2019

CPChain White Paper 2.0

Towards the Trusted Future

JUNE 2019

Executive Summary

We are entering the second half of the Internet age—the digital and the intelligence business era. Emerging technologies such as the Internet of Things (IoT) and blockchain are accelerating the empowerment of traditional industries. In the future, an increasing number of commercial services will operate online as business data and the demand for IoT technology become more and more important in the traditional transportation, medical, logistics, warehousing and supply chain sectors.

Traditional centralised IoT systems suffer from high connectivity costs and inefficient business models. Meanwhile, with data collection techniques continuously developing, privacy leakage issues continue to persist and in some cases even worsen. The public's growing security concerns necessitate a reliable privacy protection mechanism that does not hinder the dispersal and exchange of data.

Cyber-Physical Chain (CPChain) deeply integrates blockchain technology with IoT to realise a brand-new decentralized, trusted and distributed IoT system. Our solution reduces the cost of system interconnection, increases the value of data sharing, and ensures user privacy and system security. CPChain focuses on the scalability, security and real-time issues that blockchain faces in the IoT industry. By combining the three technologies— blockchain, IoT and distributed encryption storage and computing— we are building a new generation of IoT infrastructure, which can provide turnkey solutions for data acquisition, sharing and application within the IoT industry. CPChain focuses on multi-party data transactions and Artificial Intelligence (AI) decision-making applications fed by big data gleaned from a broad constellation of IoT devices, establishes multi-faceted trust and heterogeneous data interconnectivity, and solves multiple industry pain points. As a result, we expect an explosive and innovative business model centred on a new generation of data-sharing to be built around CPChain.

Table of Contents

1. Overview

1.1 Internet of Things: Current Stage and Pain Points

1.1.1 Internet of Things: Industry Requirements and Market Overview

Internet of Things (IoT) is a major development and revolutionary opportunity in the field of information technology. It comprehensively integrates advanced information technology, communication technology, sensor technology and computing technology to establish a dynamic global 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 coverage, reliable delivery and intelligent processing.

IoT is all about bridging the real world with the realm of virtual data. According to Gartner's most recent industry report, IoT devices will outnumber 26 billion by 2020, and the collective revenue stream enabled by IoT products and services is expected to reach $300 billion. IoT is playing an increasingly essential role in the movement towards seamless data integration and data value chain formation.

1.1.2 Challenges in the Centralised Architecture of Internet of Things Systems

Currently, IoT systems adopt centralised technology and operational models in the fields of smart mobility, smart home and healthcare under a "data silo" IoT architecture, and faces common problems in terms of connectivity costs, trust, data value and business models.

Technological Challenges

Low Compatibility: Many IoT Systems are poorly designed and implemented, requiring diverse protocols and technologies that create complex and oftentimes conflicting configurations.

Inefficient Architecture: In recent years, as the price of components such as computing devices, storage devices and sensors has declined, IoT device usage has skyrocketed. However,

existing IoT solutions are expensive due to the diverse protocols and architectures involved. Today's data centres are built for specific projects and each IT system has its own management tools and databases, forming isolated islands of information in an era inundated with billions of connected devices. In sum, the industry is highly fragmented.

High Cost: Most IoT devices have long life cycles and profit margins far lower than those of intelligent terminals with fast consumer goods properties, such as PCs and smartphones. However, manufacturers need to maintain corresponding IT systems over the long term and the profits are not sufficient to support maintenance costs. Therefore, equipment manufacturers' costs are unsustainable.

Low Scalability: Existing IoT device and technology platforms do not meet growing complexity and interconnectivity requirements, resulting in scalability issues.

User Data Privacy Concerns

Privacy Concerns: The internet needs to be built on trust. Events such as Snowden's windfall disclosure also prove that "trusted third parties" are not entirely trustworthy. People have lost much of their privacy ever since the internet entered the big data age. Therefore, at the beginning of IoT development, privacy must be integrated into the IoT infrastructure to ensure that users enjoy more convenient and smart services without revealing their personal information, allowing users to truly own the data they create and take advantage of its value. In addition, the concept of "closed is safe" in the current centralised architecture is outdated. New technology solutions enabled by the blockchain are building a brand-new "open is secure" interconnectivity among everything.

Data Ownership: As the Big Data Era matures, the monetization of data-driven capabilities is increasingly important. Currently, a small handful of enterprises employ a series of IoT devices to gather users' data, develop smarter algorithms to provide customised services, and consequently grow their revenue streams. As a result, data is mostly held by a few big platforms. Meanwhile, the *General Data Protection Regulation (EU)* became enforceable in May 2018, underscoring the general trend towards giving control to individuals over their personal data.

A blockchain-centric IoT convergence system would protect personal data ownership while realising the full value of data.

Data Incentives: Personal data will be an increasingly valuable resource in the foreseeable future. Most people do not bother gathering and managing their own data without proper incentives. Although the current pool of personal data is relatively small, from a data economy perspective it is analogous to the capillaries of a body, which accounts for 97% of all human blood vessels. The widespread collection, management and application of personal data among the majority of individuals is a prerequisite to boosting the data economy. Under the current situation, large enterprises hold most of the data-generated revenue. Individuals should be motivated and rewarded, since they are the main data contributors. Only with appropriate incentive mechanisms can individuals be motivated to contribute more valuable data, which in turn will enrich and expand the databases which fuel various organisations and enterprises.

Data Value: IoT systems incessantly generate large amounts of data. 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. Healthcare organizations can design more customized care plans using sensor data embedded in devices 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 centralised platforms, in which case efficient interconnectivity cannot be achieved. Small and medium-sized companies cannot take advantage of these resources, and universities and other research institutions have difficulty obtaining high-quality datasets, which seriously hinders the progress of scientific research and efforts to fully capitalize on the value of the data cannot. In addition, for most IoT devices, being connected to the Internet alone is meaningless. Only comprehensive analysis of big data will create value. If the data cannot be connected, then its value cannot be delivered.

Business Model: Networking, computing, storage and other functions of IoT devices bring about an increase in costs. But for most traditional devices such as sensors, networking is not their core function, and relying on hardware sales alone cannot support the huge overhead incurred by the long-term maintenance of corresponding IT systems. Under the current centralised architecture, most manufacturers cannot make full use of the IT functionalities of

their IoT devices, and any business models today simply sell user data. This allegedly infringes upon the rights and privacy of users. With the continued development of IoT systems for more openness, user safety and awareness, current business models will certainly be ushered into a new era of change.

1.2 Blockchain Technology Brings New Potential to the Internet of Things

As an emerging technology, blockchain has shown great potential in solving data security and privacy issues. At present, many researchers and enterprises have introduced blockchain technology into an increasing number of fields. Among them, the combination of IoT and blockchain technology is one of the most promising avenues. Blockchain technology is capable of reshaping underlying operational structures and solves a series of challenges stymying the current centralised "chimney" system.

Significantly Reduce Equipment Interconnectivity Costs

The core concept of blockchain technology is the distributed ledger, i.e. an open, distributed database maintained by multiple parties. Leveraging this technology, we can build a decentralised 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 interconnectivity and post-IT system maintenance. Therefore, decentralised IoT systems, based on blockchain technology, are capable of supporting tens of billions of connected devices, and the data they consequently generate.

Significant Privacy Protections

The biggest advantage of blockchain technology lies in the security of privacy brought about by decentralization. Without any third parties controlling user data, there will not be a large amount of data stored in a centralised data centres, which reduces the risk of hacks and malicious disclosures. An IoT data infrastructure based on blockchain technology can be a fully open and secure decentralised system where users will control their own data and protect their privacy and interests.

Realization of Data-sharing

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

Creating Brand New Business Models

Blockchain technology changes the roles of users, IoT devices and vendors in the IoT system. Unlike the current centralised architecture, users in the new IoT system can dynamically develop data authorization mechanisms and interaction rules with a diverse ecosystem of devices and services. Rather than a device performing a single function, the blockchain not only simply connect the device, but also enable devices to interact with each other autonomously. Vendors no longer need to maintain hundreds or thousands of IT systems across different platforms. Changing roles will attract more participants, reshape market rules, and create entirely new business models.

1.3 IoT-Blockchain System: Market and Applications Forecast

A blockchain-based decentralised approach to IoT networking would solve many of the traditional IoT system's issues. Adopting a standardized peer-to-peer communication model to process the hundreds of billions of transactions between devices will significantly reduce the costs associated with installing and maintaining large centralised data centres and will distribute computation and storage needs across the billions of devices that form IoT networks. This will prevent a failure in any single node in a network from bringing the entire network to a halting collapse.

Research and Markets, a well-known research institute, recently published a report on the blockchain market estimating that the total value of the blockchain-IoT market will increase from $113.1 million in 2010 to $3.021 billion in 2024, growing at a 92.92% compound annual rate.

Key drivers of the blockchain-IoT market include:

- The increasing amount of IoT devices;
- The increasing demand for networks' safety and stability;
- The increasing demand for operational effectiveness and efficiency;
- Blue ocean opportunities unlocked by blockchain IoT technology;
- Potential usage of smart contract and digital identification.

1.4 Commercial Blockchain Systems Are Facing Scalability Issues

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

High Data Storage and Calculation Costs

Blockchain is a decentralised database maintained by a large number of nodes. Data keeps accumulating, oftentimes without any eventual removal or maintenance, resulting in high storage and computing costs. However, public blockchain application platforms inevitably carry large-scale data. Under the storage costs of current blockchain solutions, a large-scale public blockchain-based data platform is simply not practical.

Versatility

There are various types of data and operations in the IoT field. To fulfil diversified operational demands, the blockchain network needs to adapt to diverse business needs and meet data sharing and data security in different scenarios. This means that the proposed blockchain solution has to be versatile, so that both structured and unstructured information can be processed, and side-chain research and development can meet future demands.

Inefficient Consensus Mechanisms

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 be constrained by a trading speed bottleneck. If the scalability of the blockchain system cannot be solved, then decentralised applications cannot be fully realized.

Under the above context, Cyber Physical Chain (CPChain) focuses on the scalability, security and real-time issues of data and transactions in the integration of IoT and blockchain technology. First, we propose a parallel distributed architecture comprised of a distributed cloud storage system and decentralization blockchain system in order to solve the scalability problem of large-scale data storage and sharing. Second, CPChain is presenting a new hybrid consensus protocol for large-scale public blockchains based on collaborative optimization design of computing and communication. Finally, by integrating smart IoT's end-edge-cloud architecture and blockchain's main-side chain design, CPChain aims to build an IoT self-sovereign identity (SSI) and decentralized public key infrastructure (DPKI) system based on blockchain technology, as well as an IoT big data sharing platform.

2. CPChain Solution

2.1 CPChain's Parallel Distributed Architecture

CPChain aims to construct a basic data platform for IoT systems, providing a full process solution for data acquisition, storage, sharing and application. CPChain will break through the core underlying technology of the application of blockchain in IoT systems and provide the infrastructure for the sharing and transaction of the data generated by IoT devices. On CPChain, we can build data aggregation and real-time data flow applications to maximize the value of IoT data. The decentralised blockchain system requires the whole network nodes to operate on the same transaction data, which has substantial disadvantages in terms of calculation and storage. For instance, this system cannot fully leverage the cooperative ability of the distributed network system, and the decentralised system can only follow the "barrel principle" and is therefore not scalable. CPChain proposes the idea of separating the data layer from the control layer by constructing a parallel architecture to enhance system scalability, providing open data sharing functions while protecting user privacy, and adopting a distributed storage scheme. The user data is encrypted and uploaded to the cloud to reduce the storage burden of the blockchain and to ensure the integrity and accuracy of the data.

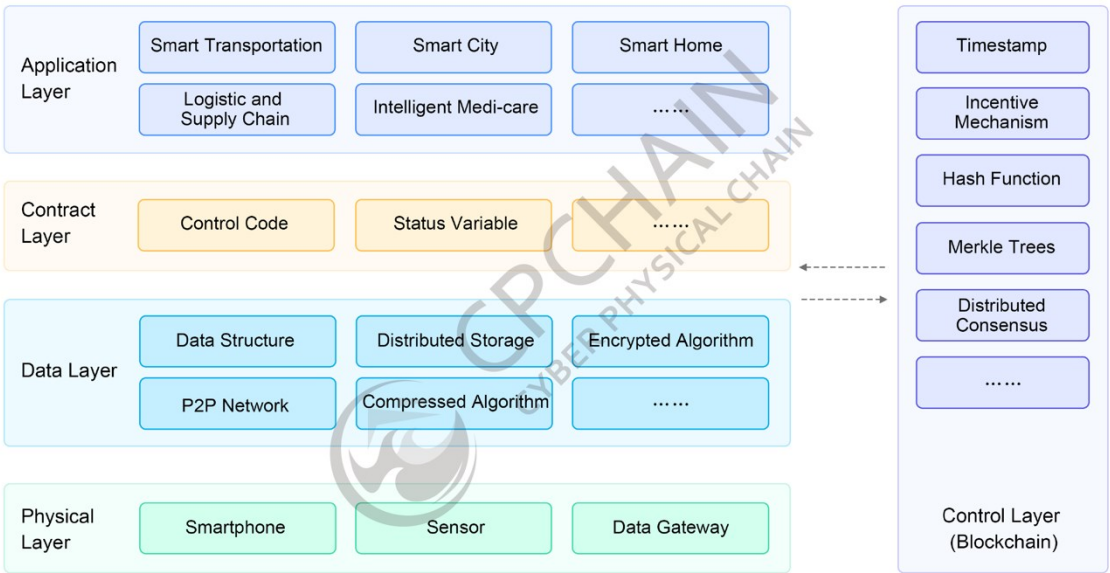


Figure 1. CPChain's System Architecture

Figure 1 shows the hierarchical structure of CPChain system, which is made up of a physical layer, data layer, contract layer, application layer and control layer. Blockchain is used as a vertical control layer to supervise data interaction. The physical layer is the basis of data acquisition in CPChain, including devices such as smart phones, sensors, data gateways 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 other functions. The data layer processes the main data, designs different data structures and compression algorithms for different applications, improves the efficiency of data reading and writing, and the original data does not need to be uploaded to the blockchain network. Rather, only hash values as unique identification for data and credentials need to be uploaded, for enhanced data integrity and accuracy. 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 smart contract is deployed on the blockchain, it is difficult to change the contract rules. Therefore, the design of the contract should be straightforward and concise, and more interactive functions should be placed in the application layer. The application layer is an interface between the user and contractual interaction, and can be developed according to different requirements. The function of the control layer is accomplished via the blockchain.

A decentralised system based on blockchain technology is different from traditional distributed systems. In a decentralised system, computing and storage tasks are redundant. Each node in a decentralised 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 and enhancing the tamper resistant qualities 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. For example, the size of the Bitcoin blockchain has exceeded 210 GB, which requires a new node to spend a lot of time synchronizing data. As time goes on, the difficulty of entering new nodes will continue to increase. Redundant computing ensures the consistency of the system’s operating state, which is valuable and essential. However, the large amount of redundant data storage makes the system burden heavier and not extendible. In order to solve the scalability problem of data storage, sharing and transaction, we are proposing the parallel distributed architecture

put forward 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, and rather 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.

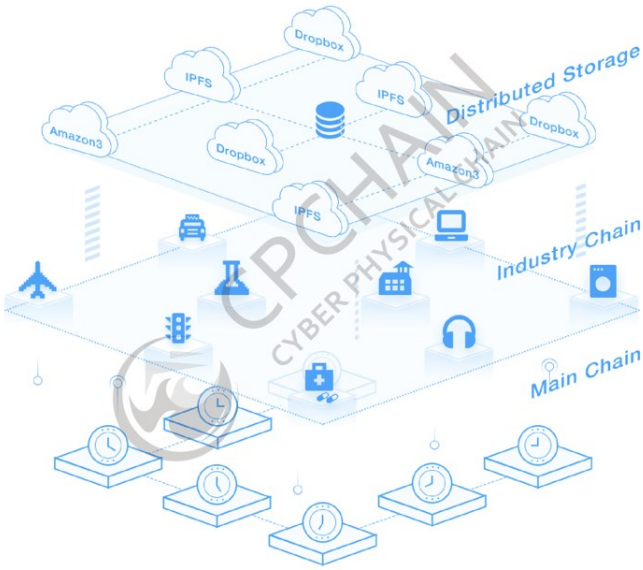


Figure 2. CPChain's Parallel Distributed Architecture

Under CPChain's parallel distributed architecture, the distributed cloud storage layer and blockchain layer are two parallel distributed networks for data storage and computing tasks, respectively. The user data will be encrypted into blocks on 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 executed on. The parallel distributed architecture separates the data layer from the blockchain, which not only preserves the security and decentration of the blockchain system, but also improves system scalability and greatly reduces block size. At present, many blockchain 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 under the same block size constraints, which can dramatically enhance the platform's transaction processing speed.

2.2 Parallel Distributed Encrypted Storage, Search and Authorised Sharing

CPChain adopts a parallel distributed architecture, in which the typical IoT data uploading and sharing process is shown in Figure 3. In order to ensure the safety, reliability and efficiency of data sharing in the network, CPChain creatively combines distributed storage technology with re-encryption technology and homomorphic encryption technology to achieve an efficient data access control mechanism. The detailed mechanism is explained in the following four aspects.

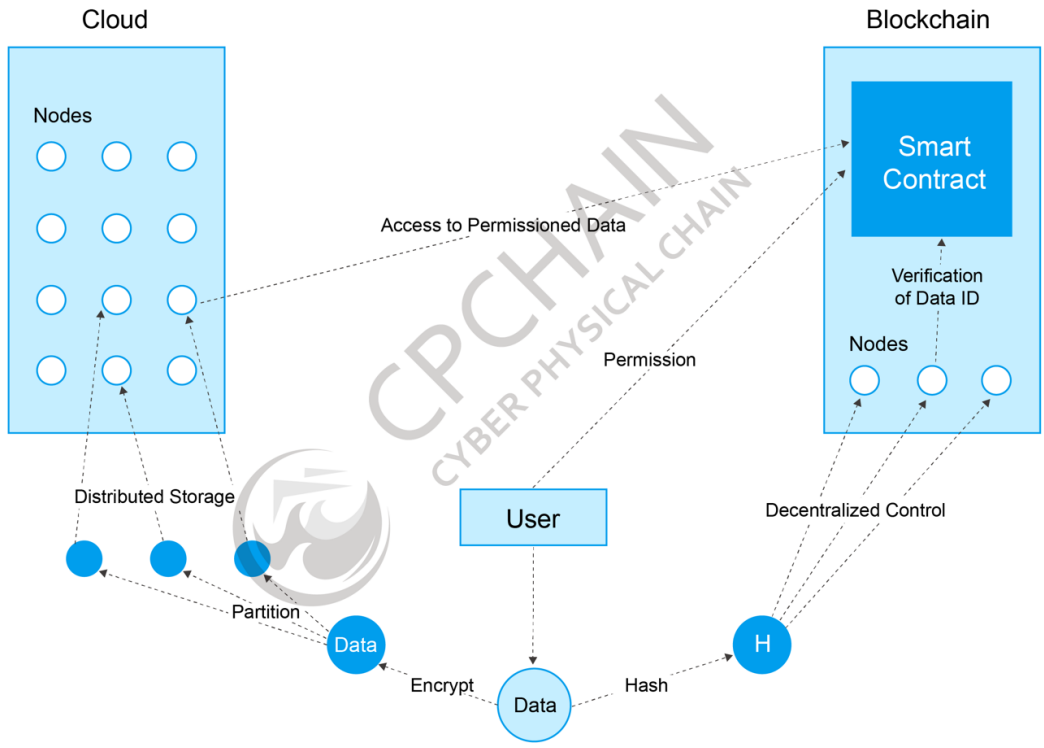


Figure 3. IoT Data Uploads and Sharing in CPChain

2.2.1 DHT

The distributed storage process of IoT data is shown in Figure 4. The system separates the data layer from the control layer. All the original data is encrypted locally and signed by the owner. After being hashed, it is stored in different nodes based on the distributed hash table method, so that the host cannot know the original data. At the same time, the hash value of the data is stored in the blockchain as a voucher for data integrity and correctness and an identification of the data.

The blockchain also performs access control on the data. When the owner of the data stores the data, the blockchain stores the access rights of each data record, which can be completed by sending a transaction containing the ID of the data. When the user wants to take out the data, he/she needs to provide proof that the ID of the data can be obtained in order to obtain access and use rights of the data. If there are malicious nodes in the system, they may ignore the access rights. However, since the data is encrypted and stored in DHT (i.e., each node only saves a random part of the data), the impact of malicious nodes is limited. Because all data is encrypted on the user side, an effective data authorization access mechanism needs to be designed to share data. The traditional distributed hash table only holds the key-value pairs of the data, which is not enough for the CPChain platform. Therefore, at the data layer, CPChain proposes an improved distributed hash table method, which combines the key used in data encryption calculation and records the correspondence between the key and the data block.

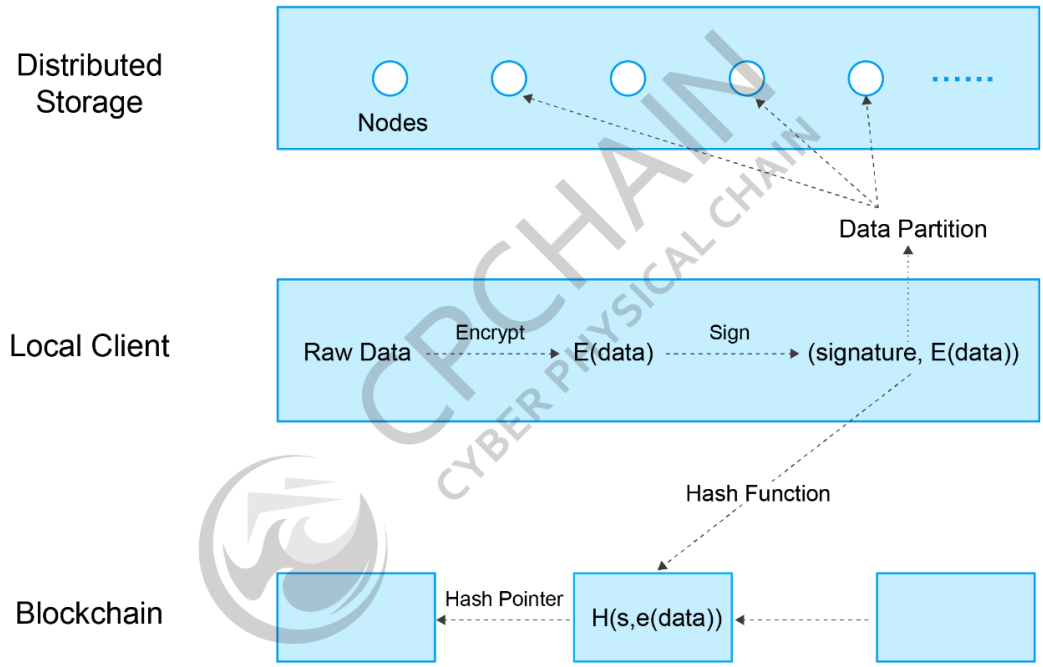


Figure 4. Distributed Data Storage Process

Both the encryption and decryption of data consume a certain amount of computing resources. Faced with the huge amount of data generated by IoT systems at all times, encrypting each data record alone is undoubtedly a huge waste of computing resources. Therefore, appropriate data structures and encryption mechanisms must be designed for different types of IoT data to meet

both data security and processing efficiency requirements. The data generated by the CPChain platform is arranged in chronological order, organized in a chain structure. In addition, a time period *T* is set, and data in this time period is packed into blocks. On this basis, the encryption interval *e* and the upload interval *u* are selected, thereby making the chain guarantee the integrity and authenticity of the data throughout the interval.

2.2.2 Data Sharing and Application

The CPChain platform strips the data layer from the blockchain network. To ensure data security and privacy, all raw data is encrypted on the user side. Since data is not visible to third parties, is issue of how to effectively implement computing or sharing of encrypted data is a central challenge for parallel distributed architectures. The public key encryption system adopted by classic blockchain platforms is no longer applicable after the introduction of distributed encryption storage, because public key encryption technology needs to use the public key of the receiver to encrypt the data, as shown in Figure 5, where authentication is conducted for each pair. In the CPChain platform, we hope that the data will be encrypted and uploaded just once and then authorized for multiple uses, as shown in Figure 6. Therefore, the CPChain platform will deeply develop re-encryption and homomorphic encryption technology and integrate encryption technology within the blockchain network to achieve safer and more efficient data sharing and service.

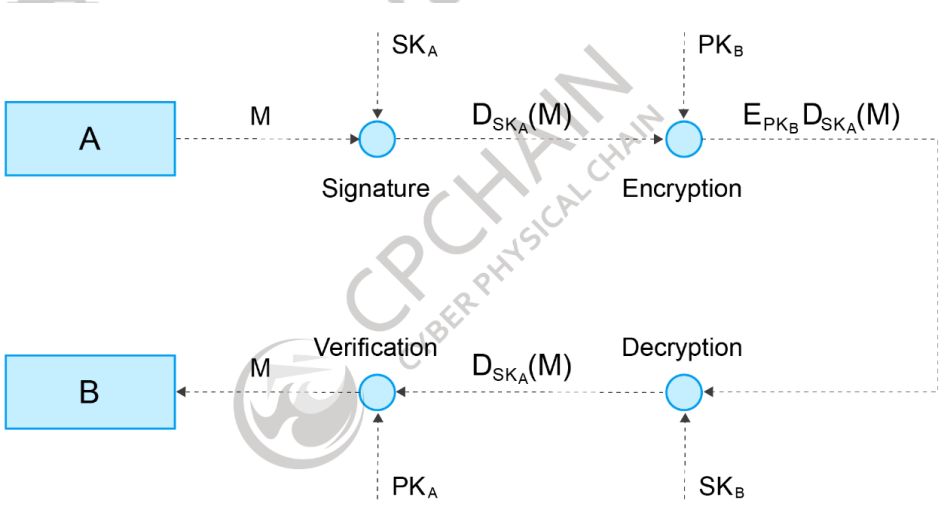


Figure 5. Public Key Encryption System

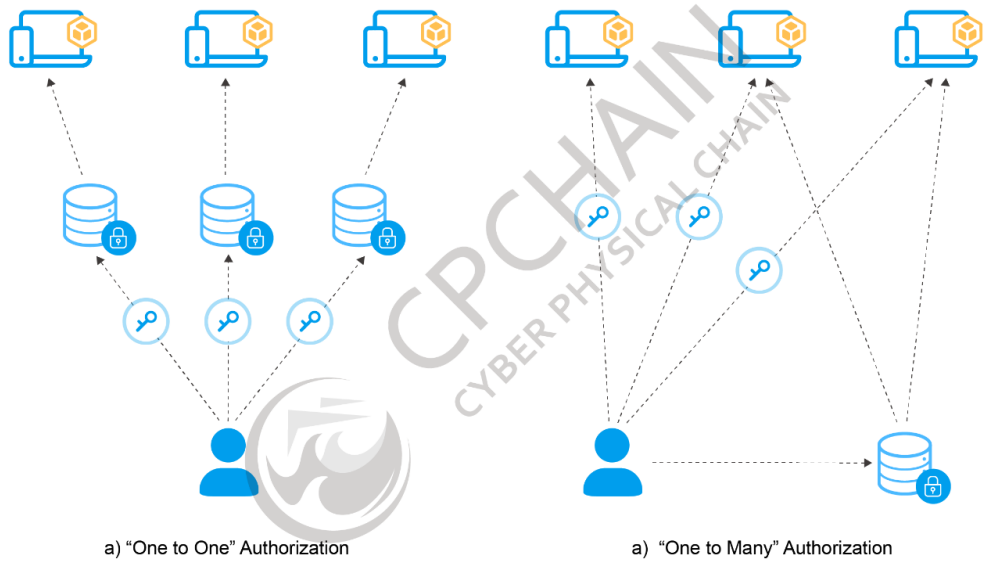


Figure 6. Public Key Encryption Authorisation

In order to realise one-time data encryption and multiple usage authorization, CPChain is constructing a set of symmetric encryption and asymmetric encryption solutions based on re-encryption technology. The user uses a symmetrically encrypted secret key for encrypting each encryption interval, that is, the same key is used for both encryption and decryption, and the correspondence between the encrypted data block and the secret key is recorded in the improved DHT. In order to improve the security of the data, the secret key needs to be updated every encryption interval. The re-encryption system based on asymmetric encryption is used to transmit the secret key used to encrypt data, thus ensuring that the authorization of data is limited to a single encryption interval.

Re-encryption technology can partially solve the data sharing problem which persists under the parallel distributed architecture, but its data is visible under the smart contract, so it faces certain security and privacy issues. To this end, CPChain will introduce homomorphic encryption technology to achieve computing and application functions under encrypted data, such as distributed encryption matching and search, to enhance the protection of user privacy.

2.2.3 Market: A Data Transaction Information Integrated Platform

PDash is a decentralized data transaction system based on blockchain technology. Under the premise of decentralization, the data design and transaction information are separated by modular design, taking into account the user's privacy and data transaction efficiency. The agent network guarantees the reliable transmission of data. In each transaction process, the agent node also serves as a witness between the seller and the buyer. Combined with a set of dispute-handling mechanisms in the smart contract, reliable transactions can be implemented in a fully distributed system.

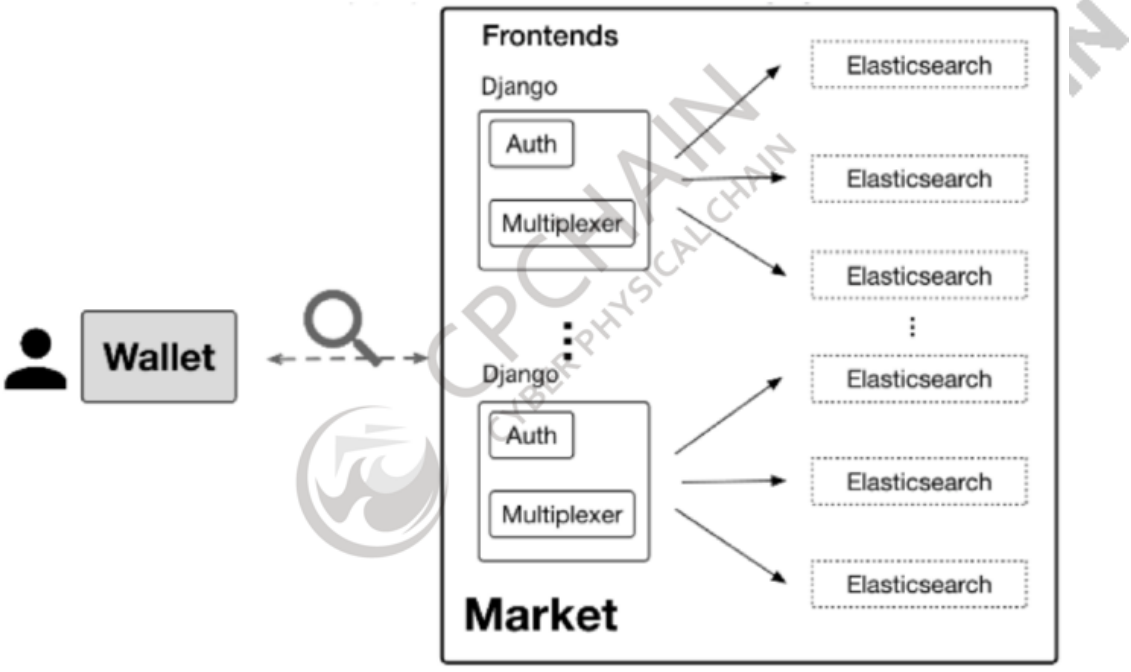


Figure 7. Market Structure

Market is the transaction information aggregation platform of PDash, and serves as an information bridge connecting data between a seller and a buyer. Market includes identity authentication, database, retrieval, and chain information synchronization modules. The seller publishes the basic description information of the owned data on Market, which is added in a structured form, including the title, label, description, price and other fields. From there, the buyer can retrieve information on Market according to actual needs, and in terms of discovery formats the program supports natural language search retrieval, and matches all fields in the data information. The hash value of the data description information is retrieved as a data index. And the hash value, AES key, and URL are correspondingly stored in the local database.

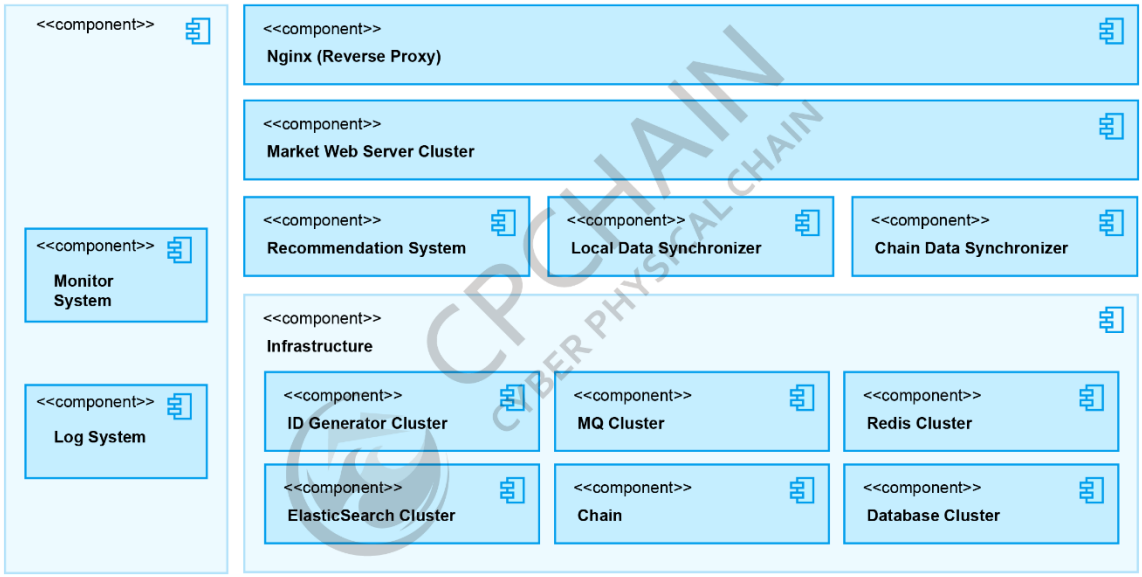


Figure 8. Decentralised Market Structure

Market's architecture shown in Figure 7 is a traditional server/client architecture that relies on centralized service provider operations. However, Market is only a platform for information aggregation in PDash. The whole transaction process does not depend on Market, but rather deals with transaction logic on the blockchain. This is similar to the Bitcoin wallet concept, where Bitcoin transfers are done on the same blockchain. Users using either client will not affect the operation of the system. Therefore, Market's architecture does not violate the PDash decentralization principles. In addition, unlike a traditional transaction system, PDash's Market adopts an elliptic curve digital signature algorithm compatible with the blockchain account system for identity authentication. Users do not need to register, and the Market operator cannot obtain user identity information. However, if there are multiple Market operators in the PDash system, the data information will result in fragmentation, which is not conducive to the free flow and aggregation of data and violates the ultimate objective of PDash. Therefore, CPChain designed a decentralised Market architecture based on blockchain technology, as shown in Figure 8. Compared with a traditional centralised architecture, the decentralized Market architecture adds modules such as *local data synchronizer* and *chain data synchronizer*, which are responsible for synchronizing local data to the chain and synchronizing the data on the chain to the local client. Through these new modules, the decentralized Market system ensures that any server running a new PDash Market can get the same data information while avoiding fragmentation.

The decentralized Market has an ID generation module that generates a unique ID for each data published to Market to synchronize data between Market and the chain more efficiently and accurately. Whenever new data information is released, the local data synchronizer will synchronize the data to the chain. At the same time, the chain data synchronizer will periodically monitor the data on the chain and synchronize new data information to the local client.

2.2.4 OTP: Blockchain-based Open Transfer Protocol

The *Open Transfer Protocol (OTP)* is a blockchain-based data transfer protocol that provides secure and trusted data transfer between clients. OTP provides a method for clients to exchange data and messages using different external storage systems. Through integrated blockchain technology, OTP supports a trust mechanism that is independent of the specific user, giving users complete control over their data. At the same time, the OTP provides a registration function that assigns users a URI (Unique Resource Identifier) in OTP format.

OTP is not only responsible for the transmission of data in PDash, but also a brand-new general data transmission protocol based on blockchain. The aims of designing OPT include:

1. A trust mechanism that is independent of the specific user. OTP uses blockchain to verify data integrity. Thus, it can verify the identity of the proxy node and provide a trust mechanism during data transmission without relying on any specific user or trusted third party.
2. A high degree of compatibility. Considering that different users tend to store data in different cloud storage systems, OTP has designed a compatible solution, and the OTP client can interact with heterogeneous storage systems.

3. An access control that the user can fully control. OTP integrates a very detailed access control scheme. The data is completely controlled by the user. Users can authorize different proxy nodes to access their own different data.

4. Excellent scalability. OTP is designed to tolerate rapid growth in terms of data volume, number of users, and visitor volume.

5. Simple trading logic. We use a network composed of proxy nodes as the data distribution network to serve as a bridge between the sender and the receiver of the data and handle complex network functions. Simplifying the logic of the client and making the data transmission easier and lighter make a great difference in IoT devices.

2.3 Dynamic Proof of Reputation (DPoR)

CPChain has adopted a Dynamic Proof of Reputation (DPoR) consensus protocol which was developed by Distributed Intelligent System Lab, Shanghai Jiao Tong University. DPoR consensus divides the whole blockchain system into three layers, as shown in Figure 9. Civilians will be eligible to run RNodes if they pass the admission requirements. Specifically designed algorithms will elect a segment of the RNodes (second layer) to form a dynamic committee (third layer). The third layer is designed for blocks' adding, verifying, broadcasting and building issues among the committee nodes. In summary, DPoR architecture can solve three main consensus issues of a large-scale network, i.e., node reputation value assessment, node election, and Byzantine Fault Tolerance (BFT) determination among the committee.

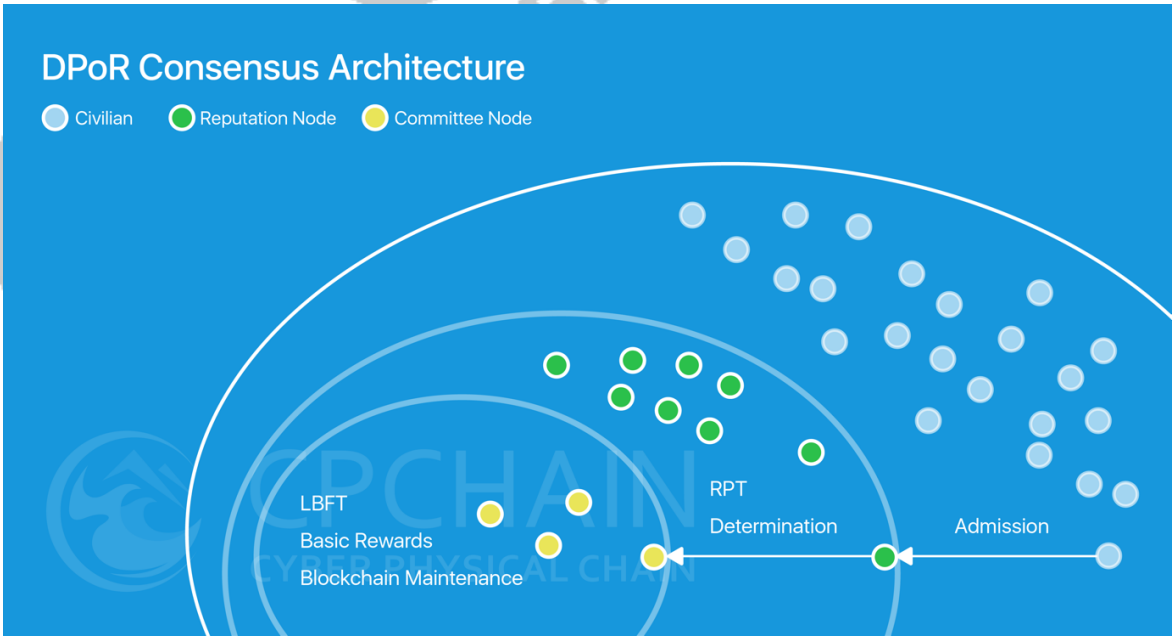


Figure 9. CPChain DPoR Consensus Architecture

2.4 LBFT 2.0 Consensus on a Large-Sale Public Blockchain

Under the large-scale CPChain system, the realization of node state consistency and distributed data storage face many challenges due to the large scale of the network and the massive volume of IoT data. CPChain is developing a hybrid consensus protocol with extendable performance and has proposed a dynamic committee election mechanism to overcome the scalability problems of existing PoW consensus protocol-based systems.

The core problem in the main chain structure lies in determining which nodes to complete the data collection and packing the chain on the block, and how to ensure block data security and consistency. Traditional distributed fault-tolerant algorithms, such as *PBFT* and *Zyzzyva*, rely more on communication complexity to guarantee consistency among nodes. For example, the *PBFT* algorithm applies a three-phase protocol to guarantee system consistency even if there is a malicious Byzantine node and recovery of node failure. However, the resulting system scalability is poor due to its increased dependence on communication to ensure the security of its algorithm. Performance thereby declines faster as the number of nodes increases, and when the number of nodes exceeds a certain threshold, the system will grind to a halt. *PBFT* relies on a primary replica which assumes the responsibility of broadcasting requests to all back-ups. Any faulty behaviours involving primary replica therefore result in a much lower throughput. Therefore, *PBFT* does not have a lower bound for its throughput. Robustness is retained as long as the system can respond in a finite time. Due to its reliability and availability at a small scale, the traditional Byzantine fault-tolerant algorithm is more suitable for a private blockchain and permissioned blockchain environments. In response to this problem, CPChain's core solution is to design a dynamic voting mechanism for its dynamic committees and elect credible committees to collect the data of the blocks and pack the tasks embedded in the blocks.

2.4.1 Bipartite Committee

Traditional Byzantine fault-tolerant algorithms cannot be directly applied to large- scale public chain scenarios, and PoW consensus protocols consume a huge amount of computing resources, which leads to a number of inefficiencies. CPChain proposes a bipartite, committee-based, three-layer agreement, *LBFT 2.0*, to enhance CPChain's consensus performance. The committee consists of two parts: *Validators Committee* and *Proposers Committee*. The

Validators Committee refers to a group of users that can validate a newly proposed block and has the following properties:

- All validators together constitute the Validators Committee.
- The Validator Committee consists of nodes nominated from the CPChain Foundation, government departments and nominated nodes.
- With the exception of some abnormal cases, validators may not produce blocks.
- The Validator Committee follows our improved LBFT 2.0 Protocol to achieve a consensus.
- The size of the number always equals to 3f + 1, where f is the number of Byzantine nodes.

The Proposers Committee is a fixed number of elected RNodes for a certain term, and has the following properties:

- The Proposers Committee is elected based on the candidate reputation and a random seed.
- Each incumbent member alternately assumes the responsibility to propose blocks during their tenure.
- The Proposer, or Block Proposer, refers to the member assigned to propose a new block in the current instance.
- A Proposer who behaves inappropriately will face impeachment from the Validators, who can punish the Proposer due to its failure in proposal.

The rest of users are named as *Civilians*. Once a civilian qualifies to run as an RNode, it can claim a campaign to be a candidate for. After being elected, the candidate can join the Proposers Committee in the future term.

2.4.2 Finite State Machine for LBFT 2.0

The LBFT 2.0 protocol can be considered as a finite state machine (FSM) with 5 states: *idle, prepare, commit, impeach prepare* and *impeach commit.* The former three states are designed for normal cases, and the latter two specialise in handling abnormal cases.

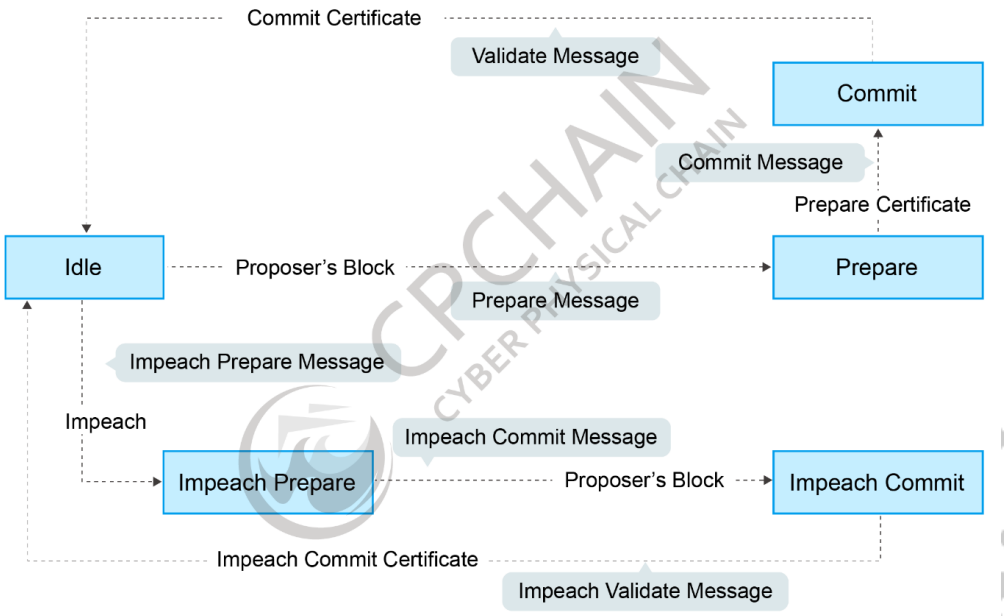


Figure 10. Finite State Machine for LBFT 2.0

Figure 10 demonstrates these five states as well as transitions between states. Under normal cases, a Validator shifts its state among idle, prepare, and commit states. While for abnormal cases, it enters either the impeach prepare or impeach commit state.

Quorum: Before we dive into explaining the case handler, let us introduce an important concept: quorum. A *quorum* is a subset of Validators Committee members structured in a way in which a consensus can be reached among this quorum in a certain state. These quorums have two vital properties:

- Intersectionality: any two quorums have at least one loyal validator in common.
- Availability: there is always a quorum available with no faulty Validator.

When members in a quorum endorse information from a same block, they collect a quorum certificate. There are two certificates, *prepare certificate (P-certificate)* and *commit certificate (C-certificate)*, which indicate that there exists a quorum which agrees on a prepare message and a commit message, respectively.

Block Production

An ordinary user claims a campaign and undergoes the admission qualification stage before being included in the candidate list. After being elected in a periodical election, a candidate

enters a block Proposer Committee. When it comes its block height, the Proposer proposes a block and broadcasts to all Validators.

Normal Case Handler

Upon receiving a newly proposed block, a Validator in the Validators Committee verifies the block via the following steps.

1. This block verification process scrutinizes the Proposer's seal, timestamp, etc.;
2. If true, this Validator broadcasts a PREPARE message to other validators;
3. Once a Validator receives 2f + 1 PREPARE messages (P-certificate), it broadcasts a COMMIT message to other Validators;
4. Once a Validator receives 2f + 1 COMMIT messages (C-certificate), it inserts the block into the local chain, and broadcasts a VALIDATE message along with these 2f + 1 Validators' signatures to all users;
5. Once a Validator receives the VALIDATE message for the first time in a block height, it broadcasts a same message to all nodes;
6. Once any user receives this VALIDATE message with enough signatures, the block is inserted into local chain.

Impeachment: Impeachment is a vital abnormal handler in *LBFT 2.0*, and is invoked when the proposer is either faulty, or unresponsive. It is a two-phase protocol in the *PBFT* manner, consisting of prepare and commit phases. When a Validator triggers an impeach process, it generates a block on behalf of the faulty (or unresponsive) Proposer. Impeachments have a higher priority compared to normal case handlers. In other words, a Validator initiating an impeachment does not process any normal case messages aside from validating messages. An impeachment can be activated under the following two cases:

- A Validator's timer expires;
- A Validator in an idle state receives an illicit block from the Proposer;

Timer expiration can be caused by several reasons, like an unresponsive Proposer, double spend attacks and improper timestamps. An illicit block can be a block with improper transactions and seal. Below are the steps necessary to complete an impeachment process.

1. A Validator V in the Validator Committee generates an impeachment block;
2. This block, used as an IMPEACH PREPARE message, is broadcast to all Validators in the committee;
3. Once Validator V receives f + 1 IMPEACH PREPARE messages with the same header and body, it broadcasts an IMPEACH COMMIT message to other Validators;
4. Once a Validator receives f+1 IMPEACH COMMIT messages, it broadcasts an IMPEACH VALIDATE message along with f + 1 signatures to all users;
5. Once any Validator receives the IMPEACH VALIDATE message for the first time, it inserts the impeach block and broadcasts the same message to all nodes;
6. All users insert the block into the local chain if they receive an IMPEACH VALIDATE message.

2.5 Side Chain Consensus System: High Real-Time Responsiveness and Security

As the basic data platform for IoT systems, CPChain is a common IoT data control layer. However, different vertical applications of IoT have different performance requirements. Typical real-time applications include unmanned vehicles, fleet coordination and so on. For such applications, CPChain needs to support secure communication and interaction with real-time control signalling in order to work efficiently and collaboratively among the various equipment nodes in the IoT system. If the data interaction is still completed through the main chain, it will face a significant 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 machine data transaction, we will focus on specific application scenarios and develop a lightweight side chain consensus protocol. Specifically, CPChain will design a side chain consensus system with edge computing and hardware security method in the industry chain to ensure that all kinds of applications can meet their delay requirements. Therefore, the high real-time responsiveness and high security of the industry chain network are realised, as shown in Figure 11.

Figure 11. Altruistic Cooperation Model with Hardware Acceleration

2.5.1 Data Gateways and Embedded Encrypted Algorithms

Due to the heterogeneity of the data collected by IoT sensors , the sensors themselves often do not have computing power, or have very limited computing capabilities. If the cognitive computing of the sensor data processing is placed in each sensor node, it will cause more delay. Because the gateway equipment deployed in the IoT system has more powerful hardware support than the sensor nodes, it can provide faster computing power, and the power of the device will not be limited. If the sensors' data is aggregated to the edge gateway for data processing and encryption computation, then the computing delay caused by data processing is reduced while the computational load of sensor nodes in the IoT is reduced, thereby prolonging the lifetime of the device.

2.5.2 Incentive and Security Mechanism for Industry Consensus Algorithms

IoT systems consists of a mesh network or wireless ad hoc network. There are many wireless communication technologies in different IoT industries, such as IEEE 802.11p and NB-IoT. Therefore, the consensus of machine transactions in IoT can make full use of the characteristics of a 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 communication layer. Additionally, considering the high concurrency, real-time usage and security requirements of machine transactions, CPChain will develop efficient altruistic cooperative incentive mechanisms and security mechanisms based on evolutionary game theory, such as altruistic

cooperative incentive mechanisms based on Directed Acyclic Graph (DAG) data structures. Therefore, the application of a CPChain side chain is more efficient, faster and safer.

2.6 Testing

The testing conducted on CPChain is a fundamental component of CPChain's continuous integration workflow. We deploy Jenkins as our automation server, and Jepsen as the framework simulating test cases.

The following sections outline our testing framework from different perspectives.

2.6.1 White-Box Testing

White box testing is for examining the internal functions and structures of the chain. Developers clearly know the functionality of all the code they test. White box testing involves three levels: *unit, integration* and *regression testing*.

Unit Testing

Unit testing is written in Golang accompanied by chain code, which is collectively stored in CPChain's repository. All unit testing files end with _test.go, and each unit testing file contains several testing functions to examine its corresponding functionality given different pairs of inputs and outputs.

Here, the functionality of Fusion API and RPC API is also tested.

Integration Testing

Some Go files in CPChain import and integrate multiple files to implement functions at higher levels. These files also have their corresponding testing files to conduct integration testing.

Regression Testing

Each time a certain branch is updated in its remote repository, Jenkins activates a regression test by going through every testing file. Through this approach, all unit testing and integration testing can be redone, ensuring that no bugs are introduced in old code blocks.

2.6.2 Black-Box Testing

Black box testing examines the functionality of the chain without a priori knowledge on its internal implementation. In black box testing, a list of test cases is curated to examine whether the chain can work properly. Each test case contains three major components:

- Scenario: briefly describe the case;
- Steps: evaluate how to reproduce the case;
- Expected result: determine the expected output as a working chain.

Abnormal Consensus

Consensus is the core of a blockchain. We need to assure the chain's safety and consistency when facing Byzantine faults among Validators and Proposers. Therefore, we have designed plenty of test cases on consensus, including abnormal and normal protocols, to test the functionality of the chain. For each possible abnormal scenario, an input and its expected output are designed for simulation purposes. This simulation is implemented by adopting the Jepsen framework.

Stability

Stability testing involves the launch, reboot, and abort of the bootnodes, Proposers, Validators, Civilians and Contract Administrators. This testing provides the proof of stability of the chain under extreme cases such as blackouts, connection errors, etc.

Mining

A Proposer has a duty to seal and mine a block. This set of test cases are categorized into several types:

- Proposer: contains curated test cases in which a Proposer conducts different behaviors.
- Campaign: examine campaign logs, APIs, candidate lists, and smart contracts.
- RNode: assures the admission of RNode is correct given different conditions.
- Reward: guarantees that both basic and maintenance rewards are correctly calculated and dispensed.

- Admission Control (AC): makes sure the threshold set for minimum CPU capacity works as expected.
- Validator: tests the validity of Validator contracts and domains.
- Start and Stop: robustness tests by aborting and restarting the chain multiple times.

Nemesis

By adopting Jepsen Nemesis, we can simulate abnormal scenarios like:

- Delays in sending packages
- Disconnection from the network
- Node crashes
- Time drifts (incorrect local clocks)

Note that some nemesis test cases may overlap with previously stated cases.

Compatibility

Compatibility is a major challenge for all decentralized systems, as not all nodes may update to the latest version. Similar to the concepts of Bitcoin's soft and hard forks, CPChain also has soft updates and hard updates. In a soft update, the old version can still work with the chain, while in a hard update, the old versions are rejected when claiming campaigns and proposing blocks, and cannot even sync with the chain.

Compatibility testing assures that the chain and all updated nodes are not affected by old version nodes.

Stress

Stress testing is conducted via increasing transactions per second (tps) to approach the thoroughput limit of the chain. Stress testing can be divided into two major classes:

1. Send out transactions in a speed close to our tps limit to help us test whether the chain can maintain stability and handle all transactions under this stress.

2. Send out transactions at a speed outnumbering our tps limit to help us test whether the chain can maintain stability and the outnumbered transactions can be postponed to successive blocks.

2.6.3 DDoS Attack

DDoS Attack, a.k.a., Distributed Denial of Service Attacks, are a major challenge all distributed systems have to confront. By uniting multiple servers, DDoS can send out a flood of requests to a single target in order to occupy all the computing resources or bandwidth of the target. A targeted machine flooded with these superfluous requests will lose its ability to answer any legal requests.

DDoS is a major concern for classic blockchains like Bitcoin and Ethereum due to their decentralised structure. Malfunctions of every single node or a small portion have literally no impact on the whole chain. However, validators of CPChain can be a latent target for DDoS attacks. Therefore, we design the following scheme to mitigate potential DDoS attacks:

1. Set up multiple trusted nodes as default Proposers.
2. Validators hold a white list that contains all default Proposers.
3. Each Validator has a monitor on its computing resources. Once the Validator experiences high performance for an extended duration, it can be considered to be under DDoS attack and activates the white list. The white list will reject all nodes except default Proposers at the firewall level.
4. When any of the following conditions are satisfied, the while list is removed:
   i. No DDoS attack detected over a period of time;
   ii. The white list has been activated for a long time;
   iii. The white list is manually deactivated.

2.6.4 Formal Specification

Software testing neither reflects any glitch, nor proves the completeness, of a piece of code from a mathematical perspective. Therefore, we are introducing a formal specification to the chain.

Formal specification languages describe a program at a higher level through a certain form or specification, such that they can determine whether the formulated is mathematically correct. Formal verification is especially important in highly parallel programs, where deadlocks and race conditions are vital issues.

To this end, we will use TLA+ as a formal specification language to ensure the correctness of CPChain's algorithms.

2.7 Performance

Under different environments, the chain performs differently. There are two particular environment setups that we are specifically interested in: a **public environment** and a **controlled environment.**

2.7.1 Public Environment

The public environment refers to the real world. It has the following traits:

- Nodes are distributed all over the world;
- Each node has drastically different configurations in terms of both hardware and network;
- Each node is operated by a distinct user that not familiar with CPChain implementation;
- Not all nodes are updated to the latest version.

All Validators deployed by CPChain Foundation have identical configurations. They are deployed on AWS (Amazon Web Services) in Singapore.

- VPS model: AWS t2.large model.
- Network condition: 1 Gbps (this is an estimated speed. AWS does not offer an exact number of network performance for AWS t2.large models)_
- Location: entirely in Singapore.
- Processor: 3.0 GHz Intel Scalable Processor.
- Memory: 8 GB.

- Number: a total of 7 servers.

Under this setting, we conducted a beta test between May 1-June 5, 2019. In total, there are 795 common nodes all over the world, and 70 RNodes and 7 verification nodes distributed across Singapore participated in the test. In the end, the Beta Mainnet received 700,000 blocks (including nearly 300,000 blocks generated during the Beta test) and 4.4 million transactions, and transaction volume peaked at 1,000 transactions per second.

2.7.2 Controlled Environment

A controlled environment refers to perfect conditions. It has the following traits:

- All nodes are either distributed in a local area network or launched across multiple threads in a server.
- The network bandwidth can be considered unlimited or having reached maximum ethernet capability.
- All nodes are updated to the latest version.
- All nodes have identical local clocks.

Under this setting, we can push our TPS to the maximum value of 10,000.

3 Business Application

3.1 Market Backgrounds

3.1.1 Smart Mobility

It is estimated that there are more than one billion vehicles on the road now globally. The extended global automotive industry is undergoing an unprecedented transformation into a new mobility ecosystem, or what we call a Smart Mobility movement driven by internet-connected and smart transportation infrastructure. The pace of change is breathtaking, and as transportation management systems evolve in in this increasingly efficient and effective era the future of mobility services will be more flexible and dynamic.

Several technological barriers and operational issues would need to be overcome before we can fully embrace the future of mobility. Technological barriers are primarily related to data collection and sharing, heterogeneous facilities and the complexity of data. Furthermore, building trust between service providers and consumers is hard, as both security and data privacy need to be treated cautiously.

In terms of operational issues, collaboration methods and incentive mechanism designs have been highlighted. User accounts and payment methods should be connected among different service providers to provide integrated services. Proper incentivization is a must to encourage new customers to share their personal data and jointly build an open data trading platform.

Blockchain's main advantages center on the fact that it is trustful, secure, collaborative and decentralised. When someone wants to trade their data on a blockchain-supported system, the trade will be protected with a decentralised platform and encryption algorithms. Hereby, blockchain can be a perfect complement to Vehicular Ad Hoc Network (VANET) technology, making personal data more secure, valid, and fully controlled by the data owners. Moreover, blockchain's incentive mechanisms can encourage more personal data sharing, thereby contributing to the vehicle data ecosystem and community. The future of Mobility as a Service (MaaS) ecosystems would benefit from the above.

3.1.2 Smart Health

Healthcare is not only a business, but a necessity. Prior to recent technological advances, health data was poorly collected, stored and shared, which restricted illness treatment and control. Since the advent of Smart Health, digitalisation and health information technology have expanded to the entire health industry. To date, medical treatment, facilities, services and business models are all on their way to becoming digitalised in a format which is widely accepted by healthcare practitioners.

Many governments have shown their support for digital health and developed related strategies. Electronic Health Record (HER) and Health Information Technology (health IT) have been widely adopted in new medical systems. However, due to the complexity of medical systems, there continue to be concerns regarding security, integrity and proper control. Moreover, hospitals, pharmacies, payers/insurance companies, and government institutions are isolated, meaning health data cannot be shared freely. These data silosthe lack of traceability medical supply chains have a negative effect on academic research and medical services, and allow for the proliferayion of counterfeit drugs production and sales.

Blockchains are traceable to a high degree of accuracy and credibility and coordinate every stakeholders' interests by deploying well-designed data sharing incentive mechanisms. Blockchain technology combined with healthcare data and infrastructure could address many urgent issues in the industry, such as cybersecurity, data interoperability, medicine supply chain transparency, insurance credentials, fraud, and more.

3.1.3 Public Security

With the rapid development of society, technology and urbanisation, public infrastructure is continually developing, resulting in a similar trend with the evolving standards of infrastructure maintenance and safety.

Prior to Smart City construction, centralised systems have been widely used in transportation, communication, utilities, social infrastructure, waterways, public escalators and elevators. Information technology is applied on a limited basis to specific scenarios, and architectural

design often does not work with overall project management, leading to more data silos. As a resul,t information technology cannot fully execute its dormant power. Furthermore, a single attack could easily crash a centralised system, leaving the infrastructure system with zero response options and resulting in public safety concerns.

Blockchain technology could provide transportation, communication, utilities, social infrastructure, waterways, public escalators and elevators with trustful and low-cost solutions, playing an important role in supply chain tracing, tracking and verifying. Blockchain can solve facilities' authentication issues and security concern by linking devices and human beings.

Blockchain-based smart city systems combine peer-to-peer networks, data encryption, consensus mechanisms, smart contracts and other technologies to effectively improve the security of smart city IoT systems. Every on-chain record is associated with a physical IoT device, which guarantees the authenticity of on-chain data. Decentralised blockchain architecture could effectively prevent large-scale IoT infrastructure from crashing. Even if one of the connected devices is under attack, the rest would continue to operate normally. As a result, social services would not suffering from any interferences.

3.1.4 Decentralised Identification (DID)

In recent years, online digital identity management has gained considerable attention. 18 OECD[1] member countries announced or are considering having digital identity management policies. The U.S. also announced the *National Strategy for Trusted Identities in Cyberspace* (NSTIC) initiative in April 2011. The initiative introduced an identity ecosystem framework in a trusted cyberspace setting. However, several concerns are still awaiting practical solutions.

Lack of Personal Data Validity: users do not have full control over their identity even once their identity is verified. It is hard to confirm the digital identification's owner as the person per se, and it is also difficult to trace DID systems.

Lack of Infrastructure: there are more than one type of personal identification, and each one applies to a different scenario. However, in most cases centralised authentication systems do

[1] Organisation for Economic Cooperation and Development

not interact with each other, and even they do system authentication is very time-consuming. Generally speaking, coordination and management are tough.

Privacy Leakage Risks, Due to Simple Authentication Technology: currently, most major authentication platforms employ simple authentication technologies, raising considerable risk in regards to privacy leakages and illegal trades.

DID is inseparable from the identification and authentication of IoT devices. The identification of IoT devices is a prerequisite for the secure communication of IoT devices. Currently, IoT device authentication suffers from following issues:

- Limited storage, computation and communication resources;
- Scalability issues brought about by the large-scale of IoT device networks;
- Risks exist when edging nodes manage a large number of IoT devices.

A blockchain-based DID system complies with end-edge-cloud architecture, forms DPKI systems and provides scalability with IoT systems. For unqualified IoT devices (which cannot support DID-related computing and storage requirements), edging nodes would assist DID generation, authentication, authorisation and other services. Lastly, to resolve management risks, a PUF module has been implemented as it allows for the device to reproduce a large number of keys without storing extra data.

3.2 Real Applications

3.2.1 Seamless Car Parking

3.2.1.1 Background

Safety is always the top issue in the transportation field, and is even more significant in the Smart Mobility sector. However, in this rapid developing society, a substantial amount of artificial intelligence systems is required to incorporate into new smart city infrastructure, such as the Xiong'an New Area case. In a transportation system where various computers, networks and processors are interconnected, a single attack could result in severe outcomes, from financial losses to the endangering of human lives.

China's rapid urbanisation has developed ahead of its infrastructure construction. Traffic, for example, is often chaotic, and parking is time- and money-consuming. These pain points persist in every major city in China and create a range of issues for city management. The government has made efforts to make parking easier, but nonetheless parking lots are unreasonably allocated and utilisation rates are quite low. With the development of electric vehicles in recent years, the lack of charging facilities has been a particular sticking poit. The irresponsible parking of traditional fuel-powered has also made the situation worse. To improve urban life, advances in information technology should foster new solutions for parking and charging issues to enhance daily life.

3.2.1.2 Solution

CPChain Foundation and a renowned luxury automobile company[2] have jointly provided a solution to the current parking and charging issue. The answer lies in distributed identification technology and a seamless charging and parking system. This system boosts the efficiency of chargeable parking lots, eliminates the practice of inappropriate parking of fuel-powered vehicles, and provides vehicle owners with seamless payment options.

Electric vehicles are equipped with an embedded blockchain device, so vehicle owners can upload their driving-related data to the blockchain and receive financial rewards as an incentive.

When the vehicle approaches the parking lot, the embedded device communicates with the smart landlock in the parking lot via Bluetooth connection, whereby the payment server verifies the identity. The embedded device would then pay the parking deposit automatically based on the blockchain's smart contract. The landlock will lower down once the deposit is verified, and the vehicle will then be ready to park. Once the vehicle is parked, an ultrasound sensor will be activated and start timing.

Once the vehicle leaves the parking lot, the ultrasound sensor will stop timing. The payment server then initiates the fees settlement and sends a message to the blockchain's smart contract.

[2] Due to Non-disclosure Agreement, this particular company's name would not be disclosed at this stage. June 2019.

Thanks to this simple, one-off auto-payment technology, parking fees will be paid automatically. For parking places who use licence plate recognition technology to calculate parking fees, smart landlocks will help manage chargeable parking lots.

The full process is unmanned, seamless, timely and secure. Along with the auto-payments and a seamless user experience, the potential value of the system's data will consequently grow.

Instead of the widely-used contactless identity authentication technology, vehicles, landlocks and charging stations use Decentralised Identification (DID) technology. A blockchain-based DID system is anonymous, unique and trustworthy. DIDs are fully under the control of the DID owners, and owners can decide which segments of their data they would like to upload to the blockchain, if any. Only the owners and authorised DIDs have access to this verified data. Unauthorised parties will only be able to see the DID's signatures on the information required for verification. This means personal data is securely protected. If a vehicle is linked to the owner's DID, the user can provide limited personal information when a parking lot or a charging station requires authentication, thereby protecting his or her personal information.

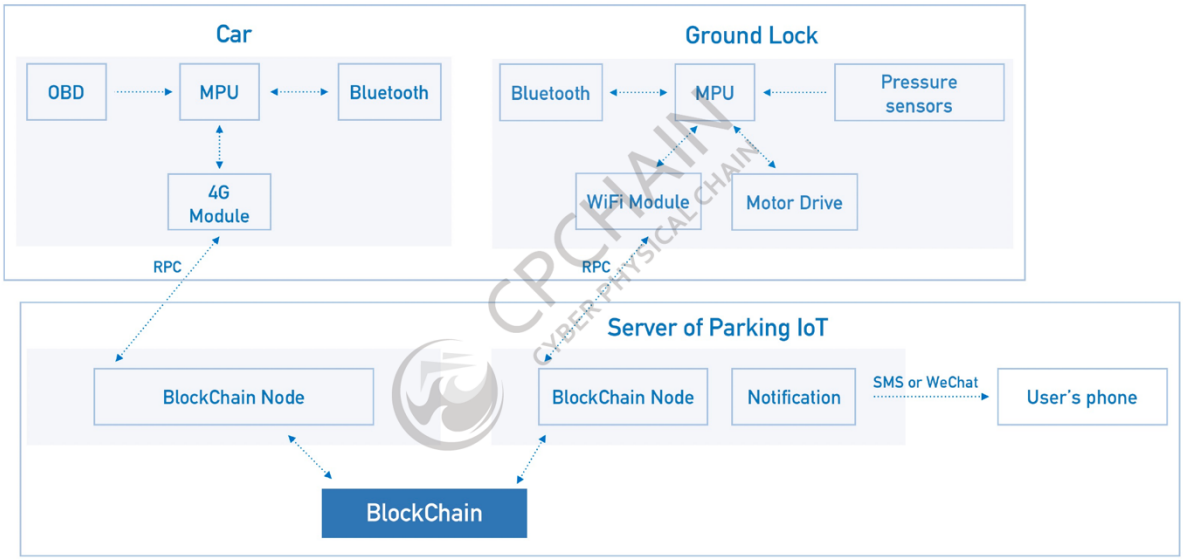


Figure 12. CPChain's Seamless Parking Architecture

3.2.2 Shared EV Charging

3.2.2.1 Background

The world still does not have enough places to recharge electric vehicles (EVs).

Drivers' Pain Points:

- Shortage of charging facilities;
- Every charging platform requires registration, which is troublesome;
- The charging station market is not sufficiently transparent.

Operators' Pain Points:

- Operators refuse to engage with one another in this highly competitive market;
- The market is highly fragmented;
- OEMs' charging facilities are complicated.

3.2.2.2 Solution

Smart facilities are used for:

- Authentication: EVs auto-connect to the charge station and verify the car owner's identity;
- Seamless charging: car owners can simply plug their cars in;
- Transaction: auto-settlements, with safe and transparent transactions.

CPChain Foundation has installed several smart IoT devices in existing electric vehicles. The device is fully developed by CPChain, supports DID and blockchain technology, and enables peer-to-peer interaction between the charging station and vehicle. For registered vehicles, users no longer need to swipe credit cards or membership cards. They can simply plug in, and the IoT device in the charging station will be activated and begin timing while the car is charging. Likewise, drivers can simply unplug when their vehicle has finished charging, and the device will calculate fees and receive payment automatically. Vehicle owners can then check the invoice in their specified channel. This is the full process of seamless charging.

This solution is expected to be applied to more vehicles, and CPChain is holding more discussions and consequently moving blockchain technology forward, adding value to the mobility industry. CPChain also attended the *Yangtze River Delta Economic Zone Innovation Exhibition* as one of the fifty-five technological representatives in Shanghai, where the solution was widely recognised and praised.

Figure 13. CPChain Charging & Sharing System

3.2.3 Drugledger: Drug Tracing

3.2.3.1 Background

Product Identification, Authentication and Tracking System (PIATS) is a barcode system used in China since 2008. The system is applied to healthcare products and requires manufacturers, repackagers, wholesale distributors and dispensers to comply with new product tracing requirements.

The US implemented the *Drug Supply Chain Security Act (DSCSA)* on November 2013, requiring drug manufacturers and repackagers to affix or imprint a “product identifier” on

packages for certain prescription drugs intended for human use. The “product identifier” must be machine-readable, unique and traceable.

The European Parliament and The Council of the European Union (EU) published *Falsified Medicines Directive* on July 1, 2011. This directive introduces collective European measures to fight medicine falsification and ensure that medicines are safe and sold in a rigorously controlled market. Measures include a unique identifier and an anti-tampering device, strengthened record-keeping requirements for wholesale distributors, and more.

Traditional medicine supply chains have following issues:

- Difficulties in protecting every stakeholders’ commercial privacy;
- Difficulty in sustaining data authentication and stability;
- Collaboration gaps within the supply chain;
- Compatible issues with the current ERP management system;
- Systems which are vulnerable to DoS attacks, which raises security concerns.

3.2.3.2 Solution

To the solve above issues, CPChain developted Drugledger, which is comprised of CSM, QSM and ASM:

Certificate Service Module (CSM)
CSM is embedded with a public key facility and provides users with dynamic management services (for example, only certificated users can enter to the blockchain network). In general, CSM plays a system supervision role.

Query Service Module (QSM)
Provides all the stakeholders and patients with medicine tracing services.

Anti-attack Service Module (ASM)
Checks for abnormal activity in the system and maintains the system services.

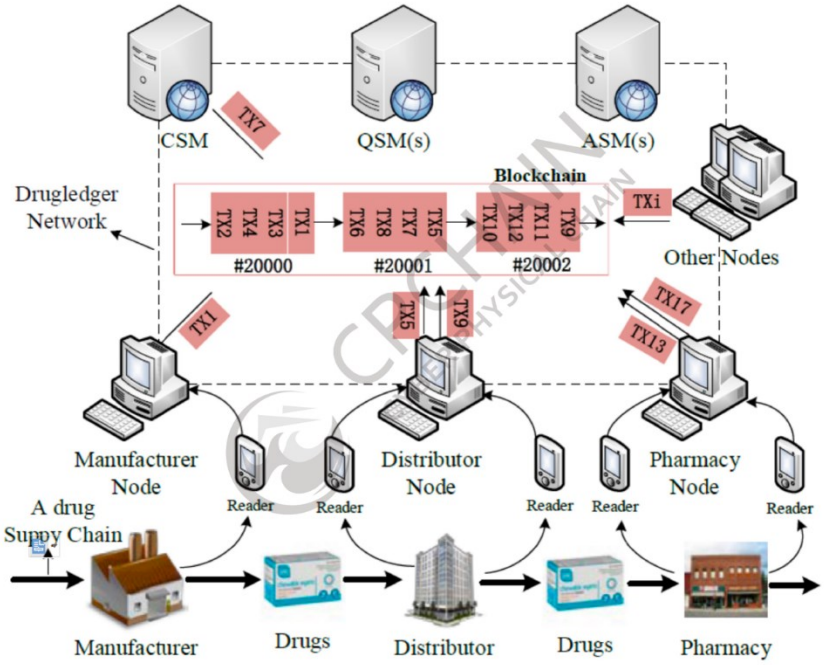


Figure 14. CPChain's Solution for Medicine Tracing

3.2.3.3 Realisation

CPChain developed a PC application for suppliers and healthcare institutions to supervise their supply chains in real-time. CPChain also developed a mobile application for healthcare suppliers and institutions, allowing them to operate drug imports and exports, packaging, and unpacking. A third application has also been developed by CPChain for consumers, who can check the logistical information of their medication in order to ascertain its authenticity.

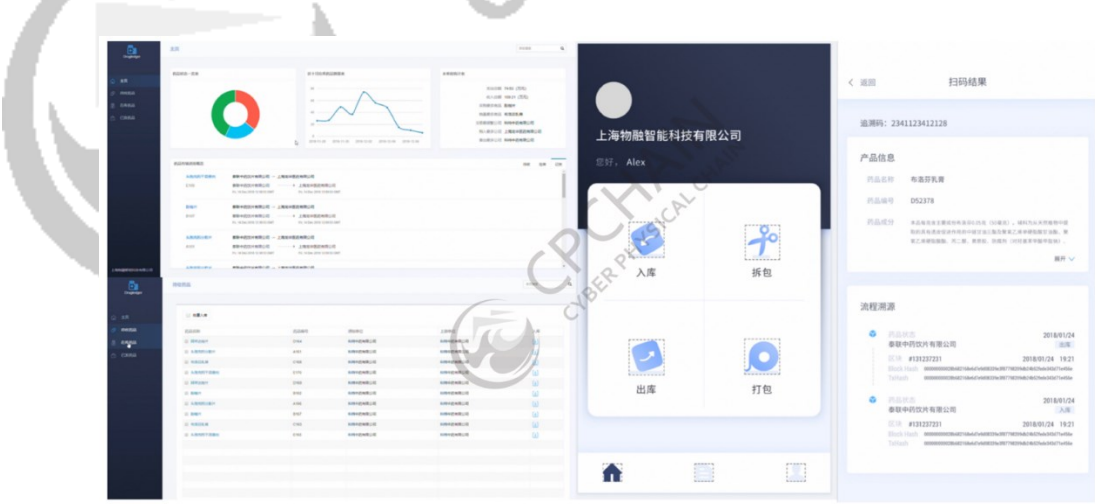


Figure 15. Drugledger by CPChain

3.2.4 Driving Training Chain

3.2.4.1 Background

- In China, driving tests can only be taken after at least 40 hours of training. However, many training hour records are fake.
- Currently, a fingerprint identification device is used to verify trainees' identification, but cheating the system is still comonplace.
- Driving training data can be tampered with by external parties.
- Lack of customised driving behaviour analysis and tracking records after training.

3.2.4.2 Solution

CPChain Foundation and the China National Safe Driving Engineering Technology Research Centre jointly proposed a new driving training hours regulatory system. The system is expected to solve multiple issues, including training fraud, scattered data records and trust issues among regulatory agencies.

This driving training system has an IoT device embedded in the training vehicle which can verify the trainer and the trainee's identification at the beginning and end of the training session. The device also has a camera to take photos randomly, ensuring that trainers and the trainees are involved throughout the entire process. Training times, routes, braking and accelerator-related data will be collected alongside these snapshots during the session, and all the collected information will be uploaded to the blockchain. Noted that the data will be undeniably genuine since it is uploaded directly from the IoT devices. If there is a tampering attempt, the system will report the tampering behaviour and mark the contaminated data for review. Meanwhile, related regulatory institutions will be included in the blockchain as master nodes.

This system also reviews data automatically and flags fraud and/or tampered data. This system will effectively guarantee that the requisite 40 training hours has been reached by every candidate, which benefits all the involved parties and contributes to a safer society.

3.2.4.3 Realisation

CPChain Foundation and Anhui Sanlian Transportation Application Co., Ltd. took the lead in applying the Driving Training Chain. Training schools' records are uploaded to the chain, then the system compares historical data with the chain on a daily basis, alerting the relevant parties of any suspicious situation. This solution won the third *China Innovation Contest and the First Yangtze River Delta International Innovation Contest: Blockchain*'s *Best Ecosystem Innovation Reward*. Furthermore, CPChain Foundation, the National Safe Driving Technology Engineering Technology Research Centre and the Distributed Intelligence Laboratory of Shanghai Jiao Tong University are jointly working on a project involving IoT technology, blockchain technology, artificial intelligence (edging computing-based) to solve problems in driving simulation, driving training and safety controls for car-pooling. The project also plans to analyse training and driving records data, generate safe driving advice, collect body temperature records from wearable devices, report emergencies based on external camera and image analysis, and mitigate inappropriate behaviour based on interior cameras and image analysis.

Figure 16. CPChain Driving Training Demonstration

3.3 DApp

3.3.1 PDash Data Sharing

3.3.1.1 Background

Let us take the mobility industry as an example. Undoubtedly, the mobility data market has great potential. According to an academic report, the market will grow to $450-750 billion USD by 2030.

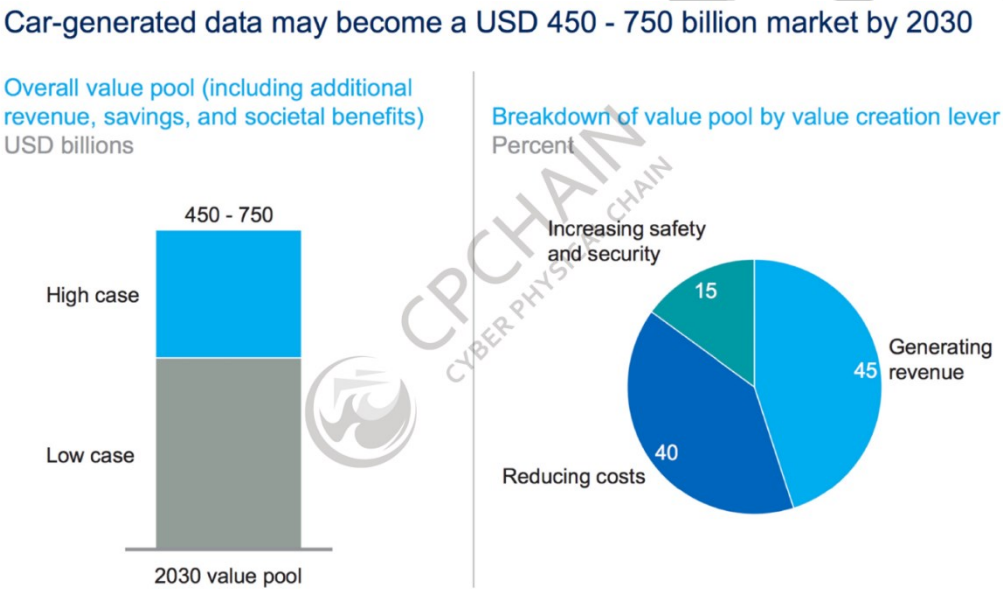


Figure 17. Mobility Data Market Forecast

3.3.1.2 Solution

PDash aims to eliminate information gaps between data providers and consumers, providing a fair, transparent and efficient data transaction platform.

- Wallet: provides transaction accounts for all types of users;
- Open market: a transaction platform for data providers and consumers;
- Distributed proxy network: protects data security and privacy.
- A public chain developed by CPChain: connects all parties.

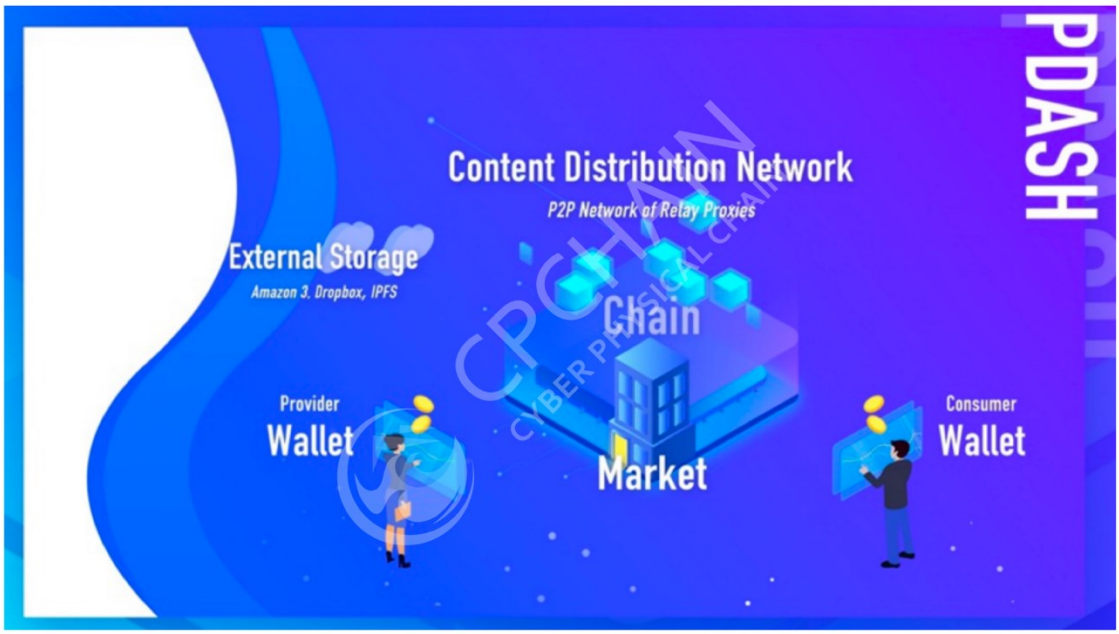


Figure 18. PDash Data-sharing Platform Architecture

3.3.1.3 Realisation

IoT static data and streaming data are currently available in PDash, and are ready for trade. Welcome to PDash!

PDash open source address: https://github.com/CPChain/pdash

4 Economic Model and Overall System

CPC is a primary asset on CPChain, and CPC's value origin relies on the fact 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 insufficient.
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 pay 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 day-to-day operations, commercial promotions and technological 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 the client company, and the application development provider receives 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 its end customers and provide its traditional enterprise customers or end users with application products while receiving CPC as its enterprise revenue. The end user can pay CPC for business products and services.

5 CPChain Community

5.1 Reputation Node Ecosystem

5.1.1 CPChain Nodes: Types and Pools

The RNode Ecosystem describes the responsibilities and rights of all nodes, including miners, and nodes are categorized into three types according to their deposit amount in two pools and balance.

- **Economy Node:** Requires a minimum of 20,000 CPC tokens deposited in the Economy Pool for participation. Investors who meet this requirement may participate as an economy node and have the right to vote in the community.
- **Reputation Node (RNode):** Requires a minimum of 200,000 CPC tokens deposited in the RNode Pool for participation. Investors with the requisite configuration for computing and storing can participate to support the CPChain Open Transmission Protocol (COTP).
- **Industry Node:** IoT Industry partners and the CPChain ecosystem's peer developers have the right to participate as an Industry Node.

Note that there are two separate pools for deposit.

- **Economy Pool:** Any node which deposits at least 20,000 CPC tokens in this pool qualifies as an economy node. The deposit is locked-up for at least 90 days, and can only be withdrawn during an assigned time window.
- **RNode Pool:** Depositing at least 200,000 CPC tokens in this pool is a prerequisite to becoming an RNode. This deposit is locked-up for 100 minutes, and RNodes that are elected to mine blocks in future terms cannot withdraw their deposits.

5.1.2 RPT Determination

The RPT (abbreviated from reputation) value of a node is evaluated by extracting data from the blockchain. By employing a RPT Contract, a node can evaluate its RPT value by the following five dimensions:

- Account Balance (AB): a node's CPC balance has a positive correlation with its RPT;
- Transaction (TX): all transactions in the system count;
- Data Contribution (DC): data uploading of a node will be rewarded by increasing the corresponding RPT value. Basic rewards will be granted once data has been uploaded, and extra rewards will be granted if the data has been purchased.
- Blockchain Maintenance (BM): every committee member will receive an RPT reward after every round of block building.
- Proxy Reputation (PR): a proxy node will acquire an RPT reward if it assists others' trades.

Each dimension has a full score of 100 points. The total score is calculated according to the following formula:

$$RPT = 0.5 * AB + 0.15 * TX + 0.1 * PR + 0.15 * DC + 0.1 * BM$$

5.1.3 Node Rewards

CPChain's ecosystem is established via a constellation of IoT enterprises, developers and users. It is a long-term process. As a result, CPChain will divide the incentive system into two stages. In the first stage, the CPChain Foundation will be the main fund provider for ecosystem establishment and chain maintenance. The next stage will mainly be operated by the market. With the optimization of the CPChain ecosystem and the increase in data sharing and transferring, the reward for RNodes will mainly be generated from smart contracts and market transactions.

Rnodes' entitlements will be allocated across two segments: *basic rewards* and *maintenance rewards*.

Basic Rewards

CPChain will create a reward pool with 5 million CPC annually (1.25 million CPC quarterly, 13,700 CPC daily). Economy Nodes will receive their corresponding CPC reward based on the ratio of the locked margin to the total margin (Economy Node and RNode both need a 90-day lock-up session). The detailed process is as follows:

Each season lasts 90 days, including the first 3 days for the raising period, the 84 days for the lock-up period, and the last 3 days for the settlement period. There is no overlap between each period, and the second period can only be opened after the end of the first period. Each period does not overlap with other one. And the contract will always either be in the raising period, the lock-up period or the settlement period. In the raising period, you can deposit tokens into the Economic Pool or withdraw the tokens. No operation is permitted during the lock-up period, and interest for each season can be taken away during the settlement period. If the user does not take the interest, the administrator will assign them one by one.

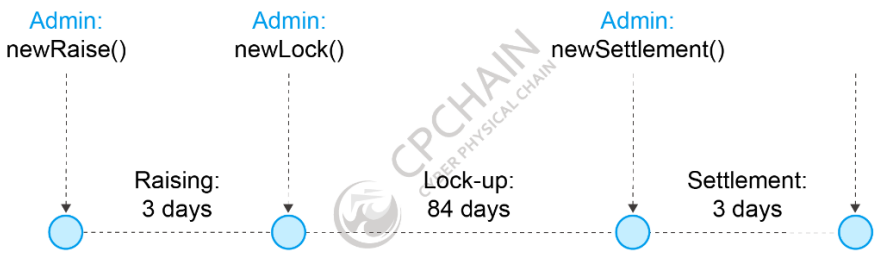


Figure 19. Economy Nodes: Basic Rewards

The reward for a certain node from the pool is proportional to its deposit in a season. In other words, the basic reward is calculated as 5,000,000 ∗ d/D, where d is the deposit of a certain node, and D is the total value of the coins in the reward pool.

Year	Rewards	No. of Blocks	Supply
1	12.65	3,162,240*	40,002,336
2	9.51	3,153,600	29,990,736
3	7.13	3,153,600	22,485,168
4	5.39	3,153,600	16,997,904
5	4.03	3,162,240*	12,743,827

Table 1: *: *Both the first and the fifth year contain a leap day (Feb 29, 2020 and 2024, respectively), which results in a larger number of generated blocks relative to the other three years.*

Maintenance Rewards

Proposers Committee nodes are entitled to blockchain maintenance rewards, after they propose a block and successfully get it inserted into the chain. As defined in the RNode ecosystem, the annual supply from maintenance is 40 million CPC in the first year, and this amount will decrease by 25% annually for the next four years. Thus, the annual supply for the first five years is 40 million, 30 million, 22.5 million, 17 million and 12.75 million respectively. After five years, the supply runs out and the system will seamlessly switch to the market incentive phase. Block rewards will be provided mainly by the gas cost of smart contracts and the transactions.

Meanwhile, the CPC Mainnet inserts a block every 10 seconds, which yields around 3 million blocks each year. The resulting reward and supply are laid out in Table 1.

Note that in our *LBFT 2.0* protocol, an impeach block is inserted into the chain if the Proposer is faulty or unresponsive, and a faulty Proposer cannot receive their reward. Hence, the actual amount of the annual supply could potentially be smaller than the values listed in Table 1.

5.2 Board of Directors

The Board of Directors is the core organisation of CPChain Foundation, and is responsible for leading CPChain to a well-managed ecosystem with high level of efficiency. The CPChain Foundation invites well-known organisations, corporations and individuals to jointly build CPChain's main chain global ecosystem. This community will provide decentralised services to various industries, corporations and individuals, and eventually create a dynamic ecosystem for the integration of blockchain and IoT.

5.2.1 Description

The Board of Directors consists of three parts, and members are either nominated or appointed by the Foundation or elected by the community.

5.2.2 Rights and Responsibilities

The Board of Directors is expected to participate in CPChain's strategy development, decision execution, financial supervision, and more. CPChain's Board of Directors is obligated to

disclose material information, such as CPChain's technological development stage, operational situation and CPC distribution, and the Board also needs to assist third-party auditors to generate audited annual reports.

5.2.3 Term

Members of the CPChain Foundation Board serve a one-year term, and are elected annually.

5.2.4 Election

Besides Directors nominated and appointed by the CPChain Foundation, all community members whose account balance is over 200,000 CPC are eligible to be elected as Directors. Candidates need to submit several documents to participate in the election process. Also, during the election period and while serving as a Board Member, elected Directors will not be allowed to sell their CPC.

5.2.5 Return

The Board of Directors has an annual income of 400,000 CPC and will be paid on a semi-annual basis.

5.3 Committee

The Board of Directors makes recommendations to the Board for discussion and action and collects different parties' opinions regarding technology trends, the community and ecosystem. The Board of Directors accomplishes much of its work through committees, and the CPChain Foundation has two standing committees: the Technology Committee and Ecology Committee.

The Technology Committee recruits and orients the developer community and develops new technologies in a collaborative manner. The Technology Committee is empowered to take charge of the main chain's maintenance and updates, ensuring that the chain aligns with the ecosystem. The Ecology Committee is in charge of the main chain ecology. It manages project

incubation, investment, business development and node management. Both committees consist of five to nine members.

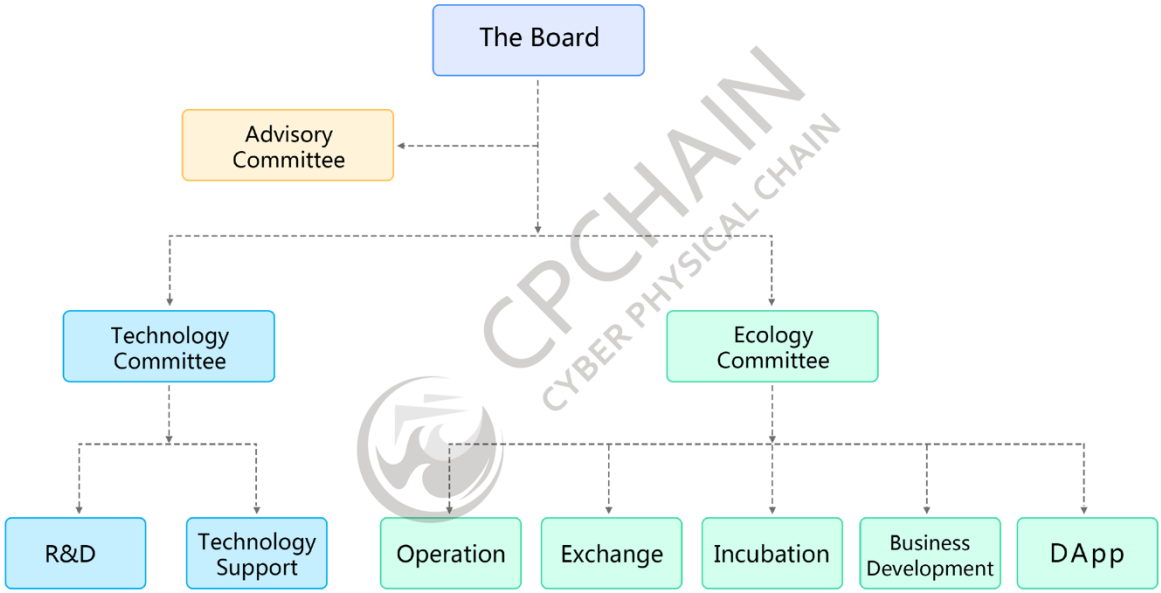


Figure 20. CPChain Structure

5.4 CPChain Foundation

5.4.1 Structure

The CPChain Foundation Board of Directors has five or more seats, including one Chairman and one Secretary. The CPChain Board of Directors is essential to the health and sustainability of CPChain ecosystem.

5.4.2 Rights

- All Foundation members have right to vote and to be elected as Directors.
- The Board makes strategic management and ecosystem development decisions.

5.4.3 Responsibilities

The Board keeps track of the Foundation's financial conditions, reviews funds using established policies and internal financial controls. The Board needs to support CPChain's technology, business and the whole ecosystem's sustainable development.

The ultimate goal of the Board is to provide strong, powerful and abundant resources to CPChain.

5.4.4 Term

Each member of the Board serves a one-year term, which can be lengthened.

5.4.5 Eligibility

Board Chairman

Secret ballots are used in the CPChain Foundation Chairman elections. Every committee member has the right to vote and be elected.

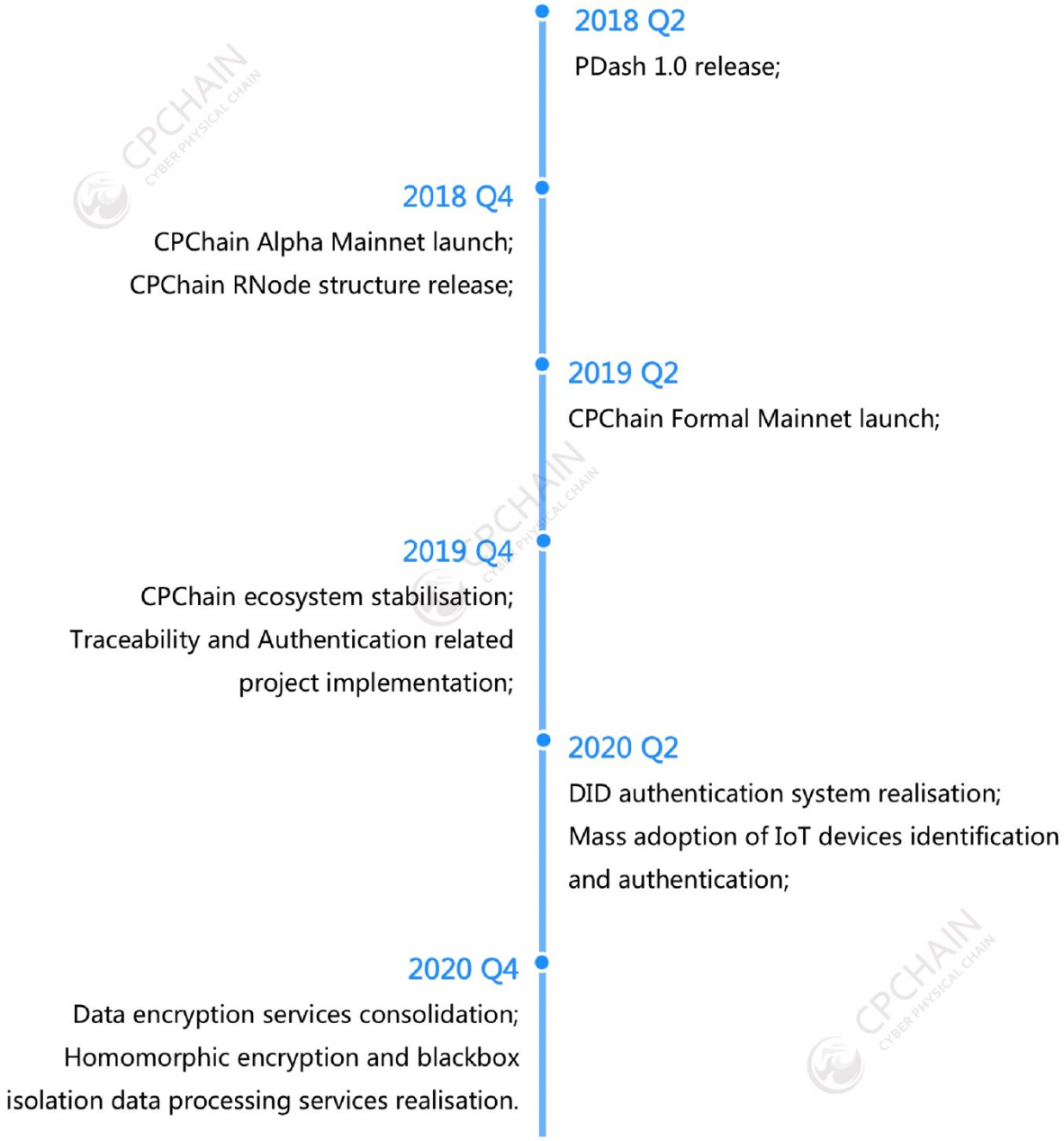
A candidate's approval rating has to reach 50% to become a Chairman. If no candidates have an approval rating of 50% or above, another election round would be conducted until a round is successful. Candidates with the lowest ratings will not progress through the election process.

Recall

Should any Foundation member come to be perceived as not properly discharging their responsibilities, they can be recalled with a written request endorsed by a specific number or proportion of voters. The recall decision must be disclosed to the community.

Recalled members have the right to publish a working report to the community, and they are allowed to appeal the recall decision.

6 Roadmap


2018 Q2
PDash 1.0 release;
2018 Q4
CPChain Alpha Mainnet launch;
CPChain RNode structure release;
2019 Q2
CPChain Formal Mainnet launch;
2019 Q4
CPChain ecosystem stabilisation;
Traceability and Authentication related project implementation;
2020 Q2
DID authentication system realisation;
Mass adoption of IoT devices identification and authentication;
2020 Q4
Data encryption services consolidation;
Homomorphic encryption and blackbox isolation data processing services realisation.

7 Financial Report

7.1 Token Distribution Plan

The total amount of CPC tokens will be 1 billion and 40% will be used for funding the 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 allotment of CPC will be used in the development of the overseas community. Institutional investors refers to enterprises within 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 CPC in their commercial activities.
20%	Founding team, development team and consultants	The founding team, as well as the development team, are making substantial contributions with their human, technological and material resources throughout the development of the project. Therefore, this CPC will be used as a reward and will be locked up for four years, with the full amount locked up in the first year and released in batches each following year.
40%	Community governance	This CPC will be used to maintain the continuous operation and development of the team, fund commercial application exploration and promotion, the selection of suitable industries for strategic deployment in the industry, project support and replacement of tokens for industrial applications that truly satisfy market needs.

7.2 Project Budgeting

Daily Operations	35%	Initial team salaries, recruiting experts and developers, technical patents and intellectual property protection, Foundation operation and marketing expenses, etc.
Technology Development	35%	Technical development, communication and sharing; regular journal publications; creation or participation of alliances; community incentives, etc.
Business Development	20%	Maintain a series of business channel collaborations such as expanding and operating of the CPChain Foundation
Investment	10%	Investment in new blockchain technology and new team members

8 CPChain Team

Chief Executive Officer, Founder

Dr. LONG Chengnian

Dr. Long is a professor with many years of R&D experience in the fields of cyber physical system security, Internet of Things, distributed intelligent systems and blockchain technology. His research results won the second prize of the National Natural Science and the first prize of the Natural Science of the Ministry of Education.

Chief Product Officer

Dr. ZHAO Bin

Dr. Zhao has more than 12 years of research and development experience in the fields of telecommunication, Internet of Things and FinTech, with extensive experience in R&D management. He has 3 patents for his inventions in the field of IoT technology.

Chief Operations Officer

Mr. SHI Qingwei

Mr. Shi is an early participant in blockchain technology and digital currency. He is the founder of *Shared Finance,* and has been an active participant in the investment and development of many successful projects.

Chief Technology Officer

Dr. MA Shiyao

Dr. Ma graduated from Tsinghua University in 2013 with a B.S. in Computer Science. In 2018, he received his Doctorate from the Hong Kong University of Science and Technology. He primarily focuses on blockchain technology, data centre networks and function parallelism.

Business Development
Director
Alec Chan

Product
UI Designer
Ivy Jin

Product
UI Designer
Cici Qin

R&D
Python Engineer
Jinlong Liao

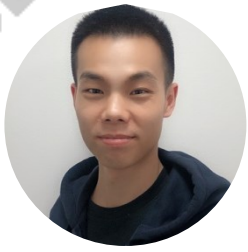
R&D
Software Engineer
Jason Liu

R&D
Software Engineer
Alex Shi

R&D
Python Engineer
Jiajing Wu

R&D
Senior Software Engineer
Mingxian Xu

R&D
Front-end Engineer
Kai Zhang



R&D
Software Engineer
Wuxiang Zhou

Operations
Content Writer
Junqinag Ma

Operations
Overseas Operations Director
Wayne Tian

Operations

Community Operations Manager

Fay Wu

Finance

Accountant

Luman Yang

Administration

Human Resources

Yue Zhang

Operations

Chinese Operations Director

Rhea Wu

Finance

Financial Director

Guoqi Zhang

Internet of Things

Engineer

Yu Luo

9 Collaborations

Industry Partnership

Project Partnership

Academia Partnership

Capital Partnership

Association

Industry Node

"The Institute of Automobile Enterprise Management and Innovation" of the NCUT

State Key Laboratory of Cognitive Neuroscience and Learning of BNU

BUPT Information Security Center

10. Disclaimer

This white paper is for informational purposes only and does not serve as a prospectus, offer file, securities offer, offer for solicited investment, or offer for the sale of products, materials, or assets (digital or otherwise). The information may not be exhaustive or completely accurate; nor does it imply any element of contractual relationship.

You acknowledge that any services provided by CPChain and information stored and transmitted on CPChain platforms may be lost, damaged, or become temporarily unavailable due to computer software failure, protocol changes by third-party service providers, network failure, or other force majeure. “Other force majeure” includes but is not limited to third-party distributed denial of service (DDoS) attacks, regular or ad hoc maintenance, and other reasons within or beyond CPChain’s control. You agree to bear complete responsibility for all losses sustained should any of the aforementioned occur.

The use and purchase of tokens sold by CPChain involves high financial risks. CPChain hereby declares that transactions made on the CPChain platform do not constitute the issuance of negotiable securities in any jurisdiction. Documents published on the CPChain platform do not constitute the raising of investment funds.

No plans are in place for CPC tokens (as defined by this white paper) to constitute as a security or other controlled product category in any country or jurisdiction. This white paper is not a prospectus or a document used for the issuance or fundraising of securities or controlled products in any country or jurisdiction. This white paper has not been reviewed by any regulatory authority in any country or jurisdiction.

This white paper makes no declarations or promises assuring that the information, statements, opinions, and all other matters (including prospective or conceptual statements and results) described or conveyed pertaining to the project are correct or complete. In addition, this white paper makes no declarations or promises assuring matters not mentioned above. No part of this white paper shall constitute or be deemed a declaration or promise regarding future affairs. To the extent enforced by applicable law, any person who has sustained any damage or loss (foreseeable or not) because of actions taken on the basis of this white paper will be held solely

responsible for said damage or loss, regardless of whether such actions have been taken due to negligence, acquiescence, and/or inattentiveness.