Chapter 15
Adaptive Proof of Driving Consensus for Intelligent Vehicle Communication

Madhusudan Singh and Iftekhar Salam

Abstract Energy and cost efficiency is a notable drawback in Blockchain Technology as well as in traditional consensus schemes and Blockchain does not have any standard consensus protocol for resource constraint applications such as vehicular communication environment. In this paper, we propose a novel Adaptive Proof of Driving (APoD) consensus algorithm for Blockchain based Vehicular Communication Networks (VCN), especially for resource constraint environments. Our developed algorithm provides secure, trusted and reliable communication environment for vehicles based on reputation. The main contribution of our paper is to improve the power consumption, miner congestion, and cost efficiency of blockchain system for vehicular networks. We evaluate, our proposed approach with the help of congestion less intersection use case for adaptive and secure distributed consensus.

Keywords Blockchain technology · Consensus vehicular communication · Intelligent transportation system

15.1 Introduction

Blockchain technology has the capability to contribute to several fields. Blockchain can contour the eHealth record process and contribute better visibility and efficiency over the supply chain to provision eminent value to the customers and trading relations. Moreover, Blockchain can trace possession of real estate and alter the mode of sharing data and forbidding fraudulence. Blockchain can also revolutionize the Internet of Things and vehicular communication [1].

M. Singh (✉)
School of Technology Studies, Endicott College of International Studies, Woosong University, Daejeon, South Korea
e-mail: msingh@wsu.ac.kr

I. Salam
School of Electrical and Computer Engineering, Xiamen University Malaysia, 43900 Sepang, Selangor, Malaysia
e-mail: iftekhar.salam@xmu.edu.my

M. Singh, *Information Security of Intelligent Vehicles Communication*,
Studies in Computational Intelligence 978,
https://doi.org/10.1007/978-981-16-2217-5_15

The vehicle is experiencing revolutionary growth in research and industry such as intelligent vehicles (IV), vehicle communications, self-driving vehicles, but it still suffers from many security vulnerabilities. Traditional security methods are incapable to provide secure vehicular communication. The major issues in vehicular communication are trust, data accuracy and reliability of communication data in the communication channel [2]. Blockchain technology works for the cryptocurrency, Bit-coin, to develop trust and reliability in peer-to-peer networks which have alike topologies to Vehicle Communication Networks (VCN). But Blockchain doesn't have any standard consensus protocol for resource constraint applications such as vehicular communication environment. In this paper, we propose a novel Adaptive Proof of Driving (APoD) consensus algorithm for Blockchain based Vehicular Communication Networks (VCN), especially for resource constraint environments. Our developed algorithm will provide secure, trusted and reliable communication environment for vehicle based on reputation. The aim of our paper is to improve the power consumption, miner congestion, and cost efficiency of blockchain system for vehicular networks. We evaluate our proposed approach with the help of congestion less intersection use case for adaptive and secure distributed consensus. We have depicted in the Fig. 15.1 is current vehicle communication environment.

The remainder of the work is outlined as follows, Sect. 15.2 has discussed a review of related work, and further, we have explained our proposed consensus algorithm for intelligent vehicles communication environment in Sect. 15.3. We have discussed an intelligent vehicle communication use case model in Sect. 15.4. At last we have concluded our article in Sect. 15.5.

15.2 Related Work

It is challenging to build a secure distributed consensus scheme but there are tremendous benefits for several applications. Bitcoin and other similar cryptocurrencies used in the financial technology are familiar. Bitcoin has several insufficiencies and several altcoin [3] schemes have been proposed to make them better but still not all deficiencies are sufficiently covered. All present cryptocurrency approaches concentrates on payment transaction and maintaining fairness is critical in such transactions as payments are done in exchange of service or goods and there is no identity reliability of the participants and also we cannot practically resolve any subsequent dispute. Another limitation is link ability, making personally identifying the Bitcoin transaction [4]. Zero cash [5] is an alternate which provision payer and payee unlink ability earned as altcoin strategies [6]. Other applications of distributed consensus other than Fin tech are driverless vehicles [7], autonomous robots, supply chain management and sharing information in the Internet of Things (IoT).

There are different requirements for every application and it is critical to decide a distributed consensus which is compatible, suitable and fulfill the requirements for that application. Energy efficiency is a critical requirement and blockchain based on

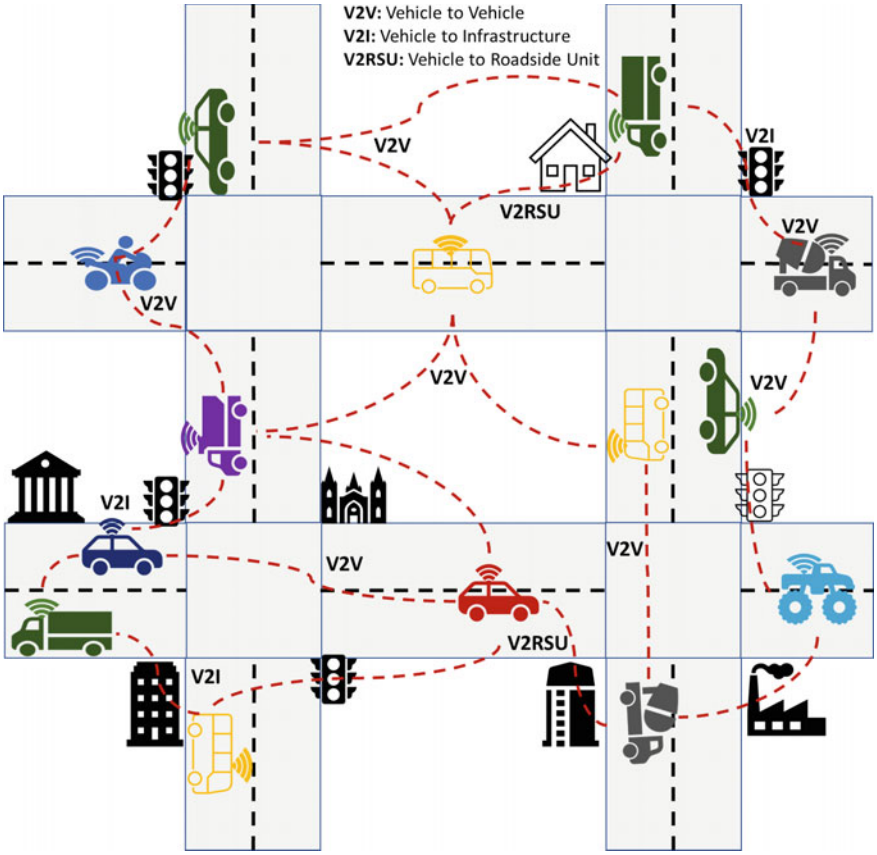

Fig. 15.1 Current vehicle communication environment [1]

"proof of work" consensus scheme like Bitcoin are not favorable in terms of usage of energy.

The traditional Byzantine fault tolerant scheme also consume a lot of energy as every participant need to send and receive the broadcasted message. We aim to develop a consensus schemes which are energy efficient. Figure 15.2 shows several existing consensus algorithms and their work.

- ***Challenges of Existing Blockchain Consensus***

As of now, there is no standard Consensus scheme fully compatible for Vehicular Communication Network (VCN). However, researchers are using traditional consensus schemes (CheapBFT [8], MinBFT/MinZyzzyva [9], and Proof of Work (PoW) [2]) in VCN. There are various limitations of consensus schemes in Distributed Computing such as safety (all valid participant's agreement on consistent value) and liveness (all valid participants finally determine a value). According to Bracha and Toueg [8] if more than f participants are Byzantine then consensus in a loosely

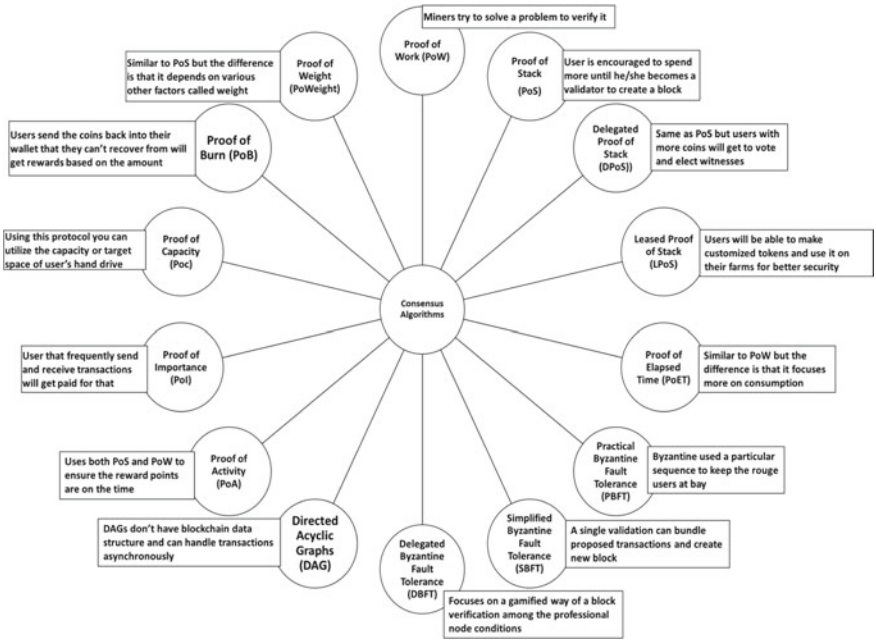

Fig. 15.2 Existing consensus algorithms for blockchain technology

synchronous communication model is not feasible among $n = 3f + 1$ participants. Likewise, Brewer et al. [9]'s "CAP theorem" states that consistency, availability and partition-tolerance cannot be assured at the same time in a distributed system. Classical PBFT [10] consensus schemes are established on state machine replication and are becoming obsolete due to their huge cost of computation, bandwidth and expected number of autonomous servers [11].

15.3 Proposed Adaptive Proof of Driving (APoD) Methodology

We have developed a decentralized distributed reputation based Vehicular Communication Networks (VCN) that use Blockchain technology to build trust among vehicles. The proposed Blockchain technology for vehicular communication is based on novel consensus algorithm, Adaptive Proof of Driving (APoD) which, increases performance and throughput by reducing miner congestion. Our proposed algorithm provides secure reliable scalable consensus mechanism for vehicular network, by combining two schemes, First Come First Serve (FCFS) and Priority (Reputation) scheme as shown in step 1 and step 2 in Fig. 15.2. The FCFS scheme maintains

the timestamp list using the blockchain server and priority scheme gives preference to lower timestamp and reputed Vehicles. To validate the reputed vehicles, we have introduced Vehicle Reputation Point (VRP) which is an issued unique crypto ID for each vehicle and the same VRP are used to enable the flow of reputation points, which act as a reputation value for vehicle to get involved in the information exchange between vehicles. For the data management of the VRP, we are using blockchain technology in the intelligent transportation system (ITS), which stores all VRP details of every vehicle and is accessed ubiquitously by vehicles [12].

- ***Adaptive Proof of Driving (APoD) Consensus Algorithm***

We propose an Adaptive Proof of Driving (APoD) consensus algorithm which uses two schemes, First Come First Serve (FCFS) and Priority to drop-off the congestion of miners to increase the performance. Figure 15.3 shows our proposed Consensus approach. The two steps step 1 and step 2 are defined below.

– *First Come and First Serve (FCFS)*: First Come and First Scheme uses timestamp t_s to reduce the miner congestion in the vehicular communication network. If timestamp t_i of a vehicle V_i is less than the timestamp t_j of a vehicle V_j, then vehicle V_i is added in the miner list as it has lower timestamp.
– *Priority Scheme*: The blockchain server maintains the miner list of first come messages based on the Vehicular Reputation Point (*VRP*) of each vehicle. The

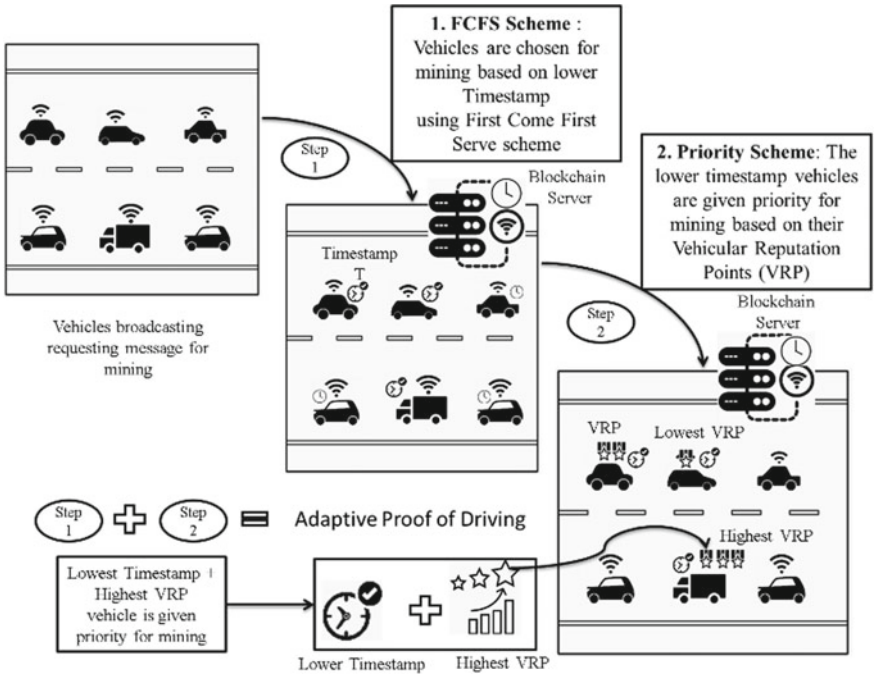

Fig. 15.3 Proposed adaptive proof of work consensus approach

priority scheme uses the Vehicular Reputation Points (VRP) to decide the priority given to vehicles in the Miner list. The higher priority vehicles are trusted and given incentives in terms of VRP. If VRP of a vehicle V_i is greater than the VRP of a vehicle V_j, then vehicle $V_i^{'}$s broadcasted message is trusted and is awarded some Reward Points.

Below is the pseudo code of APoD Consensus scheme:

Pseudocode of APoD Consensus Scheme

$\boldsymbol{FCFS(V(t_s))}$

1. *For timestamp instant* t_s
2. *If* $(V_i(t_i)) < \left(V_j(t_j)\right)$
3. $Miner_{list} \leftarrow V_i$
4. $return\ Miner_{list}$
   $\boldsymbol{Priority(Miner_{list}(VRP))}$
5. *For Vehicular Reputation Points* VRP
6. *If* $\left(VRP[V_i] > VRP[V_j]\right)$
7. $VRP[V_i] \leftarrow VRP[V_i] + Reward\ Points$
8. $return\ VRP[V_i]$
9. $else\ VRP[V_j] \leftarrow VRP[V_j] + Reward\ Points$
10. $return\ VRP[V_j]$

Our proposed APoD algorithm is energy efficient, cost efficient and builds trust and reliability in the blockchain network.

15.4 Intelligent Vehicle Communication Use Case Scenario

We discuss the intersection scenario for, utilizing cost and energy and building trust and reliability in the blockchain based vehicular communication network. In an intersection scenario as shown in Fig. 15.4, all vehicles are coming from all directions at the intersection and all vehicles cannot cross the intersection simultaneously as deadlock situation will happen. Therefore, vehicles must cross the intersection one at a time to avoid deadlock situation. Now, the problem arises as to which vehicle will cross the intersection first and in what order so that all vehicles can cross and there is no deadlock situation. To solve this problem, we applied our proposed Adaptive Proof of Driving (APoD) consensus algorithm which uses two schemes, First Come First Serve (FCFS) and Priority to drop-off the congestion of vehicles, deciding which vehicle to cross the intersection first thereby utilizing energy, cost and building trust and reliability in the blockchain network. The description of each of the scheme is as follows:

First Come First Serve (FCFS) Scheme: In this scheme the vehicle which arrives first at the intersection, is stored in the miner list which is later used by the priority

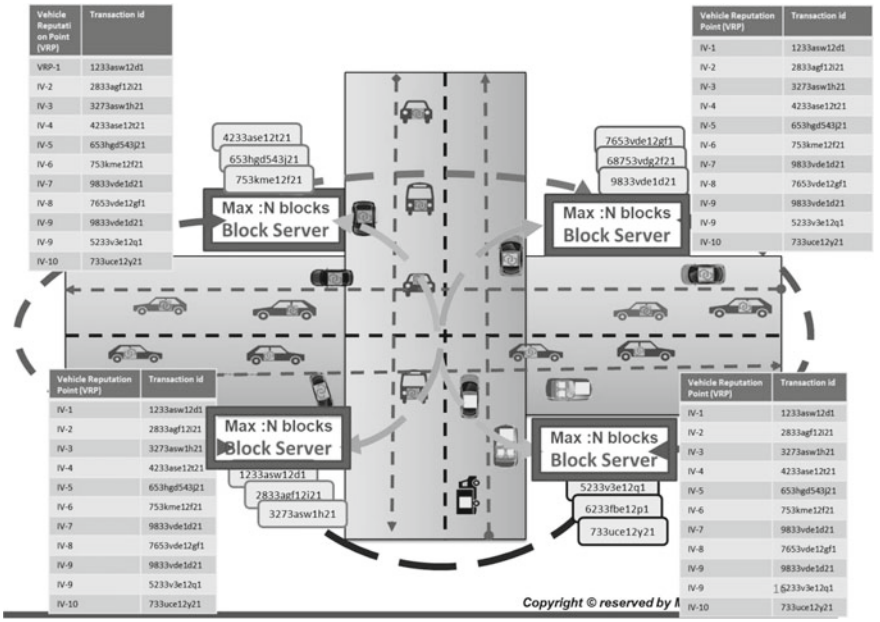

Fig. 15.4 Overall intelligent vehicle communication based on adaptive proof of driving consensus algorithm

scheme to determine the priority to mine based on the vehicle's Vehicle Reputation Point (VRP) to find the order of vehicles to cross the intersection.

For example: Assume four vehicles V_1, V_2, V_3, *and* V_4 arrives at the intersection at 1.65, 1.63, 1.66, 1.61 s respectively, then the vehicle whose arrival time is minimum (arrives first at intersection will be eligible as miner). So, V_4 with minimum arrival time of 1.61 s will be the first miner added in the miner list. Thereafter, V_2, V_1 and V_3 will be given preference for mining in ascending order of their arrival time [12].

Priority Scheme: In this scheme, each vehicle in the miner list is assigned a priority based on the Vehicle Reputation point (VRP) it owns as shown in the distributed ledger of each blockchain server in Fig. 15.4. The amount of VRP indicates the trust and reliability the vehicle has. The greater the VRP, the greater is the vehicle's trust and highest will be the vehicle's priority. The highest priority vehicle with the lowest arrival time at the intersection will first cross the intersection and the lowest priority vehicle with highest arrival time at the intersection will cross the intersection at the last. The miner vehicle will generate the table accordingly.

Vehicles with same VRP or same priority will follow the FCFS scheme to decide the order in which they will cross the intersection.

For example: The vehicles V_1, V_2, V_3 and V_4 have 10, 15, 20, and 35 VRP respectively and the miner list ascending order is $\{V_4, V_2, V_1, and\ V_3\}$ then the vehicle V_4, having lowest arrival time of 1.61 s and greatest VRP of 35 will be considered the most

trusted and reliable vehicle in the network of the four vehicles. Similarly, vehicle V_1 having 10 VRP (minimum in the network) will be considered the least trusted and least reliable vehicle in the network of the vehicles. Therefore, vehicle V_4 will have the highest priority to do the mining to find out the order of vehicles to cross the intersection.

Note: In same VRP and Time stamp then we will consider 2nd significant figures of the arrival time of the vehicles at the intersection. After applying our proposed APoD algorithm to the intersection scenario shown in Fig. 15.4, the vehicular communication becomes seamless avoiding deadlock and utilizing energy, cost and building trust and reliability in the blockchain based vehicular network.

15.5 Conclusion

We proposed a novel Adaptive Proof of Driving (APoD) consensus algorithm for Blockchain based Vehicular Communication Networks (VCN). Our proposed APoD algorithm provides secure reliable consensus mechanism for vehicular network, by combining two schemes, First Come First Serve (FCFS) and Priority (Reputation) scheme. The FCFS scheme maintains the timestamp list using the blockchain server and priority scheme gives preference to lower timestamp and reputed Vehicles thereby improving the power consumption, miner congestion, and cost efficiency of blockchain system for vehicular networks. To validate the reputed vehicles, we have introduced Vehicle Reputation Point (VRP) which is an issued unique crypto ID for each vehicle and the same VRP are used to enable the flow of reputation points, which act as a reputation value for vehicle to get involved in the information exchange between vehicles. In future, we will implement our consensus algorithm for Blockchain-based secure decentralized reliable vehicular communication networks through simulations and real-life experiments.

Acknowledgements This research was funded by Woosong University Academic Research in 2021.

References

1. M. Singh, S. Kim, Crypto trust point (cTp) for secure data sharing among intelligent vehicles, in *The 2018 International Conference on Electronics, Information and Communication (ICEIC 2018)*, Sheraton Waikiki Hotel, Honolulu, Hawaii, USA, 24–27 Jan 2018. https://ieeexplore.ieee.org/document/8330663/
2. B. Leiding, P. Memarmoshrefi, D. Hogrefe, Self-managed and blockchain-based vehicular ad-hoc networks, in *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2016, pp. 137–140. https://dl.acm.org/citation.cfm?id=2971409
3. S. Kim, Blockchain for a trust network among intelligent vehicles. Adv. Comput. **111** (2018). ISSN 0065-2456. https://www.sciencedirect.com/science/article/pii/S0065245818300238

4. G.S. Veronese et al., Efficient byzantine fault-tolerance. IEEE Trans. Comput. **62**(1), 16–30 (2013). https://ieeexplore.ieee.org/document/6081855/?arnumber=6081855
5. R. Kapitza et al., CheapBFT: resource-efficient byzantine fault tolerance, in *EuroSys* (ACM, 2012). https://doi.acm.org/10.1145/2168836.2168866
6. M. Vukolić, The quest for scalable blockchain fabric: proof-of-work vs. BFT replication, in *International Workshop on Open Problems in Network Security* (Springer, 2015). https://link.springer.com/chapter/10.1007/978-3-319-39028-4_9
7. L. Luu et al., Demystifying incentives in the consensus computer, in *CCS* (ACM, 2015). https://doi.acm.org/10.1145/2810103.2813659
8. Bracha, S. Toueg, Asynchronous consensus and broadcast protocols. J. ACM **32**(4), 824–840 (1985). https://dl.acm.org/citation.cfm?id=214134
9. E.A. Brewer, Towards robust distributed systems (abstract), in *PODC* (ACM, 2000). https://doi.acm.org/10.1145/343477.343502
10. M. Castro, B. Liskov, Practical byzantine fault tolerance, in *OSDI* (USENIX Association, 1999). https://dl.acm.org/citation.cfm?id=296806.296824
11. V. Buterin, A next-generation smart contract and decentralized application platform (2014). https://github.com/ethereum/wiki/wiki/White-Paper
12. M. Singh, S. Kim, Branch based blockchain technology in intelligent vehicle. Comput. Netw. (2018). ISSN 1389-1286. https://doi.org/10.1016/j.comnet.2018.08.016