Methodize of Block Chain Technology

M. J. Abinash, V. Vasudevan

Abstract*: *A blockchain is a collection of records with cryptography. All records or exchanging information are checked by all members. Once enter the information's into the blockchain record means, it will be never changed or deleted. Distributed and Peer authentication technology is used in blockchain technology. A blockchain is maintaining a record in decentralized with high secure manner, so all users are easily accessed. Blockchain technology is mainly used in financial sectors and banking sectors. This new technology mainly used in IoT, Gaming and entertainment sector, Government Public services, online fund transformation, etc. In today world, blockchain technology mainly used exchanging the documents and money. In blockchain technology is based on the bit coin money transaction. This bit of coin technology will be reducing the intermediate of the money transformation. The main scope of the blockchain technology is both money related and non-financial world.

Keywords* : *Blockchain, bit coin, cryptography.

I. INTRODUCTION

The principle of the theory in block chain is maintaining the secured records in online. Each and every time user wants to access the record means, authorized person only access the information's.

Bit coin is the most well-known model that is characteristically attached to Block chain innovation. It is likewise the most questionable one since it empowers a multibillion-dollar worldwide market of unsolved exchanges with no administrative control. Henceforth it needs to manage various administrative issues including national governments and monetary foundations.

Be that as it may, Block chain innovation itself is non-questionable and has worked impeccably throughout the years and is by and large effectively connected to both money related and non-monetary world applications. A year ago, Marc Andreessen, the doyen of Silicon Valley's business people, recorded the Block chain disseminated accord model as the most significant innovation since the Internet itself. Johann Palychata from BNP Paribas wrote in the ideal magazine that bit coin's Block chain, the product that permits the advanced money to capacity ought to be considered as an innovation like the steam or ignition motor that can possibly change the universe of account and past.

Current computerized economy depends on the dependence on a specific confided in power. Everything on the web exchanges depend on confiding in somebody to disclose to us reality it very well may be an email specialist co-op revealing to us that our email has been conveyed; it tends to be a confirmation expert disclosing to us that a specific advanced endorsement is reliable; or it very well may be an informal organization.

The benefits of blockchain innovation exceed the administrative issues and specialized difficulties. One key rising use instance of blockchain innovation includes "keen contracts". Brilliant contracts are essentially PC programs that can naturally execute the terms of an agreement. At the point when a preconfigured condition in a keen contract among partaking substances is met then the gatherings associated with a legally binding understanding can be naturally made installments according to the agreement in a straightforward way.

Shrewd Property is another related idea which is with respect to controlling the responsibility for property or resource by means of blockchain utilizing Smart Contracts. The property can be physical, for example, vehicle, house, cell phone and so on or it tends to be non-physical, for example, offers of an organization. It ought to be noted here that even Bit coin isn't generally cash Bit coin is tied in with controlling the responsibility for.

Non-Financial applications openings are additionally unending. We can imagine putting verification of presence of every single authoritative report, wellbeing records, and faithfulness installments in the music business, legal official, private securities and marriage licenses in the blockchain. By putting away the unique mark of the advanced resource as opposed to putting away the computerized resource itself, the secrecy or protection target can be accomplished.

II. RELATED WORKS

In 2008, Bit coin technology was introduced [1]. In this technology mainly used for money transformation with secured. In this financial transaction no need intermediate [2]. It is a main feature of the block chain technology. In block chain technology mainly used bit coin money transformation technology. This new technology used for money transaction without intermediate [3]. The author [4] proposed the transaction of the music to another networks used by block chain technology. This is new business like iTunes.

In block chain transaction used for the secured transaction. Sometimes some mistakes are occurs based on the human mistakes. If one human mistake will happen means organization or industries to make more and more likely [5]. In public health information's also stored in block chain manner. All health information's are transferred and maintained in data base.

Revised Manuscript Received on December 15, 2019.

***** Correspondence Author

Abinash*, Department of Information Technology, Kalasalingam Academy of Research and Education, Srivilliputhur, India. Email: mj.abinash@gmail.com

Vasudevan, Department of Information Technology, Kalasalingam Academy of Research and Education, Srivilliputhur, India. Email: vasudevan.klu@yahoo.co.in

This type of technology is called Protected Health Information's [6]. HIPAA (Health Insurance Portability and Accountability Act of 1996) [7] is a main rule of the protection of the health information. In HIPAA is stored the all patient information is stored individually with secured manner. This information's are stored like block chain technology. In block chain technology mainly used inside the supply chain technology with ERP [8]. In social network, block chain technology mainly used. Authentication process and also all information's are stored to the linked format. This process is a user friendly [9].

A. Short History of Bit coin

In year 2008, an individual or gathering composing under the name of Satoshi Nakamoto distributed a paper entitled "Bit coin: A Peer-To-Peer Electronic Cash System" [1]. This paper portrayed a shared adaptation of the electronic money that would enable online installments to be sent legitimately starting with one gathering then onto the next without experiencing a monetary establishment. Bit coin was the first acknowledgment of this idea. Presently word cryptographic forms of money are the mark that is utilized to depict all systems and mechanisms of trade that utilizes cryptography to verify exchanges as against those frameworks where the exchanges are directed through a brought together confided in element.

A couple of months after the fact, an open source program actualizing the new convention was discharged that started with the Genesis square of 50 coins. Anybody can introduce this open source program and become some portion of the bitcoin shared system. It has developed in prominence from that point forward.

- 2008
  - **August 18** Domain name "bitcoin.org" registered
  - **October 31** Bitcoin design paper published
  - **November 09** Bitcoin project registered at SourceForge.net
- 2009
  - **January 3** Genesis block established at 18:15:05 GMT
  - **January 9** Bitcoin v0.1 released and announced on the cryptography mailing list
  - **January 12** First Bitcoin transaction, in block 170 from Satoshi to Hal Finney

Fig. 1.History of bitcoin technology.

The prevalence of the Bitcoin has never stopped to increment from that point forward. The fundamental Block Chain innovation is presently finding new scope of utilizations past money.

B. How does it work?

We clarify the idea of the blockchain by clarifying how Bitcoin functions since it is naturally connected to the Bitcoin. Be that as it may, the blockchain innovation is appropriate to any computerized resource exchange traded on the web.

In web business, all records are confidentially transfer to the another person. Third party members are not access and modify the records. So bit coin technology is believed by outsider. In bit coin technology exchange the cost will be high. In bit coin technology is used by the cryptography. When exchange the money or other information, user transaction information will be encoded used the secured key. This encoded information will be non-readable format. So, outsider was believed the bit coin technology.

Every money transaction in this technology used by the public key and the private key. Private Key is a main responsible for the money transaction of the block chain technology. Every transaction and exchange information's are recorded. Each and every exchange should be confirmed for legitimacy before it is recorded in the open record. Confirming hub needs to guarantee two things before account any exchange. Figure.2 show the working principles of block chain technology.

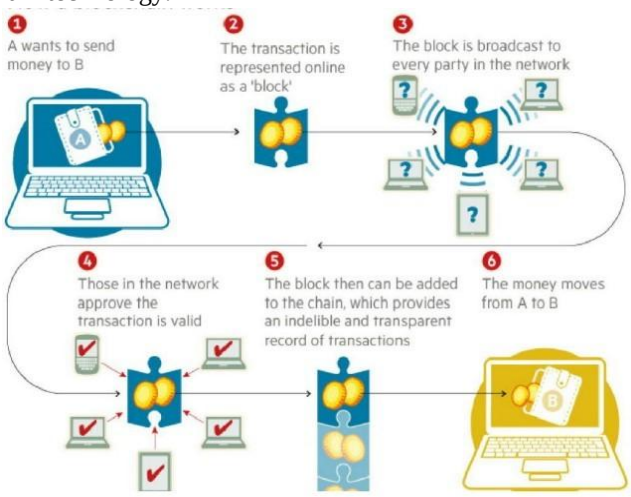

Fig. 2.Financial transaction using blockchain technology.

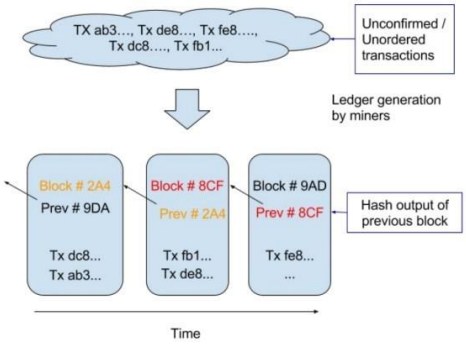

Fig. 3. Generation of block chain from unordered transaction

In bit coin exchange [10], every information pass by the Hub in distributed systems. The exchanges don't come all together in which they are created and thus there is requirement for a framework to ensure that twofold spending of the digital currency does not happen. Taking into account that the exchanges are passed hub by hub through the bitcoin organize, there is no assurance that orders wherein they are gotten at a hub are a similar request where these exchanges were created.

This implies there is have to build up a component with the goal that the whole Bit coin system can concur in regards to the request of exchanges, which is an overwhelming assignment in a dispersed framework.

Figure.3 shows the block chain transaction from unordered transaction. Unordered information's are transferred to the ordered format used by the block chain innovation. Unordered information transfer to the ordered format used by the linked list concept. In linked list is used the collection of nodes. Each node denotes the square in figures. Each square connected to the next square used by the linked list concept, this is called block chain. In each square have the previous square hash information.

There still stays one issue. Any hub in the system can gather unverified exchanges and make a square and after that communicates it to rest of the system as a recommendation about which square ought to be the following one in the blockchain. How does the system choose which square ought to be next in the blockchain? There can be different squares made by various hubs in the meantime. One can't depend on the request since squares can touch base at various requests at various focuses in the system.

Bitcoin takes care of this issue by presenting a scientific riddle: each square will be acknowledged in the blockchain gave it contains a response to an extraordinary numerical issue. This is otherwise called "confirmation of work" hub producing a square needs to demonstrate that it has put enough figuring assets to illuminate a numerical riddle. The normal exertion required is exponential in the quantity of zero bits required however confirmation process is exceptionally basic and should be possible by executing a solitary hash.

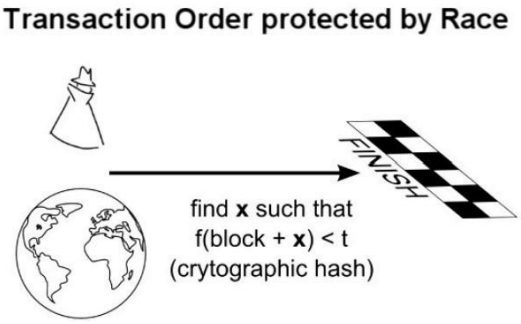

Fig. 4.Protection of the I3- transaction based on mathematical race.

This numerical puzzle isn't minor to understand and the difficulty of the issue can be balanced so that overall it takes ten minutes for a hub in the Bitcoin system to make a right idea and create a square. There is exceptionally little likelihood that more than one square will be created in the framework at a given time. First hub, to take care of the issue, communicates the square to rest of the system. Every so often, be that as it may, more than one square will be settled at a similar time, prompting a few potential branches. However, the math of comprehending is very convoluted and henceforth the blockchain rapidly balances out, implying that each hub in understands about the requesting of hinders a couple over from the finish of the chain. The hubs giving their processing assets to explain the riddle and produce square are classified "minor nodes" and are monetarily granted for their endeavors.

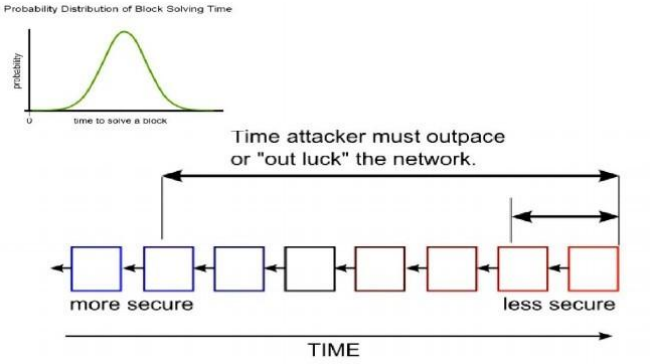

Fig. 5.Protection of the II4- transaction based on mathematical race.

The system just acknowledges the longest blockchain as the substantial one. Henceforth, it is alongside unthinkable for an attacker to present a fake exchange since it has not exclusively to produce a square by understand a numerical puzzle however it needs to in the meantime numerically race against the great hubs to produce every single resulting hinder all together for it cause different hubs to acknowledge its exchange and square as the legitimate one. This activity turns out to be even progressively troublesome since squares in the blockchain are connected cryptographically together.

III. MAIN PROPERTIES OF BLOCK CHAIN TECHNOLOGY

The three principle properties of Block chain Technology which have helped it increase broad praise are as per the following:

- Decentralization
- Transparency
- Immutability

A. Decentralization

In a decentralized framework, the data isn't put away by one single element. Truth be told, everybody in the system possesses the data.

In a decentralized system, in the event that you needed to associate with your companion, at that point you can do as such straightforwardly without experiencing an outsider. That was the principle belief system behind Bit-coins. You and just only you are accountable for your cash. You can send your cash to anybody you need without experiencing a bank.

B. Transparency

Well… an individual's personality is shrouded by means of complex cryptography and spoke to just by their open location. In this way, if you somehow managed to look into an individual's exchange history, you won't see "Balusent 1 BTC" rather you will see

"1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7NZJ sent 1 BTC". The following figure.5 of ethereal transactions will show you what we mean:

Fig. 6.Sample transaction details in block chain technology.

Along these lines, while the individual's genuine personality is secure, you will in any case observe every one of the exchanges that were finished by their open location. This dimension of straightforwardness has never existed inside a money related framework. It includes that additional, and truly necessary dimension of responsibility which is required by a portion of these greatest foundations.

Talking absolutely from the perspective of digital currency, on the off chance that you know the open location of one of these enormous organizations, you can just pop it in a traveler and take a gander at all the exchanges that they have occupied with. This powers them to be completely forthright, something that they have never needed to manage.

In any case, that is not the best use-case. We are almost certain that a large portion of these organizations won't execute utilizing digital forms of money, and regardless of whether they do, they won't do ALL their exchanges utilizing cryptographic forms of money.

C. Immutability

Immutability is the one of main principle is Block chain technology; because any one of the information will be entering in to block chain, it will be not changing anybody. In this technology mainly used in the business people, banking sectors.

In block chain technology, our information will be changed to unread format used by cryptography hash function technology. In hash function, any length of the string will be take the will be produce used by the Secured Hash Algorithm 256.

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Fig. 7.Sample cryptography with sha-256.

As should be obvious, on account of SHA-256, regardless of how huge or little your info is, the yield will dependably have a fixed 256-bits length. This wind up basic when you are managing an enormous measure of information and exchanges. So fundamentally, rather than recalling the information which could be colossal, you can simply recollect the hash and follow along.

Even if you changes the one letter in our previous input, the Hash function output totally changed. See the following input and Hash output:

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Fig. 8.Example of small change in cryptography

D. Problems are solved by block chain technology

- Currency and Transaction Support
- Supply chains
- Voting
- Government operations
- Intellectual Property
- Cloud storage
- Charity
- Real estate
- Crowd funding

IV. CONCLUSION

Blockchain technology is not about crypto-currency anymore. Block chain technology applications are used for the many places like: Hospitals, banking sectors, online purchasing, and all government service exams. It is economically support to the all industries. Blockchain has created exciting new opportunities and innovative application models: Global collaboration systems, self-governing systems, open government. Private, public and permission (consortium) models to meet diverse business needs. There is a role to play for each and every one of you.

ACKNOWLEDGMENT

The author would like to thank the management of Kalasalingam Academy of Research and Education for supporting the research through University Research Fellowship.

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, 2008, pp. 9.
2. S. Underwood, “Blockchain beyond bitcoin,” *Commun. ACM*, vol. 59, no. 11, 2016, pp. 15–17.
3. G. Hurlburt, “Might the Blockchain,” no. April, pp. 12–16, 2016.V. Vapnik and V.Vapnik, *Statistical learning theory Wiley*. New York,1998, pp.156-160.
4. B. Libert, M. Beck, and J. Wind, “How blockchain technology will disrupt financial services firms,” *Knowledge@Wharton*, 2016, pp. 2–7.
5. W. E. Summary and S. Plants, “Power and the Industrial Internet of Things (IIoT),” no. January, 2015, pp. 1–14.
6. U. S. D. of H. and H. Services, “Standards for privacy of individually identifiable health information; proposed rule.” *Fed. Regist.*, vol. 64, no. 212, pp. 59917, 1999.
7. Centers for Medicare and Medicaid Services, “Security Standards: Technical Safeguards,” *HIPAA Secur. Ser.*, vol. 2, 2007, pp. 1–17.
8. A. Banerjee, “Block chain Technology: Supply Chain Insights from ERP”, *Advances in Computers, Elsevier*, 2108. https://doi.org/10.1016/bs.adcom.2018.03.007
9. R. Yu et al., “Authentication with Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network,” *IEEE Access*, vol. 5, 2017, pp. 24944–24951.
10. K. Delmolino, M. Arnett, A. E. Kosba, A. Miller, and E. Shi, “Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab.,” *IACR Cryptol. ePrint Arch.*, 2015, p. 460.

AUTHORS PROFILE

Abinash he is a full-time research scholar in the department of information technology of Kalasalingam Academy of Research and Education Krishnankoil Srivilliputhur India. His areas of interest are big data analytics, bio informatics and block chain technology. He has published 5 papers in international journals and conferences.

Vasudevan he is working as senior professor in the department of information technology of Kalasalingam Academy of Research and Education Krishnankoil Srivilliputhur India for past 27 years and his areas of interest are big data analytics, cloud computing, network security and block chain technology. He has published 170 above papers in international journals and conferences. He has produced twenty above PhD scholars and currently guiding five PhD scholars. He is a life time member in ISTE and IAENG. He received Dr. APJ Abdul Kalam Award for life time contribution in teaching on 2016.