BHP

Blockchain of Hash Power

White Paper V3.0

BHP Foundation

December 2019

1 Project background

As a pioneer of digital cryptocurrency, BTC has achieved great success, not only leading the development wave of blockchain technology, but also staying in the top position in a decade-long competition, and occupying more than half of the market value of the digital currency market for a long time. The foundation of all currencies is credit, so does BTC. The BTC network finally created a physical credit similar to gold by means of encryption algorithms, P2P networks, PoW consensus mechanisms, and economic incentives. Although various altcoins and forkcoins tried to replace the status of BTC, relying on the huge amount of hash power as a credit endorsement, the security and decentralization of BTC have been widely recognized by more and more people. Up till now, Bitcoin is still the most accepted digital cryptocurrency with the most widely circulation and the highest market value.

However, Bitcoin is not so perfect. Low payment efficiency, high transfer cost and other defects limit the bitcoin’s circulating convenience seriously, and bitcoin is more used as a means of value storage. The huge amount of hash power behind Bitcoin network doesn't support smart contract calculation, which results in low expansibility of the Bitcoin network and that the Bitcoin network can not satisfy the increasingly diversified applications in finance. To address the defects of Bitcoin network, many projects have been explored for improvement, which could be roughly summarized to two directions: the first one is to release a more technically advanced blockchain to replace the position of Bitcoin; however, due to the insufficiency of hash power as the basis of credit, the new chains can not shake the status of Bitcoin; the second one is to transfer Bitcoin to a new side chain to extend its application based on cross-chain technology. However, as Bitcoin hash power is not introduced into the new chain as the infrastructure support, potential risk exists, and the operating effect needs to be verified.

Furthermore, in the era of AI, all the developments of big data, cloud computing, IoT, robot, 5G, blockchain and other technologies are pointing to AI. Large number of intelligent objects fueld with computing power will gradually be applied to various industrial fields. Except for the hash power applied to digital cryptocurrency field, kinds of new computing power are emerging such as complex genetic computing power for biomedical engineering, IPFS computing power for distributed storage, and AI computing power based on big data. The demands for computing power resources from industries will keep increasing, and at the same time, human beings are entering the era of "computing power monopoly" and "computing resources monopoly". Computing power is rapidly showing a trend of centralized monopoly, bringing huge threats to the society of human beings.

In order to break computing power monopoly, ensure the security of human beings in the intelligent machine era, address the imbanlance between computing power supply and demand, and the computing power supply, management, transaction, closing, clearing and derivative financial services of various computing power networks urgently need a decentralized, intelligent, neutral and independent blockchain network which can be assimilated into various computing power ecosystems in a transparent manner, and introduce the interests of the owners and producers of different kinds of computing power s into a new consensus mechanism, and further expand the computing power ecosystem through smart contract, side chain, cross-chain and other technologies, provide ‘connecting’, ‘circulation’, ‘credit’ and other services among different kinds of computing power, and finally build a decentralized computing power infrastructure with a sustainable, secure, and trusted framework, enabling everybody to easily enjoy the fruits of digital civilization in the age of AI.

2 Introduction to BHP public chain

BHP(Blockchain of Hash Power) is a global intelligent computing power network. It’s endeavored to build a set of infrastructure centering on computing power ecosystem so as to provide basic services to various emerging computing power ecosystems represented by digital cryptocurrency hash power, genetic computing power, IPFS computing power and AI computing power, and to expand the application scenarios of these kinds of computing power, build an ecosystem centering on computing power asset credit, and to promote the convenient supply, acquisition, circulation, transaction, settlement and derivative financial service of various kinds of emerging computing power around the world.

Through the consensus mechanism of mixed equity entrustment of computing power holders and BHP holders, BHP introduces the computing power holders into the governance structure.The computing power holders’ equity and the BHP holders’ equity are mutually bundled and constrained to achieve the transfer of computing power credit to the BHP public chain. Essentially, the BHP computing power public chain is a decentralized blockchain network with computing power as the credit endorsement and supports smart contract.

The application scenarios of BHP public chain include:

- Computing power ecosystem services: on-chain computing power, tracing, circulation, and output distribution etc.
- Computing power mortgage loan: release of computing power mortgage loan based on cross-chain and smart contracts.
- Digital asset circulation: To provide a safe and efficient online and offline payment service for stablecoin based on computing power and guarantee with computing power.
- Other financial services.

As an independent, non-profit membership organization, the BHP Alliance aims to coordinate and provide a BHP management network framework, sustain and lead social influence for the funding of BHP public chain. The members of the Alliance consist of a network of verified nodes running the BHP public chain. Members of the BHP Alliance will include businesses, non-profit and multilateral organizations and academic institutions from all over the world. The initial members will jointly complete the articles of the Alliance as "Founding Members". These members are Wuzhou Capital, Red Overtone Earth, Chenlian Capital, Jingdu Capital, MATRIX, Juntong Capital, Chuangxiang Space, Block Chain VC, Renren Capital, Bothwin Capital, Bit Mining, West CRYPTO, UK Hash Power Alliance, DSQ Spring, etc. Node members will be updated every year, with the total number no more than 20.

In addition, the BHP public chain will be open to everyone: Any consumer, developer or company can use the BHP network to develop products and add value to their services. Open access ensures a low barrier to entry and innovation and encourages stakeholders to conduct healthy competition.

2.1 Basic services for computing power ecosystem

Along with the success of BTC, mining has evolved from the original decentralized PC mining to the current complex ecosystem including mining machine manufacturers, large mining farms, mining pools, cloud hash power sellers and renters. However, with the continuously increasing mininge difficulty, hash power is almost concentrated into the large mining farms, and it is more and more difficult for individual miners to participate in mining. Although there have been many cloud hash power sellers and renters facing individual investors, a lot of practical problems still exist. For example, the hash power is completely provided by a centralized organization, and the authenticity and transparency of hash power cannot be guaranteed; the hash power is mostly tied to the mining machines, which is inconvenient to split and is very unfriendly to individual investors; in most cases, the individual investors just purchase hash power only once, and the purchased hash power has poor liduidity; generally individual investors are very sensitive to transfer fee due to lowbitcoin output.

BHP public chain will provide basic services such as computing power on-chain and unitization, settlement and output distribution for computing power ecosystem. The miners can realize free transfer of future income right and carry out the hedging when they are accessed to the computing power chain. The users can easily obtain the income right of computing power with high transparency, reliability and liquidity on the computing power chain.

BHP public chain supports unique registration of all kinds of computing power accessed to the BHP network, ensuring every unit of hash power is real, open and transparent. The on-chained computing power can be quantized as different units such as THs, Ms and TFLops for the convenience of usage and circulation; Any sale and transfer process of computing power can be checked on the chain and the process can be traced to ensure the security and transparency of the computing power transactions. Please see below Figure 2-1 for the quantitative model of computing power asset digitalization:

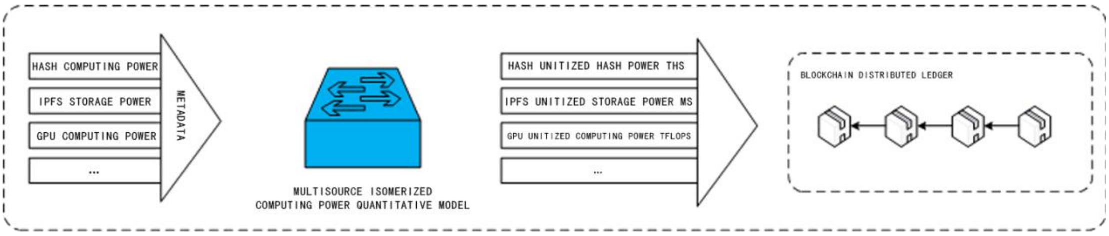

HASH COMPUTING POWER
IPFS STORAGE POWER
GPU COMPUTING POWER
...
METADATA
MULTISOURCE ISOMERIZED
COMPUTING POWER QUANTITATIVE MODEL
HASH UNITIZED HASH POWER THS
IPFS UNITIZED STORAGE POWER MS
GPU UNITIZED COMPUTING POWER TFLOPS
...
BLOCKCHAIN DISTRIBUTED LEDGER

Figure 2-1 Hash power asset digitalization model

2.2 Computing power asset management service

The new generation of block chain represented by ETH is characterized by the introduction of smart contracts, making various financial applications possible. BTC itself does not support smart contracts, but the emergence of cross-chain technology enables hash power to be transferred from BTC network or other hash power network to another public chain, thus realizing the application expansion of hash power. Adopting cross-chain technology and smart contracts, BHP public chain can build DeFi applications based on computing power.

The program of using smart contracts for mortgage loan and creating stable coins has already gained initial success on the Ethereum network, such as Maker DAO. Compared to ETH, computing power has smaller fluctuations and higher market value, enabling computing power-based mortgage systems to achieve higher mortgage ratios while supporting the generation of stable coins with a higher theoretical amount. BHP public chain will launch BTC hash power-based mortgage loan and stable coins, on the one hand, through mortgage loan, BTC hash power holders can use the funds more efficiently and realize rapid asset appreciation. On the other hand, stable coins, as the bridge connecting the legal currency world, can be more widely adapted to payment scenarios.

2.3 Payment system and its ecosystem construction

Starting from BTC, blockchain technology is naturally an innovator of traditional payments. The P2P transaction that does not require a third-party organization makes the payment process simple, safe and efficient. Especially facing the high-cost and inefficient scenarios such as cross-border payment, the payment advantage based on blockchain technology is more obvious.

However, even for the most widely accepted BTC, its payment function has not been applied in large-scale due to the following reasons: high fluctuation of the coin price limits the acceptance of BTC be used as transaction medium; low payment efficiency makes BTC is not suitable for daily consumption scenarios; transfer fee is not friendly to micropayments. The above shortcomings slower the progress of BTC's payment ecosystem. On BHP public chain, users can obtain stable coins through BTC hash power mortgages for daily payments, not only enjoying the appreciation of assets but also obtaining a wider payment acceptance. At the same time, BHP public chain is characterized by features such as high concurrency, low charges and high security, which greatly improves the convenience of micropayments.

Through the measure such as open consensus nodes to share benefits with exchanges, financial institutions and merchants, BHP can establish payment alliances, break through payment barriers, and create better payment experience for users.

The whole BHP application ecosystem is divided into six layers, as shown in Figure 2-2:

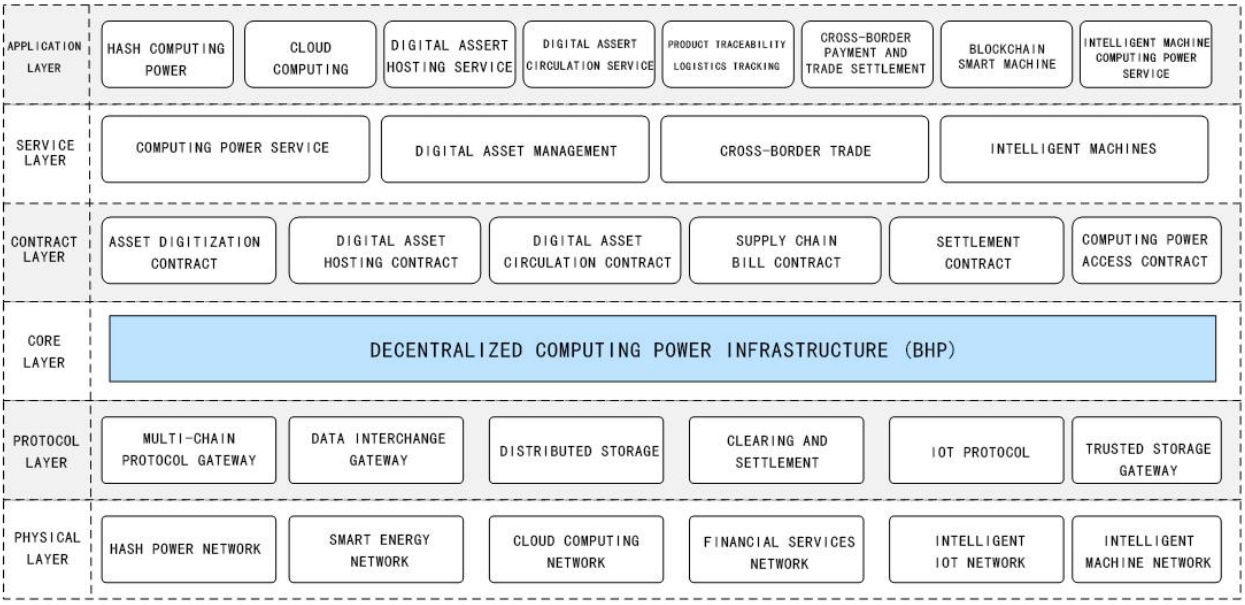

APPLICATION LAYER
HASH COMPUTING POWER
CLOUD COMPUTING
DIGITAL ASSERT HOSTING SERVICE
DIGITAL ASSERT CIRCULATION SERVICE
PRODUCT TRACEABILITY LOGISTICS TRACKING
CROSS-BORDER PAYMENT AND TRADE SETTLEMENT
BLOCKCHAIN SMART MACHINE
INTELLIGENT MACHINE COMPUTING POWER SERVICE
SERVICE LAYER
COMPUTING POWER SERVICE
DIGITAL ASSET MANAGEMENT
CROSS-BORDER TRADE
INTELLIGENT MACHINES
CONTRACT LAYER
ASSET DIGITIZATION CONTRACT
DIGITAL ASSET HOSTING CONTRACT
DIGITAL ASSET CIRCULATION CONTRACT
SUPPLY CHAIN BILL CONTRACT
SETTLEMENT CONTRACT
COMPUTING POWER ACCESS CONTRACT
CORE LAYER
DECENTRALIZED COMPUTING POWER INFRASTRUCTURE (BHP)
PROTOCOL LAYER
MULTI-CHAIN PROTOCOL GATEWAY
DATA INTERCHANGE GATEWAY
DISTRIBUTED STORAGE
CLEARING AND SETTLEMENT
IOT PROTOCOL
TRUSTED STORAGE GATEWAY
PHYSICAL LAYER
HASH POWER NETWORK
SMART ENERGY NETWORK
CLOUD COMPUTING NETWORK
FINANCIAL SERVICES NETWORK
INTELLIGENT IOT NETWORK
INTELLIGENT MACHINE NETWORK

Figure 2-2 BHP application ecosystem structure

Physical layer refers to a physical network carrier that maps digital assets to physical assets or vice versa such as hash power network of Bitnet, cloud computing network that provides highly available storage and network bandwidth, open interconnection, user-centered and distributed peer-to-peer energy interconnection network, open and transparent service information platform that benefits all participants in financial activities, and interconnection network based on the Internet that all ordinary physical devices or intelligent machines can be independently addressed.

Protocol layer refers to a protocol network through which the BHP connects to the physical layers: a multi-chain protocol gateway connecting hash power; a data gateway for information interaction with smart energy network; a distributed storage protocol that provides data validation for cloud computing network data storage; a layer of clearing and settlement protocol in cross-border trading services; a service access relay and trusted storage gateway protocols connected to the smart IoT.

Core layer refers to the core layer of computing power infrastructure realized by the blockchain technology which can provide decentralized, trust-free, tamper-proof data and distributed storage network services for asset circulation. It mainly consists of digital encryption algorithm, distributed ledger, P2P network, consensus protocol, incentive mechanism, virtual machine of contract operation, etc.

Contract layer refers to a business logic and algorithms based on the blockchain virtual machine, as the basis of realizing the programmable and operational data of the blockchain system. The contract layer encapsulates all kinds of script codes, algorithms and more complex smart contracts generated by the blockchain system, which enables the blockchain to support many applications in the real world. The smart contract layer provides procedural guarantee for asset circulation and forms a decentralized value circulation system. On the premise of no participation of the third-party central organization, it fully guarantees the privacy and data security of all assets, and at the same time, provide flexible and diverse smart contract logic for all parties to realize the maximization of resources and interests in the competition.

Service layer refers to the interface layer that provides blockchain services for the application layer. It is a routing channel connecting the physical assets and the digital world mapping the the application layer's business requirements with the contract layer, and the asset value transfer and sharing are realized through the smart contract. At present, the main services provided include the digitization and circulation of computing power assets, the hosting and circulation of digital assets, the tracing and clearing of goods in cross-border trading, the interconnection of AI equipment information and the export of AI services.

Application layer refers to the interaction layer provided to the third-party blockchain application DAPP. It is the application platform to complete the digitization of computing power assets and the circulation of digital assets, and is the entrance and management tool for users to access the blockchain.

3 BHP management mode

3.1 Economic model

The computing power coin (BHP Coin, BHP for short) is the original token of BHP public chain, and is also an equity token, which is used to stimulate the block chain construction and manage the block chain ecosystem.

- Right to share the outputs of computing power: while the BHP public chain provides basic services for the computing power ecosystem, it shares a certain percentage of computing power output as the service fee.
- Right to vote: BHP holders can participate in the consensus node campaign voting and share the node block rewards.
- Right to future benefits: as the public chain ecosystem grows, BHP holders can further share the various potential benefits of the block chain ecosystem, including payment charges.

3.2 Issuance mechanism

The authorized number of BHP is 100 million in total, with a minimum unit of 0.00000001. BHP is generated along with the formation of each new block. Forty-five million of them were issued to 21 initial super nodes of the BHP Foundation (50% of the total BTC output werebe attributed to BHP Foundation, and the other 50% were be used to calculate the daily operation cost of the computing power) in proportion according to donated BTC hash power of these super nodes before the public chain goes online. Each node provided not less than 10PHs of BTC hash power, and the highest node provided more than 100PBTC hash power. The issuance was directly generated in the Genesis Block after the public chain was online, and was mapped to this part of hash power contributors in the initial stage.

The remaining 55 million BHP will be used to stimulate BHP's computing power ecosystem construction.

BHP, like Bitcoin, is halved every four years. It will stop producing new coins in about 2140 when the total number of produced coins reaching the 100 million. The interval of each block of BHP is about 15-20 seconds, and the formation of 2 million blocks takes about a year.

In the first cycle, 4.96 BHPs are generated for each block. In order to keep up with the half of Bitcoin in May 2020, a total of 3315200 blocks and 15548288 BHPs will be generated.

In the second cycle (4 years in total), 2.345 BHPs are generated for each block, a total of 8400000 blocks and 19698000 BHPs will be generated.

In the third cycle (4 years in total), 1.1725 BHPs are generated for each block, a total of 8400000 blocks and 9849000 BHPs will be generated.

And so on, BHP will stop generating new BHPs until the total amount reaches 100 million in about 2140.

3.3 Governing mechanism

BHP is the only governing token in the public chain with 100% voting rights.

On-chain governance: BHP holder is the owner and manager of the BHP network. The management right is realized by constructing voting transactions on BHP network, and the usage right of BHP network is realized by acquiring BHP. BHP can be transferred.

Off-chain governance: BHP Foundation is a standing management organization established by the founder of BHP project. It consists of a management committee, a technical committee and a secretariat, which are respectively responsible for strategic decision-making, technical decision-making and implementation. The BHP Foundation is responsible to the BHP community with the primary objective of promoting and developing the BHP ecosystem.

3.4 Incentive mechanism

The computing power ecosystem services are the primary economic sources for BHP public chain in its initial stage. BHP public chain provides basic services such as computing power on-chain, tracing, transfer, and output distribution for computing power holders. In order to encourage computing power holders to participate in ecosystem construction, all block outputs of BHP network will be divided into consensus incentive and ecological incentive, which will be distributed to computing power providers and BHP holders every day. The distribution proportion shall be adjusted by the community from time to time according to the development of the computing power ecosystem. At the present stage, the distribution proportion of BHP output per day is as follows: 70% as incentives to computing power providers, and 30% as consensus incentives. The revenue of BHP public chain is managed by the BHP Foundation, and the funds are used for technology development of the public chain, and buyback of BHP to supplement ecological incentives.

3.5 Consensus mechanism

The BHP public chain adopts a decentralized governance structure, in which the consensus computing power holders and BHP holders jointly vote to elect X consensus nodes (the total number of consensus nodes is not limited, which will gradually increase with the development of BHP ecosystem) for block verification. The consensus node will receive a 10% consensus award and all transaction fees. 90% of the consensus awards are allocated to BHP holders by number of votes. The BHPs obtained by the consensus node are used for the operation of its BHP network nodes. All other future revenues of the BHP public chain shall be owned by the BHP holders and shall be returned to the BHP holders in the form of dividend or buyback.

3.6 Pledge interest

BHP holders pledge BHP on the public chain, transfer PoS mining power (i.e. right to use) to nodes, and the nodes will replace users to generate revenue through mining and then distribute the revenue to users. The ownership of the BHP is still in the hands of users. The total number of BHP is constant, and the block output is halved at the same time with bitcoin. In order to maintain the stability of the Staking income, the revenue of public chain will be used to buyback BHP as supplementary incentives to ensure the smooth operation of the public chain.

Currently 90% of 30% of BHP's daily block production is used for Staking income. The real yield rateof user Staking is determined by inflation rate, mortgage rate, price change and many other factors.

4 Technology realization

4.1 Computing power routing model

The on-chain in the real world is to establish a digital model through effective confirmation and measurement of the right to use assets and the ownership of assets, and then convert them into programmable digital assets on the chain. We call this process computing power virtualization, that is, computing power assets digitization. The process of each new computing power virtualization is the process of generating a new side chain by slicing the public chain. The real-time delivery, transfer and extraction of computing power in the side chain need a transparent and trustable access link point, for which we call "computing power routing". In fact, the mechanism of computing power routing is the mechanism of computing power on-chain. The delivery process of computing power between producers and users is the switching process of “computing power routing”. The computing power routing model is shown in Figure 4-1 below:

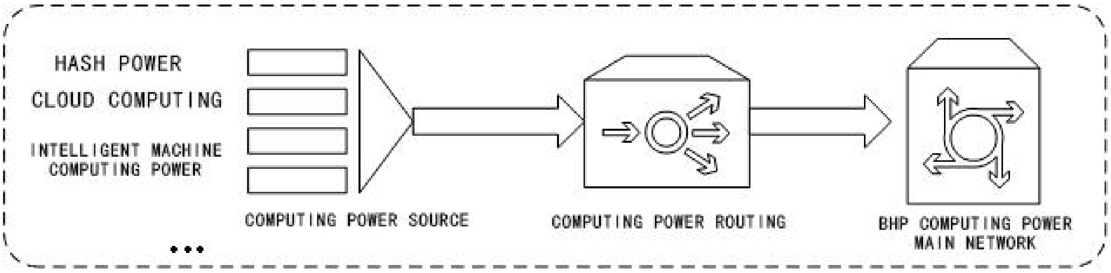
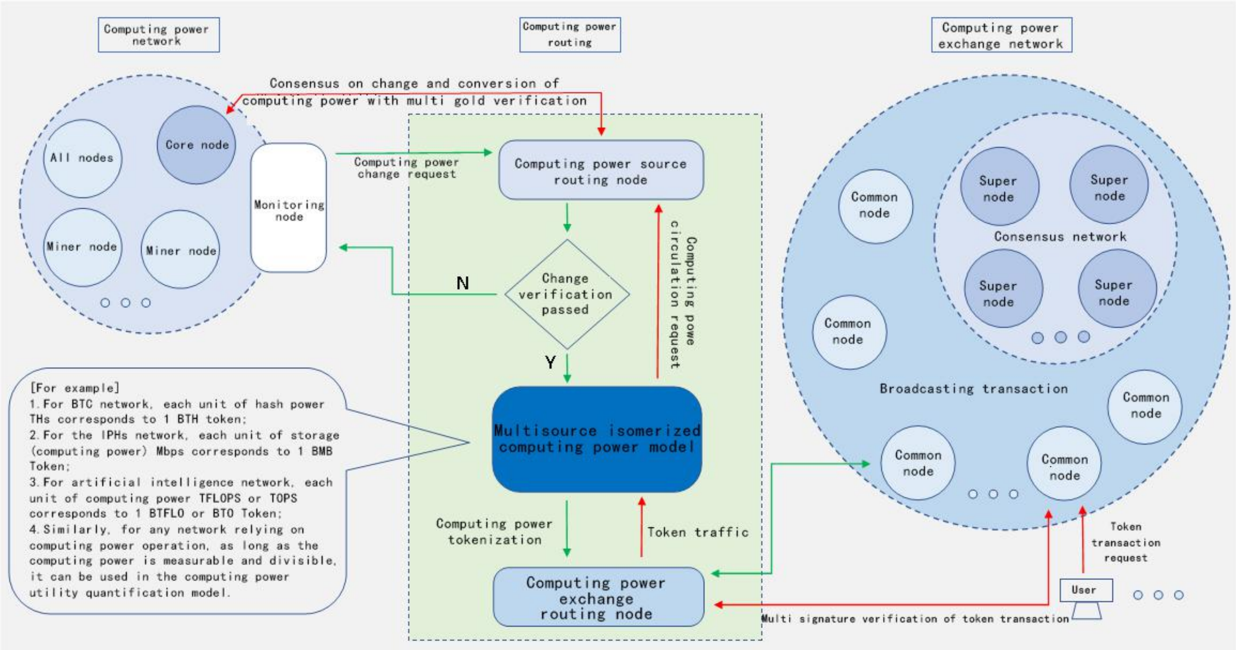


Figure 4-1 Computing power routing model

The computing power source network realizes the digitalization of computing power assets and the circulation of digital assets through the computing power routing network. The circulation of digital assets in the BHP computing power main network synchronizes with the assets in the side chain through the computing power routing network.


Computing power network
Computing power routing
Computing power exchange network
Consensus on change and conversion of computing power with multi gold verification
All nodes
Core node
Miner node
Miner node
Monitoring node
Computing power change request
Computing power source routing node
N
Change verification passed
Y
Computing powe circulation request
Multisource isomerized computing power model
Computing power tokenization
Token traffic
Computing power exchange routing node
Common node
Super node
Super node
Consensus network
Super node
Super node
Common node
Broadcasting transaction
Common node
Common node
Common node
Token transaction request
User
Multi signature verification of token transaction

[For example]
1. For BTC network, each unit of hash power THs corresponds to 1 BTH token;
2. For the IPHs network, each unit of storage (computing power) Mbps corresponds to 1 BMB Token;
3. For artificial intelligence network, each unit of computing power TFLOPS or TOPS corresponds to 1 BTFLO or BTO Token;
4. Similarly, for any network relying on computing power operation, as long as the computing power is measurable and divisible, it can be used in the computing power utility quantification model.

Figure 4-2 Computing power routing network

It can be seen from Figure 4-2 that multisource isomerized computing power model and side chain routing node are the core functions of computing power routing network. There are many sources of computing power, with different functions, for example, CPU resources, storage resources and network bandwidth in cloud computing network, machine vision computing power, AI computing power and genetic engineering computing power in intelligent machine network. As long as these kinds of multisource isomerized computing power are measurable and divisible, they can be verified on BHP computing power network by using multisource isomerized computing power quantification model, so as to complete asset confirmation and transfer of usage right, that is, digital asset circulation on the BHP computing power network.

4.2 Computing power network structure

Computing power network is the multilayer structure of different functions connected by protocol stacks. These protocols define how computing power interaction occurs, how data is routed between layers, how smart contracts work, and how decentralized application driver models work.

Computing power network has 5 layers in total, and basic structure is shown in Figure 4-3:

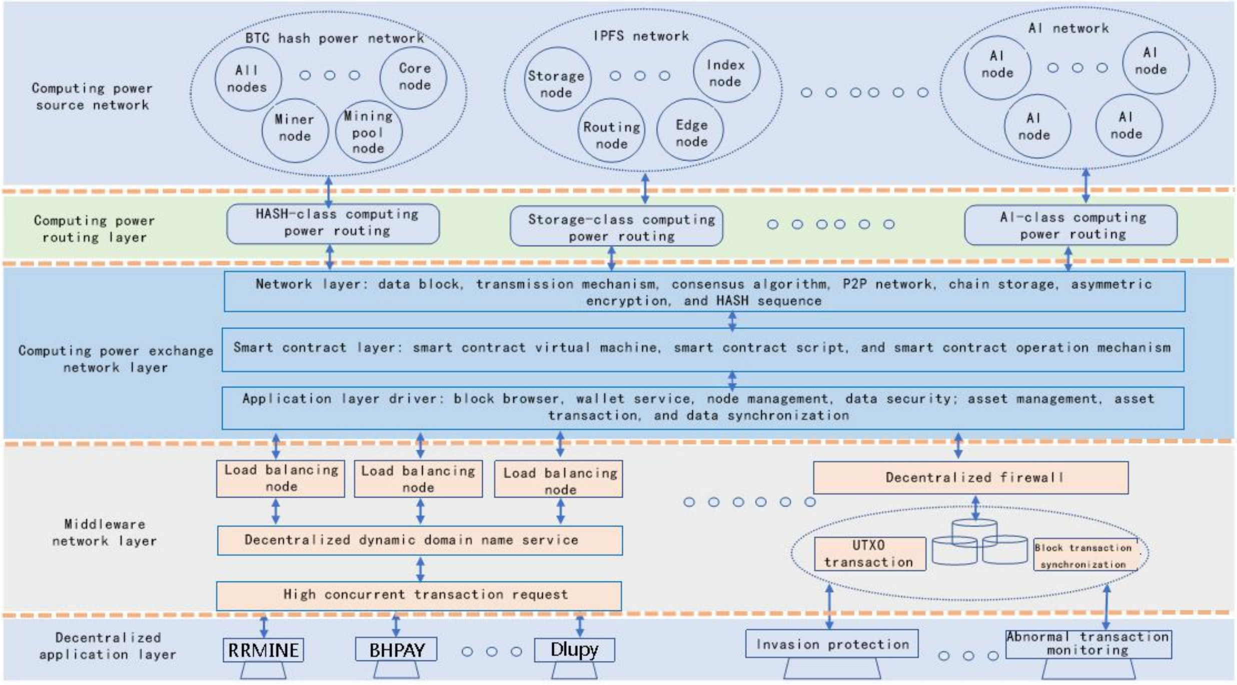
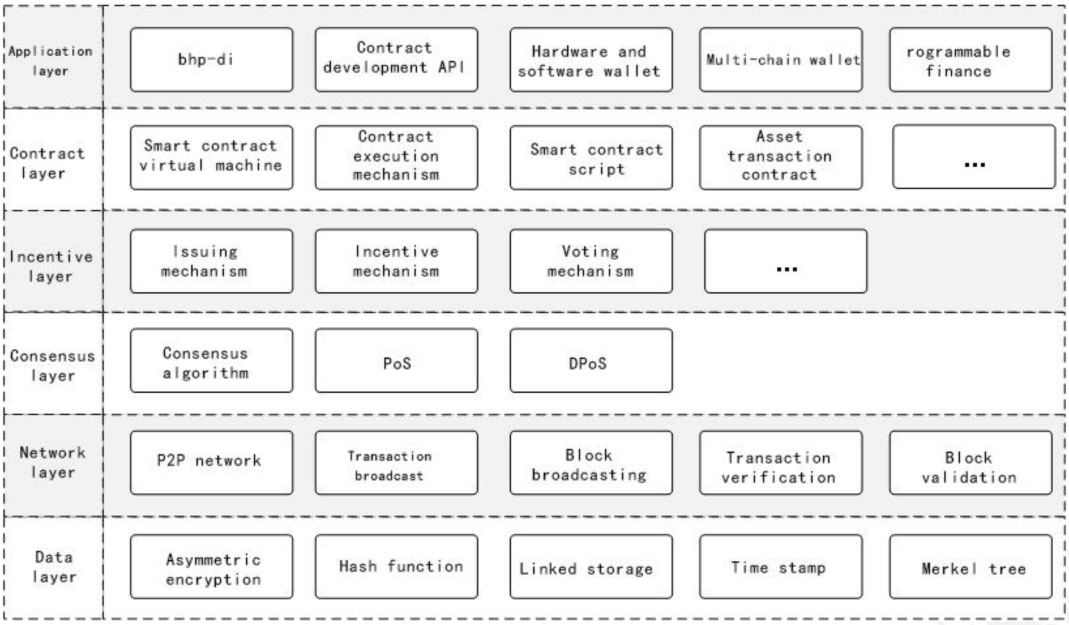

Computing power source network
BTC hash power network
All nodes
Core node
Miner node
Mining pool node
IPFS network
Storage node
Index node
Routing node
Edge node
AI network
AI node
AI node
AI node
AI node
Computing power routing layer
HASH-class computing power routing
Storage-class computing power routing
AI-class computing power routing
Computing power exchange network layer
Network layer: data block, transmission mechanism, consensus algorithm, P2P network, chain storage, asymmetric encryption, and HASH sequence
Smart contract layer: smart contract virtual machine, smart contract script, and smart contract operation mechanism
Application layer driver: block browser, wallet service, node management, data security; asset management, asset transaction, and data synchronization
Middleware network layer
Load balancing node
Load balancing node
Load balancing node
Decentralized dynamic domain name service
High concurrent transaction request
Decentralized firewall
UTXO transaction
Block transaction synchronization
Decentralized application layer
RRMINE
BHPAY
Dlupy
Invasion protection
Abnormal transaction monitoring

Figure 4-3 Computing power network

The computing power source is a network that provides physical computing power. After the computing power in the computing power source is verified by the multisource isomerized computing power quantitative model in the routing layer, the computing power exchange network will convert different computing power assets into digital assets on the blockchain to achieve asset digitalization. The common forms are: asset chain, asset transaction, asset transfer, asset cancellation, etc. The exchange network is responsible for the management of digital assets on the blockchain, including data privacy security, transaction security, asset custody, asset circulation, etc. The decentralized application layer is running on the distributed network, the data information is protected on the blockchain anonymously and safely, and the decentralized operation is carried out through the network nodes. It is an asset circulation protocol, a smart contract or a group of smart contracts executed according to the conditions set on the blockchain.

4.3 Blockchain technology structure

The BHP blockchain technology structure from bottom to up includes the bottom data layer, adopting asymmetric encryption and hash functions which combine public and private keys to ensure that information will not be tampered with, chain storage structure, timestamp, Merkel number and other technologies; the network layer mainly includes P2P network, transaction broadcast and transaction verification mechanism; the most core consensus layer solves the consistency problem of distributed system; the consensus mechanism is the interest proof mechanism PoS; the issuance and incentive mechanisms in the incentive layer are the combination of economics and distributed computing, so that highly decentralized nodes can consciously participate in the system maintenance and construction; the contract layer is the deployed contract script code that smart contracts run the virtual machine, contract execution engine, consensus algorithm; the application layer encapsulates various application scenarios of blockchain, such as user interface, smart contract API, software and hardware wallet, multi-chain wallet, cross-border payment system and other blockchain applications built on the blockchain, and programmable finance and programmable society will also be built on this layer, as shown in Figure 4-4 below:



Application layer	bhp-di	Contract development API	Hardware and software wallet	Multi-chain wallet	rogrammable finance
Contract layer	Smart contract virtual machine	Contract execution mechanism	Smart contract script	Asset transaction contract	...
Incentive layer	Issuing mechanism	Incentive mechanism	Voting mechanism	...	
Consensus layer	Consensus algorithm	PoS	DPoS		
Network layer	P2P network	Transaction broadcast	Block broadcasting	Transaction verification	Block validation
Data layer	Asymmetric encryption	Hash function	Linked storage	Time stamp	Merkel tree

Figure 4-4 BHP blockchain technology structure

4.4 Smart fragmentation network

Block expansion and horizontal expansion can be adopted to improve the throughput of network transactions. The BHP public chain realizes the horizontal expansion of the blockchain with the smart dynamic load balancing autonomous dynamic fragmentation technology. Different transactions can be processed in each fragment at the same time, and the processing performance of the entire network is significantly improved. In each cycle, the system randomly combines the nodes into a fragment, and the nodes within the fragment only verify the respective transactions and broadcast the verification results to the parent blockchain to help the parent blockchain finalize the block. Each node in the smart fragmentation network stores a distributed ledger of the main chain.

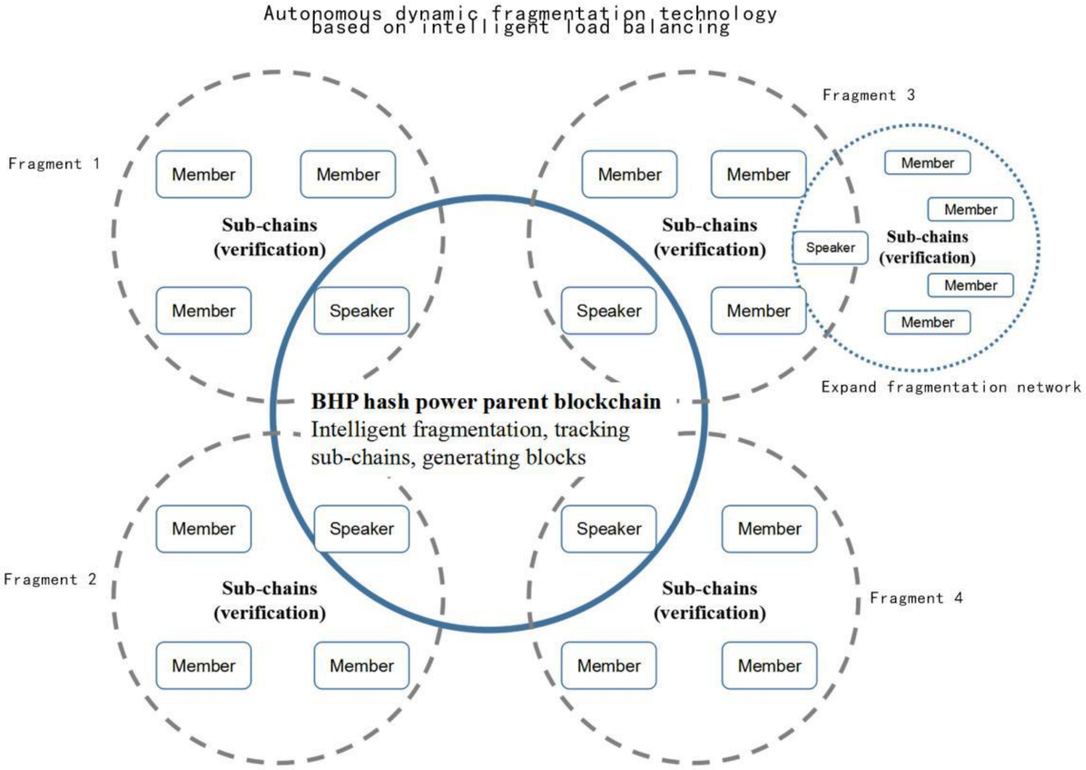

Autonomous dynamic fragmentation technology based on intelligent load balancing
Fragment 1
Member
Member
Sub-chains (verification)
Member
Speaker
Fragment 3
Member
Member
Sub-chains (verification)
Speaker
Member
Member
Member
Speaker
Sub-chains (verification)
Member
Member
Expand fragmentation network
BHP hash power parent blockchain
Intelligent fragmentation, tracking sub-chains, generating blocks
Fragment 2
Member
Speaker
Sub-chains (verification)
Member
Member
Speaker
Member
Sub-chains (verification)
Fragment 4
Member
Member

Figure 4-5 Intelligent fragmentation network

Parent blockchain network	Fragment network
Autonomous dynamic fragmentation with intelligent load balancing	Verify the transaction on the fragmentation
Voting transaction accounting rights (produce block chain)	Confirm parent block chain
Save fragment network information	

In the same cycle, if there are N fragmented networks, each fragment can process N transactions, so there are N2 transactions in total can be processed by the system. Therefore, this proposal is named quadratic fragmentation.

4.5 Introduction to consensus protocol

Due to the high network delay existing in the P2P network, the sequence of transactions received by each node may be inconsistent. Therefore, the blockchain system needs to design a mechanism to make consensus on the sequence of transactions occurring within a certain period of time. This algorithm, aiming at a consensus on the sequence of transactions within a time window, is called "consensus mechanisms".

BHP public chain adopts the consensus mechanism of DPoS (Delegated Proof of Stake), and innovatively introduces the equity certificate of computing power holders. Consensus computing power holders and BHP holders elect N consensus nodes for transaction verification. The Delegated Byzantine Fault Tolerance (DBFT) was adopted in the Consensus Algorithm.

DBFT selects a special accountant (accounting node) in terms of the equity holding proportion, and then the accountants reach a consensus through the Delegated Byzantine Fault Tolerance. DBFT can tolerate any type of errors, and there are multiple special accountants in charge of each block to be finalized and not forked. The accountants in the BHP system refers to the numerous nodes that own super computing power accessed to the BHP network. With the help of DBFT consensus mechanisms, a block is being generated every 5 to 20 seconds, with thousands of TPS transaction throughput volume. After optimization by load balancing network, with the unique state channel mechanism, tens of thousands or even higher TPS can be achieved to support large-scale commercial applications. The general process of the consensus algorithm is shown in the figure below:

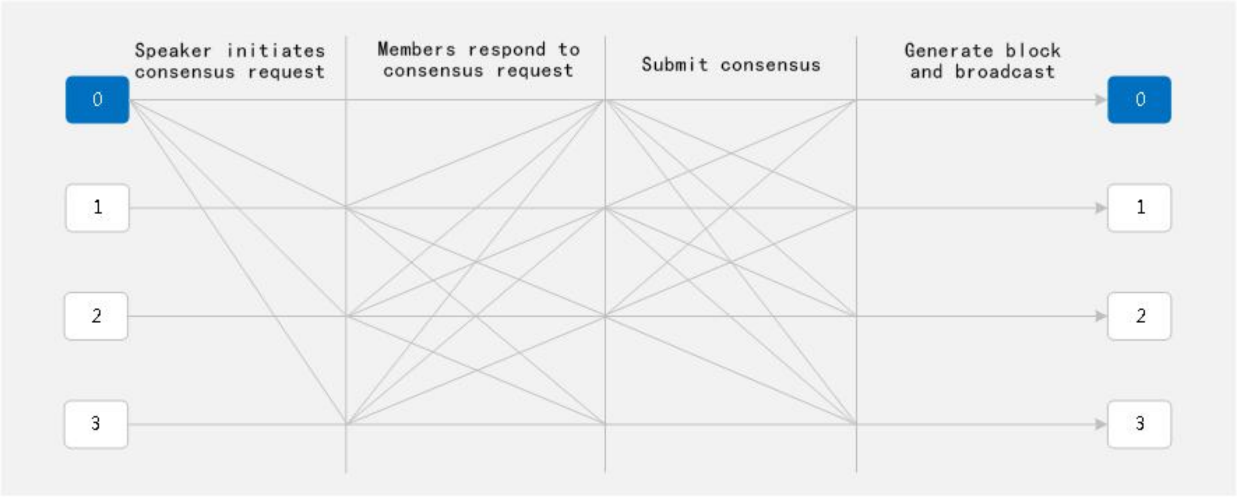

Speaker initiates consensus request
Members respond to consensus request
Submit consensus
Generate block and broadcast
0
1
2
3
0
1
2
3

Figure 4-6 General process of consensus

The node broadcasts transaction in the BHP network. When receiving the transaction, the accounting node opens the consensus view and initiates the proposal broadcast. The member starts to verify the transaction, when the error node participating in the consensus does not exceed (n-1)/3 after t seconds, this round of consensus is successful.

4.6 Blockchain data structure

Block structure is a kind of distributed database with chain storage structure, composed of block head and block body. The HASH value of block head is stored in each block head to link the whole distributed ledger database, as shown in Figure 4-7:

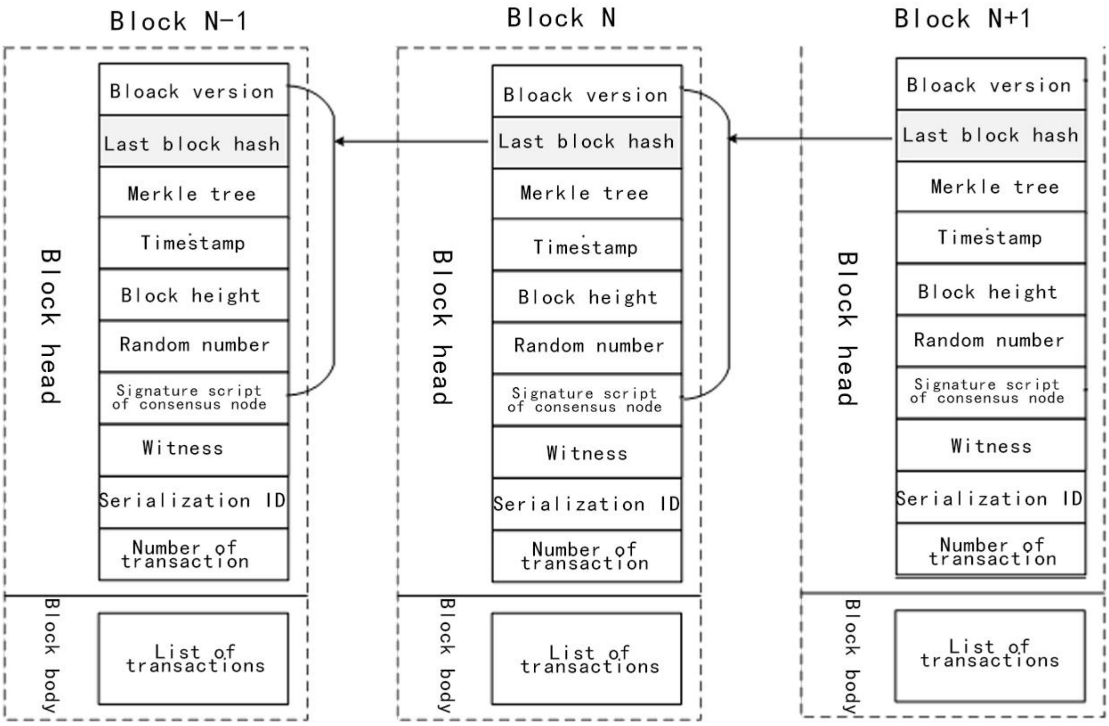


Figure 4-7 Blockchain structure

The block ID is the block hash value. Block hash value is obtained by two SHA256 operations on the first seven data of block head. In normal operation, BHP only has one chain, and each block is added to the blockchain after being confirmed by more than two-thirds of nodes of the consensus node, so the height of each block on the blockchain is unique. Block height must be equal to the previous block height plus 1. Because any information change in a block will cause the block hash value to change, the block hash value is the unique ID of the block. The block height is not affected by the information in the block, slightly low in security, so it cannot be the only identification. The timestamp must be later than the that of the previous one. The time interval between two blocks is about 15 seconds. Consensus node signature script is the hash value of a multi-party signature script. When the script is verified, more than two-thirds of consensus node signatures are required as parameters. The sample script is as follows:

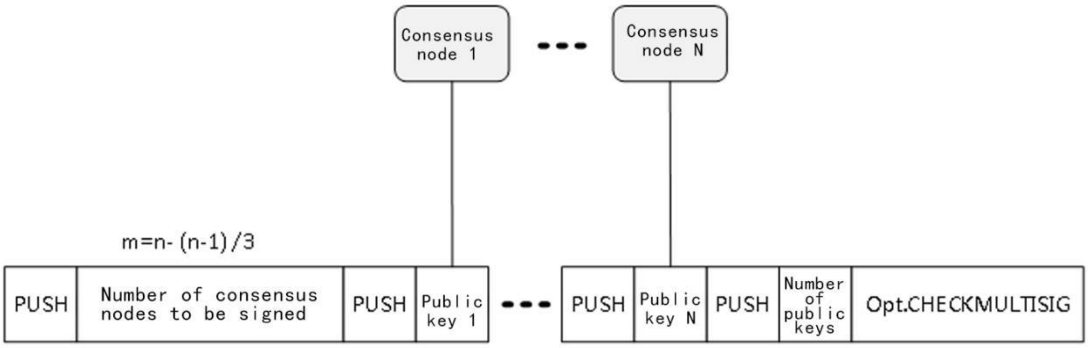


Figure 4-8 Consensus node signature script

Each block will have a consensus node signature script field to lock nodes participating in the next round of consensus. In the previous round of consensus, the speaker node calculates the consensus nodes of next round according to the voting results at that time, and then generates multi-party signature contracts, storing the hash value of the contract script into the consensus node signature script field of the proposal block. If the proposal block finally reaches a consensus and becomes the confirmed block, the consensus verifier of this round is one of the multi signature contract addresses in the last confirmed block. The witness is the validation script for this block, and its structure is execution script plus verification script. The execution script contains the parameters required for validation, and the validation script is the that to be used for specific validation.

4.7 Block transaction model

In the BHP payment system, a block, consisting of a block body and a block head, is generated every 15 seconds. The block body mainly refers to the transactions generated in the current time period. The block head includes the hash value Hr-1 of the previous block, the Merkle Root Hash Merkle TX produced by the current transaction, the timestamp T and the random number Nonce. For the hash value included in the block head points to the previous block, a "Chain" structure is made by the block.

The BHP blockchain accounting book has the same principle with the BTC. BHP replaces traditional accounts with a mode of unexpended transaction output (UXTO).

There are two rules for UXTO system to comply with:

(1) Except for mining transactions, all sources of funds must come from the UXTO of one or several previous transactions;

(2) The total input of any transaction must be equal to the total output, and both sides of the equation have to be equal. (Generally, if the output is less than the input, and the difference belonging to PoS miners is the transfer fee.)

The biggest benefit of the UXTO model is the ability to faithfully record transactions. Our real world flows with time, and transactions occur one by one. The blockchain system faithfully records what happened in the world, cannot be rolled back, and cannot be deleted.

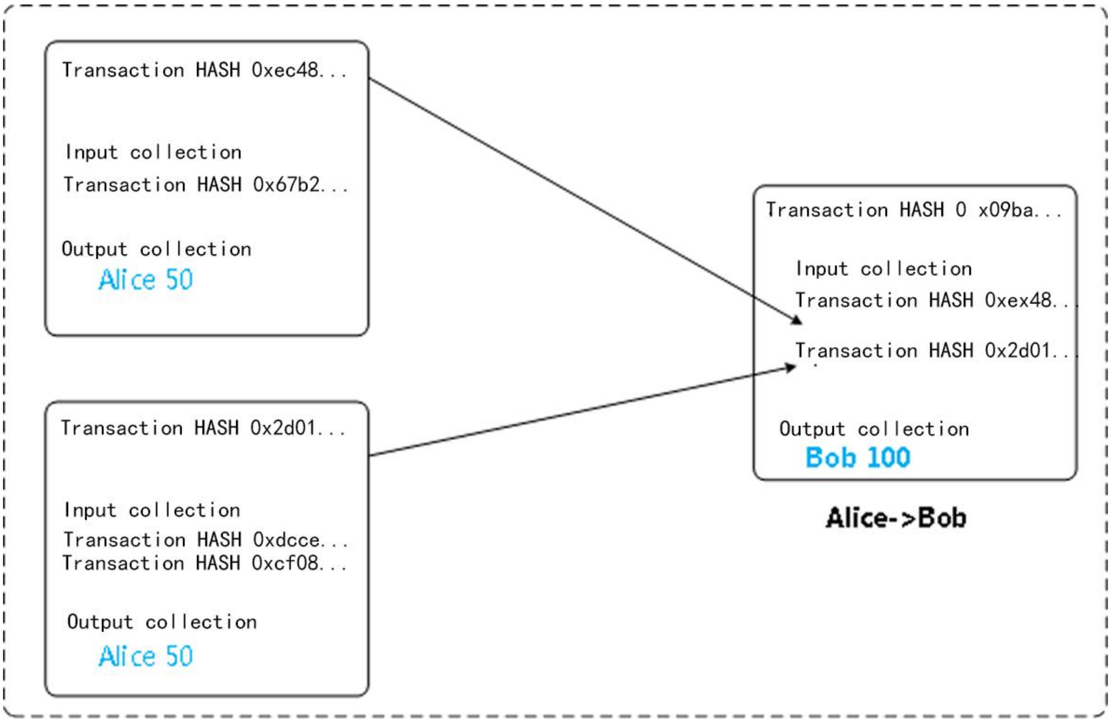

Transaction HASH 0xec48...
Input collection
Transaction HASH 0x67b2...
Output collection
Alice 50
Transaction HASH 0x2d01...
Input collection
Transaction HASH 0xdcce...
Transaction HASH 0xcf08...
Output collection
Alice 50
Transaction HASH 0 x09ba...
Input collection
Transaction HASH 0xex48...
Transaction HASH 0x2d01...
Output collection
Bob 100
Alice->Bob

Figure 4-9 UTXO transaction model

4.8 Smart contract system

Smart contract, of which the concept was first proposed by Nick Szabo in 1994, is a computer protocol aims at propagation, verification or implementation of contracts in an informational way. It allows credible transactions which are traceable and irreversible to go on when there is no third party. BHP Contract, as the independent smart contract system for BHP, is a smart contract execution environment that is microcore and not related to platform. It provides a set of instructions including stack operations, procedure control, logical calculations, arithmetic calculations, cryptographic calculations, string operations and array operations, while only two computing stacks are provided on the aspect of hardware. However, blockchain developers are allowed to create their own virtual hardware, as well as open to smart contracts in the form of interfaces, which makes the contracts obtain platform-related data, persistent storage and access to the Internet at runtime during operation. Although this may bring about some uncertainties about the contract, the blockchain developer can eliminate this uncertainty by properly writing virtual hardware. However, due to short in compiler and development environment to support AVM, it is quite difficult to develop smart contracts based on AVM, and developers have to use a syntax similar to assembler to write contracts, which requires high technical ability.

The BHP smart contract system architecture is shown in Figure 4-10 below:

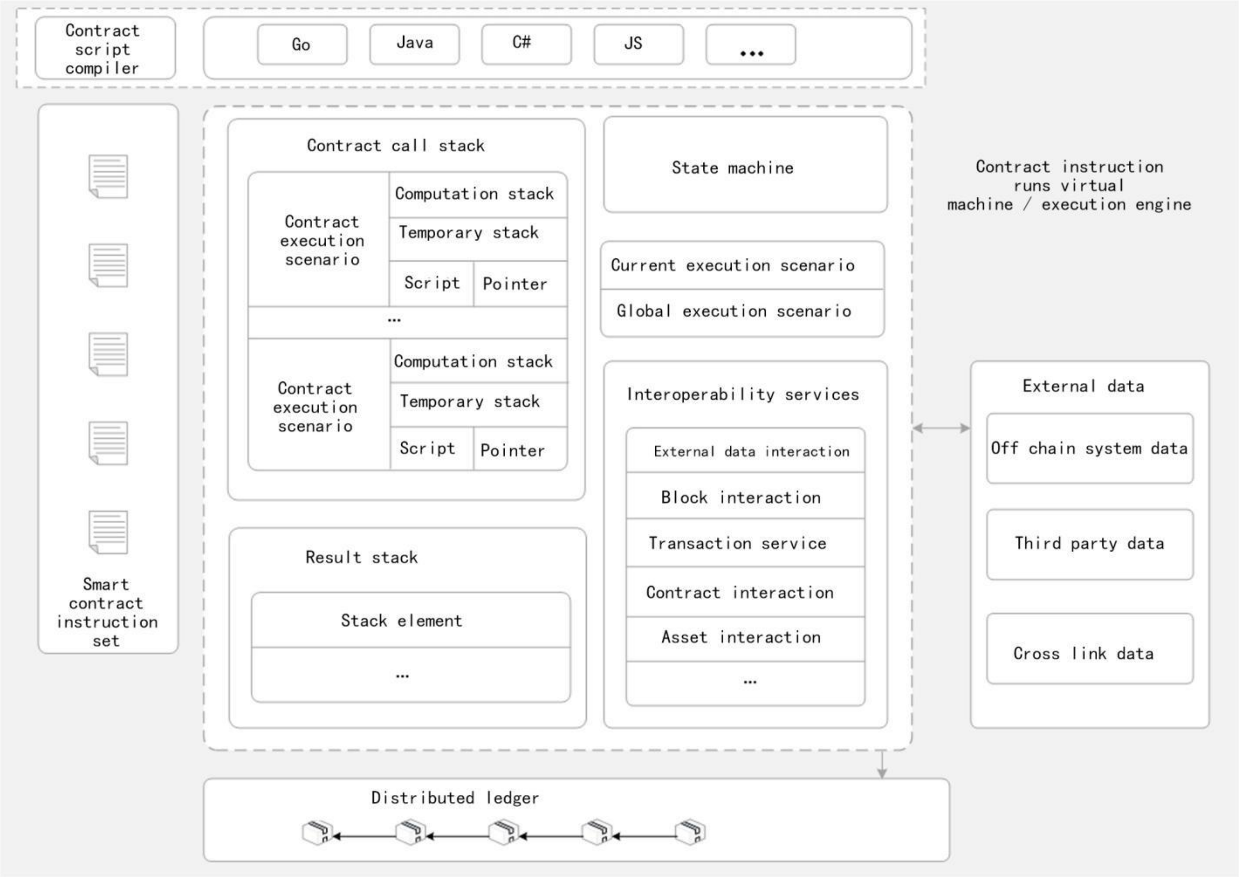


Figure 4-10 smart contract system structure

BHP smart contracts run on the BHP VM with high certainty, high concurrency and high scalability. According to the designed goal of BHP computing power block chain, the realizable smart contracts based on BHP Contract include: deposit interest contract, credit mortgage contract, commercial payment contract, transfer transaction contract, asset investment contract, etc. In the future, with the smart contract protocol continuously upgrading, BHP computing power block chain will support users to develop more smart contracts.

4.9 Cross-chain exchange protocol

BHP, a distributed payment system that supports multi-side chain association, supports the architecture of ‘computing power parent blockchain+ high-performance multi-side chain’, achieving efficient exchange among multiple assets. The cross-chain interoperability protocol of BHP consists of two parts:

‘Cross-Chain Asset Exchange Protocol’ and ‘Cross-Chain Distributed Transaction Protocol’.

(1) Multi-chain atomic asset exchange protocol

With the extension of BHP on the double-chain atomic asset exchange protocol, it allows multiple participants to exchange assets across different blockchains and ensures the success or failure of all steps in the entire transaction process. To achieve this function, a contract account is created for each participant with the functions of the smart contracts. The individual digital assets exchange, across two completely unrelated blockchains, can be achieved.

Multi-chain atomic asset exchange protocols do not add complex communication mechanisms among chains, but they can guarantee that such exchanges are atomic and credible, without the situation that equity is transferred but creditor's rights is not transferred.

(2) Cross-chain distributed transaction protocol

Cross-chain distributed transactions mean that multiple steps of a transaction are executed across different blockchains while keeping consistency. This is an extension towards cross-chain asset exchange, extending the behavior of asset exchange to arbitrary behavior. BHP will use cross-chain smart contracts. A smart contract can execute different parts on multiple different blockchains, either all executed or all returned to the pre-execution state.

4.10 Oracle machine technology

The oracle machine, as well as a chain code, is a smart contract deployed on the chain. Oracle machine technology needs to be used when external data is required on the blockchain. The whole workflow of the oracle machine is as follows: the oracle machine firstly obtains the required data from the trusted party, then transfers to the address on the specific blockchain with the price information written into the transaction remarks, so that only with the specific area’s transaction record viewed, can the required data be obtained. Since the blockchain automatically stores the blocks containing the transactions, only with the local transaction record viewed, can the required data be obtained. It not only ensures the access efficiency, but also ensures the consistency of the data. In general, it is that the oracle machine (third party) pushes the data to the blockchain, rather than the smart contracts actively pull data from third parties.

The user trusted computing power assets are on-chained through the oracle machine technology, which can provide reliable external data for the smart contracts of PoS revenue, solve trust problems and promote consensus.

4.11 Hash power payment

At present, the slow transfer speed and high transfer fee of BTC restrict the BTC payment to be widely applied in business. The BTC payment principle, which is based on BHP network proposed in this paper, refers to carrying out a large number of transactions out of the BTC blockchain, aiming to realize the rapid payment of BTC with very low charges and promoting the commercial application of BTC payment.

Hash Witness: A and B respectively pre-storee the corresponding BTCs into the BHP network, with the witness by the credit of the 21 super hash power nodes of BHP, to obtain the BTC payment pass of the BHP network.

Hash Consensus: when A transfers to B, A signs with private key, and broadcasts transaction in BHP network; after the consensus confirmation of the 21 super nodes of BHP, the transfer transaction is recorded in the BHP network. When withdrawing, the final accounting book on the BHP chain is submitted to the BTC network.

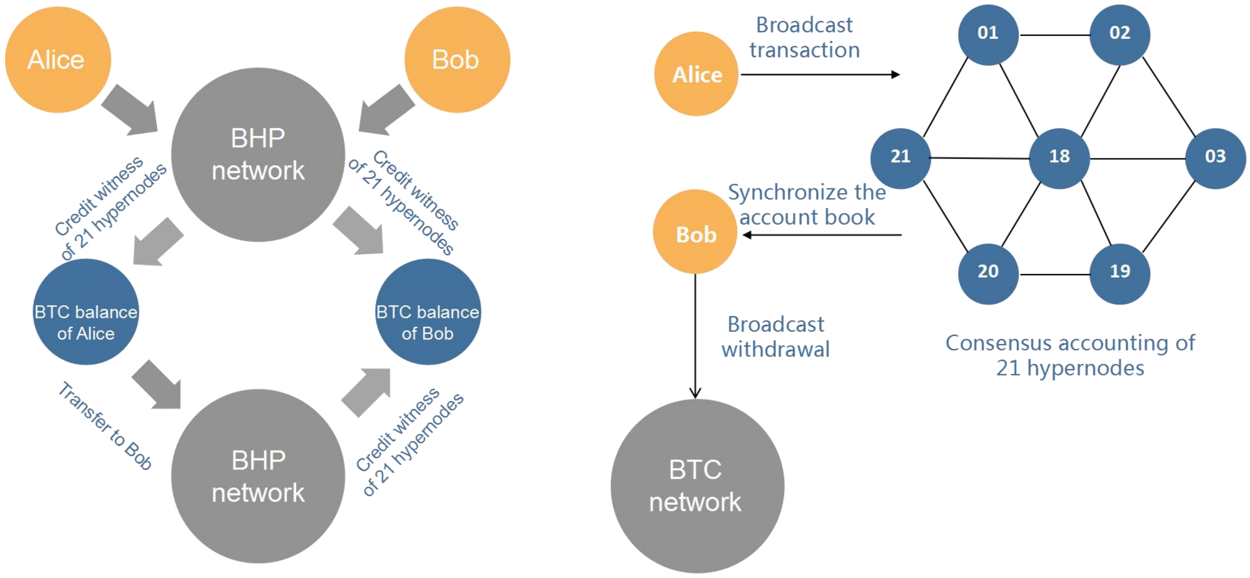

Alice
Bob
BHP network
Credit witness of 21 hypernodes
Credit witness of 21 hypernodes
BTC balance of Alice
BTC balance of Bob
Transfer to Bob
BHP network
Credit witness of 21 hypernodes
Alice
Broadcast transaction
01
02
21
18
03
20
19
Synchronize the account book
Bob
Broadcast withdrawal
Consensus accounting of 21 hypernodes
BTC network

Figure 4-11 Bitcoin hash power payments in a BHP Network

Payment characteristics of BHP network: (1) fast transaction: the transfer transaction is completed immediately through the payment direct mode of the BHP network; (2) the transaction is on the chain, with 21 super hash power nodes consensus, all transactions are recorded on the chain; (3) offline payment: B can be offline when A makes transaction with B; (4) payment channel: any two or more transactions can be performed at the same time in the BHP network, not restricted by a single payment channel; (5) large-amount payment, both sides of the transaction carry out direct transfers, without intermediate nodes, and are not restricted by the network status and insufficient funds of the intermediate nodes;(6)Payment and application scenarios are moderately isolated. BHP adopts a public/private chain-based value registration and transfer model, which can be used among systems of multiple business entity without exposing personal information to all operators.

5 Development program

BHP will develop in the following chronological order:

Table5-1: BHP development program

Time	**PROGRAM**
05/2018	Launched the BHP project
08/2018	Formed the project team
03/2019	Constructed the underlying architecture
06/2019	Published the White Book
08/2019	Launched Blockchain browser and wallet, and began to support the BTC hash power on-chain
12/2019	To open access to multiple countries/territories, and support the on-chain of all kinds of isomerism computing power as well as the clearing and settlement of isomerism computing power on chain
06/2020	To initiate the access of AI hardware computing power and begin to support digital asset banking services
2020	To launch global commercial application promotion, and begin to build a computing power ecosystem

6 Risk tips and disclaimer

- As a new investment mode, digital asset investment has various risks. Potential investors should carefully evaluate the investment risks and their own risk tolerance.
- This document is used for guiding the progress of the BHP project, only with the function to circulate the information, instead of constituting a recommendation to buy or sell BHP Coin. The above information or analysis does not constitute an investment decision. This document does not constitute any investment advice, investment intention or instructing investment.
- This document neither constitute nor is construed as any act purchase and sale actions, or any invitation to buy or sell any form of securities, nor is it a contract or commitment in any form.
- Relevant intent users clearly understand the risks of the BHP project. The investor participating in the investment means that he or she has learnt and accepted the risk of the project and is willing to personally bear all the corresponding results or consequences.
- The project team is not liable for any loss of assets caused by participating in the BHP project.

➢ Project risk:

➢ Policy risk: because blockchain technology is in its early stag, there are uncertainties for the regulatory policies of blockchain projects in various countries, as well as changes in operational entities and operational management for the project;

➢ Volatility risk: investors should have great psychological endurance, for the digital assets issued by BHP are not legal currency and the price has high fluctuation;

➢ Technology risk: for the developing blockchain technology, technical loopholes and hacking attacks cannot be absolutely avoided in project operation;

- Team risk: the core personnel may resign due to stress, physical and personal factors in the development of BHP.