Cyber-Physical Chain (CPChain) Whitepaper

Decentralized Infrastructure for Next Generation Internet of Things

CPCHAIN

CYBER PHYSICAL CHAIN

CPChain Team

January 10, 2018

Executive summary

Cyber-Physical Chain (CPChain) deeply integrates blockchain with Internet of Things (IoT) to realize a decentralized and trusted brand-new distributed IoT systems. It can reduce the cost of system interconnection, increase the value of data sharing, and ensure user privacy and system security. CPChain focuses on the scalability, security and real-time issues that blockchain faces in the Internet of Things industry. By combining the three technologies: blockchain, Internet of Things and distributed encryption storage and computing, it builds a new generation of Internet of Things, which can provide entire solutions for data acquisition, sharing and application in IoT industry. CPChain focuses on multi-party data transactions and IoT-big-data-based Artificial Intelligence (AI) decision-making applications, establishes multi-faceted trust and heterogeneous data interconnection, and solves the pain points in the industry. Moreover, an explosive and innovative business model of new generation of data sharing is built based on CPChain.

Contents

1. Background

1.1 The Challenges in Centralized Architecture of IoT Systems

Internet of Things (IoT) is a major development and revolutionary opportunity in information field. It highly integrates advanced information technology, communication technology, sensor technology and computer technology to establish a global dynamic network infrastructure. All smart objects (RFID tags, sensors, smartphones, wearable devices, etc.) are interconnected and all information and data are shared and transmitted for full awareness, reliable delivery and intelligent processing. Currently, the IoT adopts the centralized technology and operation mode in the fields of intelligent transportation, smart home and medical care, i.e. the "chimney" IoT architecture, and faces the common problems in connection costs, trust, data value and business models.

Cost of device connectivity. In recent years, as the price of components such as computing devices, storage devices and sensors has declined, IoT devices are exploding. IBM Research Institute predicts that by 2020, the world will have over 30 billion connected devices. However, the existing IoT solutions are high costs and mostly "chimney-type" vertical architecture. The data centers are built for one single project and each IT system has its own management tools and databases, forming an isolated island of information in the era of billions of connected devices. Therefore, the current inefficient architecture cannot satisfy the demand. In addition, most of IoT devices have long life cycles and the profit is far lower than that of intelligent terminals with fast consumer goods properties, such as PCs and smartphones. But the manufacturers need to maintain the corresponding IT systems for the long term and the profits are not enough to support maintenance costs. So the equipment manufacturers are unsustainable.

Privacy concern. The internet needs to be built on trust. Events such as Snowden also prove that "trusted third parties" are not 100% trustworthy. People have lost much of their privacy ever since the internet came into the big data age. Therefore, at the beginning of the development of the Internet of Things, privacy must be integrated into the IoT infrastructure to ensure that users enjoy more convenient and smart services without revealing their personal information, and allowing users to truly own the data they create and its value. In addition, the concept of "closed is safe" in the current centralized architecture is out of date. The new technology represented by the blockchain is building a brand-new "open is secure" interconnection of all things.

Data value. IoT systems generate large amounts of data at all times. These data are of great value in both commercial applications and research fields. For example, based on traffic travel data, deep learning is used to train more accurate and efficient path planning algorithms. Medical care organizations can design more customized care plans using sensor data such as cameras to more accurately determine the patient's condition. However, under the "chimney-shaped" island system, a large amount of traffic data is held by a few centralized platforms, in which case efficient interconnection cannot be achieved. Small and medium-sized companies cannot take advantage of these resources, and universities and other research institutions have difficulty in obtaining high-quality data sets, which seriously hinders the progress of scientific research and the value of the data cannot be fully reflected. In addition, most of the IoT devices connected to the Internet alone is meaningless. Only comprehensive analysis of big data will create value. If the data cannot be connected, the value cannot be thus delivered.

Business model. Networking, computing, storage and other functions of IoT devices bring about an increase in costs. But for most of the traditional devices such as sensors, networking is not the core function, and relying on the mode of selling hardware alone cannot support the huge overhead incurred by the long-term maintenance of corresponding IT system. Under the current centralized architecture, most

manufacturers cannot make full use of the IT function system of the IoT device, and the business model is simply selling user data. This is allegedly infringing upon the rights and privacy of users. With the IoT system further development and openness and users' safety awareness, the current business model will certainly usher in change.

1.2 Blockchain Technology Brings New Potential to the Internet of Things

As an emerging technology, blockchain has shown its great potential in solving data security and privacy issues. At present, many researchers and enterprises have introduced blockchain technology into more and more fields. Among them, the combination of the Internet of Things and the blockchain is one of the most promising directions. Blockchain technology has the opportunity to reshape its basic structure and solves a series of challenges in the current centralized "chimney" system.

Significantly reduce the cost of equipment interconnection. The core concept of Blockchain technology is distributed ledger, that is, an open, distributed database maintained by multiple parties. Based on the blockchain, we can build a decentralized and distributed IoT data platform, which can effectively solve the "isolated data island" problem. Manufacturers no longer need to establish a complete set of data solutions for their single products, significantly reducing the cost of equipment interconnection and post-IT system maintenance. Therefore, the decentralized IoT system, based on the blockchain technology, is sufficient to carry tens of billions of connected device data.

Significantly protect the privacy. The biggest advantage of blockchain technology lies in the security of privacy brought by decentralization. Without any third party controlling user data, there is not a large amount of data stored in a centralized data center, which reduces the risk of hacker attacks and malicious disclosure. The Internet of Things based on blockchain is a fully open and secure decentralized system for users to control their own data and protect their privacy and interests.

Realizing the share of data. The blockchain-based IoT system is a peer-to-peer decentralized network where all participants can participate equally in the data sharing process. All users can authorize their own data access, data applications and legally get a large number of valuable data at a lower cost from service providers, and on this basis to create more intelligent services, to realize the value transfer through the real-time data flow.

Create the brand-new business model. Blockchain technology changes the roles of users, IoT devices and vendors in the IoT system. Unlike the current centralized architecture, users in the new IoT system can dynamically develop data authorization mechanisms and interaction rules with devices, etc. Not only does the device perform a single function. The blockchain not only simply interconnects the device, but also enables devices to interact with each other autonomously. Vendors no longer need to maintain hundreds or thousands of IT systems in different systems. Changing roles will attract more participants, reshape market rules and create entirely new business models.

1.3 Commercial blockchain systems are facing the bottleneck problem of scalability

Although blockchain technology brings a high degree of security and privacy, scalability is the bottleneck of its application to large-scale industrial systems. The existing blockchain system architecture is not enough to support the demand of high-throughput, high-concurrency commercial systems.

High cost of data storage and calculation. Blockchain is a decentralized database maintained by a large number of nodes, which has a high storage and computing cost. However, the public blockchain application platform inevitably carries large-scale data. Under the current storage cost of blockchain, large-scale of the public blockchain based data platform is not practical.

Low efficiency of consensus mechanism. Consensus algorithms based on PoW in the current blockchain consume a great deal of computational resources. In many application scenarios, users cannot obtain strong computational power and all mining-based consensus algorithms will face the bottleneck of trading speed. If the scalability of the blockchain system cannot be solved, the decentralized application cannot really fall to the ground.

Under the above context, Cyber-Physical Chain (CPChain) is focus on the scalability, security and real-time issues of data and transactions in the integration of the Internet of things and blockchain technology. First, a parallel distributed architecture of distributed cloud storage system and decentralization blockchain system is proposed to solve the scalability problem of large-scale data storage and sharing. Second, CPChain presents a new hybrid consensus protocol for large-scale public blockchain based on collaborative optimization design of computing and communication. Finally, a side chain consensus system with high security, real time and high concurrent machine transaction is designed by combining edge computing and hardware security methods in the industry chain.

2. Parallel Distributed Architecture of CPChain

CPChain aims to construct a basic data platform for the IoT system, providing a full process solution for data acquisition, storage, sharing and application. CPChain will break through the core underlying technology of the application of block chain in the Internet of things system, and provide the infrastructure for the sharing and transaction of the data in the Internet of things. On CPChain, we can build data aggregation and real-time data flow applications to maximize the value of Internet of things data. The decentralized blockchain system requires the whole network node to operate on the same transaction (data), which has great disadvantages from the point of view of calculation and storage. It cannot give full play to the cooperative ability of the distributed network system. The decentralized system can only follow the "barrel principle", so it is not scalable. CPChain proposes the idea of separating data layer from control layer, constructs parallel architecture to enhance system scalability, provides open data sharing function while protecting user privacy, and adopts distributed storage scheme. The user data is encrypted and uploaded to the cloud to reduce the storage burden of the block chain and to ensure the integrity and accuracy of the data.

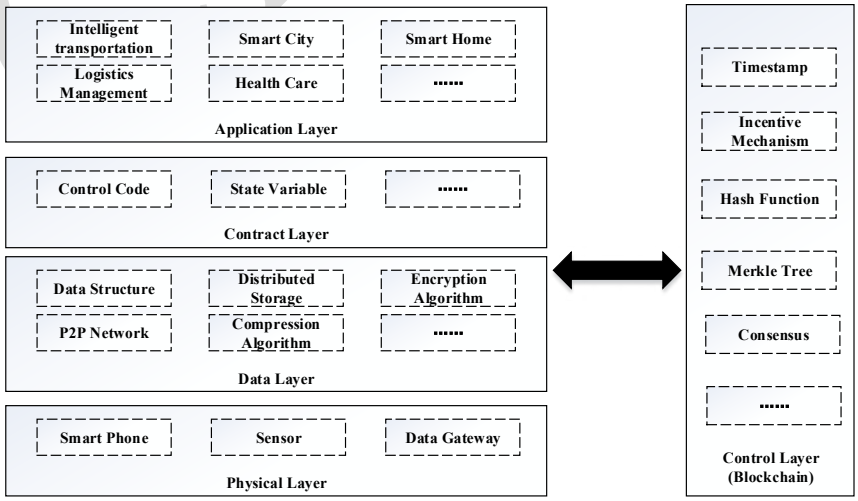


Fig. 1. System architecture of CPChain

Figure 1 shows the hierarchical structure of CPChain system, which is made up of physical layer, data layer, contract layer, application layer and control layer. Block chain is used as a vertical control layer to supervise data interaction. The physical layer is the basis of data acquisition in CPChain, including smart phone, sensor, data gateway and so on. The intelligent device joining the CPChain network needs to run a blockchain node or communicate with the blockchain network. At the same time, it also acts as a running environment for the decentralization application, dealing with encryption, consensus and so on. The data layer processes the main data, designs different data structure and compression algorithm for different applications, improves the efficiency of data reading and writing, and the original data does not need to upload block chain. Upload only hash values as unique identification of data and credentials for integrity and correctness. Raw data is encrypted on the user side and stored in a distributed hash table (DHT). The contract layer is the core of the system function. Because the intelligent contract is deployed on the blockchain, it is difficult to change the contract rules. Therefore, the design of the contract should be basic and concise, and more interactive functions should be placed in the application layer. The application layer is an interface between user and contractual interaction, which can be developed according to different requirements. The function of the control layer is accomplished by the block chain. In the beginning, the public chain platform such as Ethereum, which supports the intelligent contract, is used to speed up the development of the prototype system.

The decentralized system based on blockchain technology is different from the traditional distributed system. In the decentralized system, computing and storage tasks are redundant. Each node in the decentralized node stores the same data and performs the same computational tasks. On the one hand, this kind of redundant storage and calculation allows the blockchain system to operate independently of a trusted third party, ensuring the integrity of the data, untamperability and the consistency of the system; on the other hand, excessive redundant data also aggravates the system's burden, making the addition of new nodes more and more expensive. In the long run, this model is not scalable and unsustainable. In bitcoin, for example, the size of the bitcoin

blockchain has exceeded 130GB, which makes the new node spend a lot of time for synchronizing data. As the time goes on, the difficulty of entering new nodes continues to increase. Redundant computing ensures the consistency of the system state, which is valuable and essential. However, the large amount of redundant data storage makes the system burden heavier and not extensible. In order to solve the scalability problem of data storage, sharing and transaction, a parallel distributed architecture is put forward, as shown in Figure 2. The main chain, the industry chain network and the distributed storage system are combined organically. As the control layer of CPChain platform, the blockchain no longer stores all the data of the system, but only uploads the identification and credentials of the data, which not only greatly reduces the storage burden of the platform, but also ensures the consistency of the system.

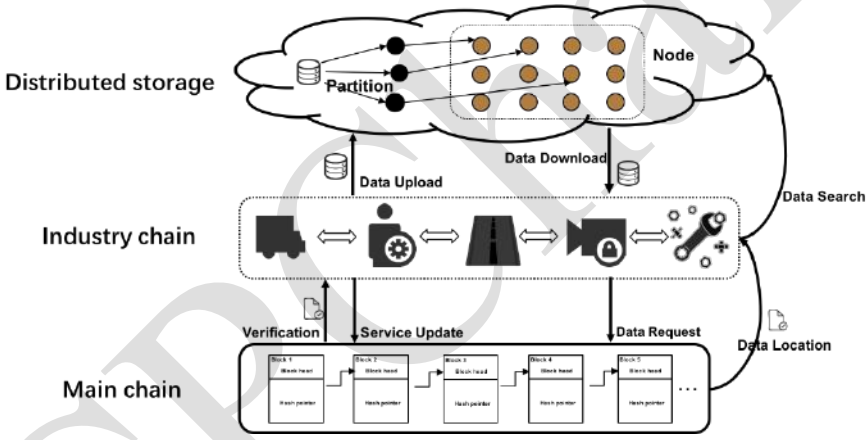


Fig 2. Parallel distributed architecture of CPChain

In CPChain parallel distributed architecture, distributed cloud storage layer and block chain layer are two parallel distributed networks for data storage and computing tasks, respectively. The user data will be encrypted into blocks at the client side, each part will enter different storage nodes, and the hash credentials will upload all the nodes in the blockchain network, so that the data can be verified, confirmed, and so on. Parallel distributed architecture separates the data layer from the block chain, which not only preserves the security and decentration of the block chain system, but also improves the scalability and greatly reduces the block size. At present, many block chain platforms are faced with the problem of capacity expansion, such as increasing

block capacity, but only increasing block capacity will increase the maintenance cost of blockchain nodes, resulting in fewer nodes and lower system security. With CPChain's system architecture, the number of transactions that can be packaged in a single block is greatly increased with the same block size, which can dramatically enhance the platform's transaction processing speed.

3. Key Technologies of CPChain

The parallel distributed architecture which separates the data layer from the control layer by CPChain can greatly improve the transaction speed and system extensibility without changing the block capacity. But it also faces new challenges. For example, after separating the data layer from the control layer, it is necessary to build a distributed storage network and ensure efficient interaction with the blockchain, and an effective connection must be established between the two parallel architectures. At the same time, the security and efficiency of the system should be guaranteed. In addition, if the data layer is independent, the block chain itself will be abandoned to protect the privacy of the data, so we must design a privacy protection scheme based on encryption technology. The encryption function based on re-encryption or homomorphic encryption has certain requirements for computing resources, but the block chain itself has limited computing resources and high cost, so it is necessary to strike a balance between privacy and availability.

In large scale P2P networks, due to the large scale of nodes and the heterogeneity of data, there is a great challenge to ensure the consistency in the process of node state synchronization and data security storage. However, the current block chain distributed network based on the power of work (POW) consensus protocol has some problems, such as scalability, waste of computational power and limited block speed. CPChain adopts the two-layer consensus protocol solution, designs the dynamic committee security election mechanism, solves the low throughput and the high delay problem, enhances the data consistency and the system security. In addition, CPChain is oriented to the characteristics of the Internet of things industry and adopts a cross-chain architecture. That is, based on the main chain, CPChain provides industry-oriented side-chain network function expansion for diversified practical application scenarios. The main chain network is mainly used for the high-speed control channel of IoT data exchange.

3.1 Parallel Distributed Encrypted Storage and Computation

CPChain uses a parallel distributed architecture in which the typical Internet of things data upload and share process is shown in Fig. 3. To guarantee data security, reliability and efficient sharing in the network, CPChain creatively combines distributed storage technology with re-encryption technology as well as homomorphic encryption technology to achieve efficient data access control mechanism, which is elaborated in the following specific two aspects.

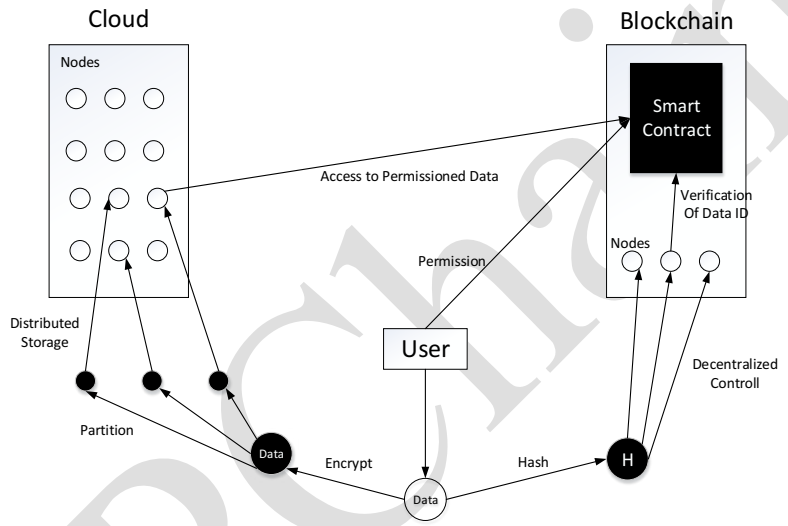


Fig. 3. IoT data upload and share in CPChain

- **DHT-based distributed encrypted storage**

The distributed storage process of IoT data is shown in Fig. 4. The system separates the data layer from the control layer, all raw data is encrypted locally and signed by the owner. After partitioning, the data are stored in different nodes with DHT method, making it impossible for the host to know the raw data. At the same time, the hash value of the data is stored in the block chain as a proof of the integrity and correctness of the data and the identification of the data. In the first phase of CPChain, we select Ethereum as main chain to speed up system prototyping and application testing.

The block chain also has access control over the data. When the owner of the data stores the data, the block chain stores access rights for each data record, which can be

accomplished by sending a transaction containing the data identity. When a user wants to retrieve the data, he or she must provide proof that the identity of the data is satisfied to obtain the right to access and use the data. If a malicious node exists in the system, it may ignore the access rights. But the data is encrypted and each node only saves a random part of the data in DHT. Therefore, malicious nodes have a limited impact. Since all data are encrypted on the user side, it is necessary to design an effective data authorization access mechanism to share data. The traditional distributed hash table only holds the key-value pair of data, which is far from enough for the CPChain platform. Therefore, at the data layer, CPChain will introduce a modified DHT to record the correspondence between the key and the data block, where the key has been used at the data encryption level.

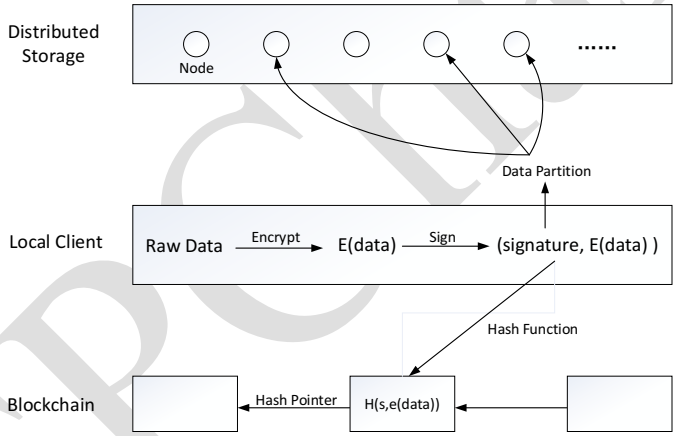


Fig. 4. Distributed storage of IoT data

Encryption and decryption of data will consume a certain amount of computing resources. In the face of the huge amount of data generated by the Internet of things system at every moment, it is undoubtedly a huge waste of computational power to encrypt each data record separately. Therefore, it is necessary to design appropriate data structures and encryption mechanisms for different types of IOT data to meet the requirements of data security and processing efficiency at the same time. The data generated by the CPChain platform will be arranged in chronological order, organized in a chain structure, and the time period T will be set to package the data in a period

into blocks. On this basis, the encryption interval *e* and the upload interval *u* are selected, so that a block record can ensure the integrity and authenticity of the data in the *u* blocks of the whole interval.

- **Data sharing and application based on encrypted computation**

To ensure data security and privacy, CPChain platform stripping the data layer from the blockchain. All the original data are encrypted on the user side. Because data is not visible to third parties, how to implement the computing or sharing of encrypted data is the primary challenge in parallel distributed architecture. The public key encryption system used in the block chain platform will no longer apply after the introduction of distributed encryption storage, because the public key encryption technology requires the receiver's public key to encrypt the data, as shown in Fig. 5. Only *one-to-one authorization* can be implemented. In the CPChain platform, it is hoped that the data is encrypted one time and used many times, which is abbreviated *one-to-many authorization* as shown in Fig. 6. Therefore, the CPChain platform will deeply develop re-encryption and homomorphic encryption technologies. The combination of encryption technology and blockchain technology will achieve more secure and more efficient data sharing and services.

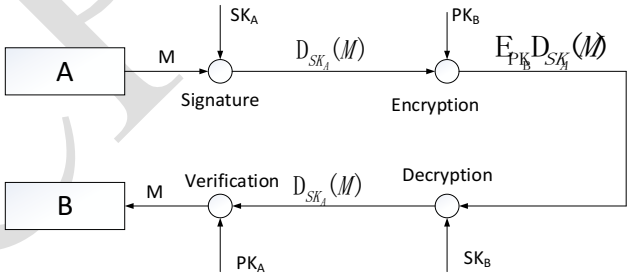


Fig. 5. Public key encryption

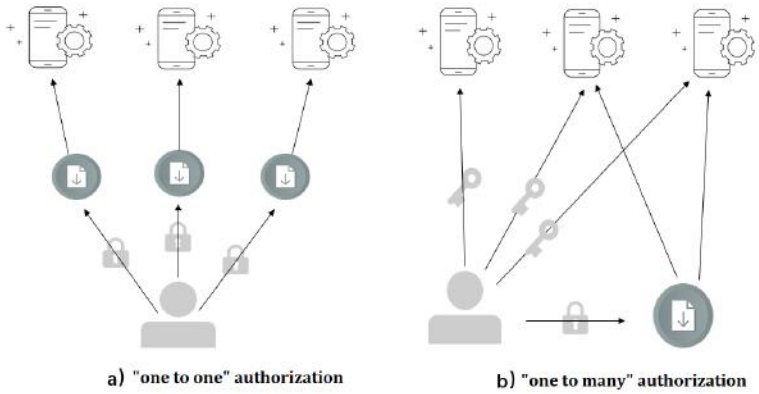


Fig. 6. a) Traditional public key encryption; b) CPChain encryption

To implementation one-to-many authorization, CPChain proposes a combination scheme of symmetric encryption and asymmetric encryption based on re-encryption technology. The user employs a symmetric encryption key in each encryption interval to encrypt data, that is, the encryption and decryption use the same secret key, and records the correspondence between the encrypted data block and the secret key in the improved DHT. To improve the security of the data, each encryption interval needs to update the secret key. The re-encryption system based on asymmetric encryption is used to transmit the key used to encrypt the data, thus data authorization is limited to a single encryption interval.

Re-encryption technology can partially solve the problem of data sharing in parallel distributed architecture. But its data is visible under the smart contract, so it faces some security and privacy problems. To this end, CPChain will further introduce homomorphic encryption technology to realize computing and application functions under encrypted data, such as distributed encryption matching and searching, so as to enhance the protection of user privacy.

3.2 Hybrid Consensus on Large-scale Public Blockchain

In the large-scale CPChain system, the realization of node state consistency and distributed data storage face many challenges due to the large scale of network and the massive data of Internet of things. CPChain will develop a hybrid consensus protocol

with extendable performance and propose a dynamic committee election mechanism to overcome scalability problems of the existing POW consensus protocol based systems.

The main core problem in the main chain structure lies in determining which nodes to complete the data collection, packing the chain on the block, and how to ensure the block data security and consistency. Traditional distributed fault-tolerant algorithms, such as PBFT and Zyzzyva, rely more on communication complexity to guarantee the consistency among nodes. For example, the PBFT algorithm applies a three-phase protocol to guarantee the system consistency even if there is a malicious Byzantine node and the recovery of node failure. However, the system scalability is poor due to its more dependence on communication to ensure the security of its algorithm. The performance declines faster with the number of nodes increasing; when the number of nodes exceeds a certain threshold, the system will not be available. Due to its reliability and availability at a small scale, the traditional Byzantine fault-tolerant algorithm is more suitable for the private blockchain and permissioned blockchain environments. In response to this problem, CPChain's core solution is to design a dynamic voting mechanism for the dynamic committees and elect credible committees to collect the data of the blocks and pack the tasks of the blocks.

- **Two-layer consensus**

Traditional Byzantine fault-tolerant algorithms cannot be applied to large-scale public chain scenarios, and POW consensus protocols consume a huge amount of computing resources, which leads to inefficiencies. CPChain proposes a committee-based two-layer agreement to enhance CPChain consensus performance. In the first round of consensus, the system performs a local electoral algorithm at the beginning of a fixed round (when a block is added, called a round) to determine the level of the nodes in the rounds. If the result is high, then the node has the right to record the round; In the second round of consensus, the process of block packing, verification, and the whole network broadcast will be completed. The consensus process is shown in Fig. 7.

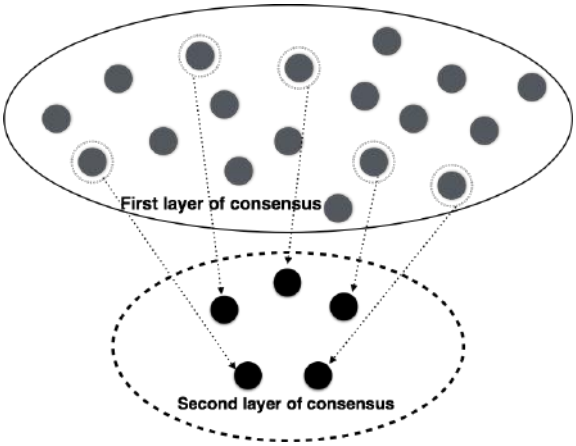


Fig. 7. Two-layer consensus structure of CPChain

- **Commission election and dynamic update based on credit evaluation model**

The main difficulties of CPChain's main chain consensus agreement include: 1) make the whole network agree with the member node in P2P network; 2) identify each other after the establishment of the committee; 3) make sure that the node level information cannot be forged. For these problems, CPChain constructs node credibility model to evaluate the node credibility. Based on the node credibility, each node presents a local trust computing to determine its role. Through the committee to carry out intra-group consensus, we can achieve block data collection, packaging, and new block creation.

In the election process, the randomness of the election process can be enhanced by the uniformly distributed probability lucky value. The malicious nodes can be prevented from making targeted cumulative credit attacks to control the behavior of the whole network. And the enhancement of randomness makes it possible for some nodes with low reputation to participate in the packaging of blocks. During the verification process, some incentives for some negative nodes are added.

Consensus agreement will last for *t* rounds and will be re-elected. During the process of adding a block, the credit value will be penalized if there is a high-level node downtime or malicious behavior. When the credit value is lower than a certain threshold, it will be deleted from the committee, and the committee changing information is added to the block so that at the beginning of the next round, a corresponding number of nodes can be dynamically re-elected to join the committee, as shown in Fig. 8.

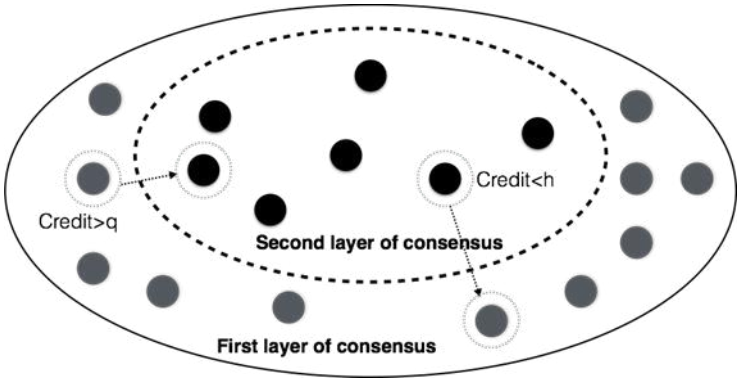


Fig. 8. Committee dynamics in the main chain of CPChain

3.3 Side chain consensus system with high real-time and security

As the basic data platform of IoT system, CPChain is a common IoT data control layer. However, different vertical applications of IoT, it has different performance requirements. Typical harsh real-time applications include unmanned vehicular, fleet coordination and so on. In such applications, CPChain needs to support secure communication and interaction with real-time control signaling in order to work efficiently and collaboratively among the various equipment nodes in the Internet of Things. If the data interaction is still completed through the main chain, it will face a great delay, which cannot guarantee the real-time requirements of all kinds of applications. In order to meet the requirements of high frequency, fine granularity, high security and real time of machine data transaction, we will select typical application scenarios and develop a lightweight side chain consensus protocol. Specifically, CPChain will design the side chain consensus system with edge computing and hardware security method in the industry chain to ensure that all kinds of applications can meet the delay requirements. Therefore, the high real-time and high security of the industry chain network are realized, as shown in Fig. 9.

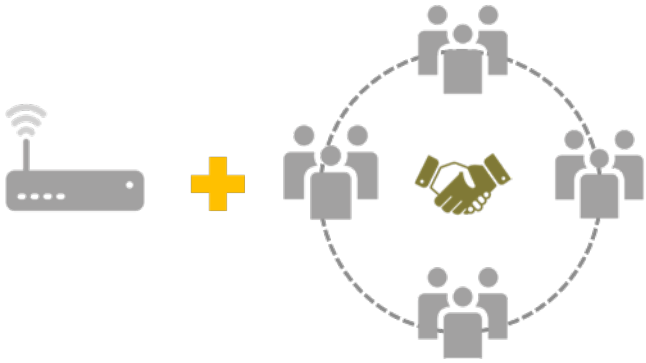


Fig. 9. Altruistic cooperation model with hardware acceleration

- **Data gateway & embedded encrypted algorithm**

Due to the heterogeneity of the data collected by the sensors in the Internet of things, the sensors themselves often do not have the computing power or computing power is very limited. If the cognitive computing of the sensor data processing is placed in each sensor node, it will bring more delay. Because the gateway equipment deployed in the Internet of things has more powerful hardware support than the sensor node, it can provide faster computing power, and the power of the device is not limited. By using the data gateway deployed in the Internet of things, the sensor data is aggregated to the edge gateway for data processing and encryption computation. On the one hand, the computing delay caused by the data processing is reduced. On the other hand, the computational load of sensor nodes in the Internet of things is reduced, and the lifetime is prolonged.

- **Incentive and security mechanism for consensus algorithm of industry chain**

The Internet of Things system consists of mesh network or wireless ad hoc network. There are many wireless communication technologies in different IoT industry, such as IEEE 802.11p, NB - IoT. Therefore, the consensus of machine transaction in the Internet of things can make full use of the characteristics of wireless network system, and embed the consensus process in the network communication protocol, so that the information interaction in the consensus process does not need to involve the data layer. The delay in the process is reduced only through the lower layer of communication layer. In addition, considering the high concurrency, real-time and security requirements of

machine transactions, CPChain will develop efficient altruistic cooperative incentive mechanism and security mechanism based on evolutionary game theory. For example, altruistic cooperative incentive mechanism based on directed acyclic graph directed Acyclic Graph (DAG) data structure. Thus, the application of CPChain side chain is more efficient, faster and safer.

4. Typical Applications of CPChain

As a common platform for data acquisition, storage, sharing and application in the Internet of things, CPChain can be widely used in intelligent transportation, intelligent manufacturing, intelligent city and other industry systems. As shown in Fig. 10, taking traffic data as an example, CPChain can provide a full process solution for personal navigation optimization, auxiliary driving, traffic scheduling optimization and customization of vehicle personalized insurance.

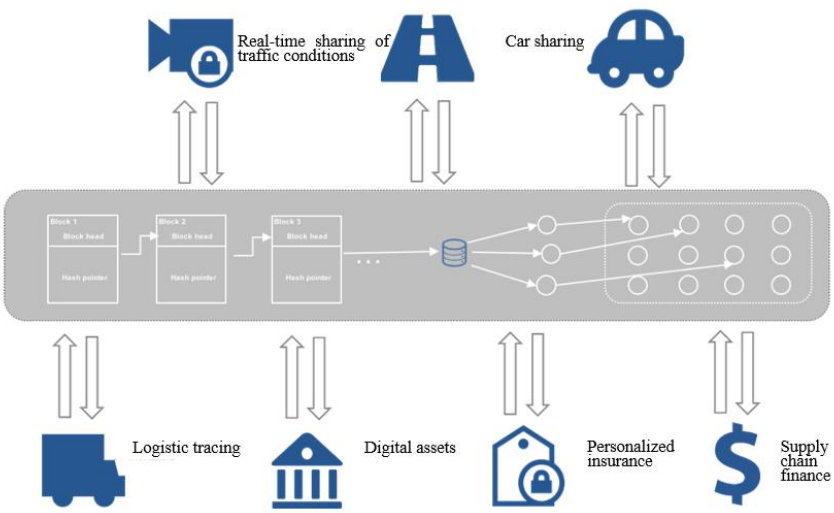


Fig. 10. Typical IoT applications based on CPChain

4.1 Big Data aggregation and artificial intelligence applications based on CPChain

IoT data sharing.

In the era of big data, the value of data is well known. The huge amount of data generated by CPChain will also be of great value, and CPChain will use block chain technology to make all data available to and at the disposal of users. It avoids big companies monopolizing data.

A large number of Internet of things equipment and user interaction data in the field of business and scientific research have very high value with the development of

artificial intelligence. High-quality data is essential, especially for small and medium-sized companies and scientific research institutions such as colleges and universities. With this open IoT data platform of CPChain, we can access to large amounts of real data at low cost, which will greatly facilitate technological progress. At present, research institutions must cooperate with large companies or rely on open data and open platforms of large companies in order to effectively carry out the training work of deep learning models. In fact, the vast majority of data held by large companies are derived from users, but users cannot control their own data. The CPChain data platform will change this situation in the CPChain data market, where users can authorize their data to different agencies and service providers to protect the privacy and rights of the data, as shown in Fig. 11. For users, the sharing of data is rewarded, and a large amount of real and trusted user data can bring greater business value.

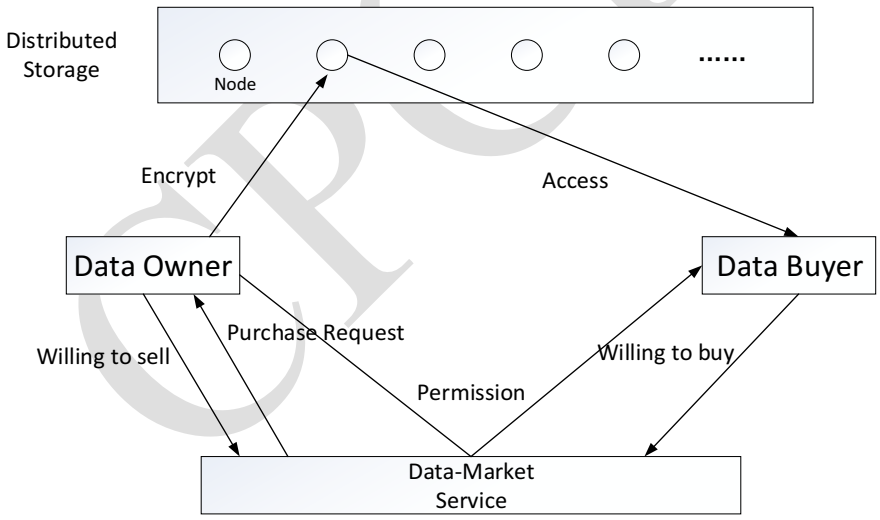


Fig. 11. Data sharing based on CPChain

Personalized auto insurance

Existing insurance programs generally have a very low level of customization. The novices or experienced drivers almost have the same plan options. Experienced drivers are often not coming with an accident within a few years, while the novice is more

likely to apply for their insurance. For insurance companies, due to the lack of adequate data support for different drivers, the driving habits of them are difficult to judge, it can only consider the risks and benefits in a general sense to design auto insurance products for different drivers. Furthermore, the cost of customized different auto insurance products is too high, which is not feasible.

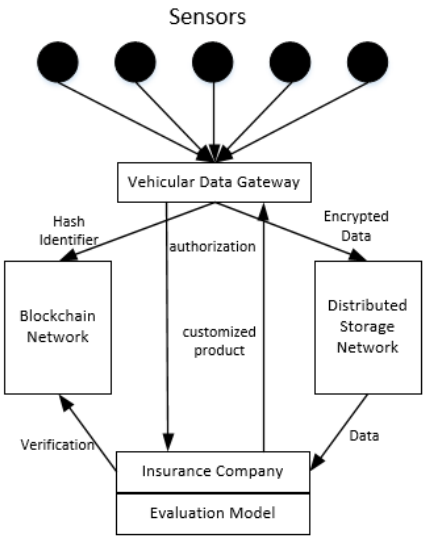


Fig. 12. Personalized auto insurance based on CPChain

The CPChain IoT data platform collects a large amount of vehicle data. Through the modeling and analysis of each vehicle data, the driver's driving style can then be evaluated well. And the insurance company can calculate the driver's risk more accurately with these results and then design more personalized car insurance, see Fig. 12. With advances in the sensor technology, combined with the CPChain data platform, unmanned set-loss and claims can be realized. After an accident happens, the responsibility can be distinguished with on-board sensors and road cameras and other equipment; the insurance company can automatically enter the claim phase through blockchain smart contract, saving a lot of time and manpower.

4.2 Applications of real-time data flow based on CPChain

Shared travel

In the application of shared travel, the three parties involved are passengers, drivers and shared travel service contracts respectively. As shown in Fig. 13, a real-time

communication system based on CPChain allows drivers and passengers to encrypt their information and broadcast it to the vehicular ad hoc network at the same time. Secure side chain consensus algorithm implements fast matching and secure transaction. The travel service is deployed in the blockchain as an smart contract. The contract can access the information of the driver and the passenger and store the data in the cache temporarily. According to the matching algorithm within the contract, the contract can find the matching vehicle for the passengers.

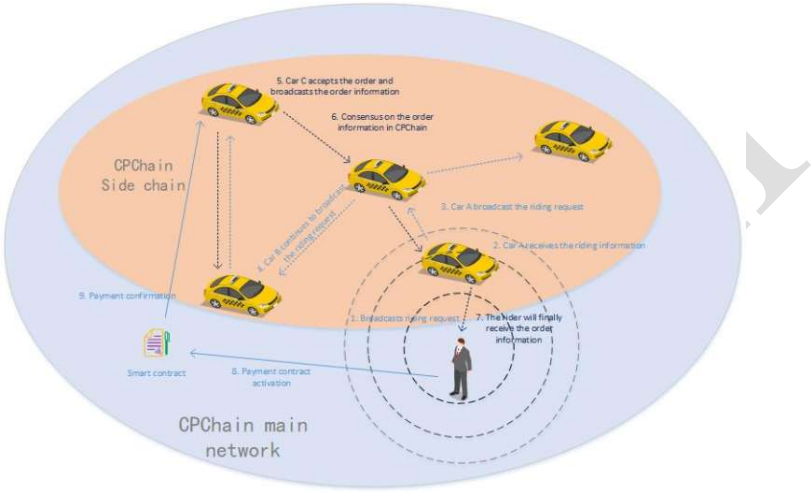


Fig. 13. Application of shared trip based on CPChain

Real-time traffic sharing and driving assistance

At present, the map app (e.g. Baidu map and Gaude map) can provide real-time traffic data. But the real-time data acquisition cost is high due to the lack of underlying traffic data platform such as CPChain. The traditional detection methods of road condition information mainly include the installation of sense coil, speed radar and video monitoring tools on the main roads of the city. These devices are mainly used to detect the occupancy rate of roads, traffic flow, speed and other coarse-grained road condition information.

With the improvement of vehicle intelligence and sensor technology, combined with the real-time sharing of CPChain side-chain data, a more efficient real-time traffic data sharing application can be constructed. Vehicles upload their real-time sensor data to the CPChain platform for rewards. The real-time data sharing application collects, analyzes and provides data to the vehicles with the need. Vehicles can learn about the

traffic jam in advance and find out more about emergencies in time. For the unmanned vehicle, the real-time road condition information can be added to the driving strategy to obtain a better control scheme and real-time adjustment.

Swarm control of unmanned vehicle fleet

In unmanned vehicle fleet control, the interior of the swarm needs intelligent identification and detection of traffic environment through real-time, reliable and secure message transmission, determine the current travel status and energy usage of the cluster members, and thus realize the safe intelligent swarm control. Combined with CPChain real-time data sharing, each vehicle historical data (including the movement status, location, terrain and other key information) can be real-time accessed and shared, so that each car can obtain more reliable and complete unmanned vehicle fleet swarm status information at a lower cost, which also will promote the optimization of cluster control algorithm. Moreover, the CPChain data real-time sharing increases system flexibility in the dynamic membership administration, completing the real-time swarm reconfiguration, and improving self-governing capabilities of unmanned vehicles and the ability of secure control in the malicious attack environment.

5. Roadmap of CPChain

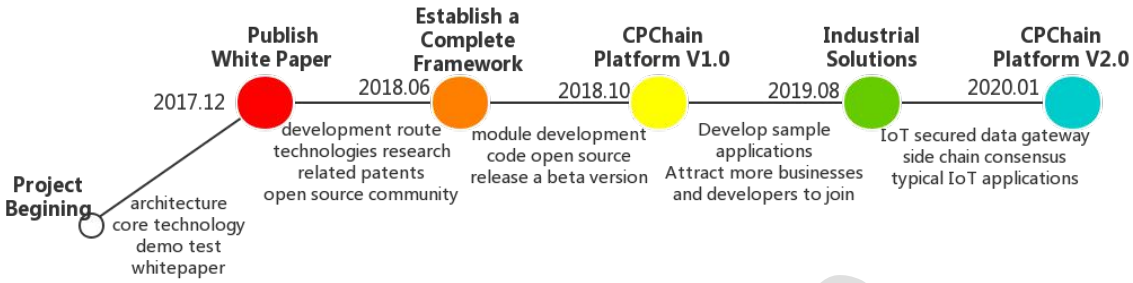


Fig. 14. Roadmap of CPChain

CPChain system architecture is complex and involves a lot of technology. The system architecture will evolve gradually in the process of development.

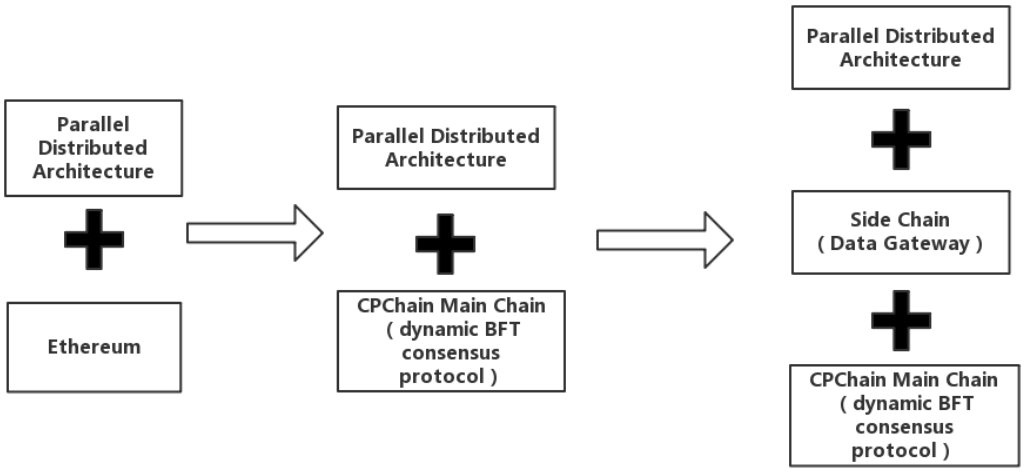
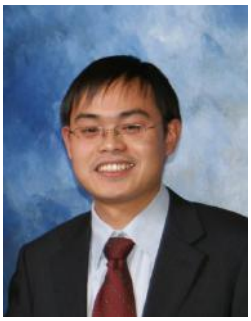


Fig. 15. Evolution diagram of CPChain system architecture

6. CPChain Team

The CPChain research team is an international team with a compound knowledge structure. The founding team consists of top talents from universities and industries of IoT, finance, security and commercial operations.



Dr. LONG Chengnian
CPChain Founder/Principal Scientist
Research Interesting：Internet of Things, Distributed Intelligent Systems with Blockchain Technology

Dr. Zhao Bin, CPChain Co-Funder.
Dr. Zhao has more than 12 years research and develop experience on communication, Internet of Things and FinTech.
Extended experience in management of R&D team. He has three patents on inventions in Internet of Things

Shi Qingwei, early participant in the blockchain and digital currency
Founder of the shared finance, participated in the preparation and investment of many projects

7. CPChain Economic Models and Usage

CPC is a primary asset on CPChain, CPC's value origin is that it can easily characterize and measure digital economic activity on CPChain. The value of CPC is based on two practical business needs. One is that the use of CPChain consumes a certain amount of CPC as fuel. The other is holding CPC is a symbol of participating in CPChain community governance.

1) The total amount of CPC is 1 billion, which will be generated when the main network is online.

2) Ordinary nodes in the CPC network (non-DAPP application nodes) have the right to send a fixed number of free transactions every day. If this number is exceeded or the transaction frequency is too fast, the system will charge a fee.

3) In order to ensure the balance of communication and computing resources, DAPP application developers must hold a corresponding amount of tokens according to the resources to be occupied by the application, and may lease them if the number of tokens is not enough.

4) For transactions resulting from DAPP applications, DAPP developers bear the corresponding costs, and pay leasing fees to miners who provide rental tokens.

The CPChain Foundation will charge CPC from developers and service providers of various smart contracts and pays for the gas required for the operation of smart contracts to ensure the operation of all business smart contracts. The majority of CPC revenue received will be rewarded to node providers, while the remaining part is used for funding follow-up day-to-day operations, commercial promotion and technology development;

The smart contract service provider pays CPC to acquire GAS to provide BaaS (Blockchain as a Service) smart contract services to the companies it serves. Based on their business rules and the added value contribution, the contract is provided to its client company, Application development provider receive CPC to provide smart

contract services;

The application development provider will further develop and process the acquired smart contract services based on the needs of the end customers and provide its traditional enterprise customers or end users with application products and receive the CPC as the enterprise revenue. The end user may pay CPC to get business products and services.

8. Token Distribution Plan of CPChain

The total amount of CPC token will be 1 billion and 40% is used for funding of Overseas community and institutional investors.

Proportion	Allocation Plan	Details
40%	Overseas community and institutional investors	The overseas community will be an important force for the future development of CPChain, and this part will be used in the construction of overseas community; Institutional Investors refer to the enterprises in the built-in distributed business ecosystem and service providers that serve these corporate customers or end-users; these business investors will focus on the future application of CPChain Token (CPC) in their commercial activities.
25%	Founding team, development team and consultants	The founding team, as well as the development team, greatly contributes their human and technology resources and material resources during the development of the project. Therefore, the CPC will be used as a reward and will be locked up for 3 years, with the first year all locked and released in batches each year
35%	Community governance	Maintaining the continuous operation and development of the team; Commercial application exploration and promotion; Selection of suitable industries for strategic deployment in the industry, project support and replacement of tokens for industrial application that truly satisfies the needs of market.

9. Project Budget

Daily Operation	35%	Including initial team salary, recruiting experts and developers, technical patents and intellectual property protection, foundation operation and marketing expenses, etc.
Technology Development	35%	Technical development, communication and sharing; publication of regular journals; creation or participation of alliances; community incentives, etc.
Business Development	20%	Maintain a series of business channel cooperation such as expanding and operating of CPChain Foundation
Investment	10%	Investment in new blockchain technology and new team

10. CPChain Community Governance

CPChain's governance adopts the three-tier governance structure of the CPC Holders' Conference, the Decision-making Committee and the Executive Committee.

The CPC Holder Conference allows the holder to participate in the governance of the community through preset code rules. The decision-making committee is responsible for the CPC holder conference and the executive committee is responsible for the execution.

The Executive Committee is responsible for the daily operation of the CPChain project. The Executive Committee consists of several management centers including Strategic Investment Center, Financial Management Center, Operations Management Center, Community Service Center and Innovation Management Center to guide the respective business units.

The CPChain team will set up a foundation in Singapore as the main body of CPChain governance with overall responsibility for the CPChain technology development and application development, maintenance of CPC holder rights, promotion of the CPChain brand and more.