International Journal on Emerging Technologies **11**(3): 427-434(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Comparisons of Blockchain based Consensus Algorithms for Security Aspects

Mansi Bosamia[1] and Dharmendra Patel[2]
[1]*Research Scholar, Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, Charotar University of Science and Technology (CHARUSAT), Changa, Anand, India.*
[2]*Associate Professor, Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, Charotar University of Science and Technology (CHARUSAT), Changa, Anand, India.*

(Corresponding author: Mansi Bosamia)
(Received 24 February 2020, Revised 17 April 2020, Accepted 20 April 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The blockchain is a relatively new technology in the field of computer science. It has received enhanced interests in recent years for Research and Scientific Industry. As its first implementation attention is crypto-currency. Blockchain provides as an immutable distributed ledger which performs transactions with untrusted participants in a decentralized network. It forms a new distributed architectures, which has no central authority and has smart contracts to shared states and perform transactions. Blockchain applications are crypto-currency based online wallets, Internet of Things, springing up, financial services, risk management, reputation system, etc. This paper aims to share knowledge on the growing importance of blockchain technology in real-world applications. This paper also focused on Blockchain core components and technologies to lay out the comparisons of typical Consensus Algorithm for security aspects. This comparison and blockchain applications concludes that alternative Merkel tree based blockchains are available in the market for faster and secure transactions.

Keywords: Blockchain, Consensus Mechanisms, Consensus Protocol, Cryptographic Hash, Distributed Ledger, Mining, Smart Contract

I. INTRODUCTION

Blockchain is not complex as much other technological topics such as artificial intelligence, machine learning, etc. But at the same time, Blockchain has so many different components of varying complexity in fluxions and it is important. At the initial level, they enable a group of users to record transactions in a distributed ledger public to that group such that no transaction can be changed once published. Blockchain might be considered as a public immutable ledger, in which transactions are stored in a chain of block and before storing all transactions should be committed. This chain of blocks continuously rises when new blocks are added to it. The blockchain has the key characteristics are anonymity, immutability, auditability, scalability, fault-tolerance, persistency, resilience and decentralization [4]. Due to these characteristics of blockchain, it can significantly improve the efficiency and save the cost. Blockchain can be applied into various applications far ahead of crypto-currencies. It allows payments to be done without any bank or any conciliator. Blockchain is used for many financial services such as online payment, digital assets, remittance, etc. Also, blockchain technology has other uses such as suitable for the management of medical records, banking transactions, notary services, users identity verification and status, data tracking, etc. [5] and internet interaction based systems, such as security service, secure transactions, smart contracts, public services, internet of things (IoT), etc. A blockchain is to merge with ideas and method to make new way applications with security. It is easy to build and deploy the solutions. This kind of applications will be consumed the whole market and operated everywhere in recent upcoming future. Main key feature attracts the developer about the blockchain is its cryptographic tools and distributed consensus mechanisms. [5] Here, all discussed application uses bit coin due to its popularity which creates a monopoly in market to use blockchain. So this paper, discusses the blockchain working in general to understand its working mechanism, typical Consensus Algorithm comparison and its applications with limitation and misconceptions. It proves that the bit coin is not only used for blockchain but alternative solutions are available in the market such as Ethereum. Thus, blockchain application developer started the implementation of Ethereum and lite coin.

This paper focuses on the technical aspects of blockchains and their security and applications. This paper has following sections: section II gives idea about blockchain evolution, section III describes blockchain definitions, Section IV provides types of blockchain, section V provides the working of blockchain, Section VI gives security of blockchain and information regarding smart contract, Section VII discusses blockchain applications, Section VIII discusses blockchain cheat possibilities and section IX has limitations and misconceptions. Finally, section X concludes the paper.

II. BRIEF HISTORY OF BLOCKCHAIN

The blockchain concept brief history is as mentioned in Table 1.

Table 1: Blockchain History.

Year	Developers Name	Technology	Description
1991	Stuart Haber and W.Scott Stornetta	Time-Stamp a Digital Document	A client has to send a document to time stamping server for time stamping it use signing of document with the current timestamp. The server created link of document to the previous document based on specific data as data pointer instead of document address. If the data is changed, data pointer becomes invalid. Checks that data should not be corrupt after sending to the server [8].
2008	Zheng *et al*	Blockchain	Blockchain was first proposed and implemented in 2009 (Nakamoto, 2008) [4]
2008	Satoshi Nakamoto	Block change Digital cash	It is a Blockchain with its most of the features such as fully peer-to-peer new electronic cash system without trusted third party [3, 12].
2009	Nakamoto	First bit coins mined	The cryptography introduced. A shared accounting ledger reflects the truth in blockchain with combining the traditional cryptography tools to enable a public network of participants without trusting each other to agree, over and over to do the transactions [12]. Bit coin is a Peer to Peer Electronic Cash System which core implementation is the Blockchain [3].
2011	Nakamoto	Removes the central authority	For digital cash, it is not possible spend same currency twice use of delay attempts for generating digital cash. In electronic exchange of the currency the central authority is critically removed. Bit coin's popularity initiated and powered online marketplace [12].
2013	Vitalik Buterin	Ethereum	The entire value of bit coins in rotation had passed $1 billion. Then, technologies recognized that blockchains could be used to track other things like record management or record authentication moreover payment transactions. The Ethereum introduced to record status of smart contracts with currency transactions [13].
2015	Vitalik Buterin	Ethereum with decentralized crypto-currency networks	Ethereum has the possible of new invention of applications that works like web apps but they are powered by decentralized crypto-currency networks instead of a company's servers. By this way now, Ethereum becomes a host of competitors and imitators [6, 13].

III. BLOCKCHAIN DEFINITION

A structure for storing data in a digital ledger in which groups of valid transactions, called blocks, form a chronological chain, with each block cryptographically linked to the previous one [1].
According to Wikipedia, a very general definition is "A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography." Each block includes a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data [16].
Blockchain has the following features:
– It can be public or private based on creation of it.
– It is permanent and append-only.
– It is mining distributed peer to peer network.
– It uses consensus protocol.
– It is an immutable ledger.
– It uses hash cryptography.
– It is secure and tamperproof.
– It guarantees decentralization.
– It has mathematical structure.
– It can be implemented for all types of valuable data and digital assets.
– It stores data in a secure way which is genuine.
– It is impossible to encode the data of blockchain when it's properly set.
– In blockchain, old transaction alteration is not allowed; just new transactions can be appended in it.
– It is about way more than money.
– It can use as a ledger for tracking currency balances.
– It can enhance trust for the transactions of organizations such as governments, banks, central authorities, outsource companies, etc. Also we can trust them by secure transactions of blockchain.

– It has distributed network across numbers of computers.
– It computerizes trust as organizing "decentralized" enterprises and institutions.
Thus, we can say that "*Blockchain is a public, permanent, append-only distributed ledger*."

Let us show the precise way of block to understand refer Fig. 1.

Data: ...
Prev. Hash: 033DFA457
Hash: 4D65E1F05

Fig. 1. A Block.

So, look at one of this block, which has some data inside it with previous hash and its own hash. Data specifically 64 characters long and more in the future. The best way to think about it is a hash as digital hash is like a fingerprint of some amount of data. The block's

previous hash reference is actually the hash of the block that came before it.

In blockchain, first block is known as Genesis block. After this block, blockchain is initialized that block will always stay blocking them on forever and ever and ever for eternity it will never change. This originate all blockchain always remain first one and it has some data, previous hash with all zeros and own hash. Next block in blockchain has genesis block hash inprevious hash, its own hash and data. As in Fig. 2 , the block is the previous hash of block number two is exactly identical or is exactly block number ones hash and that is where the link comes. That is why abortion is called a chain or a blockchain because the blocks are cryptographically linked with each other through these hashes. Anything was to change in the data but hash cannot be change. Then next block generated cryptographically linked with previous block and so on. If hash not match up longer means something wrong.

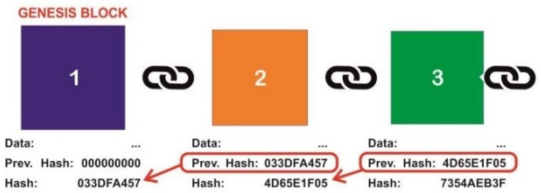

Fig. 2. Blocks are cryptographically linked together.

Blockchains are collection of blocks. A block is a collection of all the transactions with a cryptographic hash of the previous block. At the time of new block to add, a new hash is generated and recorded in recent block's header and in its next block header which created chain. By the time each block header has its previous block hash and its next block hash. This way of chain (link) of block is known as cryptographic links of blocks to validate and undertakes a consensus decision. Old blocks cannot be modified; just new block can be added in chain. New blocks are duplicated across the ledger in the distributed network as a blockchain is distributed ledger and to avoid conflicts rules are made. Simply, blockchains are distributed immutable digital ledgers of cryptographically signed transactions that are grouped into blocks. [3]

IV. TYPES OF BLOCKCHAINS

Blockchain platforms have two main types based on its access are:

A. Public Blockchain.

A public blockchain is known as permission less blockchain, because anyone can join the network. It is one kind of open-ended blockchain, meaning that database is public information. [2] Examples are bit coin and Ethereum. Public blockchain cannot own or controls by a single entity. In public blockchain anyone can read and write (means anyone can participate) to it.

B. Private Blockchain.

A private blockchain is known as permissioned blockchain, requires authentication of the participants within the network, who are typically known to one another [2]. It is one kind of close-ended blockchain Examples are hyper ledger Fabric and Multi-chain. In private blockchain, only specific users can read and write to it.

V. WORKING OF BLOCKCHAIN

Blockchain works in a 6 steps as follows: [1]

A. Born a transaction.

Suppose the transaction is sending crypto-currency from one person A to another person B or anyone can create a transaction that places a line of code to set rules is called a smart contract of the blockchain. In bit coin, it is a transaction while in Ethereum it can be used to mechanize multiple different transactions. A and B can send money to an account based on smart contract. Smart contract controls program and prompt encoded conditions in the contract are met then and then run otherwise not. A smart contract can also send transactions to the rooted blocks of the blockchain [1].

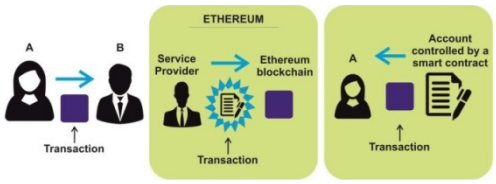

Fig. 3. Born a transaction.

B. After verifying the transaction is broadcast to a computer network.

Here person A sends money to person B. For this transaction is created and person A's computer have to verify link based on B's transaction address using private key to check sufficient fund. After verifying and adding this transaction in blockchain, updated blockchain is broadcast to the computer network. In computer network, nodes will authenticate the transaction for proper rules are followed or not. If found proper, mining nodes will admit it and it will become part of a new block. [1]

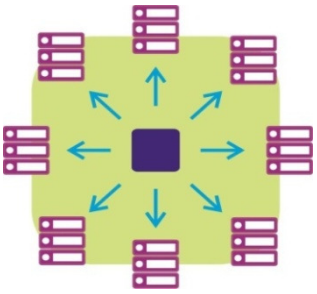

Fig. 4. After verifying, transaction is broadcast to a computer network.

C. Creates new blocks and miners compete for cash

In this step, miners have the race to create new blocks and earn more cash. Miners validate the transaction and arranges into block, then block add into blockchain lists with cryptographic reference to previous block. Miners have a competition to create unique new block based on nonce value with validation and to earn maximum reward in terms of crypto-currency. A nonce is an arbitrary number that is used to connect the blocks using hash to generate cryptographic communication [1].

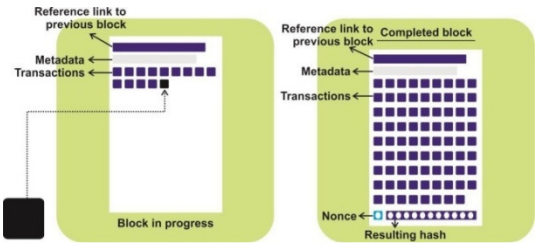

Fig. 5. Creates new blocks

D. Completing a new block

To complete a new block need to work for it. The generated hash must meet certain condition mention in the contract; if it does not meet the condition, the miner try to calculate the hash again based on the arbitrary nonce. Miners have to try lots of numbers to find a valid hash. These processes of blockchain give prevention from hackers to update the ledger and give security. Few blockchain uses proof of work for security and it is the most systematically battle-tested [1].

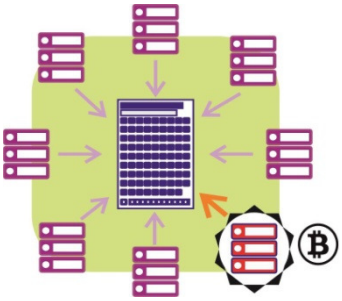

Fig. 6. Completing a new block.

E. Add a new block to the blockchain by another link.

Adding a new block adds another link in the blockchain. This step can secure the ledger. Miners are working on node to earn a crypto-currency/digital token reward for first finding the new block's hash from number of nonce values. Then a miner sends that block to the network for verification. Blockchain's protocol contains the mining difficulty encoding. Difficult blockchain block solving is Bit coin and Ethereum for cryptographic purpose. In blockchain, each block has reference to the previous block and the next block to make mathematical blockchain. Interfering with previous block would necessitate replication of the proof of work for all the blocks in the blockchain [1].

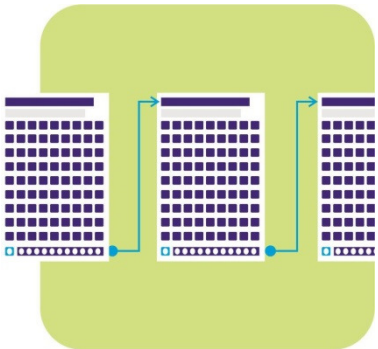

Fig. 7. Add a new block to the blockchain by another link.

F. Forking

Centralized systems are difficult to update at the best of time. When a system is contained of many users, circulated around the world, and governed by the consensus of the users, blockchain changes and implementation becomes tremendously difficult is knows as a forks [3].

Soft Fork: Soft forks occur when the blockchain is updated, but the network nodes running the older version of blockchain and allows approving new blocks. Non-updated nodes of network will identify the new blocks are valid. [3]

Hard Forks: A hard fork occurs when the blockchain is updated, but the blockchain divide in old version and new version of blockchain where nodes are running the older version of blockchain will not accept the transactions created on the new version of the blockchain [3].

VI. SECURITY OF BLOCKCHAIN

Blockchain can share people valuable data secure and tamperproof way to increase trust. For that blockchain store data using new software rules and advanced math that are tremendously difficult for attackers to manipulate. There is still possibility of blockchain systems can fail in places by skilled manipulators in real world, but still security alive and fraud are few. Why blockchains are secure, let us see the Bit coin example. Bit coin's blockchain has the accounting ledger of each and every shared data's history and each Bit coin transactions. This ledger copies shared and store in computer network nodes. The transaction submitted to the ledger after validating the transaction to verify that bit coin available in sender account and receiver account is valid. Validated transactions added into "blocks" and add them in to the blockchain with cryptographic hash to previous block. These blocks blockchain updated as mining nodes. The owners of these blocks are known as miners. Miners have to compete for adding new blocks to the blockchain and to receive the bit coin reward [1]. Mining takes the large amounts of memory and processing power. Here, no centralized point to identify which is then next block will be added in the blockchain. In computer network each node maintains the copy of the blockchain. In blockchain, invalid blocks are identified and removed or deleted from the blockchain. Each block in a blockchain verify and validated computationally is very difficult [3].

Blockchain makes system theoretically immutable by below things:

A. A unique cryptographic hash to each Block

Miners generate a unique hash based on lots of computation power and time. It proofs that miners have to do much work to earn a reward by solving a computational cryptographic puzzle. Block changes also requires a generation of new cryptographic hash [1].

B. Consensus Protocol

The nodes in the network agree on a shared history process is consensus protocol. It also verifies that the hash matches its block or not. It is easy when they updated their respective copy of block in all nodes of the network with the new block [1].

C. Consensus Mechanisms

There are many Consensus Mechanisms [6]

– Proof of Work (PoW)
– Proof of Stack (PoS)
– Delegated Proof of Stake (DPoS)
– Proof of Elapsed Time (PoET) [7]
– Ripple
– Tendermint
– Practical Byzantine Fault Tolerance (PBFT)
– Federated BFT

Table 2 gives a comparison between different consensus algorithms.

Table 2: Typical Consensus Algorithm Comparison [4, 6, 7].

Property	PoW	PoS	DPoS	PoET	Ripple	Tendermint	PBFT and Variants	Federated BFT
Blockchain Type	Open/ Permisionless	Open/ Both	Open	Both	Open	Permissioned	Permissioned	Permisionless
Energy Saving	No	Partial	Partial	Yes	Yes	Yes	Yes	Yes
Tolerated power of advisory	<=25% Computing power	<51% stake (Depends on specific algorithm used)	<51% validators	Unknwon	<51% faulty nodes in UNL	<33.3% byzantine voting power	<=33.3% faulty replicas	<=33.3%
Example	Bit coin	Peer coin	Bitshares	Coin desk, Hyper ledger Saw tooth	Ripple	Tendermint	Hyper ledger Fabric	Stellar, Ripple
Transaction finality	Probabilistic	Probabilistic	—	Probabilistic	—	—	Immediate	Immediate
Transaction Rate	Low	High	Medium	Medium	High	High	High	High
Token needed?	Yes	Yes	Yes	No	—	—	No	No
Cost of participation	Yes	Yes	Yes	No	—	—	No	No
Scalability of peer network	High	High	High	High	—	High	Low	High
Trusted Model	Untrusted	Untrusted	Untrusted	Untrusted	Semi-trusted	—	Semi-trusted	Semi-trusted

Smart contract: According Wikipedia, "*A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are traceable and irreversible*" [17].

In blockchain, Smart Contract gives:
– Contractual clauses for blockchain transactions and executed partially or fully with self-enforcement.
– To give security in blockchain transactions at low cost.
– Offers the public methods to send future transaction to blockchain can then send data.
– Makes transactions simpler and secure for amount transfer between accounts.
– Performs calculations, stores data and makes amount transfer from one to another.
– All miners have to execute the smart contract when mining a new block at that time smart contract execution becomes little costly compared to simple blockchain crypto-currencies.
– Smart contact has also time limit for its execution, if it is exceeded, then transactions execution stops and discarded. This makes the blockchain immutable or tamperproof [1]. These mechanisms to prevent the malicious users to restrict for deploying new block in blockchain.
– Performs a secure transaction without consuming all the resources as denial of service on the mining nodes [3].

Blockchain system security guarantee is decentralization. It keeps copies of the blockchain on the each nodes of large distributed network; there is no weak point to attack. To threaten the computer network requires a large computing power so it is difficult to attack this kind of network. If mining capacity increase may not guarantee the security. Alternative is consensus protocol, which is not depending on the mining as security.

For more security of blockchain require permission to join. These kinds of systems are generally not acceptable due to the anti- hierarchical methods of crypto-currencies but it has only benefit of shared cryptographic database [1].

Thus, a smart contract is a collection of functioning rules and data state which is deployed in a blockchain.

VII. BLOCKCHAIN APPLICATIONS

Blockchain technology is recently most popular for its various applications which are:

Finance and Insurance: Blockchain allows the financial of insurance payment transactions to be finished without third party and to keep bank transaction record in a private blockchain. Here, participant each bank's signing block available under the distributed consensus algorithm with the ability to overcome its immutability. For more security sometimes anonymous transactions can join by bank id [3]. Blockchain can also be used for KYC (Know Your Customer) process by sharing the identity proof not the data [5, 11]. Blockchain can be used in other financial services like online payment, transfer of funds, digital assets, issue and trade assets like bonds, crypto-currency like Bit coin, smart contracts, distributed ledger technology for clearing and settlement, public services, internet of things (IoT), security services, reputation systems, insurance sector like insurance deductible and DAO application etc. [5,

6].

Medical: In medical, there are many persons such as, nurses, doctor, medical providers, pharmacies, insurance companies, have your medical records access without duplication. Just need to take care of record change, runs of the blockchain on which computer network, system governed by you or hospital, etc [3]. Sharing of private medical data records such as, x-rays, blood test results, and other reports between different stakeholders is difficult due to lots of rules and regulations with different data formats and report quality confidence. A blockchain gives a tamper-proof records management for prescription refills. At the time of report sharing, a smart contract gives patients precise control over his/her medical records. Some currently working projects on blockchain at IBM, Massachusetts General Hospital, the Mediledger Project, Kaiser Permanente, Simply Vital Health, etc [1].

Energy Industry: Blockchain can be used to recording autonomous transactions, machine-to-machine electricity use transactions, recording energy certificates, trading of excess renewable energy, devices measuring and recording energy usage, to open new investing and trading opportunities, etc. These all recorded transactions on smart grid gives to analyse the digital platform opportunities and current business model enhancement possibilities. [3] Another blockchain application can be use of the solar panel for the energy production, which is becoming more decentralized and gives a capable field of blockchain [5]. In energy industry, the power grid is always targeted by hackers and blockchain gives security on all transactions data by cryptographic hash. Some currently working projects on blockchain are Power Ledger, the Energy Web Foundation, the Enerchain project, Grid Singularity, Grid+ [1].

Social Media and Internet Advertising: People are managing their personal data on Facebook, Google and others site and had a fear to get exploit it for profit orany reason. Then to avoid fear and to achieve security one of the option is blockchain. Blockchain stores data in encrypted form on a decentralized network instead of particular company servers. Private Blockchain gives opportunities to manage our own identity kind of sensitive data to control its access, even surf the data on the internet is done secretly. Few applications on blockchain are Block stack and Protocol Labs [1].

Food & Agriculture & Supply Chain: Blockchain have a digital ledger that has cryptographic form information so no one can mess it. For example, chocolates to mangoes are tracked using blockchain, if something is wrong then blockchain can track and stop the manufacturing process and inform the process owners. This kind of blockchain system can be useful for farmers and distributors to modify the blockchain and trust enhance that they can't broke due to blockchain security [1]. An interesting application of blockchain technology are store and manage the recoding production, transfer of goods, records of shipping terminals, records of ships, cargo train and delivery trucks, etc. A blockchain provides faith and transparency with end customers and also monitor the supplier actions. Blockchain can also be used for warehouse to manage stocks in it to avoid overstocking [3]. Blockchain can be used for verifying what we bought is organic or not, free of antibiotics, etc. Few applications are IBM, Unilever, Wal-Mart. Nestle, and Cargill [1, 10].

Elections: Blockchain could secure the sensitive data and avoid the risks of the electronic voting system. Voter database is connected with internet and election vote can be given by the voter online to calculate result easily using the distributed ledger. Here need to decide public blockchain used by bit coin or Ethereum, ballots be kept anonymous, permissioned system or not, take care of voter to don't misuse their voter address. Few applications are Agora, Voatz, and Democracy Earth [1].

Trusted Time stamping: Trusted time stamping is the mechanism to verify that certain information is available at specific point of time. Blockchain allows a trusted party to access the data for specific period of time after that access is denied. Best use of time stamping in blockchain is to verifying the task completion on specific date with digital signature approval of task completion [3].

Mobility: In mobility, the distributed ledger technology is used to store the care data securely. Blockchain can be used for decentralized transportation ecosystem; in this people have a token for bus/car/bike ride and everything manage and organize without central authority. Here we can add the feature of passengers and drivers identity verification in a decentralized architecture [5].

As a blockchain, it is a self-sufficient technology for explore more applications but the its combination with other technologies can enable new perspectives of applications such as Assets management, Data Management, Market Places, Data Exchanges and Processes Automation, DAOs, etc.

VIII. BLOCKCHAIN CHEAT POSSIBILITIES

Half the mining power: A group of miners controls the mining computing power or hash rate. So the other miners have the half mining power which increase the possibility of blockchain threaten. Technically, it prevents the new transactions or halts the payments of user by already solved block by selfish miner. It wastes the time of other miners. Sometimes we have one taken for two transactions which prove that blockchain is damaged.

Eclipse attack: In this attack, blockchain specific nodes becomes an isolated in computer network instead of attacking the whole network. Other remains constant active in computer network. Attackers proves that specific isolated nodes gives fake data so by the time it proves that this node is waste of time and resources for transactions confirmation.

Hot wallets money steals: Hot wallets prime targets are online crypto-currency exchanges. Hot wallet applications are connected through the internet and store the private cryptographic keys in it. These keys are used for wallet transactions/payment.

Smart Contract alteration: Blockchain uses smart contract for security enhancement and to perform automated transactions. At the time of smart contract alteration hackers exploited the smart contract and alter as per they want. This happens by stealing a block of smart contract in blockchain. Some cases are their where steal block data or blockchain wallet money from the DAOs.

IX. BLOCKCHAIN LIMITATIONS AND MISCONCEPTIONS [3]

There are the highlights of blockchain limitations and misconceptions.
– A widespread misconception is blockchains has no control or owner and it is permission less but a group of core developers still maintain some level of control.
– Another misconception is blockchain systems are trustless due to lack of trusted third party. There is trust in the cryptographic technologies used.
– A big problem is attackers have enough processing power to damage the blockchain.
– It has possibility to create a huge amount of collision of transactions.
– It can create nasty mining actions like alternative chain creation, ignore the transactions, add empty blocks to make chain longer, etc.
– The concept of immutability within a blockchain system could be attacked.
– Attackers make fake blocks and get rejection of blocks from the network node which disrupts the blockchain sharing on computer network.
– Malicious attackers are annoyances and harm for short-term; to overcome these blockchain performs hard fork.
– Money lost recovery is depending on the blockchain users and developers of it.
– Blockchain users are sometimes sharing the private/public keys.
–Usually finding the required computational power is excessively costly.
– It has proof of work for measuring the processing time and electricity consumption.
– At the time of new node creation, blockchain uses a lot of network bandwidth and increasing a strain on resources.
– Blockchain cannot be used as storage/database. It has limited data storage.
– Transactions require being comparatively small.
– Blockchain stores large amount of data as numbers of pointer/references/hashes.
– Blockchains are decentralized so there is no central control for keys management which makes burden of transfer of Credential Storage to user.
– Blockchain users have to manage their own private keys; there no option/feature in blockchain system like forgot my password to recover the details of lost keys.
–There is no one-to-one relationship between user's private key, not between blockchain addresses and public keys.
– Sometimes blockchain transactions are validating using digital signatures for proving identity in cyber security. This creates confusion for blockchain identity management.
– Blockchain does not support transaction signature authentication by its creator using private key to link the transactions.

X. CONCLUSION

A blockchain platform is capable enough to meet real-world application requirements like high performance, scalability, urgent transaction conclusiveness, low discontinuation, immutable ledger, publicly shared, verifiable, etc. which gives a new pathway for technological advancements. A blockchain relies on existing distributed computer network, cryptographic, and recordkeeping technologies for transactions but uses them in a new manner without trusted third party to achieve the lots of benefits like decentralization, persistency, anonymity and auditability. This paper gives consensus algorithm comparison for security aspects for Blockchain Applications to identify new trusted model for blockchain implementation as Ethereum using Merkel tree. These comparison gives based on Blockchain Type, Energy Saving, Tolerated power of advisory, Transaction finality and rate, token requirement, cost of access and Scalability. Thus, Ethereum and lite coin use started by blockchain based application developers instead of bit coin.

XI. FUTURE SCOPE

Blockchain technologies have tremendous potential to make smart cities solutions to build, operate, consume and market in the near future in e-governance, medical, IOT apps, etc. with respect to security, privacy, efficiency, transparency, and fault-resistances using different blockchain applications using Merkel Tree. Although many research studies going on blockchain technology usage in collaborative applications such as, finance and insurance (like Bit coin, Ethereum, Lite coin, Smart contracts, etc.), medical, energy industry, social media and internet advertising, food-agriculture- supply chain, elections, trusted time stamping, mobility, assets management, data management, market places, data exchanges and processes automation, DAOs, etc.

ACKNOWLEDGEMENTS

This research was supported and guided by Dr. Dharmendra Patel, Associate Professor at CHARUSAT, Changa. We thank our colleagues from CMPICA who provided insight and expertise that greatly assisted to conduct this research.

Conflict of Interest. The authors declare no conflict of interest associated with this work.

REFERENCES

[1]. May/June 2018, Blockchain, MIT Technology Review, *121*(3).
[2]. Kulkarni, S. (2018). The Beauty of the Blockchain. Open Source for you, the Complete Magazine on Open Source, *6*(8), 22-24.
[3]. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.
[4]. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352-375.
[5]. Hamida, E. B., Brousmiche, K. L., Levard, H., & Thea, E. (2017). Blockchain for enterprise: overview, opportunities and challenges, 1-7.
[6]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data,* 557-564.
[7]. Baliga, A. (2017). Understanding blockchain consensus models. *Persistent, 4*, 1-14.

[8]. Haber, S., & Stornetta, W. S. (1990). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography, 437-455.
[9]. Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: *Regulating emerging technologies in Canada. International Journal, 72*(4), 538-562.
[10]. Aixa, D. R. (2018). Analysis and study of data security in the Internet of Things paradigm from a Blockchain technology approach.
[11]. Bosamia, M., & Patel, D. (2018). Current Trends and Future Implementation Possibilities of the Merkel Tree. *International Journal of Computer Sciences and Engineering*, *6*(8), 294-301.
[12] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin. pdf.
[13]. Mikhaylov, A. (2018). Simple and secure Ethereum transactions, theseus.fi.
[14]. Satish Chandra Gullena (2018). IoT Architectures based on Blockchain Technologies. *International Journal of Computer Sciences and Engineering*, *6*(7), 874-878.
[15]. Jiang, H., Liu, D., Ren, Z., & Zhang, T. (2018). Blockchain in the eyes of developers. arXiv preprint arXiv:1806.07080.
[16]. https://en.wikipedia.org/wiki/Blockchain.
[17]. https://en.wikipedia.org/wiki/Smart_contract.

How to cite this article: Bosamia, M. and Patel, D. (2020). Comparisons of Blockchain based Consensus Algorithms for Security Aspects. *International Journal on Emerging Technologies*, *11*(3): 427–434.