



Blockchain Technology

Subhojit Mitra¹ and Rupa Saha²

Student, Department of Computer Application, Narula Institute of Technology, Kolkata, India¹

Assistant Professor, Department of Computer Application, Narula Institute of Technology, Kolkata, India².

Abstract: This paper discusses the basics of Blockchain technology with human needs. The need of blockchain is discussed here various times. The process by which it works is also discussed afterward. Then the security layers and levels are included and elaborated accordingly with examples. This new methodology was also appreciated worldwide and this is depicted here by company names. Company names and a few objects of this technology were considered as keywords in this paper.

Keywords: Hash, Block, Genesis Block, organization names.

I. INTRODUCTION

There are so many under-table transactions that happen today in the world. These transactions get stored in some databases which are not so reliable. The reason is we do not have access to that database and the admin can change the data anytime.

Therefore, we need a decentralized database in which several persons have authority to that. Changing and manipulating this database becomes near too impossible. This database is called Blockchain. It was invented in the 90s but implemented in the 2000s by a developer named **Satoshi Nakamoto**, who developed Bitcoin using blockchain.



Fig. 1 Technology Objects

II. HOW DOES IT WORK?

The blockchain consists of ledger book-like objects containing records known as **Blocks**. Bitcoin, stores transaction details and it stores the most important data is **“hash.”** Hash is like a fingerprint that is stored for each data which gets stored. Hash is a unique code that is generated for every block. Again, a record is stored in the blocks that are the hash of the previous block.

A hash of the current block is also stored on the next block in sequence. So, it forms a linked list-like chain by which we can track the history of blocks and records. The first block does not store the hash code of any previous block. This first block is known as Genesis Block.

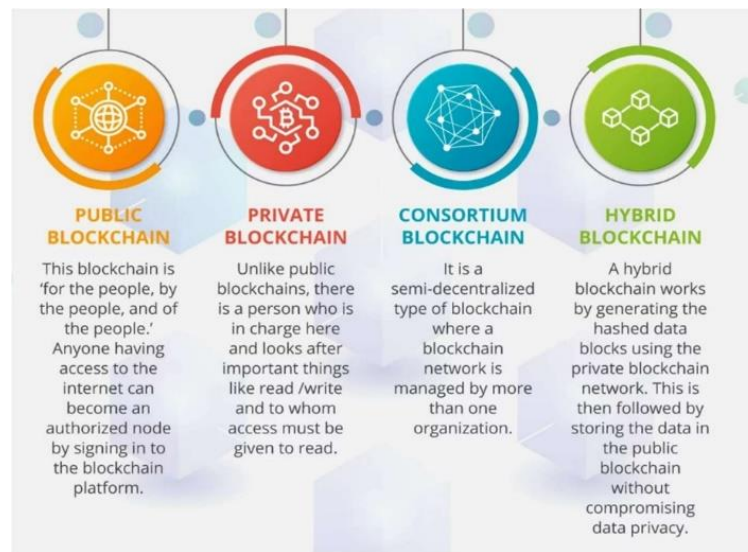


Fig. 2 Security level types

III. SECURITY LEVELS

There are four types of Blockchain networks based on security levels:

- 1) Public blockchains: Where anyone can perform the transaction is known as public blockchains. Here anyone can join for free and participate in their activities. Examples are **Bitcoin, Lit coin, and Ethereum** (the latest introduced in 2013).
- 2) Private blockchains: This blockchain network does not give authority to all users. It only gives access to a particular organization. And permits only some specified and uniquely identified members to perform activities. Examples: **Hyperledger, R3 Corda, Ripple.**
- 3) Consortium blockchains: It is a group of companies that jointly handles a Blockchain network. It helps to control and govern the network easily and certainly. Examples: **Multichain, Quorum, Hyperledger, Ethermint.**
- 4) Hybrid blockchains: This network is used by large organizations. They implement here, private, and public blockchains with the permission-enabled system. The most known example of that is **"IBM Food Trust or IBM Hybrid Blockchain."**

IV. WHY IS BLOCKCHAIN IS USED?

1. To increase security in a financial transaction.
2. To compact the database management system.
3. To give a good authorization of database management.
4. Blockchain works as a tool for the development and management (Not only cryptocurrency but other non-monetary objects as well).

Financial transaction safety was the main the cause of the development of blockchain technology. It was developed by adding some characteristics to database management. Therefore, blockchain works as a new tool for database management. Database security is increased by implementing proper authorization of that database. Through blockchain technology, database authorization is maintained by many few members. In addition, blockchain is a new tool to develop better database connections and software. Management also can be optimized by that technology.

V. DEBUT AS DECENTRALISED TECHNOLOGY

Blockchain tech is a decentralized management system. All other financial systems before this innovation were centralized. Decentralized networking is used in blockchain transaction distribution. In a centralized system, every participant in the network has to communicate with each other through a particular owner or authority. So, here dependency on that central owner is very crucial. On the other hand, decentralization works through multiple authorities that again work in a centralized manner individually. Here every individual participant can be the owner or authority. In this view, a famous quote works for blockchain i.e. "Everyone is an Owner; everyone has an owner."



Benefits of Decentralization:

- (i) It settles a trustless working environment. No one must trust anyone else for issues. Every participant in the network has a shallow copy of other's data as a "**Distributed Ledger.**" If corruption happens then that particular ledger is rejected.
- (ii) There are weak points in the network that can be reduced by using a decentralized environment. So, optimization gets increased.
- (iii) Catastrophic failure gets reduced by implementing resource distribution.
- (iv) Responsibility for security gets layered and shared through participants. So, the burden of work on security is reduced for individuals. Decentralization is considered an innovation therefore.

VI. DISTRIBUTED LEDGER TECHNOLOGY

Ledger is a collection of accounts that are used in financial transactions. Blockchain is a model of Distributed Ledger Technology (DLT). In that scenario, platforms are formed with many ledgers which are again separated among devices. So, this technology is as follows:

1. Ledgers are made with many accounts related to the transactions.
2. Ledgers are divided among devices and all the devices are connected through a network.

By the way, blockchain has few more characteristics than DLT. DLT is a tree and blockchain is the extension of that tree. DLT is a type of database that is shared, replicated, and synchronized through participants that are across the Globe. While blockchain is a chain of blocks that are used in transactions. DLT does not need any chain like used in blockchain. So, they are different. Blockchains are a type of DLT but DLT is not blockchain. All blockchains are DLTs but all DLTs are not blockchains.

VII. WHY BLOCKCHAIN IS UNHACKABLE?

We already talked earlier that Blockchain is made up of ledgers. The blockchain ledger is an upgraded version of the ledger that was previously we had. Every record that is written in the blockchain ledger has a unique key. This key is nearly unbackable based on cryptography and hash key formation. Another thing that happens on a blockchain is based on the network architecture and is very strong for security. Every record is written and stamped by the trusted party that wrote the very record. Again, an important thing happens so that privacy and security are maintained. i.e., when another record is written everything in the first record including the key and the contents of the second record is put into the formula and outcomes a key for the second record. So, there is a dependency between records that are created. Again, when the third record is created all contents and both keys of the first and second record are put into the formula and the key is formed, and so on. Therefore, a chain is formed and strong bonds between chains are created. Now, if someone wants to inspect and remove one record then its hash key will be changed and its successive record's hash key is also changed, and so on. Therefore, the chain and data will be destroyed and a blast of compactness will happen. Now if someone wants to change all hash keys then it will take a long time. Every person in the network has a copy of the whole blockchain. So, if anyone tries to change a copy the copy should be shared among all participants in the chain. Then, all the members must agree with your changing aspects. Only then, one can change the data of a record.

So, based on a network if hacking is performed to tamper with a record:

Trust between members will prevent this.

And if because of an algorithm, hacking is performed:

then, time management will be a problem and the chain will be blasted.

VIII. CONCEPTS AND COMPANIES BASED ON BLOCKCHAIN

NVIDIA, IBM, and PayPal are the major known companies that use blockchain. But all of them use this technology in different ways,

- NVIDIA uses this to get a revolution in the GPU industry. Bitcoin mining is a profitable business nowadays for many new entrepreneurs. But, using an old and weak CPU does not satisfy this need. To make a powerful memory and processing unit GPU is needed. Therefore, GPU companies have gained much revenue after the Bitcoin rise and blockchain implementation.
- IBM is known as a leading software development company and product-efficient organization. Blockchain technology requires ledger implementation. IBM has developed Hyperledger, which is a leading open-source ledger framework. This



helps to use blockchain finely by many individuals. So, IBM has caused blockchain to be a part of this big industrial revolution.

- PayPal is a financial transaction-based company. They prefer their users to use blockchain technology to transact with users and others. The implementation of blockchain in monetary transactions helped them to gain recognition. On the other hand, many other transaction-based companies have become partners with PayPal.

Concept to implement blockchain

Mainly C++ is used to implement blockchain technology. Many OOP concepts are needed to implement blockchain like run-time polymorphism, method overloading, and multithreading. These are obtained using object-oriented programming languages like C++, and Java. There are a few steps that are needed to follow for implementing blockchain technology. These steps are,

- Creating a block in a database and making a block class to add configuration and connections to that database object.
- Defining a blockchain to ensure authorized access and other network-based configuration.
- Making a connectable hash function to build security to blocks and connection to other records in the blocks.
- A proof of development method to get back against hackers.
- And finally, an API to build user interactivity and interface.

IX. FUTURE OF BLOCKCHAIN

Many government agencies and government transactions are not done using blockchain technology. In the future, the implementation of blockchain is needed for voting and government sector transactions. This will help in building a compact and corruption-free society. In addition, many companies will gain large profits from blockchain implementation and crypto mining. The share market and overall GDP will be increased after the implementation of blockchain. It is estimated that in future 20 years, business values using blockchain will be increased by 400 million dollars.

X. CONCLUSION

In the coming years, we can expect to see blockchain technology play a pivotal role in shaping the future of finance, governance, and data management. It has the potential to empower individuals, promote inclusivity, and enable new forms of collaboration and innovation. However, its success will depend on our collective ability to navigate the challenges ahead and leverage blockchain's capabilities responsibly and effectively.

In summary, blockchain technology represents a paradigm shift in the way we conceive and implement digital systems, offering the promise of a more secure, transparent, and decentralized future. It is an exciting journey that is only beginning, and its impact on our world will undoubtedly be profound.

REFERENCES

- [1]. Anita N. and Vijayalakshmi M. (2019). Blockchain security attack: A brief survey. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1-6, IEEE.
- [2]. Bodkhe U., Tanwar S., Parekh K., Khanpara P., Tyagi S., Kumar N. and Alazab M. (2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, 8, 79764- 79800.
- [3]. Irma D., Maemunah S., Zuhri S. and Juhandi N. (2021). The future of cryptocurrency legality in Indonesia. Journal of Economics and Business Letters, 1(1), 20-23.
- [4]. Nofer M., Gomber P., Hinz O. and Schiereck D. (2017). Blockchain. Business & Information Systems Engineering, 59, 183-187.
- [5]. Singhal B., Dhameja G., Panda P.S., Singhal B., Dhameja G. and Panda P.S. (2018). How blockchain works. Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, 31-148.
- [6]. Sunyaev A. and Sunyaev A. (2020). Distributed ledger technology. Internet computing: Principles of distributed systems and emerging internet-based technologies, 265- 299.
- [7]. Zhuang Y., Sheets L.R., Chen Y.W., Shae Z.Y., Tsai J.J. and Shyu C.R. (2020). A patient-centric health information exchange framework using blockchain technology. IEEE journal of biomedical and health informatics, 24(8), 2169-2176.