Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

APPLICATION OF BLOCKCHAIN IN INTERNET OF VEHICLES TOWARDS IMPROVEMENT OF SMART TRANSPORTATION SYSTEMS - A CONVERGENCE SURVEY

[1]GIRIJA .V
Research Scholar, Dr. MGR Educational and Research Institute,
Deemed to be University, Chennai-95,
Tamil Nadu, India.

[2]Dr VICTO SUDHA GEORGE G,
Guide -Computer Science and Engineering,
Dr. MGR Educational and Research Institute,
Deemed to be University, Chennai-95,
Tamil Nadu, India.

Abstract - With the recent advancements achieved towards the field of Internet, the adaptation of the smart transportation system with the Internet of Vehicles (IoV) are evolving as a paradigm. The ascent in the transportation concept made IoV an important area of research because of its application in the smart city, smart parking, product delivery, and mobility model. In IoV, vehicles are given human ability to communicate with each other to avoid untoward problems. In regard to possibility of such vehicular networks with security, privacy, and trustworthiness, blockchain ledger technology could be used. This makes the adaptation of the blockchain in IoV a participatory research.In this research, we present a convergence survey of recent research works related to the application of the blockchain in IoV for the betterment of the smart transportation system. Even with the transportation system as key enabler, the priority is also given to other existing networking model which incorporates the blockchain. The survey paradigm is formulated with respect to the application of blockchain properties such as authentication, sharing, trust management, security, privacy preserving, integrated and miscellaneous applications. Effort is also made to investigate the key challenges in the existing literatures. Furthermore, challenges related to the blockchain application on smart transportation system are discussed with recommendations in the research direction.
Keywords- Intelligent Transportation System, Blockchain, Vehicular Networks, Road Side Unit, Incentive.

I. INTRODUCTION

In recent years, with the initial development and distributed advancement of electronics in the field of the transportation most of the regular embedded systems are deployed with a change over named as smart transportation system. The advantage of smart system is that it is connected over the internet technologies which provide a bridge between the connecting devices and the physical world [1]. In regard to other application oriented environment, everything is changed to smart with its arrival. One

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

piece of such entity is the Intelligent transportation system. The adaptation of the Intelligence in the transportation infrastructure is suitable for most of the working environments. Intelligent transportation systems (ITS) provide accessibility in both the data access and the travel experience in most of the use cases. To make its more advantageous, in the recent trend ledger technology is also used with the smart transportation system to make it more secure. One among them is the blockchain, Blockchain is initially intended as a distributed ledger of the bitcoin [1]. The key solution of blockchain is that it allows transaction based establishment of trust among the entities which is very of the essence in the field of the transportation system. Fig. 1 depicts the illustration and usage of the blockchain in intelligent transportation unit. The transportation unit embedded in any use case comprise of vehicle unit, Road side unit and control unit. The vehicle unit is the mobile block which collects information and send it to blockchain for mechanism which will make the decision and send back the tracking or any information to the vehicle via the RSU. Such technologies are being adapted in most of the recent vehicular technologies which gives the ability of being autonomous or semi autonomous stature, thus creating a potentiality for the field of Intelligent Transportation System.. In regard to existing paradigm of ITS, Internet of Vehicles is introduced which seems of same behaviour in more connected manner with the help of Internet of Things (IOT). Such technologies provide easier communication between the vehicles and provide monitoring, and sensing ability for the environment. Hence, the IoV ecosystem is considered nowadays as an extended component of ITS [2-10].

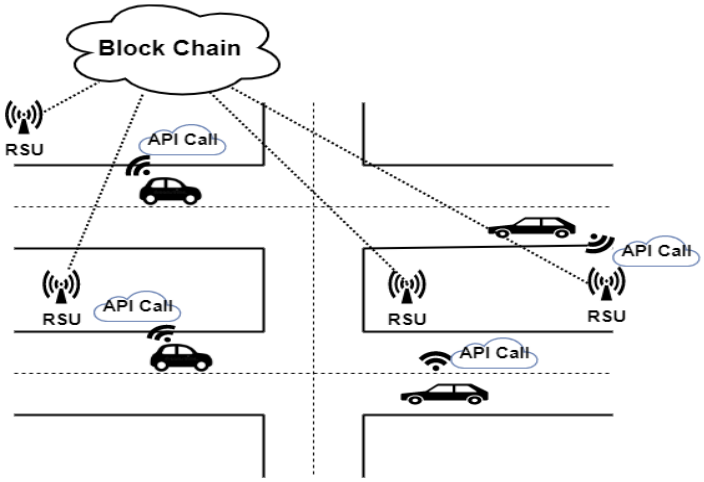

Fig. 1 Intelligent Transportation System

Such abundant use of the vehicular application in the fully automated world increase the usage of the smart vehicular services. The problem withe the development is that it increased the data to be handled within the ITS environment. The difficulties among

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

such connected environment is to achieve high mobility, reduced latency, complexity in the context, and heterogeneity behaviour. Moreover, the problem with attaining compatibility among all the vehicle units and interoperability with trust factors among the entities for different service providers. This makes the need of data exchange in the IoV to be a more effective distributive adaptive decentralized with high flexibility and scalability. Thereby, the full potential of the IoV in the ITS can be achieved. In addition to that, the advantage of being distributive it is evident that ITS platforms are vulnerable to intrusions because of the internet presence which require essential suppliant for ensuring the privacy, security, and trust. .Consequently, by adapting the blockchain technology along with modern AI or machine learning techniques, and fog computing, the impact of the ITS can be improved in a reliant manner.

A. Why Blockchain?

The reason for the connection of the blockchain in ITS is deliberated in this section. To know the usage of the blockchain, the findings of IOT is essential. Internet of Things is nothing but a system unit which collects the information from the physical devices, process it and to make some decision making. The mere introduction of IOT started from the 19th century, where computer is made to control individual things. The example for Internet of Things are defibrillator device, dog neck chip, smart sensors, etc. The added advantage of IoT device is that it is never supposed to be a standalone device unlike the device in vehicle which reads the tire pressure, or other vehicle conditions. Each of the device in the IOT have an unique address from which the communication is made possible which co-relates the usage of the blockchain with it. In general, blockchain is a network of incorruptible digital ledger of information exchange. It does not only store the information in addition exercise some consensus mechanism on the financial transaction. One among the blockchain technology is bitcoin, which have the ability to store anything with it which seems relevant for the ITS. In a common man perspective, blockchain is nothing more than a giant collection of data records with resilient to be erased, deleted or edited. As there exist no central computer or device on which the entire chain are saved making it a distributed and decentralized network. Rather, each block nodes involved in centralized transactions keeps a copy of the transactions and the data of the previous are saved in the new blocks contiguously. Each cycles add more data to the chain, which makes it ever growing. Some of the major elements in the blockchain are Transactions, and Blocks. Transaction is a trivial action initiated by the nodes associated to the blockchain whereas blocks are nothing more than recorded transactions. The recorded transactions are arranged in sequence and are in their original form. In addition to the stored transaction, the timestamp associated to the transaction is also added to each blocks.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

B. Recurrence of Blockchain Assisted Internet of Vehicles

Even with the application of blockchain in numerous area starting from the smart contracts, cryptocurrency, music, fraud detection, real state and internet of things, the research on the application of the ITS is still blooming. With its advantage proved over the cryptocurrency transactions, many ITS systems are looking for the usage of the blockchain in the IoV as well as ITS. Such extreme are proven to future proof for the burgeoning yet risk prone systems. A recent idea that has to do with our newly adopted technology: Internet-of-Vehicles is being powered by blockchain for the smart transportation system. Spending on the IoT market keeps growing and it is predicted to reach about $1 Trillion mark in few years. Blockchain-Internet-of-Vehicles convergence have the possibility to render the predominant execution to monitor the billions of smart-devices coming online histories over the coming years by making use of its incorruptible permanent ledger. Fig. 2 illustrates the recurrence of the blockchain and internet of vehicles in a combined working environment. The working starts from the vehicle from where the collected data is send local server via RSU. The server initiates the blockchain process where smart contracts withhold the data as transaction and send to the data via consensus mechanism to the database associated to it. The chain blocks will resettle information and send it to the IoV which may include tracking information, location information etc which makes the safe travel in traffic scenarios or even supply chain logistics.

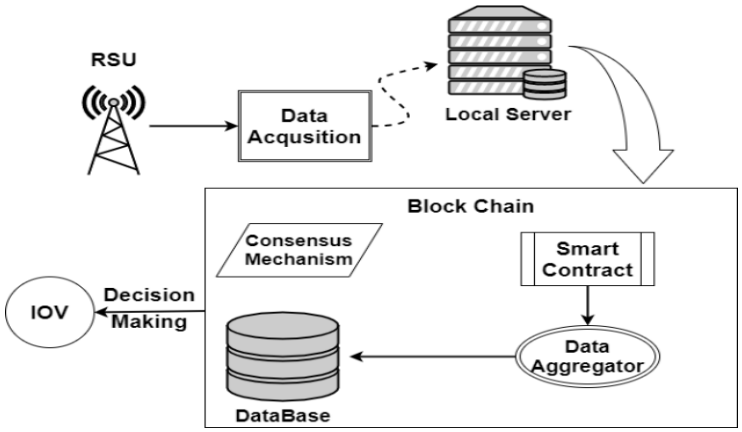

Fig. 2 Recurrence of Blockchain and Internet of Vehicles

C. Focused Model

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

The model type in blockchain based intelligent transportation unit are of two types, They are centralized model and decentralized model. The decentralized model is preferred over the centralized approach because of its substantial reduction in the installation cost, and its availability of largely collected data organization unit.

II. SURVEY FORMULATION

The mere existence of the blockchain is found beneficiary in the field of the transportation system in the recent years and is found to be one of the abundant framework introduced paradigm. In this section, the intelligent transportation system ecosystem from the recent works are formulated with its description for finding the introductory advantages, disadvantages, issues and recommendation in the field. The contribution of the survey is formulated in a paradigm pattern considering the importance of the blockchain in specific service area. They considered opinionated regarding are depicted in Fig.3. The structure of the survey is divided into six parts each part analyzing the relevant literature. The survey is performed in such a way that in addition to the consideration of the recent works, they research method associated with it were also briefed.

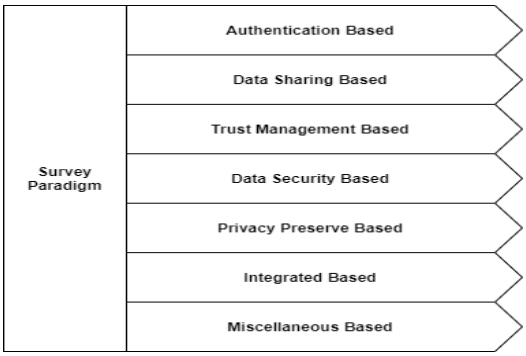

Fig. 3 Proposed Survey Paradigm

From the survey paradigm depicted in figure 3, it is evident that the survey is formulated centered on the Internet of Vehicle application scenario for the transportation system.

A. vis-à-vis Data Authentication

The consideration of the blockchain technology in the vehicular network in regard to the internet of things seems to provide better authentication mechanism since the data shared among the vehicles to the blockchain for the contract consensus mechanism via cloud. In most of the researches considered on the direction of the authentication, techniques such as cryptography, pseudonyms etc were used for collective

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

authentication of the data employed over the application oriented environment [42]. To address the challenges related to the data authentication schemes, Xiaomin Du [11] et al. developed a blockchain adapted smart transportation unit with the ability to overcome the authentication problem with the help of the decision-making trial and evaluation laboratory scheme. They used fuzzy set theory approach for the data aggregation to provide useful information to the framework. They also used the linguistic variable in hindrance for the authentication. In contrary to the aforementioned fuzzy related authentication scheme, the system with the focus on reduce energy consumption, increased efficiency, vehicle related accidents were proposed by Zisang Xu et al [12]. The problem of the mutual authentication which is followed in the most of the existing research work was overcome with the help of the key agreement protocol. They were managed to establish cross trust authority among the internet of vehicles which was found helpful in a huddled contract epitome of the blockchain. They were able to make the authentication by sending multiple messages among the party for the affirmation of the confirmed party. Another protocol based implementation was performed by Anil Kumar Sutrala et al [13] for the better authentication for the internet of vehicles. They employed cluster based broadcast scheme for the message transfer between the roadside unit and vehicle unit, the authentication performed on the blockchain was well protected because of the multiple layer authentication scheme. In addition to the authentication, their proposal was resilient against most of the attacks ranging from middle-in-the-middle attack, privileged-insider attack etc. As opposed to the authentication schemes derived in the most of the research, Merzougui [14] concentrated on a different elliptic curve cryptography based model of Internet of Vehicle environment to achieve the confidentiality of the data. The authors were able to achieve robust protection against DDoS attack, reply attack.

B. vis-à-vis Data Sharing

The reason for the consideration of the data sharing application as one of the survey paradigm is because of its ability to provide a cooperative resource sharing platform for most of the stationary as well as the running vehicles. The data sharing among the vehicles in the environment aid in the computation overhead, cost and other entity sharing as well. Even though the data sharing is a valid option in the IoV, it is limited with trust factor among the vehicles as well as the trustworthiness of the block chain. If the data sharing among the vehicles are proper, it increases the access control of the system oriented environment [43]. One of the recent research for information sharing in the blockchain based IoV was developed by Sanjeev Kumar et al [15]. They adopted a decentralized network with the data immutability property, in addition to that authentication was also validated with the help of the protocol. The sharing was more successful in their approach because of the division of the events in the application use case namely, registration phase, event detection phase, and block update phase. The

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

scalability in exchanging the resource was found better in their use case. With being limited terminal resources, the sharing system proposed by Qikun et al [16] was able to achieve better resource sharing among the RSU to the blockchain unit. The information was shared only after negotiating a group key among the members of the IoV. The key agreement made sure that no illegal members are connected to it. Moreover, the privacy of the data was well protected in their system.

Lei Zhang et al [17] implemented a secure data sharing system for IoV with the challenges of sharing bundle vehicular message with the help of the block chain. They were able to achieve a well secured data sharing unit because of the divisive feature they employed for the information sharing. Initially, the regions among the vehicular environment is divided into multiple regions. To each region, a parent and auxillary blockchain were deployed to store the messages from the information was shared to other parent/auxillary blockchain regions. They were also able to find the true identity of fake users who are trying to access the shared information. In [18], Anik Islam et al excelled data sharing scheme for the the data collection in UAV environment based transportation unit. The data sharing was performed in the blockchain in consent with the validators. The availability of the communication channel among the units made sure the information exchange without any error.

C. vis-à-vis Trust Management

Trust management application is considered as one of the vital factor in the field of vehicular transportation unit because trust makes the system less vulnerable more suitable for the resource sharing [44]. When it comes to the trust management of the vehicles in the IoV, it is mandatory for the reputation of the vehicles to be incorporated only then sharing record to the blockchain will be well maintained. The trust management make sure whether a vehicle is a connected member or not, even it also validated the consensus mechanism of the blockchain. This section deliberates the research work related to the trust management in the field of IoV. Basudeb Bera et al [19] developed an IoT enabled blockchain scheme for the trust management among the drones in their vehicular unit with the help of the ripple protocol. The blockchain receives the collective information from the drones and were send to station server where the transaction to block conversion is made and was checked for alteration. If any alteration was on the received block, that particular drone is marked with no trust thereby managing the trust among all other drones. Like wise in [20], authors proposed an novel model for managing trust worthiness in the IoT specific environment with the help of validation protocol. The trust of the network was mandated with the help of priority and was found less time critical. The prioritized members were considered trustworthy in their approach which was well advantageous over most of the existing random based or fee based trusting mechanisms.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

Rajesh Gupta et al [21] automated a blockchain based trusting mechanism scheme for smart transportation system with the the help of threat classification algorithm. The human interference of this system was found very minimal even with hundred of GBs of data collected from the surrounding environment. They made sure every viable transaction of the automated vehicle with utmost certainty which enabled the trusting scheme more relevant for all the participating members starting from the blockchain nodes, automated vehicles as well as road side units. In regard to trustworthiness, Xingzhi Wang et al [22] developed an trust driven approach for vehicle product service system. The trust issue in IoV of unknown members in the vehicular unit from scam, and frauds were overcome by employing the collection process. They collected usefull information about each vehicle and consolidated with the help of the blockchain whether it is legal or illegal and only then it is allowed inside the working environment.

D. vis-à-vis Data Security

With the increase in the application of the IoV, the vehicles getting into acceptance of the unit is also increased which thereby increase the amount of data to shared among the network to make the system more successful and enhanced. Data security among such network is indispensable factor to employed while utilizing because of the placement of the vehicular or road side unit nodes in a distributive manner which makes them vulnerable to intrusion, or any type of privacy attacks. Moreover, the operating issue related to multiple service providers also makes the regulation of the data with security a trivial task [45]. Since data security is non-negotiable as a property most of the intelligent transportation unit gives priority for the security over most other use case of the properties. In [23], authors prioritized a access guarantee scheme for the protection of the data in the vehicular network to adapt to a well secured working environment. The data efficient in relation to the security was maintained in their technique even with the distributive providers by sync process. The smart contract itself was developed with the access scheme which made sure the data is not susceptible to attack.

Hongeng Zhu et al [24] on the other hand developed two novel lightweight protocol for the security of the data transfer. Their method was found efficient because of the adaptation of the semi quantum reflected scheme. The state of each node in this use case used quantum state for any trigger of actions. The delay was also found in quantum which makes sure the quantum bits received among the providers were safe from attacks. In [25], Chuka Oham et al proposed a smart vehicle paradigm for security the information with the help of the challenge-response data. The response scheme is adapted in the vehicle unit as well as the provider unit. The system first validate the communication using the challenge only then the information are transferred to the provider which ensures the authenticity of the data. Another approach depicted in [26]

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

showcased the adaptability of the providers in ensuring the data security using the cooperative data transfer schemes.

E. vis-à-vis Privacy Preserving

Privacy preserving application is one of the well engraved property in the IoV as well as the smart transportation unit because the preserving architecture make sure the information is withheld on the provider end. The usage of the blockchain for the data aggregation will make sure the the information is preserved well without any subjection to attacks, or delegation. However, the data exchange among the providers and the vehicle units makes it a fiddling process to withhold [46]. The privacy preserving transportation unit makes sure the data are immutable even if its unused. In [27], Debio et al demonstrated the importance of the privacy preserving IoV network with the help of the recovable message based authentication scheme. The revocation in this method was found efficient because of the pairing free signature associated with each vehicle or road side unit. They also exploited the importance of the trust management, with respect to the consistency in the information transfer. Towards the privacy preserving scheme, Zhitao Guan et al [28] proposed an energy efficient trading scheme for the IoT. The problem conjoined with the number of entities in the network for every successful transaction in the blockchain form diversified course of action were overcome in his method with the help of blockchain based energy trading scheme. They were also able to maintain scalability without affecting the credibility of the system.

In relation to scalability, Hakima Khelifi et al [29] developed a named data networking model with the ability to preserve the information with the help of reputation based blockchain mechanism. The reputation scheme aids in the data forwarding plane as well as content caching plane.On the other hand, Sushil Kumar Singh et al [30] proposed an privacy preserving backed by artificial intelligence. The method was called divergence method because of the consideration of the AI. They aided in all aspect of the blockchain consensus. The computational cost and energy cost in this method was found minimal compared to the existing researches of same direction. In regard to the Vehicular Social Networks, Yuwen Pu et al [31] proposed an efficient privacy preserving scheme based on the pseudo mechanism. The anonymization of the vehicle in this method was performed with the help of incentive punishment mechanism. Such report encouraged in preserving the privacy of the data without any tolerance.

F. vis-à-vis Integrated

In this section, Integrated means the possibility of the challenges in integrating the blockchain and Io Scenario on any application oriented environment. When the integration is made for the well fare of the smart transportation unit, the proceedings are mandate in four directions. They are security and privacy, performance, Optimized

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

consensus, and incentive mechanisms. The integration should be made with the capability to handle large number of data with trustworthiness, adaptability to the dynamic working environment with high latency [47]. Ismaila kamil et al [32] proposed an integrated IoV intended for the data authentication as well as the privacy preservation. They enhanced the performance of the system by combining blockchain and neuro-fuzzy algorithms. The DoS attack related to fake authentication from multiple vehicle to RSU was overcome in their model. Moreover any invalid nodes were restricted from authentication preventing the privacy of the information shared between the system units. The integration of IoT and blockchain in the transport monitoring system was employed by Jingwen Zhang et al [33]. They relied on real time data collected from physical car such as speed, temperature, GPS location, image etc for the management. The collected information was given to blockchain for consensus mechanism which provide the proper pathway for the transport. They effectively managed to outsmart most of the existing system because of the consideration of relevant real time system. The system was adapted for the transport of the cultural relics from the museum of the western harn dynasty. Another integration mechanism was adapted by Elnaz Irannezhad et al [34] for the logistics and freight transportation. They employed synchronization, integration and encryption scheme for overcoming the disputes over conventional IoV. The conventional database usage made their decentralized more adaptable to any system specific environment. A methodology of as such was found in [35,36]. In [37], authors et al. developed an integrated system unit for IoV with the ability to vulnerable network latency without any compromise in the security of the data received or for the data responded over the request on the mobile vehicles.

G. vis-à-vis Miscellaneous

In the miscellaneous application oriented survey paradigm, the literature which depicted the usage of the modern day technologies such as artificial intelligence, machine learning, optimization algorithm as assistance to the smart transportation system are deliberated. The capability of the automatic learning in the IoV will provide new scopes and aspects for the application scenarios [48]. Lijuin Sun et al [38] developed an miscellaneous model centered on reputation based crowd-sourcing blockchain for IoV. The advantage of their model was its ability to provide timely feedback to user with respect to the transportation information. The trustworthiness of the malicious and normal nodes in the system unit was differentiated using the RC-chain built on the blockchain platform. Moreover, they used reputation model which calculates the reputation values of the node and thereby preserving the privacy of the data. The choice of miscellaneous inclusion is because of the existence of such literature itself. In [39], Saurabh Singh et al deliberated the importance in acceptance of new age technologies in the IoV as well as the smart transportation unit. They presented in detail about the

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

convergence of the blockchain and artificial intelligence which increases the impact of the blockchain system in the smart cities.

Ahmed et al [40] proposed an quantum inspired blockchain methodology for the smart city using cryptologic algorithms. This research is included in the miscellaneous paradigm because of the authentication scheme adapted here with the optimization algorithms. They concentrated on the data transfer among the IoT devices with high efficacy and resilient attack issues. Another miscellaneous tryout was found in the research of Suaib Akhter et al [41] with multi level blockchain framework for the vehicular area network. They aided in the authentication of the vehicle in the environment with the help of the global authentication center and local authentication center which provided easy handover of information between the internal cluster of the vehicle. They tried the implementation as an simulation approach and were able to achieve better performance in terms of throughput etc.

III. INTRODUCTORY FINDINGS OF SURVEY

In this section, the research findings of the survey formulated in section II is deliberated.

TABLE I - SURVEY FINDINGS TABLE

Research Paper	Blockchain Nodes	Approach	Findings
[11]	RSU	Incentive fuzzy set theory based	Theoretical Approach
[12]	Vehicle	Key Agreement Protocol	Simulation Approach (ProVerif Tool)
[13]	RSU, Vehicle	Voting based Practical Byzantine Fault Tolerance	Computational Overhead is high, Simulation approach
[14]	RSU	Elliptic Curve Cryptography	AVISPA Tool oracle model.
[15]	RSU, Vehicle	Central Authority based resource sharing scheme	VANET Simulation. Enhanced scalability
[16]	RSU	Asymmetric Group Key agreement protocol	Simulation Approach. Eliminates the computation task in resource-constrained environment
[17]	Vehicle	Punish - Reward Mechanism	Theoretical Approach. Auxillary blockchain based identity management.
[18]	Unmanned Aerial Vehicle	BHEALTH Scheme	Practical Approach. The adaptation is intended only for the data

ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

			collection no decision making
[19]	Unmanned Aerial Vehicles	Ripple Protocol Consensus Algorithm	Practical approach. Well Secured over most of the attacks.
[20]	Internet of Things Network	Transaction based validation protcol	Simulation Approach. Energy Efficient
[21]	Vehicle	Threat classification algorithm	Simulation approach. Resilient to intrusion attacks
[22]	Vehicle	PSS Framework	Connected Real time service mechanism. Provenance on each stage of transaction
[23]	Vehicle, RSA	Blockchain based special vehicle priority access guarantee scheme	Simulation approach. Tested on Ethereum clients
[24]	Vehicle, RSA	Semi Quantum Approach	Simulation approach. Well secured data transfer over every single round of completion
[25]	Vehicle	Challenge-Response data Exchange scheme	Simulation Approach. Possibility to identify compromise in-vehicle
[26]	Vehicle	Cooperative Scheme	Simulation Approach NS2
[27]	Vehicle	VSI-bciov Scheme	Simulation approach. Provide better counter measure over different types of attack
[28]	Internet of Things Network	Energy Trading Scheme	Simulation approach. Showed improved efficiency with low processing time
[29]	Vehicle	Reputation based scheme	Simulation approach. Limited resource for invalid malicious node in the network
[30]	RSU	Intelligence based scheme	Simulation approach. Potential improvement on centralization issues
[31]	Vehicle, RSU	Pseudonym Mechanism based scheme	Simulation approach. Prevent malicious entities from data manipulation
[32]	Vehicle	Elliptic Curve Cryptography and Hash function	Simulation approach. SUMO. The computation overhead is very less
[33]	Vehicle	Distributive management scheme	Real time system. Explicit benefit over untoward incidents.
[34]	Flight Model	Mitigation Scheme	Simulation approach. Tracking and traceability is well maintained.
[37]	Vehicle	Minor Node Selection algorithm	Simulation approach. Mobility is considered a key factor for

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

			networking

IV. ANALYSIS

In Table II, the analysis of the surveyed research works in terms of the working environment, and the computational cost of the blockchain assistance in the processing is listed out. The research indicates that most of the use case in the works are connected to simulation approach rather than the practical approach. The promising results are obtained in the existing research works in terms of the computation over head. Most of the systems resulted in reduced computation cost and the cost is directly proportional to the size of the transaction block associated to it. These show much reason why we need to strongly make our device more resilient in connected with the computation cost without leaving one behind privacy, security etc. The number of IoV units is also a factor of the security which is expected to be vulnerable over the years via different forms of attack.

TABLE II- Analysis of the surveyed research

Research Paper	Application Environment	Computational Cost
[11]	Urban Greening Layout	Electronic management
[12]	Road Environment	Increases with respect to VN-RSU
[13]	Smart City	Increases with number of transactions per block
[14]	Traffic Road Environment	Increases with the number of blocks
[15]	Road Environment	Increases in relation to the phase: registration/update
[16]	Smart City	Increases with respect to number of group in IoV
[17]	Traffic Road Environment	Increases with signers (regions)
[18]	Healthcare Environment	Increases with validation time of the Units
[19]	Drone Flying Environment	Increases with respect to ground station server
[20]	Networking Environment	Increased with respect to the transaction of the new block
[21]	Smart City Environment	Increases with respect to the number of blocks mined for the consensus mechanism
[22]	Product Delivery Environment	Increased with respect to stage of request/result call from data analytic unit
[23]	Traffic Environment	Increase with the scheduling time
[24]	Urban Greening Layout	Increase with the preparation time of each

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

		node in the IoV
[25]	Smart City Environment	Increase with respect to the time taken for the validation of challenge
[26]	Traffic Environment	Increase with respect to the validation time of the electronic signature
[27]	Smart Parking System	Increase with respect to the time of smart contract transaction
[28]	Network Environment	Increase with respect to the transaction matching time
[29]	Road Environment	Increase with respect to the content associated to it.
[30]	Traffic Road Environment	Increase with respect to the track data usage
[31]	Smart City	Increase with respect to return data

TABLE III - ANALYSIS TABLE

Research Paper	Application Environment	Computational Cost
[31]	Smart City	Increase with respect to return data
[32]	Urban Mobility Model	Increase with respect to authentication transactions
[33]	Traffic Environment	Increase with respect to the data transfer
[34]	Product Delivery Environment	Increase with respect to pilot data in the use case specification
[37]	Smart City Environment	Increase with respect to request/response time

V. TERM ACCEPTANCE

In this section, the issues found on the survey formulation are depicted. In most of the existing system, the systematic mapping are only theoretical without any real time application system. Moreover, not all the possible attributes in the field of intrusion is considered. It is very important to understand the knowledge of the blockchain and IoT model for aggregating the smart transportation unit. The research irregularities are mostly associated with the methodology that perceive only the research gaps in the block chain. The findings related to the IoV system model should also considered afresh for betterment of the ITS. In regard to containing the security threats of the blockchain technology, cryptographic algorithm can be employed to prevent the privacy and data leakage for each transactions to and from each vehicle, RSU or any connecting device and also by setting permissions to each device using fuzzy algorithms. Hence, the

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

objective from the survey formulation is to search and analyse similar researches to the technical aspects of blockchain technology and more importantly how it can be utilized in securing IoT systems, we decided to drop the single term blockchain. It is believed that by making use of the search string blockchain and IoV, most of the research materials that considers the working perspective on blockchain are brought forward.

V. CONCLUSIONS

In this research, the important characteristics challenging the properties of the Intelligent transportation system such as data authentication, sharing, trust management, security, privacy preserving, integrated and miscellaneous are considered as a survey paradigm and are dictated with findings over the existing literature deliberating their importance, issues and recommendations. The usage of the blockchain application in the smart transportation system is evident from the comparative analysis over the existing system which for tel the efficiency of the blockchain technology in the ITS. The usage of the blockchain consensus mechanism either with incentive or non-incentive mechanism for the Internet of Vehicle model showed different improvements in assorted research direction. It is concluded that the blockchain adaptability with safety mechanism in every possible level of the transportation system is the viable direction which grants a well optimal ITS. In regard to the blockchain, key based encrypted and decryption standards can be adopted to mitigate the data from the aggregation unit or even for viable control data collection. The standing as research findings are in the area of degree of information retrieval, security of the data, tracking technique, data synchronization and data management.

Acknowledgment
This survey is acknowledged and made possible with the research works deliberated in the reference section. The effort of the researchers in the direction of the Intelligent transportation system using blockchain technology and Internet of Things technology is applauded from authors side from which the recommendations are made possible for our future direction in the field of this research. We wish to acknowledge all other Intelligent Transportation System based literature contributors for developing and maintaining this research to be in this extreme.

REFERENCES

[1]Leo Mendiboure, Mohamed Aymen Chalouf, Francine Krief, “Survey on blockchain-based applications in internet of vehicles”, Computers and Electrical Engineering, vol. 84, 2020.

[2]J. Ni, X. Lin, and X. S. Shen, “Toward edge-assisted internet of things: from security and efficiency perspectives,” IEEE Network, vol. 33, no. 2, pp. 50–57, 2019.

ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

[3]A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, “Artificial intelligence-driven mechanism for edge computing-based industrial applications,” IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4235–4243, 2019.

[4]W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, “Edge computing: A survey,” Future Generation Computer Systems, vol. 97, pp. 219–235, 2019.

[5]F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, “Towards edgebased deep learning in industrial internet of things,” IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4329–4341, 2020.

[6]F. Li, K.-Y. Lam, X. Li, Z. Sheng, J. Hua, and L. Wang, “Advances and emerging challenges in cognitive internet-of-things,” IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5489–5496, 2019.

[7]H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, Cyber-physical systems: foundations, principles and applications. Academic Press Elsevier, 2017.

[8] H. Ji, O. Alfarraj, and A. Tolba, “Artificial intelligence-empowered edge of vehicles: Architecture, enabling technologies, and applications,” IEEE Access, vol. 8, pp. 61 020–61 034, 2020.

[9] J. Zhang and K. B. Letaief, “Mobile edge intelligence and computing for the internet of vehicles,” Proceedings of the IEEE, vol. 108, no. 2, pp. 246–261, 2019.

[10] Z. Ning, J. Huang, X. Wang, J. J. Rodrigues, and L. Guo, “Mobile edge computing-enabled internet of vehicles: Toward energy-efficient scheduling,” IEEE Network, vol. 33, no. 5, pp. 198–205, 2019.

[11] Xiaomin Du, Yang Gao, Chia-Huei Wu, Rong Wang, and Datian Bi, “Blockchain-Based Intelligent Transportation: A Sustainable GCU Application System”, Journal of Advanced Transportation, vol. 2020, 2020.

[12] Zisang Xu, Wei Liang, Kuan-Ching Li, Jianbo Xu, HaiJin, “A blockchain-based Roadside Unit-assisted authentication and key agreement protocol for Internet of Vehicles”, Journal of Parallel and Distributed Computing, vol. 149, pp. 29-39, 2021.

[13] Palak Bagga, Anil Kumar Sutrala, Ashok Kumar Das, Pandi Vijayakumar, “Blockchain-based batch authentication protocol for Internet of Vehicles”, Journal of Systems Architecture, vol. 113, 2021.

[14] Merzougui Salah Eddine, Mohamed Amine Ferrag, Othmane Friha, Leandros Maglaras, “EASBF: An efficient authentication scheme over block chain for fog computing-enabled internet of vehicles”, Journal of Information Security and Applications, vol. 59, Jun 2021.

ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

[15] Sanjeev Kumar Dwivedi, Ruhul Ami , Satyanarayana Vollala, Rashmi Chaudhry, “Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities”, Computers and Electrical Engineering, vol. 86, 2020.

[16] Qikun Zhanga, Yongjiao Li , Ruifang Wanga, Jianyong Li , Yong Ganb, Yanhua Zhanga, Xiao Yuc, “Blockchain-based asymmetric group key agreement protocol for internet of vehicles”, Computers and Electrical Engineering, vol. 86, 2020.

[17] Lei Zhang , Mingxing Luo , Jiangtao Li , Man Ho Au , Kim-Kwang Raymond Choo , Tong Chen , Shengwei Tian, “Blockchain based secure data sharing system for Internet of vehicles: A position paper”, Vehicular Communications, vol. 16, pp. 85-93, 2019.

[18] Anik Islam, Soo Young Shin, “A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things”, Computers and Electrical Engineering, vol. 84, 2020.

[19] Basudeb Bera , Durbadal Chattaraj , Ashok Kumar Das, “Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment”, Computer Communications, vol. 153, pp. 229-249, 2020.

[20] a. S. M. Sanwar Hosen , Saurabh Singh , Pradip Kumar Sharma , Uttam Ghosh , Jin Wang , In-Ho Ra And Gi Hwan Cho, “Blockchain-based Transaction Validation Protocol for a Secure Distributed IoT Network”, IEEE Access , vol. 8, pp. 117266 - 117277, 2020.

[21] Rajesh Guptaa, Sudeep Tanwa, Neeraj Kumar b, Sudhanshu Tyagi, “Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review”, Computers and Electrical Engineering, vol. 86, 2020.

[22] XingzhiWang, YuchenWang, AngLiu, “Trust-Driven Vehicle Product-Service System: A Blockchain Approach”, Procedia CIRP, vol. 93, pp. 593-598, 2020.

[23] Yue Wang , Jiguo Yu , Biwei Yan, Guijuan Wang , Zhiguang Shan, “BSV-PAGS: Blockchain-based special vehicles priority access guarantee Scheme”, Computer Communications, vol. 161, pp. 28-40, 2020.

[24] Hongfeng Zhua, Xueying Wanga, Chien-Ming Chenb, Saru Kumari, “Two novel semi-quantum-reflection protocols applied in connected vehicle systems with blockchain”, Computers and Electrical Engineering, vol. 86, 2020.

[25] Chuka Oham , Regio A. Michelin , Raja Jurdak , Salil S. Kanhere , Sanjay Jha, “B-FERL: Blockchain based framework for securing smart vehicles”, Information Processing and Management, vol. 58, 2021.

[26] Vittorio Astaritaa, Vincenzo Pasquale Giofr , Giuseppe Guidoa and Alessandro Vitalea, “The use of a Blockchain-based System in Traffic Operations to promote

ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

Cooperation among Connected Vehicles", Procedia Computer Science, vol. 117, pp. 220-226, 2020.

[27] Debiao He, Weizhi Meng, "Introduction to the special section on blockchain techniques for the internet of vehicles security (VSI-bciov)", Computers & Electrical Engineering, vol. 87, 2020.

[28] Zhitao Guan, Xin Lu , Naiyu Wang, Jun Wu , Xiaojiang Du , Mohsen Guizani, "Towards secure and efficient energy trading in IIoT-enabled energy internet: A blockchain approach", Future Generation Computer Systems, vol. 110, 2019.

[29] Hakima Khelifia, Senlin Luoa, Boubakr Nour , Hassine Mounglac,Syed Hassan Ahmede, Mohsen Guizani , "A blockchain-based architecture for secure vehicular Named Data Networks", Computers and Electrical Engineering, vol. 86, 2020.

[30] Sushil Kumar Singh, Shailendra Rathore, Jong Hyuk Park, "BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence", Future Generation Computer Systems, vol. 110, pp. 721-743, 2020.

[31] YuwenPu, TaoXiang, ChunqiangHu, ArwaAlrawai, HongyangYan, "An efficient blockchain-based privacy preserving scheme for vehicular social networks", Information Sciences, vol. 540, pp. 308-324, 2020.

[32] Sunday Oyinlola Ogundoyin, Ismaila Adeniyi Kamil, "An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy", Vehicular Communications, 2021.

[33] JingwenZhang, MeitingGuo, BiyanLi, RuiminLu, "A transport monitoring system for cultural relics protection based on blockchain and internet of things", Journal of Cultural Heritage, vol. 50, pp. 106-114, 2021.

[34] Elnaz Irannezhad, "Is blockchain a solution for logistics and freight transportation problems?" , Transportation Research Procedia, vol. 48, pp. 290-306, 2020.

[35] Saeed Asadi Bagloeea, Madjid Tavana, Glenn Withers, Michael Patriksson, Mohsen Asadi, "Tradable mobility permit with Bitcoin and Ethereum – A Blockchain application in transportation", Internet of Things, vol. 8, 2019.

[36] Raja Wasim Ahmad, Haya Hasan, Raja Jayaraman, Raja Jayaraman, "Blockchain applications and architectures for port operations and logistics management", Research in Transportation Business and Management, 2021.

[37] Rajat Chaudhary a, Anish Jindal b, Gagangeet Singh Aujlac, Shubhani Aggarwal a, Neeraj Kumar a, Kim-Kwang Raymond Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system", computers & security, vol. 85, pp. 288-299, 2020.

ISSN:1673-064X
E-Publication: Online Open Access
Vol: 64 Issue 11 | 2021
DOI 10.17605/OSF.IO/T953Z

[38] Lijun Suna, Qian Yanga, Xiao Chenc, Zhenxiang Chen, “RC-chain: Reputation-based Crowdsourcing Blockchain for Vehicular Networks”, Journal of Network and Computer Applications, vol. 176, 2021.

[39] Saurabh Singh, Pradip Kumar Sharma, Byungun Yoon, Mohammad Shojafar, Gi Hwan Cho, In-Ho Ra, “Convergence of Blockchain and Artificial Intelligence in IoT Network for the Sustainable Smart City”, Sustainable Cities and Society, vol. 63, 2020.

[40] Ahmed A.Abd El-Latif, BassemAbd-El-Atty, IrfanMehmood, KhanMuhammad, Salvador E.Venegas-Andraca, JialiangPeng, “Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities”, Information Processing & Management, vol. 58, 2021.

[41] A. F. M. Suaib Akhter, Mohiuddin Ahmed, A. F. M. Shahen Shah , Adnan Anwar and Ahmet Zengin, “A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET”, Sustainability , vol. 13, 2021.

[42] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, “A secure and efficient blockchain-based data trading approach for internet of vehicles,” IEEE Transactions on Vehicular Technology, vol. 68, no. 9, pp. 9110–9121, 2019.

[43] Z. Li, Z. Yang, and S. Xie, “Computing resource trading for edgecloud-assisted internet of things,” IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3661–3669, 2019.

[44] G. Qiao, S. Leng, H. Chai, A. Asadi, and Y. Zhang, “Blockchain empowered resource trading in mobile edge computing and networks,” in ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019, pp. 1–6.

[45] H. Chai, S. Leng, K. Zhang, and S. Mao, “Proof-of-reputation basedconsortium blockchain for trust resource sharing in internet of vehicles,” IEEE Access, vol. 7, pp. 175 744–175 757, 2019.

[46] S. Wang, X. Huang, R. Yu, Y. Zhang, and E. Hossain, “Permissioned blockchain for efficient and secure resource sharing in vehicular edge computing,” arXiv preprint arXiv:1906.06319, 2019.

[47] W. Al Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, “Privacy-preserving smart parking system using blockchain and private information retrieval,” in 2019 International Conference on Smart Applications, Communications and Networking (SmartNets). IEEE, 2019, pp. 1–6.

[48] [48] T. Xiao, T. Qiu, N. Lv, Q. Pei et al., “Smart-contract based economical platooning in blockchain enabled urban internet of vehicles,” IEEE Transactions on Industrial Informatics, 2019.