企业级数字资产保险箱

白皮书

WWW.BOX.LA

2017/12/26

目录

摘要

BOX (Enterprise Token Safe Box) 是一个企业级数字资产保险柜应用，它利用区块链、密码学、通信安全等领域的公理性技术对各类数字资产的私钥、操作指令进行保护，从原理上解决了私钥、指令的盗取、篡改等问题。

一. 背景

1. 数字资产规模快速增长

随着数字资产市场规模的迅速增长，越来越多的投资机构、企业、创业团队进入到这个领域，他们持有的各类数字资产规模也在快速增长。但是目前针对企业的数字资产管理工具极度缺乏，大量的资产被保存在个人钱包、交易平台或冷钱包中，这种情况与企业传统的资产管理流程存在巨大的差别，随着不断被媒体爆出的个人钱包被盗、私钥丢失、交易平台钱包被盗等新闻，使得企业对数字资产安全、便捷等问题产生严重担忧，这些问题已经制约了企业用户对数字资产的投资和管理。

2. 缺少企业级数字资产管理系统

在过去的几年中，区块链领域的个别团队也曾尝试过或正在尝试利用各种技术增强钱包的安全性，但是由于种种原因，至今没有一个通用的、成本较低的、方便部署使用的解决方案公开发布。基于对于区块链行业的信念和热爱，我们针对各种应用场景，通过大量的理论讨论和场景论证，

总结出一个高安全级别数字资产管理系统，BOX 由此诞生。为了感谢区块链行业社区内还在为信念奋斗的同行们，我们会在正式发布后，立即将该系统全部开源，任何组织和个人均可以在不以商业为目的的前提下，无偿部署并使用该系统。

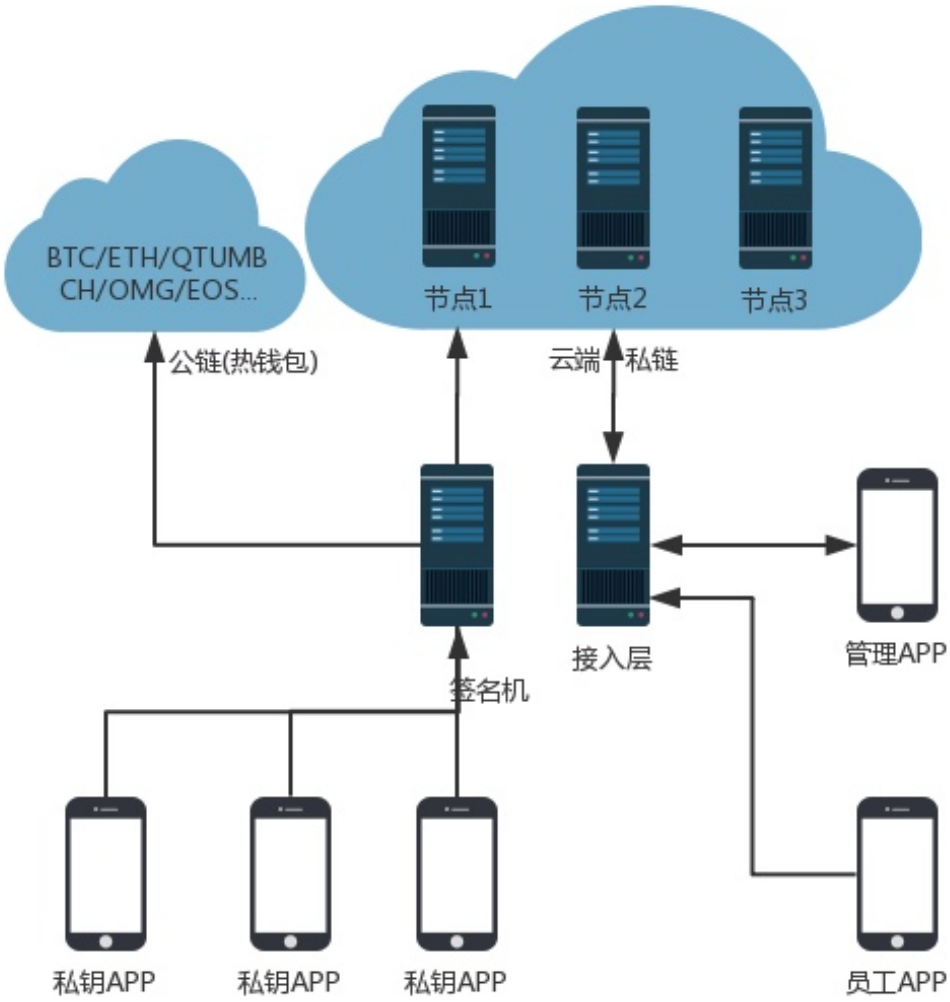
3. 企业级数字资产管理的需求

通过我们多年的实际体验以及大量走访，了解到行业内有如下需求：

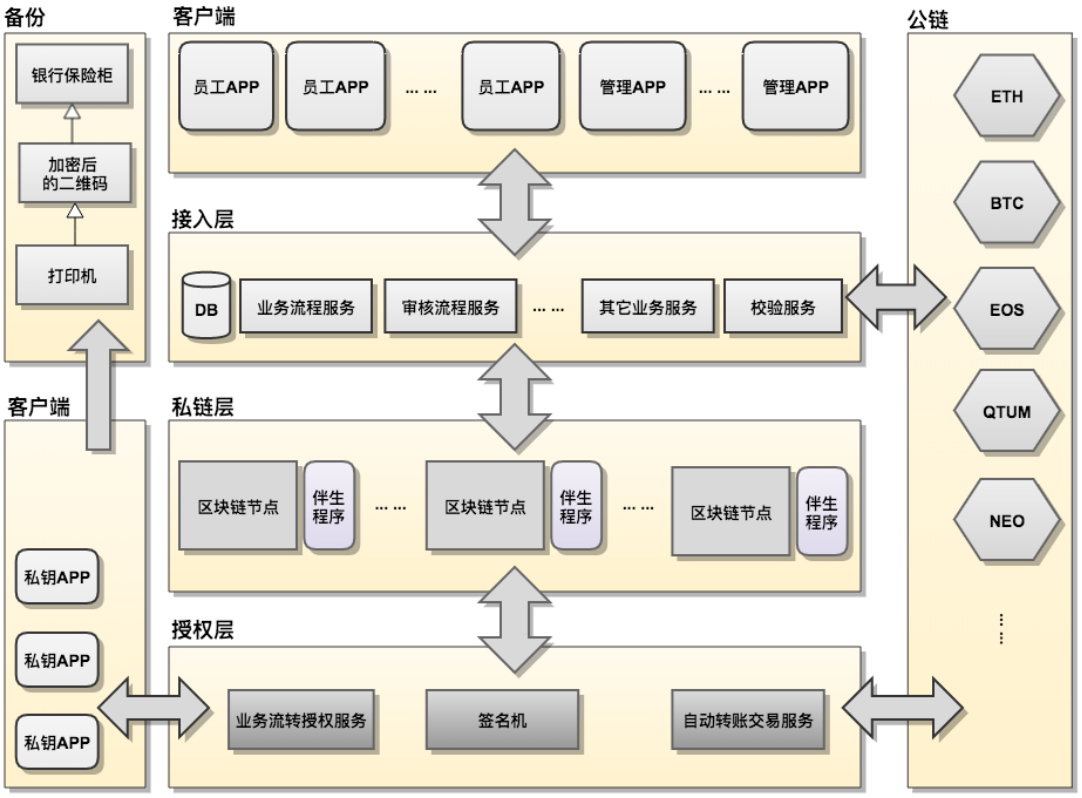
a) 多种数字货币的一站式管理；
b) 多人共管最高管理权限，使得数字资产归属于企业，而不是个人；
c) 企业可以拥有对外的统一收款地址，即数字资产对公账户；
d) 允许设定企业财务审批流程，降低人为操作失误的可能；
e) 在任何情况下，私钥均不能以明文形式暴露；
f) 不可伪造转账指令盗取资产；
g) 方便企业将数字资产入账及审计；
h) 私钥持有人一旦发生意外事故导致不能行使权力，企业资产不能丢失

二. 设计思想

BOX 是一套企业自主拥有的数字资产银行系统。通过 BOX 系统统一管理企业所拥有的各类数字资产钱包做到集中管理，通过将私钥加密运行在内存中的方式让其永不暴露，通过企业自主拥有的私有区块链网络保证操作指令和资产数据的存证和验真，通过顺序性私钥签名方式构建企业订制化资产管理业务流，通过 SSL/TLS 加密保证通信通道的绝对安全。BOX 从原理上做到了防范外部黑客、内部黑客、单人误操作等当前个人钱包普遍存在的漏洞，同时，BOX 具有入侵锁死、系统重置等安全机制，以此保证企业数字资产的高安全性。



私链节点数量为 2n+1(n≥1),私钥 APP 数量最少为 3 个,具体数量由各企业内部自主定制，签名机是一台独立的物理服务器，应用服务器为云端服务器，不会与签名机有任何通信，签名机仅能够与私链通信，仅有签名机才能向热钱包发出转账指令，员工 APP 为转账指令发起方，管理 APP 执行审批。



BOX 系统可以接入所有支持离线签名的数字货币。首次发行版将接入以太坊及 ERC20 代币。在未来的版本中，将陆续接入其他币种。

三. 私钥安全机制

1. 私钥的存储

私钥储存在签名机的内存中，不会做持久化存储。在极端情况签名机被入侵之后，入侵者很难在短时间内寻找到私钥，大大降低私钥暴露的风险。

签名机是一台独立存放的服务器, 建议存放在安全级别非常高的地点，例如金融级机房、企业自己控制的高安全性机房、某个私密地点。该签名机需要有 24 小时不间断供电和网络接入及固定 IP 地址, 该签名机应该不能轻易地被任何人接近和操作，包括企业的 IT 主管人员。

企业的数字资产实际存储在各个数字货币公链上（本文内指代为"热钱包"），如果该数字货币的官方钱包支持离线签名，则私钥可以被存储在签

名机的内存中，通过离线签名实现在不暴露私钥的前提下，完成确权并转账。

2. 私钥的生成

为了防止私钥的生成被模拟，我们采用 RFC6979 协议的变形形式：k = SHA256(d + SHA256(m1) + SHA256(m2) + SHA256(m3) + …), d 为服务器随机数，m 为私钥 APP 输入的关键句。私钥的生成由三个私钥 APP 分别输入关键句的方式生成，关键句是由任意的字母和数字组合而成的字符串。三个或多个私钥 APP 依次输入关键句后，由三个关键句生成的私钥即被存放在签名机的内存中，同时由此私钥生成的公钥地址将被注册在公链上，即生成公链热钱包。私钥 APP 不会存储该关键句，该私钥 APP 的源代码也将同步开源。

私钥 APP 的所有传输过程都需要双向认证，私钥 APP 的授权方式为限制分发方式，即服务器分发的证书只有 N 个（N 为私钥 APP 的个数），并且会将证书与其设备 ID 绑定，其他的连接请求都会被拒绝。

如果私钥 APP 丢失，因为 APP 里并不记录任何关键句和密码，所以没有安全风险。拥有关键句的控制人可以重新安装私钥 APP，并使用原关键句重新获取服务器证书，然后签名机重新绑定新的私钥 APP 的设备 ID。

3. 私钥的恢复

由于签名机一旦停机，内存中的私钥会立即消失，所以当签名机需要重启时，需要所有私钥 APP 重新输入正确的关键句。如果某个私钥 APP 持有人无法输入正确的关键句，此时需要启用私钥关键句的冷备份，由于此流程属于实际企业管理流程，本文仅给出冷备份的建议方案，请参考"私钥的备份"章节。

四. 私链

1. 私链的作用及优势

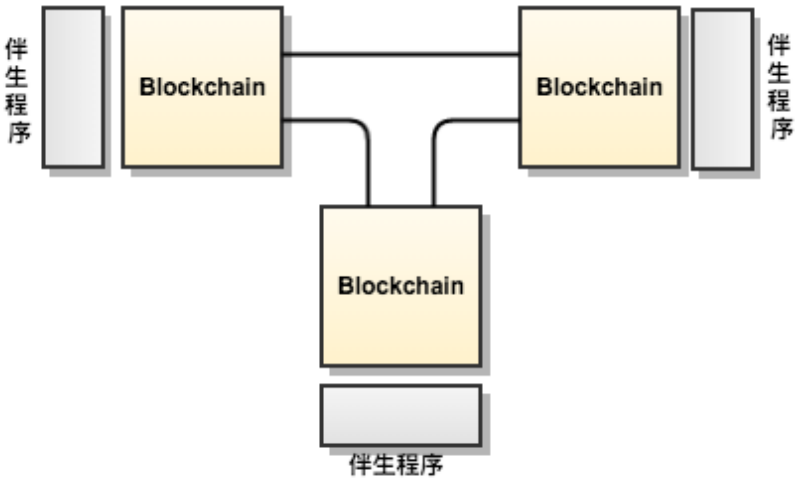
私链在整个 BOX 系统中起到存证和验真的作用。利用区块链的不可篡改的特性，将审批流程和转账审批流程上链保存，为程序实现转账自动化提供可靠依据。BOX 系统首次发行版本采用以太坊搭建私链，未来计划支持更多的搭建私链的方案。

在企业内部部署一套私链，企业不仅获得一套存证和验真的系统，而且可以独立自主控制其全部节点，通过设置节点参数，来控制每个区块最大可打包交易数量、出块时间间隔和参与节点的数量。这些参数决定了单位出块时间窗口内，可以接受的交易笔数——即审批流转处理的吞吐量。

由于是私链，使得 gas 消耗可以忽略不计，同时对上层应用弱化 gasPrice 的消耗，使得在区块链上驱使合约的代价降低。

私链采用 PoA（Proof of Authority）共识机制，直接指定哪些私链节点拥有记账权限，没有记账权限的节点将作为备份节点存在。

2. 伴生程序

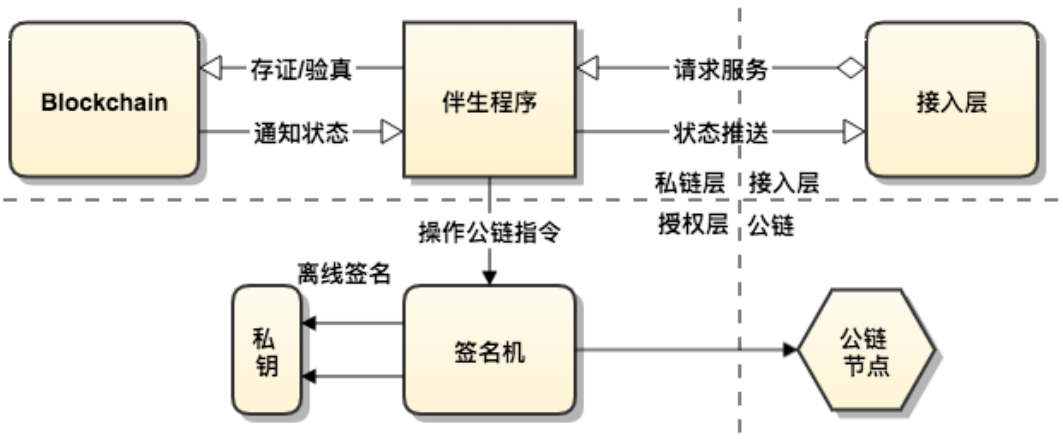


伴生程序就是以太坊 DAPP。每个私链节点都会配备同一个伴生程

序，被用于处理传统的 CS（客户端-服务器）应用程序请求、处理数据上传私链、执行智能合约、监听智能合约事件、发送状态通知、协调上层应用和授权服务之间的交互等功能。

伴生程序之间是对等的，且只与处于同一台服务器上的私链节点通信。伴生程序之间没有直接的网络连通。每个伴生程序都会对应一个私链的账户，该账户用以执行智能合约的方法。

伴生程序协调接入层与授权层之间的交互。发生一笔转账交易要经过以下四个过程：1. 发起交易；2. 服务受理；3. 交易成功；4. 通知结果。我们将这四个过程划分为四个象限，如下图所示。伴生程序处于私链层这一象限维度，通过将数据上链实现对现实中的转账交易进行存证和验真，同时将成功的结果通知到签名机，由签名机根据最终结果操作公链资金账户。伴生程序隔离了交易发起者与公链资金账户之间的直接关联，整个过程由程序根据审批流自动执行。



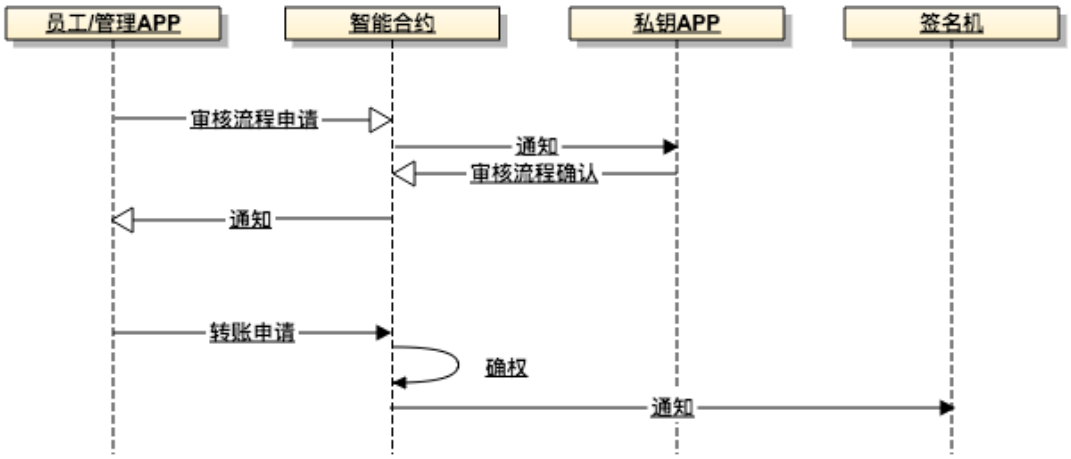
3. 智能合约的共识机制

上链存证的数据存放在智能合约内。智能合约采取投票的方式来确认一笔上链存证的数据，每一笔数据都必须通过 51%的私链节点投票，且每次投票的内容一致才被确认为有效存证。每个节点分别对应一个操作同一合约的账户，除非超过 50%的节点被全部攻陷，否则上链存证的数据是可

以被保证有效的。

智能合约投票系统需要分配合理的权限给正确的账户。所有私链账户在私链搭建完成后即被确定下来。当需要增加私链节点时，必须由所有私链账户授权新帐号，系统将自动重新平衡 51%策略，无须重新部署新合约来适应其变化。

存证的数据分为审核流程和转账申请。如下图所示：在提现之前，需要设置审核流程；审核流程用于确定企业内部在使用数字货币时需要参与审核的部门，参与审核的部门需要多少人确认；审核流程需要由掌握企业管理最高权限的所有私钥 APP 来授权；授权过后的审核流程可以用来发起转账申请。



五. 接入层

接入层采用权力离散式的构架方式。

整个系统的权力被离散在了各个 APP 端，接入层服务器虽然承担了各种业务的转承并合，但是却对信息所行使的权利无法修改和执行。

权力离散式的实现，依赖于基础算法 ECDSA（ Elliptic Curve Digital Signature Algorithm ）。 算法中 ECC（Elliptic curve cryptography）则采用比特币经典曲线 secp256K1。

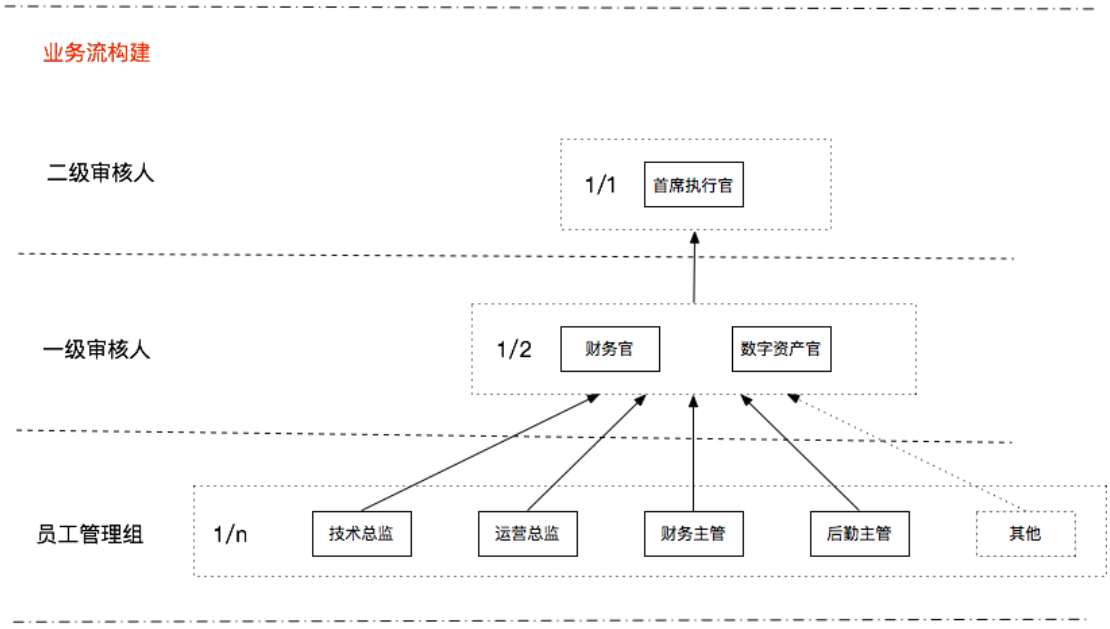
转账过程为：由员工 APP 和管理 APP 产生签名，然后在接入层完成转

移，并在私链层得到确认，最后签名机在公链上进行实施。

接入层业务分为两大部分：1、审批流的构建和修改。 2、审批流的执行。

1. 审批流的构建和修改

在执行转账前需要先构建企业转账审批流，该审批流为多级审核模型，最底层为员工管理组，其上可以有多级审核，每级审核可以有多个审核人，需要指定最小审核人数。



举例说明，企业审批流如下图所示：

当企业确认了审批流，则可以通过管理 APP 录入系统，构建成系统可识别的协议格式，该协议格式在 BOX 系统中被命名为 boxflow。

boxflow 建立完成之后为未授权状态，如果需要授权，则转交给接入层，接入层检查格式并哈希上私链，由私链所有节点投票存证，存证后通知签名机。由私钥 APP 授权签名机将审批流哈希写入公链，公链确认后，将私链上审批流的哈希状态设置为有效，则 boxflow 授权成功（关于私钥 APP 的安全性及重要性，见私钥安全和指令安全章节），企业可以通过该

boxflow 进行转账。

boxflow 的修改流程需要私钥 APP 先取消当前 boxflow 的授权，再重新建立 boxflow。

2. 审批流的执行

当 boxflow 授权成功后，需要先建立员工账号，才能进行基于该 boxflow 的审批流转账。

在 BOX 系统里员工账号由员工管理组分配公私钥。当 boxflow 授权成功后，员工 APP 将获取到当前 boxflow，员工选择员工管理组申请私钥，员工管理组衍生出子私钥，分配给该申请员工 APP。

员工 APP 获取私钥后，可以发起转账申请。申请格式如下：

```
{ balance: 100E18,
   timestamp: 1512719484736,
   destination: '0x6E9483f00cCd685c5F12709Fd542Da1FB20c4d2e',
   miner: E16,
   currency: 'ETH',
   applicant:
    { username: 'bluce'} }
```

此时生成的申请为未签名状态，需要将该申请使用 SHA256 算法进行哈希，并将哈希签名放入申请中，格式如下：

```
 { balance: 100E18,
   timestamp: 1512719484736,
   destination: '0x6E9483f00cCd685c5F12709Fd542Da1FB20c4d2e',
   miner: E16,
   currency: 'ETH',
   applicant:
    { username: 'bluce',
      sign:
'474w3zgKRLwaddG6LadzKQ3ut1JyQUc4HpVLkydR6xdk2TwS7zEXKf4E5AyGH
xQkfLYxJsccxhqdY5Qm5352P2H4' } }
```

该员工的申请，只能由其对应的员工管理组账号审核。

员工管理组审核通过后，对申请（包括签名）进行哈希并签名。签名完成后交给上级审核人进行审核，上级审核人对下级签名信息验证后，对

哈希进行签名。以此类推直至最上层审核人签名完成。

最后生成的转账审核流视为一次记账，称之为 transbox。

该 transbox 哈希后为该次交易的交易 ID，当接入层收到 transbox 并校验其匹配对应的 boxflow 后，将交易 ID（哈希）进行上私链存证。私链通过投票确认交易 ID 后通知签名机进行验证和签名。

签名机收到原始信息后，从 transbox 中提取 boxflow 并在账户里验证是否合法，然后依次检验签名是否完整，验证通过后说明为合法 transbox，进行公链转账，并将公链交易 ID 上私链存证。接入层可以根据交易 ID 在公链上实时查询结果。

3. 多审批流的支持

在第一个公开发行版本中，BOX 仅支持单一审批流，在后续升级版本中，将支持多审批流。

六. 审批流安全机制

自动化转账的安全有两个重要部分，其一是私钥本身的安全（已在私钥安全性章节中阐述），其二是使用权（审批流）的安全。本章将对审批流的安全展开阐述。

1. 审批流的有效性

一个合法的审批流需要经过私链存证、私钥 APP 授权和公链确认。由于私钥 APP 是由 N 位企业管理人员掌控，因此审批流是否有效是由 N 位企业管理人员共同确认，并且写进公链私链，该审批流有效性无法篡改。

2. 转账的生成

转账由员工 APP 发起并签名，经过员工管理组及各层审核人员依次验证无误后签名，转账即生成。因为公私钥只有 APP 上存在，其他任何人在传输的过程中都无法篡改转账信息。

3. 转账的有效性

转账的有效性分为两个部分，其一是本身签名的有效性，其二是其对应的审批流的有效性。由于 BOX 采用的是嵌套签名的方法，因此只需要按照顺序依次验证签名，即可知道签名本身是否有效。转账本身是对应一个审批流，需要提取对应的审批流，并在账户中验证该审批流是否有效。如果两个条件均满足，证明该次转账是由有效审批流指定的 APP 确认的，并且是无法篡改的。

七. 通信安全机制

1. 签名机与私链的通信

签名机即授权层中的服务所在的服务器。签名机与私链的通信即授权层的服务与私链层服务之间的通信。服务与服务之间的通信使用 gRPC + SSL/TLS 双向证书认证。gRPC 是一个高性能 RPC 框架，基于 HTTP/2 协议标准设计，基于 ProtoBuf(Protocol Buffers)序列化协议开发，HTTP/2 协议标准本身要求对数据进行加密传输（SSL/TLS）。BOX 系统将针对所有公链开发授权服务模块。由于 SSL/TLS 双向认证证书的存在，将极大程度保证信息安全，服务器之间一旦有异常连接就会立即拒绝请求，可以防止中间人攻击的风险。

2. 员工 APP 与接入层的通信

所有与接入层通信的 APP，都采用 HTTPS 的方式。员工签名用的私钥是通过管理 APP 颁发的。处理步骤如下：

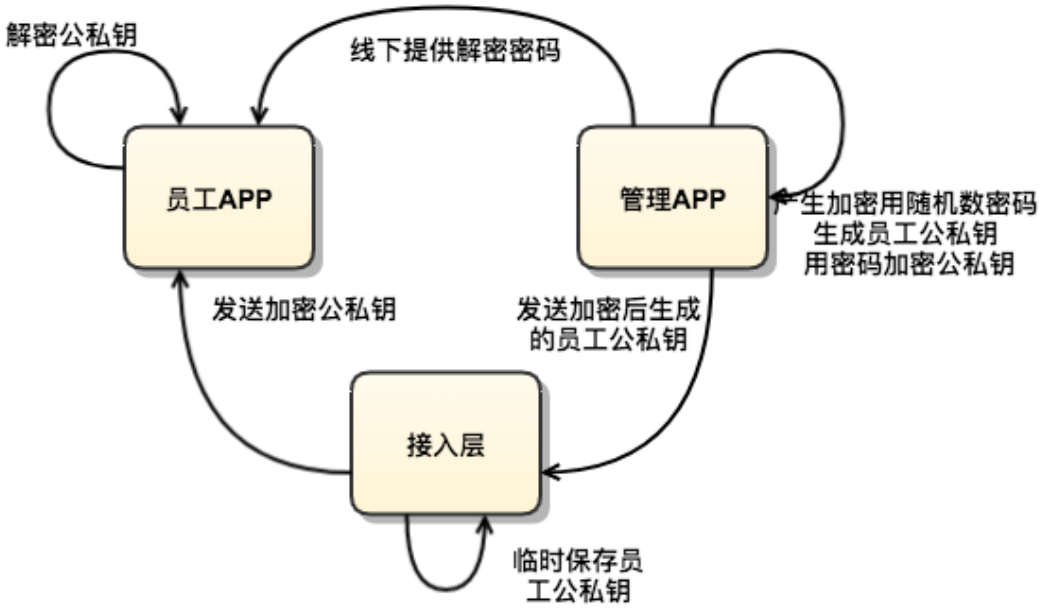
A) 管理 APP 生成员工私钥，并生成对称加密用的随机数密码；

B) 管理 APP 用密码以对称加密的方式将员工私钥加密；

C) 管理 APP 通过线下方式将密码告知员工；

D) 管理 APP 将加密后的员工私钥发送给接入层暂存；

E) 员工 APP 从接入层下载加密数据并用给定密码解密。



3. 接入层与私链节点的通信

接入层与私链之间属于内部通信，采用 TCP/IP 协议连接。此时接入层传递到私链的数据已经经过了签名授权，并产生了信息摘要，私链只需要使用签名校验程序对其验真，如果校验失败，拒绝服务。接入层向所有私

链节点发送请求，每个私链节点对应一个帐号，每个帐号将验证后的请求数据以投票机制上链存证，私链上的智能合约被超过 50%帐号确认之后，数据上链成功。接入层提供签名和摘要供私链确认，私链通过投票向接入层提供投票结果。以上过程可以归纳为两个公式：

signature = sign(hash)

public key == recover(hash, signature)

八. 私钥的冷备份

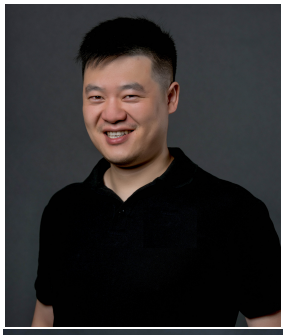
打印并存放在银行保险箱！

为了防止某个私钥 APP 持有人的意外情况导致私钥无法重置，我们建议将所有关键词进行物理备份。例如在每个私钥 APP 持有人输入关键词后，私钥 APP 所运行的手机可以连接一台不联网的迷你型打印机，采用打印的方式将该关键词自动以二维码的方式打印到纸条上，并且将打印两份，所有关键词纸条将被分为两份，封存在两个信封内，建议企业将此迷你打印机与两份关键词备份件分别存放于两家银行保险箱中，保险箱的其中一把钥匙可以委托给企业律师持有，并约定仅允许在企业董事会决议的同意下才可以启封此备份。

九. 开发计划

- 2017 年 10 月开始项目规划。
- 2018 年 1 月完成 demo 版。
- 2018 年 4 月开源 1.0 版。
- 2018 年 7 月开源 2.0 版。
- 2019 年 1 月开源 3.0 版。

十.主要成员介绍



项目发起人：尚维斯，花名达摩；

16 年互联网从业经验，曾任职知名区块链企业 VeChain 唯链 COO、eBay 易趣高级产品经理、楼顶科技 CEO 等职。

项目技术负责人：裘春荣，花名阿尔法；

15 年软件开发及架构经验，曾任职唯链架构师、大智慧架构师，高级 Java、Go 工程师、以太坊开发工程师。

项目运营负责人：马卓，花名安东尼；

16 年互联网运营经验，纽芬兰纪念大学经济学硕士，曾任职 Coach 大中华区电商负责人、eBay 易趣市场经理；

CFO:　张楷沅　Bryan Zhang

20年企业内控管理、 税务筹划、并购整合、商业流程重整、企业管理工作经验。曾先后任职于家乐福（中国）总部、英博(中国)总部、麦德龙(中国)总部等知名跨国企业的财务和税务部门，并担任中国区经理职位。之后任职于法国艾美斯集团，并担任副总裁职位。

十一. 关于加密令牌 BOX 的分发

1. 令牌分发简介

令牌代码	BOX
令牌名称	BOX Token
分发总量	100,000,000 枚（壹亿枚）
分发日期	2017 年 12 月 26 日 UTC00 时 00 分 00 秒(Boxing Day)
代币分配	20%团队预留，30%为机构私募，50%为企业战略投资
兑换比例	1 枚 eth 兑换 2500 枚 box
锁定期限	全部没有锁定期限制
上架日期	待定
官网地址	BOX.LA

2. 分发比例及组成

组成	说明	比例	数量
团队预留	天使资助人奖励	2.5%	2,500,000
	创始团队奖励	2.5%	2,500,000
	商业推广	5%	5,000,000
	持续经营	10%	10,000,000
企业战略投资		50%	50,000,000
机构私募投资		30%	30,000,000

3. 经济模型

BOX 作为一种 BaaS（Blockchain as a Service）解决方案，将以 ERC20 代币 BOX Token（缩写符号为 BOX）作为 BOX 系统的价值中介及社区中的投票权。BOX Token 总量 1 亿枚，永不增发。

BOX 系统将会全部开源，任何组织和个人均可以无偿部署并使用该系统，对项目团队有增值服务的需求时可以使用 BOX Token 购买官方的技术支持服务，服务的价格会依市场供需关系动态调整。

团队收取的 BOX Token 将会锁定，在每年的 12 月 26 日 UTC 伦敦时间 00:00:00 释放，释放方式为定向出售，价格为释放开启时间之前的最近 7 日均价的 90%，所获取资金全部用于团队发展运营使用。

BOX 开源社区中的代码更新、选举、网络参数变更等投票权重取决于钱包地址中 BOX Token 的数量。