PCHAIN Position Paper

The first native multi-chain system that supports EVM in the world
Making large-scale blockchain applications possible

PCHAIN Foundation
pchain.org
2018/3/1

Contents

1 Abstract

The Internet has greatly enhanced the efficiency of information dissemination. Human society has fully stepped into the self-media age after two decades of rapid development. The blockchain, which is hailed as the value internet, has dramatically increased the efficient distribution of digital asset and made self-financing possible. A broad range of industries will be remodeled by the blockchain in the future, just as the Internet has reshaped the traditional industries. There are usually two ways to achieve a historical breakthrough, one is finance and the other is technology. The combination of finance and technology is called Fintech and the core of Fintech is the blockchain. Blockchain was born with financial properties. Blockchain without financial properties can only be called a DLT distributed ledger. Other Fintech technologies, such as big data, cloud computing, artificial intelligence, can be applied to support finance. Nevertheless, finance is not the native property of these technologies.

Blockchain technology began with Nakamoto's Bitcoin, a peer-to-peer cryptocurrency system [1]. Ethereum [2] expanded Bitcoin's capabilities and intended to provide a blockchain with a built-in fully fledged Turing-complete programming language for writing smart contacts, thus opening up a new blueprint for the restructuring of a variety of industries. Ethereum runs a smart contract based on the Solidity language that serves as a platform for writing and deploying DApp (distributed applications/blockchain applications).

Finance is the exchange of funds and assets. In the new economic blueprint formed by the blockchain, it manifests as digital currency represented by bitcoin and digital asset represented by smart contract. Digital currency and blockchain record revenues and expenditures as a distributed accounting system. Smart contracts allow users to customize rules and write code to express their logic. Both utilize the decentralization and immutability of the blockchain to ensure the recording and delivery of values. Blockchain systems for smart contracts are faced with the following major problems at the same time:

1) There is a lack of a unified and effective Oracle. In the closed bitcoin ecosystem, all the data in the system is generated by the system, so there is no problem of the validity and authenticity of the data/knowledge itself. In a smart contract environment, however, we need to obtain the external system data/knowledge, and the validity and authenticity of external data/knowledge often become the bottleneck and obstacle of smart contracts.

2) Insufficient support for large-scale transactions. Inevitably, single-strand competition causes the waste of resources and browsing and restoring transactions are more complicated.

3) Increasing demand for cross-chain supports. Handling the compatibility problems for smart contract data is far from easy.

PCHAIN is a new system with native support for multi-chain applications, making it possible for large-scale enterprise applications based on smart contracts. The core technologies underlying PCHAIN include:

1) The first native multi-chain architecture that supports EVM, with a consensus of POS based on multi-layer sharding mechanism that tremendously improves the performance of transactions.

2) A new Oracle mechanism based on the knowledge graph makes it easier to encapsulate smart contracts. PCHAIN's endogenous W3C-compliant smart data effectively addresses the issue of non-intelligence in smart contracts and can become a fundamental element of smart contracts, just like the market exchange rate data from the external.

3) The goal of PCHAIN Smart Data is to generate valuable data that filters out noise and make it an integral part of Oracle. These smart data can be used in various PCHAIN's smart contracts and other cross-chain requests.

   Smart data, on the one hand, can serve as an intermediary between blockchain and artificial intelligence, and on the other hand, facilitates the integration of blockchain with big data.

   Therefore, it has a vast application prospects, including decentralized question and answer, forecasting markets, the construction of distributed knowledge graph [3], social networks, digital identities and others.

4) The trunked cross-chain solution makes the exchange of digital currency and digital assets more convenient. Various Token (e.g. BCH, ERC20) can be directly used to invoke smart contracts in PCHAIN.

2 Current Situation of Smart Contract

Essentially, bitcoin completes the transition from the ledger state S_t to S_{t+1} via a series of transactions, which can be represented as triples $\langle From, To, Value \rangle$, occurring from time t to time $t+1$. While Ethereum expands the transaction into a six-tuple $\langle From, To, Value, SmartContract, Function, Parameter \rangle$ containing smart contract calls to complete the transition from state S_t to S_{t+1}.

Compared with the blockchain supporting digital currency, the main purpose of the blockchain supporting smart contracts is not only to record the flow of digital currency, but to convert the agreed rules in real life to a smart contract.

After smart contracts are deployed on the blockchain, no one can change the existing rules at will. And after triggering condition, the rules will be automatically executed, no one can intervene.

With the development of smart contracts, it is not only converting the rules to codes now; blockchain applications in a variety of industries begin to deploy more sophisticated smart contracts to record data previously recorded in the database to the blockchain so that the data cannot be modified; thus the blockchain data and operations/transactions are more and more complex, and the scale of applications are also growing.

2.1 Solutions to Support Smart Contract

Commonly, the user uses a specific smart contract language to write the program, deploys it on the blockchain. Then the blockchain will execute the contract in a virtual machine and return the result.

Now there are two ways to deal with the programming language and virtual machine:

One way is to define a new programming language and develop a virtual machine to run the application written in that language. For example, Ethereum uses the Solidity language and Ethereum Virtual Machine [4] [5].

Another way is to use existing programming languages and virtual machines, such as HyperLedger [6], using the Java language and JVM. (HyperLedger is mainly used to build consortium chains and private chains; and our aim is to build a public chain, so for the time HyperLedger is not the focus of our discussion.)

2.2 Existing Problems

From a practical point of view, the blockchains supporting smart contracts have the following problems:

- **Insufficient support for large-scale transactions**

  Taking Ethereum as an example, Ethereum currently deals with about 13 transactions per second, While Facebook handles about 175,000 transactions per second. In terms of the size of the transactions, the current blockchain is still far from the most mainstream social applications.

  In terms of the transaction mechanism, the support for large-scale transactions is also not strong enough. Currently, all DApp transactions are put together and packaged into the same block. When a DApp is very busy, sending too many transactions, and cannot form a new block in time, other DApp's transaction cannot enter the block too, and then all DApps cannot response in time. The status ICO event [7] some time ago is an example that a DApp congestion causes the system not to work properly.

- **All DApps exist on one blockchain, browsing and restoring transactions are complex**

  When there are many DApps deployed on the main chain, each DApp's data including transaction data, is spread across blocks of the blockchain. Tracing and restoring operations on a particular DApp on the blockchain will require traversal of the entire chain, which is less efficient.

- **Lack of a unified and effective Oracle method**

  The Bitcoin system itself is a complete closed loop from the generation, distribution and transfer of digital currencies. When expanding to smart contracts, the entire system is often an open-loop state, requiring an intermediary node to inform the blockchain of external information in the form of an Oracle prophet.

- **POW with single chain at present is a waste of calculation power [8]**

  At present, most of the public chains that support smart contracts use the POW mechanism to reach a consensus. When miners compete to generate a new block, each block consumes the calculation power of all miners. This mechanism causes tremendous waste of calculation of the blockchain network.

  And POW is easy to bring a fork, this will bring some barriers to make transactions confirmed immediately. While POS avoids the waste of calculation power, the public released POS systems do not effectively solve the classic problem Sybil attack.

- **Smart contract data compatibility issues, inconvenient to upgrade**

  Since the data saved on the blockchain (including the codes of smart contracts) cannot be modified, in theory, the smart contracts that have been deployed are immutable. In this way, if there is a bug in the existing smart contract, it will be very difficult to fix it. Although there are various options to solve this problem, it is not easy. For example, export all the original smart contract data, and write them in the new smart contract. In this scenario, if the amount of data is huge, it takes a lot of time, and the transaction-related data of the original smart contract is likely to be lost.

  As software development (including smart contracts) inevitably leads to bugs, how to ensure that smart contracts can be upgraded in a way that ensures data is immutable is already a more urgent requirement.

2.3 Related Work

Multi-chain technology effectively divides the original structure of single-chain into different shardings through the way of the structural reconstruction , which makes the whole block chain structure no longer show the processing power of a single computer. As the number of multi-chain increases, its computing power and storage capabilities increase linearly. A number of related efforts have been made in this field, such as LISK [9], Asch [10] and Ardor [11]. However, none of these multi-chain structures provide direct and effective support for EVM. When the smart contract comes accross problems, it easily falls into an endless loop due to non-Turing complete or without considering the gas limit. Its improved BFT algorithm has a strong centralized tendency. PCHAIN is the first blockchain project to support EVM on a multi-chain structure.

Cross-chain considers the transactions between multiple chains or within the native multi-chain. Early work is usually based on BTC, such as BTC Relay [12], BlockStream [13] and RootStock [14]. RootStock is a secondary chain attached to the Bitcoin blockchain, and provides intelligent contract function through the exchange between BTC and its endogenous SBTC. However, its secondary chain is still single-stranded so that it also faces serious performance bottlenecks like Ethereum. Polkadot [15] further defines cross-chain as Parachain, Relaychain and Bridge. PCHAIN supports the smart contract call of non-native Tokens, which differs from universal cross-chain targeting for one size fits all as Polkadot expected. Cosmos [16] proposes a structure called ABCI to link different heterogeneous chain. However, its current improved BFT Consensus algorithm is costly to communicate and does not support the dynamic joining and exiting of validate.

A number of performance-enhancing efforts are designed from the perspective of improving Transaction Processing and stochastic consensus, such as Dfinity [17], Zilliqa [18] and Aelf [19]. Different from these work, PCHAIN improves the overall performance of the blockchain from the perspective of Data Processing and Sharding through a multi-chain structure, and designs a new consensus approach based on multi-chain structure.

3 Framework and Key Technologies of PCHAIN

In response to the defect of single-chain method which supports smart contracts, a multi-chain approach is proposed to improve the support for DApp. The multi-chain approach has a new structure of a main chain and multiple side chains (as shown in Fig.1). The main chain with the two adjacent side chains looks like the Greek letter , so we name it PCHAIN.

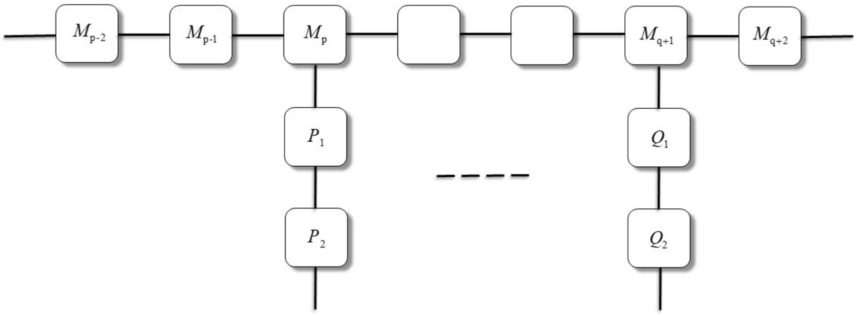


Fig.1 The Structure of Main Chain and Side Chains

The characteristics of PCHAIN will be introduced in detail below.

1) **The growth of PCHAIN**

As shown in Fig.1, the blockchain in the horizontal direction is the main chain and the vertical chains are the side chains.

When you create a new DApp (e.g. a new smart contract), a side chain will be created. Taking Fig.1 as an example, the current block in the main chain is M_{p-1}, and now a request for creating a smart contract is received. The main chain will execute the request and generate a block M_P. Meanwhile, a new side chain P will be generated and the first node P_1 of P points to the block M_P. P_1 contains the binary code of the smart contract. When a request calling the smart contract on the PCHAIN is coming, it will be processed by the PCHAIN. And the PCHAIN will generate a new block P_2. The side chain P is growing in the way that deals with the smart contract.

Besides, side chain also has a growth way (i.e. upgrading the smart contract). When upgrading the smart contract on the chain, the binary code of the latest smart contract will be placed in the newly generated block.

2) **The duty of the main chain and the side chain**

As described in the above section, the main chain stores various account information and transfers digital currency among accounts. It is also responsible for interacting with other existing external public or consortium blockchain and providing interfaces to provide the corresponding service for the side chain. The side chain mainly records the data related to the specific smart contract.

3.1 Key Technologies of PCHAIN

3.1.1 Invocation of Smart Contract for Non-native Token

PCHAIN supports cross-chain calls. With the toolkit provided by PCHAIN, the smart contract on PCHAIN can be invoked using non-native Token on other chains. The toolkit currently supports BCH and Tokens following the ERC20 protocol.

The principle is as follows. When the toolkit provided by PCHAIN, which is used on other blockchains, invokes the smart contract of PCHAIN with a certain number of Tokens in this blockchain, the exchange rate between the Token and PCH (Token of PCHAIN) will be acquired by the toolkit firstly through the smart data in Knowledge Graph. When the convertible PCH is enough to run the called smart contract, the toolkit will transfer corresponding number of Tokens to PCHAIN and consume the corresponding quantity of PCH of PCHAIN to invoke the smart contract.

Taking BCH as an example, the calling process is as follows. Before calling, the caller tells PCHAIN the name, functions and parameters of the smart contract that he needs to invoke through the toolkit. PCHAIN will calculate the PCH to be consumed according to the call, then use the exchange rate between BCH and PCH to calculate the corresponding number of BCH and return them to the caller. The caller fills in the toolkit with the number of BCHs returned in the previous step and imports the name, functions and parameters of smart contract again. After signing the smart contract, the caller will send the request. While PCHAIN receives the request, it will consume the corresponding PCH, then call the corresponding smart contract and return the result.

In the toolkit provided for BCH, the information of the called smart contract is carried by OP_RETURN. In view of the limited amount of information carried by this instruction, it will be considered to propose BUIP to add new instructions for carrying more information in the future.

For the Tokens that follow ERC20 protocol, after obtaining the entitlement of a certain number of the Token, PCHAIN can use the ERC20 interface to make the Token withdrawals and consume corresponding PCH internally according to the exchange rate to invoke the smart contract.

In addition, since PCHAIN itself supports EVM, it also certainly supports the issue of Token that follows the ERC20 protocol. PCHAIN can access a variety of external public blockchain and consortium blockchain, as shown in Fig.2.

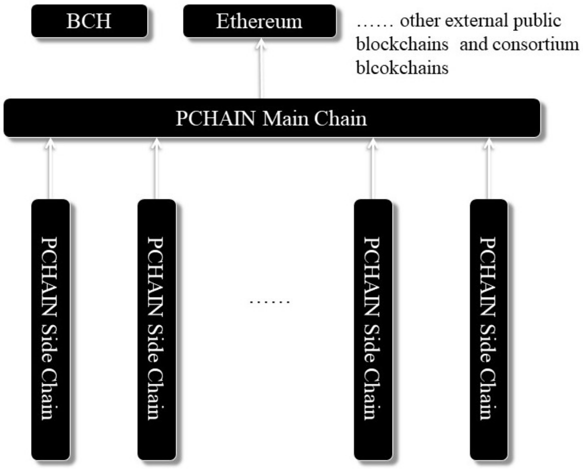


Fig.2 The overall structure of PCHAIN

3.1.2 Consensus of Sharding

PCHAIN supports Shardings at different levels and offers a choice of POS consensus mechanisms to improve the efficiency of operation and storage and support chain expansion.

As far as the current consensus mechanism is concerned, all transactions ultimately can only be executed and verified serially, no matter in POS or POW consensus mechanism. For the current popular POW-based public blockchain, whether it is the Bitcoin network or the Ethereum network, the time consumption of mining even goes far beyond the time consumed by the execution and verification of transactions. The ultimate result is that the entire network can only exploit the power of one node, which causes the situation that it is difficult to improve the performance and expand the structure.

PCHAIN supports expansion of chain and improves operational efficiency by introducing Sharding mechanisms at different levels and supporting POS consensus mechanism.

PCHAIN executes Sharding in two ways:

1. **Hierarchical structure of Main chain and side chain**

   The main chain provides registration, search, storage, deposit and other services for side chains and supports cross-chain transactions. You can create a side chain to complete specific business logic.

   This eliminates the need for all business transactions to be done on one chain, greatly reducing the operation and storage pressure on the main chain, while the side chain also eliminates the interference of other services under the original single-chain model.

2. **For specific chains with more nodes, PCHAIN use transaction-level Sharding**

   PCHAIN automatically enables this Sharding mechanism inside the chain when there are more nodes and too many transactions in the chain. Specific implementation is as follows:

   - Mark the current time point as the beginning of a new epoch.
   - PCHAIN first separates all the nodes in chains by verifiable random functions, and sequentially divides them into different groups called the execution group. Through the same process, select some of the 'qualified' nodes to form a separate group called the governance group.

     Note: The word 'qualified' means that there is enough PCHs and applies to become a member of the Governance Group.
   - The incoming transactions are classified, for example, by sending transactions to a specific execution group, depending on the different categories of users who initiated the request. The execution group performs and verifies the transaction internally and reaches a consensus at the transaction-level.
   - After a certain time interval, all the execution groups will package and submit the transaction list that has been verified to the governance group. The governance group collects these transaction lists from different execution groups to reach a consensus on the block-level for forming a block and broadcasting the new block to the whole network.
   - At the end of each epoch, make sure all nodes are synchronized to the newest block in a consistent state; then enter a new epoch.

   In this way, the transaction really has a parallel implementation of the verification,and gets rid of the single-node drawbacks in a single chain . Fig.3 and Fig.4 show transactions entering different execution groups, respectively, as well as the governance group packaging process:

   PCHAIN offers a POS mechanism for each chain:

   Currently every chain uses POS as a consensus mechanism in the initialization by default . POS as a consensus mechanism can greatly reduce the

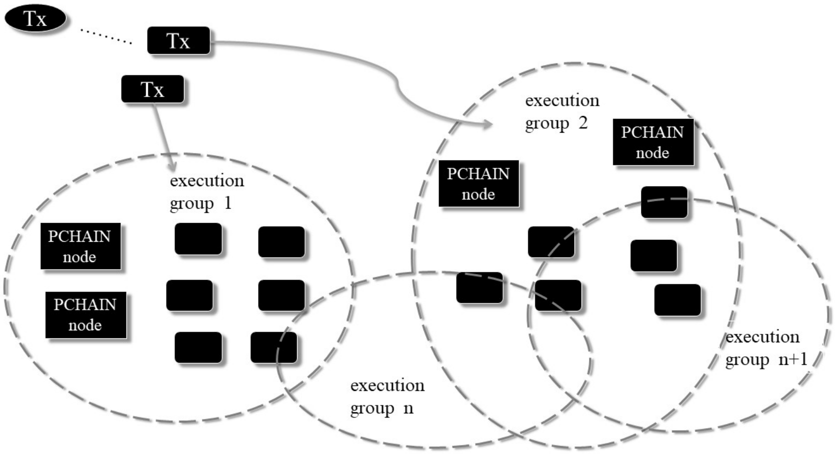


Fig.3 Distributed Transaction Execution

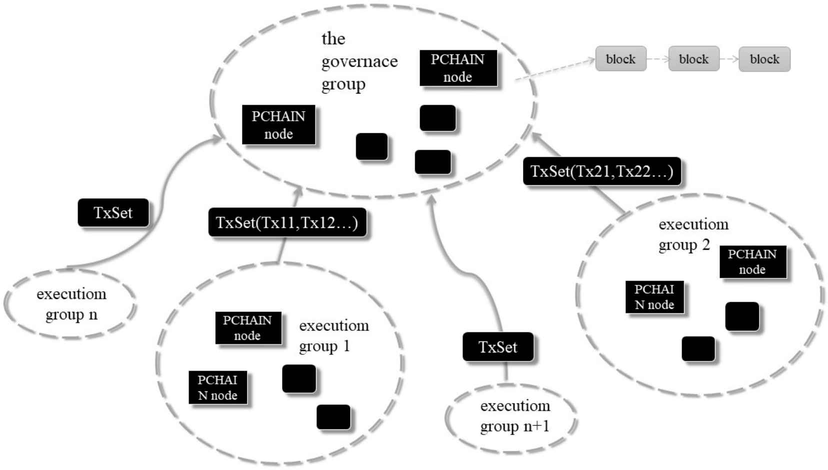


Figure4. Transaction Aggregation and Packing

time needed to reach a consensus and package transactions very quickly to form blocks. So as to avoid the consumption of mining time, and improve the operation efficiency.

3.1.3 Knowledge Graph and Smart Data

The current development of smart contracts is subject to the acquisition of valid external data. There is a lot of information which needs to be obtained from outside the blockchain, such as weather forecast, traffic information, stock price, exchange rate, etc. In Ethereum, there is a solution like Oracle (Prediction Machine) and smart contracts deployed in the blockchain can obtain the corresponding external information from Oracle. However, there is no standard for the Oracle mechanism at present, so it's difficult to realize the cooperation and exchange among different blockchains.

Knowledge Graph, called Ontology Around 2007, evolves constantly under the impetus of Tim Berners-Lee, the father of the Internet. RDF (Resource Description Framework) is a markup language for describing web resources, and an XML (a subset of the standard general-purpose markup language) application that describes metadata as a data model by using XML syntax and RDF Schema (RDFS). An RDF file contains multiple resource descriptions, where a resource description is composed of multiple statements, and a statement is a triple consisting of resources, attribute types, and attribute values, indicating a property of the resource. The statement in resource description corresponds to the statement of natural language. The resource corresponds to the subject in natural language, the attribute type corresponds to the predicate, and the attribute value corresponds to the object. In the RDF terminology, it is called SPO (Subject, Predicate, Object). SPO includes two forms: entity-attribute-value, entity-relation-entity. These triples combine to form a linked digraph called Knowledge Graph.

PCHAIN writes standard RDF triples into the built-in blockchain knowledge base to form Smart Data. The goal of PCHAIN Smart Data is to generate valuable data, filter the noise of the data, and become an element of the smart contracts Oracle. Smart Data can be widely used in various PCHAIN smart contracts, as well as other cross chain requests. Smart Data can be an intermediate layer combining blockchain and artificial intelligence, and can facilitate the combination of blockchain and external big data. Therefore, it has broad application prospects, including decentralized distributed Q&A, market forecast, distributed Knowledge Graph building [18], social networking, digital identity and so on.

As shown in Fig.5, the PCHAIN node has built-in the corresponding modules of Knowledge Graph. The PCHAIN Knowledge Graph module consists of a series of endogenous APIs. The main chain of PCHAIN takes the initiative to access a variety of public trust structures, obtains knowledge of related fields, records in a specific form to fill in the Knowledge Graph module and provides APIs internally; Other smart contracts can invoke the services of the Knowledge Graph module to get relevant information. At the same time, the Knowledge Graph module will be open to the outside world and maintain the audit system. The access of knowledge providers will be welcome, and the PCHAIN will have a certain review of the access service. With the increase in the number of knowledge providers, access to external information will become more and more convenient. Smart Data can support the application of a variety of Knowledge Graph, such as community incentive mechanisms based on blockchains [18].

3.1.4 Supporting EVM

From the implementation of Non-Turing-complete script language to Java, Go and Nodejs, popular blockchains basically support the smart contract; there are many ways which can well meet the needs of their fields. Differently, EVM

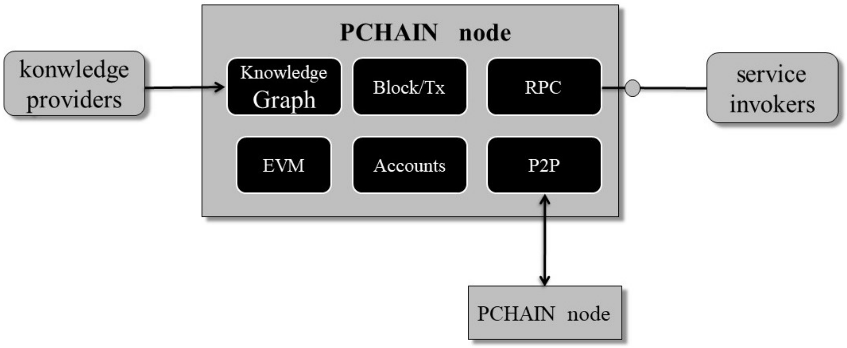


Fig.5 PHCAIN node components and communication diagram

supports a new language called Solidity. EVM completes the logic of business and takes control of all instructions and thus to resist malicious code logic (such as Infinite Gas), While making reasonable and transparent calculations of the costs of calling smart contracts (through the execution of instructions and memory consumption) by implementing Turing complete Solidity.

In addition, EVM + Solidity has established a complete RPC mechanism which can be accessed through http. EVM + Solidity gets quite perfect support of Nodejs Truffle framework, thus you can use js to access it and this provides a great deal of convenience for application programming. These are the reasons why the EVM is popular and has received a great deal of support.

With these factors, PCHAIN now uses Solidity + EVM for smart contracts in both its main chain and side chain so that existing EVM users can quickly build new or migrate existing PCHAIN DApp application.

3.2 Other Technologies

Account mechanism

The mechanism of current blockchain account is divided into UTXO and balance. UTXO (Unspent Transaction Output) which is used by bitcoin mainly uses the address to identify related accounts. If you need to count the available balance of an address, you need to collect the relevant UTXO statistics. Ethereum is based on the balance. The balance becomes an attribute of the account, and the transaction causing the change of amount is recorded separately.

The main purpose of PCHAIN is to deploy and execute DApp, so PCHAIN uses balance mechanism to directly deduct or increase the balance when expenses or benefits occur.

Multilink consensus

Based on the unique multi-chain structure, transaction requests from multiple chains will enter the system at the same time. All request processing is done on a client which means a client participates in all chain consensus and transaction storage. The process of reaching consensus here is mainly divided into three stages.

1) Choose chains to participate in the consensus

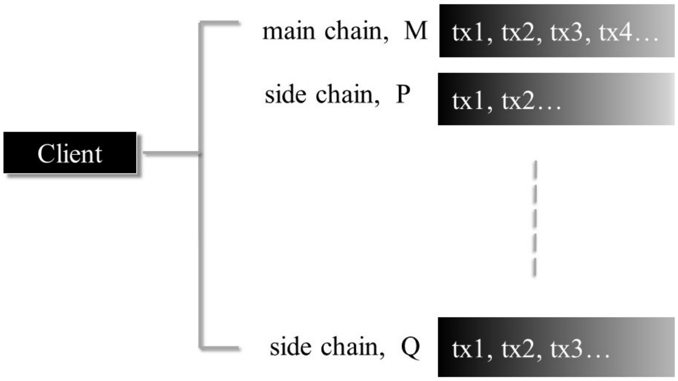


Fig.6 Chain transaction set schematic

As shown in Fig.6, a client receives requests from each chain and prepares a corresponding set of transactions for each chain. The main chain M has transactions txm1, txm2, etc., the side chain P contains txp1, txp2, txp3, etc., and the side chain Q includes txq1, txq2, txq3, etc. These transactions are ready to participate in consensus.

Considering the simplest case, where the client participates in the consensus of one chain at some point. The client knows the speed of the block generated by each chain in the previous period and the number of pending transactions of each chain. When the incentive of generating blocks and processing transactions has been determined, the client can determine which chain is most favorable to generate blocks. Participating the chain which generates blocks slowly will have higher success rate. The incentive mechanism described next may prompt the client to participate in the chain of more pending transactions at present. These mechanisms achieve the requirement that each chain should be duly processed according to the number of transactions included in it.

If the client wants to participate in multiple chains consensus, the process is similar to a single chain but needs to start multiple threads to handle respectively. Note that the number of chains that the client can participate in depends on the hardware and software performance of this client.

2) Generating the master node randomly

If there are enough clients expressing the need for building consensus for a certain chain (assuming is P), they form a set of nodes the next operations are in this set.

First, selecting a node from the clients in this set randomly to act as the master node.

3) Using BFT to generate blocks and broadcasting to the entire network

   After generating the main node, it will enter the BFT protocol and begin to negotiate the transactions of the block chain P that needs to be processed. Then it verifies the vote and finally forms a block.

   After generating the block, it will be broadcasted to the entire network. The consensus mechanism and other multi-block generation mechanisms all can generate multiple blocks at a same time, but there are differences in the growth mechanism of chains [20] [21].

The issuance and incentive mechanism of PCH

In PCHAIN, digital Token PCH is used to measure the labor of the generated blocks.

When blocks are generated, PCH will be issued to the accounts of all nodes participating in the consensus. This is PCH's issuance. When a user invokes the smart contract, statistics are made on the resources required for the command to be invoked to calculate the PCH that the user needs to pay. This part of PCH will also be issued to the accounts participating in the consensus.

Storage mechanism

The blockchain includes account balance and public key; transactions between accounts; the address and binary code of the contract; the storage and call records of the contract; etc. These transactions will make use of Merkle Tree as the hash tree to verify and are stored in the underlying database (e.g., LevelDB).

Smart contract upgrade

The Ethereum EVM and Solidity language have been relatively mature and go through a long test at present. As a result, this project chooses to upgrade on the basis of EVM to support smart contracts and upgrade of smart contracts. The solutions for supporting smart contract upgrading are as follows:

1) The original smart contract C, its publisher is A, its original storage is S, all calls/transactions are T, and all of these are recorded in the side chain P.

2) The new smart contract C1 should be released by A, and C1 will also be deployed in the side chain P. The C1 can increase the storage field, but can not reduce the field, besides, it can add new methods, but can not reduce the method.

3) We can choose whether original contract C still can be invoked when the new contract C1 has been deployed. If permitted, C and C1 provide services. Otherwise, all invocations of C will return a prompt, "Version is deprecated, please use the new version". By extension, the subsequent new contract C2 can decide whether C and C1 will be deprecated. The version cant be reopend to provide services when it has been deprecated.

The underlying mechanism manages different versions of the smart contract. When the smart contract is called, it matches the version of the contract according to the address, and select corresponding code to execute on the virtual machine.

External interface

PCHAIN provides an RPC externalservice similar to the Ethereum [22], which provides a variety of management and query functions, for example, account query, transfer, block and transaction query, contract storage query, etc. REST API based on HTTP is supported currently.

4 Advantages of PCHAIN

PCHAIN is the first blockchain that supports Smart Data, based on which knowledge graph is formed and smart contract can be executed within a closed loop.

Every DApp has its own chain that makes it easy to browse and restore transactions

For the DApps of interest, all the relevant data can be obtained through traversing corresponding side chain from origin block to latest block and thus transactions can be restored to provide browsing, which is different from the single chain that still needs to scan all unrelated blocks. In this way, efficiency can be greatly improved.

Supporting large-scale transactions

When the accumulation of transactions of multiple DApp results in a large overall scale, the scale of the corresponding side chain is relatively small. Now every side chain grows itself without affecting the main chain and other side chains.

When the scale of transactions of single DApp is large, the computing power of the whole network focus on the chain because of incentive mechanism to ensure blocks can be produced in time and transactions can be completed as soon as possible.

If there are many DApps and many transactions in each DApps, the system will be busy and it is hard to avoid congestion. However, this situation is less likely to happen.

New consensus make computing parallelism

Under the original POW mechanism of the public blockchain, every node mines and thus there is a high probability to produce new blocks at same time. However the probability of fork also is high. Under the new consensus mechanism, a group is formed for consensus and the probability of fork is reduced. Meanwhile, with the new mechanism, when a group reaches a consensus, intensive CPU operation is not needed anymore, which can save a lot of power. All nodes can be divided into many small groups and each group has a consensus on one chain, which is concurrent consensus. Besides, groups have intersection, i.e., a node may join consensuses of many chains. Therefore, the computing power is fully utilized and the growing of PCHAIN is smooth.

Supporting smart contract upgrade

PCHAIN supports upgrade of smart contract through the methods above.

High fault tolerance

In construction of PCHAIN, main chain just records, and errors will not occur in theory. When some error happens in a side chain, main chain and other side chains are not affected and only corresponding side chain needs to be corrected.

Expansibility

It is easy to deploy a new DApp with expanding a new side chain. Under the consensus mechanism, the growing of new chain does not cause much burden.

5 The Prospect and Application Scenarios of PCHAIN

5.1 The Prospect of PCHAIN

PCHAIN is the first native multi-chain system which supports EVM which makes it possible to apply blockchain at large scale.

5.2 Application Scenarios

PCHAIN can be applied to many scenarios based on smart contracts:

- Distributed artificial intelligence, distributed question and answer, big data transaction.

- Digital asset transaction - provide reliable records of digital asset transactions.

  Digital assets include digitized certificate of asset, or they are digital network virtual assets (various game props, token, etc.)

  Smart contracts can record every operation such as login, transfer and sale in blockchain. These records are open and transparent to all participants which offer convenience for censorship.

- Game C Set rules for the game to prohibit cheating.

  Here are mainly refers to the games of chance. After the rules are established, the game process and the results will be carried out strictly in accordance with the rules, thus avoiding the artificial influence on the results(e.g. the lottery game and the dice game).

- Notary system - Provide a promise with a basis that cannot be tampered with.

  In the notary system, the authenticity of the basis is very important. There wont be any question on the authenticity of the basis if its recorded in the blockchain.

- Trace sociality C record all the words that have been said.

Most of the existing social records will be cleared after a long time. There are also some social scenes that support the way of burn after reading. However, as for some serious talk, we may want to store them forever and view them whenever we want, which can be achieved with the smart contract combined with blockchain.

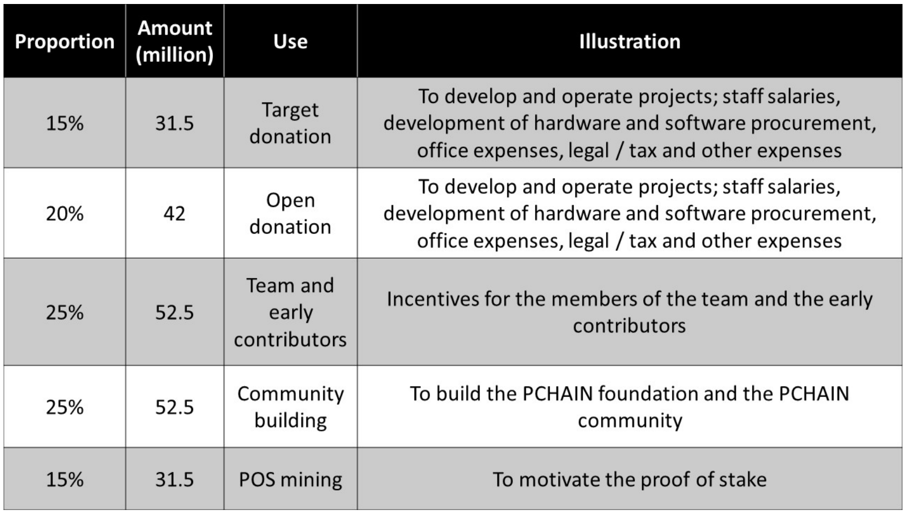
- Full-cycle collaboration system C it works on the whole process, from planting, harvest to entering market.

  This system tracks the whole Green ecological chain, from farming, to slaughter, to transportation and finally to sales. In the field of logistics supply chain, the whole process will also be tracked from product production to transportation to shelf and finally to consumers' hands. These full - cycle collaboration systems enable the participants in each part to share data and increase collaboration and trust in them.

6 Development Plan

6.1 Fund Raising and Management

6.1.1 Ways of Fund Rasing



Proportion	Amount (million)	Use	Illustration
15%	31.5	Target donation	To develop and operate projects; staff salaries, development of hardware and software procurement, office expenses, legal / tax and other expenses
20%	42	Open donation	To develop and operate projects; staff salaries, development of hardware and software procurement, office expenses, legal / tax and other expenses
25%	52.5	Team and early contributors	Incentives for the members of the team and the early contributors
25%	52.5	Community building	To build the PCHAIN foundation and the PCHAIN community
15%	31.5	POS mining	To motivate the proof of stake

The project will be funded by target and open donation of token.

1) The name of PCHAIN's Token is PCH, and a total of 210,000,000 (210 million) PCH will be issued.

2) Donation and Distribution.

Among all the token, 15% is used for the target donation. 20% is used for open donation. 25% is reserved for the core team and early contributors. 25% is used for community construction. The remaining 15% is used for POS mining.

Token donation phase consists of target donation stage and open donation stage. Open donation is only offered to the citizens of countries and regions permitted by relevant laws and regulations. The start time of target donation depends on the development and operation of the first round.

15% as the first round of target donation: 31.5 million PCH	20% as open donation: 42 million PCH	
	Early bird week (one week)	Ending week (one week)

6.1.2 The Use of Funds

The fund will be used as follows:

- 65% - PCHAIN system research and development, including wages, software and hardware procurement, etc.
- 20% - Carrying out the marketing campaign, including wages, promotion expenses, etc.
- 10% - Carrying out operations, including holding all kinds of activities, etc.
- 5% - Conducting legal compliance, including the payment of counsel fees, etc.

6.1.3 PCHAIN Foundation

The PCHAIN Foundation (PCF) is a nonprofit organization. Through the establishment of relevant departments, the PCF is committed to the research and development of PCHAIN, the management of PCHAIN's open source, the community construction and the feature recommendations. At the same time, it is committed to the finance management, team building and external relations of the project to make the project run better.

The PCF plans to establish the following departments:

- **General Executive Department**

  The PCF will set up the general executive department, which is responsible for the normal operation of the foundation, including departmental establishment, function adjustment, personnel recruitment and external communication.

- **DApp Management Department**

  DApp management department is responsible for tracking and managing all the DApp added to PCHAIN, and communicating with DApp developers(companies or individuals), so as to ensure PCHAIN can provide the best service for DApp development and deployment.

- **Code Review Department**

  Due to the attack of hacker, even very large blockchain projects encounter a large number of cases of asset loss. Here, learning from other communities, we can set up a code review committee to review all the code submitted to the open source community, especially the part involved in the circulation of PCH.

- **Administration and Public Relations Department**

  Responsible for financial and personnel management, that is, to coordinate and master the expenditure of the project and the change of personnel. When the project has a major release or an influential event happens, it is responsible for advocacy and response.

6.1.4 System Use

There are two main uses of PCHAIN system:

1. **Promoting the combination of smart contract and blockchain**

   After the establishment of PCHAIN, a certain amount of cost is required to pay while combining smart contract with blockchain and invoking smart contract, which is settled by PCH. In addition to mining, PCH can also be obtained in the market. After PCHAIN is built, there will be more and more applications on the chain, more and more transactions will be carried out on the chain, the demand for PCH will also increase, and the value of PCH will increase. As a result, the value of PCHAIN project will increase.

2. **Providing PCHAIN-based services**

   As the provider of PCHAIN platform, we have the leading power to the core technology and application development interface of PCHAIN. We can provide convenient products based on PCHAIN, such as query platform, and also provide technical solutions for DApp's demand side which makes the development of DApp smoother, for example, the upgrade of smart contracts.

For now, 3 international well-known large blockchain application projects has been planned to be established based on PCHAIN. For example, cultural blockchain project built by international famous music producer has been recognized by Japan's Blockchain Association and reported by Japan's rich television, Phoenix, People's Network, Sina, Sohu, Tencent, Netease and many other media; the research of anti-quantum blockchain in cooperation with State Key Laboratory of Tsinghua University has been recognized by many academicians. In addition, a number of blockchain application projects are underway.

6.1.5 Legal Risk

The PCF will comply with the relevant laws and regulations of each country, and provide technical and financial support for the PCHAIN community and enthusiasts around the world so as to promote the smooth progress of the PCHAIN project. However, due to unforeseen changes in market and technologies, this project may not achieve the anticipated goal and in the worst case PCH token might become valueless, even though we have done thorough market analysis and technical preparation. Investors should be aware of this risk and conduct risk control accordingly.

6.2 Team Members

A global team of internationally recognized experts with years of experiences in the blockchain industry will oversee the research, development and management of PCHAIN project. Their roles and relevant experiences are introduced in below.

- **Feng Cao (Vision & Algorithm)**

  Dr. Feng Cao graduated from Fudan University in Computer Science. He is the inventor of the 1st International Blockchain patent from China, the Co-Founder of ChinaLedger, the most influential blockchain alliance of China, the Chief Scientist of Blockchain Application Committee in China Federation of Logistic and Purchasing (The 1st Gov Association in Industry), and a Senior Fellow of the China Blockchain Research Alliance. Dr. Feng Cao and his team successfully accomplished the 1st blockchain-based assets earning rights transfer in the world in September 2016, which is also the 1st Financial Blockchain Transaction in China. He is a bold player in financial blockchain industry in China. He found several blockchain startups that attracted investment from top funds and received a few financial blockchain innovation grand awards. He was the Chief Scientist of Internet Finance and co-chair of the patent review board in IBM Research-China. Dr. Feng's innovative achievements have been successfully adopted in China, US and other 150 countries. He won IBM Global Technical Achievement Awards three times. He published 22 papers in ACM/IEEE top conference and 30+ international patents.

- **Haojing Lv (Architecture)**

Haoijing is a Master of Computer Science with Tsinghua University. He is a blockchain technology pioneer of China and responsible for a few global blockchain projects as team leader. He has worked for several leading international company such as SAP Shanghai Lab, with rich commercial experiences in product optimization and innovation, system level software design and implementation, distributed cluster deployment, big data storage, mining and visualization, large-scale software development process and quality control.

- **Ruosong Xu (CMO)**

  Ruosong is the former chief marketing officer of GXS (Gong Xin Bao). He received the Bachelor of physics at Fudan University. He has worked for HUAWEI, China Mobile and Tong Dun Technology with extensive experience in the field of big data, credit risk control, communication and IoT.

- **Zhanfeng Ma (Blockchain Storage and Optimization)**

  Zhanfeng is a Master of Computer Science with Xian Jiaotong University. He is a senior software engineer and expert of core blockchain technologies. He has over 10 years working experiences at Global Top 500 companies with focus on database systems and distributed systems. He holds a few US patents in database area and has rich experiences in system development and performance optimization.

- **Kai Zheng (In-memory Data Management)**

  Dr. Kai Zheng is a Full Professor of Computer Science with University of Electronic Science and Technology of China. He received his PhD degree in Computer Science from The University of Queensland in 2012. He has been working in the area of spatial-temporal databases, uncertain databases, social-media analysis, in-memory computing and blockchain technologies. He has published over 100 papers in prestigious journals and conferences in data management field such as SIGMOD, ICDE, VLDB Journal, ACM Transactions and IEEE Transactions. He is authoring the book Blockchain Technology and Practices. His Google Scholar citation is over 1400 with H-index = 21. He was the recipient of Australian Discovery Early Career Research Award in 2013, and Best Paper Award of International Conference on Data Engineering (2015). He was the Program Committee Co-chair of the of the 18th APWeb Conference and General Co-chair of the 22nd DASFAA Conference. He is a PC member of over 10 top conferences and invited reviewer for the most prestigious journals.

- **Zhihong Chong (Knowledge Graph)**

  Dr. Zhihong Chong is an associate professor in the college of computer science and engineering at Southeast University. He was visiting scholars of University of New South Wales in Australia and University of Illinois

Research Center in Singapore. He has focused on theoretical and applied research and development of blockchain, big data, knowledge graph and deep learning. He has led and participated in the National Natural Science Foundation, National 863, the national key defense projects, and more than 10 enterprise cooperation projects such as HUAWEI, China Electronics Group and Focus Technology Co. Ltd. He has published more than 10 papers in major conferences and journals in the field of database and artificial intelligence.

- **Zhenjie Zhang (Query Speedup and Indexing)**

  Dr. Zhenjie Zhang received PhD degree of computer science from National University of Singapore, and is now a senior research scientist at the University of Illinois Advanced Digital Science Center. His research areas include database query, indexing of high dimensional data mining and causality analysis, data mining and machine learning in privacy protection, high-speed data stream processing, and elastic cloud computing technology. He has published over 50 prestigous papers in databases, data mining and machine learning fields, including SIGMOD, VLDB, ICML, VLDB Journal and IEEE TKDE, which have more than 1800 Google Scholar citations. He was the PC co-chair of International Data Privacy Seminar (2013) and Asia-Pacific Web Conference (2015), and program committee at over 10 top international conferences. He won President Award of National University of Singapore in 2008, Early Career Research Award of the IEEE Data Engineering Technology Committee (TCDE) in 2015, and the best paper award at the IEEE International Conference on Cloud Computing in 2013.

6.3 Road Map

- PCHAIN Position Paper completed – T
- Dewdrop stage – T + 7 months

  Complete the development of PCHAIN core system which supports account system and deployment of smart contract, publish technical white paper, conduct a test online.
- River Stage – T + 12 months

  Publish the product on the major network, complete document of external API and wiki.
- Sea Stage – T + 15 months

  Expand the capabilities of knowledge graph and Smart Data Blockchain and support external development interfaces.
- Ocean stage – T + 18 months

  Introduce several blockchain application projects to form Knowledge Graph Blockchain Alliance.

After examining the results of the 18-month milestone, a new plan will be maked for the specific development, so that PCHAIN can maintain the correct R&D and service direction and maintain the leading position in technology and market.

References

[1] Bitcoin,
https://bitcoin.org.

[2] Ethereum,
https://ethereum.org.

[3] S. Bai,
http://blog.csdn.net/TgqDT3gGaMdkHasLZv/article/details/78146296.

[4] Solidity,
https://solidity.readthedocs.io/en/develop/.

[5] ethdocs.org, "What is Ethereum? Ethereum Homestead 0.1 documentation,"
https://ethdocs.org/en/latest/introduction/what-is-ethereum.html#ethereum-virtual-machine.

[6] HyperLedger,
https://www.hyperledger.org/about.

[7] Bitcoin.com,
https://news.bitcoin.com/status-ico-generates-over-60-million\\-but-fails-to-deliver-meanwhile-ethereum-flounders/.

[8] wikipedia,
https://en.wikipedia.org/wiki/Blockchain\\#cite_note-te20151031-1.

[9] LISK,
https://lisk.io/.

[10] Asch,
https://www.asch.io/.

[11] Ardor,
https://www.ardorplatform.org/.

[12] B. Relay,
https://btcrelay.org/.

[13] BlockStream,
https://www.blockstream.com/.

[14] Rootstock,
https://www.rsk.co/.

[15] Polkadot,
https://polkadot.io/.

[16] Cosmos,
https://cosmos.network/.

[17] Dfinity,
https://dfinity.org/.

[18] Zilliqa,
https://www.zilliqa.com/.

[19] Aelf,
http://aelf.io/.

[20] B. Wiki,
https://en.bitcoin.it/wiki/Merged_mining_specification.

[21] J. P. V. Buterin,
https://www.plasma.io/plasma.pdf.

[22] JSON-RPC,
https://github.com/ethereum/wiki/wiki/JSON-RPC.