Co-funded by the Erasmus+ Programme of the European Union

Pathway in Enterprise Systems Engineering (PENS)

Blockchain: history, technology, and applications

Salvador Sanchez-Alonso – Univ. de Alcala

6/June/2022

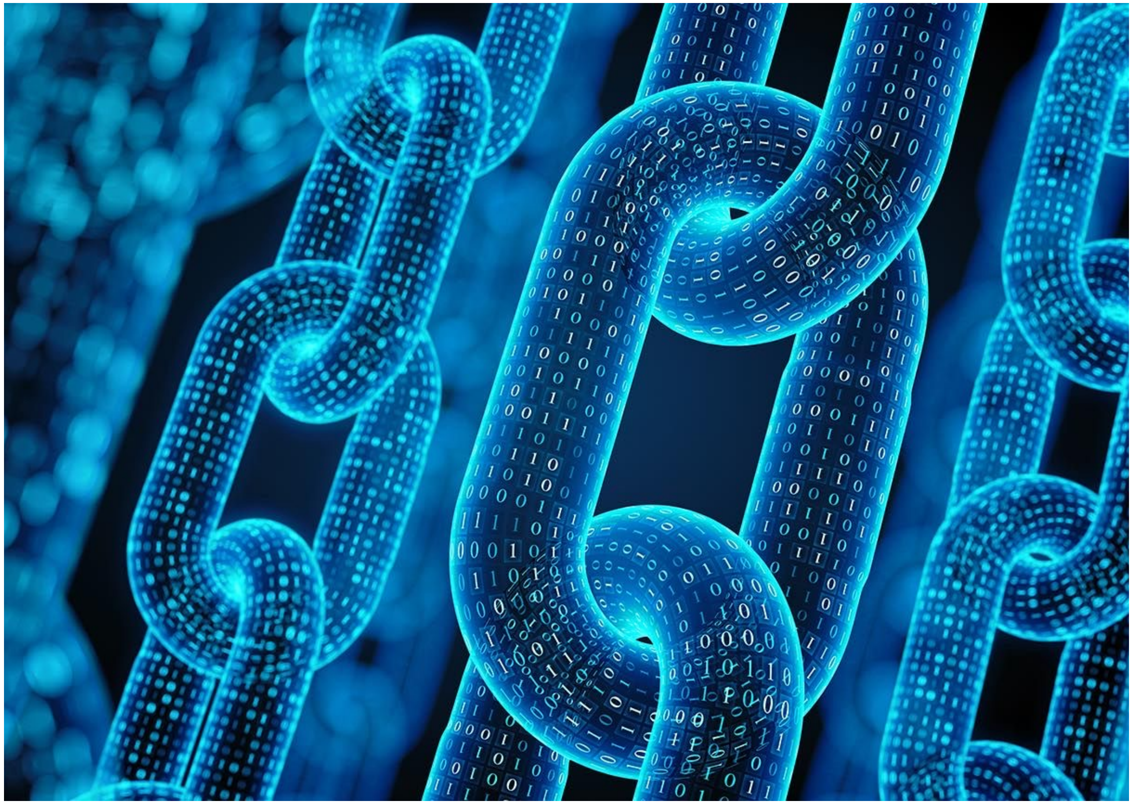
Birzeit University, Ramallah, Palestine

جامعة بيرزيت
BIRZEIT UNIVERSITY
Middlesex University London
Universidad de Alcalá
جامعة القدس
Al-Quds University
ASD
جامعة سوسة
University of Sousse
1986
UNIVERSITE DE MONASTIR
PROXYM GROUP

What this talk will cover

- What is Blockchain
- A Little history: From Bitcoin to the world
- Technical details: From blocks to blockchains
- Types
- Governance
- Blockchain related concepts
  - Smart contracts
  - Sidechains
  - Oracles
- Ideas for Master theses on blockchain topics

What is a blockchain?



A blockchain is…

- A chain of blocks that contains information
- A distributed ledger open to anyone
- A list of transactions that anyone can view and verify
- A shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a network
- A digital ledger of transactions that is duplicated and distributed across an entire network of computer systems
- A distributed approach to collecting and maintaining records, allowing for greater degrees of accuracy, transparency, security and immutability than in centralized approaches

Co-funded by the
Erasmus+ Programme
of the European Union

A little bit of history

Bitcoin

- 13 years ago, a programmer operating under the pseudonym Satoshi Nakamoto deployed a piece of code that would change the world forever
- Bitcoin: set of concepts and technologies that make up a digital money ecosystem
  - Mining, blockchain, consensus, cryptography
- bitcoin: monetary unit that allows storing and transmitting value among the participants of the Bitcoin network
- The Bitcoin blockchain contains a record of every time someone sent or received bitcoins

Co-funded by the Erasmus+ Programme of the European Union

Blockchain contributions to cryptos

- The blockchain technology that powers cryptocurrencies make it possible to transfer value online without the need for a middleman like a bank or credit card company → Decentralization

- Once a data has been recorded it becomes very difficult to change it→ Immutability

- Transactions in the blockchain are verified and shared by a huge amount of computing power, what enables secure payments to be made between people who don't know each other → Security

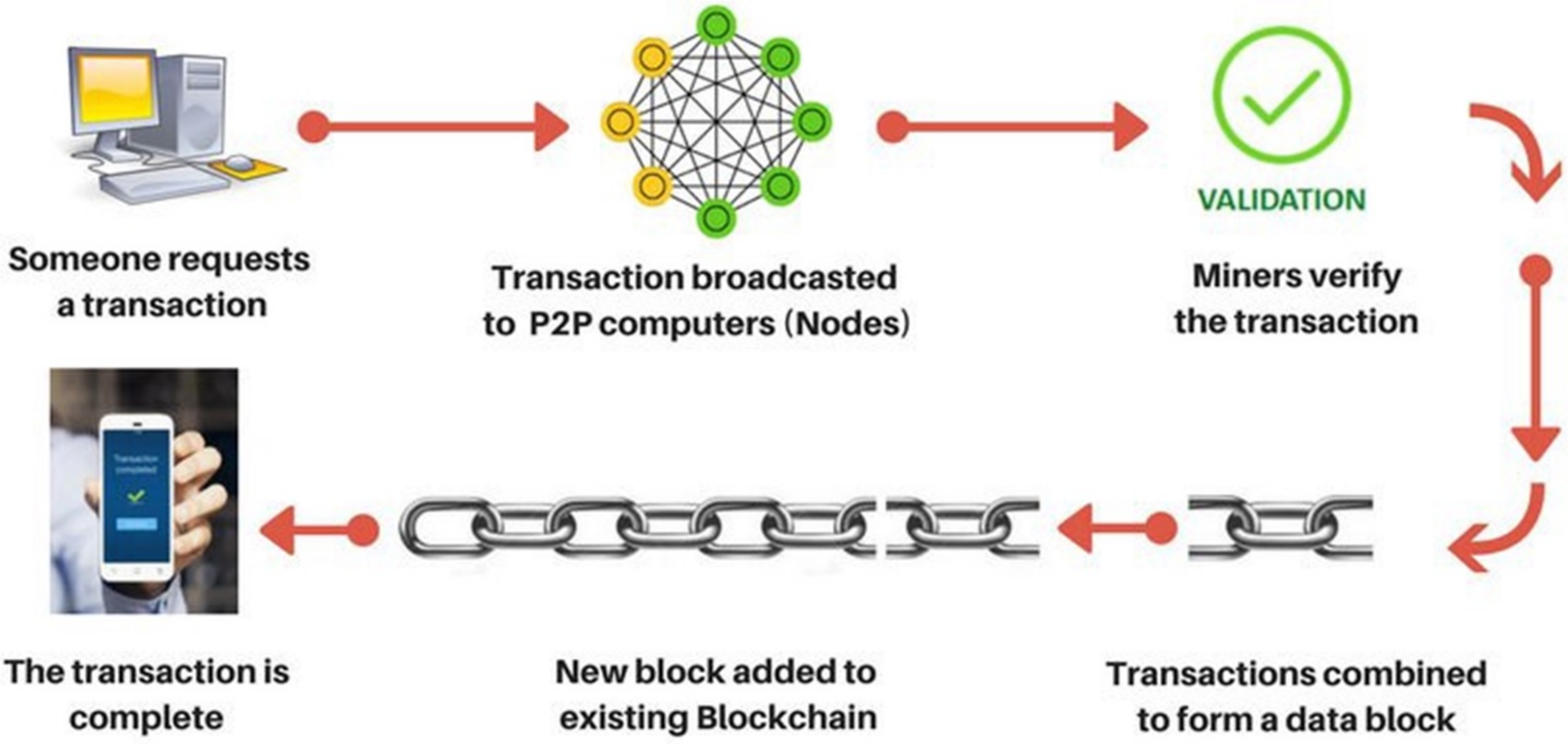
Mining

- Mining nodes (anyone!) create and register transaction blocks in the blockchain every 10 minutes
- High difficulty task → advanced computational resources
- Competitive fight for a (declining) reward → halving
- Based on a problem which is difficult to solve but easy to verify → Proof of work

Co-funded by the Erasmus+ Programme of the European Union

Miners

HOW BITCOIN TRANSACTION WORKS



VALIDATION

Someone requests a transaction

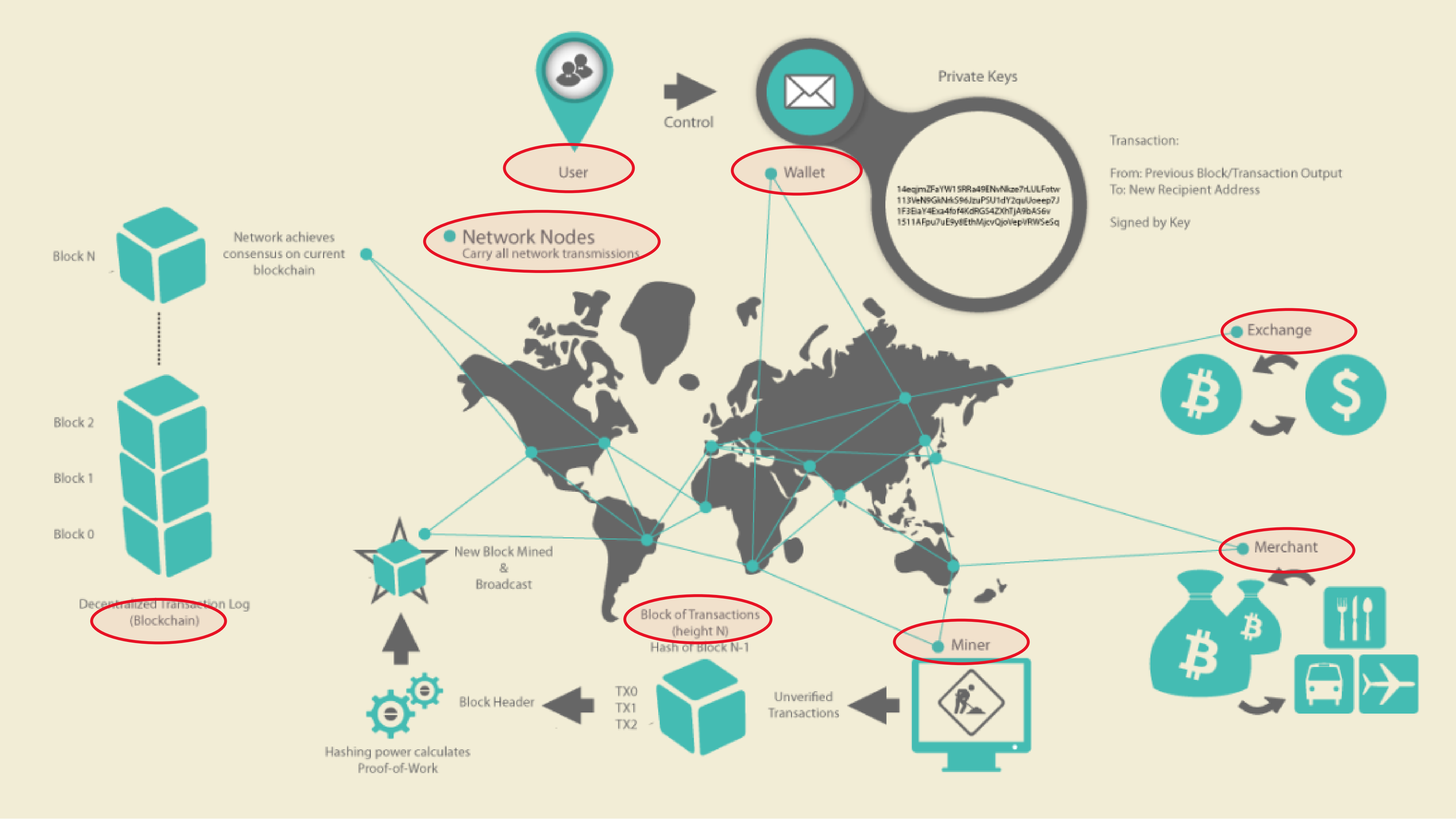
Transaction broadcasted to P2P computers (Nodes)

Miners verify the transaction

Transactions combined to form a data block

New block added to existing Blockchain

The transaction is complete

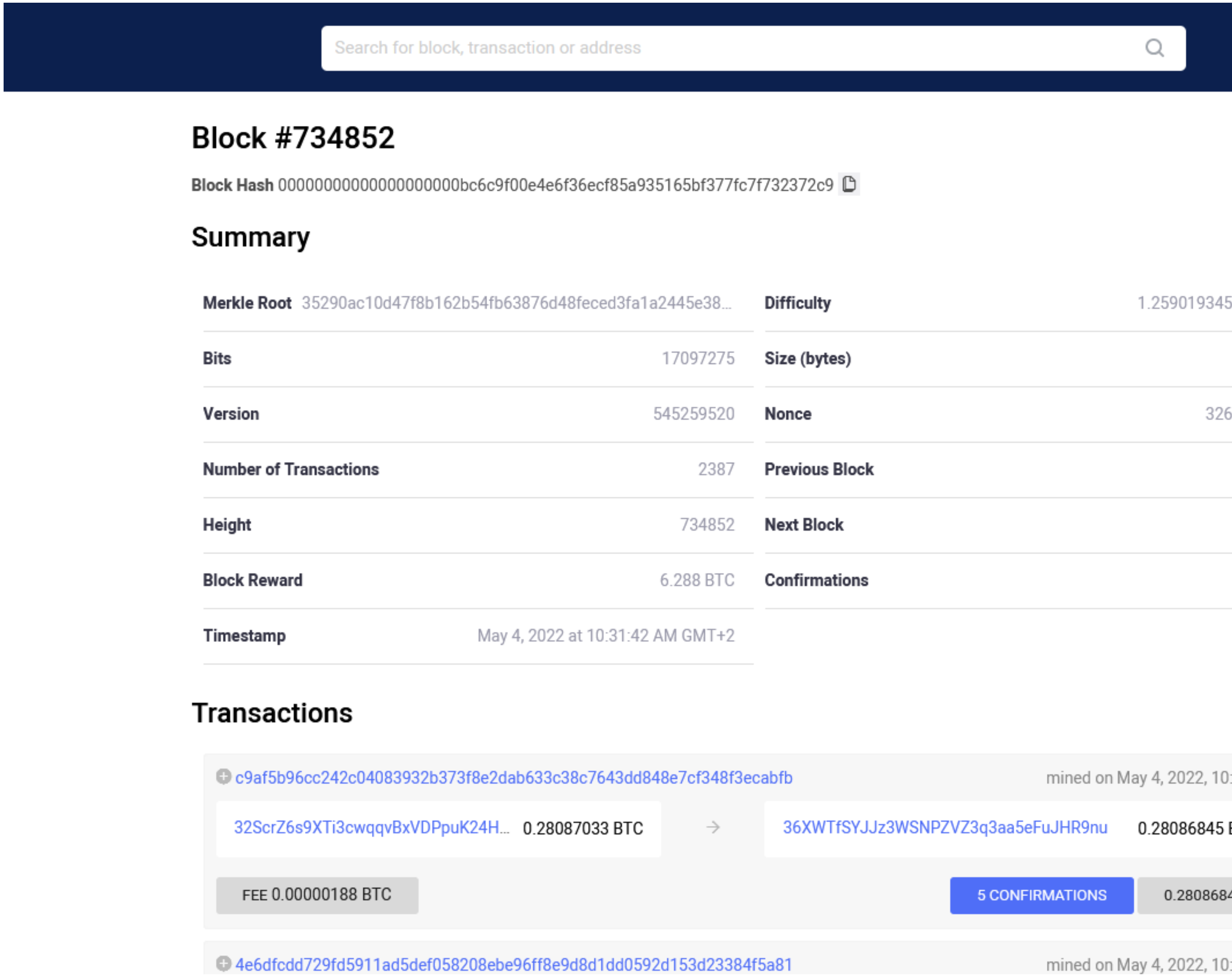

User
Control
Wallet
Private Keys
14eqjmZFaYW15RRa49ENvNkze7rLULFotw
113VeN9GkNrkS96JzuPSU1dY2quUoeep7J
1F3EiaY4Exa4fof4KdRGS4ZXhTjA9bAS6v
1511AFpu7uE9y8EthMjcvQjoVepWRWSeSq
Transaction:
From: Previous Block/Transaction Output
To: New Recipient Address
Signed by Key
Network Nodes
Carry all network transmissions
Block N
Network achieves consensus on current blockchain
Block 2
Block 1
Block 0
Decentralized Transaction Log
(Blockchain)
Exchange
New Block Mined
&
Broadcast
Merchant
Block of Transactions
(height N)
Hash of Block N-1
Miner
Block Header
TX0
TX1
TX2
Unverified Transactions
Hashing power calculates Proof-of-Work

The Blockchain concept revisited

- A type of database to record and maintain data with the unique character of (a) having distributed / decentralized ledger approach and (b) temporally ordered
  - In a centralized database, a single authority has full control over all aspects, including data entry, ensuring its validity and the maintenance of that data.
  - In the decentralized blockchain approach, data is recorded in "blocks" that are distributed and validated among several participants (nodes) in a P2P network.
  - Property of coins is based on an ownership chain
- Although anyone can create data on public blockchains by creating a new block and chaining it to a previous block, the consensus-based validation approach means that no one can edit or forge the data once enough block confirmations have been received

Co-funded by the Erasmus+ Programme of the European Union

Technical details



Block #734852

Block Hash 00000000000000000000bc6c9f00e4e6f36ecf85a935165bf377fc7f732372c9

Summary

Merkle Root	35290ac10d47f8b162b54fb63876d48feced3fa1a2445e38...	**Difficulty**	1.259019345
Bits	17097275	**Size (bytes)**	
Version	545259520	**Nonce**	326
Number of Transactions	2387	**Previous Block**	
Height	734852	**Next Block**	
Block Reward	6.288 BTC	**Confirmations**	
Timestamp	May 4, 2022 at 10:31:42 AM GMT+2		

Transactions

c9af5b96cc242c04083932b373f8e2dab633c38c7643dd848e7cf348f3ecabfb mined on May 4, 2022, 10:

32ScrZ6s9XTi3cwqqvBxVDPpuK24H... 0.28087033 BTC → 36XWTfSYJJz3WSNPZVZ3q3aa5eFuJHR9nu 0.28086845 B

FEE 0.00000188 BTC

5 CONFIRMATIONS

0.2808684

4e6dfcdd729fd5911ad5def058208ebe96ff8e9d8d1dd0592d153d23384f5a81 mined on May 4, 2022, 10:

Co-funded by the
Erasmus+ Programme
of the European Union

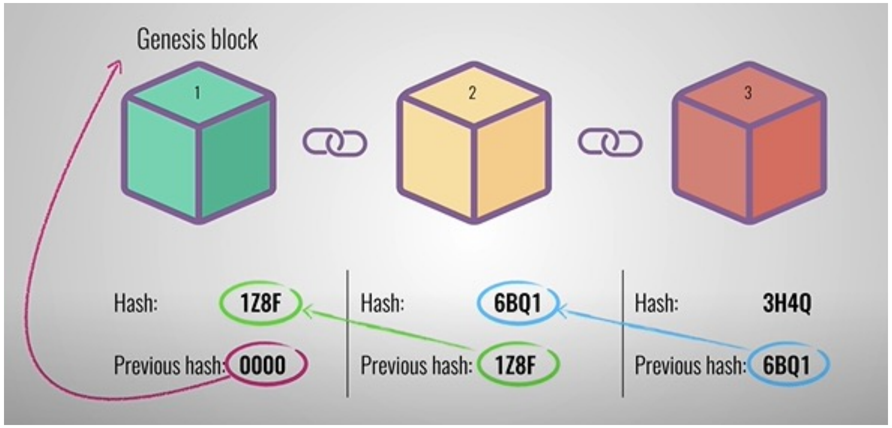
Blocks

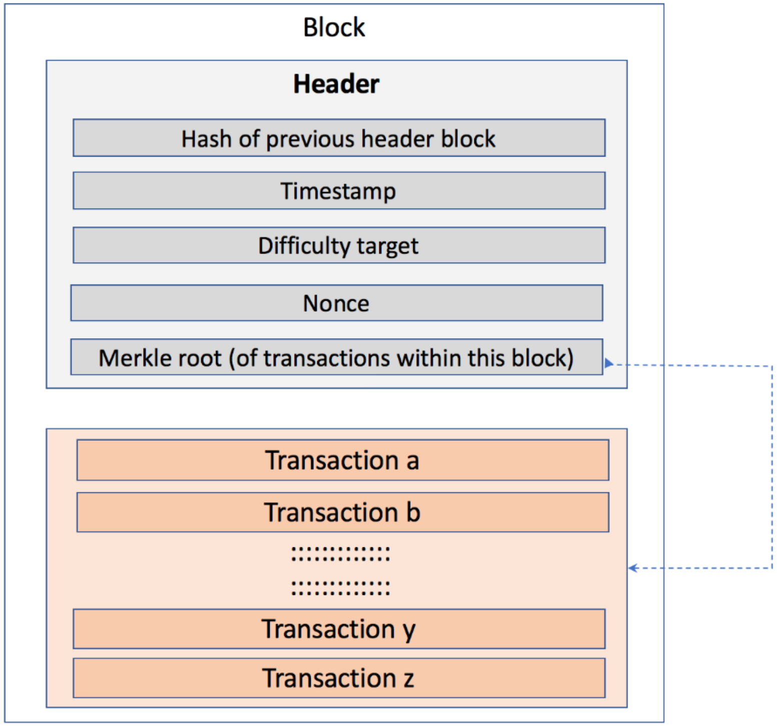
- The primary identifier of a block is its cryptographic hash
  - In bitcoin, id is obtained by applying SHA256 with the header twice 32 bytes
  - It is called block hash, it is more accurate to call it header hash.
- Other identifier: block height (not always unique)
- Chain up to the genesis block
- It is possible to reverse a chain for a longer one, but its probability decreases with time

Co-funded by the Erasmus+ Programme of the European Union

Blocks

- Header + data
- Header: id of this block + id of previous block





Block

Header

Hash of previous header block

Timestamp

Difficulty target

Nonce

Merkle root (of transactions within this block)

Transaction a

Transaction b

::::::::::::

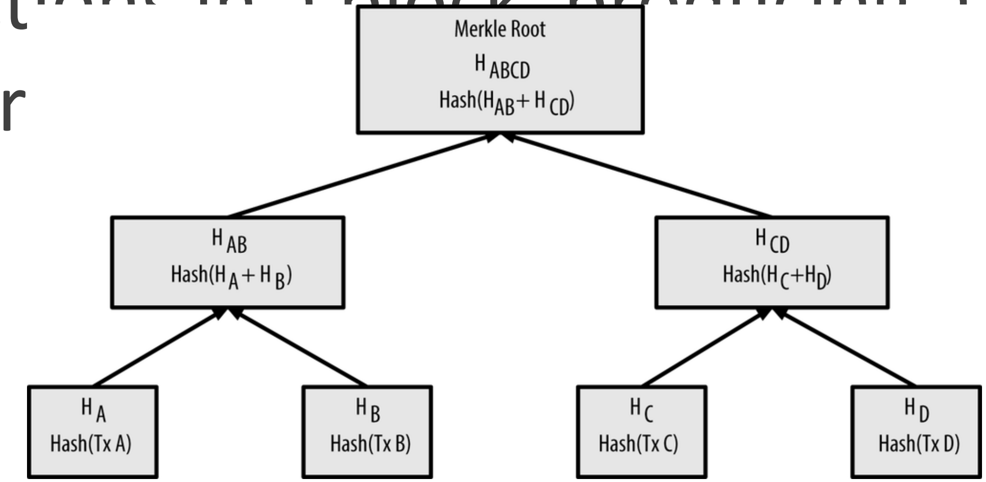
::::::::::::

Transaction y

Transaction z

Merkle trees

- Binary hash tree used to summarize and validate data sets
- In bitcoin blockchain MTs summarize all transactions in a block, producing a complete fingerpr set+



Block creation

- Any node that validates a transaction writes it to the pending transaction pool.
- A miner that receives a block knows that it lost the last competition, but a new one starts.
- It takes transitions from the pending pool and creates the next candidate block.
- While solving the current puzzle, it receives and accumulates transactions for the next one.

https://www.blockchain.com/btc/unconfirmed-transactions

Co-funded by the
Erasmus+ Programme
of the European Union

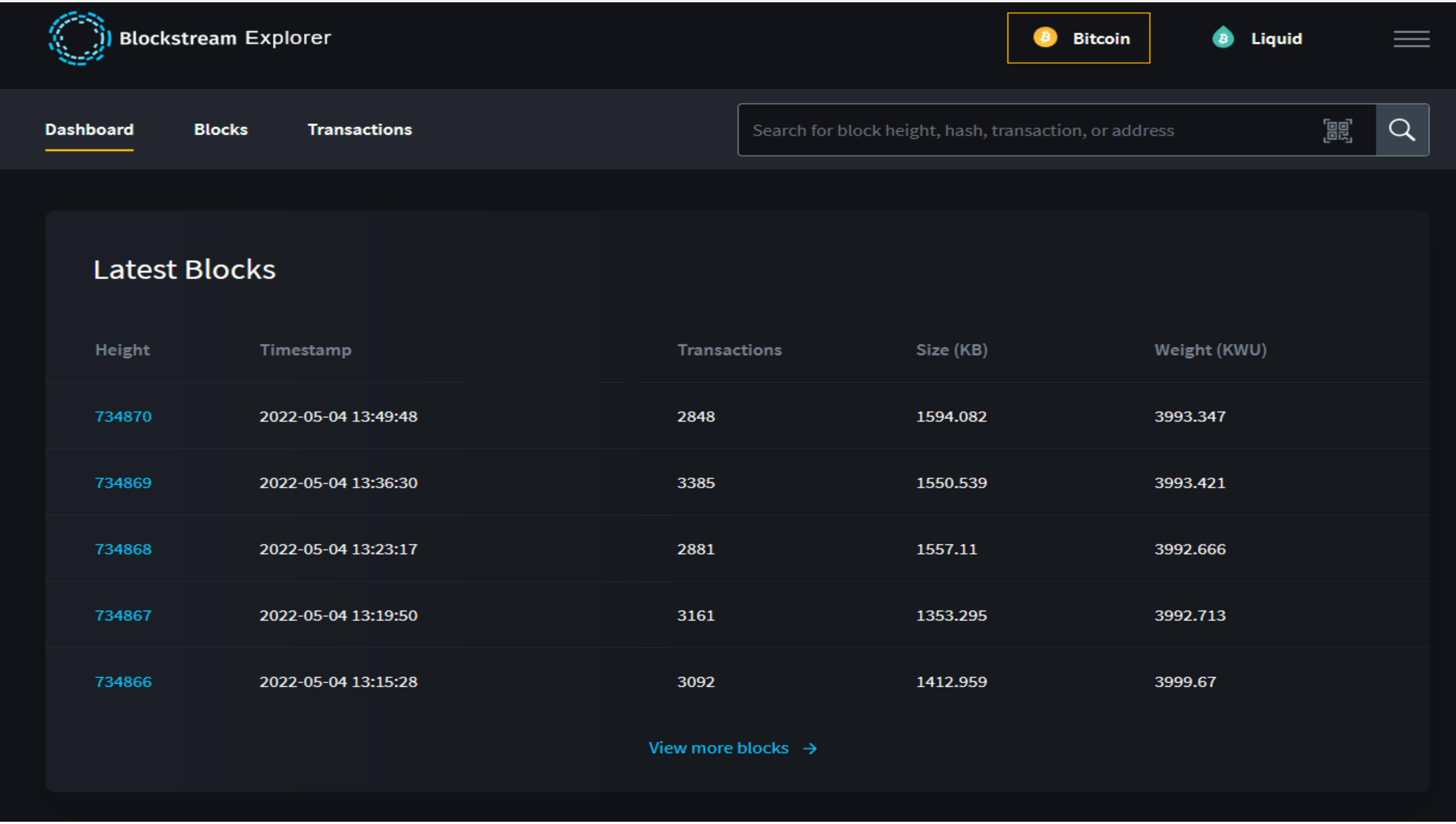
Types of blockchains

Public blockchains

- Anyone can download the code and manage a public node, validating transactions on the network
- Anyone is entitled to participate in the consensus process of which blocks are put on the chain.
- Anyone can make transactions on the chain: Any valid transaction will be added.
- Anyone can access and view the transactions using a block explorer, (transactions are public, but anonymous).
- Type of blockchain network mostly associated with cryptocurrencies

Co-funded by the Erasmus+ Programme of the European Union

Blockchain explorer



Latest Blocks

Height	Timestamp	Transactions	Size (KB)	Weight (KWU)
734870	2022-05-04 13:49:48	2848	1594.082	3993.347
734869	2022-05-04 13:36:30	3385	1550.539	3993.421
734868	2022-05-04 13:23:17	2881	1557.11	3992.666
734867	2022-05-04 13:19:50	3161	1353.295	3992.713
734866	2022-05-04 13:15:28	3092	1412.959	3999.67

Private and consortium blockchains

*“**A private blockchain is an oxymoron.** The whole reason that the blockchain was invented is to make Bitcoin a decentralized and anonymous system in which everyone can come to the same arbitrary consensus about the history of Bitcoin.”*

-- Bitcoin researcher and Director of Research at Satoshi Nakamoto Institute, Daniel Krawisz

Private blockchains

- A non-decentralized ledger that operates as a closed, secure database based on cryptography concepts.
- Not everyone can run a full node on the private blockchain, make transactions, or validate/authenticate the blockchain changes.
- Utilities are very restricted to one company and probably are not interesting for public people to access.
- Biggest advantages: simplifying complex data management flows and reducing costs.
- Criticism:
  - The very concept of a closed blockchain negates the need for a blockchain: One could simply use a MySQL database.
  - Marketing strategy, buzzwords…

Public permissioned blockchains

- Permissioned blockchains aren’t private blockchains but…
  - additional access control layer as a security measure
  - only identifiable participants can execute certain on-chain actions
- Examples:
  - Proof of stake networks such as Ethereum
  - Ripple payment network uses a consensus mechanism, via a group of bank-owned servers, to confirm transactions
  - Distribution chain networks where participants have different roles

Co-funded by the Erasmus+ Programme of the European Union

Permissioned blockchains

- A consortium blockchain is a private network for a group of companies
- The consensus mechanism is maintained by a series of nodes that have been pre-selected and trusted in advance
- Difference with private blockchains: pre-selected nodes are not part of a single company.

Co-funded by the
Erasmus+ Programme
of the European Union

Blockchain Governance

Blockchain governance

- Mechanisms by which decentralized networks adapt and change over time
- Generally broken up into on-chain governance and off-chain governance.
- On-Chain: protocol upgrades happen automatically in response to coin (token) voting.
- Example: bitcoin's scaling debate (supporters of increasing the block size vs. those proposing to move transaction to layer 2 solutions)

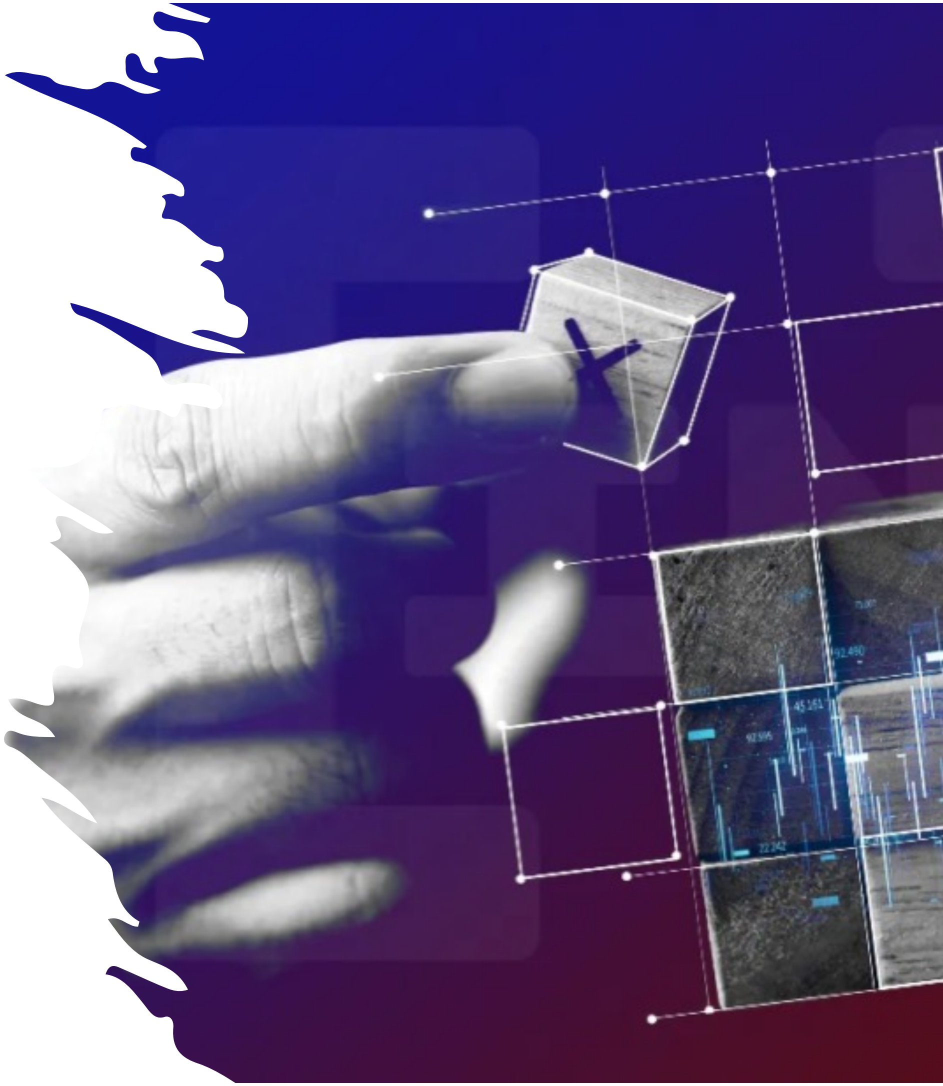
Co-funded by the Erasmus+ Programme of the European Union

Blockchain governance

- Off-Chain: Network stakeholders coordinate to decide how network upgrades are handled
- Most networks today employ off-chain systems
- Process:
  - Developers submit improvement proposals
  - Network stakeholders coordinate through community channels
  - Protocol developers integrate new features
  - Node operators signal their support or dissent for the changes
  - Miners decide which chain to secure

Co-funded by the
Erasmus+ Programme
of the European Union

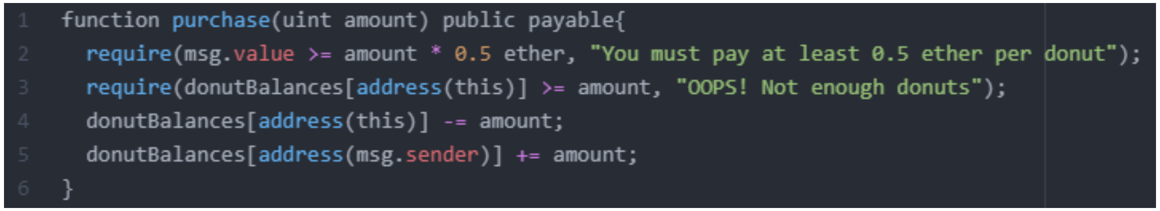
Blockchain-related concepts



Co-funded by the
Erasmus+ Programme
of the European Union

Smart contracts

- A program that runs on the (Ethereum) blockchain.
  - It is a group of code (its functions) and data (its state) that exists at a specific address on the blockchain.
  - Specific programming language: Solidity / Vyper



```
function purchase(uint amount) public payable{
  require(msg.value >= amount * 0.5 ether, "You must pay at least 0.5 ether per donut");
  require(donutBalances[address(this)] >= amount, "OOPS! Not enough donuts");
  donutBalances[address(this)] -= amount;
  donutBalances[address(msg.sender)] += amount;
}
```

- They can not directly access to off-chain information
- Just as a vending machines eliminate the need for an employee, smart contracts can replace middlemen in many industries.

Co-funded by the
Erasmus+ Programme
of the European Union

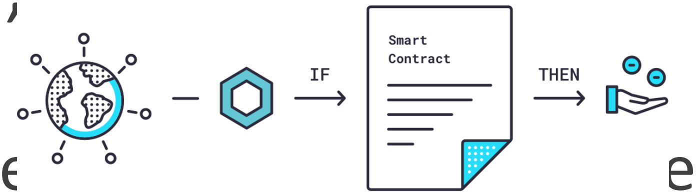
Sidechains

- A separate blockchain which runs in parallel to Mainnet and operates independently.
- Both chains can communicate and complement each other's capabilities.
- Example: RSK enables smart-contracts, near instant payments, and higher-scalability in blockchain.
- How they work:
  1. The cryptocurrencies are sent to a specific address
  2. Funds are frozen
  3. A notification is sent to the sidechain
  4. The sidechain will automatically create the exact same number of tokens corresponding to the funds that were sent
  5. The sidechain will use the funds for the purpose indicated

Co-funded by the Erasmus+ Programme of the European Union

Oracles

- A data source external to the blockchain, which can forward data from off-chain sources onto blockchains.
  - Data can be used by smart contracts deployed on a blockchain
  - Data sources can be humans, software, or hardware (IoT sensors)
- For smart contracts to craft agreements beyond blockchain data, they need off-chain data in an on-chain format.



  - Oracles provide er, financial markets, geolocation, sport or political events, etc.

Blockchain Master Project ideas

- Authorichain: Blockchain-based system to keep track of consent authorizations present in most web applications today
- Medchain: A medical recording system that retrieves information from several sources. Implementation on Ethereum using oracles
- Blorganick: Organic products traceability system based on a permissioned blockchain
- Sblocktify: Blockchain technology that certifies the authorship of musical assets and calculate the appropriate compensation for their owners and pay them when their creations are consumed.
- CVChain: Document management platform aimed at bringing together all of an individual's academic grades and qualifications in a secure way
- Artchain: Demo website where art-linked NFT owners can mint tokenized fractional ownership of their NFTs using Fractional

salvador.sanchez@uah.es

Thank you for your attention!

Co-funded by the
Erasmus+ Programme
of the European Union