

ADDIS ABABA UNIVERISITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE  
 DEPARTMENT OF COMPUTER SCIENCE

BLOCKCHAIN TECHNOLOGY

CoSc4411\_: TECHNICAL REPORT WRITING

BY

|  |  |
| --- | --- |
| **NAME OF STUDENT** | **ID** |

NAHOM TESFAYE ………………………………………………….UGR/1797/12

SOLOMON ASHAGRE ……………………………………………..UGR/5156/12

YOHANNES FIKIRE …………………………………………………UGR/5191/12

TADESSE TSEGA …………..................................................................UGR/7317/12

PROJECT ADVISOR: Mrs. FIKIRTE G.

Feb 2023

# Declaration

This is to declare that this report is done under the supervision of Mrs. FIKIRTE G and having the title “block-chain technology” is the sole contribution of

1. NAHOM TESFAYE

2. SOLOMON ASHAGRE

3. YOHANNES FIKIRE

4. TADESSE TSEGA

No part of the report work has been reproduced illegally (Copy and Paste) which can be considered as plagiarism.

We will be responsible and liable for any consequence if violation of this declaration is proven.

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Group Members

Full Name Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 

# Certificate

I certify that this technical report document entitled “Blockchain technology” by:

1. NAHOM TESFAYE

2. SOLOMON ASHAGRE

3. YOHANNES FIKIRE

4. TADESSE TSEGA

is approved by me for submission. I certify further that, to the best of my knowledge, the report represents work carried out by the students.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Name and Signature

# Acknowledgment

First and foremost we would like to thank the Almighty God for the completion of this report document. We would like to express our sincere gratitude to all those who have supported us throughout the accomplishment of this report paper.

We would like to thank our Report advisor Mrs. Fikirte G, whose guidance and support were invaluable throughout this Report writing. She provided us with insightful feedback, critical advice and helped us stay focused on the main objectives of the technical report.

We would like to extend our appreciation to our family and friends for their unwavering support and encouragement. Their moral support was crucial in keeping us motivated and focused throughout the project.

We would also like to thank our fellow students for their helpful comments, feedback, and suggestions that have improved the quality of our work.

Contents

[Declaration i](#_Toc127793613)

[Certificate ii](#_Toc127793614)

[Acknowledgment iii](#_Toc127793615)

[1. INTRODUCTION 1](#_Toc127793616)

[2. Objective 3](#_Toc127793617)

[3. WORKING 3](#_Toc127793618)

[3.1. WORKING 3](#_Toc127793619)

[3.1.1. Blocks 3](#_Toc127793620)

[3.1.2. Miners 4](#_Toc127793621)

[3.1.3. Nodes 4](#_Toc127793622)

[4. TYPES OF BLOCKCHNAINS 6](#_Toc127793623)

[4.1. PUBLIC BLOCKCHAIN 6](#_Toc127793624)

[4.2. PRIVATE BLOCKCHAIN 8](#_Toc127793625)

[4.3. CONSORTIUM (FEDERATED) BLOCKCHAIN 9](#_Toc127793626)

[4.4. HYBRID BLOCKCHAIN 11](#_Toc127793627)

[5. ADVANTAGES of block-chain 12](#_Toc127793628)

[6. Drawback of blockchain 12](#_Toc127793629)

[7. APPLICATIONS 14](#_Toc127793630)

[8. CONCLUSION 17](#_Toc127793631)

[8.1. CONCLUSION 17](#_Toc127793632)

[8.2. THE FUTURE OF BLOCKCHAIN 18](#_Toc127793633)

[9. REFERENCES 19](#_Toc127793634)

**LIST OF FIGURES**

[Figure 1 Block-chain technology 1](#_Toc127789372)

[Figure 2 operation of block-chain 5](#_Toc127789373)

[Figure 3 public block-chain technology 6](#_Toc127789374)

[Figure 4 private block-chain technology 8](#_Toc127789375)

[Figure 5 consortium block-chain 10](#_Toc127789376)

[Figure 6 Hybrid block-chain technology 11](#_Toc127789377)

[Figure 7 application of block-chain technology 14](#_Toc127789378)

[Figure 8 Future of block-chain technology 18](#_Toc127789379)

**ABSTRACT**

The real-world use cases of blockchain technology, such as faster cross-border payments in economics, identity management, smart contracts, cryptocurrencies, and supply chain–blockchain technology are here to stay and have become the next innovation, just like as the Internet. In this paper, we will see the attempts to formulate digital money, but they have not been successful due to security and trust issues. However, blockchain needs no central authority, and its operations are controlled by the people who use it. Furthermore, it cannot be altered or forged, resulting in massive market hype and demand. Blockchain technology has gained a significant attention in recent years due to its potential to revolutionize the way we store and transfer data. This technical report provides an overview of Blockchain technology including its underlying principles, architecture, and key components. In this paper, we review the basics of Blockchain, its background history, types, advantages and drawbacks, applications of Blockchain, and working of Blockchain. Blockchain has moved past cryptocurrency and discovered implementations in other real life applications; this is where we can expect blockchain technology to be simplified and not remain a complex concept. We first conduct a thorough analysis of blockchain technology in this paper, paying particular attention to its evolution, applications and benefits. This paper presents a detailed review of blockchain technology, its applications in different fields. Blockchain in the transaction system is explained in detail with a summary of different cryptocurrencies. Some of the suggested solutions are given in the overall study of the paper.

# INTRODUCTION

Blockchains are tamper evident and temper resistant digital ledger implemented in a distributed pattern (i.e., without a central repository) and usually without a central authority (i.e., bank company or government) [1]. At their basic level, they enable a community of users to record transactions in in a shared ledger within that community. Such that under normal operation of the blockchain network no transaction can be changed once published. The data is recorded in a public ledger, including information of every transaction ever completed [2]. The information about every transaction ever completed in Blockchain is shared and available to all nodes.[2]. This attribute makes the system more transparent than centralized transactions involving a third party. In addition, the nodes in Blockchain are all anonymous, which makes it more secure for other nodes to confirm the transactions. Bitcoin was the first application that introduced Blockchain technology. Bitcoin created a decentralized environment for cryptocurrency, where the participants can buy and exchange goods with digital money.[2]. Since each activity in the system is visible and auditable by all members, thus this type of decentralized system creates the foundation of trust.[3]. Bitcoin is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one since it helps to enable a multibillion-dollar global market of anonymous transactions without any governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions

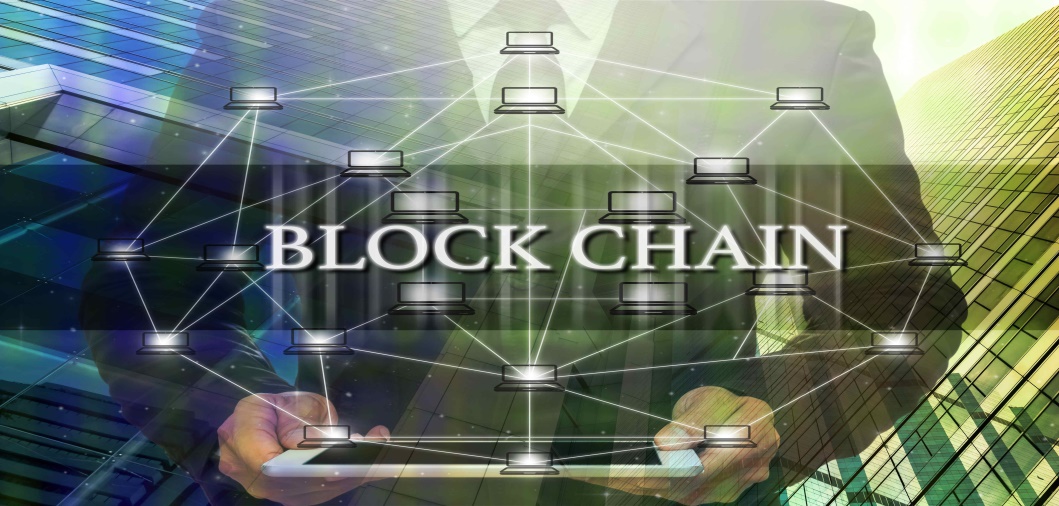


Figure Block-chain technology

Current digital economy is based on the reliance on a certain trusted authority. All online transactions rely on trusting someone to tell us the truth— it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains that these third-party sources can be hacked, manipulated or compromised.

This is where the blockchain technology comes handy. It has the potential to revolutionize the digital world by enabling a distributed consensus where each and every online transaction involving digital assets, past and present, can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The distributed consensus and anonymity are two important characteristics of blockchain technology.[6]

* 1. **Background and history**

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The PartTime Parliament [11] to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed [3]. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer-to-Peer Electronic Cash System [4], which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network. Nakamoto’s paper contained the blueprint that most modern cryptocurrency schemes follow (although with variations and modifications).

The author **Satoshi Nakamoto** is however presumed to be a pseudonym for what is yet an unidentified person or persons. It is known that Nakamoto was responsible for creating the majority of the official bitcoin software and was active in making modifications and posting technical information on the official bitcoin forums. However, the true identify is still unknown. Probably made because the bitcoin creators were afraid of convictions and trials,especially in USA. Since the U.S. Mint had informed in 2006 that the circulation of medallions such as the Liberty Dollar as legal tender, is considered a federal crime and they had also seized a large amount of liberty dollars in 2007 as well as made formal criminal charges against its inventor Bernard von NotHaus in 2009.Meaning that the bitcoin inventors could easily face similar threats.

## Objective

1. **General Objective**

This study is limited to the discussion on possible innovations in different sectors especially healthcare services using block-chain technology. The main objectives are:

(1) To learn blockchain technology as distributed ledger tool and its potential capabilities across industries,

(2) To find out the current status and potential usage of blockchain technology in the healthcare industry sector based on a systematic review,

(3) To predict the possible innovations in the healthcare sector using blockchain technology,

(4) To identify the opportunities and challenges of blockchain technology in various areas of healthcare service and stages of its implementation,

(5) To develop and analyses research agendas by identifying the research gap on the use of block chain technology in the healthcare industry.

1. **Specific Objective**

The specific objective of writing a report on block-chain technology is to provide an overview of the technology, its uses and applications, and its potential impact on health sector. The report may also discuss the challenges and limitations of block-chain technology, as well as its future-work. Additionally, the report can be used to explore the various block-chain platforms and technologies that exist and their relative strengths and weaknesses. Overall, the goal of writing a report on block-chain technology is to educate and inform the reader about blockchain.

# WORKING

## WORKING

The whole chain of block-chain is to let people – in particular, people who don’t trust one another – share valuable in a secure, tamperproof way. Block-chain consists of three important concepts: blocks, nodes, miners.

### Blocks

Every chain consists of multiple blocks and each block has three basic elements:

* The data in the block.
* A 32-bit whole number called a nonce. The nonce is randomly generated when a block is created, which then generates a block header hash.
* The hash is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates a cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

### Miners

Miners create new blocks on the chain through a process called mining. In a block-chain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block is not easy, especially on large chains. Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256 bits, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens miners said to have found the “golden nonce” and their block is added to the chain.

Making a change to any block earlier in the chain requires re-mining not just the block with the change, but the entire block that come after. This is why it’s extremely difficult to manipulate block-chain technology. Think of it is as “as safety in math” since finding golden nonce requires an enormous amount of time and computing power. When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially.

### Nodes

One of the most important concepts in block-chain technology is decentralization. No one computer or organization can own the chain. Instead, it’s a distributed ledger via the nodes connected to the chain. Nodes can be any kind of electronics device that maintains copies of the block-chain and keeps the network functioning.

Every node has its own copy of the block-chain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified. Since block-chains are transparent, every action in the ledger can be easily checked and viewed. Each participant is given a unique alphanumeric identification number that shows their transactions.

Combining public information with a system of checks- and-balances help the block-chain maintains integrity and creates trust among users. Essentially, block-chains can be thought of as the scalability of trust via technology.

Another major advantage of the block-chain technology is that it is decentralized. It is decentralized in the sense that:

* There is no single device that stores the data (transaction and associated blocks); rather they are distributed among the participants throughout the network supporting the block-chain.
* The transactions are not subject to approval of any single authority or have to abide by a set of specific rules, thus involving substantial trust as to reach a consensus.
* The overall security of a block-chain eco-system is another advantage. The system only allows new block to be appended. Since the previous blocks are public and distributed, they cannot be altered or revised.

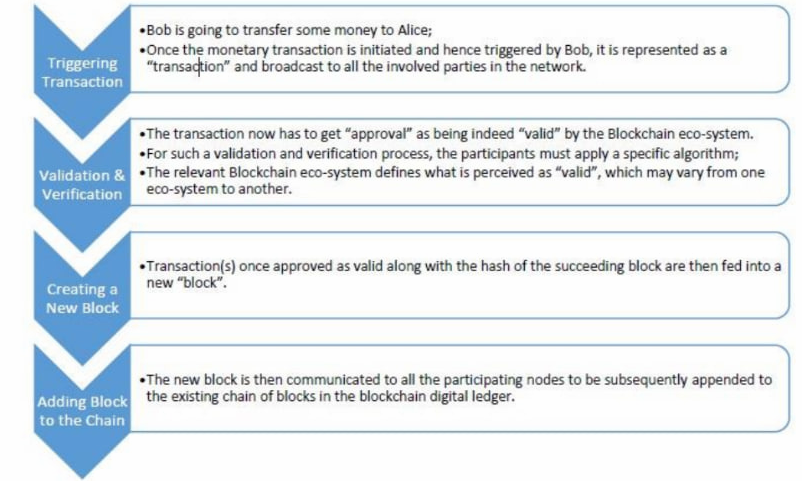


Figure operation of block-chain

For anew transaction to be added to the existing chain, it has to be validated by all the participants of the relevant block-chain eco-system. For such a validation and verification process, the participant must apply a specific algorithm. The relevant block-chain eco-system defines what is perceived as “valid”, which may vary from one eco-system to another. A number of transactions, thus approved by the validation and verification process, are bundled together in a block. The newly prepared block is then communicated to all other participating nodes to be appended to the existing chain of blocks. Each succeeding block comprises a hash, a unique digital finger print, of the preceding one.

Fig 2.2 demonstrates how block-chain transaction takes place, using a step-by-step example. Bob is going to transfer some money to Alice. Once the monetary transaction is initiated and hence triggered by Bob, it is represented as a “transaction” and broadcast to all the involved parties in the networks. The transaction now has to get “approval” as being indeed “valid” by the block-chain eco-system. Transaction(s) once approved as valid along with the hash of the succeeding blocks are then fed in to a new “block” and communicated to all the participating nodes to be subsequently appended to the existing chain of blocks in the block-chain digital ledger.

# TYPES OF BLOCKCHNAINS

At a glance there are four different types of block-chain technologies. They include the following.

* Public
* Private
* Hybrid
* Federated

## PUBLIC BLOCKCHAIN

Is a major type of Blockchain, and that is not only open but also decentralized in nature. And in this type of Blockchain technology computer networks are basically accessible to anyone interested in transaction. Here based on validated person basically receives the transaction rewards and furthermore, two kinds of proof of works and proof-of-stake models are being used.[14]

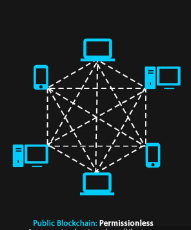


Figure 3 public block-chain technology

It is also called a permission less blockchain.Bitcoin is the best example describing permission less blockchain. There is no restriction as to who can use it. Any person can access wallet, process a transaction, run a node, mining software as long as they obey the rules of the blockchain.these types of blockchain are open and transparent anyone can review it at any instant of time.[15].

The verification of the transaction is done through consensus methods such as Proof-of-Work (PoW), Proof-of-Stack (PoS), and so on. At the core the participant nodes require to do the heavy-lifting including validating transactions to make the public block-chains work. If a public block-chain doesn’t have the required peers participating in solving transactions, then it will be non-functional. There are also different types of block-chain platforms that use this various types of block-chain as the base of their project. However, each platform introduces more features in its platform aside from the usual ones.

**Example of Public Block-chain**: Bitcoin, Ethereum, Litecoin, NEO.[15]

**Advantages**:

Public block-chains are good at what they do. Its advantages include the following.

* Anyone can join the public block-chain.
* Trustable: for participating node there is no need of knowing and trusting each other because the proof-of-work procedure no fraudulent transaction.[14]
* Secure: a public network can have as many nodes as it needs and wants, making the system difficult for the hackers to hack the entire network. The more number of participants there, the more secure it is.[14]
* Transparent: the data is transparent and open to all member nodes. Every node has a copy of the blockchain records[14]
* Anonymous Nature.[16]
* No regulations and strict policies[16]
* Distributed[16]

Though there are plenty of advantages, there is some disadvantages or drawbacks.

**Disadvantages:**

* They suffer from a lack of transaction speed and It can take a few minutes to hours before a transaction is completed. For instance, bitcoin can only manage seven transaction per second compared to 24,000transactions per second done by VISA.[16] This is because it takes time to solve the mathematical problems and then complete the transaction.
* Another problem with public block-chain is scalability. They simply cannot scale due to how they work. The more nodes join, the clumsier, and slow the network becomes. There are steps taken to solve the problem. For Example, Bitcoin is working on lighting the network, which takes the transactions off-chain to make the main bitcoin network faster and more scalable. [16]
* Due to the proof of work energy consumption public blockchain highly suffers from higher energy consumption. [16]

**Use cases:**

There are multiple use-cases of the block-chain. To get a better idea, let’s list some of them below.

* **Project ubin:** a collaborative project of the Singapore government. It uses Ethereum for clearing and processing of payment[17]
* **We.trade:** it’s a built on IBM platform of blockchain using Hyperledger fabric. It gives a service of simple user interface for banks’ users[17]

## PRIVATE BLOCKCHAIN

Are restricted and not open, this type of blockchain also has features of access. Permission is allowed for the transaction from the system administrator[11] It is also a permissioned block-chain that is under the control of an entity.



Figure 4 private block-chain technology

They are closed blockchain where any one can’t join the blockchain network.[12] they need some sort of permissions. there is a central authority which might be private individual or an organization who looks after the permissions [12]. The organization can also set different parameters to the network, including accessibility authorization, and so on! So, how is it different from public block-chain? It is different in the way it is accessed. Otherwise, it offers the same set of features as that of the public block-chain, providing transparency, trust, and security to the selected participants.

Another major difference is that it’s kind of centralized as only one authority looks over the network. So, it doesn’t have a decentralized theoretical nature. There are also various types of block-chain platforms that use private block-chain as the base of their platform. More so, each one of them tends to be unique and offer a different features. In many cases, a private block-chain is considered permissioned block-chain. But the concept of permissioned block-chain is much broader as it can include public block-chain as well.

**Example of private block-chain:** Multichain, Hayperledger Fabric, Hayperledger sawtooth, corda

**Advantages:**

* Speed and velocity. The TPC(transaction per second) is greater than a public blockchain i.e. greater speed than public blockchain.[11]
* Private block-chains are more scalable. The scalability is possible because, in a private block-chain, lonely a few nodes are authorized to validate transactions. This means it doesn’t matter if the network grows; the private block-chain will work as its previous speed and efficiency. The key here is the centralization aspects of decision making.[11]

**Disadvantages:**

* Private block-chains are not truly decentralized. This is the biggest disadvantages of private block-chain and goes against the core philosophy of distributed ledger technology or block-chain in general.[11]
* Achieving trust within the private block-chain is tough because the centralized nodes make the last call.[11]
* Lastly, as there are only a few nodes here, the security isn’t all that good. It’s important to understand that it is possible to lose security if a certain number of nodes go rogue and compromise the consensus method utilized by the private network.[11]

**Use cases:**

There are multiple private block-chains use-cases. Some of them are listed below.

* **Supply chain management:** Organization can deploy a private block-chain to manage their supply chain.
* **Asset ownership:** Assets can be tracked and verified using a private block-chain.
* **Internal voting:** private block-chain is also effective at internal voting.

## CONSORTIUM (FEDERATED) BLOCKCHAIN

A consortium block-chain is one of the difference types of block chain technology. Its permissioned blockchain. Unlike private blockchain its ruled by more than one organization[15]. It excersises a higher decentralization resulting in higher levels of security.[15] In a consortium block-chain, some aspects of the organizations are made public, while other remains private. The consensus procedures in a consortium block-chain are controlled by the preset nodes. More so, even though it’s not open to mass people, it still holds a decentralized nature[16]. How? Well, a consortium block-chain is managed by more than one organization[16]. So, there is no one single force of centralized outcome here.are being used in areas such as banks, government organizations etc.[16]

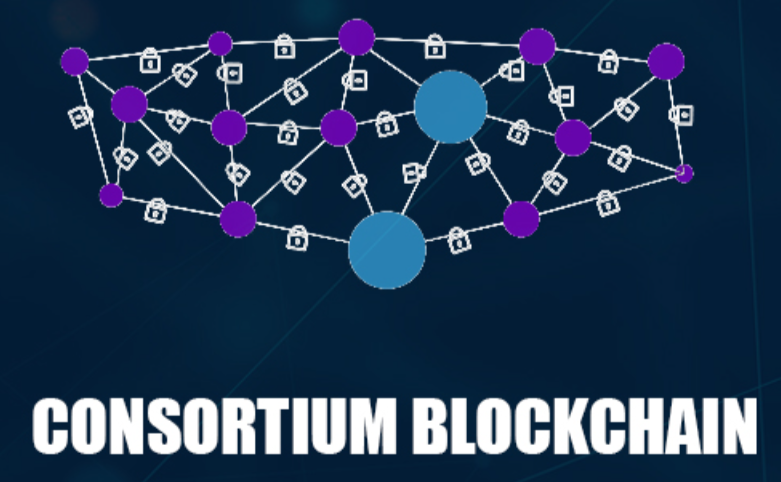


Figure 5 consortium block-chain

To ensure proper functionality, the consortium has a validator node that can do two functions, validate transactions, and also initiate or receive transactions. In comparison, the member node can receive or initiate transactions.

In short, it offers all the features of a private block-chain, including transparency, privacy, and efficiency, without one party having consolidating power.

**Example of consortium Block-chain:** Marco polo, Energy Web Foundation, IBM Food Trust.

**Advantages:**

* It offers better customizability and control over resources.
* Consortium block-chains are more secure and have better scalability.
* It is also more efficient compared to public block-chain networks.
* Works with well-defined governance structures.
* It offers access controls.

**Disadvantage:**

* Even though it is secure, the whole network can be compromised due to the members’ integrity.
* It is less transparent.
* Regulations and censorship can have a huge impact on network functionality.
* It is also less anonymous compared to other types of block-chain.

**Use Cases:**

There are multiple use-cases of consortium block-chain. Some of them include the following

* **Banking and payments:** A group of banks can work together and create a consortium. They can decide the nodes that will validate transactions.
* **Research:** A consortium block-chain can be used to share research data and results.
* **Food tracking:** it is also great for food tracking.

## HYBRID BLOCKCHAIN

Hybrid block-chain is one of the difference types of block-chain technology. More so, hybrid block-chain is the last types of block-chain that we are going to discuss here. More so, hybrid block-chain might sound like a consortium block-chain, but it is not. However, there can be some similarities between them.

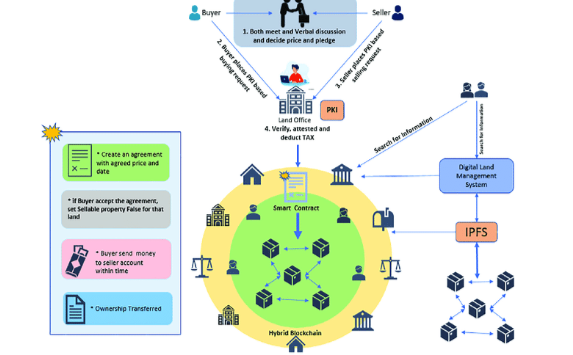


Figure Hybrid block-chain technology

Hybrid block-chain is best defined as a combination of a private and public block-chain. It has use-cases in an organization that neither wants to deploy a private block-chain nor public block-chain nor simply wants to deploy both worlds ‘best.

**Example of Hybrid Block-chain:** Dragon-chain, XinFin’s Hybrid blockchain

**Advantages:**

* Works in a closed ecosystem without the need to make everything public.
* Rules can be changed according to the needs.
* Hybrid networks are also immune to 51% attacks.
* It offers privacy while still connected with a public network.
* It offers good scalability compared to the public network.

**Disadvantages:**

* Not completely transparent.
* Upgrading to the hybrid block-chain can be challenge.
* There is no incentive for participating and contributing to the network.

**Use Cases:**

Some of the best use-cases of the hybrid block-chain are as follows:

* **Real estate:** you can use hybrid networks for real-estate purposes where real-estate companies can use it to run their systems and use the public to show information to the public.
* **Retail:** Retail can also use the hybrid network to streamline processes.
* **Highly regulated markets:** hybrid block-chains are also ideal for highly regulated markets such as financial markets.

# ADVANTAGES of block-chain

The main benefit of this technology is that blockchain is decentralized technology. We don’t need any third party or organization or central administrator for transaction[12]. All participants of this blockchain make the decisions because the system works without intermediary. If the not use blockchain database is needed and it is important to keep this database, because there is a higher risk of hacking and the data may turn up in the wrong hands. The process of the database security might take a lot of time and money. If use blockchain technology can be avoided, because the transaction has its own proof of validity and authorization.[18]

Blockchain technology immutable because it’s impossible to erase or replace recorded data. This make the blockchain prevents tampering of data in the network.[19]. Each action is tracked and recorded to the blockchain and every participant has access. Generally the above properties make blockchain transparency, immutability and trusty.[18]

Because of the absence of control on any single party, blockchain technology is free from censorship. Therefore, there is no interruption by single authority including government. Blockchain creates irreversible audit trial, making tracing and changes easy [19].

# Drawback of blockchain

Of course, every system has both merits and drawbacks Block-chain technology to for an industry has the following drawbacks:

The main drawbacks of the block chain are the high energy consumption. For a real time ledger the consumption of power is needed. When a new node is created then at the same time it communicates with other node. In this way the transparency is created. The miners are trying to solve a lot of solutions per seconds to validate the given transactions. In this time they use a certain amount of computer power.[18]

Blockchain is only a few years age technology so people do not have much confidence in it. Despite its current applications on various industries still it needs to win the confidence of the users to be ratified for its complete utilization.

The other drawback is its time consuming. Because to add the next block in the chain miners need to compute many times this makes it time consuming. Block-chains especially those using proof of work are inefficient because of the highly competitive nature of mining. In mining there is just one winner every ten minutes, in this time the work of every other miner is wasted. the other drawback is legal formality. In most part of the world. Money is centralized and controlled by government and banks so it becomes difficult for bitcoin to get accepted by the preexisting institutions.[20]

There are also some other drawbacks to consider. Here are a few potential drawbacks:

Scalability: One of the biggest challenges with blockchain technology is its scalability. As more transactions are added to a blockchain, it can become slower and more expensive to use. This can be a particular issue for public blockchains like Bitcoin and Ethereum, which have limited transaction processing capabilities.[12]

Lack of regulation: Because blockchain technology is relatively new, there is still a lack of regulation in many areas. This can create uncertainty and risk for businesses and individuals who want to use blockchain-based systems.[6]

Irreversibility of transactions: Once a transaction has been recorded on a blockchain, it cannot be reversed or altered. While this can be seen as a positive feature for security and trust, it can also be a drawback in situations where errors or fraud occur.[12]

Limited interoperability: There are many different blockchain systems and protocols, and they are not always compatible with one another. This can create difficulties when trying to integrate different block chain systems or use them together [12].

# APPLICATIONS

Block-chain technology can be applied to a variety of different applications in the industry, such as simplifying and streamlining supply chain management, increasing the security and efficiency of financial transactions, increasing data security and privacy, and reducing time and cost of transactions. Block-chain technology also has potential applications in healthcare, government, real estate, and education. Block-chain based solutions enable secure and immutable transactions of assets and data that are uncorrupted, cost effective, and real time. These solutions can be used to securely store medical records, prevent fraud and corruption in government-run programs, and offer a secure, traceable method of validating real estate ownership and educational credentials.

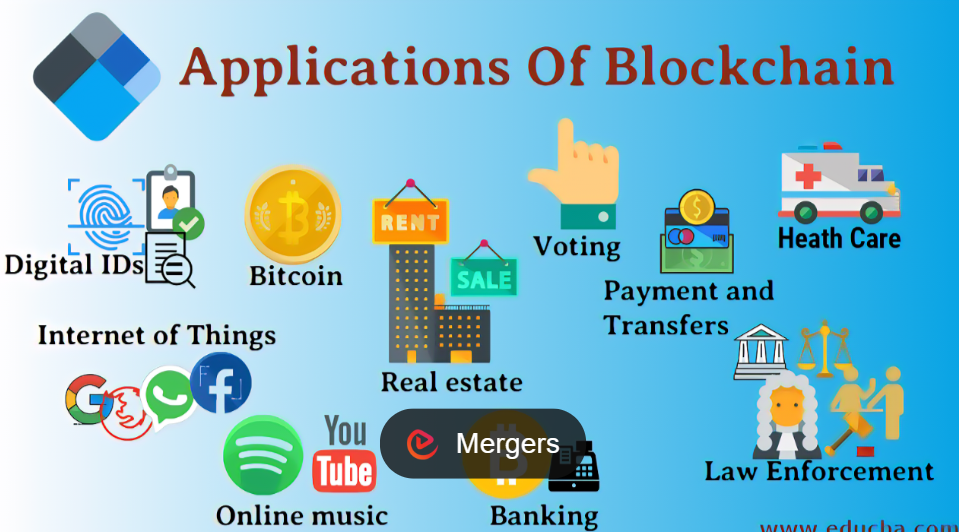
****

Figure application of block-chain technology

Block-chain technology has a variety of potential applications in various industries. Here are some of the most promising applications of block-chain technology:

1. **Payment and Transfer**: Block-chain technology has enabled individuals and businesses to transfer money and other digital assets securely and cost effectively. The emergence of cryptocurrency and smart contracts has created new possibilities for transferring value without intermediaries.

*Banking and Financial services:*

Block-chain technology has revolutionized the way financial institutions and banks manage transactions. It has made financial operations more secure, faster and more efficient by eliminating the need for intermediaries and reducing costs.

*Supply Chain Management:*

Block-chain technology has enabled companies to monitor their supply chains in real time and maintain digital records for goods and products. This provides visibility and transparency into the sustainability of products and the efficiency of the supply chain.[11]

*Cybersecurity:*

With its decentralized and distributed architecture, block-chain technology can be used to create secure digital identities that can be used for authentication purposes and to protect digital assets from malicious activities.[1]

*Government:*

Governments around the world are exploring block-chain technology to improve the efficiency and accountability of their public services. From digital identity to digital voting, block-chain technology can be used to make government operations more transparent and secure.

*To the Internet of Things*

Block-chain technology is being increasingly used as a secure way to store and transfer data between devices in the Internet of Things (IoT). By leveraging the near-instant security and data immutability that this technology provides, companies are able to create secure and reliable networks of connected devices with low cost and time.[6]

Block-chain enables the Internet of Things to become more secure, efficient, and reliable. It can provide a secure and decentralized way of storing and transferring data between multiple devices. This data can include anything from energy data and health data to digital asset information and financial transactions. Furthermore, linking various IoT devices together with block-chain makes it much easier to establish trust between multiple parties.[10]

Furthermore, decentralization of data allows for faster responsiveness, faster to accurate decisions, and increased security over shared resources. The result is an improved user experience, with secure and efficient networks that can provide improved reliability, robustness, and scalability. The block-chain also allows for the development of intricate smart contracts, enabling secure and reliable transactions of data between two parties without the need for any third-party intermediary. Smart contracts can drastically reduce costs, increase efficiency and ensure that the terms and conditions of an agreement are enforced.[13]

*To the organization of online data*

Block-chain technology can be used to organize online data in several ways. First, it can be used to store and protect data securely. This could be used for crucial customer data or intellectual property that needs to be kept safe and secure. Block-chain-based databases can also provide secure sharing of data, allowing documents and information to be accessed and shared by multiple parties. It can also be used to verify a user's data, whether it is personal or financial information. Additionally, it can be used to create digital contracts, such as smart contracts, which are ratified and enforced by each party's signature. Finally, block-chain can also be used to provide a more efficient way to securely transfer data between parties.[6]

Block-chain technology can be used to ensure that the ownership and transfer of a digital asset is tracked, secure and protected against fraud. This can be done through the use of a public ledger, or block-chain, which contains a record of each transaction that occurs related to the asset. By utilizing a distributed ledger system, multiple copies of the ledger are accessible to all parties and are updated in real time whenever a transaction takes place. This increases transparency, allowing all parties involved in the digital asset's ownership to easily keep track of and verify ownership. In addition, using smart contracts and cryptography, the transfer of an asset can be automated and securely verified, removing the risk of fraudulent activity or a financial dispute.[10]

# CONCLUSION

## CONCLUSION

The application of the block-chain concept and technology has grown beyond its use for Bitcoin generation and transactions. The properties of its security, privacy, traceability, inherent data provenance and time-stamping have seen its adoption beyond its initial application areas. The Block-chain itself and its variants are now used to secure any type of transactions, whether it be human-to-human communications or machine-to-machine. Its adoption appears to the secure especially with the global emergency of the Internet-of-Things. Its decentralized application across the already established global internet is also very appealing in terms of ensuring data redundancy and hence survivability. Thus the invention of the block-chain can be seen to be a vital and much needed additional component of the internet that was lacking in security and trust before.

Blockchain technology is a powerful tool that has the potential to transform the way we store and manage data [19]. Its decentralized and transparent nature allows for secure and efficient transactions, without the need for intermediaries [18]. By providing a tamper-proof and immutable ledger, blockchain technology can enhance trust and accountability in a variety of applications, ranging from finance and healthcare to supply chain management and voting systems. However, as with any emerging technology, there are also potential drawbacks and challenges that need to be addressed [16]. These include issues around scalability, energy consumption, regulation, transaction irreversibility, and interoperability. Nonetheless, the benefits of blockchain technology continue to attract interest and investment from businesses and governments around the world, and it is likely that we will see continued innovation and growth in this field in the coming years.

## THE FUTURE OF BLOCKCHAIN

The future of blockchain technology is exciting, and there are many potential applications and developments that we can expect to see in the coming years. Here are a few trends and predictions for the future of blockchain:

Interestingly, block-chain takes away the concerns of risks and costs involved in such transactions traditionally. Businesses could build block-chain networks with different approaches.



Figure Future of block-chain technology

Block-chain still remains in the region of “peak of Inflated Expression” with forecast to reach plateau in “five to ten years”. However, this technology is shown going downhill into the region of the “Trough of Disillusionment”. Because of the wide adoption of the block-chain in a wide range of application beyond cryptocurrency. Block-chain possesses a great potential in empowering the citizens of the developing countries if widely adopted by e-governance applications for identity management, asset ownership transfer of precious commodities such as gold, silver and diamond, healthcare and other commercial uses as well as in financial inclusion. However, this will strongly depend on national political decisions.

Mainstream adoption: As blockchain technology becomes more widely recognized and understood, we can expect to see increased adoption in a variety of industries. This could include everything from financial services and healthcare to logistics and energy management.

Interoperability and standardization: As more blockchain systems are developed, there will be a growing need for interoperability and standardization to ensure that different systems can work together seamlessly.

Scalability improvements: Scalability has been a major challenge for blockchain technology, but there are ongoing efforts to improve the performance of blockchain systems. These could include solutions like sharding, sidechains, and off-chain transactions.

Advances in privacy: While blockchain technology is inherently transparent, there are also efforts to enhance privacy and confidentiality through techniques like zero-knowledge proofs and homomorphic encryption.

Increased integration with other technologies: Blockchain technology is not an isolated technology, and we can expect to see increasing integration with other technologies such as artificial intelligence, the Internet of Things, and cloud computing.

Overall, the future of blockchain technology is bright, and we can expect to see continued innovation and growth in this field in the years to come. While there are still challenges to be addressed, the potential benefits of blockchain technology make it an exciting area to watch.

# REFERENCES

[1] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone, “Block-chain Technology Overview”, pp 1-4, National Institute of Standards and Technology Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology, October 2018.

[2] Lamport, Leslie. “The Part-Time Parliament.” ACM Transactions on Computer Systems, vol. 16, no. 2, Jan. 1998, pp. 133–169.

<https://dl.acm.org/citation.cfm?doid=279227.279229>.

[3] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

[4] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, pp 4-8, satoshin@gmx.com [www.bitcoin.org](http://www.bitcoin.org), April 1997.

[5] Cornelius C. Agbo \*, Qusay H. MahmoudORCID and J. Mikael Eklund, “Blockchain Technology in Healthcare: A Systematic Review”, pp 5-13, Ark Invest: New York, NY, USA, 2016

[5] Nermin Kişi, “Exploratory Research on the Use of Blockchain Technology in Recruitment”, pp13-19, Department of Management and Organization, Çaycuma Vocational School, Zonguldak Bülent Ecevit University, Zonguldak 67900, Turkey, August 2022

[6] P.K. Paul1\*, P.S. Aithal2, Ricardo Saavedra3 and Surajit Ghosh, “Blockchain Technology and its Types—A Short Review”, pp 192-195, December 2021, International Journal of Applied Science and Engineering.

[7] By Shyamli Jha, “The Complete Guide for Types of Blockchain!”, pp 1-5, Senior Research Analyst at Simplilearn ,Feb 17, 2023

[8] Kathleen E. Wegrzyn Eugenia Wang, “Types of Blockchain: Public, Private, or Something in Between”, pp 8-15, Manufacturing Industry Advisor Innovative Technology Insights Dashboard Insights, 19 August 2021.

[9] Bela Shrimali a, Hiren B. Patel b, “Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities”, Volume 34, Issue 9, Pages 6793-6807, The blockchain consensus layer and BFT, India, October 2022.

[10] A. Bahga, V. Madisetti, “The Advantages and Disadvantages of the Blockchain Technology”, Journal of Software Engineering and Applications, No. 9, pp. [36]533-546, 2016.

[11] J. Spasavski, P. Eklund, “Proof of Stake Blockchain: Performance and Scalability for Groupware Communications”. Conference paper, November 2012.

[12] Dataflair team, “Advantages and disadvantages of Blockchain Technology” [online]. 2018.

Available from: <https://data-flair.training/blogs/advantages-and-disadvantages-of-blockchain/>

[13] A. Bahga, V. Madisetti, “Internet of Things: A Hands-On Approach”, Atlanta, 2014 [3] A. Litviņenko, A. Āboltiņš, “Computationally Efficient Chaotic Spreading Sequence Selection for Asynchronous DS-CDMA”. Electrical, Control and Communication Engineering, vol.13, pp.75-80, 2017 [14] A. Songara, L. Chouhan, “Blockchain: A Decentralized Technique for Securing Internet of Things”. Conference paper, October 2017

[15] A. Shanti Bruyn, “Blockchain an introduction. Research paper”, 2017. Available from: https://beta.vu.nl/nl/Images/werkstuk-bruyn\_tcm235-862258.pdf [16] Ascribe, “Lock in attribution, securely share and trace where your digital work spreads.” [online]. Available from: https://www.ascribe.io/

[17] BitFury Group, “Proof of Stake versus Proof of work. White paper”, September 2015

[18] J. Garzik, BitFury Group, “Public versus Private Blockchains. Part 1: Permissioned Blockchains. White Paper”, October 2015

[19] J. Golosova, A. Romānovs, “Overview of the Blockchain Technology Cases”. In Proceedings of thr 59th Internetional Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), October 2021.

[20] J. Spasavski, P. Eklund, “Proof of Stake Blockchain: Performance and Scalability for Groupware Communications”. Conference paper, November 2017