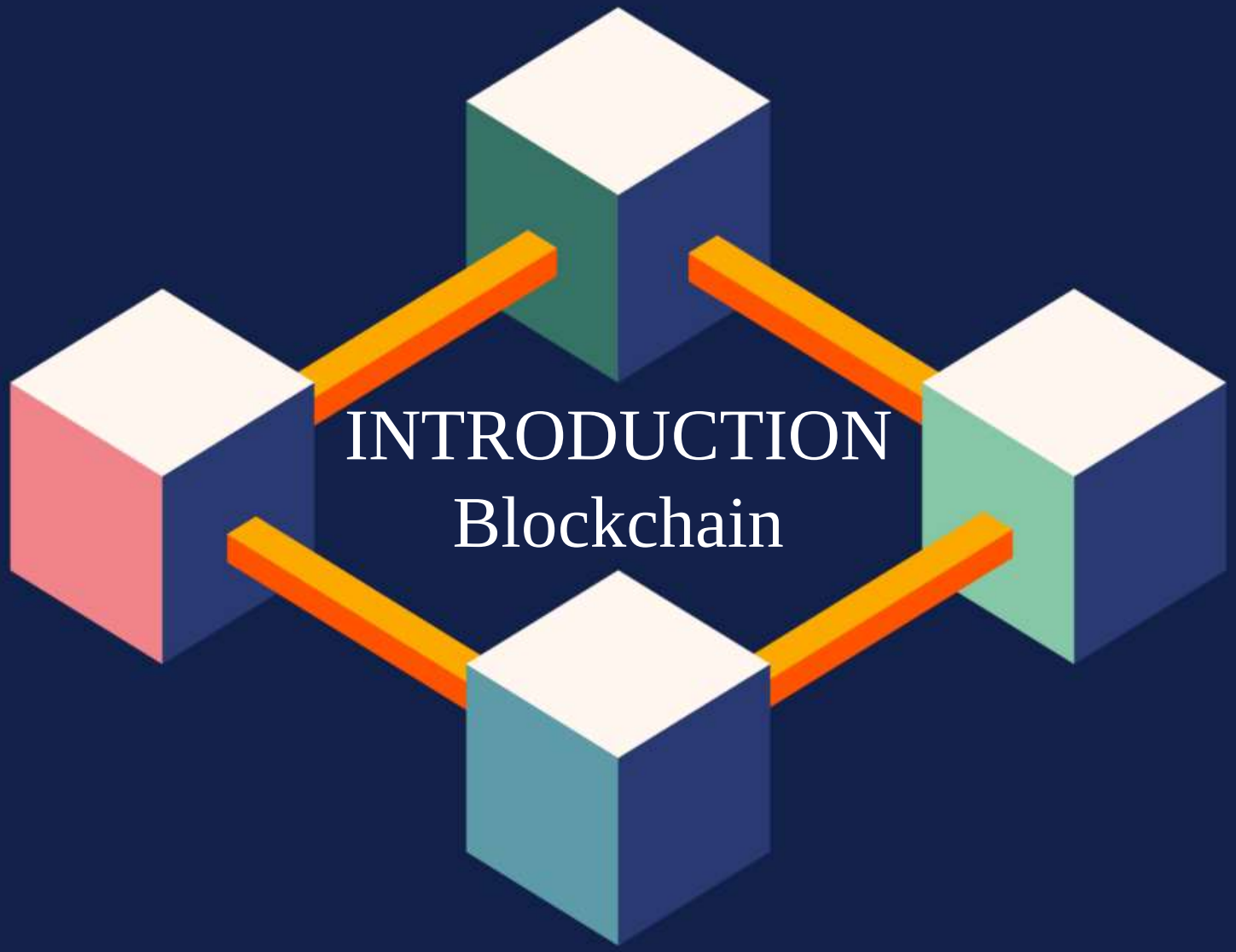
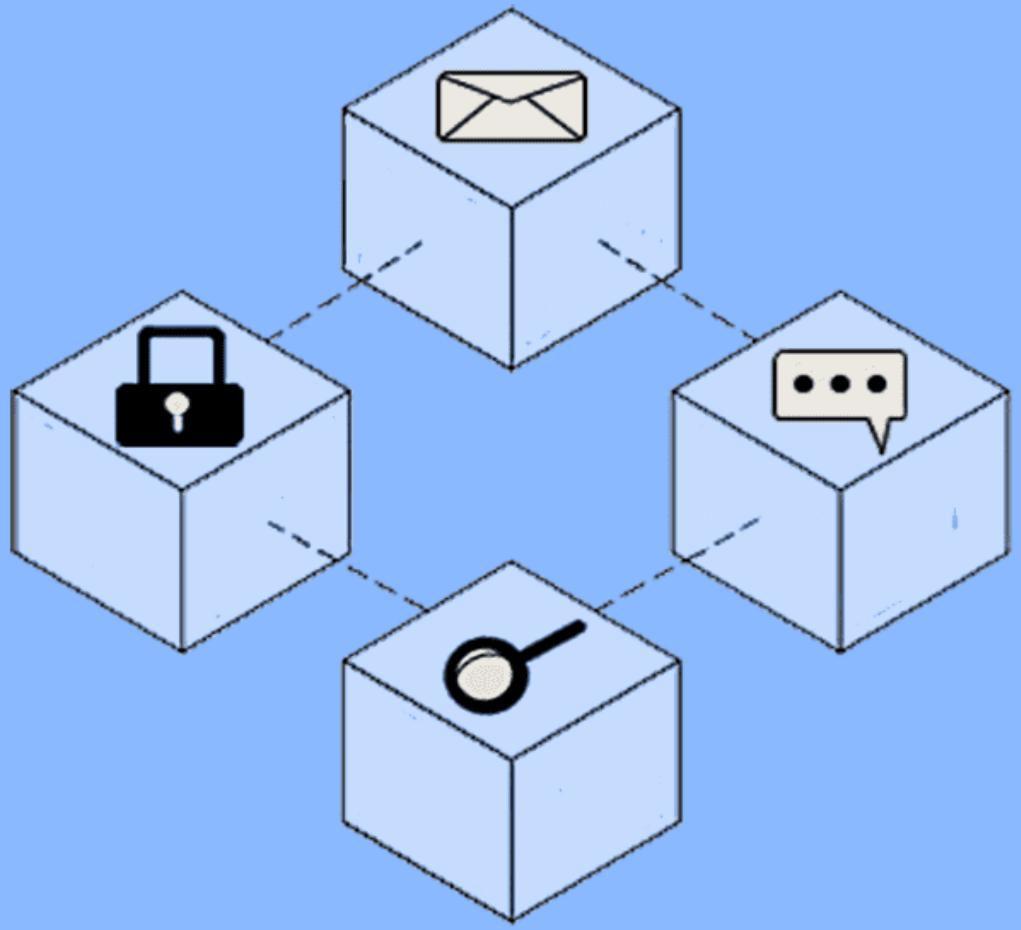
SEMINAR PRESENTATION

TOPIC: BLOCKCHAIN

SUBMITTED BY: VAISHAK RAJESH S6 BCA
DEPARTMENT OF COMPUTER SCIENCE
REG NO:220021086141



INTRODUCTION
Blockchain



Blockchain

['bläk-,chān]

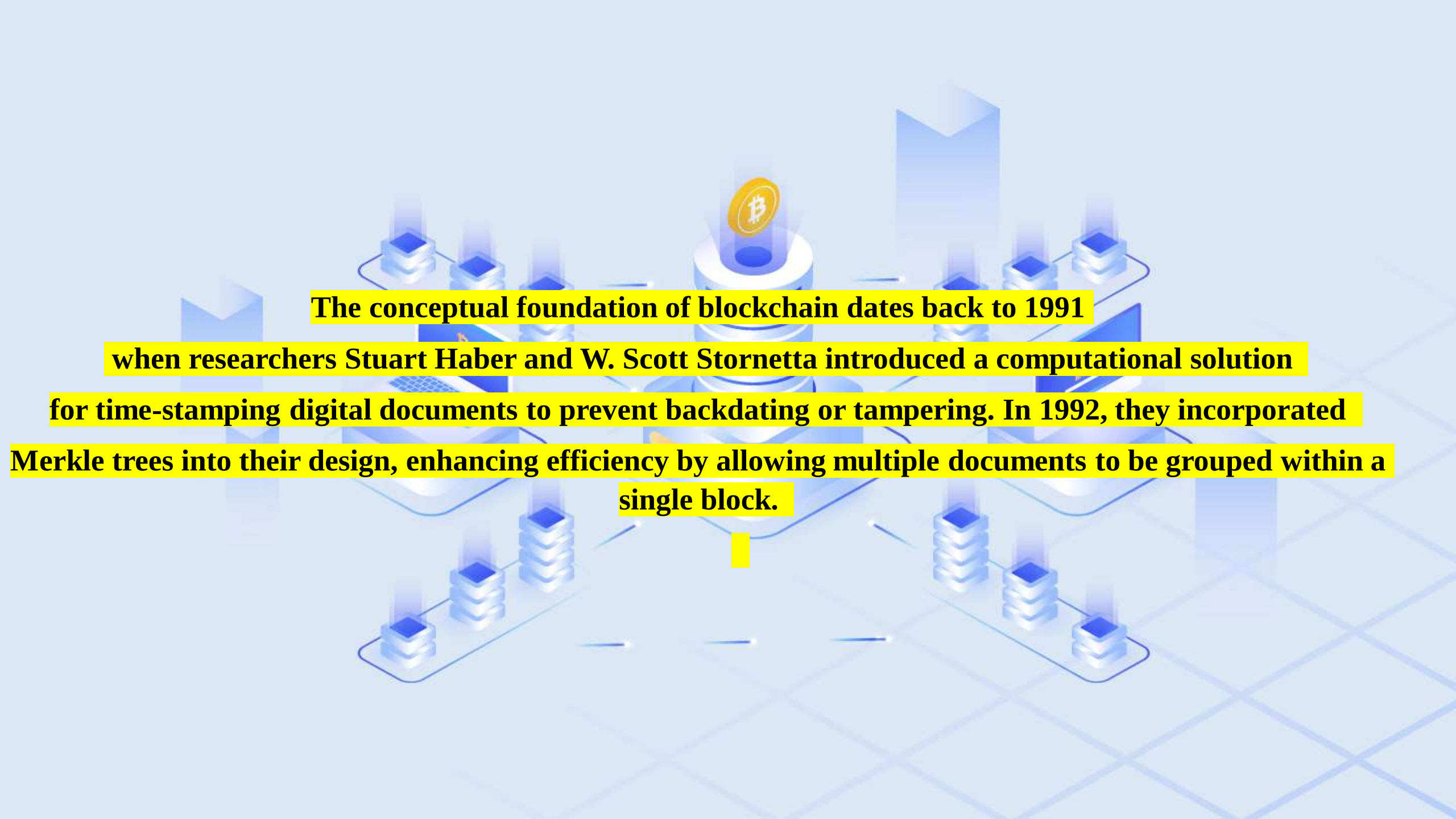
A digital database or ledger that is distributed among the nodes of a peer-to-peer network.

Blockchain is a distributed ledger technology that enables
the secure and transparent recording
of transactions across a
network of computers.
In this system,data is stored in blocks,
each containing a collection of transactions.

These blocks are linked chronologically in a chain through cryptographic hashes, ensuring the integrity and immutability of the recorded information.

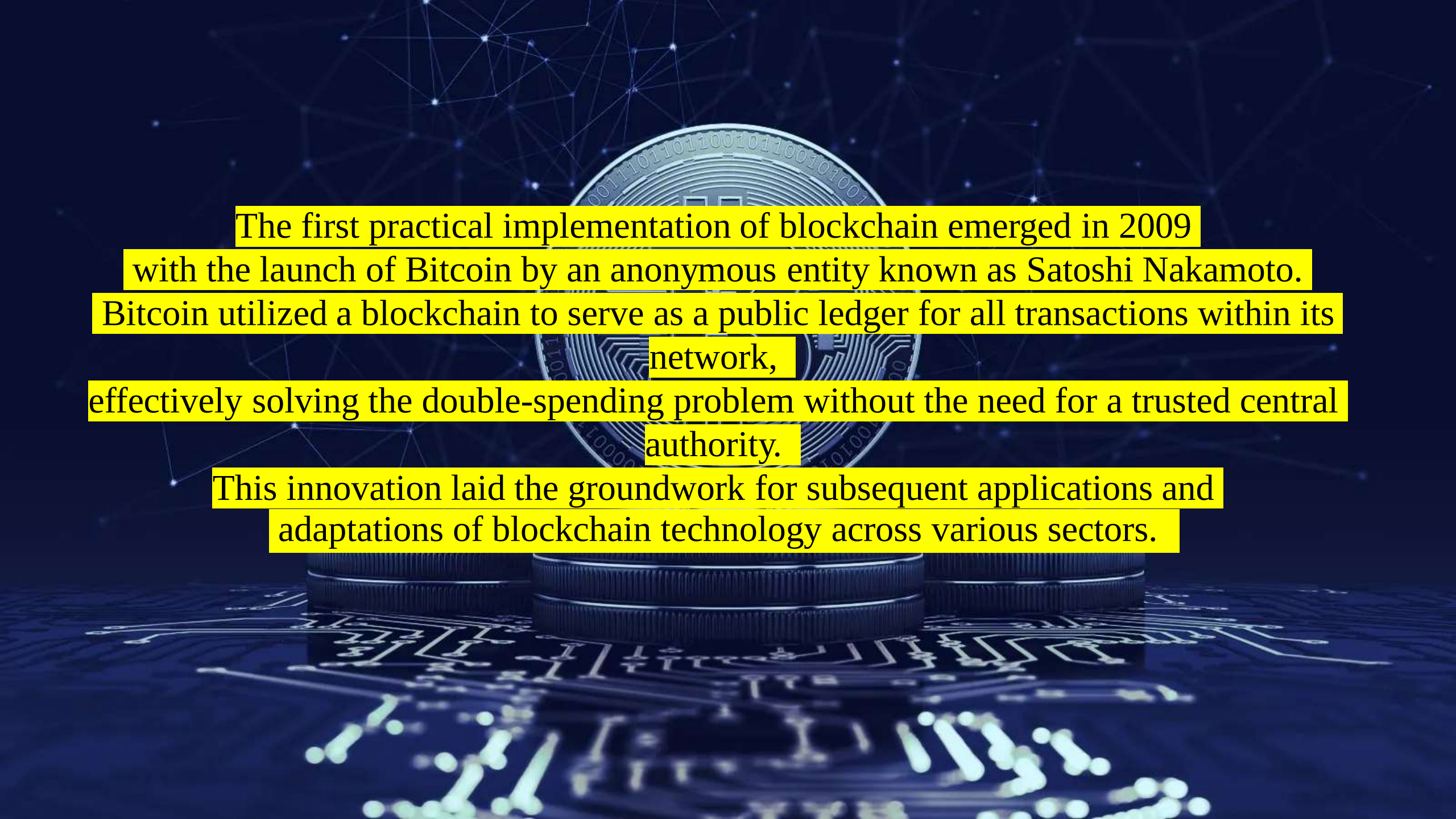
This decentralized structure eliminates the need for a central authority, allowing participants to verify and audit transactions independently.

HISTORY OF BLOCKCHAIN

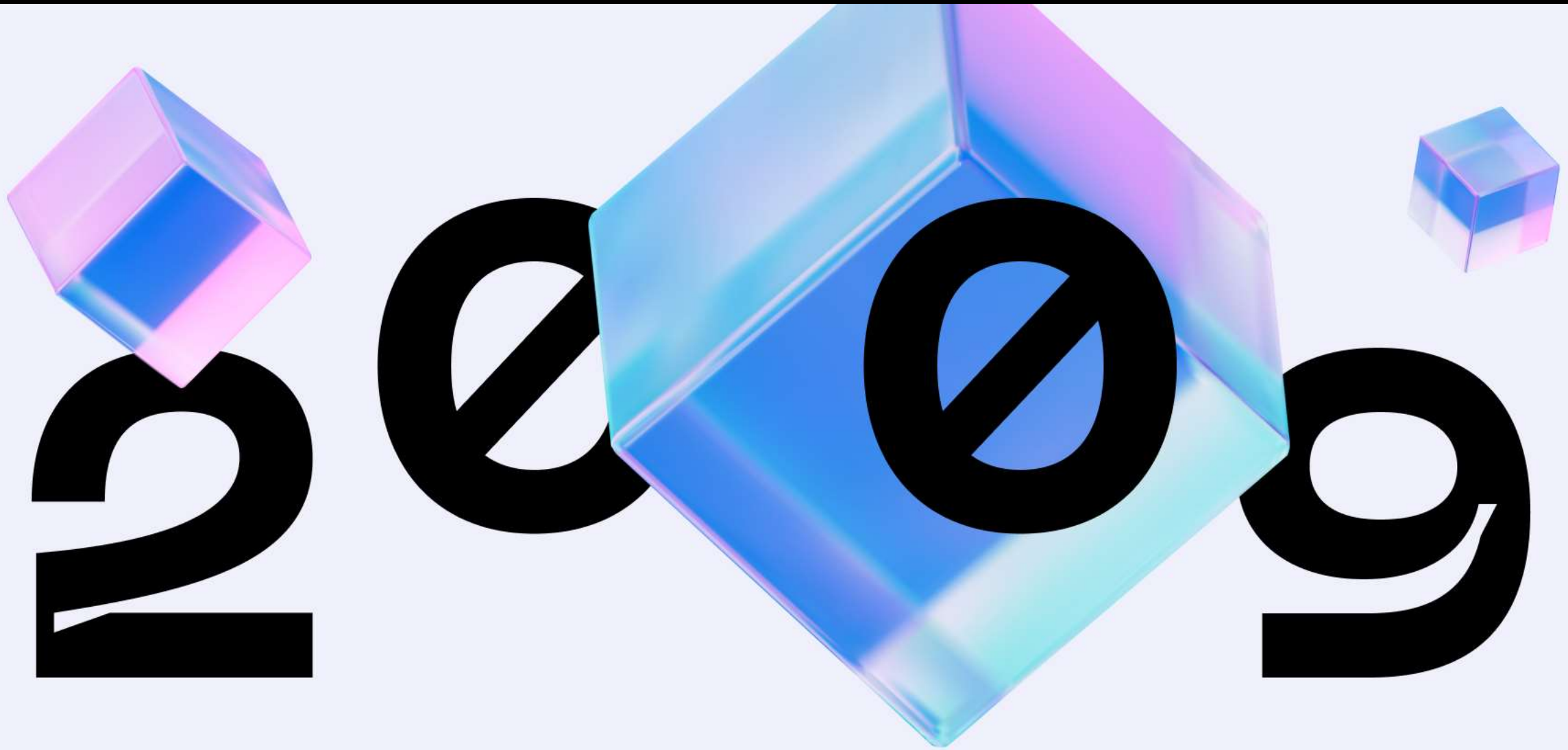


The conceptual foundation of blockchain dates back to 1991 when researchers Stuart Haber and W. Scott Stornetta introduced a computational solution for time-stamping digital documents to prevent backdating or tampering. In 1992, they incorporated Merkle trees into their design, enhancing efficiency by allowing multiple documents to be grouped within a single block.

Satoshi
Nakamoto
Bitcoin creator



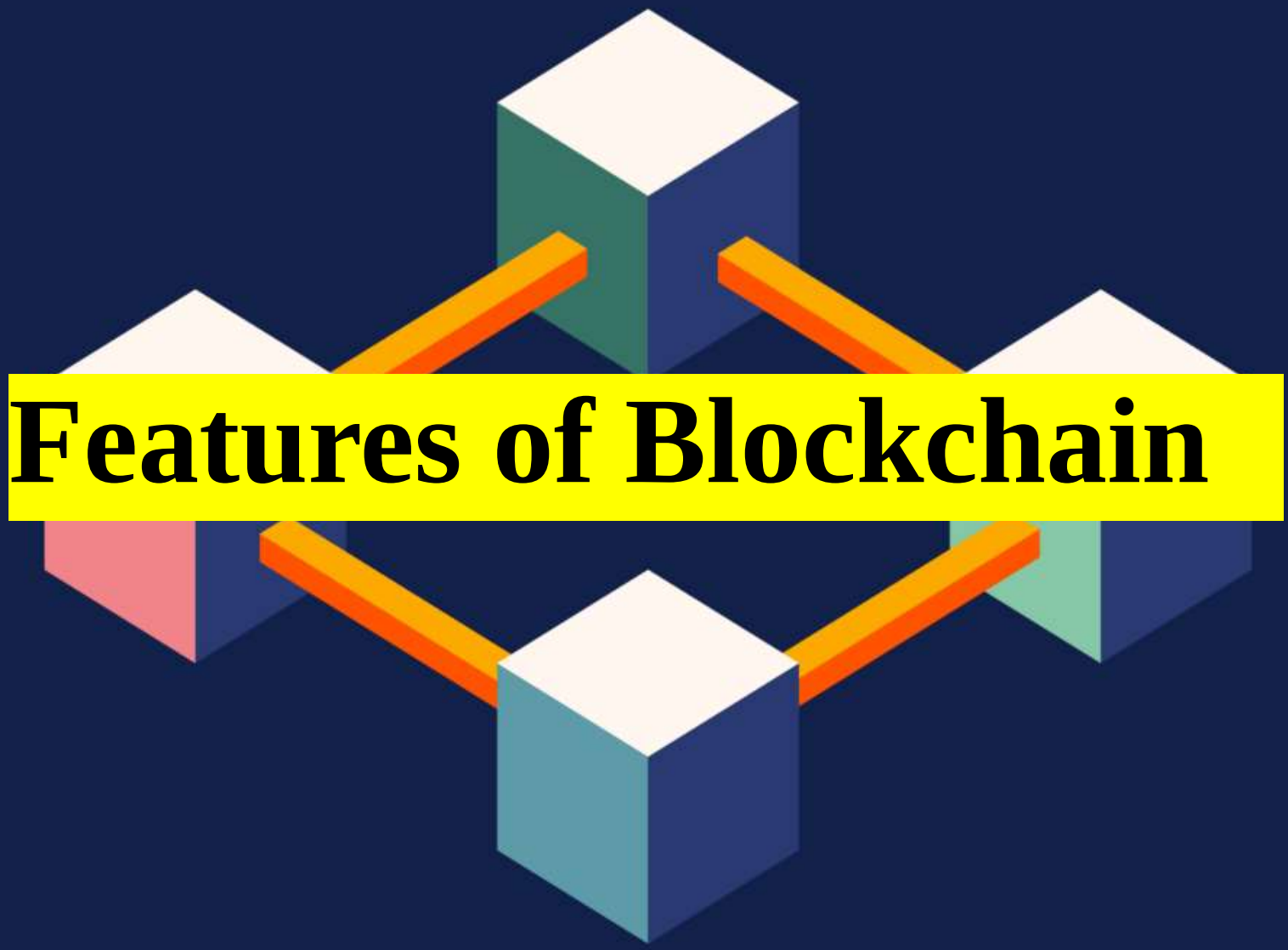
The first practical implementation of blockchain emerged in 2009 with the launch of Bitcoin by an anonymous entity known as Satoshi Nakamoto. Bitcoin utilized a blockchain to serve as a public ledger for all transactions within its network, effectively solving the double-spending problem without the need for a trusted central authority. This innovation laid the groundwork for subsequent applications and adaptations of blockchain technology across various sectors.



1/15

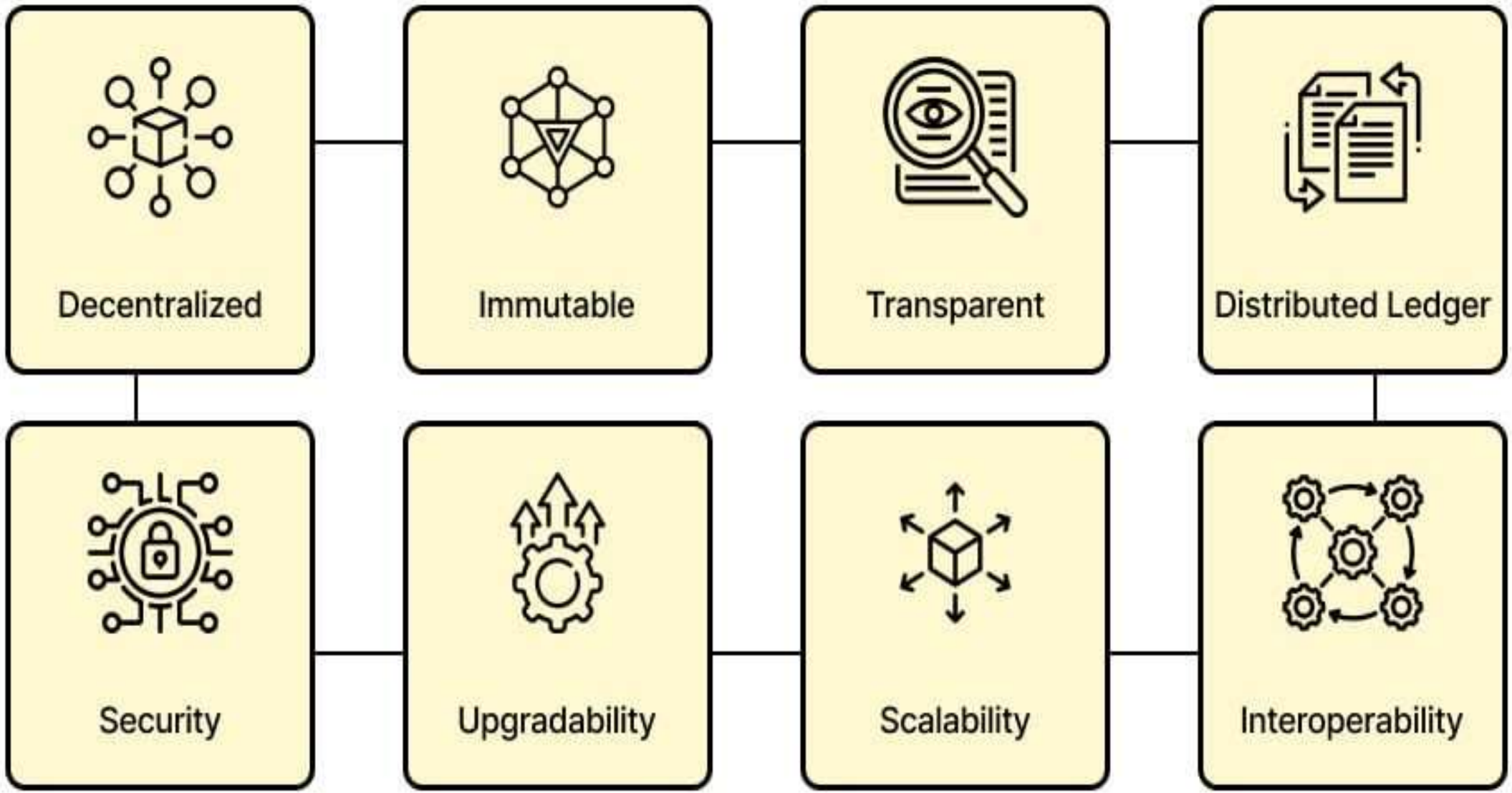
Bitcoin Anniversary

Genesis Block and First BTC Transaction



Features of Blockchain

Features of Blockchain Technology



Decentralization:
Unlike traditional centralized systems, blockchain operates on a decentralized network of nodes, eliminating the need for a central authority. This structure enhances system reliability and
reduces the risk of single points of failure.

Immutability: Once data is recorded on the blockchain, it cannot be altered or deleted. This immutability ensures the integrity and trustworthiness of the information stored.

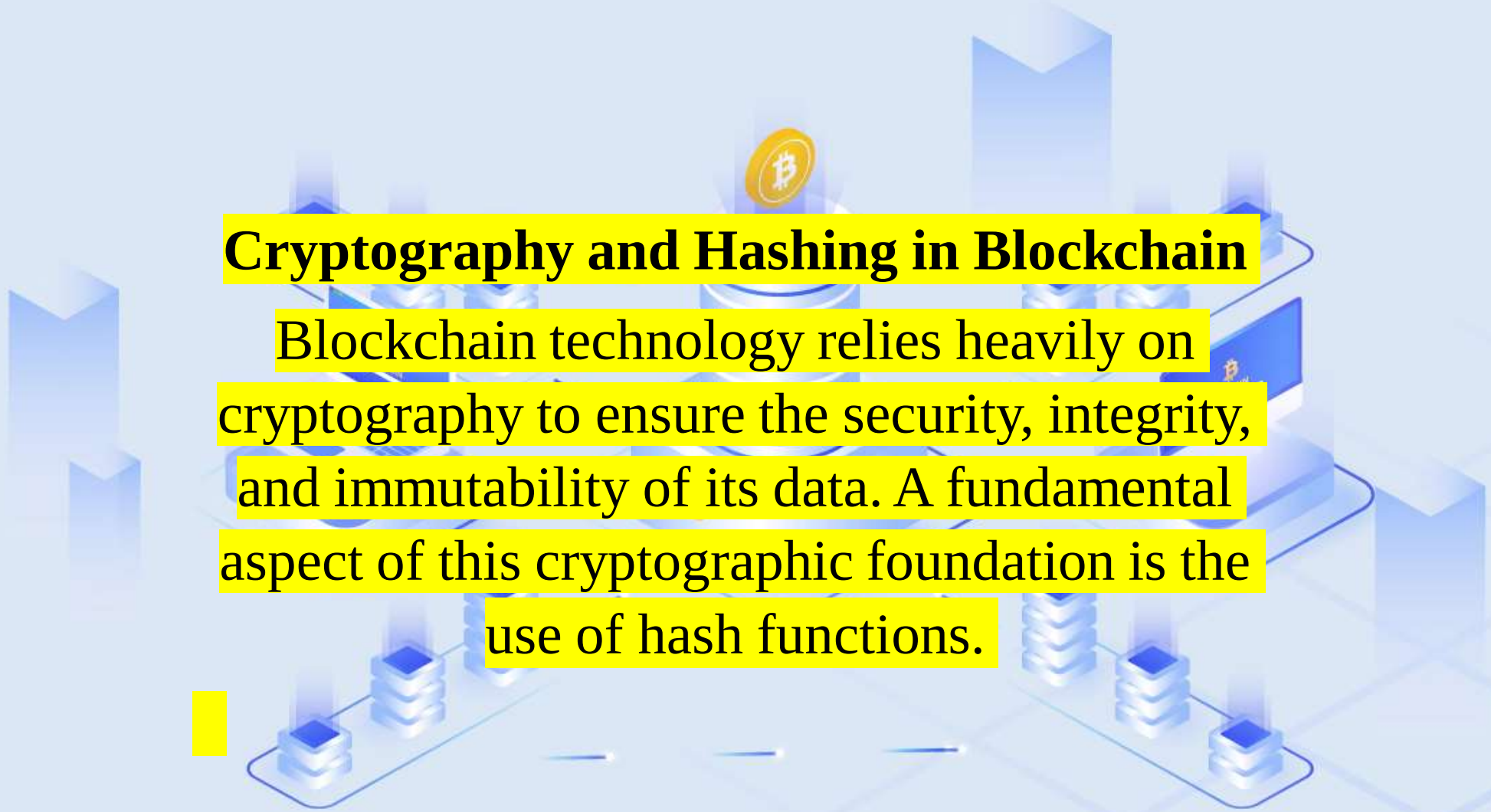
Transparency: All transactions on a public blockchain are visible to all participants, promoting accountability and trust within the network.

Security: Blockchain employs advanced cryptographic techniques to secure data, making it highly resistant to fraud and cyberattacks.

Consensus Mechanisms:

Blockchain networks utilize consensus algorithms, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate transactions and maintain the integrity of the ledger.

BLOCKCHAIN FUNDAMENTALS



Cryptography and Hashing in Blockchain

Blockchain technology relies heavily on cryptography to ensure the security, integrity, and immutability of its data. A fundamental aspect of this cryptographic foundation is the use of hash functions.

Cryptographic Hash Functions

A cryptographic hash function is an algorithm that transforms input data of any size into a fixed-size string of characters, typically a hexadecimal number. This output, known as a hash, is unique to each unique input; even a minor change in the input data results in a significantly different hash. This property is crucial for verifying data integrity, as any alteration in the original data will produce a different hash, signaling tampering.

Common Hash Functions in Blockchain

Several cryptographic hash functions are utilized in blockchain technology:

- **SHA-256**: Used extensively in Bitcoin and other cryptocurrencies, SHA-256 produces a 256-bit hash value and is known for its security and reliability.
- **SHA-3**: The latest member of the Secure Hash Algorithm family, offering enhanced security features.
- **Blake3**: Known for its speed and security, Blake3 is gaining attention for its efficient performance.

Consensus Mechanisms in Blockchain:

Proof of Work (PoW) and Proof of Stake (PoS)

In blockchain networks, consensus mechanisms are protocols that ensure all participants agree on the validity of transactions and the state of the ledger. They are essential for maintaining the integrity and security of decentralized systems. Two of the most prominent consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS).

Blockchain architecture and components

Blockchain architecture is the underlying framework that enables decentralized, secure, and transparent data management across a network.

1. Nodes: The Backbone of the Network

Nodes are individual devices—such as computers or servers—that participate in the blockchain network

2. Ledger: The Immutable Record

The ledger is a decentralized and immutable record of all transactions within the blockchain network. Unlike traditional centralized databases, this ledger is distributed across all nodes, ensuring transparency and resistance to tampering.

3. Blocks: Structured Data Containers

Blocks are fundamental units that contain a set of transactions.

4. Transactions: The Core Operations

Transactions are the basic operations that transfer data or value between participants in the network.

5. Consensus Mechanisms: Ensuring Network Agreement

Consensus mechanisms are protocols that ensure all nodes in the network agree on the validity of transactions and the state of the ledger.

6. Smart Contracts: Automated Agreements

Smart contracts are self-executing contracts with the terms directly written into code. They automatically enforce and execute agreements when predefined conditions are met, eliminating the need for intermediaries and reducing the potential for disputes.

Decentralized Applications (dApps): Blockchain-Based Software

dApps are software programs that operate on a blockchain or peer-to-peer (P2P) network, rather than a single computer. They are collectively controlled by users, eliminating central authority. Often built on platforms like Ethereum, dApps serve various purposes, including finance, gaming, and social media.

BLOCKCHAIN APPLICATIONS

Supply chain management and logistics

Blockchain technology is revolutionizing supply chain management and logistics by enhancing transparency, security, and efficiency. Its decentralized and immutable nature addresses longstanding challenges in these sectors.

Financial services and banking

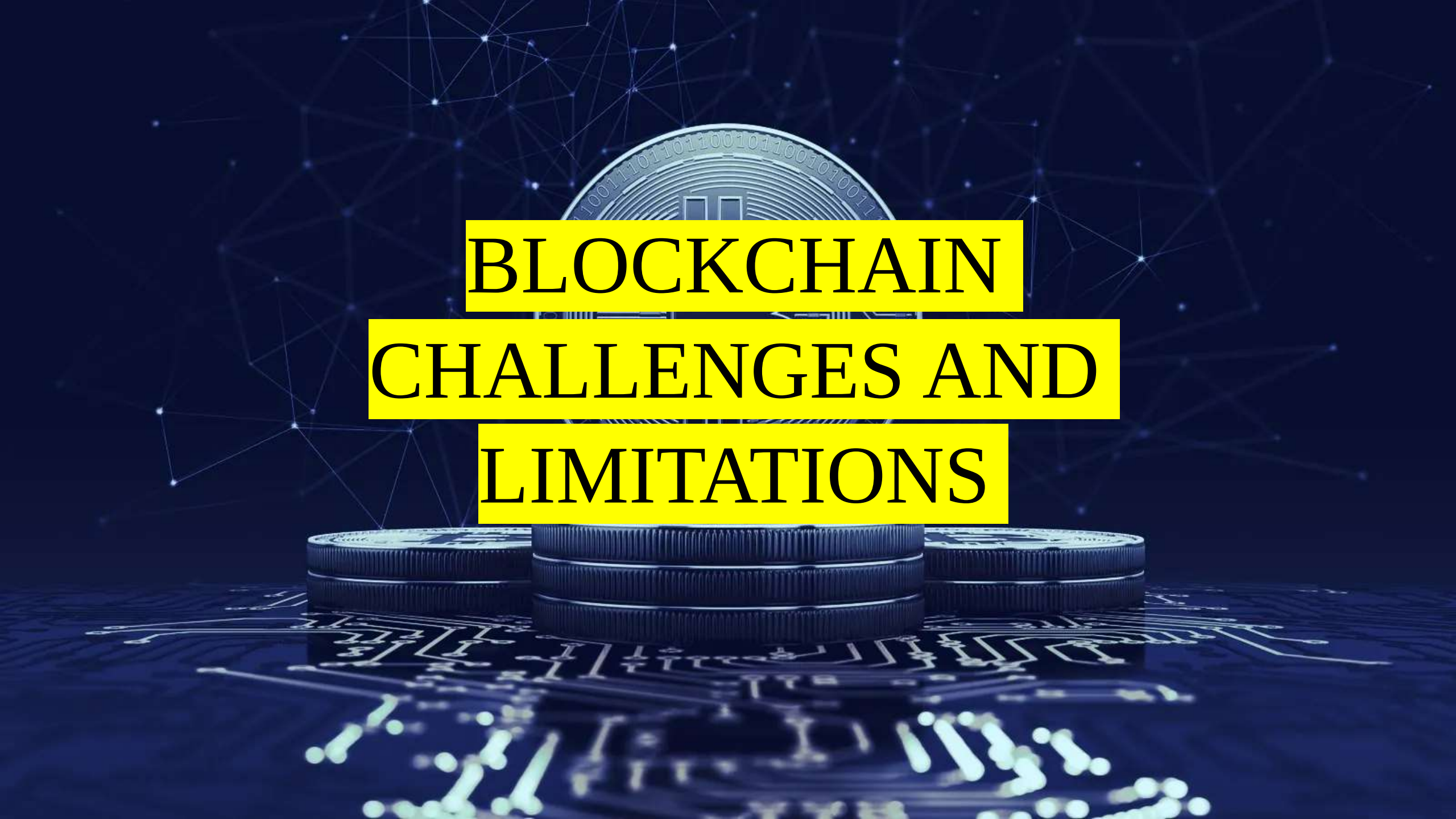
Blockchain technology is revolutionizing the financial services and banking sectors by introducing enhanced efficiency, security, and transparency. Its decentralized nature offers numerous applications that are transforming traditional financial operations.

Healthcare and medical records management

Blockchain technology is increasingly being explored in healthcare, particularly for managing electronic health records (EHRs). Its inherent features—decentralization, immutability, and security—offer promising solutions to longstanding challenges in medical records management.

Cybersecurity and data protection

Blockchain technology is emerging as a pivotal tool in enhancing cybersecurity and data protection across various sectors. Its inherent characteristics—decentralization, immutability, and transparency—address numerous challenges associated with traditional security measures.


BLOCKCHAIN
CHALLENGES AND
LIMITATIONS

Scalability and performance issues

Blockchain technology has revolutionized various industries by introducing decentralized and secure systems. However, scalability and performance remain significant challenges that hinder its widespread adoption.

Security risks and vulnerabilities

Blockchain technology, while celebrated for its decentralized and secure framework, is not impervious to security risks and vulnerabilities.

Security risks and vulnerabilities

Blockchain technology, while celebrated for its decentralized and secure framework, is not impervious to security risks and vulnerabilities.

LIKE

51% Attacks

Smart Contract Vulnerabilities

Phishing Attacks

Energy consumption and environmental impact

Blockchain technology, particularly cryptocurrencies like Bitcoin, has been scrutinized for its substantial energy consumption and environmental impact like

High Energy Consumption

Carbon Emissions

E-Waste Generation

FUTURE ENHANCEMENT

Emerging trends and technologies

Blockchain technology continues to evolve, giving rise to emerging trends and innovations collectively referred to as "Blockchain 3.0." This phase aims to address limitations of earlier blockchain versions, enhancing scalability, interoperability, and real-world applicability.

Convergence with Artificial Intelligence (AI):

The integration of AI with blockchain technology is opening new avenues for innovation. This convergence enhances data analysis, decision-making processes, and the creation of more intelligent decentralized applications, leading to more personalized and efficient user experiences.

THANK

SUBMITTED BY:
VAISHAK RAJESH
S6 BCA
DEPARTMENT OF COMPUTER SCIENCE