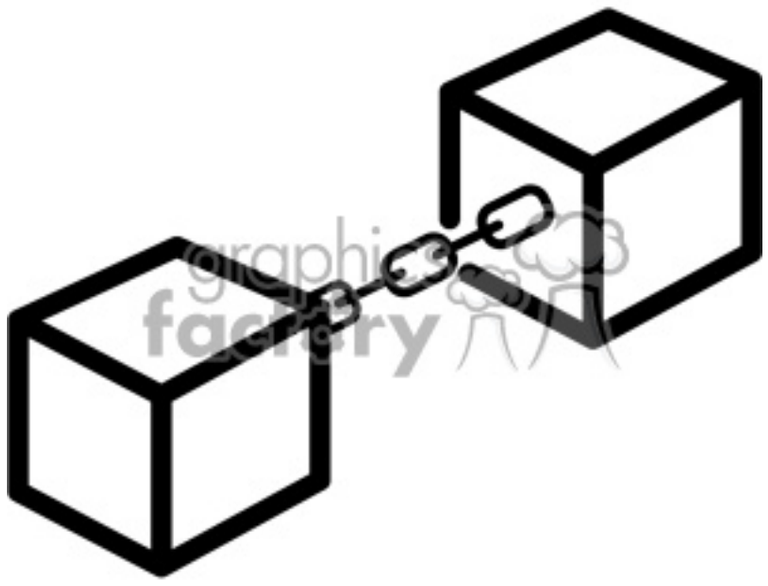
- We need an account to interact with the blockchain
- Roughly, an account's id/address is a public key and whoever holds the private key owns it.
- For example see: <https://etherscan.io/accounts>

Transactions

A transaction is an operation that changes something on the blockchain.

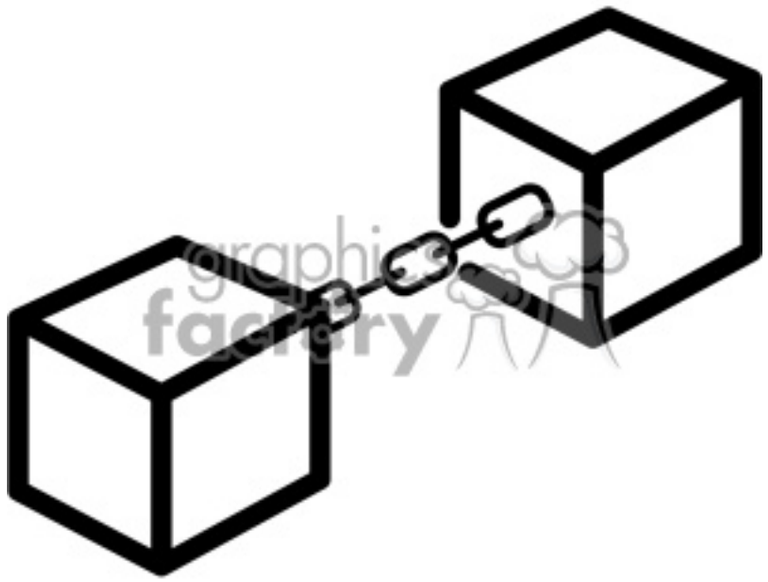
The information on transactions is public to everyone on the blockchain.

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	25
0x22…	0x9E…	0x2F…	0
0xC3…	0x9E…	0x77…	7



Blocks

- A block is storage unit in the blockchain database
- Transactions are bundled into a block
- Is linked to the previous block
- It contains a timestamp



Blocks

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	25
0x22…	0x9E…	0x2F…	0
0xC3…	0x9E…	0x77…	7

Block 245452

Hash
0xd015f8981f292616e74…3b249b9a9240

TimeStamp
2019-10-01T09:13:49.663753+02:00

Previous block
0xf8bc8ede2727cce01b4…bda50490bd90

Nonce
0x3afc82ca9063c17e

Transactions

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	25
0x22…	0x9E…	0x2F…	0
0xC3…	0x9E…	0x77…	7

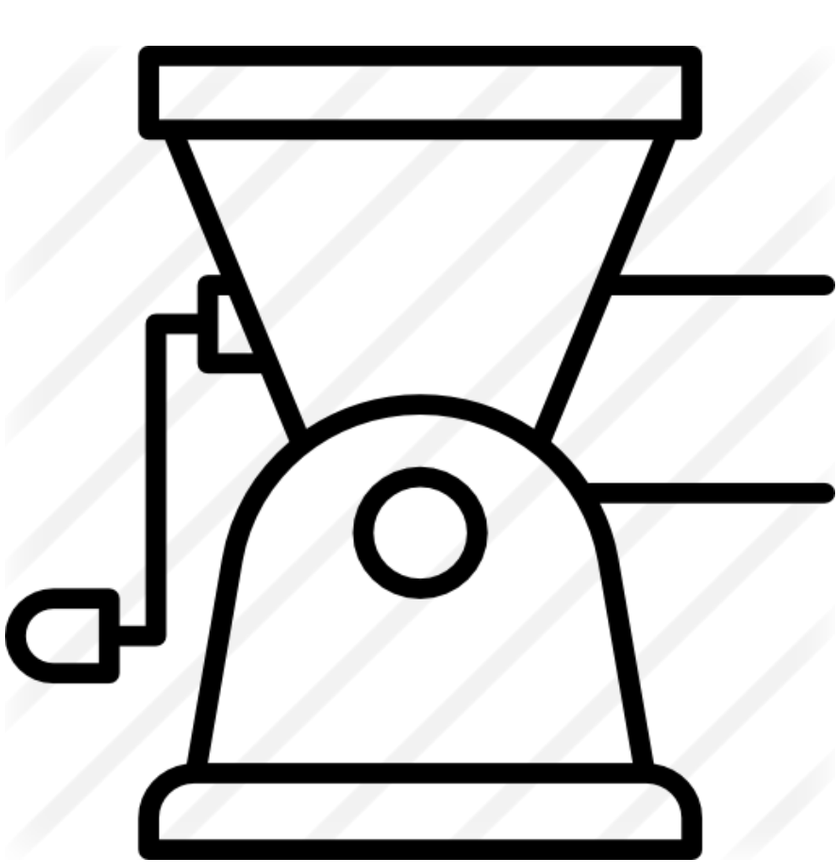
How are the Blocks Linked?

Previous block
0xf8bc8ede2727cce01b4…bda50490bd90

TimeStamp
2019-10-01T09:13:49.663753+02:00

Nonce
0x3afc82ca9063c17e

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	25
0x22…	0x9E…	0x2F…	0
0xC3…	0x9E…	0x77…	7

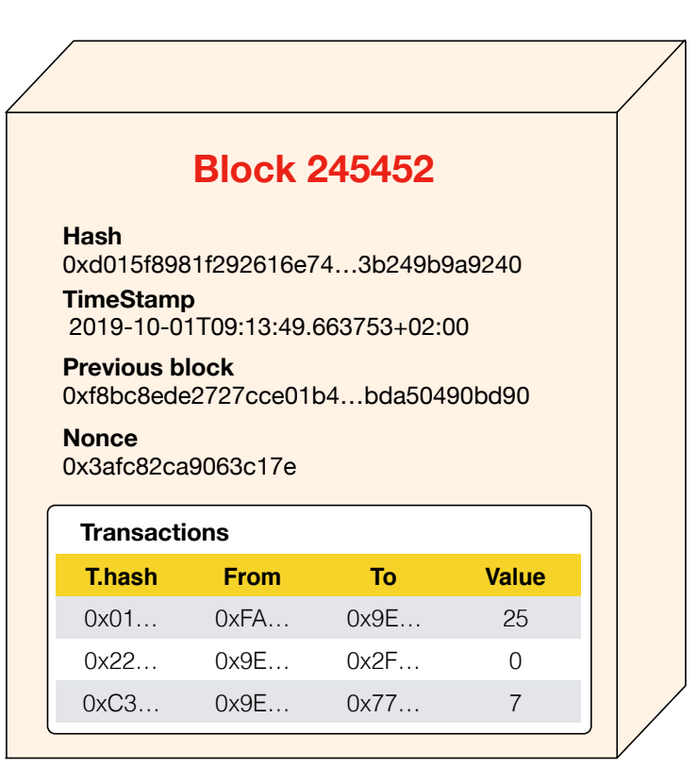


HASH

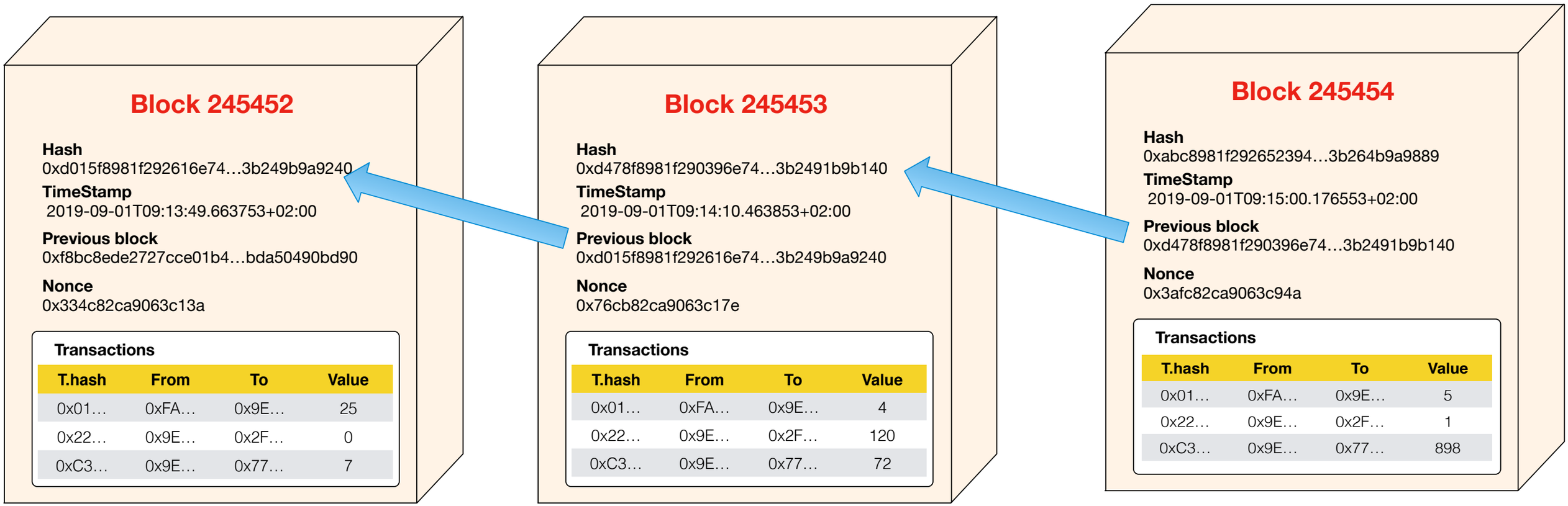
0xd015f8981f292616e74…3b249b9a9240

How are the Blocks Linked?

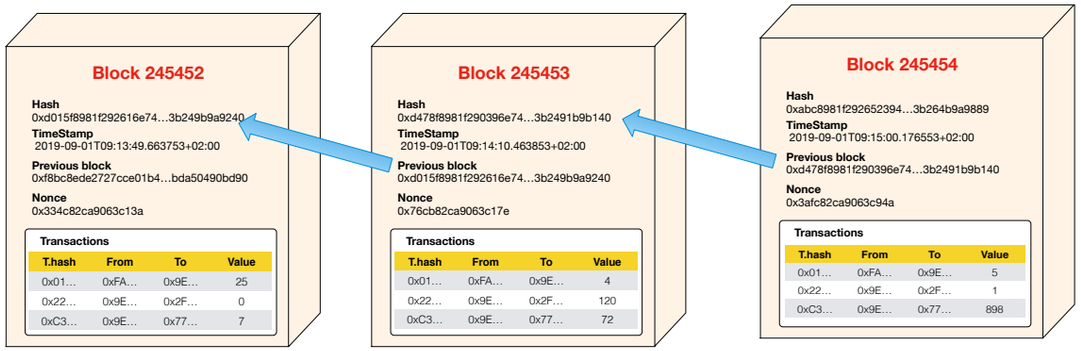
- The blocks are linked by a Hash number computed over the body of the block
  - Previous block's hash
  - The timestamp
  - The transactions
  - The nonce



Linking Blocks Example



Linking Blocks Example

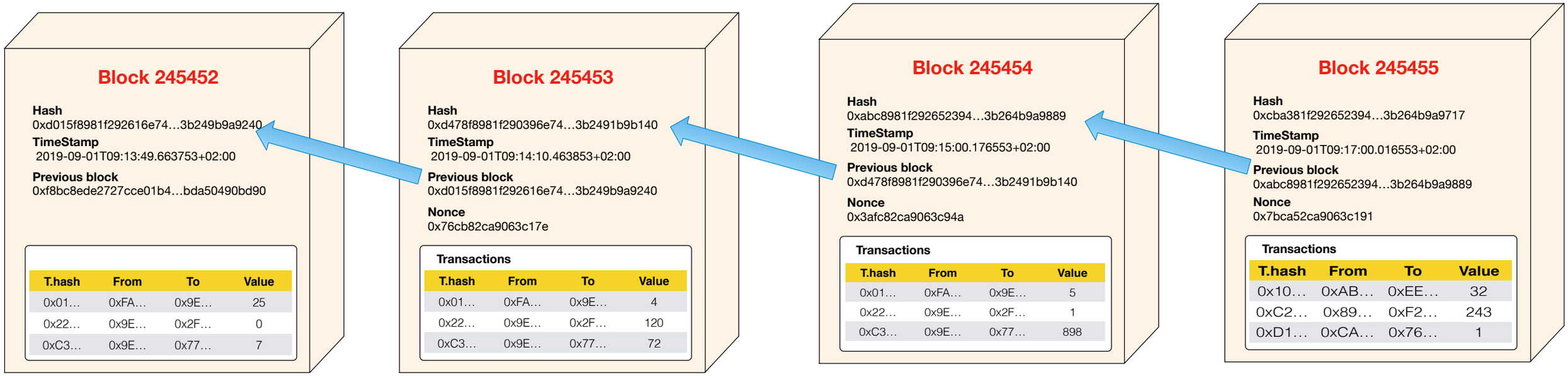


TimeStamp
2019-09-01T09:17:00.016553+02:00

Previous block
0xabc8981f292652394…3b264b9a9889

T.hash	From	To	Value
0x10…	0xAB…	0xEE…	32
0xC2…	0x89…	0xF2…	243
0xD1…	0xCA…	0x76…	1

Linking Blocks Example



What if…  Someone Tampers the Blocks?

- For manually rollback an error
- For modify a transaction with malicious intentions

Tampering Blocks

Block 245453

Hash
0xd478f8981f290396e74…3b2491b9b140

TimeStamp
2019-09-01T09:14:10.463853+02:00

Previous block
0xd015f8981f292616e74…3b249b9a9240

Nonce
0x76cb82ca9063c17e

Transactions

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	4
0x22…	0x9E…	0x2F…	120
0xC3…	0x9E…	0x77…	72

Block 245454

Hash
0xabc8981f292652394…3b264b9a9889

TimeStamp
2019-09-01T09:15:00.176553+02:00

Previous block
0xd478f8981f290396e74…3b2491b9b140

Nonce
0x3afc82ca9063c94a

Transactions

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	5
0x22…	0x9E…	0x2F…	1
0xC3…	0x9E…	0x77…	898

Tampering Blocks

Block 245453

Hash
0xd478f8981f290396e74…3b2491b9b140

TimeStamp
2019-09-01T09:14:10.463853+02:00

Previous block
0xd015f8981f292616e74…3b249b9a9240

Nonce
0x76cb82ca9063c17e

Transactions

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	4
0x22…	0x9E…	~~0x2F…~~ 0x49…	120
0xC3…	0x9E…	0x77…	72

Block 245454

Hash
0xabc8981f292652394…3b264b9a9889

TimeStamp
2019-09-01T09:15:00.176553+02:00

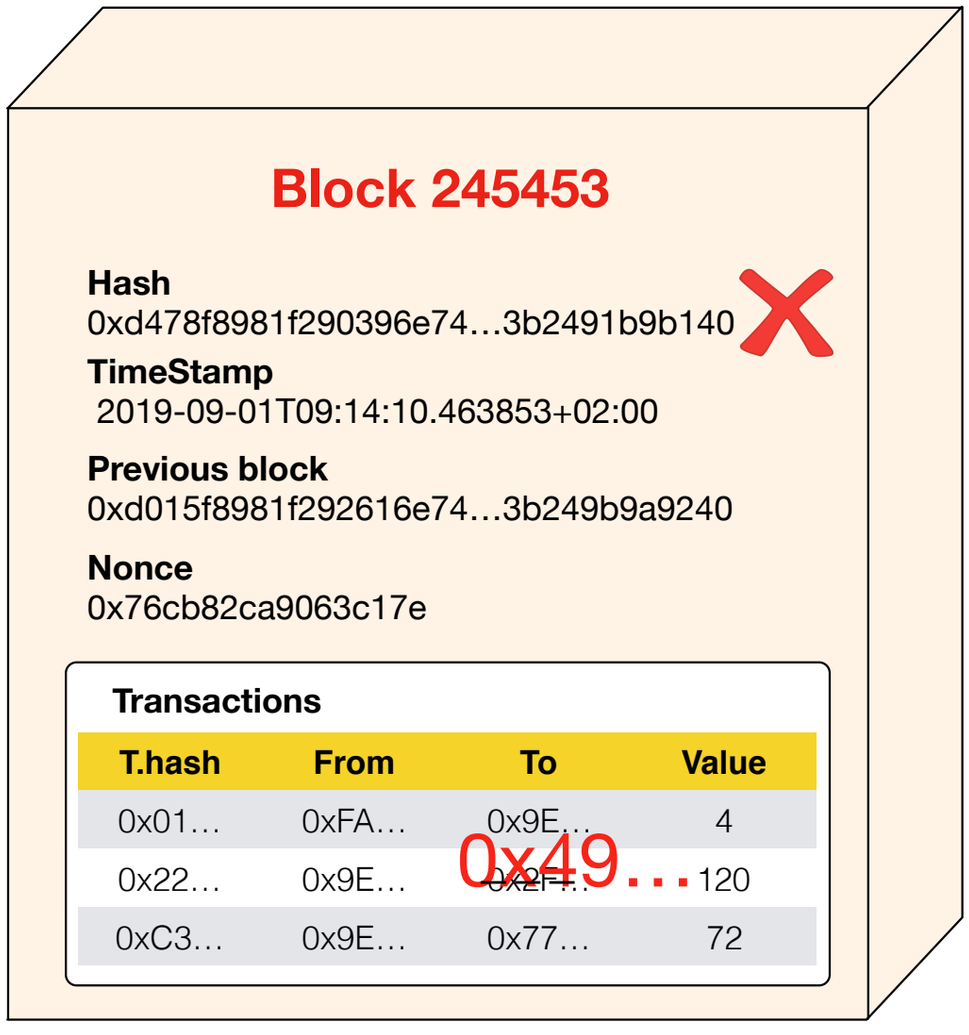
Previous block
0xd478f8981f290396e74…3b2491b9b140

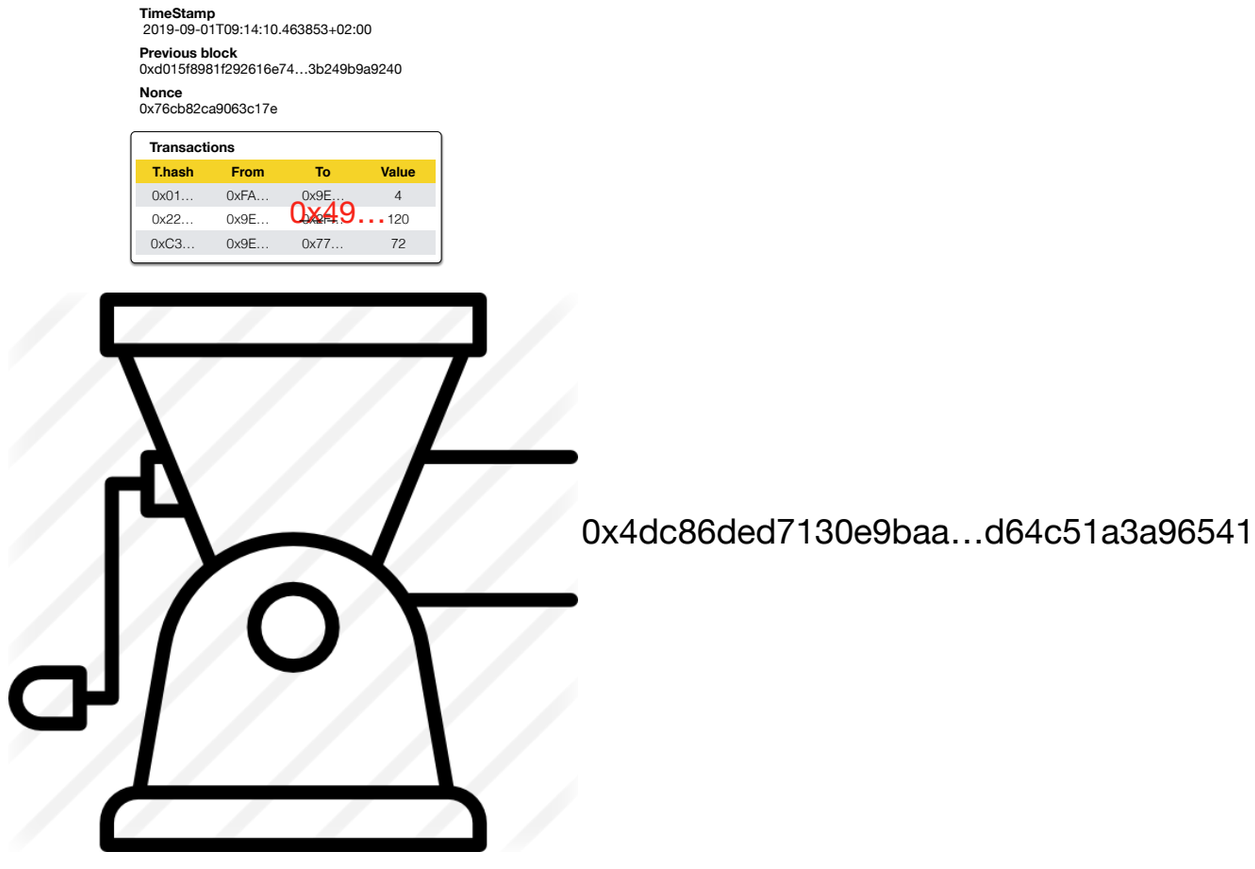
Nonce
0x3afc82ca9063c94a

Transactions

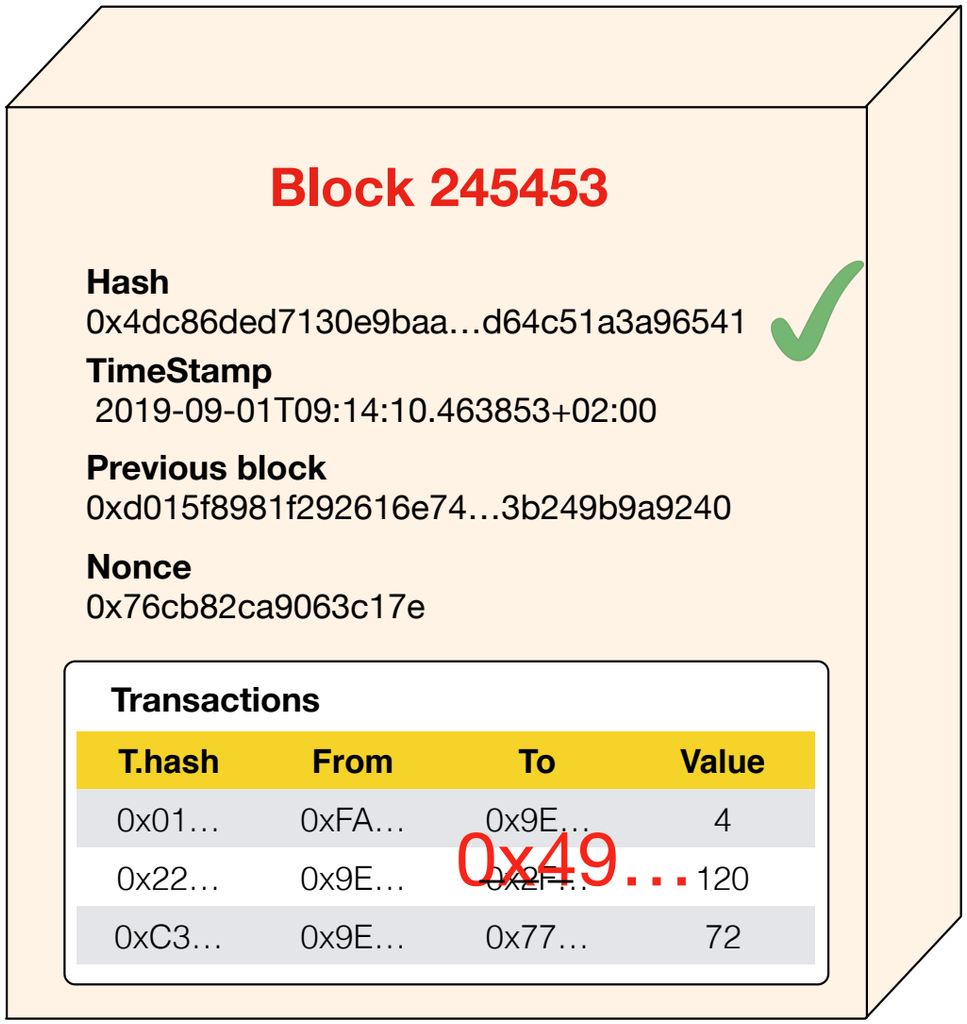
T.hash	From	To	Value
0x01…	0xFA…	0x9E…	5
0x22…	0x9E…	0x2F…	1
0xC3…	0x9E…	0x77…	898

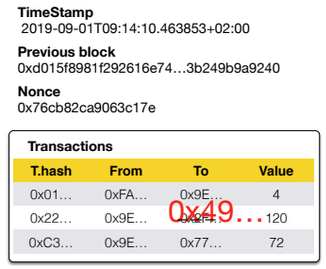
Verification Process

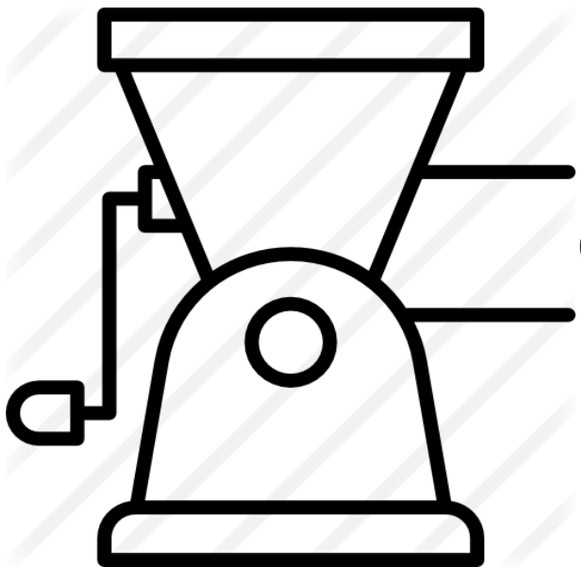




Verification Process

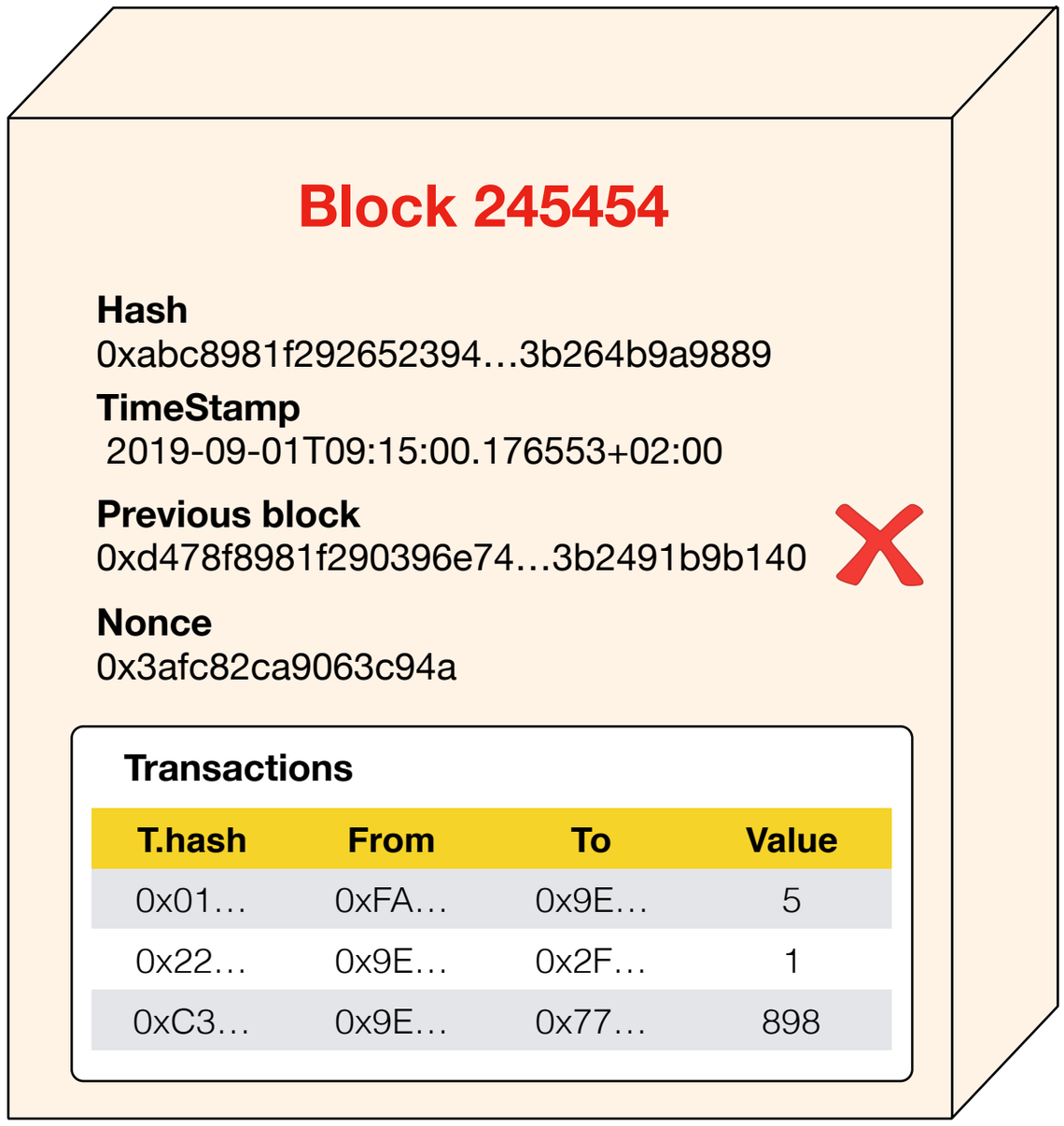






0x4dc86ded7130e9baa…d64c51a3a96541

Verification Process



Cool but…
what is it good for?

Ensure traceability

Trustless Trust

The transactions/blocks are verified by every node (trustless).

This ensures the approved transactions/block are legit (promoting trust).

And allows entities to interact without a trusted 3rd party.

Mining

Mining

- To Mine is the process of creating a valid block and adding it to the blockchain

- A Miner is someone who mines the blockchain.

- A miner that creates a valid block, earns the right of acquiring a parametrisable amount of cryptocurrency

What is a valid block?

What is a valid block?

One that is accepted by the consensus algorithm of the network

Consensus algorithms

- Verify / accept modifications
- Ensure that the miner has something to lose

Consensus algorithms

Verify / accept modifications

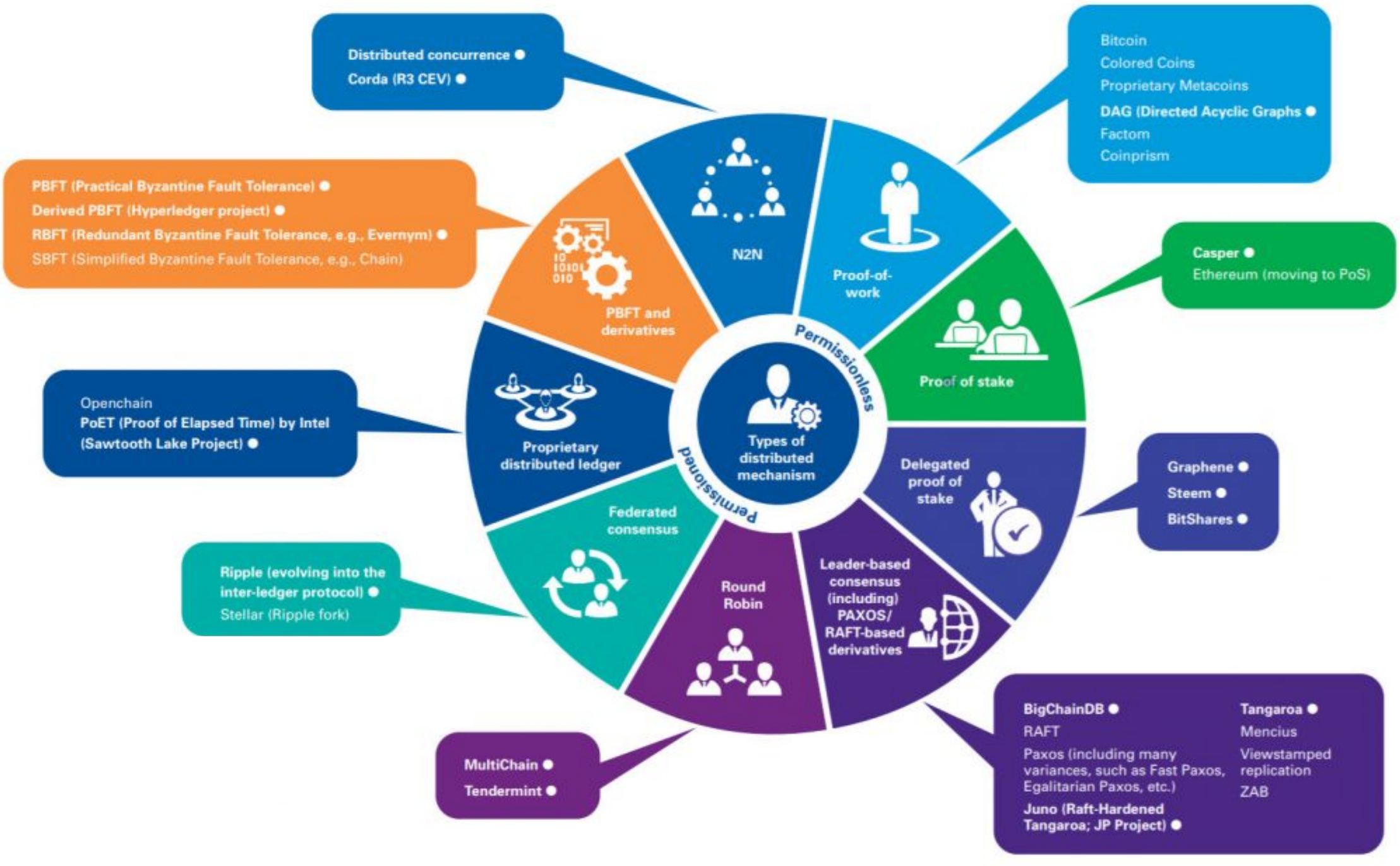
- Verify block hashes
- Verify non-double spent
- Verify transactions consistency

Consensus algorithms

Ensure that the miner has something to lose

- Ensure that the miners do not complot for modifying history
- Ensure that the miners do not have parasitic behaviours

Consensus algorithms



Proof of work

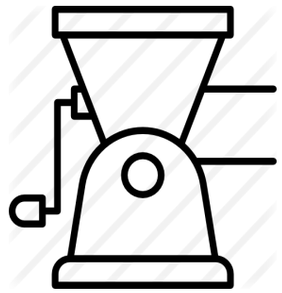
- Requires the resolution of a crypto-puzzle
- Ensures the economic engagement of the miners
- Super high energy consumption

Proof of work: The puzzle

Hash
0xabc8981f292652394…3b264b9a9889
TimeStamp
2019-09-01T09:15:00.176553+02:00
Previous block
0xd478f8981f290396e74…3b2491b9b140
Nonce
0x3afc82ca9063c949

Transactions

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	5
0x22…	0x9E…	0x2F…	1
0xC3…	0x9E…	0x77…	898

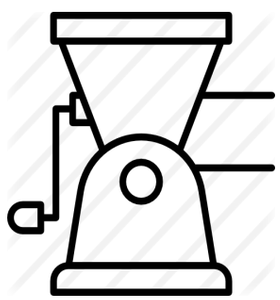


0x03bcaced7130e9baa…d64c51a3a96541

Hash
0xabc8981f292652394…3b264b9a9889
TimeStamp
2019-09-01T09:15:00.176553+02:00
Previous block
0xd478f8981f290396e74…3b2491b9b140
Nonce
0x3afc82ca9063c949 0x3afc82ca9063c94a

Transactions

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	5
0x22…	0x9E…	0x2F…	1
0xC3…	0x9E…	0x77…	898

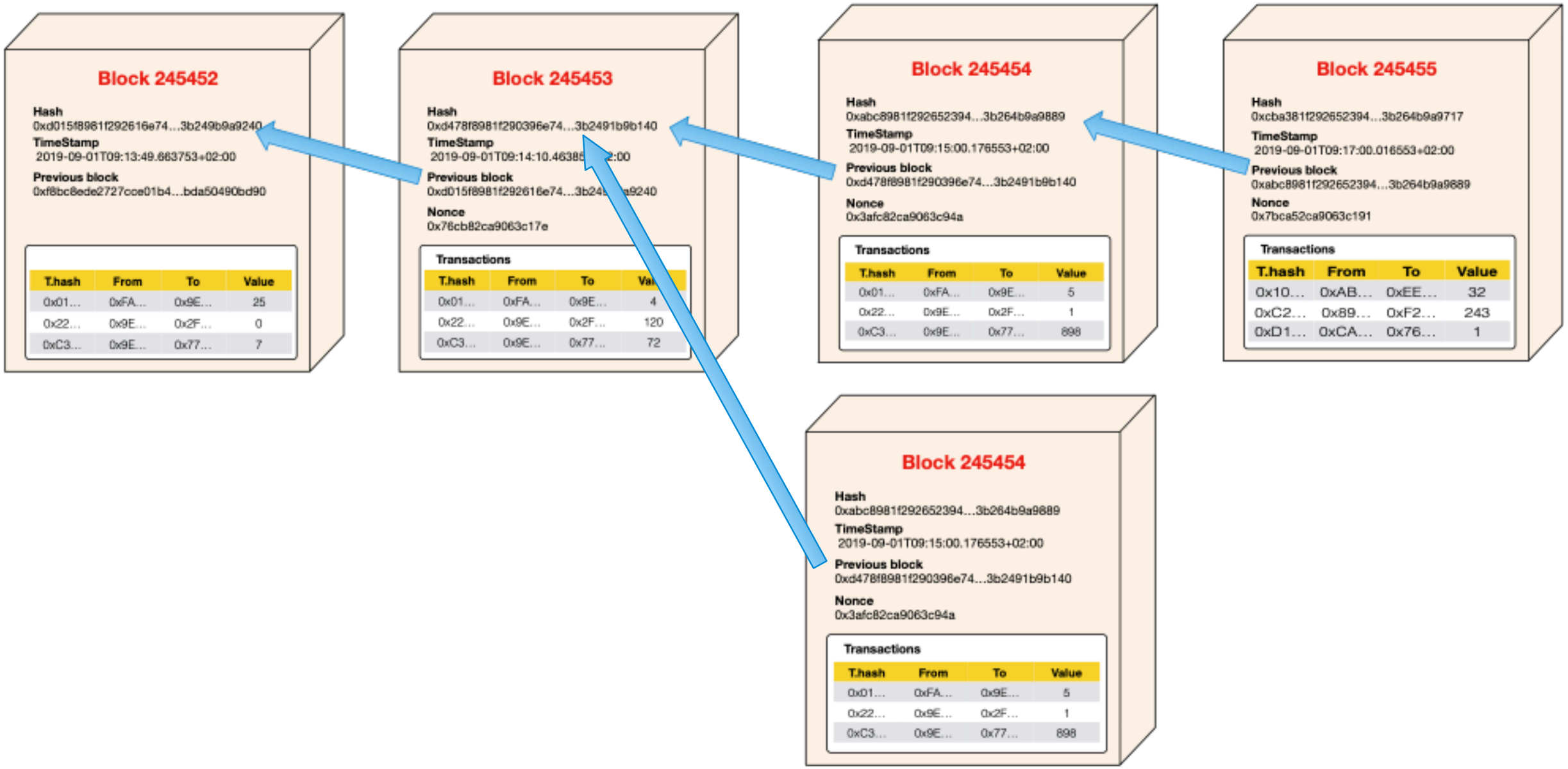


0x000000ed7130e9baa…d64c51a3a96541

What is a valid blockchain?

The longest chain

The longest chain



The longest chain

- Ensures that tampering is near impossible
- Chooses the chain that most of the users is using for

Brief Blockchain

Brief

- P2P Open Network
- Transactional Append only database
- Administrated and surveilled by an engaged community
- Rules defined by a consensus algorithm

Smart Contracts

Smart Contracts

[Fritz Henglein, Smart Contracts…, 2017]

- "Smart Contracts are neither Smart nor Contracts"

  - Smart Contracts are self-executing programs coded in complex Turing-complete language.

  - Rules & Actions intermixed (not a contract)

  - Low-level programs hard to analyze (not smart)

Smart Contracts

[Ethereum Doc, 2018]

- Contracts should not be seen as something that should be “fulfilled” or “complied with”

- They are more like “autonomous agents” that live inside the blockchain

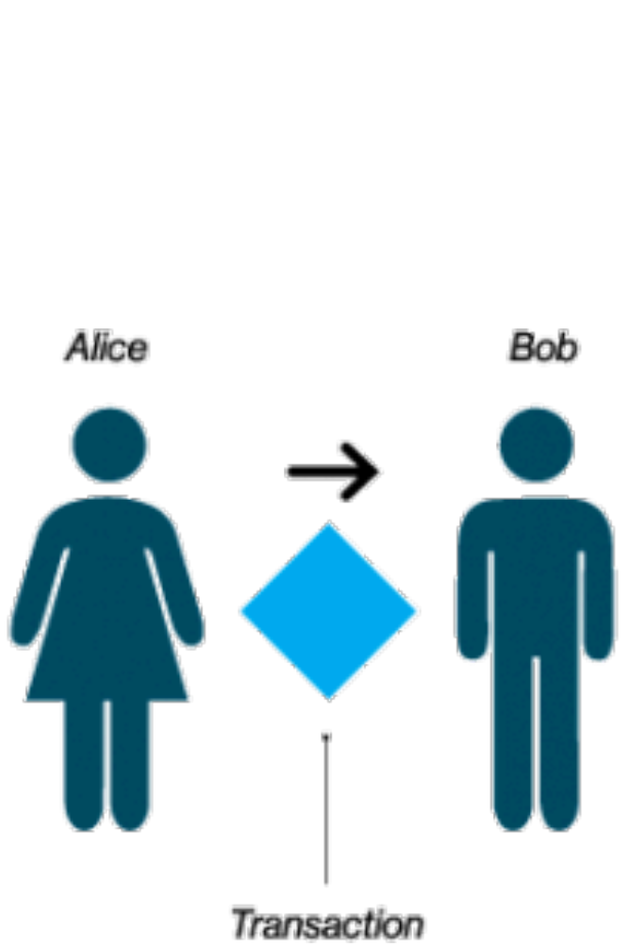
- Executing a specific piece of code when “poked” by a message or transaction

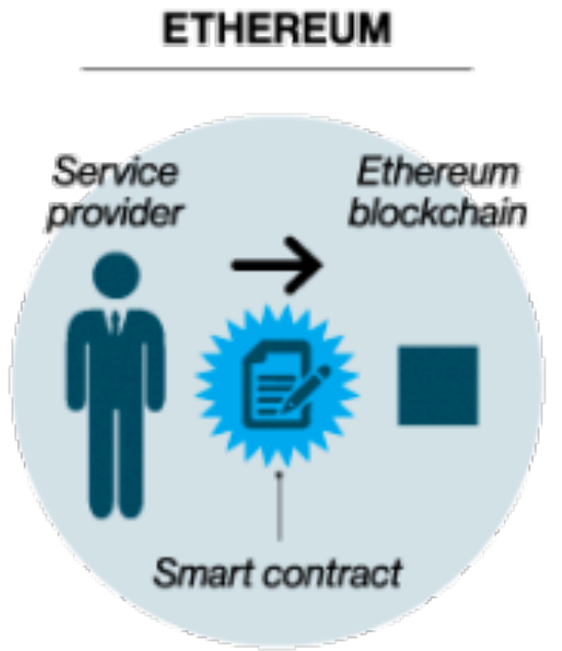
- Have direct control over their cryptocurrency and attributes to store their permanent state.

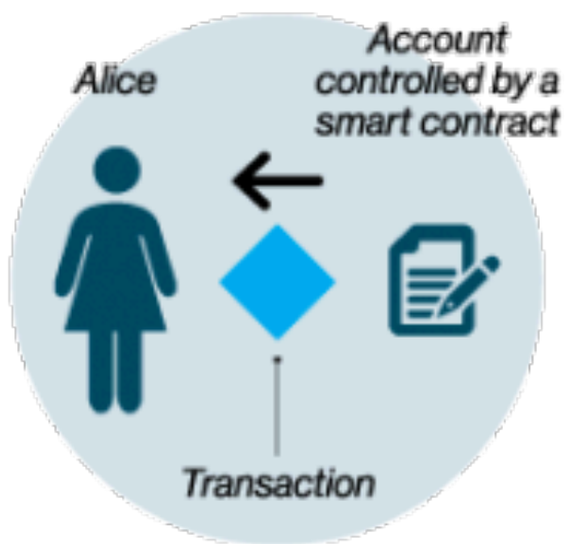
Contract Ex: Pair Storage

```
1  pragma solidity^0.4.24;
2  /**
3   * @title Simple Pair Storage contract
4   * @author Henrique
5   */
6  contract SimplePairStorage{
7      int private data1;
8      uint data2;
9
10     function setData(int _data1, uint _data2) public {
11         data1 = _data1;
12         data2 = _data2;
13     }
14
15     function getData() public view returns(int,uint){
16         return (data1,data2);
17     }
18 } //end of contract
```

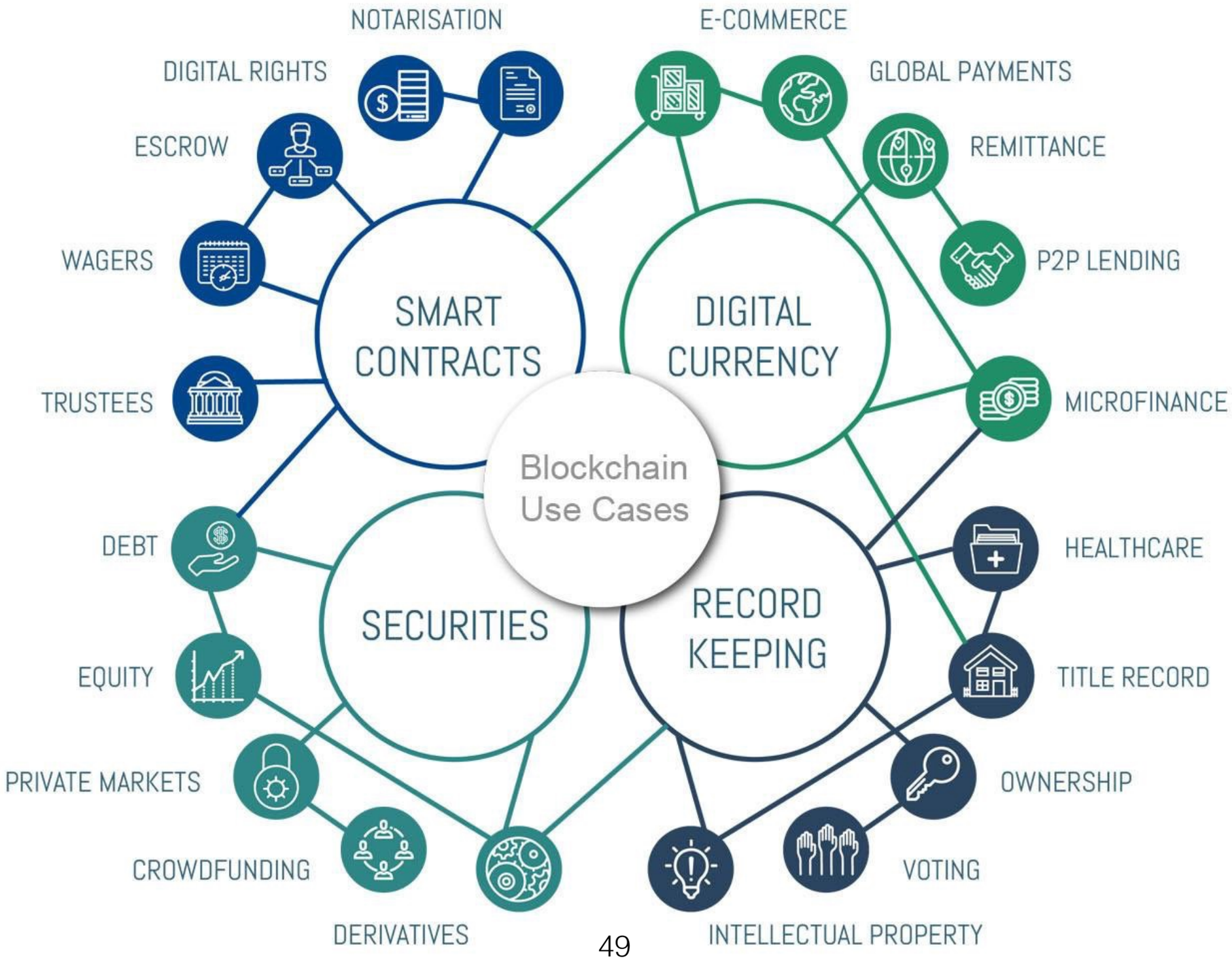
Diagram Contract Interaction







Blockchain Use Cases



50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION

Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS

The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE

A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION

The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS

IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM

HYPERLEDGER

ENTERPRISE

Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL

Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS

IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM

Walmart

HEALTHCARE

A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING

Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE

Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

PROPY

ENERGY

Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY

Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION

Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING

New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL

Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM

Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT

Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY

Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC. Louis Dreyfus Company

DIAMONDS

The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

De Beers Group of Companies

FINE ART

By storing **certificates** of authenticity on the blockchain, it's possible to dramati- cally reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY

For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM

In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION

In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY

Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS

Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

грузовая компания НОВОТРАНС

ENTERPRISE

Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google

Alphabet

MUSIC

Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

FISHING

Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

Blockchain Research

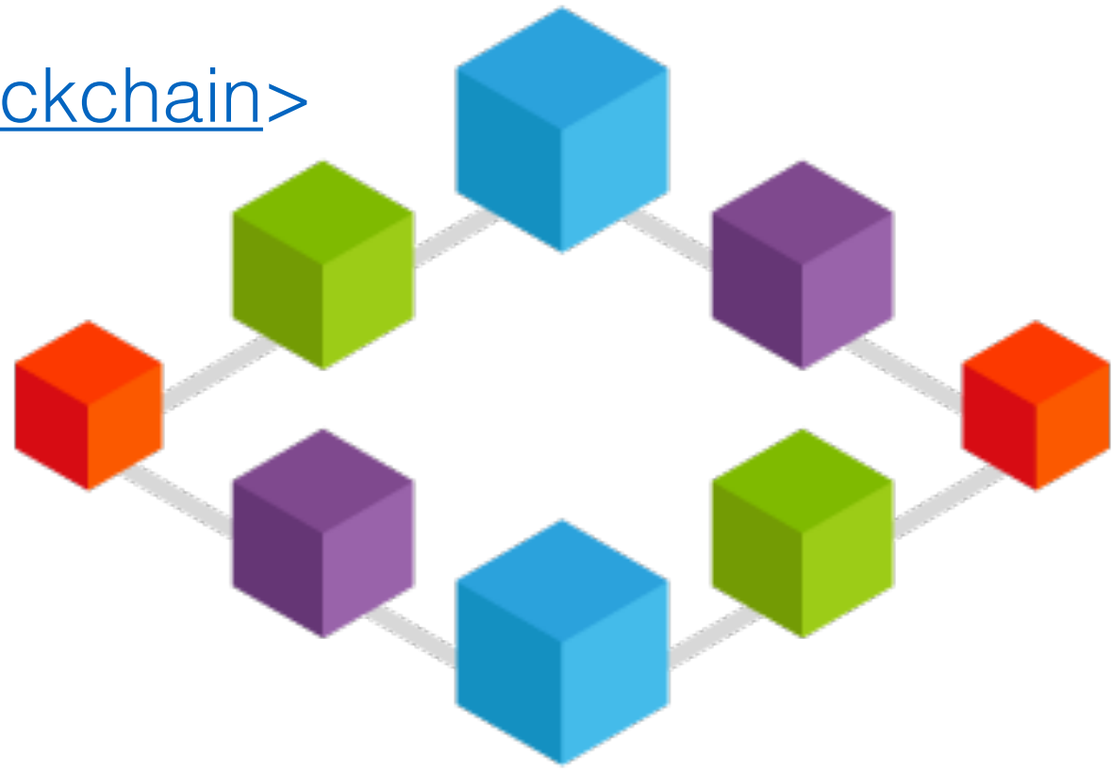
Rmod

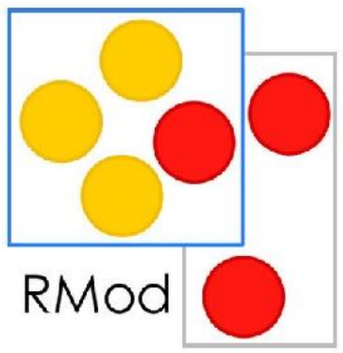
We welcome any research idea you may have for us.

We are also open to industrial and academic partnerships to advance blockchain research.

<https://github.com/RMODINRIA-Blockchain>

<https://rmod.inria.fr/web>



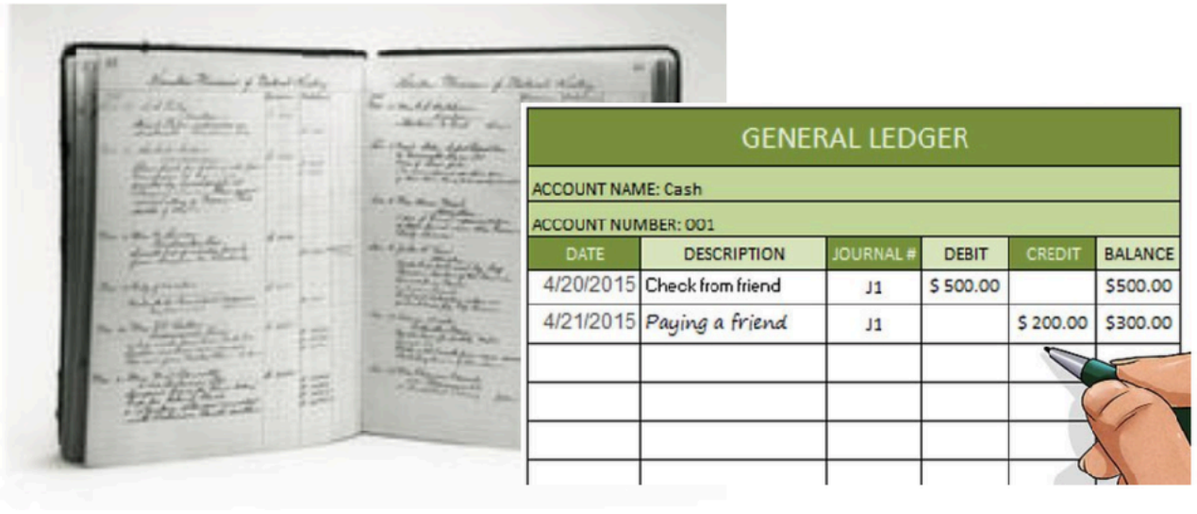


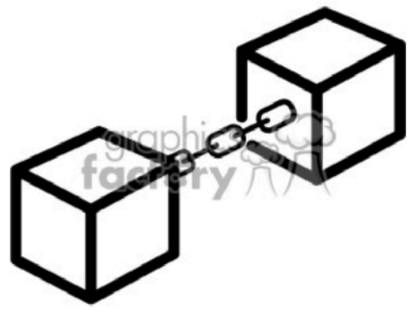
Rmod

- SmartInspect: Contract internal state inspector
- EQL: query language for Ethereum blockchain
- SmartMetrics: Metric suite for contracts
- SolVis: Visualization tool for Solidity contracts
- BcModel: Modeling tools
- Business process Orchestration

What is Blockchain?
From an User's Perspective

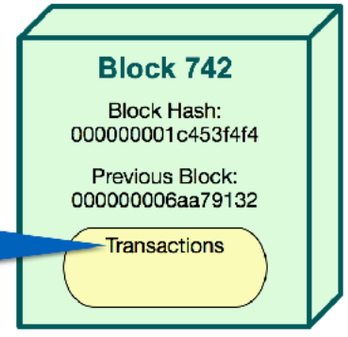
- An open distributed Ledger that promotes privacy





Blocks

T.hash	From	To	Value
0x01…	0xFA…	0x9E…	25
0x22…	0x9E…	0x2F…	0
0xC3…	0x9E…	0x77…	7



Blockchain Use Cases

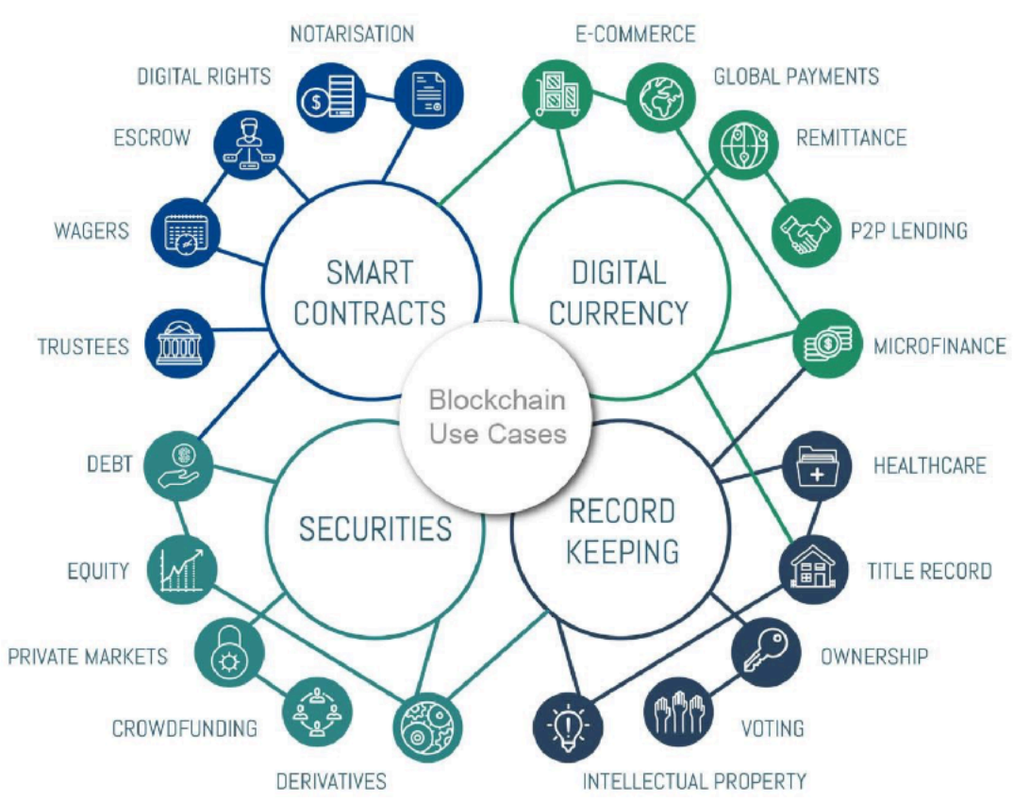
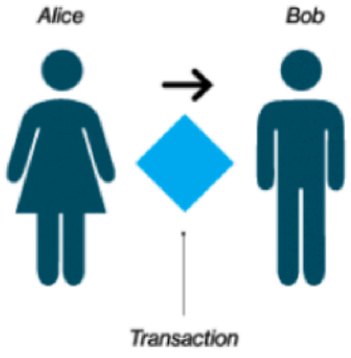
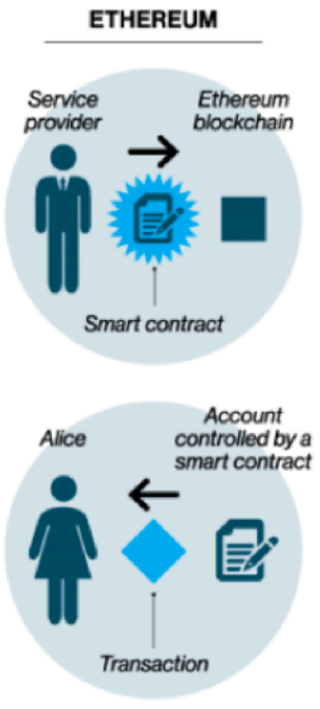


Diagram Contract Interaction





Thanks… questions?

Break :)