Blockchain & Decentralized Finance (DeFi)

Carlos J. Costa

Feb. 2024

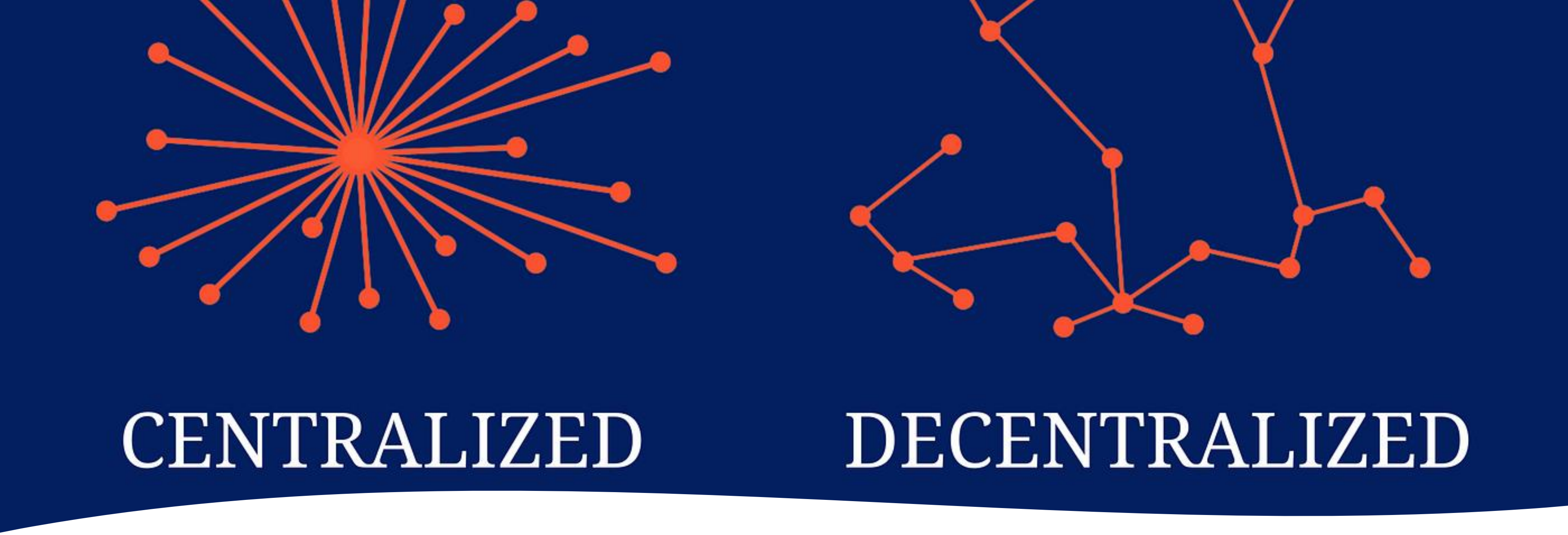
Blockchain

- Blockchain is a decentralized and distributed ledger technology that has gained prominence due to its application in cryptocurrencies like Bitcoin.

  https://andersbrownworth.com/blockchain/

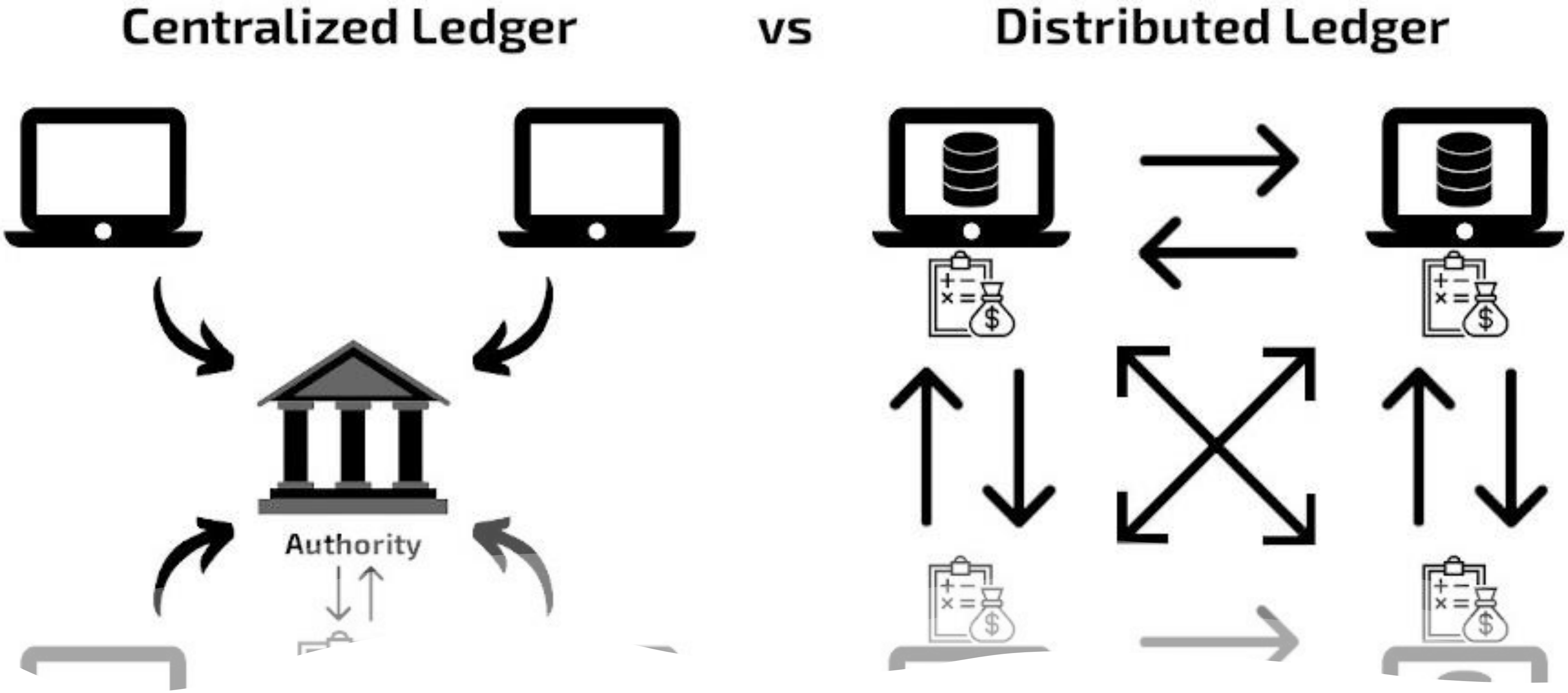
Blockchain

- The main concepts of blockchain include:
  1. Decentralization
  2. Distributed Ledger
  3. Consensus Mechanism
  4. Blocks and Transactions
  5. Cryptography
  6. Immutability
  7. Smart Contracts
  8. Public and Private Keys
  9. Permissioned and Permissionless Blockchains
  10. Mining (Proof of Work)
  11. Tokenization
  12. Usage and adoption



Decentralization

- Blockchain operates on a decentralized network of computers (nodes) rather than relying on a central authority.
- This decentralization ensures that no single entity has control or ownership over the entire network.



Distributed Ledger

- The ledger, or record of transactions, is distributed across all nodes in the network.
- Each node maintains its copy of the ledger, making it transparent and resistant to tampering.

Consensus Mechanism

- Consensus mechanisms are protocols that enable nodes in the network to agree on the state of the ledger.
- Common consensus mechanisms include Proof of Work (used in Bitcoin) and Proof of Stake.
- These mechanisms prevent malicious actors from manipulating the ledger

	Proof-of-work	Proof-of-stake
Power consumption	Huge amounts of electricity required to secure the blockchain due to the processing needed.	Much lower amounts of electricity required to secure the blockchain.
Security	Required to have more than 50% of the processing power to hack.	Required to have more than 50% of the stake (coins) to hack. Can be more expensive to hack due penalties defined in the protocol such as loss of the stake.
Risk of centralisation	There is a risk of having mining pools, group of miners working together, controlling vast amounts of mining power. Currently, three different mining pools control more than 50% of the mining power [9].	Lower risk due to economies of scale being less of an issue. Not dependent on mining equipment.

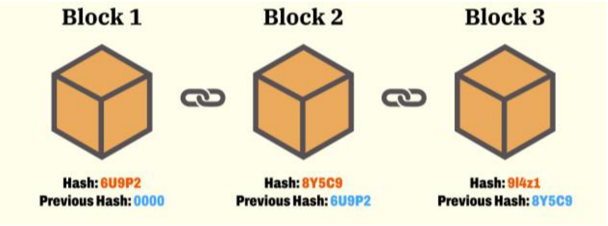
Abreu, Aparicio & Costa (2019)

Mining (Proof of Work):

- In Proof of Work-based blockchains like Bitcoin, miners compete to solve complex mathematical problems.
- The first miner to solve the problem adds a new block to the blockchain and is rewarded with newly created cryptocurrency and transaction fees.

Blocks and Transactions

- Transactions are grouped together in blocks, and each block contains a reference to the previous block, forming a chain.
- This chain of blocks ensures the chronological order and integrity of transactions.



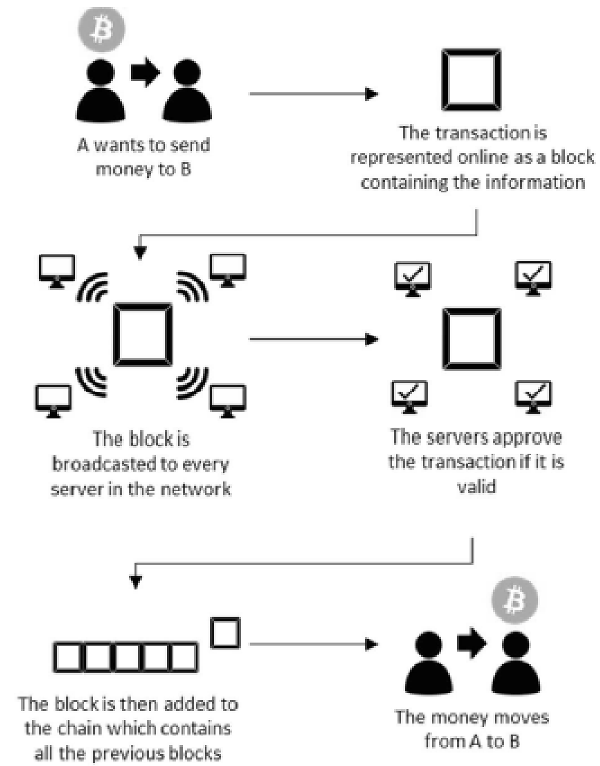
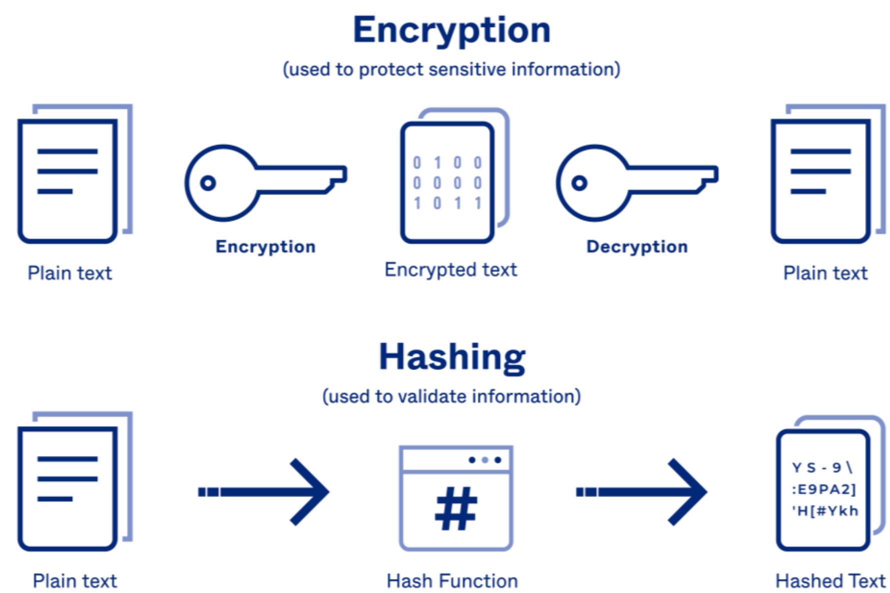


Figure 2: How does a transaction in the blockchain work?

Abreu, Aparicio & Costa (2019)

Cryptography



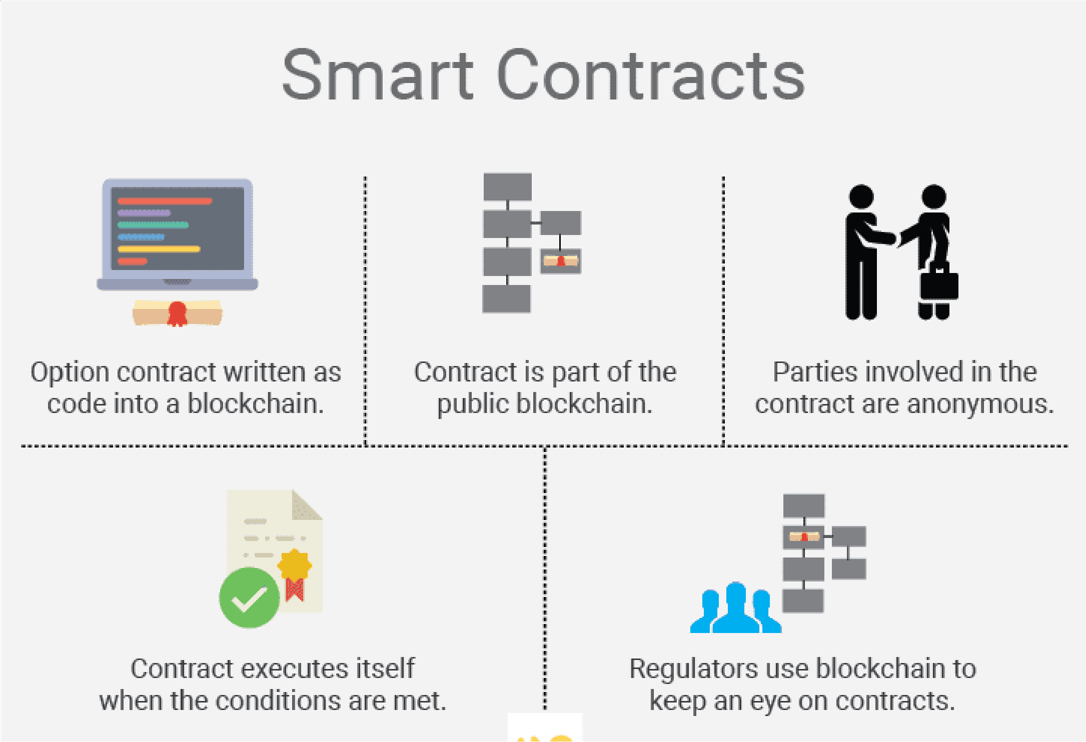
- Cryptographic techniques, such as hashing and digital signatures, are fundamental to blockchain security.
- Hash functions create unique identifiers for blocks, and digital signatures verify the authenticity of transactions.

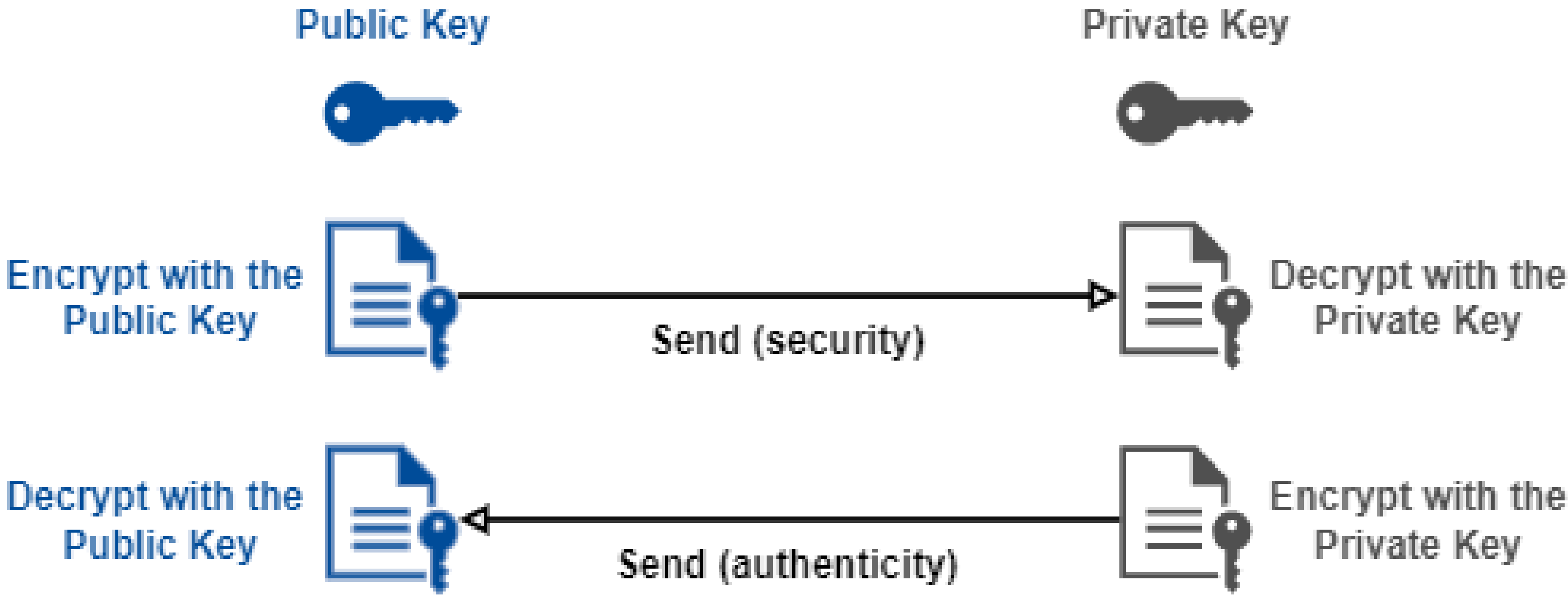
Immutability

- Once a block is added to the blockchain, it is challenging to alter or remove.
- This immutability is achieved using cryptographic hashes and the consensus mechanism, making the blockchain a reliable and secure record of transactions.

Smart Contracts

- Smart contracts are self-executing contracts with the terms directly written into code.
- These contracts automatically execute predefined actions when specific conditions are met.
- Smart contracts are deployed on blockchain platforms like Ethereum.



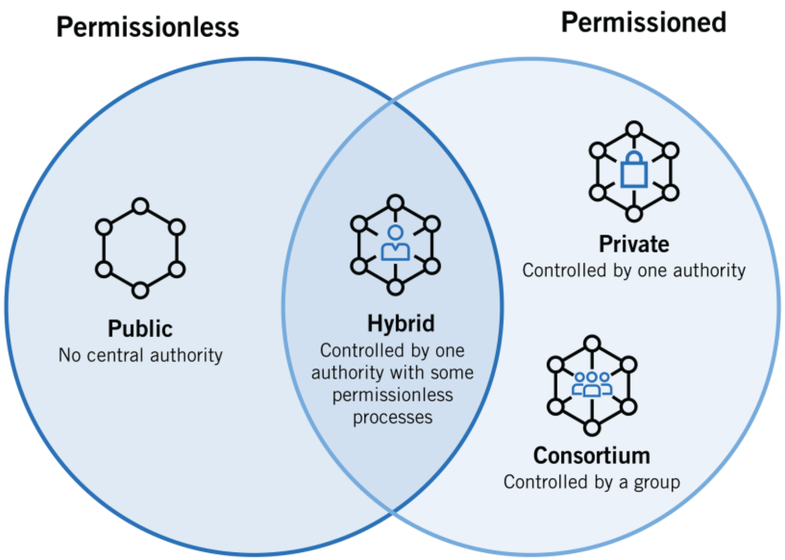


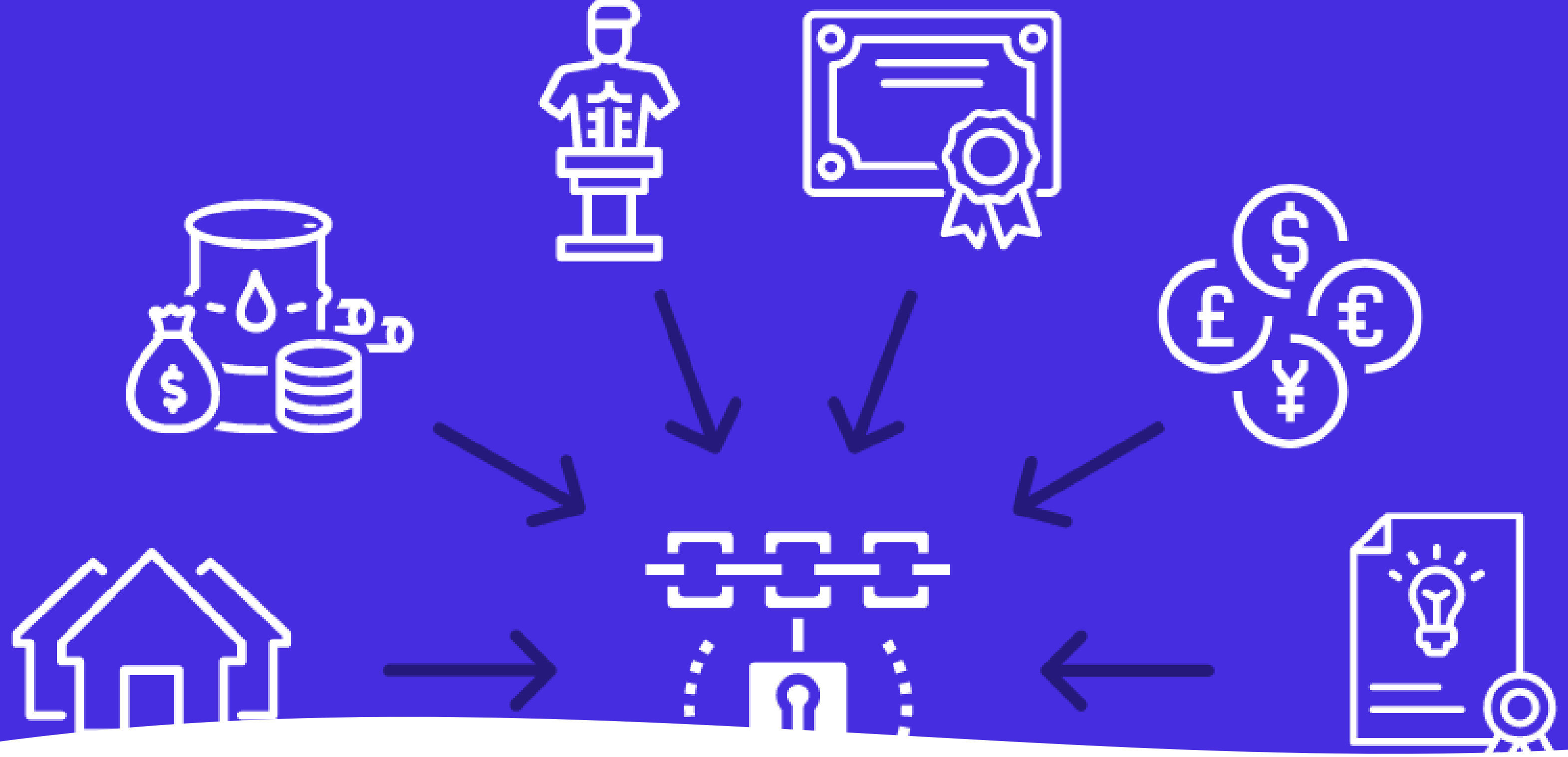
Public and Private Keys

- Public and private key pairs are used for secure transactions and identity verification.
- The public key is shared openly, while the private key is kept secret.
- Cryptographic signatures, generated with private keys, verify the authenticity of transactions.

Permissioned and Permissionless Blockchains

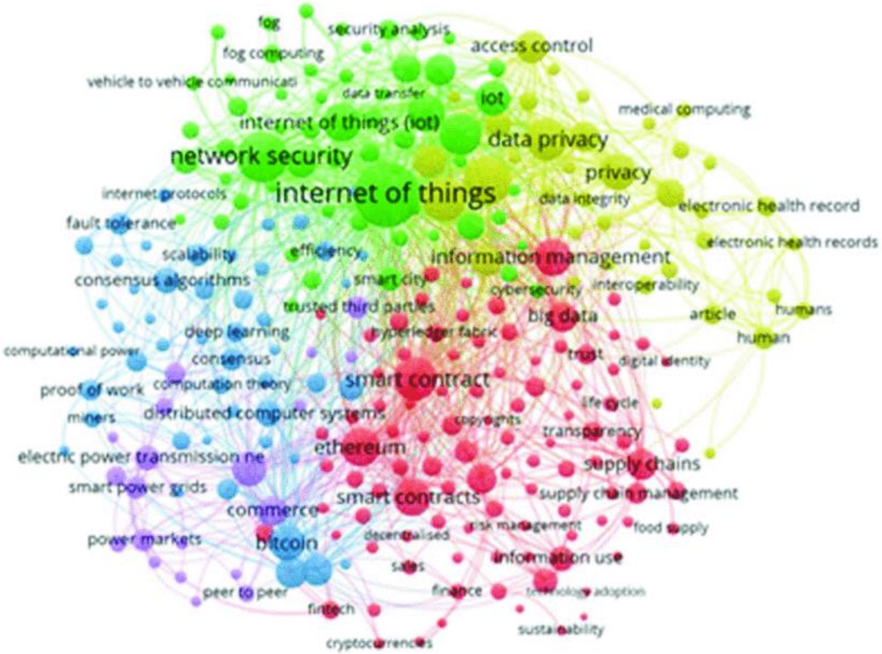
- Permissionless blockchains, like Bitcoin, allow anyone to participate in the network.
- Permissioned blockchains restrict access to authorized participants, making them suitable for business and consortium use

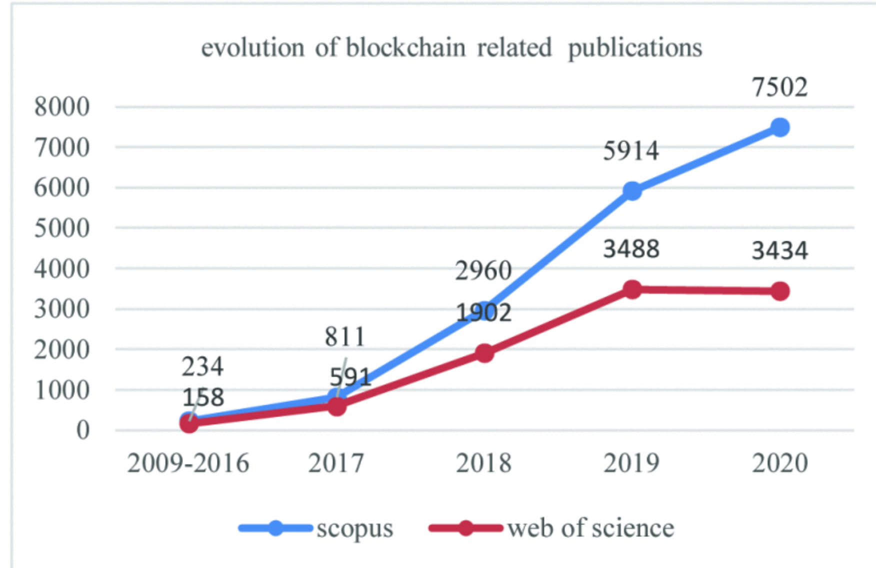




Tokenization

- Blockchain enables the creation of tokens, representing assets or rights.
- Tokens can be traded on blockchain platforms and are often used in Initial Coin Offerings (ICOs) or tokenization of real-world assets

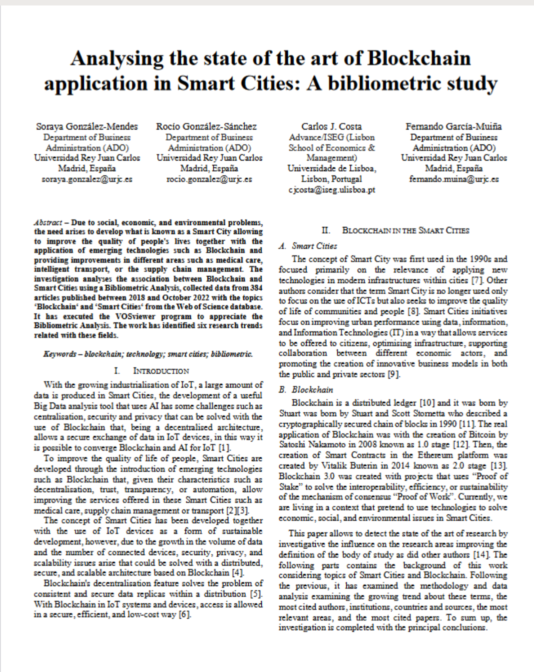




Bernardino, C, Costa, J. & Aparício, M. (2022)

Research

Research: Smart Cities



Analysing the state of the art of Blockchain application in Smart Cities: A bibliometric study

Soraya González-Mendes
Department of Business Administration (ADO)
Universidad Rey Juan Carlos
Madrid, España
soraya.gonzalez@urjc.es

Rocío González-Sánchez
Department of Business Administration (ADO)
Universidad Rey Juan Carlos
Madrid, España
rocio.gonzalez@urjc.es

Carlos J. Costa
Advance/ISEG (Lisbon School of Economics & Management)
Universidade de Lisboa,
Lisbon, Portugal
cjcosta@iseg.ulisboa.pt

Fernando García-Muiña
Department of Business Administration (ADO)
Universidad Rey Juan Carlos
Madrid, España
fernando.muina@urjc.es

Abstract – **Due to social, economic, and environmental problems, the need arises to develop what is known as a Smart City allowing to improve the quality of people's lives together with the application of emerging technologies such as Blockchain and providing improvements in different areas such as medical care, intelligent transport, or the supply chain management. The investigation analyses the association between Blockchain and Smart Cities using a Bibliometric Analysis, collected data from 384 articles published between 2018 and October 2022 with the topics 'Blockchain' and 'Smart Cities' from the Web of Science database. It has executed the VOSviewer program to appreciate the Bibliometric Analysis. The work has identified six research trends related with these fields.**

Keywords – blockchain; technology; smart cities; bibliometric.

I. INTRODUCTION

With the growing industrialisation of IoT, a large amount of data is produced in Smart Cities, the development of a useful Big Data analysis tool that uses AI has some challenges such as centralisation, security and privacy that can be solved with the use of Blockchain that, being a decentralised architecture, allows a secure exchange of data in IoT devices, in this way it is possible to converge Blockchain and AI for IoT [1].

To improve the quality of life of people, Smart Cities are developed through the introduction of emerging technologies such as Blockchain that, given their characteristics such as decentralisation, trust, transparency, or automation, allow improving the services offered in these Smart Cities such as medical care, supply chain management or transport [2][3].

The concept of Smart Cities has been developed together with the use of IoT devices as a form of sustainable development, however, due to the growth in the volume of data and the number of connected devices, security, privacy, and scalability issues arise that could be solved with a distributed, secure, and scalable architecture based on Blockchain [4].

Blockchain's decentralisation feature solves the problem of consistent and secure data replicas within a distribution [5]. With Blockchain in IoT systems and devices, access is allowed in a secure, efficient, and low-cost way [6].

II. BLOCKCHAIN IN THE SMART CITIES

A. Smart Cities

The concept of Smart City was first used in the 1990s and focused primarily on the relevance of applying new technologies in modern infrastructures within cities [7]. Other authors consider that the term Smart City is no longer used only to focus on the use of ICTs but also seeks to improve the quality of life of communities and people [8]. Smart Cities initiatives focus on improving urban performance using data, information, and Information Technologies (IT) in a way that allows services to be offered to citizens, optimising infrastructure, supporting collaboration between different economic actors, and promoting the creation of innovative business models in both the public and private sectors [9].

B. Blockchain

Blockchain is a distributed ledger [10] and it was born by Stuart was born by Stuart and Scott Stornetta who described a cryptographically secured chain of blocks in 1990 [11]. The real application of Blockchain was with the creation of Bitcoin by Satoshi Nakamoto in 2008 known as 1.0 stage [12]. Then, the creation of Smart Contracts in the Ethereum platform was created by Vitalik Buterin in 2014 known as 2.0 stage [13]. Blockchain 3.0 was created with projects that uses "Proof of Stake" to solve the interoperability, efficiency, or sustainability of the mechanism of consensus "Proof of Work". Currently, we are living in a context that pretend to use technologies to solve economic, social, and environmental issues in Smart Cities.

This paper allows to detect the state of the art of research by investigative the influence on the research areas improving the definition of the body of study as did other authors [14]. The following parts contains the background of this work considering topics of Smart Cities and Blockchain. Following the previous, it has examined the methodology and data analysis examining the growing trend about these terms, the most cited authors, institutions, countries and sources, the most relevant areas, and the most cited papers. To sum up, the investigation is completed with the principal conclusions.

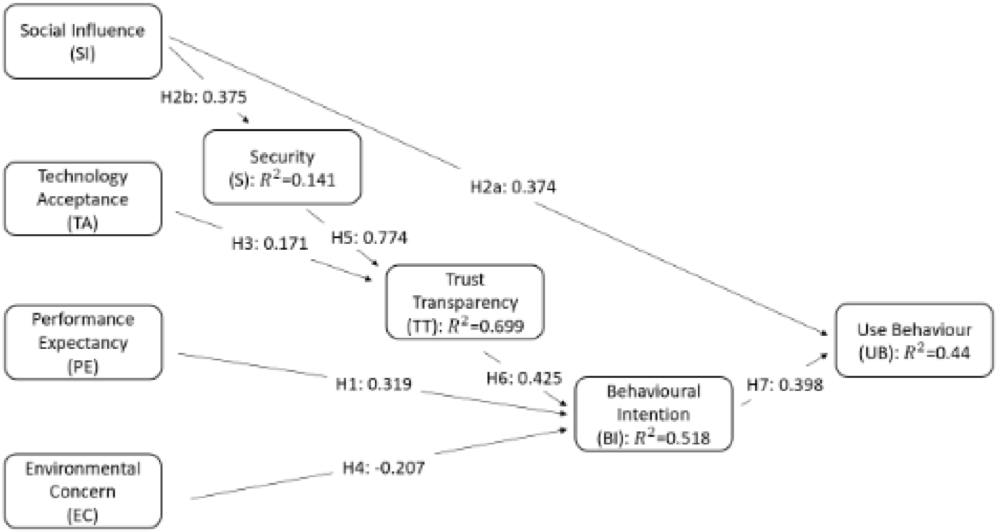
TABLE VI. MOST RELEVANT KEYWORKS IN CLUSTERS

Cluster	Colors	Most Relevant Keywords	Application Area
Cluster 1	Security & Privacy in Management	Privacy; Security; Authentication; Smart Contracts; Ethereum; Protocol; Service; Scheme; Efficient; Access Control; Model; Trust; Management	Smart Contracts Security Management
Cluster 2	Sustainability & Renewable Energy in Smart Cities	Smart Cities; Big Data, System; Renewable Energy, System; Future; City; Sustainability; Platform	Sustainability Smart City
Cluster 3	Data Analytics & Cloud Computing	Cloud Computing; Data Analytics; Algorithm; Smart Grids; Vehicles; Medical Services; Intelligence; 5G	Cloud Analytics
Cluster 4	New Sensors Design with IoT & Blockchain	Blockchain; Internet of Things; Optimisation; Communication; Design; Sensors; Data Models; Data Privacy; Data Sharing; Task Analysis; Monitoring	Blockchain Internet of Things Data Optimisation
Cluster 5	Security & Privacy on the Internet	Internet; Deep Learning; Machine Learning; Security and Privacy, Selection	Machine Learning Security and Privacy
Cluster 6	Energy using Technology	Technology; Energy; Cybersecurity; Supply Chain; Logistics; Healthcare	Technology Energy Supply Chain

González-Mendes et al. (2023)

Research: Usage and Adoption

- Importance of Trust/Security
- Social Influence
- Environmental Concerns



Cesario et al. (2023)

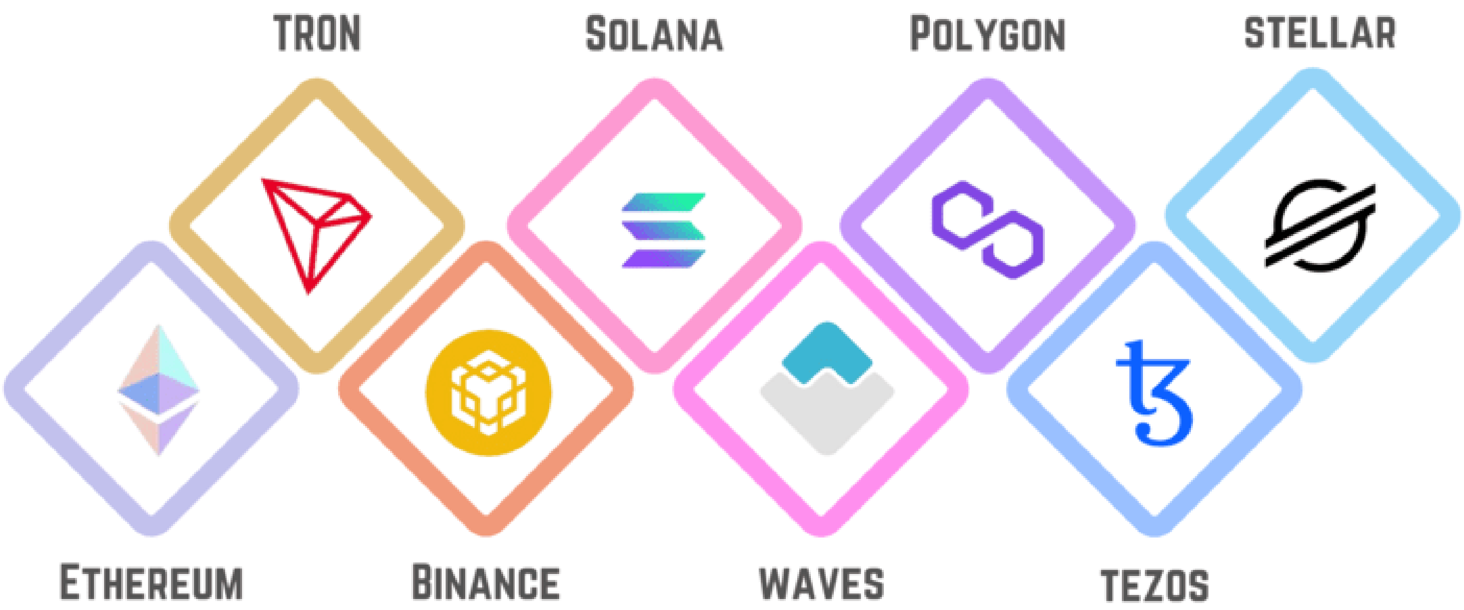
Decentralized Finance (DeFi)

- is a financial system built on blockchain technology that aims to recreate and improve upon traditional financial services in a decentralized manner.

Decentralized Finance (DeFi)

- The key components of DeFi include:

1. Blockchain Platforms
2. Smart Contracts
3. Decentralized Exchanges (DEX)
4. Decentralized Lending and Borrowing Platforms
5. Stablecoins
6. Decentralized Asset Management
7. Insurance
8. Oracles
9. Cross-Chain Solutions
10. Wallets
11. Governance Tokens
12. Yield Farming and Liquidity Mining
13. Liquidity pool
14. liquidity providers,
15. liquidity tokens and
16. automated market makers.
17. Impermanent Loss



Blockchain Platforms

- DeFi applications are typically built on existing blockchain platforms, with Ethereum being the most popular.
- Other platforms also host various DeFi projects.

Smart Contracts

- Smart contracts are self-executing contracts with the terms directly written into code.
- They automate the execution of financial agreements, enabling decentralized applications (dApps) to operate autonomously.

Decentralized Exchanges (DEX)

- DEXs facilitate peer-to-peer trading of digital assets without the need for intermediaries.
- Users retain control of their private keys and assets during transactions.
- Examples include Uniswap, SushiSwap, and PancakeSwap

Decentralized Lending and Borrowing Platforms

- Platforms like Compound, Aave, and MakerDAO enable users to lend or borrow cryptocurrencies without intermediaries.
- Users can earn interest by providing liquidity or borrow assets against collateral.

- Stablecoins are cryptocurrencies pegged to the value of traditional fiat currencies, providing stability in volatile markets.
- Examples include DAI, USDC, and USDT.
- Stablecoins are often used in DeFi lending and borrowing.

Decentralized Asset Management

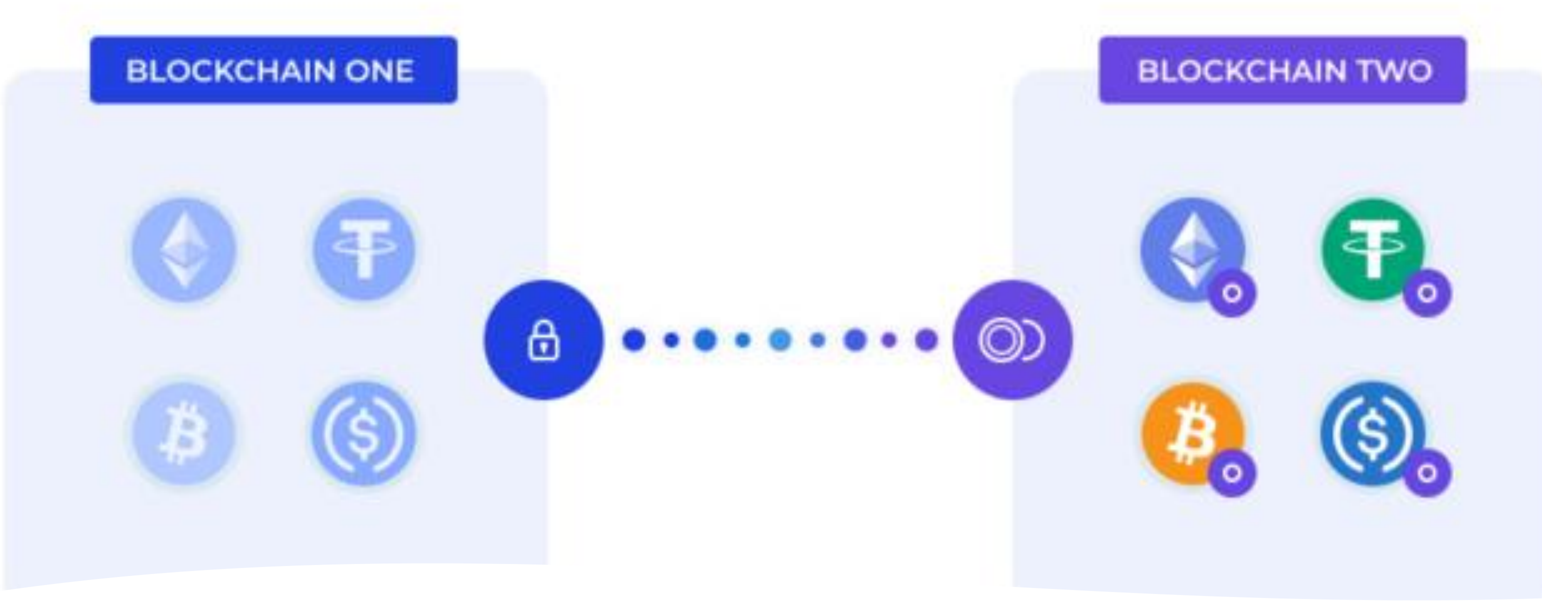
- DeFi platforms offer decentralized asset management services, allowing users to pool their funds together and participate in yield farming or liquidity provision.
- Examples include Yearn Finance and Curve Finance.

Insurance

- DeFi insurance platforms like Nexus Mutual and Cover offer decentralized insurance coverage for smart contract vulnerabilities, hacks, and other risks associated with the DeFi ecosystem.

Oracles

- Oracles provide real-world data to smart contracts.
- DeFi platforms use oracles to fetch external information, such as price feeds, to facilitate accurate and secure execution of smart contracts.



Cross-Chain Solutions

- Cross-chain solutions like Polkadot and Cosmos aim to connect different blockchain networks, enabling interoperability between various DeFi platforms and ecosystems.

Wallets

- Wallets are essential for users to store and manage their crypto assets.
- DeFi users often use non-custodial wallets, such as MetaMask, Trust Wallet, or Ledger, to interact with decentralized applications.

Governance Tokens

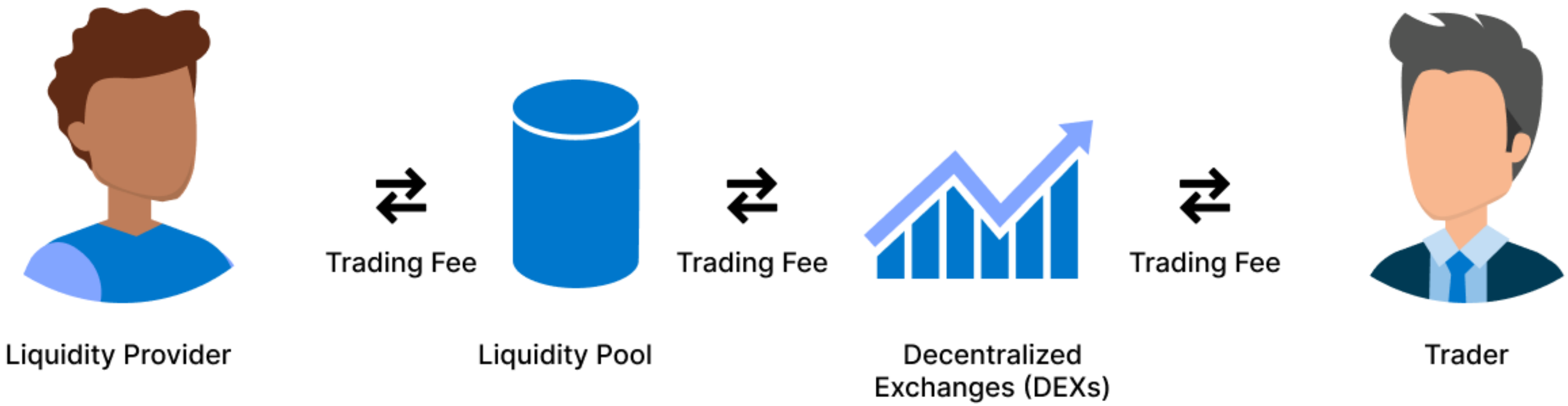
- Many DeFi projects have introduced governance tokens that grant holders the right to participate in the decision-making process of the platform.
- Users can propose and vote on changes to the protocol

Yield Farming and Liquidity Mining

- Yield farming involves providing liquidity to DeFi platforms in exchange for rewards, often in the form of additional tokens.
- Liquidity mining incentivizes users to contribute to the liquidity of decentralized exchanges and other platforms.

Liquidity pool

- is a smart contract where tokens are locked for the purpose of providing liquidity.
- is a smart contract that contains a reserve of two or more cryptocurrency tokens in a decentralized exchange (DEX).
- Liquidity pools encourage investors to earn passive income on cryptocurrencies that would otherwise be idle.
- Some of the important concepts required to understand how liquidity pools and decentralized exchanges work include:
  - liquidity providers,
  - liquidity tokens and
  - automated market makers.



Liquidity providers

- refer to entities or services that facilitate the availability of funds in cryptocurrency markets.
- they play a crucial role in ensuring smooth trade operations by offering a constant supply of digital assets for buying or selling.

Liquidity provider tokens

- (or LP tokens) are tokens issued to liquidity providers on a decentralized exchange (DEX) that run on an automated market maker (AMM) protocol.
- Uniswap, Sushi and PancakeSwap are some examples of popular DEXs that distribute LP tokens to their liquidity providers.

Automated Market Makers

- (AMMs) allow digital assets to be traded without permission and automatically by using liquidity pools instead of a traditional market of buyers and sellers.
- On a traditional exchange platform, buyers and sellers offer up different prices for an asset.

Impermanent Loss

- Liquidity pools are primarily in pairs e.g. ETH/USD.
- Providing liquidity for DEXs is a type of yield farming and some investors see it as more profitable than just buying and holding because LPs receive rewards from trading fees.
- However, LPs lose money due to Impermanent Loss (IL)

Blockchain in Agriculture

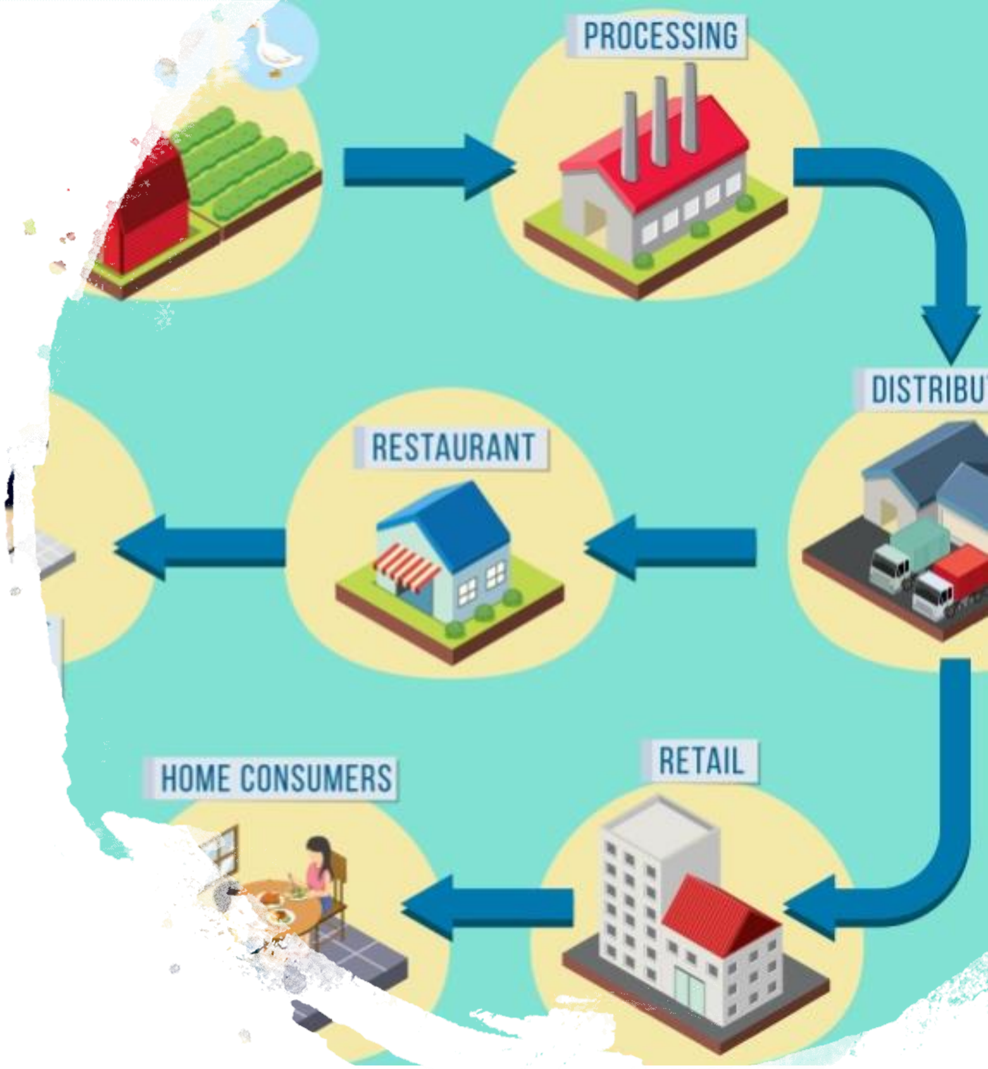
- Blockchain technology has the potential to bring transparency, traceability, and efficiency to various aspects of the agriculture industry.

Blockchain in Agriculture

- Here are some ways in which blockchain can be applied in agriculture:
  - Supply Chain Traceability
  - Smart Contracts for Agreements
  - Quality Assurance
  - Payment and Transactions
  - Data Management and Sharing
  - Asset Tokenization
  - Insurance and Risk Management
  - Regulatory Compliance
  - Decentralized Marketplaces
  - Carbon Footprint Tracking

Supply Chain Traceability

- Provenance Tracking:
- Blockchain can be used to create an immutable and transparent ledger of every transaction within the supply chain.
- This allows consumers to trace the journey of agricultural products from the farm to the table, ensuring the authenticity of the product and providing information about its origin, processing, and transportation.



Smart Contracts for Agreements

- Automated Transactions:
- Smart contracts, which are self-executing contracts with the terms directly written into code, can be employed for various agreements in agriculture.
- This includes contracts between farmers and suppliers, distributors, or buyers.
- Automated transactions can streamline processes and reduce the risk of fraud.

Quality Assurance

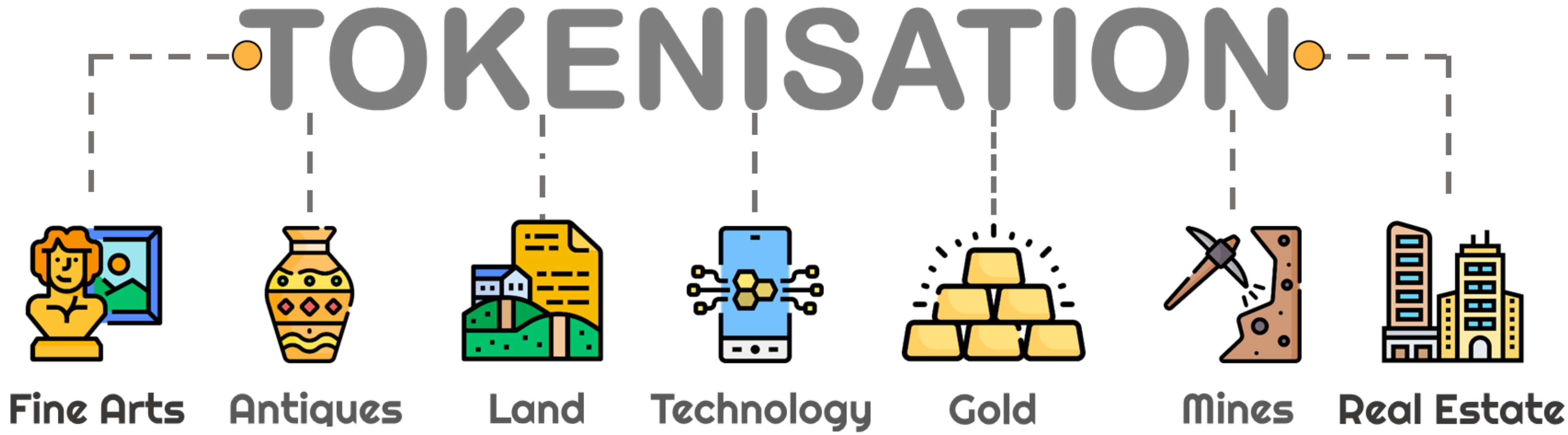
- Record-Keeping:
- Blockchain can be used to maintain a secure and unalterable record of data related to crop quality, certifications, and compliance with regulatory standards.
- This information can be easily accessible to stakeholders, reducing the chances of fraud or misinformation.

Payment and Transactions

- Financial Transactions:
- Blockchain can facilitate transparent and secure financial transactions within the agriculture supply chain.
- This is particularly beneficial for international trade, where parties may not have established relationships and trust.
- Blockchain ensures that payment is made only when predetermined conditions are met.

Data Management and Sharing

- Decentralized Data Storage:
- Decentralized storage on the blockchain can enhance data security and integrity.
- Farmers can control access to their data and share it with trusted parties, such as researchers, insurers, or government agencies, without compromising privacy.



Asset Tokenization

- Fractional Ownership:
- Blockchain can enable the tokenization of agricultural assets, allowing farmers to raise capital by selling fractional ownership of their land, equipment, or crops.
- This can provide new opportunities for investment and financial inclusion in the agriculture sector.

Insurance and Risk Management

- Parametric Insurance:
- Blockchain, combined with smart contracts, can automate insurance processes.
- Parametric insurance, where payouts are triggered by predefined parameters (such as weather conditions), can be efficiently managed on a blockchain, reducing delays in claims processing.

Regulatory Compliance

- Immutable Records:
- Blockchain's immutability ensures that once data is recorded, it cannot be altered.
- This feature is beneficial for compliance purposes, providing a trustworthy and transparent record that can assist in regulatory audits.

Decentralized Marketplaces

- Direct Transactions
- Blockchain can support decentralized marketplaces, allowing farmers to connect directly with buyers.
- This eliminates the need for intermediaries, reduces transaction costs, and ensures fair compensation for farmers.

Carbon Footprint Tracking

- Environmental Impact
- Blockchain can be used to track and verify the environmental impact of agricultural practices.
- This is particularly relevant in sustainable and organic farming, where consumers are increasingly interested in the carbon footprint of the products they purchase.

References

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

Aparicio, J. T., Romao, M. & Costa, C. J. (2022) "Predicting Bitcoin prices : The effect of interest rate, search on the internet, and energy prices," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-5, IEEE

Bernardino, C, Costa, J. & Aparício, M. (2022) "Digital Evolution: blockchain field research," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6, IEEE

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

Cesario, F., J. Costa, C., Aparicio, M., & Aparicio, J. (2023). Blockchain Technology Adoption: Factors Influencing Intention and Usage. In A. R. da Silva, M. M. da Silva, J. Estima, C. Barry, M. Lang, H. Linger, & C. Schneider (Eds.), Information Systems Development, Organizational Aspects and Societal Trends (ISD2023 Proceedings). Lisbon, Portugal: Instituto Superior Técnico. ISBN: 978-989-33-5509-1. https://doi.org/10.62036/ISD.2023.9

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

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

González-Mendes, S, González-Sánchez, R., Costa, C. & García-Muiña, F. (2023) "Analysing the state of the art of Blockchain application in Smart Cities: A bibliometric study," 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), Aveiro, Portugal, pp. 1-6, doi: 10.23919/CISTI58278.2023.10211371.

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

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

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