FIOV: the Future Internet of Vehicles Based on Blockchain

Xingyu Lv[1,a]

[1]*School of Computer Science and Network Engineering, Guangzhou University, Guangzhou, China*
a. lvxingyu@woyiyun.net

Keywords: IOT, IOV, blockchain, P2P.

Abstract: With the development of information technology, the emergence of the IOT (Internet of Things)[1] can connect objects through intelligent terminals , and connecting everything becomes a new development trend. As one of the most important transportation for human beings, the IOV(Internet of Vehicles) which is composed of vehicles has naturally become the main application field of the IOT. However, the current development of IOV is still not perfect, there are still many problems such as users data privacy, lacking of uniform standards of IOV management and so on. With the constant iteration of technology, these issues are likely to be resolved in the near future. To this end, we propose the concept of the FIOV(Future Internet of Vehicles), and integrate the emerging blockchain technology for the problems existing in the current IOV, so that vehicles and their infrastructure can form a P2P(point-to-point) network to communicate. In this way, the IOV becomes more free and open, and even accesses third-party services, facilitating information transmission and friendly communication between vehicles and the natural space, which is the vision of the FIOV.

1. Introduction

The emergence and development of the IOT has brought a lot of convenience to human life, and connecting everything has become a consensus. This is the case, the IOV came into being. The IOV can realize the connection between people, vehicles and vehicles, vehicles and people, vehicles and businesses, which will greatly facilitates people's lives to enhance the level of intelligent vehicle and autonomous driving capabilities[2]. It will build a new business model for automobiles and transportation services meantime, thereby improving traffic efficiency, improving vehicle driving experience, and providing users with intelligent, comfortable, safe, energy-saving and efficient integrated services.

The reason why the IOV is so important is because its unlimited market potential. With the rapid development of China's social economy, vehicles have entered thousands of households. With the increase of the scale of the new energy vehicle market and the continuous landing of autonomous driving technology, China's vehicles market is bound to enter into a golden period of development. In

the face of a huge market need, China's current IOV technology has obvious shortcomings. For example, the big data privacy accumulated by the IOV cannot be effectively protected, and the network data formed by each area is not interoperable, and it is impossible to create greater benefits and the like. Therefore, it is very necessary to build a smart, open and controllable IOV.Most of the current IOV platforms are characterized by centralization. The information transmission between vehicles and the vehicle infrastructure are managed by third parties and are generally inactive.

The emergence of blockchain technology has made it possible to help IOV become a decentralized distributed system[3],[4]. Blockchain, is applied to the an decentralized electronic cash system, which is packaged into the transaction constituting the blockchain are connected in chronological order, communicate via P2P network connection, using a cryptographic algorithm ensures the security of transaction data. Of course, we use blockchain technology not to issue electronic cash money, but to use it to improve the IOV and solve some problems in the current IOV. The data we put in blockchain can't be tampered to improve the security of the entire IOV architecture.

Based on the above problems and introductions, we propose the concept of FIOV (the Future Internet of Vehicles). In the future, IOV is a internet based on blockchain technology. Vehicles and their related infrastructures form the nodes in the blockchain network. The communication is carried out through a P2P network, and the data of the node is encrypted by a cryptographic encryption algorithm to ensure that it is not tampered with. The node network of the FIOV is composed of a DAG[5] network, which can asynchronously write and write transactions to improve the efficiency of the network. The FIOV is better than the current network architecture because it has the following characteristics:

Data security: For the data written to FIOV, its legality and authenticity are ensured after agreed nodes or core nodes of the whole network approve the record. The record is allowed to be permanently written to the chain. Since the data block in the chain is encrypted storage, node user only has the private key can decrypt the core data block, thereby obtaining the block content. It is also resistant to DDOS (distributed denial of service)attacks, and traditional IOT is vulnerable to network denial of service attacks. Because FIOV is decentralized, when an attacker attacks a node, even if the node fails, it will not affect the entire blockchain system.

System efficiency: FIOV is a DAG network. Currently, there are many projects such as IOTA[6] and Byteball[7]. DAG has successfully built a public blockchain that can run stably for a period of time, which proves the technological advancement and performance of the DAG blockchain. In FIOV, the information of each vehicle or each charging post is packaged into a unit (Unit), and the unit and the unit are linked to each other to form a DAG diagram. Since the unit can be linked to any one or more of the previous units, there is no need to pay more computational cost and time cost for the consensus problem, and there is no need to wait for strong data synchronization between the nodes, or even the concept of assembling multiple blocks of data units. Therefore, the transaction volume can be greatly increased and the confirmation time can be minimized.

Convenient and Low-cost: the deployment costs of FIOV system is very low. As long as you deploy terminal network on the vehicle or deploy sensors on infrastructure such as charging piles, you can join the FIOV blockchain network, which increases the heterogeneous network.In FIOV, the information exchange between differentnodes is convenient, but also conducive to access third-party service platform, which is accessible for vehicle owners to enjoy services such as vehicle maintenance and other ancillary services.

2. Related Works

We already learn the underlying mechanism of the blockchain and want to design and validate a new consensus mechanism, to explore block area in the chain of things especially in terms of IOV applications.

The POW(Proof of Work) consensus mechanism in bitcoin[8] network exists some problems. The first one is the 51% attack problem: if a group controls 51% of the computing power and launches an attack, the bitcoin transaction may be tampered with, and the miners' interest group that has a considerable amount of computing power may also conduct self-propelled mining and other malicious behavior. The second is the issue of POW energy consumption cause the large workload. According to the related data, the mining energy consumption of Bitcoin has been equal to that of a country in Argentina. The IMF and many governments are critical of the virtual currency mining energy consumption. Therefore, it is extremely important to design a consensus mechanism that can be combined with specific scenarios. For the IOV, efficiency and convenience are especially significant. Therefore, we can boldly assume that there is such a common consensus mechanism, called POD (Proof of Driving), which can represent the driver's proof of driving the vehicle, including driving time, driving speed and so on. In this way, the role of a node in the entire network is marked. The accumulated big data can be used for traffic analysis, road planning, business circle setting, etc. The behavior of the user node itself is based on the contribution to the entire vehicle network. At the same time, we can design a reward mechanism to encourage user nodes to participate in the maintenance of traffic order.

In addition, we also conducted research on the security of the IOV. At present experiments, remote self-driving systems without physical contact has been experimentally verified, so we hope to explore a security solution that can match the FIOV.One is the security of node network communication. Nodes communicate through P2P communication protocol. There will be attacks similar to sybil attack[9], eclipse attack[10] and others. To prevent these types of attacks requires in-depth consideration, you can add more nodes to connect inward and outward or verify the connection before add its data to blockchain and so on. On the other hand, there are security vulnerabilities in the system itself. The IOT is actually implemented in the application. When designing a product for an application scenario, we need to consider what security problems it has, because the vulnerability of the platform is never ending. Therefore, we consider introducing an intelligent intrusion monitoring and processing solution, which can use the wireless robot's solution 7*24 hours to monitor the data and whether the operation is abnormal, the log information records the operation, and the feedback obtained is optimized by the artificial intelligence model parameter adjustment.

3. FIOV Architecture

3.1. Overall Overview

We propose a FIOV model, this model is based on the blockchain technology to build.The FIOV model blockchain consists of the vehicle or vehicle infrastructure nodes, the communication between nodes relys on P2P protocol. Traffic conditions data can be shared among active nodes of the vehicle, and can also be uploaded to the cloud of the government transportation department to facilitate route planning and traffic guidance, which contributes to smart transportation in large cities[11]. More importantly, it can make the data owners reach a consensus between the collection and demand, easing the contradiction in the long-term IOV industry facing difficult balance of interests. At the same time, the system uses security encryption algorithm to provide data transmission protection and help protect user privacy[12]. In addition, the FIOV can also access third-party service platform,

which will help users find the vehicle-related services such as vehicle charging post to charge and other maintenance services just like Figure 1 shows.

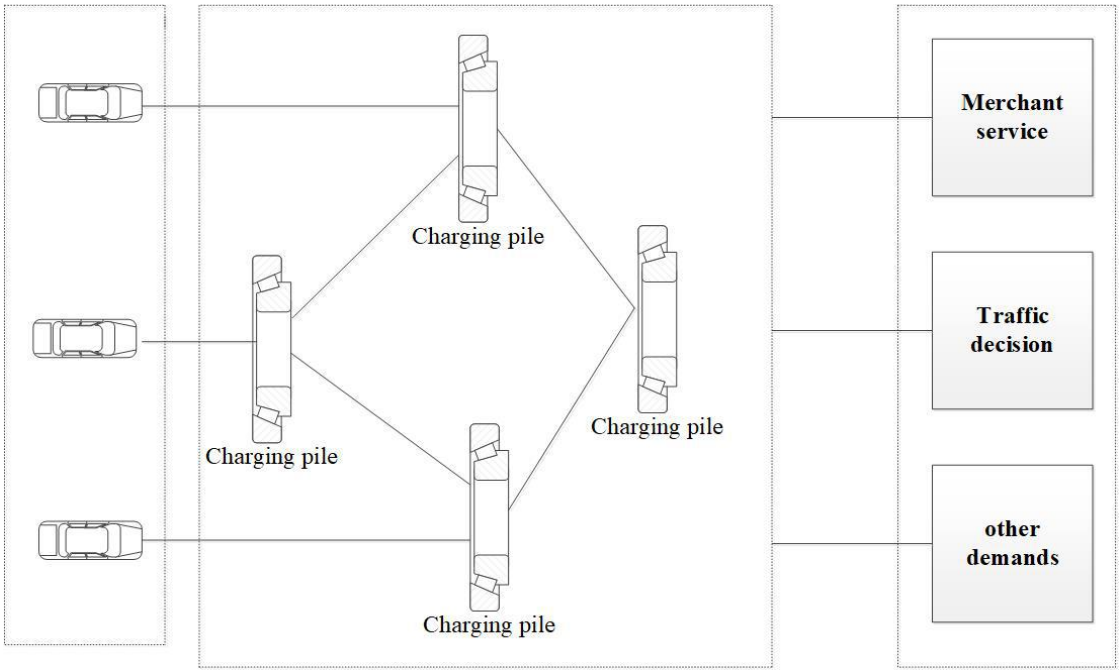

Figure 1: FIOV architecture overall overview.

3.2. FIOV Model

In the FIOV model, the vehicles or their infrastructures form the nodes. When a vehicle joins the blockchain network, the vehicles will record the hash index value of the current blockchain information, the real data is still local for users, which can be achieved through IPFS[13]. If a user needs to browse the data of other users, they need to get confirmation from the data owner. Certainly, some kind users can also share useful data for free to improve the driving behavior of other users. For instance,We can filter the important data collected by the vehicle sensor and store it in the node:

Table 1: Vehicle node data

Hash	Timestamp	who	Data
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#

Users can choose to share this data into different clouds for data analysis just like Figure 2 shows.

We use public key encryption algorithm to protect the privacy of each communication[14],[15]. In addition, we can learn from the privacy calculations in the blockchain, such as using zero-knowledge proof[16], secure multi-party computing[17] and other knowledge while designing a module that protects the privacy of user data. Protecting user privacy has always been a hot topic. In FIOV systems, we are more inclined to implement a pluggable privacy mechanism, because privacy

protection is dynamically developed, and we want to strike a balance between performance and efficiency.

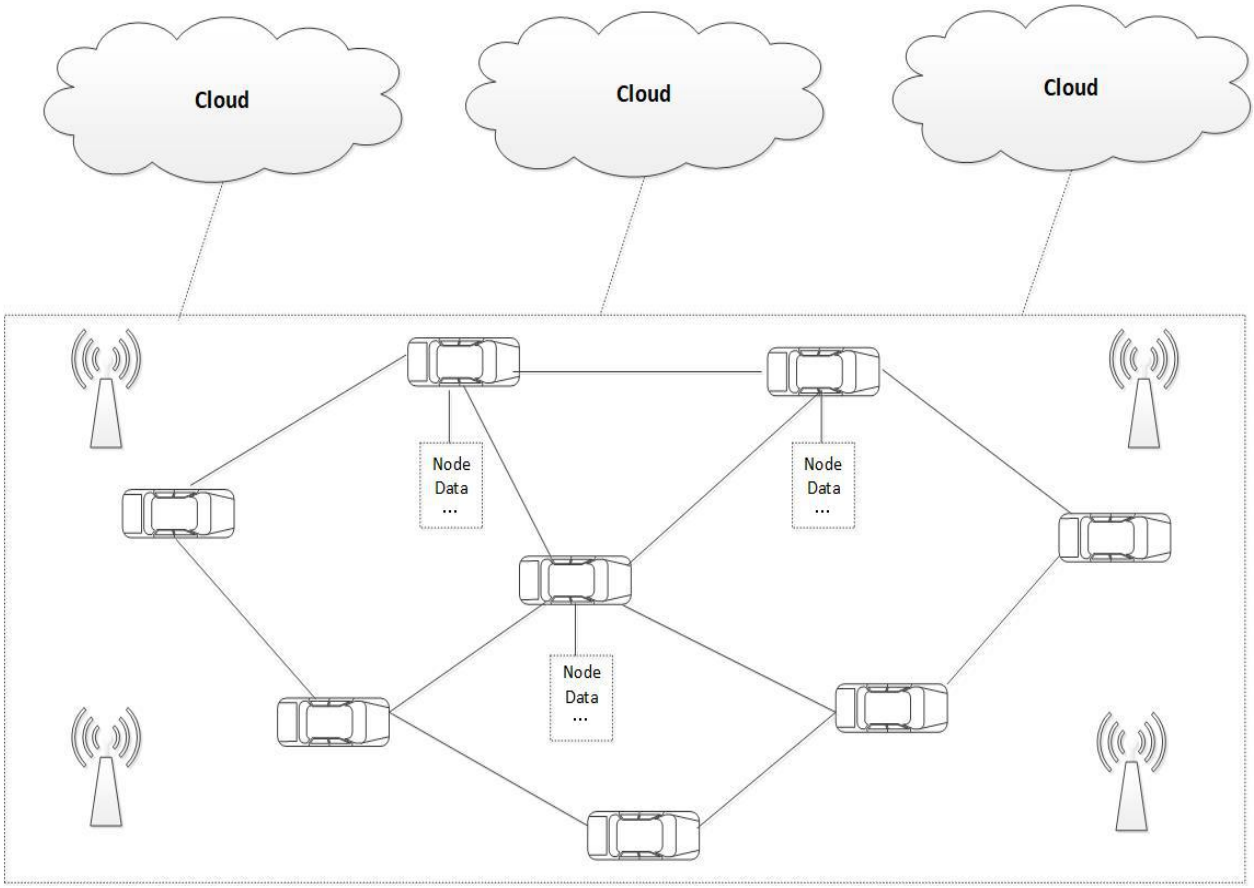

Figure 2: The proposed FIOV application scenario.

3.3. FIOV Level

We proposed the seven levels of FIOV. It is based on the blockchain technology that can be used to complete the empowerment of the vehicle. It is also a breakdown of the specific scenarios and operations. I think the FIOV is just a exploration of development of future IOV, because the actual development is definitely beyond the current belief. We make a simple analysis of these levels:

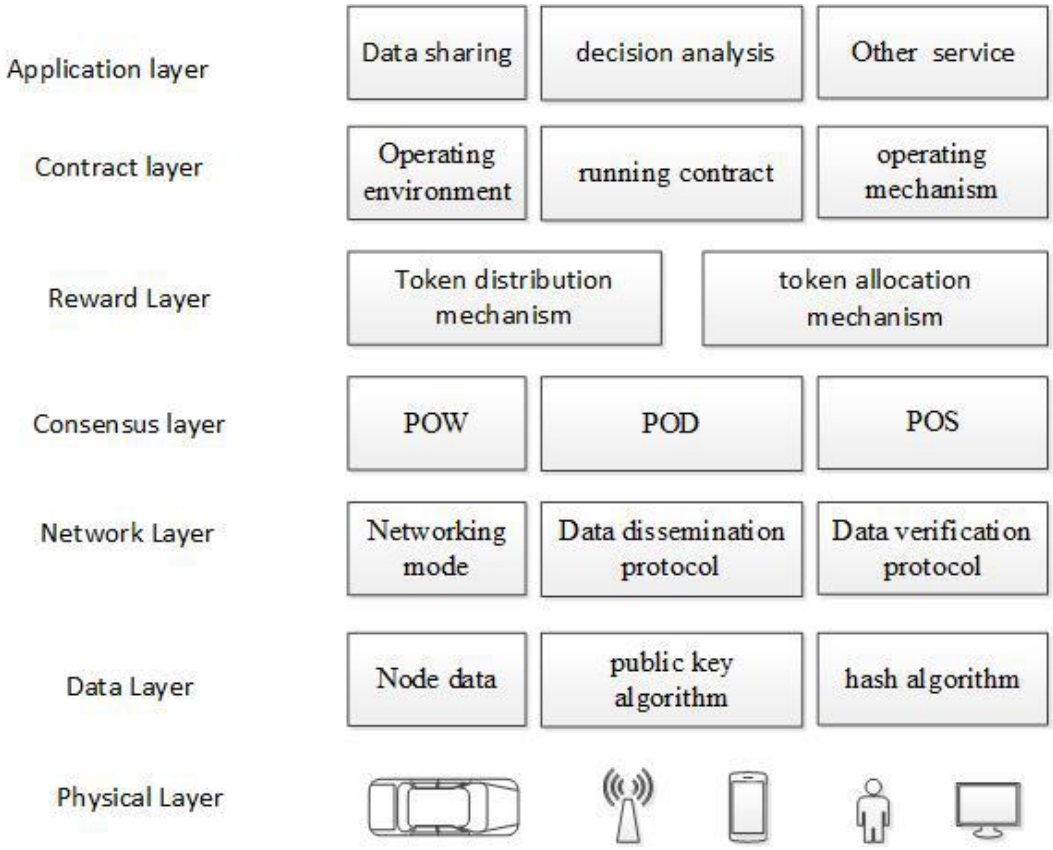

Figure 3: Seven-layer model of FIOV.

Physical layer: This layer represents the basic entity that constitutes FIOV, including the content covered in the current IOV, such as vehicles, intelligent terminals, communication facilities, etc. This layer is the basis of FIOV, and the vehicle nodes carried by these infrastructures are a huge network of information communication to promote mutual communication between people and vehicles, and provide a source of data for high-tech IOV development.

Data layer: The data stored layer contains the node data , related mathematical encryption algorithms used and hash algorithms to protect the user's private data.

Network layer: Nodes communicate through a P2P network. This layer represents the node networking mode and data propagation protocol, and the mechanism for verifying data in nodes. Once the data recorded on the blockchain is verified, it cannot be changed.

Consensus layer: This layer refers to the problem of reaching consensus among nodes. The legitimacy of data needs to be confirmed by some nodes. Moreover, different stakeholders also need a consensus mechanism to reconcile and achieve a win-win goal. The consensus mechanism can be chosen for different situations, such as POD which means a proof of users driving in FIOV .

Incentive layer: This layer represents a system of incentives. The tokens issued by the corresponding part of the platform are rewarded to useful data upload such as user behavior, driving safety behavior and so on. Giving appropriate incentives can effectively motivate users to participate in the construction and maintenance of the entire network.

Contract layer: The contract layer represents the user's easy-to-program environment for specific operations. For this level of users, smart contracts can be combined with many current life scenarios to interact. At the same time, the contract can also guarantee the security and reliability of the transaction to a certain extent.

Application layer: The application layer represents the various services and applications that FIOV can access. Because of the Internet of Everything, FIOV is not an isolated island. Through this layer, users in FIOV can use various services quickly and easily.

4. Conclusions

At present, the IOV is becoming an hit field of intense research, but it also has some problems, such as user data privacy protection, lacking of unified management and operation, etc. The emergence of blockchain technology can greatly improve the existing IOV. To this end, we put forward the concept of FIOV , which can form the vehicle terminal or vehicle infrastructure nodes to build blockchain. At the same time, FIOV can access third-party services, which is of great significance for ensuring user data security and improving smart city traffic management. By explaining the seven levels of FIOV, we know that blockchain technology mainly contributes to improve the quality of current IOV,addressing security, efficiency and application issues based on the nature of the data in this field. In addition, it also creates value for user data,which is the original destination of FIOV.Of course, FIOV 's proposal is to make the IOV more open, secure and reliable. It may be an expectation now, but it will become a reality in the near future.

References

[1] Atzori L,Iera A, Morabito G. The Internet of things: Asurvey. (2010) Comput Netw 54(15):2787–2805.

[2] Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park. (2017) Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City. JInf Process Syst. Vol.13, No.1, p.184~195.

[3] Yu Zhang, JiangtaoWen. (2016) The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Netw. Appl.

[4] Joan Antoni Donet Donet, Cristina P_erez-Sol_a, and Jordi Herrera-Joancomart. (2014) The Bitcoin P2P network. researchgate Conference.

[5] DAG. https://en.wikipedia.org/wiki/Directed_acyclic_graph.

[6] IOTA. https://www.iota.org/

[7] Byteball. https://obyte.org/

[8] Satoshi Nakomoto. (2009) Bitcoin: A Peer-to-Peer Electronic Cash System, BITCOIN.ORG 3.

[9] Morteza Babazadeh Shareh. (2020) Corrigendum to Preventing Sybil Attacks in P2P File Sharing Networks Based on the Evolutionary Game Model. Inf. Sci. 509: 317.

[10] Ethan Heilman, Alison Kendler, Aviv Zohar, et al. (2015) Eclipse Attacks on Bitcoin's Peer-to-Peer Network. USENIX Security Symposium. Washington, D.C,August 12–14, 2015 , ISBN 978-1-931971-232.

[11] S. Olariu, M. Eltoweissy, and M. Younis. (2010) Toward autonomous vehicular clouds. ICST Trans. Mobile Commun. Comput. vol. 11, no. 7–9, pp. 1–11.

[12] C. Wang, Q. Wang, K. Ren, and W. Lou. (2010) Privacy-preserving public auditing for data storage security in cloud computing. Proc. IEEE INFOCOM, pp. 1–9.

[13] IPFS. https://en.wikipedia.org/wiki/InterPlanetary_File_System.

[14] D. Singh, M. Singh, I. Singh, H. J. Lee. (2015) Secure and reliable cloud networks for smart transportation services. International Conference on Advanced Communication Technology (ICACT), p. 358-362.

[15] B. Fleming. Smarter and safer vehicles. (2012) IEEE Vehicular Technology Magazine, vol. 7, no. 2, pp. 4-9.

[16] Zero-knowledge proof. https://en.wikipedia.org/wiki/Zero-knowledge_proof.

[17] Chuan Zhao, Shengnan Zhao, Minghao Zhao, et al. Secure Multi-Party Computation: Theory, practice and applications. (2019) Inf. Sci. 509:p. 357-372.