International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 03 | March - 2022 ISSN: 2582-3930

RESEARCH PAPER ON

Blockchain Technology

KEVIN JOY JOSEPH

Keraleeya Samajam's Model College, Dombivali East, Mumbai, Maharashtra, India

ABSTRACT :-

Blockchain, the muse of Bitcoin, has received extensive attentions recently. Blockchain is Associate in Nursing immutable ledger that permits transactions ensue in a very localised manner. Blockchain-based applications ar coming up, covering varied fields together with monetary services, reputation system and net of Things (IoT), and so on. However, there ar still several challenges of blockchain technology such as quantifiability and security issues waiting to be overcome. This paper presents a comprehensive summary on blockchain technology. we offer an outline of blockchain architechture firstly and compare some typical agreement algorithms used in different blockchains. moreover, technical challenges and recent advances ar concisely listed. we tend to additionally lay out potential future trends for blockchain.

Key Words : - Blockchain, decentralization, consensus, quantifiability

1. INTRODUCTION :-

Nowadays cryptocurrency has become a cant in each industry and academe. in concert of the foremost eminent cryptocurrency, Bitcoin has enjoyed an enormous success with its capital market reaching ten billion greenbacks in 2016 [1]. With a specially designed knowledge storage structure, transactions in Bitcoin network may happen with none third party and also the core technology to make Bitcoin is blockchain, that was 1st proposed in 2008 and enforced in 2009 [2]. Blockchain could be thought to be a public ledger and every one committed transactions ar hold on in a very list of blocks. This chain grows as new blocks ar appended to that endlessly. Asymmetric cryptography and distributed agreement algorithms are implemented for user security and ledger consistency. The blockchain technology usually has key characteristics of decentralization, tenacity, namelessness and auditability. With these traits, blockchain will greatly save the price and improve the potency.

Since it permits payment to be finished with none bank or any go-between, blockchain is utilized in numerous monetary services like digital assets, remission and on-line payment [3], [4]. to boot, it can even be applied into alternative fields including good contracts [5], public services [6], net of Things (IoT) [7], name systems [8] and security services [9]. Those fields favor blockchain in multiple ways that. 1st of all, blockchain is immutable . dealings can not

be tampered once it is packed into the blockchain. Businesses that need high reliability and honesty will use blockchain to draw in customers. Besides, blockchain is distributed and may avoid the one point of failure state of affairs. As for good contracts, the contract could be dead by miners mechanically once the contract has been deployed on the blockchain.

Although the blockchain technology has nice potential for the construction of the long run net systems, it's facing a number of technical challenges. Firstly, quantifiability may be a vast concern. Bitcoin block size is proscribed to one MB currently whereas a block is well-mined regarding each 10 minutes. after, the Bitcoin network is restricted to a rate of seven transactions per second, that is incapable of addressing high frequency trading. However, larger blocks means that larger cupboard space and slower propagation within the network. this may cause centralization bit by bit as less users would love to keep up such an outsized blockchain. thus the exchange between block size and security has been a tricky challenge. Secondly, it has been established that miners may accomplish larger revenue than
their justifiable share through ungenerous mining strategy [10]. Miners hide their well-mined blocks for additional revenue within the future. In that way, branches may ensue oft, that hinders blockchain development. thence some solutions have to be compelled to be place forward to mend this drawback. Moreover, it's been shown that privacy outflow may additionally happen in blockchain even users only create transactions with their public key and personal key [11]. moreover, current agreement algorithms like proof of work or proof of stake face some serious issues. For example, proof of labor wastes an excessive amount of electricity energy while the development that the made get richer may seem in
the proof of stake agreement method.

There is loads of literature on blockchain from numerous sources, like blogs, wikis, forum posts, codes, conference proceedings and journal articles. Tschorsch et al. [12] made a technical survey regarding localised digital currencies including Bitcoin. Compared to [12], our paper focuses on blockchain technology rather than digital currencies. Nomura Research Institut created a technical report regarding blockchain [13]. distinction to [13], our paper focuses on state-of-art blockchain researches together with recent advances and future trends. The rest of this paper is organized as follows. Section II introduces blockchain design. Section III shows typical consensus algorithms utilized in blockchain. Section IV summarizes the technical challenges and also the recent advances during this area. Section V discusses some potential future directions and section VI concludes the paper.

2. BLOCKCHAIN ARCHITECTURE :-

Blockchain may be a sequence of blocks, that holds a whole list of dealings records like typical public ledger [14]. Figure one illustrates Associate in Nursing example of a blockchain. With a previous block hash contained within the block header, a block has just one parent block. it's price noting that uncle blocks (children of the block's ancestors) hashes would even be hold on in ethereum blockchain [15]. the primary block of a blockchain is called genesis block that has no parent block. We then explain the internals of blockchain in details.

- Block :-

A block consists of the block header and also the block body as shown in Figure a pair of. particularly, the block header includes:
(i) Block version: indicates that set of block validation
rules to follow.
(ii) Merkle tree root hash: the hash worth of all the transactions within the block.
(iii) Timestamp: current time as seconds in UT1
since Gregorian calendar month one, 1970.
(iv) nBits: target threshold of a sound block hash.
(v) Nonce: Associate in Nursing 4-byte field, that typically starts with zero
and will increase for each hash calculation (will be explained
in details in Section III).
(vi) Parent block hash: a 256-bit hash worth that points to
the previous block.

The block body consists of a dealings counter and transactions. the most range of transactions that a block will contain depends on the block size and also the size of each dealings. Blockchain uses associate uneven cryptography
mechanism to validate the authentication of transactions [13]. Digital signature supported uneven cryptography is employed in an devious surroundings. we tend to next in short illustrate digital signature.

B. Digital Signature :-

Each user owns a try of personal key and public key. The personal key that shall be unbroken in confidentiality is employed to sign the transactions. The digital signed transactions area unit broadcasted throughout the full network. the standard digital signature is attached 2 parts: language phase and verification part. as an example, associate user Alice desires to send another user Bob a message. (1) within the language part, Alice encrypts her knowledge along with her personal key and sends Bob the encrypted result and original knowledge. (2) within the verification part, Bob validates the worth with Alice's public key. therein approach, Bob may simply check if the info has been tampered or not. The typical digital signature formula utilized in blockchains is the elliptic curve digital signature formula (ECDSA) .

C. Key Characteristics of Blockchain :-
In summary, blockchain has following key characteristics.

• *Decentralization. In typical centralized dealings systems, every dealings must be valid through the central sure agency (e.g., the central bank), inevitably ensuing to the value and also the performance bottlenecks at the central servers. distinction to the centralized mode, third party isn't any longer required in blockchain. Consensus algorithms in blockchain area unit wont to maintain*
data consistency in distributed network.

• purpose. Transactions are often valid quickly and invalid transactions wouldn't be admitted by honest miners. it's nearly not possible to delete or rollback transactions once they're enclosed within the blockchain. Blocks that contain invalid transactions can be discovered straightaway.

• namelessness. every user will act with the blockchain with a generated address, that doesn't reveal the real identity of the user. Note that blockchain cannot guarantee the proper privacy preservation thanks to the intrinsic constraint .

Auditability. Bitcoin blockchain stores knowledge regarding user balances supported the unexpended dealings Output (UTXO) model [2]: Any dealings must see some previous unexpended transactions. Once the present dealings is recorded into the blockchain, the state of these referred unspent transactions switch from unexpended to spent. So transactions can be simply verified and half-tracked.

CONSENSUS ALGORITHMS *:-*

In blockchain, the way to reach agreement among the devious nodes could be a transformation of the Byzantine Generals (BG) downside, that was raised in [20]. In BG downside, a group of generals WHO command some of Byzantine army circle town. Some generals opt to attack whereas other generals opt to retreat. However, the attack would fail if solely a part of the generals attack town. Thus, they have to reach associate agreement to attack or retreat. the way to reach a agreement in distributed surroundings could be a challenge. It is also a challenge for blockchain because the blockchain network is distributed. In blockchain, there's no central node that ensures ledgers on distributed nodes area unit all a similar. Some protocols area unit required to make sure ledgers in several nodes area unit consistent. we tend to next gift many common approaches to reach a agreement in blockchain.

A. Approaches to consensus *: -*

PoW (Proof of work) could be a agreement strategy utilized in the Bitcoin network [2]. during a suburbanized network, somebody has to be chosen to record the transactions. the simplest approach is random choice. However, random choice is prone to attacks. therefore if a node desires to publish a block of transactions, a lot of labor must be done to prove that the node isn't probably to attack the network. usually the work means that pc calculations. In PoW, every node of the network is calculative a hash price of the block header. The block header contains a time being and miners would amendment the time being often to get completely different hash values. The agreement needs that the

calculated price should be up to or smaller than an exact given price. once one node reaches the target price, it would broadcast the block to alternative nodes and every one alternative nodes should mutually ensure the correctness of the hash price. If the block is valid, alternative miners would append this new block to their own blockchains. Nodes that calculate the hash values are known as miners and also the POW procedure is termed mining in Bitcoin

PoS (Proof of stake) is associate energy-saving different to POW.
Miners in PoS have to be compelled to prove the possession of the quantity of currency. it's believed that folks with a lot of currencies would be less probably to attack the network. the choice based on account balance is kind of unfair as a result of the one richest person is sure to be dominant within the network. As a result, several solutions area unit planned with the mix of the stake size to come to a decision that one to forge ensuing block. In specific, Blackcoin [26] uses organization to predict the next generator. It uses a formula that appears for very cheap hash price together with the dimensions of the stake. Peercoin [21] favors coin age primarily based choice. In Peercoin, older and larger sets of coins have a larger chance of mining the next block. Compared to POW, PoS saves a lot of energy and is more practical. sadly, because the mining value is almost zero, attacks may come back as a consequence. several blockchains adopt POW at the start and rework to PoS step by step. For instance, ethereum is planing to maneuver from Ethash (a kind of PoW) [27] to Casper (a reasonably PoS) [28].

PBFT (Practical byzantine fault tolerance) may be a replication algorithm to tolerate byzantine faults [29]. Hyperledger cloth [18] utilizes the PBFT as its accord algorithmic program since PBFT could handle up to 1/3 malicious byzantine replicas. A new block is set in an exceedingly spherical. In every spherical, a primary would be elect in step with some rules. And it's to blame for ordering the dealings. the full method might be divided into 3 phase: pre-prepared, ready and commit. In each phase, a node would enter next part if it's received votes from over 2/3 of all nodes. thus PBFT needs that each node is thought to the network. Like PBFT, Stellar accord Protocol (SCP) [30] is additionally a Byzantine agreement protocol. In PBFT, every node needs to question different nodes whereas SCP provides participants the proper to decide on that set of different participants to believe. supported PBFT, Antshares [31] has enforced their dBFT (delegated byzantine fault tolerance). In dBFT, some skilled nodes square measure voted to record the transactions. DPOS (Delegated proof of stake). the key distinction between PoS and DPOS is that PoS is direct democratic whereas DPOS is representative democratic. Stakeholders elect their delegates to come up with and validate blocks. With considerably fewer nodes to validate the block, the block might be confirmed quickly, resulting in the short confirmation of transactions. Meanwhile, the parameters of the network like block size and block intervals might be tuned by delegates. in addition, users needn't to fret regarding the dishonest delegates as they could be voted out simply. DPOS is that the backbone of Bitshares [22].

Ripple [23] may be a accord algorithmic program that utilizes collectively-trusted subnetworks at intervals the larger network. In the network, nodes square measure divided into 2 types: server for participating accord method and consumer for under transferring funds. every server has AN distinctive Node List (UNL). UNL is important to the server. once decisive whether or not to place a transaction into the ledger, the server would question the nodes in UNL and if the received agreements have reached eightieth, the transaction would be

packed into the ledger. For a node, the ledger can stay correct as long because the share of faulty nodes in UNL is a smaller amount than two hundredth.

Tendermint [24] could be a byzantine accord algorithmic program. A new block is set during a spherical. A proposer would be elite to broadcast associate unofficial block during this spherical. It might be divided into 3 steps: 1) Prevote step. Validators opt for whether to broadcast a prevote for the projected block. 2) Precommit step. If the node has received quite 2/3 of prevotes on the projected block, it broadcasts a precommit for that block. If the node has received over 2/3 of precommits, it enters the commit step. 3) Commit step. The node validates the block and broadcasts a commit for that block. if the node has received 2/3 of the commits, it accepts the block. Contrast to PBFT, nodes have to be compelled to lock their coins to become validators. Once a validator is found to be dishonest, it would be censured.

C. Advances on consensus algorithms :-

A good accord algorithmic program suggests that potency, safty and convenience. Recently, variety of endeavors are created to improve accord algorithms in blockchain. New accord algorithms ar devised going to solve some specific problems of blockchain. the most plan of PeerCensus [33] is to decouple block creation and group action confirmation in order that the accord speed is considerably multiplied. Besides, Kraft [34] projected a replacement accord methodology to make sure that a block is generated during a comparatively stable speed. it's famed that high blocks generation rate compromise Bitcoin's security. So the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection rule [35] is projected to unravel this drawback. Instead of the longest branch theme, GHOST weights the branches and miners may opt for the higher one to follow. Chepurnoy et al. [36] given a replacement accord algorithmic program for peer-topeer blockchain systems wherever anyone United Nations agency provides noninteractive proofs of retrievability for the past state snapshots is in agreement to come up with the block. In such a protocol, miners only have to be compelled to store recent block headers rather than full blocks.

IV. CHALLENGES & RECENT ADVANCES :-

Despite the nice potential of blockchain, it faces varied challenges, that limit the wide usage of blockchain. We enumerate some major challenges and up to date advances as follows.

A. Scalability :-

With the number of transactions increasing day by day,
the blockchain becomes large. every node must store all transactions to validate them on the blockchain as a result of they have to check if the supply of the present group action is unexhausted or not. Besides, because of the first restriction of block size and the interval accustomed generate a replacement block, the Bitcoin blockchain will solely method nearly seven transactions per second, which cannot fulfill the necessity of

process lots of transactions in period of time fashion. Meanwhile, because the capability of blocks is incredibly tiny, several tiny transactions may well be delayed since miners like those group actions with high transaction fee. There ar variety of efforts projected to handle the scalability drawback of blockchain, that might be classified
into 2 types:

Storage optimisation of blockchain. Since it's tougher for node to control full copy of ledger, Bruce projected a novel cryptocurrency theme, during which the recent group action records ar removed (or forgotten) by the network [37]. A information named account tree is employed to carry the balance of all non-empty addresses. Besides light-weight client may additionally facilitate fix this drawback. a completely unique schem named VerSum [38] was projected to produce another way permitting light-weight purchasers to exist. VerSum permits
lightweight purchasers to source expensive computations over giant inputs. It ensures the computation result's correct through scrutiny results from multiple servers.

Redesigning blockchain. In [39], Bitcoin-NG (Next Generation) was projected. the most plan of Bitcoin-NG is to decouple standard block into 2 parts: key block
leader election and microblock to store transactions.The protocol divides time into epoches. In every epoch, miners have to be compelled to hash to come up with a key block. Once the key block is generated, the node becomes the leader United Nations agency is responsible for generating microblocks. Bitcoin-NG additionally extended the heaviest (longest) chain strategy during which microblocks carry no weight. during this manner, blockchain is redesigned and therefore the exchange between block size and network security has been self-addressed.

B. Privacy Leakage :-

Blockchain will preserve a particular quantity of privacy through the public key and personal key. Users interact with their
private key and public key with none real identity exposure.
However, it's shown in [40], [5] that blockchain cannot
guarantee the transactional privacy since the values of all
transactions and balances for every public key ar in public
visible. Besides, the recent study [41] has shown that a user's
Bitcoin transactions is coupled to reveal user's data. Moreover, Biryukov et al. [11] given associate methodology to link user pseudonyms to science addresses even once users ar behind
Network Address Translation (NAT) or firewalls. In [11], each
client is unambiguously known by a collection of nodes it connects
to. However, this set is learned and accustomed notice the
origin of a group action.

C. Selfish Mining :-

Blockchain is liable to attacks of colluding egotistic miners. specially, Eyal and Sirer [10] showed that the network is vulnerable notwithstanding solely atiny low portion of the hashing power is employed to cheat. In egotistic mining strategy, selfish miners keep their strip-mined blocks while not broadcasting and the personal branch would be discovered to the general public solely if some necessities area unit glad. because the personal branch is longer than this public chain, it might be admitted by all miners. Before the personal blockchain publishment, honest miners area unit wasting their resources on Associate in Nursing useless branch while egotistic miners area unit mining their personal chain while not competitors. therefore egotistic miners tend to urge a lot of revenue.

Based on egotistic mining, several different attacks are proposed to point out that blockchain isn't therefore secure. In stubborn mining [48], miners might amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks.

The trail-stubbornness is one in all the stubborn strategy that miners still mine the blocks notwithstanding the personal chain is left behind. nonetheless in some cases, it may end up in thirteen gains in comparison with a non-trail-stubborn counterpart. [49] shows that there area unit egotistic mining ways that earn more cash and area unit profitable for smaller miners compared to straightforward selfish mining. however the gains area unit comparatively little. what is more, it shows that attackers with but twenty fifth of the machine resources will still gain from egotistic mining. to assist fix the selfish mining downside, Heilman [50] given Associate in Nursing novel approach for honest miners to settle on that branch to follow. With random beacons and timestamps, honest miners would select a lot of recent blocks. However, [50] is susceptible to forgeable timestamps. ZeroBlock [51] builds on the easy scheme: every block should be generated and accepted by the network among a most quantity. among ZeroBlock, selfish miners cannot accomplish over its expected reward.

V. POSSIBLE FUTURE DIRECTIONS :-

Blockchain has shown its potential in business and domain. we tend to discuss attainable future directions with relation to four areas: blockchain testing, stop the tendency to centralization, big knowledge analytics and blockchain application.

A. Blockchain testing :-

Recently completely different varieties of blockchains seem and over 700 cryptocurrencies area unit listed in [52] up to currently. However,
some developers would possibly falsify their blockchain performance to attract investors driven by the large profit. Besides that, when users need to mix blockchain into business, they have to apprehend that blockchain fits their necessities. So blockchain testing mechanism must

be in situ to check
different blockchains.

Blockchain testing can be separated into 2 phases:

standardization section and testing section. In standardization
phase, all criteria ought to be created and in agreement. When a blockchain is born, it can be tested with the in agreement criteria to valid if the blockchain works fine as developers claim. As for testing section, blockchain testing must be performed with completely different criteria. for instance, Associate in Nursing user WHO is guilty of on-line retail business cares regarding the outturn of the blockchain, that the examination must take a look at the common time from a user send a dealings to the dealings is packed into
the blockchain, capability for a blockchain block and etc.

B. Stop the tendency to centralization :-

Blockchain is intended as a suburbanized system. However,
there is a trend that miners area unit centralized within the mining pool.
Up to now, the highest five mining pools along owns larger than 51% of the full hash power within the Bitcoin network [53]. Apart from that, egotistic mining strategy [10] showed that pools with over twenty fifth of total computing power might get a lot of revenue than justifiable share. Rational miners would be attracted into the selfish pool and at last the pool might simply exceed fifty one of the total power. because the blockchain isn't meant to serve a few organizations, some ways ought to be projected to resolve
this downside.

C. Big data analytics :-

Blockchain can be well combined with massive knowledge. Here
we roughly categorised the mixture into 2 types: knowledge management and knowledge analytics. As for knowledge management, blockchain can be accustomed store vital knowledge because it is distributed and secure. Blockchain might conjointly make sure the knowledge is original. for instance, if blockchain is employed to store patients health data, the data couldn't be tampered and it is arduous to scarf those personal data. once it involves data analytics, transactions on blockchain can be used for big knowledge analytics. for instance, user mercantilism patterns would possibly be extracted. Users will predict their potential

partners' mercantilism behaviours with the analysis.

D. Blockchain applications :-

Currently most blockchains area unit utilized in the money domain, more and a lot of applications for various fields area unit showing.
Traditional industries might take blockchain into thought and apply blockchain into their fields to boost their systems. for instance, user reputations can be keep on blockchain. At a similar time, the enterprising business could create use of blockchain to enhance performance. For
example, Arcade town [51], a ridesharing startup offers Associate in Nursing
open marketplace wherever riders connect directly with drivers
by leverage blockchain technology. A smart contract may be a processed dealings protocol that executes the terms of a contract [54]. it's been projected
for very long time and currently this idea will be enforced with blockchain. In blockchain, good contract may be a code fragment that could be dead by miners mechanically. good contract has transformative potential in numerous fields like money services and IoT.

VI. CONCLUSION :-

Blockchain has shown its potential for reworking ancient business with its key characteristics: decentralization, persistency, obscurity and auditability. during this paper, we present a comprehensive summary on blockchain. we tend to initial provide an overview of blockchain technologies as well as blockchain architecture and key characteristics of blockchain. we tend to then discuss the standard accord algorithms employed in blockchain. We analyzed and compared these protocols in numerous respects. Furthermore, we tend to listed some challenges and issues that would hinder blockchain development and summarized some existing approaches for finding these issues. Some attainable future directions are planned. these days blockchainbased applications square measure bobbing up and that we arrange to conduct in-depth investigations on blockchain-based applications within the future.

ACKNOWLEDGEMENT :-

I am pleased to present "Blockchain Technology " project and take this opportunity to express our profound gratitude to all those people who helped us in completion of this paper. I thank our college

for providing us with excellent facilities that helped us to complete and present this paper. I would also like to thank our guide Asst. Prof. Jyoti Samel for permitting us to use computers in the lab as and when required for research. We express our deepest gratitude towards our project guide for her valuable and timely advice during the various phases in our project. We would also like to thank her for providing us with all proper facilities and support as the co-coordinator. We would like to thank her for support, patience and faith in our capabilities and for giving us flexibility in terms of working and reporting schedules.

REFERENCES :-

[1] "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," 2015.

[4] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.