Blockchain Based Intelligent Transport System

Muhammad Waseem[1], Khawaja Arslan Ahmed[2], Muhammad Talha Azeem[3]

Xian University of Science and Technology, Shaanxi Sheng, Xian Shi, Beilin Qu, Yan Ta I T Shang Quan, China

E-mail: wasem.hanif89@gmail.com[1], askankhawaja@gmail.com[2], Talhaazeem82@gmail.com[3]

Abstract. Blockchain technology is widely studied in these days and has vital role in the ITS and Vehicular network. Intelligent Transport System (ITS) have resolved several issues of transportation like congestion, electronic toll collection, traffic light cameras, traffic updates, and environment forecasting. The vehicular network is the ever-increasing network it is not only facilitates us but also brings new challenges with it. The mobile nature of vehicular networks it is very important to collect and broadcast information of traffic events in real-time. A little delay to broadcast important information or deciding on this information can cause a serious situation in the mobile vehicular network. Moreover, malicious vehicles in the network broadcasting false information about these traffic events cause a disturbance in the network. In large-scale scenarios, the transmission of malicious messages offers a lot of danger to the system. They can wrongly claim the roads and provide false information about the incident. These traffic events can be life-threatening and cause unwanted situations like accidents, wastage of time and other resources. Therefore, it is very much important to provide real-time information on recent traffic events and real-time authentication of vehicles that broadcast information in the network. Traditional studies are unable to solve these security issues and contain a single point of failure issue. These studies are centralized and dependent on a single higher authority. Moreover, they have serious security concerns that are harmful for vehicular network. Moreover, any vehicles are unwilling to share their private information while broadcasting information about traffic events because they are strangers to each other. And if a vehicle does not want to share its private information like name, id, etc. It is not possible to authenticate this vehicle and manage trust in the network. It means that it is very crucial to prevent vehicles to broadcast wrong information in the network while preserving their privacy at the same time. Therefore, there is a need to authenticate vehicles and manage trust in the network while preserving their privacy simultaneously. Blockchain can offer better solution to solve these issues due to its secure distributed environment and features that ensure immutability about actions. The purpose of this report is to provide real-time security and privacy in the network. It is also ensured that vehicles get real-time authenticated information about traffic incidents from legitimate vehicles while simultaneously preserving their privacy. It means that only authenticated and legitimate entities (vehicles) can participate in vehicular network and privacy of both sender and receiver is secured in the network. Details of conducted experiments are given, and shreds of evidence are provided to evaluate the performance of architectures for authentication and trust management. The shreds of evidence show that these blockchain-based systems can solve security and trust issues more effectively.

Keywords: Intelligent transport system, blockchain technology, real-time information, vehicular network

1. Introduction

In recent years, considerable academic advancement, and business growth in Intelligent Transport Systems (ITS) has been enabled through the exponential development of new sensing, networking, research and computational technologies and tools. Intelligent Transportation System (ITS) provides services to enhance traffic management and makes the use of the traffic network more safely. Moreover, it increases the efficiency of road traffic and applied to all modes of transport [1].

In general, ITS services are namely:

1) intelligent transport, an efficient path can be selected in terms of economy and time by intelligent routing preparation and navigation, preventing traffic jams, etc.

2) With the help of vehicles interconnectivity, barriers early warnings can be issued, or internal or external system failures can be conveyed to the driver.

3) Driver or vehicle support services, such as fines for violation of road laws, automated repair of vehicles.

4) Entertainment for onboard users, such as streaming media, etc.

5) providing statistical data about the surrounding areas, traffic, and environment, from crowdsourcing method [2].

Blockchain is known as one of the most transformative technology of current time. A distributed ledger system in form of blockchain, is new data storage and processing method. The major characteristics of mutual honesty, anonymity, data confidentiality and transparency have a great opportunity for resolving the challenges of the established ITS.

The goal of ITS is to gather, analyze and apply all transport-related data to monitor the flow of vehicles in order to increase traffic quality and safety [3]. Researchers predict that blockchain deployment in transport should primarily concentrate on the application of technology to minimize or by third party cost elimination (i.e., shared mobility, fare increases, asset transfer and supply chain), by minimizing a particular point of failures (i.e., the internet of services like wired and autonomous vehicles) and improve efficiency (i.e., supply chain and transfer of assets) that show in figure 1[4]. ITS professionals commonly seek to create new tools (e.g., property, road) and intelligent technologies (e.g., sensors, self-driving cars) [4].

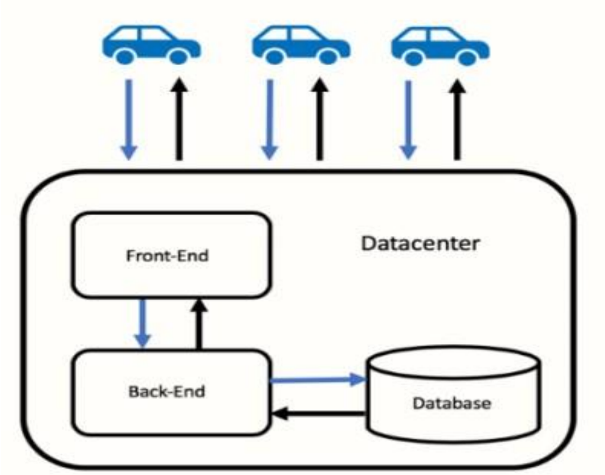

Figure 1. Central Server Vehicular-network.

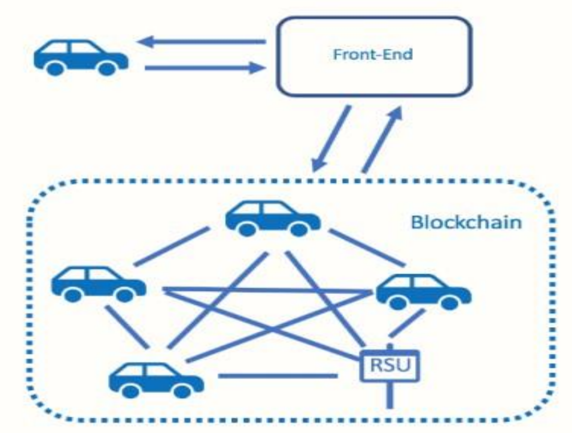

Figure 2. Blockchain-based Vehicular network.

The issues that ITS is facing now can be solved by Blockchain and the underlying architecture can also be used for social dealing. Blockchain is a perfect solution to the key issues faced by ITSs, and also a potential underlying architecture for dealing with the social [4]. Such intelligent systems collect and process a variety of arriving vehicle details as input tables to produce optimized traffic plans at each location that shows in figure 2. According to restricted computing capacity in real-time processing and their central algorithms and data centers, they are vulnerable when the input table involves malicious attacks vehicle information [5]. It is Difficult to detect malicious attacks.

New vehicles are becoming increasingly dependent on the on-board device and control functions. Attacking the internal software or control functions of a vehicle (e.g., downloading on-line malicious software) can cause severe safety problems for drivers and passengers [2-5]. Any of the issues described above can be addressed by implementing new transport policies. In fact, the approach aligns for extreme situations, but may not be suitable in insignificant circumstances. Another plan adds more services by constructing new roads and/or upgrading existing facilities, such as bridge widening [6]. However, Due to the ever-increasing volatility, variety, and sophistication of behaviors, processes and techniques involved in this environment, ITS has now indicated a high degree of social complication rather than intelligent forecasts for days, leaving some early issues unresolved or even worse behind. Security threats posed by the emerging movement towards centralization of ITSs are a primary issue. Fast-growing inventions, like IoT, made it easier for analyzing data and decisions processing by the authorities to be used. A block chain based ITS system is proposed which describe an ITS-based, seven-layer computational model for blockchain and to discuss core research concerns in blockchain based ITS on this basis. Study found blockchain to be one of the stable and trustworthy frameworks for the development of newly built parallel transport management systems [4].

Brief introduction and overview of both emerging technologies blockchain and ITS are described in below sections.

1.1. Blockchain Technology

It was first introduced in 1991 by two researchers, who was working for a digital timestamp for documents which cannot be backdated or changed [6]. Satoshi Nakamoto implemented blockchain technology first time in 2008 and introduced a cryptocurrency named as Bitcoin [8]. The dilemma of centralized data storage and information management was solved in the Bitcoin white paper. This section presents an overview of blockchain technology.

1.1.1 Components of Blockchain. There are set of basic components of blockchain which include ledger, block, hashing, transaction, minor and consensus mechanism.[10].

The **ledger** is a data structure that is used to store different kinds of data. It is used to store all transactions ever made on the network by all participating users. The ledger was also distributed between the participating nodes, so each user has their own copy of the ledger.

Each **block** comprises a series of transactions and has been chained together by storing the preceding block's unique hash value in the current block. Like a chain, this connection interlocks together.

The **hash** function is essentially a mathematical problem that minors must crack to find a block. It verifies the data integrity of the contents of each block.

The smallest process unit is a **transaction**, and a collection of transactions are combined in a block and processed.

A certain transaction cannot be added to the block until permission is confirmed by most of the participating nodes in the blockchain network. For minors, the size of a transaction is important as small transactions require less power and are simpler to verify. Minors are computer/agents that attempt mining to discover new block [10].

In the blockchain, different blocks are chronologically connected and make a chain. Each block has a previous block hash in its header. Each block in chain contains previous block hash, data, nonce and timestamp shown in figure 3. First bock of chain is called genesis. A nonce is a magical number given by miners to complete hash according to the format of blockchain, timestamp describes time and day at which the block is created [11].

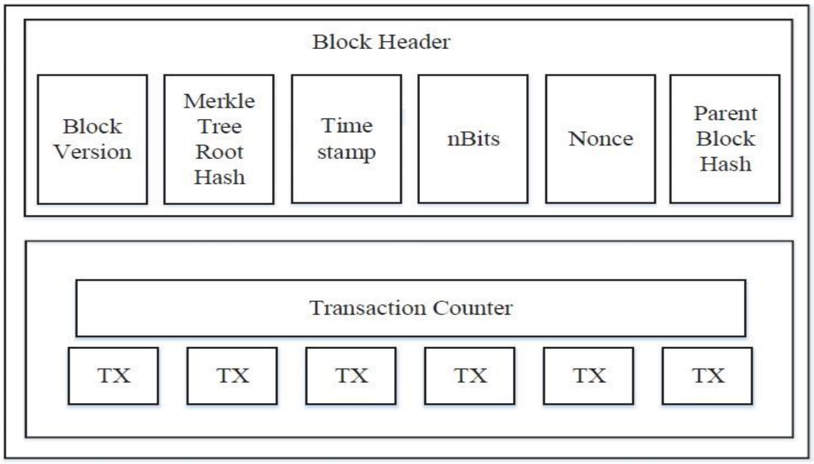

Figure 3. The architecture of Block in Blockchain.

1.1.2 Layered Architecture of Blockchain. The blockchain system consists of six layers namely, data layer, network layer, consensus layer, incentive layer, contract layer and application layer as shown in figure 4. The data layer consists of the underlying data blocks and related techniques like Merkle tree timestamp encryption etc.

The network layer encapsulates the mechanisms for distributed networking, data transmission and data verification. The consensus layer mainly includes various consensus algorithms for network nodes. Consensus layers have consensus algorithms like proof of work, and proof of storage. Incentive layer defines distribution incentives for nodes and allocation of incentive to receiving nodes. Contract layers provides rules and algorithms in scripting languages for node agreements. Application layer defines the area of deploying the blockchain like, IoTs, smart city, and market security etc. [12].

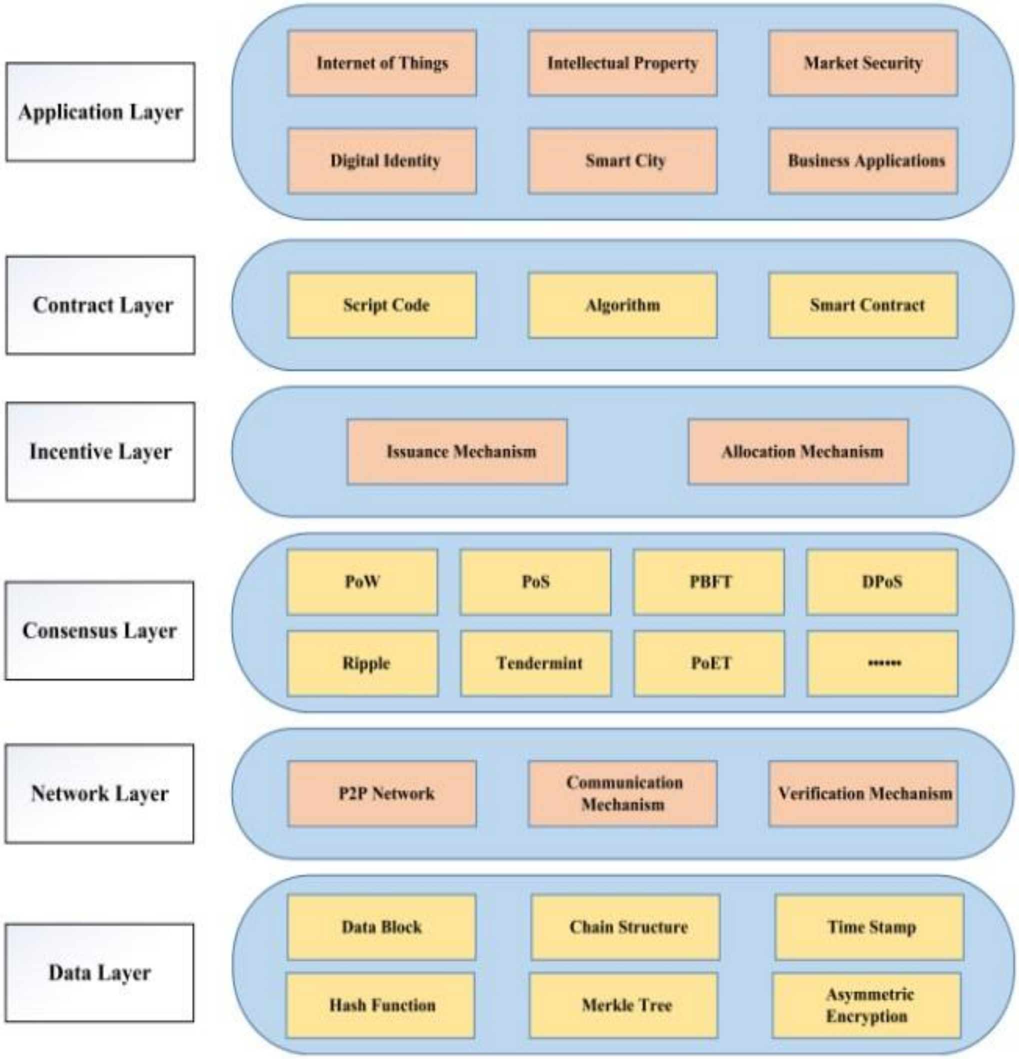

Figure 4. The Layered Architecture Of Blockchain System.

1.1.3 Blockchain Types. Types of blockchain Mainly blockchain is dividing into three types [13]. Following are the main types:

- Public blockchain.
- Private blockchain.
- Consortium blockchain.

Following table is defining the properties of all these types of blockchain.

Table 1. Comparison of types of blockchains.

Blockchain Properties	Public type blockchain	Private type blockchain	Consortium type blockchain
Consensus by	All entities	Entities selected by Organization	Predefined nodes by administration
Data access	Public	Public or restricted	Public or restricted
Immutability	Impossible to temper	Could be tempered	Could be tempered
Mining efficiency	Very low	Very high	Very high
Decentralized	Yes	No	Partially decentralized
Consensus type	Permission less	Permissioned	Selective permissioned

1.2. Intelligent Transport System ITS

Transportation is the movement of different things (goods) and people from one region to another. As we come to know that ITS can be very helpful for traffic system management and road safety. A lot of research has been done on ITS for improving the efficiency of ITS since a few years. ITS is transportation system which processes and share information about congestion, traffic management, environmental changes. ITS have wide range of communication ability between vehicle to vehicle (V2V), vehicle to infrastructure (V2I). Also, ITS incorporates wireless and wire line communication-based information. Commonly, V2V and V2I have wireless technology whereas infrastructure to infrastructure have wire line communication. Internet of Things (IoTs) are used in ITS for collection of data like, congestion detection, electronic toll collection, traffic light cameras, traffic updates, and environment forecasting.

1.2.1. Working of ITS. ITS is controlled by a local authority with limited area. So, different areas have different ITSs [17]. Further these ITSs are also interconnected. In an ITS system have following operation performed by authority:

- Data collection: IoTs are fixed in all nodes of ITS to collect data from various sources. Data collected by IoTs are delays, location, travel time, and surveillance etc.
- Data transmission: In ITS real time communication is primary concern of every node or vehicle. Vehicle transmit collected data to nearby data center. After data analysis, data send back to concern vehicles as an information. V2V communication is done by

dedicated short range communication (DSRC) whereas V2I is done by continuous air interface long and medium range (CALM).

- Data analysis: After data receiving at nearest data center, the process of data cleaning, error rectification, data synthesis, and further logical analysis. This analyzed data is used for current situation and for future forecasting.

1.2.2. Component of ITS. Every ITS has different component based on its application [18]. We are describing the general component that is compulsory for every ITS as shown in figure 5.

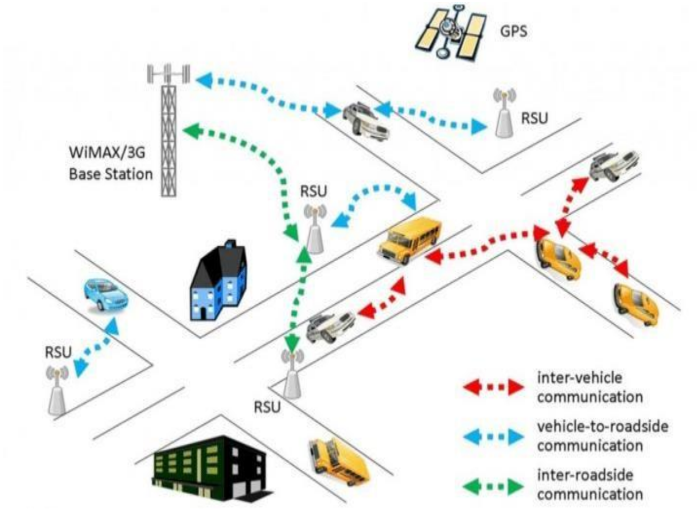
GPS
WiMAX/3G
Base Station
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Figure 5. Working of Intelligent Transport System.

- Global positioning system (GPS): For the location purposes, this component is used and ITS gather information of all vehicles from GPS.
- Cloud storage: ITS have large number of vehicles which send and receive large amount of data. This data cannot be stored locally, so cloud server is used for this purpose.
- Roadside unit (RSU): Vehicles cannot communicate directly with long distance vehicles. For this purpose, RSU are installed along with road. Vehicles communicate with nearest RSU and RSU then convey his message to other vehicles or RSUs.
- Vehicles and other devices: Transportation system have different type of vehicles. All have different IoT sensors and variety of communication channels. ITS have ability to incorporate all the vehicles. Other devices have cell phones, laptops, and watches.

1.3. Blockchain and ITS

With the increasing of digitalization, transportation system also needs security, privacy, and immutability. Whereas blockchain is a technology which can efficiently overcome such issues [19]. Traditional transportation system can only handle by physical presence whereas with blockchain cross border vehicle management is possible. Further, there is trust issue on third party and cross border entities, blockchain provides trust between both parties. Blockchain provides security during making contract. In the carpooling services, blockchain provides anonymity and easy payment method. In electric vehicle charging system, blockchain provides anonymity and charging payment method more securely and easily. V2V communication require anonymity and reward for message initiator, blockchain provides all the effective features that in V2V communication.

1.4. Scope

In Blockchain-based systems in transportation, the centralization is eliminated and all vehicles in the network are equally responsible for making decisions. The architecture of the vehicular network based on blockchain is shown in figure 6.

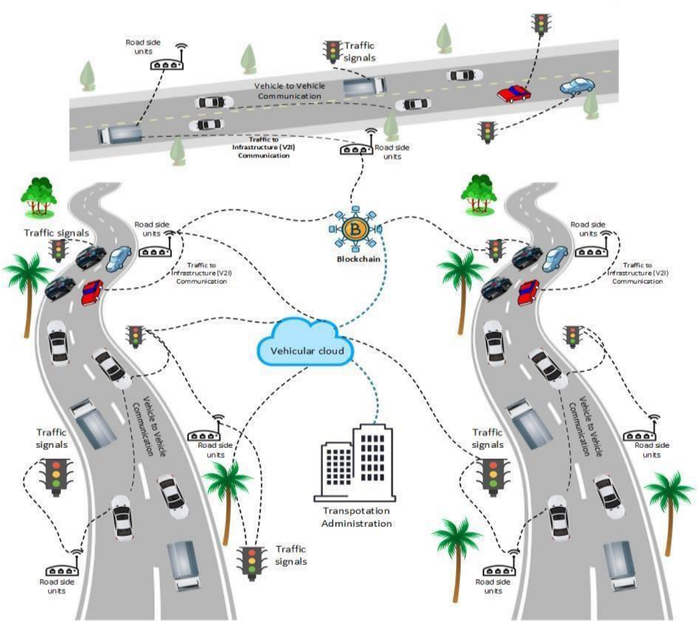
Road side units
Traffic signals
Vehicle to Vehicle Communication
Traffic to Infrastructure (V2I) Communication
Road side units
Traffic signals
Road side units
Traffic to Infrastructure (V2I) Communication
Blockchain
Road side units
Traffic to Infrastructure (V2I) Communication
Vehicular cloud
Vehicle to Vehicle Communication
Traffic signals
Road side units
Transpotation Administration
Traffic signals
Road side units
Vehicle to Vehicle Communication
Traffic signals
Road side units
Road side units

Figure 6. The Architecture of Vehicular Network based on Blockchain.

This architecture shows that vehicles are directly connected and with other entities like the sensors and RSU without third party involvement. In this vehicular network, all vehicles and other entities are continuously monitoring the actions of each other and each device authenticates to a pair in the network as shown in figure 4. This blockchain-based vehicular architecture covers following areas which are explained below.

2. Literature Review / Methodology

The data and knowledge for this report are collected by well-known research repositories ScienceDirect, Google Scholar and IEEE Xplore. Few selective articles are included related to the topic of blockchain based system and vehicular transportation. Main focused topics are security, trust and privacy of data and process in ITS technology and vehicle network.

A mechanism proposed in [25] solves many issues regarding vehicular networks like offering high bandwidth, quality of service and low latency. However, pervasive, secure, and reliable communications are not provided by the 5G cellular network. They proposed a scheme to achieve the scalability and security of Vehicular Ad-hoc Networks (VANETs). An SDN is used efficiently to manage the ubiquitous system. A twofold blockchain-based security module is proposed. First, the vehicles are registered in the network by providing their credential. When any vehicle is broadcast any message or share data in the network then the legitimacy of the vehicle is checked by the authentication module in the first instant. If the vehicle is registered, then its data is reached to other entities in the network. Otherwise, the data is revoked, and such a vehicle is announced as a malicious vehicle in the network. However, the control plane creates the single point of failure issue.

When a control plane is exploited by an attacker, the central control point is damaged and the whole information flow of the system is disturbed. In [26], it is highlighted that it is very difficult to spread information in a volatile vehicular network. The authors in [27] highlighted that message should be broadcasted anonymously in the network since it contains the secret information. However, it is difficult to expose the vehicle if the message is broadcasted anonymously. So, to overcome this issue, the author in [28] proposed that the concept of conditional privacy that is achieved by a registration authority. [29]and [30] provides a mechanism that overcomes traditional mechanisms which are purely relied on centralized data centers. Mobile behavior of vehicles is the main issue in the scheme which can lose their connectivity. Therefore, it is more difficult to authenticate moving vehicles in real-time. However, the authors authenticate the vehicles directly from the blockchain. The reason is that blockchain provides a distributed database that makes real-time authentication possible.

In a vehicular network, wireless communication allows the vehicles to monitor the exchanged data through the network. However, it results in breaching the privacy and safety of vehicles. Malicious vehicles can be dangerous for the existing network by providing false information [31]. Any selfish node can provide fake information about roads to increase his traveling speed and hackers can take over the central authority to spread fake information globally [32]. In VANETs, many vehicles are unwilling to share their private information because they are strangers to each other. In large-scale scenarios, the transmission of malicious messages offers a lot of danger to the system. They can wrongly claim the roads and provide false information about the incident. While VANETs require a secure IoT environment for communication. In [21], Proof of Event can solve this problem by setting the threshold of the correct data which is validated by different nodes. So that event will never be triggered. If bogus messages are received from the other vehicle then miner nodes verify and immediately report to the Law Enforcement Authority. In [27] and [32], the system requires information from a legitimate vehicle so that message should be authentic, credible and immutable to protect from attackers. In [27], the authors used a new framework of blockchain assisted with the real-time cloud-based video reporting system, which carries the trust management and message of the vehicle. The authority authenticates the legitimacy of the vehicle by issuing public and private keys. Then these vehicles are allowed to transmit real-time videos and messages about the road condition.

In [30], the author proposed a privacy-preserving trust model, which gives an unknown reputation system to get rid of forged messages. Lexicographic Merkle Tree (LMT) is used for the extension of blockchain for preserving privacy. The link-ability between real identity of vehicle and its public key is eliminated from the blockchain. Certificate Authority (CA) is responsible for issuing certificates to new vehicles and revoking certificates of malicious vehicles. All actions performed by CA are monitored and stored in blockchain for transparency. The authors proposed the scheme for blocking the forged messages, which gives the reputation system in which the algorithm calculates reputation. In [25] and [31], the authors proposed the scenario of Software Defined Network (SDN) working with 5G to maintain the vehicular network. The proposed model is equipped with 5G and SDN. The control plane and data plane are decoupled to maintain the network for ubiquitous functionality, scalability; moreover, they are easy to manage. Open flow switches and routers act as a controller while the base stations and access points are working under the data plane to take command from the controller and proceed accordingly. These nodes usually are RSUs and there is no consensus participation by sensing nodes. So, there is less chance of identity breaching or data privacy. Besides, the security mechanism will faster as be compared to the traditional mechanism. The authors in [28] proposed the Internet of vehicles-based networks working on the mechanism of blockchain. The proposed system provided the V2I authentication mechanism, which leads toward the dependability of CA. This model performs the accountability of malicious vehicles. The authors also proposed the storage mechanism that reduces the storage load and provides the integrity of data and privacy. They provide security analysis that performs efficiently as compared to other schemes [30].

The regular consensus takes place by the Proof of Work (PoW) and PoS so that malicious vehicles do not participate in the system. If any vehicle is detected as malicious then it will be banned temporarily. Besides, to track back the malicious vehicle, the privacy of legitimate vehicles still be hidden from the rest of the network [27]. Blockchain is introduced to overcome the issue that arises in the centralized database system [21]. A consortium blockchain is proposed in which the pre-selected node can participate in the consensus mechanism. Only their calculated solution will be considered [31]. The authors implemented a new mechanism of consensus that is PoE. It allows the vehicle to meet any threshold. If the PoE result confirms any incident, then the information will be broadcasted by participated vehicles and stored on the blockchain publicly. PoE mechanism also confirms the selfishness and malicious behaviors of the vehicles [32].

3. Critical Discussion and Evaluation

One of the important operations in the vehicular network is to broadcast and receive important information about traffic events in a very short time. It is very important to collect and broadcast information of particular traffic events in real-time. A little delay to broadcast important information or deciding on this information can cause a serious situation in the mobile vehicular network. This information is only for a specific region of the vehicular network. Moreover, malicious vehicles in the network broadcasting false information about these traffic events cause a disturbance in the network. Therefore, it is very difficult to spread information in a volatile vehicular network when there are trust issues and malicious nodes in the network. In [26], there is a blockchain-based architecture for storing and broadcasting node information and the trust values of vehicles of the vehicular network. Here, trustworthiness and node information behave like a transaction in bitcoin. This mechanism is scalable for large scale networks. When an unconfirmed event occurs, other vehicles verify this event and update (store) it in the blockchain.

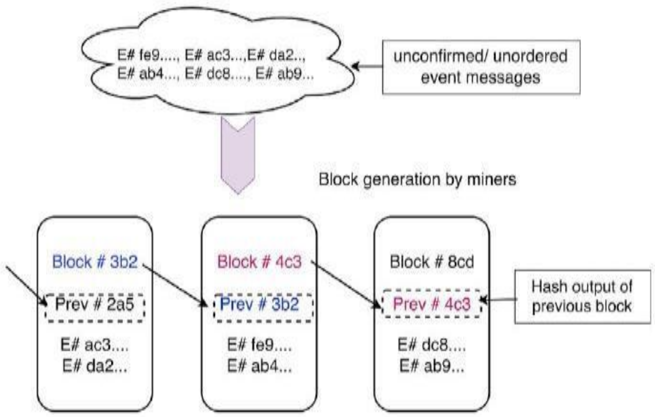
E# fe9...., E# ac3...,E# da2..,
E# ab4..., E# dc8...., E# ab9...
unconfirmed/ unordered event messages
Block generation by miners
Block # 3b2
Prev # 2a5
E# ac3....
E# da2...
Block # 4c3
Prev # 3b2
E# fe9....
E# ab4...
Block # 8cd
Prev # 4c3
E# dc8....
E# ab9...
Hash output of previous block

Figure 7. Blockchain Architecture for Messages Verification.

The architecture of blockchain when an unconfirmed event occurs (vehicle broadcast information in the network) is shown in figure 7 Blockchain Architecture For Messages Verification. To evaluate the performance message and storage overhead is calculated. Each safety message in this network has a size of 512 bytes10 and the header of the block has the size of 80 bytes. Therefore, one block with single message consumes 600 bytes. The authors assume that 100s are required to generate a block to prevent attacks. In this way, 36 blocks are generated in 60 minutes (1 hour). Hence in one year, there is 180.45MB of storage overhead for a blockchain with a message explained below:

$$\text{Storage overhead} = 600\text{bytes}*36*24*365 = 180.45\text{MB/year}.$$

To evaluate the proposed mechanism in terms of message overhead, an assumption is made that 2000 vehicles are traveling in a specific region (area). These vehicles broadcast messages in this region for a specific period. The transaction of this message carrying important information can be calculated as Tx*(B*t). Here, Tx is the number of messages per period, t is unit time and B is the block size. Table 2 shows the size of the block generated in a specific time in the vehicular network.

Table 2. Evaluation of the growth VANET blockchain network.

Message transaction	Per second	Per minute	Per hour	Per day	Per year
Tx	Tx*(B*1)	Tx*(B*60)	Tx*(B*60*60)	Tx*(B*60*60*24)	Tx*(B*60*60*24*365)
200	117.18 KB	6.87 MB	0.402 GB	9.66 GB	206.51 TB

500	292.96 KB	17.17 MB	1.006 GB	24.14 GB	516.27 TB
1000	585.93 KB	34.33 MB	2.012 GB	48.28 GB	1032.55 TB
1500	878.91 KB	51.49MB	3.017 GB	72.42 GB	1548.82 TB

Local blockchain is used due to which the size of the network can be controlled. However, scalability is still an issue in the network [26]. What happens when the proposed mechanism is desired to deploy in a large scale public vehicular network where the growth of vehicles cannot be controlled? Moreover, the PoW consensus mechanism is used in the scheme, which consumes extra resources of the network. Instead of PoW, edge computing should be used in the network to reduce the propagation delay. This edge computing is also helpful for the mining process in the network which consumes a huge amount of network resources. The use of edge computing is appropriate for resource constraint vehicular network and also helpful for well time message availability in the network due to its fastest mining power.

With the authentication of information of vehicular network events, it is important to authenticate the sender and forwarder of this information. The authentication is more critical with moving vehicles. As we know, the vehicular network is composed of different regions. Vehicles move continuously across these regions and lost their connectivity with previously visited regions. Because in every region another data-center is installed and there are fewer chances of registration of nodes with this. So, it becomes more difficult for moving vehicles to authenticate in real-time [29]. The authors proposed a system model in which volatile vehicles move from one data-center to another. Each data center consists of a specific service manager which is responsible to manage the vehicular fog service. The data of vehicular fog service is stored in fog and the hash of this data is stored in the blockchain. The service managers are also responsible for storing ledger with which the vehicles are authenticated. As the same ledger is present at each service manager database, the service manager of the different regions is now able to authenticate the vehicle easily. This will prominently reduce the time of authentication. Blockchain becomes the solution, which is more secure and trustable. The protocol used in the scenario is 801.11p and the packet size of the massage is 24 bytes. Massage is transmitted in the 2.137ms. Java run time environment is used for the measurement of the average time of the authentication is 0.596 and 1.473. The Interaction between Different modules of Architecture for authentication is shown in figure 8.

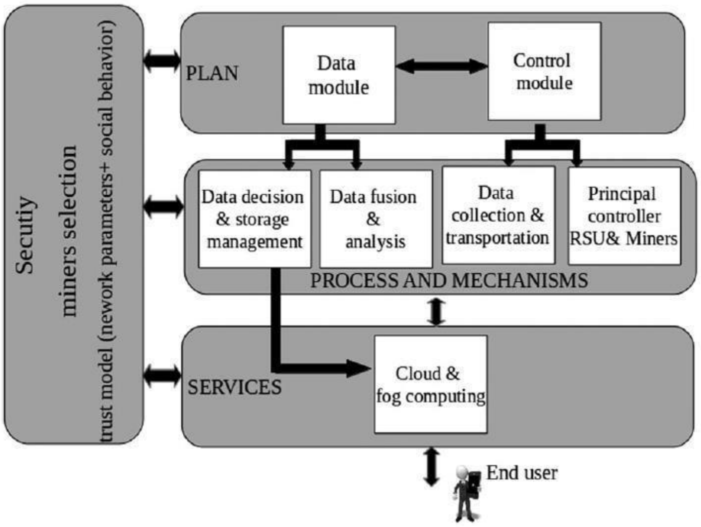
Secutiy
miners selection
trust model (nework parameters+ social behavior)
PLAN
Data module
Control module
Data decision & storage management
Data fusion & analysis
Data collection & transportation
Principal controller RSU& Miners
PROCESS AND MECHANISMS
SERVICES
Cloud & fog computing
End user

Figure 8. Interaction between Different modules of Architecture.

4. Conclusions

Blockchain operates without the involvement of a third party. The seller and buyer are directly connected without relying on any arbitrator. All the transactions are stored in the blockchain as proof. Once these transactions are stored, these transactions cannot be removed or altered. The major inferences that are drawn from this report are given below:

1. Blockchain is helpful to provide well time messages and sender authentication without taking a lot of time. In vehicular networks, the vehicles are mobile and moving continuously, therefore, they required rapid response for decision making. However, the task of authentication of sender and message is a time-consuming task for individuals, but in the vehicular network, it is not affordable to spend this amount of time for authentication. This may result in unwanted situations like accidents, wastage of time, resources, etc. The solution to this real-time response issue is provided by the blockchain. Blockchain uses built-in algorithms for authentication whose response time is in milliseconds. Therefore, by using blockchain technology in vehicular networks, the information and credentials of stakeholders (sender, receiver and other entities) can be processed and authenticated in no time for clients and stakeholders can focus on decision making without any uncertainty.
2. In the vehicular network, the cyber-attacks are common and due to which the privacy of users and participants can be compromised. Blockchain is a hack-proof protocol and it is one of the best security protocols than other protocols used in the industry. In this way, blockchain restricts attackers from identity theft and provide a secure and privacy preserved environment.

3. All the transactions are stored in the ledger which is accessible by each entity in the network. In this way, blockchain provides transparency about transactions in the network. Once the transaction is recorded in the public ledger, it cannot be removed or altered. In a vehicular network, the broadcasted message is considered as a transaction and once any entity spread or broadcast the message in the network. The message is verified by miners and its result (true or false) is stored as proof in the blockchain. In this way, the vehicles avoid broadcasting wrong information as it can be used against them in case of any dispute.
4. A little human error or uncertainty in a vehicular network can cause a lot of damage. As we know, blockchain operates automatically without human involvement. Moreover, it uses highly précised and calculated algorithms. Therefore, it eliminates errors and provides very precise and accurate calculations. In this way, blockchain is suitable for the vehicular environment in which vehicles are moving continuously.
5. Blockchain provides a cost-effective solution for vehicular and other networks as no third party is involved in the blockchain network. According to a study, the use of blockchain technology can help in saving 20 billion dollars a year [24].

References

[1] Guo, W., Zhang Y., Li L. The integration of CPS, CPSS, and ITS: A focus on data / W. Guo, Y. Zhang, L. Li // Tsinghua Science and Technology. – 2015. – № 20(4). – P. 327-335.

[2] Yuan, Y. Towards blockchain-based intelligent transportation systems / Y. Yuan, F.-Y. Wang // 19th International Conference on Intelligent Transportation Systems (ITSC). – 2016. – P. 2663-2668.

[3] Zhang, J. Data-driven intelligent transportation systems: A survey / J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, and C. Chen // IEEE Transactions on Intelligent Transportation Systems. – 2011. – № 12(4). – P. 1624-1639.

[4] Liu, X. "A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs / X. Liu, H. Huang, F. Xiao, Z. Ma, // IEEE Internet of Things Journal. – 2019. – № 7(5). – P. 4101-4112.

[5] Haber, S. How to time-stamp a digital document / S. Haber and W. S. Stornetta // in Conference on the Theory and Application of Cryptography. – 1990. – P. 437-455.

[6] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system / S . Nakamoto // Manubot. – 2019.

[7] Atlam, H.F. A Review of Blockchain in Internet of Things and AI / H.F. Atlam, M.A. Azad, A.G. Alzahrani, G. Wills // Big Data and Cognitive Computing. – 2020. – № 4(4). – P. 28.

[8] Zheng, Z. An overview of blockchain technology: Architecture, consensus, and future trends / Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, // " in 2017 IEEE international congress on big data (BigData congress). – 2017. – P. 557-564.

[9] Hu, W. "A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles / W. Hu, Y. Hu, W. Yao, H. Li // IEEE Access. – 2019. – № 7. – P. 139703-139711.

[10] Morkunas, V.J. How blockchain technologies impact your business model / V.J. Morkunas, J. Paschen, E. Boon // Business Horizons. – 2019. – № 62(3). – P. 295-306.

[11] Camacho, F. Emerging technologies and research challenges for intelligent transportation systems: 5G, HetNets, and SDN / F. Camacho, C. Cárdenas, D. Muñoz // International Journal on Interactive Design and Manufacturing (IJIDeM). – 2018. – № 12(1). – P. 317-335.

[12] Jeong, S. Component-Based Interactive Framework for Intelligent Transportation Cyber-Physical Systems / S. Jeong, Y. Baek, S. H. Son // Sensors. – 2020. – № 20(1). – P. 264.

[13] Hîrţan, L.-A. Blockchain-based reputation for intelligent transportation systems / L.-A. Hîrţan, C. Dobre, H. González-Vélez // Sensors. – 2020. – № 20(3). – 791.

[14] Alladi, T. Blockchain in smart grids: A review on different use cases / T. Alladi, V. Chamola, J.J. Rodrigues, S.A. Kozlov // Sensors. – 2019. – № 19(22). – P. 4862.

[15] Haddadou, N. A job market signaling scheme for incentive and trust management in vehicular ad hoc networks / N. Haddadou, A. Rachedi, Y. Ghamri-Doudane // IEEE transactions on vehicular technology. – 2014. – № 64(8). – P. 3657-3674.

[16] Din, S. Hierarchical architecture for 5g based software-defined intelligent transportation system / S. Din, A. Paul, A. Ahmad, S.H. Ahmed, G. Jeon, D.B. Rawat // in IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). – 2018. – P. 462-467.

[17] Garg, S. SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective / S. Garg, K. Kaur, G. Kaddoum, S.H. Ahmed, D.N.K. Jayakody // IEEE Transactions on Vehicular Technology. – 2019. – № 68(9). – P. 8421-8434.

[18] Shrestha, R. A new type of blockchain for secure message exchange in VANET / R. Shrestha, R. Bajracharya, A.P. Shrestha, S.Y. Nam // Digital communications and networks. – 2020. – № 6(2). – P. 177-186.

[19] Xie, L. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs / L. Xie, Y. Ding, H. Yang, X. Wang, // IEEE Access. – 2019. – № 7. – P. 56656-56666.

[20] Zheng, D. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs / D. Zheng, C. Jing, R. Guo, S. Gao, L. Wang // IEEE Access. – 2019. – № 7. – P. 117716-117726.

[21] Yao, Y. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services / Y. Yao, X. Chang, J. Mišić, V. B. Mišić, and L. Li // IEEE Internet of Things Journal. – 2019. – № 6(2). – P. 3775-3784.

[22] Lu, Z. "A privacy-preserving trust model based on blockchain for VANETs / Z. Lu, W. Liu, Q. Wang, G. Qu, Z. Liu // IEEE Access. – 2018. – № 6. – P. 45655-45664.

[23] Zhang, X. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network / X. Zhang and X. Chen // IEEE Access. – 2019. – № 7. – P. 58241-58254.

[24] Dorri, A. Blockchain: A distributed solution to automotive security and privacy / A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak // IEEE Communications Magazine. – 2017. – № 55(12). – P. 119-125.

[25] Garg, S. SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective / S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, D. N. K. Jayakody // IEEE Transactions on Vehicular Technology. – 2019. – № 68(9). – P. 8421-8434.

[26] Shrestha, R. A new type of blockchain for secure message exchange in VANET / R. Shrestha, R. Bajracharya, A. P. Shrestha, S. Y. Nam // Digital communications and networks. – 2020. – № 6(2). – P. 177-186.

[27] Xie, L. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs / L. Xie, Y. Ding, H. Yang, X. Wang // IEEE Access. – 2019. – № 7. – P. 56656-56666.

[28] Zheng, D. A traceable blockchain-based access authentication system with privacy preservation in VANETs / D. Zheng, C. Jing, R. Guo, S. Gao, L. Wang // IEEE Access.

– 2019. – № 7. – P. 117716-117726.

[29] Yao, Y. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services / Y. Yao, X. Chang, J. Mišić, V. B. Mišić, L. Li // IEEE Internet of Things Journal. – 2019. – № 6(2). – P. 3775-3784.

[30] Lu, Z. A privacy-preserving trust model based on blockchain for VANETs / Z. Lu, W. Liu, Q. Wang, G. Qu, Z. Liu // IEEE Access. – 2018. – № 6. – 45655-45664.

[31] Zhang, X. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network / X. Zhang, X. Chen // IEEE Access. – 2019. – № 7. – P. 58241-58254.

[32] Dorri, A. "Blockchain: A distributed solution to automotive security and privacy / A. Dorri, M. Steger, S. S. Kanhere, R. Jurdak // IEEE Communications Magazine. – 2017. – № 55(12). – P. 119-125.

[33] Awais Hassan, M. A secure message-passing framework for inter-vehicular communication using blockchain / M. Awais Hassan, U. Habiba, U. Ghani, M. Shoaib // International Journal of Distributed Sensor Networks. – 2019. – № 15(2). – P. 15501477-19829677.

Abbreviations

ITS	Intelligent Transportation	V2V	Vehicle to vehicle
V2I	Vehicle to Infrastructure	RSU	Roadside Unit
WSN	Wireless Sensor Network	IoT	Internet of Things
VANETs	Vehicular Ad-hoc Networks	CA	Certificate Authority
SDN	software Define Network	CMT	Chronological Merkle Tree
PoW	Proof of Work	PoS	Proof of Stake
PoA	Proof of Authority	P2P	peer to peer