A Survey of Blockchain Technology and Challenges

Shehna C S
Department of Computer Science
St. Joseph's College (Autonomous)
Irinjalakuda, Thrissur, Kerala

Ambily Jacob
Department of Computer Science
St. Joseph's College (Autonomous)
Irinjalakuda, Thrissur, Kerala

***Abstract*— Block chain technologies is one most of the major in style difficulty in current years, it's already changed people's way in a few space thanks to its best influence on numerous commercial enterprise or enterprise, and what it's going to do can nonetheless maintain cause impact in several places. Although the feature of block chain technology may additionally bring us greater dependable and handy services, the security problems and challenges in the back of this innovative method is also an essential subject matter that we need to concern.**

Keywords— Blockchain; Smart Contracts; Security,privacy

I. INTRODUCTION

The Blockchain is one of the innovations which showed up in the most recent decade and carried a great deal of guarantee with it. Work is as yet being done to investigate the full capacities of Blockchain and where it very well may be utilized. Some accept that Blockchain is the key for a decentralized society. Our present environment is totally incorporated, which means the ability to settle on choices is in the hands of a couple [1]. For instance our whole money related framework is constrained by government approved banks and in associations choices are made distinctly by a couple of individuals from the board. Indeed, even monsters like Google and Facebook, utilized by billions of clients regular choose what they need us to see. While a decentralized is with any position, the force is conveyed among every one of the individuals from the system [1]. Bitcoin is a model where there is no need of a bank or any mediator for the exchanges since every one of the exchanges are unmistakable to every one of the gatherings and blockchain keeps the history too which permits anybody in the system to follow back any exchange to its cause. This paper will examine What is Blockchain and a few regions where it is being actualized

II. THE CONCEPT OF BLOCKCHAIN

Blockchain technologies isn't simply solely single one technique, however contains Cryptography, arithmetic, algorithmic rule and economic model, combining peer-to-peer networks and victimization distributed agreement algorithmic rule to resolve ancient distributed info synchronize problem, it's an integrated multi- field infrastructure construction

- **Decentralization.**

In typical centralized dealings systems, every dealing has to be valid through the central trustworthy agency (e.g., the central bank) inevitably ensuing the value and also the performance bottlenecks at the central servers. Differently, a dealing within the block chain network is conducted between any 2 peers (P2P) while not the authentication by the central agency. In this manner, block chain will considerably cut back the server prices (including the event value and also the operation cost) and mitigate the performance bottlenecks at the central server.

- **Persistency.**

Since everything about exchanges spreading over the system must be affirmed and recorded in squares circulated inside the entire system, it's almost impractical to alter. Also, every communicated square would be substantial by various hubs and exchanges would be checked. So any distortion could be distinguished effectively.

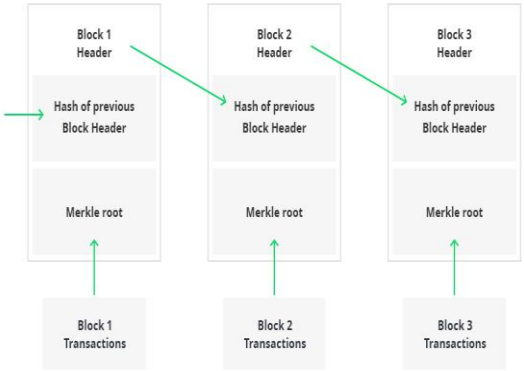
- **Anonymity**

Every client will act with the block chain coordinate with a produced address. Further, a client may produce a few delivers to maintain a strategic distance from personality introduction. There is presently no focal gathering keeping clients' close to home information. This component protects an accurate amount of security on the exchanges encased inside the block chain. Note that block chain can't ensure the best possible protection conservation because of the characteristic imperative

- **Auditability**

Since every of the transactions on the block chain is valid and recorded with a timestamp, users will simply verify and trace the previous records through accessing any node in the distributed network. In Bitcoin block chain, every dealing can be copied to previous transactions iteratively. It improves the traceability and therefore the transparency of the info hold on within the block chain

Fig



Block chain architecture

A. HOW BLOCKCHAIN WORKS?

The fundamental working procedures of square chain square measure as follows:

1) The sending hub records new information and broadcasting to arrange.

2) The accepting hub checked the message from that information which it got, in the event that the message was right, at that point it will be put away to a square.

3) All accepting hub in the system execute confirmation of work (PoW) or evidence of stake (PoS) calculation to the square.

4) The square is keep into the chain when beating understanding algorithmic guideline, every hub inside the system concede this square and can ceaselessly expand the chain base on this square.

B. THE STRUCTURE OF BLOCKCHAIN

For the most part, in the square, it contains principle information, hash of past square, hash of current square, timestamp and other data. Figure 1 shows the structure of square. Principle information. Contingent upon what administration is this square chain applicate, for instance: exchange records, bank clearing records, contract records or IOT information record. Hash. At the point when an exchange executed, it had been hash to a code and afterward communicate to every hub. Since it could be contained a huge number of exchange records in every hub's square, square chain utilized Merkle tree capacity to produce a last hash esteem, which is likewise Merkle tree root. This last hash worth will be record in square header (hash of current square), by utilizing Merkle tree work, information transmission and processing assets can be definitely decreased. Timestamp. Time of square produced. Other Information. Like mark of the square, Nonce esteem, or other information that client characterize

C. HOW TO GET CONSENSUS?

Accord work is a system that settle on all block chain hubs have understanding in same message, can ensure the most recent square have been added to the chain effectively, ensure the message that put away by hub was a similar one and won't occurred "fork assault", even can shield from malevolent assaults.

D. PROOF OF WORK (POW)

A proof of work could be a bit of information that is extreme (expensive or tedious) to give anyway easy to others to confirm and that fulfills bound necessities. Delivering a sign of work are frequently an irregular strategy with low possibility so huge amounts of experimentation is required on the normal before a sound evidence of work is created. Bitcoin utilizes the Hash cash confirmation of work framework. While figuring Pow, it's classified "mining". Each square has an irregular worth called "Nonce" in square header, by changing this nonce esteem, Pow need to create a worth that makes this square header hash esteem not exactly a "Trouble Target" which has just been set up. Trouble implies how much time it will take when the hub ascertaining hash esteem not as much as target esteem. All together for a square to be acknowledged by organize members, excavators must finish a proof of work which covers the entirety of the information in the square. The trouble of this work is balanced along these lines on limit the speed at that new squares are regularly created by the system to at any rate one every ten minutes. Because of the horrendously low possibility of made age, this makes it flighty that representative pc inside the system will be prepared to produce following square [2, 10].

E. PROOF OF STAKE (POS)

Since Proof of Work technique will cause a ton of power force and processing power be squandered, Proof of Stake doesn't require costly registering force. With Proof of Stake, the re-source that is thought about is the measure of Bitcoin an excavator holds - somebody holding 1% of the Bitcoin can mine 1% of the "Confirmation of Stake squares" [3]. A Proof of Stake technique may give expanded assurance from a noxious assault on the system. Extra insurance originates from two sources:

1) the death penalty AN assault would be undeniably increasingly overrated.

2) Reduced motivating forces for assault. The assaulter would need to have a near larger part of all bitcoin. Thusly, the aggressor experiences seriously his own assault.

F. TYPE OF BLOCKCHAIN

Square chain advances are frequently generally partitioned into 3 sorts. 1) Public square chain: everyone will check the dealings and confirm it, and may furthermore take an interest the technique for getting agreement. Like Bitcoin and Ethereal are both Public Block chain. 2) Consortium square chains: It implies the hub that had authority can be pick ahead of time, typically has associations like business to business, the information in square chain can be open or private, can be viewed as Partly Decentralized. Like Hyper record and R3CEV are both consortium square chains. 3) individual

square chain: Node will be confined, not every hub will take an interest this square chain, has exacting power the board on information get to. Regardless of what sorts of square chain is, it every ha advantage. At times we need open square chain since its accommodation, however here and there we perhaps need private control like consortium square chains or private square chain, contingent upon what administration we offer or what place we use it.

III. APPLICATION OF BLOCKCHAIN TECHNOLOGY

Since the emergence of Block chain, a lot of research is being done to explore what more can we do with this amazing technology. Applications of Block chain are still being discovered, a few of those will be discussed here.

a. Financial Application of Blockchain

The first and largest use of Block chain is in finance. It all started with bitcoin where block chain was used to keep a record of the financial transaction, eliminating the middleman. Since bitcoin, different block chain technologies have given birth to different cryptocurrencies so much so there are hundreds of cryptocurrencies are being traded in the world right now [4]. Figure 2 shows us a bitcoin block chain. Whenever a new transaction is made it is broadcasted across the network. Miners record these transactions and after the verification, the transaction is cryptographically sealed and becomes a block. Now this block is attached with the previous block by hashing [5].

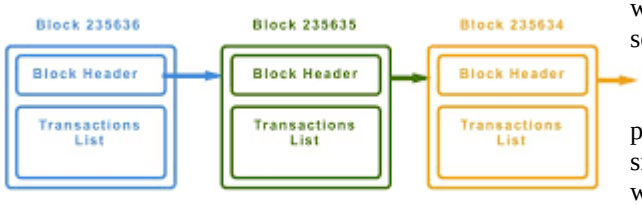


Figure 2. Bitcoin block chain

b. Smart Contracts

Exactly like the name says, Blockchain with smart contracts can eliminate the need for lawyers and intermediaries. Smart contracts will be available to all the parties and any change in the contract must be done after reaching Conesus. Smart contracts can be helpful in business as well as private dealing [6].

c. Blockchain and Internet of things

The Internet is a big part of everyone's life now, sometimes we don't even know how much connected everything is. All the devices like smart watches, smart fridges, cameras and your mobile phone etc. are connected to the internet. Internet of things(IoT) is basically a web of smart sensors and devise that is connected to the internet and are sharing information with each other to make our lives easier. There is no denying that IoTs has made our environment smarter for us, but they also make us vulnerable too. Imagine you live in a smart home, where every this connected and all the devices are tracking and watching you, to help but all your data are on the internet, which is not secure [13]. block chain as a decentralized and temper proof is very attractive for the Internet of things(IoTs) industry. The number of nodes in IoT is increasing day by day and so is the data that are being gathered. The security of data has always been an issue, block chain can help secure and manage this data.

d. Blockchain in Developing countries

Block chain can help kill or possibly decline the debasement in creating nations. It can help make every one of the exchanges straightforward and accessible to the open which thus makes it difficult for records to be adjusted. The straightforwardness will make the framework dependable and privileges of the individuals will be secured [10].

e. Medical Data

Therapeutic Industry is particularly inspired by Block chain innovation to verify and follow restorative information gathered from the patient. Restorative information is critical, and any misstep or alteration can prompt outrageous outcomes. With Block chain information can be freely accessible for use without the dread of transformation [6].

A. The Majority Attack (51% Attacks)

With Proof of Work, the likelihood of mining a square depends on the work done by the excavator (for example CPU/GPU cycles spent checking hashes). As a result of this instrument, people can wish to hitch along to mining a ton of squares, and become "mining pools", a spot where holding most figuring force. When it holds fifty-one figuring power, it will assume responsibility this square chain. Clearly, it causes security issues [7,8].

In the event that somebody has over 51% registering power, at that point he/she can discover Nonce esteem snappier than others, implies he/she has position to choose which square is admissible. What it can do is:

1) Modify the managing data, it might cause twofold spending assault [9, 10].

2) To stop the square confirming exchange.

3) To stop excavator mining any accessible square.

A greater part assault was a ton of conceivable inside the past once most exchanges were esteem significantly over the square prize and once the system hash rate was rich lower and in danger of revamping with the appearance of late mining advances [11].

B. Fork Problems

Another issue is fork issue. Fork disadvantage is said to redistributed hub adaptation, understanding once the product framework redesign. It is an extremely fundamental issue because of it including an enormous objective square chain.

• Types of Forks When the new form of square chain programming distributed, new understanding in accord rule likewise changed to the hubs. Subsequently, the hubs in square

chain system will be partitioned into 2 sorts, the New Nodes and the Old Nodes. So here return four circumstances: 1) The new hubs consider the gathering activity of square that is causation by the past hubs. 2) The new hubs don't concur with the exchange of square which is sending by the old hubs. 3) The old hubs concur with the exchange of square which is sending by the new hubs. 4) The old hubs don't concur with the exchange of square which is sending by the new hubs. In view of these four entirely unexpected cases in acquiring understanding, fork issue occurs, and as indicated by these four cases, fork issues can be separated into two sorts, the Hard Fork and the Soft Fork. Notwithstanding recognize the new hubs and the old hubs, we need to think about the figuring intensity of new hubs with old hubs, and accept that the processing intensity of new hubs are more than 50

Hard Fork implies when framework goes to another rendition or new understanding, and it didn't perfect with past form, the old hubs couldn't concur with the mining of new hubs, so one chain became two chains. Albeit new hubs processing power were more grounded than past hubs, old hubs will at present keep on keeping up the chain which it however was correct. Figure 5 shows the hard fork issue. At the point when Hard Fork occurs, we need to demand all hubs in the system to update the understanding, the hubs which haven't been overhaul won't keep on filling in of course. On the off chance that there were progressively old hubs didn't overhaul, at that point they will keep on dealing with the other totally extraordinary chain, which implies the standard chain will fork into two chains. Figure 6 shows the explanation of why hard fork will occur.

Delicate Fork implies when framework goes to another adaptation or new understanding, and it didn't good with past rendition, the new hubs couldn't concur with the mining of old hubs. Since the registering intensity of new hubs are more grounded than old hubs, the square which is mining by the old hubs will never be affirm by the new hubs, however new hubs and past hubs can at present work on consistent chain. Figure 7 shows the delicate fork issue.

At the point when Soft Fork occurs, hubs in the system don't need to overhaul the new understanding simultaneously, it permits to redesign progressively. Dislike Hard Fork, Soft Fork will just have one chain, it won't influence the steadiness and viability of framework when hubs redesign. In any case, Soft Fork makes the past hubs unconscious that the understanding guideline is adjusted, in spite of the standard of each hub can check effectively somewhat. Figure eight shows the clarification of why delicate fork can occur.

C. Scale of Blockchain

As square chain developing, data increases and bigger, the stacking of store and figuring additionally will get increasingly solid and progressively strong, it sets aside loads of effort to synchronize data, in a similar time, information still persistently increment, carries a major issue to customer when running the framework [9].

Improved Payment Verification (SPV) is an installment check innovation, without keep up full square chain data, just need to utilize square header message. This innovation will incredibly reduce client's stockpiling in square chain installment check; bring down the client's weight once managing definitely enlarged inside what's to come.

D. Time Confirmation of Blockchain Data

Contrasted with customary online MasterCard exchange, as a rule takes 2 or 3 days to affirm the exchange, bitcoin exchange just needs to use around 1 hour to check, it's obviously superior to the standard thing, yet it's as yet not sufficient to what we need it to. Lightning Network could be a response to disentangle this drawback [9]. Lightning Network is a proposed execution of Hashed Time lock Contracts (HTLCs) with bi-directional installment channels which permits installments to be safely steered over various distributed installment channels. This permits the development of a system any place any friend on the system will pay the other companion despite the fact that they don't straightforwardly have a channel open between each other.

E. Current Regulations Problems

Use Bitcoin for example, the characteristics of decentralized system, will weak the central bank's ability to control the economic policy and the amount of money, that makes government be cautious of block chain technologies, authorities have to research this new issue, accelerate formulating new policy, otherwise it will have risk on the market.

F. Integrated Cost Problem

Of course it will have lot of cost including time and money to change existing system, especially when it's an infra-structure. We have produce} positive this innovative technology not solely create economic advantages, meet the wants of management, however additionally bridge with ancient organization, and it continually encounter difficulties from internal organization which is existing no

IV. PRIVACY OF BLOCKCHAINS

Security is the ability of a solitary individual or a gathering to disconnect themselves or information accordingly communicating discerningly. Security in square chain implies having the option to perform exchanges without spilling recognizable proof data. Simultaneously, security permits a client to stay consistent by discerningly revealing themselves without displaying their movement to the whole system. The objective of improving security in square ties is to make it very hard for different clients to duplicate or utilize other clients' crypto profile. A vast volume of varieties can be seen when applying square chain innovation. Some regular attributes are

A. Stored data sorting.

Blockchain provides the flexibility to store all forms of data. The privacy perspective in block chain varies for personal and organizational data. Although privacy rules are applicable for personal data, more stringent privacy rules apply to sensitive and organizational data.

B. Storage distribution.

The nodes in the network that stores complete copies of the block chain are called full nodes. The full nodes in combination with the append-only characteristic of block chain leads to data redundancy. This redundancy of data

supports two key features of block chain technology including transparency and verifiability. The compatibility of application with data minimization decides the level of transparency and verifiability of that network for an application.

C. Append-only.

It is impossible to alter the data of previous blocks in the block chain undetected. The append only feature of block chain in certain cases does not curtail to the right to correction of users, especially if data is recorded incorrectly. Special attention needs to be provided while assigning rights to data subjects in block chain technology.

D.Private vs public blockchain.

The accessibility of block chain is remarkable from the standpoint of privacy. In an advanced level the restricted data on a block can be encrypted for conditional access by authorized users as every node in the block chain has maintains a copy of the entire block chain.

V. CONCLUSION

There's no uncertainty that square chain is a hot issue as of late, despite the fact that it has a few themes we have to see, a few issues has just been improved alongside new system's creating on application side, getting all the more any longer develop and stable. The legislature need to make comparing laws for this innovation, and endeavor should prepare for grasp square chain advances, forestalling it carries a lot of effect to current framework. At the point when we appreciate in the benefit of square chain advancements bring to us, in a similar time, we despite everything need to remain wary on its incense and security gives that it could be have

REFERENCES

[1] A. Kaushik, A. Choudhary, C. Ektare, D. Thomas and S. Akram, "Blockchain – Literature Survey," in 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), India, 2017.
[2] I. Bentov, A. Gabizon, and A. Mizrahi, “Cryptocurrencies without proof of work,” CoRR, vol. abs/1406.5694, 2014.
[3] S. King and S. Nadal, Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake, 2012. (https://archive.org/stream/PPCoinPaper/ppcoin-paper_djvu.txt)
[4] p. tasatanattakool and c. techapanupreeda, "blockchain: challenges and applications," in international conference on information networking (icoin), chiang mai, thailand, 2018.
[5] t. d. m. tomaso aste and paolo tasca, " blockchain technologies: the foreseeable impact on society and industry," computer, pp. 18-28, 2017.
[6] w. gao, w. g. hatcher and w. yu, "a survey of blockchain: techniques, applications, and challenges," in 27th international conference
[7] N. T. Courtois and L. Bahack, “On subversive miner strategies and block withholding attack in bitcoin digital currency,” CoRR, vol. abs/1402.1718, 2014.
[8] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” CoRR, vol. abs/1311.0243, 2013
[9] O. Karame, “Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin,” in Proceedings of Conference on Computer and Communication Security, pp. 1–17, 2012.
[10] M. Rosenfeld, “Analysis of hashrate-based double spending,” CoRR, vol. abs/1402.2009, 2014.
[11] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, “Tampering with the delivery of blocks and transactions in bitcoin,” in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (CCS’15), pp. 692–705, New York, NY, USA, 2015
[12] k. nir and j. voas, "blockchain in developing countries," it professional, pp. 11-14, 2018.
[13] Y. Gupta, R. Shorey, D. Kulkarni and J. Tew, "The Applicability of Blockchain in the Internet of Things," in 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 2018.
[14] QalabEAbbas,JangSang-Bong “A Survey of Blockchain and Its Applications”
[15] Iuon-Chang Lin and Tzu-Chun Liao “A SURVEY OF BLOCK CHAIN SECURITY ISSUES AND CHALLENGES”