BitKeep

wallet

Global Largest Multi-Chain Wallet

White Paper V1.1

2019.02

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. 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 multi-chain 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) Support the most main chain, now it is supporting BTC, USDT, ETH, EOS, NET, ONT, TRX, NULS, IOST and other main chains and tokens, and planning to add 20 new main chain currencies in the near future; 2) Self-created DESM double encryption algorithm, storage of user mnemonics or private keys, to ensure users'

asset security; 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 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

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. BitKeep Wallet

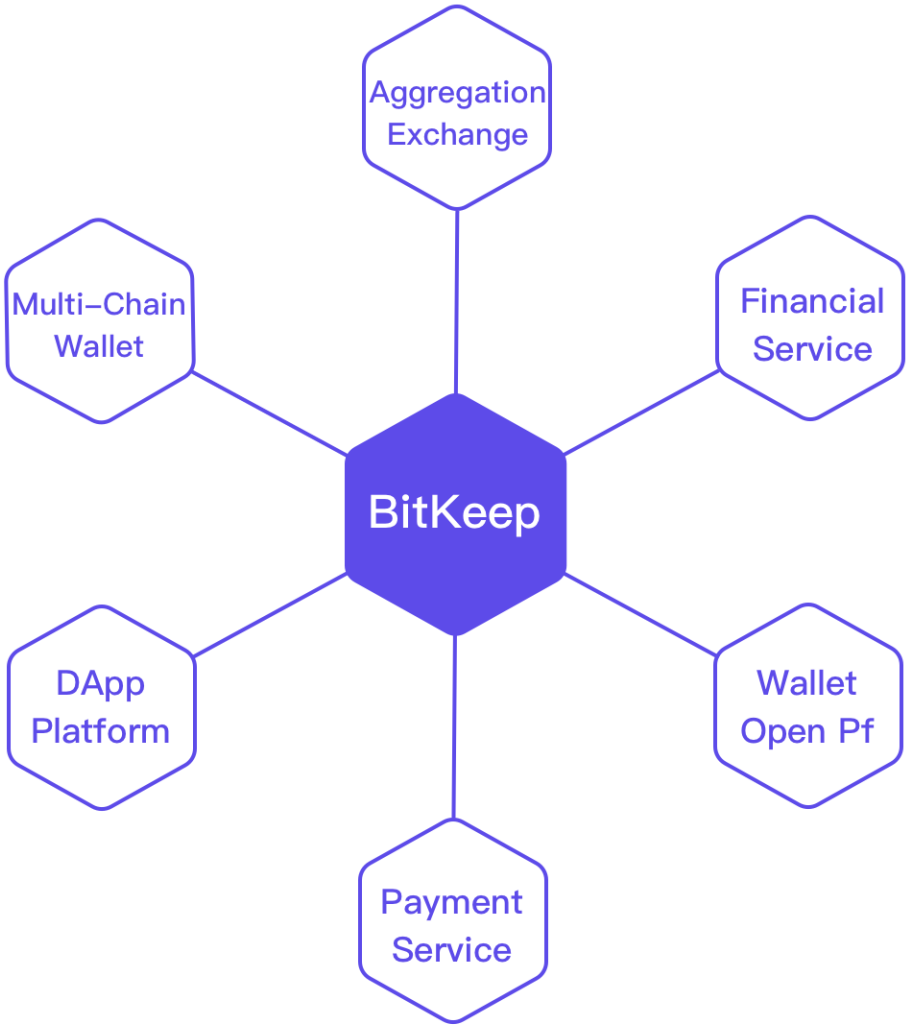
BitKeep launched iOS and Android versions in June 2018, which solved the problem of one-stop management of user assets and connects with several exchanges to manage user assets on exchanges. Over the past four months, the project has maintained the a jogging speed of principle of agile development. More 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 called BCloud 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.

In October 2018, the DApp Open Platform was released. It accessed to multiple mains, including ETH, EOS, TRX, etc. Hundreds of apps have been released online. The transaction volume exceeded 30,000 EOS on the day of EOS DApp online.

In February 2019, the web version of Aggregation Exchange was released. It gets the buy and sell data from other hot exchanges all of the world. Base on the dispatch system, user can buy and sell digital currency by one-click.

Now, BitKeep's business has involved multiple areas, including multi-main wallet, aggregation exchange, financial service, DApp open platform, wallet open platform, payment service, etc.



3.1 Multi-Chain 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:

- Multi-Chain and Multi-Coin

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, TRX, NULS, IOST 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 Multi-Wallet

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.

- 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.

- Candy Send (Airdrop)

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. This feature is original creation from BitKeep.

- Batch Transfer

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.

- Web Version of Wallet

In March 2019, BitKeep's web wallet released, for use in multiple scenes. Larger screen for a better operating experience.

3.2 Aggregation Exchange

From the development trend of blockchain technology, the first generation main chain represented by Bitcoin and the second generation main chain represented by Ethereum intelligent contract gradually evolve to the third generation main chain represented by EOS\TRON intelligent ecology. The main value of the first and second generation main chain lies in the global circulation and value exchange of assets, and its value is realized through the centralized exchange. The third generation main chain offer free transfer and rapid asset recognition. Therefore, the development ecology of DApp has been realized. Because of this particularity, most of the value exchange is completed within the main chain, users can manage and use assets directly through decentralized wallets. Thus, users in these ecosystems have a large number of decentralized main chain assets.

The goal of the BitKeep aggregation exchange is to realize the value exchange between the decentralized main chain and the centralized ecology of the exchange, aggregate the transaction depth of the high quality centralized exchange, and open up the users' assets on the decentralized main chain. Allows users' assets to be freely exchanged on decentralized and centralized platforms.

The first stage, aggregating the depth of high-quality exchanges around the world, requires only one BitKeep account to trade all currencies, and at the same time enjoys the best depth of trading, ideally help users to "buy at the lowest price，sell at highest price." Based on this idealized principle, BitKeep aggregation exchange can be described as the deepest trade exchange in the world. At present, Binance, Huobi and OKEX exchanges have been aggregated, and will continueally support Bitfinex, Coinbase,

Bithumb and other top exchanges, follow-up and gradually support USD, KRW and other legal tender trading pairs.

The second stage, the integration of decentralized wallet assets, through multi-chain wallet, directly put users' assets into the aggregate exchanges, to achieve convenient trading, so as to avoid the tedious process of recharge and withdrawal.

3.3 Financial Service

Multi-currency financial management is the first financial business launched by BitKeep, users can directly transfer the assets in the multi-chain wallet to financial products, keep the principal and interest, at the same time, there are a variety of time periods to choose.

BitKeep will release C2C loan service. If you have coins, you can borrow money form other users through mortgage you coin assets. If you have money, you also can borrow coins from BitKeep. The interest rate decides totally by market. Low fees, real-time arrival, you can finish all process in BitKeep App. BitKeep provide warranty service, it is safe and reliable.

Balance God is our new financial service coming soon. You can deposit and withdraw your coin anytime. It is very freedom and easy. It support multiple currency, no limit.

3.4 DApp Open Platform

Wallet is naturally DApp's entry tool, and the experience of this approach is the best. The entire process of user identification to payment can be completed without logging in or registering, just like the combination of PC browser + sites, and even beyond that combination. At present, the BitKeep DApp platform has been opened to application developers, and has successfully launched hundreds of DApp applications at BitKeep.

Base on multi-chain wallet, BitKeep DApp open platform will continue to launch development interfaces that based on each main chain, and will continue to iterate on performance optimization and interface richness, provide blockchain node services, reduce the development cost of DApp in multiple dimensions, and enhance the experience of use.

According to the data effect, BitKeep can collect channel dividend and advertising revenue.

3.5 Wallet Open Platform

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

3.6 Payment System

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.

4. Security and Technology Innovation

4.1 Node Deployment

All supported main chains deploy multiple private full nodes, local area network access, private, thus ensuring speed and security.

Cloud services are deployed in a distributed manner and are equipped with 12 proxy nodes around the world, which can accommodate at least one million concurrency and have high scalability.

4.2 DESM 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 Online-Offline Hot-Cold Separating 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.

4.4 Various Currency’s Contract Bulk Transfer

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.

4.5 Crossing Exchanges Trading Dispatch System

By Synchronizing the trade depths of all exchanges in real-time, then merger and summary the data, show new depths to user. When user makes a order, the system use the AI algorithm and big data, split the order with best price in each exchanges. Let use to buy in with lowest price and sell out with highest price.

5. BitKeep Token(BKB)

BKB, also called as BitKeep Token, is the platform token of BitKeep services, which plays an important role in the development of BitKeep. BKB is based on Ethereum ERC20, with a total of 1 billion pieces, never issued again.

5.1 Allocation

Percentage	Number(BKB)	Participant
40%	400,000,000	Team Reward
30%	300,000,000	Public Offering
20%	200,000,000	Platform Operation
10%	100,000,000	Early Investor

5.2 Issuance

The part of team reward is released in 5 years, 20% each year.

The public offering is immediately released. The platform operation part is released on demand according to the product and community operation rhythm. Early investors need to lock in a linear release within a year after six months.

5.3 BKB Usage

BKB will serve as a symbol of the platform's user privileges and membership, and holding BKB will enjoy specific rights and services, including, but not limited to:

- ✓ Discount for list new coin
- ✓ Discount for support new chain
- ✓ Custom function for coin
- ✓ Discount for list new DApp
- ✓ Discount for Ad
- ✓ Discount for Wallet Open Platform
- ✓ Discount for Payment System
- ✓ Discount for exchange fee
- ✓ Discount for withdraw fee
- ✓ Speed for recharge and withdraw
- ✓ Increase interest for financial
- ✓ Discount for VIP levels
- ✓ Dividend rights
- ✓ Votes
- ✓

6. Core Team

Gavin Nation – CEO

Gavin Nation, Co-Founder of BitKeep, is an executive Internet practitioner, specialising in managerial workflow and digital marketing. After receiving his B. S in Civil Engineering from UTS in Sydney, Gavin has worked with John Holland 2014, Sydney Metro 2015 and has held senior management positions before advising startups in the crypto currency field. Gavin has over six years of internet experience and four years of experience in blockchain marketing.

Kevin Yan - CTO

Many years of entrepreneurs, founders of three companies. Before 2016, as the technical director of Qihoo 360 in China, response for the 360WiFi project and achieve over 100 million users, with rich experience in security technology. In May 2016, went to Singapore, start the Meecha project, the largest social platform for strangers in Southeast Asia and the Middle East. After having the first one bitcoin in 2012, begin to have a strong interest in blockchain technology.

刘扬 - CMO

Many years of entrepreneurs, founders of four companies. ，In 2017, join the blockchain industry, invest multiple token projects.

Kartal Burak - Director of Operations

Experienced Middleware Engineer with a demonstrated history of working in the wireless, financial, and machine learning industry.

Simon Suster - Product Manager

CoinBene PM, Extensive project management experience, leading development teams, consulting, integration technology, middleware, planning, design, project management and business process modeling.

Stephen Shuster – Technical Manager

Multifaceted software engineer with image compression and text-to-speech machine learning experience, Google-scale infrastructure, computational neuroscience background, and interest in human-centric projects

NGYEN ANH DAO - Technical Manager

Machine learning frameworks developer, customized infrastructure was designed and implemented using Amazon's Web services and MIT's Starcluster.

Joel Shor - Technical Manager

Lightworx framework Developer, LessCloud BaaS Founder, BccExx Co-Founder。

7. Cooperative Organization

7.1 Investor

matrix PARTNERS

F | B | G CAPITAL

7.2 Cooperative Organization

CJ Capital
DFund
ColinStar
Maxthon
Ontology
BiShiJie
CoinTime
Ethereum
Pivot
PeckShield