BOX

Enterprise Token Safe Box

Whitepaper

WWW.BOX.LA

Contents

Abstract

BOX (Enterprise Token Safe Box) is an enterprise-level digital assets safe application that uses the axiomatic techniques in blockchain, cryptography and communications security to protect private keys and instructions. BOX, in principle, seeks to prevent the theft and tamper of private keys and instructions.

i. Background

1. Rapid Growth of Digital Assets

With the rapid growth of the digital asset market, an increasing number of investment agencies, enterprises and start-up teams have entered this field, and the amount of various digital assets that they hold is also rapidly increasing. However, the current digital asset management tools that are available to enterprises are extremely limited. A large number of digital assets are kept in personal wallets, trading platforms or cold wallets, which is different from traditional asset management processes. As such, enterprises generally have concerns in terms of digital assets management and investment, such as the loss of private keys, and the theft of trading platform wallets disclosed publicly by the media. These problems have restricted the investment and management of digital assets by enterprise users.

2. Shortage of Enterprise Digital Asset Management System

In the past few years, a few teams have tried or are trying to use various technologies to enhance the security of their wallets, but for a variety of reasons, there has not been a generic, low cost and easy solution that has been deployed so far. Based on the belief and love for blockchain, we have created a high-security digital asset management system through a large number of theoretical discussions and scenario demonstrations for different application scenarios. BOX WAS BORN. In order to thank the communities who share the same faith, we will make the code open source immediately after its official release. Any organisation or individual may deploy and use BOX for personal (and not commercial) purposes only.

3. Demand for Enterprise Digital Asset Management

We learned, through many years of practical experience and grassroots research, that the following requirements are urgently needed:

a) one-stop management tools for digital assets;

b) shareholders and partners intending for the digital assets to belong to the enterprise, rather than individuals;

c) a unified enterprise wallet address for public accountability;

d) internal financial approval process and reduce the possibility of misoperation

e) no exposure of private key under any circumstances;

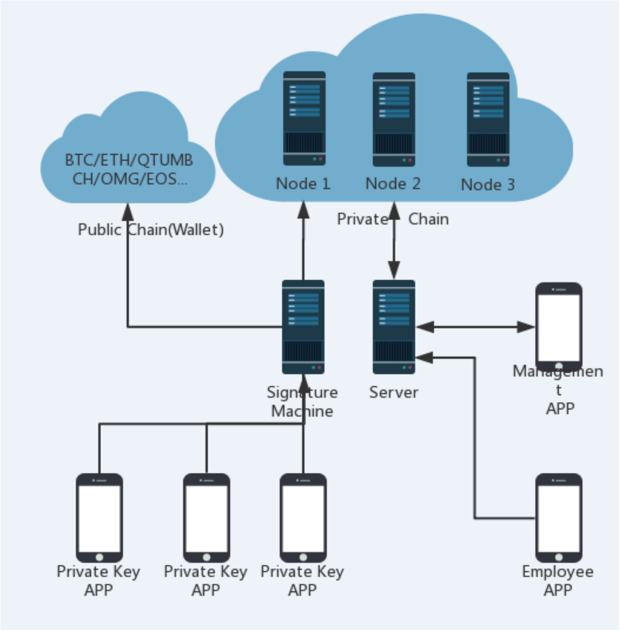
f) unforgeable transaction instructions to prevent the theft of digital assets;

g) facilitate enterprises to record and audit digital assets; and

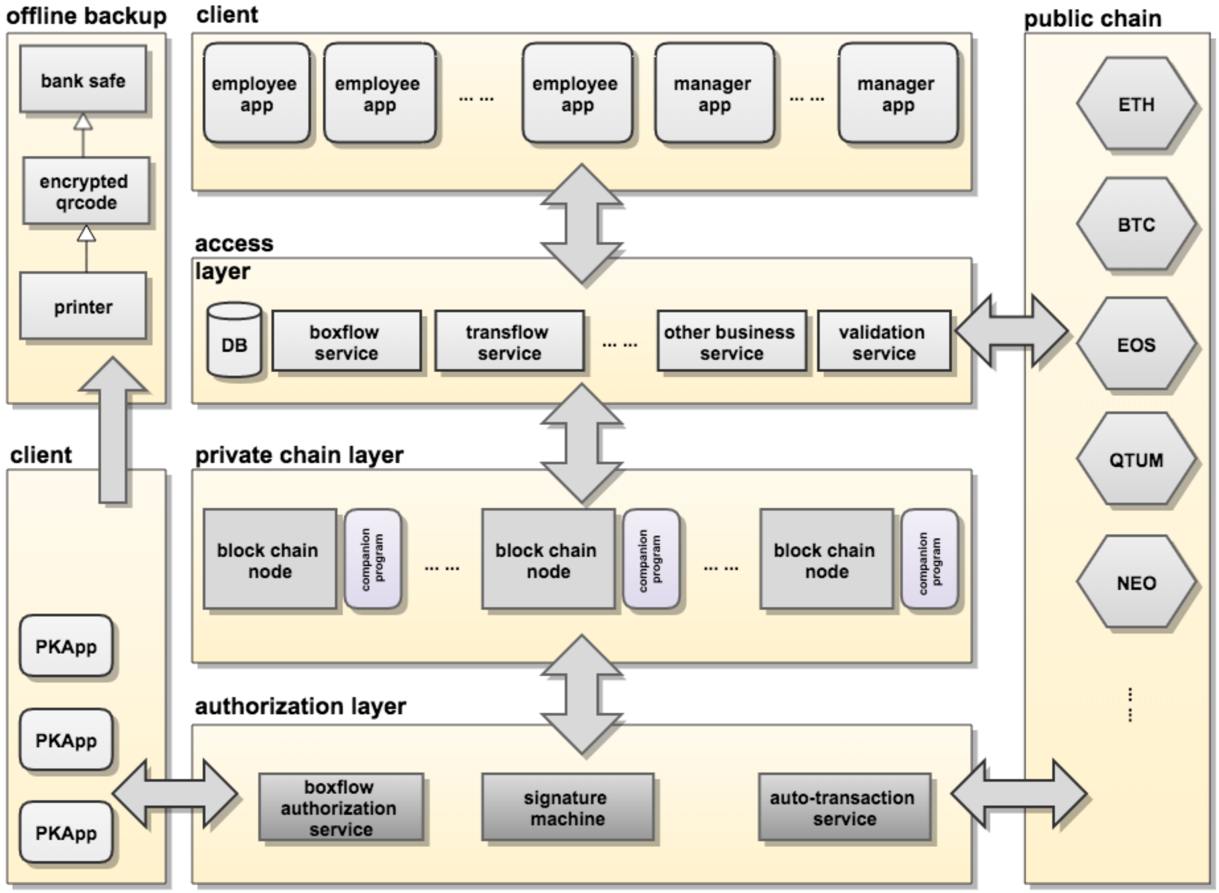
h) ensure the safety of enterprises' digital assets under the circumstances that the private key holder(s) will not or cannot exercise his or her authority.

ii. Design Philosophy

BOX is an independent digital assets bank system owned by the enterprise. The BOX system unifies and manages all types of enterprises that own digital assets, by encrypting private keys in memory in order to prevent exposure; by recording and verifying instructions in the enterprise-owned private chain; by customising the digital asset management business flow through orderly signature; and by SSL/TLS to ensure security of the communication. BOX seeks, in principle, to prevent ubiquitous wallet problems such as hacking, moles and misoperations. Meanwhile, BOX can ensure the high security of enterprise digital assets via intrusion lock, system reset and other mechanisms.



The number of private chain nodes is 2n + 1 (n≥1), the minimum number of private key APPs (PKApp) is 3 (the specific number of which can be customised independently by each enterprise) and the signature machine is an independent physical server. The access layer is a cloud server and has no communication with the signature machine. The signature machine can only communicate with the private chain, and only the signature machine can issue transaction instructions to the public chain. The employee APP (EApp) initiates the transaction request and thereafter, the management APP (MApp) approval is required.



The BOX system can access all digital assets that support offline signatures. The first version will support Ethereum and ERC20 tokens. In future, more digital assets will be supported.

iii. Private Key Safe Protocol

1. Private Key Storage

The private key is stored in the memory of the signature machine and will not be stored permanently. In the unfortunate scenario that the signature machine is hacked, since it is almost impossible to crack the private key in a short time, the risk of exposure will be reduced greatly.

The signature machine should be an independent server. It is recommended that the signature machine be stored in a facility with very high levels of security, for example, a financial computer center or a high security computer room owned by the enterprise. The signature machine needs 24 hours of uninterrupted power, internet access and a fixed IP address. The signature machine should not be easily accessed by anyone, including the enterprise’s IT officer.

The enterprise’s digital assets are actually stored on each public chain.

If the official digital wallet supports offline signatures, the private key can be stored in the signature machine’s memory and be used for the transactions confirmation without exposing the private key.

2. Private Key Generation

In order to prevent the private key generation from being cracked, BOX uses the variant of RFC6979 protocol: k = SHA256 (d + SHA256 (m1) + SHA256 (m2) + SHA256 (m3) + ...), with d being the server random number, and m being the key sentence that is inputted by PKApp. It is generated by inputting a minimum number of three key sentences (KS), which are strings of any combination of letters and numbers. After three or more PKApps sequentially input the KS, the generated private key is stored in the signature machine memory, and the public key address generated by the private key will be registered in the public chain. The PKApp does not store the KS, and the BOX code is open to the community.

All transaction processes of the PKApp require mutual authentication. PKApp numbers are fixed during the first setup. The server only distributes certain number of certificates, and the certificate is bound to a device ID, and other connection requests will be rejected.

If the PKApp is lost, there is no security risk because the APP does not record any KS or passwords. The owner of the KS can reinstall the PKApp and retrieve the server certificate using the original KS. Then, the signature machine will rebind the device ID of the new PKApp.

3. Private Key Recovery

Once the signature machine’s power is turned off, the private key will disappear immediately. Therefore, when the signature machine restarts, all PKApps are required to re-enter the correct KS. If the owner of a PKApp cannot enter the correct one, you need to enable the cold backup of KS. Since this process belongs to the enterprise management process, this document only provides the recommended solution of cold backup. Please refer to the “Private Key Cold Backup” section for the recommended solution.

iv. Private Chain

1. Private Chain Function and Advantage

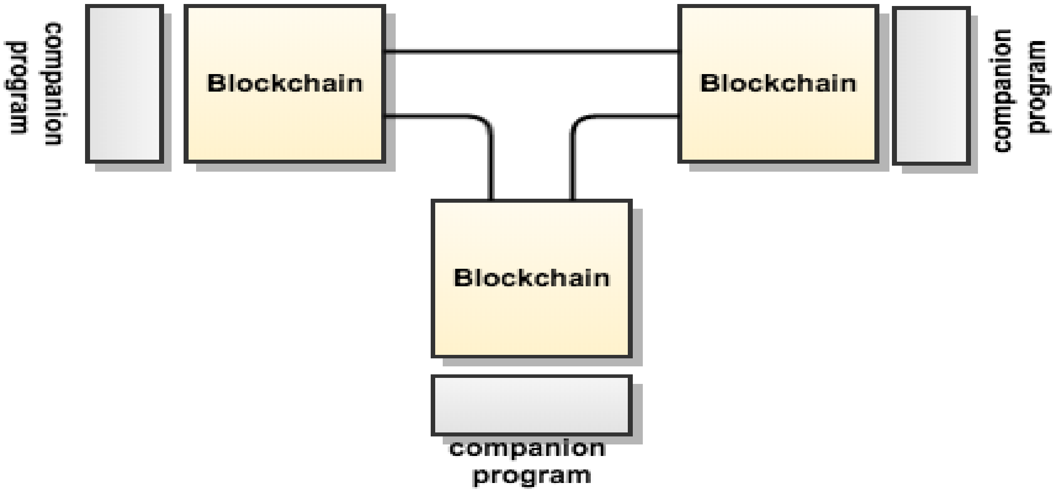
The purpose of the private chain in the BOX system is to record and verify the transaction flow. The transaction flow setup and transaction flow approval process are recorded on the private chain, and it will be the reliable basis for the auto-transaction on the public chain. BOX system (version 1.0) will build the private chain based on Ethereum, and the future plans are to support more chains.

The enterprise not only gets a set of systems of record and verification, but also independently controls all nodes via deploying private enterprise chain. The enterprise can control the maximum transactions number per block, the block time, and node numbers by defining the genesis block settings.

Gas (i.e. the cost to transfer a token) is negligible as it is on a private chain and gas is transparent for access layer.

The private chain adopts the Proof of Authority (PoA) consensus mechanism to directly specify which private chain nodes have accounting rights and the other nodes will exist as backup nodes.

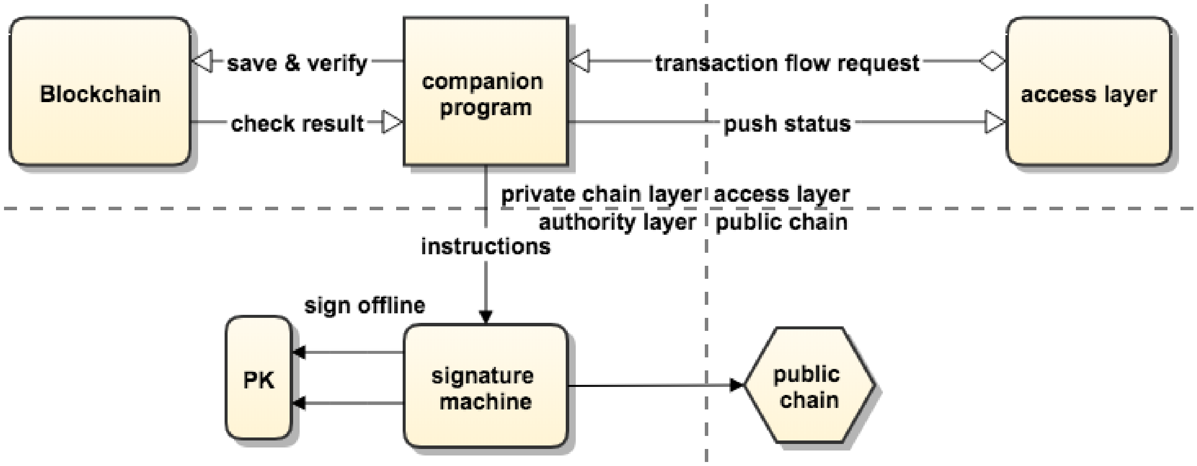
2. Companion Program



The companion program is the same as the Ethereum DAPP. Each private chain node is equipped with the same companion program that is used to handle traditional client-server application requests, process data to upload private chains, execute smart contracts, monitor smart contract events, send status notifications, coordinate interactions between access layers and manage the signature machine.

The companion programs are parallel and communicate only with private chain nodes on the same server. There are no direct connections between the companion programs. Each companion program links to one private chain account for the execution of smart contracts.

The companion programs coordinate the interaction between the access layer and the signature machine. A transaction consists of four steps: 1. initiate the transaction request; 2. approve the transaction request 3. complete the transaction on the public chain; 4. check the transaction status on chain. We have divided these four processes into four sections, as shown in the figure below. The companion programs operate in the private chain layer section, recording and verifying the transaction flow through the private chain, and thereafter, returning the transaction flow results to signature machine. All chain transactions will be operated by the signature machine. The companion programs isolate the direct interaction between the transaction requester and the public account, and this process is automatically executed by the programs in accordance with the approved transaction flows.

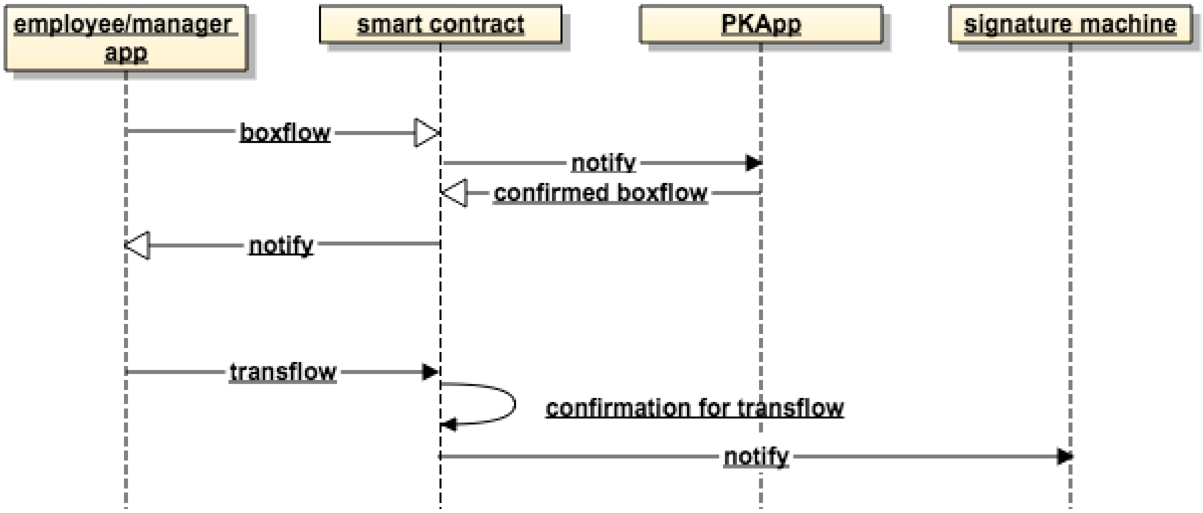


3. Smart Contract Consensus Mechanism

Data is stored in a smart contract on the private chain. Smart contracts use voting to confirm the data on a private chain. Each data must be confirmed with more than 50% of the nodes having the same content. Each node represents one account operating the same contract. The data on the private chain can be guaranteed to be valid, unless more than 50% of the nodes are fully compromised.

The smart contract voting system needs to assign reasonable authority to the accounts. All private chain accounts are fixed after the private chain setup. Whenever a new node is to be added, all the existing private chain accounts must authorise the node. Thereafter, the system will automatically re-balance the 51% strategy without redeploying the new contract to adapt to the change.

The recorded data includes the approval process and transaction requests. As shown below, prior to a transaction, you need to set up an approval process which is to identify the departments and corresponding participants that need to be included for a transaction request approval. The number of people needs to be confirmed. The transaction request needs to be approved by the highest level of the enterprise's management. The approval process is used to initiate the transaction.



v. Access Layer

The access layer uses the separation of powers architecture.

The power of the entire system is dispersed in the Apps, the access layer takes a variety of transactions coordination, but it does not have the right to execute and modify the transaction.

The separation of powers architecture depends on the Elliptic Curve Digital Signature Algorithm. The Elliptic curve cryptography uses the Bitcoin classic curve secp256K1.

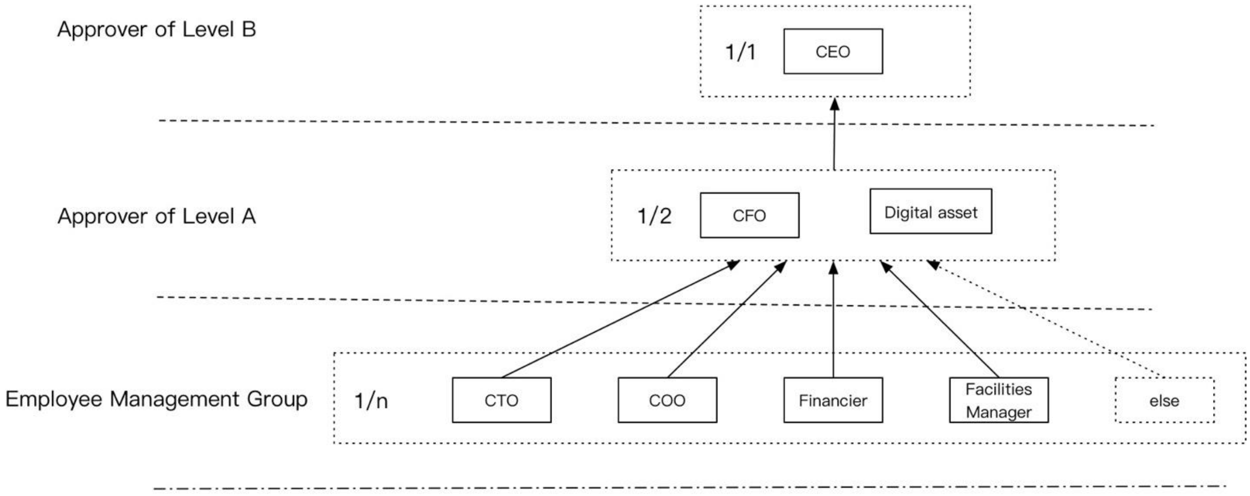
The transaction process is as follows: the signature is generated by the EApp & MApp; following which the transfer is coordinated in the access layer; and subsequently confirmed on the private chain. Finally, the signature machine issues the transaction on the public chain.

The access layer business includes: 1) the transaction flow setup; and 2) the transaction flow approval, as further explained below.

1. Transaction Flow Setup

A transaction flow is setup before executing the transaction. It is a multi-level approval model. The first level of approval is from the employee group; and there will be several approval levels with defined minimum approvals.

An example of the transaction flow is shown below:



When the enterprise finishes the transaction flow setup, a system-recognisable protocol format will be inputted via MApp. It is named boxflow in the BOX system.

Boxflow is, by default, an unauthorised state. If authorisation is needed, it is flowed into the access layer. The access layer checks the format, checksum, and upload hash to the private chain. All nodes vote and record, then notify the signature machine. The signature machine authorised by PKApp uploads hash to the public chain, and the hash status is set into valid on private chain once the transaction is successful. Once these processes are completed, boxflow will be in an authorised state and an enterprise can make transactions via boxflow in its authorised state.

Any modification to boxflow (once it is in an authorised state) will require the PKApps to cancel the current authorisation and then re-establish a new authorisation.

2. Transaction Flow Approval

After the authorisation of boxflow, employee accounts would need to be created.

In the BOX system, employee accounts are assigned public and private keys by the employee management group. The EApp obtains the current authorised boxflow, the employee selects the employee group to apply the private key, and the employee management group derives the sub-private key and assigns the keys to the employee.

The EApp can initiate a transaction request with a private key, the application format of which is as follows:

```
{ balance: 100E18,

      timestamp: 1512719484736,

      destination: '0x6E9483f00cCd685c5F12709Fd542Da1FB20c4d2e',

      miner: E16,

      currency: 'ETH',

      applicant:

        { username: 'bluce'} }
```

Current request is unsigned, and the request needs to be hashed with SHA256 algorithm and signed, and the hash signature is put into the request with the following format:

```
{ balance: 100E18,

      timestamp: 1512719484736,

      destination: '0x6E9483f00cCd685c5F12709Fd542Da1FB20c4d2e',

      miner: E16,

      currency: 'ETH',

      applicant:

        { username: 'bluce',
        sign:
'474w3zgKRLwaddG6LadzKQ3ut1JyQUc4HpVLkydR6xdk2TwS7zEXKf4E5AyGHxQkfLYxJsccx
hqdY5Qm5352P2H4' } }
```

The employee's request can only be approved by its corresponding employee management group account.

After approval by the employee management group, the request (including the signature) will be hashed and signed. The request after the signature is handed over to the upper level management for approval and, the upper level management may sign the hash after verifying the lower level signature. This approval process would be repeated until the final level.

The final approved transaction request would be considered a transaction, and it is named as transbox.

The transbox hash is the trade ID. After the access layer verifies transbox and matches the corresponding boxflow, the trade ID (hashed) would then be recorded on the private chain for voting. The signature machine will be notified of a transaction on the public chain after successful voting.

After receiving transbox, the signature machine extracts the boxflow and verifies the validity, and then subsequently verifies the transbox signature. Transaction on the public chain is issued after transbox verification by signature machine. The transaction ID is recorded in private chain and access layer can check the status anytime.

3. Multiple Boxflow

In the first version, BOX will only support a single boxflow. Multiple boxflows will be supported in future upgrades.

vi. Boxflow Safe Protocol

There are two important parts to secure auto-transaction. One is the security of the private key (refer to the section on “Private Key Safe Protocol”) and the other one is the security of usage rights. This chapter will explain boxflow.

1. Validity of Boxflow

A valid boxflow needs to go through the private chain record, PKApp authorisation and public chain confirmation. The valid boxflow is confirmed by N enterprise approvers together and recorded in the private chain. The validity of boxflow is tamper-proof.

2. Generation of Transbox

The transaction request is initiated and signed by the EApp. After the employee management group and the approvers verify the correct signatures, the transbox is generated. As the public and private keys exist only on the Apps, the transbox generation is tamper-proof.

3. Validity of Transbox

The validity of Transbox includes two parts, one is the validity of the signature, and the other one is the validty of boxflow. BOX uses a nested signature method, whereby you will only need to validate the signature in sequence, and you will know the signature validity. The transbox itself corresponds to one boxflow which needs to be verified. If both conditions are satisfied, it is proved that transbox was confirmed by boxflow and it is tamper-proof.

vii. Communication Safe Protocol

1. Signature Machine and Private Chain Communication

Communication between the signature machine and the private chain uses bi-direct gRPC + SSL/TLS authentication. gRPC is a high-performance RPC framework which is designed with the standard HTTP/2 protocol, and developed with ProtoBuf (Protocol Buffers) serialised protocol. HTTP/2 protocol requires encrypted data transmission (SSL/TLS). The BOX system will develop signature machines for all public chains. Security will be greatly ensured with the SSL / TLS mutual authentication. In this regard, man-in-the-middle attacks can be prevented as the connection request will be immediately denied once an abnormal connection appears.

2. Employee APP and Access Layer Communication

All Apps that communicate with the access layer use the HTTPS protocol. The private key for employee's signature is issued through the MApp.

The steps are as follows:

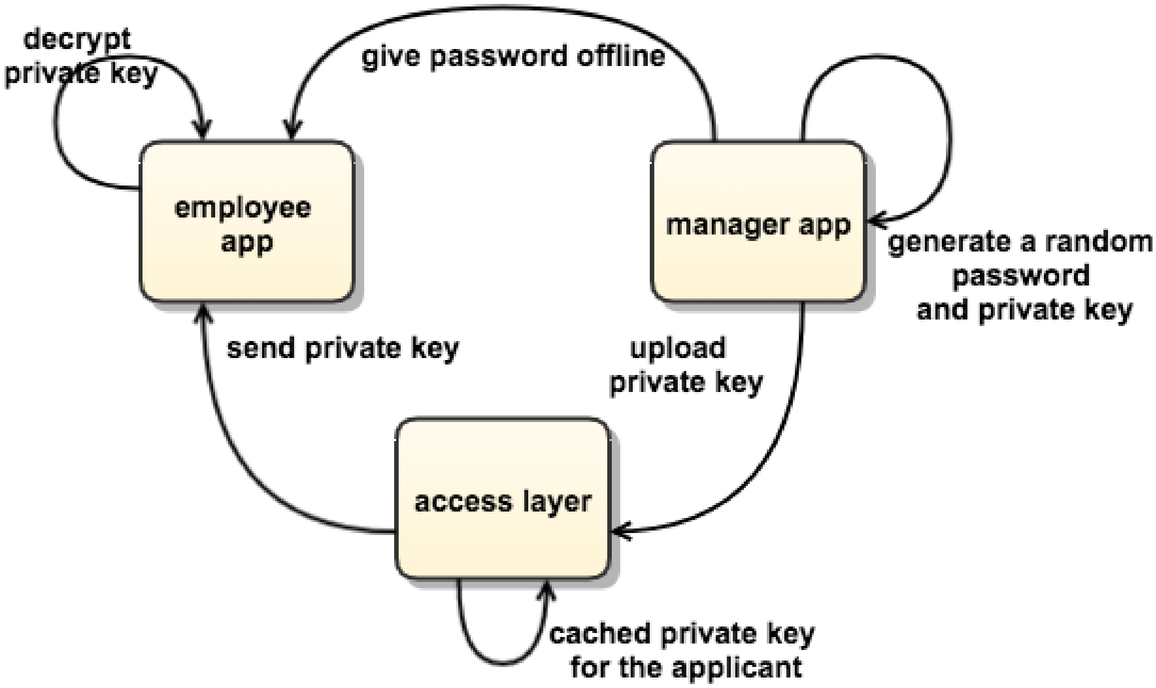
a) the MApp generates an employee private key and a corresponding random number for encryption;

b) the MApp encrypts an employee's private key via symmetric-key algorithm;

c) the MApp informs the employee of the password offline;

d) the access layer caches the encrypted employee private key from the MApp; and

e) the EApp downloads the encrypted data from the access layer and decrypts it with the given password.



3. Access Layer and Private Chain Nodes Communication

Communication between the access layer and the private chain is internal communication via the TCP / IP protocol connection. The data passed by the access layer to the private chain has been authorised by the signature and generates a message digest. The private chain only needs to use the signature verification program to verify the data. If the verification fails, the service is denied. The access layer sends a request to all private chain nodes, with each private chain node corresponding to one account. Each account uploads the verified data to the private chain, and the data will be successfully confirmed once more than 50% of the accounts are confirmed. The access layer provides voting to the access layer. The above process can be summarised into the following two formulas:

signature =sign(hash)

public key == recover(hash, signature)

viii. Private Key Cold Backup

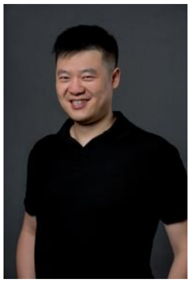
Print and store in the safebox in the bank!

We recommend that all key sentences be physically backed up to avoid a situation where the private key is unable to reset in any circumstances. For example, each private key APP holder prints the encrypted key sentences via an offline printer, then store the printer/key sentences separately in two different banks safe. The key can be kept by the enterprise’s lawyer and only be used with the requisite consent as evidenced by a resolution of the enterprise’s board of directors.

ix. Road Map

- 2017.10 Project planning
- 2018.01 Demo Version
- 2018.04 Version 1.0- open source
- 2018.07 Version 2.0- open source
- 2019.01 Version 3.0- open source

x. Team



Founder: Shang, WeiSi; Leon;

Leon has over 16 years' experience in software development and operation in the internet industry. He was Vechain’s COO. He worked for eBay as a senior product manager, and was the CEO of Louding Technology Co. Ltd..

CTO: Qiu, Chunrong; Alpha

Alpha has over 15 years' experience in software development and architecture. He was Vechain’s Architect, DZH’s Architect; Senior Java’s Engineer, Golang’s Engineer, and Ethereum’s Engineer.

COO: Ma, Zhuo; Antonio

Antonio has over 16 years' experience in the internet industry. He worked for Coach as the Head of E-Commerce for Great China. He also worked for eBay as a marketing manager.

CFO: Bryan Zhang

Bryan has 20 years of working experience in relation to Internal Control, Tax Advisory, Mergers & Acquisitions, Business Process Restructuring and Corporate Management. He has worked for famous multinational companies, such as Carrefour (China) HQ, Inbev (China) HQ, Metro (China) HQ. Later, he joined HMY (a French Group) as Vice President.

xi. Economic Model

As a Blockchain as a Service solution, BOX tokens can be used following the ERC20 token standards.

The BOX system is designed to be publicly available and is an open-source software which can be used free of charge. BOX token holders can participate in community governance activities, such as code updates, team elections and network parameter changes in the open source community.

For the avoidance of doubt, participating in community governance activities does not represent or confer any shares, stock, ownership, right or stake, participation, or any other right, title or interest of any form with respect to any company, enterprise or undertaking, including but not limited to, any right or option to receive future revenue, shares, stock, ownership right or stake, participation, securities, voting rights, dividends, distribution, redemption, liquidation, proprietary, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to the BOX platform or BOX Group Limited ("**BOX Group**").

To obtain value-added services or technical support services, BOX token holders may opt to exchange these services for BOX tokens. The BOX tokens that are exchanged will be locked and released at 00:00 UTC London time on December 26th of each year. These BOX tokens will be sold directly by BOX Group at a price evaluated at 90% of the average price 7 days prior to December 26th of each year.

All funds will be used for developing and operating the BOX system.

xii. BOX Token Allocation Plan

1. Token Allocation

Symbol	BOX
Token name	BOX Token
Total Supply	100,000,000
Allocation Date	2017-12-26 UGT 00:00:00
Proportion of Allocation	Team, 20%; Private investors, 30%; Enterprise investors, 50%;
Box Price	1ETH=2500 BOX
Locking Period	None
Website	BOX.LA

2. Allocation and Constitution

Constitution	Description	Ratio	Amount
Team	Angel investors	2.5%	2,500,000
	Team Bonus	2.5%	2,500,000
	Business Promotion	5%	5,000,000
	Operation	10%	10,000,000
Enterprise Investors		50%	50,000,000
Private Investors		30%	30,000,000

xiii. Definition

BOX	Enterprise Token Safe Box
PKApp	private key App

EApp	employee APP
MApp	management APP
KS	key sentence
PoA	Proof of Authority

xiv. Legal Disclaimer

PLEASE DO READ THIS SECTION VERY CAREFULLY. IF YOU ARE IN DOUBT AS TO ANY ACTION YOU SHOULD TAKE, PLEASE CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER SUITABLE PROFESSIONAL ADVISOR(S).

No information in this White Paper should be considered to be business, legal, financial or tax advice regarding BOX Group or the BOX tokens. You should consult your own legal, financial, tax or other professional advisors regarding BOX Group and its business and operations, and the BOX tokens. You are fully aware and understand that in the case where you wish to purchase any BOX tokens, there are risks and uncertainties (including financial and legal risks and uncertainties) associated with the BOX token sale and BOX Group.

The White Paper is intended solely for general information purposes, for community discussion and is not legally binding. The White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities, an invitation to make an offer of securities, a solicitation for investment in securities in any jurisdiction, or any offer to sell any product, item or asset (whether digital or otherwise).

Any agreement as between BOX Group and you as a purchaser, and in relation to any sale and purchase of the BOX tokens, is to be governed by only a separate document setting out the terms and conditions of such agreement (the "**T&Cs**"). In the event of any inconsistencies between the T&Cs and this White Paper, the former shall prevail. BOX Group does not owe the holder any rights or obligations except as expressly set out in the T&Cs.

In any case, you acknowledge and agree that you are not eligible to purchase any BOX tokens if you are citizen, resident or domiciliary of the Republic of Singapore.

The BOX tokens are not intended to constitute securities in any jurisdiction and in any manner, including but not limited to, any kind of currency (other than cryptocurrency), debentures, stocks or shares issued by any person or entity, rights, options or derivatives in respect of such debentures, stocks or shares, rights under a contract for differences or under any other contract the purpose or purported purpose of which is to secure a profit or avoid a loss, units in a collective investment scheme, units in a business trust, derivatives of units in a collective investment scheme or business trust, or any other security or class of securities.

BOX Group shall use all proceeds of sale of the BOX tokens to fund BOX Group's cryptocurrency project, businesses, team development and operations.

To the maximum extent permitted by the applicable laws, regulations and rules, BOX Group shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this White Paper or any part thereof by you.

BOX Group does not and does not purport to make, and hereby disclaims, all representations, warranties, undertakings, assurances or guarantees to any entity or person (including, but not limited to the accuracy, completeness, suitability, timeliness or reliability of the contents of this White Paper or any other materials published by the BOX Group). Nothing contained in this White Paper is or may be relied upon as a representation, warranty, undertaking, assurance or guarantee as to the future performance or policies of BOX Group or the BOX system.

Where this White Paper includes information that has been obtained from third party sources, BOX Group has not independently verified the accuracy or completeness of such information. Further, BOX Group does not have an obligation to amend, modify, or update this White Paper or to otherwise notify a reader or recipient thereof in the event that any matter stated herein, or any opinion, projection, forecast or estimate set forth herein, changes or subsequently becomes inaccurate.

No regulatory authority has examined or approved of any of the information set out in this White Paper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this White Paper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

This White Paper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this White Paper is prohibited or restricted. In any case, no part of this White Paper is to be distributed, reproduced, or disseminated without including this section.

The use of any company and/or platform names or trademarks herein (save for those which relate to the BOX Group) does not imply any affiliation with, or endorsement by, any third party. References in this White Paper to specific companies and platforms are for illustrative purposes only.

This White Paper may be translated into a language other than English and in the event of conflict or ambiguity between the English language version and translated versions of this White Paper, the English language version shall prevail. You acknowledge that you have read and understood the English language version of this White Paper.

There are risks in the process of development, maintenance and operation of the BOX system, many of them are out of BOX Group's control. You acknowledge that you understand and agree to the assumption of the following risks, including but not limited to:

(a) **Uncertain laws relating to digital token offerings**: The regulatory position of BOX tokens and distributed ledger technology is unclear and/or unsettled in certain jurisdictions, and there may be risks that the BOX tokens may be considered to be a security, or that it might be considered to be a security in the future, in these jurisdictions. BOX Group may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction.

(b) **Security issues**: Hackers or other malicious groups or organisations may attempt to interfere with the BOX tokens and/or the BOX system in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or BOX Group may unintentionally introduce weaknesses into the core infrastructure of the BOX system and/or the BOX tokens, which could negatively affect the BOX system and/or the BOX tokens.

(c) **Ethereum-based protocols**: As the BOX token and the BOX system are based on Ethereum-based protocol and architecture, any malfunction, breakdown or abandonment of the relevant Ethereum-based protocol or architecture may have a material adverse effect on the BOX tokens and/or the BOX system. Moreover, advances in cryptography, or technical advances (including, but not limited to, the development of quantum computing), could present unknown risks to the BOX tokens and/or the BOX system by rendering ineffective the cryptographic consensus mechanism that underpins the Ethereum-based protocol.

(d) **Imperfect information disclosures**: The BOX system is at the stage of development as of the date of this White Paper and its algorithm, code, consensus mechanism and/or various other technical specifications and parameters could be updated and changed frequently and constantly. While the White Paper and other marketing materials (as the case may be) released relating to the development of the BOX system has been prepared with the then up-to-date key information of the BOX system, it is subject to adjustments and updates from time to time following the growth and development of the BOX system and/or the ecosystem on the BOX system. Due to the decentralised nature of the BOX system, BOX Group may not be able to, and is not obliged to, update you on all details relating to the development of the BOX system (including, but not limited to, its progress and expected milestones). By purchasing, holding and using the BOX Tokens, you accept that there may be an insufficiency of the information disclosed.

(e) **Early development risks**: You understand and accept that the BOX system is currently in a development phase and requires substantial development. Due to unforeseeable material conceptual, technical and commercial changes before the final release, you understand and accept the risk that the development of the BOX system may not be executed or implemented as planned, for reasons including but not limited to, the event of a decline in the prices of any digital asset, virtual currency or BOX tokens, unforeseen technical difficulties, and the shortage of funds for developing BOX Group's cryptocurrency project.

(f) **Illiquidity**: There is no prior market for BOX tokens and the BOX tokens sale may not result in an active or liquid market for BOX tokens. The BOX token is intended to be used solely within the network of the BOX system, hence there may be an illiquidity risk with respect to any BOX token held.

(g) **Uninsured losses**: The BOX token is uninsured unless you specifically obtain private insurance to insure them. In the event of loss or loss of utility value of the BOX token, there is no public insurer or private insurance arranged by BOX Group to offer any recourse to you.

(h) **Tax treatment**: The tax characterisation of the BOX token is uncertain. You must seek your own tax advice in connection with the purchase, holding and/or usage of the BOX tokens, which may result in adverse tax consequences to you, including withholding taxes, income taxes and tax reporting requirements.

(i) **Competitors**: It is possible that alternative networks could be established that utilise the same or similar code and protocol underlying the BOX token and/or the BOX system and attempt to re-create similar facilities. The BOX system may be required to compete with these alternative networks, which could negatively impact the BOX token and/or the BOX system.

(j) **Risks arising from insufficient interest**: It is possible that the BOX system may not be used by a large number of companies and other entities or that there may be limited public interest in the creation and development of distributed ecosystems (such as the BOX system). Such a lack of use or interest could negatively impact the development of the Platform and therefore the potential utility of the BOX token.

(k) **Risks of dissolution**: It is possible that, due to any number of reasons, including, but not limited to, an unfavourable fluctuation in the value of cryptographic and fiat currencies, decrease in the utility of the BOX token due to negative adoption of the BOX system, the failure of commercial relationships, or intellectual property ownership challenges, the BOX system may no longer be viable to operate and BOX Group may be dissolved.

(l) **Risks arising from lack of governance rights**: As the BOX token confers no governance rights of any kind with respect to the BOX system or BOX Group, all decisions involving the BOX system or BOX Group will be made by BOX Group at its sole and absolute discretion, including, but not limited to, decisions to discontinue the services and/or the ecosystem on the BOX system, to create and sell more BOX tokens for use in the ecosystem on the BOX system, or to sell or liquidate BOX Group. These corporate decisions could adversely affect the BOX system and the BOX token you hold.

(m) **Loss of talent**: The development of the BOX system depends on the continued co-operation of the existing technical team and expert consultants, who may have specialised knowledge and expertise in their respective sectors. The loss of any member may adversely affect the BOX system or its future development.

(n) **Risks involving cloud storage**: As the BOX system may provide a decentralised cloud storage service to institutional clients including users and applications, the BOX system (and services thereon) are susceptible to a number of risks related to the storage of data in the cloud. The BOX system (and services thereon) may involve the storage of large amounts of sensitive and/or proprietary information, which may be compromised in the event of a cyberattack or other malicious activity. Similarly, the BOX system and/or services thereon may be interrupted and files may become temporarily unavailable in the event of such an attack or malicious activity. Because users can use a variety of hardware and software that may interface with the BOX system, there is the risk that the BOX system and/or services thereon may become unavailable or interrupted based on a failure of interoperability or an inability to integrate these third-party systems and devices that BOX Group does not control. The risk that the BOX system and/or services thereon may face increasing interruptions and the ecosystem on the BOX system may face additional security vulnerabilities could adversely affect the BOX system and ecosystem thereon, and therefore the future utility of any BOX token that you hold.

(o) **Risks relating to "forking"**: The BOX system is based on certain open-source elements and BOX Group does not monopolise the development, marketing, operation or otherwise of the BOX system. Any entity may independently develop a patch or upgrade to the BOX system and the acceptance of these patches or upgrades by a sufficient percentage of BOX token holders could result in two or more divergent networks. The community on the BOX system may split in support of the divergent networks respectively. The temporary or permanent existence of forked networks could adversely affect the operation of the BOX system and the BOX token that you hold.

(p) **No ownership and control rights**: Ownership of the BOX tokens does not grant you the right of ownership or right to share in BOX Group. The BOX tokens do not give BOX token holders the right to participate in the decision making about the direction and development of the BOX Group business. However, the opinions of BOX token holders and the BOX system users are very important to BOX Group and may be taken into account by BOX Group when such decisions are being made.

(q) **Risk on the number and value of the BOX tokens**: The quantum and value of the BOX tokens may be affected by factors, within or outside BOX Group's control, including but not limited to the supply and demand for BOX tokens in the market, and the number of tokens which are released for circulation by BOX Group for "business promotion" purposes. These factors could adversely affect the quantum and value of the BOX tokens.

In addition to the risks as stated above, there are other risks associated with your purchase, holding and usage of the BOX tokens, including those that BOX Group cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks.

xv. Contact us

Official website: WWW.BOX.LA

Email: contact@box.la