

Blockchain

8.1 Introduction

A blockchain is a decentralized, distributed digital ledger based on cryptographic hash functions that are used to record transactions across many computers. Blockchain maintains a continuously growing list of ordered records, called “blocks.” These blocks are linked using cryptography to form a chain. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data. It is considered to be impossible to change, hack or manipulate the information recorded on these ledgers.

The purpose of the blockchain is to share information amongst all parties that access it via an application in a protected manner, meaning that any alteration is easily and immediately detectable.

8.2 Structure of the Blockchain

The blockchain stores transaction records in blocks linked together in sequence to form a chain. Each block contains a hash, timestamped batches of recent valid transactions and the hash of the previous block. The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. A block is composed of a header containing all the metadata and a body including all transaction details as shown in Figure 8.1. A blockchain starts from its genesis block and new blocks are appended periodically as shown in Figure 8.2.

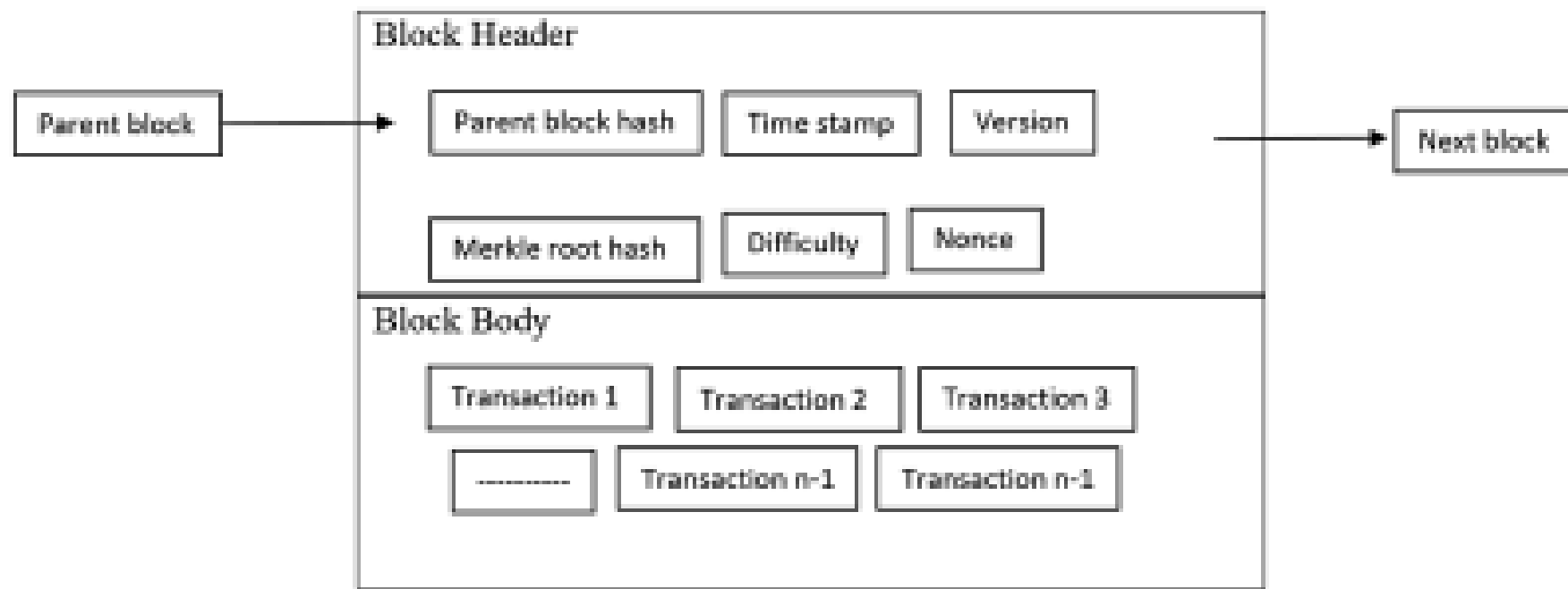


Figure 8.1 Structure of a block.

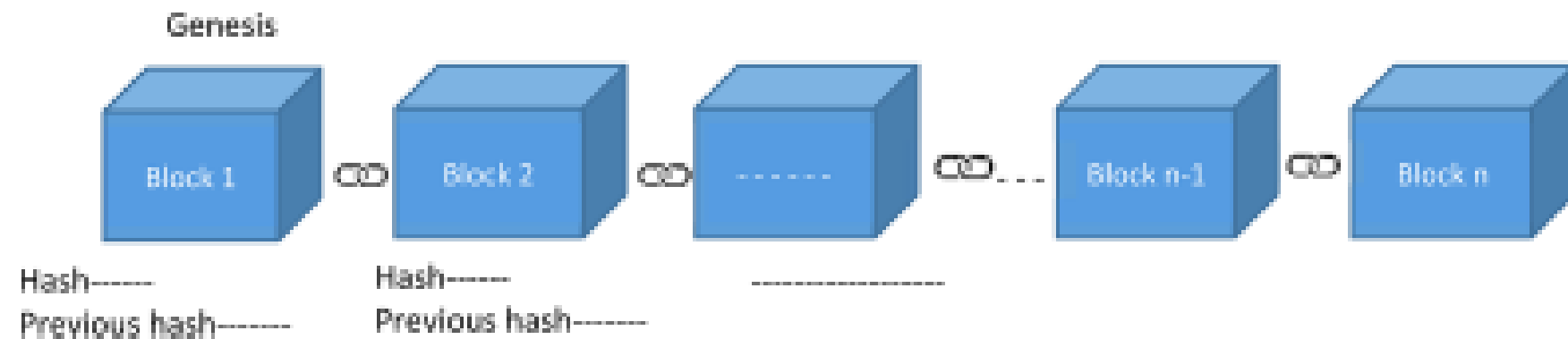


Figure 8.2 Structure of blockchain.



The parent block hash is a part of the metadata that links the current block to the one before it in the blockchain. Metadata also contains information about the mining like the difficulty level and timestamps. The nonce is a string of random numbers that is attached to the hashed contents of the block, which is then rehashed. The Merkle tree root is a data structure that is included in the final metadata. This data structure is used to efficiently summarize all of the transaction details that are contained within the associated block.

8.3 Security Features of the Blockchain

Blocks in a blockchain contain two types of information. The first is the payload which is application-specific information that records transactions or smart contracts, and the second is internal information that secures the block and specifies how it's chained to another. Security in blockchains is implemented at two levels.

8.3.1 Block Linking

For every new block, a hash is generated using the hash of the parent block and a random number “nonce.” Since the nonce is hard to calculate, misplacing a block or changing the content of a block means redoing nonce computations of all blocks subsequently linked to it which is infeasible.

8.3.2 *Consensus Mechanism*

A blockchain system functions in a peer-to-peer mode without a central trusted entity. The consensus mechanism is based on verification by every node that the received information complies with a set of predefined rules, and on verification of the nonce. For consensus, a majority of nodes (over 51%) need to agree on the next block that extends the chain.

8.4 Types of Blockchain

There are four different types of blockchain as shown in Figure 8.3.

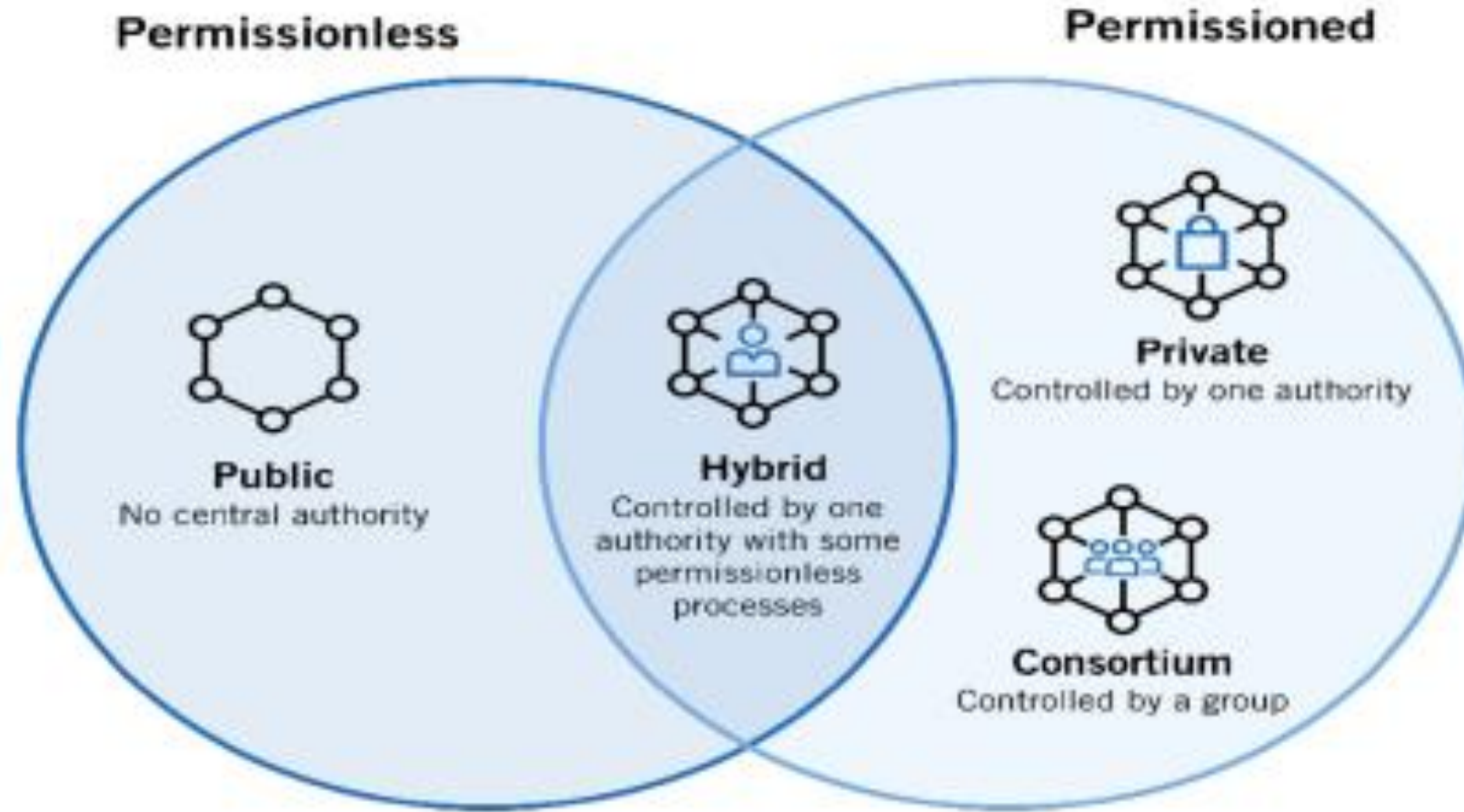


Figure 8.3 Types of blockchain (Wegrzyn & Wang, 2021).

8.4.1 *Public Blockchain*

The public blockchain is the most simple and easily accessible blockchain for the general public. Any agent can sign into a public blockchain and become an authorized participant, which allows them to become a user, miner or developer. Public blockchains are open-source, decentralized and fully distributed networks. Public blockchains do not impose any restrictions and do not require permission to use. Every node has unrestricted access to the ledger, which ensures that all transactions can be viewed by all parties. The key advantage of public blockchains is that they don't have a central control. To ensure the integrity of the public blockchain, each and every node participates in the various consensus procedures. Examples of public blockchains are mining activities and the trading of cryptocurrencies like Bitcoin, Ethereum and Litecoin.

8.4.2 *Private Blockchain*

A private blockchain is limited, centralized, permissioned and can only operate within closed networks. Each private blockchain has a centralized authority that has complete control over the accessibility, participation and permission of the blockchain network. To join a private blockchain network, permission is required from the centralized authority. The ledger is accessible only to the authorized users, and the authorization of the network's administrator is required before any alteration, additions or deletions may be made to its records. Private blockchain networks are therefore more secure and controllable than public blockchains, and they are frequently used in applications such as private businesses, electronic voting, supply chain management, etc. Examples of private blockchain networks are Hyperledger and R3 Corda blockchains.

8.4.3 Consortium Blockchain

The consortium blockchain is a subclass of private blockchain that differs from other types of private blockchain in that instead of just one, multiple organizations control and maintain the blockchain. As a result, it offers advantages that are analogous to those of a private blockchain. A consortium blockchain offers better security. Additionally, consortium blockchains are optimal for collaboration with multiple organizations. Consortium blockchains are most frequently utilized by financial institutions, governmental organizations and other types of collaborative institutes. Examples of consortium blockchains are the Energy Web Foundation and R3.

8.4.4 Hybrid Blockchain

Combinations of public and private blockchains are known as hybrid blockchains. Hybrid blockchain networks are private blockchains that allow special access for authorized individuals. They combine the privacy and permissioned features of private blockchains with the ease-of-use, flexibility and transparency of public blockchains on a single platform. Dragonchain is the most common example of a hybrid blockchain.

The comparison of the three types of blockchains is summarized in the Table 8.1.

Table 8.1 Types of Blockchains

<i>Parameter</i>	<i>Public</i>	<i>Private</i>	<i>Consortium</i>
Authority	No central authority	Single central authority	Multiple central authority
Participants	Anybody	Allowed agents	Allowed agents
Permission	No permission required	Permissioned	Permissioned
Decentralization	Fully decentralized	Centralized	Less centralized
Reading rights	Anyone	Invited user	Case dependent
Writing rights	Anyone	Approved user	Approved user
Consensus	PoS/PoW	Multiparty consensus	Multiparty consensus
Speed	Slow	Fast	Fast
Usability	Document validations and IoT operations	Supply chain, real estate and asset ownership	Finance, supply chain and research work

8.5 Blockchain Evolution

The theoretical concept of allotting a timestamp to a digital document using an encrypted chain that can verify when data was created as well as identify any changes made was proposed by Stuart Haber and W. Scott Stornetta in 1991. However, the actual implementation of this concept into technology was first done by Satoshi Nakamoto, a pseudonym behind an individual/organization, in 2008. Satoshi Nakamoto used this concept to develop the first cryptocurrency, “Bitcoin.” Since then blockchains have evolved with time as shown in Figure 8.4.

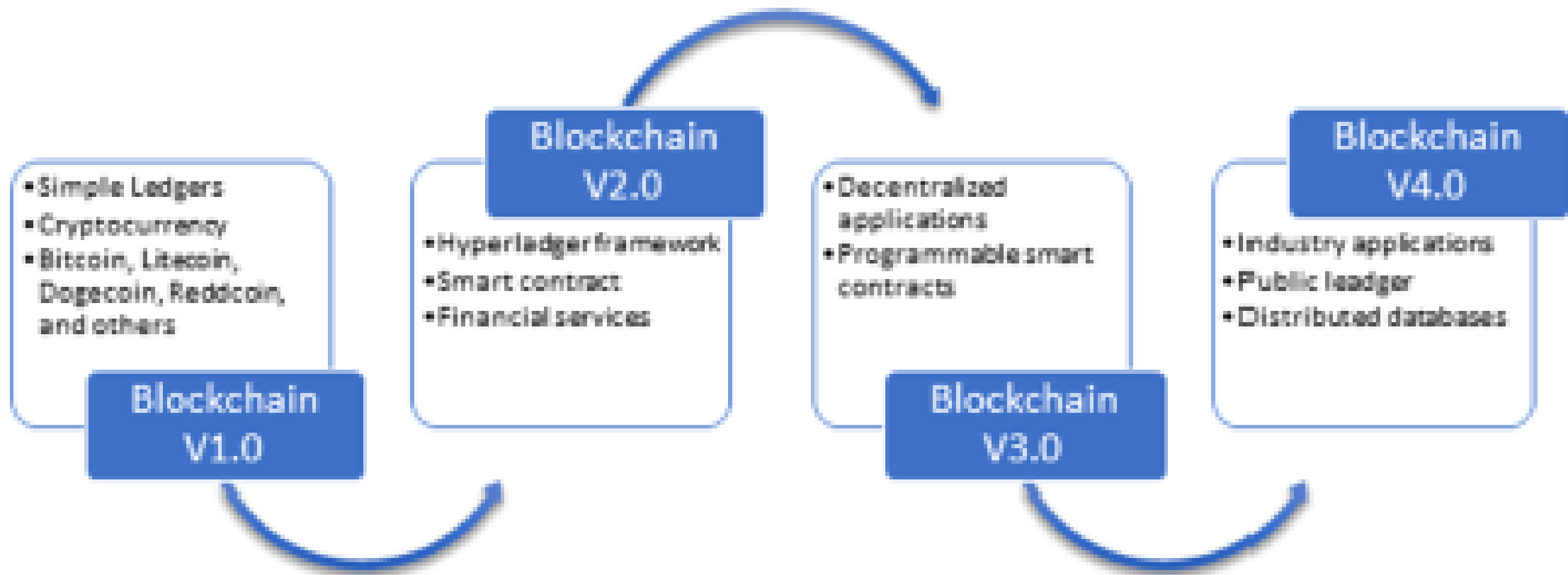


Figure 8.4 Evolution of blockchain.

8.6 Advantages of Blockchain

Blockchain is an emerging technology with many advantages in an increasingly digital world:

- **Highly secure:** Blockchain's security features protect against tampering, fraud and cybercrime. Blockchain supports immutability, meaning it is impossible to erase or replace recorded data. It uses a digital signature feature to conduct fraud-free transactions, making it impossible for other users to corrupt or change the data of an individual without a specific digital signature.

- **Transparency:** Blockchain is decentralized, meaning any network member can verify data recorded in the blockchain. Therefore, the public can trust the network.
- **Smoother and faster transactions:** Conventionally, the user needs the approval of regulatory authorities like a government or bank for transactions; however, with blockchain, transactions are done with the mutual consensus of users resulting in smoother and faster transactions.
- **Censorship:** Blockchain technology is free from censorship since it is not under the control of any single party. Therefore, no single authority can interrupt the operation of the network.

- **Automation capability:** Blockchain is programmable and can generate systematic actions, events and payments automatically. With the use of smart contracts, human interference can be reduced and the next step in the transaction or process is automatically triggered when the criteria of the trigger are met.
- **Traceability:** Blockchain creates an irreversible audit trail, allowing easy tracing of changes in any block on the network.
- **Time saving:** Traditional transaction processes require third-party mediation and are time-consuming. Blockchain slashes transaction times from days to minutes. Transaction settlement is faster because it doesn't require verification by a central authority.
- **Cost saving:** Transactions need less oversight. Participants can exchange items of value directly. Blockchain eliminates duplication of effort because participants have access to a shared ledger.

8.7 Disadvantages of Blockchain

Blockchain is the current trend and many organizations and individuals are looking forward to making best use of it. However, there are some key disadvantages of blockchain which should not be ignored (Budhi, 2022)

8.7.1 Security Risk

Blockchain involves cryptography for integrity and security with the use of public and private keys. If a user loses their private key, they may face various security issues.

8.7.2 Speed and Performance

Blockchain technology carries out multiple operations to perform one transaction. These operations include signature verification, a consensus mechanism and implementing redundancy, where the network requires each node to play a crucial role in verifying and storing each transaction. Because of these computations blockchain is considerably slower than a traditional database.

8.7.3 Scalability

Scalability restrictions are another disadvantage of blockchain networks. The number of transactions per node is limited in blockchain. Hence, it may take a lot of time to complete multiple transactions.

8.7.4 Data Modification

In blockchain, it is not possible to change or add information after it is recorded. To alter any information requires rewriting the codes in all of the blocks, which is time-consuming and expensive. The downside of this feature is that it is hard to correct a mistake or make any necessary adjustments.

8.7.5 High Implementation Cost

Compared to a traditional database, blockchain implementation is costlier and needs proper planning and execution.

8.8 Applications of Blockchain

While blockchain is still largely confined to use in recording and storing transactions for cryptocurrencies, there are various industries that are implementing blockchain for different applications. Key application aspects of blockchain technologies are:

- Virtual coins
- Smart contracts
- Money transfer and payment processing
- Digital IDs
- Secure data sharing
- Royalty and copyright protection
- Secure data backup

8.8.1 Banking and Financial Industry

Blockchain technology helps in increasing operational efficiencies across the banking and financial industries, including global trade, trade finance, clearing and settlement, consumer banking, lending and other transactions.

8.8.2 Healthcare industry

Blockchain technology helps the healthcare industry to improve security for patient's private data while making it easier to share records across stakeholders like patients, doctors, healthcare agencies and researchers. Blockchain enables patients to have complete control over their data access which increases trust in the system.

8.8.3 Supply Chain Management

By providing end-to-end transparency, streamlining processes and resolving issues faster blockchain helps in building trust between trading partners and improving supply chain management.

8.8.4 Food Chain Management

Blockchain technology can be effectively used in the food industry to ensure food safety and freshness and reduce waste. In the event of contamination, food can be traced back to its source in seconds rather than days.

8.8.5 Governance

Blockchain technology can be used for smart governance. The secure sharing of data between citizens and agencies can increase trust in the government while providing an immutable audit trail for regulatory compliance, contract management, identity management and citizen services. Blockchain technology-enabled digital voting provides enough transparency so that any regulators can see if something was altered on the network.

8.8.6 Internet of Things Network Management

Blockchain technology can be very effective in regulating IoT networks to identify devices connected to a wireless network, monitor the activity of those devices and determine how trustworthy those devices are. It can also be used to automatically measure the trustworthiness of new devices being added to the network, such as cars and smartphones.