TPI: BLOCKCHAIN

Instructor: Luis A. Huergo

Students: Agustín Granes, Luca Vigna, Luciano Vega and Fabrizio Giordanelli

Year: 4 Division: AO

Teacher: Malvasio, Martin

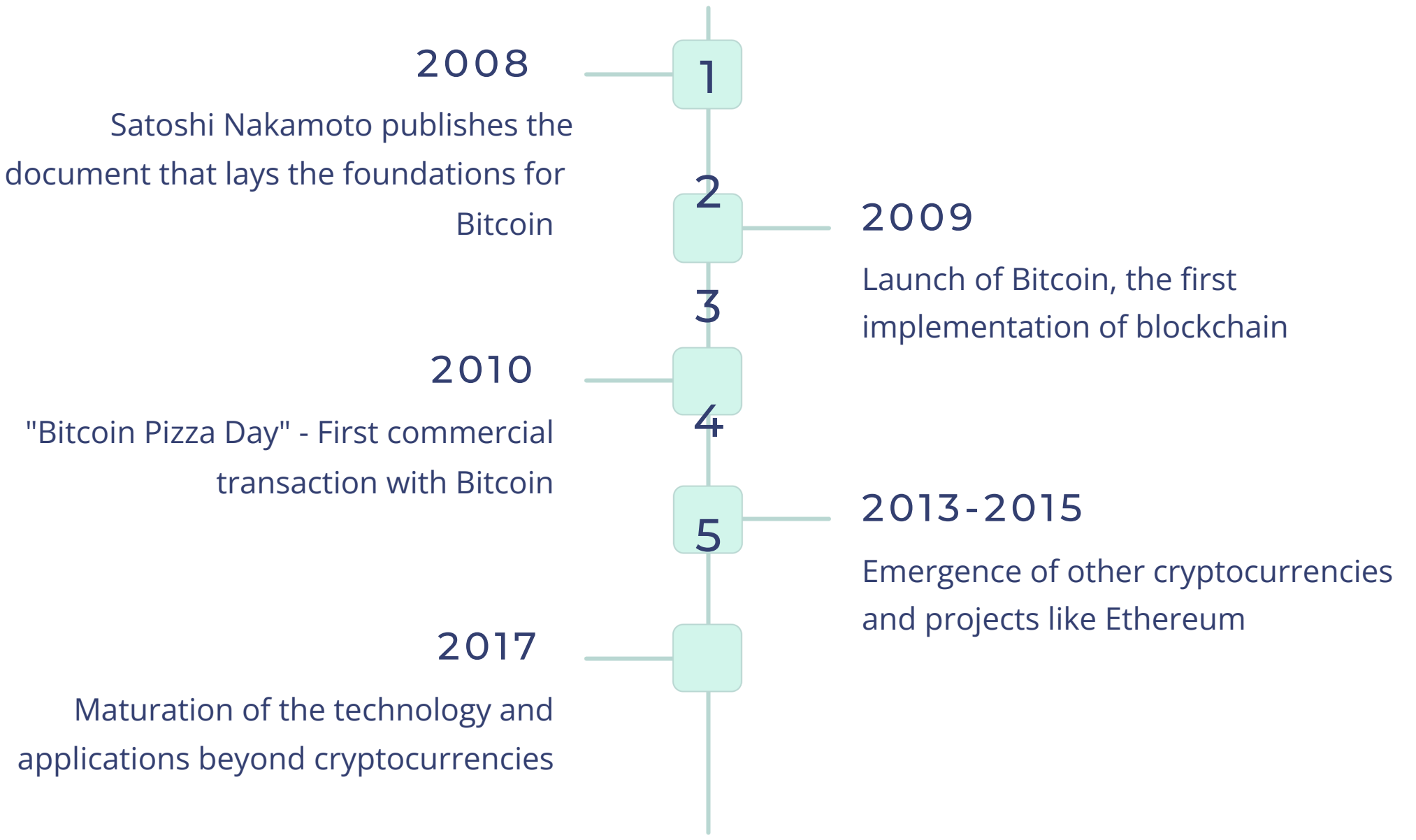
por Agustin Ignacio GRANES

History of Blockchain

It began in 2008, when a person or group under the pseudonym of Satoshi Nakamoto published a document titled "Bitcoin: A Peer-to-Peer Electronic Cash System". This document laid the foundations for the development of Bitcoin, the first cryptocurrency and the first application of blockchain technology.

The first implementation of a blockchain occurred with the launch of Bitcoin in 2009. The main idea was to create a decentralised digital money system that would allow secure transactions without the need for an intermediary, such as a bank. During the early years, Bitcoin was primarily used by technology and cryptography enthusiasts. However, it gradually began to gain acceptance and recognition.

In 2010, the first known commercial transaction using Bitcoin took place: the purchase of two pizzas for 10,000 bitcoins. This event, known as "Bitcoin Pizza Day", is a milestone in the history of the cryptocurrency. As interest in Bitcoin increased, so did interest in the underlying technology, blockchain.



Basic Blockchain Operation

As mentioned before, it is a distributed data structure that ensures the integrity and security of transactions without the need for intermediaries. This technology is based on decentralisation, cryptography and consensus to operate efficiently and securely.

In a blockchain, information is grouped into blocks. Each block contains a set of transactions, a timestamp and a cryptographic link to the previous block, thus forming a chain. This structure ensures that once a block is added to the chain, it is practically impossible to alter it without modifying all the previous blocks, providing immutability.
When a transaction is made, it is transmitted to a network of nodes, which are computers running the blockchain software. The nodes verify the validity of the transaction using cryptographic algorithms, ensuring that the sender has the necessary funds and that the transaction complies with the protocol rules.
Once the transaction is verified, it is grouped with other transactions into a block that is added to the chain. This is where consensus comes into play, which is the process by which the nodes in the network agree on the validity and order of the blocks. There are several consensus mechanisms, the most common being Proof of Work (PoW) and Proof of Stake (PoS).

Security and Cryptography

These elements ensure the integrity, confidentiality and authenticity of transactions and data stored in the blockchain. The combination of advanced cryptographic techniques and consensus mechanisms provides a secure and tamper-resistant environment.

Decentralisation

Unlike traditional centralised databases, where a single point of failure can compromise data integrity, the blockchain distributes information across the aforementioned network of nodes. Each node stores a complete copy of the blockchain, making it extremely difficult for an attacker to alter the information without being detected.

Hash Functions

Cryptographic hash functions are one of the most important tools in this context. A hash function takes data input and produces a fixed-length output, unique to that input. Any change in the input results in a completely different output, allowing the detection of data alterations.

In the blockchain, each block contains a hash of the previous block, creating an immutable chain. If an attacker attempts to modify a block, the block's hash will change, breaking the chain and alerting the network to the tampering.

Public and private keys also play a fundamental role in the security of the blockchain. Each user possesses a pair of cryptographic keys: a public key, which is used as an address to receive transactions, and a private key, which is used to sign and authorise transactions. Public-key cryptography ensures that only the owner of the private key can authorise transactions from their address, thus protecting the authenticity and confidentiality of the transactions.

Impact on the Economy

Blockchain technology has had a significant impact on the global economy, transforming various sectors and creating new opportunities.

In the financial sector, blockchain has revolutionised the way transactions are carried out. Cryptocurrencies, such as Bitcoin and Ethereum, have created an alternative financial system that has significantly reduced the costs of international transactions and improved financial inclusion, allowing unbanked individuals to access financial services. Additionally, blockchain technology has facilitated the creation of new financial instruments, such as tokens and digital assets, which offer new forms of investment and diversification.

Furthermore, thanks to its security system, companies can track products from their origin to the final consumer, ensuring authenticity and reducing the risk of fraud. This is particularly important in industries such as food, where traceability is crucial for product safety and quality. The blockchain's ability to provide an immutable record of transactions has also facilitated auditing and regulatory compliance, reducing costs and improving trust among the involved parties. The adoption of blockchain has also driven the creation of new industries and jobs. The demand for blockchain developers, cryptography experts, and security professionals has increased significantly. Additionally, the technology has fostered the growth of new companies and startups that are exploring innovative applications in various areas.

Challenges and Limitations

Blockchain technology, despite its numerous benefits and innovative applications, faces a series of challenges and limitations that must be addressed for its widespread adoption and use. These challenges include issues of scalability, energy consumption, regulation and governance, privacy and security, among others.

Challenge	Root Cause	Possible Solution Implement
Scalability	Limitations in the ability to process transactions in real-time	solutions such as sharding, Lightning Network, or sidechains Adopt
Energy Consumption	High dependence on consensus mechanisms like Proof of Work	alternative mechanisms such as Proof of Stake or Proof of Authority
Security	Risk of 51% attacks or errors in smart contracts	Promote regular audits, code testing, and develop more resilient systems Incorporate
Privacy	Transparent transactions that can expose sensitive information	advanced encryption techniques like zk-SNARKs or privacy protocols like Monero or Zcash

The adoption of blockchain also faces challenges related to usability and education. The technology can be complex and difficult to understand for non-technical users. The lack of user-friendly interfaces and a steep learning curve can deter individuals and businesses from adopting blockchain-based solutions. It is crucial to develop accessible tools and platforms that facilitate the use of the technology and provide education and resources to help people understand and leverage its benefits.

The Present of Blockchain

At present, blockchain technology has consolidated itself as an essential tool in various sectors, demonstrating its capacity to revolutionise processes and improve efficiency. Its adoption has grown exponentially, and more and more industries are exploring and applying blockchain-based solutions to solve complex problems and create new opportunities.

Financial Sector

Cryptocurrencies, such as Bitcoin and Ethereum, have gained significant acceptance and are being adopted by traditional financial institutions and new market players. Decentralised finance (DeFi) has emerged as an important trend, allowing people to access financial services without traditional intermediaries.

Supply Chain

The adoption of blockchain in the supply chain has improved the transparency and traceability of products. Companies around the world are using blockchain-based solutions to track the origin and journey of products, ensuring authenticity and reducing the risk of fraud.

Other Applications

The technology is also being explored in areas such as energy, governance, art, and media. In the energy sector, blockchain enables the creation of decentralised energy networks, where users can buy and sell energy directly with each other.

In summary, the present of blockchain is a period of accelerated growth and adoption, with innovative applications in multiple sectors and an evolving infrastructure. The technology has demonstrated its ability to transform processes and improve efficiency, and its impact continues to expand as more industries discover and leverage its benefits.

The Future of Blockchain

The future of blockchain technology is full of promises and opportunities. As the technology continues to evolve, we are likely to see even greater adoption and the development of new innovative applications across various sectors. There are several trends and advancements that indicate how the future of blockchain might unfold.

Application Area	Primary Use	Key Benefit
Decentralised Finance (DeFi)	Provide financial services such as lending, savings, and insurance without intermediaries	Greater financial accessibility and reduced costs
Supply Chain Management	Track and verify products throughout the supply chain	Transparency and reduced fraud
Digital Identity	Create unique and secure digital identities for individuals and businesses	Personal data protection and greater control over information
E-Governance	Automate and authenticate real-time voting and governance processes	Greater transparency and citizen participation

Interoperability between different blockchains will also be a crucial aspect in the future. The ability to transfer data and assets across multiple blockchain networks will enable greater collaboration and the creation of more integrated ecosystems.

Opinion on the Importance of Blockchain

Blockchain technology has proven to be a transformative innovation with a significant impact on multiple industries and the global economy. Its importance lies in its ability to provide a secure, transparent and decentralised infrastructure, which enables transactions and data management to be carried out efficiently and reliably through traceability and important security measures.

However, there are several issues that need to be addressed. Many malicious people are using the cryptocurrency system to carry out scams, for example: The company "Kelsen Ventures" launched its own cryptocurrency, the alleged profits of which would be used to support entrepreneurial projects in Argentina. This project was supported and publicised by the President of Argentina, Mr Javier Gerardo Milei, who was defrauded just like the users who bought $LIBRA. What was the scam? People who had access to the project and its information bought at the second 0 of the crypto's release, which would be impossible without knowing or having information about the project's launch. After massively buying at second 0, they wait a few minutes and massively withdraw the money, causing the cryptocurrency to lose its value, but they take the profit. This scam is called a "Rug Pull", a scam in which several famous people were defrauded, such as "Haliey Welch", who created her own crypto with the help of a company, whose employees carried out this scam.

Likewise, the credibility and trust of the people (although it is increasing), is still not total. Therefore, it is necessary to educate people who do not know how to buy crypto, which takes time (like any adaptation to new technologies).

Frequently Asked Questions

What is Bitcoin?

Bitcoin is a cryptocurrency, that is, a form of digital money that operates in a decentralised way without the intervention of central authorities, such as banks or governments. It emerged in 2009, the result of the vision of an entity or group under the pseudonym of Satoshi Nakamoto, with the aim of providing a secure, transparent payment system without centralised control.

What is Blockchain?

Blockchain is a distributed ledger technology that allows transactions to be tracked and verified in a transparent, secure and immutable way. It is made up of a chain of blocks, where each block stores a set of transactions along with an identifying code (hash) that links it to the previous block, creating a linear sequence that makes any attempt to alter it difficult.

What is a Decentralised App?

A decentralised application, known as a dApp, is software that operates on a distributed network, generally based on blockchain, rather than relying on a central server or infrastructure controlled by a single entity. This architecture allows the application to function autonomously and without single points of failure, increasing resistance to attacks and censorship.

What is a Smart Contract?

A smart contract is a self-executing computer program that operates on a blockchain network and allows agreements between parties to be established and fulfilled in an automated way. Essentially, it is a set of instructions and conditions that, once met, trigger actions without the need for human intervention.