UNIT 4 BASICS OF BLOCKCHAIN TECHNOLOGY

Structure

4.1 INTRODUCTION

The year 2009 was a remarkable one when bitcoin was launched based on blockchain technology. The feature of blockchain technology is that it makes the role of intermediaries redundant in any type of transaction. Thus elements of security, integrity, immutability, and transparency get embedded into transactions. These transactions happen in various sectors, be it the financial sector, healthcare, supply chain, real estate etc., to name a few. Hence the applications of blockchain technology are vast and are applied in various sectors. Key components of blockchain technology include hashing methods, consensus mechanisms, transactions and blocks. Blockchain technology is evolving. It has evolved from the first generation of cryptocurrency to second generation finances to the third generation digital society and is still evolving. No doubt there are associated challenges with evolution. These challenges get manifested in terms of scalability, loss of privacy and selfish mining. The impact of blockchain technology can be seen in very diverse sectors. Think of a sector where intermediaries exist, and you can see the role of blockchain technology. That is why the financial sector, supply chain, healthcare, tourism, government sector, smart cities, IoT, energy exchange, and insurance sector are applying blockchain technology to give security and transparency to the stakeholders.

Objectives:

In this unit, you will learn about the basics of Blockchain Technology, applications of Blockchain in different fields, the impact of Blockchain technology, and associated challenges to Blockchain technology. After reading this unit, you will be able to:

- Identify elements of Blockchain Technology
- Visualize the evolution of Blockchain Technology
- Appreciate application of Blockchain Technology in different spheres
- Discern limitations and challenges to Blockchain Technology and
- Comprehend different Blockchain Protocols

4.2 BLOCKCHAIN TECHNOLOGY AND ITS COMPONENTS

4.2.1 Concept of Blockchain Technology

Cryptocurrency is the first application of blockchain technology. A cryptocurrency is a medium of exchange, like the Indian Rupee, but is digital and secured by cryptography. Bitcoin was the first cryptocurrency developed in 2009 by the elusive Satoshi Nakamoto. Since then, many cryptocurrencies have come into existence to fulfil different needs and purposes. Thus, cryptocurrency, like bitcoin, is one of the applications of blockchain technology. There are numerous other applications of blockchain technology, for example, in the financial sector, government and public sectors, Supply Chain Management, Internet of Things, Healthcare, and Smart cities. Businesses that use intermediaries can be disintermediated using blockchain technology, thus bringing transparency. Blockchain can be used wherever authentication is required. One of the consequences of disintermediation and authentication will be reflected in lower transaction costs. Blockchain technology is evolving. Blockchain 1.0, i.e. the first generation of blockchain, refers to cryptocurrency, i.e. digital currency. Blockchain 2.0, i.e. the second generation of blockchain, refers to digital finance and Blockchain 3.0, i.e. the third generation of blockchain, refers to digital society.

Blockchain technology is based on Distributed Ledger Technology (DLT). Ledger is the record of transactions. These transactions may be financial deals, supply chain management, and copyright ownership. In a distributed ledger, records of transactions are available on a blockchain network. A blockchain network is a peer-to-peer network. A peer or node in a peer-to-peer network is a computer that has software installed in it. Being a peer-to-peer network, it does not require a central authority or trusted intermediaries to authenticate or settle the transactions. This feature brings transparency to transactions. Whereas in the centralized system, the records of transactions are available in a central server, and these records are managed by intermediaries, a role played by institutions like banks. Blockchain technology completely removes the role of intermediary or the third party. Transactions in Blockchain technology is immutable, i.e. once a transaction is made, it is permanent and can't be altered.

Transactions in the blockchain are stored in a block. A block is chained to another block through a cryptographic hash chain. This chain keeps growing as long as new blocks are created and maintained. This way, modern financial systems that track transactions/assets without the need for centralized parties can be enabled.

In a nutshell, blockchain is a network of devices named nodes connected to each other over the internet. All nodes on a blockchain are equally important. A node can play diverse roles like storing information recorded in a blockchain, storing a copy of all the information recorded on a blockchain, and processing transactions to add a new block in the network.

4.2.2 Working of Blockchain

The working of blockchain technology can be illustrated through one of its applications. Cryptocurrency is one of the applications of blockchain technology, and the working of blockchain technology can be demonstrated through a transfer

of cryptocurrency. Let a user ‘X’ wants to send money to user ‘Y’. The process of transfer of money from user ‘X’ to user ‘Y’ is as shown in Figure 4.1.

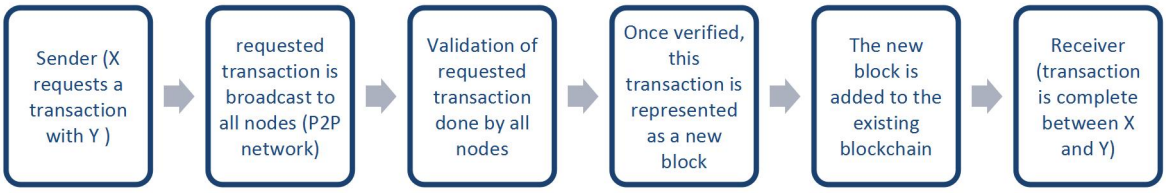

Figure 4.1: Working of Blockchain (user X sends money to user Y)

Here sender ‘X’ requests a transaction for sending money to the receiver ‘Y’. The requested transaction is broadcasted to the P2P network (it consists of computers known as nodes). This P2P network containing all nodes validates the transaction. Once verified, this transaction is represented as a new block. The new block is then added to the existing blockchain. Thus the transaction is completed, and receiver ‘Y’ receives the money.

The above was the simplest explanation of the working of blockchain. Now see what happens at every stage of the transaction in a bit of detail. When sender ‘X’ wants to send money to the receiver ‘Y’, then ‘X’ should know the wallet address of ‘Y’. The transaction gets initiated as user ‘X’ sends the money to user ‘Y’. Every node of the blockchain will have to verify this transaction. Only then will user ‘Y’ get money in his/her wallet. Thus every node will record this money transaction from user ‘X’ to user ‘Y’. Hence, records will be stored in thousands of computers, but the user may not like his/her transaction information on many computers. This issue is resolved by blockchain by keeping the transaction anonymous. For maintaining transactions’ integrity over the network, there is the need for consensus protocol, cryptographic hashes, and digital signatures at nodes. Consensus protocol guarantees that transactions recorded in public ledgers are exact copies. No transaction record can be changed without accessing all the nodes of the network. Thus making transaction records immutable. SHA-256 (Secure Hash Algorithm of output size 256 bits), a cryptographic hashing algorithm, is used to assure that any change in transaction leads to a new hash value being computed. Digital signatures ensure that the transactions are initiated from genuine senders.

4.2.3 Types of Blockchain

Blockchain can be classified into the following three major types.

- Public Blockchain
- Private Blockchain
- Consortium Blockchain or Hybrid Blockchain

A public blockchain is one in which anyone can join and participate. It means anyone can be a user or a miner, and anybody can add new blocks. This ensures transparency in public blockchain networks. A public blockchain is also called permissionless as it permits anyone to take a copy of the blockchain and involve in block validation. Bitcoin and Ethereum are examples of a public blockchain.

A private blockchain is a permissioned blockchain suitable for individual organizations. Here an organization decides who is allowed to participate and maintain a shared ledger. Hyperledger is an example of a private blockchain.

A consortium blockchain is a permissioned blockchain where several organizations take responsibility for maintaining the blockchain. Consortium blockchain has the privacy benefits of private blockchain and the transparent nature of public blockchain. A consortium blockchain is also called a hybrid blockchain. Dragonchain is an example of consortium blockchain.

Features of the above three blockchain types is as shown in Table 4.1:

Table 4.1: Features of Blockchain Types

Feature	**Public Blockchain**	**Private Blockchain**	**Consortium Blockchain**
User access	Public	Restricted	Restricted
User identity	Anonymous	Approved users	Approved users
Permission status	Permissionless	Permissioned	Permissioned

4.2.4 Advantages of Blockchain Technology

Following are the advantages of blockchain technology:

- Decentralization
- Transparent and Anonymous
- Less transaction fees and no taxes
- Theft resistant

The above mentioned advantages/characteristics of blockchain technology helped the rapid evolution of blockchain technology from application in cryptocurrency (bitcoin) to Industry 4.0 in such a short interval of 10 years.

Security, transparency, traceability, and automation are some of the important concerns for any business or industry. Blockchain technology can address the above concerns. As records created through blockchain can't be tampered with and are end-to-end encrypted, blockchain enhances security for any business or industry. Privacy issues can also be addressed on blockchain by making personal data anonymous.

Decentralization is the hallmark of blockchain technology. There is no role of an intermediary or third party in blockchain technology. This feature of blockchain technology provides protection against corruption and tampering. Further, all transactions in the blockchain are maintained in the public ledger. This ensures transparency.

4.2.5 Components of Blockchain Technology

Blockchain technology is based on cryptographic concepts and record keeping principles. Cryptography is the study of secure communication techniques. Cryptographic techniques use hashing, asymmetric key cryptography and digital

signatures. Some of the key components of Blockchain technology have been discussed here for a better understanding of blockchain technology.

Hashing Methods

The most important component of blockchain technology is the cryptographic hashing function. A hash algorithm is a mathematical function that transforms any input into a fixed size output. The input can be a text, file or image, and the output is a fixed size alphanumeric string. As shown in Figure 4.2, the conversion of an input message (Hello world) to hash value using SHA 256 algorithm. You can generate a hash value for any input and see for yourself that the output is always a fixed size alphanumeric string (you can use python online: colab.research.google.com).

Hashing is a one way function where any input of arbitrary size can be uniquely expressed as a string of characters. The meaning of one way function is that it is easy to go from the input to the hash but extremely difficult to go the other way. Meaning thereby by knowing only the hash, you can't find the original message. In other words, anyone with the original message and the hashing algorithm will produce the same hash.

Figure 4.2: Hash Function

What is the purpose of hashing in blockchain? The answer is data integrity and privacy. Hashing protects data integrity by hiding and encoding the original message (i.e. input) to a unique string. For the hash function to be cryptographically secure and usable in blockchain technology, it needs to be collision resistant. Collision resistant means that it should be practically impossible to find two inputs that produce the same output.

Most blockchain implementation uses Secure Hash Algorithm (SHA) that generates an output of size 256-bit. Cryptocurrency like bitcoins uses Secure Hash Algorithm 256, also known as SHA-256.

Transaction

A transaction is a digitally signed message authorizing some particular action associated with a blockchain. For a cryptocurrency, the dominant transaction type is sending cryptocurrency units or tokens to someone else. As shown in the Figure 4.3, the five step process of the blockchain transaction. The blockchain transaction process has been elucidated in the following five steps.

- **Transaction initiation:** The transaction information contains the Receiver's public address, the value of the transaction and a cryptographic digital signature.
- **Transaction authentication:** The nodes in the blockchain network receive transaction information and authenticate its validity. When the transaction

is validated, it is placed in the pool of transactions. Transaction pool is the place where all unconfirmed transactions are placed.

- **Block creation:** the pool of transactions is then placed on the block by one of the participating nodes of the network.
- **Block validation:** the participating nodes begin the validation process upon receiving the block of transaction.
- **Block chaining:** the block is chained into the existing blockchain, and an updated blockchain ledger is broadcast to the network. The entire process takes 3-10 s.

Figure 4.3: Transaction Process

Public Key Cryptography

Public key cryptography is an encryption scheme that uses two mathematically related but not identical keys: a public key and a private key. A public key is used to encrypt, and the private key to decrypt.

Address and Wallet

Blockchain addresses are used to send or receive transactions on a network. An address usually presents itself as a string of alphanumeric characters.

A wallet is a file that contains a collection of private keys and communicates with a blockchain. Wallets contain keys, not coins. Wallets require backup for security reasons.

Blocks

A block is the most basic unit of a blockchain database. Each block contains a record of some or all recent transactions and references to the block that came immediately before it. As shown in Figure 4.4, the structure of a block. A block consists of Block number, nonce, data, previous hash and hash. The block number is a unique number assigned to each block by the user who creates the block. The

nonce is a special value mined by the miner algorithms employed by the creator of the block. A nonce is a 4 byte field, usually starting at 0, and the value increases with every calculation. This value calculation is also known as puzzle solving. Nonce ensures that the hash value generated for a block has a particular format, like starting with three zeros or ten zeros.

The previous hash is the encryption of the previous block. The hash is calculated using the SHA-256 algorithm on the combination of the nonce, previous hash and data.

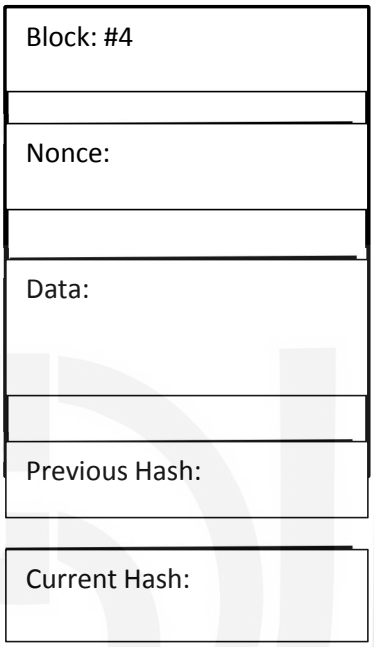

Figure 4.4: Structure of Block

A block has only one parent. The first block of a blockchain is called the 'genesis block'. The 'genesis block' has no parent block.

Consensus Features

The consensus protocol is the set of rules and arrangements to carry out blockchain operations. Consensus algorithms are designed to achieve reliability in a network involving multiple unreliable nodes. The consensus algorithms ensure that the next block in the blockchain is the one and only one version of the truth. The most common consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Authority and Ripple.

PoW protocol is one of the first utilized consensus protocols. PoW protocol is based on computational load, requiring miners to find a solution to the puzzle. The downside to this method of generating consensus and securing the network is that it requires a large amount of computing power and, therefore, energy and cost. To reduce the high resource cost of mining, PoS was proposed. PoS assigns a difficulty value to a puzzle based on how much stake the owner has in the network.

Proof of Authority (PoA) is a reputation based consensus approach where the preselected validators attempt to validate by leveraging the value of identities. Therefore, PoA blockchains are scalable and secured as the preselected nodes are considered as trustworthy entities to verify transactions.

Smart Contract

Smart contracts are translations of an agreement consisting of terms and conditions into computational code (or program/script). Smart contracts are self-executing digital contracts. In smart contracts, there are no chances of fraud or intervention of third parties. Ethereum platform allows the use of the smart contract. Smart contracts can be used in many applications. One of the applications of the smart contract is crowdfunding. A crowdfunding platform is used to raise funds from multiple investors by a startup company. A conventional case of crowdfunding requires a third party intermediary to control the fund flow as per conditions of the contract. A smart contract is a secure alternative to an intermediary.

Check Your Progress 1

In this section, you studied blockchain technology and its components, now answer the questions given in Check Your Progress-1.

Note: a) Write your answer in about 50 words

b) Check your answer with possible answers given at the end of the unit

(1) Explain the working of Blockchain Technology.

---

(2) Discuss components of Blockchain Technology.

4.3 EVOLUTION OF BLOCKCHAIN

Blockchain technology is continuously evolving with time. In a short span of a decade, it has seen four generations of its evolution. The first generation of Blockchain, i.e. Blockchain 1.0, originated from the concept of Distributed Ledger Technology and was meant for cryptocurrency only.

Blockchain 2.0, i.e. the second generation of Blockchain, is based on the smart contract concept and the Proof of Work consensus mechanism. The smart contract is a programming code embedded in a distributed ledger. The smart contract gets executed when predefined conditions are satisfied. The second-generation blockchain network was introduced in 2013.

Blockchain 3.0 overcomes the setbacks of Blockchain 1.0 and Blockchain 2.0. What are the setbacks of Blockchain 1.0 and Blockchain 2.0? Blockchain 1.0 and Blockchain 2.0 are not scalable at all. Apart from that, these are mainly based on Proof of Work. Apart from smart contracts, Blockchain 3.0 mainly involves Decentralized Apps (dApps). A dApp can be thought of as decentralized software code that gets executed across all the nodes in given blockchain architecture. A dApp is very similar to the applications already in use today on smartphones, tablets, or Desktops. Blockchain 3.0 also utilizes the Proof of Stake and Proof of Authority consensus mechanism.

Blockchain 4.0 means making Blockchain 3.0 usable in real life business scenarios. Blockchain 4.0 makes Blockchain technology usable to Industry 4.0 demands. Industry 4.0 refers to the fourth revolution that has occurred in manufacturing. Industry 4.0 technologies employ Artificial Intelligence, the Internet of Things, Big Data etc.

Unibright is the framework for Blockchain 4.0. In other words, the introductory platform for Blockchain 4.0 utilities is Unibright.

Comparison of Different Generations of Blockchain:

As shown in Table 4.2, the evolution of blockchain technology based upon different parameters. The consensus mechanism for the first generation blockchain technology is Proof of Work. The fourth generation of blockchain technology uses Proof of Integrity. When it comes to the application of blockchain technology, it has achieved many milestones. It began with application in the financial sector and now heading towards application in Industry 4.0. The fourth generation of blockchain technology is incorporating Artificial Intelligence. Blockchain technology is moving from guaranteed transaction authenticity to a faster consensus and transaction confirmation, removing the initial bottlenecks and hiccups.

Table 4.2: Comparison of Different Generations of Blockchain

Parameter	**Blockchain 1.0 (2008)**	**Blockchain 2.0 (2013)**	**Blockchain 3.0 (2015)**	**Blockchain 4.0 (2018)**
Principle	Distributed Ledger Technology (DLT)	Smart Contracts	Decentralized Apps (dApps)	Blockchain with Artificial Intelligence
Consensus mechanism	Proof of Work	Delegated Proof of Work	Proof of Stake, Proof of Authority	Proof of Integrity
Example	Bitcoin	Ethereum	Cardano, Anion	Unibright, SEELE
Application	Financial Sector	Non-Financial Sector	Business Platforms	Industry 4.0
Features	Guaranteed transaction authenticity	Creating and transferring digital assets	Completely open-source; autonomous operation	Faster consensus and transaction confirmation

Source: Blockchain Technology: Applications and Challenges (Springer 2021) and other sources

Check Your Progress 2

In this section, you studied the evolution of blockchain technology, now answer the questions given in Check Your Progress-2.

Note: a) Write your answer in about 50 words

b) Check your answer with possible answers given at the end of the unit

(1) Discuss the evolution of Blockchain.

---

(2) What are the setbacks of Blockchain 1.0 and Blockchain 2.0?

---

(3) Compare different generations of blockchain technology on parameters like principles and applications.

4.4 BLOCKCHAIN APPLICATIONS

Wherever there is a requirement of trust, security, accuracy, and transparency, there is the application of Blockchain technology. Blockchain applications can be vividly seen in the government and public sectors. Governments can use Blockchain in improving record management. Governments keep people's records like birth and property exchanges. Blockchain can make the record more secure. Decentralized file storage protects files from getting hacked or lost.

The financial sector has seen the benefits of blockchain technology from the very beginning. The most popular application of blockchain technology is cryptocurrency. Other industries and sectors are exploring opportunities actively for the implementation of blockchain technology in their fields and domains.

The applications of blockchain technology in the financial services, Governments and public sectors, healthcare, Industry and Internet of Things (IoT) have been discussed here.

4.4.1 Financial Applications

Banks and other financial institutions are highly susceptible to money laundering, identity theft and digital transfer of funds. These institutions are highly affected as far as services rendered, and reputations are concerned. Banking institutions are already using blockchain technology to solve their traditional problems.

4.4.2 Blockchain Applications in Government

Typical problems faced by governments in many countries pertain to land registry records. Keeping track of ownership of hundreds of years of land records is a difficult task. The problems faced by land registry officials are: discrepancies with paperwork, forged documents, and loss of documents.

Blockchain technology can take care of above mentioned problems in a cost-effective way. Blockchain technology provides immutable records and secure access as well as storage. Governments can use Blockchain in the following areas:

- Record management for secure record-keeping of people
- Identity management for proof of identity
- Government services like public safety and welfare

- Payment infrastructures to collect dues, taxes and other payments fast and safe
- Smart property to digitally record assets

4.4.3 Blockchain Applications in Healthcare

There has been an increase in the hacking of healthcare records. The year 2018 witnessed the hacking of medical records of 1.4 million patients from the UnityPoint Health hospital network of the USA. The hacked records included sensitive information, including the patient's social security number and insurance information.

Blockchain technology provides data security and integrity. Patients, healthcare providers (hospitals, doctors, lab technicians etc.), data analysts and insurance providers are key stakeholders of healthcare. The Distributed Ledger Technology/Blockchain technology in healthcare guarantees the security and privacy of healthcare data of all stakeholders. These stakeholders can share information without compromising data security and integrity.

4.4.4 Blockchain Applications in Industry:

Tracking of movements of goods and services is vital in any industry. Be the movement of goods under process or processed goods, visibility at every stage of production is very much needed. Blockchain technology can help in tracking the movements of goods and services efficiently. Almost all business operations, be it purchase management, customer relationship management, supply chain management or operation management, blockchain technology is there to address business concerns.

4.4.5 Blockchain Application in the Internet of Things (IoT)

In IoT applications, smart devices interact with each other using the internet. The biggest concern is the security of data generated by these smart devices within distributed nature of wireless networks. As blockchain is distributed public ledger, it will take care of the security of data generated by smart devices.

Check Your Progress 3

In this section, you studied blockchain technology applications, now answer the questions given in Check Your Progress-3.

Note: a) Write your answer in about 50 words

b) Check your answer with possible answers given at the end of the unit

(1) Discuss Blockchain technology's application in cryptocurrency.

---

(2) Discuss Blockchain technology's application in governance.

---

(3) Discuss Blockchain technology's application in healthcare.

4.5 LIMITATIONS AND CHALLENGES OF BLOCKCHAIN

Though blockchain has numerous benefits, it is prone to some technical challenges also. Challenges in terms of scalability, loss of privacy, selfish mining and energy have been discussed here.

4.5.1 Scalability

As transactions are increasing in numbers, the blockchain network keeps on growing day by day. As blockchain network is growing, data and resources are burdening the system. Due to this reason, nodes will take more time to synchronize data and carry out the complex computation. Thus affecting the effective working of the blockchain system. Storage optimization and redesigning of blockchain can resolve these issues.

4.5.2 Loss of Privacy

In the blockchain, a considerable amount of privacy is maintained by using a public key cryptography mechanism in transactions to keep the user identity anonymous. However, transactional anonymity cannot be assured by blockchain because the identities of all transactions and balances for each cryptographic key are publicly accessible. Thus it is possible to recognize the user by keeping track of the transactions.

4.5.3 Selfish Mining

In Bitcoin's blockchain, the process of adding new blocks to the blockchain is called mining, and the nodes that do the job of generating a new block are called miners. Selfish Mining is a strategy where an over-ambitious miner secretly keeps his blocks without publishing them. It would be revealed to the public only if some conditions were satisfied.

4.5.4 High Energy Consumption

The blockchain network uses Proof of Work (PoW) as a consensus protocol. It requires a lot of energy and computing resources to calculate the required hash value for a block.

Check Your Progress 4

In this section, you studied the limitations and challenges of blockchain technology, now answer the questions given in Check Your Progress-4.

Note: a) Write your answer in about 50 words

b) Check your answer with possible answers given at the end of the unit

(1) What are the challenges associated with Blockchain technology?

---

(2) Explain selfish mining.

4.6 IMPACT OF BLOCKCHAIN TECHNOLOGY

The impact of blockchain technology can be seen in businesses. The impact may be manifested in different forms. It may be business models; it may be the business environment. The existing business models may change or transform in view of the new reality of market requirements. Some of the impacts of the blockchain in the financial and non-financial sector has been discussed here.

4.6.1 Impact of Blockchain Technology in Financial Sector

It is the transaction that takes place in the Financial sector like banking, where the introduction of blockchain technology can make its impact the most. The standard practice of transactions in the Financial sector like banking is based on a trusted third party. This role of a third party is the main source of worry for all stakeholders. This trusted third party can be eliminated by using blockchain technology in the Financial sector like banking. The architecture of the standard banking system is based on a centralized server/clients model, and hence a copy of the database is centralized at the server level only. As a blockchain technology-based system gets introduced in the banking system, the peer-to-peer network model will be there, ensuring multiple copies of transactions in a database. A comparison of existing banking system models and blockchain-based models are as shown in Table 4.3.

Table 4.3: Comparison of Transactions between Existing Financial Sector like Banking and Blockchain-based Financial Sector like Banking

Transactions in Existing Financial sector like Banking	**Transactions in Blockchain-based Financial sector like banking**
Trusted third party	Trustless
Centralized server/clients	Peer-to-peer network
A single copy of transactions in the database	Multiple copies of transactions in the database
Intermediation	Consensus mechanism/ Proof of work

Source: Adapted from Blockchain and Distributed Ledger Technology (DLT): What impact on the Financial Sector by Klara Sok

4.6.2 Impact of Blockchain Technology Application in Supply Chain:

Supply Chain Management (SCM) is the handling of the entire production flow of goods or services. SCM takes into account the handling and processing of raw materials to delivering finished products to the consumers. There are five key components of SCM.

- Planning
- Sourcing

- Manufacturing
- Delivery and logistics
- Returning

When blockchain technology is used in Supply Chain, the following benefits can be had.

- All information pertaining to supply and demand can be captured in real time
- The status of an item in transition/process can be known
- Smart contract management can be done (customized or individual contract can be defined for each function)
- Operational efficiency in Supply Chain can be achieved

Check Your Progress 5

In this section, you studied the impact of blockchain technology, now answer the questions given in Check Your Progress-5.

Note: a) Write your answer in about 50 words

b) Check your answer with possible answers given at the end of the unit

(1) Discuss the impact of Blockchain technology in the financial sector.

---

(2) Discuss the impact of Blockchain technology in the supply chain.

4.7 BLOCKCHAIN PLATFORMS/PROTOCOLS

The rules that govern a blockchain network are referred to as blockchain protocols. Blockchain protocols are essentially the common communication rules that the network follows. These rules include the following:

- Rules for governing and validating transactions
- An algorithm that defines the mechanism for all participating nodes to interact with each other
- Application programming interface (API)

Some of the blockchain protocols have been discussed here.

4.7.1 Bitcoin

Bitcoin protocol supports crypto payment transactions over a distributed network.

Characteristics of Bitcoin Protocol:

i. Every node has access to complete information on the blockchain. Therefore, it is a decentralized one.

ii. Users can conduct a nonreversible transaction without the need to explicitly trust a third party.

Advantages of Bitcoins:

- Payment freedom
- Control and Security
- Very low fees

4.7.2 Ethereum

Ethereum is a public, open source, blockchain-oriented protocol. Ethereum platform allows the use of the smart contract. Ethereum is the first prominent platform that introduced the idea that blockchain technology can be used in applications other than cryptocurrency.

Characteristics of Ethereum Protocol:

- This protocol enables developers to build and deploy distributed applications
- It allows users to write their own applications

Advantages of Ethereum:

- The energy efficiency is high with the help of Proof of Stakes (PoS)
- The uptime of the network is high
- It is used to develop many decentralized applications

4.7.3 Hyperledger

Hyperledger is an open-source blockchain platform. It supports blockchain-based distributed ledgers and cross-industry blockchain technologies.

Hyperledger protocol mainly supports business transactions. Hyperledger is used to solve the problem of enterprise approval of blockchain. In Hyperledger, only trusted entities can join the network and verify the transactions.

Characteristics of Hyperledger Protocol:

- Hyperledger blockchain technology is mostly used for business applications
- It has a modular and versatile design
- It preserves privacy

Benefits of Hyperledger

- Productivity enhancement
- Handling of intellectual property
- Data on a need-to-know basis
- Rich querying capability
- Performance scalability and levels of trust

4.7.4 Ripple

Ripple is an open source blockchain platform. Ripple acts as both a cryptocurrency and a digital payment network for financial transactions.

Characteristics of Ripple Protocol:

- Ripple protocol is known for its digital payment network
- It has its own cryptocurrency XRP (digital asset Ripple)
- Ripple transactions are confirmed in seconds
- Ripple transactions use less energy than bitcoin.

4.7.5 R3's Corda

Corda is an open source blockchain protocol used for industries such as financial services, insurance, healthcare, trade finance, and digital assets. This protocol is used for storing, coordinating, and controlling financial agreements.

Characteristics of Corda:

- Corda allows businesses to transact securely and seamlessly
- This protocol organizes the business operation

Benefits of Corda:

- Privacy
- Agile and flexible
- Interoperability
- Open development
- Open design

Check Your Progress 6

In this section, you studied blockchain protocols, now answer the questions given in Check Your Progress-6.

Note: a) Write your answer in about 50 words

b) Check your answer with possible answers given at the end of the unit

(1) Enumerate the characteristics of the Ethereum protocol. What are the advantages of the Ethereum protocol?

---

(2) Discuss the Ripple protocol.

---

(3) What are the features of Blockchain protocols?

4.8 SUMMARY

This unit discussed the basics of blockchain technology. The learners were introduced to the working of blockchain. Further, the essential components of blockchain were outlined to give better insight into the working of blockchain.

The applications of blockchain technology have seen penetration in various sectors and industries. This unit explored a few applications in government, public sectors, finance, healthcare, industry, and the Internet of Things. This unit also discussed challenges like scalability, selfish mining and high energy consumption. An overview of the evolution of blockchain technology was given to demonstrate the power of blockchain technology in different sectors and industries. Blockchain platforms and protocols showed how blockchain can accommodate other sectors and industries.

4.9 KEYWORDS

API: API stands for an application programming interface. API is a software intermediary that allows two applications to talk to each other.

Consensus algorithm: An algorithm that defines the way consensus will be reached on the network to verify the transactions.

Dragonchain: Dragonchain is an enterprise and start up ready platform to build flexible and scalable blockchain applications.

Ethereum: Ethereum is an open source software based on blockchain technology.

Genesis Block: The first block in any blockchain-based protocol is the genesis block. It is the foundational block on which further blocks are added to form a chain of blocks.

Hashing: A hash function is a complex mathematical function that processes arbitrary input of any length into the output of a fixed length. Example of software for hashing: MD family of software and SHA family of software.

Hyperledger: Hyperledger is an open source blockchain platform. It supports blockchain-based distributed ledgers and cross industry blockchain technologies.

Industry 4.0: Industry 4.0 refers to the fourth revolution that has occurred in manufacturing. Industry 4.0 technologies employ Artificial Intelligence, the Internet of Things, Big Data etc.

Miners: Specific nodes which perform the block verification process before adding anything to the blockchain structure are called miners.

Node: The user or computer within the blockchain architecture is a node.

Nonce: A unique number related to mining. A nonce is an abbreviation for "number only used once". It is a number added to a hashed block in a blockchain that, when reshared, meets the difficulty level restrictions. The nonce is the number that blockchain miners are solving for.

P2P architecture: Peer to peer (P2P) architecture is a network of interconnected systems in which they are capable of sharing resources and information. Every system connected to the network is called a node or peer.

Proof of Work: In the Proof of Work (PoW), the participating nodes are engaged in high computational and mathematical work to reach a consensus.

Proof of Stake (PoS): In the Proof of Stake (PoS), the network randomly selects the participating node based on its proportional stake in the network to approve the transaction.

Proof of Authority (PoA): Proof of Authority (PoA) is a reputation based consensus approach where the preselected validators attempt to validate by leveraging the value of identities.

Protocol vs consensus algorithm: Bitcoin and Ethereum are protocols, whereas Proof of Work (PoW) and Proof of Stake (PoS) are their respective consensus algorithms. The protocol regulates what procedures are. The algorithm tells the system what steps need to be taken to comply with these rules to produce desired results.

Ripple: Ripple is an open source payment protocol. It acts as a cryptocurrency as well as a digital payment network for financial transactions.

SHA-256: SHA-256 is a cryptographic hash function that takes an input of any size and produces a fixed-sized output.

Smart contract: Smart contracts are translations of an agreement consisting of terms and conditions into computational code (or program/script).

Wallet: Bitcoin wallet is a software program that stores bitcoins. It is used to send and receive bitcoins.

4.10 CHECK YOUR PROGRESS 1 – POSSIBLE ANSWERS

1) Explain the working of blockchain technology.

Let a user 'X' wants to send money to user 'Y'. For this monetary transaction to happen, user 'X' should know the wallet address of user 'Y'. The transaction gets initiated as user 'X' sends the money to user 'Y'. Every node of the blockchain will have to verify this transaction. Only then will user 'Y' get money in his/her wallet. Thus every node will record this transaction of money from user 'X' to user 'Y'. Hence, records will be stored in thousands of computers, but the user may not like his/her transaction information on many computers. This issue is resolved by blockchain by keeping the transaction anonymous. For maintaining transactions' integrity over the network, there is the need for consensus protocol, cryptographic hashes, and digital signatures at nodes. Consensus protocol guarantees that transactions recorded in public ledgers are exact copies. No transaction record can be changed without accessing all the nodes of the network. Thus making transaction records immutable. SHA-256 (Secure Hash Algorithm of output size 256 bits), a cryptographic hashing algorithm, is used to assure that any change in transaction leads to a new hash value being computed. Digital signatures ensure that the transactions are initiated from genuine senders.

2) Discuss components of blockchain technology.

Blockchain technology is based on cryptographic concepts (e.g. hashing, asymmetric key cryptography and digital signatures) and record keeping principles. Some of the key components of Blockchain technology are as under:

- Hashing methods
- Transaction
- Public key cryptography
- Consensus Features
- Address and wallets

- Blocks

Check Your Progress 2 – Possible Answers

1) Discuss the evolution of Blockchain.

The first generation of Blockchain, i.e. Blockchain 1.0 originated from the concept of Distributed Ledger Technology. Blockchain 2.0, i.e. the second generation of Blockchain or Ethereum, is based on the concept of the smart contract along with the Proof of Work consensus mechanism.

Blockchain 3.0 overcomes the setbacks of Blockchain 1.0 and Blockchain 2.0. What are the setbacks of Blockchain 1.0 and Blockchain 2.0? Blockchain 1.0 and Blockchain 2.0 are not scalable at all. Apart from that, these are mostly based on Proof of Work. Apart from smart contracts, Blockchain 3.0 mainly involves Decentralized Apps (dApps). A dApp can be thought of as decentralized software code that gets executed across all the nodes in given blockchain architecture.

Blockchain 4.0 makes Blockchain technology usable to Industry 4.0 demands. Industry 4.0 refers to the fourth revolution that has occurred in manufacturing. Industry 4.0 technologies employ Artificial Intelligence, the Internet of Things, Big Data etc.

2) What are the setbacks of Blockchain 1.0 and Blockchain 2.0?

Blockchain 1.0 and Blockchain 2.0 are not scalable at all. Apart from that, these are mostly based on Proof of Work.

3) Compare different generations of blockchain technology on parameters like principles and applications.

Comparison of different generations of blockchain technology based on principle and application is as below:

Parameter	**Blockchain 1.0**	**Blockchain 2.0**	**Blockchain 3.0**	**Blockchain 4.0**
Principle	Distributed Ledger Technology (DLT)	Smart Contracts	Decentralized Apps (dApps)	Blockchain with Artificial Intelligence
Application	Financial Sector	Non-Financial Sector	Business Platforms	Industry 4.0

Check Your Progress 3 – Possible Answers

1) Discuss Blockchain technology's application in cryptocurrency.

Cryptocurrency is the first application of Blockchain technology. Bitcoin was the first cryptocurrency developed in 2009. Since then, many cryptocurrencies have come into existence to fulfil different needs and purposes.

2) Discuss Blockchain technology's application in governance.

Typical problems faced by governments in many countries pertain to land registry records. Keeping track of ownership of hundreds of years of land records is a difficult task. The problems faced by land registry officials are: discrepancies with paperwork, forged documents, and loss of documents. Blockchain technology can

take care of above mentioned problems in a cost-effective way. Blockchain technology provides immutable records and secure access as well as storage.

3) Discuss Blockchain technology's application in healthcare.

Blockchain technology provides data security and integrity. Patients, healthcare providers (hospitals, doctors, lab technicians etc.), data analysts and insurance providers are key stakeholders of healthcare. The Distributed Ledger Technology/Blockchain technology in healthcare guarantees the security and privacy of healthcare data of all stakeholders. These stakeholders can share information without compromising data security and integrity.

Check Your Progress 4 – Possible Answers

1) What are the challenges associated with Blockchain technology?

Key challenges faced by blockchain technology are:

- Scalability
- Loss of privacy
- Selfish mining

2) What are the clean energy options for the transport sector?

In Bitcoin's blockchain, the process of adding new blocks to the blockchain is called mining, and the nodes that do the job of generating a new block are called miners. Selfish Mining is a strategy where an over ambitious miner secretly keeps his blocks without publishing it. It would be revealed to the public only if some conditions were satisfied.

Check Your Progress 5 – Possible Answers

1) Discuss the impact of Blockchain technology in the financial sector.

It is the transaction that takes place in the Financial sector like banking, where the introduction of blockchain technology can make its impact the most. A standard practice of transactions in the Financial sector like banking is based on a trusted third party. This role of a third party is the main source of worry for all stakeholders. This trusted third party can be eliminated by the use of blockchain technology in the Financial sector like banking. The architecture of the standard banking system is based on a centralized server/clients model, and hence a copy of the database is centralized at the server level only. As a blockchain technology-based system gets introduced in the banking system, the peer-to-peer network model will be there, ensuring multiple copies of transactions in a database.

2) Discuss the impact of blockchain technology in the supply chain.

When blockchain technology is used in Supply Chain, the following benefits can be had.

- All information pertaining to supply and demand can be captured in real-time
- The status of an item in transition/process can be known
- Smart contract management can be done (customized or individual contract can be defined for each function)
- Operational efficiency in Supply Chain can be achieved

Check Your Progress 6 – Possible Answers

1) Enumerate the characteristics of the Ethereum protocol. What are the advantages of the Ethereum protocol?

Following are the characteristics of the Ethereum protocol:

Characteristics of Ethereum Protocol:

- This protocol enables developers to build and deploy distributed applications
- It allows users to write their own applications

Following are the advantages of the Ethereum protocol:

Advantages of Ethereum:

- The energy efficiency is high with the help of Proof of Stakes (PoS)
- The uptime of the network is high
- It is used to develop many decentralized applications

2) Discuss the ripple protocol.

Ripple is an open source blockchain platform. Ripple acts as both a cryptocurrency and a digital payment network for financial transactions. Its native currency is termed as a Ripple. Ripple enables instant, safe, and almost free global financial transactions. The protocol supports tokens presenting cryptocurrency. Ripple is the biggest cryptocurrency in terms of market capitalization.

Following are the characteristics of ripple protocol:

- Ripple protocol is known for its digital payment network
- It has its own cryptocurrency XRP
- Ripple transactions are confirmed in seconds
- Ripple transactions use less energy than bitcoin.

3) What are the features of the blockchain protocol?

Following are the features of the blockchain protocol:

- Distributed ledgers
- Smart contracts
- Coins
- Tokens
- Trustlessness
- Decentralized
- Immutable

4.11 REFERENCES AND SELECTED READINGS

1. P. Raj, K. Saini, and C. Surianarayanan, "Blockchain Technology and Applications", CRC press, 2020.
2. S.K. Panda, A.K. Jena, S.K. Swain, and S.C. Satpathy, "Blockchain Technology: Applications and Challenges", Springer, 2021
3. S. K. Panda, A.A. Elngar, V.E. Balas and M. Kayed, "Bitcoin and Blockchain: History and Current Applications (Internet of Everything (IoE))", CRC Press, 2020.
4. C. Alexis and K. Sok, "Blockchain and Distributed Ledger Technology (DLT): What impact on the Financial Sector", Digiworld Economic Journal, 103, 2016.
5. M.H. Joo, Y. Nishikawa, and K. Dandapani, "Cryptocurrency, a successful application of blockchain technology", Managerial Finance, 2019
6. W. Yang, S. Garg, A. Raza, D. Herbert, and B. Kang, Blockchain: Trends and Future", In Pacific Rim Knowledge Acquisition Workshop 2018, Aug 27 (pp. 201-210), Springer, 2018.
7. Benefits of blockchain, https://www.ibm.com/topics/benefits-of-blockchain
8. Blockchain for Beginners: The complete step by step guide to understanding blockchain technology, Author: Mark Watney, USA