Bit Asset Chain

Decentralized high-performance digital asset management chain

V 3.0.0

2020.08.01

Contents

Bit Asset Chain.....1

Decentralized high-performance digital asset management chain.....1

Chapter 1 Summary.....4

Chapter 2 Status and improvement.....6

2.1 Stable performance and reliability.....6

2.2 Economic system recognized by the community.....7

2.3 Perfect supporting ecology.....8

2.4 Supervision supporting mechanism.....8

2.5 Upgrade space.....9

Chapter 3 BAC Chain.....10

3.1 Consensus mechanism.....10

3.2 Smart contracts and built-in contracts.....13

3.3 Storage network.....14

3.4 Cross-chain.....14

Chapter 4 Decentralized Finance (DeFi) Application.....16

4.1 Issuing Token.....16

4.2 Stablecoin.....17

4.3 Decentralized trading protocol DEX.....18

4.4 Decentralized lending.....21

4.5 Credit reporting system.....27

4.6 Fund Account.....27

Chapter 5 Other blockchain applications.....29

5.1 Logistics traceability.....29

5.2 Digital copyright.....29

5.3 Payment.....29

Chapter 6 Technical Details of BAC Chain.....31

6.1 Economic System.....31

6.1.1 Original ZI-POS consensus mechanism (Zero Inflation Prove of Stake).....31

6.2 Overall module.....32

6.3 POS+BFT consensus.....34

6.4 Cost model and incentive system.....38

6.5 Smart Contract.....40

6.6 Oracle.....40

6.7 Governance.....41

6.8 Data storage.....42

6.9 Secure Multi-Party Computing (MPC).....43

6.10 Supervision.....44

6.11 Security.....44

6.12 Extension.....46

6.13 BAC's supporting ecology.....47

Chapter 7 Technology Roadmap.....49

7.1 Mainnet launch in April 2020.....49

7.2 Store online in July 2020 49
7.3 Promote open source and start applications in August 2020 49
7.4 Realization of decentralized transaction agreement in November 2020 49
7.5 January 2021 Built—in contract to realize DeFi business model 50
7.6 June 2021 smart contract goes live 50
7.7 Mainnet expansion after 2021 50
Chapter 8 References 51

Chapter 1 Summary

Since the first Bitcoin was mined on January 3, 2009, blockchain technology has gone through 10 years. In the past ten years, the blockchain industry has developed steadily amidst doubts and has gradually been recognized and accepted by the public. Nowadays, central banks in various countries are already studying the issuance of digital legal currency based on blockchain technology, and multinational companies like Facebook have also released the Libra project based on blockchain technology, and established financial institutions such as Goldman Sachs and Bloomberg have also begun to get involved in blockchain business. .

Digital assets originate from Bitcoin, which is a distributed ledger system based on cryptography and based on public and private keys. The birth of digital assets makes it possible to decentralize financial services. Compared with traditional financial bank-centric account systems, decentralized financial services have higher efficiency, lower costs, and the operating mechanism is more open, fair and transparent. It is expected that in the near future, more users and institutions will participate in the decentralized financial world, and many new services related to digital asset management will be born. These services may be the continuation of the existing types of financial services, such as transfers, derivatives transactions, wealth management funds, asset custody, mortgage loans, supply chain finance, etc., or they may be brand-new types of financial services, such as digital asset wallets. Centralized exchange, DeFi, stable currency, etc. The use of blockchain technology features such as traceability, credit investigation and other functions have already entered the supply chain systems of major enterprises, and more application scenarios will be obtained in the future.

BitAsset Chain aims to design an efficient public chain specifically for decentralized financial services, with the public chain as the underlying infrastructure, built-in powerful digital asset management capabilities, combined with the wallet application front-end to achieve a complete DeFi support system, and truly achieve Valuable applications landed. In terms of specific implementation, Bit Asset Chain uses the BCV and BAC dual currency economic system to ensure the balance of public chain basic services and mortgage mining, and uses ZI—POS consensus to ensure the efficiency of the public chain under a safe and deflationary economic model. Use tendermint consensus engine and cross—chain interaction protocol IBC to build a side chain and relay chain system, achieve cross—chain goals, realize cross—chain asset circulation, and meet the design of multi—source digital asset management. While supporting smart contracts and ensuring the expansion of common functions and services, Bit Asset Chain implements typical businesses such as DEX protocols, lending, and funds in a built—in form, and attaches importance to the user experience and the construction of product peripheral facilities, combined with digital asset wallets, etc., for users DeFi ecology that provides a good experience.

Chapter 2 Status and improvement

In the world of digital assets, a public chain must be needed to serve the new decentralized financial environment. We believe that a public chain that can meet the needs of digital asset management applications requires the following conditions:

2.1 Stable performance and reliability

In the computer world, if the performance of the operating system is poor or unstable, all the software on the computer cannot run normally, let alone use the computer to complete work efficiently. The performance and stability of the public chain are as important to the blockchain system as the operating system is to the computer. First of all, a public chain that can be widely used must have reasonable performance. We know that the performance of a decentralized system is difficult to match the performance of a centralized system. This is the price that needs to be paid to enjoy the security and other advantages brought by the decentralization, but we can still work hard to seek changes and upgrades. A public chain that meets the current mainstream DApp performance needs. For example, on public chains represented by TRX and EOS, transfers can basically be completed within a few seconds. Users do not need to wait for more than 10 minutes like Bitcoin. There are already thousands of DApps running on these public chains. Millions of users use it every day, and the traffic has surpassed many centralized applications.

Whether it is ETH or EOS, and other mainstream public chains, there have been stability problems, such as vulnerabilities in smart contracts, problems during mainnet upgrades, etc. These problems have dealt a blow to the ecology of the public chain, as well as users' assets. Caused a loss. We should also learn from the lessons of our predecessors, work with professional security teams, do our best in safety and stability, actively and passively avoid problems in the public chain, especially at the level of smart contracts and mainnet upgrades. The core mechanism of the system takes precautions, once a problem occurs, the loss can also be minimized.

2.2 Economic system recognized by the community

In the POS consensus blockchain system, the economic model is designed from the perspective of satisfying the function and security of the public chain. The node can obtain the identity of the verification node by staking the token, and the user obtains the income by using the token to vote for the supporting node. If a node does evil, its revenue will be affected, and users will also transfer their votes to a more reliable node to prevent the node from doing evil. Although this widely adopted staking mechanism satisfies the POS consensus in terms of functionality and security, it lacks economic considerations. After the user can purchase the tokens as collateral in one time, they can continuously and permanently obtain the voting profit reward. If the number of new mortgages decreases and the number of tokens produced continues to increase, the value of the tokens will not be supported, and investors in the entire public chain ecology will suffer losses, which is detrimental to the long-term development of the public chain ecology.

The verified mathematical model of the Bitcoin POW consensus on the market has a certain degree of deflation, the total amount is constant, and the output will be periodically halved. As long as the activity of project users continues to grow, the value of the token will be supported. Although the design of this economic system is reasonable, its performance cannot reach the standard of POS public chain.

Therefore, the blockchain industry needs a new consensus system that can not only meet the needs of large-scale applications in terms of performance, but also support the value of the token in the economic system, which will better encourage community users to have a deeper depth The participation and promotion of the public chain can also create soil for the long-term development of the public chain ecology.

2.3 Perfect supporting ecology

A popular public chain is inseparable from developers and initiators who use the public chain. To attract users to participate in the ecology of the public chain, it is necessary to create a simple and easy—to—use R&D environment for developers. For example, node building tutorials, wallet components, IDE tools required for smart contract development, as well as complete documentation tutorials, frameworks, class libraries, templates, etc. can greatly reduce the user's entry barrier and research and development time costs. The more convenient the development of the public chain, the more developers will choose this public chain, and the better the ecology of this public chain will develop. In addition to being friendly to developers in the development process, users in the public chain ecosystem are also indispensable for developers, because only with the participation of users can the developed applications be used and can truly create value.

2.4 Supervision supporting mechanism

Although the blockchain has high credibility of decentralization, it also has a certain degree of anonymity and irreversibility. If these features are used incorrectly, it is likely to make the public chain a hotbed of crime. For the healthy development of the public chain, we believe that the public chain system must also be subject to certain supervision. Such supervision should not be too strict. This will violate the philosophical logic of blockchain decentralization and equality for all and hinder the public chain. development of. But in the same way, it cannot be completely without supervision, otherwise malicious people will be allowed to abuse the public chain. We believe that the public chain system must also comply with the regulatory mechanisms of various countries. Although there are currently no clear laws and regulations governing public chains, we believe that with the increasing popularity of blockchain technology, relevant policies will definitely be formulated. For the long—term and stable development of public chains, regulatory policies must be implemented. Cooperate and carry out related development.

2.5 Upgrade space

Although the current blockchain technology has improved a lot from when it was first born, there are still many imperfections.

For example, the current public chains are all running serially, that is, only a single transaction can be processed at the same time. A global public chain that can support large—scale applications must be able to process multiple operations concurrently. At present, the concurrency technology of the public chain has not made a breakthrough, so the performance of the public chain is greatly restricted.

In addition, decentralized storage is also a big challenge. Mainstream public chains such as Bitcoin and Ethereum can only store simple transfer records, which is far from meeting the needs of large—scale applications. Several highly anticipated distributed storage projects, such as IPFS, have not yet been launched and need to be verified by the market.

These technically imperfect factors have restricted the popularization of blockchain applications. We believe that these problems will eventually be resolved and a collective explosion of blockchain applications will usher in the near future. And our public chain also needs to keep up with the trend of technology and constantly upgrade and improve, in order not to be eliminated.

Chapter 3 BAC Chain

3.1 Consensus mechanism

3.1.1 Contradictions among current mainstream consensus mechanisms

The current popular public chain consensus mechanisms mainly include the POW workload proof mechanism represented by BTC and the POS equity proof mechanism represented by the 3.0 public chains such as EOS and TRX.

Among them, the economic system of POW has the characteristics of constant total volume and periodic halving of output. This deflation—like economic system provides a certain guarantee for the value of the token. The continuous increase in the price of BTC over the years is due to this economic system , Is an economic system that has been verified by the market and has achieved success. However, the POW consensus has too many nodes that need to be synchronized due to the slow block production speed, and it is difficult to meet the public chain application requirements of the new era in terms of performance.

If POW is a referendum mechanism, POS consensus is like a people's congress mechanism. POS selects verification nodes among many participants and is responsible for the block generation of the blockchain on behalf of the user, so that the nodes that need to be synchronized in the network are divided by several One hundred thousand drops to dozens, which greatly improves the performance of the public chain, but the economic system of the POS consensus mechanism is an inflationary economic system. It is necessary to issue more tokens to reward nodes and users who vote for nodes. Under this inflationary model, the value of the token is difficult to support.

3.1.2 ZI-POS consensus mechanism

In order to solve the contradiction between the economic system and performance, BAC Chain invented the ZI—POS (Zero Inflation Proof of Stake) consensus mechanism. Based on the traditional POS consensus mechanism, it established a dual currency dual deflation economic model, making BAC Chain not only has the performance of a POS consensus mechanism, but also has an economic model recognized by the market like BTC, ensuring the ecological stability and sound development of the public chain, and creating more benefits for ecological nodes and community users participating in voting.

3.1.3 Dual currency

BCV: BAC Chain's equity token, holding BCV means enjoying the rights of BAC Chain. Therefore, as the main network node at the core of BAC Chain, it is necessary to hold and mortgage at least 100,000 BCV to participate in the election. Users who vote for nodes need to destroy BCV to obtain voting rights.

BAC: BAC Chain's functional token, BAC Chain's on—chain business, such as transfer fees, smart contract execution, distributed storage and other businesses need to consume BAC. The economic model of BAC refers to the constant total amount of BTC, and the output halving mechanism. Mining output starts from 0 circulation, and 0 is reserved by the initiator.

3.1.4 Deflation destruction mechanism

BCV: The total amount of BCV is 1.2 billion and will never be issued. Users mortgage or destroy BCV to buy BAC voting mining machine mining is the only way to obtain BAC. In addition, each BAC voting mining machine also needs to recharge the energy value to continue mining. Destroying BCV is also the only way to obtain energy value.

BAC: The total amount of BAC is 43,695,126. At the beginning, each block produced by BAC Chain will give the block producer 10 BAC as a reward. After that, the number of rewards is halved every six months and rounded down until all BACs are mined after about two and a half years.

Before all BACs are mined, users will use BAC to pay for transaction fees for transfers using

BAC Chain, for running smart contracts, and for storage of the storage network. All BACs paid will be paid before mining is completed. Was destroyed.

	Total Amount	Destruction Mechanism	Acquisition
BCV	1,200,000,000	Buy BAC Miner	Exchange
BAC	43,695,126	Transfer fees	Mortgage or destroy BCV mining

Time	Number of awards per block	Total number of awards per day
First six months of first year	10	144, 000
Last six months of first year	5	72, 000
First six months of second year	2	28, 800
Last six months of second year	1	14, 400
Third Year	0	0

3.1.5 Verification node and voting miner

Like the traditional POS mechanism, ZI—POS requires a verification node as a block producer to build a blockchain network. In the traditional POS consensus mechanism, the tokens pledged by the verification node and the block rewards obtained are the same token. Under the ZI—POS consensus mechanism of BAC Chain, the token pledged by the node is the BCV as the equity token. The block reward is BAC as a functional token. In this way, not only can two different tokens be separated according to their different functions, but it can also avoid over—issuance of tokens and avoid inflation.

As a community user, you need to vote for the node to express your participation in the community and support for the node. Users need to destroy BCV to obtain voting rights. The node will distribute its own block rewards to users who support it. In order for users to better understand this mechanism, we virtualize voting rights as voting mining machines. Users' voting behavior can also be equivalent to a mining behavior, so that nodes can also be equivalent to mining pools.

The more the node mortgages and the number of votes it obtains, the greater the trust and support of the community that the node has, the higher the probability that the node will get the opportunity to generate blocks, and the greater the revenue. On the contrary, if the node does evil or does not act, it will be punished by slash, and users will transfer their votes to other nodes.

3.2 Smart contracts and built—in contracts

3.2.1 Smart Contract

Smart contracts are indispensable to the financial management public chain. BAC Chain smart contracts not only have the basic characteristics of Turing complete, flexible, safe and reliable smart contracts, but also provide an eco—friendly contract engine BVM. BVM provides execution security, performance, and multi—language support for smart contract execution through webAssembly and oracle technology.

3.2.2 BVM virtual machine

BVM is improved on the basis of webAssembly. webAssembly is an efficient loading, portable, platform—independent bytecode format, which can execute programs at a speed close to the original on the platform. This is a brand new web standard. Supported and developed by several major companies such as Google, Apple, Microsoft, and Mozilla. webAssembly is a technology that has been verified by EOS, and EOS smart contracts have been executed steadily along with the launch of EOS. In addition, BVM also considers that the ecology of webAssembly is very good. Many programs that can be written in high—level languages can be programmed into wasm bytecode programs. The wasm bytecode can be compiled into machine code and then executed, or it can be directly executed using an interpreter. , This reduces the learning cost of developers.

Security issues are critical to smart contracts. Security issues may arise during execution, such as excessive use of computing and storage resources, and inconsistent node execution effects. BVM attaches great importance to the security and correctness of the contract from the design level. It uses the gas mechanism to prevent excessive use of resources. BVM has made many security restrictions on the depth of execution and the time—consuming execution. BVM clarifies the permissions between interfaces at the code level. The entry function of the smart contract needs to be restricted to prevent developers from calling unauthorized functions in the entry function and destroying the contract execution content.

3.2.3 Built-in contract

BAC Chain has written the protocol layer and the functional requirements with strong versatility into a built—in contract. These contracts are hard—coded on the chain. Developers can call according to the interface parameters of the contract. Requests that do not meet the interface requirements will be directly rejected. Such contracts not only provide developers with convenience, but also improve security. And stability.

The current built—in contract functions planned by BAC Chain are as follows:

Issue Token

Decentralized transaction agreement

Account credit review

Decentralized lending

Fund institution special account

3.3 Storage network

BAC Chain realizes the storage network function, and the following factors are considered in the design process:

1. The stored data needs to be sent in the form of transactions and stored in the form of state. In such a hard upgrade, transaction data will be stored on the mainnet before the upgrade, and the status data is always bound to the account, and can still be queried on the mainnet after the upgrade. BAC Chain treats the data that needs to be stored as assets;
2. Considering the diversity of commercial data, users can customize the data format storage when implementing storage to ensure user convenience;
3. BAC Chain carries the digest of the stored data or the signature of the data. The real data can be stored in other distributed systems, which can reduce the number of the chain itself, and achieve data consistency and prevent tampering. Currently, FastDFS is used The cluster serves as the back—end file system;
4. Users can choose whether to encrypt storage when storing to ensure data security;
5. The storage itself needs to consume resources, and the storage in BAC Chain needs to consume the corresponding BAC as a cost. The larger the amount of data stored, the greater the storage cost consumed. This part of the cost can be selected by community voting to consume or gain The method is distributed to mining users and is currently consumed directly;
6. The stored data has a location field, which can easily retrieve the version, height and transaction prefix on the main network.

BAC Chain has initially realized the function of the storage network and is exploring its application in the commercial field.

3.4 Cross—chain

The current mainstream blockchain cross—chain technical solutions are divided into three main categories according to their specific implementation methods, namely, notary mechanism, hash lock, side chain and relay chain.

The security of the notary mechanism depends on the notary system, and the parties involved in the cross—chain need to have greater trust in the notary mechanism. Hash lock is currently more suitable for the exchange of partial assets or key data, and its usage scenarios are more restricted. The bottom layer of BAC Chain uses tendermint consensus engine and cross—chain interaction protocol IBC to build a side chain and relay chain system to achieve cross—chain goals. For early digital asset chains, such as BTC/ETH, cross—chain technology was used to transfer the value of BTC/ETH to BAC Chain. For those that have supported the IBC asset chain, use the IBC agreement to achieve cross—chain goals.

Chapter 4 Decentralized Finance (DeFi) Application

The birth of blockchain technology, in addition to the centralized value storage mechanism centered on banks, provides us with a new option for decentralized storage and transfer of asset value. Blockchain is a value storage medium. The digital assets stored on the chain can empower many financial services, and all on—chain services are also decentralized. All services existing in the traditional financial field should be redesigned and implemented in a decentralized form on the blockchain.

A reasonable decentralized financial public chain needs the following basic functions to meet the needs of the application:

1. Token can be issued
2. Has stable coins
3. There is a decentralized transaction agreement (DEX)

Because the current smart contracts have poor security and are not easy to upgrade, for these typical businesses, we will use built—in contracts to implement DeFi functions, which not only guarantees better security, but also makes transactions more efficient, which is also for the future Upgrade to provide more convenient space. Of course, if the functions we provide cannot meet the needs of the project party or users, users can also use smart contracts to implement additional functions in the future.

4.1 Issuing Token

BAC Chain supports the function of issuing tokens in the form of built—in contracts. Users only need to run a few lines of code to issue their own tokens on the chain. Users can customize the token name, decimal point accuracy, total issuance and other parameters. You can also use BCV as the backing asset behind the issuance of Token to increase the credit of Token.
All Tokens issued on the BAC Chain can be transferred freely on the chain, and users only need to pay the BAC fee. If the Token has a reputation problem, the user can exchange the Token held by it into the BCV asset guaranteed behind it in an equal proportion to reduce their own losses, and the Token after the exchange will be directly destroyed.
In order to further reduce the user's operating threshold, Biwei Wallet also released the pass product, as the front end of the application that supports the issuance of Tokens by BAC Chain, issuing Tokens on BAC Chain with one click.

BAC Chain has now launched the mainnet issuance function of digital assets. The specific fields are as follows:

Field	Type	Description
outer_name	string	Name specified at release, e.g., ABC; user-specified
inner_name	string	New name created at release, outer_name with a suffix
supply_num	bigInt	Total issuance; user specified
margin	string	Safe Deposit: user-specified
website	string	Token Description URL: user designation
description	string	Token description: user designation
precision	uint8	Accuracy: user specified
exchange_rate	string	exchange_rate= deposit/supply;
owner_address	string	User address:user specified

4.2 Stablecoin

4.2.1 Centralized stable currency scheme based on qualification endorsement

USDT uses this scheme to achieve it. Tether company endorses it. For every 1 USDT issued, 1 U.S. dollar is exchanged. USDT is currently the most widely used stable currency scheme, but this scheme itself has some problems. USDT reserves are not It is not transparent, and its additional issuance may lead to a crisis of trust, face uncertain regulatory policies and so on.

4.2.2 Decentralized stablecoin scheme based on DCEP and Libra

This type of stable currency is based on the endorsement of the country or major bank, and its operation will be highly regulated. The monetary policy is controlled by each country. It is also based on blockchain technology and has a certain degree of anonymity. This type of stable currency needs to be considered. More and more complicated. At present, it is still in the discussion or experimental stage, and has not entered the mainstream market.

4.2.3 Completely decentralized stablecoin solution

DAI is a stable currency anchored at USD 1:1 created and issued by makerDAO, which is based on the Ethereum chain. Unlike BTC, ETH, EOS, and general tokens, Dai is not generated through mining, but a certain amount of ETH must be pledged by Dai demanders, and then a certain amount of DAI must be issued to ETH pledgers by the action of smart contracts. At present, DAI is far less active than USDT.

In the implementation of various businesses in DeFi, stablecoins are an indispensable medium. Project parties can use BAC Chain's built-in token issuance mechanism to issue their own qualified endorsed stablecoins. The stablecoins can also use BCV as the backing assets, or anchor the value of stablecoin assets in other ways.

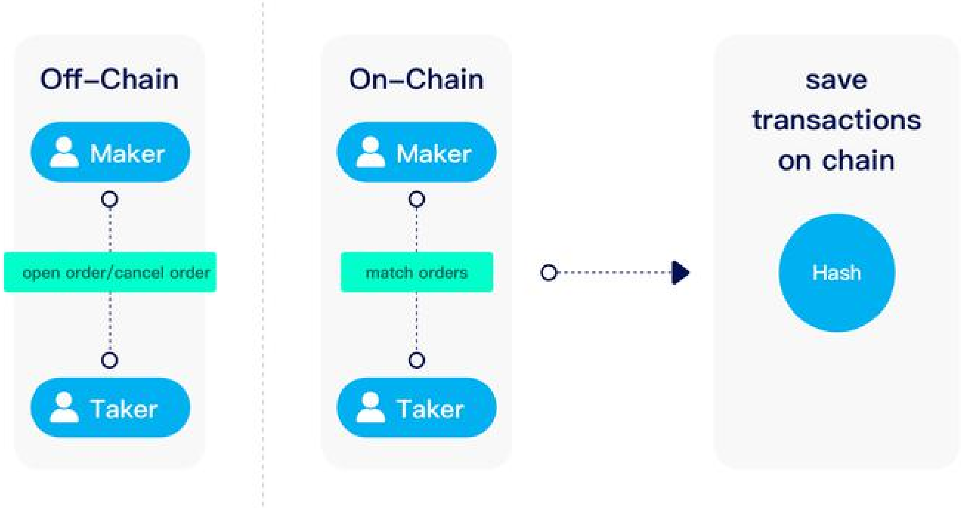
In addition, stablecoins issued on other mainnets such as ETH/TRX can also be used on BAC Chain through the cross-chain mechanism of BAC Chain, providing support for mainstream stablecoins such as USDT/USDC.

4.3 Decentralized trading protocol DEX

Now mainstream exchanges operate in a centralized manner. Users can check the flow of their assets on the chain only when depositing and withdrawing coins, but the transaction records are not recorded on the blockchain, and each transaction All have their own independent account systems, and these account information are also centrally stored. At present, this centralized trading mechanism of mainstream exchanges does not match the DeFi decentralized system, and it is also impossible to truly decentralize and realize slightly complicated DeFi business processes. We need a decentralized transaction protocol to support DeFi business. The user's address is the transaction identifier. The user only needs to hold the private key to conduct the transaction. It is compatible with DeFi applications, and the transaction records can be checked directly on the chain, which is more transparent public.

4.3.1 On–chain and off–chain hybrid mechanism

In view of the limitations of the current immature blockchain technology, on—chain performance cannot meet the millisecond—level response requirements for users to place and cancel orders. In addition, if the user's operations of placing and canceling orders, if there is no transaction, they are all recorded on the chain, not only consumes on—chain storage space, but without a good commission experience, it will also consume unnecessary user fees. Therefore, BAC DEX adopts a hybrid mechanism combining on—chain and off—chain. The user's order signature is only recorded in the off—chain system. When a transaction is matched, the user's transaction will be completed and uploaded to the chain.



4.3.2 Basic data structure of BAC DEX

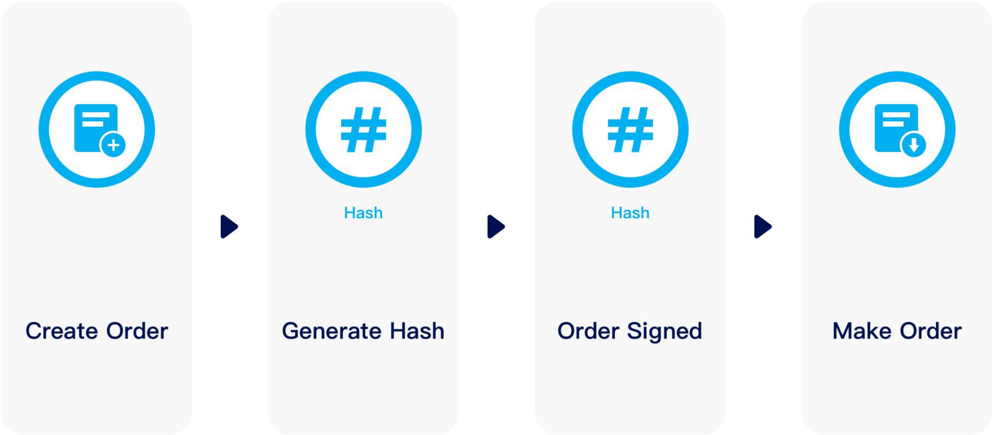
Variable	Function
makerAddress	Maker Address
takerAddress	Taker Address
makerData	Maker details, such as price, number of transactions, time of order, type of commission, etc

takerData	Taker details, such as price, number of transactions, time of order, type of commission, etc
makerAmount	Maker amount of orders
takerAmount	Taker amount of Orders
makerFee	Maker Fee
takerFee	Take Fee
commitID	Unique identifier of the transaction

4.3.3 Transaction signature mechanism

Every transaction of the user requires digital signature verification to ensure the authenticity and integrity of the transaction, to ensure that the transaction is from the real controller of the address, and that the order information has not been tampered with during the information transmission process.

Every transaction of BAC DEX uses a digital signature and encrypts the order. This allows the orderer to be assured that no one can conduct unauthorized transactions with their address except for the order they have authorized. At the same time, potential transaction parties can also verify whether the order is a safe and effective order.



4.3.4 Multi-platform sharing depth

Because the transaction logic of BAC DEX is completed using BAC Chain's built—in contract function, users can build multiple decentralized exchanges based on BAC Chain's public agreement, and these exchanges share the same data structure and are matched on the same public chain. Therefore, multiple exchanges can share the depth of transactions, and users on different exchanges can also trade each other's orders.

4.4 Decentralized lending

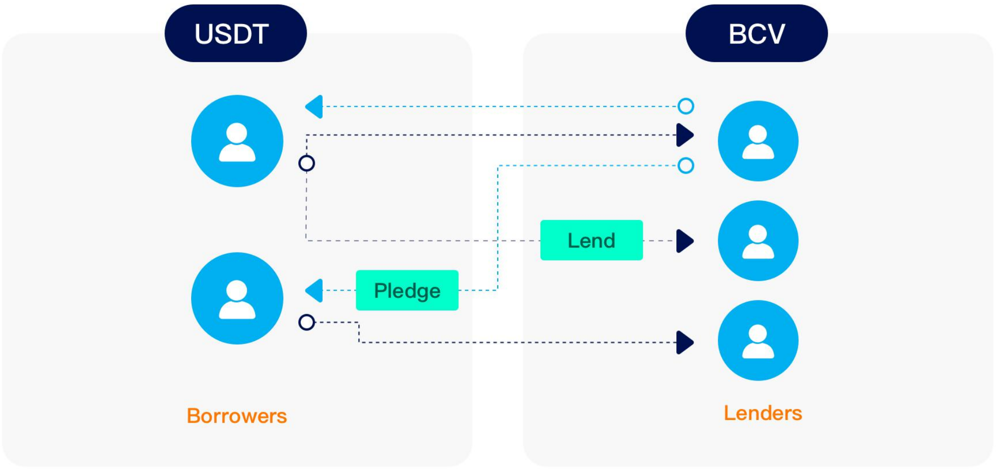
Lending is a basic application in the financial field. On the one hand, it can meet the capital needs of borrowers, and on the other hand, it can also provide interest income for lenders. Compared with the traditional lending system, the decentralized lending system has the advantages of convenient operation, low risk, and fast lending. It will be one of the main application scenarios of DeFi in the future.

The BAC chain combines the current mainstream DeFi lending technology and traditional financial lending mechanisms, and provides support for lending functions in the built—in contract. The system can support two different lending mechanisms, a multi—point—to—point lending model and token exchange, as well as multiple mortgage lending mechanisms such as installment repayment and single payment. Users can easily lend or borrow money, and project parties can also use the built—in The contract interface quickly develops a fully functional lending platform. If the functions of the built—in contract cannot meet the demand, the project party can also use the combined smart contract to conduct secondary development on the basis of the built—in contract.

4.4.1 Peer-to-peer lending model

Peer—to—peer lending is an address—to—address lending mechanism. The lender can initiate a lending request on the chain and set the expected interest rate, repayment time, and mortgage rate. The lender can also initiate a loan request on the chain. And set the expected loan amount and the type of mortgage assets. If both the lender or the lender have matching intentions, BAC

Chain's on—chain lending model will match the accounts of both parties and match the lending transactions on the chain. The lender can get the loan immediately, and the lender will also get the mortgage immediately. The right to lock in tokens. If the lender defaults or closes its position, the borrower can also immediately obtain the lender's collateral, thereby minimizing the risk.



4.4.2 Interest calculation method

In the lending model of BAC Chain, because there are already locked tokens as collateral, the risk is low, so there are many different repayment methods. Classified from the traditional repayment methods, it supports the repayment form of equal principal and interest and equal principal. Equal principal and interest repayment means that the borrower repays the loan principal and interest in equal amounts every month. Equivalent principal repayment means that the borrower repays the principal in equal amounts every month. The loan interest decreases with the principal month by month, and the repayment amount also decreases month by month. In addition, if the lender agrees, it can also support the method of repaying the principal and interest in one go when the loan due date expires. In addition, users can also choose to repay the interest in a currency different from the loan currency, such as a user loan USDT, but the monthly interest during the repayment can be paid with BCV, and the amount paid is based on the real—time price of the oracle. Converted. The lender cannot redeem the collateral until the loan is fully paid off.

Basic data structure

Lending of assets	USDT, BUSD, BCV, BAC etc.
interestRates	Annualized interest rate as a percentage
interestAsets	USDT, BUSD, BCV, BAC etc.
dateofLoan	Time of day of loan
repaymentPeriod	Repayment period like 30 days
maturityDate	Expiry Date of the Loan
typeofRepayment	equal loan payment or equal principal payment
collateralRatio	Minimum collateral ratio
lenderAddress	Lender's address BAC Chain address
borrowerAddress	Borrower's Address BAC Chain address
collateralizedAsset	collateralized asset type
LendingAssets	Type of Lending of assets
amountReimbursed	Amount reimbursed
interestRepaid	Interest repaid

4.4.3 Liquidation

If the value of the mortgaged assets of the lender reaches the liquidation line, or the lender defaults, the system will automatically transfer the ownership of the mortgaged property of the lender to the borrower. The lender has the full right to dispose of the mortgaged property. The lender can choose to transfer the collateral to the exchange for sale. If the exchange's liquidity is poor, the lender can also choose to auction the collateral in the auction system of the BAC lending platform.

4.4.4 Point-to-point lending and mining mechanism

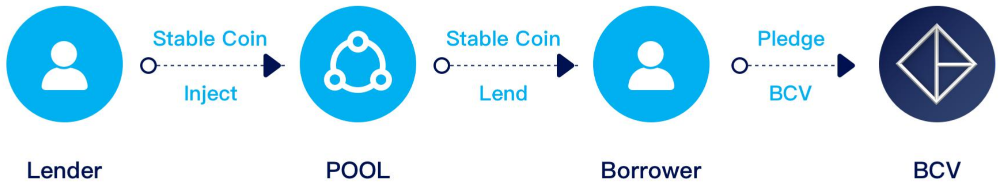
Since peer—to—peer lending has certain liquidity problems, such as when the lender is much larger than the borrower or the borrower is much larger than the lender, people's borrowing needs cannot be met immediately, which greatly affects the user's lending experience. BAC Chain has a built—in peer—to—peer lending module and a mining mechanism. The lending platform can deposit a certain amount of BAC as a mining reward. If the lending order is not satisfied within a certain period of time, the mining mechanism will be triggered and the user will complete the loan Demand, will get BAC rewards, and the longer the waiting time for the loan demand, the more BAC will be obtained when the demand is met.

4.4.5 Liquidity Pool Lending System

The peer—to—peer lending system is a one—to—one lending system. This application is suitable for relatively small—scale lending platforms or the lending behavior of individuals who are acquainted with both parties or parties.

The liquidity pool lending system is more like a bank. Users can deposit funds in banks to earn interest, and lenders can also mortgage tokens from the fund pool, pay interest, and lend funds. Both borrowers and lenders withdraw from each other in the liquidity pool, and they are not bound to each other. It first gathers all the assets together, and then allocates the loan when the borrowing demand is received, and then returns the interest to the depositor.

Since the liquidity pool pools everyone’s assets together, the assets of a particular depositor are not locked in a particular loan. This means that depositors can withdraw their assets at any time if needed, which is more convenient and flexible than peer—to—peer lending. However, this is only possible if not all of the assets in the liquidity pool have been borrowed.



4.4.6 Calculation of interest rate

In today's real world, interest rates and liquidity reserves are determined by the country's central bank. However, in the DeFi world, interest rates will be determined by the market, which can more naturally balance loan demand and token supply. The greater the demand for loans, the higher the interest rate. vice versa.

In general, not all assets deposited in the liquidity pool will be lent. The more the assets provided by the user are lent, the higher the asset utilization rate and the greater the return, but at the same time this also means that the user has lower liquidity and not all assets can be withdrawn at any time.

4.4.7 Deposit interest rate

When the lender deposits the stablecoin in the liquidity pool, he will get the ALT certificate for the invested assets. The formula for the exchange ratio between the stablecoin and ALT is as follows:

totalCash = the number of stablecoins that have been put into the liquidity pool but have not yet been borrowed

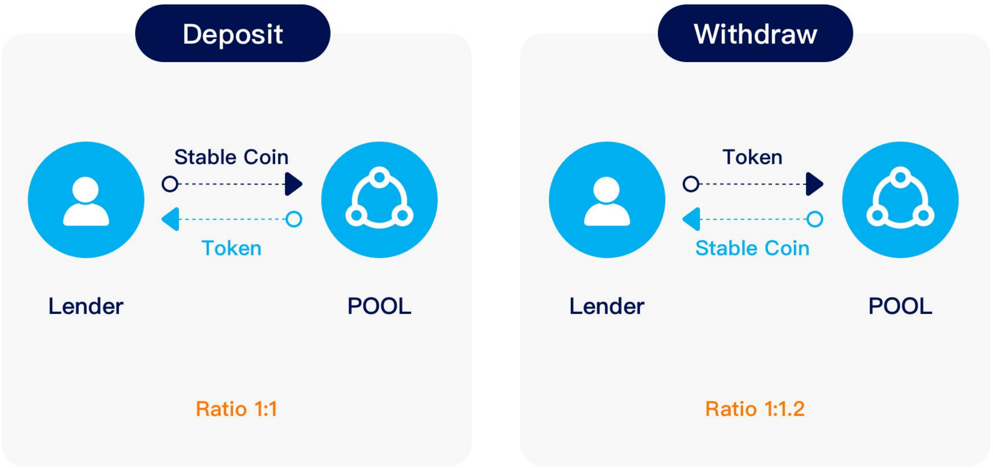
totalBorrows = The total amount of stablecoins that all borrowers should repay, including principal and interest

totalReserves = total reserve amount

totalSupply = total amount of all redeemed ALT

Conversion ratio = (totalCash+ totalBorrows− totalReserves)/ totalSupply

It can be seen that as the number of borrowings increases, the exchange ratio will increase accordingly. For example, when users deposit stable coins, the exchange ratio is 1:1. When the stable coins are withdrawn one year later, the exchange ratio is 1.11, and the user will get A 10% annual deposit interest rate.



4.4.8 Borrowing rate

The interest rate of borrowing should float freely according to the current market supply and demand relationship. Generally speaking, the greater the demand for borrowing, the interest rate will rise, thereby attracting more people to lend, and ultimately maintaining the interest rate in a dynamic equilibrium system.

The annual interest rate of borrowing is affected by the following three factors
1. **Basic interest rate**: The basic interest rate is the basic interest rate of the entire network, which is determined by the project party or the project community
2. **Utilization rate**: Utilization rate is the ratio of loaned use in the current liquidity pool, showing the current supply and demand relationship in the market

Utilization rate UtilRate = totalBorrows/(totalCash+ totalBorrows)
3. Recharge rate: used to adjust the impact of utilization rate on interest rates
Utilization rate UtilRate = totalBorrows/(totalCash+ totalBorrows)

Borrowing interest rate = base interest rate + utilization rate * replenishment rate

4.4.9 Lending interest rate

The lending rate is affected by the following three factors
1. Borrowing interest rate
2. Usage rate
3. Reserve interest rate: The reserve interest rate is the basic interest rate of the entire network, which is determined by the project party or the project community

Lending interest rate=borrowing interest rate*(1-reserved interest rate)*utilization rate

Since the liquidity pool is an open and free fund pool, users can deposit and withdraw assets at will. The lender can also pay interest at any time to return the loan principal and redeem the mortgaged assets. There can be different types of stablecoins in the liquidity pool, and different stablecoins also have different lending rates according to market supply and demand. However, the overall lending process and repayment method are relatively simple. We believe that liquidity pools and peer-to-peer lending are two complementary lending mechanisms. Users can choose the right service according to their needs.

4.5 Credit reporting system

Although the blockchain has a certain degree of anonymity, BAC Chain still has a mechanism to evaluate the credit rating of each address. Factors affecting credit ratings include account flow, account loan records, account default records, account asset value, account transaction records, etc. The Defi application can choose to only open services to certain addresses based on the credit rating of the account.

4.6 Fund Account

Since the opening of digital assets trading, more and more asset management service teams Token Fund have established digital asset funds. However, most of these funds are operated on centralized exchanges. Due to the lack of management measures in the digital currency market, it is difficult to guarantee the asset security of the funds.
As the technology of decentralized exchanges has become more mature and popular, it has become

possible to use a decentralized account system for fund asset management.

BAC Chain specifically designed an institutional account controlled by a built—in contract for fund management institutions. The deposit and withdrawal of the institutional account are restricted by a series of parameters, which can ensure the safety of investors' assets.

4.6.1 Fund account structure

Fund—raising quota：total fund—raising quota

Liquidation rules：When the account triggers the liquidation line, the contract will automatically return the account assets to the investor address in proportion to the investment

Maximum number of fundraisers：Maximum number of fundraisers

Dividend mode：The dividend mode of the fund will be written in the contract, and the system will automatically distribute dividends on the dividend day according to the dividend mode.

Settlement date：The settlement date of the fund.

When an institution needs to set up a fund to raise funds, it can open a BAC Chain fund account address, and set the relevant fund—raising quota, dividend model and liquidation rules. After the setting is completed, although the fund manager holds the private key of the account, it cannot withdraw coins through means other than the dividend model and liquidation rules.

The fund manager can manage the assets of the account to obtain profits through decentralized exchange transactions. The smart contract will automatically distribute dividends on the dividend day according to the profit situation and the dividend mode setting, and transfer the income to the investor's address.

Fund managers can also use the decentralized lending function to deposit stable coins to obtain fixed income, diversify asset allocation, or pledge small coins to obtain stable coins, and buy them back to short the market after the price of small currencies drops.

The fund account can not only simplify the fund—raising and dividend management procedures, but also increase the transparency and credibility of the fund.

BAC Chain uses a built—in contract to provide users with a complete decentralized financial application that can meet most of the application needs, including trading, lending, financial management, deposits, credit investigation, etc.

Chapter 5 Other blockchain applications

5.1 Logistics traceability

Blockchain has great advantages in the application of logistics traceability, especially in the fields of food safety, certificate of origin and traceability of green organic products. The non-tamperable feature of blockchain can give traceability greater credibility and more Low cost. Especially when the blockchain technology and the Internet of Things technology are combined, they can exert great efficiency.

Users can use IoT temperature data, oxygen content and geographic location sensors to collect relevant data in the key links of logistics, and record them on the BAC Chain blockchain, enable early warning, and monitor the measured data in real time; based on the blockchain The non-tampering characteristics of the data can ensure the safety and effectiveness of the data and develop a complete logistics traceability system. Based on data analysis and monitoring, the system can ensure the overall safety of the logistics process and accurately recall defective products when problems occur. In addition, logistics data can also be shared with insurance companies and relevant departments to help them provide more comprehensive insurance and supervision.

5.2 Digital copyright

On the Internet, digital information is easily copied and spread. If the distribution of digital information is through the BAC Chain solution, relevant data such as copyright registration, content distribution, and copyright transfer can be stored on the blockchain. The relevant unstructured data can be stored on the storage network, and only one copy can be guaranteed at the same time. Dissemination to realize the traceability of intellectual property rights. The solution is based on the characteristics of immutability, openness, and transparency of blockchain technology, which can reduce the cost of content providers for copyright registration, content distribution, and copyright transactions, realize point-to-point distribution, and make content circulation and transactions faster, Transparent.

5.3 Payment

BAC Chain's POS+PBFT hybrid consensus mechanism can ensure that a single transfer can be confirmed on the chain within 5 seconds. The confirmation time of the user's on-chain transfer is almost the same as the confirmation time of the current centralized online payment system. Provide users with a payment experience similar to the current systems such as Alipay and WeChat Pay. Cooperating with the application layer function of Biwei Wallet, it can be completed in a decentralized form, with functions such as QR code payment and face payment.

Chapter 6 Technical Details of BAC Chain

Bit Asset Chain (BAC Chain) is a decentralized high-performance digital asset management public chain developed by the BAC Chain Asset Management Platform. The design concept of BAC Chain takes advanced high reliability and high performance technology as the core, with mature economic system and community governance mechanism accumulated through long-term practice, and a series of supporting applications and development tools focusing on user experience. Strive to create a global digital asset public chain that is efficient, reliable, easy to use, and can meet all-round application scenarios.

6.1 Economic System

BCV Chain is a high-concurrency public chain based on the POS consensus system for asset management services and supporting enterprise-level applications. In order to solve the disadvantage that the traditional POS consensus mechanism cannot avoid inflation, BCV Chain improved the existing POS economic system and designed the ZI-POS (Zero Inflation Prove of Stake) economic model, which combines the traditional POS system with the classic bit The currency mathematical model is combined to establish a POS economic system with deflationary attributes, which can create more benefits for ecological nodes and community users who participate in voting.

6.1.1 Original ZI-POS consensus mechanism (Zero Inflation Prove of Stake)

The traditional POS consensus mechanism has the following disadvantages:
Inflation: Although different POS projects have their own additional issuance mechanisms and different rewards, in general, the traditional POS consensus mechanism rewards verification nodes by issuing additional tokens through the inflation mechanism.

Comparison of traditional POS + Bitcoin mathematical models

	ZI-POS	POS	POW
Token	Two	Single	Single
Performance	High	High	Low
Degree of decentralization	Low	Low	High
Deflation/Inflation	Two token both deflated	Inflation	Deflation when Meet certain conditions
Mining	Destroy	Pledge	Entity miners

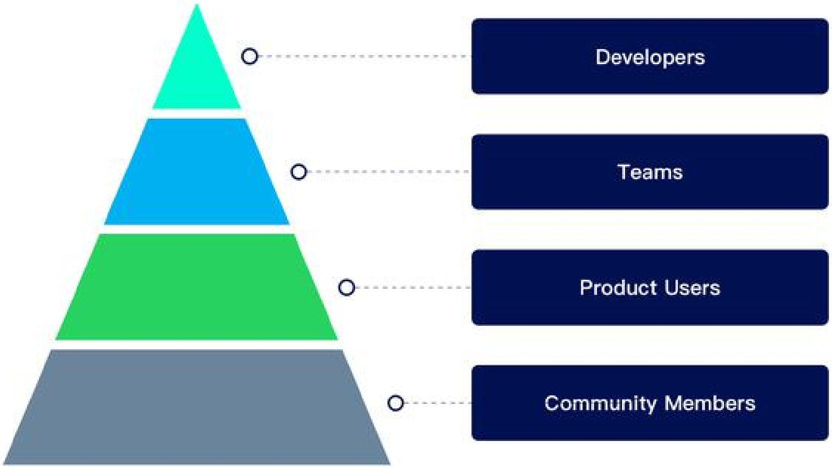
6.1.2 Dual currency

Why dual currency?

n an economic system, assets can be divided into two types according to users' holding intentions. The first is assets that can appreciate. People are willing to hold this type of assets for a long time, but the willingness to spend it is relatively low. The other is a highly liquid asset. This asset may not have as much appreciation potential as the first, but it has a high degree of recognition and can be easily circulated. People are willing to transfer and exchange such assets. There is a certain contradiction between these two kinds of assets. If there is only one asset in the economic system, people will have a entanglement between spending it or saving it. In order to solve this problem, we adopted a dual currency system to separate the long-term equity tokens from the miners' fee tokens used to support the circulation of the main network to better meet the needs of users and reduce people's troubles.

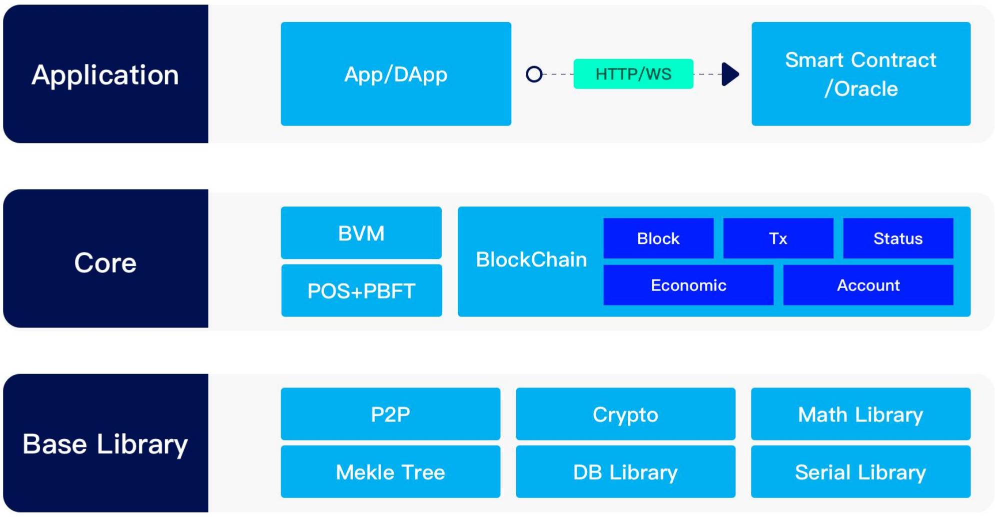
Equity token：BCV is used for equity mortgage of public chain verification nodes

Mining pass：BAC (BCV for Circulation) is used to verify the mining rewards of nodes, and to pay the transfer fees for using the public chain.



6.2 Overall module

BAC Chain is a supervisable, high-performance, and fully decentralized asset management public chain dedicated to digital asset services. Mainly divided into the following modules:



Base Library: Provide basic library services for BAC Chain

P2p provides services for message transmission between nodes

Crypto provides the cryptographic functions required by the public chain

Math Library calculation library: provide precision calculation services

Merkel provides message digest, compression and other functions

DB Library provides storage services required by the public chain

Serrial Library provides serialization services for message data

Core: The main components of BAC Chain

BVM provides an execution environment for smart contracts

Block provides block storage and retrieval block services

Tx provides transaction storage and retrieval services

Status provides the current or previous version of the data status of the public chain object

Economic public chain economic model

Account Model Account model, manage account assets

Application application layer:

App/Dapp provides services to users

Smart Contract

Oracle Oracle

6.3 POS+BFT consensus

With the continuous development of the blockchain, the number of blockchain users and the number of various operations increases, the security, reliability and performance requirements of the consensus algorithm are also getting higher and higher. The current pow protocol is very resource intensive and transaction confirmation is slow. , DPOS is relatively neutral, BAC Chain uses the consensus model of POS+BFT to achieve rapid consensus.

6.3.1 POS model

In BAC, the POS model includes the following three steps:

6.3.1.1 Create a validator

To become a validator, you need to initialize the following parameters:

A. Node public key: The private key corresponding to the public key will sign the block and the consensus state, and the public key will be used by each node as the block verification and hash state.

B. Node name: The node name will be displayed on the main network as an identification

C. Number of mortgages: The number of voting rights obtained by the node's own mortgage of BCV. The larger the number, the more it can be recognized by the miners.

D. Minimum mortgage ratio: the ratio of the node's own mortgage amount to the total mortgage amount of the node.

6.3.1.2 Miners voting

Miners who want to get profits can destroy BCV to obtain voting rights, and then vote for the verification nodes. The verification node is responsible for verifying blocks, packaging transactions, and generating blocks. The economic model will reward the verification nodes, and the verification nodes will distribute the proceeds to the miners according to the number of votes of the miners. Because the verification node needs a stable network, hardware equipment or cloud service. If the verification node cannot produce blocks stably, the system will reduce the rights and interests of the node and the miners under the node, which will help miners choose better nodes to vote.

6.3.1.3 Simplification of the allocation model

After each block is generated, the validator will be allocated rewards, and then these rewards will be distributed to his miners. If such an iteration is performed every time a block is generated, it will consume a lot of resources and even affect the overall operation of the system. BAC Chain uses the following model to simplify processing

A miner pledged x bcvstake to the verification node at a height h. The total amount of pledged by the verification node in the block i is s_i, the total reward allocated is the mining machine withdrawing at the block, the reward that can be withdrawn is

$$\sum_{i=h}^{n} \frac{x}{s_i} f_i = x \sum_{i=h}^{n} \frac{f_i}{s_i}$$

For a period of time, if there is no new mining machine or node mortgage, s_i will remain unchanged. A period of time that remains unchanged called p. In this period, the reward T_p received by the verification node v, and the mortgaged asset is N_p; as above Miners start mining at a height h, the beginning interval is p_{init}, and the ending interval p_{final} is then the above formula can be expressed as

$$x \sum_{i=h}^{n} \frac{f_i}{s_i} = x \sum_{p_{init}}^{p_{final}} \frac{T_p}{N_p}$$

p_0 is the first mortgage interval for the validator

When a miner needs to mortgage mining, it will create a data structure $entry_f$, $entry_f$defined as

$$entry_f = \sum_{i=0}^{f} \frac{T_i}{N_i} = \sum_{i=0}^{f-1} \frac{T_i}{N_i} + \frac{T_f}{N_f} = entry_{f-1+} \frac{T_f}{N_f}$$

One $\mathbf{entry_f}$ is created for each change in the number of collateralized verification nodes. Then the miner creates a miner in the interval **k**, and submits the income in the interval **f**, the income he should withdraw is

$$x \sum_{i=k+1}^{f} \frac{F_i}{N_i} = x\left(\sum_{i=0}^{f} \frac{F_i}{N_i} - \sum_{i=k}^{f} \frac{F_i}{N_i}\right) = x(entry_f - entry_k)$$

BAC Chain will store the cumulative reward $\mathbf{entry_f}$ for each unit **i** mortgage amount from interval 0 to interval k. In this way, when processing each miner's reward, there is no need to iterate each block, reducing computational complexity.

6.3.2 BFT consensus process

There are two roles in the agreement:

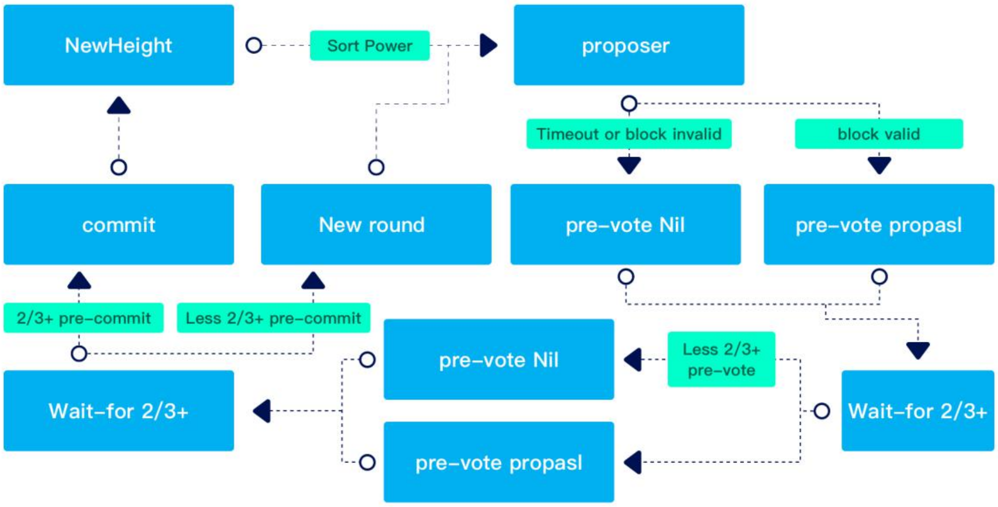
A. Verifiers: Different verifiers have different powers (power) during the voting process. Power comes from their own mortgage and mining machine delegation

B. Proposer: The validators take turns.

The validators take turns to propose and vote on the blocks of the transaction. Blocks are submitted to the chain, and each block is a block height. However, the block submission may fail. In this case, the protocol will choose the next validator to propose a new block at the same height and start voting again.

The validator selects the proposer according to the power ratio. The proposer proposes a block proposal (Block Proposal) for the current height. Each block corresponds to a height. After all validators receive the Block Proposal, they will initiate a pre—vote vote. When the node receives

After more than 2/3 of the validators have pre—vote the same block in the same round of proposals, they will enter the pre—commit stage. When the node receives more than 2/3 of the validators in the same round of proposals, the same After the block has been voted pre—commit, it is determined that the block has been approved by more than 2/3 people, and the block will be committed



6.3.2.1 Block Proposal process

The node selects the node with the largest current power as the block producer according to the state of the previous round. The node will collect transactions from the local transaction pool, encapsulate it into a block, and then broadcast the block into the proposal. Due to offline or network delays, the proposer may fail to propose a block. This situation is also allowed in the consensus, because the validator will wait for a certain time before entering the next round of proposals to receive the block proposed by the proposer. This process is equivalent to the pre—prepare phase of pBFT.

6.3.2.2 Pre—Vote process

When a node collects a complete proposal, it will verify the correctness of the block in the proposal, and then pre—vote the block. If the node does not receive the proposal within the proposal time, it will post it An empty ticket. The node collects the pre—vote votes of other nodes during the pre—vote time period, and enters the pre—commit stage when the node obtains more than 2/3 of the pre—vote. Entering this process is equivalent to the prepare phase of pBFT. The goal is to prevent the prosoal node from being a BFT node.

6.3.3.3 Pre—Commit process

When the node gets more than 2/3 of the pre—vote votes, it will enter the pre—commit stage. The node will cast pre—commit votes. If the node does not receive more than 2/3 of the votes in the pre—vote, it will Nil tickets are delivered in the pre—commit stage. At this stage, the node will collect the pre—commit votes of other nodes. If more than 2/3 of the votes are collected, the node will commit the block and modify the power value of the verification point. This process is related to the commit phase of pBFT. The goal is to commit the block when more than 2/3 of the nodes have agreed to commit the block.

6.4 Cost model and incentive system

The cost model and incentive mechanism are important guarantees for stimulating the entire participating ecosystem, and are essential for the safe and stable operation of the main network.

6.4.1 Block rewards

BAC Chain uses a similar Bitcoin reward model, with an initial reward of 10 BAC per block, which is halved every six months. The detailed rewards are as follows:

Time	Number of awards per block	Total number of awards perday	Total number of awards granted	Halving at the Height
First six months of first year	10	132920	24275070	2427508
Last six months of first year	5	66460	36412605	4844015
First six months of second year	2	26584	41267619	7282522
Last six months of second year	1	13292	43695126	9710029
Third Year	0	0	43695126	

6.4.2 On—chain transaction gas consumption

On—chain transaction gas can also be adjusted according to the governance requirements of public chain verification nodes, and the settings are now as follows:

Iterative operation	1000nbac
Write operation per byte	30nbac
Write operation	2000nbac
Read operation per byte	3nbac
Read operation	1000nbac
Delete	1000nbac
Existential judgment	1000nbac

6.4.3 Transaction hash gas consumption

Every transaction executed requires gas, and the gas consumed by this transaction is equal to the sum of the operations executed by this transaction.

6.4.4 Verifier delegation

The validator needs to pledge bcv to exchange into bcvstake when it is created, and these bcvstakes can be exchanged back and converted into bcv again.

6.4.5 Mining machine mining and destruction

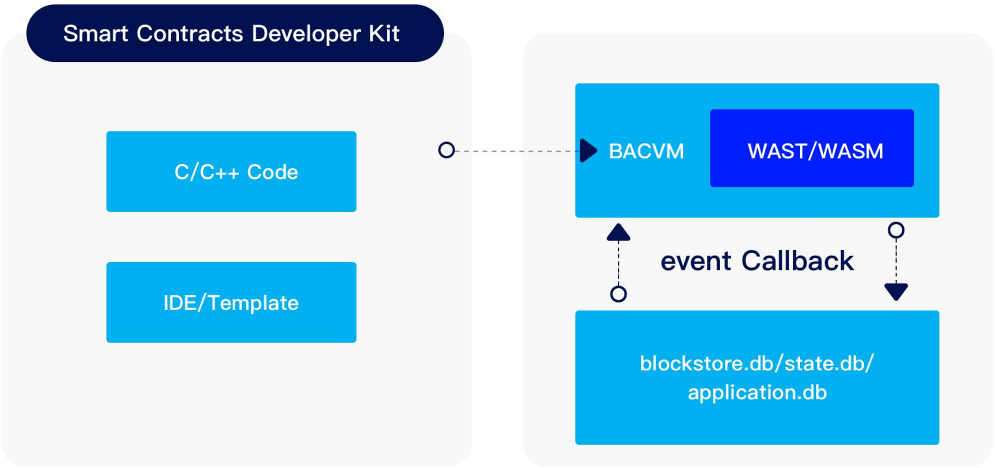
The miner needs to destroy bcv and replace it with bcvstake when it is created, and the bcvstake cannot be redeemed.

6.4.6 Destruction of mining energy

Mining requires energy (energy), and the mining machine consumes electricity during the mining process. 1 bcv stake 1 highly consumes 1 energy, and users can destroy bcv to exchange energy.

6.5 Smart Contract

Smart contracts are essential to the financial management public chain. BAC Chain smart contracts not only have the basic characteristics of Turing complete, flexible, safe and reliable smart contracts, but also provide an ecologically friendly contract engine BVM. BVM provides execution security, performance, and multi—language support for contracts through webAssembly and oracle technology. The smart contract execution is as shown below:



6.6 Oracle

The BAC ORACLE module is the realization of the oracle, which is mainly divided into an internal oracle and an external oracle. The oracle establishes a readable channel for smart contracts and data. BAC ORACLE uses a pre—defined configurable oracle, and smart contracts can ensure that only when the smart contract verification conditions are met will the real value transfer occur, and at the same time, the smart contract can interact with external data. At the same time, disputes can be avoided in accordance with the performance of the agreed contract rules. Pre—machine smart contracts can support any JSON API type.

6.7 Governance

BAC Chain allows any user holding bcvstake to participate in the common governance of the public chain and the common governance of the blockchain. Bcvstake can be obtained through bcv mortgage or destruction. Bcvstake holders can submit proposals by signing special types of transactions or indicate whether they support (or do not support) proposals submitted to the blockchain network. Governance is mainly divided into the following steps

6.7.1 Deposit stage

Any holder of bcv tokens can initiate a proposal. For proposals that want to enter the voting stage, they need to deposit at least 1000 bcv tokens within two weeks after submitting the proposal. This is the minimum deposit amount to enter the voting stage Claim. In addition to the proposal initiator, others can also send a deposit transaction to provide deposit for the proposal. After the proposal is created, it can be queried, and users can query the progress of the proposal through the browser. When the proposal meets the deposit requirement within the specified time, the proposal will be approved. If the requirement is not met within the specified time, the proposal will be rejected.

6.7.2 Voting stage

Once the proposal meets the minimum deposit requirement, the proposal will enter the voting stage for a certain period of time. During this period, all mortgage miners, that is, holders of bcvstake, can vote on the proposal. There are currently four voting options, namely "Yes", "No", and "No with Veto" ", "Abstain."

The number of holdings of bcvstake determines the influence on the proposal decision. The miner can inherit the verifier's vote. If the miner does not vote, the verifier's vote will override the verifier's decision.

6.7.3 Voting results

After the proposal is accepted in the voting stage, the vote must at least meet the following conditions to be accepted.

More than 40% of bcvstake voted

More than 50% of bcvstake needs to support the proposal (that is, the result of the selected vote is "Yes");

Less than 33.4% of bcvstake exercised the "No with Veto".

If any of the above requirements are not met at the end of the voting period, such as the quorum is not reached, then the proposal cannot be passed. If the proposal is not passed, the deposit of the proposal will not be refunded and will be included in the community pool. If it is passed, the deposit will be refunded.

The governance of BAC Chain is still in the early stage and will be gradually improved following the opinions of the ecological community.

6.8 Data storage

The distributed ledger of the blockchain is limited to storing simple transaction data, and cannot store excessively large documents. For example, complex data streams such as transaction history and historical data require dedicated storage space, especially for unstructured documents. Direct storage on the blockchain, rather than structured documents, such as contract electronic file backups, deposit images, are closely related to the data on the blockchain in business. In order to support the association of data and related unstructured documents on the chain, and realize the rapid storage and query of data, we introduced the traditional distributed file system to associate with the blockchain system, forming a "scalability" and "decentralization" "Open storage agreement.

For a transaction on a blockchain, if a related document exists for the transaction, the MD5 Hash value of the document is placed in the transaction record and stored in a special field.

When reading the record, first read the data on the chain, then locate the distributed file system according to the hash value in the transaction record, read the content of the document, and verify the consistency of the document while reading it. In the case of ensuring that the Hash value matches, it means that the file is a correct file and it is safe and reliable.

Using a distributed file system is the first step, and the second step can also further store files in decentralized file storage projects, such as IPFS and Lambda and other services provided by projects.

6.8.1 Privacy data protection

Data is the most important production resource in the future, as well as the most important hidden asset for individuals and enterprises in the future. How to store and circulate such hidden assets efficiently, reasonably and safely is also one of the key issues that the BAC Chain public chain must solve. BAC Chain will continue to explore the problems of privacy leakage encountered in the storage and circulation of private data

6.8.1.1 Data encryption storage

BAC Chain encrypts user data outside the chain with a private key and stores it in a file system with multiple copies such as ipfs or hdfs, and then generates a file hash using cryptography and adds it to the BAC Chain main chain, which can reduce the storage resources of the main chain. Use can also give data a choice in private storage and public access.

6.8.1.2 Authorized access to data

Asymmetric encryption and decryption technology ensures that during data transmission, only the two parties holding the private key can decrypt the content, thereby ensuring that the third party cannot intercept and blast the content. BAC Chain uses ECDH to calculate the shared key between two pairs of public and private keys, so that the account can be authorized to access.

6.8.1.3 Private data exchange

BAC Chain can consider the following solutions in different scenarios:

6.9 Secure Multi-Party Computing (MPC)

It was formally proposed by Yao Qizhi in 1982. It mainly discusses that n participants input information to calculate a predetermined function, while ensuring the correctness of the calculation, it does not reveal the privacy of the participants' input data. Specifically, for n participants, each participant i knows its own input xi, and they want to jointly calculate a predetermined function f(x1,...,xn) = y, so that all participants can obtain the final The result of y, but the input data of other participants cannot be obtained.

6.9.1 Homomorphic encryption (HE):

Homomorphic encryption is an encryption method that allows calculations on ciphertext. In addition to the original components of the traditional encryption scheme, there is another calculation algorithm that takes the objective function F and encrypted data as input. Homomorphic encryption generates an encrypted result. When decrypting this result, the obtained message is like performing F on the plaintext of the encrypted data. A cryptographic system that supports arbitrary calculations on ciphertext is called Fully Homomorphic Encryption (FHE).

6.10 Supervision

6.10.1 Community supervision

BAC Chain selects a type of supervision node through voting and election. The supervision node will supervise the operation of the entire main network and crisis management. For example, in the case of currency theft, the stolen can declare to the supervisory node that the stolen currency account is temporarily blocked, the supervisory account sends a specific transaction, and the transfer function of the stolen currency account is suspended. The verification node will execute the transaction after receiving the transaction. Currency accounts will be temporarily frozen. The supervision node is mainly used for emergency handling of crisis situations.

6.10.2 Policy supervision

The decentralization of the blockchain is the advantage and limitation of the blockchain. In the current situation, the users of the blockchain do not care whether the security of the business is endorsed by the decentralized blockchain or by the policy rights. The blockchain also needs to be supervised by the industry and policies. , BAC Chain accepts policy supervision through privacy authorization access method.

6.11 Security

6.11.1 Man-in-the-middle attack

A man—in—the—middle attack is a long—standing network intrusion method. Attacks such as SMB session hijacking and DNS spoofing are typical MITM attacks. The principle is that by intercepting normal network communication data, and performing data tampering and sniffing, the communicating parties cannot know. BAC Chain uses a protocol similar to Station—to—Station (STS) to establish a shared key when establishing communication between nodes. Messages will be encrypted using this key, which can effectively avoid man—in—the—middle attacks.

6.11.2 Double spend attack

Double—spending attack means that when z blocks have passed after a transaction is issued, the attacker regenerates a new blockchain in a very short time, making the new chain faster than the previous one , So that the attacker can retrieve the virtual currency spent in the previous transaction and use it for the second transaction. Because in the blockchain, the system will automatically recognize the longest chain as a valid chain. BAC Chain uses a consensus protocol similar to pbft. Once the consensus is reached, it cannot be changed, which can effectively avoid this problem.

6.11.3 Witch attack

Sybil attack refers to the use of a small number of nodes in a social network to control multiple false identities, thereby using these identities to control or affect a large number of normal nodes in the network. BAC Chain uses bcvstake as the right currency. Only by holding the currency can you obtain the corresponding income and execute related transactions, so the double—spending attack will not pose a threat to BAC Chain.

6.11.4 Fork Attack

Fork attacks are when attackers obtain computing power directly or indirectly, allowing them to help them fork the longest blockchain. When BAC Chain handles the mortgage relationship, if a validator's mortgage amount is too large, the miner's mortgage will be rejected, which can effectively prevent a validator from having excessive rights.

6.11.5 DDos attack

Denial of service attack (DDOS), also known as flood attack, is when an attacker uses a compromised computer on the network as a "zombie" to launch a "denial of service" attack to a specific target. The purpose is to exhaust the target computer's network or system resources. , The service is temporarily interrupted or stopped, causing its normal users to be inaccessible. BAC Chain can be in sentinel mode, shielding the back—end node server, effectively protecting the block machine, avoiding or reducing DDos attacks.

6.11.6 Quantum Attack

The non—symmetric cryptographic signature algorithms commonly used in previous blockchain systems, such as the RSA algorithm based on the integer factorization problem and the ECC algorithm based on the discrete logarithm calculation problem on the elliptic curve, can be measured by the Shor algorithm. The NP problem becomes the P problem, which is never easy to crack. The BAC Chain system will promptly introduce anti—quantity calculations based on the progress of the project and the development of computer practicality to crack encryption algorithms, such as Lattice—based cryptography, a code—based cryptography system (Code based cryptosystems) and multivariate cryptography; among them, various cryptographic systems such as encryption, signature, key exchange, etc. can be designed based on lattice cryptography, which is an important aspect of post—quantity cryptographic algorithms. At the same time, we will also follow up on the cutting—edge research directions of the amount of cryptographic systems.

6.12 Extension

With the development of business, if you want the public chain to truly achieve deeper application and popularization, the public chain will eventually encounter a key problem and bottleneck, which is to solve the problem of transaction throughput and transaction speed. This is in the block The chain is also called scalability, and BAC Chain will continue to explore the implementation of various scalability solutions below the public chain.

6.12.1 Single-chain scalability

Assuming that each transaction is 200Byte, under 10Mbps transmission bandwidth, the throughput can reach 6000Tps, the Tps of ordinary hard disks can reach more than 10000Tps, and the Tps of ordinary CPUs can reach 8000Tps. At present, the Tps of mainstream public chains are far from being reached. Use optimized The data structure and algorithm may further mine the performance of the single chain and increase the Tps of the public chain.

6.12.2 Side chain technology

SideChains are proposed for Bitcoin, so this concept is more about Bitcoin—related expansion in the later period. Its definition is: Bitcoin can be safely transferred from the Bitcoin main chain to other blockchains. , An agreement that can safely return to the Bitcoin main chain from other blockchains. The side chain is an independent system, an isolated environment, even if there are internal problems, it will not affect the original system.

6.12.3 Fragmentation

Sharding is to divide the blockchain network into several smaller networks that can handle transactions. Each small network can process transactions that have not established connections in parallel to increase the amount of concurrency in the network, so that the number of nodes increases.

6.13 BAC's supporting ecology

The current blockchain technology does not lack various improvement ideas, but the most lacking is application. Technology without application scenarios, there is no future. Many public chains only consider technology implementation. After the main network is launched, there are no application scenarios, no users, and no use or creation of value at all. Therefore, it lacks value support and cannot motivate participants to participate for a long time.

As the ecology of the public chain, nodes and miners themselves are motivated to maintain the basic operation of the entire public chain. As for the ecology of applications, we mainly separate from the following three roles:

6.13.1 Developers

After the main network of the public chain runs, the development of public chain applications based on the underlying public chain requires the public chain and developers to build a developer ecosystem in both directions. The public chain development team needs to open source the public chain code, provide mainnet services to call APIs, SDKs for various languages and services, supporting development and testing tools, and of course documents for all these technical tools. These contents can also be completed by the developer community. Developers develop various applications based on the basic functions of the public chain and end—user—oriented business needs, including tools, games, finance, and evidence—based scenarios. BAC Chain will provide complete documents, tools, SDKs, etc., based on the wallet, to provide developers with convenience.

6.13.2 Users

The applications developed by developers must provide services to users. Developers can gain user growth with their own service value. However, if there are a large number of users and application scenarios in the public chain ecology itself, it will provide developers with important motivation and motivation to develop applications based on the public chain. Experimental scenarios, so users are also a very important part of the public chain ecology.

Both the BAC Chain ecology and the BCV wallet are members of the BCV ecology. The BCV wallet provides users and traffic support for the BCV ecology with millions of users. The BAC Chain application developed by the developer can be given priority to the users of the BCV wallet. , The public chain enriches the applications of users for BCV Wallet, and BCV Wallet provides developers with a low—cost experimental environment and convenient circulation channels.

Chapter 7 Technology Roadmap

7.1 Mainnet launch in April 2020

The mainnet goes online stably, realizing that users who hold BCV can mine to obtain BAC. BAC can support the circulation of the main network as a payment fee.

7.2 Store online in July 2020

The storage network and other supporting storage facilities are online, combined with the main network to consider the storage economic model, and support users to store data for a long time.

7.3 Promote open source and start applications in August 2020

Realize the support of multiple language development kits, and open the source code of the public chain. Begin to explore existing wallet and exchange businesses, such as on-chain such as account asset verification, to achieve transparent operations.

7.4 Realization of decentralized transaction agreement in November 2020

The decentralized transaction protocol is the foundation of asset management and lending business on the chain.

7.5 January 2021 Built—in contract to realize DeFi business model

Realize the built—in contract function, realize the loan, fund and other models in the form of built—in contract to realize the support for the DeFi business on the pure chain.

7.6 June 2021 smart contract goes live

The smart contract development is completed, and some migration explorations are made for businesses suitable for smart contracts.

7.7 Mainnet expansion after 2021

Strengthen the experience of running business on the main network, consider sharding, layering, side chain, cross chain and other expansion of the main network, and use mature technical means to achieve business goals.

Chapter 8 References

[1] NAKAMOTO, S. Bitcoin: A peer—to—peer elec— tronic cash system, 2008. http://bitcoin.org/ bitcoin.pdf.

[2] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 1982.

[3] A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER https://ethereum.github.io/yellowpaper/paper.pdf

[4] Vitalik Buterin. Ethereum: A Next—Generation Smart Contract and Decentralized Application Platform. 2013a. http://ethereum.org/ethereum.html

[5] CRYPTOKITTIES. Cryptokitties, 2017. https:// www.cryptokitties.co.

[6] cosmos white paper https://cosmos.network/resources/whitepaper/zh—CN

[7]Slasher: https://blog.ethereum.org/2014/01/15/slasher—a—punitive—proof—of—stake—algorithm/

[8] PBFT: http://pmg.csail.mit.edu/papers/osdi99.pdf

[9] TheDAO: https://download.slock.it/public/DAO/WhitePaper.pdf

[10] 0x protocol: https://0x.org/docs

[11] uniswap:https://uniswap.org/docs/v2