Analyze state-of-the-art achievements and trends in IT In perspective Of Blockchain Technologies for Vehicle Registration

Zeba Mahmood

zeba.mahmood@ktu.edu

Abstract— World population is

growing in fast numbers as people try to maintain their need of transportation buses, trains come up in mind with first thought but Motor vehicles bring the revolution to the industry and bring new perspective and open new doors and compile a full market of vehicles as Motor vehicle agencies need to collaborate with external organizations like the Departments of Justice and Insurance to register vehicles. Maintaining the most updated information is essential to enable these organizations to register and track vehicles accurately. Current systems that facilitate this process are prone to errors due to duplication of records or incomplete information. As blockchain is covering up this era of technology with its new trends so vehicle market is also enabling the power of IT to collaborate it and make their vehicle system totally automated and as well management system of vehicle to organize this module according to government administration level. This highlights the need of having secure network in order to transfer the Vehicle in an efficient way. In vehicle dealing business due to invalid record, problems are highly recorded. As we all know, Blockchain has literally enabled the technology ecosystem to take a significant leap of innovation. Along the years, as Bitcoin has managed to take prominence and grabbed attention from all over the world, people took to studying all about cryptocurrency and Blockchain the very platform that enabled crypto transactions to take place. IT trends are tackling the industries to make them grow with latest technologies and bring the perspective of blockchain which is bringing new secure, efficient, authorized platforms according to need of market.

I. INTRODUCTION

Blockchain technology and trust concentrated on identifying trust pathways. These pathways are necessary conditions to create any contracting relationship that uses a decentralized ledger technology (DLT) such as blockchain as a foundation. The next step is to apply pathway identification to an actual implementation problem on blockchain registration. Blockchain is based on distributed ledger to keep record of transactions that can be viewed by users of network. Now, if a new piece of information arrives that is to be added in the blockchain, the consensus must come forward to check the validity of that information by the help of independent verifiers. Consensus is basically algorithms which are very important for creating any blockchain based program or design because consensus providing solution according to the need. This new piece of information can be related to transfer Vehicle new owner name or

property information that is available for transfer or anything like that. Each and every transaction that is held in blockchain is somehow linked cryptographically to the previous block[41]. Thus, in order to change the data that is stored on blockchain is extraordinary difficult or any such change can be detected readily. In this way, blockchains are considered as immutable and can serve the purpose of storing data of ownership. While processing the transaction in blockchain, the user/customer makes use of the public address as well as the private key that is cryptographically linked to the blockchain transactions that have already taken place. Public key is used for the sake of other users in the network so that the transaction details can be made transparent to each and every user of the network. The purpose of private key is to digitally sign the transactions to provide authentication in order to ensure that the user has genuinely perform the transaction. Blockchain is one of the new emerging

technologies and has become popular with the Bitcoin application introduced in 2009[8] After that, Ethereum blockchain was launched in 2015 and the main addition to this blockchain type was the implementation of the distributed Bit ledger capability. Code to be written in blockchain can be accessed publicly as this code runs on multiple computers and therefore the problem of a single point failure in the centralized approach is eliminated and the trust from the distributed booklet is not restored by the third party. published research work also provides a big weight- age to get admissions in reputed varsity [4]. The blockchain technology gained importance by its application "Bitcoin". The main characteristic of this application was the problem solving ability without using the traditional payment methods which is to trust the single third party. The main problem with this approach is that if the only single 3rd party which is involved in transaction verification process is doubted or can cheat its users then how

person can securely handle their transactions. Blockchain technology is being used so that each and every transaction performed by the users can be verified by multiple nodes present on blockchain network and after verification process the transaction is performed and is made visible to all nodes of the network.

II. TAXONOMY OF BLOCKCHAIN BASED VEHICLE REGISTRATION APPLICATIONS

First, In various countries, enlisting a motor vehicle with the fitting experts is one of those fundamental assignments on assuming liability for vehicle. From the owner's perspective, it when in doubt gives some proof of ownership and offers a benefit to drive the vehicle on open roads (expecting the appropriate charges have been paid). From the express specialists' perspective, the enlistment system gives various limits, including a strategies for making salary, for issuing traffic infringement usage sees and for ensuring

that vehicles driven on individuals by and large boulevards meet the required prosperity standards [3]. In any case, the vehicle enlistment system can in like manner accept a vocation in

preventing and recognizing vehicle bad behavior. For example, it gives a techniques by which the police can certify the association between a vehicle's ownership and its driver in the midst of an ordinary traffic stop, which may perceive a stolen vehicle. The vehicle enlistment system can moreover be expected to decrease the open entryways for profiting by vehicle burglary by making it hard to re-enroll a stolen vehicle. Alterations to the vehicle enrollment structure have for very some time been recognized in the UK as a strategies by which vehicle bad behavior could be diminished. Without a doubt, as in front of calendar as 1920, the Metropolitan Police in London recognized the potential for lessening vehicle bad behavior by upgrading the then separated vehicle selection structure, which allowed vehicles stolen in one close-by master district to be re-enrolled in another (Webb 2005)[5]. Even more as of late, an extent of bad behavior decline recommendation for fixing the vehicle selection structure were delivered (Webb et al. 2004; Laycock and Webb 2005).[7]

Controlling the vehicle selection structure as a techniques for diminishing vehicle bad behavior can be viewed as a component of a tradition of using authoritative responses to decreasing social issues, correspondingly that bearing has tended to fencing of stolen items through pawn shops (Fass and Francis 2004), unlawful firearm ownership (Bricknell 2012), cannabis use in some US states 7 (Chemerinsky et al. 2015), prostitution in a few Australian states (Wightman 2012) and around the world tax avoidance through the budgetary structure (Walters et al. 2011). Such bearing usually incorporates a ton of standards, set up through sanctioning, an authoritative code that shows how the sanctioning will be operationalized and a strategies for watching consistence with the fundamentals (Baldwin et al. 1998)[3]. This will much of the time incorporate a state association with commitment in regards to managerial watching and consistency.

Imperatively, the association responsible for authoritative consistence will much of the time be discrete from that in charge of continuously expansive policing commitments. With respect to the vehicle selection system for example, this will much of the time be an alternate vehicle enlistment expert, arranged under an organization office responsible for other transport related issues. In this sense, vehicle enlistment experts give an outcast policing limit Mazerolle and Ransley 2005) by watching consistence with vehicle bearings[10]. In a couple domains, a progressively clear outcast policing employment may be played by vehicle enlistment specialists in trying to diminish vehicle burglary. In Australia, there has been a reliable progression of the structure over the span of late years proposed to address express vulnerabilities that have empowered the re-selection of stolen vehicles. These progressions have reflected what Sparrow (2000) has noted to be three key segments of an progressively expansive move towards proactive heading a consideration on results, the gathering of

basic reasoning frameworks to achieve results and working in association [12].

III. APPLICATIONS AND SYSTEMS FOR VEHICLE REGISTRATION

The relentless developing danger of sorted out vehicle lawful offense and dealing presents vast difficulties to requirement specialists. Improved security for testament records will encourage. It not exclusively offers police the vital capacity to loyally see doctored vehicle enrollment archives, it also helps trust in reports setting up legitimate belonging. This has offered ascend to the electronic VRC (eVRC), a tamper evident authentication of auto ownership that has confirm an impressive weapon inside the battle against vehicle enrollment extortion. as a result of the eVRC establishes a sealed connection between assessment installments on record and vehicle ownership, it disposes of the probability for vehicle house proprietors to evade tax assessment with imagine tags and knave work. Shutting escape clauses,
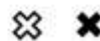
expanding income Veridos is in a situation to create clients with the latest innovations for the improvement of electronic VRC. the appropriate response might be a significant apparatus in shutting escape clauses, appropriately enrolling all vehicles on the street and at last expanding income by gathering all extraordinary vehicle tax. Switchover might be troublesome, anyway the customer edges from the organization's enormous generation mastery in security printing and ID cards from its parent firms Giesecke and Devrient and Bundesdruckerei [66] This understanding and experience licenses it to create able help and steerage all through the complete technique, from enlistment to supply. the corporate furthermore provides recommendation what's more, help to choose that reasonable administrations should be fused, similar to versatile vehicle enlistment and elective improvements to the client expertise. An extreme accomplice for the long run. Clients will predict to incredibly verify, charge card measured with other key accomplices. the corporate additionally provides recommendation

and help to decide that sensible services ought to be incorporated, like mobile vehicle registration and alternative enhancements to the user expertise. An tough partner for the long run. VINchain and Veridos used for perform vehicle registration Customers will foresee to extremely secure, credit card-sized with other key partners for this situation, the police and protection industry. vehicle registrations from Veridos. These high quality sensible cards are sturdy, flexible, compatible with security enhancements and reasonable to provide. they're compliant with major standards (ISO/IEC, European Vehicle Registration and AAMVA) and might be customized centrally or localized as fits the customer's wants. however maybe most significantly, Veridos has established itself because the most well-liked life-time partner during this field, with the product, solutions and technology our customers want for the long run [51].

IV. VEHICLE REGISTRATION SYSTEM LIFECYCLE

Vehicle Sale/Registration Workflow:

•   The Dealer can start vehicle deal contract.

•   A keen contract can then naturally convey demands for enrollment and protection.

•   The RTO and protection office can approve required information about vehicle and client from Blockchain and give enrollment and protection individually.

•   On fruitful preparing of the above advance, the vehicle proprietorship can be naturally exchanged to the client by the keen contract.

Manufacture   Pushes   the vehicle to blockchain, by adding basic details like create, model, variant, chassis variety, engine variety etc. and executes the sale of   the   vehicle. Dealer Executes the sale of the vehicle to the top client [19]. Insurance Agency   Validates   the   client   and

vehicle   information   and   provides insurance. Registration Authority RTO are   accountable   for   approving registrations   and providing the number, playing vehicle transfers and vehicle selling.   Police   Provides   clearance purchasable and transfer of auto similarly as   problems   challans   for   traffic violations. Service Center Adds service details   like   job   cards   and   half replacements [44]. As Smart contracts having   very   vital   role   in   providing certificates and blockchain and smart contracts combination is the safe and trustable on this point if we try to recall this registration system online the block of the existing information is already created and it is not able to process further   because blockchain provide the chain of block which are not able to temper as it provide the uniqueness that every block on the that created chain contains the information of the previous block so when it will not match with the information of the previous block information it will not process future because here the algorithm will come up with decision that block is not available so

no person can register information of any vehicle until he provides all details. Such as the bitcoin blockchain, offered not very many implicit apparatuses to computerize exchanges Consensus Algorithm having properties as Consensus knows as solving problem in distributed programing and connecting nodes on two ways

1.Propose

2. Decide in figure below this property does not Satisfy uniform Consensus Algorithm and its identifiable that the process is crashed [45].
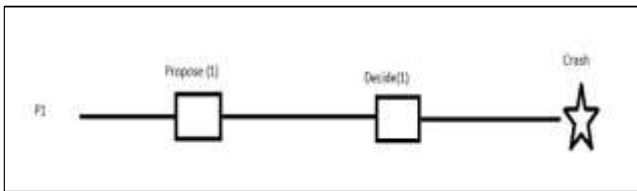

Figure 1. Process of Evaluation of Consensus Algorithm

Blockchain is comprised of sequence of blocks. These blocks are responsible of holding the complete transaction details just like in conventional public ledger Blockchain as sequence of blocks Each block present in the network points to the previous block by reference which is the previous block's hash value known as parent block. Uncle blocks i.e. child of ancestor blocks hash values are also stored in case of Ethereum blockchain [10].

$$\dot{x}_i(t) = \sum_{j \in N_i} a_{ij}(x_j(t) - x_i(t)) \ , \ t \geq 0$$

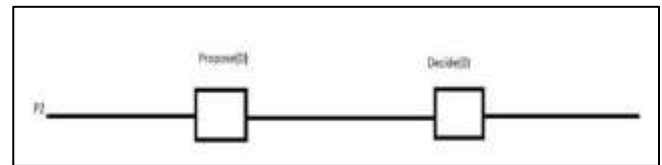extended. The main issue here is that what if the data of block is changed [17].

Figure 2. Evaluation of Validity Consensus Algorithm

As an owner sell his car according to owner he having proof of ownership of the vehicle and uploaded the document on the system and set a desirable amount which will be displayed and here blockchain will use public type where data is available and purchaser can verify it through verification of vehicle by using vehicle registration system, And once he satisfy

with all the procedure he request for purchase and smart contract now act like 3rd party between both of customers as smart contract provides the bank account of the person to whom money will be transferred and once payment process completed smart contract issue a certificate which will be usable as purchase document and invoice of payment to owner after that vehicle registration system will acknowledge this new customer as new owner and create a new block for vehicle identification number by connecting all previous details of the person who sell it. By this procedure now new owner will be able to see his data as new owner after department of vehicle registration system done all its documentation process on behalf of both parties.

- Programming language

- Type of consensus mechanism

- Authorized participants that are present in blockchain network

- Smart contract topology

where, $xi(t)$ is the information state of node i at time t with $xi(0)$ being the initial state of node i. The algorithm can be interpreted as the change of agent i's information being the difference between its own information and the agents connected to agent i's information.

In blockchain, the first block is called as genius block and it is worth noting that genius block .The work flow of blockchain is that the sending nodes in blockchain network first record the new data and then broadcast it to the network. After broadcasting process, the receiving nodes checks the authenticity of the data and if found correct, the received data is stored on the blocks. On that block, consensus algorithm i.e. proof-of-stake or proof-of-work is run by the receiving nodes and after that the block is stored into chain and each and every node in the network will acknowledge that block and then the chain base of this block will be continuously
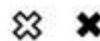
The collective feature of mentioned variants is that any person can join if he is willing to sustain the ledger and withdraw at any moment as well. Hence, such types are called Public or open Blockchains. Due to liberty of joining, the concept of implementing human realistic consensus [9] is difficult, wherein the outcomes must be obtained from the entire nodes before the conclusion. The main cause is the unidentified and difficult to manage the execution of these nodes. When numerous nodes exist, the communication for exchanging agreements among these may become complex. It is worse, as there is possibility to cope the nodes, captivating agreement as of all of these might lead to various possible risks, which could possibly destruct the holding procedure of the ledger. Accordingly, to add on a block to the sequence, called chain, the entire nodes must demonstrate that their "qualification" is more compared to others to perform this job. And so, a consensus algorithm of such type may possibly be entitled a "proof-based consensus". Moreover, in public Blockchain, to boost nodes to keep up the

ledger, the nodes will get some recompense after a block addition to the chain by these nodes to keep up the ledger, the nodes will get some recompense after a block addition to the chain by these nodes.

VI. CONCLUSION

The potential uses of this emerging technology are almost in all fields such as finance, administration etc. as the transaction takes place between the agents without the involvement of any central authority and with unquestionable transparency. , we are focusing on practical implementation of blockchain in property management in which smart contract operations are involved that allows the secure and fast ownership of Vehicle in Vehicle registration system. Blockchain technologies are coming up the world up trend to convert all your system and information in blockchain using fastest and accurate methods to transfer information using transport layers to intact your information in data packets .and it is very effective for the government for using this type of hybrid technology which having public and private phases to show the data they want and configure the rights they don't want to share even though they having secured platform to share as much they can do Verification of nodes by several nodes,

No single point of failure and Advantages of disintermediation, manufacturers, customers, authorities and all other involved parties of time-consuming, manual, and repetitive tasks.

61

REFERENCES

[1]   M. Ali "CSN: A network protocol for serving dynamic queries in large-scale wireless sensor networks," in *Proc. 2nd Annunal Conf. Commun. Nettwork Services Res.*, Fredericton, May 2004, pages 165-174.

[2]   S. Krco and D. Parker, "P2P mobile sensor networks," in *Proc. 38th Annunal. Hawaii Int. Conference Syst. Sci.*, USA, 2005,p. 324c

[3]   S. King, "PPcoin: peer-to-peer crypto-currency with proof-of-stake," 2012 [Online]. Available at: https://decred.org/research/king2012.pdf.

[4]   T. Tuan *et al.*, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. on Knowledge and Data Eng.*,volume 30, no. 7, pages 1366–1385, 2018.

[5]   P. Sharma and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, volume 6, pages 115–124, 2018.

[6] P. Vasin, "Blackcoin's proof-of-stake protocol v2," 2014

Available online: https://blackcoin.co/blackcoin-pos-protocol- v2-whitepaper.pdf

[7]   G. Wood, ``Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project, 2014.

[8]   Z. Li, J. Kang, D. Ye and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions Ind. Informatics*, no. 8, pages. 36900–3700, 2018.

[9]   Hyperledger Available online: http://hyperledger.org/.

[10] T. Duong and H. S. Zhou, "2-hop Blockchain: combining proof- of-work and proof-of-stake securely," Available online: https://eprint.iacr.org/2016/716.pdf.

[11]Corda Available online: https://www.corda.net/.

[12] M. Isaja and J. Soldatos, "Distributed ledger technology for decentralization of manufacturing processes," *Proc. IEEE Industry Cyber-Physical Sysem. ICPS 2018*, pages 696–701,

2018.

[13] S. Duan, S. Peisert, and H. Zhang, "BChain: byzantine replication with high throughput and embedded reconfiguration," in *Prin. of Distributed Sys*. Cham, Springer, 2014, pages 91-106.

[14] D. Schwartz, and A. Britto, "The Ripple protocol consensus algorithm," 2014 Available online:

https://ripple.com/files/ripple_consensus_whitepaper.pdf

[15] Hyperledger iroha Available online:

https://github.com/hyperledger/iroha.

[16] *Hyperledger-Fabric*. Accessed on Apil. 10, 2018. Available online: https://www.hyperledger.org/projects/fabric

[17] G. T. Nguyen and K. Kim, "A survey about consensus algorithms used in Blockchain," *J. Inf. Process. System.*, volume 14, no. 1, pages. 101–128, 2018.

[18] Hyperledger fabric, Available online:

https://github.com/hyperledger/fabric.

[19] Hardjono, "Cloud-based commissioning of constrained devices using permissioned blockchains". *In Proc. of 22nd ACM Int. Workshop on IoT Privacy and Security* (IoTPTS 2016), Xi'an, China, 2016; pages 29–36.

[20] Herbert, J.; Litchfield, A. "A novel method for decentralised

peer-to-peer software license validation using cryptocurrency blockchain technology". *In Proc. of the 36th Australasian Comp. Conference, ACSC 2015*, Sydney, pages. 27–30, Jan. 2015; p. 30.

[21] S. Dziembowski and K. Pietrzak, "Proofs of space" in *Adv. in Cryptology–CRYPTO 2015*. Springer, 2015, pages. 585-605.

[22] Hyperledger Sawtooth, Available online:
https://sawtooth.hyperledger.org/docs/

[23] K. Schwarz, "Cuckoo Hashing," Available online:
http://web.stanford.edu/class/cs166/lectures/13/Small13.pdf

[24] S. King, "Primecoin: cryptocurrency with prime number proof- of-work," 2013 Available online:
http://primecoin.io/bin/primecoin-paper.pdf

[25] W. L. Heimerdinger, "A conceptual framework for system fault tolerance,"

Def. Technical Inf. Center, *Technical Report CMU/SEI-94-TR-033*, 1992.

[26] I. L. C. Bentov and M. Rosenfeld, "Proof of activity:Extending Bitcoin's proof of work via proof of stake [extended abstract],"in Proceedings. 9th Economics workshop, Syst. Comput., USA, June 2014, pages. 34-37.

[27] D. Schwartz and A. Britto, " The ripple protocol consensus algorithm," Ripple Labs, USA, White Paper, 2014.

[28] I. Eyal, E. G. Sirer, and R. Van Renesse, " Bitcoin-NG: A scalable blockchain protocol," in Proc. 13th USENIX Symposiym. Networks Syst. Design Implement, USA, March 2016, pages 45-59.

[29] D. Wilson and G. Ateniese, "From pretty good to great: Enhancing PGP using Bitcoin and the blockchain," in *Proceedings. Int. Conf. Network*

64

Syst. Secur., USA, November 2015, pages 368-375.

[30] T. Bocek, B. B. Rodrigues, and B. Stiller, "Blockchains everywhere_A use-case of blockchains in the pharma supply- chain," in *Proceedings. IFIP/IEEE Symp. Netw. Service Manage. (IM* , May 2017, pages 772-777.

[31] M. Siddiqi, S. T. All "Secure lightweight context-driven data logging for body worn sensing devices," in *Proc. 5th International. Symp. Digital. Forensic Secur. (ISDFS)*, Romania, 2017, pages 1-6.

[32] M. Samaniego and R. Deters, "Internet of smart things-IoST: Using blockchain and CLIPS to make things autonomous," in *Proc. IEEE International.Conf. Comput. (ICC)*, USA, June 2017, pages 9-16.

[33] S. Miyake and M. Bandai, "Energy-efficient mobile P2P communications based on context awareness," in *Proeedings. IEEE 27th Int. Conference. Adv. Inf. Network*

.Applications. (AINA), Spain, March 2013, pages 918-923.

[34] Herbert, J.; Litchfield, A. "A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology". In Proc. of the 36th Australasian Comp. Conference, ACSC 2015, [36] Sydney, pages. 27–30, Jan. 2015; p. 30.

[35] S. Dziembowski and K. Pietrzak, "Proofs of space" in Adv. in Cryptology–CRYPTO 2015. Springer, 2015, pages. 585-605.

[36] Hyperledger Sawtooth, Available online:

https://sawtooth.hyperledger.org/docs/

[37] K. Schwarz, "Cuckoo Hashing," Available online:

http://web.stanford.edu/class/cs166/lectures/13/Small13.pdf

[38] S. King, "Primecoin: cryptocurrency with prime number proof- of-work,"

65

2013 Available online: http://primecoin.io/bin/primecoin-paper.pdf

[39] W. L. Heimerdinger, "A conceptual framework for system fault tolerance," Def. Technical Inf. Center, Technical Report CMU/SEI-94-TR-033, 1992.

[40] https://shorishresearch.com/2017/12/08/blockchain-registration- part-1/ D. Wilson and G. Ateniese, "From pretty good to great: Enhancing PGP using Bitcoin and the blockchain," in Proceedings. Int. Conf. Network Syst. Secur., USA, November 2015, pages 368-375.

[41] T. Bocek, B. B. Rodrigues, and B. Stiller, "Blockchains everywhere_A use-case of blockchains in the pharma supply- chain," in Proceedings. IFIP/IEEE Symp. Netw. Service Manage. (IM , May 2017, pages 772-777.

[42] M. Siddiqi, S. T. All "Secure lightweight context- driven data logging for body worn sensing devices," in Proc. 5th International. Symp. Digital. Forensic Secur. (ISDFS), Romania, 2017, pages 1-6.

[43] M. Samaniego and R. Deters, "Internet of smart things-IoST: Using blockchain and CLIPS to make things autonomous," in Proc. IEEE International.Conf. Comput. (ICC), USA, June 2017, pages 9-16.

[44] S. Miyake and M. Bandai, "Energy-efficient mobile P2P communications based on context awareness," in Proceedings. IEEE 27th Int. Conference. Adv. Inf. Network Applications. (AINA), Spain, March 2013, pages 918-923.

[45] Ghuli, P. Kumar, Shettar, R. "A review on blockchain application for decentralized decision of ownership of IoT devices". Advance Comput. Science Technol. 2017, pages, 2449–2456.

[46] D. Mazieres, "The Stellar Consensus Protocol: a federated model for internet-level consensus," 2015, Available online: https://www.stellar.org/papers/stellar-consensus-protocol.pdf