International Journal of Research in Circuits, Devices and Systems

E-ISSN: 2708-454X
P-ISSN: 2708-4531
IJRCDS 2022; 3(1): 92-97
© 2022 IJRCDS
www.circuitsjournal.com
Received: 08-11-2021
Accepted: 13-12-2021

Ismaheel Faheem
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Application of cryptocurrency in industrial field: Storing and recording

Ismaheel Faheem

Abstract

Blockchain has the potential to change the face of manufacturing industries. Blockchain which is associated with cryptocurrencies can be used to store and record transactions. This paper is trying to discuss about how people in the industrial field keep track of and store these kinds of things. A cryptocurrency is an encrypted, decentralised digital currency that allows people to exchange value by exchanging crypto tokens. Cryptocurrencies are used to buy and sell goods and services. The public ledger is a record-keeping system that keeps track of people's identities and cryptocurrency balances in a safe and (pseudo-)anonymous way, as well as a record of all real transactions between network participants. The two people who were involved in the transaction can check and look up the transaction details on a cryptocurrency public ledger. However, no one in the network can know the identities of the people who are in the network. Transactions are only allowed and recorded if the sender can be proven to be able to pay. Otherwise, they are thrown away. All of the important information is stored and recorded in a safe way. Everyone else, except the people who made the transactions, can't see them. The public ledger method is a simple way to store and keep track of cryptocurrency for things like logistics in the industrial field.

Keywords: Blockchain, distributed ledger technology, cryptocurrency, industry field

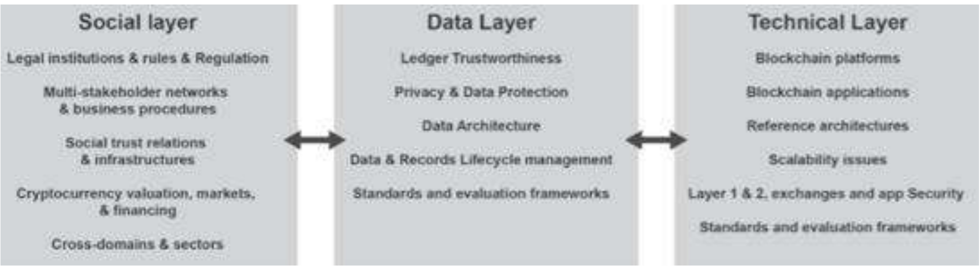
Introduction

Cryptocurrency has already reached and affected almost every aspect of modern-day human life. It not only gains popularity, but also receives wider accumulation of acceptance as more and more people can enjoy the benefits of using digital currency [1]. It's known that cryptocurrencies are not suitable for use in some industries. For instance, the process of exchanging cryptocurrencies is performed by the users themselves, which means that it easily impacts business efficiency. According to statistics, on average, 5% of work time is spent on transactions.

A way to make people trust you is to change the information that they need.

- Creating and storing records: Blockchain technology uses cryptography to make records that can't be changed. This makes tamper-proof proof of what people have done.
- Decentralization: Blockchain technology runs on a peer-to-peer system, which means there is no central authority. Instead, participants are free to act on their own, which makes it hard for them to work together, and the records that are made in this system can be trusted.

Blockchains use cryptographic recordkeeping, consensus in an effort of finality and immutability of records. Blockchain's interacting trust layers are shown in *Figure 1.*



Social layer
Legal institutions & rules & Regulation
Multi-stakeholder networks & business procedures
Social trust relations & infrastructures
Cryptocurrency valuation, markets, & financing
Cross-domains & sectors

Data Layer
Ledger Trustworthiness
Privacy & Data Protection
Data Architecture
Data & Records Lifecycle management
Standards and evaluation frameworks

Technical Layer
Blockchain platforms
Blockchain applications
Reference architectures
Scalability issues
Layer 1 & 2, exchanges and app Security
Standards and evaluation frameworks

Fig 1: Three layers Trust model of Blockchain Technology

Correspondence
Ismaheel Faheem
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Execution of Blockchain Transactions

Traditional blockchain applications, like cryptocurrency, involve two people making a deal with each other. Each valid transaction is recorded in a block that may be made up of multiple records for speed. Cryptographic methods, like hashing, are used to make sure that things can't be changed [2, 9, 13-15]. Figure 2 shows how a simple blockchain should look like.

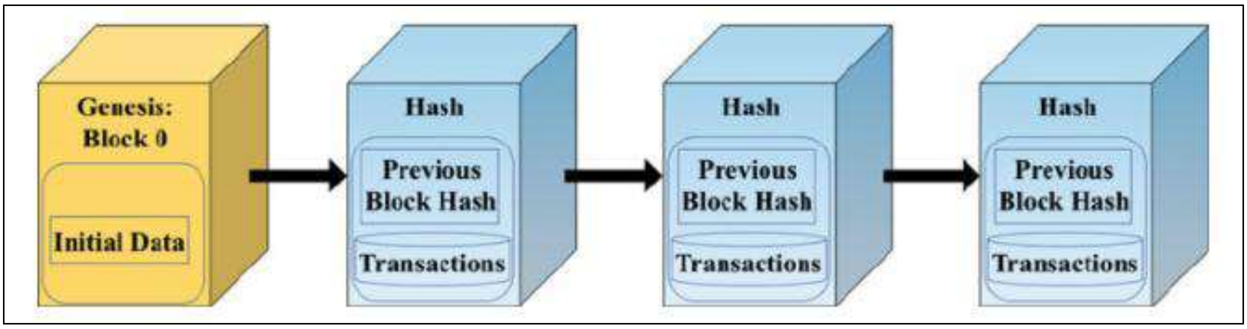
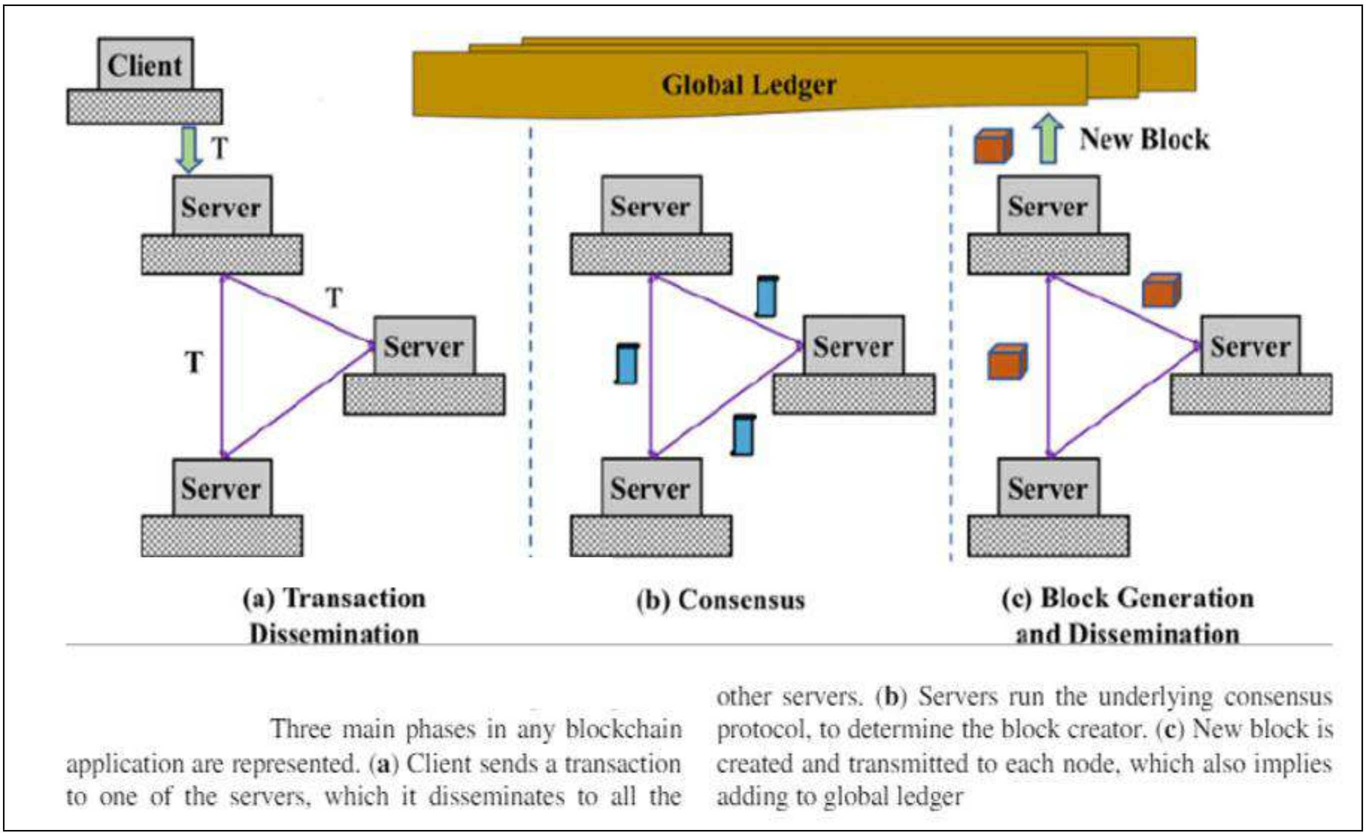


Fig 2: Blockchain Transaction Processing

Blockchains are linked lists, and each block in the chain has its hash stored there. In order to change a block, an attacker would have to change all the previous blocks in the linked least as well. These hashes provide cryptographic integrity. This makes the change cryptographically infeasible.

There are three steps that any blockchain app must go through in order to make a new block. These steps are: It's one of the servers that gets a transaction request from the client and sends it to the client. In this case, it sends the request to all the other servers at the same time. In this phase, transactions are spread out across a lot of different places. Before the servers start a consensus process, each one has a copy of what the client asked for. The choice of a consensus protocol affects how long it takes and how much time and money it takes to come to a consensus. Consensus phase: The winner makes the next block and sends it to all of the other servers. A block is added to the global distributed ledger just like that, so this is the same thing. The figure below shows the three steps that need to be done (refer fig. 3).



Three main phases in any blockchain application are represented. (**a**) Client sends a transaction to one of the servers, which it disseminates to all the other servers. (**b**) Servers run the underlying consensus protocol, to determine the block creator. (**c**) New block is created and transmitted to each node, which also implies adding to global ledger

Fig 3: Blockchain and its working

Hashing in Cryptography

There are many algorithms for hashing, which is the process of turning an input of n length into a fixed-size string or integer. As an example, let's say we want to find an item in a hash table using a hash function that turns a given key into another number [3, 4]. This is called a hash table.

Choosing a hash function

An efficient hash function should be built such that the index value of the added item is distributed equally across the hash table. An effective collision resolution technique should be created to generate an alternate index for a key whose hash index corresponds to a previously inserted position in a hash table. Hash collision occurs when two are more inputs are mapped to the same keys as used in the hash table. This collision cannot be completely avoided but can be minimised using a good hash function and a bigger table size. The hash algorithm selected must be fast to calculate.

Collision Hashing Techniques

- Open Hashing (Separate Chaining): It is the most commonly used collision hashing technique implemented using *Lined List*. When any two or more elements collide at the same location, these elements are chained into a single-linked list called a chain.
- Closed Hashing (Open Addressing): In this, we find the next vacant bucket in Hash Table and store the value in that bucket.
- Linear probing: Linearly checks every next bucket and see if it is vacant or not.
- Quadrating probing: n^2th bucket is checked and see if it is vacant or not.
- Double Hashing: The generated key from the hash key is subjected to another hash function.
- Load factor: This is a measurement of how full a hash table may become before its capacity is increased.

Time Complexity of Hash Function

Hashing gets O (1) complexity. Load factor is used to ensure that each block stores the maximum number of elements fewer than the load factor on average. In practice, this load factor is constant.

Benefits of Cryptographic Hash Functions

- Avalanche effect: A small change in the data can make a big difference in the end result.
- This means that every input has a unique output.
- The hash function will always give the same result to any input that is passed through it.
- Speed: The output can be made in a short amount of time.
- There is no way to do this.

Blockchain Topologies

Public, private, protected, and hybrid are the four types of blockchain systems we can look in figure 4.

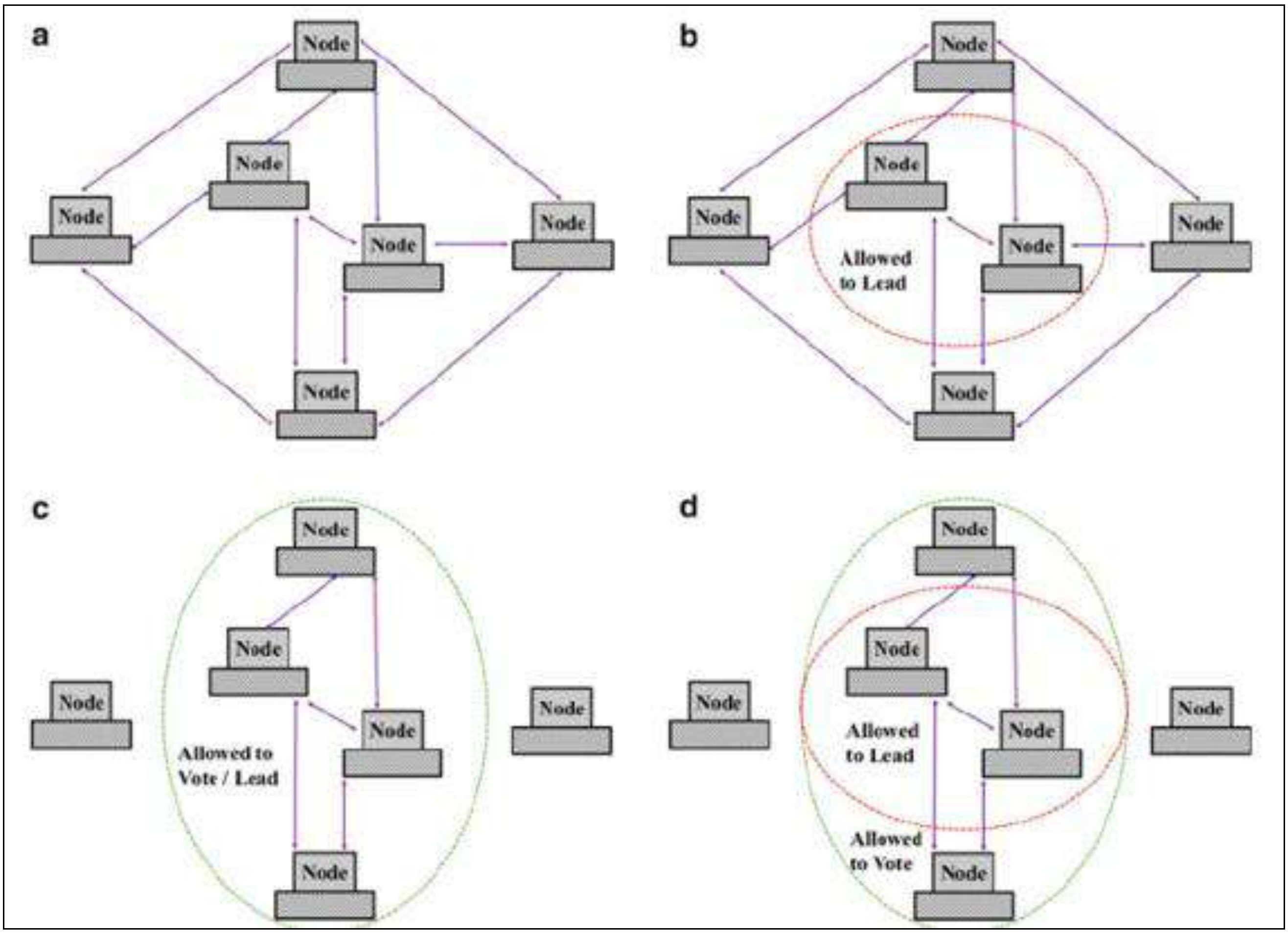


Fig 4: Blockchain Transaction Processing. a). Public Blockchain b). Hybrid Blockchain, c). Permission blockchain d). Private blockchain.

There are public blockchain systems like Bitcoin and Ethereum that let anyone be a part of the consensus process and make the next block in the chain. Any node can do this, and any node can make the next block. People who play this game know that each node has the same chance of making a new block. It's possible to make private blockchain systems that only let a small group of nodes be part of the consensus process. Only a few of these nodes can add a block. It is possible for any node in hybrid blockchain systems to be a part of the consensus process and help reach a consensus. Few people can start a new block [5, 6].

If users want to use permissioned blockchain systems, you can't use them in the same way as public blockchain systems. If only a few nodes have the same rights, they can all make new blocks. Because each node can make new blocks, this means that the whole system can make new blocks.

Blockchain Consensus Algorithm

Most of the blockchain applications are built on top of a distributed consensus algorithm called "distributed consensus." Proof-of-Work (PoW) was suggested as a way to get all the nodes involved in the network to agree. Every node in PoW has to show that it can do something that isn't easy. In a complex puzzle, for example, all the nodes compete with each other to find a SHA value that is 256 bytes long. In PoW, the nodes that have the most computing power are the ones that win.

Proof-of- Stake wants to keep the blockchain network as decentralised as possible. People who have a lot of resources get a lot of chances to make new blocks in the PoS algorithm. PoS is based on the idea that the node with the most stake gets to make the next block. In the game, one or more factors could be used to figure out how much a node is worth [15]. These factors could be wealth, resources, or other things like that. In this algorithm, some people need to act as "validators." But the algorithm doesn't say how many people need to do this. Because of its stake, any node that wants to be a validator must lock itself out of its own resources in order to show that. Only people who are "validators" can make new blocks in PoS, and only validators can do this. Validators then make a new block and add it to the chain of blocks already there. In this case, how many times the validator gets chosen is set to a certain amount of time. To choose the next block to add to the list, the BFT-style algorithm runs a byzantine fault tolerance algorithm that is hard to understand. There are people who are called "validators," and they can choose the next block that will be added to the list. This means that all chain-based PoS algorithms are always in sync, but BFT-style PoS is only partly in synchronization.

Proof-of- Authority is meant to work with blockchain systems that aren't public. This is the most important thing to do. It is important for users to name a group of nodes as the authority. These nodes are in charge of making new blocks and making sure that transactions are correct, so they are important. PoA makes a block part of the blockchain if most of the nodes that are allowed to sign it do. A node that has a good reputation and gets bonuses is in the best interest of keeping that reputation and getting bonuses. This is shown by the incentive model in PoA. So, the PoA doesn't pick nodes based on how much money they say they have, so that's why.

Unlike PoW, Proof of Space isn't the same as Proof of Capacity (PoC). Proof of Space is a consensus algorithm that isn't the same as Proof of Capacity [16]. It's a way to make people agree. To show that they have enough space to solve a complicated computational puzzle, it wants nodes to show that they have enough space to do so. When there are computational problems that need a lot of memory space to solve, the PoC algorithm is used to solve them. They say that PoC-based approaches are better for the environment than PoW-based approaches. People who use a cryptocurrency called Space Mint say that this is true. This is because it takes less energy to store things than it does to move them around.

PBFT runs a three-phase process to get all the non-byzantine nodes to agree. To use PBFT, you have to set a limit on the number of byzantine nodes. It's good that PBFT-based algorithms don't use a lot of resources, but the message complexity (order O(n2)) is a big problem. For this reason, these algorithms are better for small or limited blockchain systems because they don't have a lot of message overhead.

Zyzzyva is another interesting fault tolerance protocol that aims to cut down on the costs of BFT-style protocols. Zyzzyva allows the replicas to come to a consensus early on by letting them run things they think will work. In Zyzzyva, the replicas don't have to make sure that all of the client requests are in the same order all over the world. This job is given to the client, who then tells the other copies if they aren't in sync.

Even though zyzzyva has a lot more throughput than PBFT, its client-based speculative execution isn't as good as it should be. This isn't good, because a bad client can stop the copies from being able to keep their linearizability. Aardvark looks into the problems caused by fast, byzantine fault-tolerant protocols and shows how to make a robust BFT protocol that isn't going to break down soon. To make sure that messages are real, the client signs them with both digital signatures and codes that show they are real. They can't do a denial-of-service attack because it costs the client to sign each message twice. Aardvark doesn't communicate with other animals in groups. Instead, it talks to each other point-to-point. He also sometimes changes the main copy. Every time there is a decrease in how much the current primary is doing, each of the other replicas looks at it and says that the current primary should be changed.

RBFT is a simple add-on for Aardvark. RBFT aims to find smartly malicious primary replicas that other replicas might not see as malicious. A node can only have one primary at a time, and RBFT doesn't allow more than one [17]. This means that each node can only have one primary instance of itself at the same time. RBFT protocol has a fourth phase, which isn't in PBFT or Aardvark. The client node sends a request to all the other nodes to start the protocol.

Blockchain Record Keeping Solutions

A. Mirror Type

As part of the "mirror" system, the blockchain is where digital fingerprints of the records are kept. Records that can be found in digital form have been hashed so that they can be identified, just like a bar code. Blockchains keep track of these hashes, and the blockchain acts as a mirror to look at the records and show them back to you. It can happen with any type of blockchain. It doesn't matter if the blockchain is private or public, because it doesn't matter that much. People use a lot of different types of blockchain recordkeeping systems. Some don't keep records on a chain. As a result, they don't run on their own and don't use the same encryption as other digital systems. Systems like this one are important because hashes can tell if records have been changed, so they are important to keep the records safe. However, many solution providers say that they keep records on the chain, even though they aren't. This isn't true, and it makes a big mistake in the design ideas [18]. There must be a way to keep the digital originals and the block chained hashes of the records in the same place. As long as you use this type of blockchain system, there aren't any big changes in how to keep the originals safe. There would be a copy of the hashes in the ledger on another node even if one of the nodes on a distributed blockchain system went down. These copies keep things safe, so this is why. Most of the time, not all nodes have to have a full copy of the ledger. So that at least one full node could live. Users can't tell whether a node has been changed if there is only one left. Nodes are judged on how well their copies of the ledger match up with other copies that still exist. Many as possible should match. Another thing that makes the network work is that the incentives that make nodes want to validate transactions are still good enough to keep them interested.

B. Digital Record Type

In these systems, a record isn't just a copy of itself, but a different record. People make it on the chain in the form of "smart contracts," which are written in code. These changes are more important than the way digital records are made and stored in databases or on cloud-based platforms. As part of a work process flow, these smart contracts usually describe how to work together with other people. As soon as the "smart code" is run, a ledger or distributed database of records is updated. Changes happen to the ledger when the smart contract is done, so the ledger will be different.

There are many ways to store and retrieve data in a database. This type of record keeping can do the same thing but also adds the distribution and redundancy of a blockchain to the mix. To keep the data safe when it's shared between a group of databases, this is what it does This means that each node in the group has its own copy of the database. In a Post Chain, the blockchain is inside the database, not outside of it. There are tables for raw transaction data, and for blockchain data, there are tables for each block in the chain. There are also tables for each transaction (headers and hashes). People who work with databases think of it as a manager for the database. It acts as a transaction layer for the database to make sure that transactions are organised, deterministic, and so on. People who make another kind of blockchain use APIs so that databases can be linked to a blockchain processing layer that runs them.

There are many ways to get the post chain to work. Right now, it's using a modified version of Practical Byzantine Fault Tolerance to get things done (PBFT). To the network in PBFT, it sends out a message (e.g., a primary node or may be more than one node, depending on the system design). People who got the message send it to all the other nodes. When enough nodes agree, it is added to the blockchain.

C. Tokenized Type

The most cutting-edge way to keep track of things on the blockchain is to use tokenized solutions. With this type of system, not only are records kept on a chain, but assets are also shown and kept on a chain. These assets can be used to show anything of value.

In Ubiquity's Brazilian pilot land titles enlistment recordkeeping system, this type of blockchain recordkeeping is used to keep track of pilot land titles. Ubitquity's answer works with a "product as a service" (SaaS) plan of action, which helps businesses and government offices keep track of land exchanges. Expenses are charged for adding and updating records in the blockchain stage. web front end that collects data from the land as well as a web server and back-up storage are part of the plan They communicate with the Colu Application Programming Interface (API), which is used by an organisation that gives resources (like land) and exchanges those resources (like land moves) to be recorded on a blockchain. The front-end web UI decodes what is typed in. If you want to "tokenize" land, you can use Colu "Hued Coins," which is a type of cryptocurrency that can be used to do this. Then you can use the Bitcoin blockchain to record transactions. People who use Hued Coins follow a set of rules and methods for addressing and managing real-world resources, like land, as an information layer on top of a blockchain. A Bitcoin is used to identify every resource, like a piece of land. When this happens, the Bitcoin can be used to move the resource between different owners. For this case, Bitcoin is also being used as a blockchain exchange recording layer, but it is also possible to use other blockchains. The ability to store data on a chain as a whole takes into account the relationship of that exchange yield to a piece of property, which is called "shading." This is why the convention's name is "Colored Coins." Due to the fact that there isn't a lot of space on the Bitcoin blockchain, Colu's "shading plan" also allows for unlimited amounts of metadata to be linked to a specific exchange through freely available downpour files, as shown in the picture. This way, BitTorrent can be used to store information or metadata about the resource and link it to an exchange. This is a common way for people to share documents, like how Bitcoin hubs make it easy to record transactions on a public record. What's more, just like with Bitcoin, friends can be found all over the world. In order for the information to stay online, there must be at least one, and ideally many, peers who have downloaded the information and start sharing it with the public BitTorrent network.

6. Archival Implications

Mainly, blockchain recordkeeping adds a layer of trustworthiness to the current recordkeeping system by adding a layer of trustworthiness. The blockchain isn't really changing how records are kept so much that it can be thought of as another tool that annalists can use to improve records. When the Inter PARES Trust Chain project is done, it wants to use the blockchain to keep a record of how the "chain of protection" works. The advanced signatory gets a public key from an outside declaration authority, just like with other carefully marked records. This makes them seem more trustworthy. These endorsements are only valid for a certain amount of time. People usually stop authenticating records when they move them to archives, which breaks a chain of protection needed to prove that the records are real from when they made them to a certain point in the future. It doesn't need anyone to give out statements because public-private key sets are made inside the blockchain. Records can be marked again in the future while their original documents are still valid, and cryptographically stored in a blockchain to show that they are still real at the time they were marked. This shows that they are still alive. In this case, the State Committee for Archives of the Republic of Tatarstan is said to have decided to look into how blockchain technology could be used to check history's records. State Archives will make hashes of archives when they move them into the chronicle so they can be part of a network called the blockchain, a report says. As soon as the next few days go by, a steady stream of information will start to flow to the server farm. At the end, their honesty will be checked. As part of its work, the UK National Archives is also looking at records from other countries. It's still in the early stages of this. Further, readers/ researchers are suggested to refer articles [6-18] to know more emerging technologies and use of blockchain in these useful sectors.

Conclusion

Blockchain technology is very exciting and quite revolutionary, but it's still early days for this technology as a whole. As with anything, there's bound to be some bumps along the road as people learn how to use blockchain to its full potential. But as time goes by and blockchain becomes more widely used, the chances of hacks and scams reducing dramatically. The methods such as hashing and other cryptographic methods are such techniques which is implemented to protect such systems.

References

1. Victoria L Lemieux, Darra Hofman, JD, MSLS; Danielle Batista, B.A.R.M, MIS; and Alysha Joo, MASLIS , Blockchain Technology and record keeping. Available from: http://armaedfoundation.org/wp-content/uploads/2019/06/AIEF-Research-Paper-Blockchain-Technology-Recordkeeping.pdf
2. Suyash Gupta, Mohammad Sadoghi. Department of Computer Science, University of California, Davis, Davis, CA, USA, Blockchain Transaction Processing. Available from: https://www.researchgate.net/publication/325116198_Blockchain_Transaction_Processing#pfb
3. Jonathan Katz, Yehuda Lindell. Introduction to Modern Cryptography. 2007. Available from: http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/Introduction_to_Modern_Cryptography.pdf
4. Victoria L. Lemieux Associate Professor, Archival Science The University of British Columbia Vancouver, Canada, A typology of blockchain recordkeeping dolutions and some reflections on their implications for the future archival preservation. Available from: https://www.researchgate.net/publication/322511343_A_typology_of_blockchain_recordkeeping_solutions_and_some_reflections_on_their_implications_for_the_future_of_archival_preservation
5. Nair MM, Tyagi AK, Sreenath N. "The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, 1-7. doi: 10.1109/ICCCI50826.2021.9402498.
6. Tyagi AK, Fernandez TF, Mishra S, Kumari S. Intelligent Automation Systems at the Core of Industry 4.0. In: Abraham A., Piuri V., Gandhi N., Siarry P., Kaklauskas A., Madureira A. (eds) Intelligent Systems Design and Applications. ISDA 2020. Advances in Intelligent Systems and Computing, Springer, Cham. 2021, 1351. https://doi.org/10.1007/978-3-030-71187-0_1
7. Tyagi K, Rekha G, Sreenath N. "Is your Privacy Safe with Aadhaar?: An Open Discussion," 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). 2018, 318-323, doi: 10.1109/PDGC.2018.8745836.
8. Goyal, Deepti, Tyagi, Amit. A Look at Top 35 Problems in the Computer Science Field for the Next Decade. 2020. 10.1201/9781003052098-40.
9. Amit Kumar Tyagi, Dr. Meenu Gupta, Aswathy SU, Chetanya Ved. “Healthcare Solutions for Smart Era: An Useful Explanation from User’s Perspective”, in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press. 2021.
10. Varsha R, Nair SM, Tyagi AK, Aswathy SU, Radha Krishnan R. The Future with Advanced Analytics: A Sequential Analysis of the Disruptive Technology’s Scope. In: Abraham A., Hanne T., Castillo O., Gandhi N., Nogueira Rios T., Hong TP. (eds) Hybrid Intelligent Systems. HIS 2020. Advances in Intelligent Systems and Computing. 2021, 1375. Springer, Cham. https://doi.org/10.1007/978-3-030-73050-5_56
11. Tyagi, Amit Kumar, Nair, Meghna Manoj, Niladhuri, Sreenath, Abraham *et al*. "Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead", Journal of Information Assurance & Security. 2020;15(1):1-16.
12. Madhav AVS, Tyagi AK. The World with Future Technologies (Post-COVID-19): Open Issues, Challenges, and the Road Ahead. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. 2022. https://doi.org/10.1007/978-981-16-6542-4_22
13. Amit Kumar Tyagi. “Analysis of Security and Privacy Aspects of Blockchain Technologies from Smart Era’ Perspective: The Challenges and a Way Forward”, in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press. 2021.
14. Amit Kumar Tyagi, Rekha G, Shabnam Kumari. “Applications of Blockchain Technologies in Digital Forensic and Threat Hunting”, in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press. 2021.
15. Shabnam Kumari, Amit Kumar Tyagi, Aswathy SU, “The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities and Challenges”, in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press. 2021.
16. Tibrewal I, Srivastava M, Tyagi AK. Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. 2022. https://doi.org/10.1007/978-981-16-6542-4_1
17. Amit Kumar Tyagi, Aswathy SU, Aghila G, Sreenath N. "AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology" IJIN, 2021;2:175-183.
18. Siddharth M Nair, Varsha Ramesh, Amit Kumar Tyagi. Issues and Challenges (Privacy, Security, and Trust) in Blockchain-Based Applications, Book: Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles. 2021, 14. DOI: 10.4018/978-1-7998-3295-9.ch012