International Journal of Research in Engineering, Science and Management
Volume-2, Issue-7, July-2019
www.ijresm.com | ISSN (Online): 2581-5792

An Overview on Blockchain Technology

Sheetal Patil[1], Sonali Panda[2], Durva Tarale[3]
[1]*Assistant Professor, Department of Computer Technology, Bharati Vidyapeeth's Jawaharlal Nehru Institute of Technology, Pune, India*
[2,3]*Student, Department of Computer Technology, Bharati Vidyapeeth's Jawaharlal Nehru Institute of Technology, Pune, India*

***Abstract*: The 21st century is all about technology. With the increasing need for modernization in our day-to-day lives, people are open to accepting new technologies. From using a remote for controlling devices to using voice notes for giving commands; modern technology has made space in our regular lives. Technologies like augmented reality and IoT (Internet of Things) that have gained pace in the past decade and now there's a new addition to the pack i.e. Blockchain Technology. A Blockchain allows untrusting parties with common interests to co-create a permanent, unchangeable and transparent record of exchange and processing without relying on a central authority. Blockchain- The revolutionary technology impacting different industries miraculously was introduced in the markets with its very first modern application Bitcoin. Bitcoin is nothing but a form of digital currency (cryptocurrency) which can be used in the place of fiat money for trading. And the underlying technology behind the success of cryptocurrencies is termed as Blockchain.**

***Keywords*: Blockchain, Untrusting parties, Crypto currency, Bitcoin.**

1. Introduction

There's a common misconception among people that Bitcoin and Blockchain are one and the same, however, that is not the case. Creating cryptocurrencies is one of the applications of Blockchain technology and other than Bitcoin, there are numerous applications that are being developed on the basis of the blockchain technology.

In the simplest terms, Blockchain can be described as a data structure that holds transactional records and while ensuring security, transparency, and decentralization. You can also think of it as a chain or records stored in the forms of blocks which are controlled by no single authority. A blockchain is a distributed ledger that is completely open to any and everyone on the network. Once information is stored on a blockchain, it is extremely difficult to change or alter it. Each transaction on a blockchain is secured with a digital signature that proves its authenticity. Due to the use of encryption and digital signatures, the data stored on the blockchain is tamper-proof and cannot be changed. Blockchain technology allows all the network participants to reach an agreement, commonly known as consensus. All the data stored on a blockchain is recorded digitally and has a common history which is available for all the network participants. This way, the chances of any fraudulent activity or duplication of transactions is eliminated without the need of a third-party. Blockchain is a new type of database. The reason why there is such a call for this new type of database is because it solves the previously unsolvable double spending problem without a middleman, opening up a range of new possibilities. In this database the data is saved in a block, which in turn is linked to other blocks in a chain creating the blockchain. To secure the blockchain a system called proof-of-work is used.

Inshort this means there is so much work (i.e. processing power) needed to find a block, it is virtually impossible to alter the blockchain afterwards. This work is done by so called miners who -when they find a block- get a small payment for their effort Blockchain does have some important aspects to keep in mind. For instance, what is saved in blockchain can never be removed or altered.

Blockchain can even be damaging to the environment because the security system used demands extreme amounts of energy. These two aspects are mentioned only as examples of possible considerations when wanting to use blockchain. In the paper itself many more are presented.

A blockchain carries no transaction cost. (An infrastructure cost yes, but no transaction cost.) The blockchain is a simple yet ingenious way of passing information from A to B in a fully automated and safe manner. One party to a transaction initiates the process by creating a block. This block is verified by thousands, perhaps millions of computers distributed around the net. The verified block is added to a chain, which is stored across the net, creating not just a unique record, but a unique record with a unique history. Falsifying a single record would mean falsifying the entire chain in millions of instances. That is virtually impossible. Bitcoin uses this model for monetary transactions, but it can be deployed in many others ways.

2. Related Work

A blockchain is a chain of blocks that contain data or information. Despite being discovered earlier, the first successful and popular application of the Blockchain technology came into being in the year 2009 by Satoshi Nakamoto. He created the first digital cryptocurrency called Bitcoin through the use of Blockchain technology. Let's understand how a blockchain actually works. Each block in a blockchain network stores some information along with the hash of its previous block. A hash is a unique mathematical code which belongs to a specific block. If the information inside the block is modified, the hash of the block will be subject to modification too. The connection of blocks through unique hash keys is what makes blockchain secure. While transactions take place on a blockchain, there are nodes on the network that validate these transactions. In Bitcoin, blockchain these nodes are called as miners and they use the concept of proof-of-work in order to process and validate transactions on the network. In order for a transaction to be valid, each block must refer to the hash of its preceding block. The transaction will take place only and only if the hash is correct. If a hacker tries to attack the network and change information of any specific block, the hash attached to the block will also get modified. The breach will be detected as the modified hash will not match with the original one. This ensures that the blockchain is unalterable as if any change which is made to the chain of blocks will be reflected throughout the entire network and will be detected easily.

A blockchain is a decentralized, distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. By design and by purpose blockchains are inherently resistant to modification of data. Functionally, a blockchain can serve as 'an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.

When Bitcoin entered the market in 2009, the value of one bitcoin was $.06 and few noticed. When the price of one bitcoin rose above $19,000 in December 2017, it and its underlying "blockchain" technology became the newest buzzwords and took the world by storm. Just adopting the word "blockchain" seemingly created value. For example, when Long Island Iced Tea, a company that sells beverages, changed its name to Long Blockchain Corp. in 2017, its stock price rose almost 300 percent in one day even though it had yet to actually be involved with blockchain. While many have invested in bitcoin, few really understand the underlying blockchain technology, where it came from, and where it is going. The Beginning It is widely believed that the first implementation of modern day blockchain technology came from Satoshi Nakamoto. In 2008, a person or group of people identified as Nakamoto published a paper, "Bitcoin: A Peer to Peer Electronic Cash System," which hypothesized a direct online payment from one party to another without the use of an intermediary third party. The paper described "an electronic payment system based on cryptographic proof instead of trust. While blockchain initially garnered interest because of its ability to be anonymous, such as in the case with cryptocurrencies like Bitcoin, the real appeal of the technology may be due to the complete transparency afforded by it. May 14, 2018 Online Indeed, many have found that the underlying blockchain technology has applications in an ever increasing number of applications in nearly every industry

3. How it works

In order to understand blockchain better, consider an example where you are looking for an option to send some money to your friend who lives in a different location. A general option that you can normally use can be a bank or via a payment transfer application like PayPal or Paytm. This option involves third parties in order to process the transaction due to which an extra amount of your money is deducted as transferring fee. Moreover, in cases like these, you cannot ensure the security of your money as it is highly possible that a hacker might disrupt the network and steal your money. In both the cases, it is the customer who suffers. This is where Blockchain comes in. Instead of using a bank for transferring money, if we use a blockchain in such cases, the process becomes much easier and secure. There is no extra fee involved as the funds are directly processed by you thus, eliminating the need for a third party. Moreover, the blockchain database is decentralised and is not limited to any single location meaning that all the information and records kept on the blockchain are public and decentralized. Since the information is not stored in a single place, there's no chance of corruption of the information by any hacker.

A blockchain, also known as distributed ledger technology (DLT), is nothing more than a digital record, or ledger, of transactions. Unlike a traditional ledger, however, a blockchain is stored collectively by all of the participants on its network. Each transaction is stored with others in a unit of data called a block, and, as the name "blockchain" suggests, those blocks securely link to one another, forming a "chain" of records going all the way back to the very beginning of the ledger. To participate in a blockchain network, a user must operate a software client that will connect it to that blockchain. The software client allows the user to record transactions, and also lends computing power to the Centralized Blockchain. | Distributed ledger technology and designing the future network to help build new blocks of records. Various mechanisms exist for reaching global decentralized consensus on the blockchain as to the legitimacy of transactions broadcast to nodes on the network.

When a user wishes to transfer a digital asset to another user, the user and its counterparty broadcast cryptographically secured digital signatures and the details of their transaction to nearby peers on the network. The users are identified in the transaction by their public keys; this is termed "pseudonymity." When a peer participant solves the mathematical puzzle required for the next block, these pending transactions may now be recorded into a block. That new block is then double checked by other members of the network until a majority agrees that it is correct. Once a majority consensus is achieved, the new block is added to the chain, and the pending transactions are recorded in the ledger

4. Types of Block Chain

Though Blockchain has evolved to many levels since inception, there are two broad categories in which blockchains can be classified majorly i.e. Public and Private blockchains. Before heading towards the difference between these two, let's keep a check on the similarities that both public and private blockchain have Both Public and Private blockchain have peer-to-peer decentralized networks. All the participants of the network maintain the copy of the shared ledger with them. The network maintains copies of the ledger and synchronizes the latest update with the help of consensus. The rules for immutability and safety of the ledger are decided and applied on the network so as to avoid malicious attacks. Now that we know the similar elements of both these blockchains, let's learn about each of them in detail and the differences between them.

5. Public Blockchain

As the name suggests, a public blockchain is a permissionless ledger and can be accessed by any and every one. Anyone with the access to the internet is eligible to download and access it. Moreover, one can also check the overall history of the blockchain along with making any transactions through it. Public blockchains usually reward their network participants for performing the mining process and maintaining the immutability of the ledger. An example of the public blockchain is the Bitcoin Blockchain. Public blockchains allow the communities worldwide to exchange information openly and securely. However, an obvious disadvantage of this type of blockchain is that it can be compromised if the rules around it are not executed strictly. Moreover, the rules decided and applied initially have very little scope of modification in the later stages.

6. Private Blockchain

Contrary to the public blockchain, private blockchains are the ones which are shared only among the trusted participants. The overall control of the network is in the hands of the owners. Moreover, the rules of a private blockchain can be changed according to different levels of permissions, exposure, and number of members, authorization etc. Private blockchains can run independently or can be integrated with other blockchains too. These are usually used by enterprises and organizations. Therefore, the level of trust required amongst the participants is higher in private blockchains.

7. Applications of blockchain

Government: Blockchain Technology (also called Distributed Ledger Technology (DLT)) is a potential vehicle to improve government services and foster more transparent government-citizen relations. The distributed tech can work to dramatically optimize business processes through more efficient and secure data sharing.

Health care: Blockchain Technology has the potential to disrupt the healthcare industry's centralized operations, opening the door for optimized business and service delivery. The Distributed Ledger Technology (DLT) is an innovation fertile with the possibility of improved transparency, security, and efficiency. Smart contracts on the blockchain operate automatically without third-party personnel needed to verify documents or specific steps using pen-and-paper processes. With automation comes a reduction in the notorious bureaucracy that currently stands in the way of patients receiving the best care possible.

Internet of Things: Blockchain technology provides the ideal engine to power a fairly new concept regarding our new connected world: Internet-of-Things. Spending on the internet-of-things market is expected to top the $1 Trillion mark in the coming years. This opportunity is poised for Blockchain Internet-of-Things to step in and provide the ultimate system to track the unique histories of the billions of smart-devices coming online over the next few years.

Insurance: Blockchain Insurance allows for the entire insurance industry to dramatically optimize business processes by sharing data in an efficient, secure, and transparent manner. Using blockchain to revolutionize insurance policies shifts systems onto smart contracts operating autonomously on peer-to-peer networks, helping to phase out antiquated pen and paper processes and eliminate red tape the insurance industry is notoriously riddled with.

Money: Cryptocurrencies provide people across the globe with instant, secure, and frictionless money, and blockchains provide the permanent record storage for their transactions. Prior systems required users to trust a central authority that the monetary supply and payment transfer will not be tampered with.

Real Estate: Blockchain technology will inevitably become a foundational pillar of the real estate industry. In a mostly paper-record based industry, block chain real estate allows for an unparalleled upgrade in how records are stored and recorded. Utilizing blockchain applications in essential functions such as payment, escrow, and title can also reduce fraud, increase financial privacy, speed up transactions, and internationalize markets.

Contract: In blockchain law applications, smart contracts are verified on the block chain, allowing for programmable, self-executing and self-enforcing contracts. Blockchain law also encompasses the idea of "Smart Corporations" which includes concepts such as Decentralized Autonomous Corporations (DAC) or Decentralized Autonomous Organization (DAO).

8. Conclusion

This paper presented an overview on blockchain technology.

References

[1] A. Shanti Bruyn "Blockchain an introduction." August 2017.
[2] Juho Lindman "Novel Uses, Opportunities and Challenges of Blockchain for Digital Services" pp.1833-1836, 2019.
[3] Xin Jiang, Mingzhe Liu, Chen Yang, Yanhua Liu and Ruili Wang, "A Blockchain-Based Authentication Protocol for WLAN Mesh Security Access," Tech Science Press CMC, vol. 58, no.1, pp. 45-59, 2019.

[4] Hong-Mei Chen, Hoh Peter "Introduction to the Blockchain Engineering Minitrack," Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019, pp. 7067-7068.

[5] Sayyad, Mangesh Pawar, Ashutosh Patil, Vandana Pathare, "Features of Blockchain Voting: A Survey," International Journal for Innovative Research in Science & Technology, Volume 5, Issue 9, pp. 12-14, February 2019.

[6] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone (Scarfone Cybersecurity "Blockchain Technology Overview."

[7] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.