火币区块链产业专题报告
钱包篇

2018 年 7 月 31 日

摘要

狭义上数字资产钱包为私钥存储工具，广义上含余额查询、发送交易等基本功能。2018 年 Q1 全球数字资产钱包用户数约 2395 万，同比增长 86%，发展迅速。基于火币研究院调研的 31 个钱包项目：**钱包行业竞争激烈，目前无较好盈利模式**；约 70%的钱包支持移动客户端，对网页端支持度最弱，仅占 26%；61%的钱包为开源项目；65%的钱包提供行情、理财、资讯等附加功能，其中提供交易功能的钱包数最多，约占 75%。

钱包种类繁多，本报告对钱包从连网与否、数据存储、私钥存储、主链关系以及私钥签名这**五方面进行了分类阐述**，分析了其在安全性、易用性和功能性等策略上的不同。

为帮助读者深入理解数字资产钱包，本报告从技术原理出发，**详细阐述了钱包助记词、Keystore、私钥、公钥和地址产生的方法及其相互关系**。此外，对于钱包安全也从**用户安全教育和钱包安全设计**两方面进行了深度剖析。

目前钱包产业存在使用门槛高、盈利模式不清晰、功能较为单一等问题，安全事件也时有发生。但未来，**钱包作为区块链世界入口的功能将不断发展完善，金融属性也将日趋强化**，有望成为多种资产一体化管理入口、DAPP 应用入口、通证使用权、收益权等功能性入口，交易和理财服务也将不断加强完善。

相关报告

1.《火币区块链产业专题报告：游戏篇 “新的财富金矿？游戏产业的割裂与重构”》2018 年 8 月 1 日
2.《全球区块链数字资产行业专题报告-公链平台篇》2018 年 6 月

作者

袁煜明
李 慧
刘 洋
类成叁
胡智威

火币区块链应用研究院

huobiresearch@huobi.com

目录

第一章 数字资产钱包产业现状

1.1 钱包产业概述

自中本聪在2008年发表《比特币白皮书：一种点对点的电子现金系统》以来，加密数字资产市场从无到有，不断扩大，根据coinmarketcap统计，在2018年7月20日，全球加密数字资产总市值已达2868.20亿美元。(Jul 20, 2018 2:50 AM UTC,COINMARKETCAP)在2017年12月17日，比特币价格达到历史最高峰19737.40美元后，数字资产热潮随之达到顶峰。正是在数字资产大幅兴起的背景下，驱动了对数字资产的安全存储需求，因而数字钱包行业迎来了一个发展契机，大量开发者以及资金开始涌入。根据Statista统计，2018年Q1全球数字资产钱包用户数为2395万人，同比增85.80%，环比增长11.34%，增长十分迅猛。

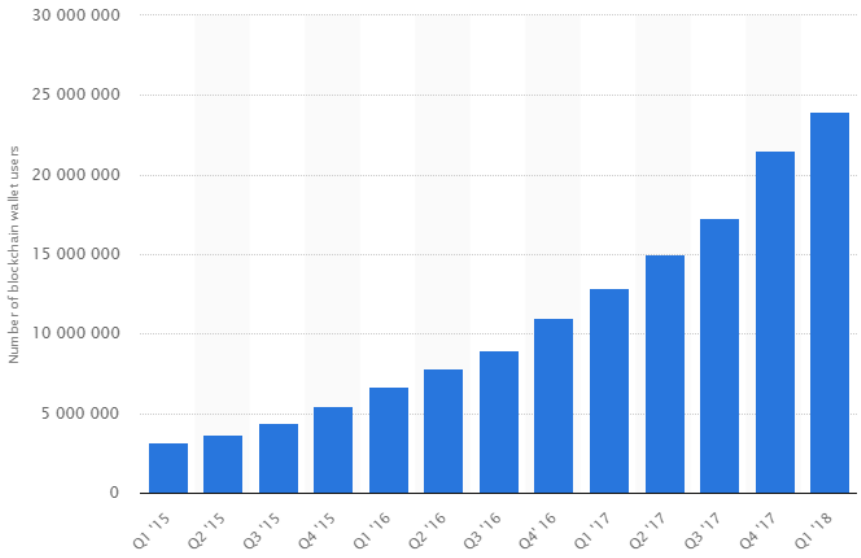

图 1.1 数字资产钱包用户数[1]

[1] 数据来源于Statista.com

数字资产钱包最狭义的定义是储存私钥工具，广义上则应该包含数字资产余额查询，发送交易等基本功能（广义上也能把交易所理解成一种钱包，但本文不将其列为讨论范围）。从不同的角度出发，对数字资产钱包的定义和分类都不相同，比如从钱包是否连网来看，可以分为冷钱包和热钱包，从数据存储完整性来看又可分为全节点钱包和轻节点钱包等。从未来发展来看，钱包不仅将作为区块链世界的入口，还会承担数字资产理财管理，交易兑换等扩展性金融功能，其重要性值得数字资产相关从业者关注。

1.2 钱包产业市场分析

钱包作为区块链产业必不可少的一环，随着区块链产业的发展和扩张也呈现并行加速的现象，越来越多的项目方加入数字资产钱包领域。相较于全球 60 亿人口和 40 亿互联网用户来说，数字资产钱包用户占比还非常小，未来市场潜力非常巨大，如下图所示。当然也意味着区块链目前还处于行业发展的初期，数字资产钱包作为行业配套基础设施也同样处于行业早期。

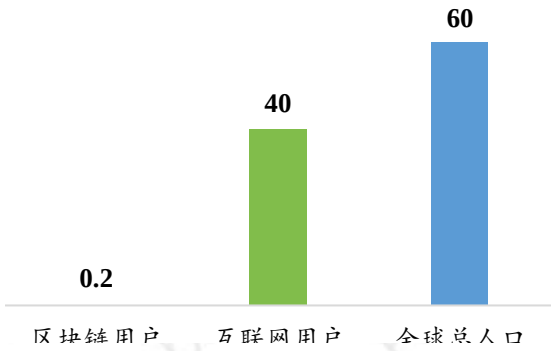

图 1.2：区块链用户数量（亿人）[2]

[2] 来源：火币研究院分析整理

火币研究院调研和分析了市场上 31 个数字资产钱包项目[3]，并对项目的成立时间、支持的平台种类、支持的主流数字资产种类、项目代码是否开源、用户数量分布以及融资额分布做了统计分析，本章所有数据统计均来源于此 31 个项目样本。

有数据可查的 28 个数字资产钱包项目中，其成立的时间分布如图 1.3 所示，该分布趋势与 BTC 价格趋势有一定的相关性，2014 年和 2017 年成立的项目数相对较多。

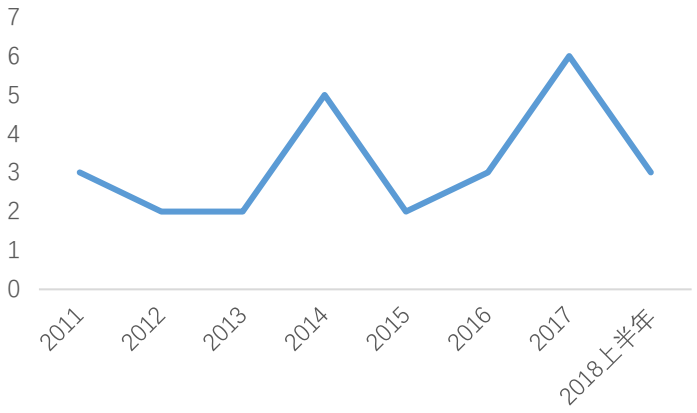

图 1.3 数字资产钱包项目成立时间分布

除个别冷钱包无客户端软件外，29 个数字资产钱包都同时支持多种平台，如图 1.4 所示，其中支持 Android 平台的项目最多，约占 74.19%，其次为 IOS，对网页支持的项目最少，只有 25.81%。总体来说对手机客户端的支持度是最好的，PC 客户端的支持度仅占不到 1/3，网页端的支持度最弱。

[3] 31 个项目列表可参考附录 2

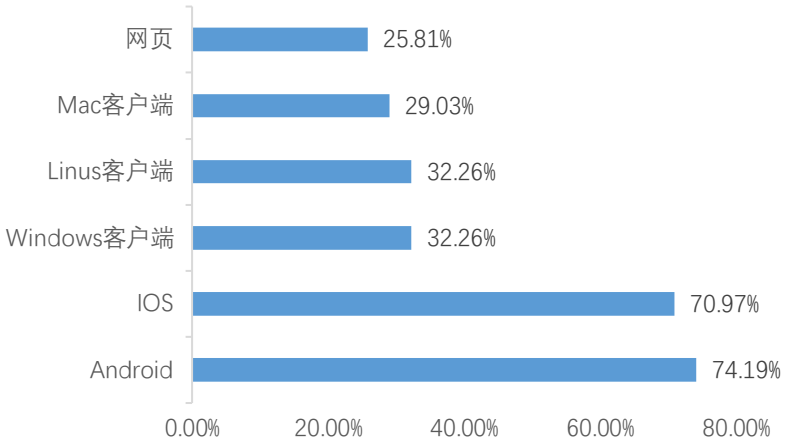

图 1.4 各钱包支持平台类型占比

火币研究院整理和分析了 31 个钱包对 11 种主流数字资产以及 ERC20 类代币的支持度，如图 1.5 所示，约 84%的数字资产钱包都支持 BTC，68%的钱包支持 ETH，对 ERC20 的支持度为 45%，对 Stellar 的支持度最弱，仅有 6%。

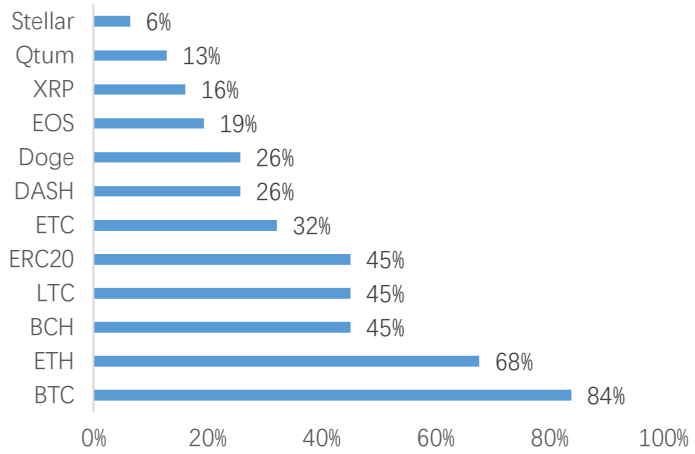

图 1.5 各钱包对各主流币种的支持度

数字资产钱包的安全性是最受关注的话题，特别是私钥的存储机制甚为关键，约 61.29%的项目选择项目开源，一方面接受各方对其代码进行监督审查，另一方面也更容易获得技术极客的帮助，不断地改进升级，如图 1.6 所示。

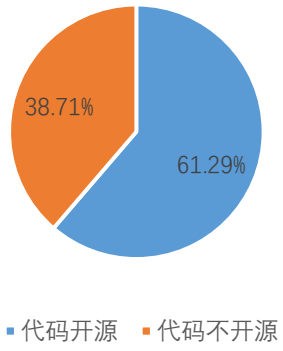

图 1.6 各钱包项目开源占比

对有数据支持的 11 个项目[4]用户数量进行分析后，发现各层级用户体量的项目数比例非常接近，如图 1.7 所示。用户数在 1~10 万的项目数略大于用户数在 10 万~100 万以及大于 100 万的项目数。

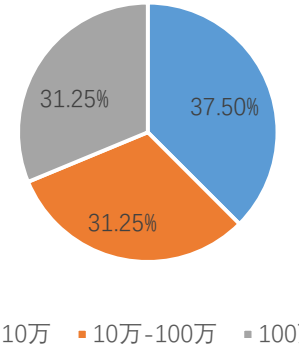

图 1.7 各钱包项目用户数量分布

火币研究院统计了公布融资额的 10 个项目，有 60%的项目融资额在 1 千万美元到 1 亿美元之间，还有 20%的项目融资额超过 1 亿美元，如图 1.8 所示。

[4] 数据来源于项目方主动披露或者网上公开信息披露

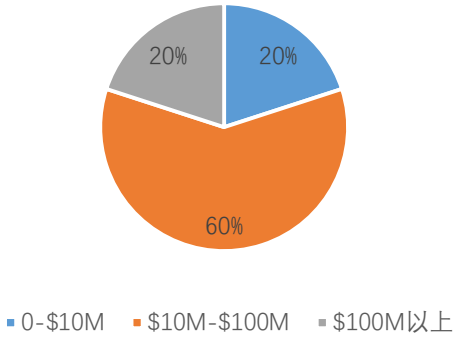

图 1.8 各钱包项目融资分布

1.3 钱包商业模式分析

钱包作为私钥管理工具，目前还没有很好的盈利变现模式，基本都处于早期积累用户和沉淀资金的状态。 为寻求收入来源，各钱包纷纷推出周边增值服务，一方面为增加用户黏性，提高流量入口，另一方面也试图增加收入来源。如提供理财、资讯、POS 挖矿、交易、资产聚合等功能。目前有 65%的数字资产钱包项目都提供附加功能，如图 1.9 所示。

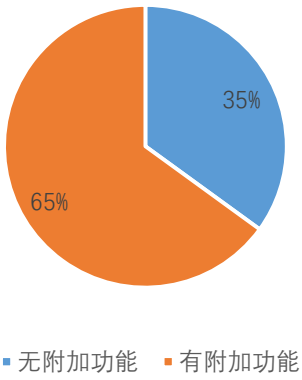

图 1.9 各钱包有无附加功能占比

经火币研究院统计分析，在提供附加功能的钱包项目中，提供数字资产交易或兑换服务的钱包数量最多，约占 75%；其次为行情服

务，约占 60%；提供资产聚合服务的钱包项目最少，仅占 5%，如图 1.10 所示。

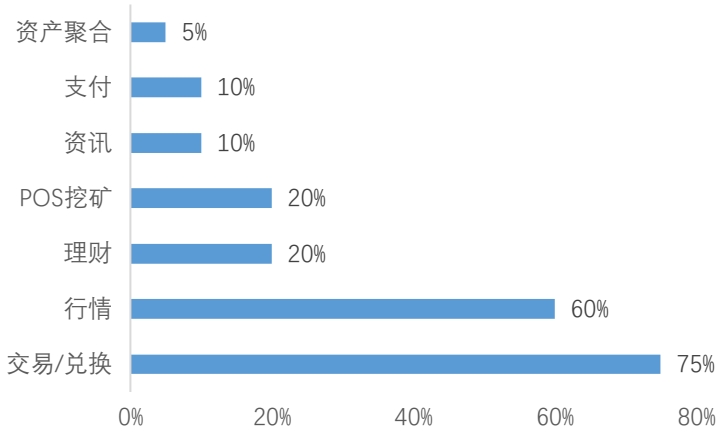

图 1.10 数字资产钱包附加功能分布

- **交易及兑换类服务**

钱包内置数字资产交易功能，有接入中心化交易所平台的钱包，如 BitPie；也有接入去中心化交易平台的钱包，如 Imtoken；还有接入 Bancor 机制的自动化交易平台如 Tokenpocket。有的钱包推出的“闪兑”功能，即不同币种之间按照一定的“汇率”进行互换，其后台通常也是用了去中心化交易所的模式进行货币的兑换。

钱包用户天然拥有交易需求，如果币不用提出钱包就可以实现交易，不但减少了用户提币转币的操作步骤，减少了犯错的概率，也增强了用户黏性，为钱包项目的后续转型提供了很好的发展方向和资金沉淀。不过内置交易所极大地增加了系统的复杂度，为本身对安全性要求较高的钱包类产品引入了更大的风险，用户资金安全性将受到一定程度挑战。

- **行情资讯服务**

钱包内置丰富的新闻资讯、行情快报、项目简介、K 线图、大额资金流动监控、代码活跃度等数字资产市场行情信息。

区块链项目的资讯和行情信息是通证持有者与市场保持同步的需求，也是集聚用户流量的大入口，钱包产品若能很好地集成资讯行情服务不仅能对现有用户产生足够的黏性，还可以带入更多的增量用户。不过资讯行情服务需要投入一定的人力财力，会较大地增加产品的运营成本。目前大部分钱包集成的新闻资讯服务并不是很完善，主要以提供行情信息为主。

- **理财服务**

钱包内置理财模块，理财类型包括长期固定收益型，余币宝短期灵活型，数字资产 P2P 融资借贷型，抵押贷款型。目前这些理财模块有的是接入第三方服务，本身不参与理财服务；有的是为本身平台的发展提供廉价资金而开发的理财产品，由平台收益来支付用户利息；有的则是将平台募集的数字资产再投入一级或二级市场交易以此来获取超额收益并支付用户利息；还有的则是提供 P2P 的数字资产借贷交易服务，为资产需求方和提供方提供撮合服务。

对于长期持币的用户来说，数字资产理财服务切中刚需，持有也能获得收益，目前各类钱包提供的理财产品年收益率在 4%~20%不等。不过区块链行业发展迅速，数字资产市场波动性较大，流动性不佳的理财产品将面临更大的风险。且目前数字资产理财市场并不成熟，还未出现行业标杆性龙头企业，风险控制经验和能力以及兑付能力还待市场考验。此外数字资产 P2P 借贷型，若是对借贷人风险难以把控，

则很容易造成违约，请投资人注意风险。

POS 挖矿服务

对于支持 POS 共识算法的区块链项目，一些钱包提供锁仓加入 POS 挖矿服务，挖矿收益将定期发送给用户。

通常由钱包项目方提供 POS 挖矿的主节点，符合一定资金要求的数字资产可参与 POS 挖矿，有固定锁定时间挖矿，也有支持随时可赎回的挖矿模式，钱包项目方将从挖矿收益中按比例抽取分成，钱包项目方和用户都能有较为稳定的额外收益。目前支持 POS 挖矿较多的币种有：达世币 DASH，闪电比特币 LightningBitcoin，小零币 ZCoin，量子链 Qtum 以及超级现金 Hcash。

资产聚合类服务

通常用户会在多个交易所和钱包里持有不同的币种，不太方便进行集中的管理和收益查询，此类钱包可为用户提供资金聚合服务，通过 API 接口将用户在多个钱包和交易所的通证持有情况进行汇总聚合，对于 API 接口服务支持度不佳的平台也可以采用手动维护进行初始输入。目前可支持交易所、钱包、ICO 资金和法币资金的信息汇总聚合服务。

目前各大交易所以及钱包平台种类较多，每个交易所以及钱包支持的数字资产品种都不一样，因此用户的资金通常会分散到不同的平台，不利于集中管理和查询，因此聚合类服务能较好地满足用户查询的需求，提升用户活跃度和用户黏性。这类钱包需要配合众多交易所、钱包等进行 API 接口开发，存在一定的开发和维护成本。

基于以上提供的各类增值服务，目前主流钱包项目方获得盈利的几种方式如表 1.1 所示。

表 1.1 数字资产钱包的盈利模式

类型	盈利模式	概述
热钱包	交易手续费	对于内置交易所的钱包，交易手续费将成为收入的主要来源，无论中心化或是去中心化交易方式，钱包项目方都可从中获得收益。
	资产管理费	钱包可提供资金托管或理财服务，并从中收取管理服务费。如 COBO 提供 POS 挖矿资产托管服务，并收取一定的资产管理费用。
	法币通道手续费	在允许法币直接购买数字资产的国家，服务商通常会收取一定的数字资产转换服务费。如 Coinbase 会根据国家/地区收取 1.5-4%的转换费。
	第三方服务费	对外提供 SDK 接口收取第三方服务手续费。如提供支付接口，并收取手续费。
	广告费	对于内置的广告或者 DAPP 收取一定的推广费用。
冷钱包	设备销售收入	与热钱包不同，冷钱包收入来源主要为硬件钱包销售收入。如库神钱包的主要收入来源为冷钱包设备销售收入。

第二章 数字资产钱包分类概述

随着行业的发展，市场上出现的钱包产品越来越多，使用的技术、策略以及侧重的功能点都不相同，本章将从五个角度出发，对现有的钱包产品做一个分类梳理和总结。如图 2.1 所示，可以从五个角度对钱包进行分类梳理，每一种分类方式其实都体现了该钱包所采用的策略重点，以及其面向的用户群体。有的体现了安全性、有的坚持易用性、而有些则强调功能。

图 2.1 数字资产钱包分类

2.1 按是否连网分类

数字资产钱包本质上是存储私钥的工具，私钥的安全性至关重要，为了将安全性做到极致，出现了不连网的冷钱包，因此可以依据钱包是否连网分为冷钱包和热钱包。依据火币区块链研究院调研分析的行

业内常见的 31 种数字资产钱包数据[5]，目前冷热钱包的项目数量占比如下图所示，冷热钱包数量基本符合二八分布定律。

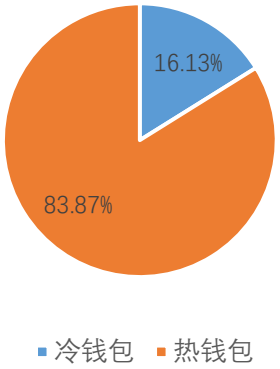

图 2.2 区块链冷热钱包占比

热钱包

- **特点：**保持实时连网上线的钱包通常称为热钱包。
- **分析：**热钱包相对于冷钱包使用起来更方便，既可在 PC 上使用，也可在手机等移动终端使用，还可对钱包内资产随时进行操作，因此目前 83.87%的钱包都为热钱包模式。但正由于其连网，也给了黑客攻击的基础条件，钱包安全性会受到挑战。不过通常钱包项目方会对存储的私钥以及通讯数据包进行加密处理，一定程度上也能避免黑客轻易入侵。

代表产品	Kcash		
公司成立时间	2018.2	产品首次发布时间	2017.10
团队规模	约 50 人	当前版本	V2.2.11
用户规模	约 90 万		
投融资情况	2018 年 5 月获千万美元融资		
支持币种	BTC、ETH、ACT、EOS 等		

[5] 31 种数字资产钱包项目列表详见附录 2

产品特点	Kcash 定位于多链热钱包，支持多条公链数字资产管理和交易，提供多重签名技术保障和两步授权验证、支持手机验证码、指纹、活体等多种验证方式。
同类产品	Imtoken、Jaxx、BreadWallet

冷钱包

- **特点：**冷钱包通常指不连网使用的钱包，也叫离线钱包。根据实现方式的不同，还可以分为硬件钱包和纸钱包。硬件钱包用来生成密钥和保存密钥，设备本身不会泄露或者输出密钥，而只是在我们按下某个按钮或者输入设备密码后显示密钥的保管情况。纸钱包，顾名思义就，就是把密钥记在纸上，然后把纸锁在保险柜里。
- **分析：**冷钱包将私钥存储在完全离线的设备上，相比于热钱包是更安全的方法，但成本更高易用性更差，比如传统的硬件钱包 Armory，需要一台不连网的电脑专门用于安装离线端。虽然冷钱包相对于热钱包更安全，但是冷钱包也不是绝对安全，可能会遇到硬件损坏，钱包丢失等情况，需要做好备份。

代表产品	库神（ColdLar）		
公司成立时间	2016.11	**产品首次发布时间**	2017.6
团队规模	约 100 人	**当前版本**	P2+、P2、P1
用户规模	3 万+，约占国内硬件冷钱包 90%份额		
投融资情况	2017 年底完成 A 轮融资，融资金额约 1000 万美元		
支持币种	支持比特币、以太币、瑞波币、新经币等多种主流币种，以及所有的 ERC-20 Token		
产品特点	库神钱包使用冷热分离架构，冷端主要负责构造交易并对交易进行数字签名，热端负责查询地址余额及广播发送交易。热端处理的都是公开透明的信息。库神钱包使用“种子密码+支付密码”的多重密码防护机制，通过“二维码非电磁波信道”的方式进行信息加		

	密传输，确保私钥永不触网，彻底根绝私钥被网络黑客窃取的风险。
同类产品	Ledger、Trezor、KeepKey

2.2 按数据存储完整性分类

数字资产钱包通常和区块链节点关系紧密，依据钱包存储节点账本数据的完整性可以将其分为全节点钱包和轻钱包，其中轻钱包也包括 SPV 节点钱包。由于全节点钱包需要下载所有的账本数据，会占用大量的存储空间以及计算资源，不适用于手机等移动终端，也不便于普通用户使用，故目前市面上约 90%的钱包都为轻节点钱包，如下图所示。

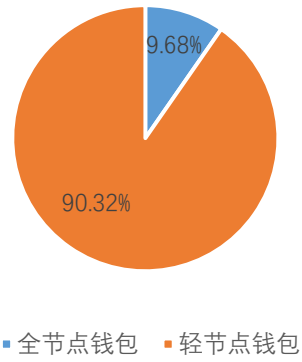

图 2.3 区块链全节点和轻节点钱包占比[6]

- **全节点钱包**

  - **特点：**全节点钱包参与到网络的的数据维护中同步了区块链上的所有数据，具有更有隐秘、验证更快等特点。但是由于数据量比较大，会导致扩展性低。
  - **分析：**由于需要同步链上信息的原因，很多全节点钱包的币种单

[6] 数据由火币研究院整理，来源附录 2 调研的 31 个钱包项目

一，不能够支持多种数字资产，一般为官方钱包。此外，全节点钱包需要占用很大的硬盘空间，并且一直在增长。每次使用前需要先同步区块数据，会导致易用性变差。

代表产品	Bitcoin Core		
公司成立时间	2013.5	产品首次发布时间	2009
团队规模	社区维护	已发布产品版本数	V1.16
用户规模	未披露		
投融资情况	无，开源社区软件		
支持币种	BTC		
产品特点	比特币核心是一个实现了全节点的比特币客户端，它组成了整个比特币网络的支架，是最早、最安全的比特币客户端。但是其它功能较少，且会占用很多的磁盘和内存空间，目前占据40G硬盘空间。		
同类产品	Ulord、Sia UI 等		

- **轻钱包**

- **特点：**轻钱包是为了解决全节点钱包需要占据很大的硬盘空间而出现的，不需要存储完整的区块数据。虽然轻钱包不会下载新区块的所有数据，但是它会对数据进行分析后，仅获取并在本地存储与自身相关的交易数据，运行时依赖比特币网络上的其他全节点，一般在手机端和网页端运行。

  SPV 钱包是轻钱包的一种，指的是可以进行简单支付验证的钱包。SPV 钱包也同步区块数据内容，但是只是临时使用，它从区块数据中解析出 UTXOs，但是并不保存区块数据。

- **分析：**轻钱包可以有更多的扩展性，一方面可以在币种上进行扩展，用来很方便地对多种资产进行管理。另一方面可以在运行 DAPP。因为它只同步和自己相关的数据，所以很轻便。轻钱包根据实现

原理可以分为中心化钱包和去中心化钱包。比如，客户端钱包，浏览器钱包，网页版钱包等。

代表产品	Imtoken		
公司成立时间	2016.5	产品首次发布时间	2017.2
团队规模	未披露	当前版本	V2.0
用户规模	月活 400 万		
投融资情况	2018 年 5 月获 IDG 资本 1000 万美元的 A 轮投资		
支持币种	BTC、ETH、ERC20、EOS		
产品特点	一是 TokenIon 提供去中心化交易功能；第二是 Dapps Browse，在钱包中构建第三方生态，与 imtoken 产生交互，来做授权、转账。		
同类产品	Kcash、Jaxx、Bitpie		

2.3 按私钥存储方式分类

私钥是数字资产领域安全的核心，而钱包的本质其实是帮助用户方便和安全地管理和使用私钥，因此，私钥的存储方式非常关键，按照私钥是否存储在本地，我们可以将钱包分为中心化钱包和去中心化钱包两种类型。如下图调研数据显示，目前去中心化钱包为主流模式，约占 82.76%。

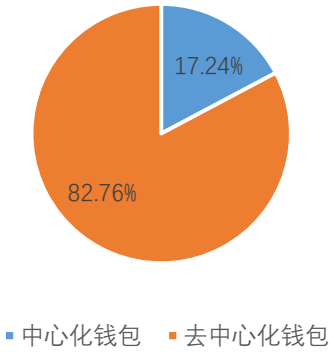

图 2.4 中心化和去中心化钱包占比[7]

[7] 数据由火币研究院整理，来源附录 2 调研的 31 个钱包项目

中心化钱包

- **特点：**私钥不由用户自持，而是由钱包项目方在链下中心化服务器上保管，通常资金也交由服务方托管。
- **分析：**中心化钱包通常也叫 Offchain 钱包，私钥和资产都交由钱包进行中心化管理，此种方式的钱包产品用户不必担心私钥丢失而导致资金损失，通常可支持密码找回功能；不过资金风险会更集中在钱包项目方，中心化服务器一旦被黑客攻克，用户将遭受不必要的损失。

代表产品	Cobo		
公司成立时间	2017.11	产品首次发布时间	2018.2
团队规模	40+	当前版本	V2.4.0
用户规模	持币用户约 20 万左右		
投融资情况	2018 年 4 月完成千万美元 Pre-A 轮融资		
支持币种	支持约 20+主链资产		
产品特点	提供中心化和去中心化存储私钥可选方案，中心化私钥托管钱包可帮助用户参与 POS 挖矿，获得收益。去中心化的 HD 钱包可支持 EOS 投票及 RAM 买卖等服务。		
同类产品	Blockchain，coinbase		

去中心化钱包

- **特点：**私钥由用户自持，资产存储在区块链上。
- **分析：**去中心化钱包通常也叫 Onchain 钱包，私钥的保管都转交给用户，若私钥遗失，钱包将无法帮用户恢复，资金将永久遗失；但去中心化钱包很难遭受黑客的集中攻击，用户也不用担心钱包服务商出现监守自盗的情况。

代表产品	TokenPocket		
公司成立时间	2018．4	产品首次发布时间	2018.2

团队规模	约 20 人	**当前版本**	V0.3.7
用户规模	约 20 万		
投融资情况	2018 年 4 月获得百万人民币天使轮融资		
支持币种	EOS、ETH、MOAC、井通		
产品特点	定位为通用型去中心化轻钱包，2018 年 6 月由于其对 EOS 底层以及 EOS RAM 交易较好的支持使得其用户数迅速提升。目前仅支持 4 个主链，后续将不断支持更多主链底层，并对外提供 API 接口服务。		
同类产品	Imtoken、Jaxx、keepKey、库神等		

2.4 按主链关系分类

目前各区块链公链都是较为独立的平台，平台和平台之间缺乏直接的互通，因此各类钱包出现了两大分化，一种是专门针对某一公链平台的主链钱包，通常由平台项目方或者社区开发提供；另一种则是同时支持多平台接口的多链钱包，支持的资产类型较为多样。依据火币区块链研究院整理的数据显示，主链钱包约占 35.48%，支持多链的钱包占绝对多数，随着行业的发展，这一比例可能进一步被拉大。

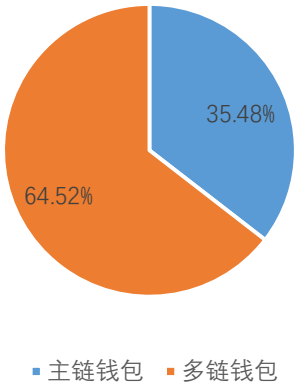

图 2.5 主链钱包和多链钱包占比[8]

主链钱包

➢ **特点：** 对于可以定制化发行通证的公链我们定义其为平台类公链，

[8] 数据由火币研究院整理，来源附录 2 调研的 31 个钱包项目

此类公链上可以运行多种 DAPP，平台专属钱包不仅是为了满足平台类通证正常使用所必备的核心组件，也可以作为一个应用商店，对基于其平台开发的 DAPP 进行集中宣发和链接跳转。

- **分析：** 对于平台类公链来说，平台通证通常具备一定的使用功能，平台上的各类角色所开展的活动都是围绕通证来进行，比如说矿工、平台用户、存储节点或者是计算节点等，因此需要钱包来作为各方进行通证存储和流通的节点。钱包也可以作为平台类项目是否可用的判断标准之一。

代表产品	EOS 钱包		
公司成立时间	2016	**产品首次发布时间**	暂未发布
团队规模	200 人以内	**当前版本**	无
用户规模	未披露		
投融资情况	EOS 项目 2018 年 6 月完成 ICO，融资约 700 万个 ETH，合计约 42 亿美元。		
支持币种	EOS		
产品特点	EOS 官方钱包主要定位于服务 EOS 生态的主链钱包，为 EOS 的超级节点投票、RAM 购买等提供通道，是行使 EOS 通证各项权利的入口和平台。		
同类产品	MetaMask、NEO 钱包、NAS 钱包		

多链钱包

- **特点：** 可支持多种主链平台通证的钱包。
- **分析：** 不同的主链通常采用的技术方案都各不相同，如果要支持多种主链平台的通证接入钱包，则需要逐一进行接口开发，有一定的开发难度和工作量。此类钱包对于支持内置交易所和跨链互兑业务有着天然的优势。

代表产品	Jaxx

公司成立时间	2016.5	**产品首次发布时间**	2016.5
团队规模	50 人以内	**当前版本**	V1.3.18
用户规模	70 万		
投融资情况	未披露		
支持币种	BTC，ETH，DASH，ETC，BCH，REP，LTC，ZEC，RSK，DGE，ICN，GNT，GNO，DGD，BCAP，CVC，STX，POE，MCI，QTUM，CFI，ART，PAY		
产品特点	定位为支持多种主链的去中心化轻钱包，用户界面友好，支持 9 种平台和设备，包括 Windows，Mac 和 Linux 桌面端，iOS 和 Android 移动端，以及 Google Chrome 和 Firefox 扩展。		
同类产品	Bitpie、Atoken、Ledger		

2.5 按私钥签名方式分类

为了加强数字资产的安全性并配合某些应用场景使用，出现了需要多方私钥签名才可使用钱包的策略，因此可将钱包分为单签名钱包和多签名钱包。依据火币调研的统计数据分析，如下图，支持多签名的钱包仅占 25.81%，单签名模式是市场上更受欢迎的方式。

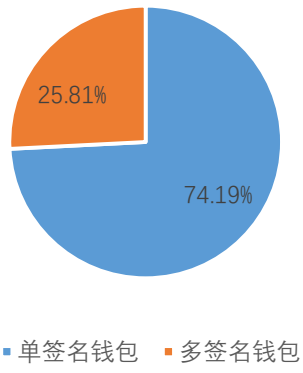

图 2.6 单签名和多签名钱包数量占比

单签名钱包

- **特点：**只需单个私钥签名即可交易。

- **分析**：单签名模式简单，用户可操作性强，但由于只有一个密钥，风险也更集中，私钥持有账户的单点沦陷——如果丢失或者泄漏私钥会可能直接导致账户中所有的资产的丢失。不过单签名钱包管理更为简便，方便用户对账户进行直接的控制且无需经过不可控第三方，因此也是市场上更受欢迎的一种模式，约 74%的钱包采用单签名模式。

代表产品	BitUniverse（币优）		
公司成立时间	2018.1	**产品首次发布时间**	2018.1
团队规模	30 人左右	**当前版本**	V2.0.2.2
用户规模	注册用户约 50 万，大部分为海外用户		
投融资情况	2018 年 2 月获天使轮融资		
支持币种	BTC，所有的 ERC20		
产品特点	定位于提供资产管理服务的单签名轻钱包，提供 200+交易所和钱包的数字资产自动导入和管理服务，为用户提供一致性的聚合交易体验。		
同类产品	Jaxx，Ledger，Bitcoin Core		

多重签名钱包

- **特点**：必须有 2 个（或多个）私钥同时签名才可以交易。
- **分析**：通常一个私钥用户保存，一个交给服务器，如果只有服务器私钥被盗，黑客没有本地私钥，交易时无法签名的。也可用于公司或者组织内由多方共同管理财产场景下使用，密钥由多位成员管理，需多数成员完成签名才可动用资产。多重签名机制相较于单签名是更安全了，但易用性却受到很大的影响，用户需要理解一些技术细节，还需要多方协同，学习和使用成本高了不少。此外，多重签名的机制更复杂，也带来一些安全隐患，如 parity

钱包的多重签名机制就被黑客利用，令逾 15 万个以太坊被盗。

代表产品	Parity		
公司成立时间	2015	产品首次发布时间	2016．2
团队规模	37	当前版本	V1.11.7
用户规模	未披露		
投融资情况	2016 年 4 月完成种子轮融资，融资金额 75 万美元		
支持币种	ETH 以及 ERC 技术下所发行的数字资产		
产品特点	定位为多签名的全节点钱包。Parity 对以太坊早期块的数据做了优化，同步区块数据速度快；支持多签名合约，支持硬件和电子冷钱包；内置 PoA、Tendermint 等共识引擎，为开发者提供稳定的开发环境。		
同类产品	BitGo、GreenAddress、Armory		

第三章 数字资产钱包技术实现原理

3.1 技术总览

数字资产钱包技术实现主要包含三个部分：1.钱包自身设计，如何生成助记词,keystore 和密码等;2.私钥、公钥和地址产生的方法;3.钱包提供商远程调用各公链 RPC 接口设计；如下图所示，可总体概括数字资产钱包实现的技术流程：

图 3.1 数字资产钱包实现技术流程概览

众所周知，私钥为一串无规律字符串，非常不便于记忆，使用更是不方便，所以从钱包设计的角度，为简化操作同时又不失安全性，就出现了助记词的方法。一般情况下，助记词由一些单词组成，只要记住这些单词，按照顺序在钱包中输入，就能打开钱包，下文将详细阐述其中的原理和方法。

根据密钥之间是否有关联可把钱包分为两类：

- 非确定性钱包（nondeterministic wallet）：每个密钥都是从随机数独立生成，密钥彼此之间无关联，这种钱包也被称为“Just a Bunch Of Keys（一堆密钥）”，简称 JBOK 钱包。
- 确定性钱包（deterministic wallet）：所有密钥都是从一个主密钥派生出来，这个密钥即为种子（Seed）。该类型钱包中所有密钥都相互关联，通过原始种子可以找到所有密钥。确定性钱包中使用

了很多不同的密钥推导方法，最常用的是使用树状结构，称为分级确定性钱包或者 HD (hierarchical deterministic)钱包。

比特币钱包(Bitcoin Core)生成密钥对之间没有直接关联，属于 nondeterministic wallet，这种类型的钱包如果想备份导入是比较麻烦的，用户必须逐个操作钱包中的私钥和对应地址，如下图包含的为松散结构的随机密钥集合的非确定性钱包：

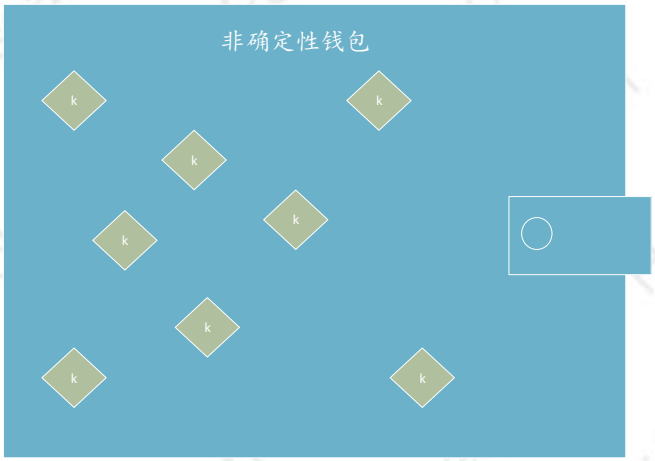

图 3.2 非确定性钱包示意图

Deterministic wallet 基于 BIP32(Bitcoin Improvement Proposal32)/BIP39/BIP44 标准实现，通过一个共同的种子维护 n 多私钥，种子推导私钥采用不可逆哈希算法，在需要备份钱包私钥时，只备份这个种子即可（大多数情况下的种子是通过 BIP44 生成了助记词，方便抄写），在支持 BIP32，BIP39，BIP44 标准的钱包只需导入助记词即可导入全部的私钥，如下图种子派生密钥的确定性钱包：

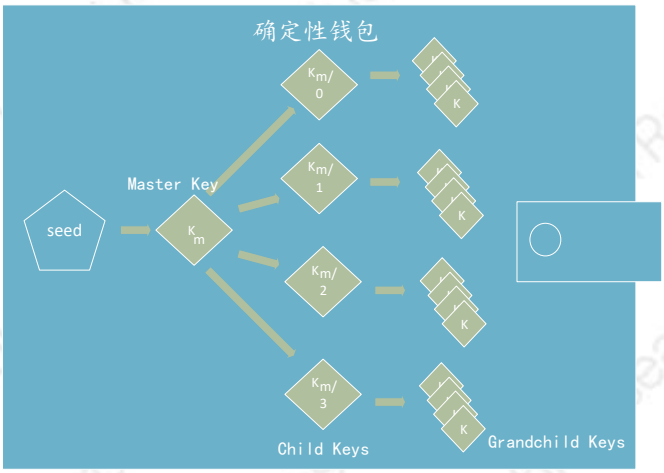

图 3.3 确定性钱包示意图

上面提到了 BIP32，BIP39，BIP44 标准，概括来说 BIP32 标准定义了种子使用 HMAC-SHA512 生成根私钥，并导出子私钥，这是 HD 钱包的主要标准；BIP39 标准定义了钱包助记词和种子生成规则；BIP44 标准定义了节点布局，用于多币种和多账户钱包；除此之外，还有 BIP43 标准用于定义多用途 HD 钱包结构。具体可以前往 https://github.com/bitcoin/bips 学习。

3.2 钱包设计框架

3.2.1 生成助记词（BIP39 标准）

助记词库有 2048 个词，用 11 位可全部定位词库中所有的词（2^11=2048），作为词的索引，故一个词用 11 位表示，助记词的个数可为(熵+校验和)/11，值为 12，15，18，21，24。规定熵的位数必须是 32 的整数倍，所以熵的长度取值为 128 到 256 之间取 32 的整数倍值，分别为 128，160，192，224，256；校验和的长度为熵的长度/32 位，所以校验和长度可为 4，5，6，7，8 位。

表 3.1 熵的位数和助记词长度对应表

熵（Bits）	校验和（Bits）	熵+校验和（Bits）	助记词长度
128	4	132	12
160	5	165	15
192	6	198	18
224	7	231	21
256	8	264	24

生成助记词的具体步骤如图 3.4 所示：

1) 生成长度为 128～256 位(bits)的随机序列(熵)，以 128 位为例；
2) 取熵 SHA256 哈希后的前 n 位作为校验和(n= 熵长度/32)，图为 128/32=4；
3) 随机序列(熵) + 校验和拼合为一个字符串，图为 128+4=132；
4) 把步骤 3 得到的结果每 11 位切割，图为 132/11 =12 个字符串；
5) 步骤 4 得到的每个字符串匹配预先定义的 2048 个词库里的单词；
6) 步骤 5 得到的结果就是助记词串，这是一个有顺序的单词组，也就是我们一直说的助记词。

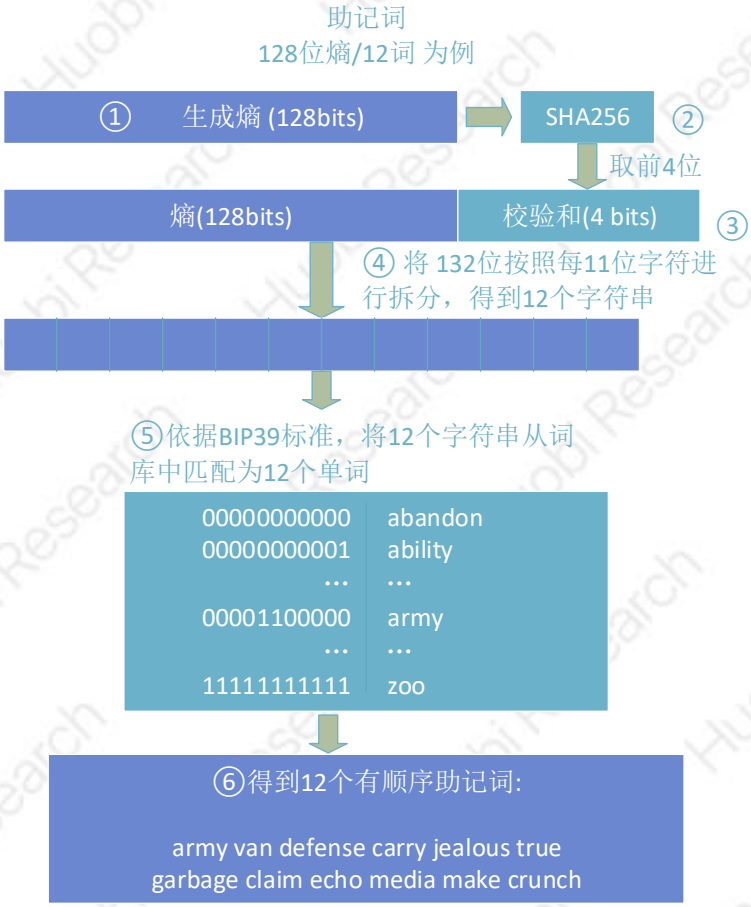

图 3.4 生成 12 位助记词算法示意图

3.2.2 通过助记词生成种子（BIP39 标准）

助记词由长度为 128 到 256 位的随机序列(熵)匹配词库而来，随后采用 PBKDF2(Password-Based Key Derivation Function 2)推导出更长的种子(seed)。生成的种子被用来生成构建 deterministic Wallet 和推导钱包密钥。

在密码学中，Key stretching 技术被用来增强弱密钥的安全性，增加了暴力破解（Brute-force attack）对每个可能密钥尝试攻破的时间，增强了攻击难度。各种编程语言原生库都提供了 key stretching 的实现。PBKDF2 是常用的 key stretching 算法中的一

种。基本原理是通过一个为随机函数(例如 HMAC 函数)，把明文和盐值作为输入参数，然后重复进行运算最终产生密钥。

如图 3.5 所示：

1) PBKDF2 有两个参数：助记词和盐。盐的目的是提升进行暴力攻击时的困难度，可以参见 BIP-39 标准。盐由字符串常数“助记词"与可选的用户提供的密码字符串连接组成；

2) PBKDF2 使用 HMAC-SHA512 作为随机算法+2048 次哈希重复计算，最终得到 BIP32 种子，512 位(64 字节)是期望得到的种子长度。即 DK = PBKDF2(PRF, Password, Salt, c, dkLen)，其中，PRF 是一个伪随机函数，例如 HASH_HMAC 函数，它会输出长度为 hLen 的结果；Password 是用来生成密钥的原文密码；Salt 是一个加密用的盐值；c 是进行重复计算的次数；dkLen 是期望得到的密钥的长度；DK 是最后产生的密钥。

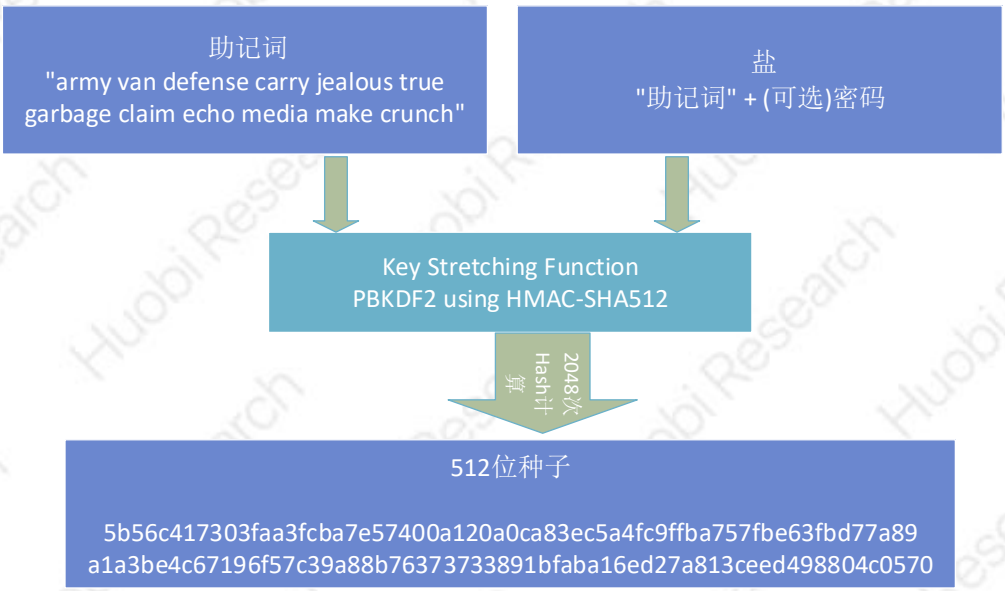

图 3.5 512 位种子生成过程示意图

3.2.3 从种子中创造 HD 钱包（BIP32 标准）

HD 钱包从单个根种子（root seed）中创建，为 128 到 256 位的随机数，任何兼容 HD 钱包的根种子也可重新创造整个 HD 钱包，所以拥有 HD 钱包的根种子就等于拥有了所有密钥，方便存储、导入及导出。

具体主密钥以及 HD 钱包的主链码生成过程如图 3.6 所示，根种子通过不可逆 HMAC-SHA512 算法推算出 512 位的哈希串，左 256 位是主私钥 Master Private Key (m)，右 256 位是主链码 Master Chain Code；链码 chain code 作为推导下级密钥的熵。

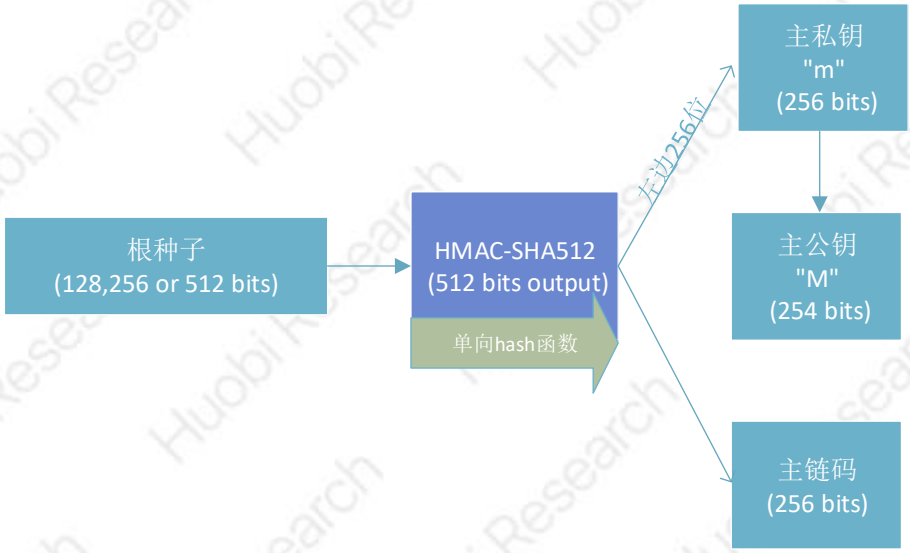

图 3.6 HD 钱包及主链码生成示意图

以上过程再结合 BIP43，BIP44，对 HD 钱包还能实现诸如多币种、多账户、多用途等功能。

3.2.4 keystore 和密码基本功能

回归到用户体验，助记词的方式仍然很复杂的，现有的密码操作

方式才是用户最为熟悉的方式。因此钱包还提供了 keystore 让用户导出密钥文件进行保存，Keystore 会存储在使用的设备里，这样每次登录只用输入相应密码即可。Keystore 是私钥经过加密过后的一个文件，需要用户设置的密码才能打开文件。即使 keystore 文件被盗，只要用户设置的密码够长够随机，短

时间内私钥也不会泄露，有充足的时间转移地址里的数字资产到其他地址。

3.3 私钥、公钥和地址产生的方式

从私钥推导出公钥、再从公钥推导出公钥哈希都是单向的，采用不可逆算法，也就是常听到的椭圆曲线算法：如图 3.7 所示。

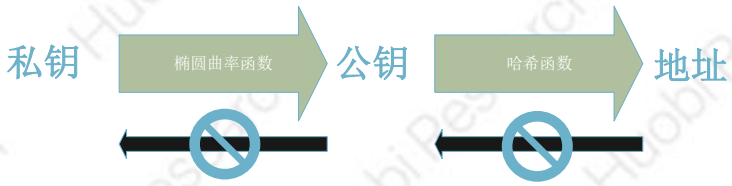

图 3.7 公钥和地址生成示意图

整体的公钥和地址生成过程如图 3.8 所示：

1) 通过随机数生成私钥；

2) 私钥经过 SECP256K1 算法处理生成了公钥；

3) 同 SHA256 一样，RIPEMD160 也是一种 Hash 算法，经过一次 SHA256 + 一次 RIPEMD160 哈希运算，由公钥计算得到公钥哈希；

4) 将一个字节的地址版本号连接到公钥哈希头部，进行两次 SHA256

运算，将结果的前 4 字节作为公钥哈希的校验值，连接在其尾部；

5）将第 4 步结果使用 BASE58 进行编码，即得到钱包地址。

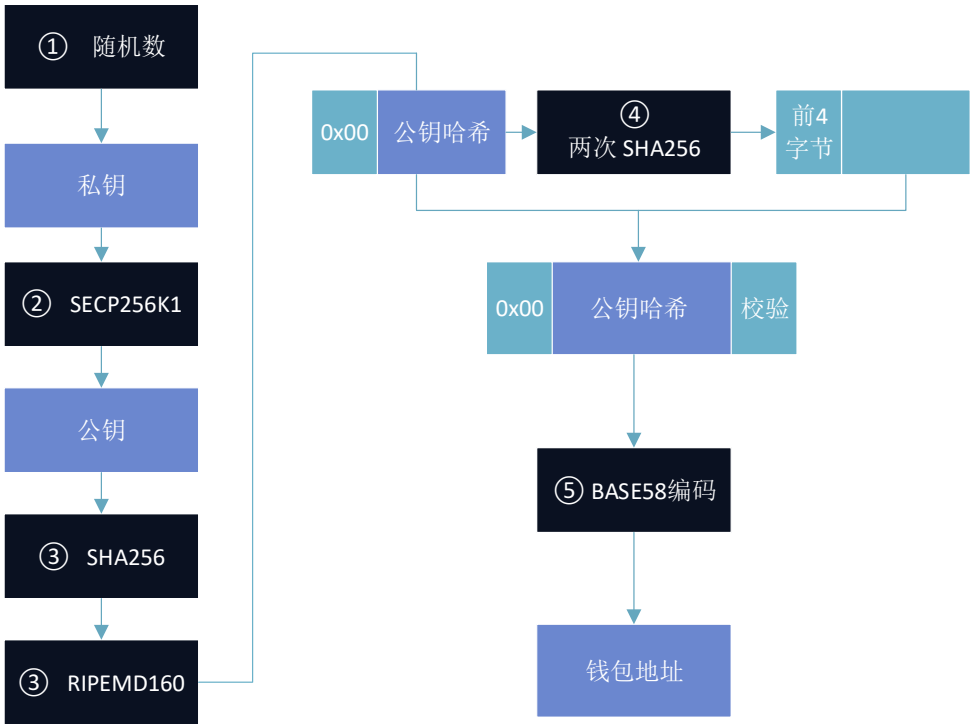

图 3.8 公钥和钱包地址生成流程图

从字节层面拆开来看，公钥的详细生成流程如图 3.9 所示：

1）私钥是 32 字节（256 位）的随机数；

2）在私钥头部加上版本号；

3）在私钥尾部加上压缩标志；

4）将私钥进行两次 SHA256 哈希运算，取两次哈希结果的前 4 字节作为校验码，添加到压缩标志之后；

5）将 2，3，4 步得到的随机数用 BASE58 进行编码，就可以得到 WIF（Wallet import Format）私钥（用于钱包之间导入导出私钥，是用户较为常见的密钥格式）。

6) 私钥经过椭圆曲线乘法运算，可以得到公钥。公钥是椭圆曲线上的点，并具有 x 和 y 坐标。

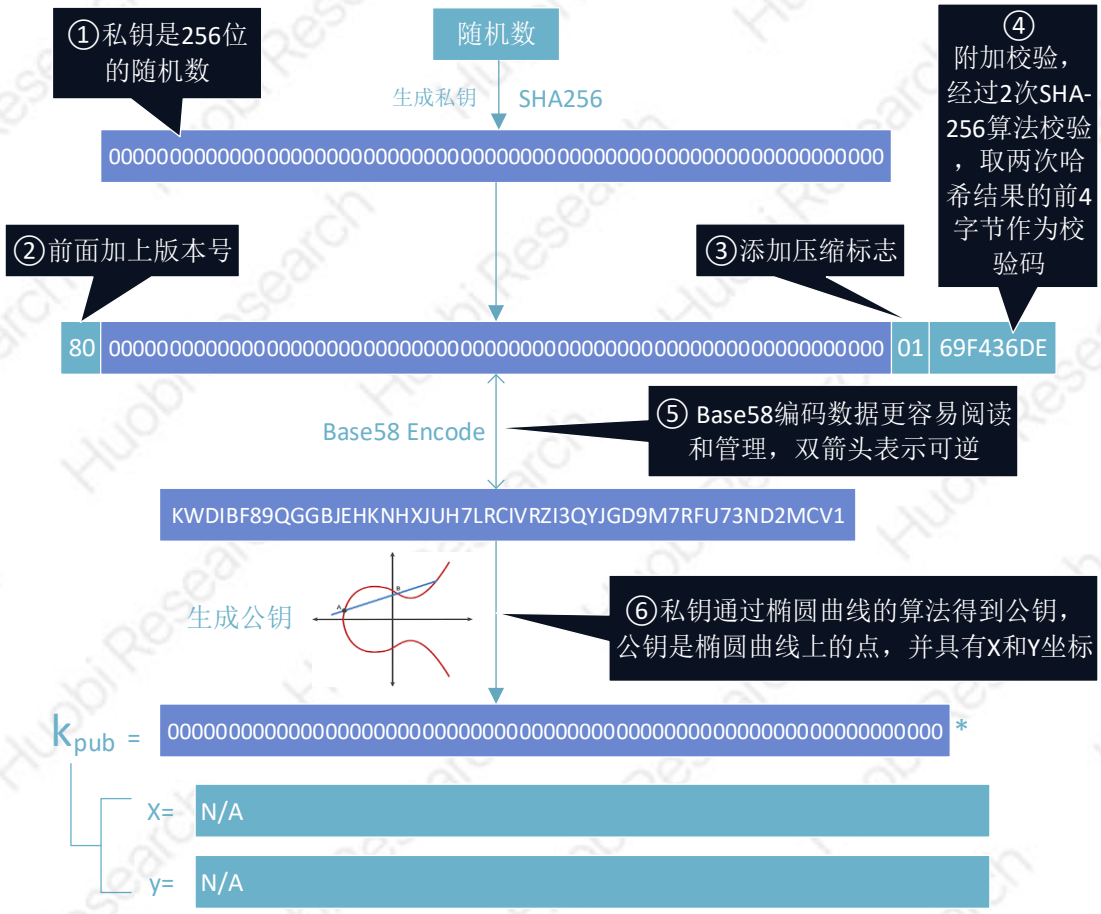

图 3.9 公钥生成详细流程解说图

从字节层面拆开来看，钱包地址的详细生成流程如图 3.10 所示：

1) 将公钥通过 SHA256 哈希算法处理得到 32 字节的哈希值；

2) 后对得到的哈希值通过 RIPEMD-160 算法来得到 20 字节的公钥哈希 Hash160；

3) 把版本号+公钥哈希 Hash160 组成的 21 字节数组进行双次 SHA256 哈希运算；

4) 将哈希值的前 4 个字节作为校验和，放在 21 字节数组末尾；

5）对组成 25 位数组进行 Base58 编码，最后得到钱包地址。

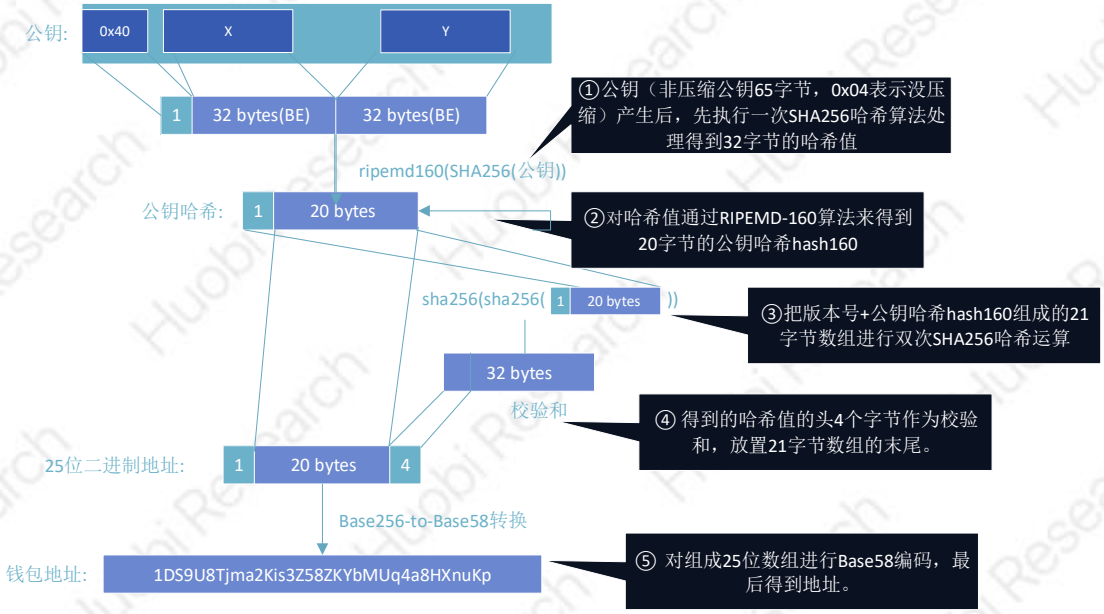

图 3.10 钱包地址生成详细流程解说图

3.4 恢复钱包的 N 种方式

了解了钱包的基本技术原理以及助记词、Keystore、私钥、公钥和地址的关系后，遇到私钥丢失等情况我们就可以有条不紊地进行钱包找回工作了，如图 3.11 所示，只要不是私钥、密码、助记词同时全部丢失，你还有 N 种方法可以恢复钱包。

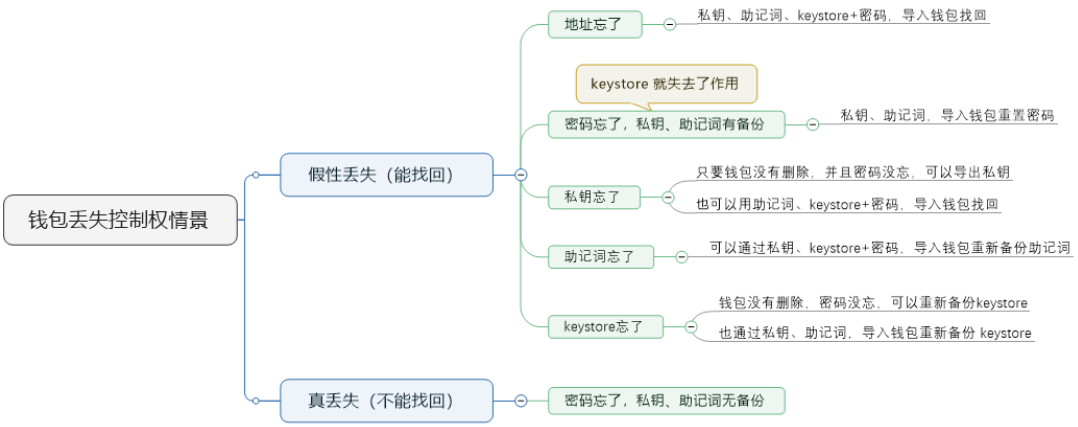

图 3.11 恢复钱包的 N 种方式

第四章 数字资产钱包安全分析

对区块链行业来说，安全将是永恒的话题，钱包涉及到用户资产的核心，其安全性更是不容忽视。近两年来，数字资产钱包安全事件不断，parity 钱包的两个安全事件则直接导致约 24 万个以太坊的损失，2018 多款冷热钱包也都爆出安全问题，如图 4.1 所示。

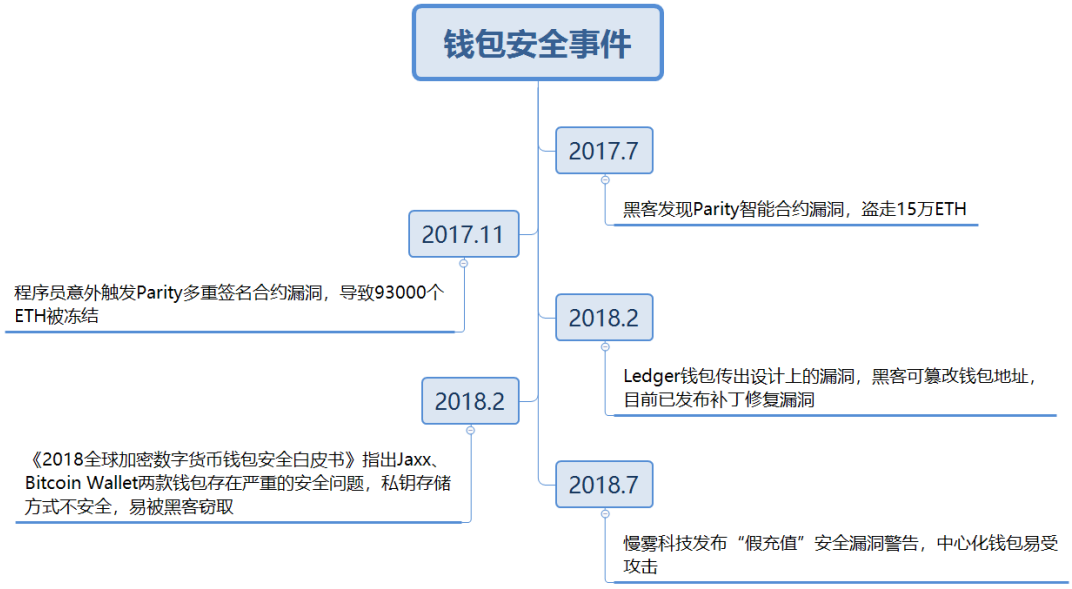

图 4.1 数字资产钱包安全事件时间轴

数字资产钱包的安全性不仅要从底层设计上就进行全面考虑，对于大部分去中心化钱包来说，对用户的安全教育也是非常重要的内容，如图 4.2 所示。

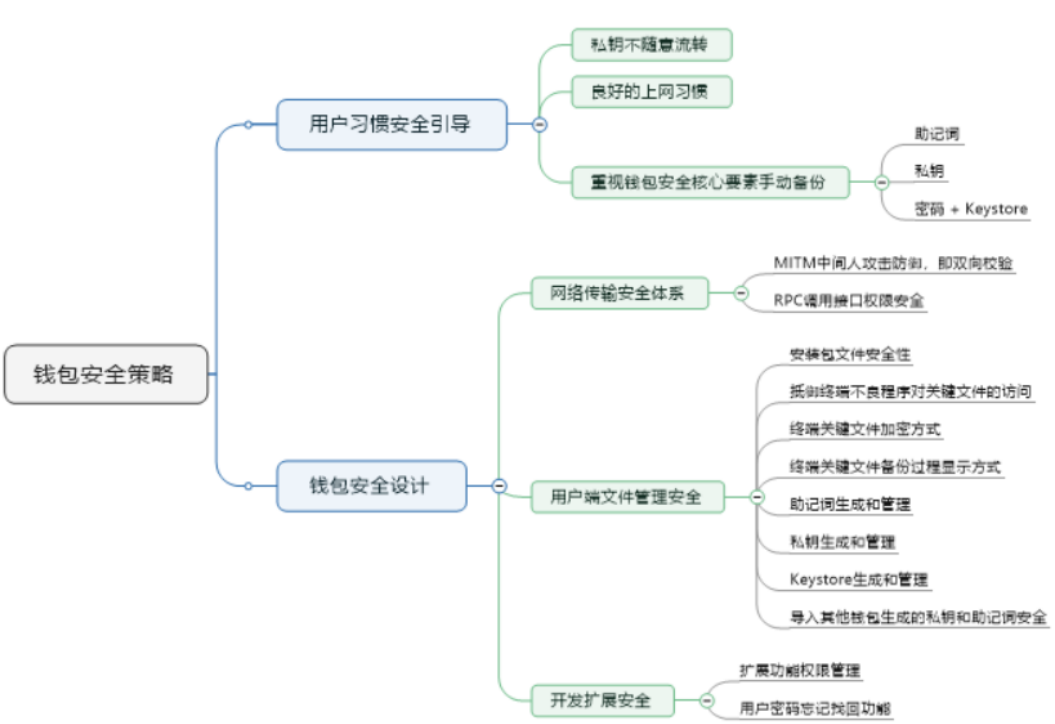

图 4.2 钱包安全策略思维导图

4.1 用户习惯安全引导

对于去中心化钱包，私钥交由用户保存，如何帮助用户正确地理解和使用密钥、助记词等成为钱包项目方重点关注的内容。目前主流钱包采用图文教程、答题考试、视频讲解等方式来帮助用户理解钱包的各种基本概念、提醒用户正确地保管助记词、私钥和本机密码等。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。

4.2 钱包安全设计

4.2.1 网络传输安全

MITM 中间人攻击防御，即双向校验

中间人攻击 MITM（Man-in-the-middle attack）：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是衡量一个数字钱包应用安全性的重要评判标准。

RPC 接口调用权限安全

钱包本身只是区块链世界的接口软件，正如前文介绍的很多都是使用 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（RemoteProcedureCall，RPC）时安全策略：如在钱包节点 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。

4.2.2 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。

- **安装包安全性**

确保软件安装包的安全和不可被反编译、破解来植入非法操作等。

- **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确认的功能等。

- **终端关键文件加密方式**

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。如 Wallet.dat 加密问题。

- **终端关键文件备份过程显示方式**

用户难免对关键文件有备份的需求，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。

- **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。

对助记词的显示采用不能进行任何操作的显示方式，供用户手动记录。

- **导入其他钱包生成的私钥和助记词安全**

导入其他钱包生成的私钥和助记词安全的思路可以从重新创建新的核心文件的方式来降低非法程序入侵的风险；也可以同时用人脸识别或者短信确认的功能等。

4.2.3 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。

第五章 存在的问题及产业发展趋势

5.1 现有产品存在的问题

安全问题时有发生

由于业务场景的快速迭代以及推广需求，无论热钱包还是冷钱包都会有一些安全隐患会被忽视。安全性和使用便捷性之间的冲突短时间无法解决。市面上的数字资产钱包良莠不齐，部分开发团队在以业务优先的原则下，暂时对自身钱包产品的安全性并未做到足够的防护，导致黑客有机可乘，类似 Parity 钱包、Ledger 钱包等漏洞事件时有发生。

支持币种少，功能单一

市面上的钱包虽种类繁多，功能却普遍单一，支持的数字资产种类也十分有限。用户在管理数字资产时，通常需要在多种钱包之间来回切换，不仅影响了用户体验，也带来了不少风险。

使用门槛较高，易用性不强

目前新进入数字资产市场的用户仍倾向于将资产放在交易所，一方面是由于交易便捷性的需要，另一方面也表明钱包对于普通用户来说仍然有较高的使用门槛，钱包仍需进一步优化业务流程，改进技术，提高使用便捷性，更需要加强用户教育，帮助用户正确、安全地使用钱包。

盈利模式仍在探索

目前大多数钱包的盈利模式仍在探索，变现能力不强，钱包项目

的生存压力较大。相较于热钱包，卖设备的冷钱包有更强的变现能力，不过其设计研发的前提投入较大，库存积压的风险也较高，受市场整体行情影响较大。

5.2 数字资产钱包发展趋势

一方面，钱包是用户与区块链交互的界面，可视为现实世界通往区块链世界的一个重要入口；另一方面，钱包的本质是私钥管理工具，与区块链及数字资产息息相关，资产属性强烈。未来数字资产钱包的发展也将紧紧围绕着这两点特性不断丰富和扩展。随着行业的发展和演进，势必有些钱包将在某一领域进行技术和资源上的深耕形成行业高壁垒，有的则将朝着全面和综合性的方向进行业务优化和资源聚合。

- **区块链世界入口功能发展并强化**

资产种类增加，一体化管理入口。当数字资产种类越来越多，用户急需统一化的平台帮助用户管理众多类型的资产。而由于目前中心化数字资产交易存在的流动性分割现状，用户需要在不同的交易所注册登录不同的账户进行查询和交易，过程繁琐，而且未来也很难改善此类现状，因此钱包将成为资产聚合的首选方案。资产一体化管理可将用户在多个钱包和交易所的通证持有情况进行汇总并提供统一的汇总、查询、分析以及交易等服务。未来支持多平台跨链兑换等功能的发展，也将满足用户流动性多样化需求。

DAPP 应用入口。互联网时代，如同各类 App 作为用户感受移动互联网的窗口。未来，区块链时代，各类 Dapp 也将成为用户直接参

与区块链的主要方式。由于用户与 Dapp 的交互需要消耗数字资产，而钱包作为协助用户管理各类数字资产工具，其重要性不言而喻，可能会成为新时代应用商店，成为区块链 3.0 时代真正超级流量入口。

通证使用权、收益权等功能性入口。未来随着区块链项目的落地，以及通证的功能属性越来越强，钱包作为区块链世界的入口将承载着非常关键的角色。用户只有自己直接掌管着私钥，才能行使通证所代表的各种功能和权力，例如 EOS 投票权、获得 POS 挖矿收益等。未来通证经济模式下还将诞生更多的通证实际使用场景，例如各类行为挖矿、分红，权力凭证等。钱包提供的直接便捷渠道，将会释放出通证除交易以外的功能潜力，更好的促进通证经济发展。

- **金融属性强化，服务和产品不断丰富**

交易属性日渐增强。钱包用户天然拥有交易需求，如果币不用提出钱包就可以实现交易，不但减少了用户提币转币的操作步骤，减少了犯错的概率，也增强了用户黏性，为钱包项目的后续转型提供了很好的发展方向和资金沉淀。另外，去中心化交易所的发展也会促进去中心化钱包的发展，这对 Onchain 钱包有天然优势。

理财服务不断完善。作为资产沉淀的平台，数字资产钱包不仅仅是工具、是流量入口更是资金入口和金融服务平台。围绕资产开展一系列理财服务将是未来钱包发展重点。目前已有一些数字资产钱包开始布局各类理财和资金托管服务，但是该领域还在非常早期阶段，和传统的资管服务很不一样，风控、盈利模式、资金安全等很多问题还需一一解决，产品设计也需结合区块链资产特点进行重新规划和考虑。

附录 1：常见名词

1. 密钥：是指某个用来完成加密、解密、完整性验证等密码学应用的秘密信息。在对称密码中，加密和解密用的密钥是同一个。而在非对称密码中，加密和解密用的钥匙不同，根据是否公开可分为公钥和私钥。

2. 私钥：在非对称密码中，加密和解密用的钥匙不同。根据是否公开，可分为公钥和私钥。公钥和私钥成对生成和使用。其中由用户自己保管、不对外公开的，称为私钥。

3. 公钥：在非对称密码中，可对外公开并传递的密钥称为公钥。

4. 地址：通常由公钥产生。公钥经过多种加密算法、哈希算法等生成用户钱包地址，类似传统金融中的银行卡号。

5. 数字签名：类似写在纸上的普通的物理签名，转移资产的时候需要用户签名才能启动。多重签名，则是地址允许多个用户用一个公钥单独发送部分地址，共同管理资产。

6. 助记词：将难以记忆的私钥通过加密算法转换成一组常见单词。私钥与助记词之间可以互相转换。

7. Keystore：通过加密算法加密过后的私钥，通常以文件格式储存。

8. 冷钱包：离线钱包，在没有连网环境下使用的，统称冷钱包。

9. 脑钱包：脑钱包的主要原理是用可预测的算法把口令转换成一对

公私钥，用户通过输入自行编写的一串字符串，即可与一个笃定的密钥生成一一对应的映射，是一种密钥生成方式。

10. 硬件钱包：用专业的硬件存储数字资产，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。

11. 纸钱包：将私钥或助记词以字符串、二维码等形式记录在纸张上来进行保存和使用的方法。

12. 热钱包：即连网又称在线钱包，处于连接互联网状态，私钥存储能被网络直接访问的钱包。

13. 重钱包：全节点钱包，保存私钥的同时，需同步所有区块链数。

14. 轻钱包：不保存所有区块的数据，只保存跟自己相关的数据的钱包。

15. 去中心化钱包：用区块链网络上其他全节点，不用保存所有区块数据，需保存和同步与自己相关的数据，无需第三方管理存储你的私钥，私钥由本人控制。

16. 中心化钱包：用户无私钥，数据均完全依赖运行提供钱包产品的中心化的第三方。

附录 2：31 个调研项目清单

Blockchain	BitGo	CoinBase	imToken
Jaxx	Kcash	MyEtherWallet	BitcoinCore
Mist	KeepKey	Ledger	Trezor
库神钱包	Armory	BitPie	Cobo
Cipher	Atoken	Tokenpocket	Mycelium
Electrum	Counterwallet	BTC.com	Breadwallet
Copay	Greenadress	Coinomi	Airbitz Wallet
Exodus	BitUniverse	HyperPay	

火币区块链应用研究院

关于我们：

火币区块链应用研究院（简称“火币研究院”）成立于 2016 年 4 月，于 2018 年 3 月起全面拓展区块链各领域的研究与探索，主要研究内容包括区块链领域的技术研究、行业分析、应用创新、模式探索等。我们希望搭建涵盖区块链完整产业链的研究平台，为区块链产业人士提供坚实的理论基础与趋势判断，推动整个区块链行业的发展。

联系我们：

咨询邮箱：huobiresearch@huobi.com

微信公众号：火币区块链

Twitter: Huobi_Research

https://twitter.com/Huobi_Research

Facebook: Huobi Research

https://www.facebook.com/Huobi-Research-655657764773922

Medium: Huobi Research

https://medium.com/@huobiresearch