CHAPTER 1

Fundamentals of Blockchain

LEARNING OBJECTIVES

Readers generally find it difficult to understand the philosophy of blockchain when they are new to the topic. Also, they do not know where to start learning about the concept or the types of problems which could be solved using blockchain. This chapter intends to give the readers a starting point to understand the Blockchain and the cutting-edge technology behind its functions. It commences with a historical look at the timeline in this field and proceeds to give a brief background into the different aspects of blockchain.

1.1 INTRODUCTION

Welcome to the world of Information Technology! You are about to explore a vibrant subject in the arena of innovative technology. Computer and information technology are a vital part of any industry. The need for humankind to perform a process with perfection and accuracy commenced with the origin of computers. The digitalized computing machines, initialized in the 1940s, merely carried out arithmetic operations marking the first step towards the innovative computers of today. Computers are part of our day-to-day life now. Computer networks connect not only computers around the globe but also human beings across the world.

Today we are at the Fifth Industrial Revolution with over 50% of the world connected via the internet and technology progressing at its most sophisticated phase with Artificial Intelligence, Big Data, virtual reality, and one of the most disruptive technologies—the Blockchain, forming the bedrock of such development.

Blockchain is fast becoming one of the most sought-after technologies of today. This exciting new technology is redefining how we store, update, and move data. In this chapter, we will see what Blockchain is and how the technology works, including the concepts of cryptography, mining, and its essential components.

1.2 Origin of Blockchain

1.2.1 What Is Blockchain

Technically, Blockchain is defined as a distributed, replicated peer-to-peer network of databases that allows multiple non-trusting parties to transact without a trusted intermediary and maintains an ever-growing, append-only, tamper-resistant list of time-sequenced records.

In short, Blockchain is a type of distributed ledger that sits on the internet for recording transactions and maintaining a permanent and verifiable record-set of information.

This innovative technology was first published in 2008 by Satoshi Nakamoto (pseudonym of a person/persons as-of-yet unknown) in a white paper titled "A Peer-to-Peer Electronic Cash System." The thought behind the design was to create a decentralized digital currency that is free from government regulation whereby two people can confidently trade directly with one another without the need for mediators or intermediaries.

In 2009, the concept became a reality when Satoshi Nakamoto implemented the first application of the Blockchain we all know as Bitcoin.

Though Bitcoin and Blockchain are often referred to interchangeably, they are not the same. Blockchain is the underpinning technology that the Bitcoin was built on. Now aside from Bitcoin blockchain, we have the Ethereum blockchain and other private blockchains that are adapted to cater to various industry applications such as supply chain, cross-border payments, and many others.

1.2.2 The Bitcoin and the Blockchain

To better understand the difference between Bitcoin and Blockchain, let us delve a little bit into what they are and what they are not.

1) Meaning

Bitcoin is a cryptocurrency, while Blockchain is a ledger or database of information. Bitcoin was created to reduce the government's control over cross-border transactions and to speed up the transaction process by removing the need for third-party intermediaries. Blockchain, on the other hand, provides a secure environment that Bitcoin needs for peer-to-peer transactions. In other words, blockchain acts as bitcoin's ledger and maintains all the transactions of bitcoin.

2) Scope of Usage

Bitcoin is limited to currency transactions, while the blockchain has numerous applications. It can not only trade currencies, property rights of stock but also be used for identity management, records management, research management, as well as many other areas that cover all aspects of the business.

3) Transparency

Bitcoin has a high degree of anonymity. Though the transactions are visible, it is close to impossible to identify the user. Until today, the identity of Satoshi Nakamoto is a mystery even though Satoshi has roughly one million bitcoins (BTC) worth around 8 billion dollars as of 2019.

On the other hand, Blockchain is quite transparent as it is expected to work across multiple industry applications. However, with Smart contracts and various consensus mechanisms, Blockchain can assure compliance to KYC and other industry standards.

Though Bitcoin will continue to hold the coveted position of the world's first decentralized cryptocurrency, its operational significance is considerably reducing with the blockchain technology taking the limelight into various industry sectors like Healthcare, Travel, Education, Government, and others.

1.2.3 The Evolution of Blockchain

The first Bitcoin was mined in 2009. Table 1.1 outlines a brief history on the journey of blockchain from the Genesis Block to the cusp of the Blockchain fourth generation.

Table 1.1 History of blockchain

Pre-blockchain – The Early Years	The 1950s	– First computers developed and adopted
	The 1960s	– 1969: **Arpanet**, the early Internet on the peer-to-peer network
	The 1970s	– 1973: **Public-key cryptography** implemented by Clifford Cocks – 1977: RSA, the public-key cryptosystem that is widely used for secure data transmissions, is released. – 1979: Ralph Merkle patents the concept of hash trees now called **Merkle tree**
	The 1980s	– 1982: IBM Personal Computer launched with DOS operating system
	The 1990s	– 1991: Stuart Haber and W Scott Stornetta work on a cryptographically secure chain – 1997: **Proof-of-work** with Hashcash – 1996: Nick Szabo introduced bit gold as a mechanism for a decentralized digital currency and smart contracts – 2000: Stefan Konst introduced a general cryptographic theory of secured chains

(*Continued*)

Table 1.1 *(Continued)*

Blockchain 1.0: Origin of Bitcoin	2008	– Oct 31: **Satoshi Nakamoto** releases Bitcoin white paper – a concept on the peer-to-peer payment system – Bitcoin.org registered in August
	2009	– Jan 03: **Bitcoin Genesis block** mined – Jan 12: Hal Finney receives first Bitcoin transaction, thus launching the first application of a public blockchain – Oct 12: Bitcoin registered open source code – Oct 31: Bitcoin Market – Bitcoin recognized as a digital currency
	2010	– May 22: First Bitcoin purchase - 10,000 BTC for a $25 pizza – Nov 06: Bitcoin marketplace surpasses $1 million
	2011	– **Namecoin**, the first Bitcoin fork – **Litecoin** released as an alternative to Bitcoin with different mining algorithm and faster transaction speed – Bitcoin reaches parity with the US dollar (1BTC=1USD)
	2012	– Diaspora, the first decentralized social network – **Ripple**, a permissioned blockchain, is launched. A payment protocol focusing on integration with banking systems – The Bitcoin Foundation launched in September
Blockchain 2.0: Ethereum and Smart Contracts	2013	– Mar 28: Bitcoin marketplace surpasses $1 billion – May 02: First Bitcoin ATM unveiled – The University of Nicosia in Cyprus accepts Bitcoin – **Mastercoin** (the first Altcoin) is one of the earliest – Vitalik Buterin releases **Ethereum** white paper
	2014	– Establishment of **R3**: a consortium of over 40 financial institutions committed to implementing Blockchain technology – Ethereum Blockchain is funded by crowdsale – PayPal announces Bitcoin integration – Microsoft accepts Bitcoin
	2015	– **Genesis block** in Ethereum created – Linux Foundation unveils **Hyperledger** to boost blockchain development. – Visa, Citi, Nasdaq, Capital One and Fiserv invest $30M in Blockchain startup Chain.com

(Continued)

Table 1.1 *(Continued)*

Blockchain 3.0: Distributed Applications	2016	– Bug in Ethereum DAO code exploited, causing theft of $50 M in ether
	2017	– **EOS** unveiled by Block.one as a new Blockchain protocol for industry-scale decentralized applications.
Blockchain 4.0: The Future	2018 - future	– Current Bitcoin marketplace between $10-$20 billion – TRON, a blockchain platform for the entertainment industry – Business-oriented hybrid blockchain projects – Integration with IoT, AI and Big Data

The concept of digital computing and cryptography started to appear in the 1900s and early 2000. It is these concepts and implementation that inspired the Blockchain 1.0 – the Bitcoin.

a) First Generation Blockchain (2008-2013): The Origin of Bitcoin

In 2009, Bitcoin became the first application of Blockchain technology. Satoshi Nakamoto formed the Genesis block. On 12 Jan 2009, the first successful bitcoin transaction on the blockchain takes place between Nakamoto and Hal Finney.

The first generation of blockchain promised transparency, immutability, accountability, and security in transactions. However, the protocols used (Proof-of-work consensus, explained later in this chapter) necessitated the use of heavy mining hardware and significant resources leading to problems in scalability, interoperability, and speed. To date, Bitcoin is one of the slowest cryptocurrency, taking about 10 minutes to confirm a transaction.

b) Second Generation Blockchain (2013-2015): Transactions with Smart Contracts

The second-generation sought to overcome the limitations of the Bitcoin. Thus emerged Ethereum in 2013, when it was realized that the underlying technology of Bitcoin could be used for all kinds of B2C and other general applications. It still used the Proof-of-work algorithm and had less-than-optimal speed. Though Ethereum required lesser energy to maintain, there were still concerns about future scalability. However, with the hosting of Smart Contracts that made available new functionalities, Ethereum was the go-to blockchain for Enterprise use.

c) Third Generation Blockchain (2015-2018): Distributed Applications

This generation saw the arrival of Hyperledger from the Linux Foundation and Decentralized Applications (DApps) of Ethereum. Though the Hyperledger is a platform that can plug in any consensus mechanism, Smart Contracts of Ethereum opened up the possibility of a Proof-of-Stake consensus mechanism. The focus of the generation was consensus mechanisms that can bring greater interoperability and boost network speeds.

Promoting cross-chain transactions, using sharding (a type of database partitioning that separates vast databases into smaller, faster, and more easily managed parts) and establishment of parallel chains are only some of the approaches being taken by the third generation blockchain solutions. However, EOS and TRON have taken over the DApps market due to the scaling issues still inherent in the Ethereum platform.

d) Fourth Generation Blockchain (2018–Future)

Blockchain technology's future appears optimistic as many governments and organizations are investing heavily in innovations and applications.

A significant innovation on the horizon is called blockchain scaling. A scaled blockchain is expected to accelerate the processing speeds, without sacrificing security significantly. This is done by assessing the computing power required to validate each transaction and then dividing the work efficiently. Progress in this front is yet to be seen, but the outlook has been positive and more is expected on this front.

1.3 Blockchain Solution

> *"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending. We propose a solution to the double-spending problem using a peer-to-peer network."*
>
> – Part of the abstract from the paper "A Peer-to-Peer Electronic Cash System."

It is evident from the paper that Satoshi Nakamoto was proposing a digital currency trading or payment solution that addressed the double-spending problem that is unique to digital currency transactions. But what is double-spending, and how is a blockchain transaction different from a traditional transaction?

1.3.1 Traditional vs. Blockchain Transactions

Business transactions are recorded in ledgers since time immemorial. History credits the Mesopotamians (now Iraq) as the first record keepers with evidence dating back to about 7000 years. Clay tablets were used to record the expenditures of goods received and traded. Paper-based ledger entries or bookkeeping can be traced back to the 13th century. It wasn't till the mid to late 20th century, until the widespread adoption of computers, that the digital ledger replaced the physical ledger. The digital ledger is a digital file or files or database that can be manipulated only using a computer program as it does not have a physical form. Although the medium of entry has changed, the fundamental principles of the recording of sales and purchases have remained the same throughout the centuries. The general ledger records the assets, liabilities, income, expenses, and capital of the company or business. While digital transactions resolved the disadvantages of manual paper-based transaction entry in terms of time-consuming recording and maintenance, human error, lack of security and limited copies that could not cater to large organizations, it, however,

brought in its own set of complexities related to data inconsistencies, potential frauds, and other technical issues with respect to outages and virus attacks.

Let us understand transactions with the following basic example. Joe purchases a painting from Ann for $50.

Scenario 1: The simple transaction would be where Joe hands a physical $50 note to Ann, who will then hand over the painting to Joe (refer Fig. 1.1). In short, Joe has received goods worth 50 dollars.

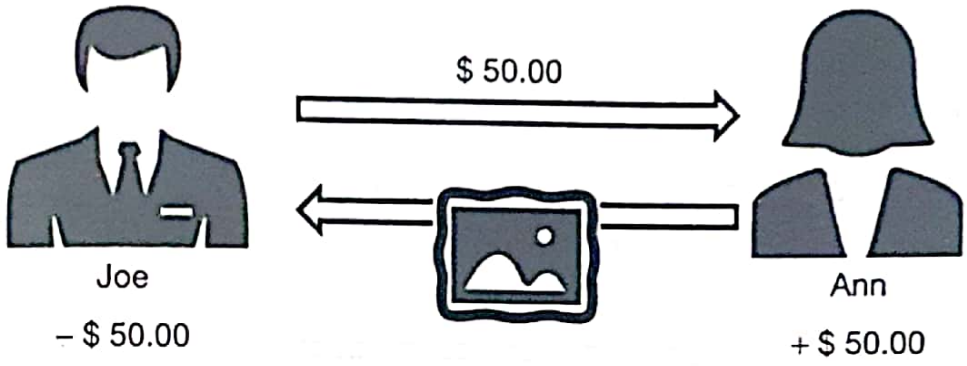


Figure 1.1: Physical transaction

Scenario 2: Assume a modern-day scenario where Joe and Ann are unable to meet. They would like to do the transaction online (refer Fig. 1.2). In such a case, the bank acts as the central authority or intermediary. In the online transaction scenario, the bank debits Joe's account by 50 dollars and adds 50 dollars to Ann's account. Once Ann verifies that her account is credited, she sends Joe the painting. Though no real money exchanges hands, a credit and debit entry is passed in the bank's centralized database or ledger. Only the bank has access to this ledger. It acts as a trusted third party for which the bank may collect a transaction fee. In our example, the bank has taken a further 1 dollar from Joe's account as a transaction fee.

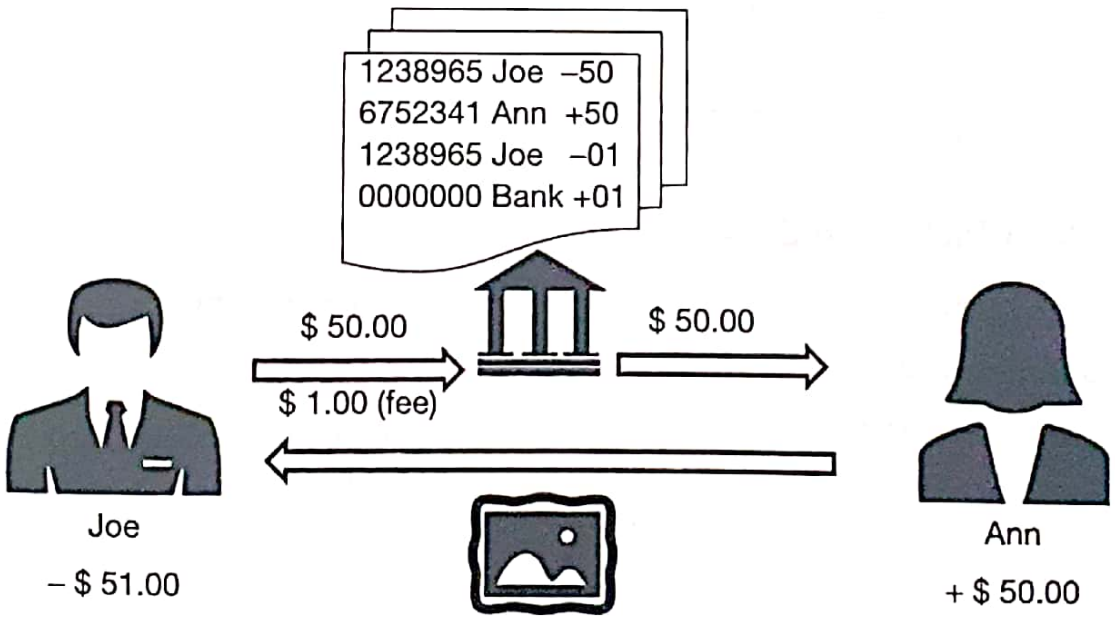


Figure 1.2: Traditional online transaction

However, this is a straightforward example. In a real-life scenario, we are talking of multiple banks or exchanges for cross-border transactions involving a large amount of money. With the advent of commerce on the internet, financial institutions have become indispensable to verify ownership, transaction maintenance, and any dispute mediation. For the services, the financial institutions need to charge fees, which increases the overall cost to the consumer.

Scenario 3: the Blockchain transaction

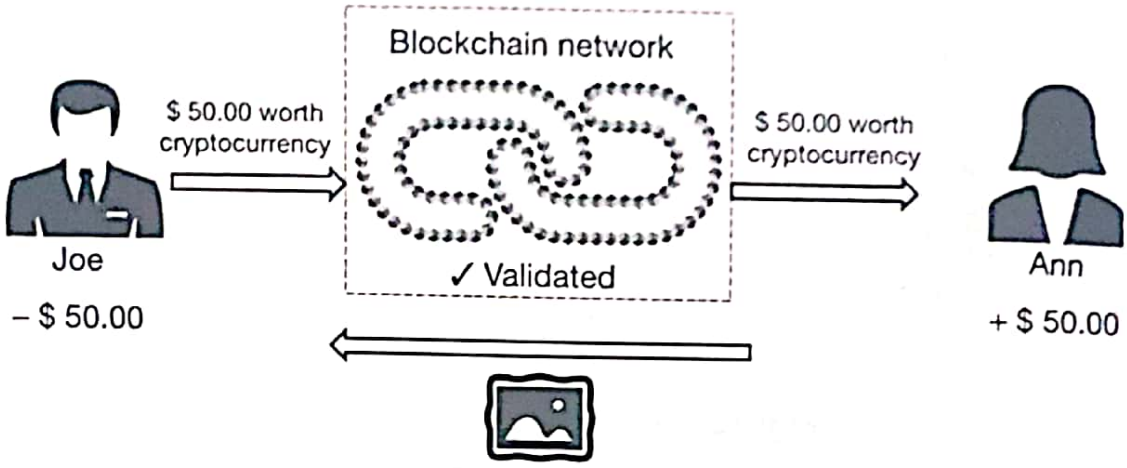


Figure 1.3: Blockchain transaction

In the blockchain scenario, Joe and Ann are both members of a blockchain network (refer Fig. 1.3). In the blockchain, transactions are done using cryptocurrency like Bitcoin. Joe initiates the transaction with 50-dollar worth of bitcoin or related cryptocurrency say. Once it is validated within the blockchain network, Ann receives 50 dollars equivalent in crypto. The whole transaction is done without any intermediary or fees. There is, of course, the reward fees that go to the miner, but that is insignificant compared to the fees charged by banks. This inherent trust in the peer-to-peer network is what makes blockchain the disruptive technology of today. As mentioned in the earlier section, the blockchain data is not just limited to money but can be used for anything like a proof of property, a loan certificate, etc. With blockchain, we are looking at the potential elimination of trusted third parties like banks, lawyers, brokers, and others.

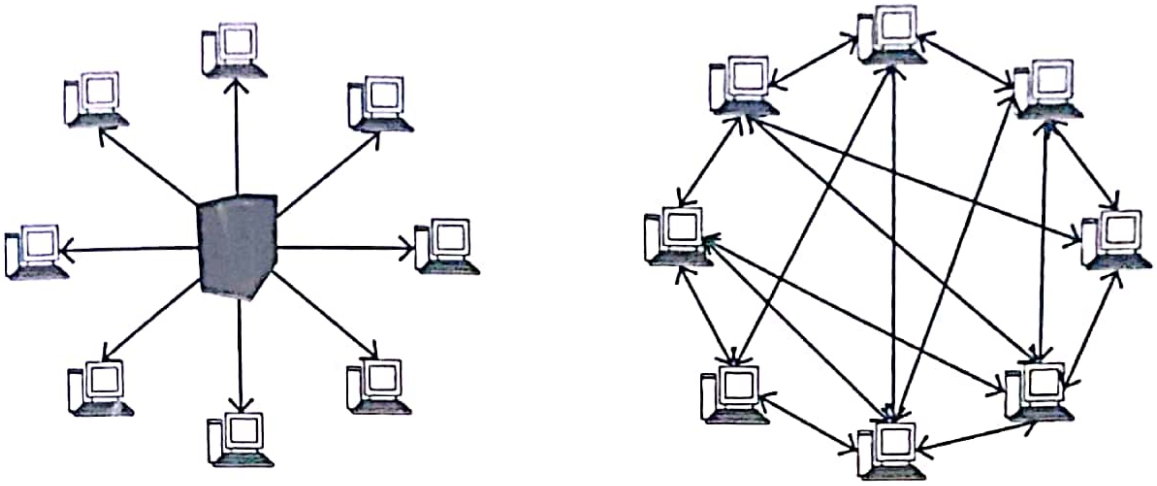
1.3.2 Key Blockchain Concepts

Three vital technological concepts are the backbone of blockchain transactions.

Peer-to-peer Network

The peer-to-peer (P2P) architecture is the cornerstone of the blockchain network that makes the deed of trust from a mediator or third parties like banks, lawyers, etc. redundant. The P2P network (refer Fig. 1.4 a) was first introduced in 1969 with Arpanet, a precursor to the Internet where every participating node (computer) could request and serve content.

The standard network model traditionally used is the client–server model (refer Fig. 1.4 b), where communication is typically to and from a central server. For example, in File Transfer Protocol (FTP) services, the client requests the transfer, and the server executes it.



(a) A **client-server network** where individual clients request services from centralized servers

(b) A **peer-to-peer (P2P) network** where interconnected nodes or peers share resources amongst each other without any centralized administrative system

Figure 1.4

The P2P network, however, works on the principle of equal peer nodes acting as both clients and servers to the other nodes within the network. The P2P architecture was popularized in 1999 by the file-sharing system Napster designed for sharing digital music files in mp3 format within its music-sharing application network.

While in the traditional network, the information is stored in one central location, in the P2P network, multiple copies of the same data are stored in different locations/computer devices on the network. This prevents a single point of failure. Even if one node or server is inactive/lost/destroyed, multiple copies remain safe and secure elsewhere. Besides, if one piece of information is changed or is inaccurate, there are other exact copies with peers (majority) in existence, making the false record obsolete. Gnutella, BitTorrent, and IPFS (InterPlanetary File System) network and protocols use the P2P architecture.

Did you know?

Arpanet (Advanced Research Projects Agency Network) of the United States Department of Defense was the first packet-switching network using the TCP/IP protocol suite, which forms the technical foundation of the Internet. The Arpanet program aimed to work on time-sharing, to enable research institutions to use the CPU (Central Processing Unit) power of other institutions for doing research.

While P2P architecture is inherently distributed, in the real-world scenario it is not necessarily fully decentralized. There is a central authority (system of servers and administrators) to guide the network activity as a single data query could flood a network to reach as many peers as possible. This results in high CPU and memory usage. Even then, there is no guarantee that the required piece of information will be found, especially if the information sits with only a few nodes in the network.

The peer-to-peer architecture of blockchain technology overcomes this issue as every full node maintains a complete updated copy of blockchain ledger (data). This allows the nodes to collectively participate in verifying the actual state of the distributed ledger, thus assuring decentralization and security that is wanting in the traditional client-server models. The distribution of the blockchain over large numbers of nodes renders it resistant to cyber-attacks like Denial-of-Service (DoS) attacks. Also, the majority of nodes must establish consensus for a data block to be added to a blockchain. Thus it is almost impossible for an attacker to alter the data, especially in big networks like Bitcoin, Litecoin, Ethereum, etc. Smaller blockchains are more prone to attacks because a single peer node or group of peers with common interests could eventually gain control over a majority of nodes. This is referred to as a 51 percent attack.

Thus an extensive distributed peer-to-peer network, paired with a majority consensus requirement, gives blockchains a relatively high degree of resistance to malicious activity.

Public Key Cryptography

Also called asymmetric cryptography, it was discovered in 1976 by two Stanford mathematicians, Whitfield Diffie and Martin Hellman. Used in PKI (Public Key Infrastructure), two keys, called the private key and the public key, are generated, which can be used to encrypt/decrypt a message. They need to be used in combination. The public key cannot decrypt the message encrypted by the public key, nor can the private key decrypt message encrypted by the private key. This enables two essential cryptographic capabilities, i.e., confidentiality and integrity.

More details on cryptography and its utilization in Blockchain are detailed in Chapter 09: Security in Blockchain.

Did you know?

Though Diffie and Hellman discovered the concept of asymmetric cryptography first, it was the RSA algorithm published in 1978 by mathematicians Ron Rivest, Adi Shamir, and Leonard Adleman that monetized the concept more effectively. This ultimately resulted in RSA Security LLC, now part of the Dell Technologies family of brands.

Distributed Consensus

The distributed consensus protocols are fundamental in avoiding double-spending and other internet attacks. In 1992, researchers Cynthia Dwork and Moni Naor presented an

approach to combat junk emails through a protocol known as the pricing function. Users would be able to assess their email service once they can compute a function or puzzle by engaging their processing power. In 1997, cryptographer Adam Back proposed a similar function called Hashcash. Hashcash utilized the cryptographic hash function SHA-1 (Secure Hash Algorithm 1) that would help email recipients to identify spam. Hashcash served as the inspiration behind the PoW consensus mechanism used within the Bitcoin distributed ledger. Once a transaction is verified, it is broadcasted over the network for a unified agreement or consensus.

More on Consensus Protocols are detailed in Chapter 2.

None of the above three technologies are new. But bring all the three together, and we have the birth of a cutting-edge technology called Blockchain.

1.3.3 How Blockchain Technology Works

One of the features in the blockchain is digital trust. In the digital world, trust relates to two questions: "Are you whom you say you are?" and "Do you have the right to do what you want to do?" This boils down to proving identity (authentication) and proving permissions (authorization).

Authentication is addressed with cryptography. Blockchain utilizes public-key or asymmetric cryptography that involves a public key and a private key (refer Fig. 1.5). When a private key is created, its public key pair is also created using a complex algorithmic process. Both the public key and private keys are generated and stored in a place referred to in the Blockchain world as "wallet." The Wallet is a software program that not only stores your private and public keys but also facilitates the sending and receiving of cryptocurrency through the blockchain, while also monitoring your balance. More on the wallet is explained in Chapter 3: Cryptocurrency.

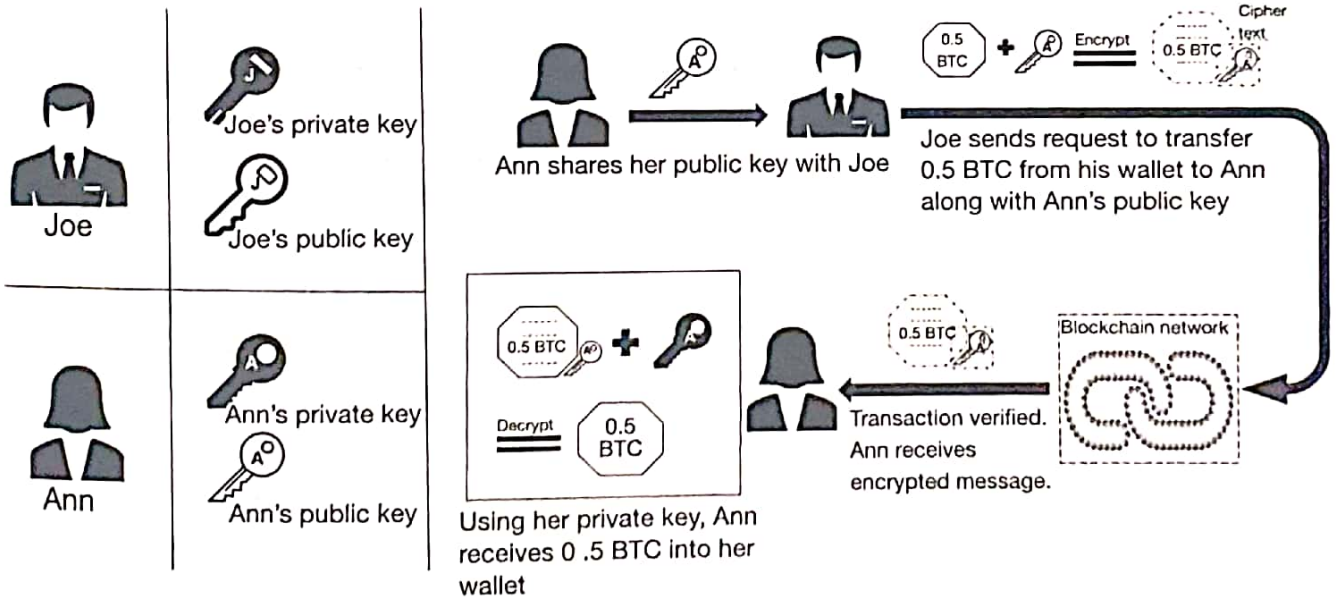


Figure 1.5: Public-key cryptography

While the private key must be maintained confidential, the public key may be distributed to anyone. You can relate the public key to your bank account number that you would need to share to receive money while your private key is similar to your bank account password or PIN that only you can access. So if anyone sends you a message with your public key, only you can open it with your private key provided no one else has access to your private key. Thus it goes without saying that the private key should not be shared with anyone.

The public key is shared across. Therefore, how can we guarantee the authenticity of the data and ensure that it will not be tampered with in transit? The answer lies in the digital signature. A digital signature provides validation and authentication in the same way signatures do but in digital form.

The digital signature algorithm generally comprises of three parts:

1) ***Generation of the private and public key:*** The keys are used to encrypt and decrypt the message in PKI.

   Let's say Joe wants to send some bitcoins, of say 0.5 BTC, to Ann (refer Fig. 1.5). Ann shares her public key with Joe. Joe takes 0.5 BTC from his wallet and, along with Ann's public key (encryption), sends the request. The transaction is routed through the blockchain network, where it is verified and sent to Ann. Ann can decrypt using her private key and receive 0.5 BTC into her wallet.

   Thus with public-key cryptography, blockchain can ensure the **security** of the transactions. Also, the transactions are time-stamped, thus making each transaction **unique**.

2) ***Signing algorithm:*** A digital signature produced through public-key cryptography safeguards the integrity of the data that is sent. This is done by combining the private key with the data that they wish to certify, through a mathematical algorithm, thus creating a digital signature (refer Fig. 1.6).

   Based on our earlier example, Joe wants to ensure that the contents of the message (in our case, the transaction) are not altered in any way, shape, or form during transit. He first shares his public key with Ann. Then Joe creates a digital signature by
   a) generating a hash of the message with a public hashing algorithm and then
   b) encrypting the hash using his private key.

   Joe appends the signature to the message and sends it to Ann.

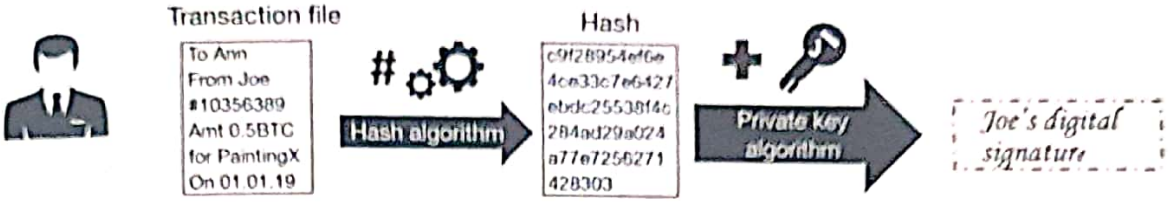
   Note: Joe can encrypt the digitally signed message again with Ann's public key (refer Fig. 1.6) for security.

3) ***Verification algorithm:*** In this process (refer Fig. 1.7), the receiver can verify the authenticity and integrity of the message received. Ann wants to be assured that the message is from Joe and it has not been tampered with in transit. This is done through a 3-step process:

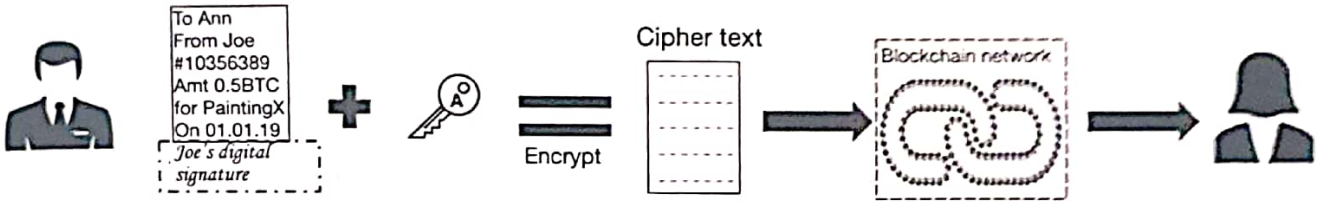
   Step 1: Ann decrypts the digital signature using Joe's public key to get the hash.

   Note: Only Joe's public key can decrypt the hashed message that was encrypted with Joes' private key.

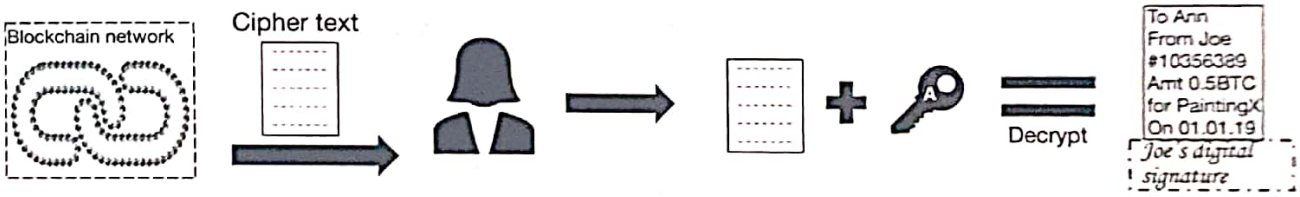
1. Joe and Ann share their public key with each other.



2. Joe generates a hash of the transaction and using his private key encrypts the hash thus creating his digital signature.



3. Joe encrypts the digitally signed transaction file with Ann's public key and sends it to Ann via the blockchain network.



4. Ann receives the encrypted transaction file. She decrypts the file using her private key to access Joe's digitally signed document

Figure 1.6: Digital signature

Step 2: Ann runs the hash function on the message she received to generate the hash
Step 3: Ann compares the two hashes. If both are the same, Ann is assured that the message is from Joe (as Joe's private key decrypted the message).

Although the verification process seems like much work, it is generally done by a software application, and the process is typically invisible to the end-user.

Digital signatures are what gives the data recorded on a blockchain its **immutability**. Thus encryption and digital signatures are the de facto ways blockchain technology guarantees the security, authentication, integrity, and non-repudiation requirements of the data or transaction.

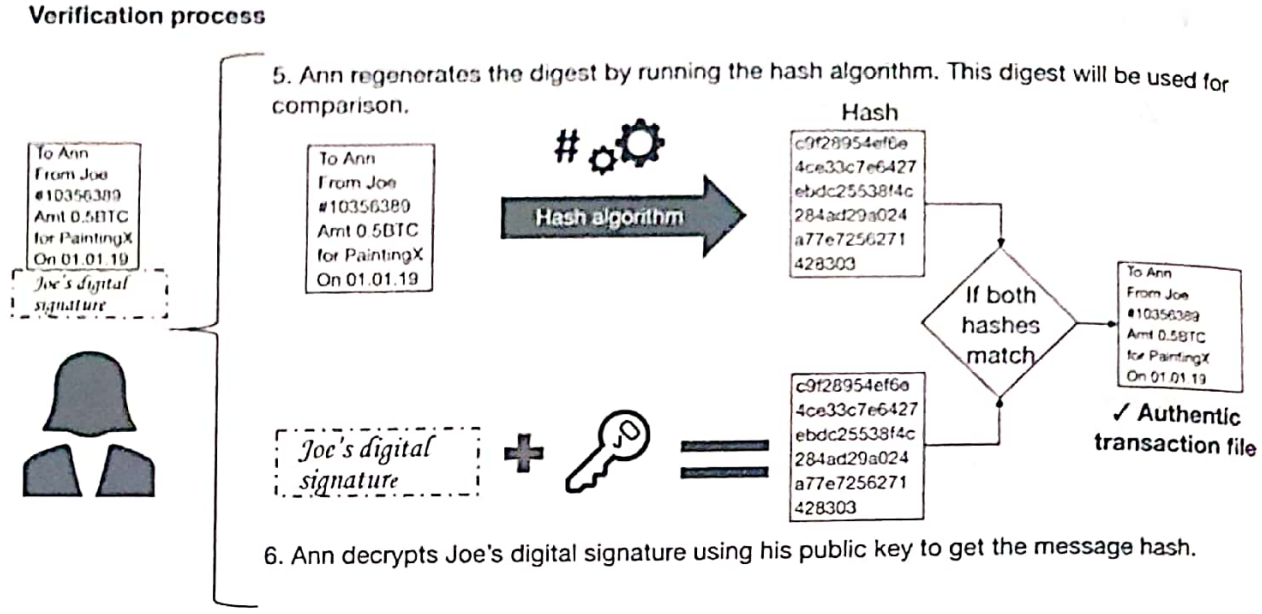


Figure 1.7: Verification

With digital signatures, we have addressed the trust question on "authentication," i.e., "Are you who you say you are?" However, what about the trust question on "authorization," i.e., "Do you have the right to do what you want to do?" The authorization question is addressed by the distributed consensus on a peer-to-peer (P2P) network of blockchain. Unlike the centralized system of today where there is a central body that defines the rules and has full control over the network data and users, in blockchain all the nodes or devices (computers, mobiles, etc.) in the network share the responsibility of ensuring the right rules or blockchain protocols are applied. There is no hierarchy within the network. All nodes are peers, each having an identical copy of the database or ledger. Hence the Blockchain network is called a peer-to-peer network since the tasks of maintaining the network are continuously shared from peer to peer. This spreads out control and responsibility among lots of different peers, thus ensuring no single point of failure and reduces the risk of corruption.

Blockchain leverages Distributed Ledger Technology to support immutable transactions on a P2P network without any centralized coordinating entity. Authentication and Authorization in blockchain systems are maintained using cryptographic signatures and consensus-based validation procedures. More details on Distributed Ledger Technology (DLT) and Consensus Mechanisms are explained in Chapter 2.

1.4 Components of Blockchain

So far, we learned about the origin of Blockchain, its inherent concepts and the technologies that make blockchain transaction secure, immutable, and indisputable. But from where does blockchain get its name, and what makes it unique? To understand the block in Blockchain, we need first to understand some of the concepts, terms, and components used in Blockchain technology.

1.4.1 Node

A node is an electronic device (computers, mobile devices, servers, etc.) that is connected to the internet. In blockchain parlance, any computer or hardware device that is connected to the blockchain network is a node. All the nodes in the network have a copy of the blockchain ledger and are interconnected. So theoretically, we can say that the Blockchain exists on nodes whose primary purpose is to preserve the integrity of the blockchain. The node supports the network by maintaining a copy of the blockchain. A node can be:

a) A Full Node

The node maintains a full copy of the transaction history of the blockchain. Computers run full nodes to help synch the blockchain. They also help the network by processing and accepting transactions/blocks, validating those transactions/blocks, and then broadcasting them to the network. This is called mining or forging, explained later in this section.

b) A Partial or Lightweight or Light Node

Nodes maintain only a partial copy of the ledger as they could be early users or those who do not have sufficient disk space for the full blockchain. Light nodes download only the block headers to validate the authenticity of transactions using a method called SPV or Simplified Payment Verification. They rely on the full nodes for the latest headers, account balance, and any transaction that affects their wallet.

However, a blockchain network needs to have more full nodes operating within the network to make it a truly trustless and decentralized system.

As a principle, blockchain is open to all. Anyone can join the network, i.e., be a node and participate in the blockchain network to validate and create blocks. This is called a **public permissionless blockchain**, e.g., Bitcoin and Ethereum. However, based on business needs, other types of blockchain are evolving – such as the private permissioned blockchain and consortium blockchain, where the blockchain is not open to everyone. Nodes need to fulfill pre-requisite criteria to join and/or to participate in the blockchain. Examples include Ripple, Hyperledger Fabric, and Monero. Different types of blockchain will be explored in Chapter 2.

1.4.2 Ledger

A ledger, in blockchain technology, refers to a digital database of information that is immutable. Blockchain is commonly referred to as a public distributed decentralized ledger. Let us see why.

a) Ledger Is Public

Anyone in the blockchain has access to the ledger and can read or verify the transactions therein.

b) Ledger Is Distributed

All the nodes in the blockchain network have a copy of the blockchain ledger. The traditional database works in a client–server environment, while the blockchain works on the principle of replication in every node.

c) Ledger Is Decentralized

Blockchain protocols are built such that no one node or group of nodes has excessive control over the ledger. There is no central control; hence it is decentralized with no single point of failure. So, while the traditional database works on central principle integrity (only the central body can validate the record), the blockchain works on the principle that anybody can validate the records.

Also, the traditional database works on the CURD (Create, Read, Update, Delete) principle. In contrast, the blockchain works in the principle of Append-only, i.e., blocks are only added to the existing blockchain (Section 1.5).

1.4.3 Wallet

A Wallet in the blockchain world is a digital wallet that allows users to manage cryptocurrency like bitcoin, litecoin, ether, etc. With a blockchain wallet, one can receive and send cryptocurrency. The term "wallet" is a misnomer, as real money is not stored. When Person A sends cryptocurrency coins to Person B's wallet, Person A is, in effect, signing off ownership of the coins to Person B. However, Person B can spend the coins only if the private key stored in Person B's wallet matches the public address the cryptocurrency is assigned to. If the keys match, the balance in Person B's wallet increases while that in Person A's wallet decreases accordingly. It should be noted that there are no real coins at play here. The said transaction is a new record added on the blockchain along with a change in the balance in the cryptocurrency wallet.

The wallet provides all the features that are needed for a safe, easy and secure transfer of funds between two parties, namely,

a) Privacy Is Maintained

Whenever a user creates a wallet, the public and private key associated with the wallet is also generated. It can be compared to how your email account works. The public key is

like email id, and the private key is your email id password. Just like you share your email id to receive an email, you share your public key to receive funds (Section 1.3.3). However, your identity and personal details are kept private.

b) Transactions Are Secure

The private key is used to send funds as well as to open encrypted messages. This keeps the transactions secure.

c) Ease of Usage

Wallets can be installed and accessed from the web, desktop, or any mobile device. Transfer of funds is relatively instantaneous, without any geographical constraints or intermediaries like banks.

d) Currency Conversion

Wallets help you to transact across various types of cryptocurrencies like BTC, ETH, XMR, LTC, and others, without worrying about the currency conversion.

Did you know?

According to Statista, one of the world's largest consumer and market data providers, the number of blockchain wallets has reached nearly 35 million users at the end of March 2019 since its inception in 2009 with the bitcoin wallet.

There are around 120 wallets that are used for cryptocurrency transactions today. Blockchain.info, Coinbase, Mycelium and Electrum are some examples of blockchain wallets.

1.4.4 Nonce

A nonce is a number generated randomly that can be used just once in the cryptographic communication. Adding a nonce to a transaction's identifier makes it additionally unique, thus reducing the chance of duplicate transactions. Nonce is the key to creating a block in a blockchain database.

1.4.5 Hash

A hash function can take data of any size, perform an operation on it, and return a "hash" that is a data of a fixed size. Whether it is a single sentence or the Oxford Dictionary, the resulting hash will always be of the same size.

Critical characteristics of hashing are:

a) It creates an almost unique identifier. In the blockchain, hashes are used as identifiers for blocks, transactions and addresses. In the Bitcoin, blockchain hashes are 256 bits or 64 characters. The hashing algorithm used in the blockchain is called SHA-256. SHA stands for Secure Hash Algorithm generating a 256-bit hash.

Input (A Text String)	Hash Result (SHA-256)
OK	565339bc4d33d72817b583024112eb7f5cdf3e5eef0252d6ec1b9c9a94e12bb3
The world is a balloon!	7e4a05ad886f9dbf1f0a167c2a5d5dd5e41b853ad5e0c331e065c2fb2c85b3da
The world is a balloon	6978378fe2785a3159b6a5e5284abc7e4140ad829a949799b7419fd72ac74813
the world is a balloon	84261d4cc1eb9e0571fb5c247f434104e10b8268846c33c2bb63322d8309e8c9

- No matter the size of the input string, the output is always 64 characters
- A completely different hash result though the change in text string "The world is a balloon!" is minute, i.e., removal of "!" or replacing "The" with "the". Provides security from tampering during transmission.

Figure 1.8: Hash output example

b) It is one-directional and hence a right candidate for encryption (Section 1.3.3). A hash function can take a string or input of any length to create a fixed-length data output. However, we cannot take the data output and recreate the string/input.

c) A very minute change gives a different hash making it one of the most secure functions (refer Fig. 1.8).

d) It keeps the database small. As mentioned earlier, the data output is always a fixed size. Hence, storing the hash of a file instead of the original file considerably reduces the size of the database. For example, you can hash the photo of the painting, including details of the painter, when and where it was painted, etc. and create a hash output. Only the hash needs to be stored in the database since the hash is mathematically associated with the original painting and data.

A hash with 64 alphanumeric characters creates an astronomical number of combinations, and there is little chance of duplication. More on hashing and SHA-256 is explored in Chapter 4.

1.4.6 Mining

Mining is the mechanism whereby nodes called "miners" in the Bitcoin world or "forgers" in the Ethereum world validate new transactions and add them to the blockchain ledger. Miners/forgers compete to solve a complex mathematical problem based on a cryptographic hash algorithm referred to earlier, basically the nonce and hashing. Mining comprises hashing a block and then introducing a nonce to the hashing function and running the hash all over again.

However, this is where the complexity occurs: The resulting hash value should be less than the "target value." The target value is a number that a hashed block header must be less than, for a new block to be awarded. If the hash is not less than or equal to the target value, the miner has to increment the nonce and rerun the hash (refer Fig. 1.9). This process is run multiple times until the required hash is reached. Once the solution is found, the new block is added to the network and propagated.

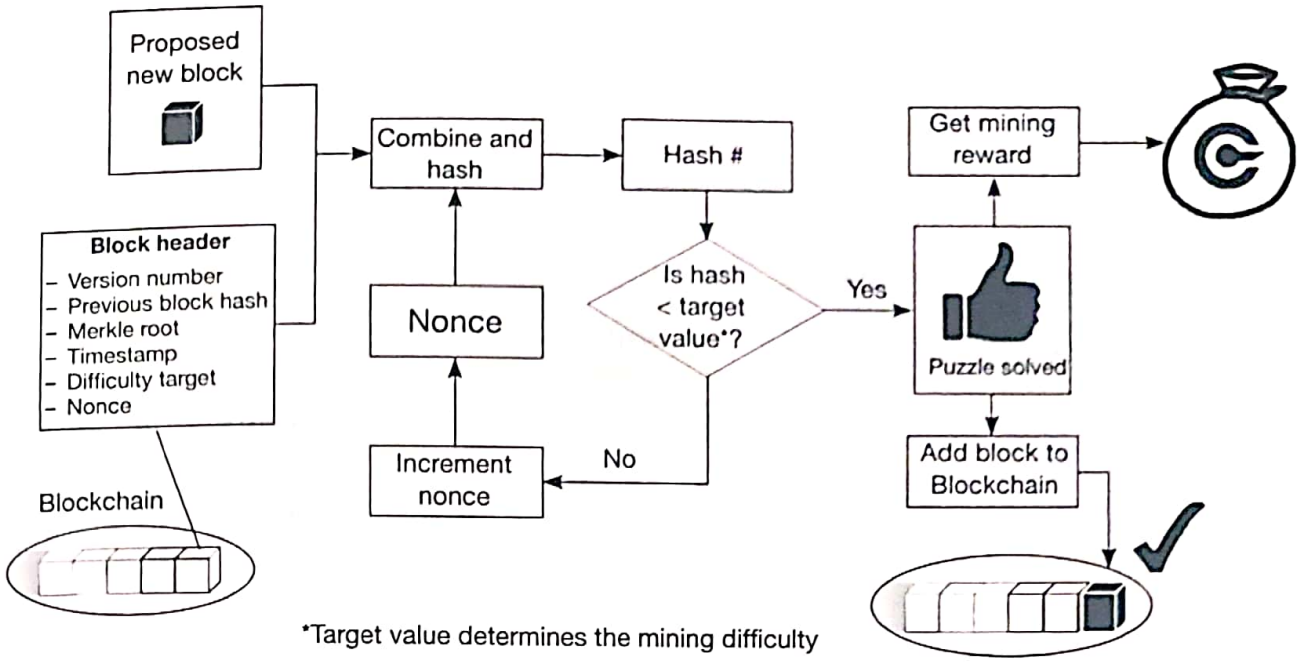


Figure 1.9: Mining process

Miner nodes compete to solve a complex mathematical problem using massive computing power, energy, and time. The first miner to create the winning hash will receive rewards in the form of transaction fees or new bitcoins. This process of computing the hash is called proof-of-work or consensus mechanism and provides **integrity** to the blockchain. Adding blocks to a blockchain without the consensus mechanism makes it highly vulnerable to either accidental faults or malicious attacks from hackers.

More details on consensus mechanism and mining can be found in the forthcoming chapters.

1.4.7 Consensus Protocol

Consensus protocols are a set of rules whereby nodes in a network can achieve agreement on the data value or state of the network such that it benefits the network as a whole and does not focus on individual interests. In the decentralized world of Blockchain technology, all the participating nodes must agree on a single source of truth, for example, whether Joe has enough money in his wallet or he is double-spending. Consensus protocols are used in blockchain to ensure that all transactions are validated before being added to the blockchain, i.e., there should be a 'consensus' or agreement between the nodes on the network on the state of a blockchain. This allows for three critical functions of the blockchain:

a) Consensus protocols
b) Spread control between nodes, thus preventing any single entity from taking control or disrupting the blockchain system. Consensus rules aim to guarantee that a single chain is used and followed.

c) They are designed to be costly and resource-heavy in terms of computing power, energy, and time, in an effort to keep the network honest.

Proof-of-Work (PoW) algorithm is used in Bitcoin protocol, while Proof-of-Stake (PoS) algorithm is in the Ethereum Casper Protocol. Chapter 2 gives more details on the different types of consensus algorithms used in Blockchain.

1.5 Block in a Blockchain

1.5.1 Meaning of the Block

The block is a record that contains the transaction data details. It comprises of the following details:

1) Hash of the block – Alphanumeric number to identify the block
2) Hash of the previous block
3) Timestamp
4) Nonce – the random number used to vary the value of the hash
5) Merkle root – hash of all the hashes of all the transactions in the block
6) Transaction data. This contains details of several transactions

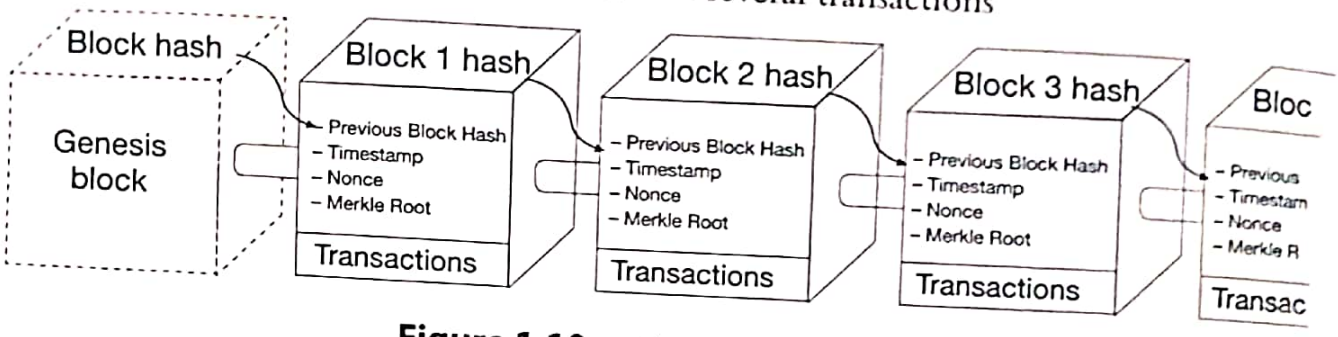


Figure 1.10: Block representation

The genesis block is the first block. It is the only block with no data hash of the previous block because no block precedes it. The genesis block contains transactions that are combined and validated to produce a unique hash.

The genesis block hash, along with all the new transactions, are processed and used as input to create a new hash that is used in the next block, i.e., say Block 1 (refer Fig. 1.10). Block 2 hash is created with a hash of Block 1 and another set of new transactions. This goes on with each block linking back to its previous block via its hash, thus forming a chain leading back to the genesis block. Hence the name, blockchain.

This continuous linkage makes it impossible for any malicious actor to alter the information or to insert a block between two existing blocks. To do so, all connected blocks would need to be altered as well. As a result, each block strengthens the previous block, including the security of the entire blockchain, because a bigger chain means more blocks would need to be changed if one wants to tamper with any information.

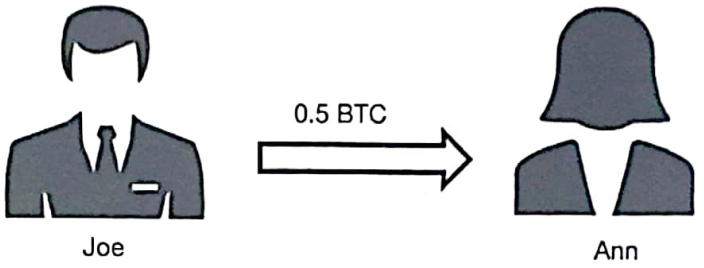
1.5.2 Blockchain Transaction in a Nutshell

Let us look at all the high-level steps involved in a blockchain transaction.

Remember:

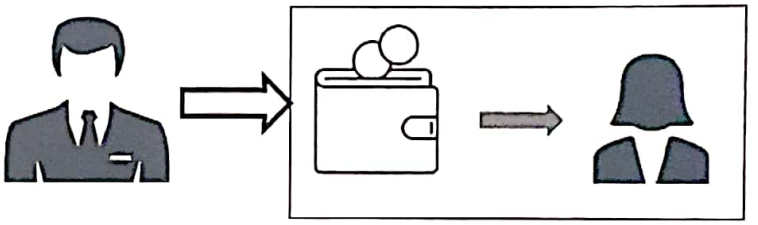
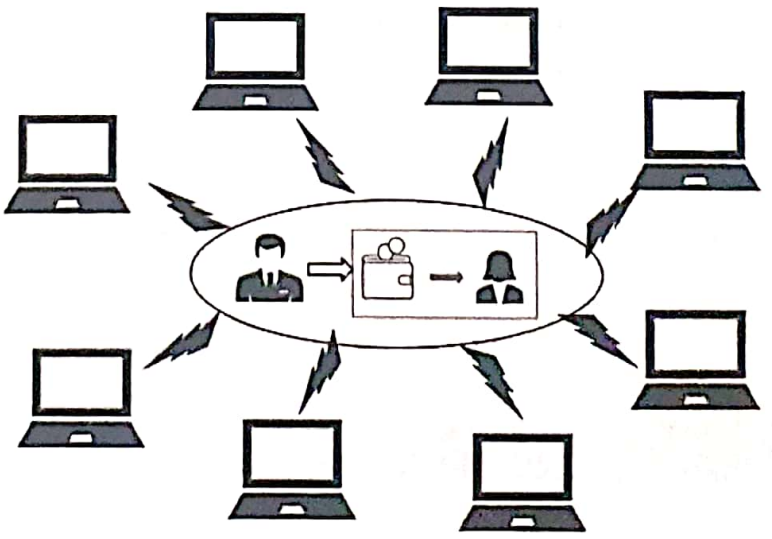
✓ Blockchain is a digital ledger or digital database
✓ The blockchain ledger is distributed to all the nodes in the network, i.e., all the nodes have the same copy of the ledger
✓ Blockchain is decentralized, i.e., there is no central control. All the nodes in the network can participate in the processing and creation of a block
✓ A unique cryptographic key secures every record on the blockchain

Let us take our example of Joe's plan to send 0.5 BTC to Ann through the blockchain.



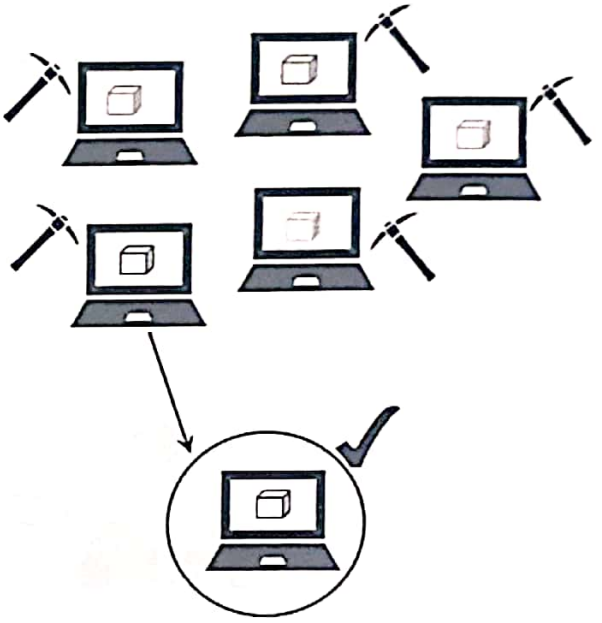
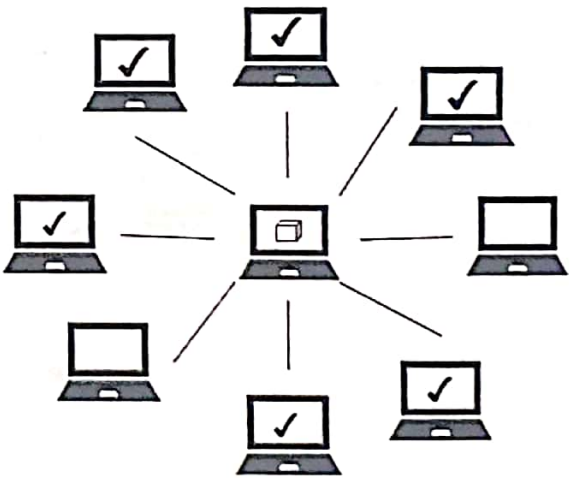
The following table gives a step-by-step representation of the transaction between Joe and Ann in the blockchain.

Table 1.2 Step-by-step representation of a blockchain transaction

Step 1: Joe requests the proposed transaction Joe sends 0.5 BTC from his Wallet app.	
Step 2: The proposed transaction is broadcast to the network	

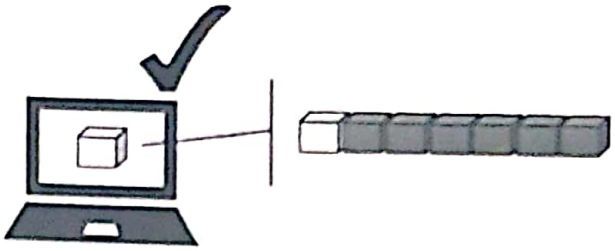
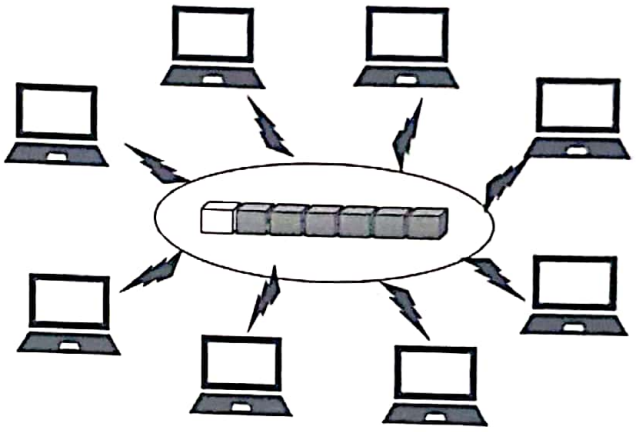
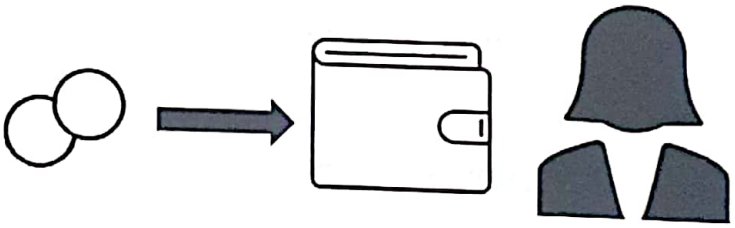
(Continued)

Table 1.2 (*Continued*)

Step 3: Miners verify the transaction and bundle it into a block along with other transactions. – The miner will validate the authenticity of the transaction, i.e., the status of Joe, his balance, etc. **Note:** Miners validate all the transactions they wish to include in the block they plan to mine.	
Step 4: Miners compete to solve the complex mathematical puzzle. – The puzzle requires much computational power to solve. – This protects the blockchain against hackers as it would be difficult and expensive to attack the network.	
Step 5: The nodes verify the miner's work. – The miner who finds the correct hash broadcasts the block to the network – Majority of the nodes/miners need to approve/verify the block for it to be accepted into the blockchain – Once approved, the winning miner can collect his reward.	

(*Continued*)

Table 1.2 *(Continued)*

Step 6: Block is added to the blockchain. – Once the block is verified, the winning miner adds his block to the existing blockchain. **Note**: Joe's transaction is added to the blockchain along with the other transactions	
Step 7: The updated copy of the blockchain is circulated throughout the network.	
Step 8: Transaction completion Ann receives 0.5 BTC in her wallet. The transaction is complete.	

So in a nutshell, the process of blockchain transaction consists of:

- A node in the blockchain (P2P network) requests a transaction via a wallet.
- The transaction is broadcasted to all the nodes in the network.
- The transaction is validated/verified by the network using consensus algorithms, i.e., preset rules set by the specific blockchain.
- The transaction is either accepted or rejected. If accepted, the transaction is added in a chronological order along with other transactions to create a new block of data that is sealed (hash).
- The transaction is now part of the blockchain and is permanent and immutable.

1.5.3 Double-spending

With the ever-growing popularity of blockchain, more and more people are moving towards transacting in digital currency. This brings about the double-spend problem, a flaw that is unique to digital currencies. Double-spending, as the name suggests, is spending the money more than once. Just as one can copy a digital file and send it to several people, it is possible to duplicate crypto-coin or token and reuse it. If this occurs in the blockchain network, it could not only breakdown the concept of trusted distributed ledger but also lead to inflation with fraudulent, duplicate currencies in the network. Remember, there is no trusted third-party to validate that the transaction is not a double-spend.

The double-spend problem is circumvented in blockchain through its consensus mechanism and the basic chronological structure of how the blocks are chained together.

A transaction is verified and added to a block via the consensus mechanism after a considerable amount of computational power and resources are spent. Going back and attempting to double-spend that transaction would require the same if not more computational power, especially with more blocks added to the chain in the interim; it is practically impossible to modify all the blocks. No one will expend enormous amount of resources if the payback is not worth the effort.

Also, the first transaction would be time-stamped and cryptographically linked to previous blocks and broadcasted to all nodes in the network. When the second (fraudulent) transaction is proposed, it will fail at the verification process and be rejected.

Once a transaction is confirmed, it is nearly impossible to double-spend it. The more confirmed blocks in the chain, the harder it is to double-spend the crypto.

However, it is theoretically possible to double-spend a cryptocurrency. Though rare, this can be done by the 51% attack (where there is control of more than half the network's hash rate), Finney attack, or Race attack. More on blockchain attacks are explained in Chapter 11.

1.6 The Technology and the Future

1.6.1 Blockchain Layers

A simple structure of the blockchain ecosystem is represented in Fig. 1.11.
It typically consists of:

a) The Presentation Layer

This layer is a door to users that gives access to the whole network and blockchain applications. The UI (User Interface) and UX (User Experience) of the blockchain app come into play here. In today's competitive market, mobility and ease of usage are paramount to customer satisfaction. It is no different for blockchain where UI and UX design could make or break a blockchain adoption. A good UX design will enhance customer satisfaction and loyalty by improving the product usability and interaction between the user and the rest of the blockchain ecosystem or company. This could relate

to faster speeds, relevant information, etc. UI design produces blockchain visuals or graphical presentations. It enhances the user's experience with aesthetics, visual hints, and icons leading to an intuitive interface.

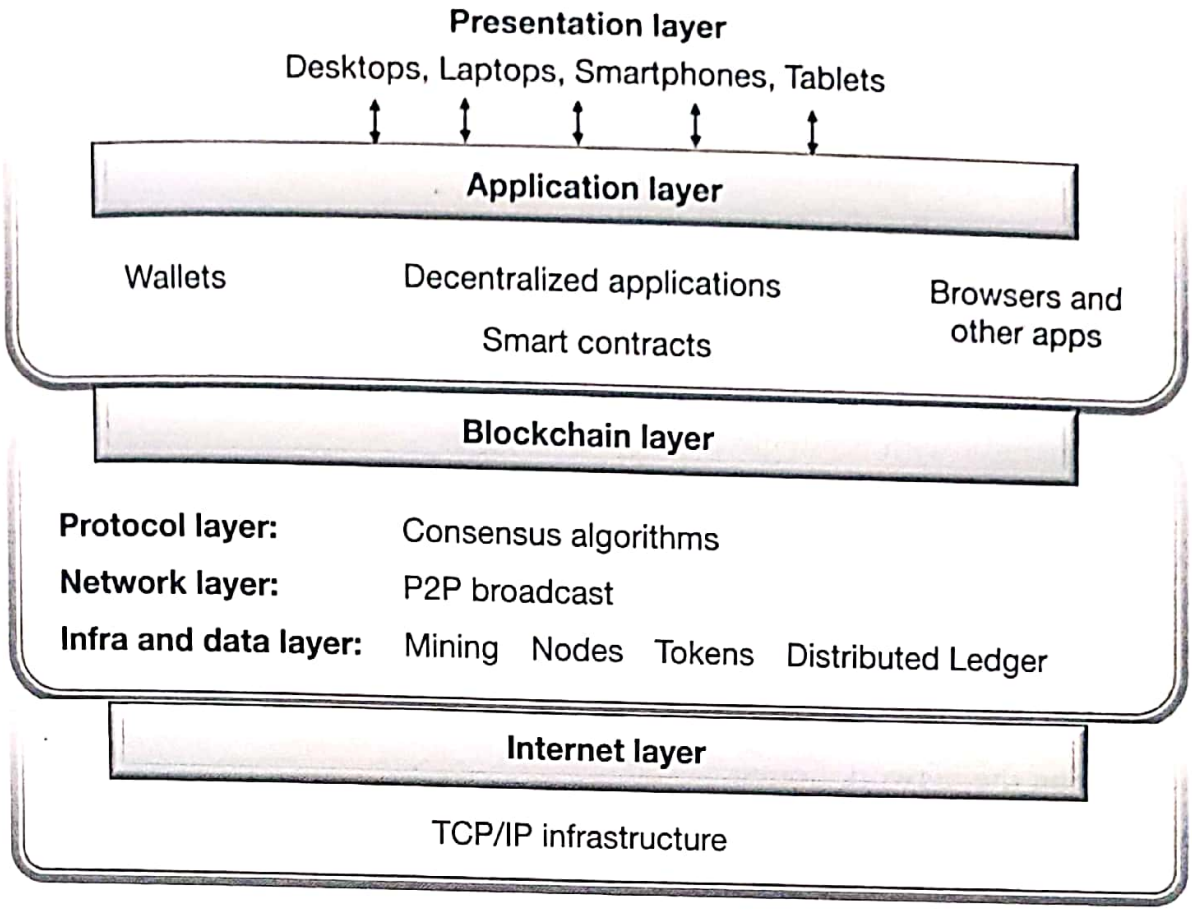


Figure 1.11: Blockchain ecosystem

b) The Application Layer

This is the layer than combines the business logic with user interactions. It consists of the Decentralized Application, better known as DApps running on a P2P network. It is the DApps that sets the communication between the Presentation and Blockchain layers. DApps is similar to a web application except that while APIs are used to connect a website to a database, DApps connects to the Blockchain via Smart Contracts. The Smart Contract is a program containing a set of rules and criteria that automatically execute if/when the pre-defined conditions are met. More on Smart Contracts and DApps are explained in other chapters within this book.

c) The Blockchain Layer

This is where the core of the blockchain subsists. It consists of the consensus algorithms (PoW, PoS, pBFT, etc.), the medium, and interface for the P2P network that decide how data is packetized and transmitted between peers. It controls the mining layer, protocols that decide the consensus methods and participation, nodes that execute protocols, and the distributed ledger.

d) The Internet Layer

Blockchain works over the internet. This layer ties all the networks together, i.e., t computers, IoT devices, smartphones, etc.

1.6.2 Pros and Cons of Blockchain

We have seen the massive potential of blockchain technology in creating decentralized permissionless, secure, and transparent applications. Let us look at some of the significant blockchain characteristics that make it unique and weigh the pros and cons to get a better insight into how the technology works.

a) Decentralized and Distributed

Blockchain technology works on the principle of ledger data distributed to all nodes that are non-hierarchical with no single central control.

Pros

- Removes any single point of failure by replicating the ledger at every node in the network.
- Better communication between nodes fosters transparency and faster consensus and synching of data.
- It allows for more engagement as everyone is involved in the decision-making process and keeping the network honest.

Cons

- In some cases, the traditional database may be more suited and do the work a lot faster and cheaper
- Specific and trusted third parties exist in some domains that may guarantee more efficient and specialized services using other technologies
- If a time-tested and fully functional database and the operational network are already in place, the benefits of replacing or introducing blockchain may not produce the required return on investment.
- Stronger players (nodes with higher computing power or with pooling) can take control of the network, impacting decentralization.

b) Trustlessness

In the blockchain, cryptography completely replaces the need for third parties to ensure trust. Also, the complex consensus protocols that are run within the blockchain network to unanimously and securely agree on what should be added and should not be added to the ledger secures it further, thus ensuring its integrity at all times.

Pros

- Allows for multiple entities or key players who do not trust each other (i.e., unknown to each other or across borders) to transact directly with one another.
- Ensures valid and accurate data.

– Disintermediation (removal of the middleman) reduces the overall cost of transacting.

Cons

– The integrity of data is obtained at the expense of time. Every node needs to run the blockchain to verify transactions and maintain consensus. Currently, blockchain can, on an average, process only 5 transactions/sec.
– Significant computing power is expended by miners leading to substantial energy consumption and wastage. Hence, it is not suitable for organizations that require instant transaction results within milliseconds.
– Nodes may prioritize transactions with higher rewards.

c) Immutability

In blockchain technology, one cannot modify data or transactions once they are recorded in the blockchain database. It becomes a permanent record that is close-to-impossible to undo. Any change required can be addressed only by adding a new block of data to the existing chain of blocks in chronological order, ensuring that the database is complete and consistent.

Pros

– Contains a verifiable record of all transactions made that is auditable
– Consensus algorithms and block propagation mitigate the risk of double-spending, fraud, and manipulation of data.
– There is provenance, i.e., ability to track transaction or product movement across accounts.

Cons

– Not every node has the capacity to maintain and run a full copy of the blockchain. This can potentially affect consensus and immutability.
– In smaller blockchains, there is a risk of a 51% attack. If one or group of malicious nodes can get 51% of the mining hash rate, they can manipulate the transactions.
– Quantum computing can potentially break the cryptographic algorithm to reverse engineer public keys of blockchain networks to obtain the private keys.

With FinTech investing in blockchain technology and innovations, there are resolutions to many of the blockchain issues faced. It is the onus of the organization to evaluate the pros and cons of implementing blockchain technology solutions. We shall deal with this in more detail in Chapter 11.

1.6.3 Potential Applications in the Industry

The issues relating to blockchain technology may be significant, but its inherent benefits of immutability, openly shared ledger, security and non-dependence of intermediaries means that blockchain cannot be ignored. All agree that blockchain is way faster than the manual validation and audit process. Following are some of the potential applications that could cut across any industry and revolutionize the way we do business:

a) Digital Identity

In today's world, proof of identity is a must for verification; be it your security number, passport, birth certificate, driver's license, etc. Without a valid form of id, one cannot open a bank account, own property, get government services, or employment. Digital identities on the blockchain can reduce the burden of maintaining physical copies or ID cards and protect from identity theft, providing control over your own identity (to share only specific information that is relevant for the purpose). Blockchain technology can provide a breakthrough for helping people who do not have legal identities such as refugees and people who live way below the poverty line and do not have ids.

Elections are another area that could benefit from digital identity. There will be greater voting participation if the voting system has a verifiable audit trail with no fraudulent or illegitimate votes, while still keeping the votes confidential.

Adoption of digital identity under blockchain technology would substantially eliminate commonly occurring issues such as impersonation and fraud.

b) Payments and Settlement

Swiss bank UBS and UK-based Barclays are exploring blockchain solutions as a means to expedite back-office functions and settlement. Some in the banking industry say this could cut up to $20B in middleman costs. Banks and other financial sectors are exploring various cases of possible blockchain use in areas such as payments and settlement of currencies, asset registries, enforcement and clearing derivative contracts, regulatory reporting, KYC, AML registries, improving post-trade processing services, etc.

c) Proof of Ownership

Blockchain can be used to track any asset, be it jewelry, property deeds, vehicle, paintings, or any artefact, for proof of ownership. Fake and stolen goods are a significant issue impacting global commerce. Currently, proof of ownership is mostly paper-based that can be stolen or faked. With blockchain, all the properties of the asset can be digitized and stored in the blockchain. As the blockchain ledger is public and immutable, the ownership of the asset can be tracked to ensure its authenticity. This aids consumers and insurance companies in terms of time and money for evaluations, legal purchases, and arbitration.

d) Records Management

Industries that rely on the manual process of verification that is heavy on paper documentation and case-by-case checking can leverage blockchain technology. The education industry can benefit from blockchain solutions for verifying academic credentials, thereby reducing fraudulent claims of unearned educational qualifications. In healthcare, vast volumes of patient data can be stored securely and made accessible only to verified authorities, thus ensuring the privacy of patient data. The blockchain can securely store intellectual property and creative digital products like music, photos, software apps, etc.

e) Supply Chain Management

The undisputable nature of blockchain data makes it possible to track the journey of a product/product starting from its origin to its destination. There is hardly any industry without a supply chain, be it pharmaceuticals, food & beverages, automotive, construction, etc. When all parties see the same data and can verify shipment, receipt, and customs clearance, this cuts cost and streamlines the whole system. By using blockchain technology and removing paper-based trails and intermediaries, businesses can quickly pinpoint inefficiencies within their supply chains is nearly real-time. Contaminated products can be tracked and traced back to the source for containment and prevention. Some say that supply chain and logistics companies can benefit the most from adopting blockchain solutions.

f) Loyalty Programs and Rewards

The application of blockchain in Retail can step up the process of customer loyalty and reward programs. Blockchain technology-based token system that rewards customers and stores can be used to incentivize customers to return to a specific store or chain for their shopping. The very nature of blockchain will eliminate the fraud and waste commonly associated with paper and card-based loyalty programs with real-time updating of points balance and improving points management across franchised operations.

g) Decentralized IoT

Blockchain can support the Internet of Things (IoT) applications by supporting transaction processing devices. The distributed nature of the ledger can foster coordination among multiple devices. Smart Energy, Smart City, Smart Building and Smart Health can all leverage blockchain for cross-communication, data accuracies, permanence and privacy, all the while circumventing single points of failure.

h) Charity

Blockchain can address the issue of accountability and transparency in transactions related to charitable donations, thereby checking organizational inefficiency and financial misconduct that can prevent money from reaching those it was meant for. Blockchain provides the donors with the ability to precisely track their donations at all points until it reaches the right hands. It provides a permanent record of charitable financial transactions across the globe, thus driving stronger trust with donors.

Blockchain technology can be adapted to different business domains and industries according to standards and needs that each company requires. A more detailed look at current blockchain implementations and projects can be found in Chapter 10.

Summary

In this chapter, we have seen the history of Blockchain and how it got its name. Blockchain is a shared distributed digital ledger that maintains a permanent, transparent, immutable record of transactional data that is tamperproof and auditable. Data is organized into blocks that are cryptographically chained together in an "append-only" mode, thus forming a chain of blocks. Hence the name Blockchain.

Blockchain technology is what makes the blockchain transactions unique. Unlike traditional databases that work on client-server network architecture with centralized control, the blockchain is a type of digital ledger technology (DTL). The ledger exists on multiple devices called nodes that communicate with each other on the peer-to-peer (P2P) network. Transactions are verified, blocks validated, and created through cryptography and consensus protocols. Figure 1.12 sums up the characteristics of blockchain.

The central vision of the creator of blockchain-enabled bitcoin Satoshi Nakamoto was an electronic payment system that could remove the need for trusted third-parties and protect the digital currency from the double-spending problem. In the blockchain, asymmetrical cryptography and consensus algorithms completely replace third-parties as the governor of trust. Network nodes run complex consensus protocols to unanimously and securely agree on what should be added to the blockchain ledger. With transactional blocks being time-stamped and cryptographically linked to previous blocks and broadcasted to all nodes in the network, it is near- to-impossible to double-spend.

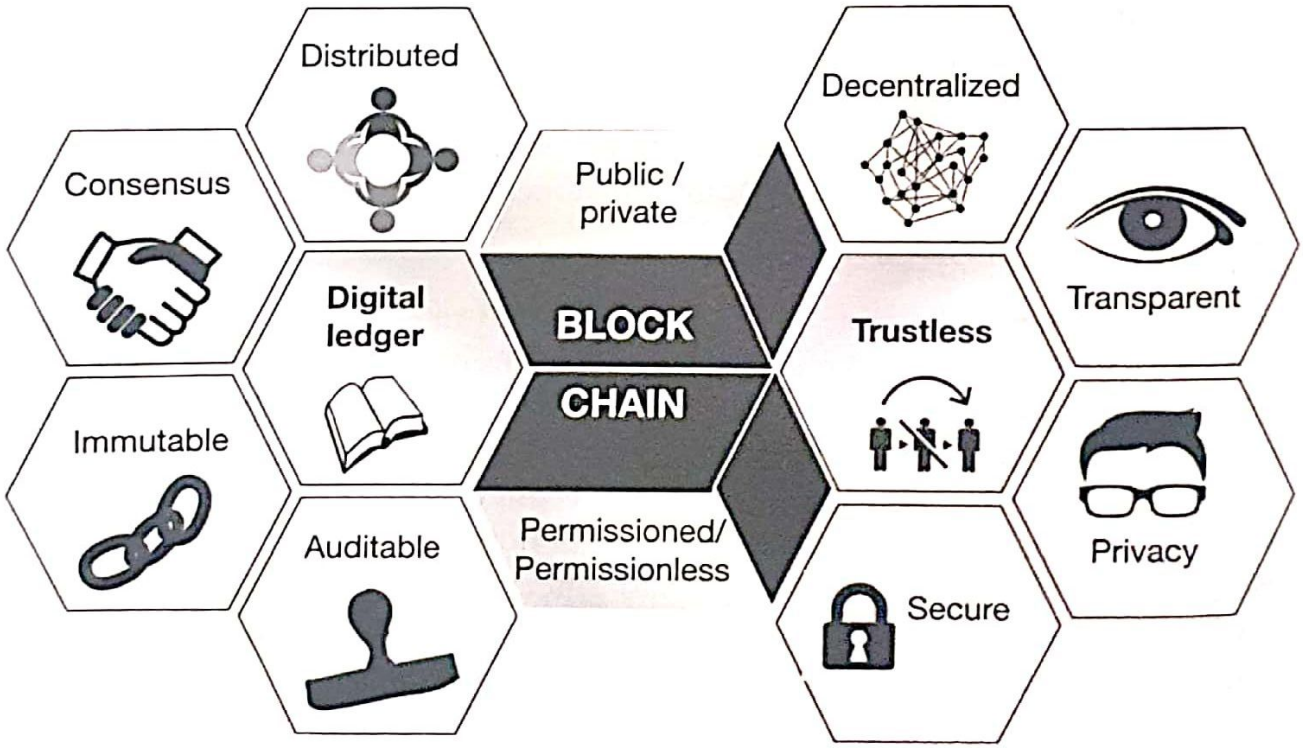


Figure 1.12: Characteristics of blockchain

Blockchain guarantees the integrity of transactions through digital signatures. Digital signatures secure not only the data but also the identity of the individual sending it. It ensures the authenticity of the data being sent and the person who is sending it.

Companies can leverage the benefits of deploying blockchain applications. The blockchain public ledger is secure, reliable, and transparent. Its distributed nature reduces the risk of a single point of failure. The complex consensus protocols that are run by miners authorize transactions to ensure an immutable, hacking resistant ledger. The trustless nature of blockchain ensures fast settlements, reduced operating costs, and savings.

Blockchain Technology has found user cases in several domains including but not limited to Banking, Healthcare, Automotive, Retail, Supply chain, and others. In the following chapters, we will delve deeper into the various concepts, components, various blockchain systems and platforms, challenges, and use cases.

EXERCISES

Multiple Choice Questions

1. **Blockchain is a type of:**
   A. Distributed ledger technology
   B. Client server
   C. Centralized ledger technology
   D. Physical ledger
   Answer: A
   Explanation: Technically, Blockchain is defined as a distributed, replicated peer-to-peer network of databases that allows multiple non-trusting parties to transact without a trusted intermediary and maintains an ever-growing, append-only, tamper-resistant list of time-sequenced records.
   In short, Blockchain is a type of a distributed ledger that sits on the internet for recording transactions and maintaining a permanent and verifiable record-set of information.

2. **Technically, the Blockchain and Bitcoin are not the same.**
   A. False
   B. True
   Answer: B
   Explanation: Though bitcoin and blockchain are often referred to interchangeably, they are not the same. Blockchain is the underpinning technology that the Bitcoin was built on.

3. **Bitcoin is a cryptocurrency, while blockchain is a ledger.**
   A. False
   B. True