Journal of Informatics
Electrical and Electronics Engineering, 2020,
Vol. 01, Iss. 01, S. No. 004, pp. 1-9
ISSN (Online): 2582-7006

Introduction to Blockchain

Amarpreet Sahani [1], Pawan Singh[2], Anil Kumar[3]

[1,2]Department of Computer Science and Engineering, Amity School of Engineering and Technology, AUUP, Lucknow, India
[3]Department of Electrical Engineering, Amity School of Engineering and Technology, AUUP, Lucknow, India.

How to cite this paper: A. Sahani, P. Singh and A. Kumar (2020) Introduction to Blockchain. *Journal of Informatics Electrical and Electronics Engineering*, Vol. 01, Iss. 01, S. No. 4, pp. 1-9, 2020.

http://doi.org/10.54060/JIEEE/001.01.004

Received: 15/01/2019
Accepted: 22/02/2019
Published: 25/04/2020

Abstract

The current monetary system has many issues associated with it like double spending, standard transaction fees, financial crisis, centralized power and private ledgers. Blockchain provides a remedy to all these ills by its basic structure, zero or minimal transaction fees and by providing a public ledger system which is visible to everyone who is the part of blockchain which makes it free from complications like double spending and financial crisis. Blockchain is basically a continuously growing list of records or public distributed ledger system called blocks linked and secured suing cryptography. Each block has multiple transaction details associated with it. It was introduced in the year 2009 by Satoshi Nakamoto, who is believed to be a Japanese man, born in 1974. Given the features and universal nature of the Blockchain, which include decentralized ledger system, proof of work and cryptography, one can appreciate that its implementation could result in far reaching changes in all domains.

Keywords

Component, Formatting, Style, Styling, Insert (keywords)

1. Introduction

Blockchain is the spine and the core technology behind bitcoins and the cryptographic system. It was introduced in the year 2009 by Satoshi Nakamoto, who is believed to be a Japanese man, born in 1974. Although it still remains a mystery who Satoshi Nakamoto is, one thing is for sure that he is one of the most interesting people as he not only came up with such a complex system but also provided a remedy to all the ills in the current monetary system. The blockchain and bitcoin was one of the key features that led to the idea of decentralized digital currency system. Blockchain is the technology that uses a publically distributed database holding encrypted ledgers. These ledgers hold a set of transactions which are verified and validated. These transaction details are hashed, encrypted and stored as a part of new block. Every transaction you use using blockchain gets added to a transaction pole, from which people verify the transaction and add it to a block. Presently, the number of transactions added to each block is 2050. In the present scenario every new block gets created every 10 minutes. This is presently fixed i.e. every 10 minutes a new block gets added to the blockchain. This varies with respect to the com-

plexity as well as the effort put in to create a new block. For every block the creator, called as miner gets 12.5 Bitcoins as a reward. This is the only way new bitcoins are created.

The first monetary system that came into existence was the Barter System. In this system people exchanged one kind of good for the other, instead of any fixed monetary. Barter system was followed by Ledger System, where gold coins were used to buy goods. Then came the age of Flat Money where paper currency was used instead of gold coins in exchange of goods. This was followed by Online Banking and Digital Banking which made it easier for us to sell and purchase goods. The online and digital banking was accompanied with implementation of Bitcoins as well as other Cryptocurrencies which were based on the decentralized digital system. The first blockchain was implemented in January 2009.

In this research the blockchain technology is explored. The first section deals with the discussion of the issues with the current system and how blockchain helps solving those issues. It also talks about various types and features of blockchain. In the second part, the immutability and the proof of work of blockchain is examined.

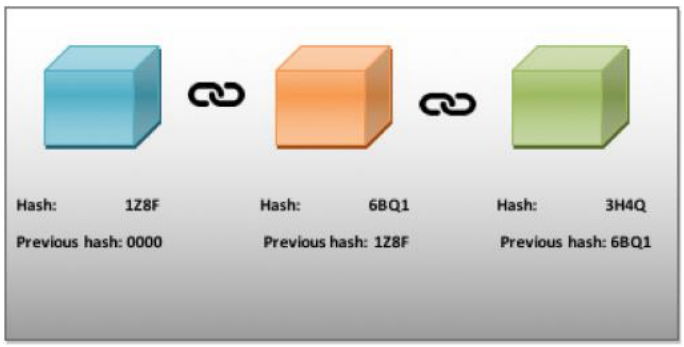

Figure 1: Structural view of blockchain

2. Features of blockchain

2.1 Peer to peer network

The collection of different nodes associated in the blockchain system together form a Peer to Peer network. Anyone who is associated with the blockchain system is a Node i.e. we are a complete node if we have a complete blockchain downloaded to the system and have a complete copy of the ledger as well. Apart from this, there are also some special nodes called Miners, who validate the transactions and work on building a new block. All blockchains run on a distributed peer to peer network i.e. the ledger holding all details of the transaction is completely decentralized (distributed). In this network, a complete copy of the transactions is provided to everyone who is a part of the network [4].

Suppose A finds the transaction: B pays 5 BTC to C. Once A identifies this transaction, he broadcasts it to both B and C that, it has been verified that B has enough balance to send it to C and thus the transaction has been approved. After the validation of the transaction, both B and C forward the transaction details to their peers i.e. to the nodes they are connected to. These details keep propagating throughout the network by repeating the same process. This is one of the major benefits that we earn I few are part of a peer to peer network i.e. we don't have to manually transfer the details, it gets propagated automatically when we send it to one of the nodes. The transaction details which get propagated are nothing but a digital signature (which is highly encrypted and secure) telling each node that a transaction has taken place and the ledger needs to be updated.

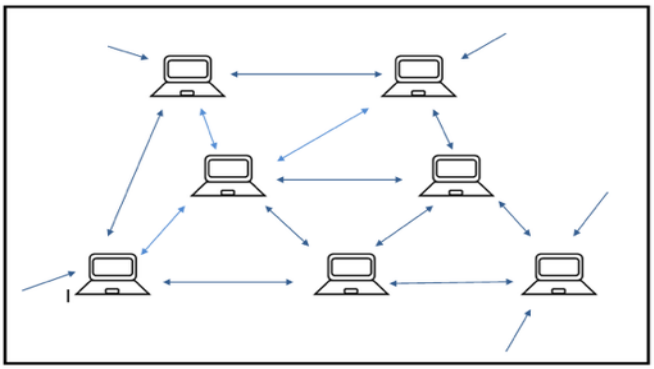

Figure 2: Peer to peer network

This concept proves to be highly useful if someone tries to manipulate the data to earn a profit out of it, as it is not possible in this type to network where everyone apart from the user has a complete copy of the ledger, thereby neglecting the changes made, and finally maintaining the consistency.

2.2. Blockchain program

Blockchain basically was an implementation or solution to create rules in the blockchain. Multiple operations can be performed using blockchain. Example: storing id cards of all citizens, validation of bitcoins etc. A blockchain program can be implemented using any programming language. It was originally written using C++ and JAVA. The most preferred and popular programming language to write a blockchain program is Solidity, since it is one of the most secure programming languages. Different blockchains have different programs in them. It is not necessary that each blockchain should have only one program, it may have multiple programs as part of it.

2.3 Cryptography

In order to make the transactions secure and immutable a public key and a private key cryptography is used to ensure that the user cannot be identified by anyone. In addition to this various hash functions are used to protect anything that is a part of the blockchain from modification. In the process of cryptography two keys are used, public and private key. Once we encrypt our data using either of the keys, we can decrypt it using the other one. [2].

Digital signature is one of the major reasons which ensure that the transactions cannot be modified and are fully secure. We first feed the data, containing a public key of the sender, public key of the receiver as well as the amount of bitcoins which have to be transferred into a hash algorithm. This is given a specific hash value which we can encrypt using private key. Once it is encrypted, it is added as a digital signature to our document which is broadcasted in the peer to peer network waiting for someone to verify it. When we broadcast, the details are received by a specialist, who takes the data from the document, hash it, and decrypt the digital signature and hash it as well. If the hash values obtained from decrypting as well as hashing the data present are same, we can ensure that the transaction is valid.

2.4 Proof of work

Proof of work is basically a mathematical proof in which a mathematical puzzle needs to be solved for the creation of another block.[1].In other words, it a computationally expensive puzzle needs to be solved to add a block to the blockchain. This is done by the people known as Miners. Apart from solving this mathematical problem, the miners also validate the changes made in the blockchain system. After successfully getting the Nonce i.e. the solution of the puzzle, miners get a desired hash value which is predetermined and the block is mined.

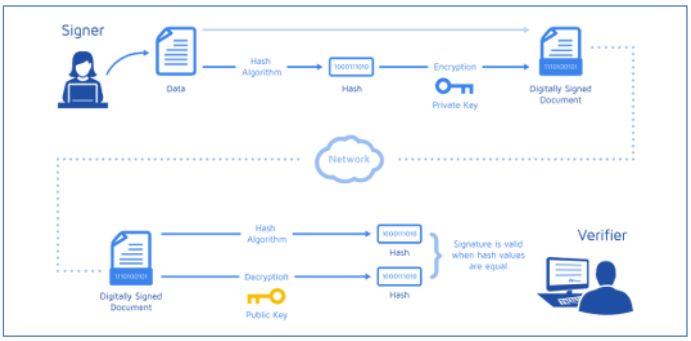

Figure 3: Proof of work

The mathematical solution ensures the validity and the verification of the transactions which are a part of the block.

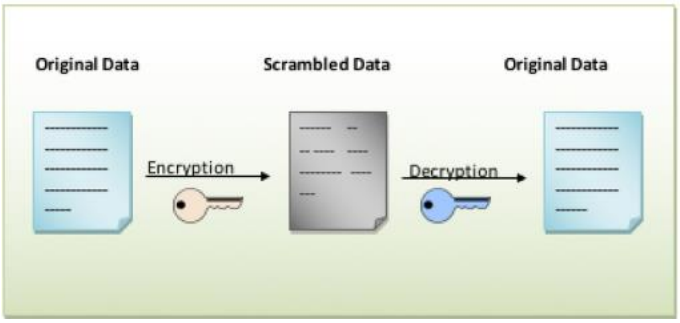

Figure 4: Working of blockchain

3. Issues with current system

3.1. Double spending

It is a fraud done in the digital currency system where illegal certificates can be used to initiate the transaction when one does not have sufficient balance. Example: Peter has $500 in his bank account, and at the same time he tries to send Anthony $400 and Rachel $500. If both the transactions take place at the same time, it becomes problematic to identify which transaction is valid, as the digital signature attached to the digital transaction can be to an extent forged or breached. This makes double spending possible. Bank transactions are prone to double spending.

3.2. Standard transaction fees

The transaction performed with the participation of third parties involves a lot of transaction fees. Most banking and financial organizations depends on the transaction fees as their source of income. Every transaction made by us through ATM, transfer or withdrawal everything is associated with a transaction fee. In the year 2015, three organizations, JPMorgan Chase, Bank of America and Wells Fargo, through ATM and overdraft transaction fees, earned about $6 million.

3.3. Centralized power and private ledgers

Every monetary system, out there today, is controlled by a central governing authority like a federal body or an anonymous personality. Almost all currencies are controlled to an extent by a central authority. Most banking and financial organizations follow a private ledger. Private ledger does not give us a clear picture of what is happening with our money whether it is being invested by the bank or not, which leads to financial crashes.

3.4. Financial crisis

Financial crisis is one of the biggest issues when we trust a third party. Due to depression and fractional reserve banking banks have become synonymous with crisis and crashes. This happens when we give all our money to a third party, we trust in, which in order to gain a profit out of it, creates a trouble not only for itself but for the us as well.

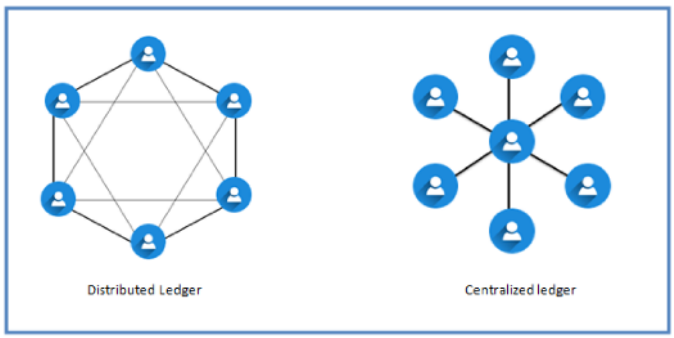

Figure 5: Transformation of ledger system using Blockchain

4. How Blockchain helps

Blockchain not only uses a decentralized ledger system, where each and everyone who is a part of the transaction gets access to the ledger but also follows a public ledger system i.e. it is visible to everyone who is the part of blockchain [5].Being a part of blockchain, we get a full copy of the transaction details i.e. how much amount is being transferred, from whom and to whom. Even this data is fully secure and encrypted. No one can decrypt the data and get the actual transaction details. A public and a private key are used for the encryption and decryption process.

Transactions are immutable, can't be hacked. It has never been hacked till date. There might be certain organizations or applications associated with blockchain being hacked, but the core technology of the blockchain has never been hacked The basic structure of the blockchain helps solving the issue of double spending. The transaction fee being zero or minimal in comparison to third parties like banks or digital transfer system, is the best part of cryptocurrencies. The transaction fee is upto the user. Since there are millions and zillions of transactions occurring globally, if a transaction fee is added to the transaction, it is taken as priority [7].

5. Applications of blockchain

Monetary aspect is just the tip of the iceberg of the blockchain technology. Blockchain is a ground breaking technology for which money is merely one of the possible applications.

5.1 Banks

In the banking domain, blockchain is currently overtaking as well as replacing the existing system of payment and transactions. Imagine what could happen if banks also implement blockchain, although it would increase the probability of reduction of jobs in these domains, but the hacking of the bank ledgers would become close to impossible due to the basic structure of blockchain. It would not only solve the issue of double spending but also reduce the bank crisis to a large extent. Since in case of blockchain, we get a clearer picture of what is happening with our money, it would also work as a shield again the issues like financial crisis. The first trade transaction using blockchain was first carried out by Barclays in September, 2016. NASDAQ will soon run on blockchain trading. [9].

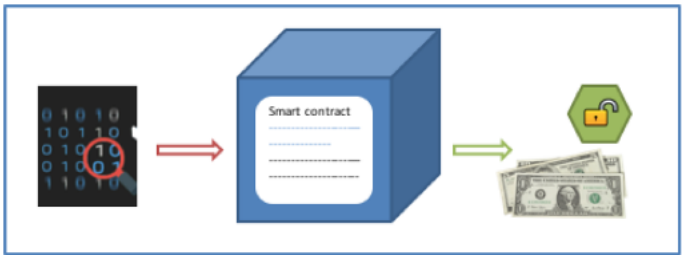

Figure 6: Smart contract

5.2 Payment and Transfers

It becomes quite easy for anyone to transfer their bitcoins or other cryptocurrencies to other users because of the rapid growth of the Bitcoin Wallet System. And these days we don't even need to bother about entering a public key, all we need to do is, scan a unique UR code which is present as a part of the blockchain wallet, and the complete transaction takes place smoothly. The security feature provided by the blockchain system completely alters the payment and transfer system.

Transaction fee is optional. If we have a huge transaction to make and we need it to be performed immediately, in that case we may attach certain fee to it, which will ensure our transaction to become a priority. This is one of the ways of miners to earn a profit in exchange of their resources and the effort they put in. This does not imply that the transaction with no fee attached to it does not get validated. Apart from this, we also do not require any account number to be linked with our bitcoin wallet, give our complete details or attend to annoying calls from banks or other financial organizations. And anonymity is completely maintained.

5.3 Internet of things (IOT)

Internet of things is one of the major current domain using the blockchain system to ensure that the transfer of data between the devices without the involvement of any sort of corruption or interferences. [3].

5.4 Voting

This is the domain which is getting revolutionarised using the blockchain technology. There is a strong possibility that next or next to next elections would be made quite convenient as well as secure and fail proof by the implementation of blockchain. Using a blockchain for voting is one of the most important ideas, which has also become a great attention seeker these days. A small Baltic Nation called Estonia is the first to implement blockchain base e-voting system.

This idea if implemented, would allow users to give their vote sitting at home. Everyone will be given a unique account number and every vote will be considered as a smart contract. [6]. It would also ensure that no duplicate votes are cast and no voting frauds are possible. The world's first open source online voting solution based in blockchain is Follow my vote.

Using the signature, the identity of everyone who is voting is authenticated and their personal information is secured. It also prevents vote frauds, lost records or foul play happening during the counting, tracking or casting of votes. As everyone is ensured that their personal details will not be leaked and no one will come to know, whom they have voted for; it would result in the increase in voter turnout. Instead of this, it is comparatively convenient for the people to become a part of the blockchain and cast their vote to their favorite candidate.

5.5 Supply demand

In this supply demand field, we can establish a consortium or a private blockchain, so that it can be modified only by the ones who are on the governing board. And the details can be viewed by anyone who is a part of the blockchain. Thus, both the

suppliers and the demanders get a clearer picture of what is happening with the goods, where exactly it is or which stage of the whole process it is.

IBM is one example of the same system which has faced a drastic change with respect to the supply chain market by the implementation of the idea of blockchain.

5.6 Music Streaming

Online music is something that is rapidly growing. Close to 90% of the artists' proceedings go because of the illegal downloading from the internet. Due to the involvement of blockchain, the music domain is completely changing and putting up its music on the blockchain. So that in addition to making it accessible to everyone, it is protected from any kind of change or modification. If a particular customer has paid for a particular song then he is provided with the details so that he also can take it from the blockchain.

The first online blockchain based platform called, Mycelia allows the artists to sell their work directly to the customers. This in turn also avoids the participation of a recording company which takes certain amount of the profit earned from the artist. Thus the implementation of the blockchain concept in the music domain not only increases the profit earned by the artist but also ensures that the illegal downloads are entirely eliminated.

5.7 Law Enforcement

In order to ensure a highly accessible database with respect to the criminals and the crimes committed by them, the law enforcement agencies are using blockchain. This is something which we would see coming up quite soon. This is also one of the domains which is being influenced by the concept of blockchain. The day is not far when we would be buying properties from the real estate using the blockchain. Blockchains reduce all the hustle of huge paperwork and the entire agent based fees. Not only this, we would also be provided with a real-time update on the transaction regarding the verification of property, verification of the documents, who is signing the document and when etc. Ubitquity provides an online blockchain system, using which anyone can manage, transfer land tiles and property deeds.

5.8 Health care

Healthcare is the domain where the concept of blockchain is used to store the details of the patients. Since the concept behind blockchain is a highly secure, no one can directly access the details and make any modifications in it. This ensures the anonymity of the patients. This domain involves the usage of consortium blockchains so that only selected people mainly the doctors can view the complete records of the patients. This ensures that if a patient is admitted in a different hospital, there is no need of sending his complete details across; instead the details can be directly accessed using blockchain.

Thus the implementation of the blockchain concept has completely revolutionarised healthcare industry. A study of IBM, Healthcare Rallies, found that about 16% of the healthcare associations plan to implement the blockchain solution this year, 56% plan to implement it by the year 2020. The issues which afflict the industry presently can be solved using the blockchain, by creating a common database for storing the health information that can be accessed by doctors irrespective of the electronic medical system used by them. It also ensures security of data and privacy of the patients, enabling the doctors to spend more time on patient care by reducing the admin time. In addition to this, it promotes better research results to facilitate new medicines and treatment therapies for patients. As per the current scenario, the healthcare organizations are flooded with data which includes patient's medical records, billing, medical research, information regarding medicines etc. Thus the adoption of the blockchains in this sector would prove as a boon to the healthcare industries and organizations.

5.8.1 Management of Medical Data

In order to improve electronic medical records and allow patients' details to be accessed securely, MedRec is a prototype implementing the concept of blockchain. In addition to this, it results in solving waste of time, money, hustle, confusion and also the issue related to the distribution of records across many different healthcare institutions. Giving the patients and the healthcare industry one-step access to the complete medical details and records is the primary goal of MedRec. All these facts prove that how drastically the healthcare industries and organizations would improve by deploying the blockchain technology.

5.8.2 Development of drugs

The deployment of the blockchain concept in healthcare domain, in addition to facilitating a new drug development by providing convenient access to complete medical records of the patients, can also result in the decrement of the fake and forged drug inferences which presently costs the loss of approximately $200 billion annually to the pharmaceutical companies.

5.8.3 Management of bills and claims

The implementation of the blockchain concept can reduce the medical frauds which, in 2016 caused the loss of approximately $30 million in United States. Additionally, through efficient processing and eliminating the need of third parties by automated activities, it results in the decrement of the admin costs.

5.8.4 Medical Research

Improvement of care and patient outcomes can be improved by centralizing the outcomes of clinical trials and the result of new treatment. Presently, there is no method through which a human can process the entire data recorded in separate systems for future treatment possibilities with the diverse and disconnected systems in play. A quick access to make medical innovations and researches can be made possible through the blockchain concept.

5.8.5 Data Security

As per the Protenus Breach Barometer report, between 2015 and 2016, the records of about 140 million patients were breached. The health IT architecture is putting in a lot of effort to keep the systems free from hacks, through the rapid growth of connected devices and the Internet of Medical Things (IoMT). Thus it can be said that the potential to be the framework that is a requirement to keep the health data private and completely secure lies in the solutions based on the concept of blockchain. New methods as to how blockchain can better support the working and operation of the medical domain, are being discovered by the healthcare industry.

These are just some of the popular domains; in addition to these blockchain is being used in various other fields. There are numerous other organizations that are investing in the blockchain concept and earning a profit out of it. [10].

6. Conclusion

Blockchain is trending technology that involves various mathematical algorithms and functions for the creation of a highly secure and a distributed ledger system which enables the execution of the transactions without the involvement of any financial organization. This is the reason why blockchain is often referred as a No Trust System i.e. you need not some third person or any organization for carrying out your transaction. At present the blockchain network is globally distributed, so if anyone wants to modify the transaction, he/she has to get the transaction (modified one) accepted by the majority i.e. by more than 50% of the group that is a part of the blockchain. It means he/she needs the approval of more than 50% of mil-

lions of people, present around the world, who are a part of the blockchain. This is not possible which implies that the blockchain works on a very complex technology which cannot be hacked or modified and also works as a remedy to all the problems in the current monetary system. Although many organizations and industries are getting revolutionarised by the implementation of the blockchain concept, it should always be kept in mind that it is a marathon, not a sprint. The different organizations and industries are experimenting how their domains can be better supported by the blockchain technology, while the future applications will inevitably be discovered along the way. It will be a compulsive and a captivating process to watch.

References

[1]. F. M. Ametrano, "Bitcoin and Blockchain Technology, "Proceeding of ICC Italia Conference, Rome, Nov 2016.

[2]. G. Foroglou, and A.L. Tsilidou, "Further applications of the blockchain, "Proceedings of the 12th Student Conference on Managerial Science and Technology, Athens, Greece, pp.1-9, May 2015.

[3]. D. Tapscott, and A. Tapscott, (2018) "Blockchain Revolution, "McKinsey Publishing, McKinsey's New York ,2018.

[4]. M. Lansiti, and K. R. Lakhani, "The Truth about blockchain, "Harward Business Review,Feb 2017 .

[5]. C. Cachin, "Blockchain, cryptography, and consensus, "ITU Workshop on "Security Aspects of Blockchain", Geneva, Switzerland, March 2017. https://cachin.com/cc/talks/20170622-blockchain-ice.pdf

[6]. K. Danial, "EOS: Is This Futuristic Blockchain All It's Cracked Up to Be, "Talk Markets Dec 2018. https://talkmarkets.com/content/eos-is-this-futuristic-blockchain-all-its-cracked-up-to-be?post=202495

[7]. G. Peters, E. Panayi, A. Chapelle, "Trends in Cryptocurrencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective, "Journal of Financial Perspectives, Vol. 3, No. 3, pp.1-43, 2015.

[8]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System, "[online] Available: https://bitcoin.org/bitcoin.pdf, pp.1-9, March2009.

[9]. K. Trublet, "Ether Cryptocurrency, a Victim of Blockchain Success, " Agence France-Presse, published on Sep, 2018.

[10]. A. Narayanan, J. Bonneau, E. Felten, et al., "Bitcoin and cryptocurrency technologies: a comprehensive introduction ", Princeton University Press, Princeton University Press Princeton, NJ, USA, , pp.1-291, 2016.