IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

Blockchain Technology and Security Issues and Challenges in Blockchain

M. Mallikharjuna, MCA Final Year, LakkireddyBalireddy College of Engineering,Mylavaram.
Y. Kranthi Kumar, Asst. Prof, Dept. of MCA, LakkireddyBalireddy College of Engineering,Mylavaram.

Abstract: Blockchain innovation is a standout amongst the most prevalent issue as of late; it has effectively changed individuals' way of life in some territory because of its incredible nuance on numerous businesses or industry, and what it can do will in any case proceed with because affect in numerous spots. In spite of the fact that the component of blockchain advancements may bring us more dependable and helpful administrations, the security issues and difficulties behind this imaginative system is likewise an imperative theme that we have to concern.

Keywords: Blockchain; Security; Internet of Things (IoT); Smart Contracts.

1. Introduction: Bitcoin is the primary use of blockchain, it's a sort of computerized cash in light of blockchain innovations, utilizing for exchange things on the web like cash as we do in reality. Since the accomplishment of Bitcoin, individuals now can use blockchain advances in numerous field and administration, for example, budgetary market, IOT, inventory network, voting, restorative treatment and capacity. Be that as it may, as we utilize these apparatuses or administrations in our everyday life, cybercriminals likewise motivate chance to participate in cybercrime [7, 8]. For instance, 51% assaults area great security issue in Bitcoin that programmer attempt to take controls the framework's component, utilizing a similar innovation base.

2. The Concept of Blockchain

Blockchain innovations isn't simply just single one strategy, yet contains Cryptography, science, Algorithm and monetary model, joining shared systems and utilizing appropriated agreement algorithm to take care of customary conveyed database

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

synchronize issue, it's a coordinated multi-field framework development [5, 6, 7]. The blockchain advances made out of six key components.

Decentralized: The essential component of blockchain implies that blockchain doesn't need to depend on unified node any longer; the information can be record, store and refresh distributed.

Transparent: The information's record by blockchain framework is straightforward to every node, it additionally straightforward on refresh the information that is the reason blockchain can be trusted.

Open Source: Most blockchain framework is available to everybody, record can be check openly and individuals can likewise utilize blockchain advancements to make any application they need.

Autonomy: In light of the base of accord, each node on the blockchain framework can exchange or refresh information securely, the thought is to trust shape single individual to the entire framework, and nobody can mediate it.

Immutable: Any records will be held always, and can't be changed unless somebody can take control over 51% nodes in a similar time.

Anonymity: Blockchain innovations tackled the put stock in issue between node to node, so information exchange or even exchange can be unknown, just need to know the individual's blockchain address.

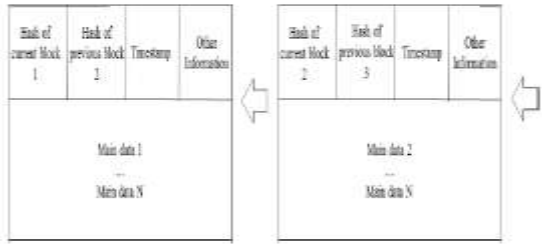

Figure 1: The structure of block chain

Blockchain Working Process: The primary working procedures of blockchain are as per the following:

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

2) The getting node checked the message from those information which it got, if the message was right then it will be put away to a square.

3) All accepting node in the system execute verification of work (PoW) or confirmation of stake (PoS) algorithm to the block.

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

4) The block will be put away into the chain in the wake of executing accord algorithm, each node in the system concede this square and will persistently expand the chain base on this block.

The Structure of Blockchain Generally in the block, it contains primary information, hash of past square, hash of current square, timestamp and other data. Figure 1 demonstrates the structure of square.

Principle information: Contingent upon what benefit is this blockchain applicant, 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 after that communicate to every node. Since it could be contained a large number of exchange records in every node's square, blockchain utilized Merkle tree capacity to create a last hash esteem, which is likewise Merkle tree root. This last hash esteem will be record in block header (hash of current square), by utilizing Merkle tree work, information transmission and figuring assets can be radically lessened.

Timestamp: Time of square created.

Proof of Work (PoW): A proof of work is a bit of information which is troublesome (costlyor tedious) to create yet simple for others to confirm and which fulfills certain necessities. Delivering a proof of work can be an irregular procedure with low likelihood so a great deal of experimentation is required by and large before a legitimate verification of work is produced. Bitcoin utilizes the Hashcash confirmation of work framework. While computing PoW, it's called \mining". Each block has an arbitrary esteem called \Nonce" in square header, by changing this nonce esteem, PoW need to produce an esteem that influences this block header to hash esteem not exactly a \Difficulty Target" which has just been set up. Trouble implies how much time it will take when the node computing hash esteem not as much as target esteem. All together for a square to be acknowledged by arrange members, mineworkers must finish a proof of work which covers the majority of the information in the block. The trouble of this work is balanced to confine the rate at which

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

new squares can be produced by the system to one at regular intervals.

Proof of Stake (PoS): Because Proof of Work strategy will cause a great deal of power and figuring power be squandered, Proof of Stake doesn't require costly registering power. With Proof of Stake, the asset that is looked at is the measure of Bitcoin an excavator holds - somebody holding 1% of the Bitcoin can mine 1% of the \Proof of Stake squares" [12]. A Proof of Stake strategy may give expanded insurance from a noxious assault on the system. Extra security originates from two sources:

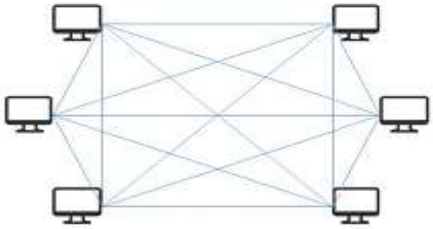

Figure 2: Public blockchain

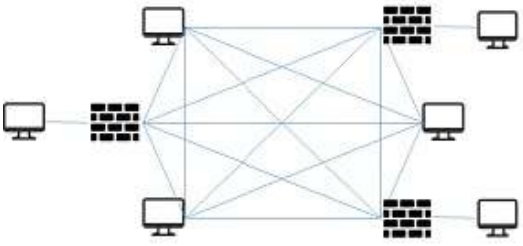

Figure 3: Consortium blockchain

1) Executing an assault would be substantially more costly.

2) Reduced motivating forces for assault.

The assailant would need to possess a close lion's share of all bitcoin. Along these lines, the aggressor experiences the ill effects of his own assault.

Type of Blockchain: Blockchain advancements can be generally separated into three kinds.

Public blockchain: Everyone can check the exchange and confirm it, and can likewise take part the way toward getting accord. Like Bitcoin and Ethereum are both Public Blockchain. Figure 2 indicates open blockchain.

Consortium blockchains: It implies the node that had expert can be pick ahead of time, more often than not has associations like business to business, the information in blockchain can be open or private, can be viewed as Partly Decentralized. Like Hyperledger and R3CEV are both consortium blockchains. Figure 3 indicates consortium blockchains.

Private blockchain: Node will be confined, only one out of every odd node can take an

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

interest this blockchain, has strict specialist administration on information get to. Figure 4 demonstrates private blockchain. Regardless of what kinds of blockchain is, it the two has advantage. At times we require open blockchain in light of the fact that its accommodation, yet now and then we perhaps require private control like consortium blockchains or private blockchain, contingent upon what benefit we offer or what put we utilize it.

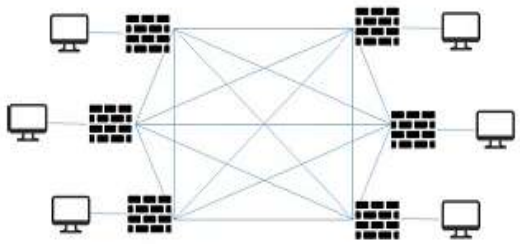

Figure 4: Private blockchain

3. Application of Blockchain Technologies

Blockchain innovations can be utilizing as a part of numerous zones, in money related application, as well as in others enterprises.

Digital Currency Bitcoin: Bitcoin's information structure and exchange framework was worked by blockchain advancements, makes Bitcoin turned into a computerized cash and online installment framework. By utilizing encryptedtechnique, stores exchange can be accomplished and doesn't have to depend on national bank. Bitcoin utilized open keys address sending and accepting bitcoin, recorded the exchange and the individual ID was mysterious. The procedure of exchange affirms needs other client's processing energy to get agreement, and after that records the exchange to arrange.

Smart Contract: Ethereum Smart Contract is an advanced get that controls client's computerized resources, detailing the member's privilege and commitment, will consequently execute by PC framework. It's not just only a PC methodology, it can be viewed as one of agreement members, will reaction to message what it get and store the information, and it can likewise send message or incentive to outside. Brilliant Contract is much the same as a man can be trusted, can hold the advantages briefly and will take after the request which has just been program [13]. Ethereum is an open source blockchain stage consolidating Smart Contract, offering decentralized virtual machine to deal with the agreement, by

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

utilizing its advanced cash called ETH, individuals can make various administrations, applications or contracts on this stage.

Hyperledger: Hyperledger is an open source blockchain stage, began in December 2015 by the Linux Foundation, to help blockchain-based circulated records. It is centered around records intended to help worldwide business exchanges, including major mechanical, money related, and inventory network organizations, with the objective of enhancing numerous parts of execution and unwavering quality. The undertaking means to unite various autonomous endeavors to create open conventions and guidelines, by giving a measured structure those backings distinctive parts for various employments. This would incorporate an assortment of blockchains with their own agreement and capacity models, and administrations for personality, get to control, and contracts.

There still have numerous utilization instance of blockchain advancements, similar to assurance of Intellectual property, traceability in production network, character confirmation, protection, universal installments, IOT, patient's security in therapeutic treatment or forecast showcase [14].

4. Security Issues and Challenges

Up until this point, blockchain has been gotten numerous consideration in various region, be that as it may, it additionally exists a few issues and difficulties needs to confront it [2, 9].

The Majority Attack (51% Attacks) With Proof of Work, the likelihood of mining a square relies upon the work done by the mineworker (e.g. CPU/GPU cycles spent checking hashes). Due to this instrument, individuals will need to combine keeping in mind the end goal to mining more squares, and move toward becoming \mining pools", a place where holding most registering power. When it holds 51% registering power, it can take control this blockchain. Evidently, it causes security issues [3, 4]. On the off chance that somebody has over 51% processing power, at that point he/she can discover Nonce esteem speedier than others, implies he/she has expert to choose which block is reasonable.

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

What it can do is:

1) Modify the exchange information, it might cause twofold spending assault [11, 12].

2) To stop the square confirming exchange.

3) To stop mineworker mining any accessible block.

A dominant part assault was more plausible in the past when most exchanges were worth significantly more than the square reward and when the system hash rate was much lower and inclined to revamping with the approach of new mining advances [8].

Types of Forks

At the point when the new form of blockchain programming distributed, new understanding in agreement control additionally changed to the nodes.

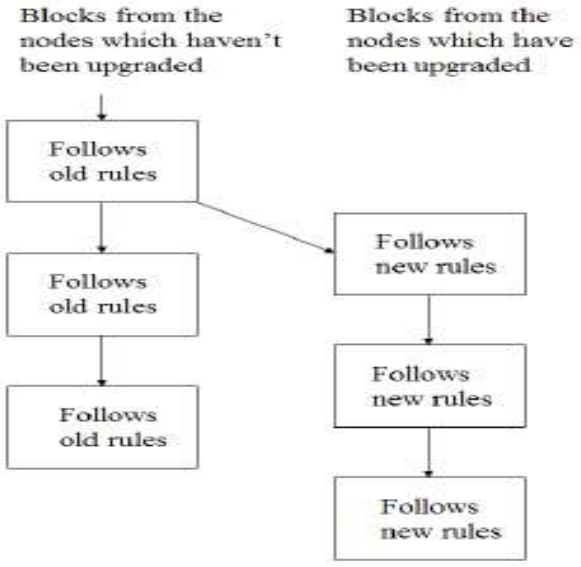

Figure 5: Hard Fork

In this way, the nodes in blockchain system can be partitioned into two kinds, the New Nodes and the Old Nodes. So here come four circumstances:

1) The new nodes concur with the exchange of block which is sending by the old nodes.

2) The new nodes don't concur with the exchange of block which is sending by the old nodes.

3) The old nodes concur with the exchange of block which is sending by the new nodes.

4) The old nodes don't concur with the exchange of block which is sending by the new nodes. On account of these four distinct cases in getting agreement, fork issue

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

happens, and as indicated by these four cases, fork issues can be isolated into two sorts, the Hard Fork and the Soft Fork. Notwithstanding recognize the new nodes and the old nodes, we need to look at the registering energy of new nodes with old nodes, and expect that the processing energy of new nodes are more than 50

Hard Fork Hard Fork implies when framework goes to another adaptation or new understanding, and it didn't well with past form, the old nodes couldn't concur with the mining of new nodes, so one chain ended up two chains. Albeit new nodes processing power were more grounded than old nodes, old nodes will at present keep on maintaining the chain which it however was correct. Figure 5 demonstrates the hard fork issue. At the point when Hard Fork happens, we need to ask for all nodes in the system to redesign the understanding, the nodes which haven't been overhaul won't keep on working obviously. On the off chance that there were more old nodes didn't redesign, at that point they will keep on working on the other totally unique chain, which implies the common chain will fork into two chains.

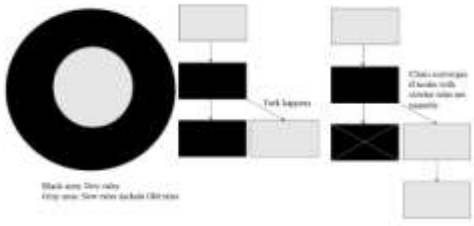

Figure 6: Hard Fork happens because the old node verification requirement is much stricter than the new node

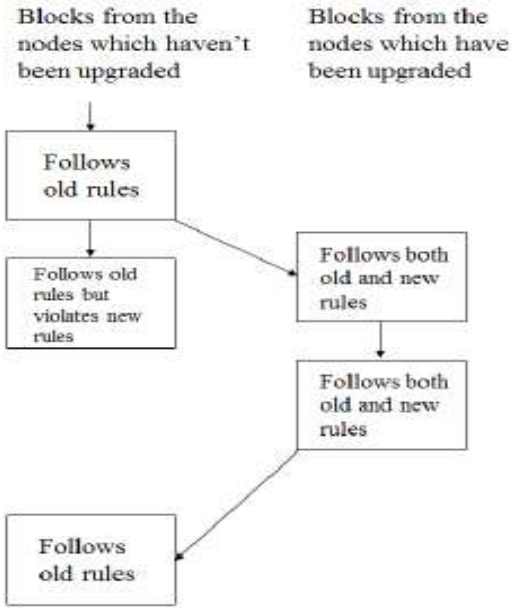

Figure 7: Compatible hard forknodes which haven't been upgrade will not continueto work as usual.

On the off chance that there were more old nodes didn't update, at that point they will keep on working on the other totally unique chain, which implies the conventional chain will fork into two chains. Figure 6

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

demonstrates the reason of why hard fork will happen.

Soft Fork Soft Fork implies when framework goes to another rendition or new understanding, and it didn't perfect with past variant, the new nodes couldn't concur with the mining of old nodes. Since the processing energy of new nodes are more grounded than old nodes, the square which is mining by the old nodes will never be endorse by the new nodes, however new nodes and old nodes will even now keep on working on a similar chain. Figure 7 demonstrates the delicate fork issue.

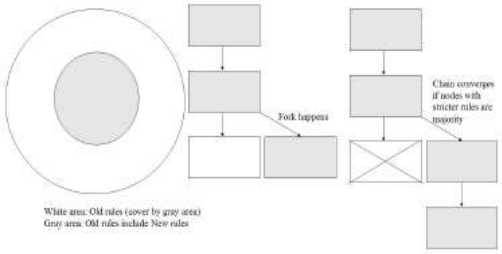

Figure 8: Soft Fork happens because the new node verification requirement is much stricter than the old node

At the point when Soft Fork happens, nodes in the system don't need to update the new understanding in the meantime, it permits to redesign step by step. Dislike Hard Fork, Soft Fork will just have one chain, it won't influence the steadiness and adequacy of framework when nodes overhaul. In any case, Soft Fork makes the old nodes ignorant that the accord control is changed, in opposition to the rule of each node can check accurately to some degree. Figure 8 demonstrates the reason of why delicate fork will happen.

Scale of Blockchain As blockchain developing, information winds up greater and greater, the stacking of store and processing will likewise getting increasingly hard, it sets aside a lot of opportunity to synchronize information, in a similar time, information still continually increment, conveys a major issue to customer when running the framework [10]. Rearranged Payment Verification (SPV) is an installment check innovation, without keep up full blockchain data, just need to utilize square header message. This innovation can incredibly lessen client's stockpiling in blockchain installment check, bring down the client's weight when exchange definitely expanded later on.

Time Confirmation of Blockchain: Information Compared to

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

conventional online MasterCard exchange, more often than not takes 2 or 3 days to affirm the exchange, bitcoin exchange just need to use around 1 hour to confirm, it's vastly improved than the standard thing, however it's as yet not sufficient to what we need it to. Lightning Network is an answer for take care of this issue [9]. Lightning Network is a proposed usage of Hashed Timelock Contracts (HTLCs) with bi-directional installment channels which enables installments to be safely steered over numerous shared installment channels. This permits the arrangement of a system where any associate on the system can pay some other companion regardless of whether they don't specifically have a channel open between each other.

Current Regulations Problems Use Bitcoin for instance, the attributes of decentralized framework, will feeble the national bank's capacity to control the monetary strategy and the measure of cash, that influences government to be mindful of blockchain innovations, specialists need to investigate this new issue, quicken figuring new approach, else it will have hazard available.

Integrated Cost Problem Obviously it will have part of cost including time and cash to change existing framework, particularly when it's a foundation. We need to ensure this imaginative innovation not just make financial advantages, meet the necessities of supervision, yet additionally connect with conventional association, and it generally experience troubles from interior association which is existing at this point.

5. Conclusion

There's almost certainly that blockchain is a hot issue lately, in spite of the fact that it has a few points we have to see, a few issues has just been enhanced alongside new strategy's creating on application side, getting increasingly develop and stable. The legislature need to make comparing laws for this innovation, and undertaking should prepared for grasp blockchain advances, forestalling it conveys excessively effect to current framework. When we appreciate in the benefit of blockchain advancements convey to us, in a similar time, despite everything we need to remain mindful on its

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

nuance and security issues that it could be have.

References

[1] M. Rosenfeld, \Analysis of hashrate-based doublespending," CoRR, vol. 1402.2009, 2014.

[2] J. Singh, \Cyber-attacks in cloud computing: Astudy," International Journal of Electronics and Information Engineering, vol. 1, no. 2, pp. 78{87, 2014.

[3] Y. Sompolinsky, A. Zohar, Secure High-RateTransaction Processing in Bitcoin,.507{527,Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[4] W. T. Tsai, R. Blower, Y. Zhu, L. Yu, \A system view of financial blockchains," IEEE Symposiumon Service-Oriented System Engineering (SOSE'16),pp. 450457, Mar. 2016.

[5] A. Gervais, G. O. Karame, K. W□ust, V. Glykantzis,H. Ritzdorf, S. Capkun, \On the security andperformance of work blockchains," Proceedings of ACM SIGSAC Conference on Computerand Communications Security (CCS'16), pp. 316,New York, NY, USA, 2016.

[6] A. Gervais, H. Ritzdorf, G. O. Karame, S. Capkun,\Tampering with the delivery of blocks andtransactions bitcoin," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS'15), pp. 692{705, NewYork, NY, USA, 2015.

[7] E. Heilman, A. Kendler, A. Zohar, S. Goldberg,\Eclipse attacks on bitcoin's peer-to-peer network,"in USENIX Security Symposium, pp. 129,Washington, D.C., 2015.

[8] G. Karame, \On the security, scalability of bitcoin'sblockchain," Proceedings of ACM SIGSACConference on Computer and Communications Secu-rity (CCS'16), pp. 1861862, New York, NY, USA,2016.

[9] G. O. Karame, \Two bitcoins at the price of one double-spending attacks on fast payments "Proceedings of Conference on Computer andCommunication Security, pp. 1{17, 2012.

[10] I. Bentov, A. Gabizon, A. Mizrahi, \Cryptocurrencieswithout proof of work," CoRR,vol. 1406.5694, 2014.

[11] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A.Kroll, E. W. Felten, \Sok:

Research perspectivesand challenges for Bitcoin, cryptocurrencies,"IEEE Symposium on Security and Privacy, pp. 10121, May 2015.

[12] N. T. Courtois, L. Bahack, \On subversive minerstrategies and block withholding attack on bitcoindigital currency," CoRR, vol. ab402.1718, 2014.

[13] I. Eyal, E. G. Sirer, \Majority notenough: Bitcoin mining is vulnerable," CoRR,vol. ab311.0243, 2013.

[14] J. Garay, A. Kiayias, N. Leonardos, The Bit-coin Backbone Protocol: Analysis and Applications,pp. 2810, Springer Berlin Heidelberg, Heidelberg,2015.

[15] A. Gervais, G. O. Karame, V. Capkun, S. Capkun,\Is Bitcoin is a decentralized currency," IEEESecurity Privacy, vol. 12, pp. 560, May 2014.

About Authors:

M. Mallikharjuna is currently pursuing his MCA,LAKKIREDDY BALIREDDY COLLEGE OF ENGINEERING, Mylavaram**,** Krishna Dt,A.P.

Mr. Y. Kranthi Kumar is currently working as an Asst. Professor in MCA Department,LAKKIREDDY BALIREDDY COLLEGE OF ENGINEERING, Mylavaram**,** Krishna Dt,A.P.