A Distributed Payment System Based on Bitcoin Hash Power Credit
(BHP Payment System)

Version：V1.0

2018.12

Github：https://github.com/BhpAlpha

Outline

Abstract

A distributed payment system based on Bitcoin hash power credit (Abbreviated as BHP payment system) is proposed in this paper. The system makes Bitcoin hash power as digital asset value exchanging medium with a broad consensus. By deploying and executing smart contracts on the blockchain of hash power (BHP), online payments can be initiated directly by one party and paid to the other. The payment process does not require any financial institutions, and supports tens of thousands of high concurrent payments per second.

The BHP payment system consists of 21 hyper nodes scattered around the world. Each hyper node permanently provides a Bitcoin mining pool with a certain amount of hash power. While these nodes provide mining hash power for the Bitcoin network, the BTC produced by these nodes is automatically stored in the BHP network, which provides a complete and real Bitcoin hash power assets credit guarantee for the generation of each block of the BHP network. Each node is not only the provider of Bitcoin network hash power, but also the consensus witness of each payment transaction of BHP. By anchoring the value of each block in BHP system and the value of BTC, the establishment of the maximum consensus of decentralized underlying hash power credit can be achieved.

BHP Coin (abbreviated as BHP) is the native token in the BHP payment system. It is a special type of ecological passport for hash power providers, package transactions and network participants in the system. It innovatively

uses the proof of power (abbreviated as PoP) mining mechanism to encourage the miners of Bitcoin and payers to participate in the whole ecosystem and it generated according to the expected release curve distribution.

Key words：Bitcoin hash power, distributed payment system, BHP hash power public chain, BHP coin, Proof of Power

1 Summary

The medium of payment and transaction that promotes commodity trading usually needs money as a general equivalent. In human history, general equivalents have experienced a long process of credit consensus from natural goods such as shells and copper coins to currency endorsed by natural physical credit of precious metals such as silver and gold, and then to paper money endorsed by national credit. Strong credit is a necessary condition for money to become a general equivalent. It can be physical credit such as gold, or national credit. However, gold is not easy to use and carry, difficult to pay, only as a value store. Inflation, currency devaluation, wealth shrinkage and even economic collapse caused by currency overruns have proved that national credit is not always reliable.

Bitcoin [1], as a new type of digital electronic currency, puts currency denationalization on the agenda of practice from the theoretical stage. Bitcoin network relies on P2P distributed network, asymmetric elliptic curve encryption algorithm [2] [3], Proof of Work [4] (PoW) consensus mechanism and other technical means, and innovatively introduces economic incentive and game mechanism, forming a perfect system of logical self-consistent decentralization, which has been on line for nearly 10 years and is still running safely.

The powerful hash power behind Bitcoin guarantees the consistency and unalterability of Bitcoin account book, guarantees the unalterability of Bitcoin issuing mechanism, creates a new credit different from gold physical credit, and lays the basic credit foundation for the free payment attribute of money. But

the inefficiency of Bitcoin payment, the high cost of transfer and the high maintenance of the system [5] make it difficult for Bitcoin to achieve a fast and convenient payment function as a currency.

This paper is focusing on digitalizing global bitcoin hash power assets by using open source block chains and digital identity technology. With the help of point-to-point distributed network technology, asymmetric elliptic curve encryption technology, secure hashing algorithm and Byzantine fault-tolerant consensus mechanism, this paper provides a distributed payment system based on bitcoin hash power credit guarantee for both parties using smart contracts, expecting to build a new convenient and efficient decentralized payment system without third party guarantee.

2 BHP Payment System Architecture

The core of BHP payment system is the BHP public chain, whose consensus basis is entirely derived from the Bitcoin hash power consensus, so behind each BHP pass is a direct binding to the Bitcoin hash power and mining field. Each node in the payment system based on BHP is a virtual pit node of bitcoin. Essentially, BHP hash power public chain is a de-centralized public chain with mutual trust based on Bitcoin hash power as credit endorsement.

With the underlying credit support of BHP payment system, such as digital asset management, e-commerce payment, wallet and exchange, derivative finance and other practical applications, all kinds of ecological applications can be established by issuing their own passes based on the main chain standard protocol BRC2.0.

BHP uses a layered model to build a BHP hash power chain, as shown in Figure 1.

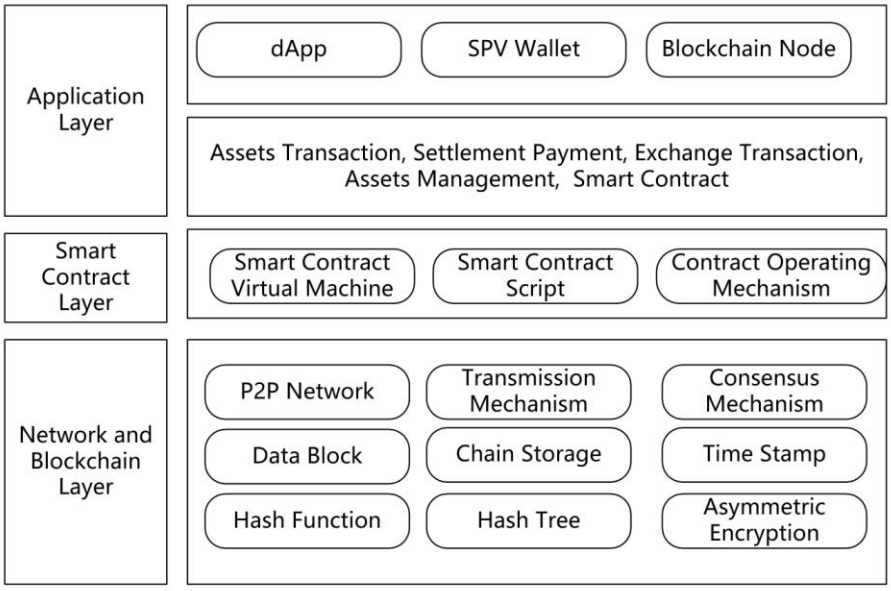

Figure 1 Hierarchical structure of BHP payment system

Application Layer: The basic application functions of BHP include smart contract execution and various services such as assets management and assets trading. Meanwhile, it provides various forms of access systems such as mobile and PC terminals.

Smart Contract Layer: Smart Contract Layer of BHP can build user's account systems and support multi-currency and multi-account binding. It ensures the security of contracts by security mechanism which can shield contract details in application layer and transfer codes in contract transport layer to underlying data to be executed by the smart contract virtual machine.

Block Chain Layer: It is the underlying blockchain layer of BHP. In this layer, all the data of trades will be packaged into the longest chain of BHP which is a public chain that can be accessed without permission.

BHP is an independent public chain. Subsequent BHP will build a side chain protocol and use BHP as a bridge to communicate multiple blockchains. The BHP main chain can realize convenient technical upgrades and system iterations without affecting the operation of each side chain.

3 Key Technology and Implementation

3.1 Encryption Algorithm

Blockchain of Hash Power uses the same public key encryption and digital signature technology as Bitcoin - - elliptic curve cryptography algorithm[6]. Koblitz Secp256k1 elliptic curve equation[6] is :

$y^2=x^3+ax+b$

Curve field parameters are specified by the unit T= (p, a, b, G, n, h).

The finite field Fp of elliptic curve is defined by:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F = $2^{256}-2^{32}-2^9-2^8-2^7-2^6-2^4-1$

The elliptic curve over Fp is defined by:

a =00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b =00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

The base point G in compressed form is:

G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

and in uncompressed form is:

G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Finally the order n of G and cofactor are:

n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

h = 01

3.2 Public Key and Address

The wallet is used to store BHP accounts and assets information in the accounts. The BHP wallet is a database file with the suffix of .json or .db3. This file is very important and requires a secure backup. Once a wallet file or wallet password is lost, it will result in the loss of digital assets. BHP wallet structure:

Address: It is like a bank account or bank card number, used to receive assets when trading.

Private key: A 256-bit random number, kept by the user and not publicly available, is the proof of the user account usage rights and ownership of the assets in the account.

Public key: Each private key has a matching public key. The public key is generated by the product of the private key and the Koblitz curve secp256k1. The public key and address generation code is as follows:

```
var publicKey = Secp256k1.G.Multiply(privateKey); //public key
var pubKeyHash = Hash160.Hash (publicKey.EncodePoint(compressed)); //pubKeyHash
byte[] addressBytes = new byte[pubKeyHash.Length + 1];
Buffer.BlockCopy(pubKeyHash, 0, addressBytes, 1, pubKeyHash.Length);
```

byte[] hash = SHA256.DoubleHash(addressBytes); //double SHA256

var address = Base58.EncodeWithCheckSum(addressBytes); //address

3.3 Distributed Network

The BHP payment system uses a distributed network architecture as shown in Figure 2. The network is built on the Akka concurrency framework based on the Actor model[7].

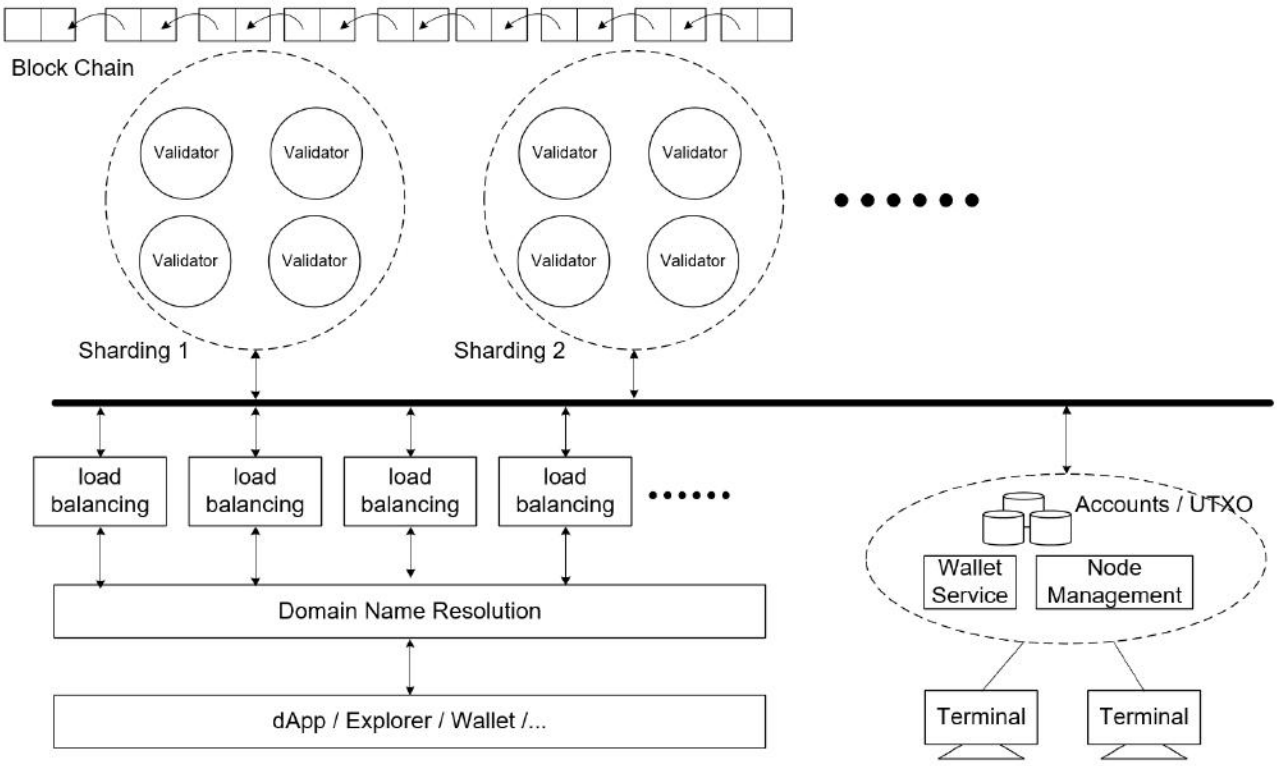

Figure 2 BHP payment system network architecture

Actors interact by sending messages to each other. The thread that executes the task is not passed to the recipient through the message, and an Actor entity can continue to run other tasks without being blocked after the message is sent. The Actor model can do more work in the same amount of

time. Actor processes messages in a sequential manner, processing one message at a time, and the sender and receiver of the message can run independently without interference. This mode of operation avoids the destruction of object encapsulation by concurrent multiple threads in traditional multi-threaded programming.

Actor model features:

(1)The execution program is decoupled by means of signaling, thus maintaining the encapsulation of the object. (the method call passes the execution environment, but the message delivery does not do this)

(2)The internal state of an Actor can only be changed by passing a message, and only one message can be processed at the same time, which eliminates the problem caused by thread contention in traditional programming.

(3)The sender of the message will not be blocked. Millions of Actors can be efficiently arranged on multiple threads. This gives full play to the potential of modern CPU. Task delegation through messages is a common mode of operation in the Actor model.

3.3.1 Network Node

The BHP payment system uses a peer-to-peer (P2P) network structure and uses TCP protocol for communication. There are two types of nodes in the network, namely ordinary nodes and accounting nodes. Ordinary nodes can broadcast, receive, and forward transactions, synchronize blocks, etc., while the accounting nodes participate in distributed consensus and create

blocks. The accounting node is the core role of the BHP blockchain, storing complete historical data and listening to broadcast transactions. The accounting nodes in the BHP payment system are distributed among many mine nodes with super hash powers around the world.

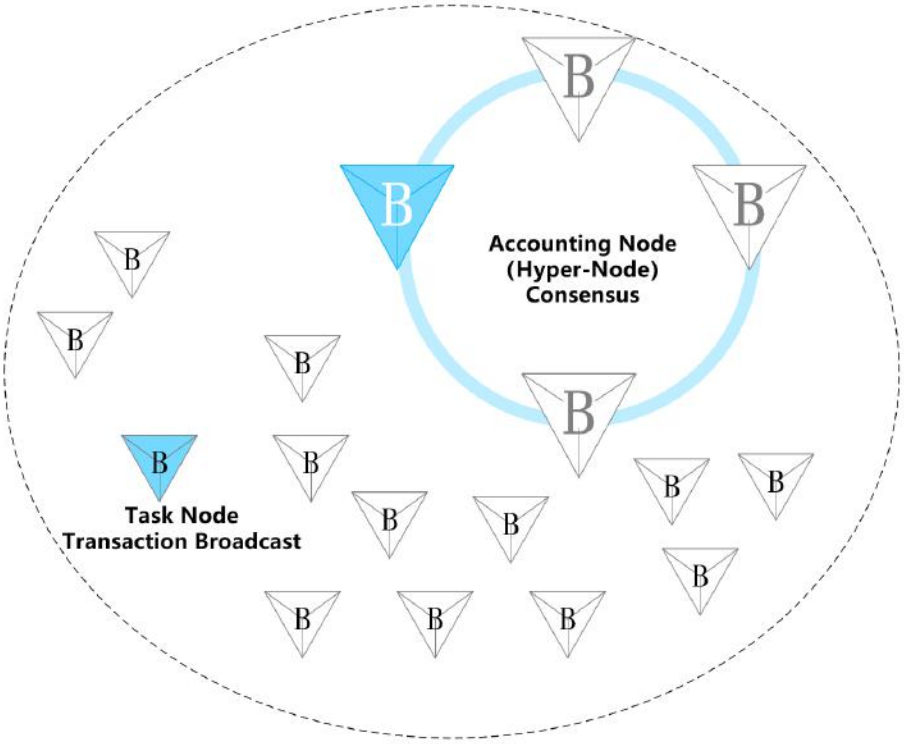

Figure 3 Network node

Ordinary users run light nodes or just access as clients. They can access the BHP network through a SPV(Simplified Payment Verification, SPV) wallet client, block browser or mobile App to synchronize and save their own data, manage their own wallets, and conduct financial transactions in digital currencies.

3.3.2 Dynamic Sharding

Block expansion and horizontal expansion can be adopted to increase network transactions throughput. The BHP payment system uses the

autonomous dynamic sharding technology based on intelligent load balancing to realize the horizontal expansion of the blockchain. Each shard can handle different transactions at the same time, and the processing performance of the whole network has been improved linearly.

In each cycle, the system randomly divides nodes into one shard, the intra node only validates respective transaction and broadcasts the verification results to the main chain to help the main chain finalize the block.

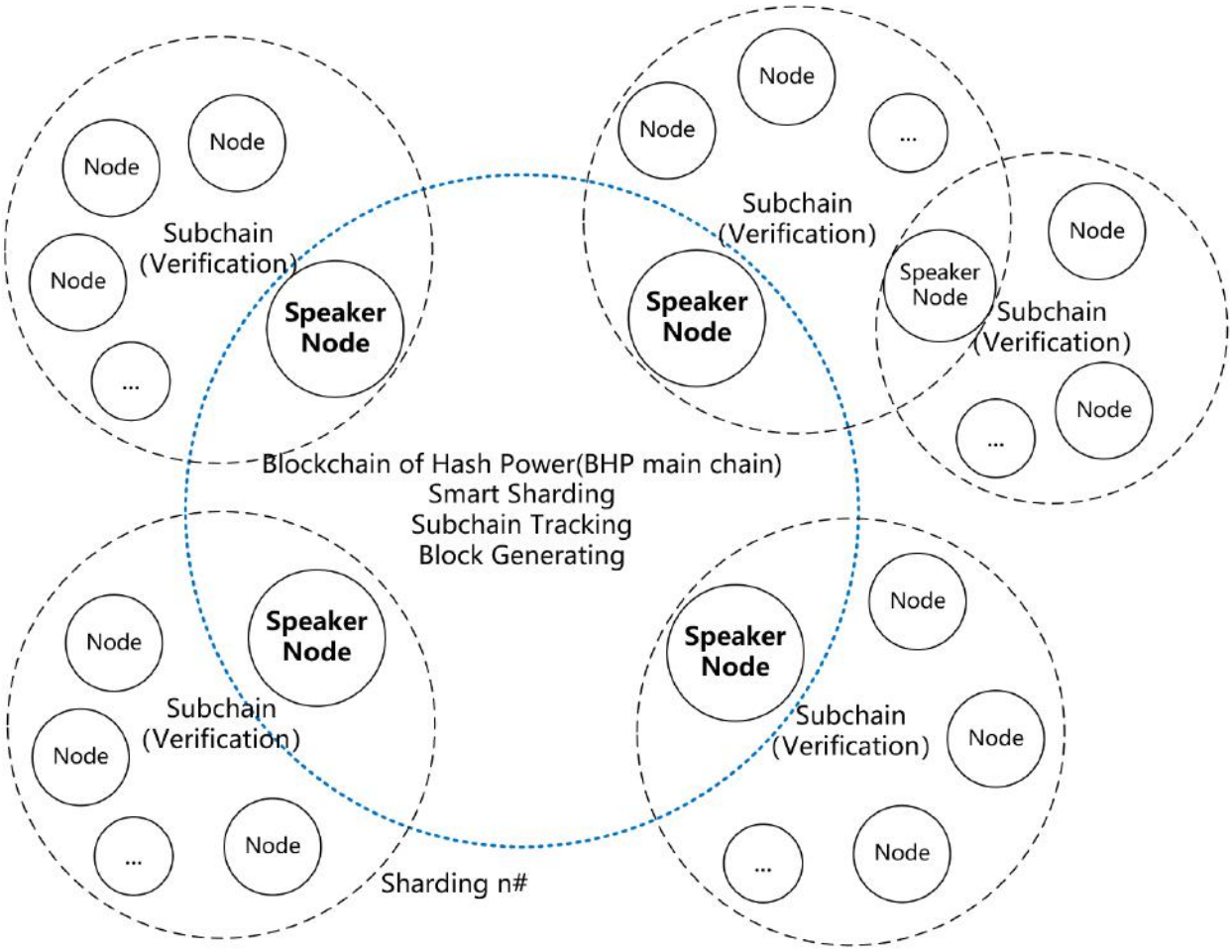

Figure 4 Dynamic sharding technology

Main chain network	sharding network
Autonomous dynamic sharding	Verifying transactions

technology based on intelligent load balancing	on fragmentation
Election transaction billing rights (generating blocks)	Identify block of main chain
Save sharding network information	

In the same cycle, assuming there are N sharding networks, each shard can handle N transactions, so the system can handle N^2 transactions altogether. So this proposal is called quadratic segmentation.

3.4 Consensus Mechanism

The core of the blockchain technology is how to reach a distributed consensus, and how each node agrees on all the transactions happening in the network. These consensuses include elements such as the content, validity and time sequence of the transaction. BHP payment system achieves a distributed consensus on the content and effectiveness of transactions through digital signatures.

Due to the high network delay in P2P networks, the order of transactions received by each node may be inconsistent. Therefore, the blockchain system needs to design a mechanism to recognize the order of transactions occurring in a certain time. This algorithm of consensus on the order of transactions in a time window is called "consensus mechanism".

The consensus mechanism of BHP no longer adopts the traditional proof of work mechanism (PoW) , but proposes a new consensus mechanism PoP

based on hash power. And with the combination of PoS (Proof of Stake) which suits the future developing trending, the PoP (Proof of Power) + PoS hybrid consensus mechanism is proposed by BHP. Continuous hash power is a key component of BHP's infrastructure. The BHP issued by BHP has the respective hash power, which applies PoW mechanism to complete the bottom mining work and obtain Bitcoin, Ethereum, or other valuable mainstream digital currency. The code library designed specifically for BHP transactions relies on the PoP mechanism to ensure high efficiency and low cost in transaction. Especially with the increasing flow of cross-border transactions, this mode will be particularly suitable for cross-border payment scenarios.

（1）Delegated Byzantine Fault Tolerance(DBFT).

Delegated Byzantine Fault Tolerance (delegated BFT) can select the special bookkeeper (accounting node) based on the proportion of ownership, and then the bookkeeper achieves consensus with each other through DBFT. DBFT can tolerate any type of error, and a special bookkeeper makes each block final and not bifurcated. The bookkeeper in BHP is the large number of mines with hyper power and access to the BHP network.

In the DBFT consensus mechanism, taking about 15 to 20 seconds to generate a block, the transaction throughput is measured up to about 1000 TPS. After optimization by the load balancing network, tens of thousands or even higher TPS can be achieved with the unique state channel mechanism, which can support large-scale commercial applications.

（2）Definition in consensus mechanism

t: The amount of time allocated for block generation, measured in seconds. The current t=15 sec, means it will generate a block about every 15 seconds. This value can be used to roughly approximate the duration of a single view iteration as the consensus activity and communication events are fast relative to this time constant.

n: The number of active Consensus Nodes.

h: The number of blocks on the block chain, which is the height of blocks.

i: Consensus Node index.

f: According to this formula, we can see that the minimum number of nodes participating in consensus is n>=4.

s: The safe consensus threshold. Below this threshold, the network is exposed to fault. s=(n-1)/f.

v: The data sets used from the beginning to the end by a consensus is called view. The number of each view is v. At the first round of consensus, v=0, and v is increasing from then on.

k: The index of the view “v”. A consensus activity can require multiple rounds. On consensus failure, “k” is incremented and a new round of consensus begins.

p: Every round of consensus requires a node to serve as the speaker p, while the other nodes are delegates. Speaker p is responsible for sending a new block proposal to the system. P takes turns between consensus nodes to prevent single nodes from being the leader in the system. The calculation formula: p = (h - k) mod n.

（3）Fault tolerance regulation of consensus algorithm

A consensus delegate has to reach a consensus on a transaction before it can be packaged into a block. When the block generation time comes, it will be written on the block chain.

A dishonest consensus node cannot persuade honest consensus nodes with fail transactions.

The delegates who participate in the consensus must be in the same state (h, k), and only when all the delegates' block heights are the same with consensus index can the consensus be reached.

（4）General procedures of consensus algorithm

① A node broadcasts transaction data to the entire network, attached with the sender signature;

② All accounting nodes monitors transaction data broadcasting independently and stores the data in its memory respectively; Consensus node sends a transaction to the whole network, using the sender's signature. Then the first view "v" will be initialized and the speaker will be confirmed.

③ After the time t, the speaker broadcasts proposals, including block height "h", consensus view number "v", speaker number "p" and block data "block", etc.

④ After receiving the proposal, the delegates "i" will verify the transaction

data and send the proposal reply, including the block height “h”, the consensus view number “v”, the delegate number “i”, the block data “block” and so on.

⑤ When any node receives at least n-f consensus results, consensus is reached and a complete block will be issued.

⑥ Any node will remove the transaction from memory after receiving the entire block and start the next round of consensus then.

（5）Transaction verification process

①Whether the data format of the transaction is in conformity with the rules? If it doesn’t conform to it, it will be judged illegal.

② Whether the transaction has been existed in the blockchain? If it has been existed, it will be judged illegal.

③ Whether all the contracts of the transaction have been properly executed? If they have not, it will be judged illegal.

④ Whether there are multiple payments in the transaction? If so, it will be judged illegal.

⑤ If all the above judgments are not consistent, it will be judged as a legal transaction.

In the BHP network, any node broadcast transaction. After receiving the transaction, the accounting node will open the consensus view, initiates the proposal broadcast. The delegate will start to verify the transaction. This round

of consensus is successful when t seconds have been waited and the faulty consensus nodes are not more than (n-1) /3.

3.5 Transaction book

In the BHP payment system, a block composed of a block body and a block head is generated about every 15 seconds on average. The block body is mainly the transaction generated during this period, and the block head includes the hash value Hr-1 of the previous block, the Merkel root hash MerkleTX composed of the current transaction, the time stamp T and the random number Nonce, etc. Since the block head contains a hash value pointing to the previous block, the block constitutes a "chain" structure.

The BHP Block Chain Account is consistent with the Bitcoin Principle. BHP replaces traditional accounts with an Unspent Transaction Output (UXTO) model. The UXTO system follows two rules:

(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 equal to the total output, and the two sides of the equation must be equal. (Generally, output is less than input, and the difference is the transfer fee, which belongs to the PoS miners.

The biggest advantage of the UXTO model is that the transactions can be recorded faithfully. Our real world flows with time, and transactions happen one by one, and the blockchain system faithfully records what happened in the world. It cannot be rolled back or deleted.

3.6 Smart Contract

The smart contract was first proposed by the cryptographer Nick Szabo in 1994. Smart contract is a computer protocol that aims to propagate, verify or execute contracts through information technology. Smart contract allows for credible transactions without third parties, which can be tracked and irreversible. BHP has an independent smart contract system: BhpContract. It is a micro-core, platform-independent smart contract execution environment that provides a set of instructions that include stack operations, flow control, logic operations, arithmetic operations, cryptographic operations, string operations, and array operations. In hardware, it only provides two calculation stacks. However, it allows the implementer of the blockchain to create its own virtual hardware which opened to smart contracts in the form of interfaces, so the contract can get platform-related data, persistent storage, and access to the Internet at runtime. Although this may also make the contract's behavior uncertain, blockchain implementer can eliminate this uncertainty by properly writing virtual hardware. However, since there is currently no compiler and development environment for AVM, it is difficult to develop smart contracts based on AVM. Developers have to use a similar assembly syntax to write contracts, which requires higher technical ability.

BHP smart contract runs in BhpVM with high certainty, high concurrency and high scalability. According to the design target of BHP blockchain of hash power, the smart contract of BhpContract mainly includes deposit interest

contract, credit mortgage contract, commercial payment contract, transfer contract, asset investment contract and so on. With the continuous upgrade of the smart contract protocols, BHP hash power chain will support users to develop smart contracts in the future.

3.7 Oracle Mechanism

The Oracle is a smart contract deployed on the chain, which is a chain code. It is necessary to use the Oracle technology when external data is needed on the block chain. The whole workflow is that the oracle obtains the required data from the trusted party, then transfers accounts to the address on the specific blockchain, and writes the price information into the transaction note, so that the smart contract can get the required data only by looking at the transaction records at the specific address. Since the blockchain automatically stores the blocks containing the transactions, the smart contract can get data information almost by accessing the local area. It not only ensures access efficiency, but also ensures data consistency. In general, the oracle (third party) pushes the data to the blockchain without the need for smart contracts to actively pull data from the third party.

The user's trusted hash power assets can be chained to provide the reliable external data for the smart contract of PoS revenue through the oracle technology, which solve the trust and promote the consensus.

3.8 Cross-chain Protocol

BHP is a distributed payment system that supports multi side chain

association. It supports the architecture of “main chain + high performance multi side chain”, and can realize efficient exchange among multi assets. BHP cross-chain interoperability protocol including two parts: “cross-chain asset exchange protocol” and “cross-chain distributed transaction protocol”.

(1)Multi chain atomic asset exchange protocol

BHP has been extended on existing double-stranded atomic assets exchange protocols to allow multiple participants to exchange assets across different chains and to ensure that all steps in the entire transaction process succeed or fail together. In order to achieve this function, we need to use smart contract function to create a contract account for each participant. It can cross two completely independent block chains to realize the exchange of them.

Multi Chain atomic asset exchange protocol does not increase the complex communication mechanism between chain and chain, but it can guarantee that this kind of exchange is atomic and credible, and there will be no transfer of ownership but no transfer of the creditor's right.

(2)Cross-chain distributed transaction protocol

Cross-chain distributed transactions mean that multiple steps of a transaction are scattered across different blockchains and that the consistency of the entire transaction is ensured. This is an extension of cross-chain assets exchange, extending the behavior of assets exchange into arbitrary behavior. BHP will use a cross-chain smart contract, a smart contract can perform different parts on multiple chains, either succeeding or reverting as a whole.

4 Conclusion

The distributed payment system based on bitcoin hash power credit is proposed in this paper. It uses high-efficiency concurrent network framework to solve high concurrent payment problems, uses asymmetric encryption digital signature technology to solve payment security problems, and uses blockchain distributed ledger technology to solve the security problem of transaction information storage. The system can be applied to many fields such as cross-border payment, transfer transaction, asset management, etc., and realize the completely decentralized payment transaction under the guarantee of the bottom credit of bitcoin hash power.

References:

[1]Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoincore.org/bitcoin.pdf, 2009.

[2] Victor S.Miller. Use of Elliptic Curves in Cryptography. Proceedings of Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, USA , 1985, 417-426

[3] N Kobitz. Elliptic curve cryptosystems. Mathematics of computation , 1987, 48(177):203-209

[4] A Kiayias, N Lamprou, AP Stouka. Proofs of proofs of work with sublinear complexity. Proceedings of International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 2016, 61-78

[5] R, Angela, B Liana. The issue of competing currencies. Case study - Bitcoin. Theoretical & Applied Economics, 2014, 21(1):103-114

[6]Certicom Research. SEC 2: Recommended Elliptic Curve Domain Parameters. http://www.secg.org/sec2-v2.pdf, 2010.

[7] https://akka.io/

[8]Nick Szabo. Smart Contracts: Building Blocks for Digital Markets. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html, 1996.