BitKeep

wallet

Your Professional Digital Assets Manager

Transactions · Trade · Finance · Deposit · App

White Paper V1.0

2018.10

Catalog

1. Abstract

In the recent years, with the swift development of technology of block chain and decentralization led by bitcoin and Ethereum, which not only attracts more and more people's attention and research, but also creates a revolutionary and new industry. The encrypted digital currency derived from Bitcoin has gradually developed into a brand-new business form. According to statistics, there are 2443 kinds of digital currencies with realized value of circulation, including 1144 of it are the main chain currencies, and the value transmission and storage of each currency need digital money wallet as a medium.

BitKeep is a decentralized multiple chains wallet’s software. It was founded in April 2018 and officially launched in June. BitKeep enters the digital wallet market from these three aspects: product experiments, professional technology and security. Its founding team mainly consists of

top technology companies are domestic and overseas. It has rich experience in block chain technology and human resources and strong technical strength. At the beginning of its establishment, it has received ten millions of investments from top international funds, and registered users have reached 900,000 in four months, now it becomes users' favorite digital wallet.

With a global population of 6 billion, 4 billion Internet users and about 20 million digital wallet users, the proportion of digital wallet users is very small, which is in the early stage of development and has huge market potential. BitKeep can enter this market, its core advantages are: 1) Self-created DESM double encryption algorithm, storage of user mnemonics or private keys, to ensure users' asset security; 2) Support the most main chain, now it is supporting BTC, USDT, ETH, EOS, NET, ONT and other main chains and tokens, and planning to add 20 new main chain currencies in the near future; 3) Deluxe experience of product interaction and multiple product innovation services.

BitKeep advocates the designing concept of combining the decentralization with centralization. It combines the product experience with technological revolution perfectly, and provides users with a safe, simple and easy-to-use one-stop asset management platform. It hopes to

become a bridge which connects the block chain technology and users, and help users realize asset management and value-added, and participate in the revolution of the world.

2. Background

2.1 The Current Status of Digital Wallet

Most of the assets by users are majorly in exchanges. Because of the factor of centralization, the assets of exchanges are extremely unsafe and can be removed by exchanges or hackers. In two recent years, reports of the stolen assets of exchanges are everywhere. Therefore, users need a truly decentralized multiple chains wallet to manage their digital assets.

At present, there are hundreds of competitors in the field of digital wallet. However, there are still some big problems in product experience and safety, such as inconvenience of currency management, insufficient currency support, low transferring speed, insufficient security, lack of extensive application of scenarios, high threshold of use and users who do not understand block chain technology could not use it properly.

2.2 Vision of The Future

BitKeep devotes itself to build a comprehensive digital asset `managing platform, which is driven by technology and services, to provide users with a safe, simple and easy-to-use wallet software. In addition to meeting the basic transfer and collection and security needs, it can also provide a one-click transaction, financial management, debit and credit, value-added circulation, payment, play Dapp and other kinds of. The auxiliary functions are like the global software Alipay in the Internet world, and BitKeep is born for this future.

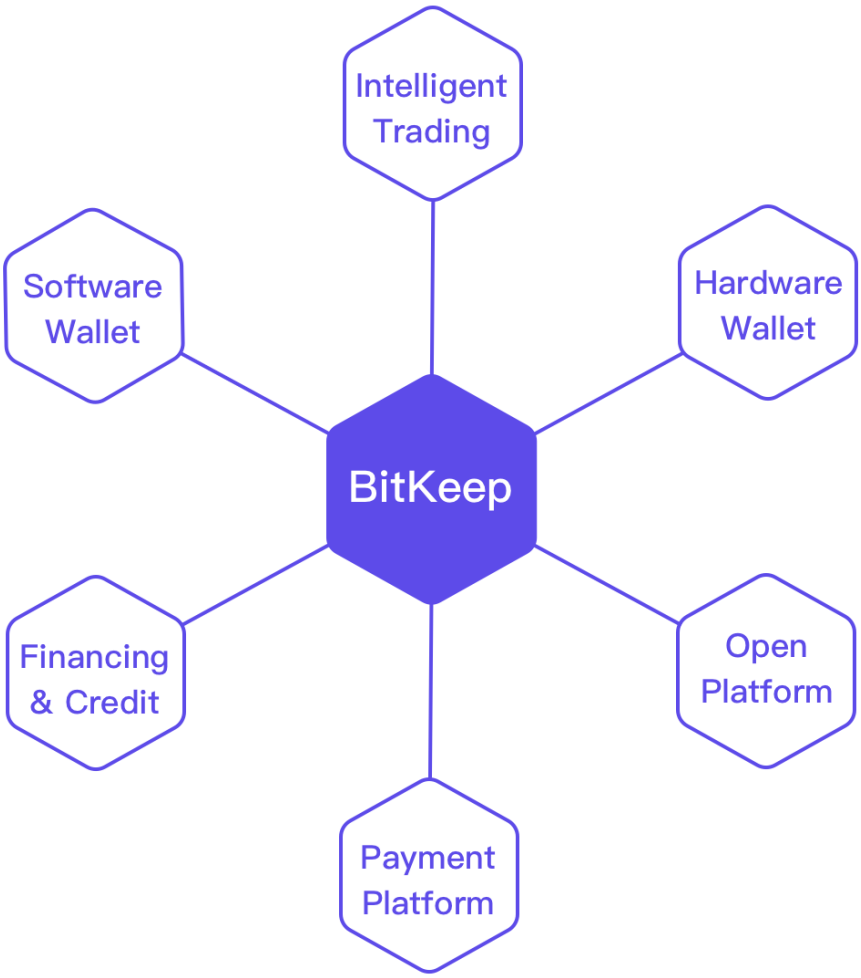
3. Intro of BitKeep

2.1 The Current Status of The Project

BitKeep launched iOS and Android versions in June 2018, which solved the problem of one-stop management of user assets and connects with several exchanges to manage user assets on exchanges. Over the past four months, the project has maintained the a jogging speed of principle of agile development. More than 20 versions have been released. As of October 2018, the total registered users had exceeded 900,000, and the total assets of users reached 100 million US dollars, which is still increasing.

In September 2018, the open platform of wallet was released to provide developers with a set of centralized wallet solution. A few lines of code can have their own centralized wallet service. At present, we have cooperated with many partners of the project to integrate the centralized wallet service into their products, including Money World, House of Leek , Three o'clock Community, etc.

2.2 The Structure of Services



Software of Wallet

The use of Software of wallet is a decentralized and online wallet. User's mnemonics or private keys are encrypted and stored locally, and the user is guided to backup. The cloud will not save users' information. Its core functions includes:

·Supporting multiple chains and various Currency

The major task of BitKeep is to continuously access all kinds of new main chains to meet users' various currency needs. At present, it supports BTC, USDT, ETH, EOS, NET, ONT and other main chains and tokens. Currency access including basic functions such as checking balance, transferring and receiving, transaction record, and some specific rules of the currency, such as EOS resource management, etc. BitKeep cloud deploys at least two full nodes for each chain. On the one hand, it deals with disaster tolerance of capacity processes to ensure that the user's experience will not be interrupted. On the other hand, block reading data and writing data are separated to avoid the possibility of malicious attacks on nodes.

·Management of Multiple wallets

BitKeep can create multiple wallets under a single account, and each wallet can be loaded into multiple currencies to support it, so that users

can feel free to switch their wallets to meet different scenarios of applications.

·Real-time display of currency values

BitKeep converts the balance of assets in it's wallet into the display of French currency assets in it's country, such as RMB or US dollar, by connecting data from major global exchanges. It is convenient for users to view their asset status and floating data in real time, and can share floating data to major social platforms with one click, to satisfy the feel of people who want to flaunt or ask for comforting.

·Daap Central Application

Undoubtedly, the wallet is the perfect carrier of Dapp. The wallet browser provides Dapp with the means of user browsing and payment. Users can play many kinds of Dapp without any costs. Dapp Application Center is one of the most important channels in BitKeep software wallet. In the future, it is expected to gradually develop into the excellent applications derived from various chains and access them in the first time. At the same time, BitKeep will also develop some applications by itself to help the industry grow together. In order to help users participate better, BitKeep's Operational Center will continue to introduce excellent Dapp introductory tutorials and more values.

·Functions of Coins

BitKeep introduces the currency applying mechanics in each currency page of details, including the basic functions of currency encyclopedia, currency details, addresses inquiring, block browser, bookkeeping, currency express and some other basic functions. It is convenient for users to have enough knowledge of the currency information so it helps users to make trading decisions. At the same time, according to the peculiarity of the currency, we will introduce some unique play methods, such as BTC cloud mining, free cloud mining bitcoin and so on.

·Issuing sugar envelope

In the world of block chain, Wechat red envelope is different from the money red envelope in other software. BitKeep's sugar envelope issues function which combines its own innovative function---batch of transfers. It uses the idea of decentralization to complete the sugar envelope issuing process with one-click, which is popular with users at present.

·Batch of transferring

Block chains such as Ethereum do not support a single transaction to achieve bulk transfer. BitKeep laboratory develops and deploys bulk transfer contracts according to user needs. Combining with the function

of product , it is very convenient for users to transfer 200 wallet addresses at the same time, which is originally created by BitKeep.

Hardware Wallet

Hardware wallet, also known as offline wallet, comparing with software wallet, in addition to having more security features, it can also give gifts and inheritance, wealth materialized and other values, for the realization of sales cash flow and user entry, also has important strategic significance.

“Golden Brick” will be BitKeep's first hardware wallet, which is expected to be released in December. It is a professional offline wallet service specially designed for BitKeep members. At present, Android system is used for the offline wallet on the market. There are several problems such as time in use by difference, low security and high hardware cost. The "Golden BRICK" uses its own embedded system hardware’s architecture, bank-level encrypting chip and initiating by fingerprint. It has long using time, high security and low hardware cost and other several major characteristics. 2.7 seconds boot speed, 200 milliseconds signature speed, 180 days using time, so that the "Golden Brick" will be more competitive in the market. Hardware is made of nickel

alloy plated mirror and 9H toughened glass film. At the same time, it is engraved with a self-defined name, which shows a full sense of deluxe.

In terms of security, “Golden Brick” uses five tiers of security architecture: 1) hardware architecture when enclosed, which can effectively defend against SPA and DPA totals; 2) customized private transmission protocol to ensure interactive security; 3) three-factor authentication to prevent fake transaction; 4) dynamic verification of fingerprint signatures; 5) 256 Bit cipher-text encrypting of private storage .

“Golden Brick” hardware team has many years of pioneering experience in the field of Internet Intelligent Hardware. It was the earliest team who designs 360 portable WiFi series products with high experience of industrial design and material process design. The members who joined afterwards are more active in cryptography and bitcoin developer’s communities.

Open Platform

·Bcloud

BCloud is a centralized wallet solution launched by BitKeep’s open platform for enterprises. Several lines of code can be quickly accessed, so that each project can have its own digital wallet service. The advantages of centralized wallet service is as in user-friendly, fast transaction, millisecond arrival, etc., which can quickly achieve a higher product service experience for the project side.

The core of centralized wallet is security. BCloud insists that the private key of wallet can't be used in the cloud, uses private room, completely achieves online and offline separately, uses separation of offline and online wallet, offline signature and other security mechanisms. At the same time, it strictly guards against self-theft, and fundamentally solves the problem of private key security.

BCloud provides very convenient access, including SDK and API access,demo of project and the address of the document:https://github.com/bitkeepcom/sdk

·Service of Inquiring Block

The data on the block chain is completely open and transparent, but

when data is used, besides deploying their own block nodes, they also need to know the technical knowledge of the block chain. Although each chain has a special block browser, it is very inconvenient to use because of the differences between the chains and chains and the language barriers. BitKeep’s block inquiring service is to simplify this problem. Users only need to enter any wallet address or transaction ID to query any data related to it, which is simple enough.

Intelligent transaction

The demand of trading currently occupies 80% of the appling scenarios in the block chain world, and several major problems of the exchange are: (1) difficulty in opening accounts; (2) lack of the depths of transaction ; (3) high cost of withdrawing currency, which has become the biggest problem for users. BitKeep wallet pioneered and originated intelligent transactions to solve with users' problems. Through technical methods, we can integrate the trading depth of various exchanges around the world, and achieve the goal of users to buy at the lowest price and sell at the highest price on the whole network. Users no longer need to open accounts on multiple exchanges, but only need a BitKeep account to be able to trade on major exchanges.

At the same time, BitKeep also supports to authorize API of major exchanges in software to manage their assets in major exchanges one-stop,in time-saving and convenient way.

Payment platform

Wallets originally have payment attributes. BitKeep is building a payment platform. Users only need to scan the QR code to realize the payment in any currency quickly. Businessmen only need to register in the back-stage of the payment system to generate their own QR code of receipts. They can choose to settle their accounts through digital currency or through the local currency.

Financial loan

BitKeep wallet is also gradually improving and perfecting the financial system. By October 2018, it has successfully launched two stages of ETH financing and one stage of BTC financing, which can achieve 24% and 12% annually, respectively. It is a leading level in the industry. Loaning products is also about to go online.

4. Safety and technological innovation

4.1 system architecture

The standard C/S architecture is adopted in the software. Besides interface interaction and data storage, Client also implements transaction signatures for all currencies locally. Server mainly implements data reading and broadcasting on block chains, as well as other basic data services.

HTTPS protocol is used for all requests of software. Each request has a unique token authenticating mechanic, which avoids user's operation is being simulated by robot and greatly enhances security.

Cloud services are deployed in a distributed way, with 12 nodes around the world. They can accommodate at least one million concurrent traffic and have higher dilatancy.

4.2 DESM double encryption algorithm

Double Encryption Storage Mechanism (DESM) is a set of algorithms

customized by BitKeep wallet to encrypt and store mnemonics or private keys. There are three kinds of common encrypting methods: 1) information digest encryption, i.e. irreversible encryption, such as md5, sha256, etc., 2) symmetric encryption, such as DES\AES etc., 3) asymmetric encryption, such as RSA, etc., and 3) block chain technology, which uses the third type of transaction signature, public key and private key technology.

BitKeep adopts the combination of encrypting method of sha256+aes256+cloud authentication. Why do we use this combination of encrypting method, we need to understand several preconditions: 1) the wallet transaction must use the private key, so the mnemonic or private key must eventually be able to restore to the real text; 2) the encrypted data needs to be stored in the mobile phone, so the hacker or the thief can get the encrypted mnemonic in the user's mobile phone’s data; 3) any APP code has the risk of being leaked or cracked.

Based on the three preconditions above, we will analyze the problems of conventional encrypting methods: 1) using simple non-reversible encryption, such as sha256. At present, most passwords registered by accounts are stored in cloud database by this encrypting method, which has higher factor of safety, but can not restore real data; 2) by code; A

designated encrypting key is symmetrically encrypted. Based on the third precondition above, the encryption key can be fully disclosed. Some other wallets do not need to enter any password when they are trading, so the security is very low. 3) The user enters a password to symmetrically encrypt each time they use it. When using mnemonics, the user enters the password again for decryption, and the software does not store the user's password. This is also the current use of other wallets. The security is moderate, but there are still some risks. Users usually set their own password is relatively simple or short, hackers can get data, exhaustive traversal, can violently crack the original data.

The algorithm of DESM of BitKeep can be understood as follows: 1) the user sets the transaction password: the client stores it in the cloud after sha256 (password + seed), and returns the new seed based on BitKeep’s account and password; 2) calculates the key needed for symmetric encryption through sha256 (password+account Seed+specific rules); 3) calculates the key needed for symmetric encryption through aes256 (mnemonic code or private key+Key) to encrypt; similarly, users also abide by this principle when entering mnemonic words. This principle has fundamentally solved the problem of security, even if hackers or internal staff can not solve it. Only in one case that is possible to crack the user's cell phone data while knowing the user's transaction password and

account password, as well as the encryption rules in the BitKeep cloud. But this possibility is extremely rare.

4.3 Fingerprint feature code dynamic encryption technology

This technology dynamically encrypts the user's private key based on the user's fingerprint information. The encrypting rules are similar to DESM. The fingerprint information is longer, more complex, more unique and more secure than the password that was set by the users themselves.

4.4 online and offline hot and cold separation technology

The biggest major problem of the security centralized wallet is how to save the user's private key. BCloud adopts the technology of online and offline computer room separately and wallet cold and hot separation. Offline computer room (local computer room) is mainly used for user private key encryption storage, transaction to account and money withdrawal business. The generator room is built independently, the external network can not be accessed, the network can only go in and out, and the data is distributively stored,and deployed in full accordance with cloud services, with strong dilatancy and high security. User’s assets are separated from hot and cold, stored in different hot and cold purses,

ensuring enough safety.

4.5 contract batch transfer technology

Batch of transfers of ETH and any tokens through contract code has been successfully integrated into products, and API will be gradually opened to third parties in the future.

4.6 cross bond trading technology

Through real-time synchronization of the trading depth for each exchange, a unified merger and aggregation can be carried out, so that users can buy at the lowest average price, sell at the highest average price, and divide into different exchanges.

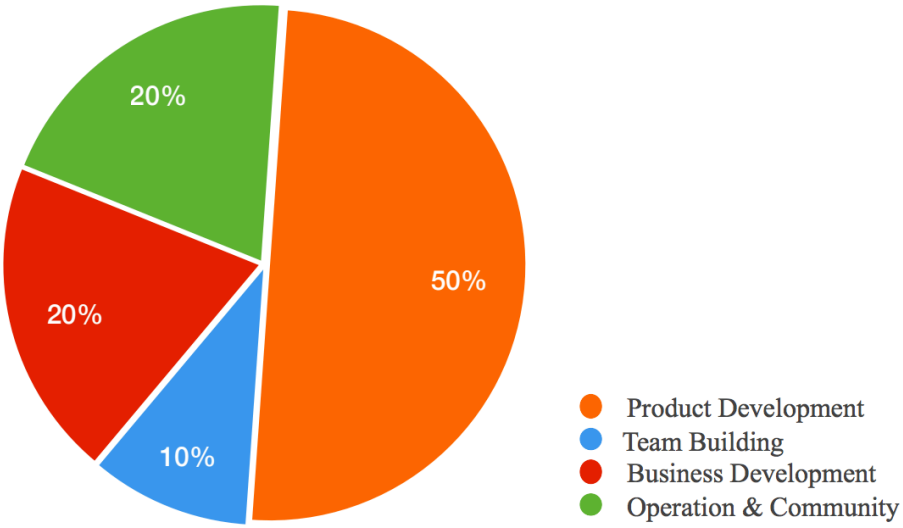
5. Token issuing plan

5.1 Estimated value and pricing

The Token issued by BitKeep is BKB, with a total issue of 10 billion.

Each BKB is priced at 0.02 USDT.

5.2 Token allocation



6.Core Team

7. Cooperating Organization

7.1 Investor

7.2 Cooperator