K. Thakur et al., *Emerging ICT Technologies and Cybersecurity*
https://doi.org/10.1007/978-3-031-27765-8_4

4. Blockchain Technology

Kutub Thakur[1] ✉, Al-Sakib Khan Pathan[2] and Sadia Ismat[1] ✉

(1) Department of Professional Security Studies, New Jersey City University, Jersey City, NJ, USA

(2) Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh

✉ **Kutub Thakur (Corresponding author)**
Email: kthakur@njcu.edu

✉ **Sadia Ismat**
Email: sismat@njcu.edu

Introduction to Blockchain Technology

Blockchain technology is a digital peer-to-peer network powered by the innovative, secure, reliable software platform for the management and processing of customers' transactions without any centralized control and management mechanism. It is fully decentralized and peer-to-peer network, which is used to manage both tangible and intangible assets through digital transactions. In this technology, the software operating at the core of the platform is fully distributed, which means that there is no centralized node like servers to control and manage. This network is managed by the automated network consisting of numerous nodes located at diverse locations, which process and verify each transaction that takes place on the network to authenticate its legitimacy and correctness. This technology consists of the following components [138–140]:

- A network of peer-to-peer nodes located at diverse locations
- A distributed data management software
- Immutable records of tangible and intangible assets
- Smart contract algorithms/protocols.

Blockchain technology is so reliable and secure that no transaction of online activities can be changed or tempered to alter the correctness of the transaction in the database because it is verified by all nodes spread across the regions in the network. Once the transaction is checked and verified for its correctness, it is stored in the form of block of data, which is also encrypted into hashes. Thus, it is also referred to as the distributed ledger of immutable transactions for management of tangible as well as intangible assets. This technology was first-time developed and used for the cryptocurrency "Bitcoin", which is a decentralized system of digital currency without any intervention of any third-party or centralized body.

Top Features of Blockchain Technology

Blockchain technology is getting increasingly popular in all sectors, industries, and governmental domains due to its wide range of capabilities, features, and characteristics. The most common features (of it) are highly beneficial for the businesses to save substantial amount of money and valuable time along with ensuring top-level security and reliability. The main features and characteristics of blockchain technology are summarized as follows [138–140]:

- A peer-to-peer network of diverse nodes that check, verify, share, and store the transactional activities on the network.
- Referred to as a digital distributed ledger of immutable records of assets.
- Entire verified record is stored in block of information, which is shared with all nodes of the network simultaneously.
- Each node participates in verification and authentication process of a transaction through different techniques to build consensus among the nodes such as:
  - Proof of Work (PoW)
  - Proof of Stake (PoS).
- At the core of the blockchain technology stands three main technologies such as:
  - A source of computer resources to process and store database of transactions
  - Distributed peer-to-peer network technology with shared ledger
  - Cryptographic keys used to encrypt the data storage in the ledger.
- This technology uses two types of cryptographic keys known as private and public keys.
- One user of the technology is defined by both of the private and public keys jointly referred to as "digital signature" or digital identity. This is the basic component used for verification and authorization of the transactions on the network.
- Numerous types of assets, both tangible and intangible can be traded and managed through this secure technology of distributed ledger.
- It reduces the cost of ledger management and transaction management in any kinds of business and removes the barrier and charges of using the services of third-party or government agencies for their approvals and agreements.
- It is highly secure and immutable technology, which cannot be tempered. Even if some mistakes occur, it is picked up by numerous nodes and the correction is stored in the form of another block of

data pertaining to that error. Thus, it is highly reliable and provides a complete details of and trail of the activities transparently.

- It can be used in a range of applications such as cryptocurrency, voting systems, government data management such as lands, revenue, contracts, purchases, finances, banking and insurance, defense and security, and many others.
- “Smart Contracts” is another futuristic use of this technology to automatically manage the entire process, activities, transactions, modification, changes, and other aspects of a business contract based on well-defined rules through this technology.

In the nutshell, blockchain technology is the future of modern processes in almost all domains of industries, businesses, governments, and societal management systems.

History of Blockchain Technology

The traces of blockchain technologies can be tracked long before it came into existence in 2008. The first trace of this technology can be found in the work of David Chaum, who enunciated a mechanism or protocol, which is like blockchain technology in 1982 in his research dissertation named as “*Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups*”. The future based on this concept was accomplished by Stuart Haber and W Scott Stornetta in 1991. Their further work along with Dave Bayer resulted in the incorporation of Merkle Tree into the design of the secure block of data through untampered timestamp. Thus, the concept of secure block of data in which timestamp cannot be tempered started getting materialized in those days.

Fast forwarding from 1992 to 2008, a group of people or just a person, who was popularized as Satoshi Nakamoto introduced highly secure and improved block of decentralized database with the help of hashcash-like method to timestamp the digital transaction without any intervention of any third-party in the process. This improved version of the blockchain technology was primarily coined as block and chain denoted separately but later on it was merged. This is very important to note that Satoshi Nakamoto remains unknown and invisible physically in the field of this unknown technology other than just one clue that this group or a single person belonged to Japan (at the time of writing this book). The chronicle timeline after this development is summarized in the following points.

- **2009—**The launching of the first-ever cryptocurrency based on the improved blockchain technology developed by Satoshi Nakamoto. The bitcoin became the new introduction of blockchain technology, which then entered into numerous other industries and business domains in the modern digital world.
- **2010—**The first commercial transaction of bitcoin based on blockchain technology took place on May 22, 2010 when Laszlo Hanyecz bought two pizzas for 10,000 bitcoins from local pizza vendor in Florida [141].
- **2011—**The second digital product based on blockchain technology and named as NameCoin DNS system was developed in April, 2011 and Litecoin later in October 2011.
- **2014—**The total size of bitcoin ledger file became 20 GB.
- **2016—**The previous structure of term was “Block Chain”. This was merged to create new term known as “blockchain” technology
- **2020—**Total size of the file of bitcoin became over 200 GB (and, still expanding).

The use of blockchain technology has become a commonplace activity in numerous business processes across all industries of the world. Newer products and services are emerging on the technological sphere that are using blockchain technologies to make the most of it.

Major Terms Used in Blockchain Technology

Blockchain technology uses different terminologies, both technical and commercial, for its use and understanding. A few very common terms used to define and convey the information among the technical and commercial users are mentioned below:

Cryptographic Hash

Cryptographic hash is an output code of a message of arbitrary size produced in equal length of code through cryptographic hash function generating algorithm. The cryptographic hash converts data of any types, sizes, or formats into output text string of equal length consisting of numbers and letters. The output is always unique for any data hashed through hashing function algorithm [142].

The main features and characteristics of cryptographic hash function used in blockchain technology are mentioned below:

- Hash code is easy to create with the help of an algorithm and almost impossible to break.
- It is not understandable though you can read the characters—letters and numbers used in the message but no meaning can be achieved.
- The cryptographic mechanism has different types, sizes, and formats of input data but it encrypts into a same-sized output message based on the technology used in hashing algorithm.
- The basic function of hashing is to compress the input message into a smaller size and cryptographic process means the encoding of the entire message. Thus, the encoded text for the compressed input message is the meaning of cryptographic hash.
- The encrypted hash code acts like a fingerprint of the file encoded with the cryptography.
- A minor change in the input message alters the output cryptographic hash message hugely that is known as Avalanche Effect.
- Cryptographic hashing is referred to as non-reversible or you cannot break and get the input message from the output code. The hackers either try to build their own huge database of hash codes and run comparison of the codes with huge database to try to break into the code or unleash brute force attacks (i.e., trying all possible options with repeated trials) for the same purpose.
- Creation of similar hash code is almost impossible due to the ability of the cryptographic hash of message collision resistance.
- Cryptographic hashing is based on mathematical procedure to generate unique output strings of data through a mathematical algorithm.
- Cryptographic hashing is also known for its foreordain property, which means that the output code for the same message is always the same.
- The main domains of application of this hashing function include:
  - Duplication detection or unique file detection applications

  - – Fingerprinting and password verification processes
  - – Digital signature applications
  - – Proof of Work (PoW) and Proof of Stake (PoS).

- The most common cryptographic hash algorithms used in the modern technological sphere include MD5, SHA-1, Bcrypt, Whirlpool, AES, and others.

Transaction

A transaction in blockchain technology is a procedure of activities to send message/data from one user account to the other concerned user accounts. It involves numerous steps to complete a transaction, which is later registered in a block of data in the blockchain database. The main steps that constitute a traction in blockchain include [143]:

- The request for a transaction originates from a single end-user in the blockchain network
- An authentication process starts for that particular request before further-proceeding
- A block is created representing that particular transaction
- All nodes of the blockchain nodes get the copy of that transaction block
- Each node has to validate that transaction based on certain validation procedure
- The nodes are rewarded for their work of validation know as Proof of Work (PoW)
- The verified block is added to the existing chain of blocks
- The update is sent out across the network to all nodes in the blockchain network
- This brings the completion of a transaction in blockchain technology.

Proof of Work

Proof of Work, precisely referred to as PoW in blockchain technology, is a process of developing consensus on the validation of a transaction and mining of a new blockchain token. In other words, it is a mathematical puzzle validation in blockchain network to avoid any malicious use of activities in the network. The main characteristics of "Proof of Work" are mentioned below [144]:

- A decentralized consensus procedure in which the members of the blockchain network expend efforts or work for solving an arbitrary mathematical puzzle for avoiding any kinds of misuse or malicious use of the network.
- This process is extensively used for cryptocurrency mining and transaction validation.
- This automatic mechanism plays the role of third-party verification agents used in the traditional systems of transactions.
- Due to extensive usage of power on computing for solving the puzzle, PoW is being replaced by a new method of consensus known as Proof of Stake (PoS).
- This is also known as the proof of expending the computational resource or power in the network for achieving the consensus on the work performed by a node.

Block

Block is a kind of data structure used in the blockchain technology to store the entire details of a transaction in it. The stored data in the block is properly authenticated, validated, and encrypted for maintaining a high level of security and reliability. The most common characteristics of a block used in the blockchain technology include [145]:

- A block is a permanent storage container of data of a validated transaction, which cannot be altered or removed once it is closed.
- A block contains the encrypted data from the previous blocks and the future blocks to make it more robust and reliable.
- The new block is created only after the validation of the information in a particular block by developing consensus among the nodes.
- Blocks of information can be used for a range of transactional information including cryptocurrency, governmental activities, revenue transition, and many others.

Mining

Mining is a process that is used in cryptocurrencies to either generate the new coins or to validate the transaction over the blockchain network. A huge network of decentralized nodes spread across the globe are the main source of mining that solve the mathematical puzzles for generating a new value on the cryptocurrency network or the validation of the transactions that are taking place on the networks powered by the blockchain technology. The blockchain technology offers an option of rewarding the mining nodes for their work with the proof that they expended the computation resources or power for the purpose of solving the mathematical puzzles.

Timestamp

The fingerprint or authorized code against a message that may be a value, title, text, or a digital asset when verified and stored in the block is known as the timestamp. This timestamp is also known as hash in the blockchain technology. Hash is a unique code generated against an arbitrary input of different size, type, and content of a digital file. Initially, the blockchain technology was invented for time-stamping purposes. A few very common characteristics of timestamp and timestamping process used in blockchain include [146]:

- The encoded hash in equal size and unique code (together) is known as timestamp of the data.
- The data may be a text file, a value, a string of text and numbers, or any title or a digital data file.
- All features of timestamp are similar to hash or fingerprint, which holds a huge amount of information about the transaction or activities within it, which cannot be removed or altered.

Stack of Technologies Forming Blockchain

Blockchain technology used in different domains is a combination of software and hardware technologies, which constitute a robust network of blockchains that is reliable, secure, and encrypted. The most common technologies that form blockchain stack are mentioned below.

Cryptographic Keys

Cryptographic keys are two different types of keys or codes used in building digital signature for authentication of the ownership of the transactional data in a blockchain-based network. There are two types of cryptographic keys such as [147]:

- Public key
- Private key.

A public key is a code that is used to identify the address of a user-entity in the blockchain technology. It is also paired with the private key for establishing ownership on the assets associated with the private key or address. It is like the email address used for email communication. Anyone can send a digitally signed transaction to your public key but cannot access it without having the combination of the private key. The public key is also encrypted form of message or information, which can easily be encoded for any transaction on blockchain technology but it is very difficult to decode or decrypt to find out the original message in the key.

On the other hand, the private key is very vital for the ownership, security, and control over the blockchain assets. It is a long string of digits, letters, or combination of both. It can be a huge number in the form of the following expressions:

- A long binary code of 256 characters
- Hexadecimal code of 64 digits
- A long mnemonic phrases
- QR (Quick Response) code.

The main features and functions of a private key in blockchain technology are mentioned in the following summarized points:

- It is a long, randomly-generated, and encrypted string of numbers or alpha-numeric characters.
- Used for the authentication and ownership of the assets on blockchain.
- Private keys are normally very long strings in such a way that they cannot be cracked through brute force attacks.
- Creating a public address or public key from a private key is very easy and possible through a mathematical calculation or mathematical puzzle solution but the reverse engineering for decrypting private key is almost impossible.
- It should always be stored carefully and should never be shared with anyone. If it is lost once, you would lose all assets on blockchain technology.

Peer-to-Peer Network with Shared Ledger

A peer-to-peer network with shared ledger is a network of wide range of nodes or computer machines installed with the blockchain technology that enables them to coordinate in a peer-to-peer network environment without any intervention of a server or any other network agent or any other third-party—either human or technological. A shared ledger of transactions operates and updates on all peer nodes across the network. This means, all nodes have the same shared ledger, which is updated on a regular basis through a robust process of authentication and authorization.

Computing Resources to Store Transactions and Network Records

The computing resources that are used for storing the network transactions on a blockchain technological network are those computing nodes that are private entities added into the global network of any private blockchain service or any private blockchain service. Those computing resources are hosted by the interested parties and they pay for the expenditures and operational charges. The owners of those computing resources to store blockchain records are shared ledger, which are verified and mined by that node. For that mining or verification purposes, the owners of those nodes are rewarded with associated cryptocurrency assets such as bitcoin or any other digital currency or any other services of tangible or intangible assets on the blockchain.

How Does Blockchain Technology Work?

A blockchain technology-based network consists of three main entities named as **Node**, **Blocks**, and **Miners**. The entire process of working is based on the activities among and on those elements of the network. The working functions and roles of the three elements are described below separately [148].

Node

A node in this case is a computer machine that hosts the mining software, unique alphanumeric ID number, and distributed ledger of blockchain technology. It is not a property of any particular controlling party but anyone has right to add a node to the blockchain node by fulfilling the requirements of the network and technology stacks. The node is rewarded for its work of mining and authenticating the transactions on the blockchain network automatically without any intervention of any centralized authority or third-party organization.

Block

A block is the basic container that contains the encoded information or message including the transactional details in the chain. A block consists of the following three major elements:

- **Data—**This is the information in a block, which is encoded, authenticated, and verified with additional details regarding the past and future blocks in the transactional series of activities on the blockchain network.
- **Nonce—**A nonce is randomly created whole number of 32-bits. It is generated when the block is created by the network. The most important functionality of nonce is to generate the block header's hash. The hash is interlinked with the nonce number. The hash is a long string of zeros with a very small value. It consists of 256-bit number, mostly containing zeros in the beginning of the string.
- **Miners—**The miners are the computing resources attached with a node and unique ID number working in relationship with the blockchain technology software. The main responsibility of miners is mining of the new encrypted resources and authentication and verification of the transactions in the network. The miners generate their own block of information that consists of a nonce of 32-bits and a long string of zeros with a very small value (automatically generated numbers) linked with each other. A new block that is added to the chain of blocks after mining or verification and validation consists of many things such as tile hash, nonce, reference to previous hash in the chain, and others. Miners find out the matching combination between the 32-bit nonce and the hash of 256-bit code through a mathematical algorithm running in a puzzle solution application. There will be around four billion possible

nonce-hash combinations to solve to reach the golden nonce. The golden nonce is rewarded with a certain value of that asset defined on the blockchain asset network.

What Is Distributed Ledger Technology (DLT)?

Distributed Ledger Technology, precisely referred to as DLT, is a detailed structure of entire stack of blockchain technology protocols that enable the entire ecosystem of blockchain technology to create, authenticate, verify, and store the message or information in the encrypted form on a distributed ledger (of long queues of blocks of information located on every node in the network). This is the core spirit of the blockchain technology or it is the real philosophy of blockchain distributed ledger technology commonly adopted in the modern digital asset management as well as in all types of cryptocurrencies and Ethereum platforms [149].

Types of Blockchain Technology

Blockchain technology has become very popular within a few years in all domains of businesses, governments, and social sectors due to the security, privacy, and robustness that it offers to the organizations and people. This technology also offers flexibility to customize the use of this technology in different ways. The most common categories in which the blockchain technology can effectively be used are the following [150]:

- Permissionless blockchain category
- Permissioned blockchain category
- Hybrid features of the above (both) categories.

In the permissionless category of blockchain, it is used in the way that no permission or control is established over the nodes of the network. The nodes in this category can join without any permission with a pseudo-anonymous approach. There is no centralized authority to regulate or control the network types falling under this ambit. The main type that works on the basis of this category of blockchain is: Public blockchain network.

In the permissioned category of blockchain, there is a centralized control of a group, consortium, or an authority. In this category, the nodes are granted permissions by the centralized authority thus, reducing the security-level, privacy, and other major features of the traditional blockchain technology. The types of blockchain networks falling under the permissioned category of networks include: Private blockchain network and Consortium blockchain network.

The third category of blockchain technology is the middle-way of the above-mentioned main categories (permissioned and permissionless). This uses the combination of the features of both categories. An example is the Hybrid blockchain network.

The details of all those types of blockchain technology networks are described separately in the following sub-sections. Meanwhile, this is very important to note that the core objectives of developing blockchain technology were to establish a network that has no influence of any centralized controlling authority or entity and to maintain high-level of privacy, anonymity, security, and reliability. If there is a control on the entry of the nodes in a network, the network gets less secure due to lesser number of nodes in a blockchain network to process the authenticity of the transactions. The example of such networks are the private and consortium networks. Let us know about these types of blockchain networks with more details.

Figure 4.1, it is very clear that the types of networks falling in the permissionless category are the public networks with full features and capabilities of blockchain network while the permissioned networks are controlled networks and the hybrid one shares the features of both the categories.

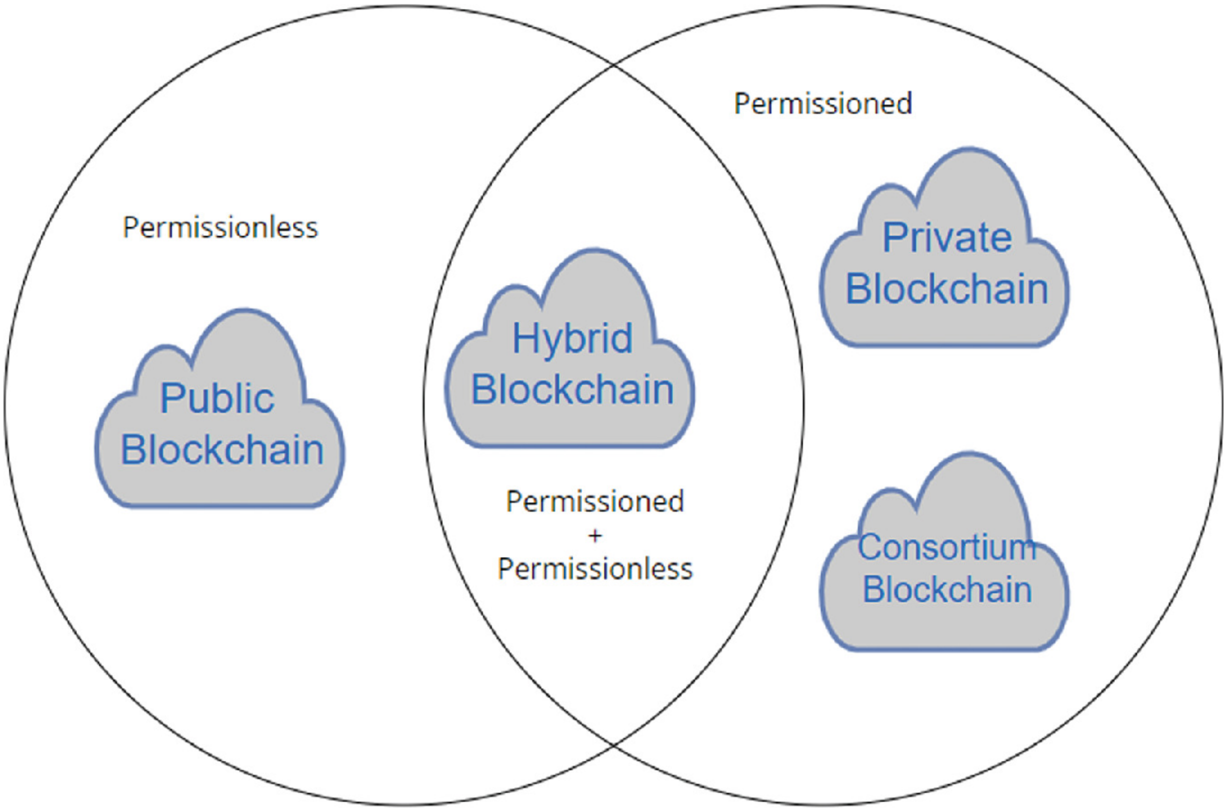

Fig. 4.1 Schematic diagram of categories and types of blockchain networks

Public Blockchain

A public blockchain technology is characterized by the most common features that were the foundation of the technology such as:

- A sub-set of permissionless category of blockchain
- Offers full decentralization of the control
- No third-party is involved at any level of control
- Any public node can participate in the network with basic prerequisites
- All nodes have equal rights in the network to access and work in the blockchain network
- All nodes can create new blocks, mine data, and authenticate transactions
- The examples include bitcoin, Ethereum, Litecoin, and so on.

Private Blockchain

The private blockchain is a controlled type of blockchain technology that is centrally managed by a third-party organization or an entity. The main features of this type of blockchain include:

- A type of permissioned category of blockchain technology, which is fully managed by the third-party organizations or persons.
- The centralized controlling authority of private network is one entity
- Any new node to be added to the network is fully under the authority of the network management body
- All nodes do not have equal rights delegated by the central management system
- Public access to participate in the network is not allowed
- The examples of private blockchain networks include Hyperledger, Ripple, and so on.

Consortium Blockchain

A consortium blockchain, as the name implies, is a network that is private-like network but with multiple controlling authorities grouped in a consortium. The main features and characteristics of consortium blockchain are:

- It is a type of blockchain network that falls under permissioned category
- The controlling authorities are more than one or a group of companies known as consortium
- It is more decentralized in nature than the private networks, which are fully managed and controlled
- More secure than public blockchain networks but less secure than private blockchain networks
- The examples of consortium blockchain technology include CargoSmart, and R3 software consortium platform.

Hybrid Blockchains

The hybrid type of blockchain technology has the characteristics and features of both the private and public blockchains. The main features of this type include:

- Blockchains that are managed by one organization with limited features of private network and other features of a public network for maintaining higher level of security.

- This is a domain-specific performance improving solution based on certain customized features and capabilities.
- The example of hybrid blockchain type of technology include the IBM Food Trust designed for the improvement of the food supply chain's performance while maintaining the high-level of security and privacy of the network.

Typical Uses of Blockchain Technology

The global market size of blockchain technology was just USD $1.5 billion in 2018. According to the Statista information, this market size is projected to cross USD $162.84 billion by 2027 with an exponential growth due to the high level of traction achieved by this technology in all domains of businesses, governments, and other fields of our day-to-day lives [151].

The use of blockchain technology is spreading across the domains, sectors, and fields all around the world. Among the use cases of blockchain technology in different fields, a few very typical ones are mentioned below with more details.

Cryptocurrency

Cryptocurrency was the most prominent use case of blockchain technology, which utilizes the power of blockchain technology to its fullest in the public category of this technology with full anonymity, security, and privacy. The popularity of cryptocurrencies, especially bitcoin, overshadowed the name of this basic technology in such a way that blockchain technology looks (sometimes) like a sub-name of bitcoin in some normal audience in the world.

According to Research and Markets projections, the global market size of cryptocurrencies will reach a whopping USD $32.42 by 2027 from just USD $1.78 billion in 2021 with a staggering growth of over 58.4% CAGR (Compound Annual Growth Rate) during the projected period. These figures are quite clear indicators of the level of traction of blockchain in the cryptocurrency market [152].

The first cryptocurrency named as bitcoin was created in 2009. Within just over a decade, there are more than 18,000 cryptocurrencies that exist in the global market size. Many new cryptocurrencies are in the development. A large number of governments are also considering to introduce their own cryptocurrencies to benefit from the huge market potential of blockchain technology in the domain of global payment systems. The most common or most popular cryptocurrencies in 2022 are bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Cardano (ADA), Dogecoin (DOGE), Binance Coin (BNB), Stellar (XLM), Dollar Coin (USDC), and so on.

Non-Fungible Token (NFT)

Non-fungible tokens, precisely referred to as NFTs, are a type of digital assets encrypted in the blockchain technology as an asset for trading like a commodity (unlike a cryptocurrency). It is a unique ID and asset created by one owner of that data. These assets cannot be exchanged or interchanged with the other commodities. In other words, NFTs are types of cryptographic assets created in the blockchain technology with unique identity number or code and metadata that differentiate this data from the other similar kinds of data on the blockchain asset network. The main features and characteristics of NFTs are listed below [153]:

- Unique code or ID on blockchain that cannot be altered or replicated
- NFTs are real-world items and assets such as photos, arts, real-estate, properties, and others
- Blockchain facilitates secure and transparent trading of unique assets created in the forms of NFTs that replace the real-world items
- This is a great area of trading and business of copyrighted assets, tangible assets, and digital assets like music, videos, photos, arts, training content, and may others.

According to the Research and Markets projections regarding the NFTs, the global market size of NFTs will reach USD $82.43 billion by 2026 from just USD $21.33 billion in 2022 with a whopping growth of over 40.2% CAGR [154]. The most common example of NFTs is the use of Ethereum, which acts as both NFT and cryptocurrency simultaneously in different types of trades.

Smart Contracts

As the name implies, smart contracts are the (automated) contracts that run automatically by the completion of different activities, actions, functions, and other responsibilities defined in an agreement after the verification and authentication of the same without any involvement of the third-party. Smart contracts have become so popular in modern processes of agreement or contract automation in all types of projects in a wide range of domains in the industries [155].

According to the Verified Market Research projections, the global market size of smart contracts based on the blockchain technologies will reach to over USD $770 million by 2028 from just USD $145 million in 2020 with a gigantic growth of over 24.55% CAGR during the forecast period between 2021 and 2028 [156].

The most important reasons for the businesses to choose blockchain technology for smart contract applications include the highest level of security of the transactions taken on the blockchain due to capability of consensus building, immutability of transaction reversal and alteration, capability of technology to avert any kinds of replication or duplication, and many more. These contracts can incorporate all major phases of a project, and many types of other contracts such as escalation matrix, payment matrix, service level agreements (SLAs), responsibility matrix, and so on. All functions and activities such as task accomplishment, collaboration, asset sharing, billing, operations, and many others required for a particular project are automatically accomplished and acknowledged by the roles that have been designated to complete those tasks. The release of payments and all other final financial transactions are also completed automatically without any intervention of a third-party entity.

Financial Markets

Financial markets, especially in the modern banking and other financial services, the use of blockchain has become very fundamental. The growth of the size of the financial market has increased significantly during past few years. According to the forecast of Statista in 2020, the global market size of blockchain-powered banking and financial services would reach USD $22.46 billion by 2028 from just USD $0.28 billion in 2018 with a dramatic exponential growth during the projected period and even beyond that period [157].

The most promising areas for the use of blockchain technology in the global as well as local financial markets include:

- International financial transaction management and securities
- Mainstream financial settlements and payments both locally and internationally
- Clearing, securities, and insurance services
- Financial derivative management and trading
- Corporate governance and credit bureau management
- Micro-payment management and financial services at local levels
- Management of pre- & post-trade processes
- Assets management, data registries, and repository services
- Enterprise resource management and financial process automation.

Electronic Voting

Electronic voting is another major use case of blockchain technology due to its capabilities of immutability, duplication- and replication-free, traceability, transparency, and security. There are many countries that have either conducted electronic voting through blockchain technology or are developing such systems with pilot projects. The most important countries that have already implemented electronic voting through blockchain technology at the local levels include the USA, Russia, Sierra Leone, and Japan (so far, at the time of writing this book). Sierra Leone is the first country that has conducted voting through blockchain. The other major countries that are also working on different levels of projects of voting systems based on blockchain technology include India, South Korea, Thailand, and others [158].

Record Maintenance

Maintenance of records transparently without any duplication, fabrication, and alteration is another very important domain of application of blockchain technologies. This is a very vast field, which covers the record keeping in different departments of government such as land, properties, reports, researches, history, and many other assets —both tangible and non-tangible. Meanwhile, numerous private and industrial domains have also huge prospects in using blockchain technology for the management and maintenance of records in different processes, activities, transactions, histories, and many more with highly effective ways.

Supply Chain

According to the Allied Market Research projections, the global market size of blockchain-based supply chain is expected to cross USD $9.853 billion by 2025 from just USD $0.093 billion in 2017 with a huge growth of over 80.2% during the projected period between 2018 and 2025 [159].

There are many companies and countries who are using a range of supply chain systems powered by blockchain technology from major players in the technological domain such as IBM and others. The most common supply chain areas that have already proved to be suitable include the vaccination supply system, food supply chains, digital identity verification and purchase systems, and container logistics. It is expected that many other domains will be explored in the near future where the use of blockchain technology for the management of supply chains will prove highly effective [159, 160].

Government

Government is one of the most promising sectors for the use of blockchain technology. This is because the procedures, assets, information, orders, decisions, and researches, discussions, and stakeholders in this sector are highly sensitive. Also, these should be treated with high level of security, privacy, and secrecy with deep traceability of the events and transactions for any kinds of future requirements to maintain transparency and confidence of the public in governments.

There are a wide range of areas and departments in the government sector where the blockchain can be deployed with full confidence. A few of those main areas and activities of governments are listed below:

- Electronic voting systems
- Land property management
- Licensing and penalty systems
- Judiciary and legislation systems
- Utility management and provisioning systems
- Social securities, insurance, and other financial systems

- Banking and trading systems
- Defense and security research and development
- Cryptocurrency and digital asset management.

In a nutshell, the government sector is the biggest one that can use the potential of blockchain technology in wide range of its activities, processes, departments, and domains to make them more robust, secure, reliable, transparent, and effective for their respective people.

Impact of Blockchain Technology on Cybersecurity

Blockchain technology is very well known for its capabilities of providing high-level security, end-to-end encryption, anonymity, immutability, data integrity, confidentiality, and privacy. If all those factors are related to one way or the other, they associate with the robust security of data, communication, applications, and devices. Simply put, the impact of blockchain on cybersecurity is highly desirable and even prospective.

Cybersecurity is based on the CIA (Confidentiality, integrity and availability) triad model. This model helps the cyberworld in protecting valuable data from getting damaged or stolen, safeguarding edge devices or network elements from any kinds of external or internal malicious exploitation, and maintaining the performance and working efficiency of the cyber-based systems of communication, data management, process management and others. All those functions fall under the summary of CIA triad model, which expresses three major components such as [161, 162]:

- Integrity
- Confidentiality
- Availability.

Let us explore the impact of blockchain technology on the cybersecurity by comparing the main features and capabilities of blockchain technology and finding their use in the enhancement of the major security issues in the cybersecurity domain. This will provide a better overview of the impact of blockchain technology on the cybersecurity enhancement. The main risk areas of cybersecurity management include the following:

- **Exploitation of protocol vulnerabilities—**This is one of the major areas that is exploited by the hackers to intrude into the cybersecurity or security systems of a network or an environment such as home automation, local area network, access control, and others. There are numerous communication protocols that have vulnerabilities that are exploited by the hackers. If all communication protocols are powered by the secure capabilities of blockchain, they can provide higher level of security through secure communication, authentication, verification, and encryption of the data during the communication and transmission.
- **Edge device vulnerabilities—**Edge-devices are the most preferred nodes or elements for the hackers or malicious users due to numerous ways to exploit them and their vulnerabilities. By using the power of blockchain technology, cybersecurity personnel can decentralize the management and control through blockchain. In fact, highly secure authentication, authorization, and verification processes could be handled by the basic features of blockchain technology.
- **DNS systems breaches—**The breach of hierarchical systems of Domain Name Services (DNS) are another main target of the malicious users. If the DNS system is decentralized and controlled through extremely secure, reliable, and robust system of blockchain for managing the DNS services, a major domain of exploitation or vulnerability can be controlled or eliminated while maintaining the performance of the system simultaneously. By using the power of blockchain, Distributed Denial of Service (DDOS) attacks can easily be averted or reduced significantly and security can be enhanced tremendously.
- **Internet of Things (IoT)—**IoT is a vast domain of concern for the cybersecurity nowadays. It consists of a huge number of devices, which are run by different operating systems, firmware, controlling systems, connectivity vulnerabilities, and many others. All those factors can easily be exploited by the hackers to intrude into the system and breach the data or security of the network. If the decentralized management of all those devices connected to the IoT

environment are managed by the decentralized processes powered by the blockchain technology, a huge boost in the cybersecurity field can easily be achieved.

- **Data integrity breaches—**The breach of data integrity can happen either on the storage device or in the transition. The end-to-end encryption and decentralized control of the transactions during the communication powered by the blockchain technology, can increase the security of data integrity significantly.
- **Miscellaneous issues—**Numerous other issues such as patch installation, verification, access control, and many other monitoring and risk assessment issues can easily be powered by the highly secure features of blockchain technology (to enhance the security level hugely).

Thus, the impact of the blockchain on cybersecurity is highly desirable and many companies, organizations, and governments are incorporating the power of this technology for boosting cybersecurity of their respective systems. This trend is expected to grow further in the coming days.

Sample Questions and Answers

Q1. Write down at least three main features and characteristics of blockchain technology.

A1. Three main features and characteristics of blockchain technology are:

- A peer-to-peer network of diverse nodes that check, verify, share, and store the transactional activities on the network.
- Referred to as a digital distributed ledger of immutable records of assets.
- Entire verified record is stored in block of information, which is shared with all nodes of the network simultaneously.