A Blockchain Infrastructure Supporting Multi-scenario Use for Smart IoV Community

TECHNICAL WHITEPAPER

Version 2.0 Hopes

July, 2019

目录

Abstract

Bitcoin, Ethereum(ETH), and *Hyperledger*，which have been successfully applied in value transfer field, have opened the door to blockchain technology for us. Though different transaction performance problems have been gradually exposed with the popularity of blockchain, people have been aggressively exploring various blockchain applications in other fields, such as anti-counterfeiting and traceability, and Internet of Things and so on. People have been developing different blockchain underlying systems to achieve their specific functions. *BitShares* and *Steemit* are two representative blockchain system applications of decentralized exchange and the decentralized social media platform. However, a resulting situation would be that each application formed an independent blockchain with no communication interaction among them. This is very similar to the early Internet situation: different organizations set up their own private networks, but none of them were connected together to build up an 'Internet'. The performance of the blockchain infrastructure and the application extension have caused widespread concern in the blockchain community. Ethereum 2.0 research uses fragmentation technology and PoS consensus algorithm to solve transaction performance problems. Polkadot researches multi-chain technology to implement multi-chain based application development and implements cross-chain technology to support interaction between applications.

IOV Blockchain, as the pioneer to apply blockchain technology to the Internet of Vehicle (hereinafter referred to as IoV) field, actively explores blockchain application in the vertical fields of automotive user communities, such as social, consumption and safety, relying on a mature car user community. *IOV Blockchain* understands well that its application scenario is derived from a mature automotive users' community, which is developed and linked by Internet technology. Therefore, *IOV Blockchain*'s core purpose has been determined as building up a blockchain infrastructure supporting multiple IoV applications, multi-chain expansion and interaction, under the consideration of adopting blockchain technology to community. On this IoV blockchain infrastructure, the community users would be able to participate in different layers or applications on the infrastructure chain according to their own

characteristics and hobbies.

IOV Blockchain has performed various comprehensive studies on existing blockchain infrastructures, from which the essence of blockchain is an open and credible way to generate and store data, which can be jointly generated and stored by multiple parties, and all parties reach an agreement through consensus algorithms. It has been concluded to be writing transaction data (including storage and script code) into the block and adding it into the chain through a trusted and secure data generation method, and verifying the authenticity and integrity of transactions through cryptographic algorithms (signatures and hashes). There are different classes of transaction data in the blockchain system, such as UTXO adopted by *Bitcoin* and account transaction data adopted by *Ethereum*, but there is no tag or support for multiple transaction data classes in the same blockchain system. In order to solve this problem, *IOV Blockchain* proposed an innovative classification of blockchain transaction data and layered the block chain data protocol. The classification of transaction data could enable the blockchain infrastructure to adopt different block consensus mechanisms and generate different single chains according to different transactions. Therefore, *IOV Blockchain* is a multi-chain blockchain infrastructure. Different chains could support different IoV applications, and users could choose the applications they're interested in to synchronize the corresponding blockchain data. The layering of blockchain data protocol allows a cross-chain communication within multiple chains through different layers of blockchain data. This provides the blockchain infrastructure a great flexibility to adapt appropriate optimization according to the application scenario, a solution to the blockchain trilemma (only two of decentralization, scalability and security could be achieved at the same time). Meanwhile, the essential nature of the blockchain open database will support the IOV Blockchain to be managed and co-constructed by all parties in the automotive verticals.

1.*IOV Blockchain*'s Implementation and Vision

IOV Blockchain is a blockchain underlying infrastructure that provides the foundation for the smart Internet of Vehicle (hereinafter referred to as IoV) industry. The infrastructure would provide the automotive industry and customers with decentralized application services and extend to travel-related multi-scenario applications. Therefore, the technical architecture goal of *IOV Blockchain* is to support multi-application scenarios in the IoV field. This technical architecture adopts a multi-chain data organization and a flexible MDPoS(Multi-Delegated Proof of Stake) consensus algorithm mechanism. For the former, *IOV Blockchain* proposes a classification of the blockchain transaction data. This classification could enable the blockchain infrastructure to adopt different block consensus mechanisms according to different transactions, and the same type of transaction data would form a relatively independent application chain. For the later, the corresponding consensus algorithm could be customized as different application chain.

Insufficient performance issue always exists in current blockchain systems, such as *Bitcoin* and *Ethereum*. *Bitcoin*'s transaction throughput is only about 7TPS, Ethernet's transaction throughput is only 15TPS, EOS's actual transaction throughput is about 4000TPS, and Visa's transaction throughput could reach 24000TPS.Vitalik Buterin pointed out that *blockchains could only at most have two of these three properties: decentralization, scalability and security* [1]. Decentralization and security are the core features of blockchain. Therefore, many blockchain technologies are currently working on how to maximize scalability, including parallel processing of transactions, consensus algorithm based on non-Proof-of-Work (hereinafter referred to as PoW), side chain, Polkadot, sharding, lightning network, Raiden network, Plasma, etc. EOS system claims to realize the parallel processing of transactions by multiple CPUs, so as to reach the million-level TPS [2]. However, EOS's current TPS is proved to be only several thousand. EOS did not reveal much about how to implement the parallel processing.

IOV Blockchain organizes the data to build different application chains by classifying the transactions. This allows a parallel processing on different transaction classes and quicker block generation. Therefore, *IOV Blockchain* could significantly improve transaction throughput and achieve the purpose of supporting large-scale application. What's more, *IOV Blockchain* would adopt Layer 3 Protocol: on-chain layer, off-chain layer and cross-chain layer. The cross-chain layer could open up the interaction between different application chains and between the application chain and the parent chain. The off-chain layer could move some intermediate transaction processes off-chain and only record the final state on the chain, so as to improve the transaction throughput of *IOV Blockchain*.

Although the as PoW mechanism improves the system security by CPU-bound to prevent the Sybil Attack, this algorithm is very resource-consuming and inefficient. In order to improve scalability, Daniel Larimer adopts DPOS consensus plugin[3] in *BitShares*, *Steemit* and *EOS*. Ethereum is also stepping up the implementation of the POS consensus plugin - Casper[4]. Both DPOS and POS algorithms are trusted verification nodes voted by stakeholders, so the block generation rate has been greatly improved, for example, EOS could generate one block every 500 milliseconds. IOTA adopts directed acyclic graph (hereinafter referred to as DAG) as consensus mechanism. DAG could greatly improve the parallel processing capacity of blockchain, because blockchain could be generated by multiple forks in parallel [5] under this mechanism.

IOV Blockchain follows DPOS on which several improvements have been made. *IOV Blockchain* not only adopts the DPOS on the parent chain, but also provides a customizable DPOS in the application chain, which we call MDPoS(Multi-Delegated Proof of Stake). *IOV Blockchain* blockchain infrastructure adopts a specially targeted technical solution to the issue in the field of IoV multi-application scenarios. In the meantime, *IOV Blockchain* guarantees great autonomy on its application layer to support app developers deploying application chain token, electing application chain miners, rewarding application developers, and constructing application communities, etc. Therefore, each application could be a relatively independent application ecological community.

IOV token was labeled "vehicle " by Etherscan as a recognition of the good performance of entity scenario application and the huge number of IOV holders. IOV ranks first in terms of basic Chain development, user scale and efficiency of project landing.

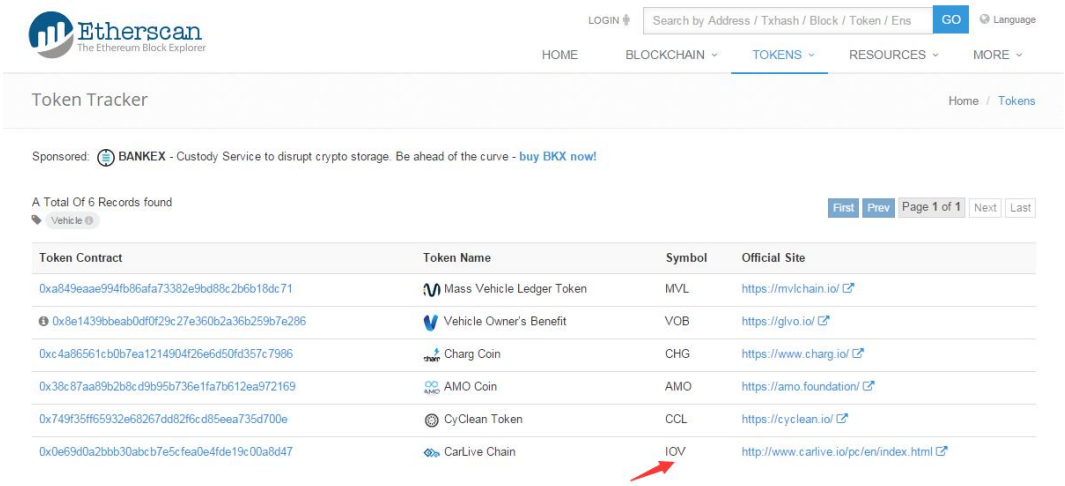

Fig. 1. IOV token was labeled "vehicle " by Etherscan

The development of *IOV Blockchain* would be divided into five following major technical development stages:

- ✧ **Newborn phase:** *IOV Blockchain* Foundation Infrastructure Chain supporting multi-application Scenarios of IoV;
- ✧ **Hopes phase:** Providing the toolkit and application framework for IoV decentralized applications development, such as IoV data exchange, personal digital identity, sharing economy, etc.;
- ✧ **Discovery phase:** Enrich the *IOV Blockchain* application framework, better support cross-application interaction on the basic chain, extend and access to more smart IoV ecological partners;
- ✧ **Beyond phase:** Achieve the Layer 3 Protocol model of on-chain layer, off-chain layer and cross-chain layer, in order to support off-chain transactions, off-chain storage and cross-chain transactions;
- ✧ **Freedom phase:** An independent and autonomous IoV community

ecosystem basing on *IOV Blockchain* is built, where vehicles provide the most convenient service for people, while people provide the safest mechanism for vehicles.

2. *IOV Blockchain* Technology Architecture

2.1 *IOV Blockchain* Technology Architecture Block Diagram

IOV Blockchain's technical architecture is shown as follows:

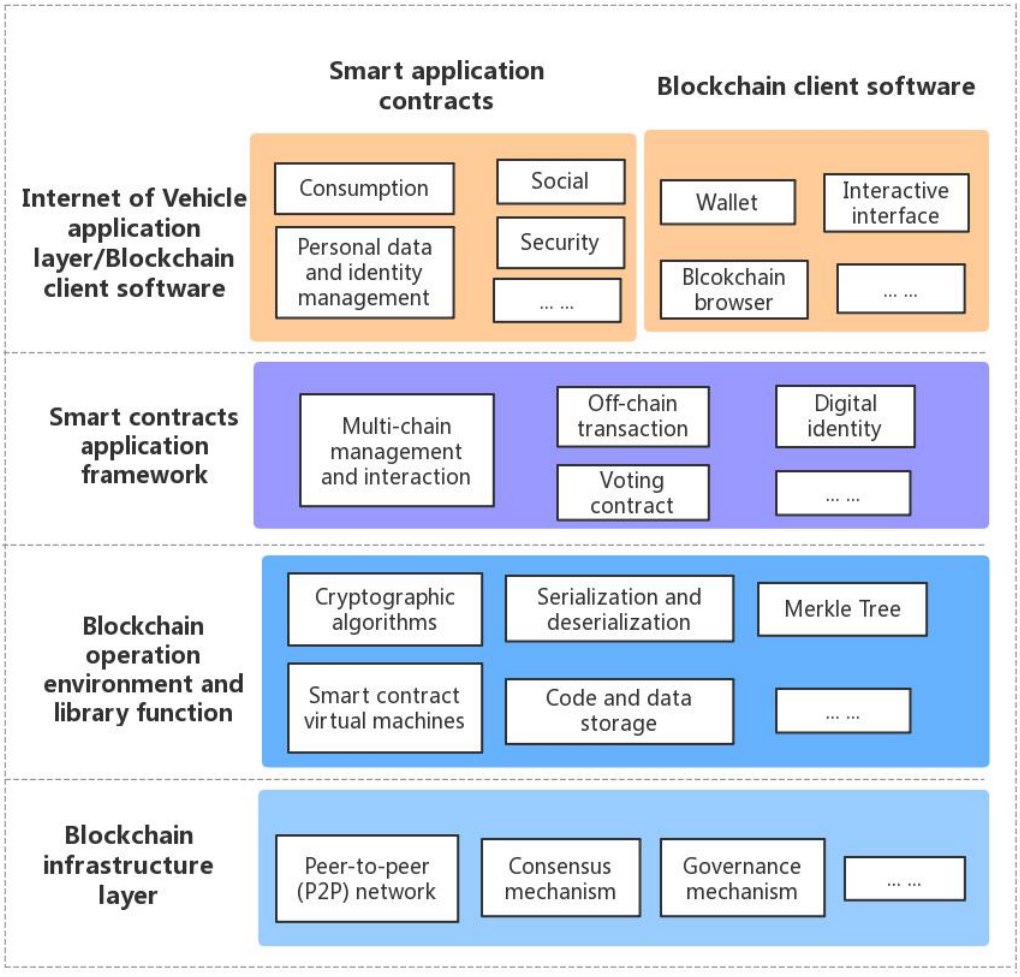

Fig. 2. *IOV Blockchain* Technology Architecture Block Diagram

IOV Blockchain adopts a four-layer architecture, listed from bottom to top: **blockchain infrastructure layer, blockchain operating environment and library function layer, application framework layer, and IoV application layer/blockchain app.**

- **Blockchain infrastructure layer:** this layer provides the blockchain system its infrastructure underlying technology, such as the decentralized network connected by *IOV Blockchain* operation nodes through peer-to-peer (hereinafter referred to as P2P) network, the distributed node data consistency and tamper-proofing guaranteed by blocks packed with transactions submitted to the system by consensus mechanism. The governance mechanism provides the economic incentives for the decentralized network, also with improvement proposal and its coordinated implementation.

- **Blockchain operating environment and library function layer:** this layer provides virtual machine operating environment, storage environment and various function libraries for blockchain application foundation.

- **Application framework layer:** this layer is a framework application added supporting a series of blockchain system basic functions, including: multi-chain management and interaction, off-chain transaction, digital identity, voting contracts, etc. Multi-chain management and interaction framework manages different application chains; off-chain transaction framework aims at writing off-chain transaction results back onto the chain; digital identity framework provides digital identity management and application functions to the blockchain system users; voting contracts framework is used for user voting such as delegates election and so on.

- **IoV application layer/blockchain app:** this layer includes application development, and blockchain front-end (including blockchain browser, and wallet) for user interaction with blockchain back-end. The users could query to and interact with the blockchain system through wallet, interaction

terminals, blockchain browser. In the meantime, the users could also develop and setup specific applications.

2.2 *IOV Blockchain* Multi-chain Architecture

IOV Blockchain classifies the basic data units (transactions) in the blockchain from the perspective of application, so that transactions of different applications could be processed in parallel. Different chains are generated for different applications, which could be called "application chains". In order to provide basic services for different application chains, the *IOV Blockchain* infrastructure would form a "infrastructure chain". A multi-chain architecture would be formed by the infrastructure chain and application chains in *IOV Blockchain*. The infrastructure chain provides an operating environment for the decentralized application chains. Users could develop decentralized applications based on the infrastructure chain, and store application codes on the infrastructure chain. A separate application chain with application transactions and data stat would be generated.

2.2.1 Transactions Classification on *IOV Blockchain*

Transaction Data Overview of Typical Blockchain System

A transaction in a blockchain could be regarded as the minimum granularity data in the blockchain, similar to a data packet in a communication protocol. According to the *Ethereum White Paper*, the blockchain could be abstracted into a state machine, and the transaction is similar to its state transition function. As a function of state transition, transactions are required to meet the following rules:

1. Their orders must be defined and distinct;

2. The transformed state should be within the normative space.

The transaction data structure of *Bitcoin* consists of the input UTXO and the output UTXO. The transactions containing the same input UTXO would be pointed through the hash value. The specific UTXO in the transaction could be pointed through the index. The user then adds an unlock script to generate a UTXO. The

output UTXO would contain a lock script, and only the receiver account could use the private key to generate an unlock script. Therefore, the *Bitcoin* transaction, as a state transition function, has a characteristic that the function directly forms a transaction between a part of the “before” state and a part of the “after” state. Therefore, *Bitcoin* transactions shouldn’t use the same “before UTXO” for more than one transaction. This is the famous "double spend" problem. The order is naturally defined for *Bitcoin* and other similar transaction structures, which means the generation of transactions relies on the existing UTXO.

The transaction data model of *Ethereum* is very different from the one of *Bitcoin*. *Bitcoin* adopts a record-based transaction model, while the *Ethereum* adopts an account-based one. The *Ethereum* stores the status of users or contract accounts as on-chain data. The data recorded in the block header includes not only the Merkle Tree root hash of the transaction, but also the Merkle Patricia Trie root hash of the account state (including the user and the contract account), and the Merkle Tree root hash of a transaction receipt.

Transaction Data Classification on *IOV Blockchain*

IOV Blockchain classifies transactions, and distinguishes them by two tag bits: "transaction class number" and " transaction model", which would be signed by the sender's private key to avoid tampering. The blockchain nodes could identify these two tag bits in the transaction and pack the same class of transactions onto the same application chain. Therefore, transactions of different classes would be written into different application chains.

Such criteria could naturally classify the transactions into different application type of the corresponding blockchain. *IOV Blockchain* could classify transactions to support different applications in the IoV community. Such an application-level transaction classification would enable nodes to process different classes of transactions in parallel. In the meantime, the users may choose to deal with only transactions in their interest. For those they’re not interested, they could just simply transfer messages. Therefore, the concept of transaction classification could improve the overall performance of *IOV Blockchain*, and could support more nodes to join the

transaction applications they are interested in. The higher and higher hardware entry threshold caused by blockchain data burst would be no longer a limitation.

Transaction class no.	Transaction model	From	To	Data/Value	Key signature

Fig. 3. Transaction data structure of classification tag

In the meantime, the "transaction model" could help *IOV Blockchain* adopt various transaction data models, such as *Bitcoin* UTXO transactions, *Ethereum* account transactions, etc. In this way, a more appropriate UTXO transaction is available to form a single blockchain data for value transfer application scenario. For other application scenarios, *Ethereum* could be a good choice as it could support the Turing-complete smart contract as transaction model. Therefore, transaction classification could provide better and more flexible support regarding to different application scenarios. It's the most suitable solution to satisfy different application needs in the CarLive IoV vertical community.

2.2.2 *IOV Blockchain* Multi-chain Architecture

The transaction data classification allows the block nodes to pack different classes of transaction data into corresponding application chains. Each chain would be used to organize the transaction data under the same application. Therefore, multiple application chains would be generated for different classes of transaction data accordingly. This could be compared to different network applications on the Internet.

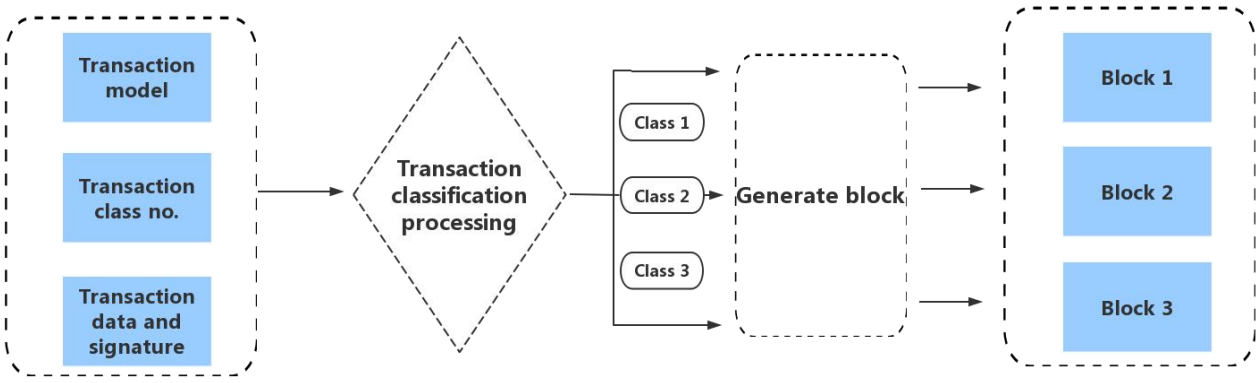

Fig. 4. *IOV Blockchain* multi-chain architecture Block diagram

For cross-chain communication transactions, we adopt a new layer of single chain to record. Its structure is shown as following figure:

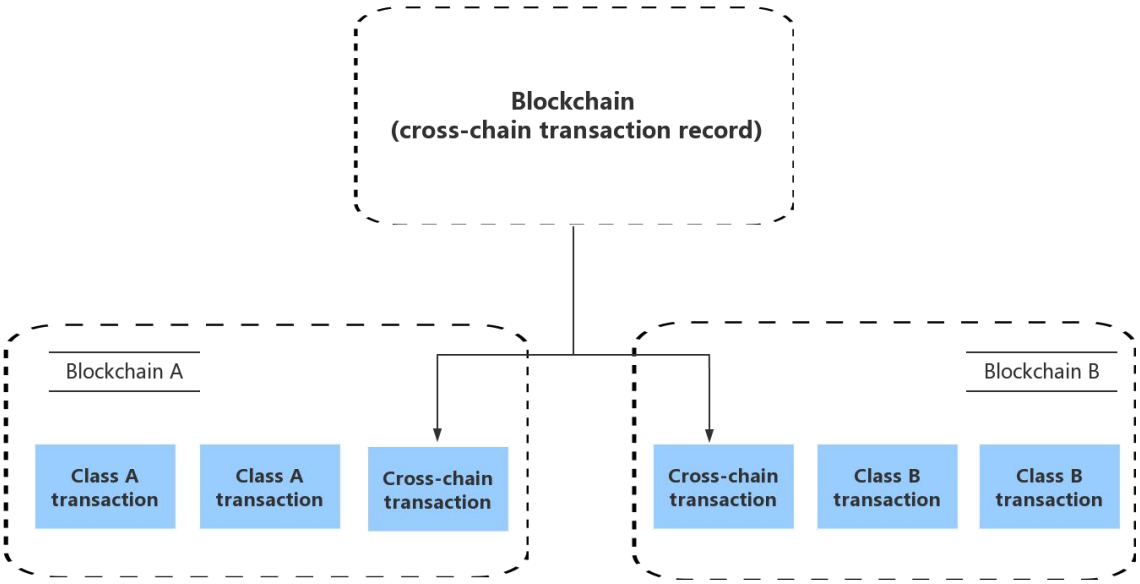

Fig. 5. *IOV Blockchain* Cross-Chain Interaction Architecture Block Diagram

By maintaining a single chain that records cross-chain transaction data, the communication and interaction among various application chains could be supported. We could abstract this multi-chain hierarchical architecture into several state machines classified by applications, and the state interactions among these machines pass through a higher level state machine maintainer. The state machine abstracted from the *IOV Blockchain* multi-chain architecture is shown as following figure. Each

single chain could be abstracted into an independent state switch. When the same class of transactions appears, the independent state could switch itself to meet the normative by adjusting the state. When there is a cross-chain transaction, the state switch on the original application layer chain could not independently adjust the state meeting with the normative. In this case, the cross-chain transaction state machine at a higher layer could record and send this cross-chain transaction state to the receiver chain state machine to change its corresponding state, and adjust its own state.

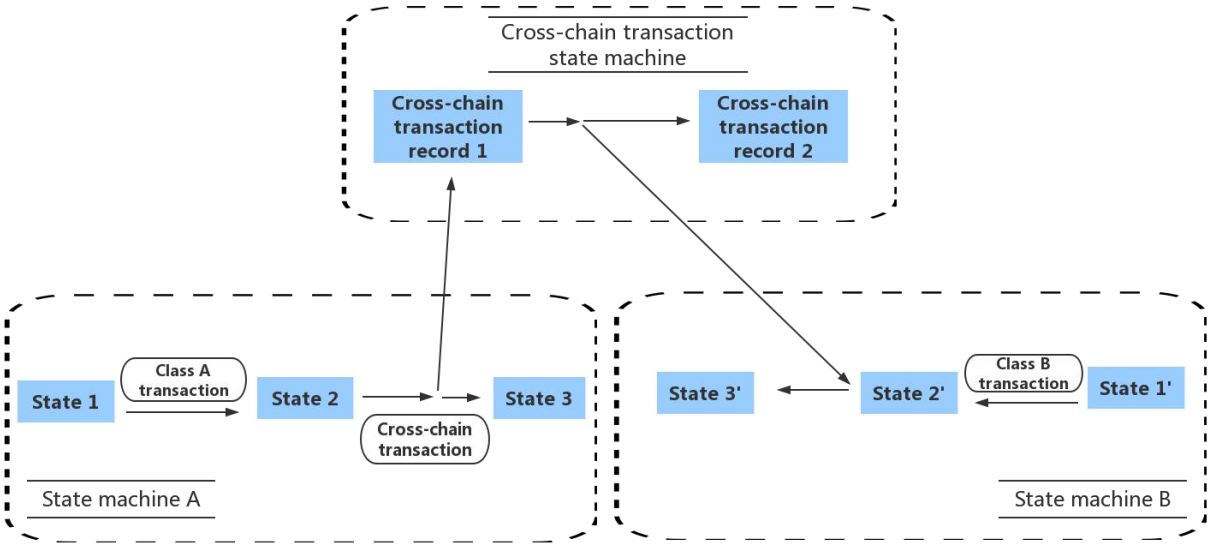

Fig. 6. State Machine in Cross-Chain Transactions

The cross-chain transaction state machine generates and maintains blocks through a specific validator. The *IOV Blockchain* infrastructure chain provides incentives to the Validator of the cross-chain transaction state machine.

2.3 *IOV Blockchain's* Layer 3 Protocol

In addition to the data organization characteristics of layer 2 protocol tech-chain and application chain, another technical feature of *IOV Blockchain* is the Layer 3 Protocol: 1st layer is the on-chain layer, the core foundation; 2nd layer is the off-chain layer, supporting off-chain transactions; 3rd layer is the cross-chain layer, supporting cross-chain transactions. On-chain layer is a protocol model used to record blockchain data and code. It provides an infrastructure for decentralized application

implementation and scalability on off-chain layer and cross-chain layer. *Bitcoin* and *Ethereum* could be considered as a type of on-chain layer. Off-chain layer is based on the applications deployed on the on-chain layer, with the role to move a large number of microtransactions between two traders to off-chain, and write the final settlement to on-chain. Cross-chain layer is an interactive validation mechanism among different application chains and between application chains and infrastructure chains, to validate the effectiveness of the transactions on other chains.

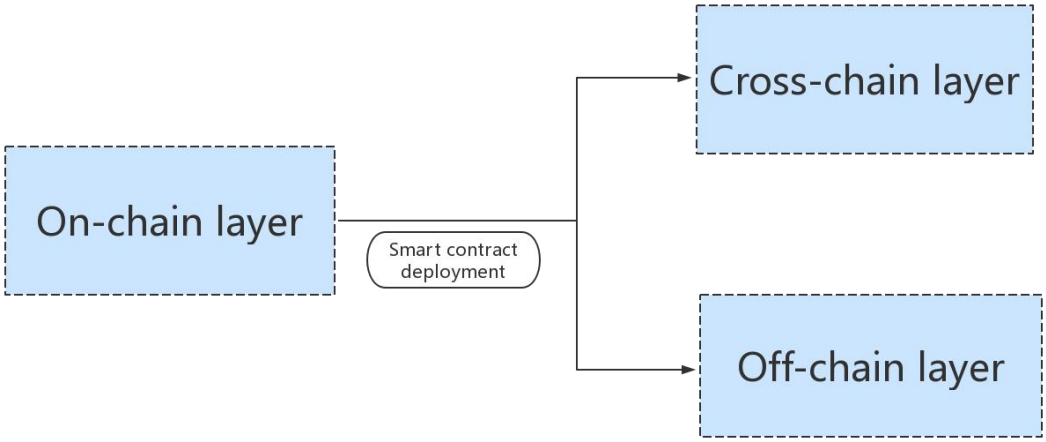

Fig. 7. *IOV Blockchain*'s Layer 3 Protocol

Such layer 3 protocol of on-chain, off-chain, and cross-chain is customized according to blockchain development trend. In summary, *IOV Blockchain* adopted the optimal top-level design proposal since the beginning.

2.4 *IOV Blockchain* Modularized Customization Consensus Algorithm

IOV Blockchain's block data protocol format is established according to transaction classification and hierarchical multi-chain architecture. What needs to be considered is how to generate block data and maintain data consistency and what kind of consensus algorithm is used to generate block data?

IOV Blockchain provides a consensus algorithm library, which could help developer configure different single-chain accordingly. Under this condition, PoW, PoS, DPoS, BFT and other algorithms could be selected for different application

single chain according to requirements. Users could also configure DPoS for voting. To run the MDPoS(Multi-Delegated Proof of Stake) algorithm, stakeholders vote a certain number of delegates, who take turns to generate blocks. The generation of blocks requires the delegates to invest sufficient hardware resources and security attributes. The blockchain offers them certain incentives as compensation. The system also punishes delegates who have violated rules.

Here is a detailed description of the customized MDPoS (Multi-Delegated Proof of Stake) voting algorithm. *IOV Blockchain*'s MDPoS algorithm needs stakeholders to vote delegates. Here, the corresponding relation between the rights owned by the stakeholders and the number of votes could be configured. It is common that the number of votes increases linearly with the rights owned by the rights holder. *IOV Blockchain* supports that users to customize various relation between the rights owned by various stakeholders and the corresponding votes. The only limitation is that the correspondence should be non-degressive. The following are some common relations between rights and votes:

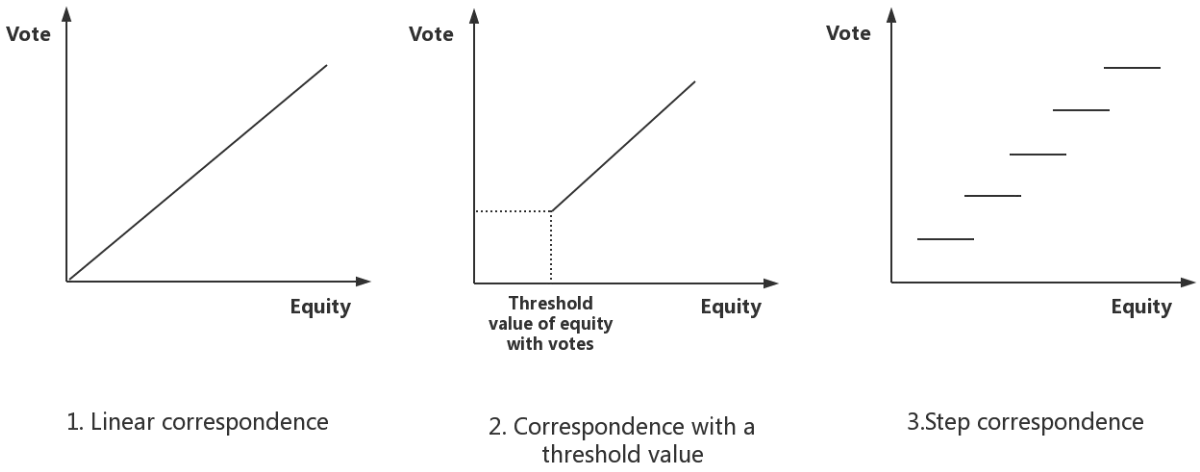

Fig. 8. Several Common Relations between Rights and Number of Votes

The corresponding function relations are as follows:

1. Linear correspondence:

$$Quota_{tickets} = \alpha \cdot Quota_{stake}$$

2. Corresponding relation with threshold:

$$Quota_{tickets} = \begin{cases} 0, When\ Quota_{stake} < Threshold \\ \alpha \cdot Quota_{stake},\ When\ Quota_{stake} \geq Threshold \end{cases}$$

3. Ladder correspondence:

$$Quota_{tickets} = n \cdot \mathrm{C}, n \cdot T \leq Quota_{stake} \leq\ (n+1) \cdot T.$$

Where C and T are constants.

IOV Blockchain Infrastructure Chain is voted by MDPoS miners nodes organized by AUH Foundation, and these miner nodes are elected by IOV Token holders. The application chain could choose its own consensus algorithm and mechanism, and could organize its own miner's election.

Combines the multi-chain architecture with the MDPoS consensus algorithm, IOV Blockchain has significantly improved transaction speed. Its infrastructure chain's transaction throughput can reach 900 TPS . Meanwhile, the expansion of the application chain will not affect the transaction speed of the infrastructure chain. And as long as the hardware conditions allow, the overall transaction throughput of the system will increase as the application chain increases.

3. *IOV Blockchain's* Governance Mechanism

IOV Blockchain's goal is to build a blockchain infrastructure for tens of millions of users, and to construct a decentralized and trusted community and ecology in the field of automotive consumption. *IOV Blockchain*, as a decentralized IoV blockchain infrastructure, would build a community ecology including miners, developers, token holders, community users and other different roles.

IOV Blockchain adopts the technology architecture of infrastructure chain+application chain in terms of chain layer architecture. The infrastructure chain has the roles of infrastructure chain miner, infrastructure chain developer, token holder, community user, etc. The application chain is a data chain deployed by

developers with smart contracts on the infrastructure chain for specific application scenarios. It's a common ledger supporting the corresponding applications. The application chain generally includes application chain miners, application developers, application token holders, application users and other roles. Application chains could form their own application communities.

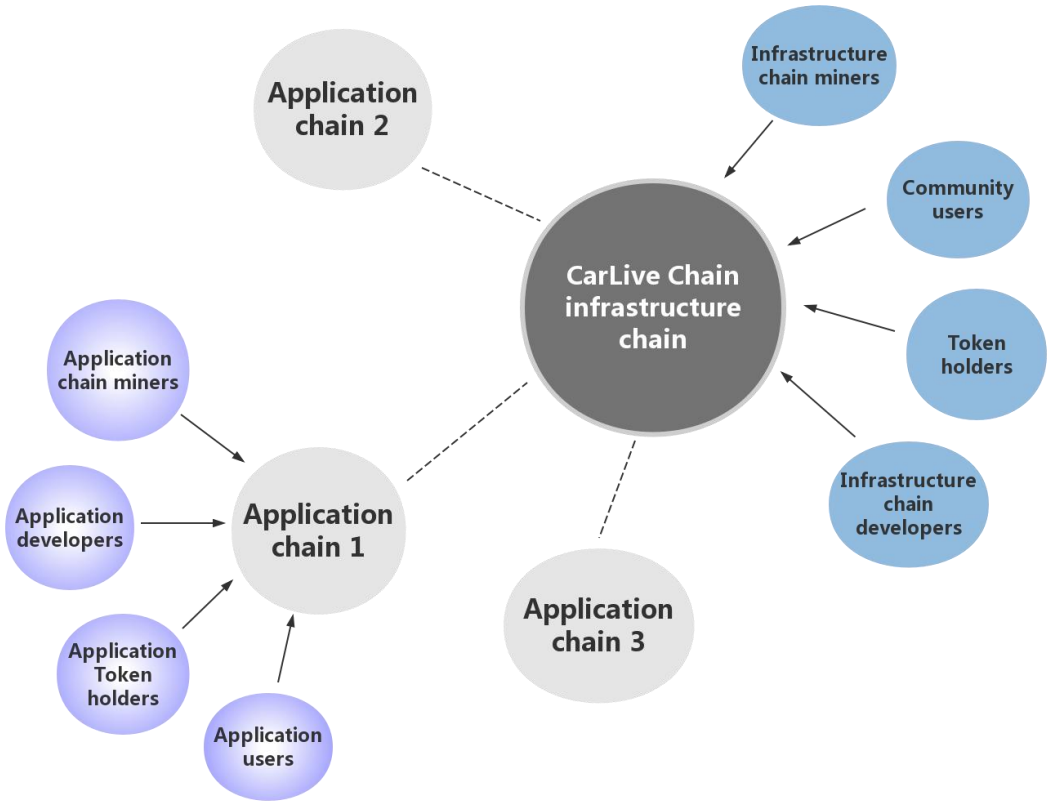

Fig. 9. Different Roles in *IOV Blockchain* Infrastructure Chain and Application Chain

IOV Blockchain's governance mainly solves three problems:

1. The project's start-up and promotion;

2. Network incentive;

3. Protocol update and upgrade.

3.1 AUH Foundation

AUH Foundation is a non-profit organization registered in Singapore and is

responsible for the operation and supervision of the *IOV Blockchain* Project. Its mission is to promote the IoV blockchain R&D, promote and manage community consensus, facilitate the establishment and application of a global ecosystem of the IoV block chain, and to gradually return the community autonomy to community users.

The AUH Foundation established an international technical advisory committee for *IOV Blockchain* in the early stage, to supervise and guide the infrastructure and application research and development, as well as the financial market operation. A cooperation has been established between the partner of AUH Foundation and internationally renowned law firm, for legal adviser of *IOV Blockchain* Project, including comprehensive legal services for the operation compliance, legal control system design and international legal consultation. In the meantime, AUH Foundation only accepts international compliance users who passed relevant KYC and AML to join the community activities.

3.2 Infrastructure Chain Governance

Every IOV Token holder on *IOV Blockchain* has the right to participate in the decentralized governance of the infrastructure chain. The operation and development direction of the *IOV Blockchain* Ecological Community would be decided by IOV Token holders through negotiation and voting.

3.2.1 IOV Token

IOV Token is the encrypted digital currency of the *IOV Blockchain* infrastructure chain. The role of IOV Token includes the following aspects:

1. Symbol of rights to participate in the governance of the *IOV Blockchain* infrastructure chain;

2. IOV Token are used for community contributors, infrastructure chain miners and infrastructure chain developers' incentives;

3. IOV Token could be used for transfer payment, application deployment and

various transaction fees;

4. Obtaining a certain amount of token distributed by the application chain is considered as dividend rights.

IOV Blockchain has been cooperating with the third-party platform in APAC region to start community contributor incentive. The users could enter the "ecological mine" in the app to get the digital assets value and IOV Token, as long as they participate in social activities (such as sharing live broadcasts, videos, image-text guides, IM communication with users, circle, reward, LBS application, content reading, comments, browsing advertisements, etc.), or start the Internet car and contribute IoV data. Users could also make contributions through *IOV Blockchain*'s car consumption and car information sharing, to generate digital assets, obtain IOV token, with which the value of various services could be exchanged.

The total distribution of IOV Token would be less than 10 billion. 35% of the distribution would be claimed by global blockchain contributor as funds (managed by AUH) for product design, technology development and operation management of IoV blockchain, and the corresponding IOV Token would be locked at the beginning and gradually released in the future; 35% is used for development team and early contributors incentives, and the token assigned to the founding team would be locked and gradually released in the future; the rest 30% would be used to motivate community ecological contributors and infrastructure chain miners. *IOV Blockchain* plans to generate 3 billion IOV Token for community ecological incentives in 10 years.

Fig. 10. IOV Token Allocation Proportion

In terms of implementation, *IOV Blockchain* distributed ERC20 IOV Taken on *Ethereum* at the beginning of the project and attracted more than 1.7 million users. As soon as the *IOV Blockchain* infrastructure chain is deployed, the ERC20 IOV Token would be mapped to the main-net. The relevant accounts state would be written correctly and precisely into the Genesis block of *IOV Blockchain* infrastructure chain.

3.2.2 Infrastructure Chain Miners

The infrastructure chain adopts *IOV Blockchain* MDPoS (Multi-Delegated Proof of Stake) as consensus algorithm. 21 super-peers are involved to generate blocks,all of the 21 are voted by IOV Token holders. The infrastructure chain would periodically count the voting results, and the 21 nodes with the highest votes are elected as the super-peers. In addition, a certain number of other top nodes out of top 21 would be

set as backup block producers. In this case, the block producer is regularly adjusted according to dynamic voting result.

The AUH Foundation would propose and review the entry threshold and election criteria for candidate nodes. Infrastructure chain miner node candidates should meet the following basic requirements:

1. The candidates should possess at least one legally established entity ;
2. The candidates should possess at least one node available to be tested by community users.
3. The candidates should possess node operation servers and maintenance technology;
4. To create a miner's node, a certain amount of IOV Token are required to be mortgaged. In case of mortgaged IOV retrieved, the eligibility of the corresponding candidates would be considered as canceled.

As an important part of the IOV ecosystem, super nodes are of great significance to the construction of the ecology and future development. Therefore, in order to ensure that the IOV ecosystem can be properly guided and developed, AUH Foundation have made the following soft requirements for the nodes that participated in the election:

1. The node candidates recognize the IOV values and are interested in promoting the development of IOV ecological construction and blockchain technology to promote industry development;

2. Node candidates are willing to provide pertinent advice for IOV development, contributing and providing resources to IOV projects;

3. The node application is applied by the person or the team in accordance with the principle of voluntary participation. After review by the AUH Foundation, each master node obeys the relevant elimination rules;

4. In order to promote the rapid development of the IOV ecosystem, the

following organizations or individuals will be given priority in the campaign:

a. Partners and community volunteers who have contributed to IOV in the areas of technology research and development, community construction, and operational development;

b. Enterprises, teams or individuals with certain resources including but not limited to technology, community, capital, market, etc.

c. Blockchain, artificial intelligence, big data related development teams.

After successfully being elected as a super node, it is necessary to fulfill the obligations related to maintaining the IOV ecosystem, as follows:

1. Review resources and sites within the IOV system to maintain an orderly development of IOV ecological health;

2. Evaluate the development plan proposed by the developer and promote the community's contribution to IOV;

3. Actively maintain and publicize IOV projects, actively organize or maintain activities such as community Q&A, community governance, online interaction, and expand the influence of IOV community.

Infrastructure miners provides infrastructure such as network, storage and calculation for *IOV Blockchain*. Block producers take turns to generate blocks regularly. 25 IOV reward would be offered every new block produced ,the total block reward consists of a super node reward (61.8%) and a voter reward (38.2%). The unit reward would be halved every two years of new blocks are generated. The first 10 years of rewards are as follows:

1~2 years: 25 IOV per block

3~4 years: 12.5 IOV per block

5~6 years: 6.25 IOV per block

7~8 years: 3.125 IOV per block

9~10 years: 1.5625 IOV per block

Calculated by new block generated every 5 second , the total amount of IOV rewarded in the previous two years: 2*365*24*3600*25/5 = 315,360,000 IOV, the infrastructure has a total of 630,720,000 IOV provided by the AUH Foundation, which deducted from the encourage community eco-contributors and platform miners (30%).

Infrastructure miners could propose and vote for events, including: blockchain dynamic parameters modifications, such as block size, block spacing, etc.; percentage of dividends paid to IOV holders when distributing token by application chain; and agreement improvement, etc.

3.2.3 IOV Token (Hereinafter referred to as IOV) holders

IOV Token holders could vote for miners. Each IOV is considered as one vote. The main-net would be started as soon as more than three super node have been elected. The voting IOV is frozen instead of consumed in the holder's own wallet ,which will not be able to perform normal transaction transfers. It will take 7 days for IOV holders to withdraw the voting IOV in IOV explore and IOV wallet, and the frozen IOV becomes normal transaction status as soon as withdrawal success.If the campaign node or super node retrieves the frozen IOV, it is considered to withdraw from the campaign and they need 7 days to withdraw the corresponding IOV. In that case, the frozen IOV voted by IOV holders who support the nodes will become normal status immediately.

IOV Holders vote for miners to govern their own community ecology,to operate and maintain the main-net, and to decide the future direction of the IOV ecosystem . In order to encourage IOV holders to actively participate in voting to select miners, a certain amount of IOV would be rewarded to IOV Token holders who voted. The total block reward consists of a super node reward (61.8%) and a voter reward (38.2%).

Eg. If the current block reward is 25 IOV per block, super node A currently has a total of 10 million votes(Including 5 million pledges of nodes), of which individual voter B casts 5 million votes, then the reward for each block as below:

Ra = Qa * 25IOV+Ra'= 61.8% * 25 IOV+38.2%*25 IOV*5,000,000/10 ,000,000=20.225 IOV

Rb = Qb *25IOV* Individual Voting / Super Node Total Voting = 38.2% * 25 IOV* 5,000,000/10, 000,000 = 4.775IOV.

Remark:

1. ***Ra** stands for reward of super node A, **Qa** stands for super node reward ratio, **Ra'** stands for reward of self-voting by super node A;*
2. ***Rb** stands for reward of voter B, **Qb** stands for voting reward ratio.*
3. *The 5 million IOV pledged by the node is equal to voting for itself and will participate in the voting distribution.*

IOV Blockchain Infrastructure Chain Incentive Mechanism ensures that miners, IOV holders, infrastructure developers and community contributors are properly rewarded, which stimulates the enthusiasm of users' participation and ensures the effective operation of the system.

3.3 Application Chain Governance

IOV Blockchain is based on a infrastructure chain and allows application developers to deploy and run different application chains. Each application chain has its own application miners, developers, token holders and users and so on. *IOV Blockchain* allows the application chains to set up flexible incentive mechanism. The application chain could motivate application miners and developers through its own token distributed.

3.3.1 Application Chain Token

Each application chain on the *IOV Blockchain* infrastructure could have its own ecosystem and its own token for ecological incentive. The application chain token could be used to motivate application chain miners, developers, IOV holders and

communities.

Application chain developers could customize the token name, abbreviation, total distribution and decimal places. And the initial allocation can be written into the application chain link block.

3.3.2 Application Chain Miners

Application developers could choose one of following modes to generate application chain miners:

Mode 1 - Directly select the infrastructure chain miner as the application chain miner. In this case, the infrastructure chain miner would enable a single thread to process the application message and generate blocks for the application chain.

Mode 2 - The application chain miners would be elected by application token holders. In this case, the application chain miners would be elected by application chain token holders.

3.4 Community Incentives

IOV Blockchain is a public blockchain in the connected car industry under AUH Foundation from Singapore. It is open to car users around the world and has created 3 billion IOV tokens in total through smart contracts. IOV Blockchain aims to help users manage their digital assets via encryption storage technology and return the ownership of driving data to car users, enabling car users to determine the value of connected car blockchain ecosystem themselves.Car users around the world can gain IOV tokens by contributing driving data to IOV Blockchain’s ecosystem. The value of such data can directly affect how quickly users can gain IOV. Under the fair value distribution mechanism, miners are greatly incentivized to contribute data. The demand side of data can also utilize more data and provide a wider range of services.This way the cost of car related services could be reduced and the connected car ecosystem can develop in a more fast and prosperous manner.

IOV Blockchain ecosystem supports mobile miner, onboard miners, and car

miners and will support SDK in the near future. Users can start mining simply by logging in the third-party board or driving their cars. Connected data includes data on car users' social behaviors, spending habits, driving location information and etc.

3.4.1 Mobile Miner

IOV Blockchain has officially released car mining function in May , 2018. The mine has already developed a serious of missions for users to obtain computing power. Users can gain IOV tokens by completing missions.

3.4.2 Onboard Miner

The IoV On-board diagnostics can not only serve as a tool to help users oversee their digital data, but could also act as a mining machine that is developed based on blockchain technology. IoV On-board diagnostics can thoroughly oversee and manage different driving data in 126 categories and contribute data to IOV ecosystem dynamically. Data contributed by users will be accumulated as computing power and the amount of such data will help determine the output efficiency of IOV tokens.

IOV Blockchain has partnered up with SF and other famous chip companies from Silicon to fully launch consensus algorithms for onboard mining machines. Readily available onboard chips include IOV designated computing chip, IOV-IPFS chip, Max-III cross-chain chip. They will gradually be applied into our series of onboard mining rigs to help users maximize their revenue on car-related digital assets.

3.4.2 Mining Car

Most car manufacturers started to install Telematics Box in cars to collect driving data as part of an upgrade of cars. However, consensus mechanisms are needed to ensure that the ownership of such data belongs to car users. IOV Blockchain has partnered up with the NürnbergMesse Group and car manufacturers such as BYD to gradually integrate IOV mining consensus into cars. Car users will be able to launch

the preinstalled the third-party board without any external devices and contribute data to gain computing power directly. The gained computing power can be converted to IOV tokens.

3.5 Coordination Mechanism

The coordination mechanism in *IOV Blockchain* is divided into two levels: infrastructure chain and application chain level. *IOV Blockchain*'s coordination mechanism could satisfy the following reasonable governance models:

- This mechanism allows all ecological participants, including those directly or indirectly affected party, to vote for the events they care about.
- This mechanism keeps cautious about voting based on " token holder";
- Governance is always prioritized, which means larger changes should take precedence over smaller ones.
- The governance system could flexibly increase or decrease the quantity of governance seats according to the ecological development.

The development and evolution of the *IOV Blockchain* infrastructure chain builds an economic foundation with the reward and flow of IOV Token. Developers and miners carry out infrastructure construction, while the community users provide or access services through *IOV Blockchain* infrastructure chain. IOV Token holders could determine infrastructure operation parameters such as dynamic parameters and miners' nodes through on-chain voting.

The technical support to on-chain governance is provided through smart contract deployment by application chain, which could govern a relatively independent application community with suitable mechanism.

4. *IOV Blockchain* Application Framework

IOV Blockchain's application framework is written in a smart contract to realize some common basic applications in the field of Internet of Vehicles, including digital identity system, e-commerce system supporting micro-payment and M2M payment, advertising application, etc.

In the meantime, *IOV Blockchain* would provide some standardized SDK interfaces at the application framework layer for developers to create their own smart contract applications. *IOV Blockchain* provides independent application chains for applications to record blockchain data. The developers would have sufficient independence to distribute their own token, select block producer, and design incentive mechanisms, etc.

4.1 *IOV Blockchain* Digital Identity System

In order to provide better community application experience to the users, *IOV Blockchain* proposed a digital identity system, enabling the users to better manage their personal data and value assets in the IoV community, in terms of managing and maintain their blockchain digital identities.

The technical scheme of digital identity is shown as below:

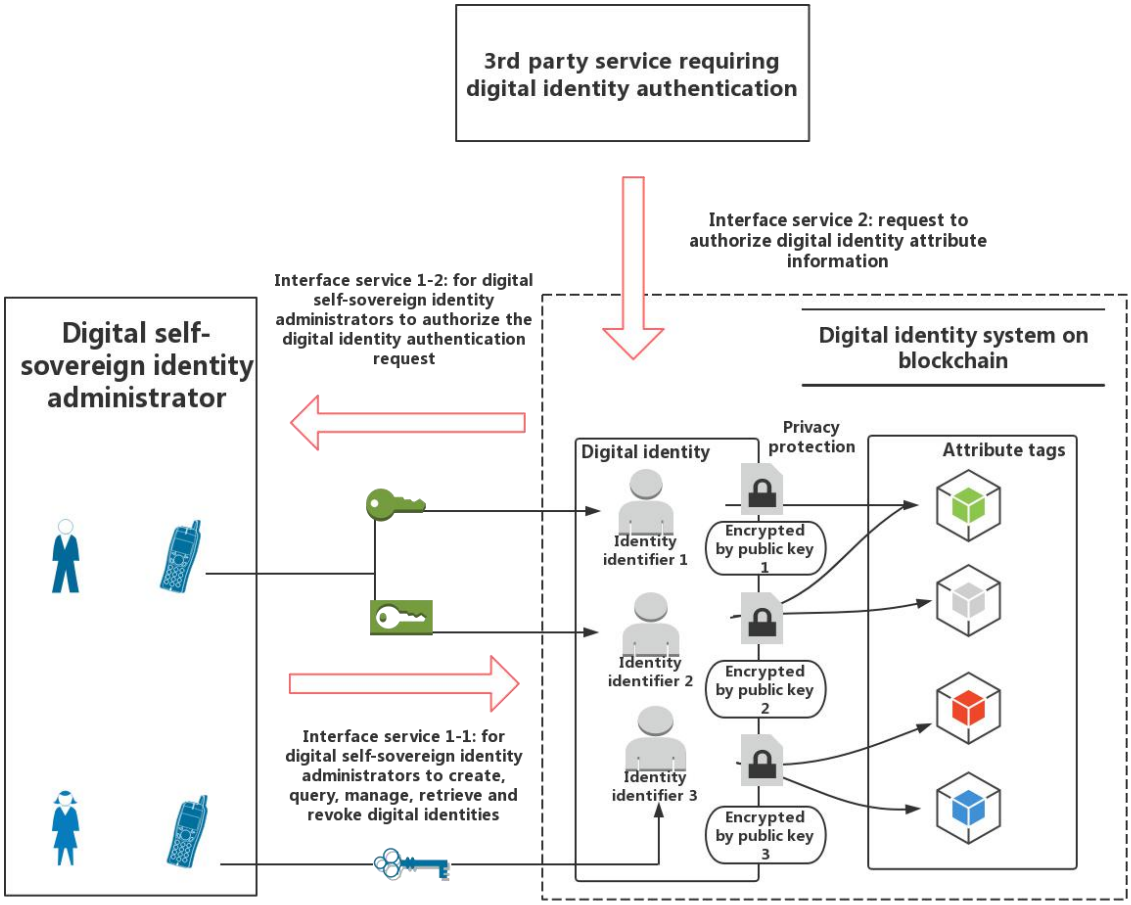

Fig. 11. Technical scheme of Digital Identity Technology

The above-presented implementation could create an autonomous digital identity for *IOV Blockchain* infrastructure users. The identifier of this autonomous digital identity is stored in the decentralized blockchaininfrastructure. This digital identity system could extend the user's independent digital identity and digital wallet management experience, and reflect the value of personal information data.

The digital identity system on the blockchain realizes a infrastructure for digital identity operation and state recording through the smart contract and consensus ledger technology. When creating a digital identity, a unique identifier would be assigned, and bound to the public key of the digital self-sovereign identity administrator, who keeps the private key as information for signing identity attribute authentication request. The digital self-sovereign identity administrator could bind attribute tags. Any aforementioned administrator who owns an attribute tag, have information

written on it. The digital self-sovereign identity administrator could use their own public keys to encrypt identity attribute information, so as to protect privacy.

This infrastructure includes three major interface services to perform two major functions:

The two main functions are as follows:

Function 1: The digital self-sovereign identity administrator could create, query, manage, retrieve and revoke digital identities on the blockchain digital identity system through interface service 1-1 (interface service for digital self-sovereign identity administrators to create, query, manage, retrieve and revoke digital identities). The users' autonomy over digital identities and unified management on them could be guaranteed by the decentralized blockchain digital identity system.

Function 2: The third-party service requiring digital identity authentication sends the message requesting identity attribute authentication to the digital identity system on the blockchain through interface service 2 (request for digital identity attributes authentication information), then the block chain digital system obtains the authentication signature from the digital self-sovereign identity administrator through interface service 1-2 (for the digital self-sovereign identity administrator to authorize the digital identity authentication request).

The details of the three interface services are as follows:

Interface service 1-1: for digital self-sovereign identity administrators to create, query, manage, retrieve and revoke digital identities. This interface could be used for the digital interaction between digital identity manager terminal and the digital identity system on the blockchain.

Interface service 1-2: for the digital identity authentication request authorized by the digital self-sovereign identity administrator. When a third party service is requiring digital identity authentication, this request would be transferred to the user's terminal through the digital identity blockchain system and interface service 1-2. The user then could authorize it on the terminal where keeps the private key.

Interface Service 2: Authentication request of digital identity attribute information. When the third party service requires the user to provide digital identity authentication, the request is sent to the digital identity blockchain system through interface service 2.

4.2 *IOV Blockchain* E-commerce System

IOV Blockchain supports the development of e-commerce application chains which could provide M2M micro-payment, auction, IOU, insurance and other functions.

The business demands of automobile consumption include insurance, automobile repair and maintenance, beauty care, second-hand cars, logistics, leasing, advertising, and so on. The vehicle could record the contents of the accepted services in the decentralized storage system, record the transaction information on the chain, and pay with digital cryptocurrency. Therefore, all the transaction information processed through this car would be immutable and checkable.

M2M micro-payment could support payment through vehicle for road charges, refueling, charging, etc. Insurance service could be customized basing on driving and maintenance records of the vehicles. Auction could be used for second-hand vehicles trading.

4.3 *IOV Blockchain* Data Flow System

IOV Blockchain supports data flow applications. The data information could be stored off-chain, such as cloud storage and IPFS storage, and the hash value of the data would be stored on the chain as a query path to the data. The data could be located in *IOV Blockchain* through its hash value.

The data flow application chain could return the ownership of the data to the individual, and only the authorized rights to use the data by the owner is recognized. The data authorizer could specify the authorized data dimension, time, and price. The query permission could be authorized after receiving the transfer from the authorization requester.

4.4 SDK Interface for *IOV Blockchain* Application Development

IOV Blockchain provides SDK interfaces at the application framework layer for developers to deploy their own application chains. Developers could develop and deploy on the infrastructure chain their own smart contracts. By calling the relevant SDK interfaces, smart contracts could vote out block producer, distribute token in independent application chains and record value transfer, send messages using P2P network protocol at the underlying system, and implement business logic by deploying smart contracts in virtual machines.

5. Conclusion and Acknowledgment

IOV Blockchain is a multi-block chain data architecture for multi-application of IoV by classifying and tagging transaction data. Single chains of different applications interact with each other through a higher-level blockchain that records cross-chain transaction state. It adopts a Layer 3 Protocol of on-chain, off-chain, cross-chain layer. Single chains of different applications could decide appropriate consensus algorithms according to different application scenarios through a customizable consensus algorithm mechanism. In the blockchain system, *IOV Blockchain* has proposed a digital identity system to enhance users' management and maintenance of their personal identity, personal data and personal digital assets, in order to improve the user experience.

The AUH Foundation also claimed that the current version of *IOV Blockchain White Paper* would be the most updated and confirmed, replacing all previous *IOV Blockchain* white paper versions and official technical documents. No further notice would be announced. Such consensus is based on rapid technical upgrade of *IOV Blockchain*, following the global blockchain technology development and implementation.

6. References

[1]https://github.com/*Ethereum*/wiki/wiki/Sharding-FAQs

[2] EOS.IO Technology White Paper V2, https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[3] DPOS Consensus Algorithm - The Missing White Paper, https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[4] Casper Proof of Stake compendium, https://github.com/*Ethereum*/wiki/wiki/Casper-Proof-of-Stake-compendium

[5]A. Back et al., "Enabling blockchain innovations with pegged sidechains", http://cs.umd.edu/projects/coinscope/ coinscope.pdf, Oct. 2014

[6]S. Popov, “The Tangle”, https://iota.org/IOTA Whitepaper.pdf (2016)

[7] J. Poon, T. Dryja, “The *Bitcoin* Lightning Network: Scalable Off-Chain Instant Payments” https://lightning.network/lightning-network-paper.pdf (2016)

[8] Raiden Network, https://raiden.network/101.html

[9] J. Poon and V. Buterin, “Plasma: Scalable autonomous smart contracts,” White paper, 2017.