Blockchain Technology: Understanding its Meaning, Architecture, and Diverse Applications

Technical Report · August 2023

DOI: 10.13140/RG.2.2.25588.32643/1

3 authors, including:

Dawit Andargachew Asmare
University of Padova
1 PUBLICATION **1** CITATION
SEE PROFILE

Fitsum Gedefaw Legese
Addis Ababa University
1 PUBLICATION **1** CITATION
SEE PROFILE

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

BLOCKCHAIN TECHNOLOGY

BY

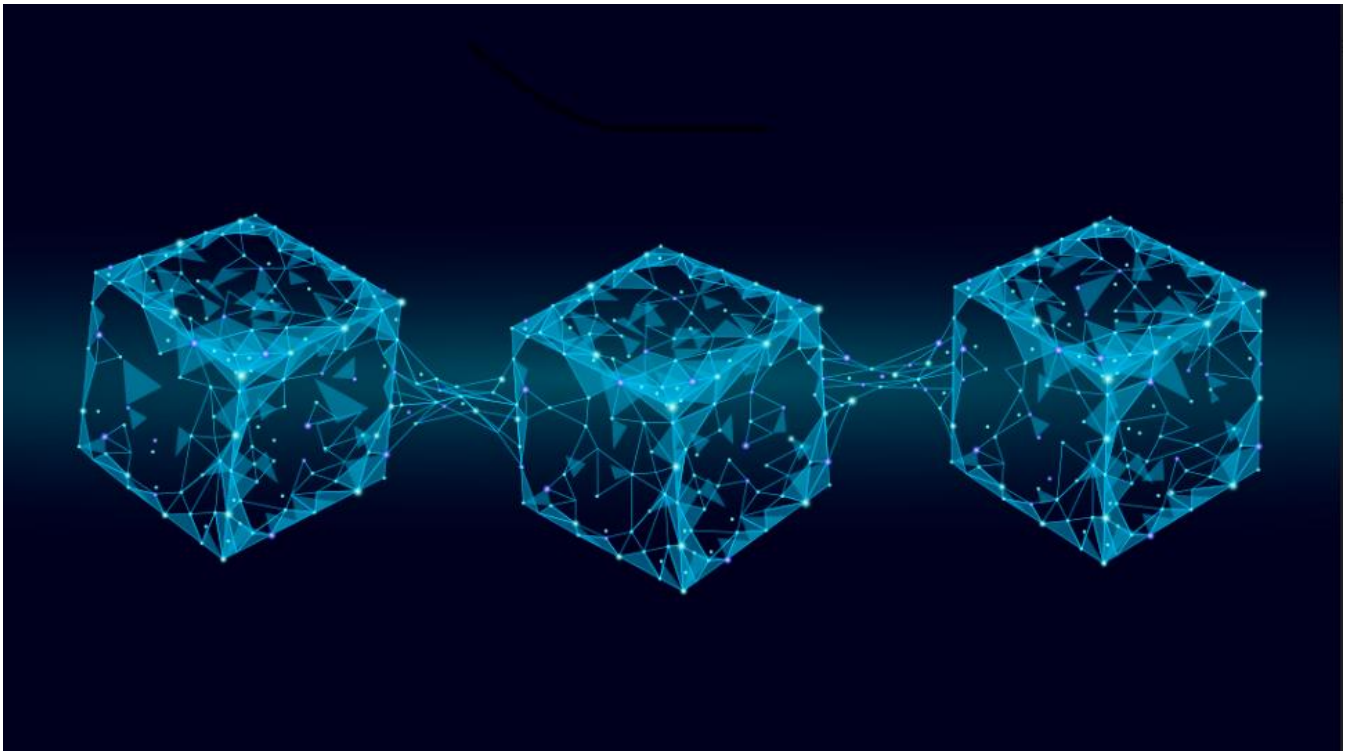
1. Dawit Andargachew UGR/3074/12
2. Fitsum Gedefaw UGR/5537/12
3. Joseph Birara UGR/5617/12

ADVISOR: Abdurehman D

February, 2023

`

Technical Report on Blockchain Technology



`

TABLE OF CONTENT

`

`

LIST OF FIGURES

`

ACRONYMS

CPU ……...……. Central Processing Unit

DPoS ……...…….. Delegated Proof of Stake

DDoS …….. Distributed Denial of Service

dApps …….. Decentralized applications

EOSIO ...……...… Ethereum Optimized Smart contract Interface Operating system

GPU …….....……. Graphical Processing Unit

IAMS ……...…….…… Identity and Access Management

NFT ...…….. Non-Fungible Token

IoT ……..... Internet of Things

PoA …….. Proof of Authority

PoA ……..…….. Proof of Activity

PoC ……..…….. Proof of Capacity

PoS ……..Proof of Stake

PoSpace ……..Proof of Space

PoW ……...……...……...Proof of Work

SPV ……..Simple Payment Verification

`

ABSTRACT

The concept of blockchain technological came into existence from the first crypto-currency, Bitcoin. It is a very new, complex and trusted technology, and researchers are working continuously to find a way to apply this disruptive technology in different aspects of our life.

This technical report discusses a brief concept about blockchain, its application in different public sectors, where it is expected to create disruptive changes, as well its future. This paper also provides a basic understanding of blockchain technology, like what blockchain and blockchain technology is, its features, advantages, types, and how it will be helpful in banking and finance, voting, asset registry, supply chain and many more.

Blockchain is a very disruptive technology that can reconfigure all aspects of society and its operations. This technology is immutable and distributed, making it difficult for transactions to be changed, duplicated, or faked.

There are many different types of blockchains and blockchain applications. Blockchain is an all-encompassing technology that is integrating across platforms and hardware all over the world.

`

CHAPTER 1 INTRODUCTION

1.1 Introduction

Most simply, the blockchain is defined as the decentralized and distributed ledger technology that provides information to be recorded, maintained and shared by a community. It is a new type of database having digital records of transactions. In blockchain technology, "*All transactions performed in the past cannot be changed or deleted. So, it provides transparency and immutability to all transactions that happened in the past*".

In blockchain, no person or entity has control over it, and none of them can go back and erase or change a transaction history. Distributed ledger technology combines transparency, immutability, and security for the participants of the network. It is nearly impossible to hack or attack the entire system based on blockchain technology,

> "*Unlike the Web or Internet alone, blockchains are distributed, not centralized; open, not hidden; inclusive, not exclusive; immutable, not alterable; and secure. Blockchain gives us unprecedented capabilities to create and trade value in society*".

Figure 1.1: A comparison of the topography of centralized, decentralized and distributed networks

Thus, it enables peer-to-peer transactions by eliminating third parties from the scenario (for instance, banks/financial institutions/state, in the case of traditional mode of exchanging currency and ensuring transparency as well as cost effectiveness. The most recent and controversial example that has been tied to this technology is its use in crypto-currency.

1.1.1 So, what is Blockchain?

Originally, blockchain was just a computer science term for how to structure and share data. The name of '*blockchain*' came from its structure, i.e. '*block*' and '*chain'*; individual records, called '*block's*, are linked together in a series to form the *'chain'*. It is an emerging technology that will change the way we acquire and share information.

It is also an online global database that anyone, anywhere at any time, with an internet connection, can use. It stores the time, date, details of participants, and other legal or contractual portions of every transaction. It is distributed identically across different decentralized nodes, ensuring no one organization can own or manipulate it. Thus, Hacking or tampering with the entire system based on this technology by faking transactions, documents, and any information becomes nearly impossible.

Transactions based on this technology are faster and more secure than the traditional ones. Blockchain technology combines many other technologies, like cryptography, peer-to-peer networks, smart contracts, and consensus mechanisms to create a new and unique database.

Blockchain's shared and distributed ledger facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible a house, a car, cash, land or intangible like intellectual property, such as patents, or copyrights. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

Blockchain is the primary technology behind crypto-currencies like Bitcoin and Ethereum, making it secure for trading digitally by verifying and storing transaction records in a distributed and time-stamp manner. The term Bitcoin, a crypto-currency, was first introduced in 2008 by Satoshi Nakamoto's work named "*Bitcoin: A Peer-to-Peer Electronic Cash System*".

And nowadays, "… *blockchain are now recognized as the 5th evolution of computing following IoT, internet Of Things*".

1.2 Brief History of Blockchain

Blockchain technology has to be one of the biggest innovations of the 21st century given the ripple effect it is having on various sectors, from financial to manufacturing as well as education. The history of Blockchain dates back to the early 1990s and others even argue it is proposed in the late 70s. Let's dive in.

1979-1991: The early years of Blockchain

Many of the technologies on which blockchain is based were in the works long before bitcoin appeared. One of these technologies is the Merkle tree, named after computer scientist Ralph Merkle.

Merkle described an approach to public key distribution and digital signatures called "tree authentication" in his 1979 Ph.D. thesis for Stanford University. This enhances efficiency thereby enabling the collection of more documents on a single block. The Merkle tree also provides a data structure for verifying individual records.

Figure 1.2: Ralph Merkle

But Merkle tree was not the only one, David Chaum described a vault system for establishing, maintaining and trusting computer systems by mutually suspicious groups in his 1982 Ph.D. dissertation for the University of California, Berkeley. This was a system that embodied many of the elements that make up a blockchain. Chaum is also credited with inventing digital cash, and in 1989, he founded the DigiCash Corporation

Figure 1.3: David Chaum

1991-2008: Creation of Blockchain Technology

The blockchain technology was described in 1991 by the research scientist Stuart Haber and W. Scott Stornetta. They wanted to introduce a computationally practical solution for time-stamping digital documents so that they could not be modified or backdated. They develop a system using the concept of cryptographically secured chain of blocks to store the time-stamped documents.

Figure 1.4 Stuart Haber and W. Scott Stornetta.

In 1992, Haber and Stornetta updated the design to incorporate Merkle trees, which enabled multiple document certificates to live on a single block.

2008-2013: Blockchain 1.0: Bitcoin Emergence

In 2008, a research paper, titled "Bitcoin: A Peer-to-Peer Electronic Cash System", appeared on online discussion forums. The paper was attributed to Satoshi Nakamoto.

Experts say the blockchain protocol outlined in the Nakamoto research paper is essentially the same as David Chaum's. The only substantive difference is the addition of the Bitcoin proof-of-work consensus mechanism for validating data blocks and mining coins.

2013-2015: Blockchain 2.0: Ethereum Development

In 2015, the Ethereum blockchain was introduced by a team that included contributors to the Bitcoin project. However, Ethereum was different, other

blockchains existed only to support specific cryptocurrencies. Ethereum was introduced as a platform for running decentralized applications. The Ethereum blockchain holds executable source code in addition to data, so it serves as the foundation for thousands of blockchain-based applications. The Ethereum blockchain's flexibility makes it ideal for hosting both NFTs and dApps.

Ethereum blockchain platform has also succeeded in gathering an active developer community that has seen it establish a true ecosystem.

2015: Hyperledger

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology. Hyperledger focuses on encouraging the use of blockchain technology to improve the performance and reliability of current systems to support global business transactions.

2017: EOS.IO

EOSIO is an open-source platform that lets third-party developers create and run decentralized applications, or dApps. EOSIO platform emulates the functions of a computer, and uses familiar computing concepts in its operations.

The smart contract platform claims to eliminate transaction fees and also conduct millions of transactions per second. It was developed by the private company Block.one and launched in 2017. The platform was later released as open-source software.

1.3 How does Blockchain Works

To understand the operation and workflow of blockchain, let's see what a block is composed of. A block is composed of a header and a body. The block header contains the hash of the previous block, a timestamp, Nonce and the Merkle root, whereas block body stores the transaction data.

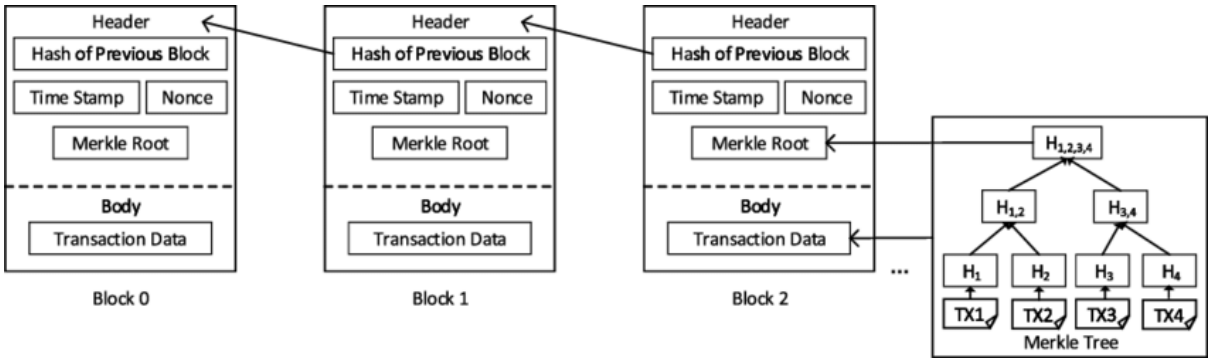


Figure 1.5: The structure of a Blockchain.

The first block of the chain is called the “Genesis Block”. Genesis blocks may also be called “Block 0” or “Day-Zero Block”. To make sure a block in a chain is submitted once, blockchain uses “*nonce*”, a 32 bit random number assigned by the minder to each block Nonce is basically an abbreviation for “number used once”, and it is a random number you can use only once.

1.3.1 What is Merkle Tree?

The concept of Merkle Tree is named after Ralph Merkle, who patented the idea in 1979. Fundamentally, it is a data structure tree in which every leaf node labelled with the hash of a data block, and the non-leaf node labelled with the cryptographic hash of the labels of its child nodes. The leaf nodes are the lowest node in the tree. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. The vast majority of hash tree implementations are binary (each node has two child nodes), but they can have many more.

Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle Root, or the Root Hash. Every leaf node is a hash of transactional data, and the non-leaf node is a hash of its previous hashes. Merkle trees are in a binary tree, so it requires an even number of leaf nodes. If there is an odd

number of transactions, the last hash will be duplicated once to create an even number of leaf nodes.

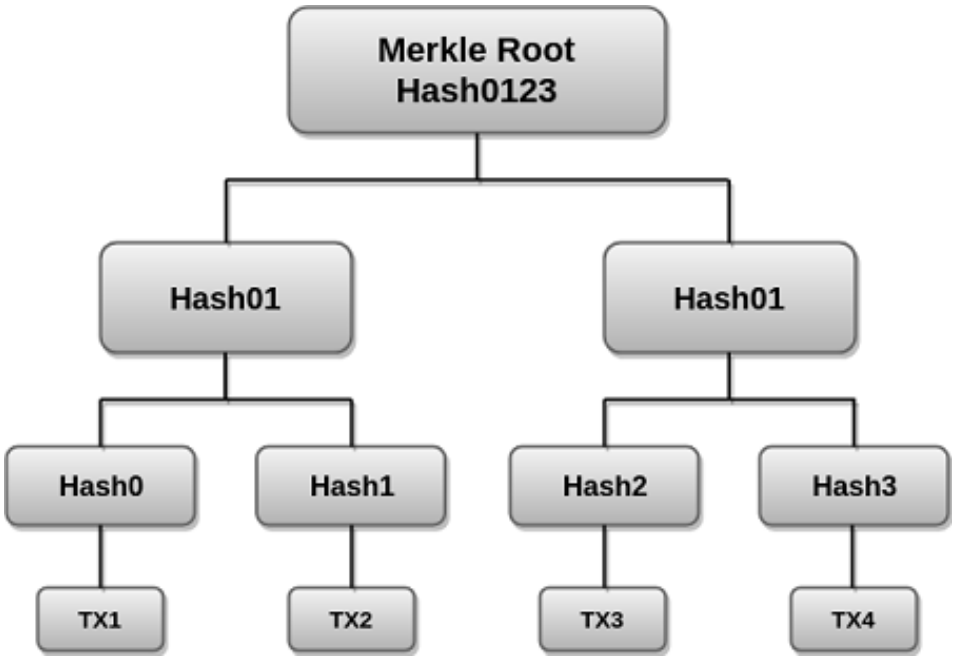


Figure 1.6: Merkel tree representation

The above example is the most common and simple form of a Merkle tree, i.e., Binary Merkle Tree. There are four transactions in the block: TX1, TX2, TX3, and TX4. The top hash which is the hash of the entire tree, is known as the Root Hash, or the Merkle Root.

Due to the tree-like linkage of hashes, if any single transaction detail or transaction order changes, these changes are reflected in the hash of that transaction. This change would propagate up the Merkle Tree to the Merkle Root, altering the Merkle Root's value and thus invalidating the block. As a result, the Merkle tree enables a quick and simple way to determine whether or not a specific transaction is altered in the set or not.

Thus Merkle root, which contains all the information about every single transaction that exists on the block, offers a single-point hash value that enables validating everything present on that block.

Basically, Blockchain is a chain of blocks, and a block consists of three things: Data, Hash, and Hash of the previous block. Each block in the chain contains a cryptographic hash of its own and the last block to stay connected in the chain.

A Block is a primary unit of blockchain. In the blockchain, a block is a collection of data or information. The information is added to the block in the blockchain by connecting it with other blocks in chronological order and creating a chain of blocks linked together. Thus, it forms a chronological database of transactions that is shared with multiple nodes, i.e. computers or servers, in a network.

Let's consider a chain of three blocks. As shown in the figure below, each block contains its own hash and the hash of the previous block. So block number 3 points to block number 2, and block number 2 points to block number 1.

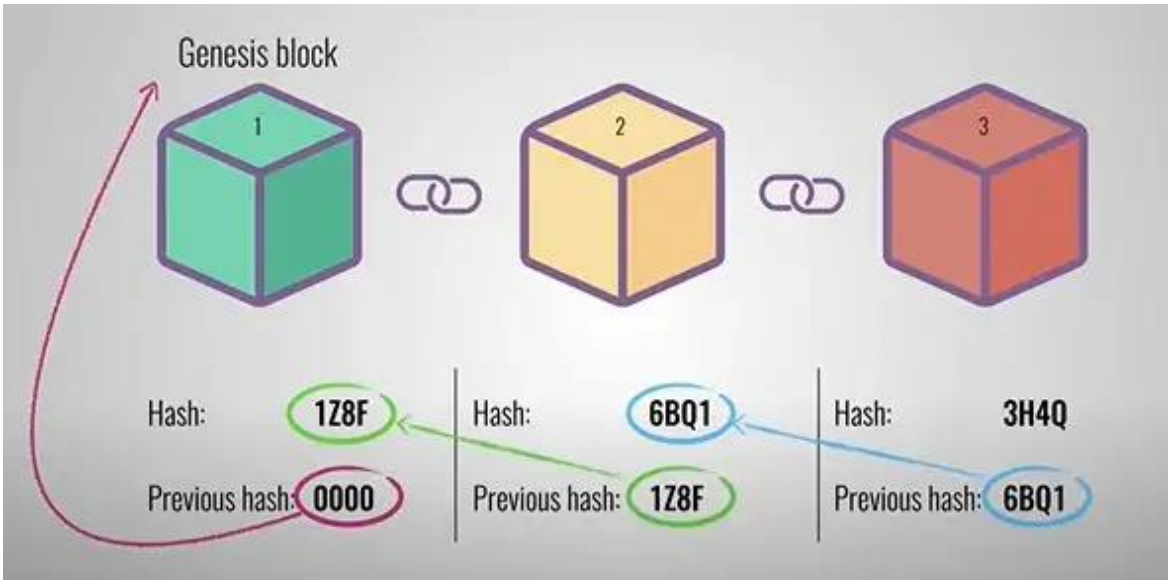


Figure 1.7: Block of chains

The first block is a bit special, as it cannot point to previous blocks because it's the first. This block is called the genesis block.

A hash identifies the block and all of its contents and is always unique. Changing anything inside the block will cause the hash to change. Hashes are very useful when you want to detect changes to blocks. If the hash of a block changes, it's no longer the same block.

A Hash is a unique alphanumeric identifying code or number generated when any transaction happens in the blockchain. Hash is based on data of its own, a hash of the previous one, and its timestamp. If the data inside existing block is changed, the hash code of that block will change as well. This hash code is unrecognisable to its successor, which

has stored the prior block's original hash, resulting in the blockchain being broken. The chain is broken when any block is tampered with or altered.

Let's say block of the previous chain is compromised by attackers. This causes the hash of that block to change. In turn, that will make block 3 and all following blocks invalid because block 3 will no longer store a valid hash of the previous block.

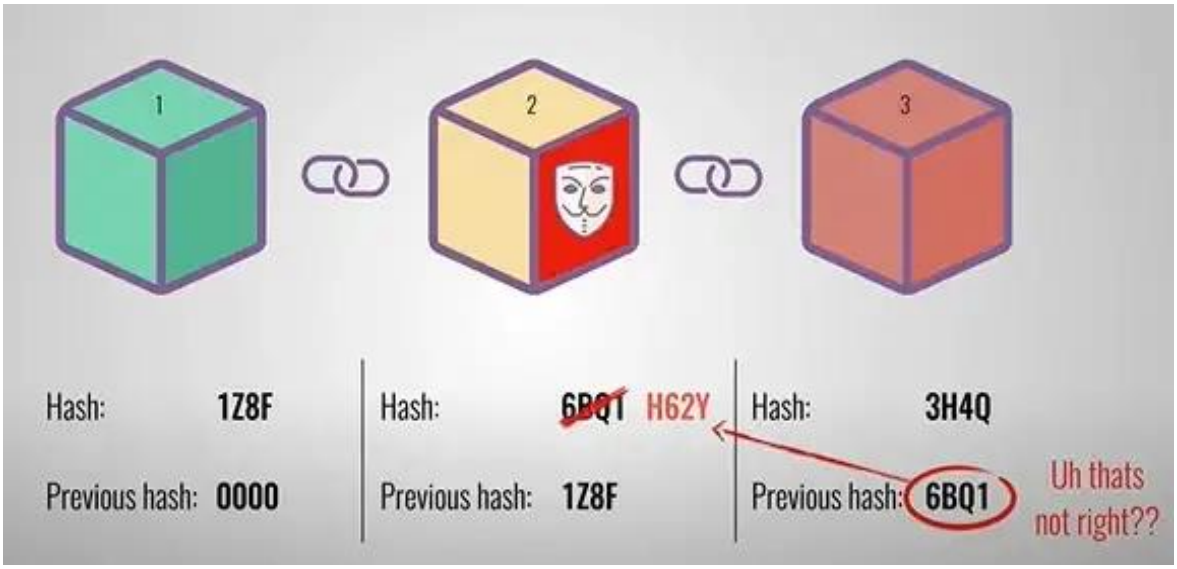


Figure 1.8: Modification of the block on a blockchain

So, as shown in the figure changing a single block will make all the following blocks invalid. That is why blockchains are believed to be immutable for the reason that data remains intact once it is saved.

CHAPTER 2 ARCHITECTURE OF BLOCKCHAIN

2.1 Permissioned vs. permissionless Blockchain

A blockchain is an immutable ledger, a record within a system of transactions that represents the activity on that network. It can be used for various types of operations such as finance, tech, authentication, and a lot more and by different types of organizations. So how do we specify who participate in the network. Let’s discuss what Permissioned and Permissionless blockchains are.

2.1.1 Permissionless Blockchain:

- In permissionless blockchain, any user may access the blockchain network in an unknown fashion and be a "node," and permissionless blockchains do not limit the rights of nodes on the network. Yet, due to the high number of nodes and the magnitude of the transactions, permissionless blockchains also frequently have slow transaction processing rates. However, it’s not a technology you could trade sensitive information on because that information would become visible to everyone on the network.

2.1.2 Permissioned Blockchain:

- Permissioned blockchains limit the nodes that can access the network and their potential access rights. The other users of a permissioned blockchain are aware of the identity of the users of that blockchain. Permissioned blockchains, in contrast, typically operate more effectively. There are fewer nodes on the blockchain network, which reduces the processing time required for each transaction.

2.2 Types of Blockchain

The most basic need or application of a blockchain is to carry out transactions or exchange of information through a secure network. But the way we use blockchain and distributed ledger technology vary from case to case. If we consider Bitcoin, its blockchain network is a public network because people from all over the world can become a node, verify other node and trade bitcoins. On the other hand, if a bank is using a private blockchain network. It will be a restricted network where only the authorized members of the bank can access confidential information. Thus, no one out of this closed network can gain access to bank data.

Permissionless and permissioned blockchains can be used to categorize all different kinds of blockchains. Here is their visual representation;

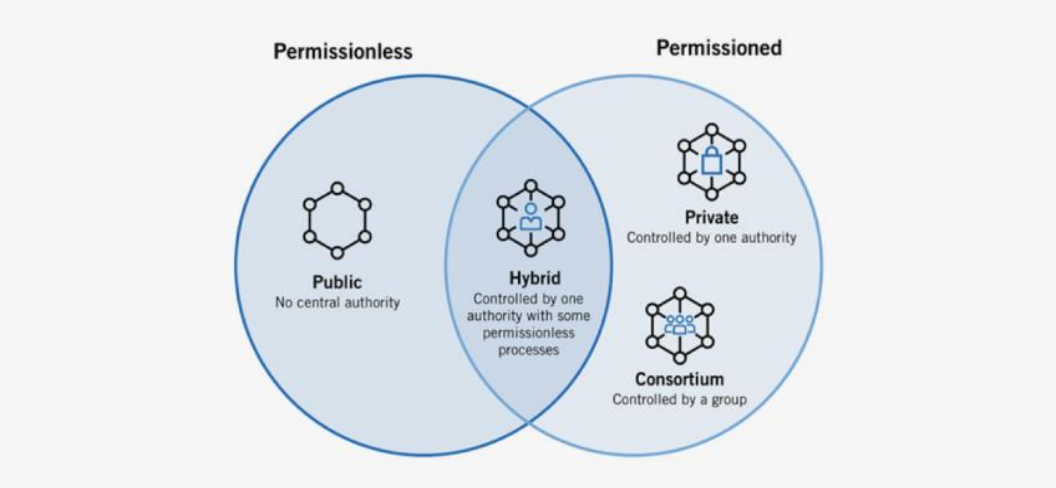


Figure 2.1: Permissioned vs. Permissionless blockchain

There are primarily two types of blockchains; Private and Public blockchain. However, there are several variations too, like Consortium and Hybrid blockchains.

2.2.1 Public Blockchain

Public blockchains are such blockchains that are accessible publicly. It is a type of blockchain, "for the people, by the people, and of the people" (Sanjay & Nabi, 2020). The public blockchain is a permissionless distributed ledger technology that allows anyone to join and conduct transactions. It is an open variant in which each user keeps a copy of the ledger. It implies that anyone with access to the internet can explore the public blockchain. The bitcoin public blockchain was among the first public blockchains to be made available to the general public. It made it possible for anyone with an internet connection to conduct decentralized transactions.

Advantages of Public Blockchain:

- Trustable: Public Blockchain nodes do not need to know or trust each other because the proof-of-work procedure ensures no fraudulent transactions.
- Secure: A public network can have as many participants or nodes as it wants, making it a secure network. The higher the network's size, the more records are distributed, and the more difficult it is for hackers to hack the entire network.
- Open and Transparent: The data on a public blockchain is transparent to all member nodes. Every authorized node has a copy of the blockchain records or digital ledger.

Disadvantages of Public Blockchain:

- Lower TPS: The number of transactions per second in a public blockchain is extremely low. This is because it is a large network with many nodes which take time to verify a transaction and do proof-of-work.
- Scalability Issues: Its transactions are processed and completed slowly. This harms scalability. Because the more we try to expand the network's size, the slower it will become.
- High Energy Consumption: The proof-of-work device is expensive and requires lots of energy. Technology will undoubtedly need to develop energy-efficient consensus methods.

Some uses of Public Blockchain:

- Voting: Governments can use a public blockchain to vote, ensuring openness and trust.
- Fundraising: Businesses or initiatives can use the public Blockchain to improve transparency and trust.

2.2.2 Private Blockchain

A private blockchain is permissioned or restrictive blockchain technology, operates only in a closed network. This blockchain is usually used within an organization or firm where only authentic members can access and do the transactions in the network. A private blockchain can be used in voting, digital identity & supply chain management etc.

Advantages of Private Blockchain:

- Speed: Private Blockchain transactions are faster. This is because a private network has a smaller number of nodes, which shortens the time it takes to verify a transaction.
- Scalability: You can tailor the size of your private Blockchain to meet your specific requirements. This makes private blockchains particularly scalable since they allow companies to easily raise or decrease their network size.

Disadvantages of Private Blockchain:

- Trust Building: In a private network, there are fewer participants than in a public network.

- Lower Security: A private blockchain network has fewer nodes or members, so it is more vulnerable to a security compromise.
- Centralization: Private blockchains are limited in that they require a central Identity and Access Management (IAM) system to function. This system provides full administrative and monitoring capabilities.

Uses of Private Blockchain:

- Supply Chain Management: A private blockchain can be used to manage a company's supply chain.
- Asset Ownership: A private blockchain can be used to track and verify assets.
- Internal Voting: Internal voting is also possible with a private blockchain.

2.2.3 Hybrid Blockchain

The hybrid blockchain is a combination of both private and public blockchain. The hybrid blockchain architecture is not open to everyone but still offers blockchain features such as integrity, transparency, and security. The hybrid blockchain members can decide who can participate in the blockchain or which transactions are made public. This brings the best of both worlds and ensures that a company can work with its stakeholders in the best possible way.

Advantages of Hybrid Blockchain:

- Secure: Hybrid Blockchain operates within a closed environment, preventing outside hackers from launching a 51 percent attack, which is an attack on a crypto-currency blockchain by a group of miners who control more than 50% of the network's mining hash rate, on the network.
- Cost-Effective: It also safeguards privacy while allowing third-party contact. Transactions are inexpensive and quick and scale better than a public blockchain network.

Disadvantages of Hybrid Blockchain:

- Lack of Transparency: Because information can be hidden, this type of blockchain isn't completely transparent.
- Less Incentive: Upgrading can be difficult, and users have no incentive to participate in or contribute to the network.

Uses of Hybrid Blockchain:

- Real Estate: Real-estate companies can use hybrid networks to run their systems and offer information to the public.
- Retail: The hybrid network can also help retailers streamline their processes.
- Highly Regulated Markets: Hybrid blockchains are also well-suited to highly regulated areas like the banking sector.

2.2.4 Consortium Blockchain

Consortium blockchain is also known as Federated blockchain. Like a private chain, a consortium blockchain is privately owned but not by a single entity or individual. Instead, a group of individuals from different sectors or a group of companies owns such a chain. It is an ideal solution that requires collaboration across the board from multiple sources. It helps keep the flow of data secured and efficient between entities.

Advantages of Consortium Blockchain:

- Secure: A consortium blockchain is more secure, scalable, and efficient than a public blockchain network. It, like private and mixed blockchains, has access controls.

Disadvantages of Consortium Blockchain:

- Lack of Transparency: The consortium blockchain has a lower degree of transparency. If a member node is infiltrated, it can still be hacked, and the Blockchain's rules can render the network inoperable.

Uses of Consortium Blockchain:

- Banking and Payments: A consortium can be formed by a group of banks working together. They have control over which nodes will validate transactions.
- Research: A consortium blockchain can be employed to share research data and outcomes.

2.3 Components of Blockchain

The main core components of a blockchain technology are wallet, node application, transaction, block, way of chaining blocks, distributed ledge, miners, cryptography or hash functions and consensus mechanism. Let’s see them one by one.

2.3.1 Wallet

A blockchain wallet contains a set of user identities. An application run by a user selects one of these identities when it connects to a blockchain network. Access rights to blockchain network resources, such as the making transactions, are determined using this identity. The wallet is accessible from web devices, including mobile ones, and the privacy and identity of the user are maintained. Some of the most known examples of blockchain wallets are Bitcoin and Ethereum.

How Do Blockchain Wallets Work?

Whenever a blockchain wallet is created, a private and a public key associated with the wallet are provided. Let's consider email as an example. Public keys are similar to the email address that can be given to anyone, and private keys are similar to the account password, that cannot be shared. Blockchain wallets follow a similar process using a public key and a private key together.

A public key is similar to email address; it can be shared to anyone. A public key allows a user to receive and send transactions. It's a cryptographic code that's paired to a private key. On the other hand, private key is similar to email password. While anyone can send transactions to the public key, private key is needed to "unlock" and prove the owner of the crypto-wallet in order to access transaction details.

So a blockchain wallet provides all the features that are necessary for safe and secure transfers and exchanges of funds between different parties.

2.3.2 Node application

Each Internet-connected computer needs to install and run a computer application specific to the ecosystem they wish to participate in. Using the case of Bitcoin as an example ecosystem, each computer must be running the Bitcoin wallet application.

In some blockchain applications, like Bankchain which is used to make payment in more than one bank, participation is restricted and requires special permissions to join. Bankchain only permits banks to run the node application, whereas the Bitcoin ecosystem allows anyone to download and install the node application and thus participate in the ecosystem.

Regardless of how one is qualified, once one has a node application one can participate in the respective blockchain ecosystem.

2.3.3 Transactions

A blockchain transaction is data transmission across the network of computers in a blockchain system. A transaction can be a contract, agreement, transfer, or exchange of assets between two or more parties. The network of computers in a blockchain store the transactional data as replicas with the storage typically referred to as a digital ledger.

2.3.4 Blocks

Blocks are the building block of blockchain technology. A block contains a block header and block data. Many blockchain implementations utilize data fields containing header and data fields. The block header contains metadata, information about it and its previous block. The block data contains a list of validated and authentic transactions which have been submitted to the blockchain network.

Block Header contains:

- The block number, also known as block height is the sequence number of the block. Genesis block, the first block in the chain, has block number 1.
- Block size: refers to the amount of data or transactions a single block in the chain can carry. In Bitcoin, each block can hold up to 2000 transactions.
- The previous block header's hash value.
- the root hash of the Merkle tree
- A hash representation of the block data (different methods can be used to accomplish this, such as a generating a Merkle tree, and storing the root hash, or by utilizing a hash of all the combined block data).
- A timestamp time when the block has been mined or added to the chain
- The size of the block.
- The nonce value a number used by miners to solve and its usually 32 bit number

Block Body contains:

- The block body is a place where Merkle tree is stored. It contains all transactions that are confirmed with the block.

2.3.5 Nodes

In simple terms, every participant in a blockchain network is a node. There exist several types of blockchain nodes, and each of them requires specific hardware configurations to

get hosted or connected. Basically, there are three types of nodes: lightweight, full and master nodes.

- Full nodes act as a server in a decentralized network. Their main tasks include maintaining the consensus between other nodes and verifying the transactions. They also store a copy of the blockchain, thus being able to securely enable custom functions such as instant send and private transactions
- Lightweight nodes: Lightweight nodes, also known as Simple Payment Verification (SPV) nodes. These types of blockchain nodes communicate with the blockchain but rely on full nodes to provide them with the necessary information. They do not need to store a copy of the blockchain, instead they only query the current status of the chain and broadcast transactions for processing.
- Master node: Master nodes are full nodes responsible for maintaining the blockchain ledger and validating transactions. However, they can't add new blocks to the blockchain. In general, they are responsible for enforcing the rules of the respective blockchain.

2.3.5. 1 What about Miner Nodes?

Miners are one of the different types of nodes in blockchain (either full or lightweight) that attempt to prove that they have completed the necessary work to create a new block on the blockchain. This process, called mining, involves solving a cryptographic problem using hardware components like CPUs, or GPUs. Once a miner has solved the problem, they broadcast the solution to the network to be verified by full nodes.

The first mining node to solve a mathematical problem receives the right to confirm a block of transactions.

2.3.6 Distributed ledger

A ledger is a database containing all transactions that are constantly updated. In case of blockchain it is distributed or shared among multiple parties. It is composed of multiple blocks (each containing several number of transactions) and these blocks are linked together into a chain using cryptography. In other words, the following block will contain the cryptographic identifiers of the previous block. So, if any block in the past has a problem, it will affect all the blocks at the back of the chain. Its distributed nature, eliminate the need for a central authority to authorize or validate any transactions.

Distributed ledgers allows real-time sharing of data which gives trust that data in the ledger is up to date and legitimate. Also Distributed Ledger Technology eliminates the single point of failure which prevents data in the ledger from being manipulated.

2.3.7 Cryptography

Cryptography is a way of securing data against unauthorized access. In the blockchain, it is used to secure transactions between two nodes in the blockchain network. Cryptography ensures security, integrity and verification of the information in the ledger or the information transmitted between the nodes. Cryptography encryption methods are almost impossible to break.

2.3.8 Consensus Mechanism

As a distinctive feature, blockchain eliminates the need for a trusted third-party to validate the transactions. Instead, a consensus mechanism is used between all the nodes before a block, recording multiple transactions, is included into the blockchain. Essentially, a consensus algorithm is used to regulate the creation of a block in an unbiased manner to resist malicious attack. It enables a group of peers – or nodes – on a network determine which blockchain transactions are valid and which are not.

There are different consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), Delegated Proof of Stake(DPoS), Proof of Activity (PoA), Proof of Capacity (PoC) or Proof of Space (PoSpace). They can be generalized in the following diagram as follows:

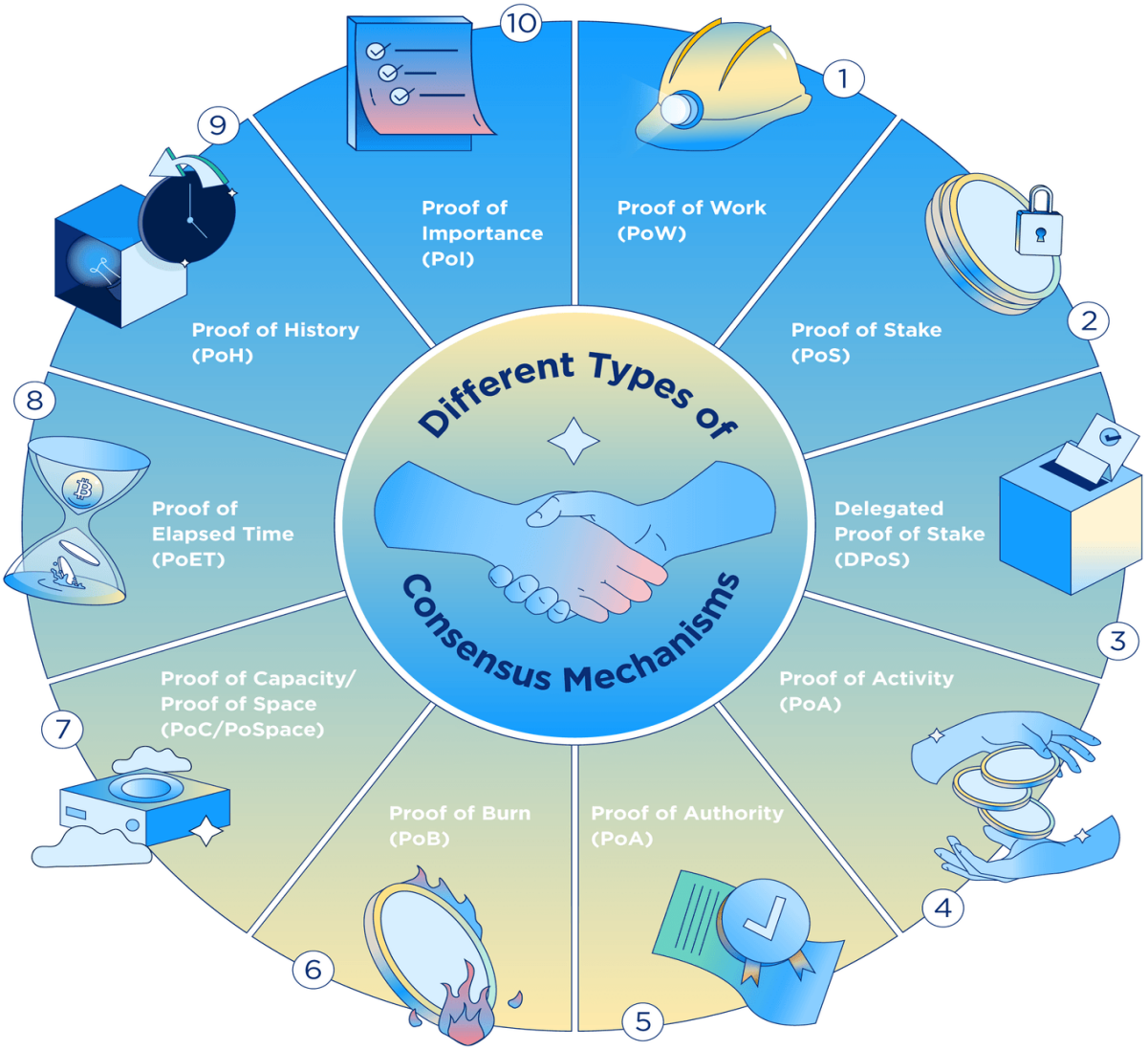


Figure 2.2: Different consensus mechanism used in blockchain

Let's discuss three of the most common consensus mechanisms.

Proof of Work (PoW)

- It is mainly used by Bitcoin, Ethereum, and many other public blockchains. It was the very first consensus mechanism created. It is generally regarded to be the most reliable and secure of all the consensus mechanisms, though there are concerns over scalability. In PoW, miners essentially compete against one another to solve extremely complex computational puzzles using high-powered computers. The first to come up with the 64-digit hexadecimal number ('hash') earns the right to form the new block and confirm the transactions. The successful miner is also rewarded with a predetermined amount of crypto, known as a 'block reward'. As it requires large amounts of computational resources and energy in order to generate new blocks, the

operating costs behind PoW are notoriously high. High electrical consumption is the most common criticism of PoW. This has led many to a more sustainable, energy-efficient consensus protocols, such as proof of stake (PoS).

Proof of Stake (PoS)

- In a proof of stake (PoS) system, miners are required to have a 'stake' of digital currency for a chance to be randomly chosen as a validator. The process is not unlike a lottery whereby the more coins you stake, the better your odds. Unlike in PoW where miners are incentivised by block rewards (newly generated coins), those who contribute to the PoS system simply earn rewards. This enables faster and lower-cost transactions.

Proof of Authority (PoA)

- Proof of authority is not as common as Proof of Work but has a unique form. It is used mainly by private companies or organizations that use blocks created by vetted sources who have special permissions to access the network. This consensus mechanism selects validators based on reputation rather than a user's digital assets. In this system, a group of validators are pre-approved in a vetting process that often includes a background check.

2.5 Characteristic of Blockchain

Blockchain technology isn't just a distributed ledger across a network, but it offers a lot more. So, what are the key blockchain features that makes it so irresistible? Why is it gaining so much popularity? Let's dive in a little deeper into the features of blockchain to answer these questions.

2.5.1 Immutability

Immutability means that the blockchain is a permanent and unalterable network, which enable the network to remain as it is. But how does it maintain that way? Instead of relying on centralized authorities, blockchain technology functions through a collection of nodes. Every node in the network has a copy of the digital ledger. To add a transaction every node checks the validity of the transaction and if the majority of the nodes think that it is a valid transaction then it is added to the network. This means that without the approval of a majority of nodes no one can add any transaction blocks to the ledger. Any validated

records are irreversible and cannot be changed. This means that any user on the network won't be able to edit, change or delete it. This promotes transparency and makes it corruption-proof.

2.5.2 Decentralized

The blockchain network is decentralized which means that there is no central governing authority that will responsible for all the decisions. Rather a group of nodes makes and maintain the network. Each and every node in the blockchain network has the same copy of the ledger. Decentralization property offers many advantages in the blockchain network like:

- As a blockchain network does not depend on human calculations, it is fully organized and fault tolerant.
- The blockchain network is less prone to failure due to the decentralized nature of the network. Attacking the system is more expensive for the hackers hence it is less likely to fail.
- There is no third-party involved hence no added risk in the system.
- The decentralized nature of blockchain facilitates creating a transparent profile for every participant on the network. Thus, every change is traceable.
- Users have control over their properties and they don't have to rely on third-party to maintain and manage their assets.

2.5.3 Enhanced Security

Added with decentralization, cryptography lays another layer of security to the entire process on the blockchain network. Cryptography is a complex mathematical algorithm that acts as a firewall for attacks. Every information on the blockchain is hashed cryptographically. Since there is no central authority, it does not mean that one can simply add, update or delete data on the network. In simple terms, the information on the network hides the true nature of the data.

2.5.3.1 Is hashing irreversible?

Hashing is mathematical algorithm that produces a different kind of value, but the length is always fixed. No one can take a public key and come up with a private key. Also, a single change in the input could lead to a completely different ID, so small changes aren't a luxury in the system.

If someone wants to corrupt the network, he/she would have to alter every data stored on every node in the network. There could be millions and millions of people, where everyone has the same copy of the ledger. Accessing and hacking millions of computers is quite impossible.

2.5.4 Distributed ledger

A public ledger provides every information about a transaction and the participant. It's all out in the open, nowhere to hide. For private or federated blockchains, however, is a bit different. But still, in those cases, many people can see what really goes on in the ledger. Distributed ledger is one of the important features of blockchains due to many reasons like:

- In distributed ledger, tracking what's happening is easy as changes propagate really fast in the network.
- Every node on the blockchain network must maintain the ledger and participate in the validation.
- Any change in the ledger will be updated in seconds or minutes and due to no involvement of intermediaries in the blockchain, the validation for the change will be done quickly.
- If a user wants to add a new block then other participating nodes have to verify the transaction. For a new block to be added to the blockchain network it must be approved by a majority of the nodes on the network.
- In a blockchain network, no node will get any sort of special treatment or favours from the network. Everyone will have to follow the standard procedure to add a new block to the network.

2.5.5 Consensus Algorithm

Consensus is a decision-making algorithm for the group of nodes active on the network to reach an agreement quickly and faster and for the smooth functioning of the system. Nodes might not trust each other but they can trust the algorithm that runs at the core of the network to make decisions. There are lots of different consensus algorithms for blockchains over the globe. Each has its own unique way to make decisions and perfecting previously introduced mistakes. Every blockchain must have a consensus algorithm otherwise it will lose its value.

2.5.6 Faster settlement

Traditional banking systems are quite slow. Sometimes it can take days to process a transaction after finalizing all settlements. It also can be corrupted quite easily. Blockchain offers a faster settlement compared to traditional banking systems.

2.5.7 Anonymity

In blockchain, it is true that every transaction is transparent and open to the public, but the actual persons are kept anonymous through the addresses. Let's say a person sends a bitcoin to someone, the receiver will know that the sender is linked to a bitcoin address, but they will not know the actual address. There are several reasons for this – one of them is privacy.

CHAPTER 3 APPLICATIONS OF BLOCKCHAIN

As a reminder, blockchain is not bitcoin. Rather it is the technology that powers bitcoin and other crypto-currencies like Ethereum, Litecoin, Dogecoin, etc. Blockchain is not only used for crypto currencies.

Blockchain technology is being used in many different industries. The annual blockchain spending will reach $16B by 2023 according to recent research by CBInsights and the rate of adoption of the technology is increasing. The technology is actually helping many adopters to stay ahead of the curve than competitors. In addition to making possible instant transactions over the peer-to-peer network and reducing the cost of middle-men, the technology uses authentication to secure data and make it harder to break than any legacy system. The biggest use case of blockchain technology so far is crypto-currencies. However, blockchain does not end there – banks and financial institutions are finding blockchain helpful because it helps them process transactions more quickly and at a lesser cost. Let’s discuss some real-world applications of blockchain.

3.1 Crypto-Currency

Perhaps one of the most popular applications of Blockchain is in Crypto-currency. One of the many advantages of crypto-currency using blockchain as it has no geographical limitations. Before bitcoin, international payments can be a long complicated process and it can take many days for the money to arrive at its destination. Blockchain has helped in simplifying these cross border payments by providing end-to-end remittance services without any intermediaries. Crypto coins can be used for transactions all over the world.

3.2 HealthCare

Healthcare systems in every country and region are struggling with the problem of data siloes, meaning that patients and their healthcare providers have an incomplete view of medical histories. In 2016, Johns Hopkins University published research showing that the third leading cause of death in the US was medical errors resulting from poorly coordinated care, such as planned actions not completed as intended or errors of omission in patient records.

Moreover, the medical industry has suffered greatly from the inability to securely share and access sensitive patient data. Blockchain, however being open and highly secure, can facilitate finely customizable openness for true interoperability. In turn, this will allow health information systems to work together within and across organizational boundaries in order to advance the effective delivery of healthcare for individuals and communities.

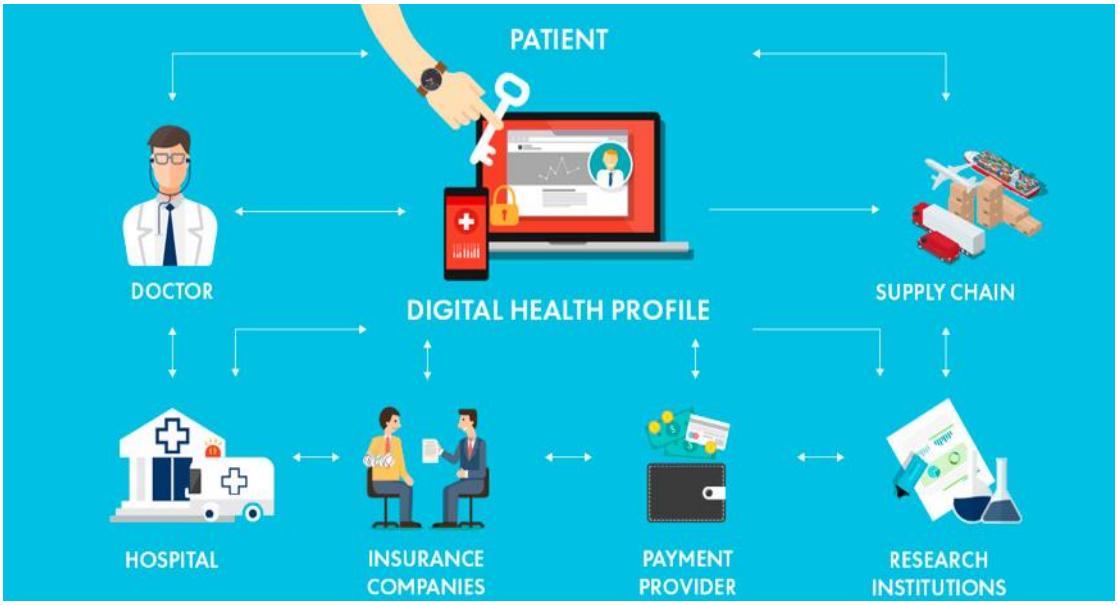


Figure 3.1: Blockchain in Health sector

3.3 Asset Management

Blockchain can plays a big role in asset management. Basically asset management involves the handling and exchange of different assets that an individual may own such as fixed income, real estate, equity, mutual funds, commodities, and other alternative investments. Normal trading processes in asset management can be very expensive, especially if the trading involves multiple countries and cross border payments. In such situations, Blockchain can be a big help as it removes the needs for any intermediaries such as the broker, custodians, settlement managers, etc. Instead, the blockchain ledge provides a simple and transparent process that removes the chances of error by using smart contracts.

2.3.1 What is smart contract?

A smart contract is a computer program or a transaction protocol that is intended to automatically execute, control or document events and actions according to the terms of a contract or an agreement. A smart contract works in the same way as a

traditional contract while also execute exactly as they are set-up (coded, programmed) by their creators. Just like a traditional contract is enforceable by law, smart contracts are enforceable by code.

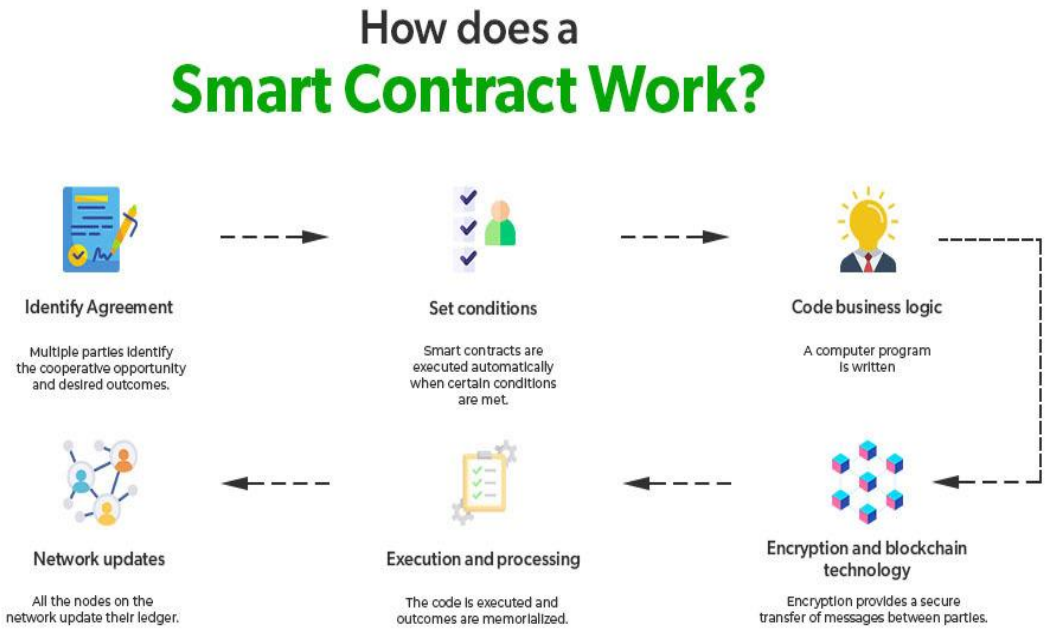


Figure 3.2: Smart contract

3.4 Internet of Things (IoT)

Internet of things is a network of interconnected devices that can interact with others and collect data that can be used for gaining useful insights. Any system of "things" becomes IoT once it is connected. The most common example of IoT is perhaps the Smart Home where all the home appliances such as lights, thermostat, air conditioner, smoke alarm, etc. can be connected together on a single platform. But where does Blockchain come into this? Well, Blockchain is needed for providing security for this massively distributed system. In IoT, the security of the system is only as good as the least secured device which is the weak link. Here Blockchain can ensure that the data obtained by the IoT devices are secure and only visible to trusted parties.

3.5 Voting

Current voting systems like ballot box voting or electronic voting suffer from various security threats such as DDoS attacks, vote alteration and manipulation, malware attacks, etc, and also require huge amounts of paperwork, human resources, and time. Using blockchain, voting process can be made more secure, transparent, immutable, and reliable. Such a system would automatically tally and maintain the result of such a vote, providing a permanent record of what conclusion was reached, for all parties to see.

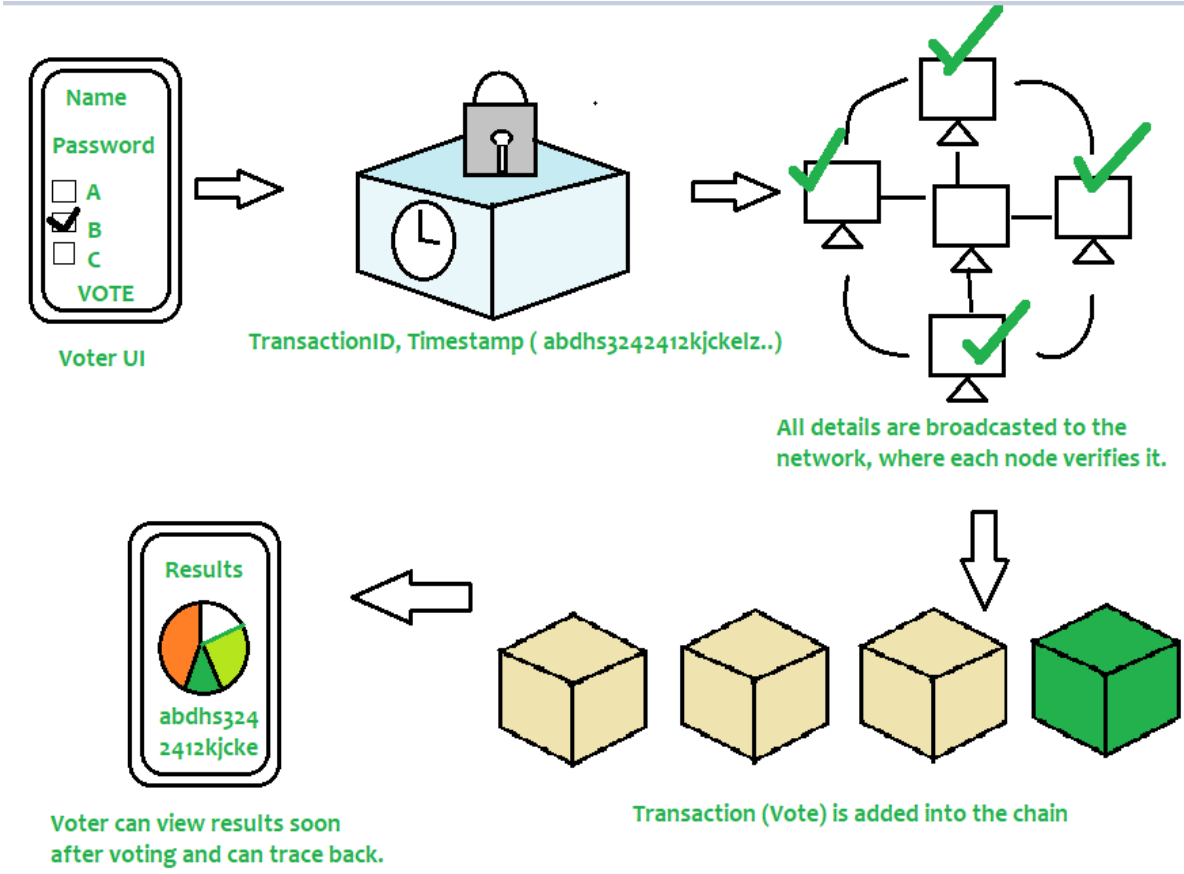


Figure 3.3: Blockchain in voting

3.6 Improved Record Keeping/Sharing

Physical systems of record keeping, from wedding licenses to criminal records and corporate filings, are difficult to organize and navigate, and generally serve little purpose beyond formality. As we all know, business runs on information. Therefore, information must be received quickly and should be accurate. Blockchain is ideal for delivering

information as it provides businesses with fast, secure, and accurate information. Blockchain is widely deployed in various sectors, such as finance, education, healthcare, etc. And blockchain also plays an important role in data management.

Additionally, law enforcement could benefit from a system by which records and sensitive information could be transmitted between departments securely and efficiently. Countless investigations go cold simply because departments didn't have the means to share information that would have resulted in a suspect being nabbed, or weren't willing to navigate arcane systems to share one file with a separate department.

Figure 3.4 Blockchain in record keeping

RESULT AND DISCUSSION

A blockchain is a distributed software network that functions both as a digital ledger and a mechanism enabling the secure transfer of transactions without an intermediary. Just as the internet is a technology that facilitates the digital flow of information, blockchain is a technology that facilitates the digital exchange of units of value. Anything from currencies to land titles to votes can be tokenized, stored, and exchanged on a blockchain network.

The first manifestation of blockchain technology emerged in 2009 with Bitcoin, a secure, peer-to-peer electronic cash system. Bitcoin is accessible and open to anyone, while some blockchains have been designed to meet the needs of a finite group of participants, where access to the network is restricted.

Regardless of the type of blockchain protocol that is deployed, its applications go beyond the digital currency field. With the same features, blockchain can be leveraged across various domains, as this paper demonstrated, like finance, asset registry and record keeping, Internet of Things (IoT), voting, healthcare, and many others.

CONCLUSION

Blockchain is a promising technology and is highly appreciated and accepted for its decentralized infrastructure and peer-to-peer nature. Blockchain has demonstrated its potential for facilitating complex processes such as transaction verification and digital currency through its design features.

Blockchains are tamper-evident and tamper-resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. The use of blockchain technology is still in its early stages, but it is built on widely understood and sound cryptographic principles.

Besides, blockchain can transform traditional business with its vital characteristics, including distribution, anonymity, immutability, and audibility. As blockchain was designed to eliminate intermediaries' roles, particularly in the financial transaction space, it employs a decentralized consensus protocol for transaction processing and validation. Thus, it holds great promise to transform centuries-old business models, paving the way for higher levels of legitimacy and security.

Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA) are the most commonly used consensus mechanisms by the existing blockchain systems. Consensus mechanisms are protocols or algorithms used on blockchain that determine the validity of transactions. Blockchain was introduced as a decentralized public ledger, but depending on the use and requirements, blockchains can be categorized into four types, public, private, consortium (also known as federated), and hybrid blockchains. Each of these blockchain networks serves its purpose and solves particular problems, and each blockchain has its own set of features and advantages over one another.

Thus, Blockchain technology, though still in its infancy, carries the promise to be the next big thing after the Internet, with its applications as wide as one’s imagination. However, with its social, political, and economic implications still unknown, the technology must be welcomed with caution.

REFERENCE

Adam Levy. (Jul 13, 2022). **15 Applications for Blockchain Technology**. https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/blockchain-applications/

Aniket Mahanti, Wajde Baiod and Wajde Baiod. "Blockchain Technology and its Applications Across Multiple Domains: A Survey" in Journal of International Technology and Information Management, Volume 29, Issue 4, Article 4 ,CSUSB ScholarWorks, 2021.

Antony Lewis. (2018).*The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT).* Mango publication press.

ANUBHAW SUMAN, Madhu Patel, "An Introduction to Blockchain Technology and Its Application in Libraries" in Library Philosophy and Practice (e-journal), pp 1 - 8, University of Nebraska - Lincoln, Winter 2021.

Bernard Marr. (2021). **A Very Brief History Of Blockchain Technology Everyone Should Read**. https://bernardmarr.com/a-very-brief-history-of-blockchain-technology-everyone-should-read/ [December 20, 2022].

Brooke Becher. (September 29, 2022). **What Are Blockchain Nodes and How Do They Work?.** https://builtin.com/blockchain/blockchain-node [January 2, 2023].

crypto.com.(May 13, 2022). **Consensus Mechanisms in Blockchain: A Beginner's Guide**. https://crypto.com/university/consensus-mechanisms-in-blockchain [January 10, 2023].

Diego Geroni. (February 02, 2021). **Blockchain For Beginners: Getting Started Guide.** https://101blockchains.com/blockchain-for-beginners/ [December 24, 2022].

Dylan Yaga,Nik Roby and Karen Scarfone. "Blockchain Technology Overview" in National Institute of Standards and Technology, Internal Report 8202,October 2018. Available: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf

Eric Rosenberg. (September 15, 2022). **What Is a Consensus Mechanism**?. https://www.thebalancemoney.com/what-is-a-consensus-mechanism-5211399#:~:text=Consensus%20mechanisms%20are%20the%20protocols,and%20governance%20of%20the%20blockchain. [January 10 2023].

GeeksforGeeks. (January 23, 2023). **Introduction to Blockchain technology | Set 1**. https://www.geeksforgeeks.org/blockchain-technology-introduction/ [January 25, 2023].

GeeksforGeeks. (May 11, 2022). **Top Applications of Blockchain in the Real World**. https://www.geeksforgeeks.org/top-applications-of-blockchain-in-the-real-world/ [January 25, 2023].

Gwyneth Iredale. (2021). **6 Key Blockchain Features You Need To Know Now**. https://101blockchains.com/introduction-to-blockchain-features/ [January 15, 2023].

Gwyneth Iredale. (November 03, 2020). **History Of Blockchain Technology: A Detailed Guide**. https://101blockchains.com/history-of-blockchain-timeline/ [December 20, 2022].

Insider Intelligence. (January 24, 2023). **The growing list of applications and use cases of blockchain technology in business and life**. https://www.insiderintelligence.com/insights/blockchain-technology-applications-use-cases/

JavaTPoint. (2021). **History of Blockchain**. https://www.javatpoint.com/history-of-blockchain [December 20, 2022].

MLSDev. (May 7, 2019). **Blockchain Architecture Basics: Components, Structure, Benefits & Creation**. https://mlsdev.medium.com/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77 [January 10, 2023].

Paul Vigna and Michael J. Case. (2018). *The Truth Machine: The Blockchain and the Future of Everything*. St. Martin's Press.

Rahul Awati. (August, 2022). **Consensus Algorithm**. https://www.techtarget.com/whatis/definition/consensus-algorithm#:~:text=Blockchain%20networks%20rely%20on%20consensus,users%20from%20validating%20bad%20transactions. [January 10, 2023].

Ravi Kumar Mathur.(2021). Introduction to Blockchain Technology, National Telecommunications Institute For Policy Research, Innovation & Training. Available:https://ntiprit.gov.in/pdf/blockchainanddistributed/Blockchain_Introduction_KR.pdf

Robert Sheldon. (August 09, 2021). A timeline and history of blockchain technology. A timeline and history of blockchain technology (techtarget.com) [December 20, 2022].

Roshan Raj. (December 20, 2022). **Blockchain Use Cases**. https://intellipaat.com/blog/tutorial/blockchain-tutorial/blockchain-use-cases/ [January 25, 2023].

Roshan Raj. (December 29, 2022**). How does Blockchain Work?.** https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/ [January 5 2023].

Shardeum Content Team. (September 14, 2022). **A Guide on the 10 Types of Blockchain Nodes.** https://shardeum.org/blog/types-of-nodes-in-blockchain/#What_is_the_Purpose_of_Blockchain_Nodes [January 5, 2023].

Software Testing Help. (January 21, 2023). **Blockchain Applications: What Is Blockchain Used For?**. https://www.softwaretestinghelp.com/blockchain-application-

examples/#:~:text=Blockchain%20is%20being%20implemented%20in,security%20token%20offering%2C%20and%20notary. [January 25, 2023].

Svetlana Cherednichenko. (November 10, 2020). **Designing a Blockchain Architecture: Types, Use Cases, and Challenges**. https://medium.com/mobindustry/designing-a-blockchain-architecture-types-use-cases-and-challenges-9894fb7b58e [January 10, 2023].

Swasti Gupta. (2018). **Introduction to Blockchain Technology. CUTS International**. https://cuts-ccier.org/pdf/Briefing_Paper-Introduction_to_Blockchain_Technology.pdf [January 10, 2023].

Tapscott Don and Tapscott Alex, "How Blockchain will Change Organizations" in MIT Sloan Management Review, Volume 58, Issue 2, pp 10 - 13, Cambridge, Winter 2017.

Tiana Laurence. (2017). *Introduction to blockchain: The many faces of blockchain technology in the 21st century*. Van Haren Publishing.

Vinay Gupta. (February 28, 2017) .**A Brief History of Blockchain**. https://hbr.org/2017/02/a-brief-history-of-blockchain [December 25, 2022].