BYSTACK

The Unique Mainchain-sidechain

Model BaaS Platform

Introduction

Blockchain technology has evolved rapidly for more than four years since 2015 when people discovered its huge potential. In the past four years, blockchain has become an innovative technology recognized and respected by fintech industry and government. Many technology and financial giants around the world have invested a lot of manpower and resources and a number of outstanding startups have emerged in the industry. However, blockchain technology is far from reaching the mature stage. Although the entire blockchain industry has its own merits and drawbacks, we are all aware that the pioneers find it hard to integrate blockchain technology into real applications on a massive scale. Given the dilemma, the Bytom team is proud to present Bystack, a blockchain solution designed for large-scale applications and optimizing consensus mechanism, smart contract, scalability, privacy, security and cross-chain interoperability.

Bystack is an enterprise-level BaaS platform that helps users to quickly deploy, manage and maintain blockchain networks and commercial blockchain applications. Its features include low development cost, fast deployment, high performance and scalability, security, reliability and ease of use.Bystack is a one-stop blockchain solution for developers and businesses.

The unique mainchain-sidechain model and Blockcenter system proposed by Bystack simplify and assemble the underlying blockchain infrastructures including network, consensus mechanism, development capabilities. In this way, Bystack offer users with familiar programmable interface and operator interface without bothering the underlying technical nuances, making application development simpler and more efficient, allowing companies and developers to focus more on the development side.

1 Preface

1.1 The goal of blockchain technology

Since blockchain was first introduced by Bitcoin, this technology itself has evolved into a wide variety of architecture in different forms, including public blockchain, consortium blockchain and private blockchain in terms of permission, PoW, PoS, DPoS and PBFT in terms of consensus mechanism, UTXO model and account model in terms of underlying model, and blockchain and DAG in terms of underlying ledger, and cross-chain and sidechain technologies.

Regardless of its presentation, all types of blockchain want to build a trustless, highly reliable, ready for use, immutable business system through its unique consensus algorithm, cryptography and distributed data storage to achieve blockchain application in real life.

1.2 Overview and problems of current commercial blockchain platforms

There are many commercial blockchain platforms on the market. They are designed to cut into the commercial and financial application scenarios with the advantages of reliability, serviceability, easy-to-use, one-click deployment, fast verification, flexible and customizable blockchain solutions. However, the incumbent blockchain platforms, in its essence, provide only cloud-based interface without disclosing source code, which is not transparent and open to users. Blockchain explorers are also usually close to the average user. Therefore, a large, free and open source practice blockchain platform is missing for community developers.

In addition, when creating blockchain solutions for enterprises, the impossible-trinity[①] is a first-principle problem, which means only two could be achieved among decentralization, security, and scalability (efficiency). If security is an indispensable attribute of all blockchain- as-a-service (BaaS), then the blockchain impossible-trinity could be reduced to a binary paradox of decentralization and efficiency. Decentralization of the public chain could be achieved but its TPS cannot meet the needs of large enterprise applications. Consortium blockchain and private blockchain are highly scalable but centralized, which means immutability and irreversible

① 《Impossible-trinity:Security, Environmental Protection and Decentralization》

transaction is in doubt.

In light of the stacking experience of the Internet TCP/IP protocol, a layered model may solve the blockchain binary paradox while building a complete commercial application architecture.

The first design principle of layering is the hierarchical stack. Each abstraction layer is created on the service provided by the lower layer, and provides services for the upper layer. That is , the lower layer does not care about running state of the upper layer, but the upper layer needs to understand the lower layer implementation.Completing some specific tasks requires a multitude of protocols working together. These protocols are distributed in different layers of the reference model, so they can be called a protocol stack.

The second design principle of layering is that the layers are independent and serve different functional requirements. In the TCP/IP protocol, the IP protocol only cares about how to make data cross the local network boundary, and the TCP protocol deal with how the data is reliably transmitted is in various networks. In reflection, blockchain needs different protocol layer to solve the problem of consensus, transaction efficiency, and business implementation.

Therefore, we propose to divide blockchain applications into three-tier architecture: the underlying ledger layer, the sidechain extension layer and the service adaptation layer . The core is Layer1 (the underlying ledger layer) and Layer2 (the sidechain extension layer). Layer1 creates a permissionless environment that guarantees decentralization and focuses on billing functions, which is the basis for transaction security and data immutablity. Layer2 is responsible for transaction efficiency, focusing on business capabilities, providing fast and powerful service access capabilities, passing the value of Layer1 to the actual business, and returning to Layer1 through relay. These two layers complement each other and have both decentralization and efficiency (Figure 1).
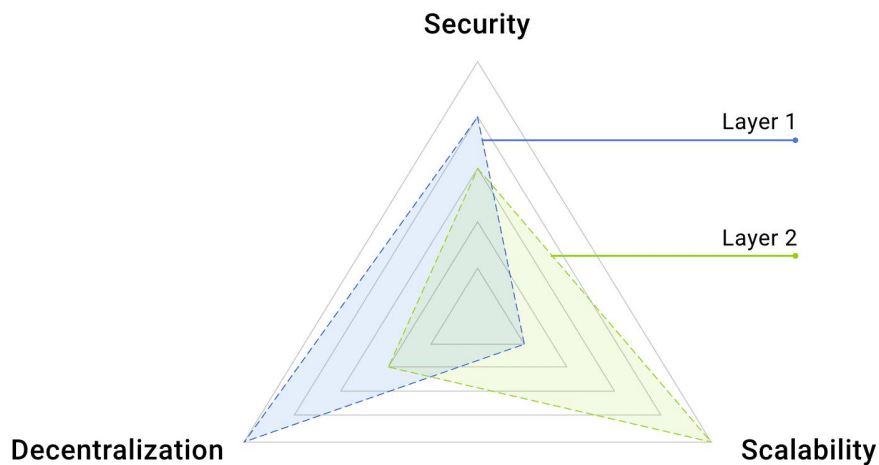
Figure 1

The industry has divided blockchain system into a settlement layer and a computing layer. The token runs on the settlement layer and is the basis of the whole system. The computing layer provides functions such as smart contracts, identity authentication, and message communication to facilitate developers to develop applications. However, the above solutions do not support different business scenarios very well. For example, the demands for blockchainized assets like equity and business royalty are different. Royalty does not require the real identity of users while equity registration do. Besides equity structure is subject to the provisions of the "Company Law" such as "the number of shareholders cannot exceed 200 ". A single Layer 2 cannot be used in all business scenarios like Layer 1. To this end, Bytom team innovatively proposed a BaaS architecture with a mainchain-sidechain architecture - Bystack , in which Bytom mainchain acting as Layer1 with access to different Layer 2 sidechains according to different business scenarios .

2 Mainchain-sidechain collaborative working model

Bystack's solution is a mainchain-sidechain (one mainchain plus multiple sidechains) collaborative working model. The mainchain uses PoW consensus to ensure the security and decentralization of diverse assets. The sidechains implement different solutions through pluggable technologies to meet the needs of different business scenarios.

The mainchain-sidechain protocol is essentially a kind of cross-blockchain solution. This solution allows for the transfer of digital assets from one chain to another and vice versa. In Bystack , the blockchain network that creates and stores assets is often referred to as the mainchain, while the assisting chain is called sidechain. The sidechain protocol is envisioned as a way to allow digital assets to be transferred between the mainchain and sidechains.

Bystack 's mainchain needs to be secure and stable, so performance, scalability and more innovative attempts will be implemented on the sidechains.

2.1 Mainchain-sidechain architecture

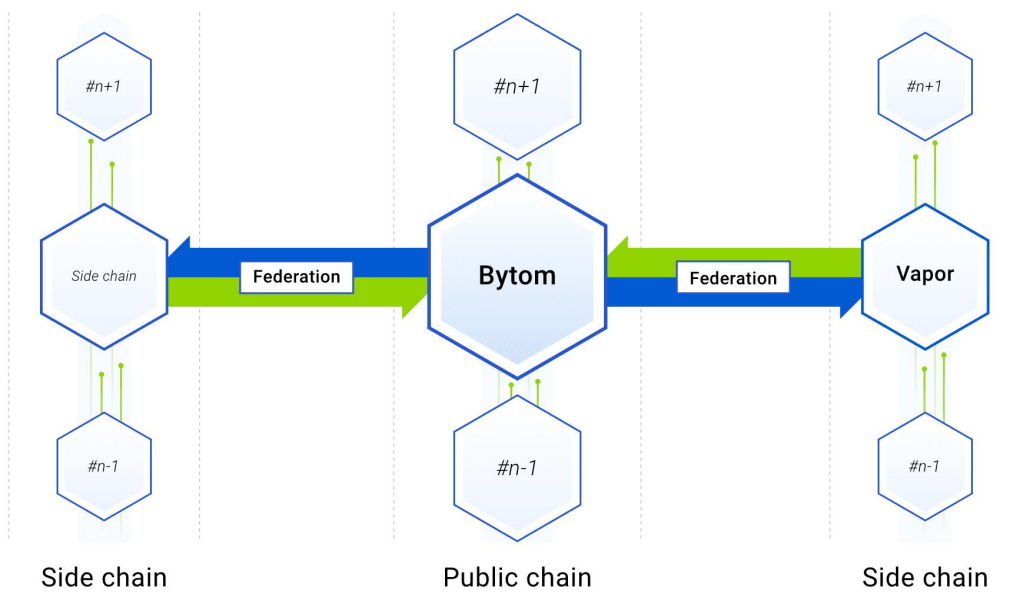The following figure is a general model diagram of the mainchain-sidechain synergy:

Figure 2

2.1.1 The role of mainchain

Bystack 's mainchain is Bytom blockchain, which is based on the AI-friendly PoW (Proof of work) algorithm Tensority. The mainchain is primarily responsible for value anchoring, value transfer and trusted deposit. Any asset creation, transmission and destruction are initiated by the mainchain and then pegged into sidechain through Federation. At the same time, all the digital

fingerprint information of business or assets are stored in the mainchain as only the mainchain guaranteed by computing power can be credibly verified.

2.1.2 The role of sidechain

Bystack 's sidechain is mainly for services in the vertical domains, and meets those services that have higher requirements for TPS and data storage. At the same time, sidechains support a more flexible deployment method. Enterprise or individual can use existing sidechains, or can generate their own sidechains and build their own applications on sidechains. Assets on mainchain is pegged to sidechain through Federation and then circulated within the sidechain. The sidechain supports pluggable consensus, database plugins, which can be better matched to meet actual business needs.

2.1.3 Federation

The following figure is the basic model diagram of Federation .
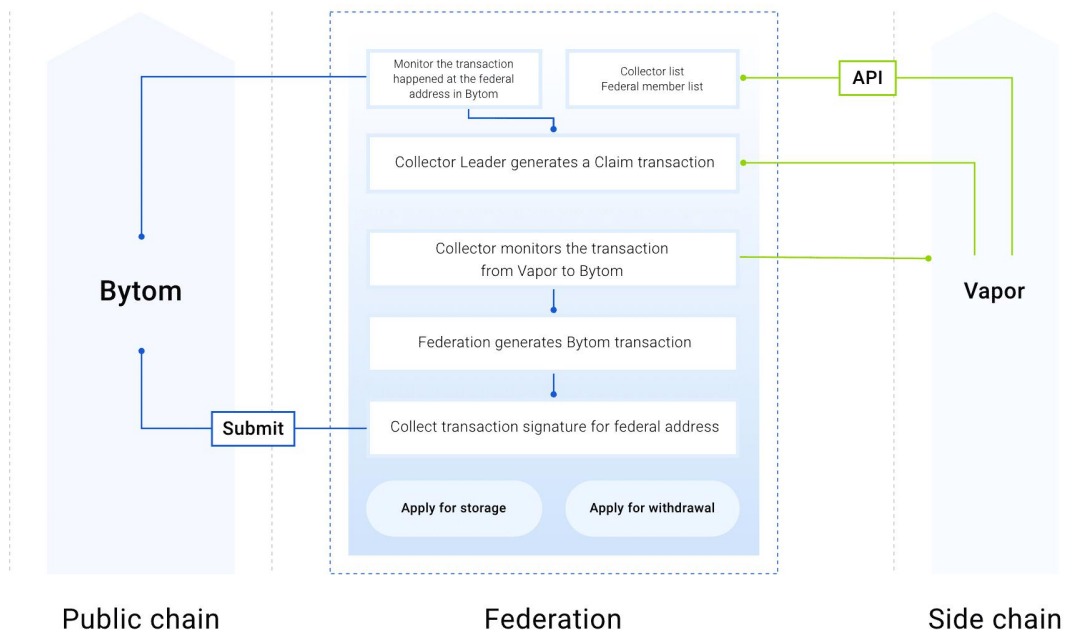

Figure 3

There are three roles in Federation :

Validator: the block producer of sidechain, Anyone can be a validator

Collector: Monitors the transaction that the mainchain locked in federation contract address, collects transactions and generates Claim transactions, sends them to the node validatior for verification and enters the mempool.

Federal address: Sidechain deposit refers to the transfer of assets from the mainchain to the sidechain, which requires the asset to be locked to the federal contract address first.

Generation of Federal contract address:

（1）The generation of Federal contract address requires public key of multiple federal members, and the system begins to be initiated by the initial block producer.

（2）After running for a period of time, users on the Vapor sidechain can register as a candidate of federal member. Then the Vapor sidechain users vote to select a federal member from the registered candidates. Each time the number of federal member that changed cannot exceed one third of the total number.

（3）After the federal member is elected, the new federal member generates a new contract address, and the previous federal contract address is transferred to the new federal contract address.

（4）After the transfer is completed, the mainchain will lock assets to the new federal address for the next run for the federation membership.

Collector:

（1）At the time of system boost, collector is undertaken by the initial block producer.

（2）After running for a period of time, the users on the Vapor sidechain can register as a candidate collectors, and the Vapor sidechain users vote to select the collectors from the registered candidates（voting starts over after one round of DPoS minting).

（3）Issue the new collector, who watch the Federal contract address on mainchain, initiate

Claim transaction with info like the list of collector, collector's signature, original transaction, and the public key of collectors.

Sidechain withdrawal process:

(1) The Vapor sidechain user initiates a withdrawal request, the assets on Vapor sidechain is burned.

(2) The federal contract address send the corresponding number of assets to the mainchain address of the Vapor sidechain user (provided the transaction on sidechain has been confirmed and cannot be rolled back) .

(3) The federal generates a transaction on the sidechain that completes the withdrawal operation.

2.1.4 Innovation

(1) Consensus layer innovation

Sidechain achieves consensus with voter (Voter), consensus node (Delegate) and leader node (Leader) to organize the network. First, Delegate is voted through DPoS, and then Delegate achieve consensus efficiently by a unique BFT model.

(2) Network layer innovation

The traditional consortium blockchain is the master-slave node architecture, even the C/S model. The server will implement the complete protocol and the client will be as compact as possible, focusing on product features and interactions. Unlike slave node that does not participate in consensus or even verification, sidechain can completely preserve the functions of the peer node, thus requiring a faster network, more reliable transmission of transaction and block data in a more complex environment.

Vapor Neuron Relay (VNR), based on the UDP and Forward Error Correction (FEC) protocol , can transport block header, compacted transaction ID and transaction information that are not available to some peer nodes.   The receiving node will attempt to use the information received, and the transaction in the local memory pool (Memory Pool) to reconstruct the entire

block. The broadcast of peer node transaction is requested only if certain transactions are still missing.

(3) Protocol layer innovation

Restrained by the serial verification model, Ethereum find it difficult to increase the throughput. Based on BUTXO protocol, Vapor can verify blocks in parallel in multiple threads. The Parallel Sliding Windows Validation algorithm (PSWV) can synchronize hundreds of blocks simultaneously and obtains all its inputs. The block batch forms a verification window and the algorithm verifier slides to verify the validity of the block transaction in the window.

(4) Storage layer innovation

The local KV database like LevelDB and RocksDB, which are commonly used by the public chain, is replaced by a more powerful database interface to meet the needs of MySQL , PostgreSQL, MongoDB and other enterprise-level databases. In addition to the needs of data analysis, the storage layer is compatible with HDFS, HIVE , and integrates into the Hadoop or Spark ecosystem.

2.2 Assets and Operation Types

2.2.1 Types of Asset

Multiple types of asset issuance is a major feature of Bystack. We define 4 types of assets in terms of the asset's Severability and Fungibility[2] (Figure 4):

1, Byte assets (BAP-01), divisible and fungible. mirrors virtual assets like tokens and real assets such as currency, royalties, equities(equal voting right), which is equivalent to the Ethereum ERC-20 protocol.

2. Atomic assets (BAP-02), divisible but not fungible. It refers to real assets such as Bytom's native asset BTM or other stocks issued through BAP-02 (weighted voting right) and is equivalent

[2] Fungibility：Something (e.g. an asset or commodity) that has an attribute that, when paid or settled, can be replaced by another equal part or quantity.

to non-homologous cryptocurrency protocol such as Bitcoin.

3. Quark assets (BAP-03) indivisible and not fungible. It's appropriate for virtual assets like game items, game pets, collectibles, merchandise, security code etc and is equivalent to ERC-721 protocol.

4. Quantum assets (BAP-04), indivisible and fungible. It can be applied to virtual assets such as red envelopes, as well as voucher-like assets such as coupons, tickets, and QR codes. ③
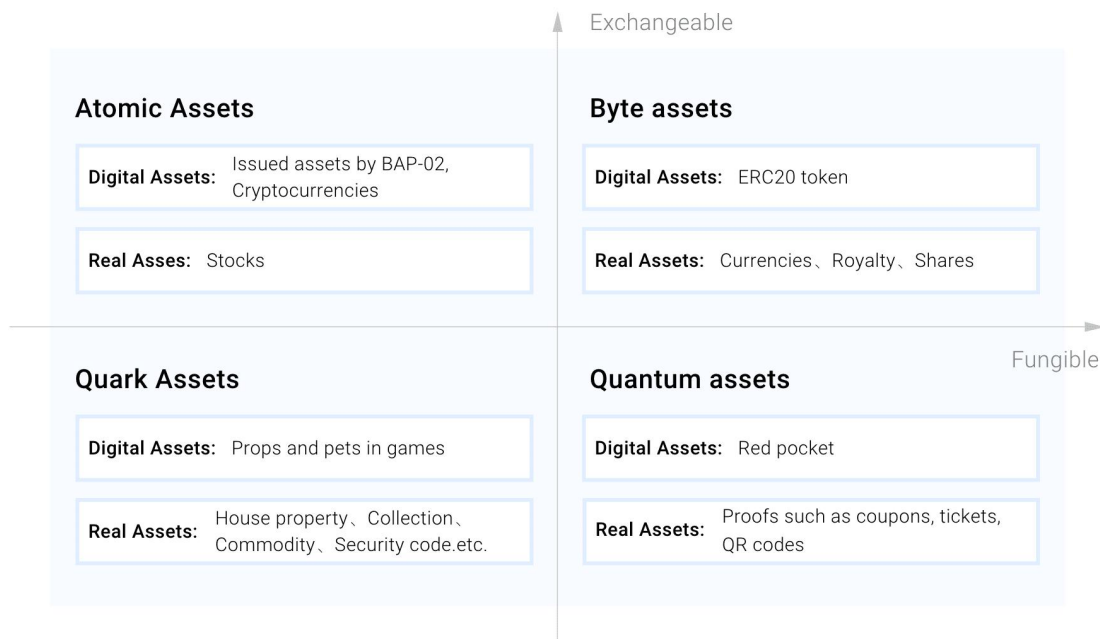

Figure 4

In fact, we did not invent new assets, but tried to map the real world assets in the world of blockchain and give a more basic classification of assets from the perspective of physical attributes in order to facilitate people in asset classification in scenarios like finance, governance, gaming, royalties.

2.2.1 Type of operation

Bystack defines interoperability between assets as four types:

③ BAP: Bytom Asset Protocol

Mapping: Asset digitization, assets in real life such as equity, IOU, income rights and other assets are registered on blockchain.

Deposit certificate: digital assetization, credit, identity, branding, behavioral data and other digital resources are stored on blockchain. Ownership and rights of use are transferred through blockchain.

Pegout: Assets are moved from the sidechain to the mainchain.

Pegin: Assets are moved from the mainchain to the sidechain.

All of the above operations are atomic operations, which means they are either executed completely or not existing at all. There is no possibility of asset loss or fraud.

2.3 Deployment and Use

Local deployment: For individual developers, users can deploy their own sidechains on the server and then test their own commercial applications on their sidechains.

Cross-cloud deployment: For enterprise users, the enterprise's sidechain can support a variety of cloud services, including Alibaba Cloud, Tencent Cloud, Huawei Cloud, and so on. Nodes of the blockchain can be deployed to different public cloud platforms.

Hybrid deployment: In order to meet different business needs, blockchain nodes can be deployed according to the requirements of the alliance participants, that is, some of the sidechain nodes run on the cloud platform, and some of the sidechain nodes run on the client's private IT environment or private cloud.

3 Consensus network

In the mainchain-sidechain model of Bytom, the mainchain mainly adopts Tensority PoW consensus algorithm④, the sidechain provides pluggable consensus to meet different business needs. Meanwhile, Bystack itself also created a unique consensus algorithm based on

④ 《 BYTOM: An interoperational protocol for diversified byte assets》

DPoS+BBFT, which will be elaborated in this chapter .

3.1 Network level

3.1.1 DPoS

The principle of DPoS is to let each token-holder vote and select a certain number of delegates, or a certain number of representative nodes. These representative nodes can complete the transaction verification and block production work. Holders can change these representatives at any time by voting to maintain the "long-term purity" and ensure that the agreement is properly decentralized.

In the incumbent blockchain model, the DPoS consensus is only used for the account model. The combination of the UTXO model and DPoS also has many additional advantages. The UTXO model is a way to storage for transaction storage, organization and verification; DPoS is a consensus algorithm used to ensure that participants in a distributed network can achieve consensus regarding transaction data.

One major obstacle in integrating UTXO and DPoS is the timestamp. DPoS is based on time and will run strictly check of the block time. The system time of full nodes must be set to be the same as the standard time, otherwise there will be problems with consensus consistency. UTXO itself also have timestamps, but which are not based on standard time. In LBTC, timestamp is unified as per the standard time protocol to ensure the normal block generation. When there are evil nodes or unsynchronized blocks, the block is often orphaned and its nodes marked as exceptional node.

In the UTXO model, the function of querying the address balance is not supported. The global traversal is performed upon UTXO data to calculate the address balance in real time. Such computing work is quite large and it is not feasible in reality. In order to meet the needs of DPoS , Vapor adds new functions such as address balance calculation, node registration, node. In view of the high performance requirements and the limited number of registered nodes, the address balance, node registration and voting information are stored in the memory, and the data is written back to the database. UTXO and DPoS are connected through database and address balance,

voting information.

The information for registration and voting is transmitted via the Vapor protocol and stored in the memory and the database. DPoS will looks at the registration and voting information and completes consensus.

3.1.2 BBFT（Bystack Byzantine Fault Tolerance）

Consensus is a certain protocol agreed by all nodes in distributed system in the final state of network. Due to the uncontrollable nature of the network environment and node state, the consensus mechanism needs to be both scalable, reliable and secure. Although PoW Consensus is widely used in the Permissionless chain, its probabilistic model sacrifices efficiency while wasting a lot of computing resources when providing higher reliability. In a specific business application environment, a Permissioned mechanism guarantees semi-trust of node, but users are more concerned with efficiency (TPS) - the time required to confirm the transaction, and finality – whether final results can be confirmed. The ByStack sidechain uses the BBFT consensus to address user pain points.

BBFT is derived from practical Byzantine fault tolerant PBFT consensus[5]. Byzantine fault tolerance has the following "C.A.S.H." feature while allowing a small amount $(f \leq N/3)$ of nodes to misbehave:

(1) Configurable:

Modular, pluggable design, on-demand configuration, and to a certain extent, compatibility with new technologies (Future-Proof).

(2) Adaptive:

BFT provides stable execution efficiency for different network environments. BFT requires nodes to exchange verification results to achieve a majority consensus. In general, each node

⑤ Practical Byzantine Fault Tolerance http://pmg.csail.mit.edu/papers/osdi99.pdf

needs to get enough ($>= (2/3) * N$) replies from other nodes to make a valid judgment. Network latency is an important factor in the efficiency of information interaction. Especially in cross-regional and cross-border applications, latency will become the bottleneck of the network. In BBFT, the consensus node maintains the current network topology, and the nodes with similar shortest path principles take priority communication, and the aggregation of communication can further reduce the delay. At the same time the role of the leader node (Leader) is weakened, just like PBFT, consensus nodes can make a judgement when more than two-thirds of votes are acquired. Thus the entire network consensus is not seriously impacted even when the communication with leader nodes are jammed.

(3) Scalablility:

BBFT ensure that consensus complexity increases along with network capacity linearly or sub-linearly. On the one hand, the more consensus nodes, the higher the reliability of the network, but on the other hand , the complexity $O(N^2)$ of the node communication in the traditional PBFT increases exponentially with the network capacity, which greatly limits the number of nodes. The effective aggregation of messages in BBFT can effectively reduce the frequency of message transmission, thus ensuring the complexity requirement of $O(N)$. Combined with the network topology, the network can be divided into multiple layers, message data can be effectively shared in the same layer, and spread across layers in the form of multi-signal aggregation. Verification of multi-signature information can use existing mature schemes. For example , MuSig algorithm based on Schnorr signature can guarantee the efficiency of multi-signature verification while resisting Rogue Key Attack .

(4) Heterogeneous:

Verification and communication of consensus are separated. The achievement of consensus requires verification and communication but there is no strong correlation between the two. Adopting a low-coupling consensus framework can further improve the reliability and efficiency of the network. The verification module often depends on the specific user logic and has certain requirements for computing power and security. The communication module and user logic are relatively independent, primarily handling network connections and requests. The calculation and

selection of the network topology and the shortest path can be done in the communication module. As it is irrelevant to user logic, the communication module may be connected to the validation module in the form of Abstraction Layer or Middleware. One of the advantages of heterogeneity is to do the best things with the best tools. Verification and communication are allowed to run on different systems. In different operating environments, the power of hardware-based hashrate and the Trust Zone are combined to maximize performance.

The consensus process is shown in Figure 5 (assuming a single-layer topology consensus network with 7 nodes):
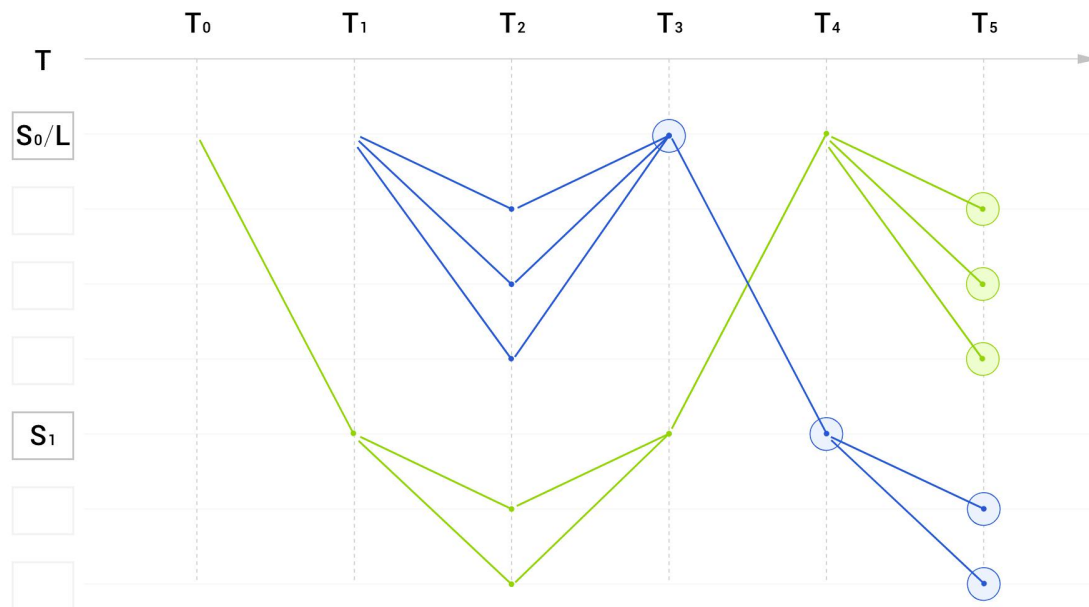

Figure 5

S0, S1 : Super consensus node. The election can be based on network topology delay and asset mortgage in order to reduce the possibility of misbehaving nodes while reducing the overall delay of the network. They work as a relay between the common node and the leader node, integrating and broadcasting information.

L : Leader node. Elections can be done by using normal polling among super nodes.

T0 : L sends the transaction and proposal (signature) to S0 and S1

T1 : S0 and S1 forwards transactions and proposals to the same-party consensus node

T2 : The consensus node verifies the transaction and sends a proposal (signature) to S0 and S1

T3 : S0 and S1 will multi-sign the proposal and send multi-signatures to each other.

T4 : S0 and S1 sends a multi-signature proposal to the same-party consensus node

At T3 , S0 has acquired more than 2/3 of the node proposal. At T4 , S1 gets more than 2/3 of the node proposal, and other nodes get all node proposals at T5 .

The authenticity of the voting result is guaranteed by the signature. The evil node can only change its voting result or increase the voting delay.

The evil leader node:

The leader node is only responsible for the sending of initial proposal, and the leader node will destroy the consensus, but will not slow down the consensus.

The evil Super consensus nodes:

Because the Super Consensus node assumes the role of input/output of the network to which it belongs, the impact of its misbehaving on the sharding is greater. In the example mentioned above, the S0 and S1 fragments are not evenly divided. If S1 is evil, it will not affect the achievement of consensus. But misbehaving S0 will affect the consensus. A reasonable network division should be selected according to the specific scenario of the application.

The common evil consensus nodes:

Since the consensus required proposal from more than two thirds of nodes, some evil nodes do not have a big impact on the overall performance of the network.

Complexity analysis:

Assuming that the total number of nodes in the network is N and the number of super consensus nodes is M , the total amount of information transmission is

$$S = M^2 + 3N - 2M$$

When $M \leq \sqrt{N}$ and $M \geq 1$时， $S \leq 4N - 2\sqrt{N}$, communication complexity is O(N)。

special case:

1. When M = 1 , BBFT = FBFT [2]

2. When M = N , BBFT = PBFT

Extension:

The key for BBFT scalability lies on efficient division and layering of the network. When there are a large number of nodes in the network, the division of horizontal (node and super consensus nodes) and vertical (multilayer network) can be adopted:

The number of nodes and the number of super-consensus nodes: The relationship between the total number of nodes N and the number of super nodes M determines the overall complexity of network communication. For any N , when $1 \leq M \leq \sqrt{N}$, the communication complexity is O(N) . When M is too small, the influence of the misbehaving super node will become bigger and bigger, and when M is too large, the communication complexity will increase.

Network hierarchy: The above example uses Level 1 Hierarchy (Single Hierarchy). In specific applications, Multi Hierarchy can also be used .

The above two types of divisions can be combined with each other. Particularly with great numbers of nodes in complex network environment, the network may be divided into Forest, which is a a tree structure composed of nodes and other consensus super nodes. The consensus network is a dynamic system, where new nodes can join, old nodes can exit, and wrong nodes will go offline. Automatic adjustment of network partitioning parameters is critical to maintaining overall network health. The BBFT network module monitors the network status regularly and adapts the network structure to ensure its high performance.

3.2 Economic level

3.2.1 Core role

Sidechain initiator: The individual or organization that dominates the side chain.

Relay node: assumes the role of linking mainchain and sidechain, responsible for locking and releasing of assets on mainchain and verification of sidechain assets.

Consensus node: The consensus node is the full node on the sidechain and produce sidechain blocks.

Client: Token-holder who entrust their tokens to consensus node.

3.2.2 Rules

The main rules of the relay node:

(1) Election mechanism

The relay node is directly designated by the sidechain initiator, and the relay node may be one or more.

(2) Reward mechanism

The relay node charges the transfer fee between the mainchain and the sidechain, and the relay node can set the ratio of the transfer fee.

(3) Exit mechanism

Sidechain initiator has the authority to replace and designate relay node.

Main rules of consensus nodes:

(1) Campaign mechanism

The candidate consensus node needs to mortgage a certain amount of BTM [6] to be eligible

---

[6] Bytom Token

to participate in the consensus node election;

Candidates who on the top list can become a consensus node to produce blocks and on the list of alternative consensus node.

(2) Reward mechanism

The total consensus node reward comes from the block reward, The Token reward part in the block is awarded to the block producer and the remaining part is allocated according to the delegation vote received by the node.

(3) Punishment mechanism

Once the relay node has the following abnormal behaviors, it will be punished:

- Packing illegal assets into the sidechain;

- Offline for a long time;

- Or other malicious acts, etc.

The consensus node identity will be removed once misbehaving nodes are detected.

(4) Exit mechanism

Token under custody will be returned to the consensus node after 20 days the consensus node proposes to withdraw the application or is dismissed from the consensus.

The principal rules of the client:

(1) Voting method

The sidechain offers the client with voting option. Client can vote their favorite nodes through token binding, which cannot be traded after binding is in effect.

(2) Income

Client's revenue comes from the block reward. The more token entrusted to a consensus nodes, the more revenue. The consensus node sets the proportion of the block reward assigned to the client.

(3) Redemption and waiting period

The client can send redemption transaction to unlock their own token. These untied Tokens will not circulated immediately.

After the redemption transaction is executed, the client cannot initiate another redemption transaction to the same node. The waiting period is 20 days. Once the waiting period is over, the untied Token will automatically become a circulating Token .

(4) Transfer custody

The client can transfer his delegated token from one validator to another. Two steps: unlock token from the first consensus node and bind the released oken to another consensus node. Unlocking cannot be completed immediately before the end of the waiting period.

3.2.3 Node revenue

The sidechain initiator can provide BTM as incentive to consensus node in the side chain , or it can provide incentives based on other assets issued on Bytom network. The sidechain intitoator regularly announce the number of awards to the public each year. The number of is determined by the sidechain initiator based on the scale of development of the sidechain ecology.

4 Bystack Introduction

4.1 Bystack Overview

Bystack is a general blockchain application stack platform that inherits and implements a blockchain three-tier architecture, which are consist of Bytom mainchain, Vapor sidechain, Blockcenter middleground, Bycoin , Byone ,Bystore and so no. The following figure is the basic architecture of Bystack :
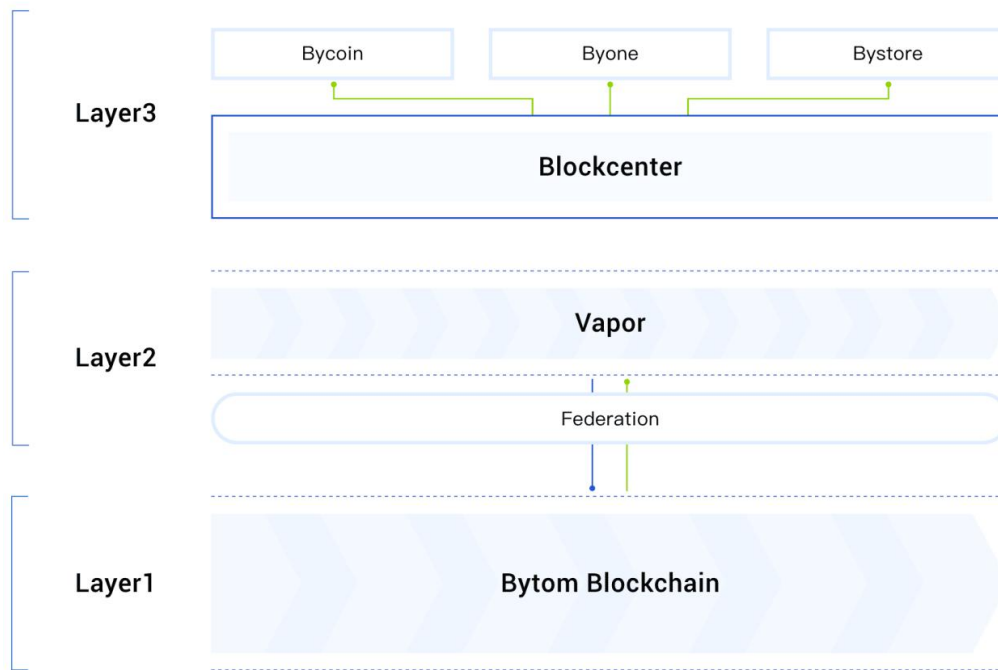
Figure 6

Bystack rely on the Bytom public chain technology platform and Vapor sidechain technology. Through Federation as an interactive protocol between the mainchain and sidechain, Bystack provides a channel for the transmission of values and lays a solid foundation to the upper application. Blockcenter is the business middleground and the core of the entire system. Along with other upper services such as Bycoin, Byone , Bystore implement the third layer of blockchain applications.

Blockcenter : On a layered basis , Blockcenter features modular and layering design. The common business flow is split into different modules. Blockcenter provides the basic capabilities and implementation framework of typical applications, allowing users to deploy their own business like "building blocks" according to their own needs and easily implement their business logic on blockchain. In terms of bottom layer, it frees users from understanding the underlying blockchain technology principles, and focuses more on their own business development. Blockcenter is the bridge between blockchain technology and commercial applications.

Bycoin: The ecological portal and solution for mobile clients. Bycoin supports the savings of multiple assets, easy exchange between assets and can be used in other systems that integrate

Bycoin SDK. Bycoin not only supports storage, distribution and exchange of multiple assets, but also provides us with many daily needs, such as entertainment, daily consumption.

Byone : Desktop client solution. We only need to install Byone on the browser side of the computer. After registering and logging in, we can use it to manage various assets on the desktop, open the application that supports Byone in the browser, connect the accounts and assets of Byone, and use Dapps and business application based on Bystack.

Bystore: It supports a complete and powerful development framework for contract development on the Bytom network. The framework supports variety of coding language for writing smart contracts. After the contract is written, pre-complie the contract and call the contract transaction interface to directly issue the contract. Bystore is very friendly to developers. With rich contract templates, developers only need to modify some parameters and enter account parameters to publish contract.

4.2   Bystack innovation

4.2.1 Open consensus

The consensus mechanism of Bystack 's sidechain is DPoS+BBFT , but other consensus algorithms can also apply. Bystack provides abundant pluggable consensus mechanism, such as DPoS , PoS, and so on. At the same time, the sidechain can allow anyone to join the consensus node, which is very different from the permission-based mechanism of consortium blockchain.

4.2.2 Mainchain-sidechain architecture

The mainchain is responsible for issuing and burning assets, and guarantee decentralization and security. The sidechain is responsible for running large-scale commercial applications, and the sidechain sacrifices part of the decentralization to greatly improve performance. An unlimited number of sidechains could co-exist to meet different areas and performance needs.

4.2.3 BUTXO

BUTXO is based on the Bitcoin UTXO model. Multiple asset transactions are supported from the underlying model. BUTXO guarantees the atomicity of asset interactions and verifiability in asynchronous transactions. It supports blockchainization of multiple assets and boolenization of smart contract. Due to the statelessness of BUTXO , the anonymity of users is enhanced to some extent.

4.2.4 Shortest path transaction

The signature is not with transaction but on each input. Transaction can be constructed autonomously at different times and between different people, thus constructing different types of transaction such as magnetic trading.

4.2.5 Customized pluggable services

The Blockcenter of Bytom can provide plenty of pluggable service. Merchants can integrate different services according to different business scenarios, such as identity service, multi-signature and private transaction.

4.2.6 Contract Virtual Machine in multiple languages

Contract Virtual Machine support Equity, Javascript , Python , Go and other languages to facilitate developers in developing commercial Dapp .

4.3 Advantages

4.3.1 Ecology Support

The blockchain can serve the financial industry, the supply chain as well as the industrial ecology of the vertical sector. But the general public blockchain or consortium blockchain can't serve every industry. Bystack can achieve more comprehensive technical support through multiple sidechains. Each sidechain is customized and assembled according to the characteristics of

different industries to meet the business needs of different industries and fields.

4.3.2 Scalability

At present, there are two scalability solutions: Layer 1 and Layer 2. Layer 1 focus mainly on blockchain itself, making the blockchain faster and its size larger. Bystack compresses transactions and increases the speed of the block generation in Layer 1. Layer 2 is to migrate complex business processes to sidechains. Blockcenter is the layer 2 scaling of Bystack.

4.3.3 Performance

The performance is mainly analyzed from the folloiwng perspective:

Block interval: Bystack 's main network is based on the Bytom network , which produces a block every 2.5 minutes. The sidechain uses DPoS+BBFT and the block speed is about 0.5 seconds.

Block size: Sidechain compress transactions to reduce block sizes, hence reducing bandwidth and allowing all nodes to synchronize blocks faster.

TPS : Sidechain can reach tens of thousands TPS, and the throughput can reach more than one million by extended scaling. It can fully meet enterprise-level needs.

Fault Tolerance: The PoW algorithms on mainchain allows less than half of the uncooperative nodes, while the sidechain BBFT consensus algorithm allows no more than 1/3 of the uncooperative nodes.

4.3.4 Security

Mainchain consensus algorithm: A single DPoS or PBFT is not a true permissionless consensus. A license requirement mean that the network is controlled by a small group of people. Data immutability and irreversible transactions no longer exist. The security of blockchain-based asset identification and data deposit will not be guaranteed. Bystack Layer1 adopts Tensority, the innovative PoW algorithm. Under the mining incentive mechanism, the hashrate of the whole network continues to grow. The cost of launching 51% of attacks has been increasing. In particular,

Tensority adopts an AI-friendly algorithm, which makes AI chips possible to mine on the network, thereby reducing hardware costs and empowering the artificial intelligence chip industry.

Sidechain Consensus Algorithm: Bystack Layer 2 uses the DPoS+BBFT consensus algorithm to provide high-available Byzantine fault tolerance, automatic recovery of consensus state, mutual recovery of blockchain data, automatic equalization of data storage,and automatic routing of node services, thereby ensuring the security and stability of the network itself.

Contract security based on BUTXO model: The mainchain adopts the BUTXO model. Each BUTXO is locked by an independent contract program. Hacking a single contract can only get access to the assets locked by the contract, and other assets are not affected, thus protecting the mainchain assets.

Mainchain-sidechain isolation: Supports Simple Payment Verificaiton (SPV), which can verify the information of Header, Merkle Tree on the mainchain. The mainchain is responsible for the update and maintenance of the ledger and data security. Key business such as asset issuance, data deposit and digital identity are completed in the main chain. Different sidechains are responsible for trading of different assets such as equity, copyright and royalty. The mainchain does not need to care about the operating state of the sidechain. When the sidechain is attacked, the security of the mainchain is not affected.

Sidechain-sidechain isolation: Different business are isolated from each other. Each industry has different sidechains. If one sidechain is attacked or affected, it will not affect the operation of other sidechains.

Federation security: Through the sidechain pegout to the mainchain, collectors, validators and other roles ensure that the asset transfer process is divided into multiple processes to prevent single validator from misbehaving.

4.3.5 Privacy Protection

Bystack offers a full range of privacy protection with a combination of encryption algorithms. High configurability ensures flexibility and adapts to different user scenarios.

Anonymous transactions: For multi-sign transactions, the Schnorr signature and the MuSig algorithm are used to verify multiple signatures. The encryption of the transaction amount can be based on Zero Knowledge Proof (ZKP) schemes such as zk- SNAKRS and Bulletproofs. In scenarios with high privacy requirements, we can use the MimbleWimble to encrypt both the transaction address and the transaction amount. The current mainstream encryption algorithms are based on Pedersen commitment scheme. Although it offers complete hiding feature, the scheme only provides limited computational binding, which means that the transaction amount may be changed. In order to cope with the sudden rise of future computing power, Perfect Binding systems, such as ElGamal encryption, can be adopted in a switch-activated mode.

Privacy Contract: The above privacy trading scheme can also be applied to privacy contracts. In addition, the Merkelized Abstract Syntax Tree (MAST) is used to optimize the contract itself to provide certain degree of privacy protection with size reduction.

4.3.6 Support Bancor Protocol

Bancor is a decentralized liquidity network that provides users with a simple, low-cost way to buy and sell tokens. Bancor 's open source protocol authorizes tokens with built-in convertibility to be immediately converted to each other without matching buyers and sellers in the transaction. Bancor wallet can automatically convert tokens directly at the price that is easier to predict than the exchange and will not be manipulated. Bystack 's Bancor protocol allows multiple assets (such as business royalty, multiple digital assets) to be converted quickly, cost-effectively and efficiently.

5 Introduction of Blockcenter

5.1 General Architecture of Blockcenter

As the core of the entire enterprise-level blockchain, Blockcenter expands the capabilities of the underlying mainchain and sidechain. On the other hand, it abstracts the underlying blockchain technology to provide a typical application development framework, while also provides maintenance, monitoring and upgrades.

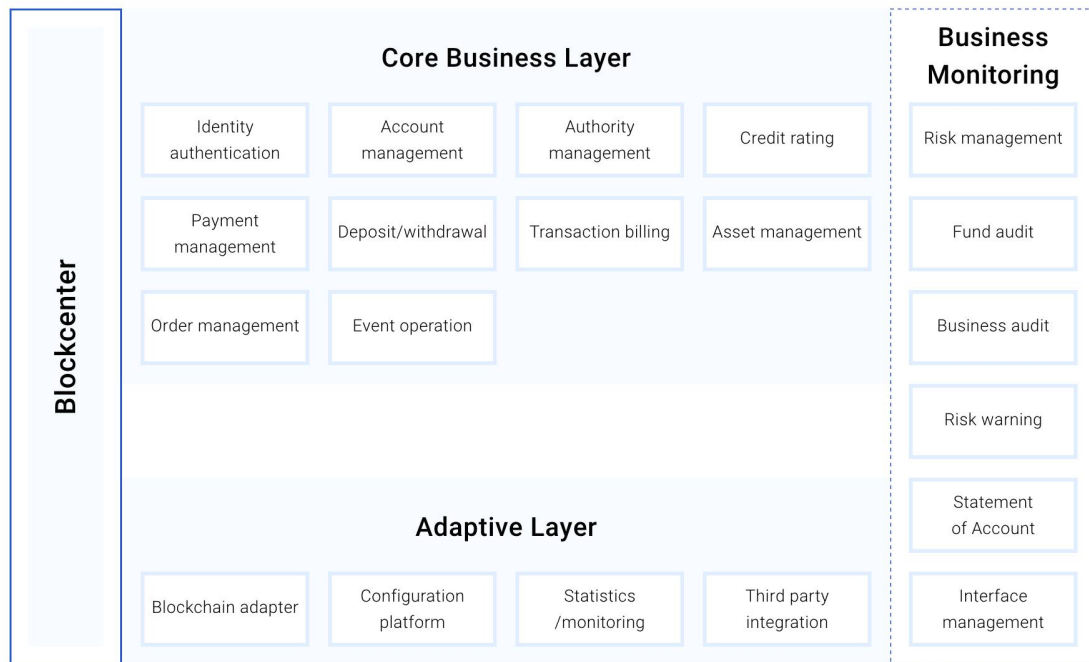The main architecture of Blockcenter is as follows:

Figure 7

From the above middleground (Blockcenter) , we can see that the entire middleground is divided into core business layer, adaptation layer and business monitoring. These are all business modules at the system level, which are explained as follows:

Identity authentication: Responsible for user identity authentication and authentication at the upper level of the service, providing user identity registration and login services. If more stringent identity authentication services are required, third-party integration can be used to connect to an authoritative certification authority.

Account Management: Manage user identity information and maintain the correspondence between user identity and blockchain identity.

Rights Management: Set the permissions of the users to expand or reduce users' operation rights.

Credit evaluation: The credit evaluation of traditional Internet is based on the credit accumulation model, and does not record the timestamp of the transaction, which brings the risk

of malicious praise or bad evaluation. As each onchain transaction destroy coindays, Bystack introduce CDD (CoinDays Destroyed) into credit rating as an evaluation factor, so that malicious rating is not possible.

$$R_n = \sum_{i=1}^{i=n} R_i * W_i$$
$$W_i = C_i * D_i$$
$$R_i \in \{-1,0,1\}, i, W_i, C_i, D \in (0, +\infty)$$

R_n represents the user's credit score, R_i is the credit value obtained by the user for the i- th trading, W_i is the CDD in the i- th trading. C_i is the amount of the i- th transaction, D_i is the time accumulated from the last transaction to the i- th transaction.

Payment Management: Provides user's payment information and conducts further statistical and risk control warning based on such information.

Deposit and withdrawal: Provide deposit and withdrawal of digital currency. Merchants can access very simply without development.

Transaction Billing: Provides a pre-paid function that automatically bills based on the merchant's debit logic.

Asset Management: Provides background management functions for different assets of the mainchain and sidechain.

Order Management: Manage user-initiated orders and track different orders.

Promotion Operations: Customize in-app activities, set up transaction fee reductions or other promotions.

Business monitoring: Monitor the entire process during the operation of the merchant application, including monitoring, early warning, risk control for users, funds, behaviors, etc.

Adaptation layer: The adaptation layer completes the abstract work of the bottom layer of the blockchain. The underlying technologies are encapsulated into service interfaces here. The underlying technical complexity are hidden in this layer. At the same time, the configuration parameters are set in the dashboard. Onchain data is monitored through statistics.

The goal of the modular design based on Blockcenter is to implement "pluggable" module applications. The core business module, the adaptation module and the service monitoring module provides the open API service at its maximum. Users are free to choose the best possible solution that meets their business needs. For example, in the decentralized trading scenario, the asset management, transaction billing and transaction management could meet the demand, which could be managed through sidechains.

5.2 Blockchain Adapter - Open up Application and Blockchain Technology

The adaptation layer functions as the core module by hiding the complexity of the underlying technology. Via the interface adapter, the upper application can easily use the underlying technology of the blockchain. We also provide more complex configuration interface for customized needs. The module diagram of the blockchain adapter is as follows:

Blockchain Adapter

| Federation Agent | On-chain identity | BUTXO management | Sidechain management |

Transaction Management

| Magnetic transaction | Decentralized swap |
| Multi-sig | Privacy transaction |

Contract Management

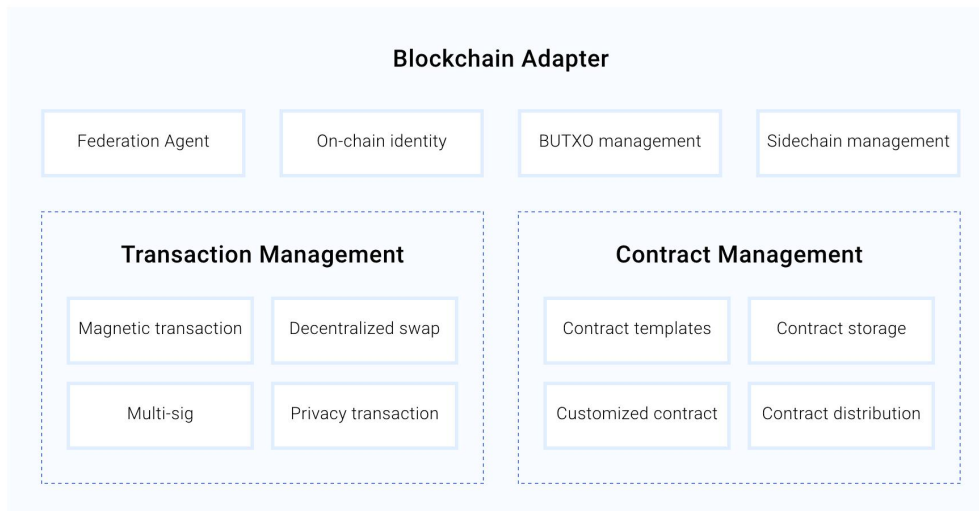| Contract templates | Contract storage |
| Customized contract | Contract distribution |

Figure 8

Federation Agent : The business intermediary of the mainchain-sidechain communication. It is responsible for the Pegout from sidechain to mainchain and he management of Pegin from mainchain to sidechain, transforming cross-chain transactions from blockchain to upper-layer business transactions.

Onchain Identity: mainly serving the decentralized identity system, The identity storage

information in the blockchain is parsed and transmitted to the core business layer for authentication.

BUTXO management: BUTXO storage and identification for each user. Choose the appropriate algorithm to determine the correct BUTXO when creating a transaction and using DAPP .

Sidechain Management: Manage the sidechains in use or created.

Transaction management: The management of the trading model of assets on mainchain and sidechain. It is compatible with multiple types of transactions.

Contract management: Moduels like Equity or WASM are available and provides onchain offchain storage. Contract content can also be customized and distributed to sidechain or mainchain.

5.3 Development Tools

Blockcenter provides complete toolkit and specifications, combined with the Bycoin SDK as a mobile solution, Byone as a desktop solution and Bystore as Dapp open platform. We support multi-language SDK, which can be used very conveniently on Blockcenter .

6 Business Application Scenarios

6.1 Royalty Redemption

Consumers will encounter different royalty systems such as banks, merchants and institutions when they spent their money. These royalty systems are closed in various organizations and cannot be used universally, resulting in difficulty in spending and low utilization rate. In addition, the royalty data can be tampered and information security is not guaranteed. Plus every royalty system is complicated and it is impossible to accurately formulate a balanced exchange ratio.

Based on blockchain technology, an immutable trust registration mechanism can be established among enterprises, which provides the possibility of exchanging different royalties.

The circulation of royalties can be activated and various customer service could be promoted. With the formation of collaborative business circle, customers can converts their own points in different merchants to general tokens on blockchain exchange. Customers are linked with their own account, which cannot be obtained between different merchants. The data cannot be modified in the blockchain to avoid data fraud.

Based on Bystack 's mainchain-sidechain architecture, it is convenient to issue the merchant's own royalty system on the mainchain, and then define a conversion ratio. Then the royalty networks between users could be exchanged.

6.2 Copyright Confirmation

The protection of copyright is not only the protection of the original author's rights, but also a symbol of social progress. The government has been actively promoting copyright protection. Many enterprises have tried to launch blockchain-based copyright application projects, and people's copyright awareness has been continuously improved.

At present, technology can realize the recording of copyright, which can be used as an evidence source for rights protection after infringement, but there is still a gap between technology and real application. At present, we didn't find any good solution. Cross-platform certification: In a single system, copyright protection and traceability are easy. However, if user A puts the content of user B on other platforms, it is easy to arouse a dispute. Therefore, it is necessary to strengthen the universal authentication, marking, and identification methods among different copyright platforms, or provide a unique authentication platform to improve the efficiency. Non-standardized copyright certification has yet to be developed: for the authentication of some non-standardized items, such as algorithms, data, etc., it may be possible that it can be traded well by zero-knowledge and other encryption methods with the prerequisite of standardized rules, which will take some time to achieve. Blockchain can promote high-quality content generation through the decentralization, or the elimination of the third-party copyright monopoly. Let the author truly own their product so that content producers will have more benefits and value realized. Blockchain-based copyright can facilitate judicial evidence and reduce copyright disputes. Based

on the copyright platform on the blockchain, the submission of the author's work, follow-up transactions and the purchase of the user are all timestamped on the blockchain. In the case of copyright disputes, the judiciary only needs to obtain the digital ID of the copyright and retrieve the historical transaction information of the copyright of the work. Case could be settled easily.

Using Bystack as a copyright-rights platform, its author can be easily have their copyrights stored on blockchain while the decentralized and tamper-proof features can guarantee dispute-free copyright.

6.3 Product traceability

The problem of counterfeiting and faking has always been a pain point to be solved in various industries. The high frequency and wide-ranging commodity fraud have made the public's appeal for the traceability of goods higher.

With Bystack's unique immutable feature on mainchain and sidechain and combined with IoT technology, we can realize traceability in the entire process from source material traceability, production, processing, warehousing, inspection, logistics, third-party quality inspection, customs clearance and anti-counterfeiting certification.

6.4 Supply Chain Finance

The funds of small and medium-sized enterprises are constantly being squeezed by upstream and downstream enterprises. Although they are the focus of national support, traditional financial financing methods are not suitable for their development. In order to keep up with their development, supply chain finance will inject new vitality into the development of small and medium-sized enterprises.

Based on Bystack technology, the transaction information and related documents of the loan are guaranteed to be open, transparent, queryable and non-tamperable. All participants have a clear understanding of the entire supply chain process through distributed ledgers. Each participant in supply chain finance is a member of a peer-to-peer network. There is no single point of failure in

the network and the entire network is highly available. The transaction speed and cost on Bystack are far superior to traditional banks. All parties can reduce labor costs and operational risks. The cash flow of the project reduce systemic risks.

6.5 Digital government affairs

From the perspective of market size, China's digital government affairs market in 2017 reached 272.2 billion yuan. In 2018, it is expected to exceed 300 billion yuan. However, digital government affairs in transition are facing difficulties such as data islands, high cost, network security, inefficiency, and lack of supervision.

Blockchain provides a new solution for digital government. At present, there are 17 kinds of blockchain digital government affairs applications in China, involving in seven categories: government auditing, digital identity, data sharing, public supervision, electronic notes, electronic deposits and export supervision.

Through the technology of Bystack , government agencies, financial institutions, regulatory agencies and other intermediaries are placed in the blockchain ecosystem. A multi-level authority management system and smart contracts are used to achieve a certain range of government processing and data sharing.

Bystack can help build a solid, transparent platform that allows government agencies to securely process sensitive information by authorizing permissions through smart contracts, ensuring data security and traceability.

6.6 Decentralized transaction

There are some flaws in centralized transaction. The most worrying one is the security issue. In order to meet the performance requirements, the current platform generally conduct transaction offchain and the order-matching data stored in a centralized database, which means hat they are acting as third-party intermediaries. Transactions are not recorded in the blockchain, which makes them vulnerable to be hacked and suffer other security breaches.   Centralized exchanges are also

less robust against special blockchain events such as hard forks and regulation changes.

From a business perspective, the decentralized transaction model is simple. It only needs to undertake major asset custody, order matching and asset clearing. There is no need to undertake non-transaction functions like the account system, KYC and fiat exchange. The user's public key on the blockchain is the identity. There is no need to register personal information, so there is no personal information security issue or KYC .

Based on Bystack 's mainchain-sidechain mode, the mainchain performs asset registration, and the sidechains will meet the needs of high TPS order matching.

6.7 Distributed Identity System

Historically, the identity documents we need in our daily life—passports, driver's licenses and social security cards—are issued by central agencies such as the national institutions or private sectors. The use of such ID poses many problems : (1) If the state revokes personal vouchers, the individual may lose his or her identity; (2) the identity is restricted by the state or territory. The identity issued by a particular nation is usually not accepted by other countries; (3) ID is controlled by a collective centralized entity or one particular online platform. User has no control over their own identity data. We also often see the identity-leaking incident. For example, in 2018 Facebook leaked 50 million user data. Also in 2018, China Lodging Group leaked 500 million citizens' personal information. These large-scale data breaches pose a great threat to users' privacy.

With the evolution of blockchain technology, new identity management models have emerged. The decentralized identity management model has the characteristics of distributed data storage, peer-to-peer transmission, encryption security and consensus confirmation, which can effectively solve the problem of identity verification and operation authorization. Blockchain identity provides a secure and decentralized solution for digital identities, enabling a distributed trust model. Blockchain technology transforms existing identity management systems by providing self-sovereign identities on decentralized networks because multiple IDs can lead to security issues and data breaches. By addressing identity theft KYC (Know Your Customer) and lack of control over personal data and other issues, blockchain technology help to improve

existing identity management.

6.8 Internet of Things +5G

5G will change the Internet of Things (IoT) as well as our perception of the connection between home, business and transportation. Many visions are coming true in the 5G world. Applications built on AR,VR and AI will benefit from massive data pipelines and ultra-low latency. Smart cars and drones will communicate with each other and coordinate things around them through low-latency networks, making them a new conduit for connecting industry and consumers. 5G will bring us closer to the real IoT world with millions of sensor access. It is foreseeable that the traditional centralized service architecture is difficult to handle the management pressure after exponential growth of the equipment, and the blockchain will be a solution.

The Tensority consensus algorithm used in the Bystack mainchain is naturally suitable for deployment in IoT devices containing AI components, connecting machines through blockchains to form a decentralized IoT system. Smart communication through the blockchain enables direct communication between machines and machines, greatly improving management efficiency. At the same time, the 5G technology enhances data transmission capacity, which reduces the blockchain communication delay and improve the communication throughput, creating the ideal environment for operation of industrial blockchain.

6.9 Company Equity Management and Trading

Although the Chinese equity investment industry is thriving with annual investment over 1.5 trillion yuan, the lack of liquidity and exit difficulties have become the biggest concern for equity holders. Due to the low probability of listing and long waiting period, traditional IPO or acquisitions can no longer meet the liquidity demands of equity holders. Company founders, investors or the employee option holder are all eager to have the opportunity to liquidate their shares before the company goes public.

The main reason for this problem is the lack of trading mechanisms and means. Dubious transaciton is often brought by unverifiable information.

Blockchain technology solves these problems. The decentralized and immutable nature of the blockchain will solve the opaque and untrustworthy problems caused by the centralization and tampering characteristics of the registration and management of equity ownership. Smart contract will solve the low efficiency and high cost problem in traditional equity issuance, granting. The Bystack- based contract transfer application will provide a fast, efficient and transparent exchange for these equity shares registered on blockchain .

6.10 Blockchain Game

Gaming is the earliest application type in the blockchain. As early as 2012, there were some games emerged on the Bitcoin blockchain, which implement some basic betting function with the intrinsic features of Bitcoin blockchain. In recent years, many blockchain games have hit the market.   Ethereum's CryptoKitties and Tencent' s "Catching the Demon" have aroused great anticipation. Bystack has a systematic consideration in the field of games from the following 3 perspectives: high TPS with low operation cost, asset types such as quark assets, and the integration of distributed and centralized

(1) High TPS with low cost. Bystack sidechain can support over 10,000 TPS, and up to 1 million after extended scaling, well-prepared for blockchain games with high demand for performance. Plus low transaction cost on Bystack sidechain, developers could easily afford development.

(2) Multi-asset interaction. In addition to meeting the basic needs of distributing game assets based on blockchain , Bystack divides assets into four categories based on the physical and equity attributes of assets, such as Bits, Atoms, Quarks and Quantums. These assets can be easily adapted to the assets in games like items and credits. All kinds of assets can be integrated like blocks to meet the needs of the game. For example, the key items in the game can be classified as Quark assets. This kind of asset is inseparable, unique and irreplaceable in the blockchain. The common gold coins in the game can be classified as Bit assets, this kind of assets are severable and

fungible.

（3）Combination of distributed and centralized. Blockchain games naturally have a higher degree of trust. Bystack establishes the transparency and information symmetry of the game process through open source contracts. The relaying node between Bystack mainchain and sidechain can act as a "gateway". Game developers and regulators may have certain regulation to ensure that the blockchain game can be freely switched between the internal circle and the external large ecology so that the organic integration between distributed and centralized can be achieved.

7 Case Study

7.1 Jifenbao

Jifenbao is a Bystack-based service platform that integrates marketing, announcement, exchange, social and user operations.

7.1.1 Background

Company reward user with royalties in order to maintain customers relations. When customers accumulate a certain amount of royalty points, they can exchange it for some gifts or discount from   merchants. Royalty program has become a common business model for banks, online business, shopping malls to retain customers and acquire new customers. However, the closed loop of royalty programs makes it difficult to circulate. In reality, royalties are either expire or settle down on merchant platform for good.

In industries where the royalties are more active such as aviation and hotels, royalties are interchangeable among commercial giants through business alliance. However, it is difficult for some enterprises with small volume and those who are weak in royalty operation to make detailed operation and commercial expansion even if they have enough user base. On the one hand, they do not have enough capital and a clear profit model to attract external partners to join the royalty ecology. On the other hand, they don't have extra manpower and financial resources to operate royalty programs. Given a series of problems such as the third party's subject attribution, industry

qualifications, service fees and corporate privacy security, it's difficult to entrust royalty with other independent entities.

7.1.2 Function Overview

In view of this, a technical solution with the Bytom mainchain + Vapor sidechain as the underlying architecture is formed to establish a blockchain royalty platform. The main mission of the platform includes the following:

（1）Creating an user identity system on Bystack. Royalty is registerd as assets on Bytom and its ownership belongs to their users, thus subverting the management mode of the centralized registration in the traditional Internet.

（2）Royalty are exchangeable through C2C market and algorithm redemption. A magnetic transaction in which multiple exchange requests are combined into one could be achieved with Bytom BUTXO model ;

（3）For the royalty assets issued by different enterprises, there is a corresponding DAPP configuration page. Enterprise or developer can develop an independent DAPP based on the asset characteristics and the business content for their customers. Customers can quickly find DAPP according to the type and properties of royalty program.

（4）Establish a user social system, expand the coverage area of royalties, deepen the social attributes of royalties.

（5）Creating an enterprise management dashboard. Enterprises can perform additional operations such as issuing, destroying and monitoring royalties through the back-end panel, collecting user consumption, circulation and exchange status, establishing user portraits according to user behaviors. It also carries out targeted operations through functions such as candy distribution, thereby enhancing user stickiness and developing external user conversion.

（6）Provide users with modules for the mutual transfer of assets on sidechain and mainchain.

7.1.3 Technology implementation

As a platform-level application, Jifenbao uses Vapor, the sidechain of Bystack, as the back-end layer, considering that its business is involved in high-frequency trading and asset-issuing scenarios.

The royalty assets will be issued by the issuer through the enterprise certified account on the BYTOM network, which will be pegged to the sidechain where Jifenbao is located, and then distributed to the user address accordingly.

Registered users will establish their own account on Vapor and conduct operations like transfer, spending regarding their royalties.

The exchange platform will be established using smart contracts.

The enterprise side can conveniently deploy and operate its own royalty program through the back-end management system, which can be established accessing the API from the server that originally host the royalty system . There is no need to overhaul the original system.

The enterprise development team or individual developer can independently develop their royalty DAPP and upload it to the Jifenba DAPP market with Bytom SDK .

7.2 Blockchain contract

7.2.1 Project Introduction

The blockchain contract is an enterprise-level contract and note platform based on blockchain technology. We try to change the status quo that service provider dominate users in the traditional Internet model. Through blockchain, we can realize the transmission of credit and secure business. Smart contract can be used to adopted in contract formulation, execution and management. At the same time, based on the security, transparency and immutability of the blockchain, it provides strong protection for the user's asset security and corresponding legal rights.

7.2.2 Project Architecture

The blockchain contract uses a three-tier structure as follows:

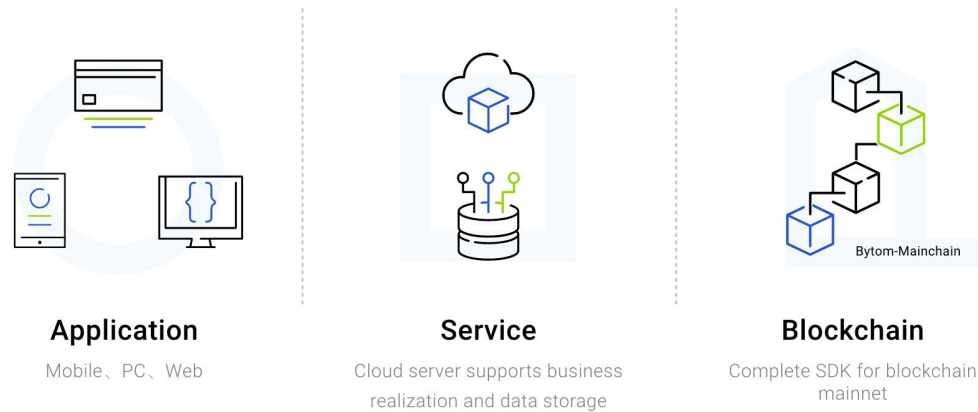| Application	Service	Blockchain
Mobile、PC、Web	Cloud server supports business realization and data storage	Complete SDK for blockchain mainnet

Figure 9

Service layer: The storage and interaction of high-performance cloud host.

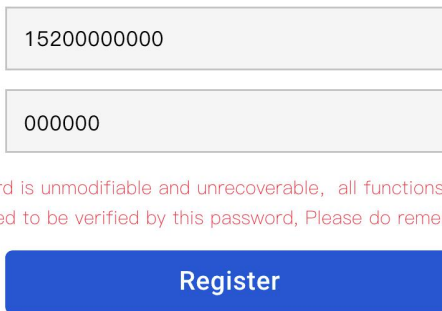Blockchainlization layer: Interoperation based on the complete SDK, synchronizing user operations and file encryption information on blockchain.

Application layer: The blockchain contract is fully compatible with PC , WEB and mobile devices in the application layer. User can conduct user information management, contract signing, file management, and chain information viewing within the application. In addition, enterprise-level users are provided with API access to for easy and fast deployment.

7.2.3 Project innovation and advantages

（１）Privatization deployment of public and private key systems

Unlike traditional Internet service where the service provider is in complete control over user's information, the blockchain contract will match the random number according to the user information during the user registration phase and generate the public and private keys in offline environment. User manage his own public and private key pairs through password (as shown in Figure 10 , Figure 11).

Generation of Public Key and Private Key

15200000000

000000

*This password is unmodifiable and unrecoverable, all functions and operations
need to be verified by this password, Please do remember

Register

Figure 10

Authentication Status

Name: YUAN

ID number: ⬜⬜⬜⬜⬜5430

Phone number: 137⬜⬜1037

Public key: 0455E109392CF06E01CAD280C8C242506351CB04661E947066
F3D7C6D967B25298722139D50EFD0CC4BBA5D173046328E7EE
3F950CA6B05180256D0B8F0159A1E4

Figure 11

(2) CA- certified blockchain identity

Traditional financial services usually deploy a public-private key pair to request authentication in order to generate a CA certificate in real time. The blockchain contract first creates a blockchain account for the user and then uses the integrated API to authenticate the public key, thus making the user's behavior on the blockchain has the same legal effect as the CA certification (the process is shown in Figure 12).

(3) Signing the contract offline based on private key

On the basis of the traditional electronic signature process, we have independently developed a signature method based on the blockchain private key and smart contract through blockchain scripting. With only one input of private key password during the user signing process. (As shown in Figure 13), local private key signatures can be implemented and recorded on blockchain in real
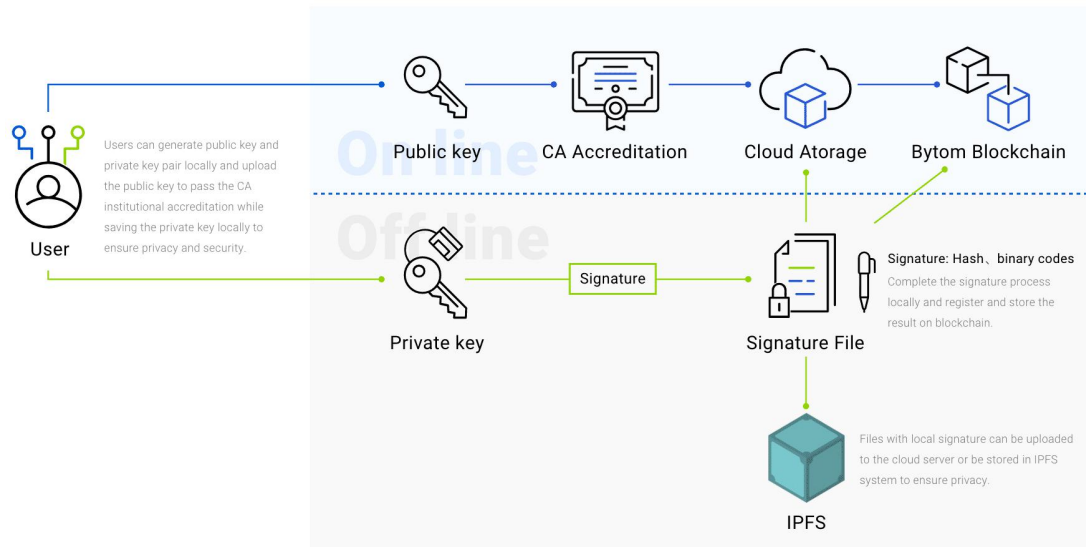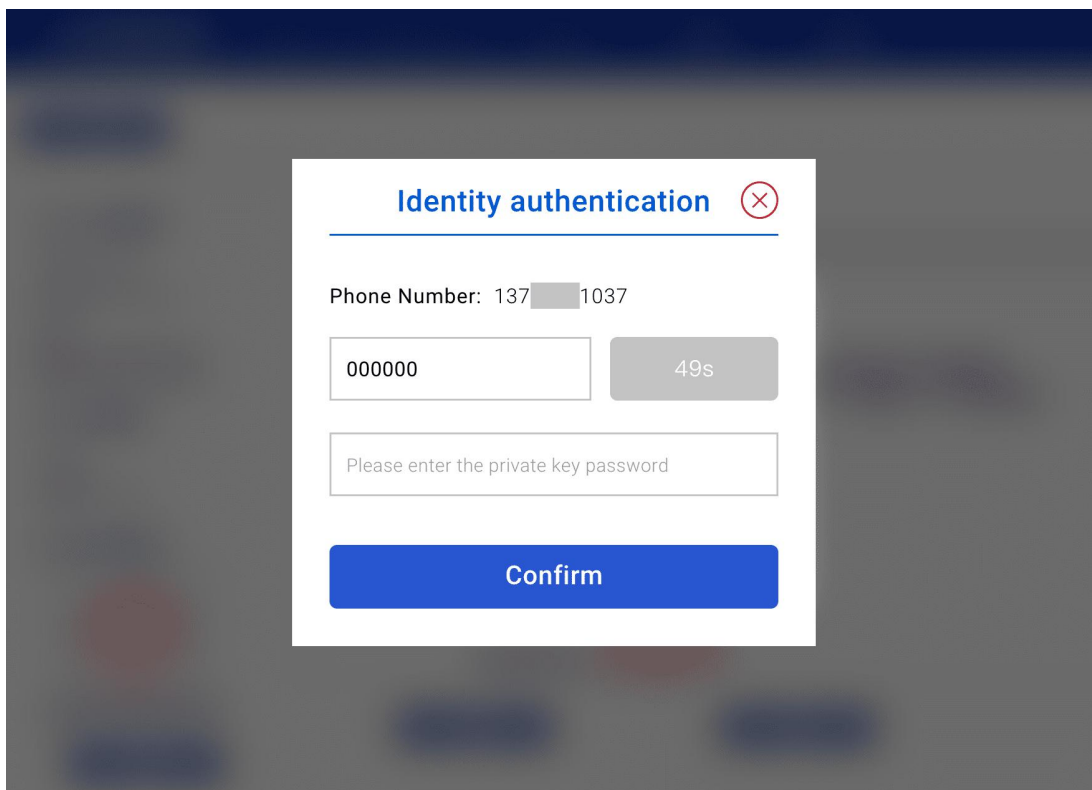
time.

Figure 12

Figure 13

(4) Storage of classified files

The contract information in traditional Internet service is stored on the operator's server. We

provide the user with a file storage option, which allows re-encryption for some documents involving funds, core articles and confidential information. Encrypted files will be upload to the IPFS network. Users can freely browse, manage and edit files while ensuring the file is only visible to the user and the authorized parties (the process shown in Figure 14).
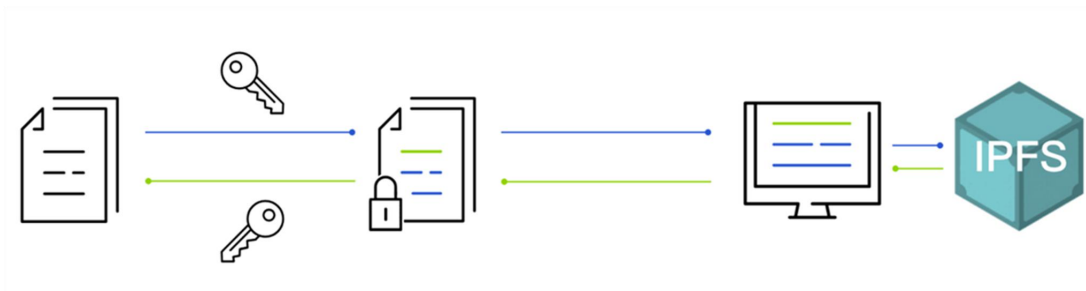
Figure 14

(5) Intelligent contract

As Bystack focus on the technical characteristics of assets, the Blockchain Contract provides users with online templates. For contracts involving financial business, the contract itself can be converted in a smart contract, thus enabling the contract to be programmable. In turn, a series of services such as intelligent writing, intelligent execution and intelligent evidence of the contract are realized (as shown in Figure 15).
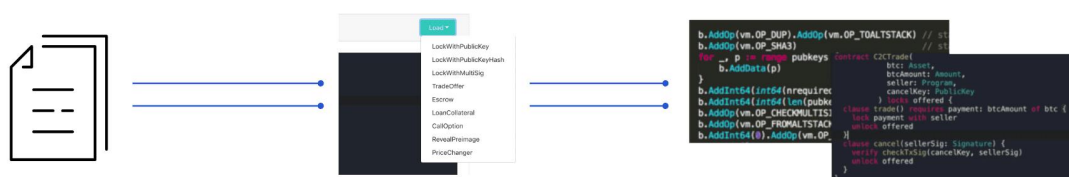

Figure 15

7.3 Digital Government Afairs Cloud Blockchain

7.3.1 Project Background

Bystack is used to rebuild the citizen ID authentication system, which is mainly responsible

for the construction and management of the municipal government data and public data including the organization and implementation of some major projects like " data brain". The Data Resources Authority decided to use the "Citizen ID Authentication System" as a pilot for the blockchain technology program. As the designated technology provider, the Bytom team will develop the whole blockchain solutions.

7.3.2 Project Overview

The function of the "Citizen ID Authentication System" is to compare the collected citizen information with the original files of the Ministry of Public Security through online terminals and online service platforms, and issue a verification certificate based on the returned results (the process is shown in Figure 16).
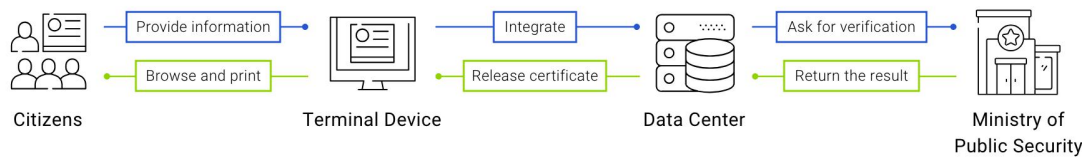

Figure 16

Under the basic structure of the system, the next step is to build the underlying service with Bytom sidechain. The feedback from the Ministry of Public Security will form the data record on the blockchain in real time with a corresponding query interface and a serial number to track its storage status on blockchain. (the flow is shown in Figure 17).
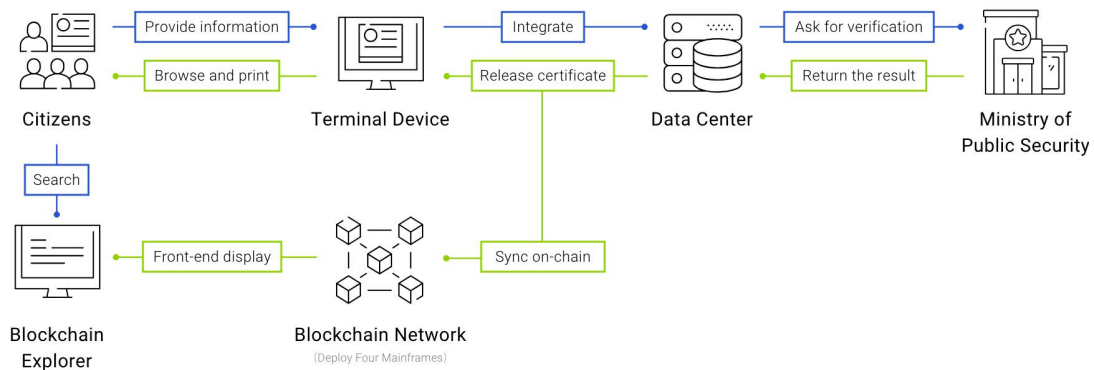

Figure 17

7.3.3 Technology implementation

The project will use the Vapor sidechain as the bottom layer. Phase one is to record information on blockchain. At present, the Data Resource Management Data Center and the Ministry of Public Security database will validate blocks and upload data. Data will be formatted and encrypted according to business needs before being uploaded. The parameters of the overall blockchain service are configurable. The consensus mechanism will initially based on DPoS and the block interval will be adjusted according to the actual service throughput.

In the future, the system will be updated to comply with collaboration needs across government sections so that the consensus of citizen ID could be formed among different departments or even cities, thus lowering maintenance cost of public services and improving efficiency.

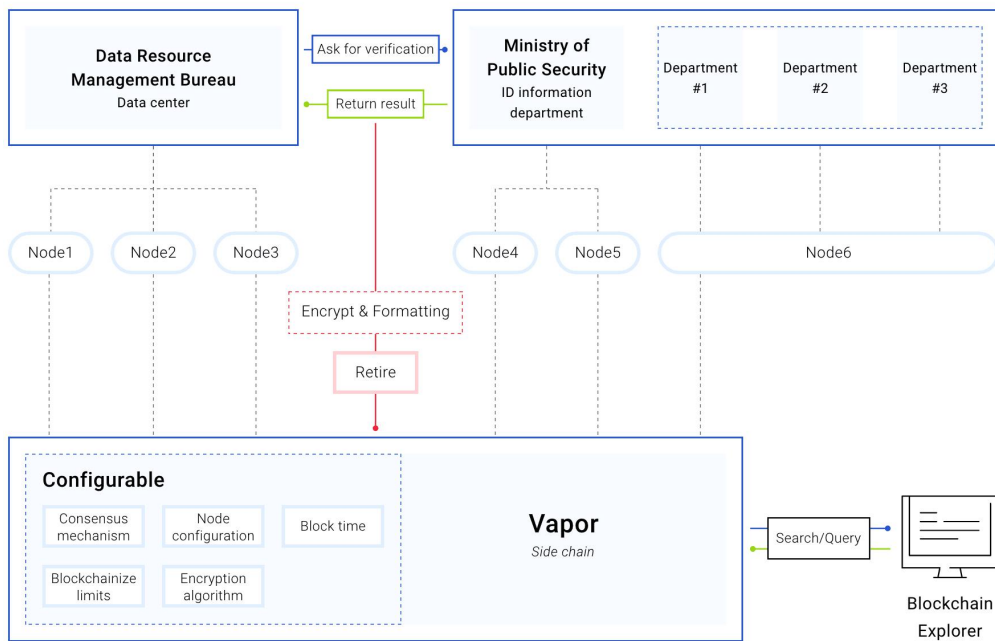The technical implementation architecture is shown below:

Figure 18

7.3.4 Project Significance

（1）After the citizen applies for the identity certificate, the query record is generated

synchronously on blockchain, and the status of the identity information can be queried in real time through the serial number;

（2）Different government departments jointly maintain system data through nodes and use the data on the blockchain as the proof and record of the workflow;

（3）The system itself is highly scalable, and can be easily extended for citizenship information systems and other government systems that requires collaboration between multiple sectors. This also provides a feasible solution for inter-departmental, cross-city and inter-provincial collaborative government offices.

With Bytom and its sidechain being implemented in a provincial government, it is a clear evidence that Bytom has reached the requirements of the municipal government system in terms of underlying technology and data security. Bytom will continue to provide blockchain service in government sector with Bytom and its sidechain technology.