International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 12 | Dec 2020 www.irjet.net p-ISSN: 2395-0072

Blockchain Technology- The future Trend

Mouna. G[1], Nagaveni. E[2]

[1,2]B.E. Student, Department of Information Science and Engineering Nagarjuna College of Engineering and Technology, Bangalore, India

---

Abstract: *Blockchain, as a technological innovation of distributed storage, peer-to-peer transaction model, consensus mechanism, and encryption algorithm, has been actively explored by quite a number of governments, organizations, and even individuals. Blockchain has disrupted the traditional practice of the business transaction processing, bringing about new opportunities for value realignment. Blockchains act as decentralized systems for recording and documenting transactions that take place involving a particular digital currency. Put simply, blockchain is a transaction ledger that maintains identical copies across each member computer within a network. The fact that the ledger is distributed across each part of the network helps to facilitate the security of the blockchain. This is mainly characterized by executing the transactions of bitcoin and other cryptocurrencies. It also enables smart contracts for enhancing Distributor-to-consumer transactions.*

Keywords: **cryptocurrencies, decentralized, bitcoin, blockchain.**

1. INTRODUCTION

Blockchain technology is what powers and supports the digital currency space. By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Blockchain originally served as an underlying technology for supporting Bitcoin that emerged in 2009. It is a type of distributed ledger technology with an incremental list of data records named “blocks”, which are validated by all the participating nodes of a network. The blocks and the contents within them are protected by powerful cryptography, which insures that previous transactions within the network cannot be either forged or destroyed. In this way, blockchain technology allows a digital currency to maintain a trusted transaction network without relying on a central authority. It is for this reason that digital currencies are thought of as "decentralized." While blockchain is most famous for its role in facilitating the rise of digital currencies over the past several years, there are also many other non-cryptocurrency uses for this technology. Indeed, some blockchain proponents believe that the technology could far outpace cryptocurrencies themselves in terms of its overall impact, and that the real potential of blockchain is only just now being discovered. As such, it's likely that financial advisors and many others in the investing world will encounter blockchain technology much more in the years to come, whether it is linked with a specific cryptocurrency or if it's being utilized in any number of other applications.

Blockchain is marked with four distinct characteristics as follows:

Decentralized: blockchain is a decentralized and synchronized database that directly bypasses any intermediary, centralized organization, or a third party.

Openness: Blockchain facilitates as open and transparent data source that allows any engaging parties to check the validity of the chain through a public interface.

Immutability: the data blocks stored on blockchain are immutable. Once everybody consents a transaction and records it on a block, the block of data cannot be changed anymore.

Anonymity: the nodes on blockchain are all anonymous, which protects the security and privacy of every node.

2. APPLICATIONS OF BLOCKCHAIN

2.1 Cross-Border Payments:

Traditionally, the transfer of value has been both expensive and slow, and especially for payments taking place across international borders. One reason for this is that, when multiple currencies are involved, the transfer

process typically requires the participation of multiple banks in multiple locations before the intended recipient can actually collect his or her money. There are existing services to help facilitate this process in a faster way, but these tend to by quite expensive.

Blockchain technology has the potential to provide a much faster and cheaper alternative to traditional cross-border payments methods. Indeed, while typical money remittance costs might be as high as 20% of the transfer amount, blockchain may allow for costs just a fraction of that, as well as guaranteed and real-time transaction processing speeds. There are hurdles to be passed, including regulation of cryptocurrencies in different parts of the world and security concerns. Nonetheless, this is one of the most promising and talked about areas of blockchain technology application.

2.2 Smart Contracts:

Smart contract are often seen as a highly powerful application of blockchain technology. These contracts are actually computer programs that can oversee all aspects of an agreement, from facilitation to execution. When conditions are met, smart contracts can be entirely self-executing and self-enforcing. For proponents of smart contracts, these tools provide a more secure, more automated alternative to traditional contract law, as well as an application that is faster and cheaper than traditional methods.

The potential applications of smart contract technology are essentially limitless and could extend to almost any field of business in which contract law would normally apply. Of course, while highly touted, smart contracts are not a magical substitute for old-fashioned diligence. In fact, the case of the Decentralized Autonomous Organization (DAO) is a cautionary tale and a warning to investors to not assume that smart contracts are any better than the information and organization that a user puts into them. Nonetheless, smart contracts remain one of the most exciting ways that blockchain technology has already extended beyond the cryptocurrency space and into the broader business world.

2.3Identity Management:

One of the most problematic results of the internet age has been identity security. As diligent as many individuals and organizations are in maintaining their online identities and securing private information, there are always nefarious actors looking to steal and profit off of these digital items. Blockchain technology has already demonstrated the potential for transforming the way that online identity management takes place.

Blockchain offers a tremendous level of security, thanks to independent verification processes that take place throughout member computers on a blockchain network. In digital currency cases, this verification is used to approve transaction blocks before they are added to the chain. This mechanism could just as easily be applied to other types of verification procedures, including identity verification and many other applications as well.

The applications for blockchain and identity management are wide-ranging. For instance, blockchain could potentially be used to aid in maintaining voter information and ensuring proper functioning of the electoral process. Blockchain could be used to securely and efficiently transfer user data across platforms and systems. The technology could also be used to maintain and protect records of real estate ownership, titles, and more.

Supply Chain Uses:

For many businesses across various industries, a key to success is a well-functioning, efficient supply chain. Blockchain technology has already been used in multiple industries as a means of keeping tabs on supply chains and ensuring their efficiency. This could eliminate human work and the potential for error from a complex and crucial process.

At this point, blockchain is a technology with an exceptionally broad set of potential uses. Although blockchain is most famous for its connections to the blossoming cryptocurrency world, several other applications have already been explored. Perhaps even more exciting, though, is that new ways of utilizing blockchain emerge every day. As such, whether you are directly involved in the digital currency space or not, it's essential to develop an understanding of blockchain and how it may be used to transform the business and investment worlds.

3. WORKING OF BLOCKCHAIN

When we are technically talking about blockchain, it is the chain of blocks where the digital information ("block") is stored in the public database ("chain"). Blocks usually contain digital pieces of information. During the initial transaction any block created contains three parts:

- Blocks store information about transactions like the date, time, and dollar amount of your most recent purchase from Amazon. (NOTE: This Amazon example is for illustrative purchases; Amazon retail does not work on a blockchain principle as of this writing)

- Blocks store information about who is participating in transactions. A block for your splurge purchase from any online website (ex: amazon) would record your name along with Amazon.com, Inc. (AMZN). Instead of using your actual name, your purchase is recorded without any identifying information using a unique "digital signature," sort of like a username.

- Blocks store information that distinguishes them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a "hash" that allows us to tell it apart from every other block. Hashes are cryptographic codes created by special algorithms. Let's say you made your splurge purchase on Amazon, but while it's in transit, you decide you just can't resist and need a second one. Even though the details of your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

While the block in the example above is being used to store a single purchase from Amazon, the reality is a little different. A single block on the Bitcoin blockchain can actually store up to 1 MB of data. Depending on the size of the transactions, that means a single block can house a few thousand transactions under one roof.

When a block stores new data it is added to the blockchain. Blockchain, as its name suggests, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things must happen:

- A transaction must occur. Let's continue with the example of your impulsive Amazon purchase. After hastily clicking through multiple checkout prompt, you go against your better judgment and make a purchase. As we discussed above, in many cases a block will group together potentially thousands of transactions, so your Amazon purchase will be packaged in the block along with other users' transaction information as well.

- That transaction must be verified. After making that purchase, your transaction must be verified. With other public records of information, like the Securities Exchange Commission, Wikipedia, or your local library, there's someone in charge of vetting new data entries. With blockchain, however, that job is left up to a network of computers. When you make your purchase from Amazon, that network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the purchase, including the transaction's time, dollar amount, and participants. (More on how this happens in a second.)

- That transaction must be stored in a block. After your transaction has been verified as accurate, it gets the green light. The transaction's dollar amount, your digital signature, and Amazon's digital signature are all stored in a block. There, the transaction will likely join hundreds, or thousands, of others like it.

- That block must be given a hash. Not unlike an angel earning its wings, once all of a block's transactions have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the blockchain.

When that new block is added to the blockchain, it becomes publicly available for anyone to view—even you. If you take a look at Bitcoin's blockchain, you will see that you have access to transaction data, along with information about when ("Time"), where ("Height"), and by who ("Relayed By") the block was added to the blockchain.

4. SECURITY OF BLOCKCHAIN

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. If you take a look at Bitcoin's blockchain, you'll see that each block has a position on the chain, called a "height." As of January 2020, the block's height had topped 615,400.

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Here's why that's important to security. Let's say a hacker attempts to edit your transaction from Amazon so that you actually have to pay for your purchase twice. As soon as they edit the dollar amount of your transaction, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update

that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on.

In order to change a single block, then, a hacker would need to change every single block after it on the blockchain. Recalculating all those hashes would take an enormous and improbable amount of computing power. In other words, once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.

To address the issue of trust, blockchain networks have implemented tests for computers that want to join and add blocks to the chain. The tests, called "consensus models," require users to "prove" themselves before they can participate in a blockchain network. One of the most common examples employed by Bitcoin is called "proof of work."

In the proof of work system, computers must "prove" that they have done "work" by solving a complex computational math problem. If a computer solves one of these problems, they become eligible to add a block to the blockchain. But the process of adding blocks to the blockchain, what the cryptocurrency world calls "mining," is not easy. In fact, the odds of solving one of these problems on the Bitcoin network were about one in 15.5 trillion in January 2020. To solve complex math problems at those odds, computers must run programs that cost them significant amounts of power and energy (read: money).

Proof of work does not make attacks by hackers impossible, but it does make them somewhat useless. If a hacker wanted to coordinate an attack on the blockchain, they would need to control more than 50% of all computing power on the blockchain so as to be able to overwhelm all other participants in the network. Given the tremendous size of the Bitcoin blockchain, a so-called 51% attack is almost certainly not worth the effort and more than likely impossible.

5. BLOCKCHAIN VS. BITCOIN

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. That concept can be difficult to wrap our heads around without seeing the technology in action, so let's take a look at how the earliest application of blockchain technology actually works.

Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.

The Bitcoin protocol is built on the blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator Satoshi Nakamoto referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party."Here's how it works.

You have all these people, all over the world, who have bitcoin. There are likely many millions of people around the world who own at least a portion of a bitcoin. Let's say one of those millions of people wants to spend their bitcoin on groceries. This is where the blockchain comes in.

When it comes to printed money, the use of printed currency is regulated and verified by a central authority, usually a bank or government—but Bitcoin is not controlled by anyone. Instead, transactions made in bitcoin are verified by a network of computers. This is what is meant by the Bitcoin network and blockchain being "decentralized."When one person pays another for goods using bitcoin, computers on the Bitcoin network race to verify the transaction. In order to do so, users run a program on their computers and try to solve a complex mathematical problem, called a "hash." When a computer solves the problem by "hashing" a block, its algorithmic work will have also verified the block's transactions. As we described above, the completed transaction is publicly recorded and stored as a block on the blockchain, at which point it becomes unalterable. In the case of Bitcoin, and most other blockchains, computers that successfully verify blocks are rewarded for their labor with cryptocurrency. This is commonly referred to as "mining."

Although transactions are publicly recorded on the blockchain, user data is not—or, at least not in full. In order to conduct transactions on the Bitcoin network, participants must run a program called a "wallet." Each wallet consists of two unique and distinct cryptographic keys: a public key and a private key. The public key is the location where transactions are deposited to and withdrawn from. This is also the key that appears on the blockchain ledger as the user's digital signature.

Even if a user receives a payment in bitcoins to their public key, they will not be able to withdraw them with the private counterpart. A user's public key is a shortened version of their private key, created through a complicated mathematical algorithm. However, due to the complexity of this equation, it is almost impossible to reverse the process and generate a private key from a public key. For this reason, blockchain technology is considered confidential.

6. CONCLUSION

Blockchain is a hugely important, transformative technology that will re-shape businesses. To keep up with the fast evolving technology is a challenge that every business leader face. And this also makes a history of any digital asset unalterable and transparent through the use of decentralization and cryptographic hashing. The decentralized distribution chain gives everyone access to the document at the same time. Blockchain is an especially promising and revolutionary technology because it helps reduce risk, stamps out fraud and brings transparency in a scalable way for myriad uses. This also increases the scope of miners in the industry through the growing blockchain technology.

REFERENCES

1. J. Kehrli, "Blockchain 2.0- From Bitcoin transactions to smart contract applications," Nov.2016.

2. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain", IEEE consumer electronics. Mag, vol 7, jul 2018.