匿名币
研究报告

2018 年 10 月

TokenClub
研究院

目录

1. 行业综述

匿名币是指在交易过程中隐藏交易金额、隐藏发送方与接收方的一种特殊的区块链代币。与之相对应的，是比特币、以太坊这些“显币”。显币能够通过区块链浏览器查询到每笔交易的金额、交易时间、发送方和接收方等信息，而匿名币则无法查到。

1.1 行业背景

2008 年，中本聪发表了白皮书《比特币：一种点对点的电子现金系统》，比特币的概念正式诞生。作为一个支付系统，比特币中涵盖了很多概念，其中包括去中心化、不可篡改、转账成本低、总量恒定、全世界流通以及匿名性。比特币一经上线，遭到了各个密码学极客以及自由主义者的热爱，早期它只是人们相互转账的“玩具”，知道披萨事件以及第一家比特币交易所上线后，它开始有了自己的价格，人们尝试用它来购买商品。由于比特币匿名抗监管的特性，它被应用到了暗网交易中。

随着比特币在暗网的广泛应用，也引起了监管部门的注意。当人们开始监管比特币地址上的资金动向的时候，比特币的匿名性便不再那么的牢固。毕竟整个比特币体系是建立在一个全网公开的分布式数据库账本中，只要搭建一个全节点，便可以监控从创世区块开始，每一个地址的所有交易信息。

除了在暗网中的应用，比特币也被用于洗钱、非法集资、跨境汇款、资产隐匿等黑色、灰色领域。但是在这些遭受重大监管的场景，人们发现比特币的匿名性无法满足要求，或者使用者单纯的就是想隐藏自己的交易痕迹，人们开始对数字货币的匿名技术进行了进一步的探索。

1.2 比特币的匿名性

在现实世界中，我们进行交易的媒介绝大多数都是采用法币。法币主要以两种形式存在，纸币和电子货币。通常，我们在使用纸币的时候是绝对的匿名，去超市购物一手交钱一手交货是无法被检测到，也很难将这笔钱的全部交易流程调查清楚。而使用电子支付则是另一回事，无论是使用银行卡、还是支付宝微信，每一笔交易记录都存储在中心服务器的节点上，用户的所有交易行为都会被探知。而比特币的匿名性相对于电子支付有了很大的提升。

1.2.1 比特币的匿名特点

比特币诞生之初一大特点在于匿名性，其匿名性体现在它切断了账户（地址）与个人身份之间的联系。可以这样解释，目前绝大多数钱包都是匿名的，不论冷钱包还是热钱包（中心化钱包除外），它只需要下载钱包并且将私钥（助记词）备份，这个过程并不需要将与个人身份相关的信息填入。通过钱包生成的地址也是随机的，因此在整个过程中都可以做到绝对的匿名。

上图是从区块链浏览器中随机抓取了一笔比特币的交易，0.177 个比特币通过一笔交易发送到两个不同的地址中，这两个地址可以看出当发送一笔到另一个地址后，余额也会发送到另一个地址中。比特币这种特殊的余额结构 UTXO（未花费的交易输出）能够保证一个私钥可以对应无限多个比特币地址，也保证了比特币的地址交易相比法币的电子货币甚至以太坊的账户都更难以被追踪。

因此，比特币所谓的“匿名”特点主要来自于两个方面：1）通过哈希地址无法还原交易人身份；2）一个人可以有无数个收款地址。

1.2.2 比特币匿名性的不足

比特币实现了匿名程度的 90%以上，但是由于它所有的交易信息在全网公开，而且它每一个地址上的余额都可以被监控，致使它无法做到百分百的匿名，比特币的“显性”主要体现在以下几个方面：

- 交易过程无法匿名；
- 地址余额无法匿名；
- 现实中的交易行为会将自己的个人 IP 与自己的比特币地址关联性暴露。

这三点决定了如果有监管能力的组织要监控某个人的比特币地址的交易情况，那么他所有的交易行为都暴露无遗，这主要有第三条有关：即使地址与地址之间的交易能够保证匿名性，但是由于比特币的用户要以实名的身份去参与整个现实世界中的交易，因此在参与的过程中会使得个人身份与个人地址被关联起来。

作为普通的数字货币投资者来说，我们获取比特币的方式无非这几种渠道。最多的是通过交易所购买比特币，然后提现到个人掌管私钥的钱包中，其次还包括场外交易。

需要意识到一个问题，中心化的交易所恰恰是暴露个人持币隐私最严重的的场所之一。我们在注册交易所账户的时候，需要经过复杂的 KYC 认证，除了手机、邮箱，甚至还包括身份证号、家庭住址等信息，如果你的币存放在交易所中，那么你的持币信息暴露无遗。若你把币提现到个人地址后，交易所以及有能力监管交易所交易信息的其他组织能够根据你的提币行为，锁定你的个人地址，毕竟你的提币地址与个人 IP 已经进行了绑定，而你之后的交易行为会在区块链上留下痕迹。

除了交易所之外，目前很多场外交易渠道为了满足监管的要求，担保人也开始记录交易者的个人身份信息。此外，利用真实的身份信息，用比特币去网上商城购物也会暴露自己的持币信息，即便是自己有一个轻钱包（小额比特币）和硬件钱包（大额比特币），也会因为这两个钱包地址有着高频的交易而被关联。

因此，比特币的匿名程度无法满足在特定场合使用的需求，也无法满足一些自由主义者对隐私的需求。人们开始探索提升比特币匿名性的解决方案。

1.2.3 混币技术

尽管比特币无法做到绝对的匿名，但可以通过某些方式去提升自己的匿名性，这其中的关键就是切断地址与地址间的关联性。这就不得不谈到一个技术——混币服务。

混币服务的原理就是由许多人参与交易，进而在某个交易场所会存在大量的买入和卖出，但是很难在买入和卖出中找到一一对应的映射关系，买入和卖出是被割裂的，所以无法从一端找出另一端。

交易所其实就是一个大的混币池，如果不考虑注册交易所的 KYC 已经暴露了你自己的 ID 的情况下，你将 1 个比特币存入交易所然后再提现，实际上就进行了一次混币。因为通常一个交易所的地址有无数人的比特币进进出出，其中还包括热钱包地址与冷钱包地址，甚至你的充币地址和提币地址是交易所的两个不同地址。因此你取出来的这个币已经不是你原来存进去的那个，而是从无数个其他地址，经过一个“池子”混合后，拿出来一个比特币给你。这样攻击者就无法观察到这个交易过程，因为是在这个“池子”中实现了混合，而这个混币的执行依靠混合协议或其他协议执行的，这个混币的过程没有第三方，安全可靠，完全去中心化。

当然，交易所的 KYC 放大了个人的隐私，因此用户通常采用其他方式混币。如果 A、B、C 三人进行混币，大致需要进行如下流程：

- A 通过 Tor 等匿名服务，在 IRC 聊天室中认识了 B，C 等人，他们也有类似的隐私权的需求。
- ABC 每人从钱包中找出包含同等金额比特币(比如 100mBTC)的 UTXO，并制造一个自己的新的公钥。
- BC 把 UTXO 信息和公钥散列给 A(本例中 A 是组织者，并且是匿名的)。
- A 构造一个交易，把所有 UTXO 作为输入(共 300mBTC)，然后把输出平均分给 ABC 的公钥散列。
- A 用 SIGHASH_ALL 模式来签名 A 提供的 UTXO，然后给 B;B 同样签名，然后给 C; C 同样签名，然后就可以发布到公开的网络中让所有人看到。

这样，除了 ABC 之外，没人能分辨到底哪个输出是谁的，也就无法跟踪之后的消费。如果大量进行混币交易，会极大的提高追踪难度。

不过对于一些非法交易者，他们想进一步提升交易追踪的难度，往往会选择暗网混币器，这种混币器不但把数量极多的各种合法非法交易混在一起，而且会采用延迟交易的办法。比如对第 N 笔交易，把其输入用于支付第 N-1 笔交易，而把第 N+1 笔交易的输入用来支付第 N 笔交易的支出。

1.2.4 闪电网络

TokenClub 研究院在《侧链技术研究报告中》介绍了闪电网络的技术原理。尽管比特币区块链上的交易信息是透明的，但是作为比特币的侧链，闪电网络是通过节点之间搭建通道来进行交易，而通道两端的节点所记录的只是交易后最终的数值，节点之间发生多少笔交易、每次的交易金额是多少都不会被记录。

因此，闪电网络中的交易匿名性要强于比特币主链上交易，但是由于闪电网络的发展趋势，会演化出很多超级节点，这些节点通常都是实名甚至会受到一定的监管，但是仍然可以有人通过搭建匿名节点来实现比特币 off-chain 交易的匿名性。

1.3 匿名币产生

尽管有针对比特币的匿名服务，但是随着比特币区块拥堵手续费增高，混币的成本也随之增高。另外，混币的流程繁琐，对于新的用户并不友好，于是人们开始寻找新的替代方案——匿名数字货币。

匿名币

涨跌比 = 4 : 22 -6.94%

总市值：¥302.8亿

全球交易量(24h)：¥45.28亿

24小时	总市值	价格	涨幅
XMR-门罗币	¥118.3亿	¥717.74	-7.59%
DASH-达世币	¥95.01亿	¥1134.67	-7.75%
ZEC-大零币	¥39.32亿	¥787.65	-8.73%
BCN-百特币	¥19.93亿	¥0.01081	-9.05%
XVG-Verge	¥15.29亿	¥0.1008	-6.52%
ZEN-ZenCash	¥4.983亿	¥101.55	-6.00%
XZC-小零币	¥3.680亿	¥63.90	-5.67%

目前收录在 TokenClub 概念板块中的匿名币共 26 种，总市值达 302.8 亿人民币，其中包括 XMR、DASH、ZEC 这三大匿名币以及其他有一定应用特点与场景的匿名加密货币。

2. 门罗币-XMR

门罗币（Monero）于 2014 年 4 月 18 日推出，原名为 BitMonero，意指 Bit 和 Monero，在五天后，社区选择将名称缩减至 Monero。它着重于隐私、分权和可扩展性。与自比特币衍生的许多加密货币不同，Monero 基于 CryptoNote 协议，并在区块链模糊化方面有显著的算法差异。

它是第一个基于 CryptoNote 货币之 Bytecoin 的分支，但有着两个主要差别。首先，目标块时间从 120 秒减少到 60 秒；其次，发行速度减速 50%（后来 Monero 恢复到 120 秒的停留时间，同时保持发行时间，使每个新块的块奖励翻倍）。此外，Monero 开发人员发现了许多低质量代码，随后将其清理和重构。

门罗币是目前市值最高的匿名加密货币，目前单价 103.5 美元，市值 16.97 亿美元，占比 0.83%，位列数字货币排名第十名。

2.1 门罗币特点

门罗币的特点主要体现在区块大小、供给曲线、加密算法这三个方面。

Monero 使用比特币开创的标准 UTXO 模型，而不是像以太坊这样的账户状态配置。与比特币一样，UTXO 存在于区块链中，用户要花费时会被挪到指定的地址。与比特币的 1MB 硬性限制相比，Monero 在区块大小上限以及区块奖励上是动态的，最大块最多可以多达上 n 个块的中间块的两倍。该协议还保持最小块 300 KB，这意味着矿工可以构建高达 300 KB 的块却并不违规。

另一方面，Monero 遵循递减的供应曲线，区块奖励随时间推移而衰减。与许多其他加密货币项目形成鲜明对比的关键是 Monero 对通货膨胀不加限制。一旦挖出 18.132 百万 XMR，会有陆续的“后续发行”将每两分钟输出 0.6XMR。Monero 社区认为，无限通货膨胀非常必要，以激励矿工提供算力从而保护全网。

Monero 利用平等主义的 CryptoNight 哈希函数，这是一种基于工作量证明机制的内存密集型共识系统，使用专用电路（GPU、FPGA 或 ASIC）获得的边际收益不会超过集成此类硬件所耗费的边际成本。因此，Monero 挖矿往往通过传统的 CPU 执行，允许任何拥有一般计算机的人都能平等地找到区块，这意味着算

力联合的威胁被大大削弱，使得协议本身避免了中心化和其他攻击向量。

2.2 门罗匿名技术

为了实现资产的匿名性，门罗通过以下三项技术予以保证：

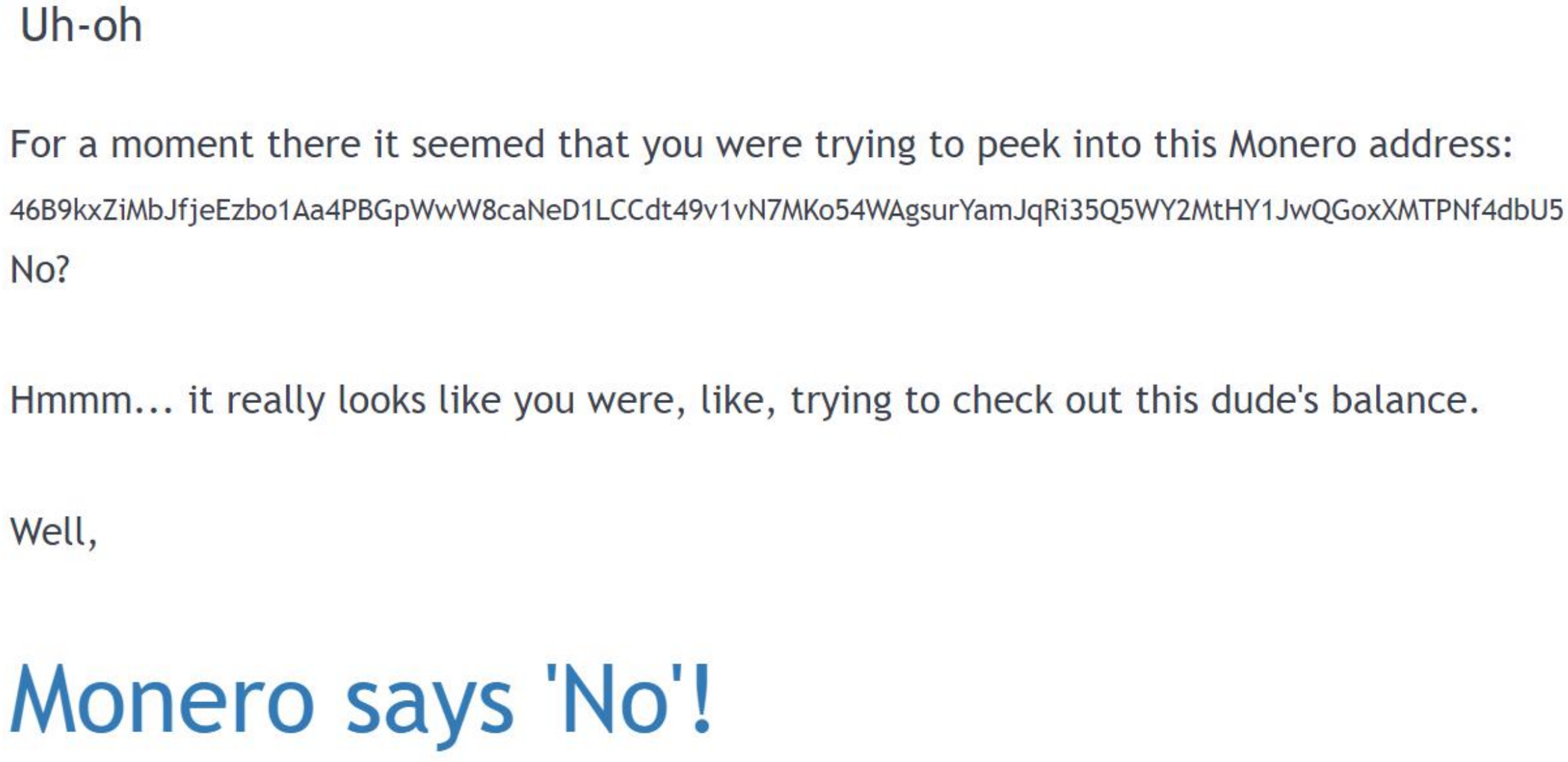
2.2.1 隐形地址

Monero 利用隐形地址来保护收币人的隐私，这是 CryptoNote 白皮书中概述的功能。与分层确定性钱包非常相似，隐形地址允许输出地址的一次性使用，防止地址重复使用妨害隐私。与 HD 钱包不同，隐形地址会增加发币人创建地址的负担。这允许接收方发布单个地址并接收无条件的匿名付款。举个例子，下面是一个门罗币地址：

门罗币地址（例）

46B9kxZiMbJfjeEzbo1Aa4PBGpWwW8caNeD1LCCdt49v1vN7MKo54WA
gsurYamJqRi35Q5WY2MtHY1JwQGoxXMTPNf4dbU5

将这个地址输入门罗币浏览器查询会出现下图的界面：**这看起来你似乎是要尝试查询这个地址的余额，门罗说“不”！**



Uh-oh

For a moment there it seemed that you were trying to peek into this Monero address:

46B9kxZiMbJfjeEzbo1Aa4PBGpWwW8caNeD1LCCdt49v1vN7MKo54WAgsurYamJqRi35Q5WY2MtHY1JwQGoxXMTPNf4dbU5

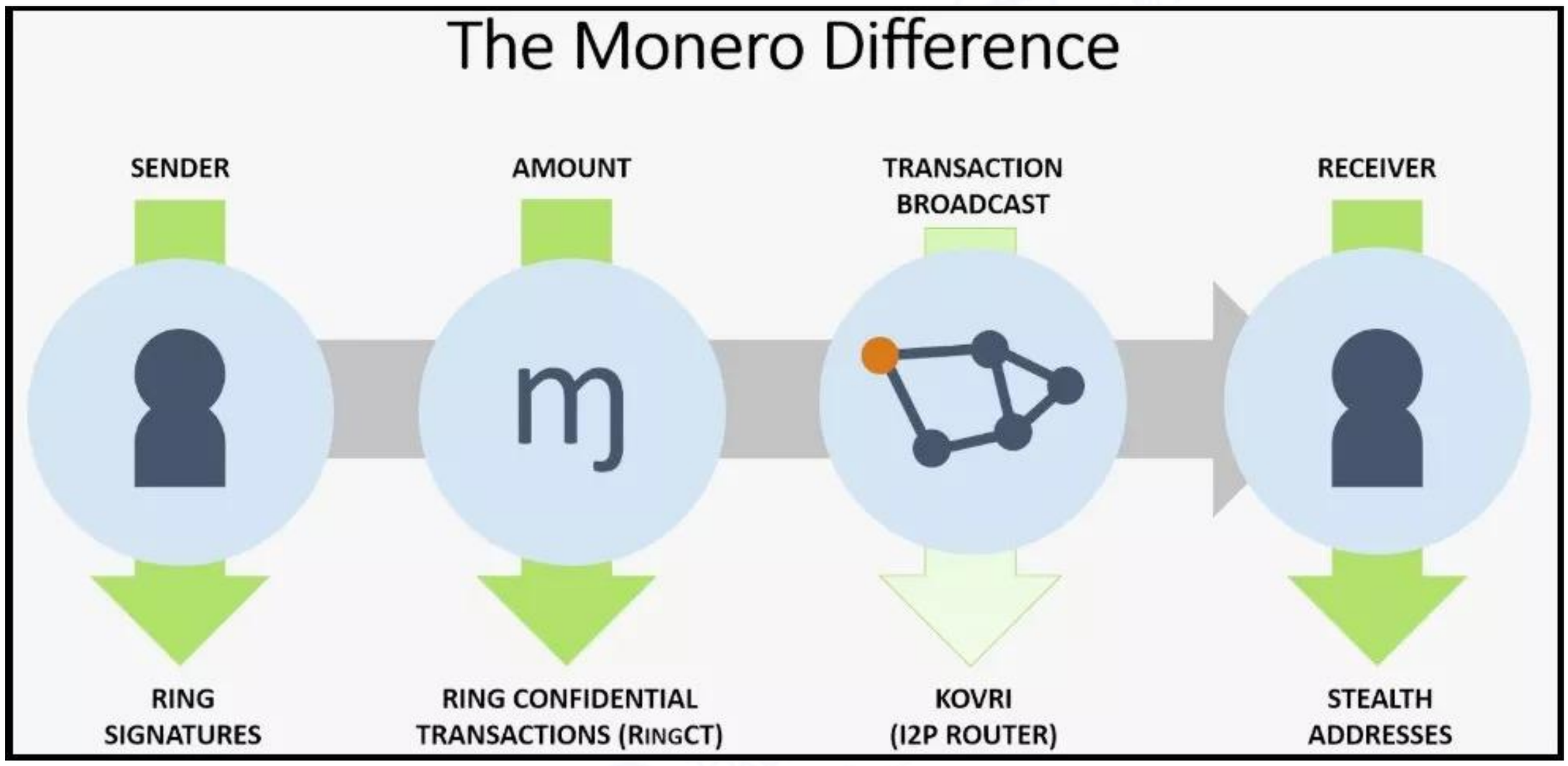
No?

Hmmm... it really looks like you were, like, trying to check out this dude's balance.

Well,

Monero says 'No'!

隐形地址的工作方式与传统的比特币地址虽略有不同，但都是从相同的基础椭圆曲线原理而来。收币人生成双 EC 密钥对，而非单 EC 密钥对，以创建一次性密钥来接收付款。



设想一个理论上存在的情景，即 Alice 向 Bob 付钱。Bob 首先生成双公私私钥对{（a，A），其中 A = aG，（b，B），其中 B = bG）}。Bob 将（A，B）连接成对人类友好的包含错误的编码格式，以创建标准地址，并将其发布到网络中。Alice 解压 Bob 的标准地址以获取公钥（A，B）。然后，她生成一个随机秘密 r，并通过乘以 r 和 A 来构造一次性公钥。Alice 随后获取该值，将其乘以生成点 G，最后将该值添加到 B。然后哈希计算结果，我们称之为 P。

P=[Hs（rA）]G+B.

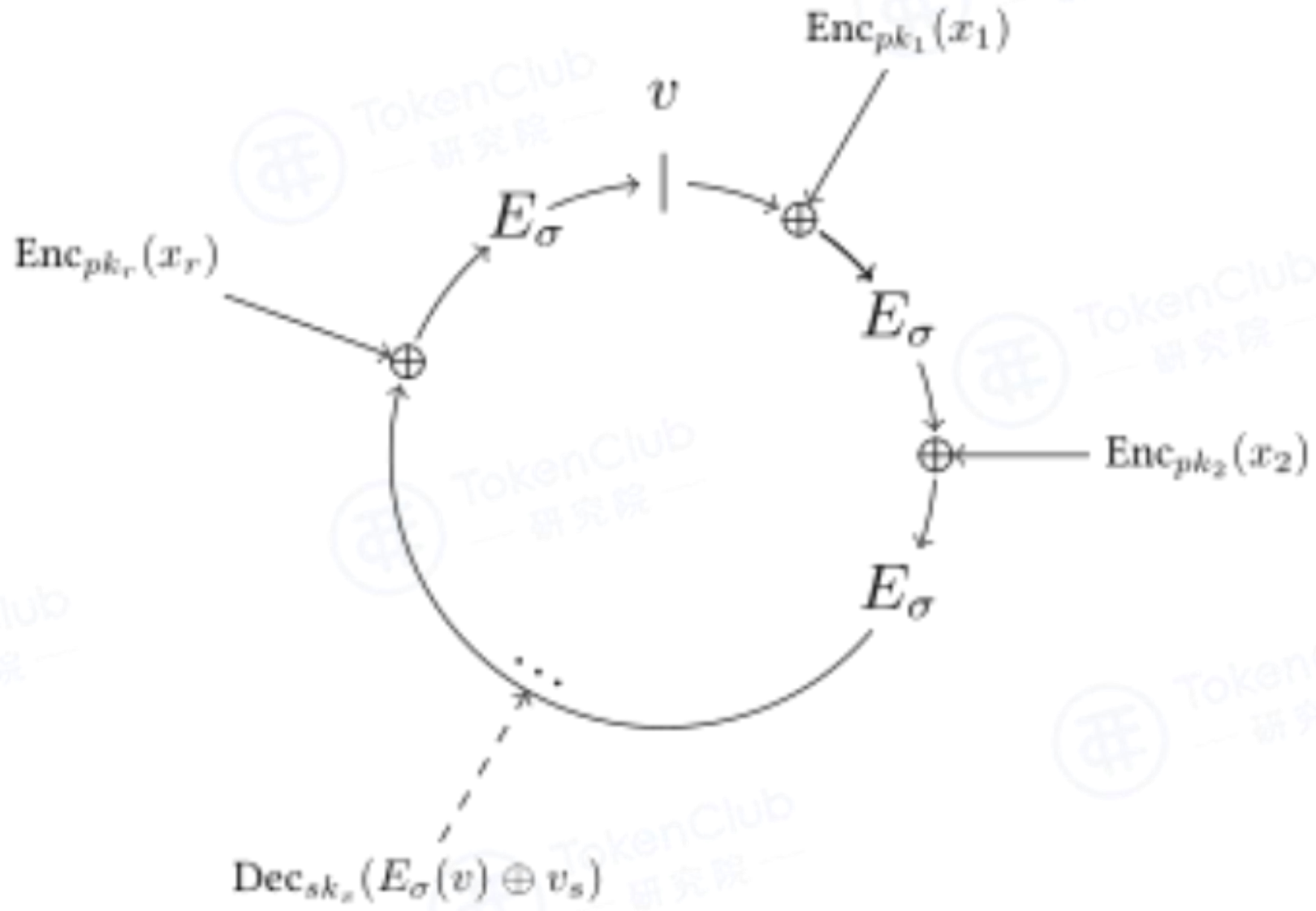
爱丽丝然后接到 P 并将其用作她的 UTXO 的目的地址。她计算散列值 R，其中 R=rG。她将 R 值打包到她的消息中并广播交易。随后，Bob 的钱包软件用他的私钥检查通过网络的每个交易，并且可以通过使用（a，b）完成的数学计算来识别发往他的地址的交易。一旦 Bob 识别出给他的输出，他就可以通过使用 x（上面的 P 的私钥）签名来恢复相应的一次性私钥并在将来的任何时间点花费资金。

因为知晓 r 是恢复一次性私钥的必备条件，所以 Alice 可以通过发布 r 或使用她知道 r 的零知识证明来提供她发送付款的可验证的证据。

2.2.2 环形签名

发送 Monero 需要用户花费一些与一次性公钥 P 关联的 XMR，正如前述的讨论所言。发币人必须通过签署一条消息来提供可验证的所有权证明，该消息将 P 与其对应的私钥 x 一起消耗掉。到目前为止，没有人知道 Bob 收到了 Alice 的付款（当然不是 Alice）。但无限期持有资金对 Bob 来说并无实际用处。他还需要花费这些资金的方法，而且要不留任何痕迹。

为了保持更强的匿名性，Monero 采用了 CryptoNote 白皮书中提出的一次性环形签名技术。环形签名通过允许发件人加入群组，然后将交易作为一个单元而不是用单个私钥签名。这种技术给发送者提供方法混入人群。验证方可以证明输出存在，该组中某一方是真正的签名者。但无法确定签名者是哪个小组成员，因为每个成员都拥有同等权重。随着组大小的增加，每个成员成为真实签名者的概率会也降低。



环形签名示意图

环形签名集合了用户的真实 P，以及分散在区块链中的过量的“模拟”的 P。签名由所有 P 验证，并且在数学上任何相应的私钥都可以签署该交易，从而混淆了真实发币人的身份。

为了防止双花攻击，在构造环时要创建一个秘钥镜像。该镜像是通过取 P 的哈希值，并与私钥 X 相乘来创建。该数学关系使得签名者不可能尝试用不同的 I 和相同的 x 制作两个签名。这种机制确保每个 P 只能用一次，新的 XMR 不能凭空创建。Monero 网络维护一个包含所有未完成密钥映像的数据库，因此，如果用户尝试再次使用该密钥，网络将看到输出已用完，并拒绝该交易。

2.2.3 环保密交易

隐形地址和环签名的组合让发币人和收币人的隐私都能受到保护。但是，CryptoNote 白皮书没有说到实现对转账金额的掩盖。如果 Alice 支付 Bob 5XMR，Bob 随后支付 Bruce，Alice 可以通过追踪手续费值来拼接交易链的各部分。

保密交易（环 CT）是 Monero 协议实施的一项措施，可以使交易价值对发送方和接收方之外的任何人都不透明。该协议通过让发送方使用交易各方间的共享密钥加密来实现这一点。然后，接收方能够使用其私人查看密钥和交易公钥的组合来解密该值。第三方仍然能够验证值的完整性，并确保新的 XMR 并非凭空创建，甚至都不需要查看金额。这是通过称为 Pedersen 承诺的密码方案实现的。

2.3 门罗币匿名性的不足

尽管 Monero 通过隐形地址、环形前面、环保密交易来提升自己的匿名性，其匿名程度远高于大多数加密货币，但是仍然有被攻击的空间。以下是三种可能的攻击方式：

EAE 攻击：这涉及从交易所向 Alice 转账，然后稍后返回交易所。存储各种 KYC/AML 信息的交交易所将得知 Alice 的一次性环签名。如果任何环签名引用了 Alice 从交易所收到的 UTXO，则交易所就能知道 Alice 是可能的发送者。

关键镜像重用：这种形式的攻击可能来自分叉网络，其中来自原链的私钥在新链上被重用（暂且称之为网络 MoneroB），环上的相同关键镜像现在同时存在于两个分叉链上。

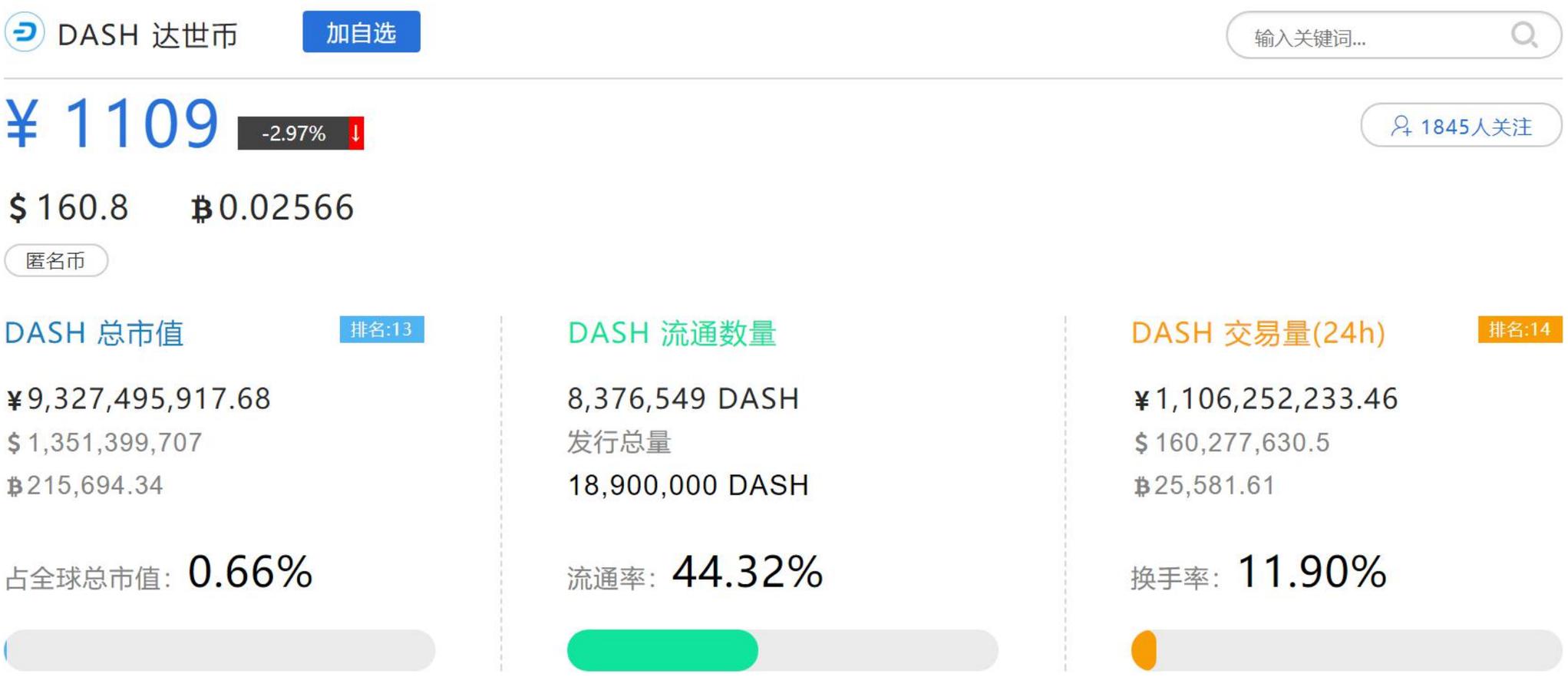
Alice 发送 XMR 到新的原链钱包，使用诱饵输入 1、2、3、4、5 和她的真实输入 6。同样地，她转账给 MoneroB 上的一个新地址，用输入 6 和诱饵输入 7、8、9、10、11 构建环。第三方可以分析这两条链并得出结论，输入 6 是真实的承诺，因为它存在于两个环中。这种情况下的一个主要问题是 Alice 的输入 6 又被用作别人构建环的诱饵（称他为 Bob）。Bob 的环由诱饵 6、12、13、14、15 和真实的 16 组成。第三方旁观者现在可以得出结论：6 是一个诱饵（因为他们已经发现它属于 Alice），这就将环的模糊因子减少了一个。通过聚合足够的信息，旁观者可以不断补充拼图，通过排除真实签名者的可能性而大大降低环的安全性。

小环攻击：与上述场景紧密相连的是，小环增加了旁观者确定环内可靠输入的概率。费用随环的大小变化，因此有动力部署较小的环，特别是对那些“无所遁形”的环来说。在攻击者可以排除某些诱饵的概率情况下，较小的环只会使攻击变得更加简单。

结论：由于门罗币的中继、发送方、接收方和交易信息都是匿名的，门罗协议提供的匿名级别异常高，尽管无法做到绝对的匿名，但是以目前的匿名程度已经可以在暗网的非法交易中规避掉监管，加之相比于其他竞争币更加的去中心化，所以目前门罗币市值位居各大匿名币的头把交椅。

3. 达世币-DASH

达世币 DASH 原名叫做暗黑币，是一款以比特币为基础，改进并添加了诸如双层奖励制网络---也称为主节点网络，等多项新功能的加密数字货币。其中还包含为提高可互换性的匿名支付（Darksend），和在不依赖中心权威下实现即时交易确认的即时支付功能。



达世币是目前市值排名第二的匿名数字货币，有时市值会超过门罗位列第一。目前 DASH 单价 160.8 美元，总市值 13.51 亿美元，排名第 13 位。

3.1 达世币特点

除了匿名性，达世币还有这些特点：

01 主节点激励

即时交易 02

3.1.1 主节点激励机制

比特币网络全节点锐减的主要原因是缺乏对运行节点的奖励。随着时间的推移，全网接入的用户会更多，对带宽的需求会更高，对节点运行者的资金需求也更多，结果使运行全节点的成本提高。考虑到成本的上升，节点运行者必须要降低他们的运行成本或者运行轻客户端，但这样完全不利于网络健康。

正如比特币网络一样，达世币的主节点也是全节点，但不同的是主节点必须对全网提供一定的服务，并需要一定量的押金才能加入。押金不会丢失，在主节点运行时也是安全的。这可让投资者为全网提供服务的同时，赚取一定的投资收益，减少了价格的波动性。

运行一个达世币主节点，需要存储 1000DASH。当主节点生效时，它可为全网的客户端提供服务，并以利息的形式获取奖励。这就使得用户为这项服务投资，但同时得到一定的回报。主节点获取的收益是来自同一个矿池，大约有 45%的区块奖励纳入到这个计划中。

3.1.2 即时交易

使用主节点的 Quorum，用户能够发送和接收即时不可逆转交易。一旦 Quorum 形成，该交易的输入被锁定到对应的特定交易去，而目前全网交易锁定的时间是大约 4 秒。如果在主节点网络达成锁定的共识，所有与之冲突的交易和区块将被永远拒绝，除非它们能匹配当时锁定的交易对应 ID。

这将允许商家在现实商业中使用移动设备来替换传统 POS 机器，用户可像使用传统纸币一样快速进行面对面的非商业交易，这段过程没有中心权威的干预。正是因为 DASH 即时交易的机制，使得 DASH 的使用体验要好于其他匿名币，也因此 DASH 是目前使用最为广泛的匿名币。

3.2 达世匿名技术

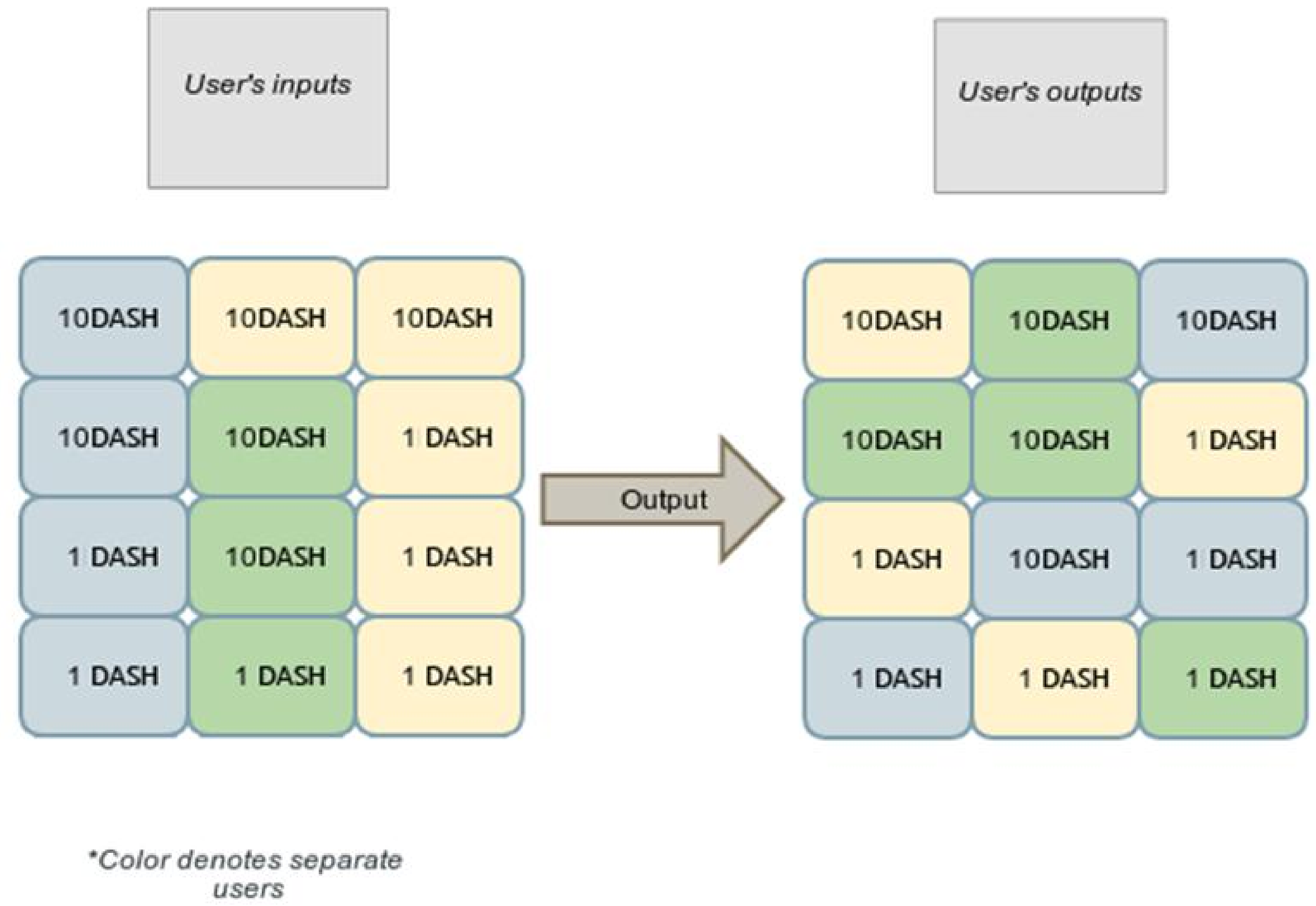
达世币的匿名技术是通过主节点混币的方式实现的，这种技术被称为 Darksend。Darksend 是 CoinJoin（提供匿名技术的软件）的改进和扩展版本。除了拥有 CoinJoin 的核心理念，还进行了一系列的改进，例如去中心化、使用链接实现强匿名、相同面值和被动先进的混币技术。

DASH 使用数字货币范围内去中心化的混币服务，能让货币本身具备完全可互换的能力，可互换性是金钱的属性，决定货币的各单位要保持平等。当你以通货的形式接收资金时，资金不应该保留之前用户的使用记录，或者用户能很轻易地与之前的使用历史撇清开来，从而做到所有货币是平等的。与此同时，任何用户在不影响他人隐私的情况下，保证公共账本的每笔交易都是诚实的。

为了提高可互换性和保持公共区块链的诚实性，DASH 使用先进的非信任制去中心化混币技术，为了保持通货的可互换性，这项服务直接整合到这个货币体系中，对于每个用户而言都可容易和安全使用。以下是达世币匿名性的技术概要：

3.2.1 增强隐私

多方的交易可以合并为一个交易，Darksend 很好地利用了这点，它将多方的资金合并在一起对外发送，这样一旦整合后就无法再次拆分。考虑到 Darksend 交易是专门为用户支付设置的，这个系统是高度安全防盗窃，用户的货币也十分安全。目前，使用 Darksend 的混币技术至少需要 3 方参与，如下图所示：



三个用户的资金合并到一个共同交易，用户会以新的打乱过的形式对外输出资金。在每轮混币过程中，所有用户应该以相同面值的形式输入和输出资金。除了使用相同面值外，交易手续费会被移除，而且所有交易会分解成分散的、独立的、前后没有关联的小交易。

3.2.2 被动的资金和区块链匿名

Darksend 每轮的混币限制为 1000DASH，并多轮混币才能匿名混合相当数量的资金。为了让用户体验方便和攻击变得困难，Darksend 以被动的模式运行。同时设定时间间隔，用户的客户端要通过主节点连接其它客户端。一旦进入主节点，用户要求需要匿名的面值数额会在全网依次排队广播，但是没有信息会将用户的身份暴露出来。

每轮的 Darksend 过程可视为增强用户资金匿名性的独立事件，然而每轮只限制 3 个参与者，因此观察者有三分之一的机会追踪交易，为了提高匿名的质量，会采用链接的方法，将资金通过多个主节点依次发送出去。

3.2.3 使用中继系统遮掩主节点

即便 Darksend 经过多轮混币技术，但是还是有一定概率追踪到单一交易，这可以进一步通过遮掩主节点加以强化，使他们不能看到用户输入/输出方向。要做到这一点，DASH 提出了一个简单的可让用户保护自己的身份的中继系统。

DASH 不让用户向矿池直接提交输入和输出的交易，而是让他们从全网随机选择

主节点然后要求它将输入/输出/的签名中继传输到目标主节点。这意味着，主节点将接收 N 次的输入/输出和 N 组签名。每轮混币只为其中一个用户服务，但主节点无法知道究竟是哪个用户。

3.3 达世币匿名性的不足

同门罗币一样，DASH 也无法做到完全的匿名，其显性表现在主节点在用户资金流过时有可能进行“窥探”。由于每个主节点都被要求持有 1000 DASH 和用户选用随机主节点来部署他们的资金，所以“窥探”的影响性不大。通过区块链追踪交易的概率计算如下所示：

攻击者控制的主节点数 / 总主节点数	区块链深度	成功概率(n/t)r	所需的 DASH
10/1010	2	9.80e-05	10,000DASH
10/1010	4	9.60e-09	10,000DASH
10/1010	8	9.51e-11	10,000DASH
100/1100	2	8.26e-03	100,000DASH
100/1100	4	6.83e-05	100,000DASH
100/1100	8	4.66e-09	100,000DASH
1000/2000	2	25%	1,000,000DASH
1000/2000	4	6.25%	1,000,000DASH
1000/2000	8	0.39%	1,000,000DASH
2000/3000	2	44.4%	2,000,000DASH
2000/3000	4	19.75%	2,000,000DASH
2000/3000	8	3.90%	2,000,000DASH

考虑到 DASH 的有限供应（此时此刻撰写白皮书时有 530 万个 DASH 在流通）和市场上低的流动性，在一次攻击中控制如此之多的主节点是不可能的。通过遮

掩主节点上发生的交易来扩展系统，也会大大提高系统的安全性。

另一方面，与 XMR 不同的是 DASH 的地址余额也是透明的，通过区块链浏览器可以查询到地址上 DASH 的余额。

Richest Addresses

Top 1000

Rank	Address	Amount	Percent of coins	Last Change
1	Xm9TJiJ7...	106,426.43 DASH	1.27 %	31 days 9 hours
2	XtbJQV8R...	77,379.51 DASH	0.92 %	92 days 23 hours
3	XtAG1982...	71,395.04 DASH	0.85 %	14 days 6 hours
4	XvwKzdsn...	40,856.49 DASH	0.49 %	36 days 23 hours
5	XbtvGzi2...	37,097.11 DASH	0.44 %	4 years 225 days
6	XcKvX5Se...	31,025.18 DASH	0.37 %	287 days 9 hours
7	XfcR4wHQ...	21,435.34 DASH	0.26 %	317 days 10 hours
8	XxXhd59h...	20,693.46 DASH	0.25 %	81 days 3 hours
9	XfcLDYdv...	20,217.12 DASH	0.24 %	1 hour 17 minutes
10	XiuyLbVT...	19,604.58 DASH	0.23 %	116 days 17 hours

总之，DASH 通过主节点混币的方式实现了它的匿名性，并且提供了三种用户转账的方式，其中包括：

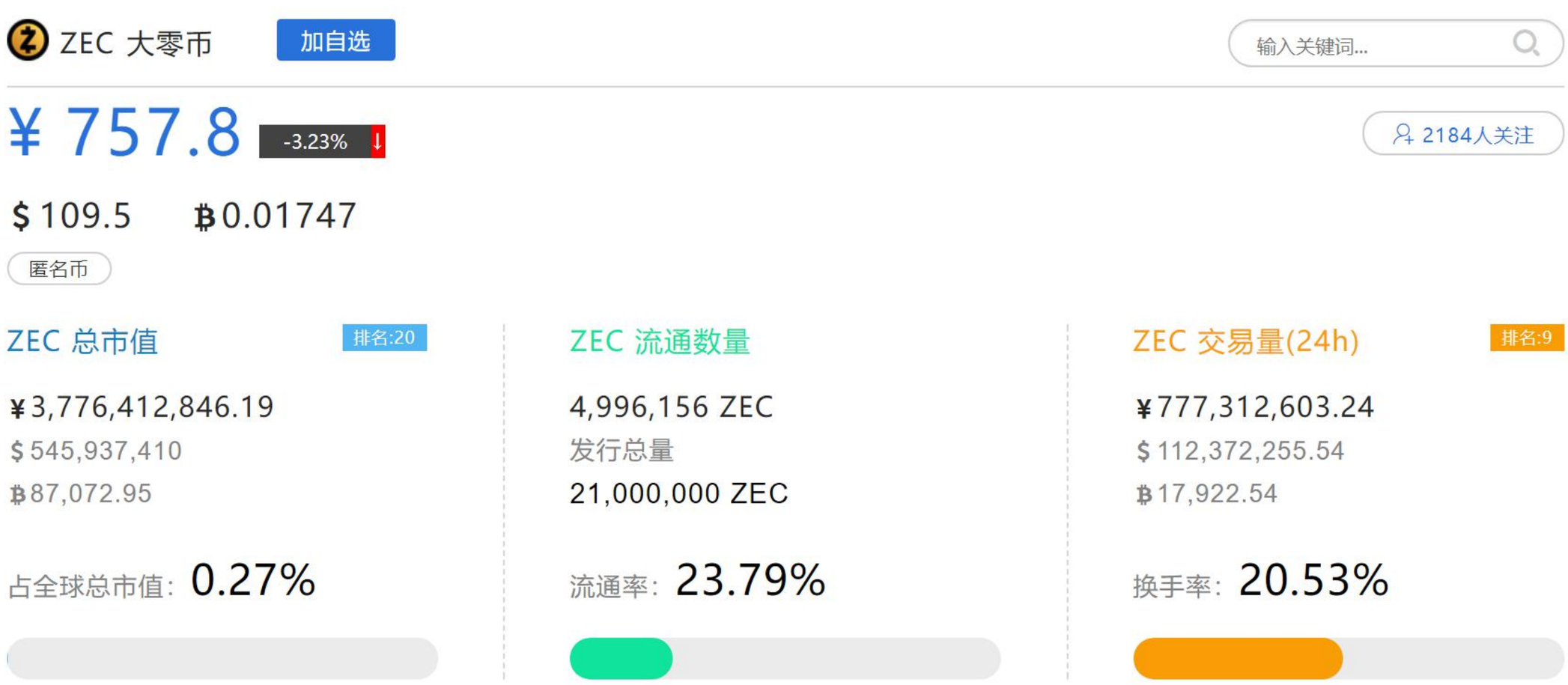
普通转账：像比特币一样需要矿工确认；

即时交易：需要经过主节点，不需要矿工打包确认

匿名交易：需要经过主节点，无法从链上查到交易

4. 大零币-Zcash

大零币 Zcash 是首个使用零知识证明机制的区块链系统，它可提供完全的支付保密性，同时仍能够使用公有区块链来维护一个去中心化网络。与比特币相同的是，Zcash 代币（ZEC）的总量也是 2100 万；不同之处在于，Zcash 交易自动隐藏区块链上所有交易的发送者、接受者及数额。只用那些拥有查看秘钥的人才能看到交易的内容，用户拥有完全的控制权，他们可自行选择向其他人提供查看秘钥。



大零币是目前市值排名第三的匿名数字货币，也是匿名性最强的数字货币。目前 ZEC 单价 109.5 美元，总市值 5.46 亿美元，排名第 20 位。

4.1 大零币特点

4.1.1 史上单价最高

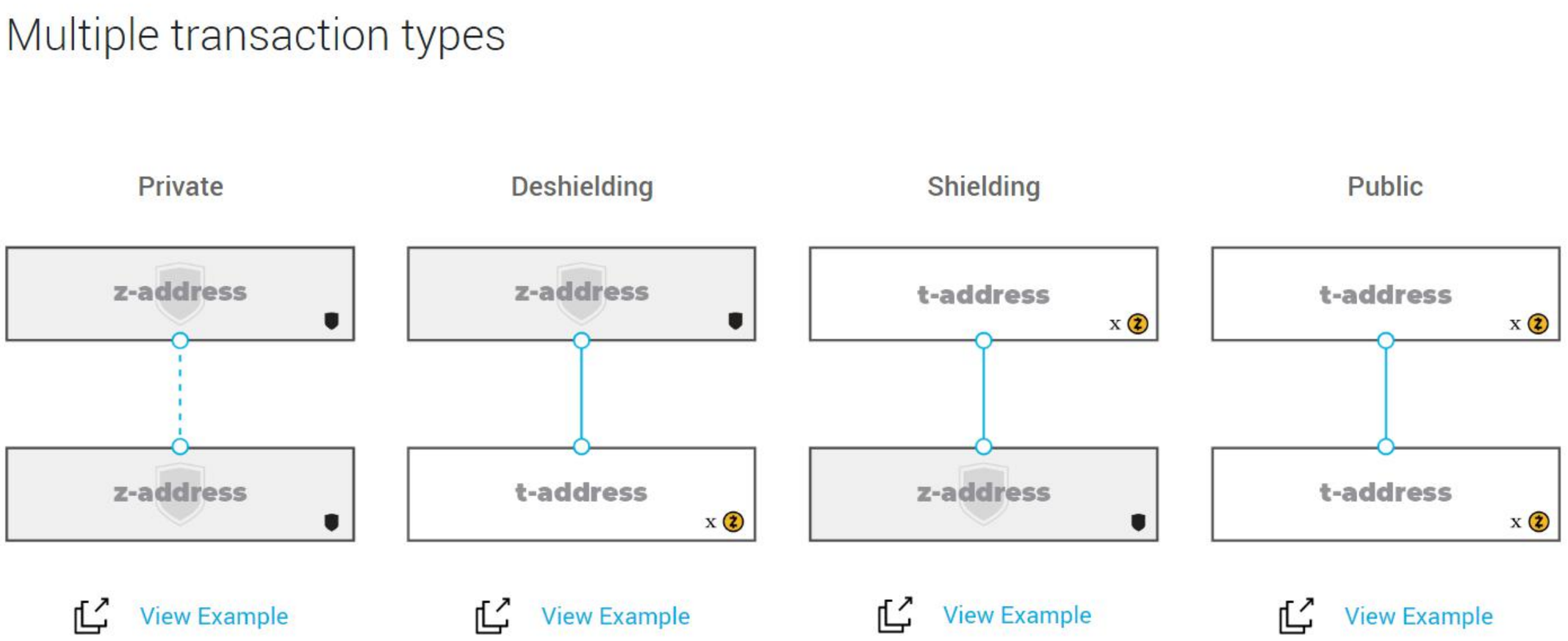
2016 年 10 月 28 日，Zcash 在 P 网正式上线，一个币的单价，一度冲到 3300BTC，相当于 200 万美元。参考 BTC 在去年牛市最高涨到 2 万美元，目前还有很长的路要走。

Zcash 的备受追捧，来自于它的终极匿名技术——“零知识证明”，通过这项技术可以做到绝对的匿名性。此外，由于它早期流通量低，稀缺性高；以及加密数字货币圈内的重量级人物包括 Gavin Andresen、Vitalik Buterin、Roger Ver 等人的支持让它备受追捧。

但是在随后的几天内，ZEC 的价格迅速下降到 0.1BTC，从 200 万美金左右，直接跌到 75 美金，跌幅近 99.999999%。

4.1.2 可选择性匿名

目前三大匿名币种中，只有门罗币的所有交易是处于匿名状态下，而 Zcash 与 DASH 的交易是可以选择匿名与非匿名两种交易形态。用户可以选择在匿名地址与非匿名地址之间相互发送，这样就有四种交易情形，如下图：



因此，在 Zcash 的显名交易中，不仅可以在区块链浏览器上查询到 Zcash 的交易信息，也可以看到显名地址上 ZEC 的数量。

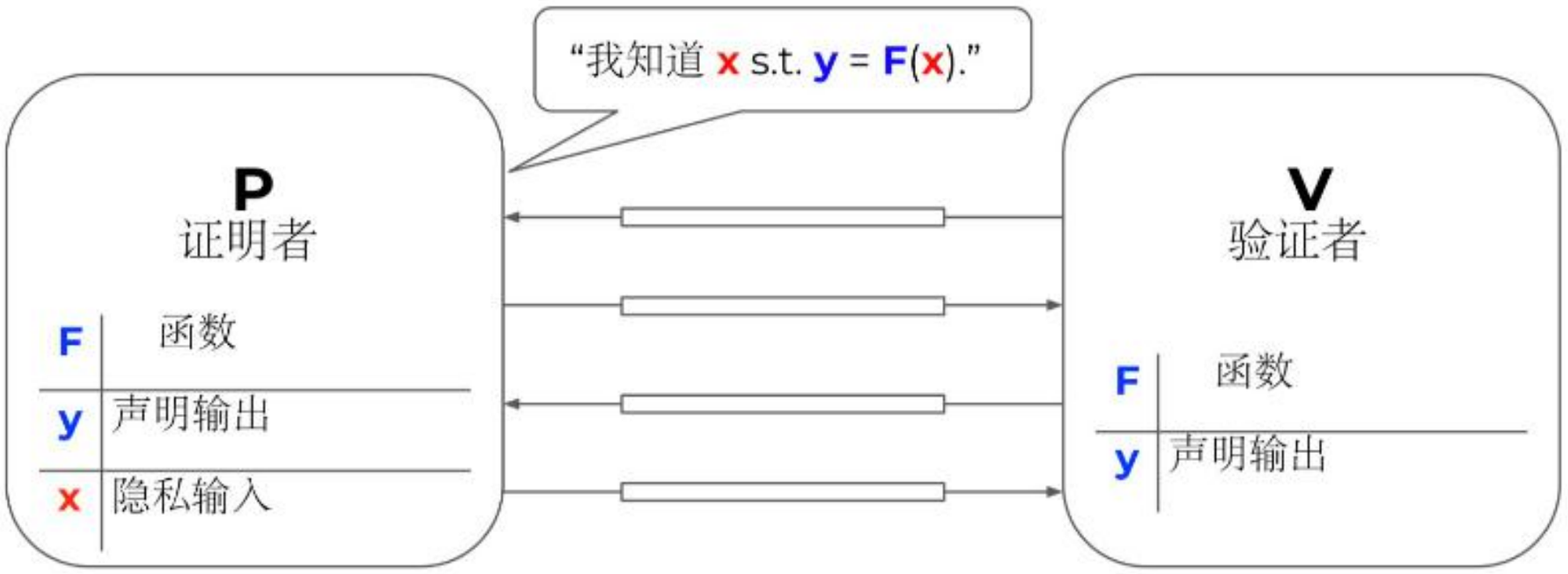
4.2 大零币匿名技术

相对于其他的匿名数字货币，Zcash 实现了绝对的匿名性，这个技术就是零知识证明。

4.2.1 零知识证明原理

零知识证明(Zero—Knowledge Proof)，是由 S.Goldwasser、S.Micali 及 C.Rackoff 在 20 世纪 80 年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

计算完整性的隐私保护密码证明。



完整性	∃ x: $y = F(x)$ → Pr[**P**(F,y,x) convinces **V**(F,y)]=1
正确性	∄ x: $y = F(x)$ → ∀ **P'** Pr[**P'** convinces **V**(F,y)]≈0
零知识	∃ x: $y = F(x)$ → **S**(F,y) ≈ view of **V**(F,y) after talking to **P**(F,y,x)

模拟器

零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任

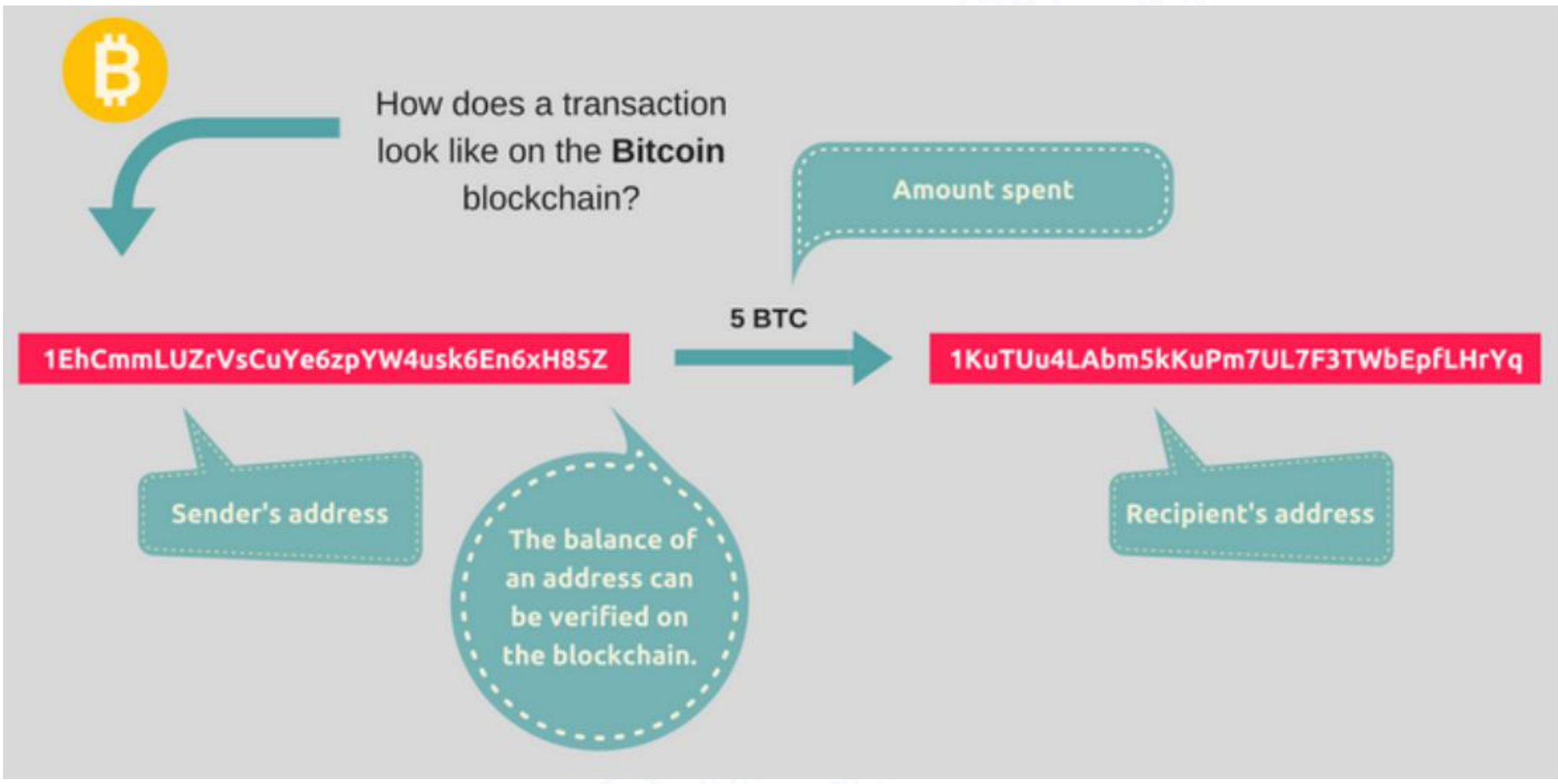
务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。大量事实证明，零知识证明在密码学中非常有用。如果能够将零知识证明用于验证，将可以有效解决许多问题。

4.2.2 零知识证明的改良——zk-SNARKs

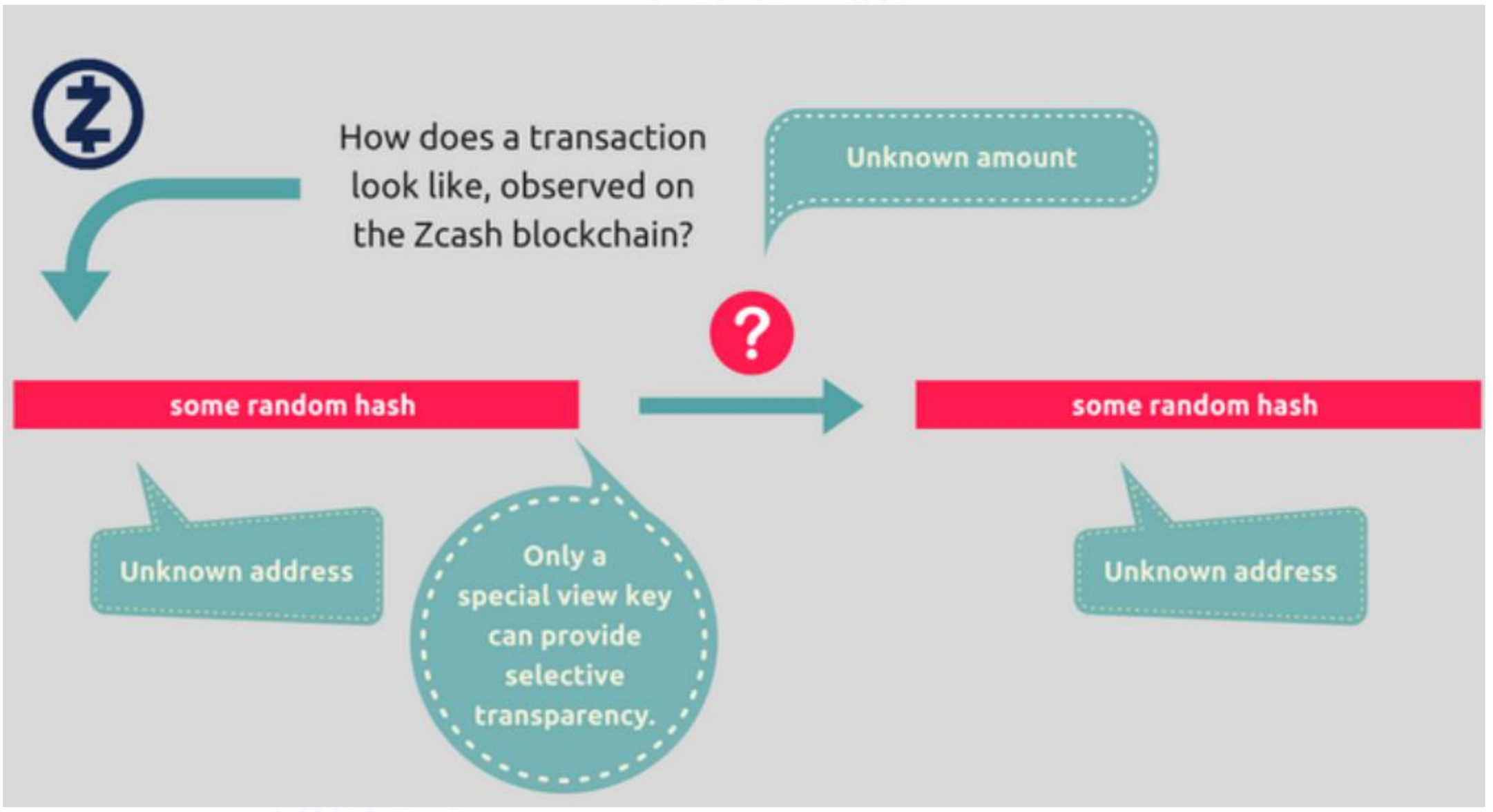
Zcash 是首个使用零知识证明机制的区块链系统，加密交易原数据，交易 100% 全匿名，同时仍能够使用公有区块链来维护一个去中心化网络。用户可以享受使用公链的优势，同时确保个人隐私不泄露。它会自动隐藏区块链上所有交易的发送者、接受者及数额。完整的交易输出并不是由 Zcash 节点保存的，只是使用称为 zk-SNARKs 的证明机制来记录花费币的能力。

涉及匿名地址，就要用到一个 zk-SNARKs (零知识非交互式证明) 隐匿交易信息，只有掌握正确的查看密钥（view key）者，才可访问这些内容。用户可自行选择哪些人可以拥有这种权限。

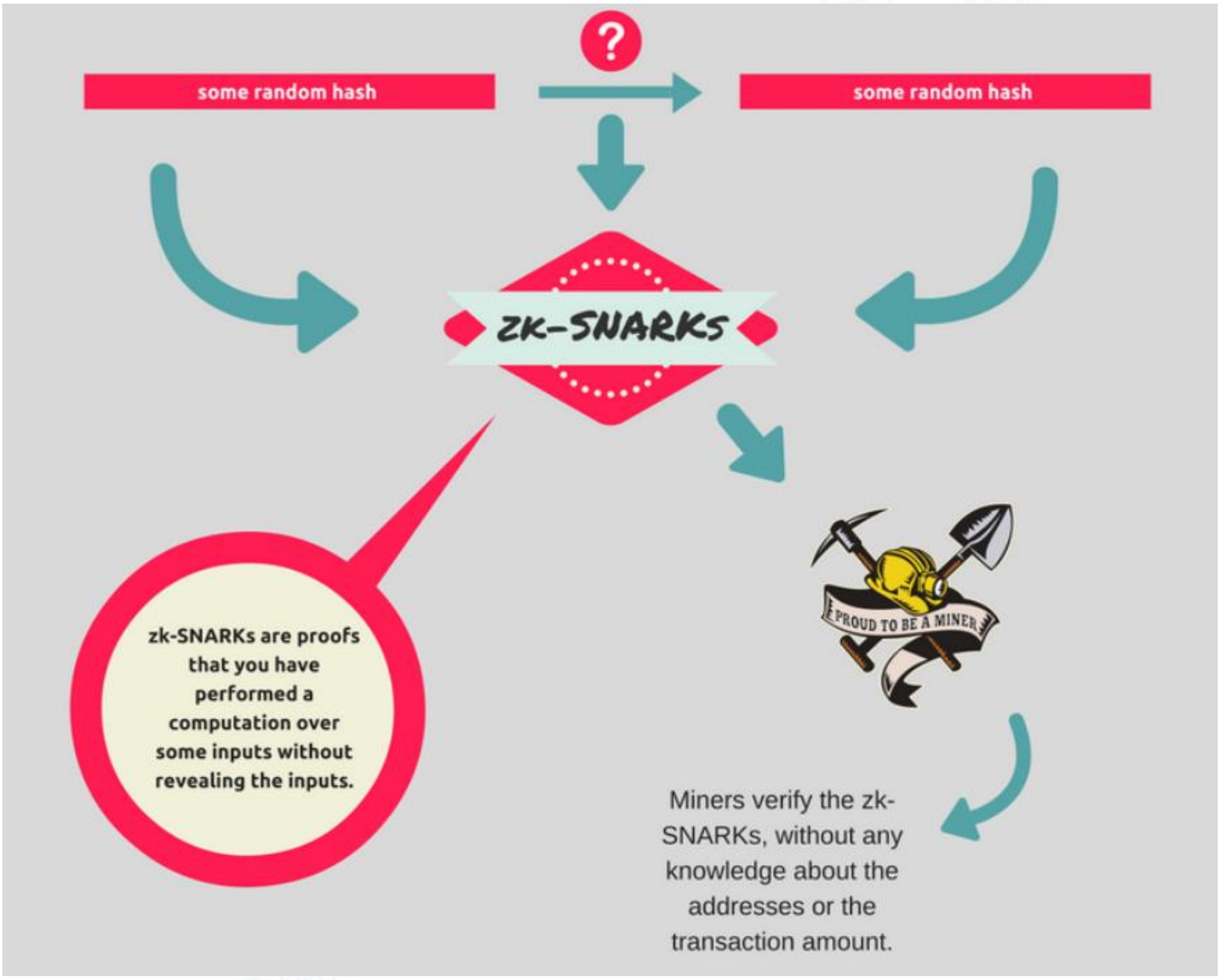
通过比特币与大零币转账之间的差异，可以更直观的了解 zk-SNARKs 的原理。比特币转账的过程中，所有的交易信息、地址余额都可以在区块链上确认，整个过程都是透明的，如下图所示：



而大零币匿名交易的过程中，地址、交易数量甚至交易的 HASH 都是被隐匿起来，只有持有私钥才能看到自己地址上的余额，如下图：



这就涉及到一个问题，区块链是通过矿工进行记账，而矿工是作为交易的第三方，如果关于交易的一切数据都被隐藏了，那么矿工如何对这笔交易进行打包记账呢?



上图可以反映出，这笔交易的信息被反映到了 zn-SNARKS 中，它证明了你已经在不显示输入内容的情况下对某些交易执行了计算，矿工只需要验证 zk-SNARKs 而不需要知道任何关于地址上的信息就可以打包这笔交易。

4.3 大零币的缺陷

在匿名程度上，Zcash 可以说做到了百分之百，但是在其他地方还是暴露出了一些问题。

首先，绝对的匿名并不一定满足市场的需求，从刚上线的暴涨暴跌能够看出零知识证明有时会被当做一个炒作的噱头，而后面再暗网上的应用也反映出 ZEC 相对于 XMR、DASH 来说并没有太大的竞争力。

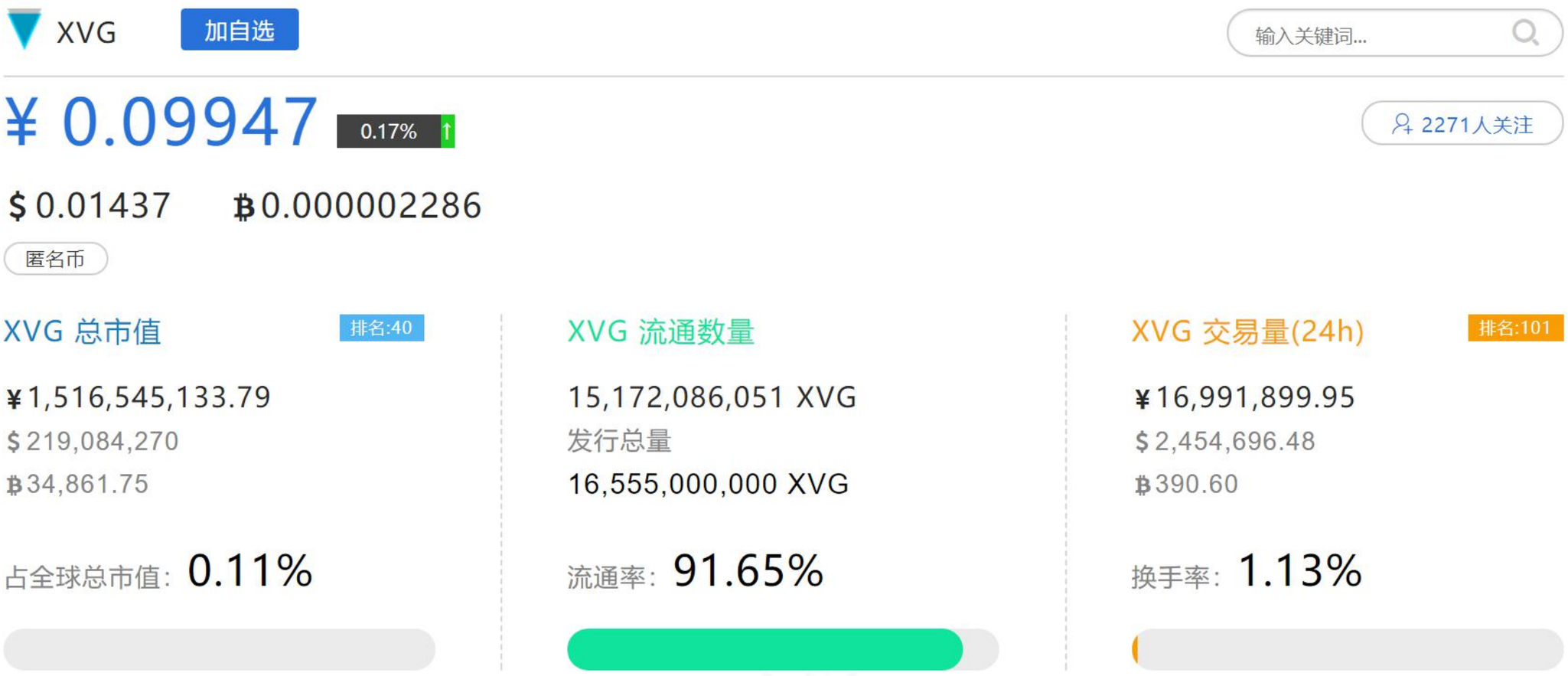
其次，匿名交易取决于用户的接受。目前只有不到 1/3 的交易是匿名的，部分原因是由于它们费用更高和传播时间更长。在进出不同的地址时，低应用率为交易分析打开了潜在的大门。在大多数用户都适用显名交易的时候，这抵消用户主权，导致安全性在某种程度上依赖其他用户的行为。

另外，相比于门罗币，Zcash 治理结构更显集中，权力严重中心化。Zcash 对协议变更的有效垄断再加上 10%的创始成员挖矿奖励税，造成用户群拥有更少的自主权。

5. 其他匿名数字货币

5.1 Verge-XVG

Verge 币于 2014 年 10 月 9 日发布，英文简称 XVG，是基于比特币技术的开源加密货币，核心算法为 Scrypt、x17。该币种在 2014 年时以“暗黑狗狗币”的名义被推出，在 2016 年时，才被改名为 Verge。它的供应总量为 165.55 亿，流通市值 2.19 亿美元，排名第 40 名。



在匿名性上，Verge 采用多重匿名中心网络，如 TOR 和 I2P。用户 IP 地址可以混淆，交易完全无法追踪。使用 Verge 付款的用户知道他们保持匿名并且他们的个人数据被隐藏。

作为一款匿名数字货币，它的特点在于小额支付。通过简单支付验证（SPV）技

术使得平均交易确认时间缩短到 5 秒，内存块链技术允许在全球处理非常快速的交易。要使用这种数字货币，只需要安装钱包软件，即可用于所有主要平台。由于 XVG 的便利性，使得它被一些商家、酒吧甚至 Pron 这样的网站所接受。

但是由于市值较低，用于维护的算力不足，XVG 在今年遭受了 51%攻击，这也给用户的信心蒙上了一层阴影。

5.2 科莫多币-Komodo

Komodo 是一个以隐私为中心的加密货币，结合了 ZCash 的匿名性和比特币的安全性。Komodo 团队开发了新的共识机制，延迟工作证明，Komodo 块可以使用比特币区块链进行公证。KMD 是通过基于 Equihash 的 PoW 协议发布的，新的块信息被发送到预先投票的公证人节点。这些节点通过创建自定义事务在 BTC 区块链上插入 Komodo 块信息。

KMD 目前流通量 1.1 亿枚左右，总市值达 1.1 亿美元，全球排名第 60 位。与 Zcash

一样，它采用了零知识证明技术来确保其安全性，因此在交易的过程中也可以确保百分百匿名。

5.3 ZenCash-ZEN

ZenCash 是 Zclassic 的一个分支，它是 Zcash 的一个分支。它于 2017 年 5 月 23 日推出，主要用于发送安全和匿名的交易，消息和发布。同比特币类似，它使用了工作量证明的共识机制，通过 equihash 算法即可挖掘。

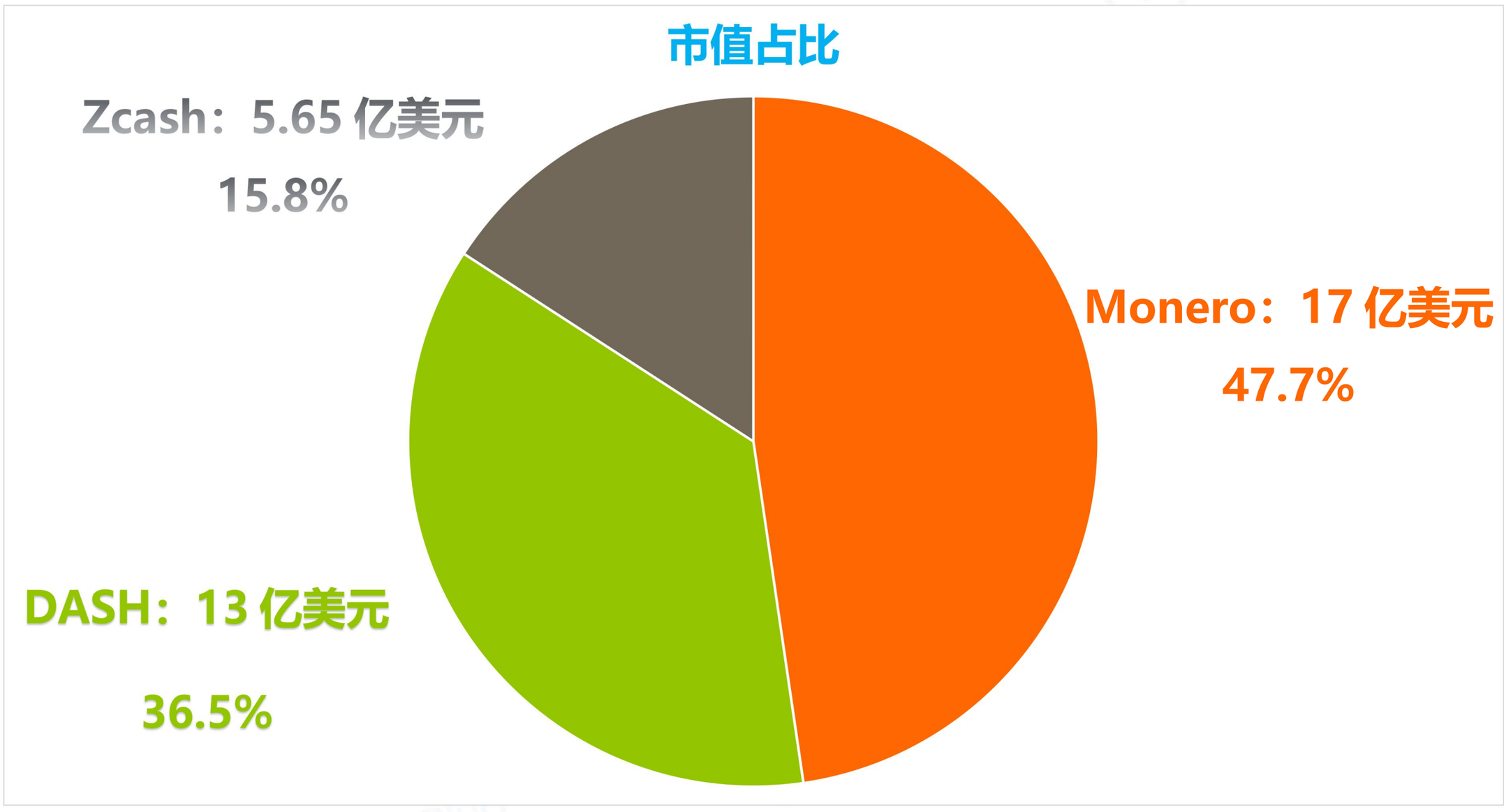
ZEN 总发行量 2100 万枚，目前流通量 492 完美，流通市值 6992 万美元，排名第 93 位。根据官网的定义，ZenCash 是一个具有领先隐私技术的区块链平台，为每个人提供隐私以及控制自己的数字资产的方案。其特点在于除了货币以外，还有包括聊天、媒体等生活上的用途。

除了上述三种匿名货币以外，还有小零币-XZC、字节雪球-GBYTE、黑洞币-BHC、深洋葱-ONION 等加密货币都采用了匿名技术。

6. 匿名币应用发展

6.1 匿名币对比

目前三大主要匿名货币市值占比大致入下图所示，其中门罗币市值最高，接近 50%，而大零币相对较小，只有 15.8%。

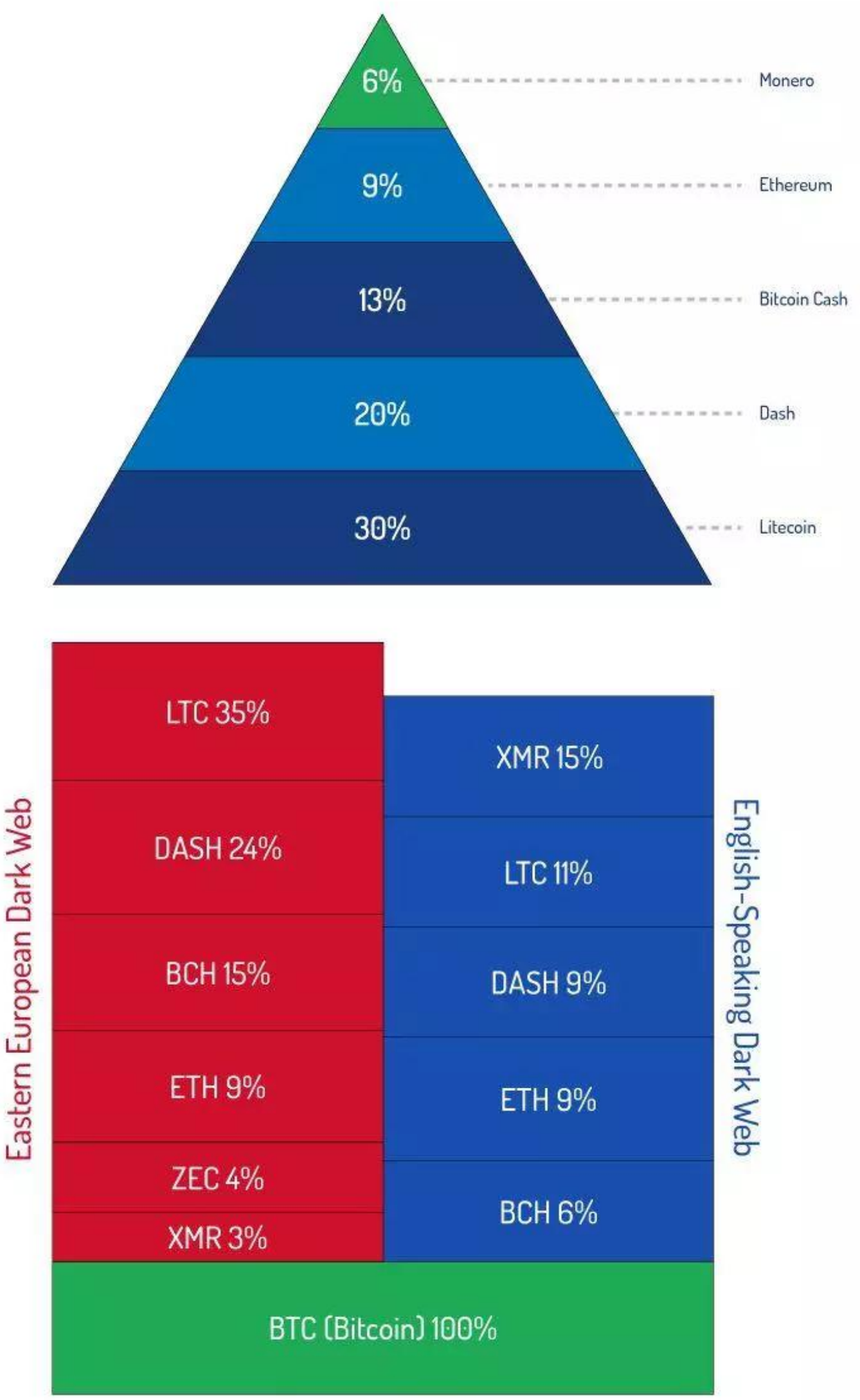


除了市值以外，其匿名程度可以通过横向比较的方式让大家有一个更加直观的了解。在加密货币中，尽管都具有一定的匿名性，但还是区分出了匿名币与“显币”。而且在“显币”中，由于比特币的 UTXO 格式，使其比以太坊的账户制形式匿名性更强。

先设置一个标准，如果把以太坊的匿名性定为 80%的情况下，那么比特币的匿名性能达到 85%，而门罗币与达世币匿名性相当，可以达到 95%，大零币的匿名性最强，为 100%。

匿名程度排名：Zcash>Monero=Dash>Bitcoin>Etherium

另外，说起匿名币，不得不提的一个领域就是暗网。比特币诞生后的早期，除了极客们转账用的玩具以及象征性的购买披萨，还没有找到大规模的应用场景。随着炒作热度的提高，以及单价的上升，比特币开始应用于暗网领域。但由于匿名性的欠缺，以及区块拥堵手续费的升高，比特币的地位逐渐被其他加密货币所取代。



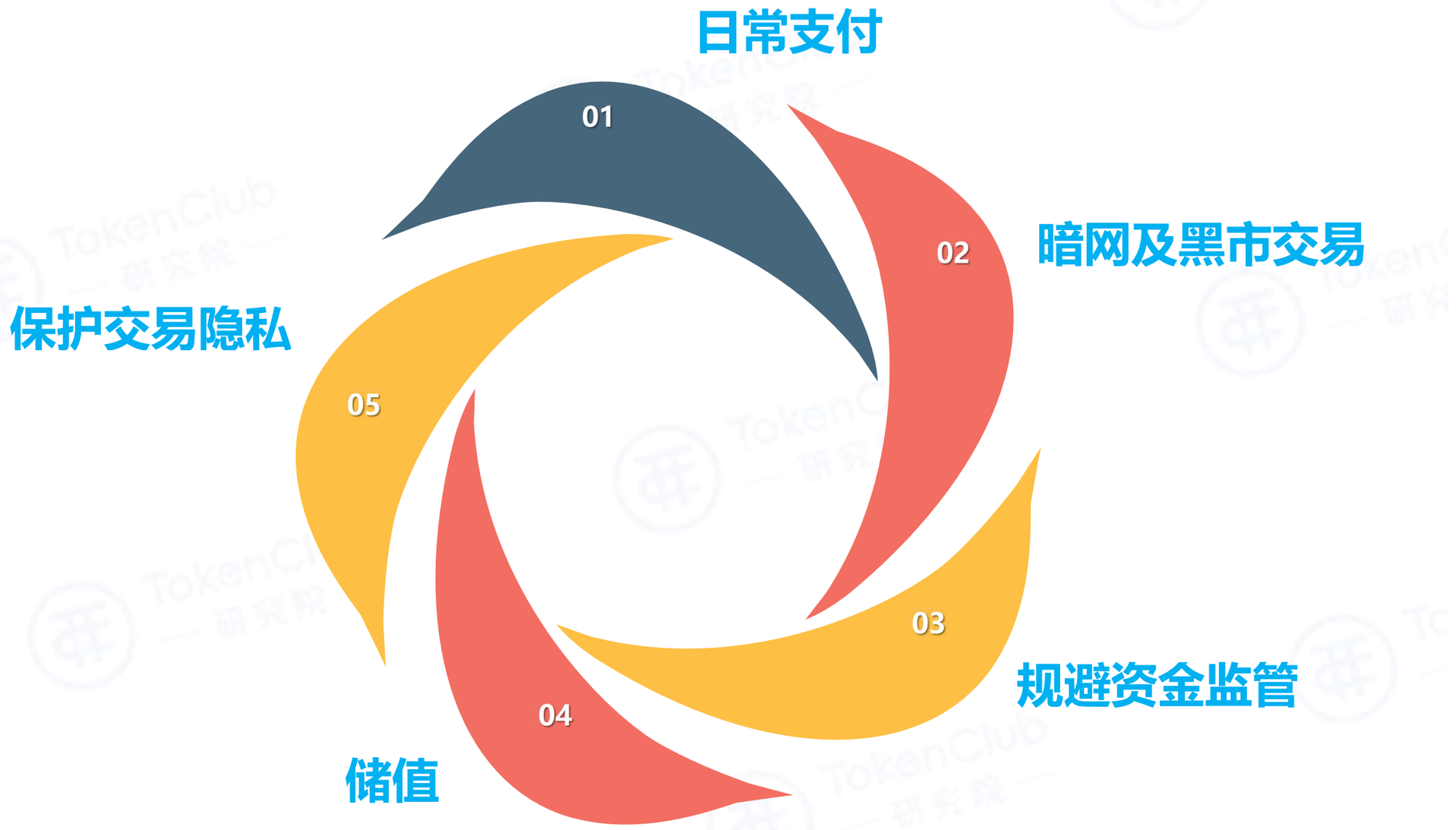
今年 3 月份，经济学家 Tuur Demeester 在社交媒体放出的一张图片显示，比特币仍在在暗网的使用中占据较大的比重。在竞争币中，应用率最为广泛的币种是莱特币、达世币、比特币现金，甚至莱特币的应用率已经超过了比特币。而匿名

币种，DASH 夺得头筹，其次是门罗，而以绝对匿名性著称的大零币用途十分有限。

在支付领域，同样也是达世币发展的最好，这主要得益于它的即时支付技术。有很多的店铺除了比特币之外，也纷纷支持 Dash、BCH、LTC 等币种，而门罗与大零币在支付领域的表现则略有欠缺。

6.2 匿名币的现实应用

匿名币是从属于数字加密货币中货币领域的一个特殊的存在，它通过匿名技术切断了地址与地址之间的关联，从而保证隐匿交易痕迹、个人资产的作用。目前匿名币在现实中已经有了一定的应用领域，主要体现在以下几个板块：



日常支付：匿名数字货币同样采用了区块链技术，而且像 DASH 这种拥有良好的支付体验，短时间内价格波动不大，因此受到了多家店铺的青睐。

暗网及黑市交易：暗网及黑市并不都是贩卖非法物品，因此很多交易使用比特币、莱特币即可进行交易而不用担心监管。但是对于一些非法交易，比特币的匿名程度无法满足规避监管的要求，于是非法人员更倾向于使用匿名币。

规避资金监管：需要规避资金监管的场所并不仅仅局限于暗网和黑市，像跨境支付、灰色收入等渠道也可以通过匿名币提升资金的私密程度。

储值：目前门罗币的地址活跃度略低于 DASH，但是市值比 DASH 要高很多。这主要是因为门罗币的去中心化程度很高，人们愿意把它当成是一种价值存储的工具。且门罗的环状签名的技术，能够保障每一个门罗币都是同质的。

保护交易隐私：即便是合法的收入，很多人也不愿意让它暴露在大众目光及资金监管之下。比如传闻吴忌寒通过门罗币支付给 Bitcoin ABC 的开发团队工资，即便这种传闻不真实但是这也是匿名币的一种很好的使用场景。

6.3 匿名币的局限

匿名币技术的推出受到了广大自由主义极客们的追捧，他们认为一个能够规避监管的加密货币更符合数字货币的完美形态，但实际上匿名币发展至今所起到的作用仍旧比较有限，比特币仍旧占据了市场上大半的份额，而匿名币则是更多给非法交易提供了方便。可见，尽管在匿名性能上进行了提升，相比于“显币”也有它自己的局限性所在，主要体现在以下三点：

为了匿名性牺牲了去中心化程度：在 3.2 章节中介绍了，达世币的匿名性是通过混币技术实现的，要增加匿名性需要增加混币轮数，而在达世币进行匿名交易的时候，它需要依赖主节点进行，这就牺牲掉了一部分去中心化的程度，这也是达世目前最为诟病的地方。

市场对匿名币需求较少：在比特币已经获得一定范围内的应用时，我们不禁思考，有了一定程度匿名性加密货币的时候，我们需要绝对的匿名币吗？实际上，市场中大部分人的资金都是合法收入，而各国政策对比特币的使用都比较包容。如果不是应用于非法领域的话，通常不会受到限制与监管。

此外，匿名币是在比特币诞生之后才推出的加密货币，当比特币具有了一定网络效应的时候，在匿名交易缺少市场需求的情况下，是很难作为匿名币的翻盘要点而存在的。目前来看比特币仍然是互联网和暗网市场的绝对硬通货，具有较稳定的市值（相比其它币）、深厚的市场深度、和广泛的接受度——这是比特币经过 10 年的发展耕耘，所积累的巨大先发优势。而匿名币的接受度仍有待提升。

来自监管的压力：在技术上，监管机构已经可以对比特币网络的交易进行监控，因而大部分黑色交易转移到了门罗、达世等匿名货币。这是匿名币在这个领域应用的优势，但也给监管与打击留下了口实。政府完全可以以打击非法交易的名义对匿名币进行打击，比如强制主流交易所下架匿名币以及通过组织大算力去干扰匿名币的网络。因此，相比于其他的数字货币，匿名币的生存环境更加的严峻。

7. 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。

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