2019

CPCHAIN
CYBER PHYSICAL CHAIN

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 era. Using Next-generation technologies like Internet of Things (IoT), Blockchain technology and more, these businesses improve operations and achieve game-changing outcomes. They invent new business models and put old ones online. They empower transportation, healthcare, logistics, warehousing, supply chain and many others.

Traditional centralised Internet of Things system suffers from high connective costs and poor business models. Meanwhile, with data collection technique's continuously developing, privacy leakage remain exists and even is getting worse. The public's growing security concern requires for a reliable privacy protection mechanism that would not hinder the sharing and flowing of data.

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

Table of Contents

1. Overview

1.1 Internet of Things: Current Stage and Pain Points

1.1.1 Internet of Things: Industry Requirement and Market Overview

Internet of Things (IoT) is a major development and revolutionary opportunity in the information field. It highly integrates advanced information technology, communication technology, sensor technology and computer technology to establish a global dynamic network infrastructure. All smart objects (RFID tags, sensors, smartphones, wearable devices, etc.) are interconnected and all information and data are shared and transmitted for full awareness, reliable delivery and intelligent processing.

Internet of Things is all about bridging the real world with the virtual data world. According to *Gartner*, a well-known market research company, IoT devices will outnumber 26 billion by 2020, and the revenue streams of IoT products and services are expected to reach $300 billion. IoT is playing an increasingly essential role in the seamless data integration and data value chain formation.

1.1.2 The Challenges in Centralised Architecture of Internet of Things Systems

Currently, the IoT adopts the centralised technology and operation mode in the fields of smart mobility, smart home and healthcare, i.e. the "data silo" IoT architecture, and faces the common problems in connection costs, trust, data value and business models.

Technology Challenges

Low compatibility: Many IoT Systems are poorly designed and implemented, using diverse protocols and technologies that create complex and sometimes conflicting configurations.

Inefficient architecture: In recent years, as the price of components such as computing devices, storage devices and sensors has declined, IoT devices are exploding. However, the existing IoT solutions are expensive because of the diverse protocols and architectures. The data centres are built for one single project and each IT system has its own management tools and databases, forming an isolated island of information in the era of billions of connected devices. In conclusion, the industry is highly fragmented.

High cost: Most of IoT devices have long life cycles and the profit is far lower than that of intelligent terminals with fast consumer goods properties, such as PCs and smartphones. But the manufacturers need to maintain the corresponding IT systems for the long term and the profits are not enough to support maintenance costs. Therefore, the equipment manufacturers are unsustainable.

Low scalability: The existing IoT device and technology do not meet the growing complexity and interconnectivity requirements, leave scalability issues.

User Data Privacy Concern

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

Data ownership. As the Big Data Era is here, monetize data-driven capabilities are important. A few enterprises employ a series of IoT devices to gather users data, develop smarter algorithm to provide customised services, and grow their revenue streams consequently. Data is mostly held by a few big platforms. Meanwhile, the *General Data Protection Regulation (EU)* became enforceable in May 2018, which illustrates the general trend of giving control to individuals over their personal data. A blockchain-IoT convergence system could protect personal data ownership while realise data value.

Data incentive. Personal data would be the main source in a foreseeable future. Most people are not bothered to gather and manage their own data without proper incentives. Individuals to data economy, is like cells to organism; it is fundamental. Getting used to collecting, managing and applying personal data among the majority of individuals is the prerequisite to boost data economy. The current situation is that big enterprises held most of data-generated revenue. Individuals should have been motivated and rewarded, as people are the main data contributors. Only with appropriate incentive mechanism, individuals would be motivated and contribute more valuable data, while organisations and enterprises would have a greater database.

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

Business model. Networking, computing, storage and other functions of IoT devices bring about an increase in costs. But for most of the traditional devices such as sensors, networking is not the core function, and relying on the mode of selling hardware alone cannot support the huge overhead incurred by the long-term maintenance of corresponding IT system. Under the current centralised architecture, most manufacturers cannot make full use of the IT function system of the IoT device, and the business model is simply selling user data. This is allegedly infringing upon the rights and privacy of users. With the IoT system further development and openness and users' safety awareness, the current business model will certainly usher in change.

1.2 Blockchain Technology Brings New Potential to the Internet of Things

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

Significantly reduce the cost of equipment interconnection

The core concept of Blockchain technology is distributed ledger, that is, an open, distributed database maintained by multiple parties. Based on the blockchain, we can build a 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 interconnection and post-IT system maintenance. Therefore, the decentralised IoT system, based on the blockchain technology, is sufficient to carry tens of billions of connected device data.

Significantly protect privacy

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

Realizing the share of data

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

Create brand-new business model

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 devices, etc. Not only does the device perform a single function. The blockchain not only simply interconnects the device, but also enables devices to interact with each other autonomously. Vendors no longer need to maintain hundreds or thousands of IT systems in different systems. Changing roles will attract more participants, reshape market rules and create entirely new business models.

1.3 IoT-Blockchain System: Market and Application 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 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 about blockchain market. It is estimated the total value of the blockchain-IoT market will increase from $113.1 million in 2010 to $3.021 billion in 2024, marks a 92.92% compound annual rate.

The key drivers of the blockchain-IoT market include:

- The increasing amount of IoT devices;
- The increasing demand for network's safety and stability;
- The increasing demand for operations effectiveness and efficiency;
- Blockchain IoT market's potential opportunities;
- Smart contract and digital identification's potential usage.

1.4 Commercial Blockchain Systems Are Facing Scalability Issue

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

High cost of data storage and calculation

Blockchain is a decentralised database maintained by a large number of nodes. Data keeps adding without any deleting, leaving a high storage and computing cost. However, the public blockchain application platform inevitably carries large-scale data. Under the current storage cost of blockchain, large-scale of the public blockchain based data platform is not practical.

Versatility

There are various types of data and operations in the IoT field. To fulfil diversified operations demands, the blockchain system 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. Both structured and unstructured information could be processed, and side-chain research and development could meet future demands.

Inefficiency of consensus mechanism

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

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 the Internet of things and blockchain technology. First, a parallel distributed architecture of distributed cloud storage system and decentralization blockchain system is proposed to solve the scalability problem of large-scale data storage and sharing. Second, CPChain presents a new hybrid consensus protocol for large-scale public blockchain based on collaborative optimization design of computing and communication. Finally, integrate smart IoT’s end-edge-cloud architecture and blockchain’s main-side chain design, CPChain aims to build an IoT self-sovereign identity and DPKI system based on blockchain technology, and an IoT big data sharing platform.

2. CPChain Solution

2.1 Parallel Distributed Architecture of CPChain

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

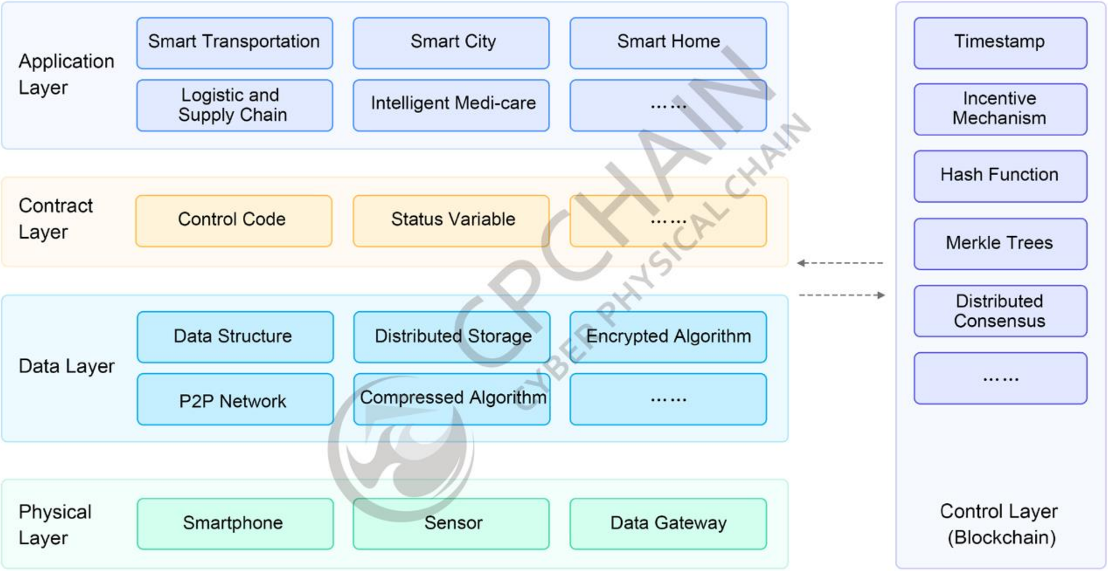


Figure 1. System architecture of CPChain

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

Ethereum, which supports the intelligent contract, is used to speed up the development of the prototype system.

The decentralised system based on blockchain technology is different from the traditional distributed system. In the decentralised system, computing and storage tasks are redundant. Each node in the 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, tamper resistance and the consistency of the system; on the other hand, excessive redundant data also aggravates the system's burden, making the addition of new nodes more and more expensive. In the long run, this model is not scalable and unsustainable. In bitcoin, for example, the size of the bitcoin blockchain has exceeded 210GB, which makes the new node spend a lot of time for synchronizing data. As time goes on, the difficulty of entering new nodes continues to increase. Redundant computing ensures the consistency of the system state, which is valuable and essential. However, the large amount of redundant data storage makes the system burden heavier and not extensible. In order to solve the scalability problem of data storage, sharing and transaction, a parallel distributed architecture is put forward, as shown in Figure 2. The main chain, the industry chain network and the distributed storage system are combined organically. As the control layer of CPChain platform, the blockchain no longer stores all the data of the system, but only uploads the identification and credentials of the data, which not only greatly reduces the storage burden of the platform, but also ensures the consistency of the system.

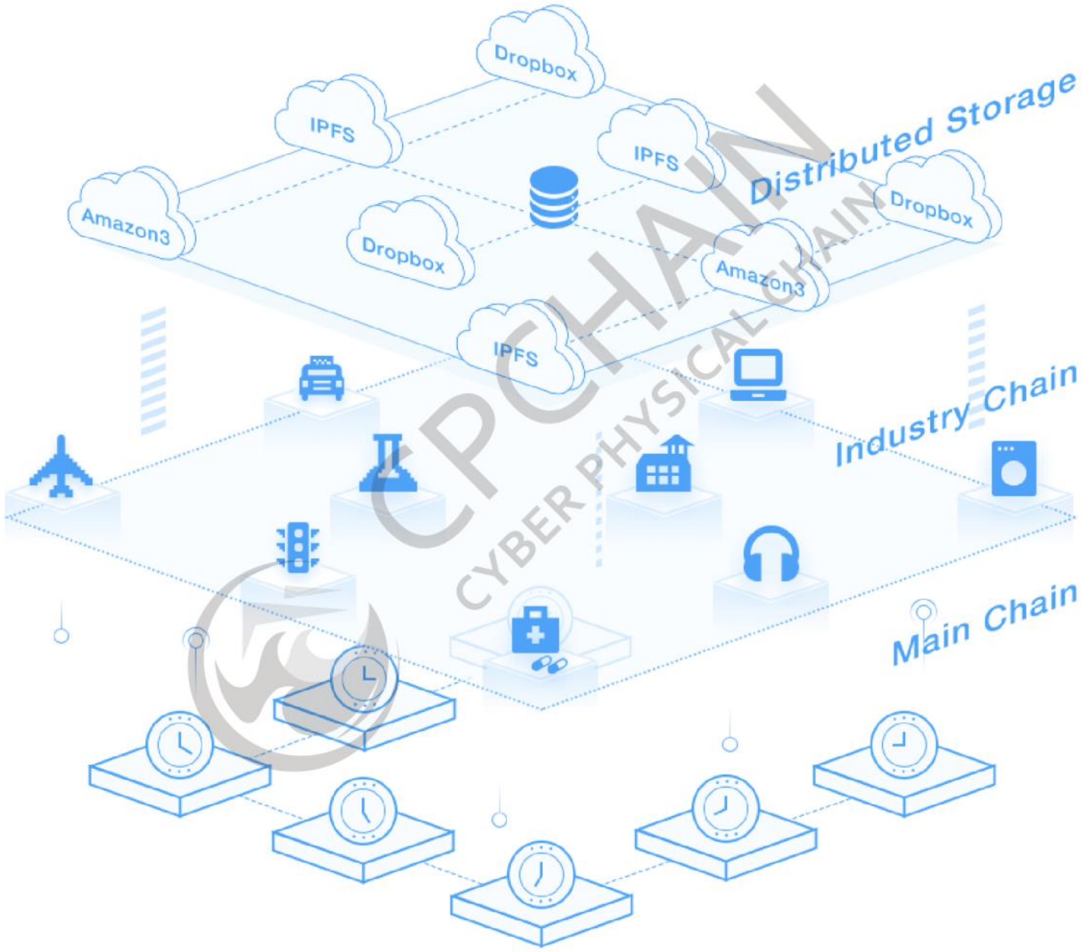


Figure 2. Parallel distributed architecture of CPChain

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

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.

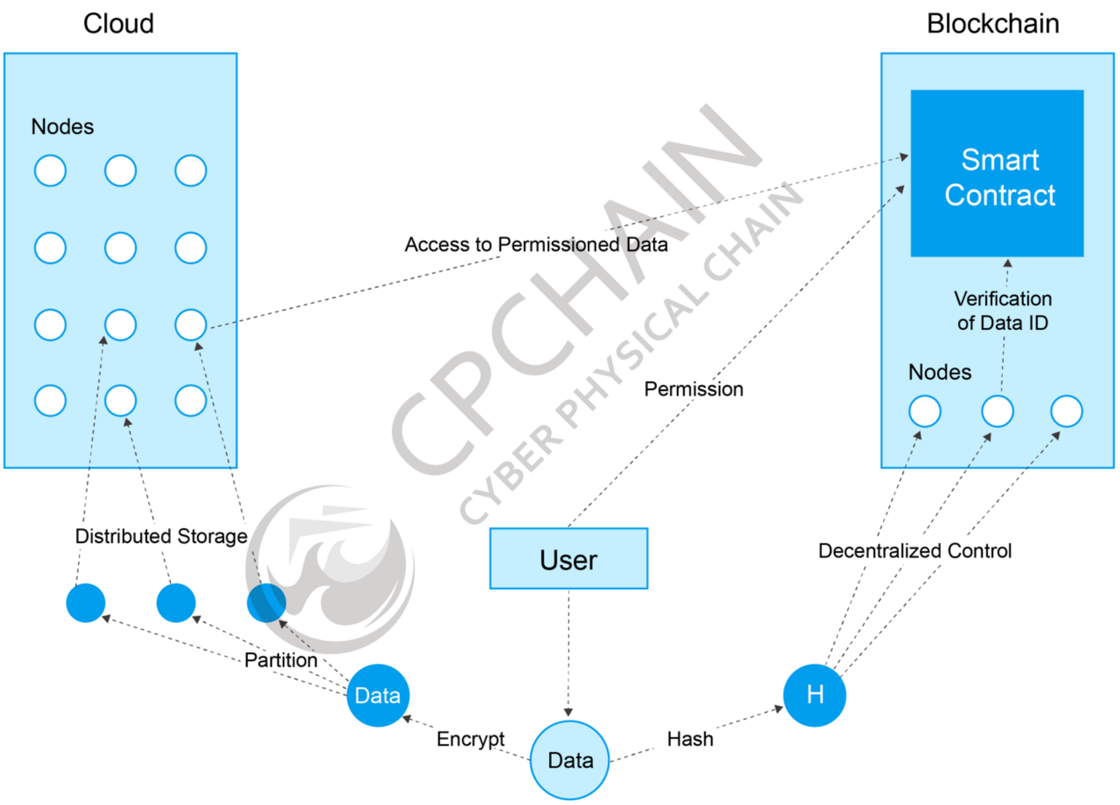


Figure 3. CPChain IoT data upload and share

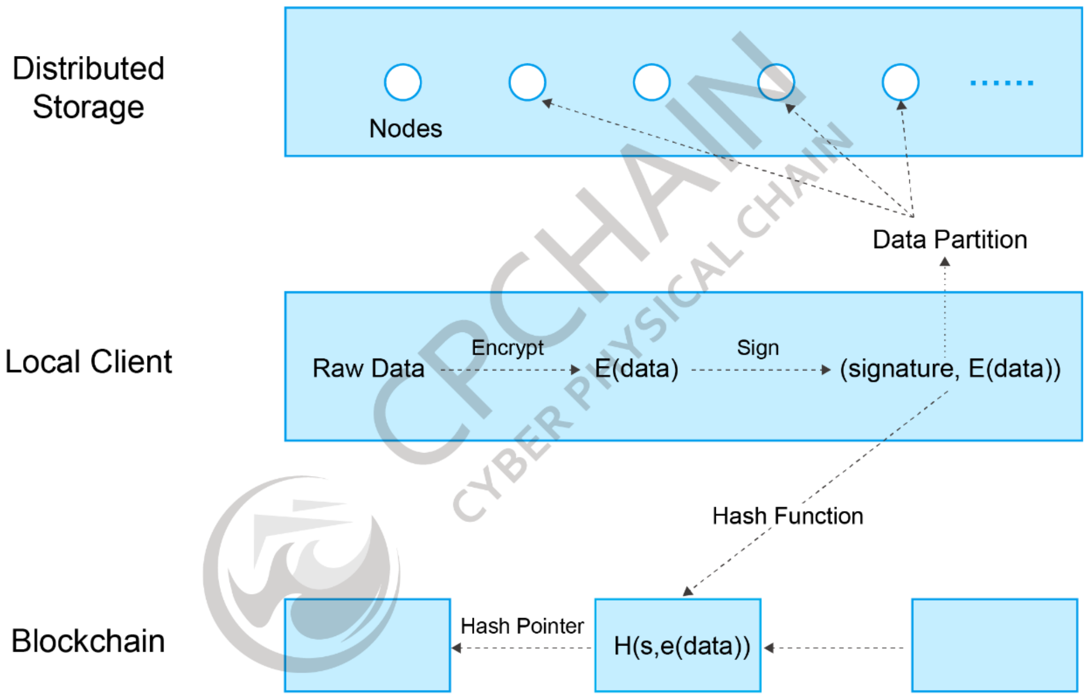


Figure 4. Data distributed storage process

Both encryption and decryption of data consume a certain amount of computing resources. Facing the huge amount of data generated by the IoT system 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 guarantees 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. To ensure data security and privacy, all raw data is encrypted on the user side. Since data is not visible to third parties, how to implement computing or sharing of encrypted data is a primary 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 the 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 once and 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 with blockchain technology to achieve safer and more efficient data sharing and service.

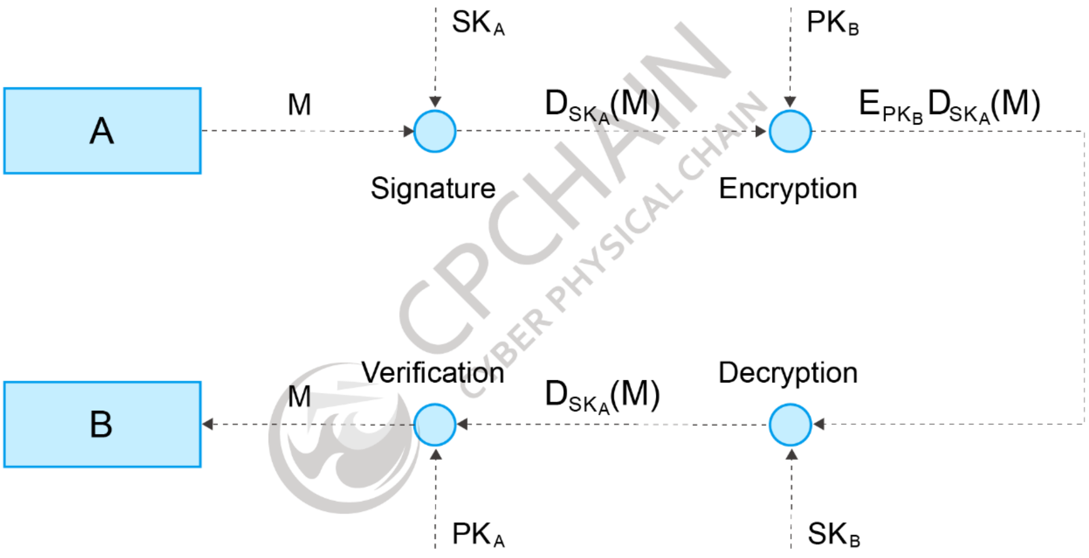
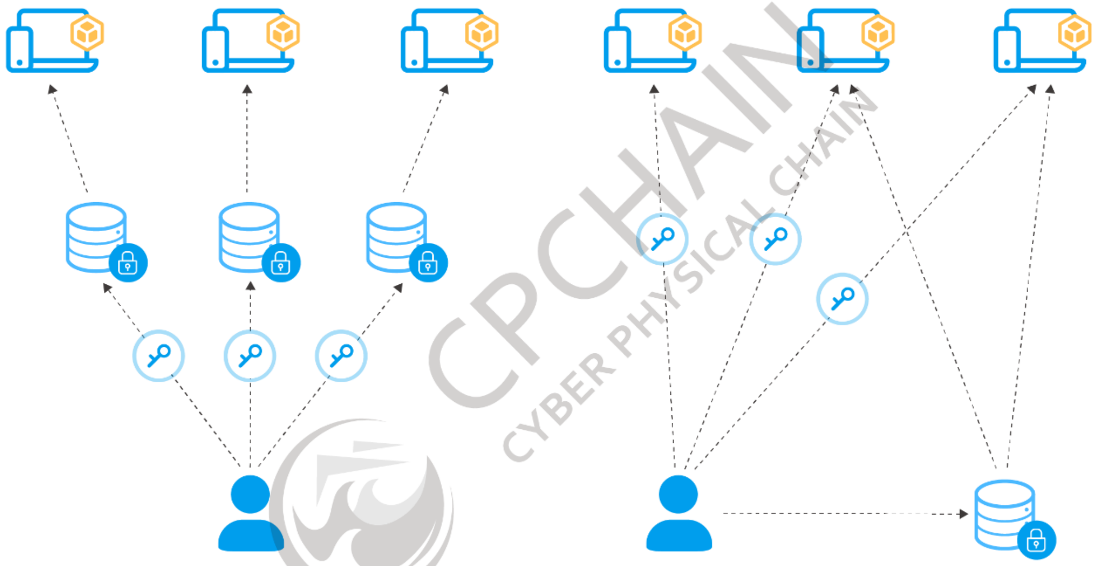


Figure 5. Public key encryption system



a) “One to One” Authorization

a) “One to Many” Authorization

Figure 6. Public key encryption authorisation

In order to realise one-time encryption and multiple authorization, CPChain constructs a set of symmetric encryption and asymmetric encryption 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 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.

The re-encryption technology can partially solve the data sharing problem 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 decentralised 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.

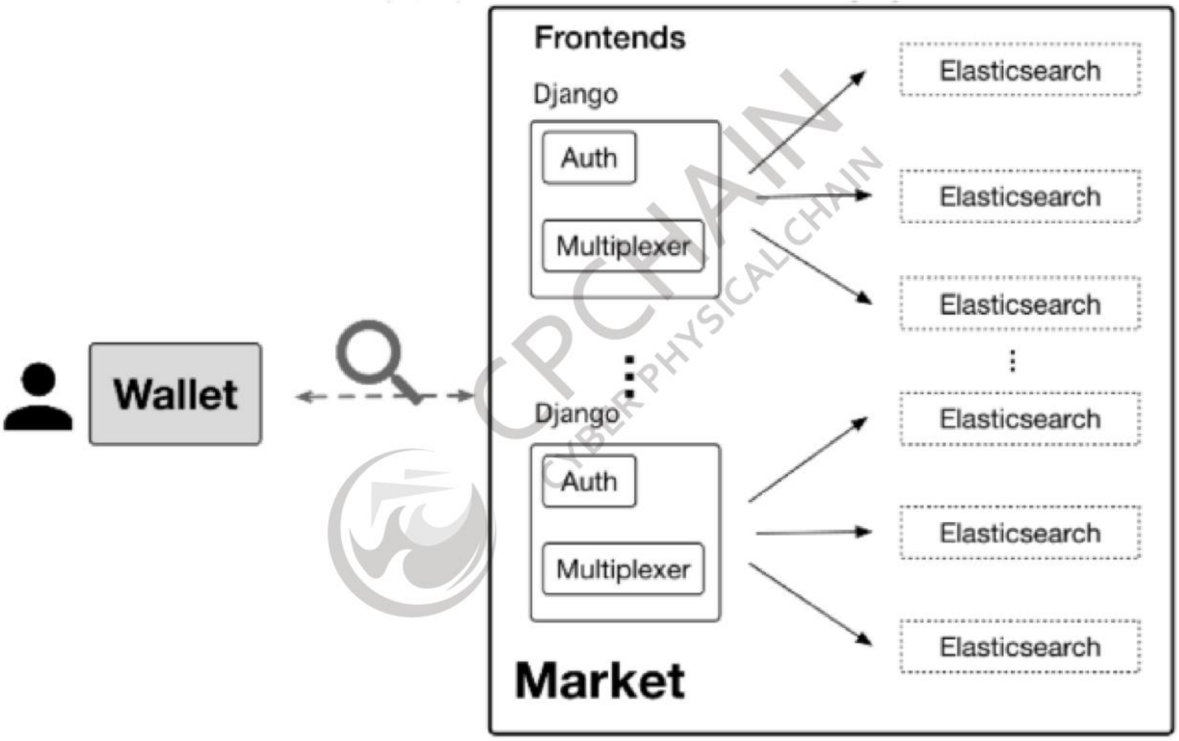


Figure 7. Market structure

Market is the transaction information aggregation platform of PDash, served as an information bridge connection data between a seller and a buyer. The Market includes identity authentication, database, retrieval, and chain information synchronization modules. The seller publishes the basic description information of the owned data on the Market, which is added in a structured form, including the title, label, description, price and other fields; the buyer can retrieve the Market according to actual needs, and the searches program supports natural language 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.

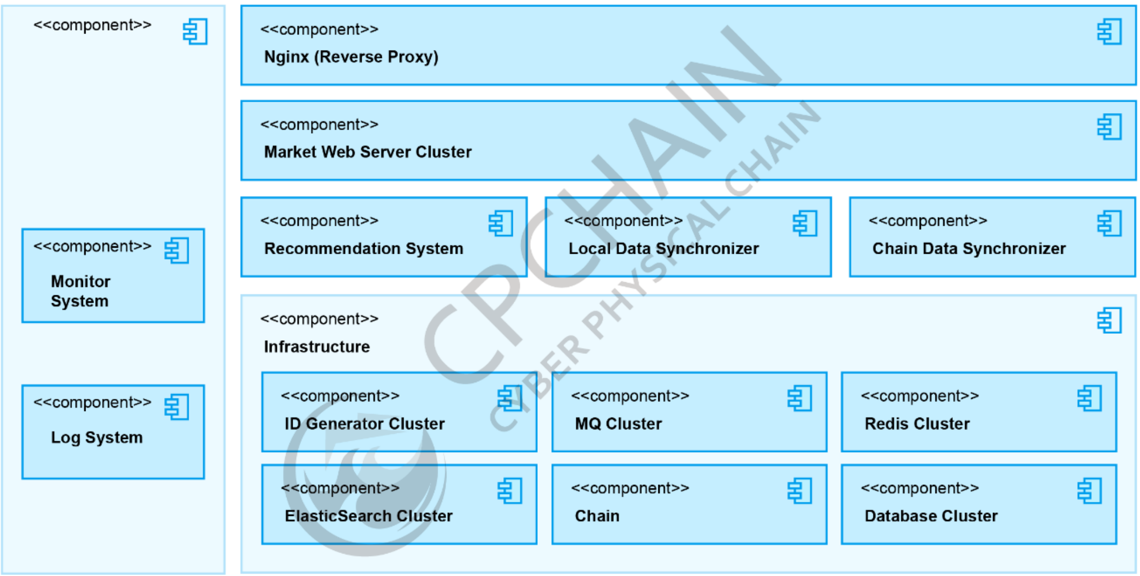


Figure 8. Decentralised market structure

The Market architecture shown in Figure 7 is a traditional server/client architecture that relies on centralised service provider operations. However, Market is only a platform for information aggregation in PDash. The whole transaction process does not depend on the Market, but deals with transaction logic on the blockchain. Similar to the Bitcoin wallet concept, Bitcoin transfers are done on the same blockchain. Users using either client will not affect the operation of the system. Therefore, the Market architecture does not violate the PDash decentralization principles. In addition, unlike the traditional mall 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, as shown in Figure 8. Compared with the traditional centralised architecture, the decentralised 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. By these new modules, decentralised Market ensures that any server running a new PDash Market can get the same data information, without fragmentation.

The decentralised Market has an ID generation module that generates a unique ID for each data published to the Market to synchronize data between the 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 the new data information to the local.

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

2.3 Dynamic Proof of Reputation (DPoR)

CPChain adopts Dynamic Proof of Reputation (DPoR) consensus, which developed by Shanghai Jiao Tong University Distributed Smart System Lab. DPoR consensus divided the whole blockchain system into three layers (Figure 11). Civilians will become to RNodes if they passed admission. Designed algorithm would elect part of RNodes (second layer) to form dynamic committee (third layer). The third layer is designed to solve blocks' adding, verifying, broadcasting and building issue among the committee nodes. In summary, DPoR architecture could solve three main consensus issues of a large-scale network, i.e., nodes reputation value assessment, nodes election and Byzantine Fault Tolerance (BFT) determination among the committee.

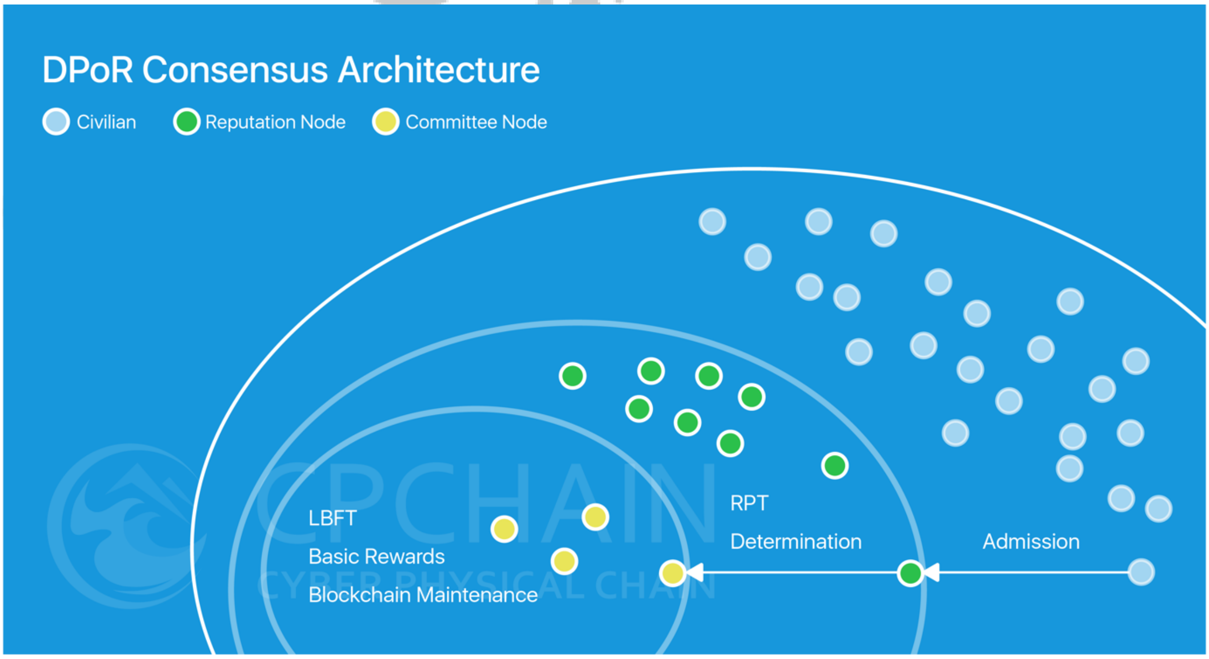


Figure 9. CPChain DPoR consensus architecture

2.4 LBFT 2.0 Consensus on a Large-Sale Public Blockchain

In the large-scale CPChain system, the realization of node state consistency and distributed data storage face many challenges due to the large scale of network and the massive data of Internet of things. CPChain will develop a hybrid consensus protocol with extendable performance and propose a dynamic committee election mechanism to overcome scalability problems of the existing *POW* consensus protocol based systems.

The main core problem in the main chain structure lies in determining which nodes to complete the data collection, packing the chain on the block, and how to ensure the block data security and consistency. Traditional distributed fault-tolerant algorithms, such as *PBFT* and *Zyzzyva*, rely more on communication complexity to guarantee the consistency among nodes. For example, the *PBFT* algorithm applies a three-phase protocol to guarantee the system consistency even if there is a malicious Byzantine node and the recovery of node failure. However, the system scalability is poor due to its more dependence on communication to ensure the security of its algorithm. The performance declines faster with the number of nodes increasing; when the number of nodes exceeds a certain threshold, the system will not be available. And *PBFT* relies on a primary replica, which assumes the responsibility to broadcast requests to all back-ups. Any faulty behaviours involving primary replica result in a much lower throughput. Therefore, PBFT does not have a lower bound for its throughput. Liveness 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 the private blockchain and permissioned blockchain environments. In response to this problem, CPChain's core solution is to design a dynamic voting mechanism for the dynamic committees and elect credible committees to collect the data of the blocks and pack the tasks of the blocks.

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 inefficiencies. CPChain proposes a bipartite committee-based, three-layer agreement, *LBFT 2.0*, to enhance CPChain consensus performance. The committee consists of two parts: *Validators Committee* and *Proposers Committee*. Validators committee refer to a group of users that can validate a newly proposed block. It has the following properties:

- All validators together constitute validators committee.
- The validator committee consists of nodes nominated from CPChain Foundation, government departments and nominated nodes.
- Except for 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 number is always equalling to 3f + 1, where f is the number of Byzantine nodes.

Proposers committee is a fixed number of elected RNodes for a certain term, which has the following properties:

- The proposer's committee is elected based on reputations of candidates and a random seed.
- Each incumbent member alternately assumes the responsibility to propose blocks during their tenure.
- The proposer, or block proposer refers to member assigned to propose a new block in the current view.
- A proposer behaves inappropriately will face an Impeachment from validators which punishes this proposer due to its failure in proposal.

The rest of users are named as *Civilians*. Once a civilian is qualified as an RNode, it can claim a campaign to be a candidate. After being elected, the candidate is about to join 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 rest, named as impeachment, specialise in handling abnormal cases.

Figure 12 demonstrates these five states as well as transitions between states.

For normal case, a validator shifts its state among idle, prepare, and commit states. While for abnormal cases, it enters either impeach prepare or impeach commit state.

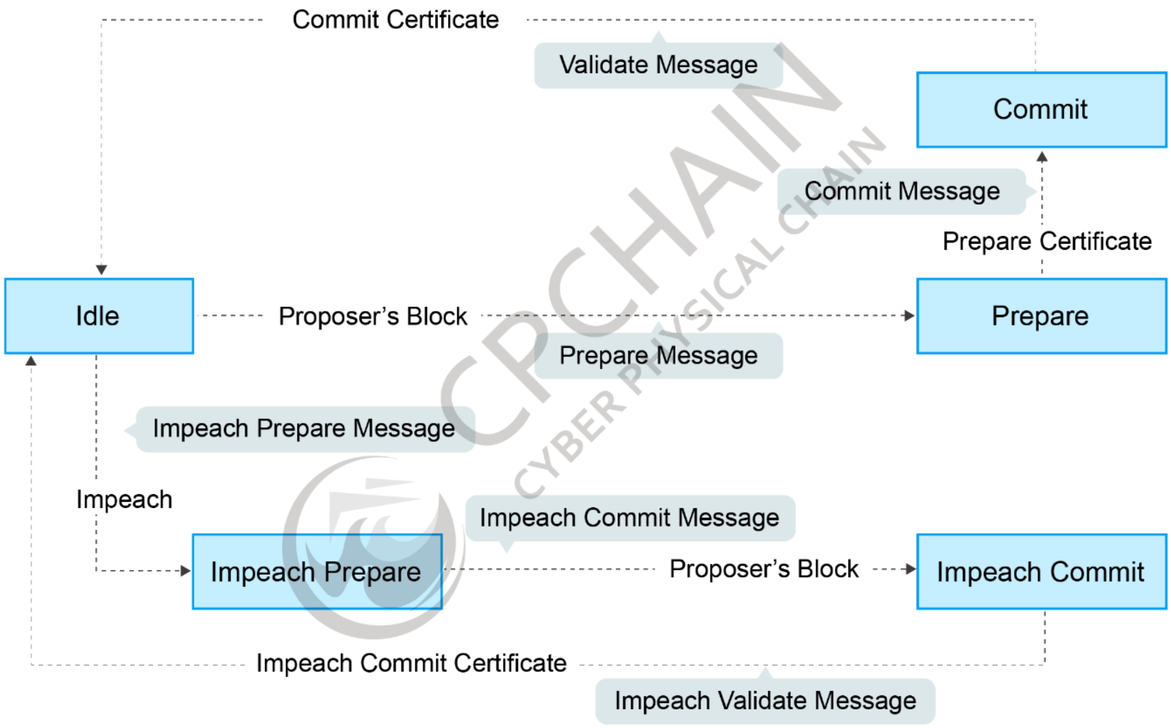


Figure 10. Finite State Machine for LBFT 2.0

Note that not all transitions are shown in this figure due to the lack of space.

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

- Intersection: 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 agreeing on a prepare message and a commit message, respectively.

Block Production

An ordinary user claims campaign, and undergoes the admission qualification, and then enters 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

Once receives a newly proposed block, a validator in validators committee verifies the block in following steps.

1. This Verification of Blocks process scrutinizes the seal of proposer, timestamp, etc.
2. If true, this validator broadcast a PREPARE message to other validators;
3. Once it receives 2f + 1 PREPARE messages (P-certificate), a validator broadcasts COMMIT message to other validators.
4. Once it receives 2f + 1 COMMIT messages (C-certificate), a validator inserts the block into the local chain, and broadcasts 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. Any user receives this VALIDATE message with enough signatures, inserts the block into local chain.

Impeachment: Impeachment is a vital abnormal handler in *LBFT 2.0*, invoked when the proposer is either faulty, or non-responding. It is a two-phase protocol in *PBFT* manner, consisting of prepare and commit phases. When a validator triggers it impeach process, it generates a block on behalf of the faulty (or non-responding) proposer. And impeachment has a higher priority compared to normal case handler. In other words, validator in impeachment does not process any normal case messages except for validating messages. An impeachment can be activated under the following two cases:

- The timer of validator expires;
- A validator in an idle state receives an illicit block from the proposer.

Timer expiration can be caused by several reasons, like a non-responding proposer, double spend attack and improper timestamp. An illicit block can be a block with improper transactions and seal. Here we list the steps for an impeachment process.

1. A validator v in the committee generates an impeachment block
2. This block, used as an IMPEACH PREPARE message, is broadcast to all validators in the committee.
3. Once receives f + 1 IMPEACH PREPARE messages with same header and body, validator v broadcasts an IMPEACH COMMIT message to other validators.
4. Oncereceivesf+1 IMPEACH COMMIT messages, a validator broadcasts an IMPEACH VALIDATE message along with f + 1 signatures to all users.
5. Any validate 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 messages.

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

As the basic data platform of IoT system, CPChain is a common IoT data control layer. However, different vertical applications of IoT, it has different performance requirements. Typical harsh real-time applications include unmanned vehicular, fleet coordination and so on. In such applications, CPChain needs to support secure communication and interaction with real-time control signaling in order to work efficiently and collaboratively among the various equipment nodes in the Internet of Things. If the data interaction is still completed through the main chain, it will face a great delay, which cannot guarantee the real-time requirements of all kinds of applications. In order to meet the requirements of high frequency, fine granularity, high security and real time of machine data transaction, we will select typical application scenarios and develop a lightweight side chain consensus protocol. Specifically, CPChain will design the side chain consensus system with edge computing and hardware security method in the industry chain to ensure that all kinds of applications can meet the delay requirements. Therefore, the high real-time and high security of the industry chain network are realised, as shown in Figure 13.

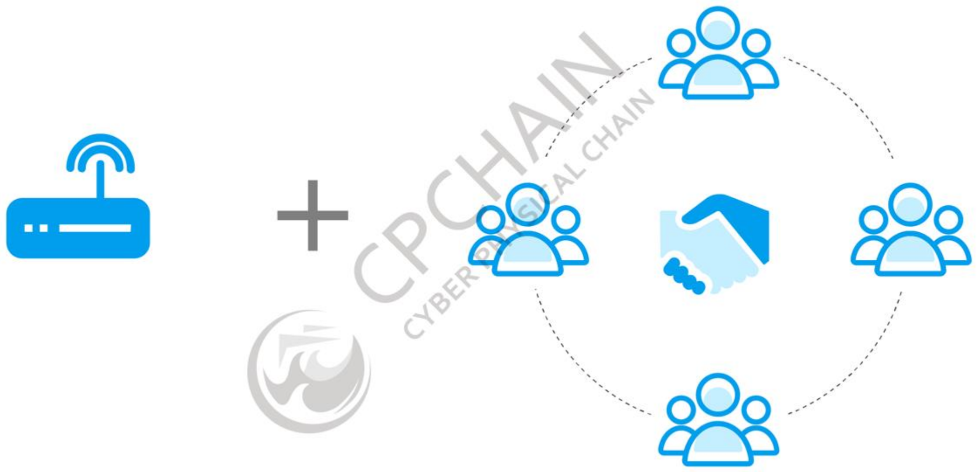


Figure 11. Altruistic cooperation model with hardware acceleration

2.5.1 Data Gateway and Embedded Encrypted Algorithm

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

2.5.2 Incentive and Security Mechanism for Consensus Algorithm of Industry

The Internet of Things system consists of mesh network or wireless ad hoc network. There are many wireless communication technologies in different IoT industry, such as IEEE 802.11p, NB - IoT. Therefore, the consensus of machine transaction in the Internet of things can make full use of the characteristics of 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 layer of communication layer. In addition, considering the high concurrency, real-time and security requirements of machine transactions, CPChain will develop efficient altruistic cooperative incentive mechanism and security mechanism based on evolutionary game theory. For example, altruistic cooperative incentive mechanism based on Directed Acyclic Graph (DAG) data structure. Thus, the application of CPChain side chain is more efficient, faster and safer.

2.6 Testing

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

In the following sections, we present our testing framework from different perspectives.

2.6.1 White-Box Testing

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

Unit Testing

The unit testing is written in Golang accompanied by chain code, which is altogether stored in CPChain repository. All unit testing files are ending with _test.go. And each unit testing file contains several testing functions to examine its corresponding functionality given pairs of input and output.

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 in higher levels. These files also have their corresponding testing files to conduct on integration testing.

Regression Testing

Each time a certain branch is updated in its remote repository, Jenkins activates a regression testing via going through all testing files. By this means, all unit testing and integration testing can be redone, ensuring that no bug is introduced in old code blocks.

2.6.2 Block-Box Testing

The 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: how to reproduce the case;
- Expected result: what is 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. Thus, we design plenty of test cases on consensus, including abnormal and normal ones, to test the functionality of the chain. For each possible abnormal scenario, an input and its expected output are designed to simulate it. This simulation is implemented by adopting Jepsen framework.

Stability

Stability testing involves the launch, reboot, and abort of the bootnodes, proposers, validators, civilians and contract administrators. This testing provides the stability proof of the chain under extreme cases like blackout, connection error, etc.

Mining

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

- Proposer: contain curated test cases in which a proposer conducts different behaviors.
- Campaign: examine the campaign log, APIs, candidate list, and smart contract.
- RNode: assure the admission of RNode is correct given different conditions.
- Reward: guarantee both basic and maintenance reward is correctly calculated and dispensed.
- Admission Control (AC): make sure the threshold set for minimum CPU capacity works as expected.
- Validator: test the validity of validator contract and domain.
- Start and Stop: robustness test by multiple aborting and restarting the chain.

Nemesis

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

- Delay of sending package
- Disconnection from the network
- Crash of a node
- Time drift (incorrect local clock)

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

Compatibility

Compatibility is a major challenge for all decentralised systems, as not all nodes may update to the latest version. Similar to the concepts of soft fork and hard fork of Bitcoin, CPChain also have soft update and hard update. In a soft update, old version can still work with the chain. while in a hard update, the old versions are rejected when claiming campaign, proposing blocks, or even cannot 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 limit of the throughput of the chain. The stress testing can be divided into two major classes:

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

2. Send out transactions in a speed outnumbering out tps limit. It can help us test if the chain can maintain stable and if the outnumbered transactions can be postponed to successive blocks.

2.6.3 DDoS Attack

DDoS Attack, a.k.a., Distributed Denial of Service attack, is 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 computing resources or bandwidth of the target. A targeted machine flooded with these superfluous requests will lose its functionality 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 has literally no impact to the whole chain. However, validators of CPChain can be a latent target for DDoS attacks. Thus, we design the following scheme for potential DDoS attack:

1. Set up multiple trusted nodes as default proposers.
2. Validators hold a while list that contains all default proposers.

3. Each validator has a monitor on its computing resources. Once the validator is under high performance for a long time, it considers it is under DDoS attack, and activate the white list. The white list will reject all nodes except default proposers in the level of firewall.

4. When any of the following conditions satisfies, the while list is removed:
    i. No DDoS attack detected in a period of time;

ii. The white list has been activated for a long time;

iii. Deactivate the white list manually.

2.6.4 Formal Specification

Software testing neither reflects any glitch, nor proves the completeness of a piece of code in terms of mathematics. Thus, we introduce a formal specification to the chain.

Formal specification languages describe a program at a higher level through a certain form or specification, such that it can determine whether it 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 the algorithm of CPChain.

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 **controlled environment.**

2.7.1 Public Environment

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

- The 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 in AWS (Amazon Web Services) in Singapore.

- VPS model: AWS t2.large model.
- Network condition: 1 Gbps (It is an estimated speed. AWS does not offer an exact number of network performance for AWS t2.large model._
- Location: all in Singapore.
- Processor: 3.0 GHz Intel Scalable Processor.
- Memory: 8 GB.
- Number: in total 7 servers.

Under this setting, we conducted a beta test between 1 May and 5 June 2019. In total, 795 common nodes all over the world, 70 RNodes and 7 verification nodes distributed in 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), 4.4 million transactions, and the transaction peaked at 1,000 transactions per second.

2.7.2 Controlled environment

The controlled environment refers to perfect condition. It has the following traits:

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

Under this setting, we can push 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 world’s roads now. The extended global automotive industry is undergoing an unprecedented transformation to a new mobility ecosystem, what we call a Smart Mobility driven by the Internet connected and smart transportation infrastructure. The pace of change is breathtaking, as the transportation management system would be evolved into a new efficient and effective era and the future of mobility services would be more flexible and dynamic.

Several technological barriers and operational issues would need to be overcome before we fully embrace the future of mobility. Technological barriers are primarily related to data collection and sharing, the 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 issue, collaboration method and incentive mechanism design have been highlighted. User accounts and payment methods should be connected among different service providers to provide integrated services. Incentive is a must to encourage new customers to share their personal data and jointly build an open data trading platform.

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

3.1.2 Smart Health

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

Many governments showed their support for digital health and made 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, the secure, integrity and right control concerns exist. Moreover, hospitals, pharmacies, payers/insurance companies, and government institutions are isolated, health data cannot be shared freely. Besides, track and trace in medicine supply chain and data silos have a negative effect on academic research and medical services, also let counterfeit drugs production and sales happen.

Blockchain is traceable, and has high accuracy and credibility. It coordinates every stakeholders' interests by deploying a well-designed data sharing incentive mechanism. Blockchain technology plus healthcare data and infrastructure could address many urgent issues in the industry, such as cybersecurity, data interoperability, medicine supply chain, insurance credentials, bill fraud, etc.

3.1.3 Public Security

With the rapid development of society, technology and urbanisation, public infrastructure is keeping developing and evolving, so does the standards of infrastructure maintenance and safety.

Prior to Smart City construction, centralised system is widely used in transportation, communication, utilities, social infrastructure, waterways, public escalators and elevators. Information technology is limited applied to specific scenarios, architecture design does not work with overall management, and data silos exist. Information technology, as a result, cannot fully execute its power. Furthermore, a single attack could easily crash a centralised system, leave the infrastructure system with zero response and result in public safety concerns.

Blockchain technology could provide transportation, communication, utilities, social infrastructure, waterways, public escalators and elevators with trustful and low-cost solutions, plays an important role in history tracing, tracking and verifying. Blockchain can solve facilities' authentication issue and secure concern, it links devices and human beings.

Blockchain based smart city system combines peer-to-peer network, data encryption, consensus mechanism, smart contract and other technologies, effectively improve the security of Smart City IoT system. 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 being crashed down. Even with one of the devices is under attack, the rest would work as per normal. Then social service would not be suffering from any crash downs.

3.1.4 Decentralised Identification (DID)

In recent years, online digital identity management has gained lots of attention. 18 OECD[1] member countries announced or are considering have 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 identity ecosystem framework in a trusted cyberspace. However, several concerns are still waiting for solutions.

The lack of validity of personal data: users do not have full control over their identity even the identity is verified. It is hard to confirm the digital identification's owner is the person per se, also is hard to trace the DID system.

The lack of infrastructure: there are more than one type of personal identification, and each one applies to different scenarios. But centralised authentication systems do not talk to each other, and even they do, system authentication is very time-consuming. General coordination and management are tough.

[1] Organisation for Economic Cooperation and Development

The risk of privacy leakage, due to the simple authenticate technology: currently, most of the major authenticate platforms employ simple authenticate technology, raising a great risk of privacy leakage and illegal trades.

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

- Limited storage, computation and communication resources；
- Scalability issue brought by the large-scale of IoT devices;
- Risk exists when edging nodes manage a large number of IoT devices.

A blockchain based DID system complies with end-edge-cloud architecture, form DPKI system and provides scalability with IoT systems. For unqualified IoT devices (cannot support DID related computing and storage requirements), edging nodes would assist DID generation, authentication, authorisation and other services. Lastly, to solve the management risk, 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 Backgrounds

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

China's rapid urbanisation has developed ahead of its infrastructure construction. Traffic, for example, is chaotic, and parking is time- and money-consuming. These pain every big city in China and raise issues to city management. The government has made efforts to make parking easier, but still, parking lots are unreasonable allocated, and the utilisation rate is quite low. Especially with the development of electric vehicles in recent years, the lack of charging facilities has been raised. Fuel vehicles' irresponsible parking also made the situation worse. To make urban life a better one, advances in information technology should have fostered parking and charging issues in daily life.

3.2.1.2 Solution

CPChain Foundation and a famous luxury automobile company[2] jointly provided a solution to the current parking and charging issue. The answer is distributed identification technology and seamless charging and parking system. This system boosts the efficiency of chargeable parking lots, eliminates fuel vehicles' inappropriate parking behaviour, and provide vehicle owners with seamless payment options.

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

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

Once the vehicle leaves the parking lot, the ultrasound sensor would stop timing. The payment server would initiate fees settlement, send message to the blockchain's smart contract. Thanks to one-off small amount auto-payment technology, parking fee would be

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

paid automatically. For parking places who use licence plate recognition technology to calculate parking fees, smart landlocks help manage chargeable parking lots.

The full process is unmanned, seamless, timely and secure. Along with the auto-payment and seamless user experience, the potential value of data grows.

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 trustful. DIDs are fully under the control of the DID owners, and owners can decide whether and which part of data they would like to upload to the blockchain. Only the owners and authorised DIDs have access to verified data. For unauthorised parties, DID's signatures on the information requires for verification are all they can see. This means personal data is under protection. 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 needs for authentication, and protect his or her personal information.

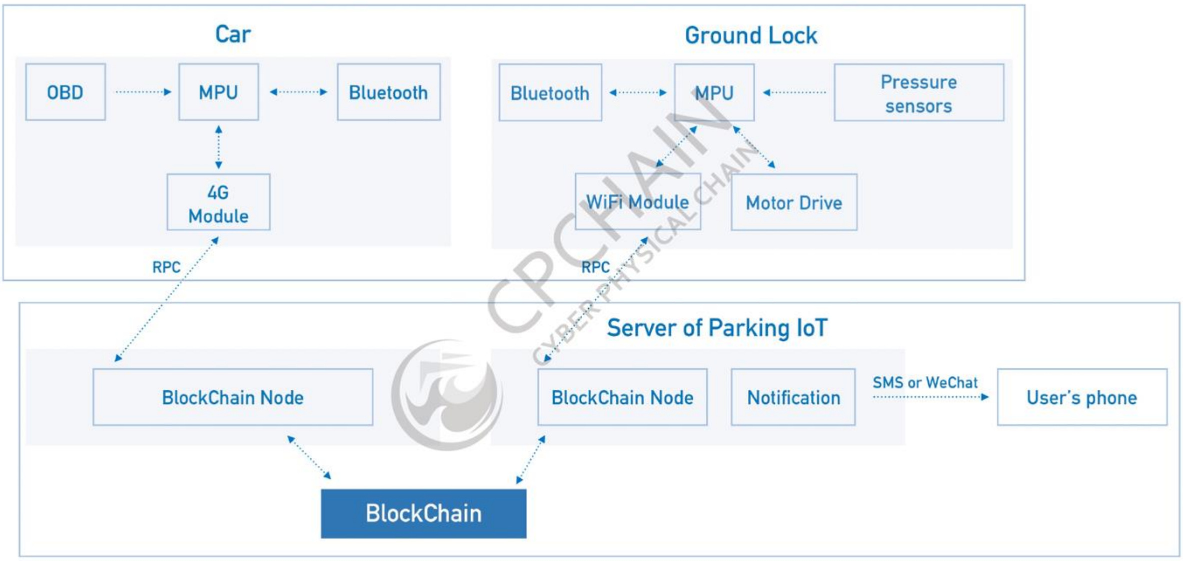


Figure 12. CPChain seamless parking architecture

3.2.2 Sharing EV Charging

3.2.2.1 Background

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

Drivers' Pain Points:

- Short of charging facilities
- Every charging platform needs for registration, which is troublesome
- Charging station market is not transparent enough

Operators' Pain Points:

- Operators refuse to talk to each other in this highly competitive market
- Highly fragmented market
- OEMs' charging facilities are complicated

3.2.2.2 Solution

The smart telecommunication computing facilities are used for:

- Authentication: EV auto-connects to the charge station and verify the car owner's identity;
- Seamless charging: car owners only need to plug in;
- Transaction: auto-settlements, safe and transparent transactions.

CPChain Foundation has installed a few smart IoT devices on real electric vehicles. The device is fully developed by CPChain, supports DID and blockchain technology, and can make point-to-point communication between charging station and vehicle. For registered vehicles, users do not need to swipe credit cards or membership cards any more. Simply plug in, IoT device in the charging station would be activated and start timing while charging; likewise, simply plug out when charging is finished, and the device would calculate fees and receive the payment automatically. Vehicle owners can 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, have more discussions, and consequently move blockchain technology forward, add value to the mobility industry. The solution also attended *Yangtze River Delta Economic Zone Innovation Exhibition* as one of the fifty-five technological representatives in Shanghai, where the solution has been widely recognised and appraised.

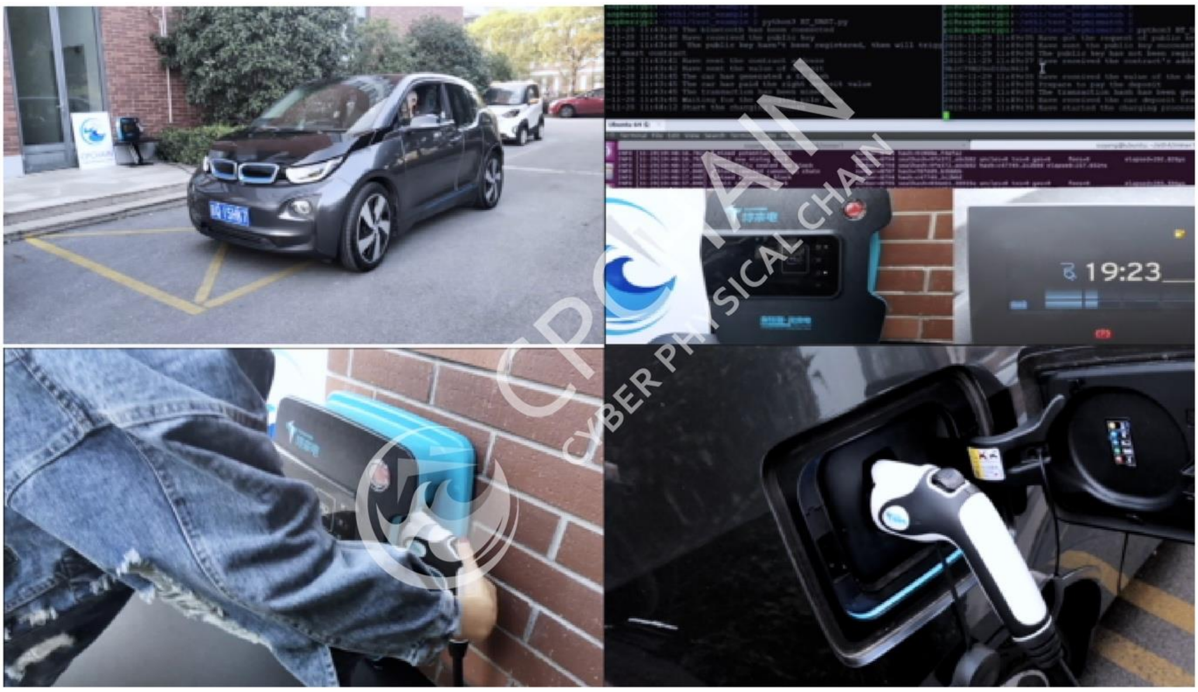


Figure 13. CPChain Charging & Sharing System

3.2.3 Drugledger: Drug Tracing

3.2.3.1 Background

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

The US implemented the *Drug Supply Chain Security Act (DSCSA)* in November 2013, requires drug manufacturers and repackagers to affix or imprint a "product identifier" on packages for certain prescription drugs 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 1 July 2011. This Directive introduces harmonised European measures to fight medicine falsifications and ensure that medicines are safe and that the trade in medicines is rigorously controlled. Measures include a unique identifier and an anti-tampering device, strengthened record-keeping requirements for wholesale distributors, etc.

Traditional medicine supply chain has following issues:

- Hard to protect every stakeholders' commercial privacy
- Difficult to sustain data authentication and stability
- Collaboration gap within supply chain
- Compatible issue with the current ERP management system
- System is vulnerable to DoS attacks, which raises security concern

3.2.3.2 Solution

To the solve above issues, CPChain came up with Drugledger, which comprises by CSM, QSM and ASM:

Certificate Service Module (CSM)

CSM is embedded with public key facility, provides users with dynamic management service (for example, only certificated users could enter to the blockchain network). In general, CSM plays a system supervision role.

Query Service Module (QSM)

Provide all the stakeholders and patients with medicine tracing services.

Anti-attack Service Module (ASM)

Check abnormal activity in the system and maintain the system services as per normal.

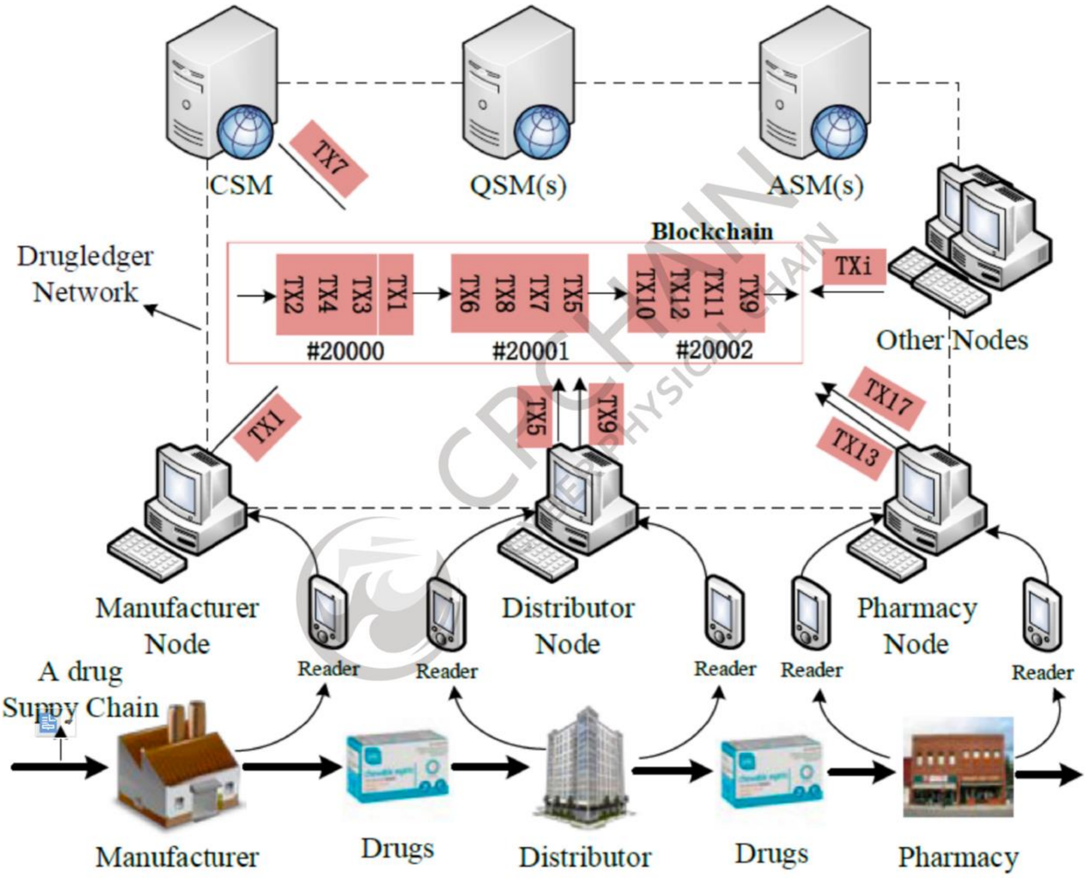
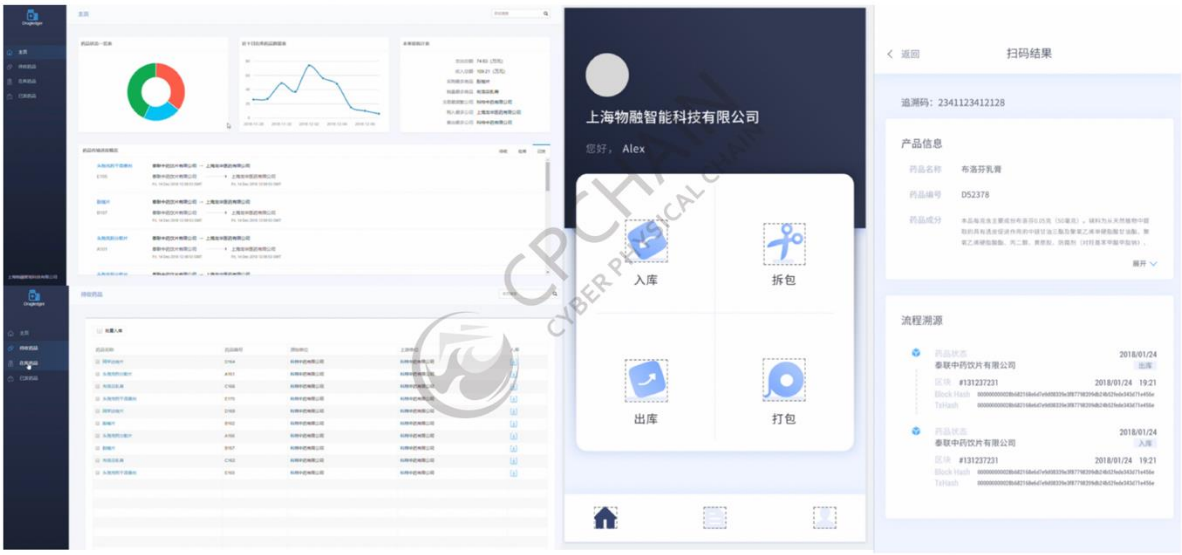


Figure 14. CPChain solution for medicine trace

3.2.3.3 Realisation

CPChain developed a PC application for suppliers and healthcare institutions to supervise the supply chain in real-time. CPChain also developed a mobile application for healthcare suppliers and institutions, allow them to operate drugs inbound, packaging, unpacking and outbound. There is a third application developed by CPChain for consumers, to check the logistic information in order to detect medicine's authenticity.



上海物融智能科技有限公司

您好， Alex

入库

拆包

出库

打包

< 返回 扫码结果

追溯码: 2341123412128

产品信息

药品名称 布洛芬乳膏

药品编号 D52378

药品成分

展开

流程溯源

药品状态 2018/01/24

泰联中药饮片有限公司 出库

区块 #131237231 2018/01/24 19:21

Block Hash

TxHash

药品状态 2018/01/24

泰联中药饮片有限公司 入库

区块 #131237231 2018/01/24 19:21

Block Hash

TxHash

Figure 15. Drugledger by CPChain

3.2.4 Driving Training Chain

3.2.4.1 Backgrounds

- In China, driving test can only be taken after at least 40 hours training. However, many training hours records are fake.
- Currently, a fingerprint identification device is used to verify trainees' identification, but cheating is still happening.
- Driving training data can be tampered by others.
- Lack of customised driving behaviour analysis and tracking record after training.

3.2.4.2 Solution

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

This driving training system has an IoT device embedded in training vehicle, which could 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, ensure trainers and the trainees are keeping training. Training time, route, brake and accelerator-related data, together with the snapshots will be collected during the session. All the collected information will be uploaded to the blockchain. Noted that data is genuine as it is uploaded from IoT devices directly. If there is a tampering attempt, system would alert for 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 picks fraud and/or tampered data out. This system guarantees the 40 training hours has been reached, benefits all the interest parties and contributes to a safe 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, alerts for 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. CPChain Foundation, National Safe Driving Technology Engineering Technology Research Centre and the Distributed Intelligence Laboratory of Shanghai Jiao Tong University are jointly working on a project, which is using IoT technology, blockchain technology, artificial intelligence (edging computing-based), solving problems in driving simulation, driving training and safety control for car-pooling. The project also plans to analyse training and driving records data, come up with safe driving advice, collect body temperature records from wearable devices, alert for emergencies based on outside camera and image analysis, and warn inappropriate behaviour based on inside camera and image analysis.

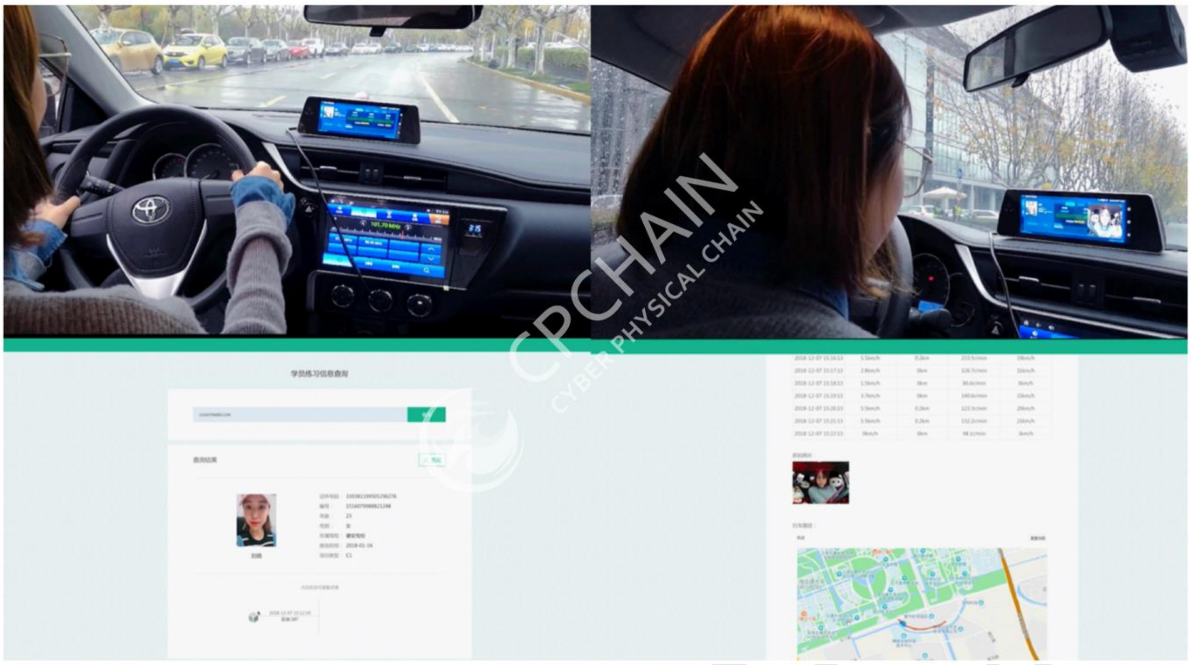


Figure 16. CPChain driving training demonstration

3.3 DApp

3.3.1 PDash Data Sharing

3.3.1.1 Background

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

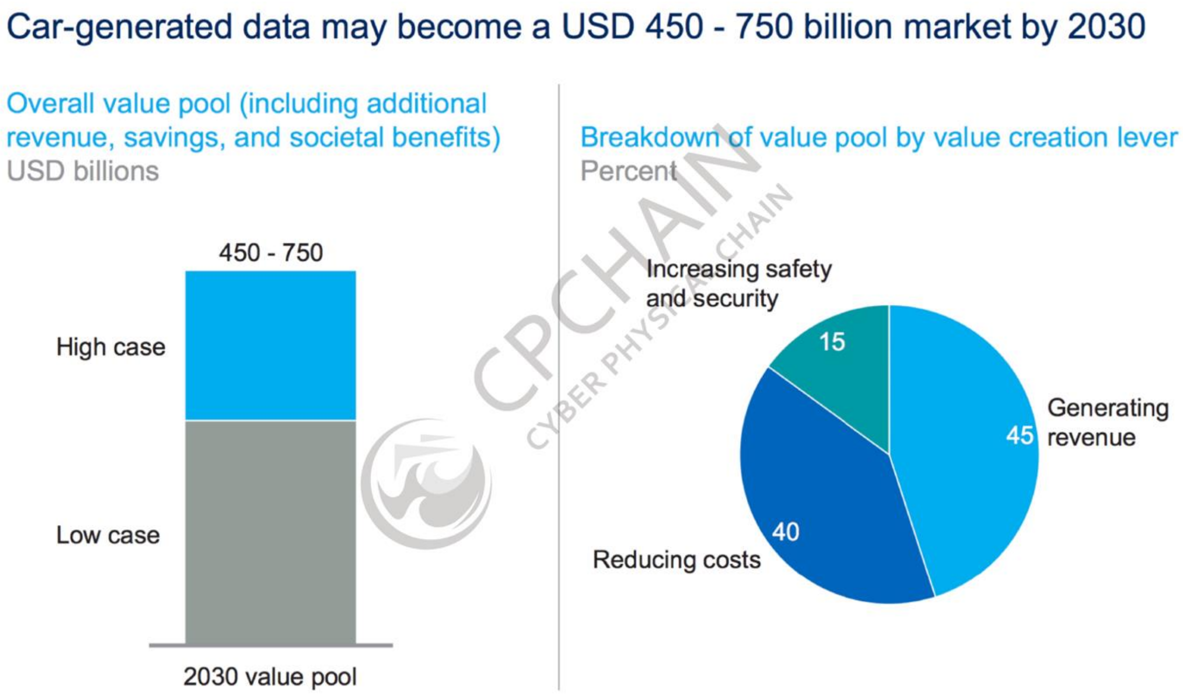


Figure 17. Mobility data market forecast

3.3.1.2 Solution

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

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

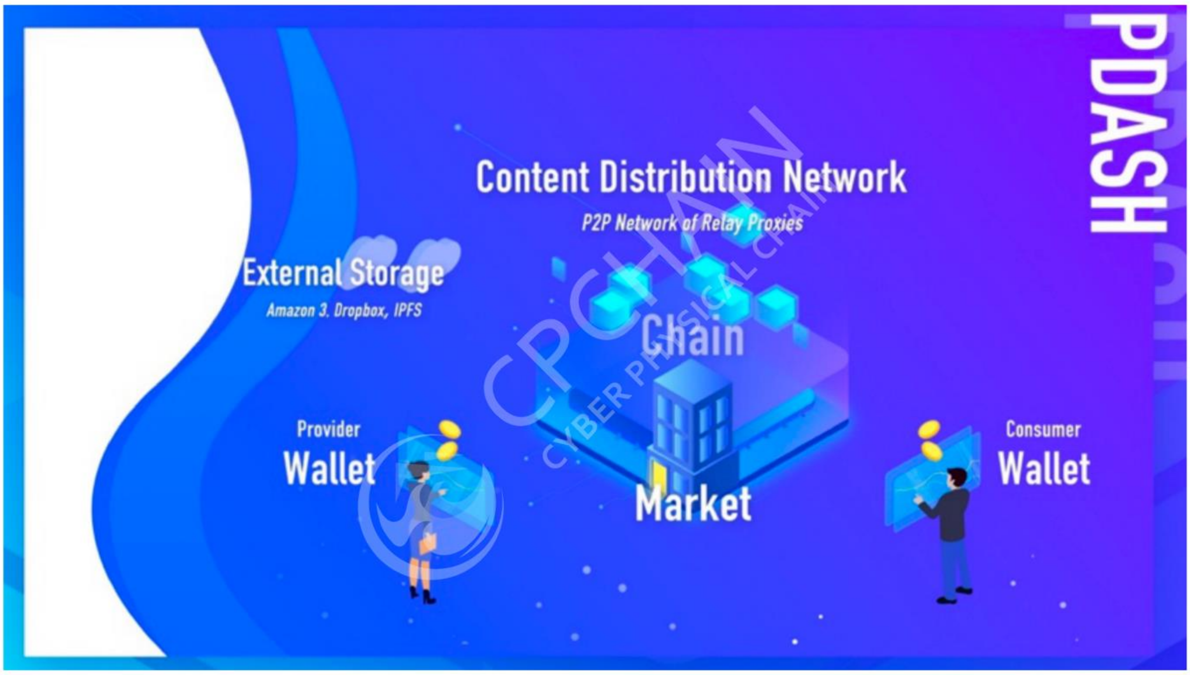


Figure 18. PDash Data Sharing Platform architecture

3.3.1.3 Realisation

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

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

2. Ordinary nodes in the CPC network (non-dApp application nodes) have the right to send a fixed number of free transactions every day. If this number is exceeded or the transaction frequency is too fast, the system will charge a fee.
3. In order to ensure the balance of communication and computing resources, dApp application developers must hold a corresponding amount of tokens according to the resources to be occupied by the application, and may lease them if the number of tokens is not enough.
4. For transactions resulting from DAPP applications, DAPP developers bear the corresponding costs, and pay leasing fees to miners who provide rental tokens.

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

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

The application development provider will further develop and process the acquired smart contract services based on the needs of the end customers and provide its traditional enterprise customers or end users with application products and receive the CPC as the enterprise revenue. The end user could pay CPC to get 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, in which nodes are categorized into three types according to their deposit in two pools and balance.

- **Economy Node:** Requires a minimum of 20, 000 CPC tokens deposited in 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 RNode Pool for participation. Investors with the basic configuration of computing and storing can participate to support the CPChain Open Transmission Protocol (COTP).
- **Industry Node:** IoT Industry partners and 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 deposit at least 20, 000 CPC tokens in this pool is qualified 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 become 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

RPT (abbreviated from reputation) value of a node is evaluated by extracting data from blockchain. By employing RPT Contract, a node can evaluate its RPT value by 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 counts;
- Data Contribution (DC): data uploading of a node will be rewarded by increasing RPT value. Basic reward 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 RPT reward after every round of block building.
- Proxy Reputation (PR): proxy node will have RPT reward if it assists others trading.

Each dimension has a full score of 100 point. And the total score is calculated as:

$$\boxed{RPT = 0.5\ast AB+0.15\ast TX+0.1\ast PR+0.15\ast DC+0.1\ast BM}$$

5.1.3 Node Rewards

CPChain's ecosystem is established by a lot 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, CPChain Foundation would be the main fund provider, for the ecosystem establishment and the chain maintenance. The next stage is mainly performed by the market. With the optimization of 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 to two parts: *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). The Economy Nodes receive the 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 goes 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 is always at a certain period, 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.

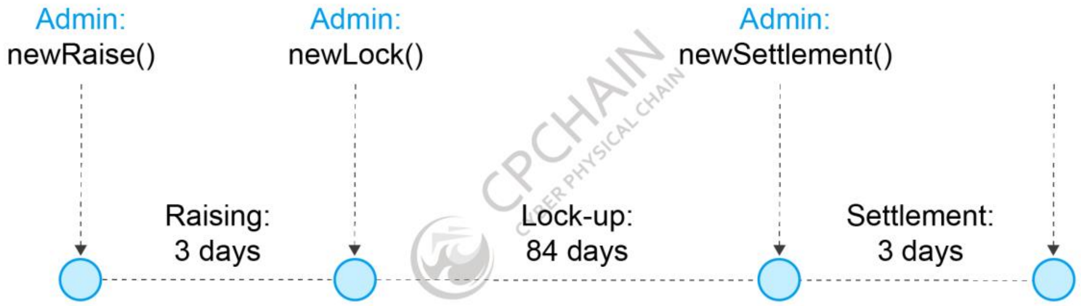


Figure 19. Economy nodes: basic rewards

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 5000000 ∗ d/D, where d is deposit of a certain node, and D is the total value of 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 1.1: *: *Both the first and the fifth year contain a leap day (29 Feb 2020 and 2024, respectively), which results in a larger number of generated blocks compared to the other three years.*

Maintenance Reward

Proposers committee nodes are entitled to blockchain maintenance rewards, after it proposes a block and successfully gets 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 being decreased by 25% annually for the next four years. Thus, the annual supply for five years is 40 million, 30 million, 22.5 million, 17 million and 12.75 million respectively. After five years, the supply runs out. In other words, no CPC is rewarded after that time.

Meanwhile, CPC Mainnet inserts a block every 10 seconds, which yields around 3 million blocks each year. Therefore, we conclude the reward and supply in the table below.

Note that in our *LBFT 2.0* protocol, an impeach block is inserted into the chain if the proposer is faulty or non-responding. Intuitively, a faulty proposer cannot receive the reward. Hence, the amount of annual supply could be smaller than the one listed in the table above.

5.2 Board of Directors

The Board of Directors is the core organisation of CPChain Foundation, responsible for leading CPChain to a well-managed ecosystem with higher efficiency. CPChain Foundation invites well-known organisations, corporations and individuals to jointly build CPChain mainchain global ecosystem. This community would provide decentralised services to various industries, corporations and individuals, and eventually create a dynamic ecosystem for the integration of blockchain and Internet of Things.

5.2.1 Description

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

5.2.2 Rights and Responsibilities

Board of Directors is expected to participate in CPChain's strategy making, decision execution, financial supervision, etc. CPChain Board of Directors is obligated to disclose material information, such as CPChain's technological development stage, operations situation and CPC distribution; the board also needs to assist third-party auditors to generate audited annual reports.

5.2.3 Term

The board of CPChain Foundation serve a one-year term, elect annually.

5.2.4 Election

Besides directors nominated and appointed by the CPChain Foundation, all the community members whose account balance is over 200,000 CPC are eligible to be elected as directors. Candidates need to submit some documents to join the election. Also, the election period and the whole term are blackout periods, CPC selling is not allowed.

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, collects different parties' opinions about technology, community and ecosystem. The board of directors accomplishes much of its work through committees. CPChain Foundation has two standing committees: technology committee and ecology committee.

Technology Committee recruits and orients developers' community and develops new technologies in a collaborative manner. Technology committee is empowered to take in charge of the main chain's maintenance and updates, make the chain in align with the ecosystem. The Ecology Committee takes in charge of the main chain ecology. It works on projects incubation, investment, business development and nodes management. Both of the Committee consist of 5 to 9 members.

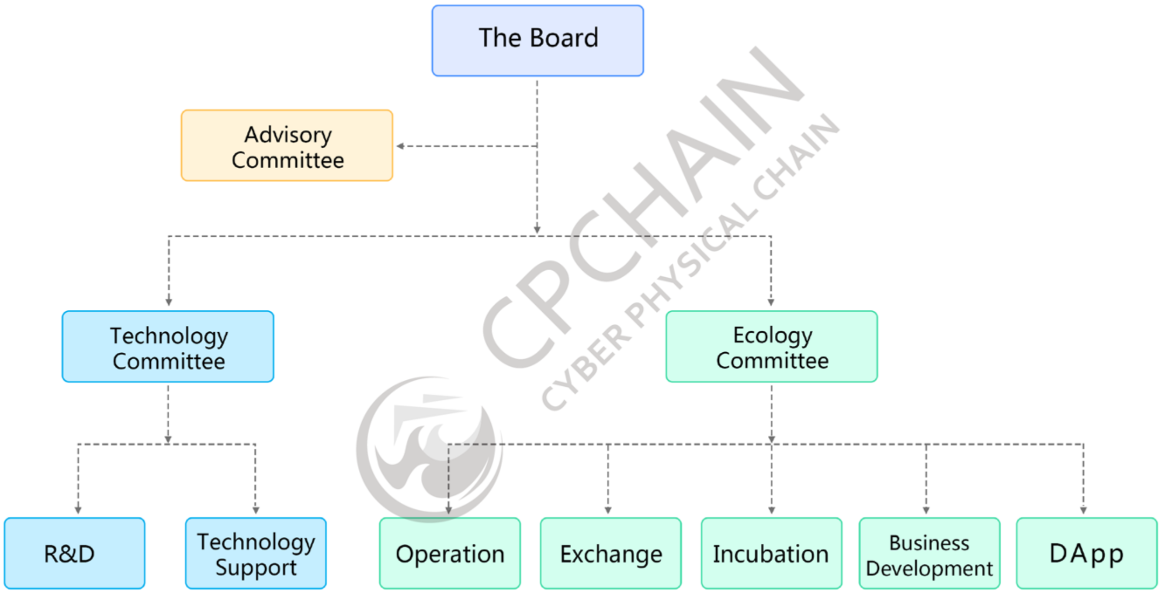


Figure 20. CPChain structure

5.4 CPChain Foundation

5.4.1 Structure

CPChain Foundation board of directors has five or more seats, including one chair and one secretary. CPChain board of directors is essential to the health and sustainability of CPChain ecosystem.

5.4.2 Rights

- All the 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 fund using policies and internal financial control. 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

The board serves a one-year term, and can be lengthened。

5.4.5 Eligibility

Board Chair

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

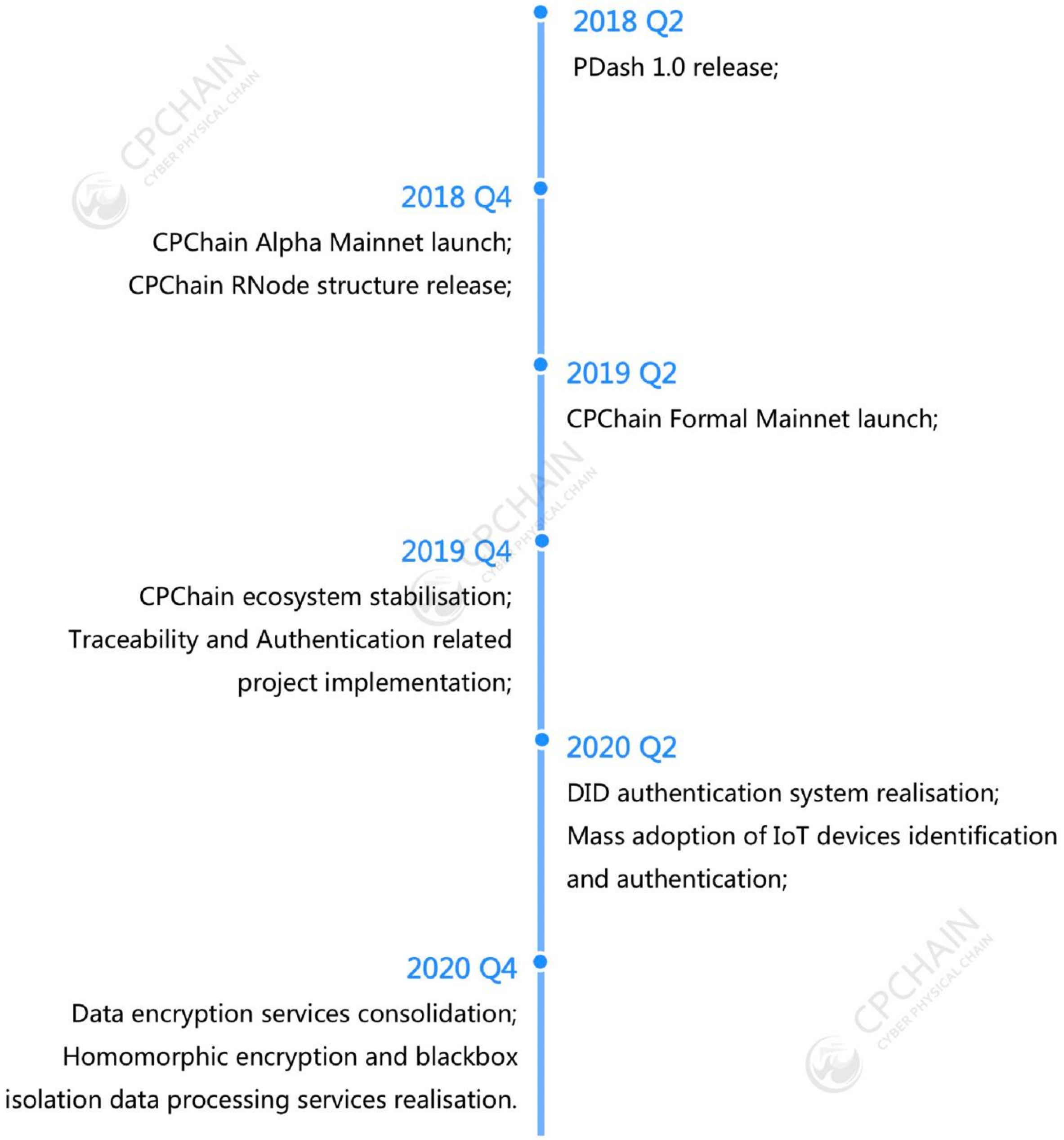
A candidate's approval rating has to hit 50% to become a chair. If no candidates have an approval rating of 50%, another election round would be conducted until successful. Candidate with the lowest rating will not continue the election.

Recall

Should any foundation member come to be perceived as not properly discharging their responsibilities, then they can be called back with the written request of 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 against 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 token will be 1 billion and 40% is used for funding of Overseas community and institutional investors.

Proportion	Allocation Plan	Details
40%	Overseas community and institutional investors	The overseas community will be an important force for the future development of CPChain, and this part will be used in the construction of overseas community; Institutional Investors refer to the enterprises in the built-in distributed business ecosystem and service providers that serve these corporate customers or end-users; these business investors will focus on the future application of CPChain Token (CPC) in their commercial activities.
20%	Founding team, development team and consultants	The founding team, as well as the development team, greatly contributes their human and technology resources and material resources during the development of the project. Therefore, the CPC will be used as a reward and will be locked up for 3 years, with the first year all locked and released in batches each year
40%	Community governance	Maintaining the continuous operation and development of the team; Commercial application exploration and promotion; Selection of suitable industries for strategic deployment in the industry, project support and replacement of tokens for industrial application that truly satisfies the needs of market.

7.2 Project Budgeting

Daily Operation	35%	Including initial team salary, recruiting experts and developers, technical patents and intellectual property protection, foundation operation and marketing expenses, etc.
Technology Development	35%	Technical development, communication and sharing; publication of regular journals; creation or participation of alliances; community incentives, etc.

Business Development	20%	Maintain a series of business channel cooperation such as expanding and operating of CPChain Foundation
Investment	10%	Investment in new blockchain technology and new team

8 Cooperation

Industry Partnership
Italks 智超医疗科技
CLT
国家车辆驾驶安全工程技术研究中心 NATIONAL CENTER OF ENGINEERING AND TECHNOLOGY FOR VEHICLE DRIVING SAFETY
安徽三联交通应用技术股份有限公司 ANHUI SANLIAN APPLIED TRAFFIC TECHNOLOGY CO., LTD
marzipr
Project Partnership
ArQit
HPB High Performance Blockchain
nuggets
connected automated driving.eu
LTO Network
FIOT-LAB
Academia Partnership
上海交通大学 SHANGHAI JIAO TONG UNIVERSITY
香港科技大學 THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY
IEEE BLOCKCHAIN
Capital Partnership
vechain
TORQUE VENTURES
VISIONZ CAPITAL
Association
MOBI
TRUSTED IoT ALLIANCE
IEEE
EASTS
中关村区块链产业联盟
Industry Node
Hyperion Decentralized Infrastructures
keystore
HashQuark
NODE.pacific
CHAIN STAR SEMI
VNT Chain
上海交通大学 分布式智能系统实验室 Distributed Intelligence System Lab, Shanghai Jiao Tong University
国家超级计算长沙中心 NATIONAL SUPERCOMPUTING CENTER IN CHANGSHA
飛馳鎂物 FutureMove Automotive
睦合达 MUHEDA
畅道 上海畅道智能交通技术咨询有限公司 Shanghai CD Intelligent Traffic Technical Consulting Co.,Ltd

"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

9 Disclaimer

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

You acknowledge that any services provided by CPC and information stored and transmitted on CPC 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 CPC 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 CPC 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 securities or other controlled products 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.