INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Abstract

The "Introduction to Blockchain Technology" chapter offers a thorough rundown of the fundamental ideas and ideas that underpin blockchain technology. Being a disruptive breakthrough that has broad repercussions for many different industries, professionals, researchers, and fans alike must grasp the foundations of blockchain technology. The fundamental elements of blockchain technology are analyzed, emphasizing the distributed and decentralized character of the ledger. We demystify the cryptographic techniques used to safeguard transactions and preserve the blockchain's integrity, illuminating how consensus processes uphold trust in a context devoid of trust. The chapter also explores blockchain network types, differentiating between public and private blockchains. Examined are real-world use cases from a variety of industries, including supply chain, healthcare, and banking, to show the broad range of uses and revolutionary potential of blockchain technology.

Keywords: Blockchain, industries, professionals, researchers, healthcare.

Author

Shaik Mulla Almas
Assistant Professor
Department of Information Technology
Vasireddy Venkatadri Institute of Technology
Andhra Pradesh, India
mulla.almas@gmail.com

Pathan Mahamood Khan
Assistant Professor
Department of Electrical and Electronics Engineering, Vasireddy Venkatadri Institute of Technology
Andhra Pradesh, India.
pathanmehemudkhan@gmail.com

Dr. K. Kavitha
Associate Professor
Department of Computer Science Engineering, Annamalai University
Chidambaram
Tamil Nadu, India.
kavithacseau@gmail.com

Copyright © 2024 Authors

I. INTRODUCTION

1. What is Blockchain?

Blockchain is a peer-to-peer, decentralized, and distributed system. It is cryptographically secure, append-only, immutable, and updateable via a consensus or agreement among all the peers.

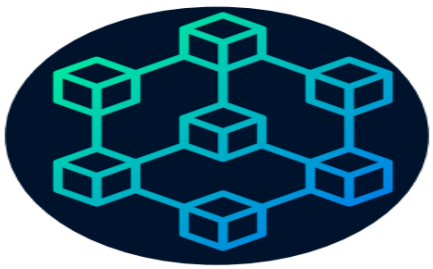


Figure 1: Showing Blockchain architecture

2. Components of Block:

The block consist of block header and body.

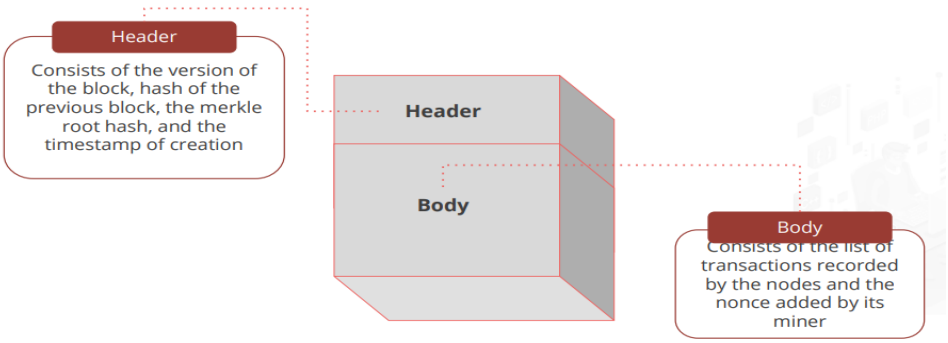


Figure 2: Showing Block Header and Block Body

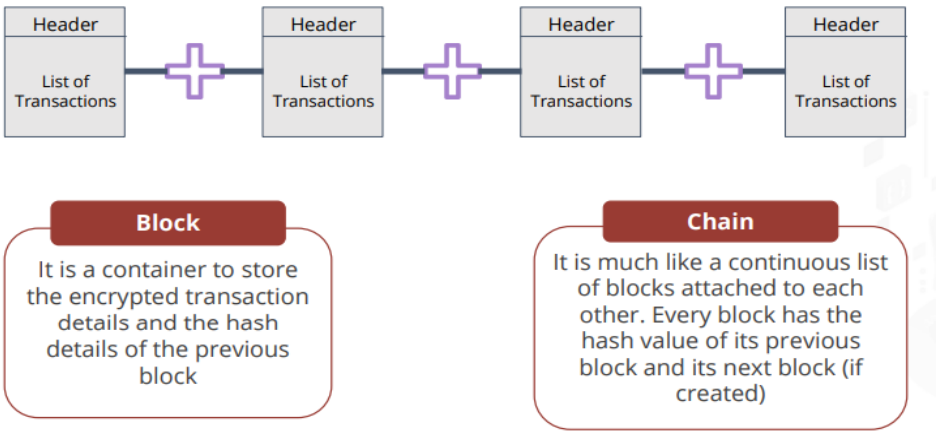


Figure 3: Showing Chain of Blocks

Copyright © 2024 Authors

II. HISTORY OF BLOCKCHAIN

Let us have a look at the history and evolution of Blockchain.

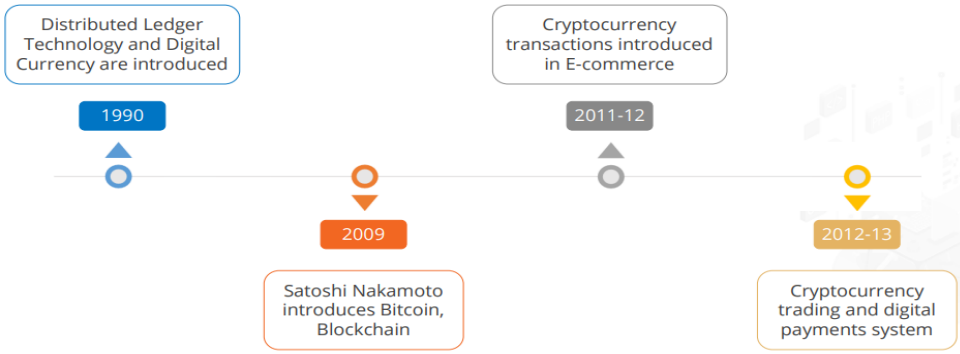


Figure 4: Evolution of Blockchain

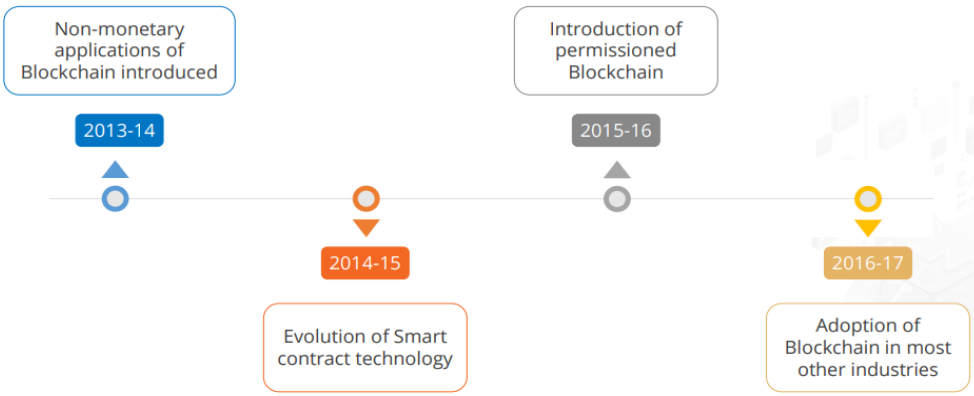


Figure 5: Evolution of blockchain

1. **Features of Blockchain:** Some of the features of Blockchain are Transparency, Immutability, High Availability, Cost Efficiency, Security.

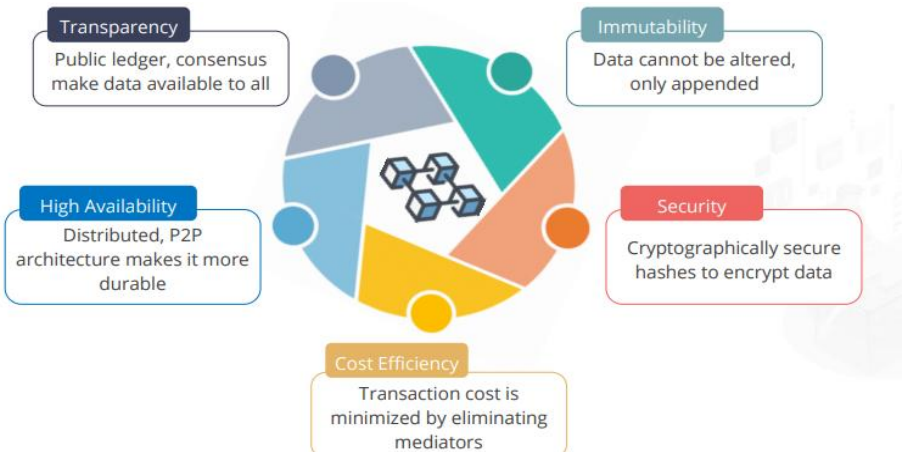


Figure 6: Features of Blockchain

Copyright © 2024 Authors

2. Difference Between Blockchain and Database:

Let us discuss about the difference between Blockchain and Database.

Database	Blockchain
Centralized network	Decentralized and distributed (peer-to-peer) network
All CRUD operations are supported	Only append operation possible
Data can be changed anytime with the correct privileges	Data is completely immutable in an ideal scenario
Difficult to scale for high availability	Highly available as distributed network is implemented
Data is not completely private. The database admin can read all the data present	Only hashes of actual data are encrypted and stored in the block

Figure 7: Difference between Blockchain and Database

III. NEED FOR BLOCKCHAIN

Challenges posed by modern organizations are addressed by blockchain technology in numerous important ways. These difficulties include:

1. **Trust and Transparency:** Blockchain offers a transparent, decentralized system in which every member has access to the same data. As a result, there is no longer a need for intermediaries and stakeholder trust is increased.

2. **Data Security:**Data security is provided by blockchain, which uses strong cryptographic algorithms to protect data and make it extremely hard to tamper with or gain unauthorized access to. This reduces the danger of data breaches and improves the security of vital company information.

3. **Supply Chain Management and Traceability:** With blockchain, firms can monitor and confirm the provenance of products all the way through the supply chain. This increases logistics and inventory management efficiency, boosts traceability, and decreases counterfeiting.

4. **Automation and Smart Contracts:** Blockchain allows for the execution of smart contracts, which are self-executing agreements with predefined conditions. These contracts streamline company operations, eliminate intermediaries, and ensure contractual trust and transparency.

5. **Interoperability and Efficiency**: Blockchain enables the secure and frictionless sharing of data across businesses and systems. It promotes interoperability by standardizing standards, minimizing friction, and streamlining procedures, resulting in enhanced efficiency and collaboration.

Copyright © 2024 Authors

By addressing these issues, blockchain technology has the ability to transform modern business by improving trust, security, efficiency, and collaboration across multiple industries.

IV. COMPONENTS OF BLOCKCHAIN

The components of a blockchain typically include the following:

1. **Distributed Ledger:** The distributed ledger is the central component of a blockchain. It's a decentralized database that keeps track of all transactions and data over a network of computers called nodes. Each node keeps a duplicate of the complete blockchain, which ensures redundancy and robustness.

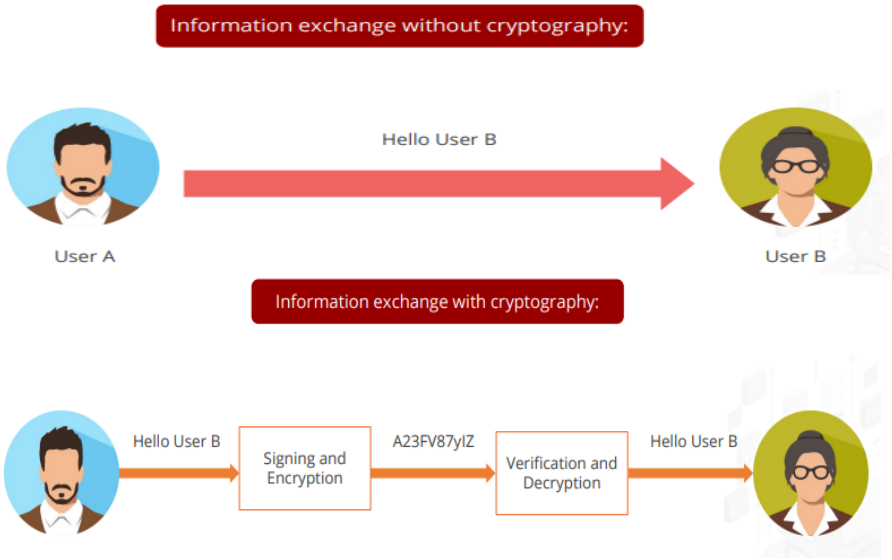
2. **Evolution of Distributed Ledger:**

3. **Blocks:** Blocks are data structures that hold a collection of transactions or information. A cryptographic hash connects each block on the blockchain to the preceding block, producing a chain of blocks. This connection secures the data recorded in the blockchain's integrity and immutability.

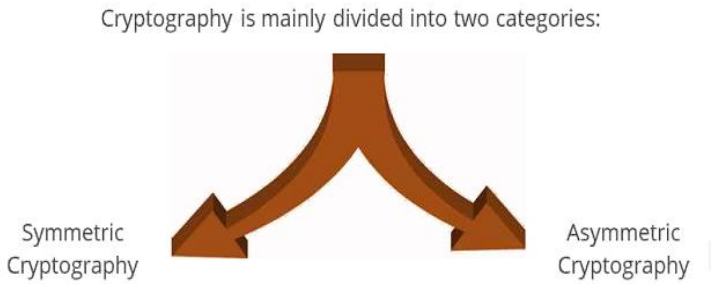
4. **Cryptography:** Cryptography is essential in blockchain because it provides security and anonymity. It uses cryptographic techniques to encrypt and decrypt data, as well as digital signatures to authenticate the validity and integrity of the data.

   - **Introduction to Cryptography:**

Copyright © 2024 Authors



- **Cryptography Categories:**



- **Keys in Cryptography:**

  Keys in cryptography are used to secure the information. There are two types of keys:

- **Public Key:**
  - A public key is a publicly available cryptographic key that can be obtained and used by anyone to send the encrypted messages to a particular recipient.
  - No one else would be able to decrypt the message because the corresponding private key is held securely by the intended recipient.
  - Once the public key encrypted message is received, the recipient can decrypt the message using a second (private) key.

Copyright © 2024 Authors

- **Private Key:**
  - A private key is a highly secure variable that is randomly generated and kept secretly by the owner of the key.
  - It needs to be protected and no unauthorized access should be granted to it.
  - It is used in cryptography with algorithms to encrypt and decrypt the data.

- **Symmetric Cryptography:** Symmetric Cryptography is a type of cryptography where the same key is used for encryption and decryption of data.

- **Asymmetric Cryptography:** Asymmetric Cryptography is a type of cryptography where the encryption key is different from the decryption key.

- **Consensus Mechanism:** Consensus mechanisms are protocols that ensure all blockchain network participants agree on the state of the ledger. They allow nodes to agree on the legitimacy of transactions and the sequence in which they are added to the blockchain. Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) are examples of consensus mechanisms**.**

V. OBJECTIVES OF BLOCKCHAIN CONSENSUS MODELS

1. **Coming to an Agreement:** The mechanism gathers all the agreements from the group as much as it can.

2. **Collaboration:** Every one of the group aims toward a better agreement that results in the groups interest as whole.

3. **Co-operation:** Every individual will work as a team and put their own interests as a aside.

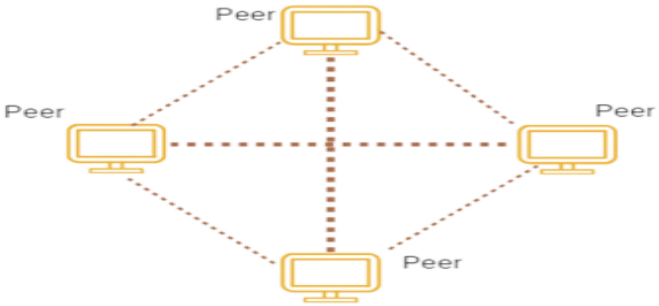
4. **Equal Rights:** Every single participant has the same value in voting.This means that every person’s vote is important.

Types of Consensus Algorithms in Blockchain:

1. **Proof of Work**
2. **Proof of Stake**
3. **Proof of Authority**
4. **Proof of Elapsed time**

- **Peer-to-Peer Network:** A blockchain runs on a peer-to-peer network, which allows all nodes to communicate and share information with one another. This decentralized network eliminates the need for a central authority or middleman, improving the blockchain's security, transparency, and resilience.

Copyright © 2024 Authors



- **Smart Contracts:** Smart contracts are self-executing contracts that have established rules and circumstances.

These components work together to produce a safe, transparent, and decentralized system for recording and verifying blockchain transactions.

VI. BLOCKCHAIN TECHNOLOGY HAS THE FOLLOWING CHARACTERISTICS

1. **Decentralization:** Blockchain functions on a decentralized network of computers known as nodes, in which no single party has complete control of the system. Because of its decentralization, no central authority can change or control the data contained in the blockchain.

2. **Transparency:** Blockchain enables transparency by allowing all network participants to view the same information. The blockchain records each transaction and data entry, establishing an immutable and auditable history of occurrences**.**

3. **Security:** To secure data and transactions, blockchain uses cryptographic algorithms. A cryptographic hash connects each block to the previous block, resulting in a tamper-evident system. Furthermore, consensus procedures ensure that transactions are securely confirmed and uploaded to the blockchain.

4. **Immutability:** Once a transaction or data input is recorded on the blockchain, changing or deleting it becomes extremely difficult. This data immutability maintains the integrity and trustworthiness of the data stored in the blockchain**.**

5. **Trust and Trustlessness:** Blockchain allows people to trust one another without relying on a centralized authority. Blockchain technology's consensus methods and cryptographic algorithms ensure that transactions are approved and verified by the network, eliminating the need for intermediaries.

6. **Efficiency and Speed:** Blockchain offers the ability to automate and streamline a variety of corporate processes. Smart contracts, a blockchain technology, allow for self-executing contracts with predefined rules and conditions. This automation reduces the need for manual intervention and can lower transaction time and expenses dramatically**.**

7. **Interoperability:** Blockchain technology can help diverse systems and organizations communicate with one another. Blockchain facilitates seamless data sharing and

Copyright © 2024 Authors

collaboration between various groups by establishing standardized protocols and data formats.

8. **Privacy and Control:** Blockchain provides privacy features that allow individuals to control and choose to disclose their data. It enables individuals or companies to retain ownership and control over their data while participating in the blockchain network.

These characteristics make blockchain a viable technology for a wide range of applications, including financial transactions and supply chain management, as well as healthcare and identity verification.

VII. TYPES OF BLOCKCHAIN

There are various types of blockchain, each with unique properties and applications. Here are some examples of common blockchains and their applications:

1. **Public blockchains**: Public Blockchain are open to the public and allow any individual or entity to participate. They provide an extremely high level of decentralization, transparency, and security. Bitcoin and Ethereum are two examples. Public blockchain applications include bitcoin transactions, decentralized apps (dApps), and asset tokenization.

2. **Private Blockchains**: Private blockchains are limited to a small number of participants. They are excellent for enterprise use because they provide privacy, control, and scalability. Businesses typically use private blockchains for supply chain management, record-keeping, and inter-organizational cooperation.

3. **Consortium Blockchains:** A consortium or collection of organizations runs a consortium blockchain. They provide a balance of decentralization and control. Consortium blockchains find use in fields where several stakeholders must collaborate, such as finance, healthcare, and logistics.

4. **Hybrid Blockchain**: Hybrid blockchains mix public and private blockchain characteristics. They allow you to take advantage of the benefits of public networks while keeping privacy and control over some areas. Hybrid blockchains can be effective in situations that demand a mix of public and private participation, such as government applications or regulated sectors.

5. **Permissioned Blockchain**: To access and validate transactions on permissioned blockchains, participants must have certain permissions. They offer control, privacy, and regulatory compliance, making them ideal for use in regulated industries like finance and healthcare.

Copyright © 2024 Authors

VIII. DIFFERENCE BETWEEN PRIVATE, PUBLIC AND PERMISSIONED BLOCKCHAIN

	Public	Private	Permissioned
Consensus Determination	All participating members	Only admins	Any member with the right access level
Data Access	Public	Restricted	Restricted to certain degree
Immutability	Almost impossible to tamper	Can be mutated	Can be mutated
Resource Required	Low	High	High
Centralization	No	Yes	Semi-centralized
Consensus Process	Permissionless	Needs permission	Needs permission

Copyright © 2024 Authors