Blockchain based Competent Consensus Algorithm for Secure Authentication in Vehicular Networks

Sana Hafeez
Department of Computer Science
Virtual University
Faisalabad, Pakistan
sanahafeez1204@gmail.com

M Rehman Shahid
Department of Computer Science
National Textile University
Faisalabad, Pakistan
mrehman0892@gmail.com

Amer Sohail
Department of Computer Science
Government College University
Faisalabad, Pakistan
amer.sohail291@gmail.com

Sohail Jabbar
Department of Computer Science
National Textile University
Faisalabad, Pakistan
sjabbar.research@gmail.com

M Suleman
Department of Computer Science
Government College University
Faisalabad, Pakistan
sulemanshakil84@yahoo.com

Madiha Zafar
Department of Computer Science
University of Agriculture
Faisalabad, Pakistan
madiha.zafar31@gmail.com

***Abstract*—Vehicular networks are constructed for efficient and secure data flow to make intelligent transportation system. It works by using central storage system which is inefficient as large amount of data is difficult to handle and also becomes the target of malicious activity. The flow of sensitive data on wireless channels for communication of vehicles with other nodes can also be chosen by attackers for attack. These challenges are tackled using blockchain solutions. The blockchain, a farfetched decentralized technology which is undoubtedly going to change overall trends of entire business and professional networking environment in the world to release the burden of centralization on the organizations even on the individuals and several developed countries have started to adopt this trend. This technology would be as dynamic, vibrant, efficient and secure as the category of consensus algorithms is used for the agreement and decision of joining the new block among network nodes. Security and efficiency of vehicular network is maintained through consortium blockchain boasting with Practical Byzantine Fault tolerance (PBFT) algorithm.**

Keywords—Vehicular Networks; Blockchain; decentralize; consensus algorithm; Consortium

I. INTRODUCTION

Internet of things (IoT) in business and industry has been becoming full-fledged for few years because of the benefits and lowering rates of wireless devices as well as the improvement of these devices in terms of power, energy and internet connectivity. The concept and applications of IoT can be seen from small home to large industries because of its uses and prolific results. One of the applications of IoT is Intelligent Transportation system (ITS). This system assures the efficiency and safety of transportation and feel people more secure by using new technologies. ITS actually works by making the network of different devices of vehicles, roadside units and other nodes and this network is called Vehicular Ad-hoc Network (VANET). In VANET there should be minimum communication latency of mobile devices to avoid any danger of accident and other problems so peer to peer (p2p) communication is considered best between the devices. Standards for P2P like IEEE 802.11p, Inter Planetary File System (IPFS), JXTA (Juxtapose) etc have been developed by observing the all these requirements [1] [2].

VANET has been facing the problem of security, privacy, authentication, user identity and data management generated by vehicles. Various solutions have been proposed but blockchain is the one which can be used to rectify all or anyone of above-mentioned problems depending on the requirements. Blockchain technology is gaining popularity as the features are mostly required and necessary by organizations and individuals. It is a decentralized distributed ledger or structured database which forms a peer to peer connection between the non-trusted parties leaving behind the sense of central authority. The methodology saves records or transactions in the form of blocks, and these blocks are connected in ordered form according to time stamping on each block which cannot be altered and cannot be denied making the connected blocks a chain called blockchain [3]. All type of actions and transactions are transparent to the whole network. Here the question arises: how transparency is achieved, how records cannot be altered and why people trust each other when no central party is involved? Transparency is achieved by having the availability of the blockchain or previous all records of the users to each node of the network [4]. Alteration or editing of records or blocks in blockchain cannot be achieved as every block is connected to another block with a Hash value which is fixed output form from the variable length input of transaction, time stamping, nonce and previous block hash. Moreover, this hash is given to the next block to produce its hash and so on. Since to produce from output hash to input data is not possible as SHA256 is applied for hash production, so to get input and to change its transaction is a far-reaching process. Trust is achieved as all nodes of the network are agreed

978-1-7281-4970-7/20/$31.00 ©2020 IEEE

on a given set of rules according to the type of network. These set of rules are the consensus algorithm. Blockchain cannot be secure and accessible if it does not use consensus method which is necessary to develop trust and agreement between the participants of the network. Consensus algorithm can be of any type by depending on the nature of blockchain and other requirements of the organizations and application. Better the consensus model, will lead to better reward giving network. One type of consensus is not able to fulfil all requirements at a time like scalability, security, less energy consumption, average type of hardware, throughput, time consumption, etc. Bitcoin was the first most application of blockchain which was carried with Proof of Work Consensus algorithm. It was introduced by Satoshi Nakamoto to the world and reached the popularity point and maturity [5].

List of few consensus algorithms is as follow:

- Proof-of-Work
- Proof-of-Stake
- Delegated Proof-of-Stake
- Leased Proof-Of-Stake
- Proof of Elapsed Time
- Practical Byzantine Fault Tolerance
- Simplified Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance
- Directed Acyclic Graphs
- Proof-of-Activity
- Proof-of-Importance
- Proof-of-Capacity
- Proof-of-Burn
- Proof-of-Weight

PBFT has medium decentralization, high throughput, low latency, low computing overhead and less storage overhead but high network overhead creates the difficulty in scalability so preeminent case is in private and permissioned blockchain. whereas adversary tolerance is less than 33% faulty replicas. For consensus mechanism, PBFT algorithm is appropriate to use, as Vehicular Networks require intense real timing [6].

The rest of the work is systematized as follow: we discussed various consensus algorithms with comparison mechanism in section II. It is discussed how to model the system for best use with PBFT in section III, while section IV concludes the paper.

II. Review of Literature

The first most implemented model in the blockchain is Proof of work, transforms a tremendous amount of energy into value by making blocks of the transaction, and these blocks are added to the blockchain. Important terms used in the proof of work are nodes, full nodes, partial nodes, mining, miners, hashing, hash function, hash value, and nonce [7].

Mining is to generate correct proofs or correct Hash and all other network nodes verify it so make a capacity to add a block on the blockchain which is an extremely complex mathematical task and involving one in this process is called miners. Here correct hash generated according to consensus rules. Miners are given reward by successfully generating the block [8]. Proof of work makes a bond of trust between the untrusting groups or individuals which is the beauty of this algorithm attracting more and more people. A transaction fee is also collected in the blockchain. Full nodes verify the blocks and store the blockchain so should have ample storage. Partial nodes can be used for wallet purpose having normal storage and normal computing powers [9].

Generally Hashing function are generated by SHA0, SHA1, SHA2, SHA3, but in consensus models, SHA2 means SHA256 (fixed out of 256 bits) and SHA512 (fixed output of 512 bits) is used.

In Proof of Stake (POS), anyone in the network having a higher number of coins can mine or validate new blocks to be added, and at the same time, every block of the network is authenticated. It does not require its users to spend huge amount of computing power to participate in generating blocks. Randomly chosen miners by noticing more coins, so more authority is qualified to be a node in the network. To be a miner has to deposit a certain amount of coins. The voting system is established to have validators. 51% attack is too expensive in this model of consensus and does not require heavy hardware backup as well as no much power consumption so more decentralized as compared to Proof of Work [11].

In Delegated Proof of Stake (DPoS), the nodes are called delegate instead of validator or minors. Delegates, nodes or participants are elected by votes to represent others and add new blocks to the chain. Users can vote for delegates whom they hope are trusted participants. Bitshare and EOS implement this method. Ultimately, Delegated proof of stake(DPoS) is destined to democratize Proof of Stake (PoS) environments by creating a trusted group of delegates which was selected and agreed by other members responsible for validating the network [10].

Leased Proof of Stake (LPoS) was fully launched in May 2017. Individuals having a small number of coins and not able to run full node can get participation in the network means staking by leasing their coins or tokens to mining nodes. They can lease their coins to the network and get benefits from there. Leased tokens are locked up to users account wallet, and the user cannot spend it or trade it. In this way stake weight of the miners increase having more chances to create the next block. Limited amount of power consumption is required. Waves introduced this platform. It is efficient towards network security [12].

Byzantine Fault Tolerance is based on voting system and majority decision is considered final which eliminates the possibility of validation of evil nodes on the network and at the same time makes it hard to find malicious node as all are the part of network. In huge and technical system, this protocol has been used despite of its difficulties in implementation. There are number of modifications in Byzantine Fault Tolerance protocol. If it is simply applied it can manage with two third malicious nodes. Other modifications include controlling communication between devices and digital signatures. It is suitable for business processes as gives liveness [13].

The flow of sensitive data on wireless channels can also be chosen by attackers for attack. These challenges can be tackled if blockchain solutions for data storage as well as the private key signature for exchanging data are used [14]. Data security sharing and storage system based on the consortium blockchain (DSSCB) is specifically proposed which assures integrity and reliability by means of digital signatures while security of database is maintained through consortium blockchain boasting with Practical Byzantine Fault tolerance (PBFT) algorithm to increase the data transaction speed and incentivized the nodes participating in data contribution by using smart contract method [6]. Storage and data sharing of vehicular network become more secure and reliable with DSSCB as compared to other conventional blockchain solutions [15] [16].

In [17], proposed solution is to combine blockchain with internet of vehicles to establish decentralize, secure, anonymous system. The suitable consensus in this system is enhanced Delegated Proof of Stake (DPoS) to choose secure miners and block verification to avoid collusion which DPoS faces if it is used as it is. Two types of secure miners named active miners and standby miners are selected by voting system on the base of reputation according to previous history and suggested opinion by other vehicles. Block created by active miners is inspected by standby miners to avoid collusion and hence reward is also given to standby miners following the contract theory. There is still space for improving the accuracy of reputation.

Instead of using PoW, PoS, DPoS, enhanced DPoS and PoA, Proof of Event (PoE) consensus mechanism is introduced to speed up the transaction process by two phase consecutive transaction, reduce the blowout of fake measures and enhance the reliability of confirming the events occurrence by including two pass threshold base event validation mechanism and saves a lot of power consumption. Inefficiency can be arisen when the number of vehicles is too hefty and requirements of huge number of blockchain messages [17]. The proposed mechanism can be extended for varied type of data like sensor networks, social media and mobile phone instead of vehicle nodes event only.

In [18] a blockchain based solution with proof of concept implementation is proposed for secure and efficient communication i.e. protecting wireless automotive software updates and other services. Proof of concept execution consist of two building blocks the overlay network with specific topology and local update process. Overhead becomes less for a greater number of vehicular interfaces and software distribution is six time faster by using blockchain approach [8] [19]

While proposed consensus mechanism works on the base of reputation and validators are selected by using reputation threshold which are responsible for ledger management. Energy and security of validator nodes can be boosted. To recognize the energy balance, the charging and discharging of electric vehicles are scheduled by using pricing-based incentive mechanism. The overall result of suggested technology makes better performance of energy nodes and electric vehicles while optimization problem can further be explored [20].

The blockchain scheme is proposed for certificate revocation list (CRL) to make the structure simple and to do the thing on distributed platform hence reduces the size of list and overhead of broadcast messages. Proposed algorithm issues decide pseudonym shuffling plan to system managers and records the most updated mapping between pseudonym sets and permanent identities in new blocks Effectiveness of the system can be elevated by approaching towards better consensus algorithm in addition to combination of accountability, security and privacy [23].

The comparison for all described above consensus algorithms is tabulated in TABLE 1 for quick evaluation and assessment.

TABLE I. COMPARISON OF CONSENSUS ALGORITHMS

Study Reference	***Consensus Algorithm***	***Advantages***	***Disadvantages***
[11] [7]	Proof of Work	Secure, harder for 51% attack	No energy efficient, Slow, prone to centralization
[11]	Proof of Stake	Energy efficient, more decentralized, no heavy hardware required, no 51% attack	Full decentralization not possible
[22]	Delagated Proof of Stake	Energy efficient, secure, scalable , fast, more decentralized	Not much transparent
[12]	Leased proof of Stake	Fair usage, Energy efficient, secure, scalable , fast, more decentralized	Energy consumption, Wastage of coins
[9]	Proof of Activity	No 51% attack,fair shair	Double spending, energy consumption
[13]	Byzantine Fault Tolerance	Easy implementation, reduced energy, fast	Prone to Sybil Attack, communication problem
[20]	Delegated Byzantine Fault Tolerance	Secure, much efficient, scalable	Several root chains
[23]	Proof of Elapsed time	Cost effective, secure, energy efficient	Slow
[9]	Proof of Weight	Scalable, customized , energy efficient	Hard Incentivized
[21]	Proof of Burn	More decentralized, stable, energy efficient	Wastage of coins
[21]	Proof of Space/Capacity	Energy efficient, no huge computation power	Redundant disk space, not much secure
[24]	Proof of Authority	Energy efficient, minimal delay	Less secure, somehow centralized

Study Reference	*Consensus Algorithm*	*Advantages*	*Disadvantages*
[25] [10]	Proof of Importance	Fair participation, vesting, secure	Slow, communication problem
[19] [8]	Proof of Concept/DAG	Scalable, more throughput , fast, secure , low cost	No explicit incentivization
[21]	Command Chain Protocol	Highly secure, privacy, fast	Less secure

III. Modeling to use PBFT

Blockchain is essentially a distributed database and improves network security. Main feature of blockchain is its ability to enable sharing of a common ledger amongst anonymous groups or users using distributed consensus algorithms which can apply cryptographic puzzles with appropriate difficulty. Transactions/messages or other records are stored in blocks, and different blocks are chained by applying digital signature, also called hash, which provide tamperproof, traceability and other security properties.

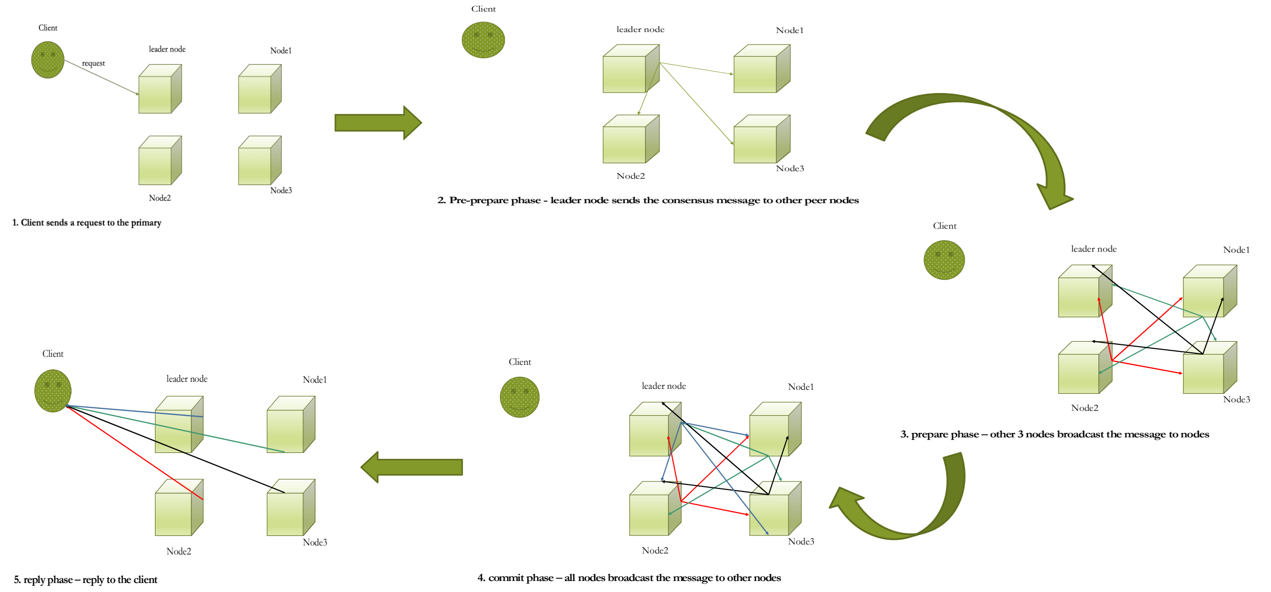
However, can be divided into three categories, i.e., public blockchain, private blockchain and consortium blockchain. To deploy it in the vehicular network, we must adopt the best one according to the properties of vehicular network. Participation by accessing and mining the block without any registration and authentication happens in public blockchain. Since the vehicles, roadside units and other equipment's should be registered from administration office of vehicles, the public blockchain is not suitable for this application. While there are restrictions for the user registration and mining the block in private blockchain but still it cannot be adopted for vehicular network because it is harder to calculate all the vehicle and RSUs are secure and only transmission fault occurs. We cannot say that there would be only one type of infrastructure in each brand of vehicle so making a place for security risk. This all concludes to implement consortium blockchain considering the byzantine errors and communication problems.

System model that is considered best for this research includes number of areas. There are few entities/nodes in each area which are described as under:

1. Inspection Node (IN): Inspection node is a fully trusted authority, which is responsible for the registration of OBUs and Facilitators and tracing illegal vehicles.
2. Facilitator Node (FN): A Facilitator Node is primarily responsible for dealing all vehicular Fog datacentres and authenticating OBUs in its area and each area has one facilitator node. Each Facilitator Node maintains a public ledger that contains all access records of vehicles. The public ledger only can be accessed by Inspection Node, Facilitator Node and SNs.
3. Spectator Node (SN): SN is a peer for writing authentication results to the public ledger through a consensus algorithm. There is a SN for each area. All SNs and Facilitator nodes (FN) form a consortium blockchain.
4. Roadside Unit (RSU): RSU is the manager of a Vehicular fog datacentre and supplies Vehicular fog Services to legal OBUs. It belongs only to an area governed by a FN.
5. Onboard Unit (OBU): OBU is a user which uses the services available to it. It is equipped with computational and communication functions such as embedded computer, wireless network interface, GPS receiver, vehicle navigation system, digital map and so on. It needs to be registered at IN to have the services available in vehicular networks.

IV. Working of Practical Byzantine Fault Tolerance

PBFT concentrates on replication that allows to tolerate Byzantine faults i.e. malicious nodes by assuming there are independent node failures and manipulated messages sent through specific nodes.



1. Client sends a request to the primary

2. Pre-prepare phase - leader node sends the consensus message to other peer nodes

3. prepare phase – other 3 nodes broadcast the message to nodes

4. commit phase – all nodes broadcast the message to other nodes

5. reply phase – reply to the client

Fig. 1. Working of PBFT

Nodes in a PBFT system are ordered in sequence with one node behaving as the leader and others referred to as backup nodes.

All nodes in the system communicate with one another with the goal being that all honest nodes will come to an agreement of the state of the system using a majority rule. Nodes must prove that messages originated from a specific peer node, and they must verify that the message was not modified during transmission by doing all in four steps as shown in Fig. 1. which includes (i) sending request to the leader node for service (ii) leader broadcasts it to all backup nodes (iii) nodes perform the request and reply to client node and (iv) The client awaits *f+1* reply from different nodes with the same result, where f represents the maximum number of potentially faulty nodes. For the PBFT system to function, the number of malicious nodes must not equal or exceed one third of all nodes in the system. Similar to the proof of work consensus mechanism, the more nodes there are in a PBFT network, the more secure it becomes.

The leading node is changed during every round and can be replaced if a certain amount of time has passed without the leading node broadcasting the request. Also, a majority of honest nodes can determine when a leader is faulty and replace them with the next leader in line.

The only problem exists here is the scalability as the communication cost is $O(n^2)$ where n is the number of nodes in blockchain network. By scaling up the network gives a huge message overhead so the model discussed in this section is considered best up till now due to the addition of upper layer of nodes less in numbers to participate in consensus.

V. CONCLUSION

The Consensus models driven by whichever blockchain platform are there for enhancement of efficiency and dwindling the security threats and not one type has all the properties of energy efficiency, scalability, cost efficiency, speediness and throughput etcetera but approaching towards the better algorithm can be furnished with various of them as vehicular networks with PBFT and improved versions to overcome scalability issues. Prologue and commendation of new models have attracted the entire assiduousness building new paths to implement technology. In depth study and comparison of each and every consensus algorithm would endow with a good opportunity for advance research.

REFERENCES

[1] M. Cebe, E. Erdin, K. Akkaya, H. Aksu and S. Uluagac, "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles," *IEEE Comunication Magazines,* pp. 50 - 57, 2018.

[2] M. Liu, Y. Teng, R. Yu, Victor and M. Song, "Deep Reinforcement Learning Based Performance Optimization in Blockchain-Enabled Internet of Vehicle," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, China, 2019.

[3] A. Reyna, C. Martín, J. Che, E. Soler and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems,* pp. 173-190, november, 2018.

[4] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda and V. Santamaría, "To Blockchain or Not to Blockchain: That Is the Question," *IT Professional,* vol. 20, no. 2, pp. 62 - 74, 2018.

[5] Rajbhandari and Rajat, "Exploring Blockchain – Technology Behind Bitcoin and Implications for Transforming Transportation, Final Report," Texas A&M Transportation Institute, 2018.

[6] D. Massessi, "Blockchain Consensus And Fault Tolerance In A Nutshell," 6 1 2019. [Online]. Available: https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03.

[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[8] L. S. Sankar, M. Sindhu and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 6-7 Jan. 2017.

[9] H. Anwar, "Consensus Algorithms: The Root Of The Blockchain Technology," 25 8 2018. [Online]. Available: https://101blockchains.com/consensus-algorithms-blockchain/.

[10] J. Sun, J. Yan and K. Z. K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financial Innovation,* 2016.

[11] L. M. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 21-25 May 2018.

[12] "Leased Proof of Stake Consensus Explained," 28 4 2019. [Online]. Available: https://www.binance.vision/blockchain/leased-proof-of-stake-consensus-explained.

[13] K. Lei, Q. Zhang, L. Xu and Z. Qi, "Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain," in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, Singapore, 2018.

[14] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *Journal of Industrial Information Integration,* vol. 13, pp. 2-39, march 2019.

[15] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng and C.-C. Liu, "Blockchain-Based Traffic Event Validation and Trust Verification for VANETs," *IEEE Access* , pp. 30868 - 30877, 2019.

[16] Y. Yao, X. Chang and J. Mišić, "BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services," *IEEE Internet of Things Journal* , pp. 3775 - 3784, 2019.

[17] E. F. Jesus, V. R. L. Chicarino, C. V. N. d. Albuquerque and A. A. d. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Security and Communication Networks,* p. 27, 2018.

[18] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 25-30 June 2017 .

[19] M. Huillet, "ebit-18-iota-and-volkswagen-present-proof-of-concept-for-autonomous-cars," cointelegraph, 11 june 2018. [Online]. Available: https://cointelegraph.com/news/cebit-18-iota-and-volkswagen-present-proof-of-concept-for-autonomous-cars. [Accessed 25 April 2019].

[20] G.-T. Nguyen and u. Kim, "A Survey about Consensus Algorithms," *journal of information processing systems,* vol. 14, pp. 101-128, 2018.

[21] "PoET 1.0 Specification," [Online]. Available: https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html.

[22] D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains," *IEEE Potentials,* pp. 26-29, 2018.

[23] M. R. Shahid, S. Mehmood, S. Hafeez, B. Zahid, S. Jabbar and R. Ashraf, "Blockchain based sahre economy trust point: case study based validation," in *3rd international conference on future networks and distributed systems* , Paris , 2019.

[24] M. A. Habib, M. Ahmad, S. Jabbar, S. Khalid, J. Chaudhry and K. Saleem, "security and privacy based access control model for internet of connected vehicles," *future generation computer systems ,* vol. 97, pp. 687-696, 2019.

[25] M. Kabeer, F. Riaz, S. Jabbar, Moayad and S. Abid, "real world modeling and design of novel simulator for effective computing inspired autonomous vehicle," in *15th international wireless comminication and mobile comuting conferenec* , morocco, 2019.