

White Paper of IBBF Project

I Blockchain Bank Fund Project

www.ibbf.io

I Blockchain Bank Fund Project Team

March 2018

Contents

Introduction.....	1
Chapter I. Project Background.....	2
I. Industry Background.....	2
II. Elaboration of Digital Currency.....	3
III. Market Demand.....	4
Chapter II. Project Presentation.....	6
I. Project Mode.....	6
II. Application Scenario.....	9
III. Technology Implementation.....	10
IV. Technical Feature and Advantage.....	13
Chapter III. Management Structure.....	17
Chapter IV. Presentation of IBBF.....	18
I. IBBF Profile.....	18
II. Issuance Plan.....	18
Chapter V. Risk Warning and Disclaimer.....	20

Introduction

As blockchain 1.0 (with Bitcoin as the representative) and blockchain 2.0 (with Ethereum as the representative) become more and more mature, the blockchain has developed beyond the conceptual stage, and will enter into the stage of blockchain 3.0. Blockchain 3.0 will break through the range of cryptocurrency and financial application, and get integrated into the practical application in various industries, so as to enable users to experience the true value of blockchain.

Since the birth of Bitcoin, the digital cryptocurrency has gradually set off a wave worldwide. Most of the blockchain projects have their own digital currency which can be used in different scenarios. With profound inherent value, some digital currencies also find wide application in investment and trading. Due to the technical features of blockchain, digital encryption must be acquired through a certain recognized mechanism (commonly known as “mining”). The recognized mechanism is positively correlated with the computing power of device. The higher the computing power is, the more possible the digital cryptocurrency will be acquired. As the mining process advances, individual device can hardly compete with professional mining device in terms of computing power.

IBBF (I Blockchain Bank Fund) project enables common users to benefit from the digital cryptocurrency. IBBF uses the collected funds for the operation of supercomputing machines which are distributed in the cooperative data centers worldwide. In the official website of IBBF, the Fund will display the computing amount of global devices, the output quantity of ETH and the ETH value available for each IBBF coin held.

IBBF is also the equity token of project. The token value anchors the total revenue and profit of IBBF. It can be not only used as the platform’s medium for value circulation and transaction (such as the computing power purchase, agreement on artificial intelligence, game payment and settlement, etc. on the platform), but also used to apply for mortgage loan to the Fund so as to obtain other digital currencies. IBBF uses scrypt as the core algorithm, and POW as the issuing mechanism. With a constant issuing amount of one billion, it has the open source code and independent offline purse, and supports open stock market transaction.

Chapter I. Project Background

I. Industry Background

Blockchain is a distributed database system participated by all nodes. It is inalterable and unforgeable. It can also be interpreted as a distributed account book system.

Blockchain is made up by a string of data blocks generated by the cryptological method, with each block containing the hash of the last block. A blockchain is formed by establishing connection from the genesis block to the current block. Each block should be generated in chronological order, otherwise hash of the last block will become unknown. All these features make Bitcoin double-spending quite difficult. Blockchain is the core innovation made to Bitcoin.

The basic principle is that the timestamp server randomly hashes and affixes a timestamp to a group of data which exists in the form of block, and broadcasts this random hash, just like posting a message in the news network or the world Usenet. Obviously, this timestamp can prove that specific data truly and definitely exist at specific time, because only when the data does exist can the random hash value for such time be obtained. Each timestamp should include the last timestamp in its random hash value, and each following timestamp should reinforce one previous timestamp, thus forming an inalterable chain made up by data blocks.

Blockchain has the following features.

1. Safety: A little sacrifice of efficiency will gain an extremely high safety. The system doesn't have a central (decentralization) account book, so it is indestructible. As a little part of the system, every node has equal rights and an identical account book. Hence, destruction of partial nodes exerts little influence on the whole system.

2. Reliability: Once the verified information is added to the blockchain, it will be stored permanently. It is useless to modify the database on a single node, unless 51% of the nodes in the system are controlled simultaneously. That is to say, though hackers can control a small number of computers to modify information, the system still judges what is the real truth by referring to opinions of the majority. Hackers will find it meaningless to change their own account books (for others will not acknowledge it).

3. High efficiency: Without a centralized intermediary, everything operates automatically according to the re-established program, which not only reduces cost significantly, but also improves efficiency. For the reason that everyone has an identical account book, the process of bookkeeping is made absolutely open and transparent.

4. Smart contract: Smart contract is a kind of contract with its terms and articles recorded with computer language instead of legal language. It can be performed automatically by a computing system. For users, smart contract is generally considered as an automatic secured

account. For instance, the program will release and transfer funds once specific conditions are met. Technically, smart contract is considered as a network server which is set up on the blockchain, instead of in the Internet environment with an IP address, so that specific contract program can run on the blockchain. Smart contract has a lot of potential advantages, such as reducing the cost of contract signing, implementing and supervising. Therefore, for many contracts concerning lower-value transaction, it greatly reduces the labor cost.

As a kind of universal underlying technical framework, blockchain will bring about a profound innovation to the fields of finance, economy, science and technology, politics and so on. According to the current development process, the blockchain technology will go through blockchain 1.0 mode (featuring the programmable digital cryptocurrency system), blockchain 2.0 mode (featuring the programmable financial system) and blockchain 3.0 mode (featuring the programmable society). All these modes develop in parallel instead of in an evolutionary manner.

II. Elaboration of Digital Currency

(I) Basic Concept

Digital currency only appears in the Internet environment in the form of electronic money. The digital currency issuer can be an individual, an organization, a company or merely a set of software system. Digital currency is mainly divided into the currency issued in a centralized manner and the cryptocurrency issued in a decentralized manner. The difference between the two is that the former has a certain individual, organization or company as its issuer, with the issue volume and issue mode controlled by such individual, organization or company and changed anytime as required. The representative digital currencies issued through centralization include Q-coin, e-gold and XRP of the Ripple system.

In contrast, for digital currency (Cryptocurrency. It is a kind of digital currency created, distributed and maintained by the encryption technology and checking technology so as to ensure no double-payment will occur, which is also referred to as cryptocurrency.) issued through decentralization, its issue volume, issue mode, issue speed and other elements, are defined by its initial issuer (an individual, an organization or a company), and then it is operated by a P2P (Peer to Peer) online system. The key parameters, such as issue volume, issue mode and so on, can no longer be modified upon the issuance. The representative digital currencies issued through decentralization include Bitcoin, Litecoin, PPcoin and so on.

(II) Digital Currency Transaction

Since its birth, digital currency has been very active. It does have sort of speculative property which is caused by the convenience and flexibility of digital currency in circulation and payment, as well as the expectation on the decentralization object of global assets. As

CoinMarketCap data suggests, up to the end of December 2017, there were 1,300 kinds of cryptocurrencies worldwide, with a total market capitalization over 600 billion dollars, worth up to 624.9 billion dollars, among which the market capitalization of Bitcoin reached 318.5 billion dollars, accounting for 51% of that of cryptocurrencies. It is indicated by Sina's US Stock data that the market capitalization of the world-famous enterprises, such as HSBC Holdings (569.642 billion dollars. The market capitalization given in the bracket is the latest. The same below), Amazon (569.317 billion dollars), facebook (524.958 billion dollars), Berkshire Hathaway (492.171 billion dollars), Alibaba (441.667 billion dollars) and so on, has been surpassed by cryptocurrencies. It is predicted that by 2018, the total market capitalization of global digital cryptocurrencies will reach a trillion dollars.

It can be seen from the above-mentioned data that from early 2017, stimulated by the rising trend of blockchain and digital currency, tokens of different kinds have become more and more popular. Many large exchanges, such as Bittrex and Poloniex, have their monthly visitor volume rise sharply from several million to over ten million, and have their daily trading volume reach up to RMB five billion yuan. Given that the transaction fee is 0.2%, they can gain a daily income of RMB ten million yuan. Currently, the market is still expanding rapidly. Governments of the global countries have changed their attitudes towards blockchain assets from prohibition, acceptance, support to legislation, meaning that the blockchain asset is one of the major developments in the future. Technologies such as digital asset blockchain are the very innovations made to and needed by the financial industry.

III. Market Demand

【Mining】 : In the decentralized blockchain network, the bookkeeping right is obtained through a certain recognized mechanism. Presently, the commonly recognized mechanisms include POW and POS. The process of using computer hardware to do arithmetical operation for blockchain network is simply a process of keeping piecing together the character strings and computing SHA256 hash until suitable hash string which is the solution, is found. The one who finds the solution gains the right to bookkeeping and will be rewarded with a certain number of digital currencies. This process is referred to as mining.

As the mining process advances, an astronomical computing power is required, which common computing devices do not have. In the Bitcoin network, it may take tens of thousands of years for a single set of personal computer to obtain the right to bookkeeping. Under such circumstance, professional mine field comes into being, in which plenty of special-purpose mining machines are used for mining. For common users who can not afford so many mining machines but desire to participate in mining, cloud mining is no doubt their inevitable choice.

【Cloud mining】 : Simply put, cloud mining is to buy the computing power generated in the large mining pool. Users buy the computing power needed, while it is the job of remote data center to get other things done and to do mining. After revenue is generated, a high dividend will be passed according to the proportion of computing power bought.

Currently, many common users have engaged in “remote” mining in this way, for the reason that it requires no additional electric power cost and that users can get the revenue without buying any equipment. However, cloud mining also has its own problems, including:

1. Centralization risk: The great thing about blockchain is centralization. However, in the process of cloud mining, centralized structures will appear, which may cause material risks of fraudulent practices and the decline of transparency. What’s worse, the service providers may even suspend the operation.

2. Low gains: People who participate in mining by means of cloud mining will not make a great profit, because it is decided by the digital currency agreement that the more people mine a limited quantity of tokens, the less possible they will find it.

3. Unpromising prospect: Cloud mining is generally done by large mining pools which have a single mode of profit-making and a poor anti-risk capability. Hence, it is very hard for common users, as investors, to grow with the platform.

4. Less service contents: These mining pools basically engage in mining only, and will hardly provide other services. Hence, common users can not have satisfying experience.

To sum up, it is found out that cloud mining is a major way for common users to obtain the original blockchain digital currency. However, the mode of cloud mining does have a lot of problems. How to meet the demand of users? How to avoid these problems?

Chapter II. Project Presentation

I. Project Mode

(I) Project Mode

IBBF will use the collected funds for the operation of supercomputing machines which are distributed in the cooperative data centers worldwide (Figure 1). In the official website of IBBF, the Fund will display the computing amount of global devices, the output quantity of ETH and the value of ETH available for each IBBF token held (Figure 2).

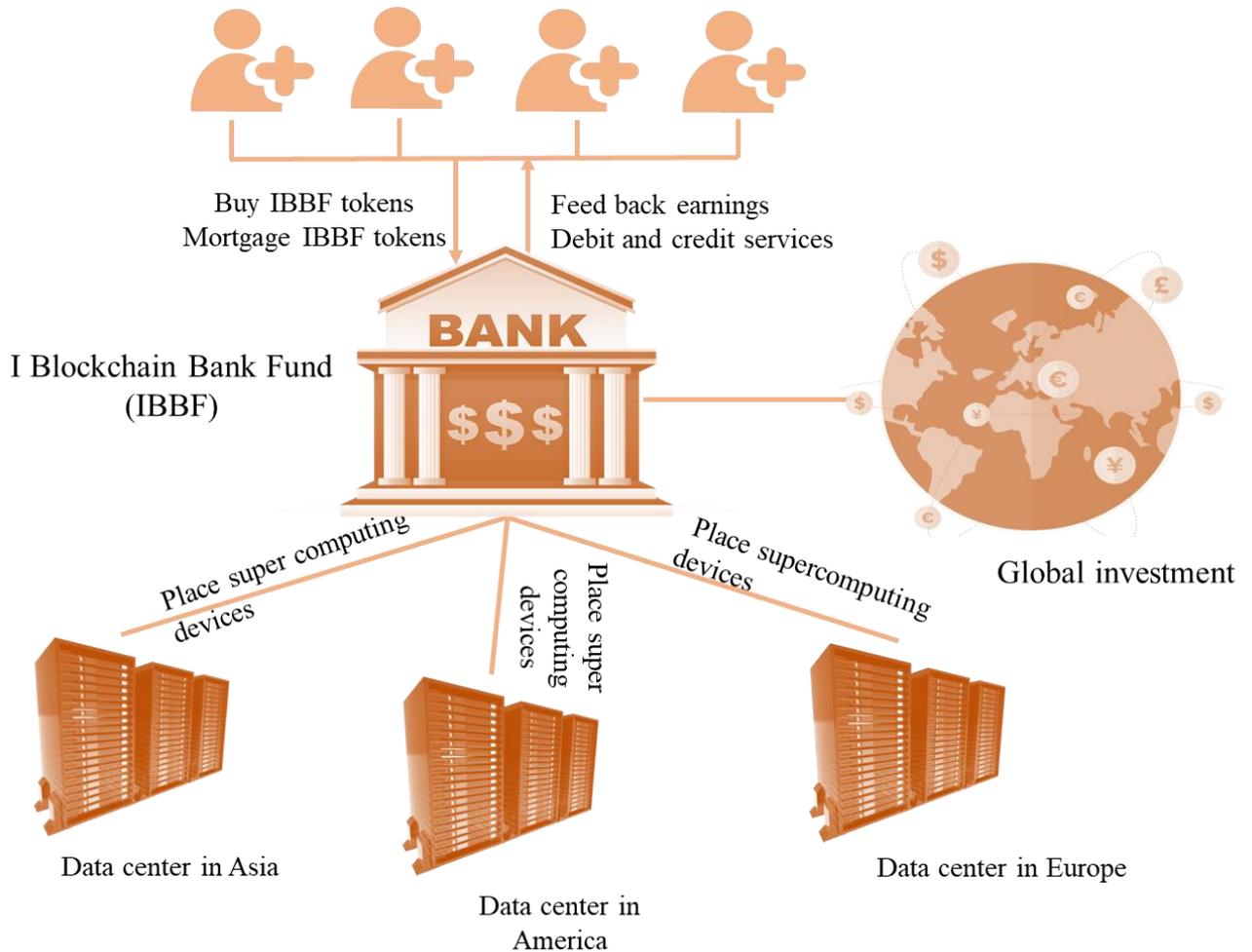


Figure 1. Project Mode

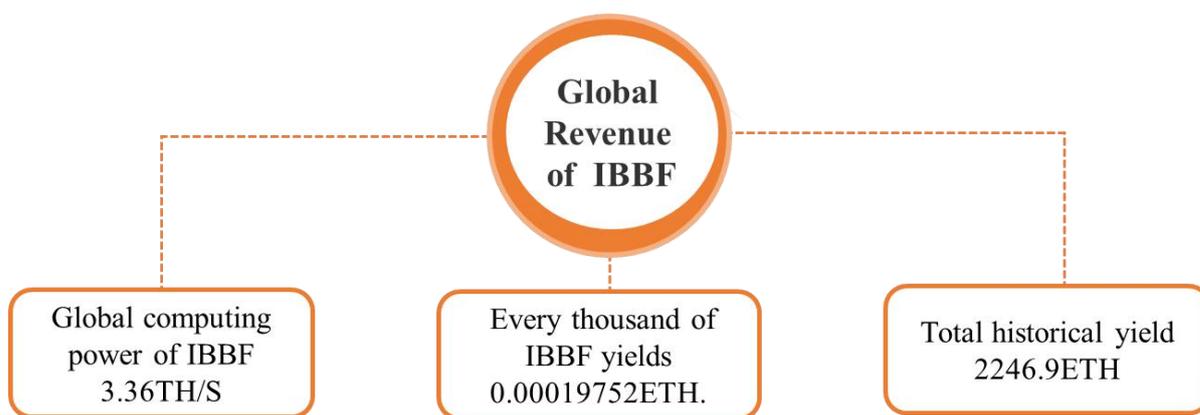


Figure 2: Schematic Diagram for the Global Revenue of IBBF (Real-time Update by the Website)

All the ETH tokens yielded by operation of the Fund will be distributed in the following way:

$N \times 80\% / 1 \text{ billion} = \text{Interest of each IBBF token holder (N represents yield)}$

$N \times 20\% = \text{Operation cost (In case 20\% is insufficient to make up for the cost, the rest will be covered by the Fund. In case the operation cost is less than 20\%, the surplus will be injected into the Fund.)}$

The Fund will hold 50% of IBBF tokens. The yield from ETH tokens will be used to buy more equipment. Theoretically, the number of ETH tokens obtained by each IBBF token holder will rise continuously.

(II) Service Content

IBBF will get the following services (Figure 3) online in chronological order.

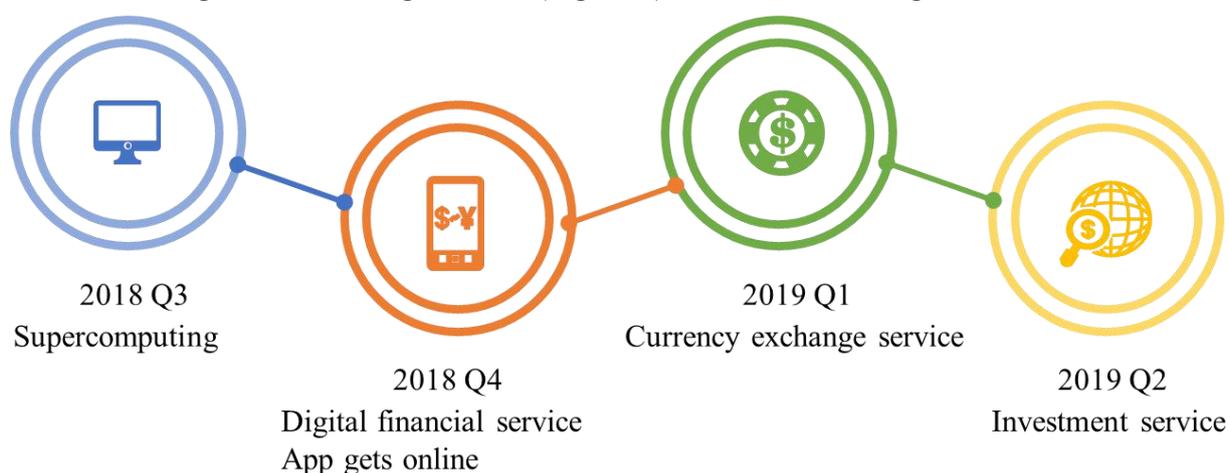


Figure 3: Service Content of IBBF

1. Supercomputing: IBBF uses the collected funds for the operation of supercomputing machines which are distributed in the cooperative data centers worldwide. In the official website of IBBF, the Fund will display the computing amount of global devices, the output quantity of ETH (and other mainstream digital currencies) and the value of ETH (and other

mainstream digital currencies) available for each IBBF token held.

2. Digital finance: The Fund provides the services such as digital currency loan. Users can mortgage the IBBF they hold to the Fund through the APP to be released, so as to obtain digital assets such as ETH, Bitcoin and so on. In addition, users can deposit the virtual currency of various blockchains in the IBBF platform to earn interest, or can decide the investment behavior (Figure 4) of the IBBF community by means of balloting. The Fund will aperiodically make buy-back with the ETH gained by IBBF and managed by the foundation, so as to keep the market value of IBBF.

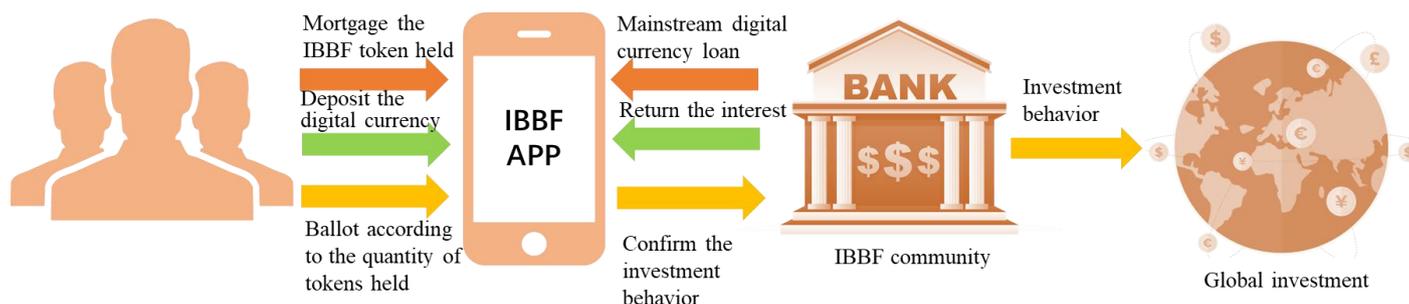


Figure 4: Service Mode of Digital Finance

3. Assets exchange: To facilitate the participation in the activities of IBBF platform by users holding other mainstream digital assets (BTC, ETH and so on), IBBF specially develops the exclusive purse which will integrate the transaction interface of the digital asset exchange. Using the exchange function of the purse, users can rapidly exchange IBBF and other digital currencies according to the real-time exchange rate provided by the exchange.

4. IBBF investment: IBBF will establish a professional investment team, and will make investment with the assets in the fund pool (including self-mining, users' mortgage and deposit) to earn profits.

(III) Solution to Pain-point Problem

With the blockchain technology, the Project is able to give a thorough solution to the above-mentioned pain-point problems. The detailed method is shown as follows.

1. Open, transparent and unalterable: The blockchain technology can guarantee the benefit of investors, and make all information of the platform, such as investment direction, profit-making condition and so on, open, transparent and unalterable. IBBF public blockchain thoroughly eliminates the malpractices such as fraud, fraudulent practices and so on, and solves the pain-point problems of this industry. For instance, the centralized organizations are unable to prove their innocence. In addition, based on a completely open and transparent environment and the universal supervision, IBBF public blockchain can also establish a credit system for the industry, so as to encourage participators to follow the spirit of contract and keep the platform in good order.

2. Smart contract delivery: With the help of customized smart contract, IBBF public blockchain achieves the assets delivery for various transaction scenarios and of different complexities, which eliminates the risk of breach of contract between participators and enables interests of participators to be deducted or arrive in a safe, timely and unobstructed manner. The pre-established smart contract can also go across time and space to achieve the forward assets delivery. Once the triggering condition is reached, the smart contract will be performed directly or provide evidence.

3. Encipherment protection: The encryption property of purse address, digital asset and other blockchain data helps to effectively protect information of all users, especially to protect the private information of mid-to-high-end clients, thus enhancing reputation of the platform and improving the service level of the platform.

4. Multiple services to guarantee your gains: IBBF expands the traditional cloud mining in a financial way. It earns profit not only by means of digital currency transaction but also by means of external investment increase, carry trade and so on. Multiple services help to balance the rate of return and guarantee users' income level. Most importantly, they make the platform more active, and provide the motive force for the sustainable development of the platform.

It can be seen that IBBF mode is proposed specially to solve the problems arising from the current cloud mining. IBBF, by grafting financial means on the digital currency mining, has fully applied blockchain's property of solving transaction mutual-trust issues to the mining industry. IBBF can greatly reduce the trust cost between users and the data center. Besides, multiple services help to reduce profit-making venture for users and improve user experience. IBBF blockchain system will be the most important link in the reform of digital currency mining ecology.

It is worthwhile and meaningful for IBBF to exist, as long as there are recognized mechanisms for digital currency. We can imagine that tokens can be used in many scenarios in the global digital currency industry chain, which provides abundant value support for the implementation and application of IBBF.

II. Application Scenario

(I) Investment with Digital Assets

IBBF project can effectively gather the assets of clients which are used to concentrate computing power to do mining so as to make gains (and to buy more equipment with the mining gains so as to form a benign cycle) on one hand, and to underpin the price of IBBF's digital asset through financial means such as mortgage loan, foreign investment, buy-back and so on, and improve the income level of investors on the other hand. It is believed that this mode of making investment with digital assets will become the major way for common users to gain

digital currency in the future.

(II) Anti-fraud and Anti-forgery

Fraud and forgery are the major risks in the cloud mining by centralized organizations. To prevent forgery, a perfect combination of big data and blockchain technology can be used. In the blockchain, data is jointly recorded and stored by each transaction node which can check the data and testify the data jointly, thus enhancing the authenticity of data. A single node is not allowed to increase, decrease and change data at will, thus reducing the possibility of a single node to fabricate error data. For instance, a private blockchain is established within the transaction platform in which a client is a node. On one hand, it avoids that mass data is recorded and stored by a single information center, thus reducing operational risks. On the other hand, the unilateral forgery can be contained by means of verification, thus ensuring the authenticity and validity of data. If people want to have the forged data pass the verification by the blockchain network, they have to control over 50% of the chain's computing power. However, when there are too many nodes, the cost of controlling the private blockchain will rise sharply. In addition, each node of the blockchain has a complete data copy, so data will get lost only when the entire blockchain system goes down. Besides, data can no longer be modified once it is recorded. Hence, being open, transparent and safe, the blockchain can improve the quality of data from the source and enhance the capacity of data verification .

(III) Establishment of Credit System

Blockchain will significantly reduce the credit cost. In the past, we used to protect the stability and unforgeability of monetary credit with laws and weapons. However, with the help of blockchain technology which has the unforgeable property and does not support double-spending, we can establish credit quite easily. At present, separation of money and account features the existing financial system. In the blockchain, money and account are integrated into one, so that books can be balanced in real time instead of being audited afterwards. Thus, a mutual trust mechanism is established between the platform and users.

(IV) Digital Currency Exchange Platform

As required by the development of business, IBBF public blockchain will develop and operate, or jointly operate a digital asset transaction platform, so as to provide a channel for the exchange, transfer and realization of various digital currencies.

III. Technology Implementation

(I) Technical Framework

IBBF is researched and developed completely based on C++ platform. The framework independently developed by our project team is used in the back end, Angular.js framework in the front end, QT framework in the client-side, leveldb in the database, C++ encapsulation

script language in both the front end and the back end, and qt-crossplatform in the interface. With its inborn asynchronous processing mechanism and powerful cross-platform advantage, it is quite suitable for the time-based real-time and interactive cryptocurrency applications, and provides solid safeguard for the high-performance instant messaging of IBBF.

(II) Side Chain

After the script engine is perfected by Bitcoin, it not only gains the function of common transfer, but also achieves the smart contract functions such as multi-party signature, mortgage guarantee, gaming and so on. However, out of consideration of the safety and the realization difficulty, the script system for Bitcoin is designed to be very crude, and has many limits. For instance, it does not support looping, and supports only several kinds of standard transactions; script length is limited. The great thing about Ethereum is that it significantly expands the function of script engine, has more new instructions such as reading blockchain, billing, skipping and so on, and also releases the limits on stack memory, function calling depth and script length.

Since the birth of Ethereum, extending the script has become a popular way to realize the decentralized development platform. However, it has a major disadvantage that the application code and the data generated by the application exist in the same blockchain, thus causing the blockchain to expand rapidly. Ethereum attempts to delay such expansion by optimizing and compressing the blockchain and the transaction itself, but it only deals with the symptom, not the cause. What's more, the script-based applications share one same account book, so parameters such as blockchain generation time, cannot be customized, which no doubt limits the personalization of applications.

The side-chain mechanism achieves extensibility through another dimension. Every side chain runs in different distributed node network, and has its own audiences, investors and development teams. Such natural dividing solution settles the expansion of blockchain. For the reason that each application has a set of personalized account book, its recognized mechanism, blockchain parameter and transaction type can be customized. Therefore, it is believed that side chain is a solution which is more cost-efficient, flexible and user-friendly than the complete transaction script.

Developer can also use IBBF side chain to have an in-depth customization of its own decentralized application DAPP. The side chain can be hosted in an independent client node cluster, thus naturally forming a dividing mechanism and delaying the expansion of main blockchain. Each DAPP corresponds to a side chain. The core logic of the side chain is developed with c++. The front end and the back end communicate generally through the json IBBF protocol.

(III) Account

In Bitcoin and its derived system, there is no such account to store users' balance which is

handled by switching the transaction status of the entire system. Here, a term will be introduced, UTXO (unspent transaction outputs). Each UTXO has a face value and its owner. A transaction has one or more inputs, and one or more outputs. Each input includes an reference of the existing UTXO and a cryptographic signature created by the private key that corresponds to the owner address. A user can consume the currency value of this UTXO, if he owns the private key. That is to say, a user's account balance is the total currency value of UTXO that corresponds to all private keys he holds.

The major advantage of UTXO lies in its high privacy. User can generate a new address for each transaction, so as to make the user untraceable. It is great for currency, but not good for various DAPPs. For UTXO, the account has the following advantages.

1. Save space. For example, if a user has five UTXOs, a memory space of $(20 + 32 + 8) * 5 = 300$ bytes (among which the address occupies 20 bytes, transaction number occupies 32 bytes, and transaction volume occupies 8 bytes) will be required, while the account only requires $20+8+2=30$ bytes (The address occupies 20 bytes, balance occupies 8 bytes and random number occupies 2 bytes.).

2. Facilitate supervision. Account makes it quite easy to differentiate digital currencies. What we need to do is to make clear which accounts these tokens come from.

3. It facilitates the encoding and understanding.

4. Constant reference. The light client can have access to any data of a user's account at constant time. In the UTXO system, data reference will change once transaction occurs.

IBBF is not a pure currency system, for it contains diverse applications. In contrast, account is a better choice for us. Different from Bitcoin, each IBBF account is made up by a password, a pair of public and private keys, and an address. Users can set a secondary password. To make it more mnemonic, we convert the 128-bit entropy into 12 words. The password is kept by the user, and will not be open to the public. Once it is lost, the user will lose the ownership to corresponding account.

(IV) Relational Database

Currently, most of the blockchain systems use the non-relational databases with a simple model, such as Berkeley DB, LevelDB and so on, to store data. Generally, these databases only provide some simple data structures such as B-tree, hashtable, queue and so on, and do not support the operation of data by SQL. These databases are enough for the electronic currency system, but are far from enough for application platforms, especially in the fields of finance, banking, e-commerce and so on. At present, all the mainstream memory systems have used the relational database which has the following advantages.

1. Transaction processing;
2. The cost of data update is very small.
3. Complex queries, such as join, can be executed.

Sqlite used by IBBF is a kind of high-performance lightweight embedded relational database with a maximum capacity of 2T. Data file can be freely shared by machines with different byte orders. Especially, it supports SQL, which brings great convenience for dapp developers.

(V) Sandboxie Mechanism

IBBF system uses the vm module of VirtualBox to achieve the Sandboxie mechanism. Retaining the cross-platform advantages, VM module is the encapsulation of virtual machine parsing engine. It can be used to execute the pure intermediate logic code, but cannot use the api at the system level, such as file system and network-transmission-related module. Besides, for the reason that it does not have the require function, the third-party library cannot easily be imported into it. Even it is not able to carry out the modularization development. Under such circumstance, DAPP developers need to use browserify technology to package the frequent-used third-party libraries into a script file, so as to load the IBBF main chain system and have it run. Some essential system-level apis, will be provided for the side chain by means of interprocess communication, which gives consideration to both safety and function completeness.

(VI) AI Drive

CapsNet is structured based on CNN algorithm, and uses the latest deep learning method to make data analysis and to predict the fluctuation of financial asset. Except the last layer, other layers of the network are the convolutional layers which all belong to the Capsule network layer. In this network, CNN scalar feature output is replaced by vector output, and the max-pooling is replaced by consistency data which is similar to CNN. A larger scope of data is observed at a higher level of the network, and the max-pooling is no longer used. For these reasons, the feature information of network data can be retained forever. For the lower layers, their spatial location can be judged only by checking which Capsules are activated. The multi-dimension Capsule at the bottom layer of the network exhibits varied characteristics. For a high-order network system, such method potentially solves the problem that how a complex issue forms an entirety level by level.

IV. Technical Feature and Advantage

As plenty of data tests and data analysis suggest, IBBF blockchain can achieve transaction verification in seconds, storage of mass data, high handling capacity and rapid synchronism of node data in terms of performance, and offers permission control strategies and a structure which meets the requirements of multiple business blockchains in terms of extensibility. Besides, it provides safe access to private key as well as privacy protection solutions.

(I) In Terms of Performance

1. Rapid Transaction Verification

IBBF blockchain can achieve rapid transaction verification in seconds by optimizing the key links such as signature algorithm, book structure, data operation, serialization, recognized mechanism, information spreading and so on. It is able to satisfy the user experience in most of blockchain application scenarios.

2. Storage of Mass Data

Blockchain adopts a mode of double-entry bookkeeping. As the system runs for a long time, historical data will be amassed little by little. By taking advantage of the separate storage and tabular storage of hot data and cold data adopted by traditional financial system, IBBF blockchain achieves the effective storage of mass data. Information, such as the old transaction data, inactive asset data, etc., can be stored in the big data storage platform (such as Hadoop, meeting the PB-level data storage).

3. High Handling Capacity

In nature, blockchain is a kind of distributed shared bookkeeping technology. Its distributed feature shows in the distributed consistency instead of in the non-distributed concurrent processing. To ensure the data consistency and avoid the Byzantine Generals problem, some certain links can only be executed in serial instead of in parallel. Over a long time of testing and optimization, the processing performance of IBBF blockchain has been able to meet the requirement of ten thousand TPS. The transaction handling capacity will be significantly enhanced, in case other mechanisms such as Off-Chain are adopted.

4. Rapid synchronism of Node Data

IBBF blockchain supports the Snapshot mechanism, so it will snapshot local account books at regular intervals, in order to achieve convenient roll-back. Under the uniform consensus, snapshot labels can be designated and rolled-back. Moreover, it shortens the cycle for new nodes to become operative. Only by synchronizing with the latest snapshot and updating a few recent transaction sets, the new nodes can be integrated into the network, and participate in consensus verification.

(II) In Terms of Extensibility

1. Block Chain Structure Designed for Multiple Businesses

With a block chain structure, IBBF blockchain can satisfy the demands of different lines of businesses, and improve system extensibility and maintenance efficiency. It can be used to label and transfer assets, provide unalterable and multi-dimensional record of events and to trace and track circulation of assets.

2. Permission Control Strategy

It provides permission control strategies for data information entry and data information reading. For data information entry permission, several users are arranged under the same account, and permissions are set for corresponding operations, so as to meet the requirement of

usage scenario controlled by multi-party signatures. For data information reading permission, users can grant and withdraw the operation permission for data to and from a single user or user group. The user group can be flexibly configured by users. Data includes users' account information, transaction information and so on. The granularity can be detailed into the attribute fields of transaction or account.

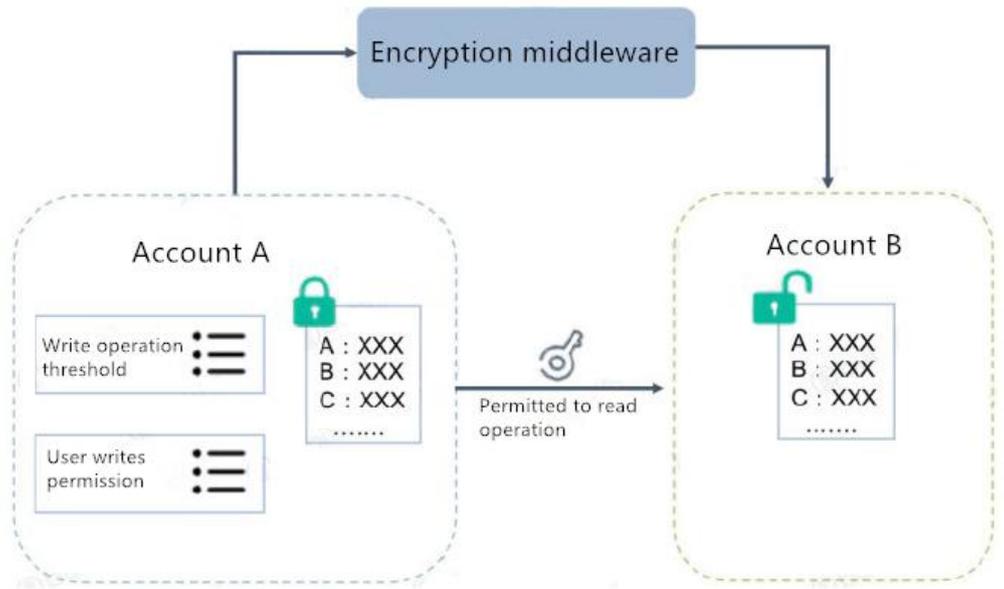


Figure 5: Permission Control Strategy

(III) In Terms of Safety

1. Safe Access to Private Key

To facilitate the use of blockchain products and services, IBBF also provides the solutions for web hosting access and private-key hardware access (U-key), besides the traditional mechanism of generation and saving at client-side. The web hosting access is to map user name and password into a private key through specific algorithms and then save them at the server-side. All private keys saved at the server-side are enciphered data, and can only be deciphered at user side. The hardware private key is created to meet the usage requirement of financial industry.

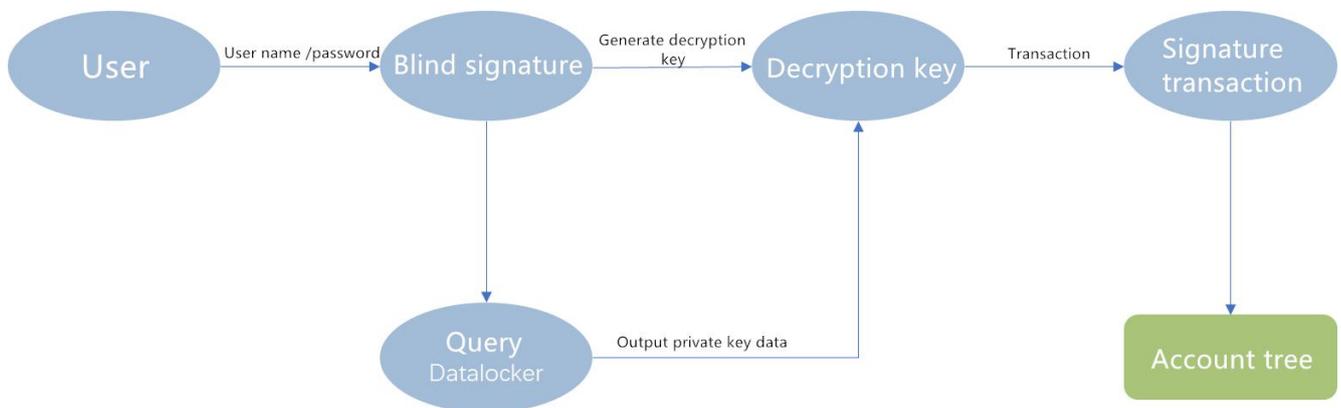


Figure 6: Safe Access to Private Key

2. Multiple Privacy Protection

It provides multiple protection for privacy. Firstly, the bottom layer of the blockchain provides homomorphic encryption to get all user data encrypted and visible to user only. Secondly, IBBF provides encryption middleware which is optional to users as business requires. Finally, the upper-layer application can encrypt data the moment it is entered. IBBF platform is responsible for entering and reading the enciphered data generated by users.

Chapter III. Management Structure

IBBF project is managed by a foundation.

The foundation is devoted to the construction and management of IBBF, and aims to ensure a sustainable development of IBBF project, a safe fund-raising and an effective management. IBBF foundation is made up by the decision-making committee, fund management committee and executive committee. The management framework also includes the operational procedures and rules formulated for daily work and special circumstances.

To avoid split of community caused by the directional and decision-making divergence between community members, the foundation establishes a sound management structure and specifies the general matters and special matters for the management of community. The management structure is designed to ensure a sustainable platform ecology, a high decision-making efficiency and a good compliance in funds management. The foundation has the decision-making committee to exercise the daily power.

Upon the expiration of the term of decision-making committee, the community will elect five core members for the committee by ballot, who should make key and emergent decisions on behalf of the foundation, and should be investigated on credit extension during their terms of office. When the foundation is firstly established, the first decision-making committee will be made up by team members and early investor representatives, so as to accelerate the progress of the project. Upon the expiration of the two-year term, committee members will be re-elected by the community. The decision-making committee has five members, among whom three are team members and the other two are early investor representatives. The 3/5 multi-signature mechanism will be adopted for all decision-making practices.

Chapter IV. Presentation of IBBF

I. IBBF Profile

IBBF is the blood to power the operation of decentralized IBBF ecological system. IBBF is a kind of contractual token used in the scenarios such as purchase of computing power, AI contract, game payment and settlement and so on. In the future, we will encourage all industry-chain entities to develop subchains based on IBBF. By then, IBBF will become the fundamental chain. IBBF will be consumed in the process of data exchange and smart contract performance between subchains and in the process of the asset, information and data exchange between links. Therefore, IBBF will become a smart contractual permit in the ecological system of the Bank Fund.

A total of one billion IBBF tokens will be issued, and will be created by IBBF public blockchain once for all. The total issue volume has been capped, and shall not be changed and increased. IBBF tokens are distributed to different holders according to specific rules and proportion. A certain proportion of digital chips will be sold to raise fund among suitable groups in proper manner to buy computing power, construct the bottom blockchain, research and develop product module, lay out the application ecology, operate and maintain the public blockchain and so on.

The digital chip IBBF holders can elect the bookkeeper by ballot, and can also participate in the decision-making for major matters of the foundation and IBBF public blockchain e-platform.

II. Issuance Plan

IBBF will be distributed in the following way.

Table 1: Token Distribution Plan

Proportion	Quantity	Distribution Plan	Remarks
30%	300 million	Sold to suitable groups in proper manner	ICO price:1ETH=2000IBBF (about 0.5 dollars)
20%	200 million	Founding team Development team Consultant team	It is used to reward the teams which have made contributions to the construction and development of IBBF public blockchain in acknowledgement of their support to IBBF

			blockchain community project in forms of human resources, technological development, community construction and so on. Tokens will be locked within a year during which they cannot circulate. After the locking ends, they will be released in linear manner by month in two years.
50%	500 million	Fund operation	It is used for operating the IBBF public blockchain foundation, including development, market, operation, service of the third-party organization and so on

Chapter V. Risk Warning and Disclaimer

- As a new pattern of investment, investment in digital assets also has a variety of risks. Potential investors should prudently assess the investment risks and their risk tolerance.
- The document is used to guide the progress of IBBF project, and is only intended for conveying information. It does not provide any opinion for the transaction of IBBF. The above-mentioned information or analysis does not constitute the investment decision. The document does not constitute any investment advice, investment intention or investment incitement.
- The document neither constitutes or should be interpreted as any act to provide any business or to invite people to buy or sell any form of security, nor is any contract or promise of any form.
- Prospective users should make clear the risks of IBBF project. The participation in the investment should be interpreted as that investors have had a good understanding of and are willing to accept these risks, and are willing to take any consequence arising hereof.
- Our project team shall not bear any direct or indirect loss of assets caused by the participation in IBBF project.
- Project risks:
 - Policy risk: Blockchain technology is still in its early development. There will be many uncertainties in the regulatory policies for blockchain project worldwide. The project may face changes in operation body and operation management government.
 - Fluctuation risk: Token for the blockchain project is not a kind of legal tender, and fluctuates greatly in price. Investors should make sufficient psychological preparations to endure such fluctuation.
 - Technical risk: As the blockchain technology advances, it is inevitable that technical bugs and hacker attacks will occur.
 - Team risk: We cannot ensure that in the development of IBBF, some core members of the team may leave office due to pressure, physical reasons, personal reasons and so on. However, we are sure that the replacement of team members will make the project grow more steadily.