# 钱包生态研究报告

2018 年 9 月

TokenClub 研究院

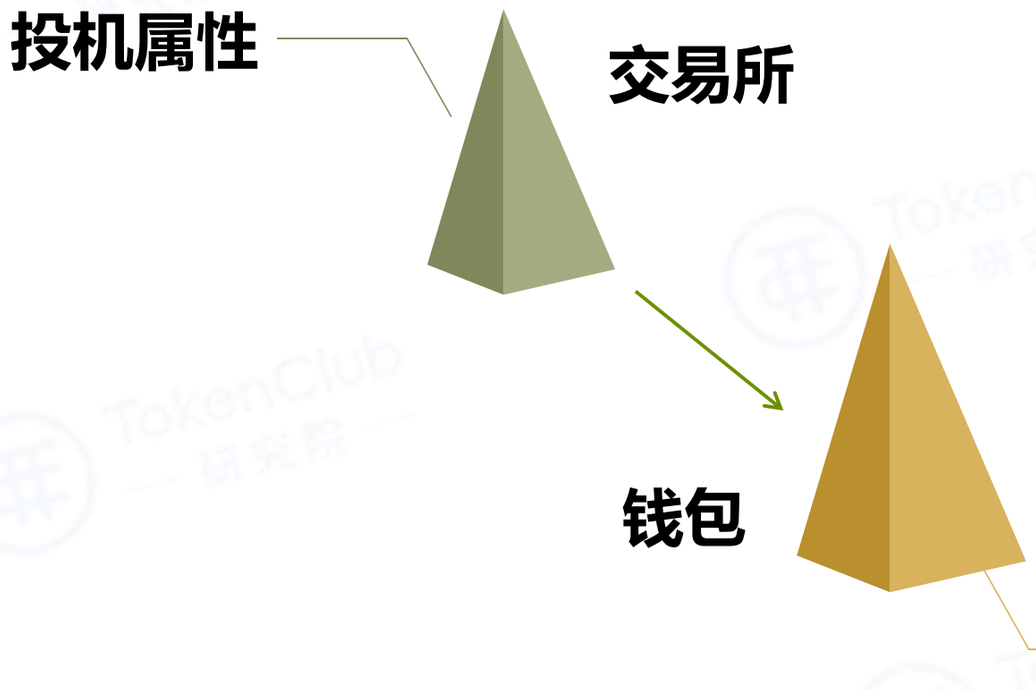
# 目录

# 1. 行业综述

关于数字货币钱包，需要澄清的是它并不是用来装钱的，也不是用来装比特币、以太坊。从技术上来说钱包就是用来存放私钥的工具，拥有了私钥就意味着你拥有了所对应地址上数字货币的支配权。

## 1.1 行业背景

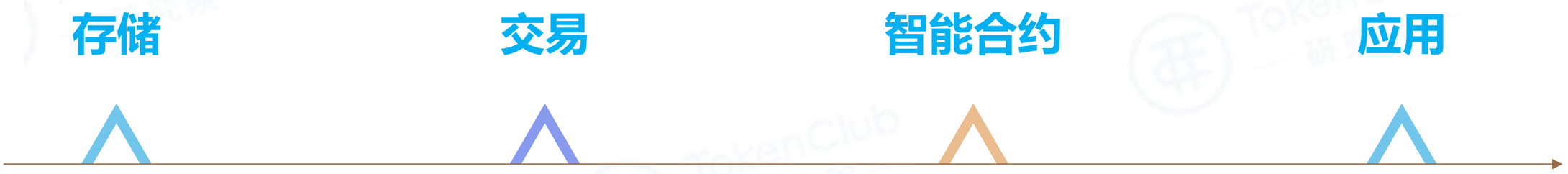
比特币的诞生拉开了加密数字货币的序幕，从早期的极客玩物到现在价值万亿市值的生态，数字货币作为一个新兴的投资标的受到越来越多人的关注与青睐。整个 2017 年，数字货币迎来了一波超级牛市，比特币整年达到了 13 倍的涨幅，其他币种甚至出现了所谓的百倍币、千倍币，可以说数字货币的投机属性在这一年得到了充分的释放。



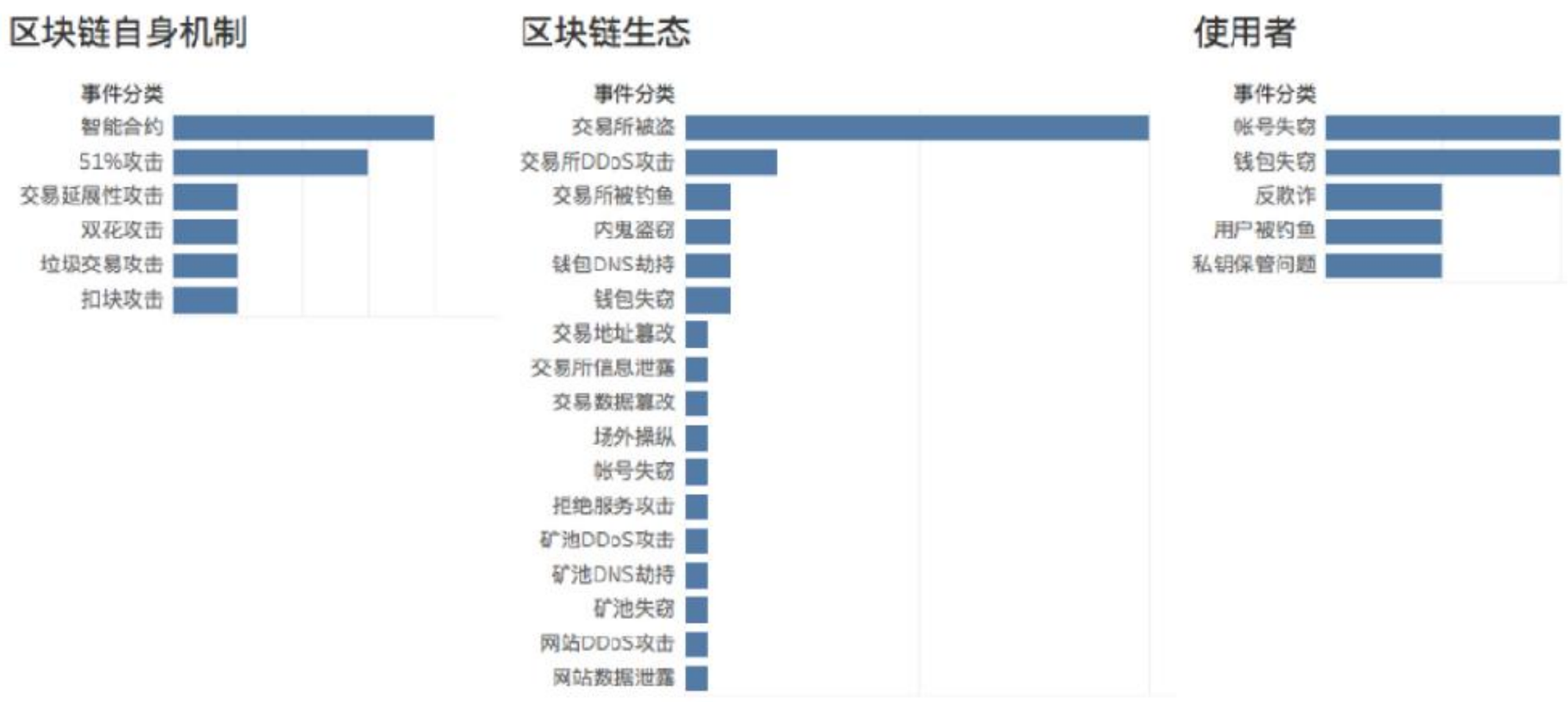

上百万倍的涨幅造就了一个又一个的财富神话，比特币也因此被人广为诟病，称它为史上最大的金融泡沫。毕竟作为一项投资标的，要想长久持续下去必然要凭

借使用价值作为依托，而不仅仅局限在交易所中相互炒作。钱包作为数字货币应用的载体，与其相关的基础设施的建设对于数字货币从投机转向实际应用尤为重要。

另一方面，区块链生态的扩大，围绕着数字货币存储、交易、智能合约、应用所搭建的场景愈发重要，加密货币的安全性对整个市场未来可持续发展具有深远影响。



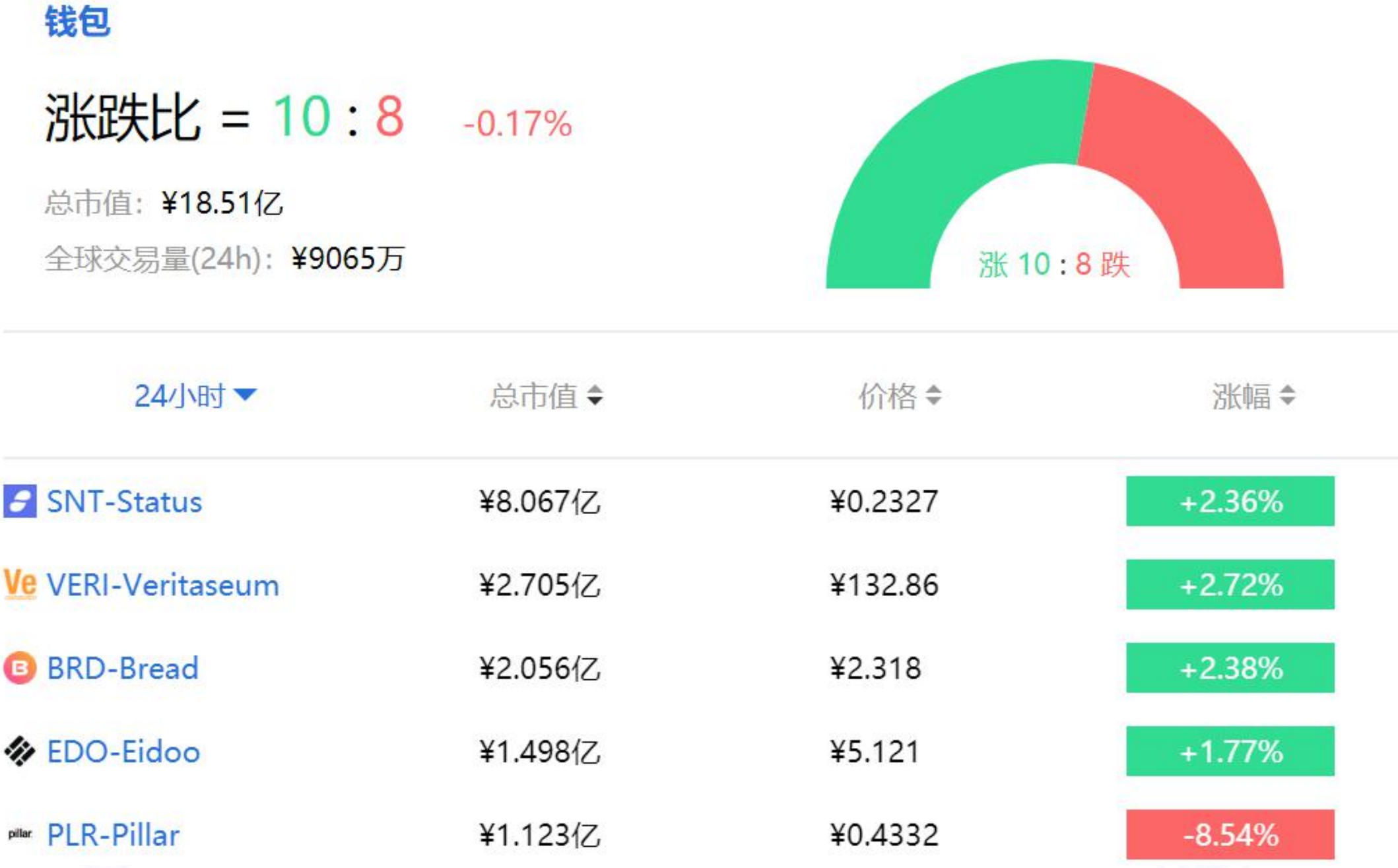

但是从比特币诞生以来，由于私钥保管不当所造成的钱包失窃现象屡见不鲜，其中影响最深的当属 Mt.Gox 交易所被盗一事，至今仍在影响着币圈价格的走势。




根据知道创宇所统计的数据显示，在区块链生态与使用者中所发生的安全事件，

交易所被盗与钱包失窃占有最大的比重，而交易所被盗也是由钱包私钥保管不当所致。因此，打造安全可靠方便易用的数字资产钱包至关重要。

## 1.2 数字货币钱包发展现状

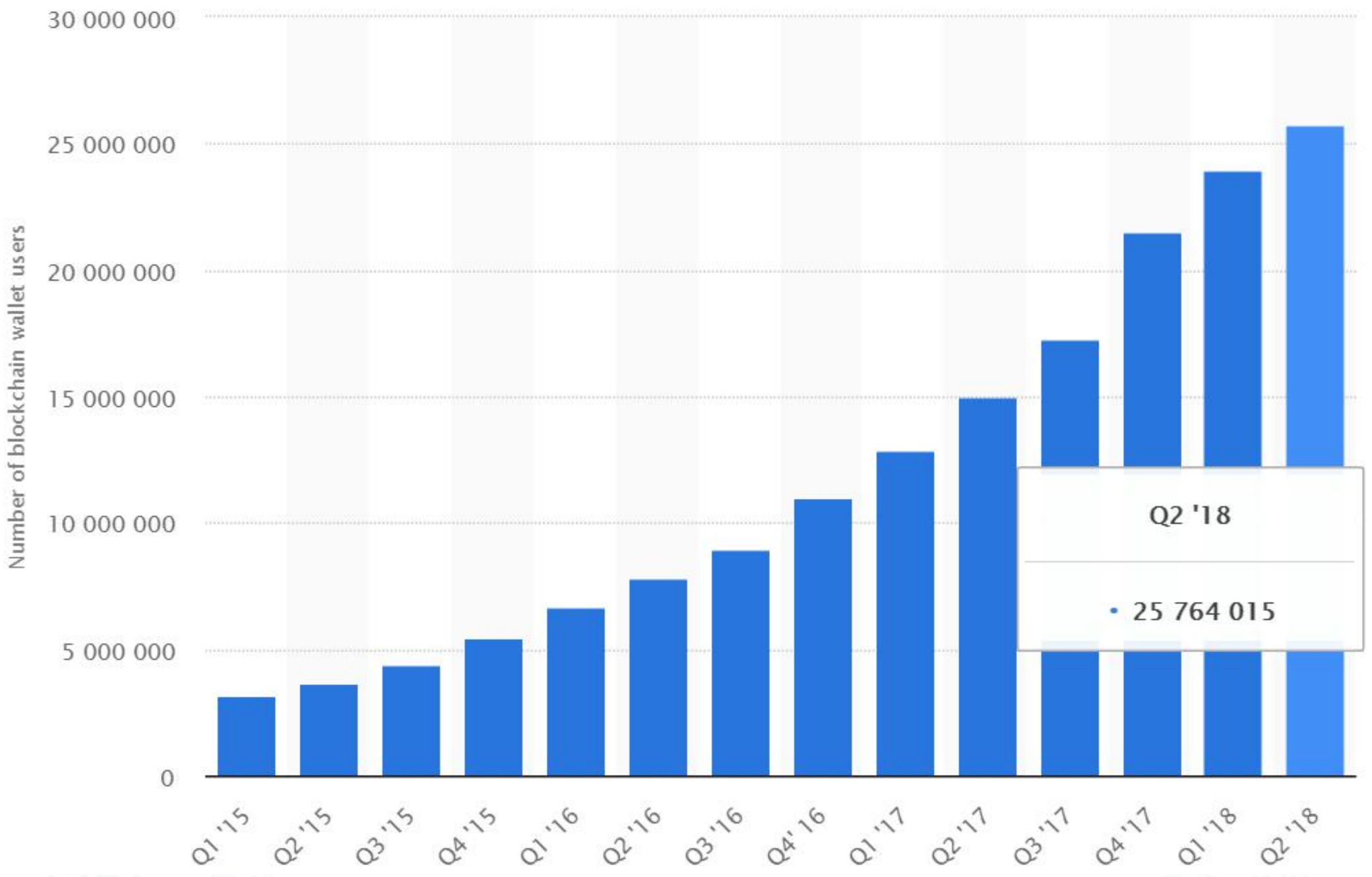



根据 TokenClub 数据显示，目前收录的钱包相关的项目共 18 个，总市值达 18.15 亿元，24 小时全球交易量为 9065 万，这与整个加密货币领域目前 1.38 万亿市值相去甚远。主要是因为目前大多数钱包商都没有采取代币融资的方式运作，很多与钱包相关的项目都不是直接去开发钱包，而是搭建具有社交平台属性的钱包，或为钱包提供技术支持与服务。

不过，根据 Statista 提供的统计图显示，自 2015 年至 2018 年第二季度，全球

连锁钱包用户数量仍在稳步上升中，已从 317 万上升到 2576 万人，较上年同比增长 66%。

**2015年第一季度至2018年第二季度全球连锁钱包用户数量**



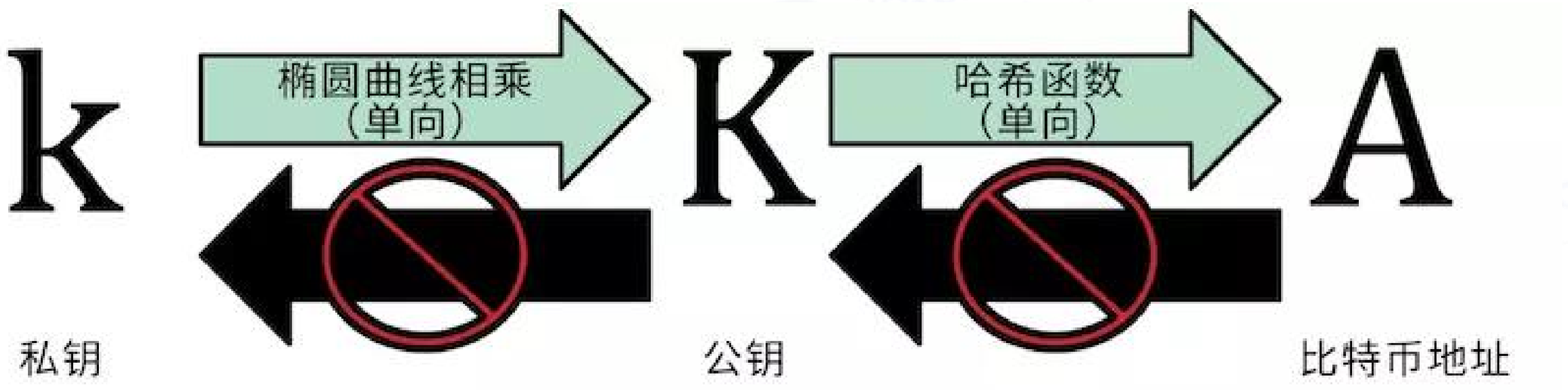

Statista 统计的数据主要来自于大的连锁钱包商中用户的数量，实际上自 2017 年中旬以来，很多团队开始着手钱包的开发，全球钱包商已达数百家。因此，实际钱包的用户要远高于这一统计数据。钱包，作为数字货币交易的入口，谁成为这个市场的佼佼者，谁就能成为区块链世界的支付宝。

# 2. 钱包技术原理

钱包是作为提供用户界面的应用程序，起到控制用户访问权限，管理密钥和地址，跟踪余额以及创建和签署交易等功能。从技术方面来看，“钱包”是指用于存储和管理用户密钥的数据结构。交易信息被记录在区块链中，用户通过与他们的钱包中的密钥签署交易来控制网络上的数字货币。本章以比特币为例，介绍数字货币钱包中各项技术机理。

## 2.1 私钥、公钥与地址

在比特币中，经常出现三个词：私钥、公钥和地址，他们经常被一同提起。一个比特币钱包中包含一系列的密钥对，每个密钥对包括一个私钥和一个公钥。私钥是一个数字，通常是随机选出的。有了私钥，我们就可以使用椭圆曲线乘法这个单向加密函数产生一个公钥。有了公钥，我们就可以使用一个单向加密哈希函数生成比特币地址。三者的产生关系大致入下图所示。




通过非对称密码学的适用性可以使得任何人都可以验证每笔交易的每个签名，同

时确保只有私钥的所有者可以产生有效的签名。

## 2.1.1 私钥

私钥是对一个比特币地址拥有取钱权限的代表，掌握了私钥就掌握了其对应地址上比特币的支配权。私钥可以算出公钥，公钥可以再算出比特币地址。每次交易的时候，付款方必须出具私钥，以及私钥产生的签名，每次交易签名不同，但是由同一个私钥产生。通常我们所看到的私钥是下面这样一串字符：

**比特币私钥（例）**

**5KYZdUEo39z3FPrtuX2QbbwGnNP5zTd7yyr2SC1j299sBCnWjss**

支持比特币协议的应用都可以正确把这段字符串转换成比特币的私钥，再转换出公钥，再得到一个地址，如果该地址上面有对应的比特币，就可以使用这个私钥花费上面的比特币。

私钥本质上是一个随机数，由 32 个 byte 组成的数组，1 个 byte 等于 8 位二进制，一个二进制只有两个值 0 或者 1。所以私钥的总数接近 $2^{256}$ 个，这个数量已经超过了宇宙中原子的总数，想要遍历所有的私钥，耗尽整个太阳的能量也是不可能的。私钥的安全是由数学保证，要想通过技术手段攻破，或许要等量子计算机技术的成熟。

## 2.1.2 公钥

通过椭圆曲线乘法可以从私钥计算得到公钥，这是不可逆转的过程：K = k * G 。其中 k 是私钥，G 是被称为生成点的常数点，而 K 是所得公钥。其反向运算，被称为“寻找离散对数”——已知公钥 K 来求出私钥 k——是非常困难的，就像去试验所有可能的 k 值，即暴力搜索。因此私钥的所有者可以容易地创建公钥，然后与世界共享，知道没有人可以从公钥中反转函数并计算出私钥。这个数学技巧成为证明比特币资金所有权的不可伪造和安全的数字签名的基础。

**比特币公钥（例）**

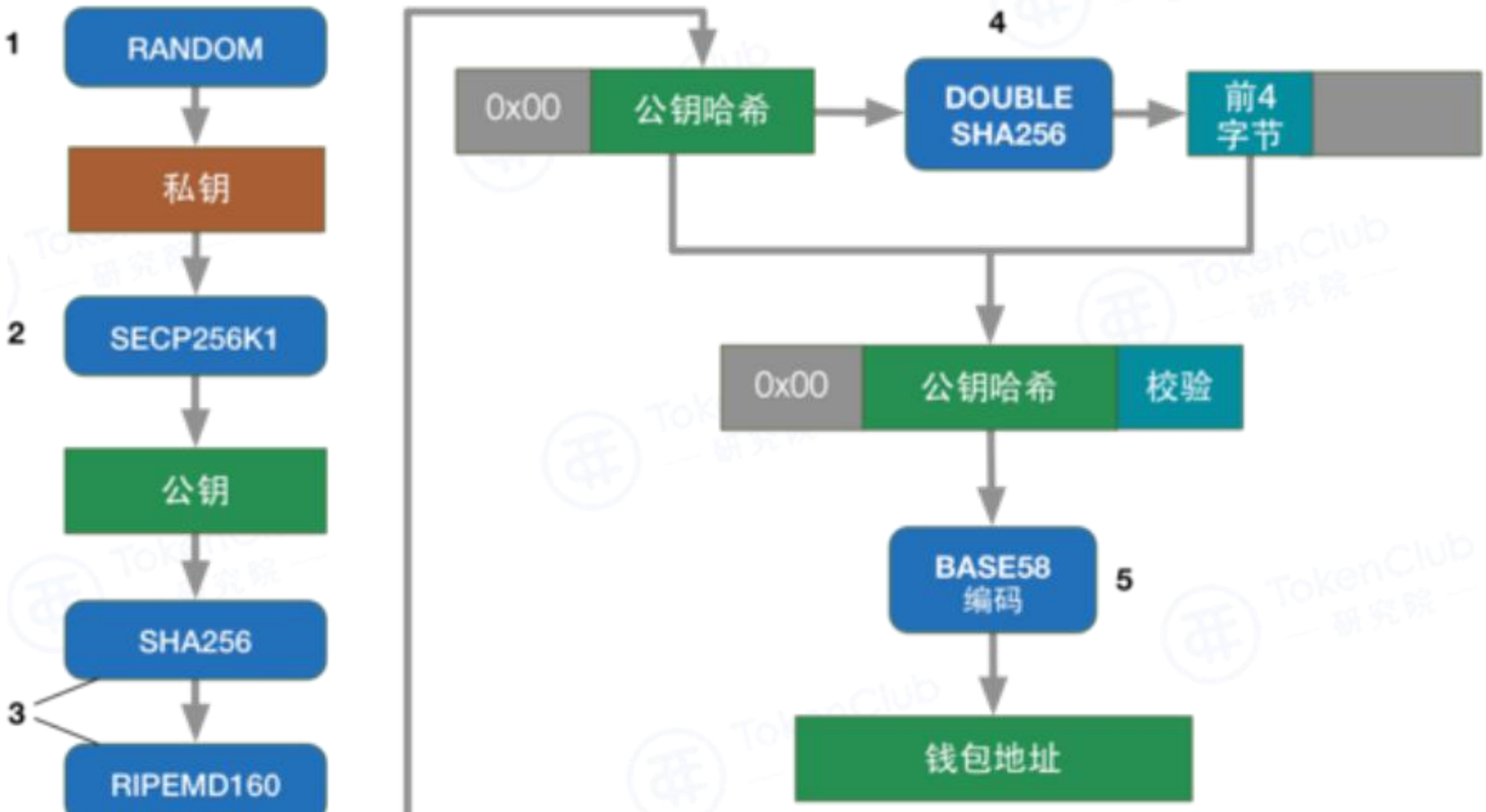
**04a34b99f22c790c4e36b2b3c2c35a36db06226e41c692fc82b8b56ac1c540c5bd5b8dec5235a0fa8722476c7709c02559e3aa73aa03918ba2d492eea75abea235**

公钥是用来验证私钥的签名，一般我们很少会看到公钥，使用私钥签名交易之后，会把自己的公钥一起和交易发送出去，这样对于一个完整的交易来说，他就使用交易里包含的公钥验证私钥的签名是否正确。

## 2.1.3 地址

比特币地址是一个由数字和字母组成的字符串，可以与任何想给你比特币的人分享。在交易中，比特币地址通常以收款方出现。如果把比特币交易比作一张支票，

比特币地址就是收款人，也就是我们要写入收款人一栏的内容。支票不需要指定一个特定的账户，而是用一个抽象的名字作为收款人，这使它成为一种相当灵活的支付工具。与此类似，比特币地址使用类似的抽象，也使比特币交易变得很灵活。



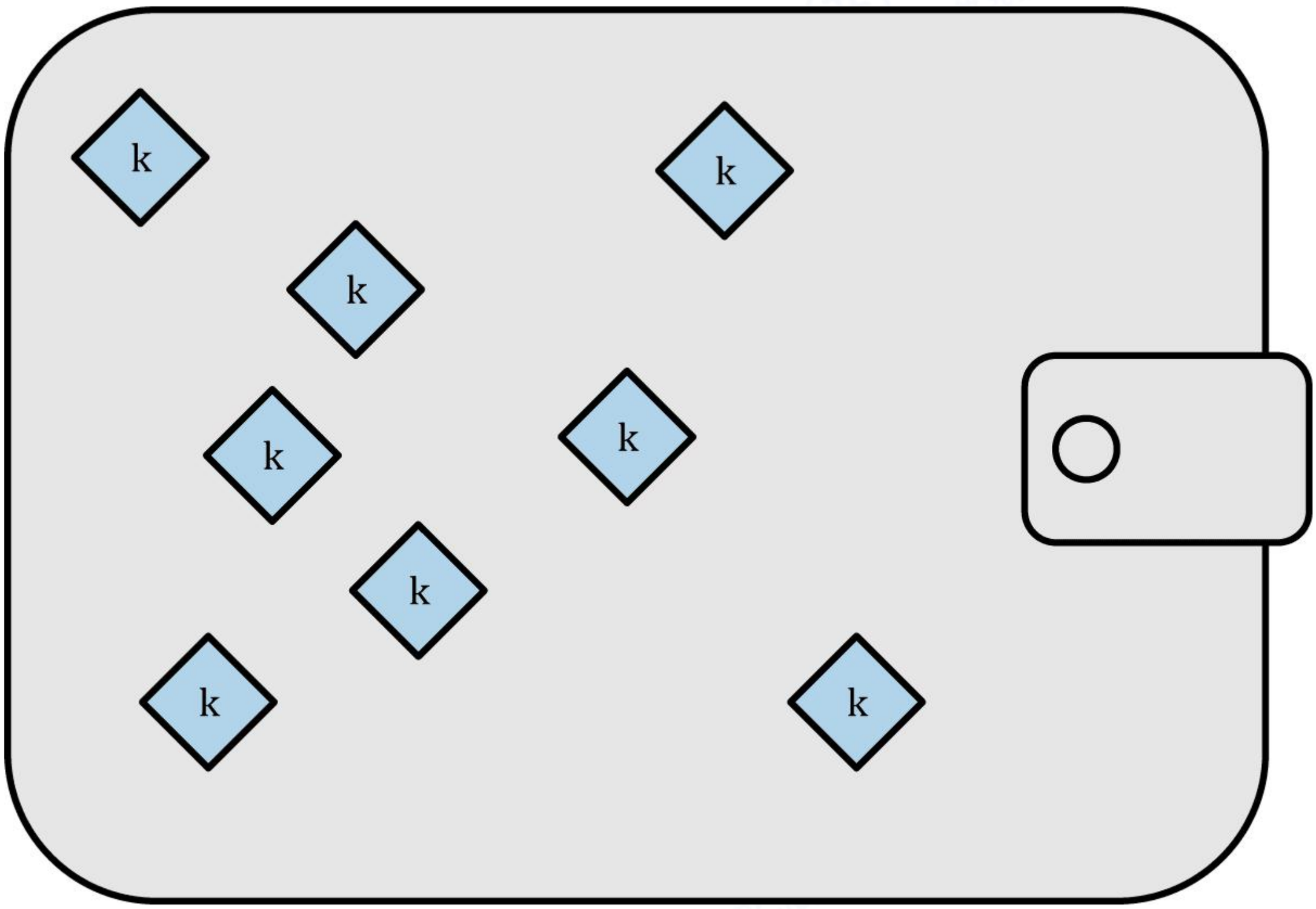

地址的产生过程大致如上图所示，就比特币而言，一个私钥可以对应多个比特币地址。通常我们使用钱包转账是从一个地址转到另一个地址，也可以扫描二维码进行，像 EOS 则是账户之间的互转。

# 2.2 钱包技术概述

根据多个秘钥是否相关联，可以分为两种不同类型的钱包。第一种是非确定性钱包，其中每个密钥都是从随机数独立生成的，密钥彼此无关。另一种是确定性钱包，其中所有的密钥都是从一个主密钥派生出来，这个主密钥即为种子（seed）。该类型钱包中所有密钥都相互关联，如果有原始种子，则可以再次生成全部密钥。确定性钱包中使用了许多不同的密钥推导方法，最常用的推导方法是使用树状结构，称为分级确定性钱包或 HD 钱包。

## 2.2.1 非确定性（随机）钱包

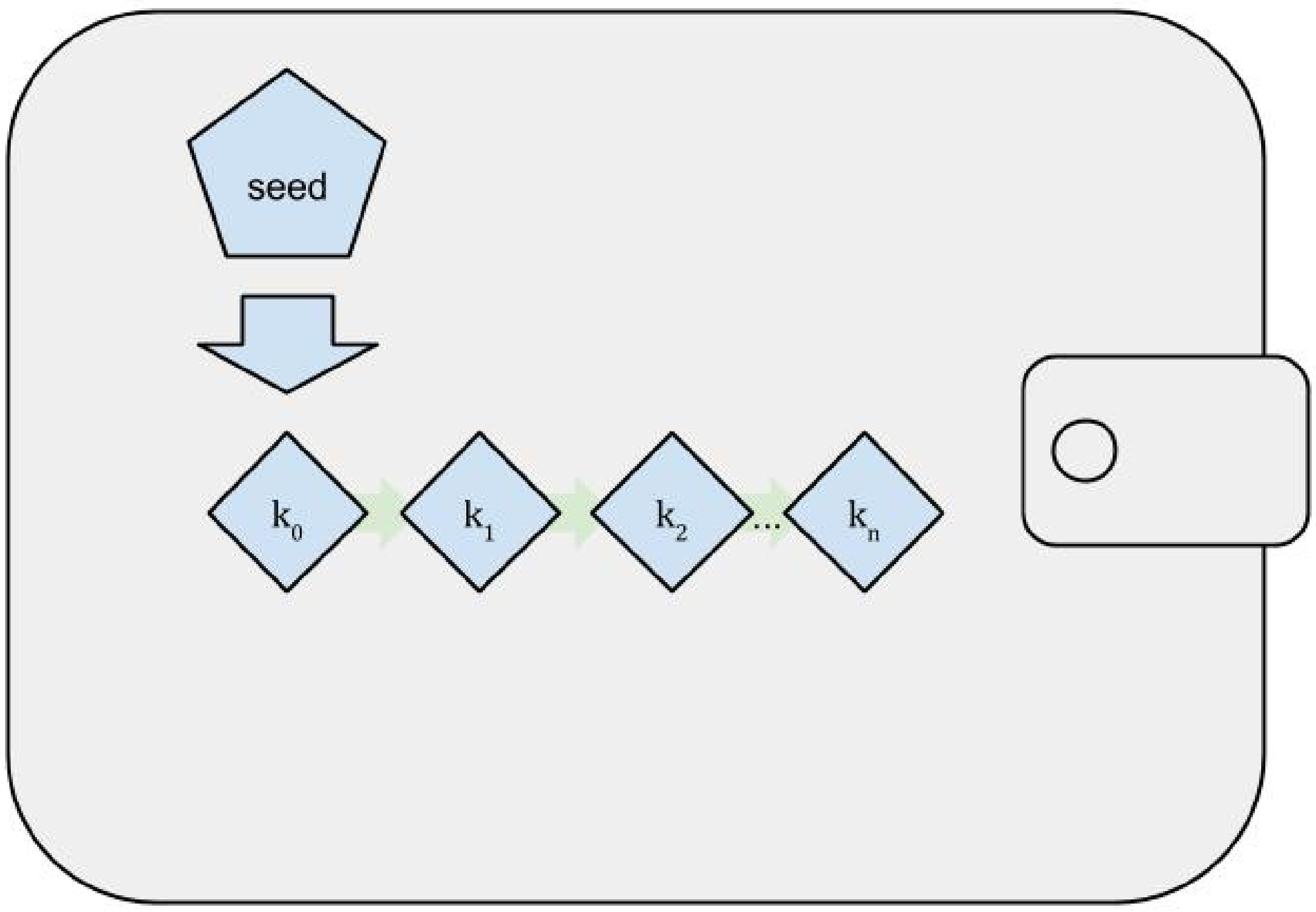
在最早的一批比特币客户端中（ Bitcoin Core，现在称作比特币核心客户端），钱包只是随机生成的私钥集合，这种类型的钱包被称作零型非确定钱包。从最开始就生成足够多的私钥并且每个密钥只使用一次。这种钱包现在正在被确定性钱包替换，因为它们难以管理、备份以及导入。随机密钥的缺点就是如果你生成很多私钥，你必须保存它们所有的副本。这就意味着这个钱包必须被经常性 地备份。每一个密钥都必须备份，否则一旦钱包不可访问时，钱包所控制的资金就付之东流。下图展示的是一个非确定性钱包，其含有的随机密钥是个松散的集合。




这种情况直接与避免地址重复使用的原则相冲突——每个比特币地址只能用一次交易。地址重复使用将多个交易和地址关联在一起，这会减少隐私。当你想避免重复使用地址时，零型非确定性钱包并不是好的选择，因为你要创造过多的私钥并且要保存它们。虽然比特币核心客户端包含零型钱包，但比特币的核心开发者并不鼓励大家使用。

## 2.2.2 确定性（种子）钱包

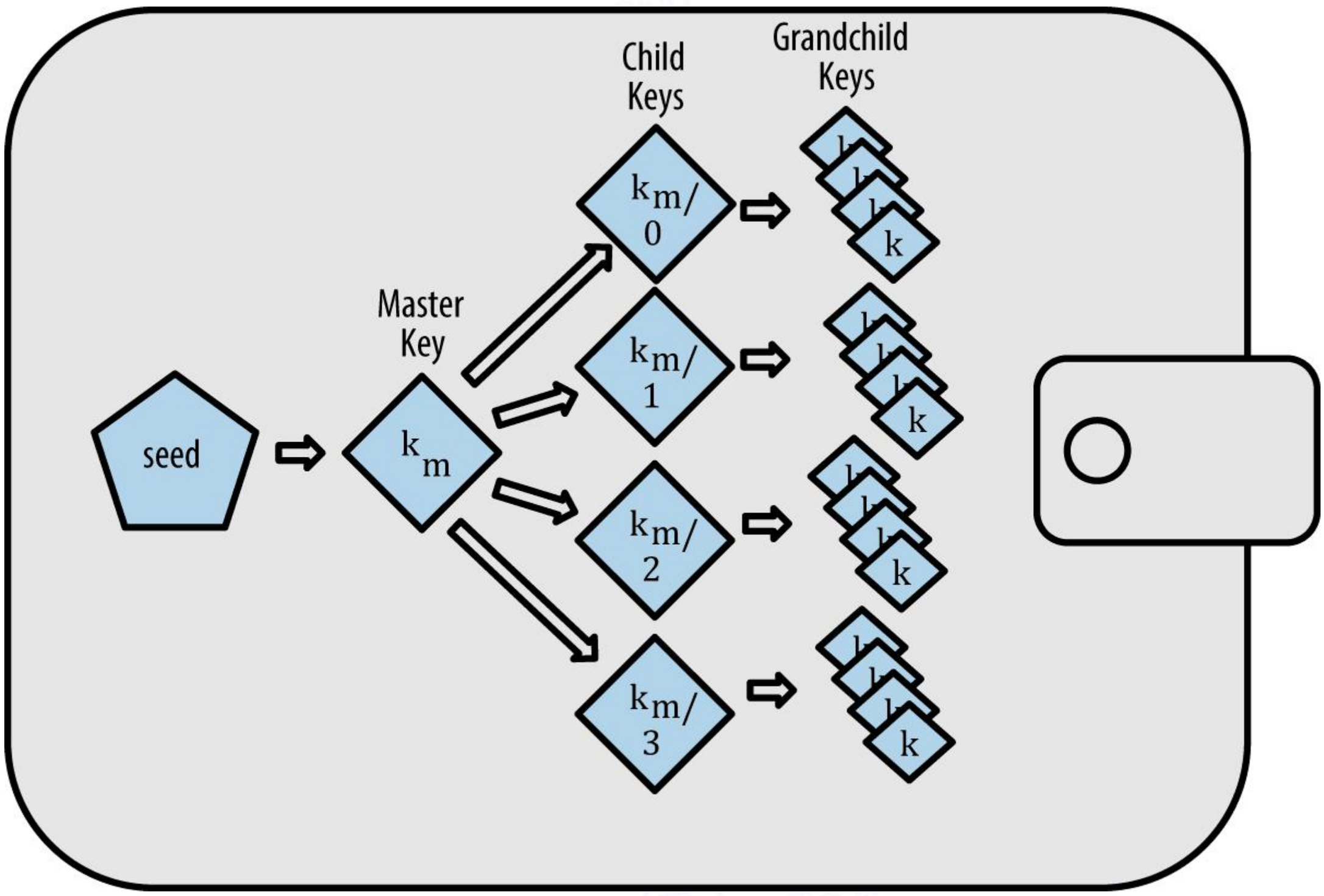
确定性，或者“种子”钱包包含通过使用单项离散函数而可从公共的种子生成的私钥。种子是随机生成的数字。这个数字也含有比如索引号码或者可生成私钥的“链码”。在确定性钱包中，种子足够恢复所有的已经产生的私钥，所以只用在初始创建时的一个简单备份就足以搞定。并且种子也足够让钱包导入或者导出。这就很容易允许使用者的私钥在钱包之间轻松转移。




确定性钱包逻辑图

确定性钱包的最高级形式是通过 BIP0032 标准定义的 HD 钱包。HD 钱包包含以树状结构衍生的密钥，使得父密钥可以衍生一系列子密钥，每个子密钥又可以衍生出一系列孙密钥，以此类推，无限衍生。

相比较随机（不确定性）密钥，HD 钱包有两个主要的优势。第一，树状结构可以被用来表达额外的组织含义。比如当一个特定分支的子密钥被用来接收交易收入并且有另一个分支的子密钥用来负责支付花费。不同分支的密钥都可以被用在企业环境中，这就可以支配不同的分支部门、子公司、具体功能以及会计类别。




HD 钱包树状结构图

HD 钱包的第二个好处就是它可以允许让使用者去建立一个公共密钥的序列而不需要访问相对应的私钥。这可允许 HD 钱包在不安全的服务器中使用或者在每笔交易中发行不同的公共钥匙。公共钥匙不需要被预先加载或者提前衍生，而在服务器中不需要可用来支付的私钥。

## 2.2.3 种子与助记词

HD 钱包具有管理多个密钥和地址的强大机制。由一系列英文单词生成种子是个标准化的方法，这样易于在钱包中转移、导出和导入，如果 HD 钱包与这种方法相结合，将会更加有用。 这些英文单词被称为助记词，标准由 BIP-39 定义。 今天，大多数比特币钱包（以及其他加密货币的钱包）使用此标准，并可以使用可互操作的助记词导入和导出种子进行备份和恢复。

**16 进制表示的种子**

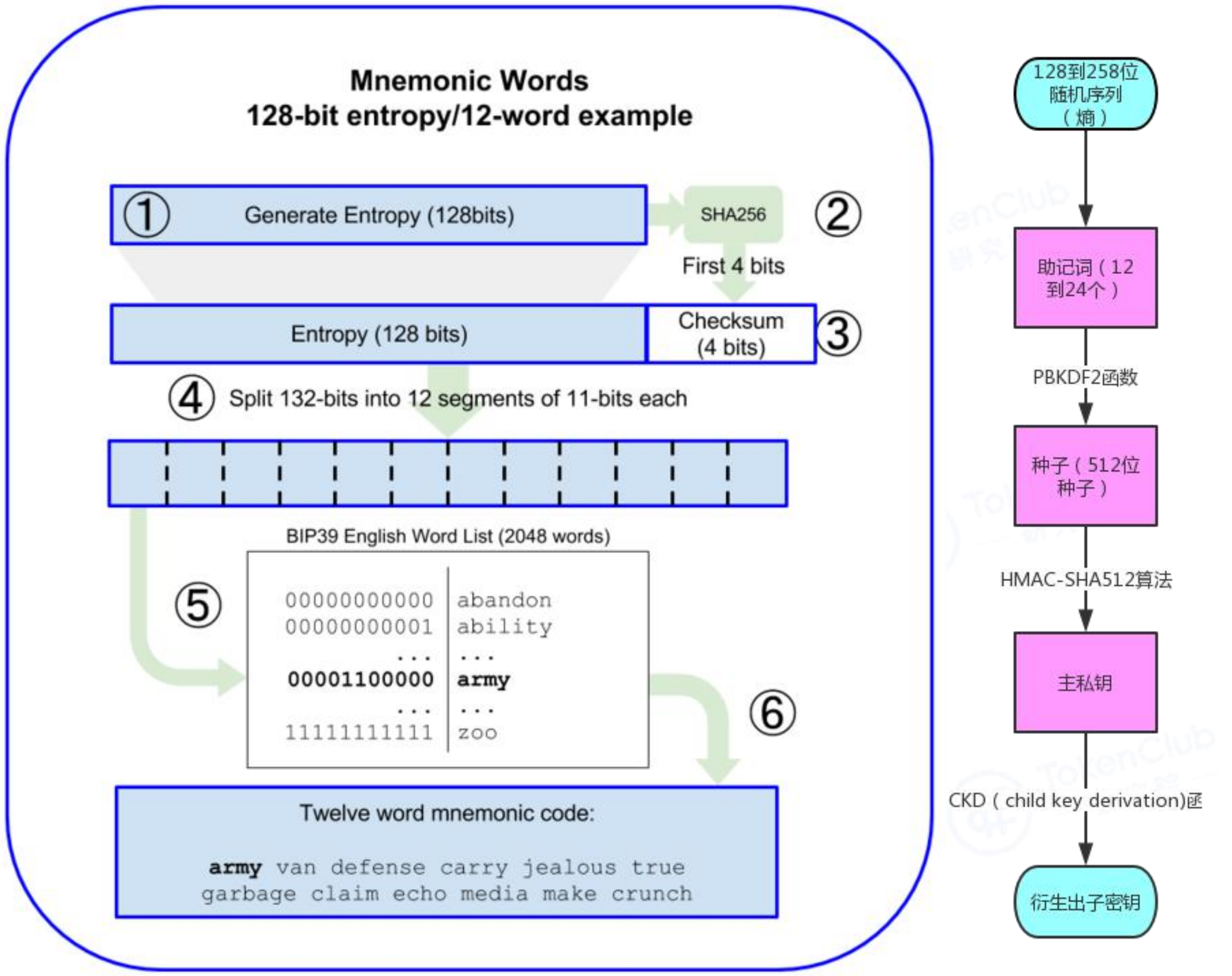
**0C1E24E5917779D297E14D45F14E1A1A**

**助记词表示的种子**

**army market defense carry jealous true garbage claim echo media make crunch**

由于私钥长度达 64 位，可读性较弱，手抄比较麻烦，而备份到电脑中有被盗的风险。因此聪明的钱包商发明了助记词，利用特殊的算法可以将 64 位长度的私钥转换成十几个甚至二十几个英文单词。

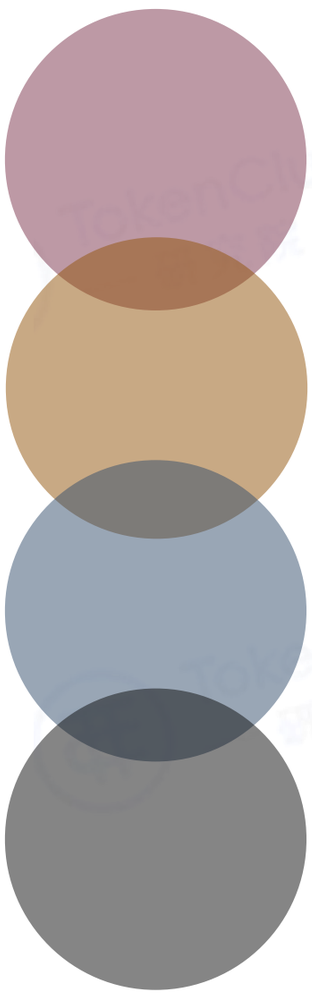
生成原理：随机生成一个 128 到 258 位的数字，叫做熵；熵通过 SHA256 哈希得一个值，取前面的几位（熵长/32），记为 y；熵和 y 组成一个新的序列，将新序列以 11 位为一部分，已经预先定义 2048 个单词的字典做对应，生成的有顺序的单词组就是助记词。




私钥和助记词可以相互转换，因此助记词是私钥的另一种体现。目前很多钱包已经采用了助记词备份的方式，很多用户因不规范的助记词保存方式比如将助记词截图或保存到电脑中，遭遇了钱包被盗的事件。正确的保存方式是将助记词抄写到纸上，保存起来；或者可以通过一些加密手段，将助记词拆分后保存到不同地方，增强安全性。

## 2.2.4 钱包技术标准

由于比特币钱包技术已经成熟，出现了一些常见的行业标准，使得比特币钱包具备广泛互操作，易于使用，安全和灵活的特性。这些常用的标准是：



**助记码：基于 BIP-39**

**HD 钱包：基于 BIP32**

**多用途钱包结构：基于 BIP-43**

**多币种和多账户钱包：基于 BIP-44**

这些标准可能会随着发展而改变或过时，但是现在它们形成了一套互锁技术，这些技术已成为比特币的事实上的钱包标准。这些标准已被广泛的软件和硬件比特币钱包采用，使所有这些钱包互操作。用户可以导出在其中一个钱包上生成的助记符，并将其导入另一个钱包，实现恢复所有交易，密钥和地址。

# 3. 钱包分类

钱包作为私钥的存放场所，以及支配个人所有的数字资产的工具，其功能不仅仅局限于数字货币的存储与交易，更是用户去参与区块链生态的入口。针对用户的需求不同，钱包商们开发出了各种不同种类与功能的钱包。

## 3.1 中心化钱包与去中心化钱包

根据私钥是否为资产所有人持有，钱包分为中心化钱包与去中心化钱包。顾名思义，去中心化钱包即私钥由个人所持有，而中心化钱包则是资产由中心化机构托管，私钥非个人持有的钱包。


### 3.1.1 中心化钱包

中心化钱包的私钥通常由钱包商控制，有些情况下多个用户的资产存储在一个地址中。当用户发起交易指令时，是由钱包方控制私钥向目标地址发送交易。因此，中心化钱包引入了第三方信用机制，其交易属性也并非一个点对点的电子现金系统。

中心化钱包其实比较常见，种类也有很多，像专门为了满足中心化的一些优点而做的钱包应用、交易所、一些数字货币中心化应用的 APP 等都是中心化的钱包。


以交易所为例，目前大多数交易所都是中心化形态，每一个交易所实际上都相当于一款钱包，当我们充币时，实际上是将数字货币冲到交易所持有私钥的地址上，交易所再在账户中予以显示出来。我们在交易所中交易的记录依靠的是交易所自有的服务器进行记录于存储，买入账户增加，卖出则账户减少，并不会发生链上的交易。


交易所钱包界面

当我们提币时，在交易所上提交申请后等待交易所转出。交易所从自己的钱包中划出指定金额的币转入到你申请的地址，随即扣减你的账户。当然了，如果我们

充入的币被交易所移作它用或者流动钱包自己不足、技术出现问题等原因，就会导致提币缓慢、甚至无法提币卡币的问题。

中心化钱包的优点在于私钥丢了可以找回，作为平台方尤其是大的交易所，通常会将安全措施做的不错，即便发生盗笔行为或许平台也会赔付。此外，在平台中进行链下交易，可以做到秒到账 0 手续费，而且像币信这种钱包，在比特币拥堵的时候，通过聚合交易的方式降低了用户的手续费。

当然，它也存在一定的缺点，即你的资金安全完全取决于平台的信用，从技术上钱包商可以将你的资产挪用甚至跑路。另外，在提交链上交易的申请时，需要经过钱包商的同意才能予以执行。

常见的中心化钱包有：Coinbase、币信、Blockchain 等。

### 3.1.2 去中心化钱包

去中心化钱包是指私钥由数字资产所有人持有，钱包商不会（实际不能）持有私钥以及操纵钱包中数字资产的交易的钱包。去中心化钱包本身不对交易数据进行存储，它只负责把处理好的支付信息发布出去，以及读取区块链上的交易记录等信息，同时把余额显示在应用的界面上。

去中心化钱包在数字货币领域用途更为广泛，它不仅是资产储存的场所，可以说每一款 Dapp 应用都需要去中心化钱包的运行才可以进行。相较于中心化钱包，去中心化钱包去掉了第三方中介机制，每一笔交易都是由持有人亲自操作，并且记录在链。

去中心化钱包的优点则在于你的资产完全交由自己控制，资产信息记录在链，除非掌控私钥，没有人能够拿走。其缺点主要是私钥不容易保管，容易被盗或者丢失。另外，去中心化钱包并不是绝对的安全，在生成私钥的过程中，可能钱包的载体比如手机或者钱包商会留有暗门，盗窃私钥。

常见的去中心化钱包包括：Imtoken、Bitpie、Jaxx 等。

## 3.2 热钱包

热钱包指的是联网的钱包，因为无时无刻连上网络，所以可以便利的进行转入和转出资产。它包括全节点钱包与轻钱包，他们都是去中心化的钱包，其区别在于是否保存所有的区块链数据。


### 3.2.1 全节点钱包

全节点钱包不仅保存私钥，也保存了全部的区块链数据，这样就可以在本地直接验证交易数据的有效性。全节点钱包不仅具有钱包的交易功能，更是行使了对于区块链数据真实性的监督权，像挖矿节点更是可以直接参与记账。对于一条区块链来说，全节点越多，账本的篡改难度越大，去中心化程度也就越高。

全节点钱包的优点在于更好的隐私性以及更快验证交易信息。但它的缺点也比较

明显，比如占用了很多硬盘空间，每次使用前需要同步数据，新手体验不够好以及不支持多种数字资产。


最常见的全节点钱包是 Bitcoin Core，该钱包可以到比特币官方论坛 Bitcoin.org 上下载。

## 3.2.2 轻钱包

轻钱包并不保存比特币网络的全部数据，只保存与自己相关的数据，所以体积很小，可以保存在手机、电脑、网页等地方。

新钱包是目前数字货币用户应用最为广泛的钱包，这主要得益于它的优点：用户体验感好，体积小不占用空间以及很多轻钱包支持多种数字资产并且在此基础上

演化出了很多功能。缺点就是验证交易会稍微慢一些，但是并不影响正常使用。

## 3.3 离线钱包（冷钱包）

冷钱包是指不联网的钱包，它不需要联网也可以发送交易。其技术原理在于因为钱包在处理支付信息并不需要联网进行，而处理支付信息这一步骤需要动用储存在本地设备的加密信息，私钥也是一个钱包最重要的信息。而进行加密后的数据传输、读取交易信息这种不会涉及到安全问题的步骤则交给联网的设备来做，通过联网的设备软件扫描冷钱包产生的二维码或者 U 盘传递数据获得交易信息后负责发送出去，这样一笔交易就完成了。

通常来说，冷钱包是安全性能最高的钱包，只要私钥永远不联网，就无需担心黑客通过网络进行盗窃。目前的冷钱包主要包括纸钱包、脑钱包和硬件钱包。

### 3.3.1 纸钱包

纸钱包顾名思义就是将比特币私钥记录在一张纸上的钱包，这张纸既可以打印出来也可以存放到电脑中。纸钱包目前被认为是最安全的钱包，这主要取决于它的生成方式：

- 准备一台电脑，永远不上网，一张纸，一根笔。
- 从其他联网的电脑中，登陆 https://bitcoin.org/en/bitcoin-core/，将 Bitcoin Core 下载到 U 盘中，然后拷贝到不联网的电脑。
- 运行 Bitcoin Core，在菜单中找到“文件-加密钱包”，给钱包加密，设置一个自己能记得住的简单密码即可。

- 然后 Bitcoin core 会自动关闭。你再重启，重启后你生成一个（或几个）新地址，使用记事本记下这个地址。
- 在 bitcoin core 的“帮助——调试窗口——控制台”的命令行里输入下面内容：walletpassphrase abc123 600 后回车。
- 在 bitcoin core 的“帮助——调试窗口——控制台”的命令行里输入下面内容：dumprivkey+你记录的地址。回车后即可获得该地址中所对应的私钥。
- 将私钥抄在纸上，保存好。

由于纸钱包的私钥是在无网状态下生成并且通过物理介质保存，因此不存在因互联网被盗的风险，接下来就是如何保管好自己的私钥了。如果想在钱包中存入比特币，那么可以通过向记录的地址发送交易，如果想要转移或使用比特币，那么重新导入私钥即可。

纸钱包最大的优点在于安全，但是其创建与使用非常之不便。

### 3.3.2 脑钱包

脑钱包的原理与纸钱包类似，其区别在于脑钱包的私钥是记录在脑海中，用户可以通过特定的加密技术将私钥与地址设置成密码，密码记在脑海中。可以通过记忆中的密码获取私钥，并且使用比特币。

# 3.3.3 硬件钱包

硬件钱包是指将私钥存储在离线硬盘里，隔绝网络。

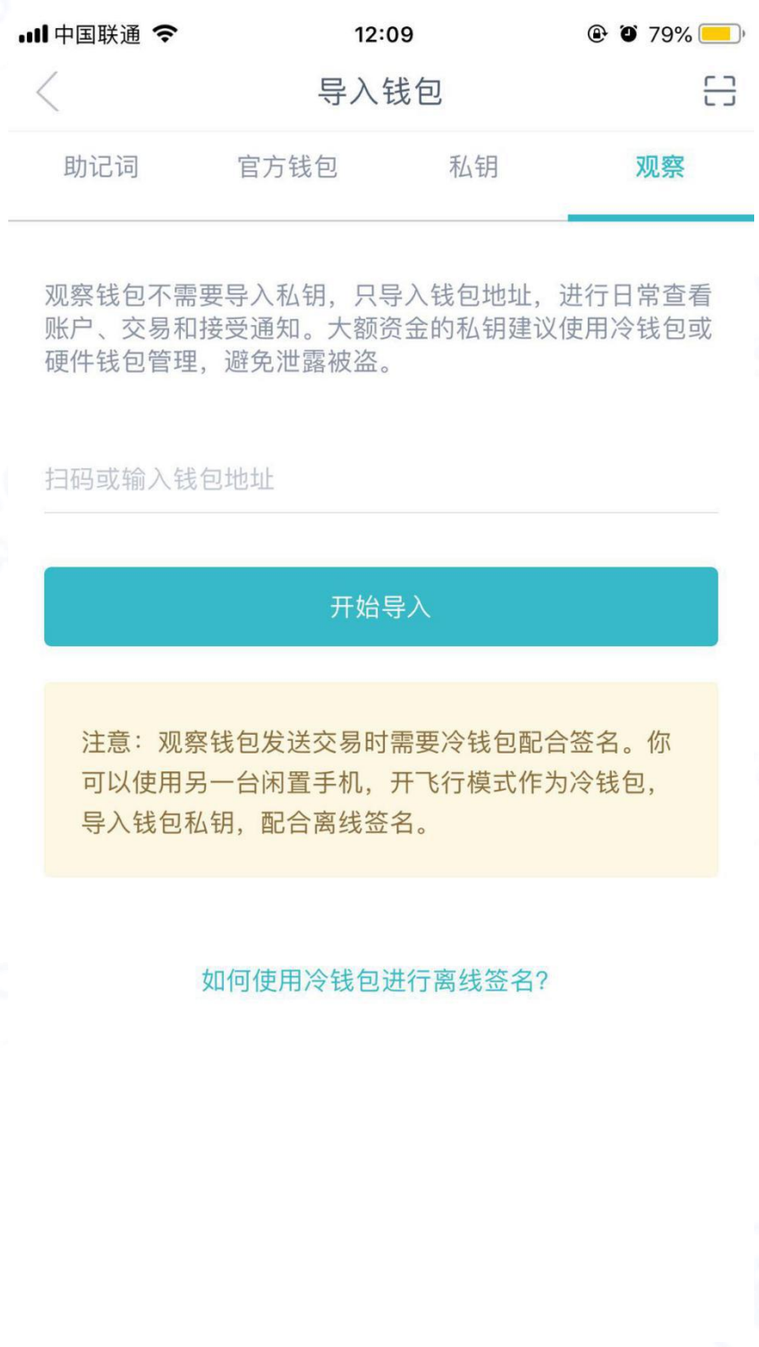
不过为了方便使用满足一些用户的需求，钱包商们专门设计用于数字资产储存交易的智能硬件，安装了相应的软件客户端，使得使用、交易、存放更加的便利。在安全性上会比之间用手机安装个钱包 app 来说更加专业和安全。目前硬件钱包也有热钱包和冷钱包之分，原理和手机 app 大体一致。


目前常用的硬件钱包品牌有 Ledger、库神、比特护盾等。以比特护盾为例，团队将钱包做成手表形状，便于佩戴。同时用户可以根据手机端的 APP 监控并使用数字资产，使用数字资产必须要与手表相配合，保障了资产的安全性与易用性。

# 3.4 其他类别的钱包

## 3.4.1 观察钱包

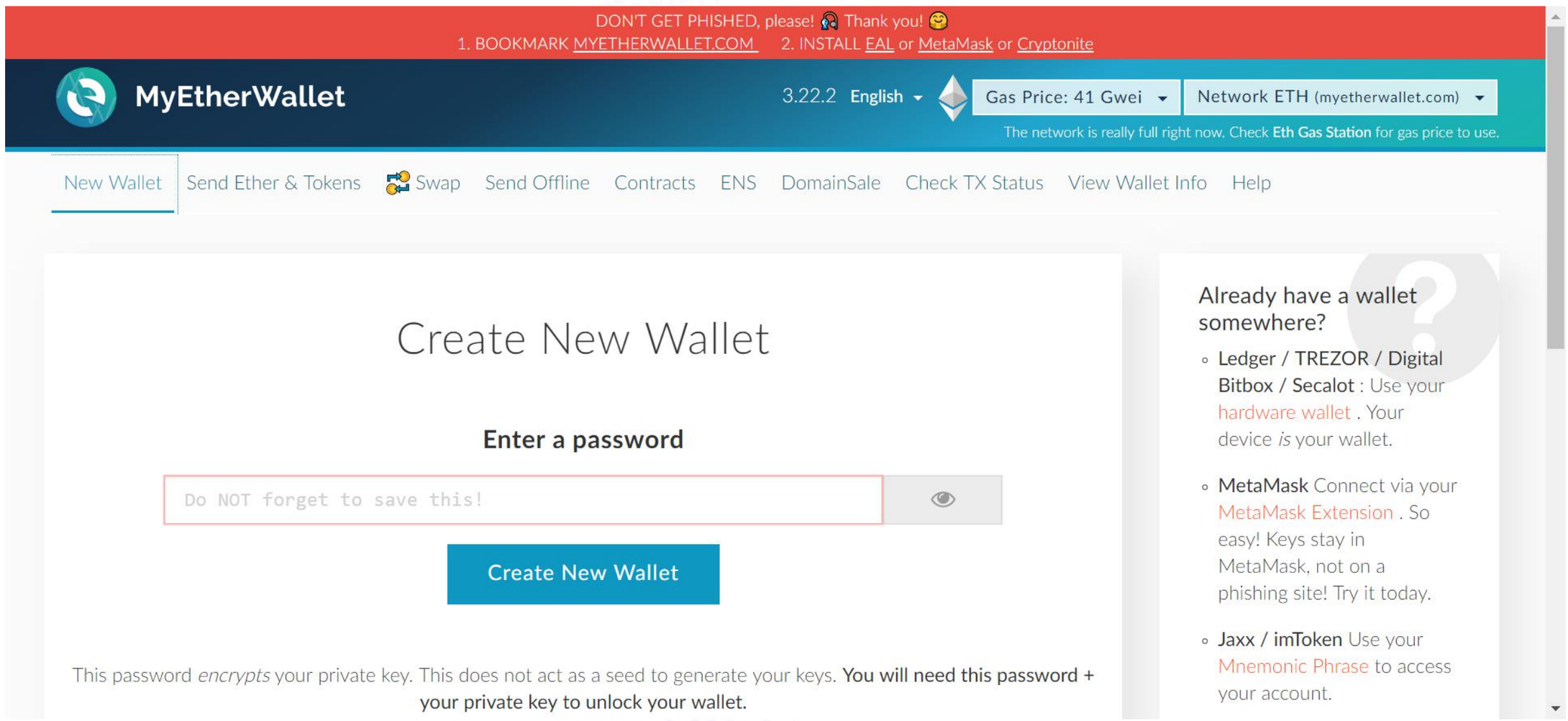
由于冷钱包是不联网的，我们在向冷钱包的地址中发送比特币交易，即便到账了我们也无法看到到账信息以及钱包中的具体余额。观察钱包就是一种提供观察冷钱包中资产变动的钱包。像 3.3.3 中比特护盾手表旁边的钱包就是一款观察钱包。


此外，imtoken 钱包也可以通过管理钱包的入口设置观察钱包，通过冷钱包提供授权，在观察钱包中导入冷钱包的地址，即可在联网的手机中创建观察钱包，实时监控冷钱包账户中资金变动情况。

## 3.4.2 网页钱包

网页钱包是指在网页中创建和使用的钱包，目前应用最广泛的网页钱包是 MyEtherWallet，此外还有 blockchain.info 等。




相较于其他钱包，网页钱包中所涉及的功能更加丰富，可以操作的手段更多。除此之外，使用网页钱包更加方便快捷，无需安装应用程序，可以跨平台，导入私钥即可使用。不过网页钱包的特性使然，它的门槛也比较低。

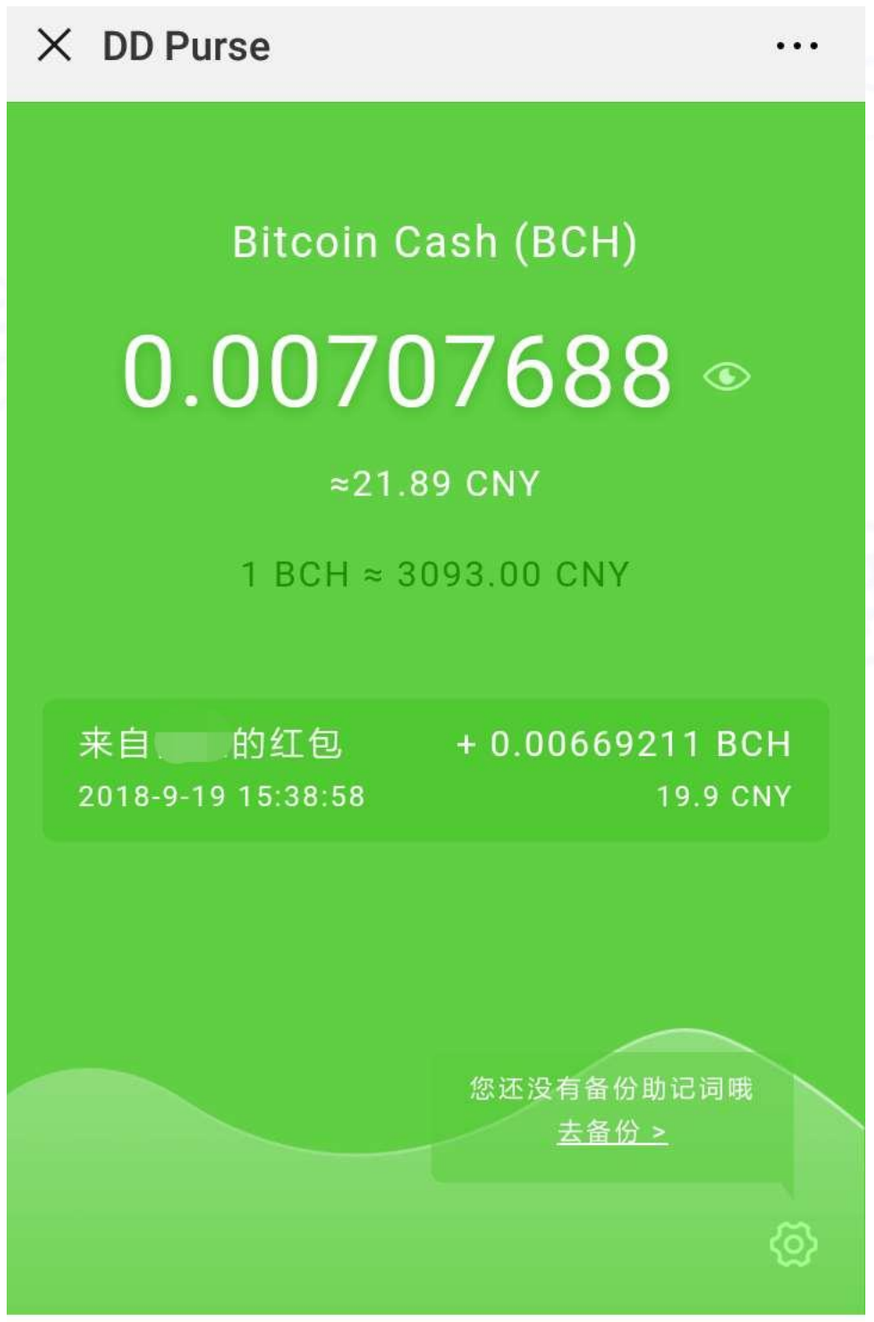
## 3.4.3 浏览器插件钱包

浏览器插件钱包是以浏览器插件的形式存在，常见的钱包有 chrome 浏览器的 Metamask 钱包插件。


使用浏览器插件钱包可以用于各种 Dapp 的网页支付，以及参与 ICO 等。像加密猫这种应用，在进行游戏中的链上操作时，需要通过 MetaMask 钱包。同样，浏览器插件钱包主要以使用为主，安全性能一般，不建议存放大额资产。

## 3.4.4 简易钱包

既然钱包只是一个存放私钥的场所，那么很多简单的区块链应用实际上就是一款钱包。这种现象在 BCH 这种灵活自由的点对点的电子现金系统中非常常见，由于 BCH 零确认以及低手续费的优势，基于 BCH 开发出了很多灵活转账的应用。




像这款用于微信中打赏、转账、发红包的软件，实际上也是用户本人控制私钥的钱包，同类型的还有微博、Twitter、手机短信中发送 BCH 的应用。

除此之外，根据钱包中所包含公链的数量，可以分为单链钱包和多链钱包。像 imtoken1.0 版本主要存放 ETH 以及 ERC20 的代币，就是一款单链钱包（单币种钱包），而比特派可以存放 BTC、ETH、BCH、EOS 等币种，则是一款多链钱包（多币种钱包）。

根据私钥的控制方式，则又可以分为单签名钱包和多签名钱包。但签名钱包是私钥由一人控制的钱包。而多签名钱包中，要使用其发送交易则需要多个人的私钥签名，有点类似于很多重要资金账户的保险柜，三把钥匙中的两把同时作用才能够打开。

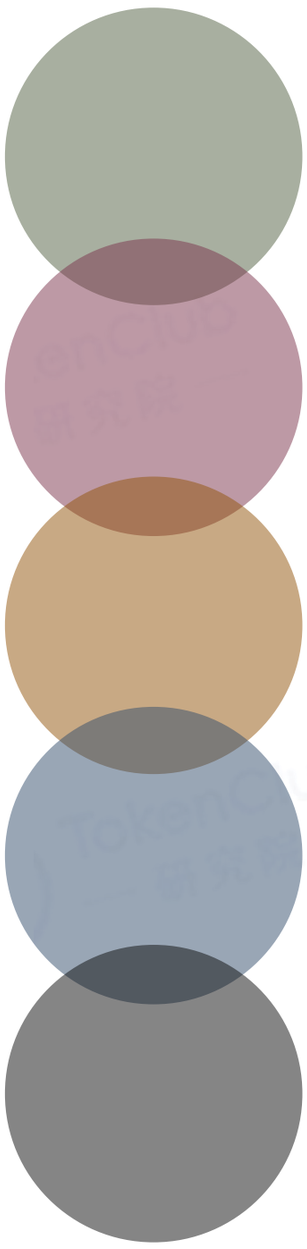
# 4. 钱包生态建设及商业模式

## 4.1 钱包功能概述

钱包功能包括基础功能与衍生功能，基础功能是指所有钱包或大多数钱包所共有的功能，它们与钱包的技术原理息息相关，直接作用于数字货币的使用；而衍生功能是寄托于基础功能之上，钱包商为了满足用户的不同需求所开发出的多项功能。

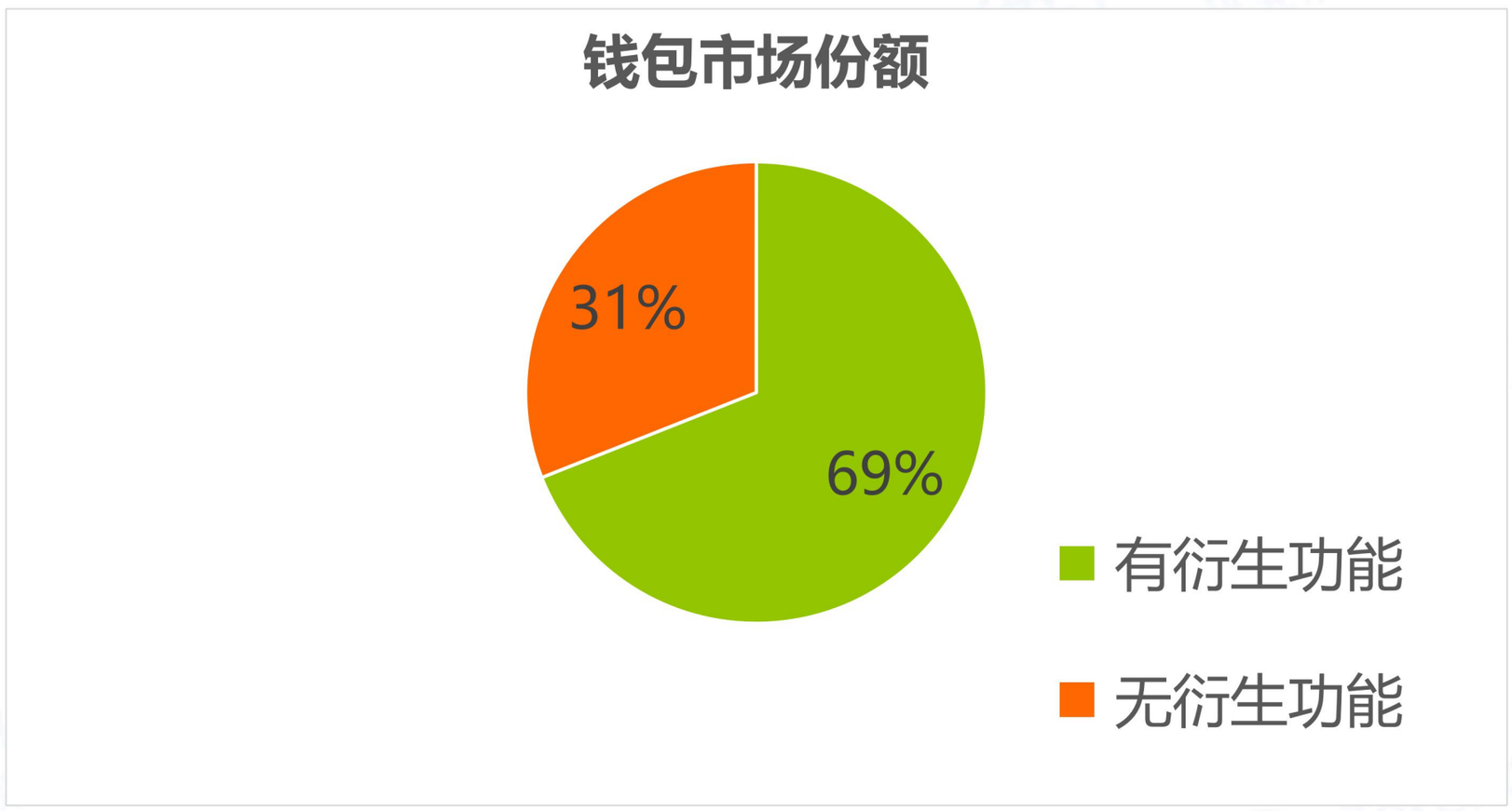
### 4.1.1 钱包基础功能

钱包的基本定义：钱包是用于储存和使用私钥的工具，拥有私钥就可以支配所对应地址中的数字货币，因此数字货币钱包的基础功能可大致分为以下几点：

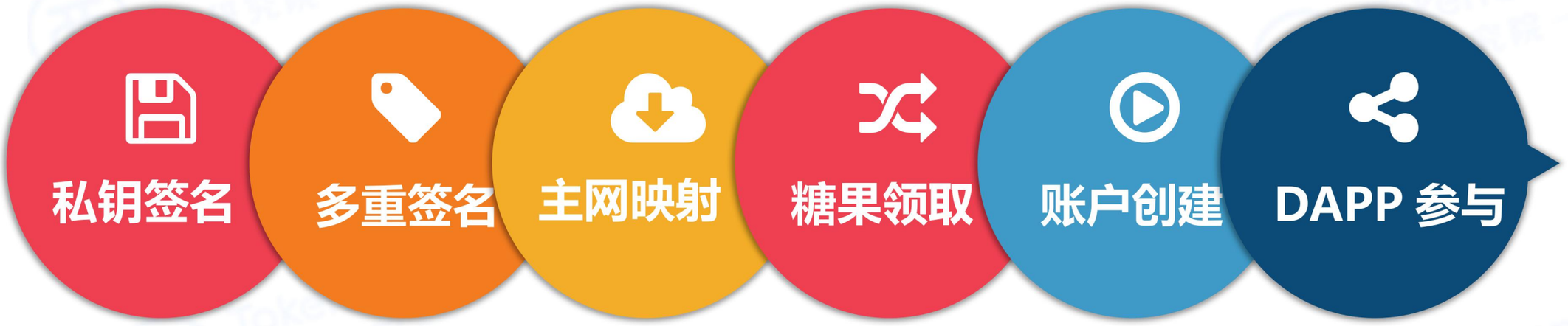



## 4.1.2 钱包衍生功能

钱包看似只是行使着私钥存放与管理的职能，却因此成为用户参与和使用数字货币生态的入口，毕竟每一个链上的交易都需要通过钱包来发起。钱包商根据这一特性又开发了很多衍生的功能。




根据统计，目前市场中约有 69%的钱包品牌都在基础功能之上添加了衍生功能，主要包括以下几点：




**私钥签名：**如果如果一个人持有私钥，他就可以使用私钥对任意的消息进行签名。签名的目的是为了证明，该消息确实是由私钥持有人发出的，任何其他人都可以对签名进行验证。验证方法是，由私钥持有人公开对应的公钥，其他人用公钥对消息和签名进行验证。如果验证通过，则可以证明该消息确实是由持有私钥的人发出的，并且未经过篡改。

**多重签名：**多重签名就是多个用户对同一个消息进行数字签名，可以简单理解为一个数字资产多个签名。多重签名的作用意义非常，如果采用单独的私钥，尽管

以目前的密码学可以保证无法被暴力破解，但是这个私钥不保证会以其他方式暴露出去，此时如果公钥是由多重签名方式生成，那么即便被盗取了其中一个私钥，盗取者也无法转移对应的数字资产。因此，多重签名能够使资产更加安全和多样化管理。

**主网映射：**部分公链类项目，在主网尚未开发完备时，通常会采用 ERC20 的代币表示，可以用于投资交易。在主网上线期间，为了保证持币者的权益，通过将以太坊网络上的资产映射到新的公链主网中，其代表性的为 EOS，待上线成功后获取新的主链上的数字资产，完成新旧代币的转换。在 EOS 主网上线过程中，绝大多数的交易所、钱包都支持用户的主网映射。

**糖果领取：**糖果主要指分叉币以及针对一些主流币种的空投币。对于同一链上的空投币，用户通常不需要做任何操作，就可以在钱包中收到空投的代币；而对于分叉币来说，由于处于不同主链，需要用户导入私钥到主网去兑换，这对于用户来说一方面操作麻烦，另一方面有私钥被盗风险，因此钱包商通常会提供代为领取分叉糖果的服务。

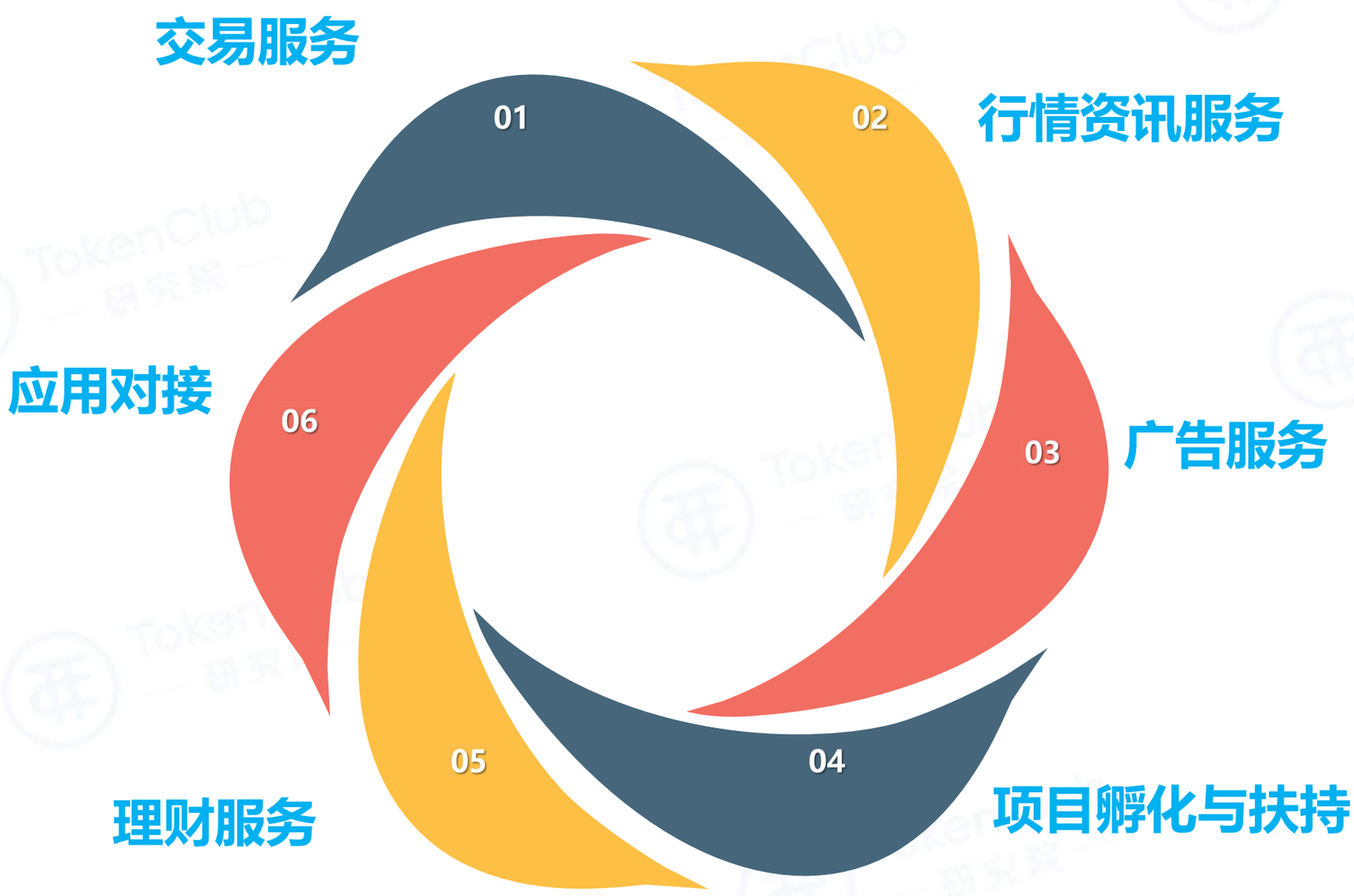
**账户创建：**目前部分主链是账户制，比如 EOS。钱包商提供账户创建服务，并且基于该账户可以进行 EOS 投票，RAM、CPU 等资源的购买、糖果索取等服务。

**DAPP 参与：**部分专门的钱包可以提供一些公链的 DAPP 入口，直接通过钱包参与到 DAPP 中去。常见的公链有 ETH、EOS，像加密猫、EOS BET 等应用都是通过专门的钱包参与。

# 4.2 钱包商业模型分析

钱包的基础功能是私钥的管理，对于一款钱包的开发推广需要大量的人力、财力成本，而仅仅凭借最简单的交易转账功能，钱包商可以说是没有任何利润可言。而钱包对于加密货币生态又不可或缺，因此钱包商通常会在基础功能之外，探索新的商业模型。

首先对于硬件钱包来说，盈利模式很容易解决，团队只需要开发稳定实用的钱包，并且将固件开源做成硬件产品在网上售卖即可解决盈利问题。如果对于一款轻钱包来说，如果设置收费模式便额外设置了一道门槛，不利于数字货币以及钱包的推广，因此他们通常会采取其他方式去拓展商业模式。



## 4.2.1 交易服务

交易服务主要包括两个方面，其一是像交易所这样的币币兑换服务，其二则是场外交易渠道。较为有代表性的两款钱包 Bitpie、币信都开通了这两项服务，场外交易渠道提供了法币入场的通道，而钱包内置交易所能够使用户资产之间转换更加方便快捷。部分钱包还提供了快速兑换的服务，钱包商会在其他交易场所进行反向操作用来对冲币价变动的风险。

尽管目前大多数钱包内置交易所的成交量无法跟传统大的交易所相比，场外交易深度也比较有限，但仍然可以通过这其中的手续费收取来获利。并且，提供交易服务满足用户的交易需求有助于提升用户粘性。

## 4.2.2 行情资讯服务

行情资讯类服务也是数字货币市场中一项不可或缺的部分，用户打开钱包可以关注到新闻资讯、行情快报、项目简介、K 线图、大额资金流动监控、代码活跃度等重要的市场信息，对于钱包来说，这是一项辅助提升用户粘性的功能。

在此之外，部分钱包会针对用户的需求，进行一些区块链知识的科普，提供一些领取糖果、参与众筹的渠道。

# 4.2.3 广告服务

以比特派钱包为例，它可以依靠自己的流量优势，为项目方或者其他币圈的机构提供广告服务，比如矿池、糖果空投、众筹参与渠道等等。

### 4.2.4 项目孵化与扶持

很多项目方，尤其是那些拥有自己主链的项目，在进行项目推广的时候不仅仅依靠自己的力量，往往会选择投资或孵化一些钱包品牌，这些钱包品牌手中会有一些用户，他们会对用户进行估值，获取钱包团队大约 10%左右的股权，目的不仅仅在于未来股权的升值，而在于依靠这种优势去推广自己的项目。

通常对于主流币之外的链，他们本身用户生态较小，第三方的钱包不会去提供这些项目的服务，因此需要项目方利用资金去打破僵局。

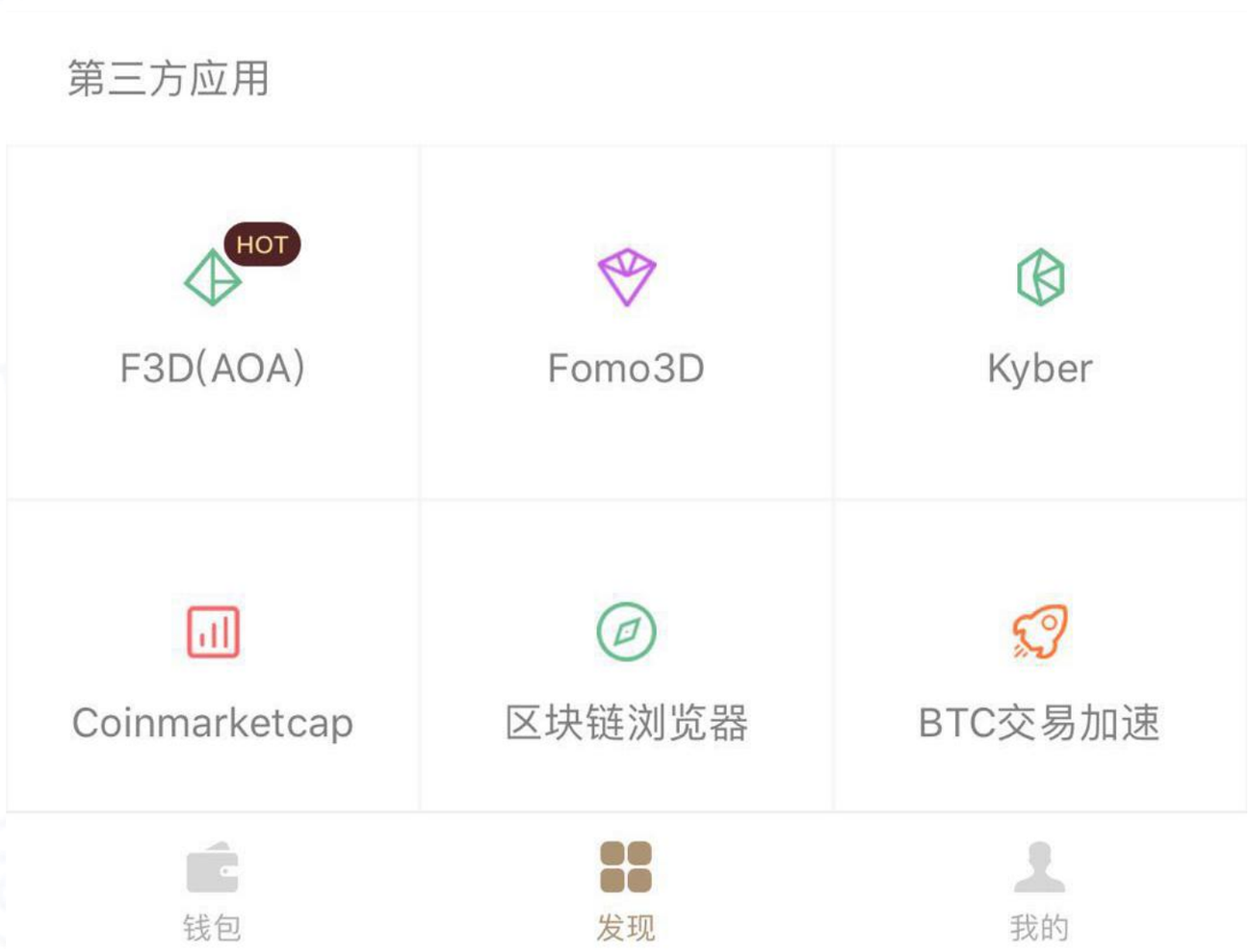
### 4.2.5 理财服务

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。

除了一些派发币息的类似于传统理财产品的服务，像 KCASH 钱包还提供抵押借币的服务。即向钱包抵押一定数量的代币，可以获得贷款用于急用。由于目前数字货币还不具备一定的法律地位，传统的金融机构很难去将其作为抵押物放贷，钱包此举恰恰可以解决持币人在短期内的融资之急。


## 4.2.6 应用对接

钱包作为应用的入口，与各种 DAPP 是一种双向促进的关系，拥有大量用户的钱包对于 DAPP 的推广尤为重要，而 DAPP 又可以为钱包增强用户粘性。钱包商可以与各 DAPP 应用达成协议，凡是通过该钱包参与 DAPP 的用户，其所消耗的数字货币，钱包商可以从中获取分成佣金。



# 5. 行业问题及发展趋势

## 5.1 目前钱包行业存在的问题

目前区块链技术仍然处于一个早期的阶段，无论是用户数量还是技术完善程度尚不成熟。钱包作为数字货币使用的载体，对于整个行业的发展尤为重要。目前市场上钱包种类繁多功能各样，但在具体应用的过程中都产生了一些问题。

### 5.1.1 安全事故及安全隐患

安全问题是钱包的第一大问题，作为数字货币的用户，无论小额大额资金的存储都需要通过钱包（包括中心化钱包）来进行，在存储的过程中各种类型的钱包都发生过数字资产被盗的问题。造成钱包安全事故及安全隐患的原因有很多，大致分为以下几种情况：

#### 5.1.1.1 中心化钱包下的安全风险

对于中心化钱包中数字资产的存储，用户大多选择一些大型的交易所存放，还有少部分存放在像币信这种中心化的钱包中。这种方式有一个问题即私钥的控制权不在用户个人手中，按照持有持有私钥才算持有数字货币的所有权的说法，这种方式实际上相当于用户将数字资产托管或者借贷给中心化的钱包机构。

而这种方式所造成的安全隐患主要有这五点：

**钱包商跑路：**钱包商享有对数字资产的绝对控制权，而数字货币的匿名性加上很多钱包（交易所）团队处于海外，一旦卷款跑路维权追偿是一个艰难又漫长的过程。

**服务器被黑客攻击：**自今年年初开始到现在，很多交易所服务器被黑客攻破，部分币种出现不正常的价格波动，对用户的资产价格造成了重大影响。

**钱包商被盗：**最著名的当属当年 Mt.Gox 交易所被盗，共损失了客户的 75 万枚比特币以及自己的 10 万枚比特币，通常黑客窃取比特币之后会选择在市场上抛售，也因此打击了用户的信心，带来了漫长的熊市。

**账户名和密码的安全隐患：**对于中心化钱包，通常我们用账户名和密码进行登录，这种方式同样也方便了广大黑客，他们窃取账户名密码、甚至邮箱与短信的验证码，通过试用谷歌二级验证的方式才能相对的保障我们资产的安全，但仍然存在着被攻击的空间。

**浏览器安全隐患：**登陆过程中浏览器漏洞和浏览器插件也会对用户资产的安全性造成影响。

### 5.1.1.2 轻钱包的安全风险

轻钱包虽然是自己持有私钥，但相对于硬件钱包及纸钱包其安全程度仍有不足之处：

**私钥错误存放：**很多用户生成私钥及助记词后，截屏存放在手机相册中、云端，这些地方很容易被黑客截取。

**生成私钥的手机、客户端不安全：**存在一种可能，及在生成助记词抄写的这段时间，手机中的木马插件，甚至钱包自身会记录下生成私钥的内容，或许在未来的某个时刻会发生被盗事件。

**私钥保管不当：**正常的私钥保存方式是通过一张纸记录下来，然后存放至安全的地方。一旦私钥遗失、损毁，而钱包又没备份，那么钱包中的数字资产将永远无法使用；另外由于不当保管导致他人看到了私钥内容，也会对数字资产的安全造成影响。

### 5.1.1.3 硬件钱包的安全问题

硬件钱包是安全系数最高的钱包之一，但仍然存在一些安全的风险：

**私钥生成阶段：**这取决于私钥生成是否随机。另一方面，很多人并非通过官方渠道购买的硬件钱包，可能会被做过手脚。

**私钥使用阶段：**很多用户喜欢将硬件设备结合网页客户端一起使用，因此黑客可以通过更换找零地址的方式窃取用户的数字资产。

## 5.1.2 支持币种少，功能简单

目前市场上大多数钱包支持的币种数量比较有限，对于持有多种数字资产的用户来说，往往需要下载多款钱包，这无论是对于数字货币的使用还是私钥的保存都是一项考验。

目前市场上大多数钱包都是 BTC、ETH 的钱包，其次是 BCH、LTC 和 EOS，使用的过程中需要在各个钱包之间来回切换，影响了用户的体验，也带来了潜在的风险。

## 5.1.3 钱包的使用门槛较高

现阶段由于技术的瓶颈，钱包商往往需要在安全性与易用性之间寻求一个平衡，为了安全考量通常在易用性能上需要作出一些牺牲。大多数人出于交易需求往往选择将数字资产存放在交易所中，主要是因为现在的钱包即便提供内置交易所，而由于交易深度不足无法满足交易需求。

另外，在使用一些 Dapp 应用的时候，部分钱包需要下载一些插件。甚至在进行数字货币转账的过程中也需要经过繁琐的流程，比如输入密码、验证指纹等等。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。

## 5.1.4 推广与盈利模式面临困难

4.2 章节中介绍了现有钱包的几个盈利模式，但是仅有少数钱包有足够的用户去构建这种生态。目前很多钱包仍然只具有简单的转账功能，用户较少且没有找到适合自己的盈利模式。团队运营及开发的成本通常依赖于消耗投资人的资金。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。

这主要是因为很多钱包替代性不大，而且考虑到用户的资金安全，通常是一些老的钱包品牌更容易被用户所接受。很多钱包为了融得资金，会采用代币融资的方式，这种方法在牛市能够融得大量资金，但泡沫化严重，虽然能在短期内筹得资金，但却是将风险转嫁给了 Token 的持有者，倘若在后续的开发运营中难以为 Token 找到一个合适的应用场景，对投资人是一种巨大的损失。

# 5.2 数字货币钱包前景展望

数字货币的应用场景如果仅仅局限于交易所中相互炒作，那么无非是叠加泡沫而失去实际应用价值。目前像 BTC、BCH、LTC 等货币类数字资产的应用场景不难找寻，在大额转账与小额支付中均脱离交易所并发挥了一定作用，这其中钱包的作用功不可没。但这种功能短时间内很难成为多数用户的刚需，阻碍了数字货币的生态进一步拓展。

未来数字货币的应用必将以钱包作为重要入口，各种 DAPP 成为人们生活中的日常，钱包的功能也将进一步丰富和完善。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，朝着全面和综合性的方向进行业务优化和资源聚合。

## 5.2.1 数字世界的入口

每一个持有数字货币的人都脱离不了与钱包的联系。即便是存放于交易所中的数字资产，实际上也依赖于交易所对于数字货币的钱包存储方式。作为数字世界的入口，钱包应当发挥更大的价值：

**繁荣的 DAPP 生态群：**在 2017 年由 ETH 所开启的公链热潮中，Dapp 作为一种去中心化的应用设施，进入到了人们的视野中。除去那些为了圈钱而发起的项目 Token，很多项目都拥有自己的用户生态、流量以及应用场景。这些人手中持有大量的数字资产，要么存放在钱包中沉睡，要么放置与交易所中炒作。

未来这些有价值的 DAPP 应用落地成熟以后，必然会有一款钱包将这些资源整合起来，或作为应用商店，或作为数字货币在这些 DAPP 间使用的平台，成为区块链的超级流量入口。

**链上的参与和治理：**数字货币作为权益的重要凭证，用户凭借自己掌握的私钥，行使通证代表的各项功能和权利。EOS 的投票制度、POS 的挖矿收益分红等等，都是通过钱包予以实现。设想在未来股权通证化的时代，用户可以直接利用钱包在链上做出决策，降低了很多投票成本，公司可以基于钱包的地址、账户进行利润分红，甚至作为公司的员工，可以在地址上领取工资、奖金。

### 5.2.2 资产属性强化，金融产品更加丰富

目前部分钱包已经开始了在理财领域的探索，不过产品较为简单。从技术上的角度上来说，传统金融的很多模式都可以复制到数字货币的世界中来，围绕资产开展一系列理财服务将是未来钱包发展重点。

## 5.2.3 交易所与钱包的融合

目前的一个趋势是钱包在做交易所，而交易所也在做钱包。现在的问题是，交易所的头部效应明显，由钱包去开发交易所会面临深度的瓶颈，而交易所去做钱包，无论是在技术上、资金上以及用户数量中，都有不可比拟的优势。最近火币网将钱包作为了自己的生态之一，钱包保证了用户资产的去中心化存储，而借用自己的优势，可以使数字资产在钱包与火币全球站之间更便捷的转移，进而丰富用户体验。


目前行业中的巨头不再满足于构建单一生态，钱包、交易所、公链等数字货币的重要环节都将成为它们生态中的一环。

## 5.2.4 谁是区块链世界中的支付宝?

2003 年 10 月，淘宝网首次推出支付宝服务，发展至今已经有 15 个年头。据统计，自 2014 年第二季度开始，支付宝就已经成为了全球最大的移动支付厂商，从诞生到广泛使用实际上也仅仅用了不到十年。就像当初支付宝处于一个不被认可的地位，数字货币也会从开始的灰色地带到慢慢被大多数人所接受，最终成为人们生活中的一部分。

世界在加速发展，区块链的第一个十年，人们看到了数字货币及去中心化应用的重要价值。下一个十年，整合了行业中所有资源的钱包生态或许会像支付宝一样伫立在我们面前，成为真正改变这个世界生产关系的存在。

# 6. 风险提示

本报告所采用的的数据均来自合规渠道，分析逻辑基于作者的职业理解，本报告清晰准确地反映了作者的研究观点，力求独立、客观和公正，结论不受任何第三方的授意或影响，特此声明。

本报告的信息来源于已公开的资料，TokenClub 研究院对该等信息的准确性、完整性或可靠性不做任何保证。在任何情况下，本报告中的信息或表述的意见均不构成对任何人的投资建议。

本报告版权仅为 TokenClub 研究院所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制、发表或引用。如征得 TokenClub 研究院同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“TokenClub 研究院”，且不得对本报告进行任何有悖原意的引用、删节和修改。

TokenClub
研究院

TokenClub 是国内领先的数字货币投资社区，致力于构建一个自治、信任、高效的数字资产投资服务生态。

“TokenClub 研究院”是 TokenClub 旗下研究区块链的专业机构，专注于区块链行业研究、项目评级。

扫码关注
TokenClub 研究院

扫码下载
TokenClub APP