CSA GCR cloud security alliance ®
GREATER CHINA REGION

数字钱包安全
开发与应用实践

@2020 云安全联盟大中华区-保留所有权利。你可以在你的电脑上下载、储存、展示、查看、打印及，或者访问云安全联盟大中华区官网（https://www.c-csa.cn）。须遵守以下: （a）本文只可作个人、信息获取、非商业用途；(b) 本文内容不得篡改; (c)本文不得转发; (d)该商标、版权或其他声明不得删除。在遵循中华人民共和国著作权法相关条款情况下合理使用本文内容，使用时请注明引用于云安全联盟大中华区。

致谢

云安全联盟大中华区（简称：CSA GCR）区块链安全工作组在 2020 年 2 月份成立。由黄连金担任工作组组长，9 位领军人分别担任工作组下的 9 个项目小组组长，分别有：知道创宇创始人&CEO 赵伟领衔数字钱包安全小组，北大信息科学技术学院区块链研究中心主任陈钟领衔共识算法安全小组，赛博英杰创始人&董事长谭晓生领衔交易所安全小组，安比实验室创始人郭宇领衔智能合约安全小组，世界银行首席信息安全架构师张志军领衔 Dapp 安全小组，元界 DNA 创始人兼 CEO 初夏虎领衔去中心化数字身份安全小组，北理工教授祝烈煌领衔网络层安全小组，武汉大学教授陈晶领衔数据层安全小组，零时科技 CEO 邓永凯领衔 AML 技术与安全小组。

区块链安全工作组现有 100 多位安全专家们，分别来自中国电子学会、耶鲁大学、北京大学、北京理工大学、世界银行、中国金融认证中心、华为、腾讯、知道创宇、慢雾科技、启明星辰、天融信、联想、OPPO、零时科技、普华永道、安永、阿斯利康等六十多家单位。

本白皮书主要由数字钱包安全小组专家撰写，感谢以下专家的贡献：

原创作者：黄连金、肖龙、姚昌林、赵伟（按照字母排序）
审核专家：陈钟、徐正伟、杨士田、姚晓宇、余弦、赵淦森（按照字母排序）
贡献单位：北京大学、知道创宇（按照字母排序）

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c-csa.cn/research/）上查看。

如本白皮书有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号：

©2020 云安全联盟大中华区-版权所有

序言

随着数字经济的发展，伴随着区块链技术而来的数字钱包形成对数字资产管理方式的冲击，对于大部分区块链的用户来说，数字钱包是他们首先接触的用户界面。数字钱包有各种不同的形式，但是都会直接或间接地对数字资产进行控制，或者说直接或间接地存储了可以控制数字资产所需要的私钥。

《数字钱包安全开发与应用实践》白皮书分析各种不同的数字资产钱包，和可能的风险和案例，对于如何开发和使用数字钱包提出了中肯的意见和最佳实践，并且提出了数字钱包安全测试标准。数字钱包的技术和安全随着区块链技术的发展，也在不断的发展，本文档对数字钱包安全进行的系统性分析和建议，希望对终端用户和钱包开发者有借鉴作用。

CSA GCR cloud security alliance GREATER CHINA REGION

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

致谢.....3
序言.....4
1 数字货币钱包分类使用场景.....6
2 数字钱包安全风险分析.....8
2.1 数字钱包使用过程安全分析.....9
2.2 数字钱包开发&应用技术安全分析.....10
3.数字钱包安全案例分析.....13
3.1 数字钱包安全事件回溯.....13
3.2 用户安全使用引导.....13
3.3 数字钱包安全设计.....14
4 数字钱包安全设计应用实践.....15
4.1 无私钥钱包用户需求分析.....15
4.2 企业级数字资产钱包需求分析.....20
5. 数字钱包安全测试标准.....25
参考文献.....37
关于云安全联盟大中华区.....38

©2020 云安全联盟大中华区-版权所有

1 数字货币钱包分类使用场景

数字货币钱包是用来帮助你存储、管理、交易数字货币的工具，利用钱包中生成的数字货币收款地址（公钥），可以接受他人给你转账的数字货币，也可以把你钱包中所拥有的数字货币资产转账给他人。

从私钥存储方式、存储数据量和使用主体三个维度将钱包进行分类介绍：

按照私钥存储方式分类，可以将钱包分类冷钱包和热钱包两大类。

（1）冷钱包：

是指使用时不需私钥接触网络的钱包，网络无法访问私钥，比如专业的硬件设备，也称硬件钱包或离线钱包，一般通过 USB 接口、蓝牙、二维码等方式完成私钥签名。

优点：安全等级最高，避免了被黑客盗取私钥的风险；自己真正拥有私钥，不受他人监管。

缺点：硬件相对较贵；创建钱包和交易相对复杂，效率偏低；只支持主流币种，一般新的小币种不支持；存在硬件丢失或损坏的物理安全风险。

适用场景：交易所、企业、银行、机构、大额持币用户等资产管理安全性较高的场景。

（2）热钱包：

使用时需要接触网络的钱包，包含电脑客户端钱包、手机 APP 钱包、网页钱包等，也称在线钱包。

优点：创建钱包和交易均简单，使用方便，转账效率高。

缺点：安全性不足，私钥容易被黑客盗取；手机或电脑丢失，私钥容易被专业人士破解。

适用场景：新手、持币数量较少者、频繁交易者用于个人用户数字资产便捷交易（客户端钱包，浏览器钱包，网页版钱包）。

©2020 云安全联盟大中华区-版权所有

按照数字货币是否中心化管理分类，可以将钱包分为去中心化钱包和中心化钱包，按照存储区块链数据方式，去中心化钱包又分为全节点钱包（重钱包）和轻钱包。

（1）全节点钱包：是指需要同步所有区块链数据的钱包。

优点：可以实现去中心化，更好的隐私性；可以在本地验证交易数据的有效性。

缺点：占用很大的硬盘空间，每次使用前需要同步数据；多币种数字资产支持不好，用户体验欠佳。

适宜人群：企业、专业人士主要代表

（2）轻钱包，指依赖区块链网络上其他全节点，仅保存和同步与自己相关的数据。

优点：占用硬盘空间较小，使用时不需同步数据；可以支持多币种数字资产，设计功能简单，用户体验好。

缺点：实现去中心化不足，交易验证相对较慢。

适宜人群：个人、小白用户主要代表

（3）中心化钱包，是指不依赖区块链网络，所有的数据均从自己的中心化服务器中获得，也称链下钱包。

优点：平台负责私钥的安全管理，私钥（密码）忘记或丢失可以找回；交易效率很高，可以实时到账，可以支持多币种；钱包被盗，大型交易所一般会给予等值赔偿。

缺点：过度依赖中心化，存在平台自盗、倒闭、跑路等风险，另外是黑客重点攻击目标。

适宜人群：炒币群体，需要频繁交易主要代表。

按照钱包的表现形态分类，分为：网页钱包、浏览器插件钱包、PC 端钱包、硬件钱包、手机 app 钱包。

（1）网页钱包：

网页形式发布的钱包程序，无需安装，打开即可使用、跨平台，有浏览器的设备即

©2020 云安全联盟大中华区-版权所有

可。

（2）浏览器插件钱包：

以浏览器插件的形式存在，比如 chrome 浏览器的 Metamask 钱包插件。

（3）PC 端钱包：

指电脑终端的数字货币钱包，可以通过这个终端进行操作，不便捷。

（4）硬件钱包：

指用专业的硬件存储数字货币，将数字资产私钥单独储存在一个芯片中，与互联网隔离，即插即用。硬件钱包是一个实体设备，不能保证 100%安全。只是相对于其他保管手段，这是最安全的储存手段之一。

（5）手机 APP 钱包：

目前最常见的，适用于新人的就是 APP 轻钱包,也是大家用的比较多的，相对于网页钱包更加灵活方便，安全性较高。但对于大额的数字资产用来说安全性欠缺，可使用不联网的手机生成冷钱包，联网手机仅用于查看钱包。

近几年 APP 钱包出现一种基于智能合约的钱包，用户可以控制私钥和资产，但是利用智能合约可以增加一些基于区块链的功能，比如 MYKEY、Argent、Gnosis Safe、Authereum 这些，核心风险主要在智能合约这块。我们在第五章安全测试标准对于这种类型的钱包的测试提出建议。

2 数字钱包安全风险分析

2019 年 1 月黑客利用 Electrum 钱包漏洞窃取了约价值 75 万美元的 BTC。

2019 年 5 月，黑客入侵币安交易所并盗取了 700 枚 BTC，总价值高达 4000 万美元。

2019 年 6 月 Gatehub 存放用户 API 访问令牌的数据库遭受入侵，初步统计已有 100 个 XRP 钱包信息泄露，损失估计为 1000 万美元。

2019 年 7 月位于新加坡的加密通证交易所 Birtue 遭受黑客攻击，因其风险管控漏

洞，黑客共盗取了价值 500 万美元的 XRP 与 ADA。

数字钱包安全性问题日益严峻，交易所钱包的安全漏洞、风险管控的疏忽使用户的加密资产面临被黑客攻击、盗取的风险，对加密通证市场的发展产生不良影响，但客观上也为未来数字钱包行业的完善进步指明了方向。

2.1 数字钱包使用过程安全分析

在加密数字货币钱包的日常操作使用过程中，主要有创建钱包和使用（包含交易，钱包余额查看等）两个环节，针对不同的环节我们整理了软硬件层面大部分的安全漏洞和黑客攻击方式。

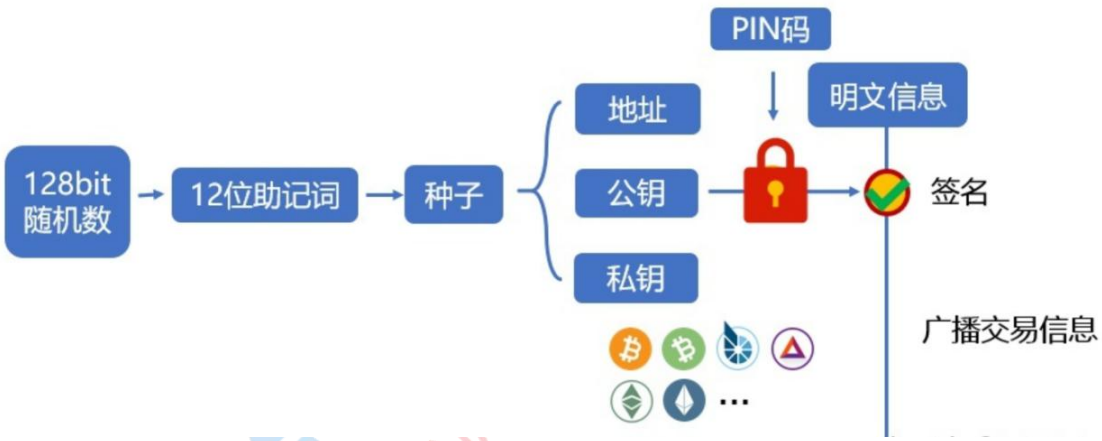

图 1-1

环节		漏洞	攻击方式
创建钱包	随机数	128bit 随机数的随机问题，空间分布不均，缺乏专门的审计流程对随机数进行安全测试	随机数攻击
	助记词	助记词保存不安全，助记词强度不足	盗取、暴力破解
	私钥存储	App 钱包数据没有加密存储，运行环境存在未知病毒以及操作系统漏洞	漏洞利用、复制盗取
		硬件钱包设备接口过多，未采用安全芯片，软系统过于复杂	盗取设备暴力破解
	私钥使用	联网操作存在 HTTPS 及 DNS 劫持风险	钓鱼攻击
交易环节	创建交易	交易双方的账号没有二次验证	收款账户信息被恶意替换
	交易签名	在线环境不安全，协议设计不严格	盗取 PIN 码
	交易广播	操作系统不安全，非私密链接	通讯拦截交易

表 1-1

2.2 数字钱包开发&应用技术安全分析

1) 运行环境的安全风险

加密数字货币钱包最核心的文件—私钥/助记词是存储在终端设备上的，无论是 PC 端还是移动端，终端设备如果出现不安全的现象，对于私钥/助记词来说是有非常高的安全风险的。一个安全的数字钱包，在设计之初就应该避免因为运行环境不安全而导致的私钥/助记词被盗的可能。终端上运行环境的安全问题主要包括病毒软件、操作系统漏洞等。

（1）病毒软件

和普通的银行客户端或支付 APP 不同的是，加密数字货币钱包的私钥/助记词不具备挂失能力，无法通过对账户进行冻结来降低损失，一旦被盗则资产一定会丢失。一款安全的数字钱包，能否对扫描出的终端环境里面的病毒软件和未知病毒软件进行防御是核心考核指标之一。

（2）操作系统漏洞

利用操作系统漏洞，可以轻易的绕过操作系统设计的一系列安全边界或沙箱机制，获得访问加密数字货币钱包私钥/助记词的能力。无论是 Android、iOS、Windows 还是 Linux，每年都有大量的安全漏洞被公开和修复，而这些漏洞里面就有不少高危的本地提权的漏洞。利用这些提权漏洞就可以轻易的打破操作系统的安全设计边界，获得访问用户数字钱包私钥/助记词存储文件的能力。

目前大多数加密数字货币钱包的安全设计都是完全依靠操作系统的安全边界，对于私钥/助记词的存储和处理还是停留在早期的使用固定密钥进行加密甚至直接明文保存，完全依靠操作系统的安全边界来限制其他 APP 的访问，由于缺乏对于系统漏洞的防御，这些数字钱包的用户如果安装了带有本地提权机制的应用，那么其数字资产将面临严重的被盗风险。

2) 网络传输的安全风险

网络传输的安全性更多的体现在是否有良好的对抗中间人攻击的能力上。中间人攻击（英语：Man-in-the-middle attack，缩写：MITM）是指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全监听和控制。

虽然大部分数字钱包应用都会使用 HTTPS 协议和服务端进行通讯，但是中间人攻击方法上是可以通过在用户终端中安装一个数字证书的方式拿到 HTTPS 协议里面的内容。

安全的数字钱包需要能够对终端里面全部的数字证书的合法性进行扫描、对网络传输过程中的代理设置进行检查并能够保障基础的网络通讯环境的安全性。在数字钱包的开发中，在网络传输层面是否使用双向校验的方式进行通讯验证也是衡量一个数字钱包应用安全性的重要评判标准。

3) 私钥（助记词）随机数生成风险

私钥的保管对于用户加密通证的安全极为关键。私钥本质是一串随机选出的一定长度的数字。这串数字控制着通证账号的所有权，因此这串数字相当重要，要具有足够的随机性。 在私钥的产生过程中，一般采用密码学安全的随机数生成器器

©2020 云安全联盟大中华区-版权所有

(Cryptographically Secure Pseudorandom Number Generator: CSPNG)，并且需要有一个来自具有足够熵值的源的种子(seed)。

硬件钱包在私钥的随机性上主要依托于自身的安全芯片进行随机数生成，而有些硬件钱包会采用更为有效的方法生成随机数，例如采集硬件噪声所生成的系统熵作为随机数，或使用自身搭载的摄像头进行环境图像采集，生成系统熵用于私钥产出。

4) 私钥（助记词）存储方式风险

对于数字钱包的私钥/助记词，终端设备的存储方式也是需要在安全性设计上加以注意的。私钥/助记词文件存放目录的访问权限、私钥/助记词存储的形式和加密算法设计都需要通过严密设计。

在对多款主流数字钱包进行安全性分析时，我们发现即便是知名的数字钱包，在私钥/助记词的存储上也是比较随意的。既有明文存储的，也有虽然是加密存储但是解密的密钥却是在代码里面固定写死的，起不到任何的安全防御作用。

5) 应用自身的安全风险

数字钱包应用自身的安全风险主要集中在应用安装包自身的安全防御上。应用安装包是否具备抗篡改能力是非常核心的技术能力。另外，应用运行过程中的内存安全、反调试能力、私钥/助记词使用的生命周期管理、调试日志的安全性、开发流程的安全等方面也是需要去设计增强的。

6) 数据备份的安全风险

如果数字钱包应用的数据能够被备份出来，就可以使用计算性能更加强大的机器对私钥/助记词进行暴力破解。举例来说，如果 Android 属性设置为允许备份，那么就可以利用系统的备份机制对应用的数据文件进行备份，而加密数字货币的私钥/助记词也就被备份到外部介质了，这就从另外一个方向打破了操作系统的安全边界设计。

©2020 云安全联盟大中华区-版权所有

3. 数字钱包安全案例分析

3.1 数字钱包安全事件回溯

2018 年 12 月 28 日，知名比特币钱包 Electrum 遭受新型钓鱼攻击已经损失近 250 个比特币（约 91.4 万美元），黑客利用僵尸网络发动约每秒 25Gb 的恶意流量阻塞服务器，然后劫持服务器并诱导用户跳转钓鱼网站。这个钓鱼网站声称用户需要升级钱包客户端并向用户提供携带后门的版本，用户升级后比特币会被立即转走。

2019 年 6 月 5 日，用于安全存储/处理 XRP 的钱包和网关——GateHub 中大约有 80-90 个受害者受到黑客攻击，被窃总量大约为 23,200,000 瑞波币。没有确凿证据指向攻击的源头，攻击的发生可能有各种方式，包括钓鱼、Gatehub 账户被黑客攻击，Gatehub 包含用户私钥的加密数据库被盗并且被离线暴力平均等。

2019 年 10 月 11 日，网页加密货币钱包 Safuwallet 被黑客通过注入恶意代码窃取了大量资金。

2020 年 7 月 25 日，数字钱包 Ledger 的数据库被未经授权访问，导致数据泄漏。泄漏的数据包括电子商务和市场营销数据。付款信息和加密资产是否安全，外界不能确定，虽然 Ledger 官方认为是安全的。 Ledger 的公告声称黑客利用被盗的 API 密钥用于未经授权访问数据库。目前 API 密钥已失效。

3.2 用户安全使用引导

- 必须要对私钥或助记词加以备份保管，放在不同安全地方，备份后并进行验证，备份信息不要接触网络。

- 钱包下载时官网下载最安全，下载后可以通过检验哈希值是否和官方公示一致的方法进行验证真伪，其他下载渠道就尽量不要使用。

- 及时更新数字钱包版本，防止最新的安全漏洞给黑客攻击的机会。

- 一般个人用户而言，选择中心化钱包，不用担心私钥备份和丢失问题。

- 对于持币量较大的用户，或者长期投资不做频繁交易的，需要选择专业的硬件

©2020 云安全联盟大中华区-版权所有

冷钱包。

- 对于去中心化钱包，私钥交由用户保存，重视钱包安全核心要素的手动备份。建议通过相对原始的方法来手动记录，远离截图、复制等一切电脑操作，养成良好的上网习惯，将风险降到最低。条件许可的话，可以考虑专门用于数字钱包的手机，不下载其他任何移动应用。

3.3 数字钱包安全设计

1. 网络传输安全

大部分数字钱包应用都会使用 HTTPS 协议和服务端进行通讯，但是中间人攻击方法上是可以通过在用户终端中安装一个数字证书的方式拿到 HTTPS 协议里面的内容。安全的数字钱包需要能够对终端里面全部的数字证书的合法性进行扫描。在数字钱包的开发中，在网络传输层面是否使用双向校验的方式进行通讯验证是衡量一个数字钱包应用安全性的重要评判标准。

2. 接口调用权限安全

钱包本身只是区块链世界的接口软件，目前很多都是使用 RPC 调用相应接口，这样调用过程对数据传输的权限控制是数据通讯时的安全之本，对代码和各种场景的设计要非常仔细。远程过程调用时安全策略：如在以太坊钱包节点 Geth 上启用远程过程调用访问时，千万不要允许带有解锁账户功能的远程过程调用的外部访问等。

3. 客户端文件管理安全

文件安全主要考虑的是安装在用户端的文件是加密并不可被破解的，以及对用户的一些禁止性操作或者增加对某些风险操作的不便利性来降低用户造成的风险。

1）抵御终端不良程序对关键文件的访问

加密数字资产钱包最核心的文件—私钥/助记词是存储在终端设备上的，无论是 PC 端还是移动端，终端设备如果出现不安全的现象，对于私钥/助记词来说是有非常高的安全风险的。一个安全的数字钱包，在设计之初就避免因为运行环境而导致的私钥/助记词存在被盗可能，比如增加用户操作要访问到核心文件时必须进行人脸识别或者短信

©2020 云安全联盟大中华区-版权所有

确认的功能等。

2）终端关键文件加密

对终端关键文件采用高安全的加密方式，防止普通程序访问，或者即使关键文件被复制出去，第三方也不能轻易破解的功能。在设计钱包时需考虑实际安全操作性采取限制直接导出关键文件的操作，或者允许导出关键文件但是解密方法以不能进行任何操作的显示方式，供用户手动记录。

3）助记词等关键信息生成和管理

对于钱包的核心关键信息，如助记词、私钥、Keystore 的生成和管理需充分考虑安全性。这三者的设计原则和思路基本相同，以助记词为例：为确保客户端生成助记词，不能经过任何云端或者服务器，这是去中心化钱包的核心，任何访问助记词的过程都需要用户主动确认，如上面提到的人脸识别或者短信确认的功能等。

4. 开发扩展安全

考虑到钱包作为区块链的接口端，对应用扩展需求很重要，所以设计上需严格控制开放端口的权限，确保通讯只是公钥签名。 同时对应用程序要严格审查是否具备抗篡改能力的核心技术能力，以及应用运行过程中的内存安全、反调试能力等。除此之外，考虑到用户密码忘记的风险，可以考虑采用多签方式增加各种应用场景，如密码找回功能等。

4 数字钱包安全设计应用实践

4.1 无私钥钱包用户需求分析

加密货币钱包一直被认为是未来加密数字经济必中不可少的基础设施。传统的加密钱包提供的解决方案是，基于密码学生成公私钥，用户通过手中的私钥来验明自己的身份，从而获得资产的控制权。但私钥的存储方式十分考究。没有了私钥，就失去了资产的掌控权，几乎所有传统钱包都在用户注册时就提示用户使用物理方式记录自己的私钥信息。出于手机的私钥存储文件可能遭遇病毒、误删清理等方式等威胁。手动抄写纸质

©2020 云安全联盟大中华区-版权所有

版私钥的方式相对更安全、隐蔽。但这样的操作逻辑对于初级用户来说是非常不友好的，不仅私钥的概念增加了其理解负担，物理存储私钥的模式也一样有丢失风险。如何在妥善保障私钥安全的前提下提升钱包易用性，是钱包开发者永恒的命题。

因为丢失助记词而导致自身加密资产无法找回的情况屡见不鲜，根据 2019 年 Coinmetrics 发布的报告：有近 170 万枚 BTC 已经丢失。许多钱包在创建的过程中，也都要求用户手抄助记词以防止在联网环境下被转移资产。为了保证资金的安全，助记词（或私钥）的保管就需要足够的小心，一方面我们要进行备份，以防私钥丢失，另一方面由于备份也会增加被盗风险，这也是钱包糟糕的体验的一大原因（安全与体验需要权衡折中考虑）。因此，如何在保障用户资产安全的同时摆脱对私钥/助记词的依赖，更好获得区块链钱包的用户体验，成为越来越多团队的研究方向。

门限签名技术实现“私钥自由”：

为了提高资产的安全性，尤其是大额资产，目前通常有这三个方案：多签签名（MultiSig）、 密钥共享（Secret Sharing）模式和门限签名(Threshold signatures：TSS)方案。

①多签签名（MultiSig）

如果大额的资产，通常会使用多签（MultiSig）的方式来分担风险与责任，多签通常需要有多个私钥（N），只有当其中的 M 个私钥参与的签名，才可以动用资产，因此正确使用（不把私钥放在一起，由不同的人保管），确实可以提高安全性，因为即使部分私钥被盗或丢失，资产依然是安全的。

多签可以理解为一个有多把钥匙的保险柜，使用多签签名时，还应该避免私钥复用，私钥复用会增加私钥泄漏的风险。多签签名通常使用链上合约（或脚本）实现，这也给多签带来一个缺点：需要支付更高的交易费用以及多人异步签名导致的更长的交易确认时间。

②密钥共享（Secret Sharing）

与多签不同，密钥共享模式 (Shamir's Secret Sharing：SSS) 可以理解为一个把钥匙分层多个部分。通过将密钥分成多个部分并以冗余方式分开保管，发起交易则将一定数

量的密钥重新组装为密钥进行签名，这个方案也可以解决密钥被盗的风险，同时解决了上述多签费用高的缺点。不过 SSS 有一个主要缺点：当密钥被重新组装时，会为攻击者提供了获取密钥的可乘之机。

③门限签名(Threshold signatures：TSS)方案

门限签名方案（简称：TSS）结合 SSS 和多签的优点，它基于多方安全计算 (MPC: Multi-Party Computation) 使用多个分片的密钥轮流进行（交易）签名，生成最终有效的签名。

Binance 门限签名方案（TSS）

- TSS 作为一种分布式密钥生成和签名的加密协议，通过分布式的密钥管理方式让私钥不再成为钱包和资产托管的最脆弱的一环。允许构造一个在不同参与方（例如三个用户）之间分发的签名每个人都只持有部分私钥碎片，为了进行交易签名，需要将至少两个用户的签名数据整合在一起才能构建有效签名。

- 对于个人而言，门限签名机制可以帮助使用持有的多个设备共同管理私钥，从而使单个受损设备不会对资产造成风险。对于业务运营商，门限签名机制可实现更好的访问控制策略，以防止内部或外部人员窃取公司资金。TSS 技术使我们可以用分布式计算替换所有签名命令，从而让私钥不再成为一个单点风险。

门限签名方案跟前面多签和 SSS 方案不同的是：

- 多签通常是需要 M/N 个签名，而门限签名（目前）需要多方都参与签名。

- 多签通常是链上进行的，费用较高，并且不同的链多签的实现方案差别很大。而门限签名是链下的纯密码学的计算生成签名，兼容性更强。

- 多签是可以异步进行签名，而门限签名要求所有参与方在操作过程中都同时在线。

- TSS 和 SSS 不一样在于，SSS 虽然分片密钥，但是最终要重构出密钥来签名，那么就存在单点故障和重构出的密钥被泄露的可能。而门限签名（TSS）不需要重构出密钥。

©2020 云安全联盟大中华区-版权所有

基于门限签名技术的无私钥钱包解决方案——ZenGo

2019 年 9 月，以色列加密货币钱包 ZenGo 发布了 2.0 版本，旨在借助突破性的加密技术，打造了第一款无私钥安全加密钱包，将安全性分布在自主可控设备与钱包服务器之间，无需担心私钥，即使被黑或者丢失了钱包，资产也始终安全，通过完全自主的控制钱包来获得最大的安全性体验。

ZenGo 基于门限签名技术方案采用将单个私钥拆分为多个私钥碎片(目前是两个部分)由约定多个参与方各自保管的模式。这里我们将其中一个密钥保存在用户自主可控的设备上，另一个存储在钱包服务器上，在进行交易的时候，手机和钱包服务器通信共同完成签名。这套机制和中心化的钱包完全不一样，只有用户本人才可以发起转账，钱包是无法使用用户资金的。如果需要发起转账，用户需要主动发起，然后服务端和客户端将会使用这两个密钥份额进行通讯并签署转账请求，但不会将这两个密钥本身暴露给对方。

备份钱包也是相当简单的。一份加密过的客户端持有的密钥会储存在钱包服务器中，而解密的方法是单独存储在用户个人账户中，只有用户本人的面部 3D 扫描图才可以用来进行解密。所以如果用户不小心删除了钱包软件，或者不小心遗失了手机，都可以在几秒钟之内恢复钱包，因为只需要扫描面部就可以取回备份数据。

钱包不仅使用了无密钥机制，还使用了「无密码授权」机制。使用期间不需要记住任何的密码，因为他们采用了一些方法才到达了这种既方便又安全的方案：

1. 通过魔法链接授权，也就是依赖邮箱的安全性。当用户通过邮件注册的时候，将会发送一个魔法链接给用户，点击后即可完成授权。

2. 基于设备的授权，也就是依赖设备本身的安全性。当用户使用 App 签署签名时，需要使用面容 ID 或触控 ID 进行授权。

3. 基于面部 3D 扫描图的授权，也就是依赖钱包提供的解决方案。当用户需要跨设备恢复账户时，就需要使用面部 3D 扫描图进行授权。

除此之外，钱包还提供了方案应对服务关停的风险：钱包构建了第三方独立的托管服务 Escrow 和 监听服务 Trustee。Escrow 可以理解为是钱包服务器的一个备份，而

Trustee 则会监听钱包服务的状态，当 Trustee 发现钱包服务关停时，它会请求 Escrow 把对应的服务器端的恢复密钥转移到 Tustee 指定的 GitHub 账号（https://github.com/ZenGo-Trustee）。钱包（客户端）会在每次启动时，判断 GitHub 提供的恢复模式，如果是恢复模式就自动进入恢复模式，从而还原客户端的私钥，这个私钥可以直接进行交易签名进行资产转移，也可以把这个私钥导入到其他的钱包。总体来说，这种数字钱包安全设计方法照顾到用户失去私钥和 ZenGo 作为企业倒闭后，钱包的系统能够继续运行，用户的私钥可以恢复。因此是一个非常好的设计。但是，也需要注意 Escrow 和 Trustee 合谋的风险，和黑客攻击 Trustee 指定的 GitHub 账号引起不必要的恢复模式和由此可能造成的合成秘钥被盗的风险。

除此之外 Imtoken 也是这类安全实践的典型，Imtoken 充分利用设备安全沙箱机制，将加密后的 Keystore 文件存储在手机设备的安全沙箱内，防止其他程序恶意读取及由此造成的用户资产损失。并通过标准的 Keystore 文件方式进行加密存储，助记词通过业界标准方案 Keystore 方式加密保存在手机内部，并设置加密次数为 10240 有效防止暴力破解的可能。

其升级后的硬件钱包 Imkey 在此基础上加入了更加成熟可靠的安全机制。

1）安全 PIN 码保护机制

安全 PIN 码是打开硬件钱包的密码，硬件钱包所有行为操作均需 PIN 码验证通过后方可执行。在 5 分钟内 ImKey 硬件钱包无按键行为操作则自动锁屏，需要重新输入正确的 PIN 码才能继续使用。为防止钱包遗失后 PIN 码被暴力破解，系统内置安全保护机制，当 PIN 码输入错误次数达到 5 次以后，钱包将会被自动销毁，私钥数据从硬件钱包完全清除，只能通过重新导入助记词方式恢复。

2）真伪验证机制

ImKey 硬件钱包在初次使用时，会进行一次服务端安全认证。托管在云服务商机房内的专用设备加密机会对 ImKey 进行真伪认证，只有 ImKey 官方渠道发售的 ImKey 硬件钱包才能通过验证。从根源上避免因为伪造和仿冒的假钱包给用户造成资产损失。

3）应用验签机制

钱包内的应用程序可以负责进行数据签名功能，为防止恶意应用被安装，应用程序签名只能由核心负责人通过私钥形式签名发布，由 ImKey 硬件进行验证，而验证公钥在出厂时已预置在硬件钱包内部不可更改替换，只有合法授权的应用程序才能被安装到 ImKey 硬件钱包。

4）绑定码安全机制

初次连接 ImKey 硬件钱包时，ImToken App 会与 ImKey 硬件钱包进行绑定。通过绑定码校验，ImKey 硬件钱包与 ImToken App 交换了生成绑定码使用的公钥，当交易时会对数据进行签名验证。通过独创的绑定码机制，可以有效防止通过对蓝牙通信攻击造成的中间人攻击。

5）所见即所签

当进行交易时，ImKey 会解析 ImToken App 通过蓝牙传输的交易数据并在 ImKey 屏幕上显示和二次确认，其中会包含本次转账金额、地址、手续费，只有当你都确认没有问题后才会进行数据签名。做到真正的所见即所签，防止黑客通过应用程序漏洞或者蓝牙通信挟持导致转账数据被篡改。

4.2 企业级数字资产钱包需求分析

数字资产钱包本身的使用门槛较高，不仅需要对加密货币本身有所了解而且还需要一定的区块链技术和数字资产的认知及操作能力；对于企业职员特别是传统财务管理人员，要从原本的中心化交易平台转换至区块链思维具有一定的难度。对于企业或机构来说，资产属于组织，不属于个人，然而目前市面上的数字资产钱包大多面向个人用户，这对于企业处理实际财税业务来说，增加了很大的管理和操作使用难度。

根据调研分析，企业级用户在数字资产管理领域目前主要的需求点包括：

1）密钥的安全生成、存储、使用与分发；

2）各种数字资产管理业务流程的信息安全管控；

3）数字资产管理商业模式涉及的信息安全支撑；

©2020 云安全联盟大中华区-版权所有

4）具体的多地址的统筹、分类、权限区别管理等。

采用 MPC 和芯片隔离技术的钱包解决方案——Fireblocks

MPC（多方安全计算）解决一组互不信任的参与方之间在保护隐私信息以及没有可信第三方的前提下协同计算问题。应用于区块链也就是将私钥拆分多个碎片由约定多个参与方各自保管，私钥碎片通过 MPC 协议生成全新私钥签名，只有完整签名结果才能上链交易。

SGX（软件保护扩展）是新一代 Intel CPU 的加密部分，提供深层次的隔离安全保护，SGX 技术不仅能增强软件的安全性，其更大的意义是和区块链技术结合后即能解决区块链数据隐私的保护和对复杂应用的支持，又不影响区块链的去中心化的特质和数据不可篡改的特性。在保留了区块链的优点的同时又改善了区块链技术的不足。

Fireblocks 突破了最新的加密与芯片隔离技术，保障用户的数字资产安全的持有与转移。Fireblocks 平台主要包括三个部分：安全热金库、安全传输环境、流程授权引擎。

安全热金库

Fireblocks 非托管的热金库使黑客无法通过单点破坏私钥，无论是通过物理破坏还是内部人员入侵。热金库采用芯片级隔离和安全的多方计算（MPC），可提供多层深度防御。它无需繁琐的部署即可实现硬件级安全性。利用 MPC 的特性将热金库的将私钥拆分碎片隔离分布在 Fireblocks 的云服务器（SGX）和客户自有的安全移动容器。不存在唯一私钥，也不能在一个地方重构，消除了单点被破坏的可能性。由于采用了这种分布式密钥管理方案，从热金库中进行资金转移需要 Fireblocks 服务器和客户持有的移动设备共同参与。但是只能在安全传输环境中对经过身份验证的地址交易进行签名，这样的安全体系结构可保障存储在热金库中的资产免于遭受黑客、内鬼或者第三方的安全威胁。

©2020 云安全联盟大中华区-版权所有

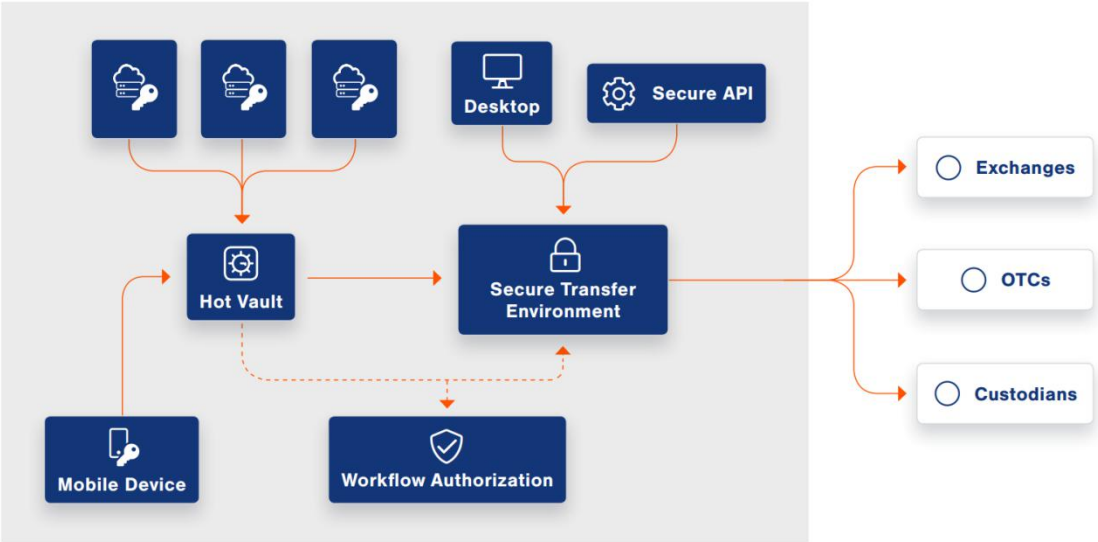

图 4-1

Fireblocks 的安全传输环境允许对目标地址进行动态身份验证，这意味着客户的资产转移将始终到达正确的目的地，而无需白名单管理以及繁琐且容易出错的安全流程。使用芯片组隔离的 SSL 加密通讯对地址进行保护和身份验证，利用 API 密钥的安全存储。这样可以防止基于网络和主机的中间人攻击和欺骗攻击，并确保不会从帐户网络中提取数字资产。

Fireblocks 工作流授权模型定义了广泛的规则集进行权限管理，自定义的规则和策略防火墙保障任何恶意或欺诈性交易将立即被阻止。这些规则是双向且基于帐户的，而不仅仅是基于地址的，因此即使钱包地址，流动性提供商或交易对手地址发生变化，规则集仍将适用。

Fireblocks 安全的存储和传输平台围绕高度敏捷且安全的基础架构构建，是稳健的数字资产保护方案，借助有效的工作流程授权，可以确保资金免受任何不必要的内外部的威胁与干扰。

企业级数字资产托管钱包解决方案实践——Cactus Custody

产品背景介绍：

2020 年 2 月底，Matrixport 发布旗下机构托管品牌 Cactus Custody 2.0。致力于为数字资产时代提供安全、透明、高效的机构级第三方数字资产托管服务。专注于构建业界

领先的系统安全设计和基础设施，以及提供适应于多样化业务场景的强大企业级财务管理功能。当前已不间断地为 10 亿美金级别的数字资产保驾护航，同时它也满足在监管和反洗钱法例的框架下提供服务。

在企业安全储存及归集大额数字资产方面，保证每个用户资金安全和公司内部财务统计上的准确性，提供更多便利企业内部财务统计的功能，极大减少了人工成本和账目出错率。Cactus Custody 降低了数字资产储存中面临的安全风险，并极大简化了数字货币资产的归集、清算流程工作。

在用户的实践反馈中，我们可以看出 Cactus Custody 像是数字货币的企业网银，使用其提供的多币种支持互转、业务线隔离、层级审批设定等功能，摆脱了过去公司资产难以实时统计，财务作业不透明，操作繁杂等弊端，做到了公司数字化资产统一、集中进行管理，让公司财务管理更加安全，透明，及时和交易可追溯。

产品功能特点：

1) 企业财务全貌展示

财务仪表盘功能，让用户时刻掌握企业的资产，业务和人员的最新状况。Cactus Custody 为客户接入实时资产价格数据，实时反应资产市值，并可以按业务线，资产类别进行筛选展示，让财务和人员分工状况一目了然。企业信息尽在管理者掌握。

2) 审批矩阵 – 灵活定制审批流程

企业内协作顺畅，业务才能高效开展，对于跨地区和业务多样化的企业尤其如此。全新的审批矩阵可以完美支持细分业务线，各种汇报审批层级，不仅支持门限审批 (m/n)，同时支持按金额设定审批门槛，更灵活，有控制，更安全。

3) 实时动态提醒 – 随时随地保持同步

从登入到设备授权，从入账通知到订单审批，所有关键指令都会触发邮件或短信提醒，无论何时何地，不会错过任何重要信息和决策，也为账户安全多走一步。

4) 风控管理 – 多管齐下，力保安全

从客户角度出发，提供全方位的风控工具：

- 账户一键冻结/解冻-- – 公司管理员应对突发事件时的秒级响应安全阀；
- 白名单保护 – 安心打币，不怕出错；
- 提币限制 – 设定不同用户的提币速率，精细控制风险范围。

5) 下载中心 – 日志流水报表一应俱全

在下载中心页面中，客户可以下载各类交易流水，日志和模板，更可按业务线，日期和资产定制生成报表，方便内外部对账和审计，节省员工大量时间并且降低出错概率。

6) 双模式钱包 – 灵活提币

提供专户型账户，用户的资产会储存在独立的区块链地址上，仅有账户所有人可以控制，地址余额链上可查，并且支持“冷”，“热”两种常见存储方式。在客户创建资产钱包时，对 UTXO 模型的资产提供了两种类型的钱包供客户选择：地址混合型钱包和地址隔离型钱包。

*混合型钱包：减轻客户操作负担，取币无需精确到地址，选定钱包即可打币。系统会通过计算最低交易费并自动为客户选择指定钱包内的出金地址组合；

*隔离型钱包：客户可以精确到地址提币。两类钱包都支持批量打币，减轻财务人员的操作负担。

产品安全能力优势：

1) 业界最高级别的加密机 HSM- FIPS 140-2 level 3，并都是高可用，随时都有另外一台 HSM 备份。私钥明文不会离开加密机，因此员工也不会接触到客户私钥明文，出来的都是加密后的密文。

2) Cactus Custody 用 Tier 4（全球最高级别的）数据中心作为热存储和冷存储的 vault，这些数据中心都是有严格的准入控制，CCTV 监控，防洪水和地震还有防电磁攻击，也都有专业的安保人员 24/7 坚守的。数据中心分布于三大洲，新加坡，瑞士和美国，冷存储大额取币需要其中两个数据中心签名（2/3 多签）。

3) 除了冷存储之外，还会有终极异地灾备（m/n shamir sharding，并把 8 片加密私

钥片段分别异地存储在 8 个银行的保险柜里，需要时 3/8 恢复）。

4) 分权分域的系统设计，客户在登陆后可以配置基于角色的授权。

5) 客户管理员一键冻结账户和一键解冻功能，极端情况下保护账户资产。

6) 客户的资金全部是地址隔离存储的，随时客户都可以上链查看地址上的余额是不是足额，所以不存在钱包平台挪用的可能，客户和客户间的资产地址隔离，也就是 A 客户的地址是给 A 客户专用的，不会再给 B 客户。

5. 数字钱包安全测试标准

图 5-1

1. 功能设计安全性测试

①导入钱包功能安全

测试方法：模拟黑客攻击，测试安全隐患。

判定标准：使用导入钱包的功能，之前用户存储在系统中的私钥有高强度加密密钥的支持下才可恢复，保证恢复过程密钥不会被泄露，相关功能设计不严格，会导致在此过程被黑客攻击。

②交易密码安全

测试方法：模拟黑客攻击，测试安全隐患。

判定标准：交易密码应有检测弱口令，防止黑客对密码进行拆解，直接进行交易；密码若本地存储，存储应当进行严格加密（加密强度应该不低于 8 位），防止黑客对其进行逆向分析，获取交易密码。

③用户输入安全

测试方法：查看相关流程是否严格，验证此安全隐患是否存在。

判定标准：用户输入数据需进行严格的功能设计，防止黑客监听窃取或者被非法留存；如果采用第三方键盘进行，需要对用户输入逻辑做校验，防止黑客获取敏感信息。

④转账地址安全检测

测试方法：模拟黑客攻击，测试安全隐患

判定标准：在钱包输入转账地址或扫描二维码转账地址后，需安全检测转账地址是否已经被篡改，保证转账地址的完整性，防止黑客恶意篡改地址窃取数字资产。

⑤助记词/私钥网络储存安全

测试方法：逆向协议分析，检查安全隐患

判定标准：助记词和私钥应当禁止以任何形式通过网络传输回钱包厂商， 防止服务器被攻击用户数据与钱财被盗取，相关回传数据操作容易导致用户数据与资产被盗

©2020 云安全联盟大中华区-版权所有

取。

⑥Https 通信中的证书校验

测试方法：模拟黑客攻击，测试安全隐患

判定标准：数据网络交互通信中，如果使用 https，终端需要确保自身设定的根证书的可信性和合法性，终端必须对证书做严格的校验，确保证书的合法性。

2. 安全性能测试

①通信加密过程安全

测试方法：执行白盒测试和黑盒测试，同时执行网络监听，测试系统。

判定标准：应保证通信建立过程的密钥交换阶段的密钥安全，数据传输过程中数据被正确有效加密，确保数据的完整性和私密性。对非法伪造的通信数据能够被合法的通信双方检测发现。对泄漏的加密数据，应该能够避免在没有密钥的情况下被破解和被解密。

②接口调试安全

测试方法：查阅设计材料，测试系统，分析接口调用的过程和数据。

判定标准：包含调试接口并有预留信息全部清理，对接口的防护启动了相关防护措施。恶意用户无法获得 API 接口的明文数据。

③中间人攻击

测试方法：查阅材料，测试系统。

判定标准：在双方进行交易的过程中，要对交易进行监听，保证传输过程中交易信息不被截取，保证在钱包交易，广播等主要的功能过程中不存在中间人攻击和通过中间人攻击获取关键信息的行为。

④升级更新安全

测试方法：查阅材料，测试系统，分析升级后代码运行情况。

©2020 云安全联盟大中华区-版权所有

判定标准：应具备在不影响系统业务处理的情况下对版本进行安全更新的能力，具有版本升级失败的应急方案，以保证钱包在升级失败时能够在规定时间内恢复可用性。升级更新过程需要对升级包的完整性和合法性进行验证。升级包应该包含有数字签名等校验信息。

⑤权限控制安全

测试方法：查阅材料，测试系统。

判定标准：应对敏感信息、重要数据和设备的访问权限、使用权限进行要求和限制。定期检查相关接口是否存在非授权调用、对相关接口的调用是否进行权限检查、对非授权调用是否进行限制、是否成功阻止非授权的访问和使用敏感信息、重要数据和设备。

⑥服务应用安全

测试方法：查阅材料，测试系统。

判定标准：数字钱包服务端应用上线前，先进行安全加固，运行时保持低权限运行，同时定期监控，黑白盒扫描漏洞。

3. 热钱包安全测试

◆运行环境安全检测

①手机系统安全

测试方法：扫描相关严重漏洞，判断当前手机系统安全性。

判定标准：钱包应当对手机当前系统版本进行检测并作出相关举措，严重系统漏洞将导致 App 容易被黑客控制权限。

②Root 环境检测

测试方法：扫描 root 常见手段，来判定设备是否已被 root。

判定标准：钱包应当对手机环境进行 root 检测，防止 App 运行在已 root 手机上，使得相关执行过程被黑客调试分析。

©2020 云安全联盟大中华区-版权所有

③APP 完整性检测

测试方法：模拟黑客攻击对 app 进行修改或者插入恶意代码，来确认是否安全。

判定标准：钱包 App 应当做完整性检测，应该可以发现 app 被修改了或者被插入了恶意代码。

④网络安全检测

测试方法：模拟黑客攻击，来确认是否安全。

判定标准：App 在运行中应当检测是否使用相关代理，防止网络数据被监听，同时验证当前使用网络的 DNS 的安全性，不存在被劫持的可能。

◆协议交互安全检测

①新用户注册安全

测试方法：测试系统新用户注册流程，查看是否存在相关安全隐患。

判定标准：在安装完应用后，新用户需要完成注册，才能使用钱包 APP。注册过程中，不能将用户敏感信息以不安全不可靠的方式上传至钱包服务器。

②创建交易安全

测试方法：测试系统创建交易的流程，查看是否存在相关安全隐患。

判定标准：在用户创建交易时，需要对交易双方的账号需要二次验证，防止收款账户信息被恶意替换后无法知道，导致用户钱财损失问题。

③交易签名安全

测试方法：交易过程逻辑代码进行逆向分析，查看是否存在相关安全隐患。

判定标准： 在交易创建后，发送正式签名交易的过程，相关协议需严格设计，需校验交易的签名信息。

④交易完毕确认

©2020 云安全联盟大中华区-版权所有

测试方法：流程查询分析，查看是否存在相关安全隐患。

判定标准：交易完毕后，需对交易内容进行确认，使用户清晰了解此次交易过程的记录，并在 App 上可查询相关信息，以及个人交易记录。

⑤余额查询安全

测试方法：账户余额查询分析，查看是否存在相关安全隐患。

判定标准：在进行余额查询时，无论是从货币官方服务器，还是钱包厂商服务器进行的查询，都应严格对其返回给客户端的数据进行完整性验证。，对于发生信息篡改的情况需要做出紧急措施，防止用户 APP 数据接收虚假、异常信息。

◆数据存储安全检测

①助记词创建安全

测试方法：对助词创建过程进行分析，查看是否存在相关安全隐患。

判定标准：新用户使用钱包 APP 时，会生成助记词要求用户记录，此过程禁用设备的检测截屏，录屏等功能，保证只有创建用户能知道助词信息。

②助记词存储安全

测试方法：在助词存储过程中，模拟黑客攻击，检测相关流程是否存在安全隐患。

判定标准：助记词生成后，不能以明文存储，必须进行加密存储，并且需要高安全性加密算法防止黑客逆向分析恢复明文。

③私钥生成安全

测试方法：在私钥生成过程中，模拟黑客攻击，检测相关流程是否存在安全隐患。

判定标准：钱包在新用户私钥生成过程，应用高安全性的算法产生用户私钥，保证相关算法不可被逆向分析，密钥生成算法理应进行保密处理，防止黑客模拟生成算法生成私钥。

④私钥存储安全

测试方法：在私钥存储安全过程中，对其进行逆向分析，查看本地是否存在敏感信息。

判定标准：私钥生成后，如果会在本地保存，不应使用明文存储，将会导致黑客进行攻击获取用户私钥信息，需要高安全性加密算法进行存储，即使在黑客得到密文信息后，也可以防止黑客逆向分析恢复数据明文。在向官方服务器，还是钱包厂商服务器发送私钥时，也应该在密文状态下进行传输，在传输的过程中防止监听并且保证数据的完整性。

4. 冷钱包安全测试

◆设备系统安全机制

①硬件钱包联网安全

测试方法：测试系统在离线状态下的使用流程中，是否存在相关安全隐患。

判定标准：设备在使用过程中，不能有联网操作，需要全程隔绝物理。在离线状态下所作出的数据更改必须进行记录，该记录在联网状态下应上传到相关服务器，更新过程中的数据可靠性强，更新状态按时间先后顺序存储，更新数据不可逆转。

②设备加密安全性

测试方法：查阅材料，对芯片各项功能进行测试。

判定标准：使用加密芯片对设备进行防护，芯片加密等级达 ELA4+及以上，设备的内部数据不可以读取并解密。

③硬件钱包系统安全

测试方法：查阅材料，测试系统。

判定标准：通过其他外部设备及外部工具无法拿到系统高级权限，禁止外部设备通过任何形式进入系统内部读取系统的重要信息及日志资料。设备若保留蓝牙，wifi，nfc 相关协议模块，要保证这些模块无法访问到钱包系统所产生的所有数据。

④硬件钱包系统漏洞更新机制

©2020 云安全联盟大中华区-版权所有

测试方法：查阅材料，测试系统。

判定标准：如果设备存在漏洞，更新机制是如何进行，要保证在安全的前提下对系统进行升级，升级完毕后必须校验系统完整性，要时刻监控系统情况，防止黑客恶意入侵对系统进行非法更新操作。

⑤设备丢失锁定方案

测试方法：查阅设备定位相关材料，对设备定位进行测试。

判定标准：利用有效的手段，例如 GPS 对钱包设备进行定位操作，在设备丢失的情况下能够快速找回；如果不能及时找回设备，应存在紧急措施去锁定设备，禁用设备关于钱包系统的一切功能。

◆设备访问权限控制

①设备连接调试安全

测试方法：测试设备连接调试流程，查看是否存在相关安全隐患。

判定标准：对设备加入严格的权限控制，防止攻击者对设备进行连接调试，。在转账的过程中因为需要双方设备进行连接，因此要有一套完整的校验机制，验证双方设备是合法设备，并且在交易过程中能保证交易只在双方设备中进行。

②设备存储区读写权限安全

测试方法：测试系统对存储区数据的访问，查看是否存在相关安全隐患。

判定标准：对于设备存储区，需要做严格加密，严格控制存储区的权限，保证存储区数据只能通过钱包系统进行有效访问，其他访问方式均为无效访问，防止黑客进行拆机对存储区做分析提取数据。

③设备内存安全

测试方法：测试系统使用流程，查看是否存在相关安全隐患。

判定标准：对设备被调试需做检测，防止内存数据泄露，防止黑客进行数据采集和逆向分析。

◆业务功能实现机制

①设备使用密码设置

测试方法：测试系统密码设置功能，查看是否存在相关安全隐患。

判定标准：需提醒用户设置解锁密码，解锁手势或指纹解锁，错误密码解锁时间周期，保证交易密码强度为高强度密码，在设备丢失后无法被人直接进入查看个人隐私信息，进行交易。

②创建钱包助记词安全

测试方法：测试钱包助记词流程，查看是否存在相关安全隐患。

判定标准：新用户使用钱包时创建助记词，利用高安全性加密算法进行加密处理，对此数据进行密文存储，防止相关数据被逆向调试分析泄露，对用户钱财造成损失。

③交易过程安全

测试方法：测试交易流程，查看是否存在相关安全隐患。

判定标准：对于收账地址需不完全显示，有效的检验交易双方地址是否为正确地址，防止用户转账转错，钱财受到损失。

④数据存储安全

测试方法：测试私钥管理流程和存储介质。

判定标准：私钥储存应该密文存储在设备中，黑客不能对此密文进行逆向还原，并且保证数据不能保存在设备存储卡上，被外部获取，否则容易被黑客攻击。

⑤系统完整性安全

测试方法：检查有没有建立完整性校验流程，具体怎么实现，记录可能的影响完整性的问题。

判定标准：设备系统需要有严格的完整性校验，用于自检设备是否被人刷机，须有正品保障，否则容易在设备出厂经销地方被黑客或攻击者进行篡改。

5. 合规安全测试

©2020 云安全联盟大中华区-版权所有

①政策合规

测试方法：合规必须本地化，检查系统是否在所在国家符合对应的金融法，银行有关的法律，和信息安全法等等法律。

判定标准：强化资产监控，具备合理有效的系统安全管理机制，满足国家政策法规对数字资产安全治理的要求，应对身份、账户、凭证的访问和更改提供安全审计功能，保障监管合规的要求。

②隐私安全

测试方法：测试系统在数据加密，隐私保护方面的技术代码和商业流程。

判定标准：应保障信息采集、传输、存储、使用的隐私安全。应有用户自主选择同意或拒绝的操作步骤；信息传输时采用全量加密策略，加密密钥和证书安全传输；对高敏感级别个人信息使用不可逆密码算法加密存储；用户信息展示的安全策略，非本人展示应先获得信息所有者的授权等。

③反洗钱策略

测试方法：测试反洗钱 (AML) 规则。

判定标准：引入反洗钱 (AML) 规则，具备高效检测非法交易及地址的安全策略，有效帮助用户验证数字资产来源，抵御欺诈，保障数字资产安全。确保交易操作历史不可更改并且可以被查询，做到可审计、可追溯。

④口令安全

测试方法：测试系统口令管理流程和具体实现方法。

判定标准：审计数字钱包所用服务口令强度，建议设置为强密码，SSH 类使用证书登陆，最好前置堡垒机。

⑤系统安全

测试方法：对于数字钱包服务端系统的安全进行测试。

判定标准：数字钱包服务端系统，高危漏洞应当及时更新，系统和内核等加固配置，

©2020 云安全联盟大中华区-版权所有

减轻未知的漏洞，预防被攻击后的提权和横向渗透等操作。

⑥访问控制

测试方法：对于钱包的访问控制策略和技术实现进行测试。

判定标准：数字钱包服务端在云上时，严格限制出入站端口和 IP 的开放，避免高危和敏感服务暴露。服务端系统，使用 Iptables 等保护系统相互隔离，控制资源仅可信域连接。

⑦日志审计

测试方法：检查关键数据访问与使用的日志，和日志保护方法。

判定标准：应具有针对关键数据访问与使用的审计记录，并对审计记录进行相应的保护。搜集和保存数字钱包服务端各种日志，用于服务状态监控，故障排查，被渗透后的溯源追踪等，日志保存时间至少 6 个月以上。

⑧冗余安全

测试方法：测试系统有没有冗余配置，如何实现？

判定标准：对数字钱包核心系统进行冗余配置，保证服务的高可用。应具备密钥等关键数据的备份与恢复机制。定期进行系统快照，核心数据备份等。

⑨代码安全

测试方法：代码的安全有没有第三方测试，测试流程是什么。

判定标准：数字钱包代码和服务端代码,上线前进行进行第三方安全审核，检查通过后，允许上线。每次改动代码后，也要进行安全复查，同时定期进行黑灰盒扫描测试，并且需要同时支持静态和动态的代码测试。另外对代码进行严格控制，防止上传到第三方代码托管平台。

⑩智能合约钱包测试

测试方法：对于利用智能合约实现数字钱包的两个重要安全机制进行测试。另外可以利用智能合约安全测试工具，第三方审计，和形式化验证等等。关于智能合约的安全

©2020 云安全联盟大中华区-版权所有

可以参考机械工业出版社的《区块链安全技术指南》这本书，也可以参考 CSA 大中华区的智能合约安全工作小组出版的白皮书。下面主要从钱包的角度提出测试标准。

判定标准：

1）对于智能合约的管理账户：大部分基于智能合约的数字钱包是支持 ERC20 的数字钱包，钱包开发者利用 ERC20 的 approve API，在钱包拥有者的同意下，可以动用钱包的资金进行交易，转账，借贷等等服务。智能合约本身是由外部帐户（EOA）进行部署和管理（比如智能合约的升级，智能合约的重要参数的修改等等）。我们可以称呼这个外部帐户为管理账户。管理账户如果由一个人拥有或者钱包开发团队拥有，就有风险。比如管理账户可能设计“逃离策略”（Exit Scheme）在可以动用资金充分多的情况下修改智能合约或者重要参数盗取用户们资金。钱包开发团队必须公开管理账户的访问控制权利，是否多签名，多签名的具体参与者（防止一个人拥有多签名地址的私钥），智能合约升级或者重要参数修改需要增加时间锁，一般时间锁设定在 24 个小时以上，容许社区审核修改内容，可以对于修改内容进行否决）。

2）抢先交易（Front Running）：在智能合约钱包用去中心化交易过程（DEX）中，如果交易是公开发布，矿工或者黑客可能利用抢先交易，或者改变交易进行不正当的价格获利。一个简单的方法是把交易分成两步骤，在第一步是存储交易数据的 keccak256 哈希，然后显示数据并在第二个步中针对哈希进行验证。这样交易在 DEX 发送过程中保密避免抢先交易，数字钱包利用以太坊网路进行保密交易可以参考 https://libsubmarine.org/。另外一个方法是利用“状态锁”锁定交易或者其他重要数据。具体怎么实现参考 https://medium.com/coinmonks/solidity-transaction-ordering-attacks-1193a014884e。

参考文献

[1] 黄连金,吴思进,曹锋,等.区块链安全技术指南[Z].北京:机械工业出版社,2018 年.

[2] Lorenz Breidenbach, Tyler Kell, Stephane Gosselin, and Shayan Eskandari, Defeat Front-Running on Ethereum, https://libsubmarine.org/

[3] Chris Coverdale, Solidity: Transaction-Ordering Attacks, https://medium.com/coinmonks/solidity-transaction-ordering-attacks-1193a014884e

CSA GCR cloud security alliance GREATER CHINA REGION ®

关于云安全联盟大中华区

云安全联盟 CSA （Cloud Security Alliance）是全球中立权威的非营利产业组织，致力于国际云计算安全和下一代 IT 安全的全面发展，聚焦在网络安全领域的基础标准研究和产业最佳实践。云安全联盟大中华区是在香港注册的独立、中立、专业的第三方非营利组织，与 CSA 美洲区、亚太区、欧非区共享 CSA 品牌与研究成果。

企业会员主要包括：世界大部分科技公司与网络安全公司如 Amazon、Microsoft、Google、Facebook、IBM、Intel、Oracle、VMWare、华为、中兴、腾讯、阿里、百度、奇安信、360、OPPO、启明星辰、天融信、深信服、安恒信息、浪潮、海尔集团、龙湖集团、格尔软件、Ucloud、数字认证、工商银行等。

云安全联盟大中华区欢迎各个单位加入，与联盟一起携手共进，共建网络安全生态。

©2020 云安全联盟大中华区-版权所有

邮箱:info@c-csa.cn
官网:https://c-csa.cn