Blockchain for finance and banks

Year: 2023-2024

Prepared by: Mrs. LOUDINI Souad

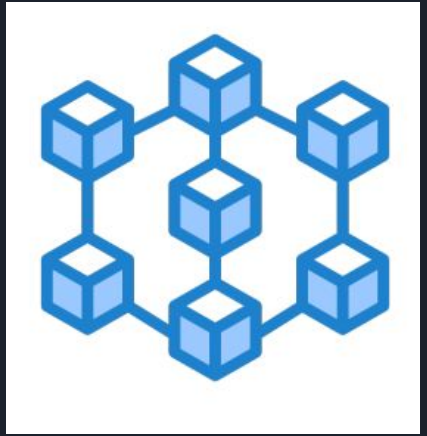
Master : Distributed Information Systems Engineering and Security

An Overview of Blockchain technology

The blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a network.

Distributed ledger technology (DLT) involves a database that is distributed and replicated across a multitude of computers.

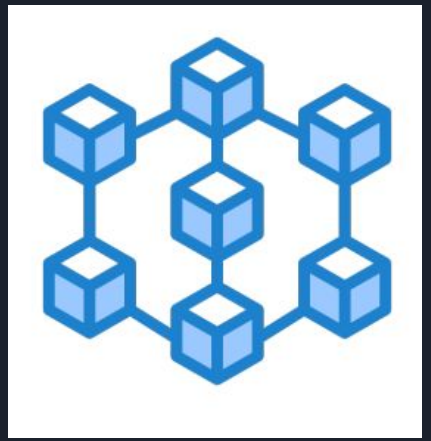
A hash is a mathematical operation that transforms input data of any size into a secure, fixed-length encrypted output. This cryptographic process ensures data integrity and security.



An Overview of Blockchain technology

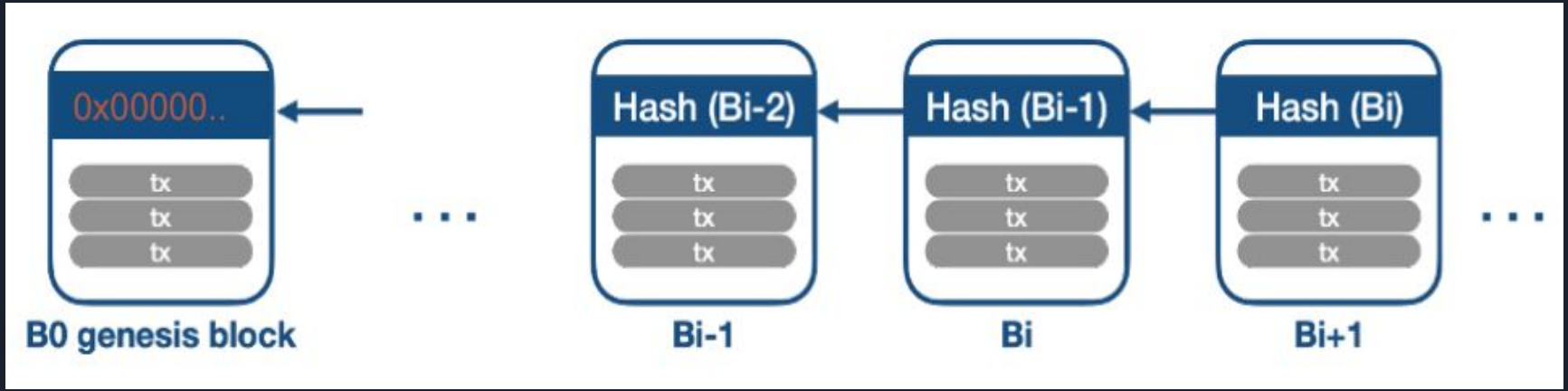
Blockchain is a secure distributed ledger of interconnected blocks of data arranged in chronological order and maintained using consensus agreements. The nodes (computers) of the blockchain network have the same copy (duplicate) of the blockchain.

The blocks are chained in such a way that each block references the hash of its previous block. In this way, blockchain data is protected against tampering. Any modification of blockchain data is detected since a change in any block will change the whole blocks in the network.



What is a blockchain?

- A blockchain is a digital ledger that consists of a series of linked blocks, where each block contains a list of transactions. These blocks are cryptographically secured and connected in a chain.
- Every block contains transaction data, a timestamp, and a cryptographic hash of the previous block, creating a secure link between them.



How does the blockchain work

1

A transaction is requested.
Ex. Alice sends BTC to Bob

Proposed transaction is broadcast through P2P network.

2

3

Nodes verify the transaction validity.

6

Block is added to to the existing blockchain.

The block is broadcast for validation. (**Consensus**)

5

4

The transaction is added to a new block, along ot her recent transactions.

Types of blockchain networks

Public

No central authority, permissionless network

Bitcoin, Ethereum, ..

Private

Controlled by one authority

HyperLedger

Consortuim

Controlled by a group

Some Concepts

1	Blocks	Blocks are batches of transactions with a hash of the previous block in the chain.
2	Chain	Blocks are “chained” together forming a chain of blocks. They are linked because hashes are cryptographically derived from the block data.
3	Nodes	A node is a computer running client software that can verify blocks and transaction data.
4	Network	Nodes are connected to each other, forming a network.

Type of Nodes

the most common types of nodes :

Full Nodes

are crucial in the Blockchain network as they maintain a complete copy of the ledger, allowing them to independently verify all transactions and blocks. Full nodes ensure the integrity of the Blockchain, operate in a peer-to-peer network.

Light Nodes

These nodes store only the essential data and rely on full nodes to function, as they do not download the full blockchain. They are designed for fast, straightforward processing of transactions

Miner Nodes

These nodes are responsible for adding new blocks to the blockchain and are typically found in blockchains that use proof-of-work consensus algorithms.

Consensus

- Consensus mechanisms are an essential part of blockchain technology, as they enable distributed networks to reach agreement on the state of the ledger.the most common ones are :

Proof of work

Miners compete to solve a computationally challenging puzzle in order to create new blocks.

A solution that is difficult to find, easy to verify

Proof of stake

Validators invest in the coins of the system by locking up some of their coins as stakes

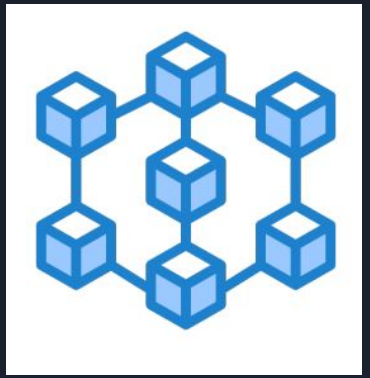
Staking gives you a chance to validate new transactions and earn rewards.

Chapter 1 :
Blockchain in banking services

Key Features and Their Relevance to Banking

Decentralization

In the context of blockchain, decentralization signifies a system where decisions, processes, or data management aren't controlled by a single entity or authority. Instead, control is distributed across all participants in the network.



Key Features and Their Relevance to Banking

Security : Blockchain relies heavily on cryptography to achieve data security . Cryptographic techniques provide digital proof of authorization, protecting transactions and ensuring that only the rightful owner can access their assets.

Transparency: Transparency in decentralized banking is achieved through public ledgers, which provide open access to transaction records. This transparency builds trust among users by allowing them to independently verify transactions and ensures the integrity of the system.

Use Cases in Banking

- **Payments, Cross-border payments :**

  Cross-border payments involve transferring money between different countries or currencies, a process traditionally burdened with challenges.

  Blockchain technology is transforming this landscape by offering a faster, cheaper, and more secure solution.

Use Cases in Banking

- **Accounting and audit :** Blockchain can provide a secure and transparent way to track financial transactions, reducing the risk of errors and fraud .Blockchain applications in supply chain management and financial reporting illustrate its practical benefits.

Use Cases in Banking

- **Syndicated loans :** Blockchain simplifies the loan syndication process by enabling lenders to exchange information securely and efficiently. It offers real-time data access, reduces delays, and automates underwriting through smart contracts. This streamlined approach lowers compliance costs, eliminates intermediaries, and enhances efficiency in loan syndication, benefiting the financial industry.

Challenges and Concerns

- **Scalability**

Blockchain technology faces significant scalability challenges, leading to high transaction costs, slow processing, and network congestion as user numbers and transactions grow. These issues limit the network's ability to handle a large volume of transactions efficiently and cost-effectively.

Challenges and Concerns

- **Integration with existing systems**

Integrating blockchain into existing systems is tough due to compatibility, data migration, change resistance, and resource allocation. Success needs planning, gradual implementation, stakeholder communication, and employee training for better efficiency and security. This is because blockchain often uses different data structures, protocols, and security measures compared to existing systems, making seamless integration a significant effort.

Challenges and Concerns

- **Awareness and understanding**

The lack of awareness and understanding of blockchain technology is a significant barrier to its adoption, especially in non-banking sectors. This lack of awareness can also lead to a lack of trust among potential users.

Challenges and Concerns

- **Privacy Concerns**

While blockchain is often associated with transparency, there are scenarios where privacy is essential. Balancing transparency and privacy is a challenging task. Techniques like zero-knowledge proofs and confidential transactions are being used to enhance privacy on public blockchains.

Clearing and settlement systems

Clearing and Settlement systems

Description:

- **Clearing and settlement** are essential steps in the financial world that help ensure that securities (like stocks) and money change hands securely and correctly after a trade is executed.
- **Clearing** is the process of verifying the legitimacy of a trade and ensuring that both parties have the necessary resources to fulfill their obligations. This is typically done by a central clearinghouse, which acts as a guarantor for both parties to the trade.
- **Settlement** is the process of exchanging funds and securities between the buyer and seller. This is typically done through a settlement system, which is a network of banks and other financial institutions that facilitate the transfer of assets.
- Overall, the clearing and settlement process is a vital part of the financial system. It helps to ensure that trades are executed fairly and efficiently, and that the rights of both buyers and sellers are protected.

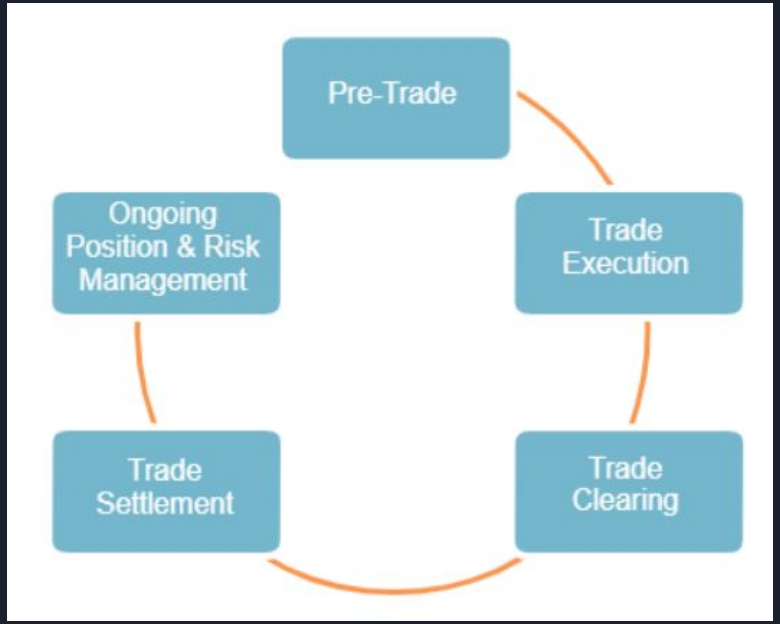
To read more visit this website Clearing and settlement systems

Participants

Clearinghouses	A clearing house is a third party that acts as an intermediary between buyers and sellers of financial instruments like stocks and derivatives. It verifies and matches trades, collects margins from members, and settles them. Clearing houses play a crucial role in the financial system by reducing risk and enhancing transaction efficiency, ensuring both parties fulfill their obligations.
Central securities depositories (CSDs)	CSDs are intermediaries that hold securities on behalf of their clients. They facilitate the transfer of ownership of securities between buyers and sellers.
Broker	A broker is a financial professional who acts as an intermediary between investors and financial markets.

Life cycle of trading

- Pre-Trade: The pre-trade step in clearing and settlement systems is the process of preparing for the trade execution.
- Trade Execution : This is the stage where the buyer and seller agree on the terms of the trade and execute it. The trade is then reported to the clearinghouse.
- Trade Clearing :The clearinghouse verifies the trade and matches it with the corresponding counterparty trade. The clearinghouse also calculates the margin requirements for each party and collects margin from the parties.
- Trade Settlement: The clearinghouse transfers ownership of the assets and funds between the buyer and seller.
- Risk Management : The clearinghouse monitors the positions of its members and manages the risk of defaults.

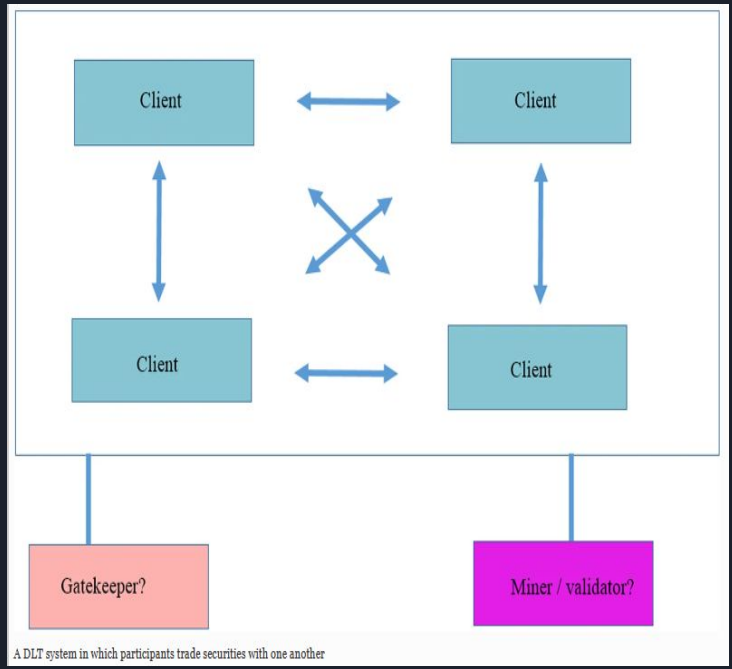


An Example of the clearing and settlement lifecycle for a stock trade

1. An investor places an order to buy 50 shares of Apple stock through their broker.
2. The trader places an order with a broker.
3. The broker sends the order to the clearing house.
4. The clearing house matches the order with an order from a seller who wants to sell 50 shares of stock A.
5. The clearing house verifies that both parties have the necessary funds or assets to complete the trade.
6. The clearing house collects margin from both parties to protect against losses.
7. The clearing house settles the trade by exchanging the buyer's and seller's shares.

Blockchain-Based Clearing and Settlement Process Overview

- Two clients enter into a trade and sign the transaction using their private keys.
- The signed transaction is broadcast to the entire DLT system for validation.
- Validators verify the transaction, including that the seller is the rightful owner of the securities being sold.
- Once consensus is reached on the validity of the transaction, it is added to the ledger.
- All participants of the DLT system receive an updated copy of the ledger.
- The settlement process is with the validation process, meaning that the new asset ownership is reflected in the system immediately.



figure

A Comparison of Traditional and Blockchain-Based Clearing and Settlement Systems

------	**Traditional systems**	**Blockchain-based settlement system**
Clearing process	In a traditional clearing system, a central clearing counterparty (CCP) acts as an intermediary between the buyer and seller. The CCP verifies the trades and matches them, and then guarantees the settlement of the trades. This means that the buyer and seller are not exposed to the risk of the other party defaulting	Blockchain can be used to create a decentralized clearing system that does not require a CCP. In this system, the trades are verified and matched by a network of nodes. Once the trades are matched, they are recorded on the blockchain. This makes the clearing process more transparent and efficient, as all parties can see the status of the trades in real time.
Settlement process	In a traditional settlement system, the buyer and seller must exchange assets and funds through a central custodian. This can be a slow and expensive process, as the custodian must verify the ownership of the assets and funds before they can be transferred.	Blockchain can be used to create a decentralized settlement system that does not require a central custodian. In this system, the assets and funds are represented by digital tokens on the blockchain. When a trade is settled, the ownership of the tokens is simply transferred from the buyer to the seller. This makes the settlement process much faster and cheaper.

Benefits of using blockchain for clearing and settlement

Efficiency

Blockchain can make clearing and settlement more efficient by automating many of the manual processes that are currently involved.

Security

Blockchain is a very secure technology , as it is tamper-proof and resistant to fraud.

Transparency

All transactions on a blockchain are recorded publicly, which makes the clearing and settlement process more transparent.

Costs

Blockchain can reduce the costs of clearing and settlement by eliminating the need for intermediaries.

Case Studies

- IBM and Hyperledger Fabric: IBM is working with the Hyperledger Fabric blockchain platform to develop a blockchain-based clearing and settlement system for the financial industry.

  To read more :visit this page

- ASX and Digital Asset Holdings: The Australian Securities Exchange (ASX) is partnering with Digital Asset Holdings to develop a blockchain-based clearing and settlement system for the Australian financial market.

  To read more : visit this page