2018年全球加密数字货币钱包行业研究报告

Kate Mao- 2018年5月7日

前言

2017年下半年，以比特币为首的数字货币发生暴涨，引发了全球对加密数字货币的关注。围绕数字货币存储、交易、智能合约等环节的安全性问题已变得越来越重要，加密数字货币安全性对这个新兴市场具有几乎致命的影响，是决定数字货币市场能否健康可持续发展的重要基石。因此，打造安全可靠的数字货币钱包作为数字资产的存储地是至关重要的。

基于对区块链领域的深度探索与挖掘研究、以及对安全领域的重视，编写2018年全球加密数字货币钱包行业研究报告，详细解读数字货币钱包的存在背景及当前发展状况、安全性等，为广大区块链技术爱好者、加密数字货币持有者提供参考价值。

本文将由以下几个部分组成：

- 加密数字货币钱包的基础知识
- 加密数字货币钱包出现的背景
- 加密数字货币钱包的发展现状
- 加密数字货币钱包存在的安全隐患
- 加密数字货币钱包未来展望

一、加密数字货币钱包的基础知识

1. 加密数字货币钱包是什么?

加密数字货币是一种基于区块链技术的数字货币。如需对加密数字货币作进一步了解，请查阅相关资料，此处不过多赘述。

和现实中的钱包一样，区块链钱包是为了更好的保护我们的数字货币资产。实现了个人财产不可侵犯、第三方未得到我们授权的情况下，无支配权。加密数字货币钱包（简称“钱包”）是专门用来管理数字货币资产的应用/硬件，可提供钱包地址的创建、加密数字货币转账、每个钱包地址交易历史的查询等基础金融功能。通俗地说，钱包是用来保管密钥的工具/容器。

2. 加密数字货币钱包有哪些功能?

加密数字货币钱包是用于管理和使用私钥的工具，有了密钥就可以拥有相应地址上的加密数字货币的支配权。

加密数字货币钱包最基本的功能包括:

私钥的生成和管理

助记词的生成和管理

钱包地址的生成

支持导入其他钱包生成的私钥和助记词

对数字资产进行转账等

3. 加密数字货币钱包分为哪几类?

按钱包私钥的存储方式分为为冷钱包和热钱包。热钱包是指网络能直接访问到个人私钥的钱包，往往是在线钱包的形式；冷钱包是指私钥存储在本地的钱包，比如不联网的电脑、手机、写着私钥的小本等等，冷钱包可以最大程度保证你的资产安全。冷钱包又可分为软件冷钱包和硬件冷钱包。

按所使用的硬件设备可分为:

（1）PC机桌面钱包，即钱包软件运行于PC机的桌面操作系统之上，如Windows、MacOS、Linux等。

（2）在线Web版钱包，即运行于云端服务器上，通过浏览器访问的钱包。

（3）移动端手机钱包，即钱包软件运行于移动终端的操作系统之上，如Android、iOS等。

（4）硬件钱包，运行与专门定制的硬件上，其功能上并不包含冷钱包的所有功能（比如查询余额、处理交易数据等操作），主要功能用于保管私钥。硬件钱包是一种比较安全且新

颖的存储方法，而且目前还没有硬件钱包被盗的事件被曝光。最热门的两款硬件钱包是Ledger Nano S和TREZOR。

（5）纸钱包，是一种冷存储形式，即脱机存储。纸钱包指的是把公钥和私钥打印在一张纸上，然后放在一个用户认为最安全的地方。目前最热门的以太坊和ERC20的纸钱包为MyEtherWallet。

按区块链数据的维护方式可分为：

（1）全节点钱包，即包含对应数字货币的全部区块链数据，这类钱包完全去中心化并且同步了所有区块链数据。唯一缺陷需要用户有足够的物理资源存储空间记录数据。

（2）SPV轻钱包，只维护与自己相关的区块链数据，基本上去中心化，必要时需依赖比特币网络上的其他全节点。

（3）中心化钱包，不依赖比特币网络，只依赖自己的中心化服务器，不同步数据，所有的数据均从自己的中心化服务器中获得。

按支持币种划分为：支持单一币种钱包、支持多样币种钱包。

4. 加密数字货币钱包的运作原理?

钱包基于密码学原理设计，可创建1个或多个钱包地址，每个钱包地址都对应1个密钥对：私钥和公钥。

- 公钥：对外交易时使用，是根据私钥进行一定的数学运算生成。
- 私钥：是唯一能够证明对于数字资产有控制权的凭证。因此，私钥的生成和存储方式决定了资产安全与否。
- 助记词：是明文私钥的另一种表现形式，目的是为了帮助用户记忆复杂的私钥，能否安全的管理助记词也是区别钱包是否安全的重要条件。

公钥、私钥一一对应，且每次交易时均需要使用私钥对交易记录进行签名以证明对相关钱包地址里面的资产有控制权。通常意义上的数字资产安全其实就是私钥的安全，一个钱包是不是安全主要看它能否安全的管理和使用私钥。加密数字货币钱包的安全隐患主要存在于钱包渠道、用户使用，以及钱包本身的安全技术设计上。

二、加密数字货币钱包出现的背景

1.数字货币交易频频发生的安全事故

据不完全统计，73%的交易所保管用户的密钥，仅有23%的交易所让用户自己控制密钥。正是这样，交易所极易成为黑客攻击的对象。下表是对近年来数字货币交易所发生比特币被盗事件的统计。

时间（单位：年）	交易所	事件
2012	Bitcoinica	两次被盗6万多枚比特币
2014	Mt.Gox	全球最大比特币交易所85万个，价值4亿6000万美元的比特币被盗一空，交易所随即倒闭
2015	Bitstamp	被盗2万个比特币
2016	GateCoin	被盗18.5万个ETH
2016	Bitfinex	全球最大的美元比特币交易平台（香港）由于网站出现安全漏洞，导致用户持有的比特币被盗，被盗比特币共119756枚，总价值约7200万美元
2018	Coincheck	日本最大的数字货币交易所遭黑客攻击，价值5.3亿美元的数字货币被盗，所有提现服务暂停，并停止加密货币交易。 Coincheck赔偿近30亿人民币
2018	Bittgrail	价值1亿7000万美元的加密货币被盗
2018	OKEx	出现近1.5个小时的极端交易行为，BTC季度合约一度比现货指数低超过20%，最低点逼近4000美元，约有46万个比特币的多头期货合约爆仓；跌到最低点后瞬间被拉涨超过10%，部分空头被爆仓。 OKEx宣布交易回滚

2.用户对安全存储数字资产、便捷实用的迫切需要

尽管数字货币市场在快速发展，但对于数字货币的存储和管理，仍然没有很 好的解决方案，如何安全备份一种数字货币的钱包密钥或地址私钥，就已经是拦在用户面前的一大门槛。现在面对越来越多的数字货币类别，用户进行不同资产配置或分散投资时，管理门槛进一步提升，而应对的策略——要么是针对不同类型的数字货币，安装不同的去中心化钱包分别管理；要么是索性放在中心化钱包或者交易所里，让中心机构代为管理。

- **全球加密数字货币用户体量**

（1）中国

据统计，中国的数字货币交易人数在300万—500万之间。

（2）日本

日本金融厅召开数字货币研讨会，截止2018年3月30日，17家在日本金融厅注册的数字货币交易所用户数总计350万人，90%的用户年龄在20岁至40岁之间，5828个账户存入1000万日元以上。

（2）交易所统计：以币安为例

截止2018年3月，币安网的用户总数已突破790万人。在上个月11月的感恩节假期，Coinbase新增账户10万个，账户总数达到1310万。根据Coinbase网站的历史记录，去年十一月，他们的用户数约为490万个。

❖ **用户使用习惯**

（1）对于刚开始购买数字货币的群体，在购买量不大或者安全意识不高的情况下，通常会把数字资产存放在交易所。

（2）对于一些资产大户，为了安全考虑会拥有一个独立的移动钱包或者专业的硬件钱包。一般来讲，这些钱包的私密性会更好一些。

三、加密数字货币钱包的发展现状

随着数字货币从极客群体逐渐走向更多普通大众。数字货币可应用的地方多了起来，比如跨境支付、比如购买金融产品等等，俨然看到围绕数字货币的生态渐渐丰富起来。

据网易科技统计，目前已知的国内数字货币钱包已有超过20个，在全球则有几百家。由于数字货币市场从出现至今一直走的是国际化路线。

钱包，这个被看作未来数字资产交易的入口，引来了诸多企业的激烈竞争。毕竟，谁拿下了这个市场，谁就有可能成为未来全球区块链版图的“支付宝”，甚至是“微信”。

1.硬件数字货币钱包提供商概括

加密货币的普及带动硬件钱包越来越受欢迎。 加密货币硬件钱包是一种实体设备，私钥储存在在设备内的受保护区域中。这些设备被认为是一种可靠的投资，从长远来看，它们可以防止网络中的恶意偷窃行为，也能让用户的加密货币更加安全。到目前为止，硬件钱包还没有发生过大规模的漏洞或黑客窃取的资金事件。世界各地的许多加密货币爱好者都使用像Trezor、Ledger、Bitbox和Keepkey这样的冷储存设备。

以下枚举较为知名的几款：

（1）国内

钱包名称	支持币种	介绍
库神	BTC ETH LTC	可以存储多种数字资产(比特币，莱特币，以太坊等等)，二维码通信方式让私钥永不触网，彻底根绝了被黑客窃取的风险。库神冷钱包由两部分组成：硬件冷钱包及联网端APP。硬件冷钱包主要负责构造交易并对交易进行数字签名，联网端APP负责联网查询余额及广播发送交易。联网端APP上涉及到的都是公开透明的信息，无安全风险。
BitHD	支持BTC，ETH，ETH下的ERC20所有代币	产品以冷钱包+智能手表形式展现，遵守 BIP32/44/39 规范，自定义的数据传输协议，内置密码管理器Password Manager功能
BitLox	BTC、BCH、BTG	Bitlox可以与标准USB连接，钱包提供BIP32和BIP39种子短语。用户可以用比特币或Paypal购买该设备并可以在全球范围内发货。

钱包名称	支持币种	介绍
Bepal	ERC20 Token	Bepal的安全性原理是冷热分离 Bepal基于移动设备 Bepal会采用BIP44规则随机生成主、私钥和密语（助记词）

（2）国外

钱包名称	所在地点	支持币种	介绍
LedgerWallet	法国	比特币、以太坊、莱特币	2016年，Leger采用TEE（可信执行环境）和HSM（硬件安全模块）解决方案在B2B市场创建了自己的操作环境。
Trezor	美国	比特币、以太坊、莱特币	Trezor可以通过USB连接电脑并签署比特币交易，不需要允许计算机访问私人信息。与冷储存(cold storage)不同，TREZOR在连接到一个在线设备时是可以实现交易的。这意味着即便是在使用不安全的电脑的时候，使用比特币都是十分安全的。
KeepKey	美国	比特币、以太坊、莱特币	KeepKey采用独特的恢复机制，使用起来更加安全。这个机制让使用者只需要用12个单词就可以恢复。额外的安全机制意味着使用者不需要在设备上储存私匙。他们可以恢复他们的私匙和交易，接着在设备上消除记录。这是当前储存比特币最安全的方法。
OPendime	加拿大	比特币、以太坊、莱特币	比特币硬件钱包制造商OPendime是数字货币安全领域“技术领先”的公司之一，它隶属于Coinkite，Coinkite是一家位于加拿大的比特币企业，提供比特币和莱特币钱包，和支付终端的服务。支持法定货币包括美元、人民币、欧元、加元、英镑、波兰兹罗提、俄罗斯卢布、澳元、日元、巴西币、瑞典克朗等。OPendime是一个硬件钱包，它的私人密钥是在设备内部生成的，并且不会被任何人知道，甚至连你都不知道!OPendime多语言用户界面：中文、日本语、英语、葡萄牙语、法语、德语、法语为大家带来便利。
Digital Bitbox	瑞士	BTC、ETH，ETC和ERC20 Token代币、LTC	Digital Bitbox是一款即插即用的硬件比特币钱包，它采用冷储存技术为您提供最高级别的安全性

2.软件数字货币钱包提供商概括

（1）国内

钱包名称	支持币种	介绍
imToken	支持ETH以及以太坊ERC2.0标准的代币(比如EOS、DGD、SNT、QTUM)	是目前以太坊系列数字货币的必备钱包。imToken官方公布的数字是月活跃用户200万。这个数字据称已经超过了市场全部体量的50%。
以太钱包	比特币	是Bitcoin.org推荐的钱包；只支持主流币，其他小币种不支持，支持币种数量10+
Kcash	**支持BTC、ETH、ACT等上万个币种，并在对接公信宝等更多公链。**	累计安装用户超过50万；Kcash 通过对多种区块链资产类型的支持，提供了安全便捷、去中 心化的一站式管理方案。；Kcash 拥有一条高性能的区块链（简称 Kchain），支持图灵完备的 智能合约；Kcash 通过和银行、发卡机构（Visa，Master 等）及其代理机 构合作，共同发行数字货币银行卡。
Qbao	支持BTC、ETH、Qtum、QBT、墨链、菩提、Vevue、Medibloc 等数字货币的跨链多币种钱包功能。	跨链钱包；涵盖了与数字货币相关的社交沟通、币币交易、支付、行情、资讯、媒体、投资、知识付费、评级等功能，近期也推出了数字货币红包功能；Qbao 支持完全免费的支付网关、清结算功能。
OKLink	比特币、以太坊、莱特币	OKLink是新一代运营汇款应用或业务的最佳全球结算平台。通过提供连接网络来扩大全球业务覆盖范围，每天处理数千笔交易，为国际上具有前瞻性的业务提供服务。OKLink目前在亚洲，欧洲和美洲的40个国家提供支付，每周新增国际走廊。
Cobo钱包	Cobo 支持比特币、以太币、莱特币等数十种主要数字资产	Cobo目前是一款托管钱包，通过中心化的操作降低了用户的使用门槛。 Cobo用的是冷热端分离存储方案保证资产安全,并为签名定制了单独的硬件。

（2）国外

钱包名称	支持币种	介绍
Mist	ETH及ERC20 Token	Mist是一个全节点钱包（全节点钱包通俗的来说就是同步了全部的以太坊区块信息的钱包）
Parity	ETH及ERC20 Token	原以太坊基金会部分成员开发的钱包，功能强大，也是一个全节点钱包

钱包名称	支持币种	介绍
MyEtherWallet	ETH及ERC20 Token	在线轻钱包，生成的私钥由用户自己保管
MetaMask	ETH及ERC20 Token	MetaMask的钱包属性偏弱，更多的是起到使Chrome浏览器兼容以太坊网络的作用
BlockCypher	比特币、以太坊、莱特币、以太经典	Blockcypher是一家为大型机构如交易所和支付服务提供商，提供比特币钱包服务的公司，Blockcypher提供的最重要的服务就是他们所称的“置信因子”（Confidence Factor）技术。
BitGo	比特币、以太坊、莱特币	BitGo的技术解决了与区块链相关的最困难的安全性，合规性和架构问题，使企业能够将数字货币集成到现有的金融系统中。
Armory	比特币	Armory是一款开源的比特币管理客户端软件，提供比特币钱包管理、加密、离线交易等服务。自称是最安全的比特币钱包软件，使用的是“冷钱包”的原理，也就是将比特币资金的私钥储存在一台离线的电脑中，并且此电脑能将比特币信息通过打印在纸上的方式进行备份。
Jaxx	以太坊、比特币	同时兼容苹果IOS、安卓（Android）、笔记本电脑（Windows和Linux）、苹果MAC等操作系统，在谷歌浏览器（Chrome）和火狐浏览器（Firefox）上都可以使用。
CoinJar	比特币、以太坊、莱特币	CoinJar是一个全球性的融资公司，人们可以很容易地购买和花比特币和其他货币。我们拥有超过70000名客户，已经处理了超过1亿美元的交易。CoinJar提供简单的工具来管理数字货币。我们使用多因素身份验证（如密码加短信验证），以确保我们的客户的比特币是安全的，即使他们的密码被攻破。
Breadwallet	比特币、以太坊、莱特币	Breadwallet是苹果 iOS 系统上第一个去中心化数字加密货币钱包，其功能有使用户无需担心服务器宕机或造成的支付中断或其他一系列问题，同时利用去中心化网络，用户也不用担心自己的钱包被“黑客”窃取。
Xapo	比特币、以太坊、莱特币	Xapo是一款服务覆盖全球的在线比特币钱包，致力于使比特币的存取更加安全和便于使用。
Blockchain.info	BTC、ETH	Blockchain.info是比特币的最流行的比特币钱包和块探险家。截至2013年1月，该网站拥有超过11万注册用户。

3.加密数字货币钱包销售状况

由于软件钱包下载安装免费，以单次交易手续费作为盈利点。因此本段仅统计硬件钱包的销售状况。本文就硬件钱包在中国淘宝网上的销售状况进行了调研，表明Ledger和Trezor是最受用户欢迎的两大硬件钱包；国产的库神钱包价格最贵。

硬件钱包产品名称	价格（单位：元）	销量排名
库神二代	4288-4688	3
库神一代	2199	4
Ledger Nano S	898	1
TREZOR	758-988	2
Keepkey	1350-1399	5
Hyundai KasseHK-1000	1000-1399	10
Digital Bitbox	546	7
CoinWallet Bepal Pro	2980-3280	6
CoinWallet Opendime	380	8
CoinWallet Digital bitbox	549	9
Archos Safe-T mini	798	11

四、加密数字货币钱包存在的安全隐患

1.用户在钱包使用上的安全隐患

（1）将私钥托管给交易所

这也是大多数用户的做法，然而这种方式至少存在4个重大安全隐患：

❖ 服务商服务器被黑客攻击

每年都有大量的交易所被黑客攻击，导致数字资产大量丢失。由于加密数字货币的不可追溯、不可挂失、匿名的特性，一旦数字资产丢失，就再也不可能找回。

❖ 账户名和密码的安全隐患

大多数用户习惯性的使用同一个账户名和密码在不同的网站里面进行注册，如果这其中有任意一个网站被黑客攻击成功，那么这个网站的全部用户名和密码都可能被用于对交易所账户系统的登录攻击。黑客在获取对于用户托管账户的控制权限后，即可对数字资产进行转移。

❖ 浏览器的安全隐患

登录过程中的浏览器漏洞或浏览器的插件也会对账户的安全性产生影响。

❖ 网络传输的安全隐患

网络传输过程中的中间人攻击行为以及HTTPS证书劫持也是一种常见的安全风险。

（2）轻钱包模式下的安全风险

❖ 在云端生成私钥

这种模式下生成的私钥被云服务器托管，一旦这个服务器被攻击成功，那么数字资产有着极大的可能性被盗取。

❖ 在客户端生成私钥

如果钱包设计上的安全性不够高，将会产生系统性风险。

（3）输入方式上存在的风险

数字资产进行交易的时候需要输入一个PIN码来验证身份。采用内置的安全键盘，键盘使用乱序的方案，可以最大程度的保证用户输入密码时的安全性。因此，PIN码输入是否采用安全键盘是衡量一个金融类数字钱包产品安全性的关键考核点。

3. 用户在私钥保管时存在的安全隐患

某一用户将钱包私钥存储在不用的旧手机中，同时将其抄写在墙上，结果有一天手机被其家人置换成其他物品，墙也被粉刷了好几层，这名用户因此丢失了自己的数字资产。

另一个用户领取“糖果”时把私钥从钱包导出，并导入某个领糖果的网站，结果就是糖果没领成，领到了“炸弹”。

4. 钱包技术上的安全隐患

加密数字货币钱包在安全技术上需要进行全方面的考核和设计，避免私钥/助记词被盗窃或丢失。据猎豹移动发布的《全球数字货币钱包安全白皮书》统计，目前钱包技术上主要存在以下5个风险：

（1）运行环境的安全风险

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。加密数字货币钱包最核心的文件——私钥/助记词均存储在终端设备上。

因此，无论是PC端还是移动端，如果终端设备出现不安全的现象，对于私钥/助记词来说是有非常高的安全风险的。终端上运行环境的安全问题主要包括病毒软件、操作系统漏洞和硬件漏洞。

❖ 病毒软件

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衡量一个钱包是否安全的核心考核指标之一。

由于加密数字货币钱包的私钥/助记词不具备挂失能力，因此用户无法通过对账户进行冻结来降低损失。因此一旦被盗，数字资产将会丢失。

❖ 操作系统漏洞

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。黑客可以利用操作系统漏洞，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。

❖ 硬件漏洞

以CPU漏洞Meltdown（熔断）和Spectre（幽灵）为例，利用CPU架构设计上的瑕疵，可以直接通过CPU在处理机密信息时留下的Cache内容，读取到用户的私钥/助记词内容。

（2）网络传输的安全风险

数字钱包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。

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。

因此，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。

（3）钱包设计时文件存储方式的安全风险

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，发现即使是知名的数字钱包，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。

（4）应用自身的安全风险

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。

（5）数据备份的安全风险

如果移动应用能够被备份出来，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:allowBackup 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。

4.硬件钱包模式下的安全风险

硬件钱包一般涉及私钥的生成、存储、使用、运输、传递及销毁。而发生攻击主要环节：

（1）私钥生成阶段：取决于生成种子的随机数是否可靠、随机。

- 按照官方指定的方式生成私钥。
- 来自供应链端的威胁：用户未从官方正规渠道购买硬件钱包，那么从非官方授权渠道购买来的硬件钱包就有被动过手脚的可能。

（2）私钥使用阶段。

由于硬件钱包在使用时处于断网状态，相比网页钱包和客户端钱包安全一些，但也会遇到安全问题。

- 很多用户喜欢将硬件设备结合网页端或者客户端一起使用，因此黑客可将攻击点放在找零地址，如用各种各样的方式去替换或者篡改找零地址。
- 硬件钱包的固件也可能受到木马植入，或者被篡改，这种情况下也会直接导致私钥泄露。

目前，国外一些硬件钱包制造商如 Ledger Nano S相比Trezor 和 KeepKey，在硬件系统本身的安全上采用加密芯片，即多了一个专用的安全加密芯片，将系统程序和密钥存储分别存储在两个芯片上。

五、加密数字货币钱包未来展望

1.数字货币钱包发展趋势

（1）演变为去中心化交易所

钱包正在积极构建生态。一些钱包陆续上线了去中心化交易所，即用户在钱包内就可以进行数字货币交易，而不用再去传统的像火币、OKcoin这样的中心化交易所去充值、交易。

（2）数字货币类理财产品

越来越多的钱包推出数字货币理财功能，即将数字货币转入该品牌的钱包，可享受类似于银行理财产品获得的高额利息，一般利率在30%左右。

（3）具体场景下特定功能性钱包

据统计，全球移民总数大约是2亿，这2亿人大约有8亿亲属，如果加在一起，这个人群总数大约在10亿。这些移民在进行跨境转帐时，不仅周期比较久，而且在通过银行系统进行跨境转账的手续费一般在转账金额的8%—10%，有的国家甚至达到15%。然而，通过钱包转账数字货币后再兑换法币，可以比通过银行系统转账减少一多半的手续费。据测算，全球如果通过这种方式转账，手续费可以降低到3%以下。

2.不断升级的交易所的安全系统架构

同时，也可以看到交易所在资金安全和信息安全领域的高度重视。目前，交易所安全系统架构主要包括冷热钱包隔离、多重签名、两步验证、 密钥保存机制、外部密码审核机制等。目前几乎所有的交易所都采用冷热钱包隔离机制，将95%的币值储存在冷钱包中，只预留5%的货币用于提现充值。冷钱包中密钥完全离线，因此黑客无法获取。以下是Ledger公司为交易所设计的基于HSM的安全架构：