IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

5th National Conference on Science, Technology and Communication Skills – NCSTCS 2K22

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 9, Special Issue 2, September 2022

Blockchain Technology – A Review

Sumit Nandi[1], Md. Mirja Galib[2], Swapnanil Sarkar[3] and Rupa Bhattacharyya[4]

Associate Professor, Department of Basic Science and Humanities, Narula Institute of Technology, Kolkata, India[1]

Student, Department of Electronics and Communication Engineering, Narula Institute of Technology, Kolkata, India[2,3]

Assistant Professor, Department of Basic Science and Humanities, Narula Institute of Technology, Kolkata, India[4]

Abstract: Blockchain is an immutable record that makes it easy to record transactions and track assets across business networks. An asset can be tangible (house, car, cash, land) or intangible (intellectual, patents, copyright, brand). Anything of value can be tracked and traded on the blockchain, reducing risk for all involved. Importance of Blockchain: Business is based on data. The faster it is received and the more accurate it is, the better. Blockchain is ideal for providing this information because it provides instant, public and transparent information stored in an immutable record, accessible only to authorized members of the network. Blockchain systems can track orders, payments, accounts, production, and more. Because members have a single view of the truth, you can see every detail of the transaction, giving greater confidence, new efficiencies and opportunities. Each transaction is recorded as a "block" of data as it occurs. Data blocks can record any information you choose: who, what, when, where, how much, even status—like the temperature of a food delivery. With blockchain, as a member-only member of the network, you can be sure that you receive accurate and timely information and that your private blockchain records will only be shared with members of the network that you specifically authorize. All network members are required to agree to the accuracy of the data, and all verified transactions cannot be changed because they are permanently recorded. No one, not even the system administrator, can break the transaction. Time-consuming entries are checked using a distributed ledger that is shared among network members. To speed up contracts, a set of rules called smart contracts can be stored on the blockchain and executed automatically.

Keywords: Blockchain; Bitcoin; Crypto currency; Smart contract

I. INTRODUCTION

A blockchain is a relevant database that is sympathize among the bulge of the computer network. As a database, a blockchain picks up data electronically in digital format. Block chains are best known for their decisive role in crypto currency systems, such as Bitcoin, for maintaining a secure and delegated record of transactions. The innovation with a blockchain is that it guarantees the constancy and security of a record of data and initiate trust without the need for a trusted third party.One key difference between a distinctive database and a blockchain is how the data is structured. A blockchain collects data together in groups, known as blocks that grasp sets of information. Blocks have certain storage capabilities and, when filled, are closed and linked to the formerly filled block, forming a chain of data known as the blockchain. All new data that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once stuffed.A database normally structures its data into tables, where as a blockchain, as its name implicit, structures its data into blocks that are tied together. This data structure genetically makes an irreversible agenda of data when implemented in localized nature. Each block in the chain is given an exact time suck when it is added to the chain.In simple terms, a blockchain is a dispense ledger that records transactions between two parties expertly and securely. This means that there is no central ascendancy that controls the network. Instead, each bulge(computer) in the network agrees to record the transaction based on the commands set by the other nodes.

Blockchain is ideal for sending that information because it distributes immediate, shared and completely translucent information stored on an unchangeable ledger that can be retrieve only by permissioned network members. A blockchain network can trace orders, payments, accounts, production and much more. And because members share a once view of the truth, you can see all details of a transaction end to end, giving you eminent confidence, as well as new efficiencies and opportunities.

II. KEY ELEMENTS OF BLOCKCHAIN

Distributed ledger technology: All network participants have access to a distributed ledger and an immutable record of transactions. With this shared record, transactions are recorded only once, eliminating the duplication of effort typical of traditional business networks.

Immutable records: No participant can alter or modify a transaction after it is recorded in the public record. If there is an error in the transaction record, a new transaction must be added to reverse the error, and both actions are visible.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

5th National Conference on Science, Technology and Communication Skills – NCSTCS 2K22

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 9, Special Issue 2, September 2022

Smart contracts: To speed up contracts, a set of rules called smart contracts are stored on the blockchain and executed automatically. Smart contracts can set the terms of corporate bond transfers, cover travel insurance premium requirements, and more.

III. HOW BLOCKCHAIN WORKS?

As each transaction occurs, it is recorded as a "block" of data

Those processes represent the movement of assets, which can be tangible (product) or intangible (intellectual). Data blocks can record any information you want: who, what, when, where, how much, and their status - such as the temperature of a food delivery.

Each block is connected to the ones before and after it

These blocks form a chain of data when assets move from one location to another or change ownership. Blocks ensure the exact timing and sequence of transactions, and blocks are securely linked so that blocks cannot be changed or inserted between two existing blocks.

Transactions are blocked together in an irreversible chain: a blockchain

Each additional block strengthens the authentication of the previous block and thus the entire block. This clearly shows the blocking, providing the power of volatility. It eliminates the possibility of malicious actors interfering - and creates a list of operations that you and other network members can trust.

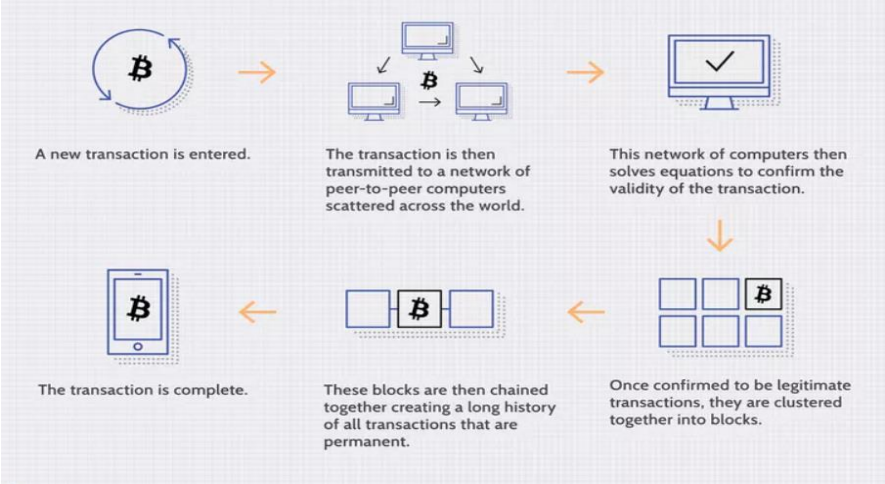

Fig. 1 Transaction process in blockchain technology

Blockchain Decentralization

Imagine you have a server farm with 10,000 computers used to store a database where all customer account information is stored. This company has a warehouse building that keeps all these computers under one roof and has complete control over each of these computers and all the data in them. However, this provides a point of failure. What if the power out there? What should I do if my internet connection goes down? What should be done if the ground is on fire? What if a bad actor ruins everything with one click? After all, data is lost or damaged.

What blockchain does is allow the data in that database to be distributed between multiple network nodes in different locations. This not only creates redundancy, but also maintains the integrity of the data in it - if someone changes a record in one instance of the database, other points will not be changed, preventing bad actors. If the user tampers with the Bitcoin transaction log, all other nodes will point to each other and easily identify nodes with incorrect information. This system helps to create an accurate and clear schedule of events. Therefore, even one point in the network cannot change the data there.Therefore, data and history (egcrypto currency transactions) cannot be recovered. Such a record can be a list of transactions (for example with crypto currency), but the blockchain can store different information, such as legal contracts, government ID cards, or a list of company products.

Transparency

Due to the decentralized nature of the Bitcoin blockchain, all transactions can be viewed transparently by having a private node or using a blockchain explorer that allows anyone to view transactions live. Each node has its own copy of the chain, which is updated as new blocks are approved and added. So if you want, you can follow Bitcoin anywhere.For example, the exchange has crashed in the past, where Bitcoin holders lost everything. Although hackers can be completely anonymous, the Bitcoins they withdraw can be easily traced. In some of these cases, it will be known if the stolen Bitcoins can be transferred or spent elsewhere.Of course, records stored on the Bitcoin blockchain (like anything else) are encrypted. This means that only the owner of the record can reveal his identity (using the public key pair). As a result, blockchain users can remain anonymous while maintaining transparency.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

5th National Conference on Science, Technology and Communication Skills – NCSTCS 2K22

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 9, Special Issue 2, September 2022

Is Blockchain Secure?

Blockchain technology brings decentralized security and trust in many ways. First, new blocks are always stored linearly and chronologically. That is, it is always added to the "end" of the block. Once a block is added to the end of the block, it is very difficult to go back and change the block's content unless most of the network agrees to do so. This is because each block has its own token with a previously assigned timestamp and hash of the previous block. Hash codes are created by mathematical functions that convert digital data into a sequence of numbers and letters. If that data is edited in any way, the hash code changes as well.

Let's say a hacker running a node on the blockchain wants to change the blockchain and steal cryptocurrency from other people. If they change their own copy, it won't be the same as the other copy. If everyone shows their samples against each other, they will see that this one sample is different and the hacker version of the chain will be removed as illegal.

Success with such a hack would require a hacker to manage and change 51% or more copies of the blockchain at the same time, so that the new copy becomes the majority copy and thus the consensus chain. Such an attack requires a lot of money and resources, because all the blocks have to be recreated because they now have different timestamps and hash codes.Due to the size of many cryptocurrency networks and how fast they grow, the cost of attracting such talent cannot be recouped. Not only is this very expensive, but it can also be ineffective. Doing so will not go unnoticed because network members will see drastic changes such as the blockchain. Network members will find it difficult to find a new version of the chain that is not affected. This will cause the target type to be devalued, making the attack ineffective as a bad actor controls properties that have no value. This is what happens when a bad actor attacks a new Bitcoin fork. The network is structured in such a way that it is more economically incentivized to participate than to attack it.

Bitcoin vs. Blockchain

Blockchain technology was first described in 1991 by Stuart Haber and W. Scott Sternest, two researchers who wanted to implement an immutable document seal system. But almost two decades later, with the launch of Bitcoin in January 2009, blockchain was first used in the real world.The Bitcoin protocol is built on the blockchain. In a research paper introducing the digital currency, Bitcoin's eponymous creator called it "a new, fully peer-to-peer electronic money system with no trusted third party."The key thing to understand here is that Bitcoin only uses the blockchain to record payments transparently, but the blockchain could theoretically be used to change data points. As mentioned above, these transactions can be in the form of votes in elections, product lists, government ID cards, PR, and more.

Today, tens of thousands of projects are trying to apply blockchains in various ways, beyond just recording transactions, to help people vote safely in democratic elections, for example. The nature of blockchain volatility means that fraudulent voting will become increasingly difficult. For example, a voting system can be used to give each citizen a cryptocurrency or token. Each candidate will then be assigned a specific wallet address, and voters will send their number or crypto address to whichever candidate they want to vote for. The transparent and traceable nature of the blockchain will eliminate the need for human vote counting and the ability of bad actors to tamper with physical ballots.

Blockchain vs. Banks

Blockchain have been heralded as a disruptive force in the financial industry, especially with payment and banking functions. However, banks and decentralized block chains are very different.

To see how banking differs from blockchain, let's compare the banking system with Bitcoin's blockchain implementation.

IV. BENEFITS OF BLOCKCHAIN TECHNOLOGY

The primary benefit of blockchain is as a database for recording transactions, but its benefits extend far beyond those of a traditional database. Most notably, it removes the possibility of tampering by a malicious actor, as well as providing these business benefits:

- **Time savings:** Blockchain slashes transaction times from days to minutes. Transaction settlement is faster because it doesn’t require verification by a central authority.
- **Cost savings:** Transactions need less oversight. Participants can exchange items of value directly. Blockchain eliminates duplication of effort because participants have access to a shared ledger.
- **Greater trust:** With Blockchain, as a members-only network member, you can be sure that you receive accurate and timely information, and that your private blockchain records will only be shared with network members you specifically authorize.
- **Greater security:** Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.
- **More efficiencies:** Time-consuming entries are checked using a distributed ledger that is shared among network members.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

5th National Conference on Science, Technology and Communication Skills – NCSTCS 2K22

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 9, Special Issue 2, September 2022

- To speed up contracts, a set of rules called smart contracts can be stored on the blockchain and executed automatically rules - called smart contracts - are stored in the blockchain and executed automatically. Smart contracts can set the terms of corporate bond transfers, cover travel insurance premium requirements, and more.
- **Blockchain for payment processing and money transfers:** Transactions processed over a blockchain could be settled within a matter of seconds and reduce (or eliminate) banking transfer fees.
- **Blockchain for monitoring of supply chains.** Using blockchain, businesses could pinpoint inefficiencies within their supply chains quickly, as well as locate items in real time and see how products perform from a quality-control perspective as they travel from manufacturers to retailers.
- **Blockchain for digital IDs.** Microsoft is experimenting with blockchain technology to help people control their digital identities, while also giving users control over who accesses that data.
- **Blockchain for data sharing.** Blockchain could act as an intermediary to securely store and move enterprise data among industries.
- **Blockchain for copyright and royalties' protection.** Blockchain could be used to create a decentralized database that ensures artists maintain their music rights and provides transparent and real-time royalty distributions to musicians. Blockchain could also do the same for open-source developers.
- **Blockchain for Internet of Things network management.** Blockchain could become a regulator of IoT networks to "identify devices connected to a wireless network, monitor the activity of those devices, and determine how trustworthy those devices are" and to "automatically assess the trustworthiness of new devices being added to the network, such as cars and smartphones."
- **Blockchain for healthcare.** Blockchain could also play an important role in healthcare: "Healthcare payers and providers are using blockchain to manage clinical trials data and electronic medical records while maintaining regulatory compliance."

V. DRAWBACKS OF BLOCKCHAIN TECHNOLOGY

- **Technology Cost:** Although blockchain can save users money on transaction fees, the technology is not free. For example, the Pow system that the bitcoin network uses to confirm transactions consumes a large amount of computing power. In the real world, the power of millions of computers in the bitcoin network is close to what Norway and Ukraine consume every year.Despite the cost of mining Bitcoin, users continue to pay electricity to validate transactions on the blockchain. This is because when miners add blocks to the bitcoin blockchain, they are rewarded with enough bitcoins for their time and effort. As for non-cryptocurrencyblockchains, miners must be paid or otherwise incentivized to confirm transactions.Several solutions to this problem are beginning to emerge. For example, bitcoin mining farms have been created using solar energy, excess natural gas from pore spaces, or energy from wind farms.

- **Speed and Data Inefficiency:** Bitcoin is a perfect example of the potential inefficiency of the blockchain. Bitcoin'sPoW system takes about 10 minutes to add a new block to the blockchain. At that speed, it is estimated that the blockchain can handle only seven transactions per second (TPS). While other crypto currencies like Ethereum are doing better than bitcoin, they are still limited by the blockchain. Legacy brand Visa can process up to 65,000 TPS per context.Solutions to this problem have been developed for years. Today, there are more than 30,000 TPS-boasting brokers. The integration between the Ethereum main net and the beacon chain (September 15, 2022) is expected to enable up to 100,000 TPS after the upgrade including sharing with more devices (phones, tablets, and laptops).) can run on Ethereum. This will increase network throughput, reduce congestion and increase traffic speed.Another problem is that each block can store only so much data. The debate over block size has been continues to be, one of the most important issues for blockchain expansion going forward.

- **Illegal Activity:** Privacy on the blockchain protects users from hackers and maintains privacy, as well as prevents illegal trade and activity on the blockchain. The most prominent example of blockchain being used for illegal activities is Silk Road, an online dark site for illegal drugs and money laundering markets that was shut down by the FBI between February 2011 and October 2013.The dark web allows users to buy and sell illegal goods and make illegal purchases in Bitcoin or other crypto currencies without tracking their web browser. Current US regulations allow financial services providers to verify the identity of each customer and verify that the customer is not on a list of known or terrorist organizations when opening an account. This system can be seen as pros and cons. This allows anyone to access financial accounts, but allows criminals to trade more easily. Many argue that the good use of crypto, such as banking the unbanked world, outweighs the bad use of crypto currency, especially since many illegal activities are still carried out through unrestrained cash.Although Bitcoin was used early for such purposes, its transparent nature and maturity as a financial asset has seen illegal activities migrate to other crypto currencies such as Monero and Dash. Today, illegal activity accounts for only a small fraction of bitcoin transactions.

- **Regulation:** Many in the crypto space have expressed concerns about government regulation over crypto currencies. While it is getting increasingly difficult and near impossible to end something like Bitcoin as its decentralized network grows, governments could theoretically make it illegal to own crypto currencies or participate in their networks. This concern has grown smaller over time, as large companies like PayPal begin to allow the ownership and use of crypto currencies on its platform.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

5th National Conference on Science, Technology and Communication Skills – NCSTCS 2K22

Narula Institute of Technology, Agarpara, Kolkata, India

Vol. 9, Special Issue 2, September 2022

VI. CONCLUSION

In short, blockchain technology is a distributed information that allows people to share data without having to trust each other. This means that no one person has complete control over the data. Instead, everyone who wants access to the data must agree to follow certain rules. These rules ensure that only authorized users can see the data and the data cannot be changed once it's been shared.

REFERENCES

[1] https://en.m.wikipedia.org/wiki/Blockchain
[2] https://www.investopedia.com/terms/b/blockchain.asp
[3] https://netslovers.com/post/what-is-blockchain-how-does-it-work/amp/?gclid=CjwKCAiAzp6eBhByEiwA_gGq5KTXdjvvlOvJzPGDXF_ryJH9tn1Q0_m8KqUCtWodT0guwsfIK5w2YhoCoKcQAvD_BwE
[4] https://www.investopedia.com/terms/b/blockchain.asp
[5] https://www.ibm.com/in-en/topics/what-is-blockchain
[6] https://en.wikipedia.org/wiki/Blockchain
[7] https://builtin.com/blockchain
[8] https://blockgeeks.com/guides/what-is-blockchain-technology/