AtoX 白皮书

2018 年 12 月 12 日

目录

摘要

如今去中心化交易承担着交易速度过慢和有限的可扩展性带来的弊端。虽然一些解决方案已经被提出，但是实现这些方案所要付出的代价，往往是限制交易对可能性的数量，或者依托中心化的交易委托平台，而中心化的交易委托簿则易受人为篡改和黑客攻击的影响，从而存在伪造交易和作弊的可能性，以及面临资金被盗的安全风险。本文为跨境交易等支付生态，构建出一套避免了上述缺陷的、从真正意义上实现去中心化的数字交易系统。我们使用“跨链闪电交易”作为核心，它利用闪电网络的可延展性使得交易方在几乎任意区块链间的高速交易成为可能，同时通过存储在 IPFS 上的脱链交易委托簿对汇率进行实时检测。考虑到对生态环境的影响，我们使用既高效节能又减轻图论问题的共识机制。

1 导语

本文旨在提供 AtoX 区块链体系结构和相应的 AXC 代币功能的概述。Section 2 奠定必要的技术背景基础，其中涵盖的专业术语将用于描述section 3 所阐述的交易脚本，以及section 4中的跨链闪电交易。Section 5将描述交易委托簿的功能。Section 6对构成闪电网络的不同节点做出区分，并且在section 7中对区块奖励体系作出解释。

历史工作。 Tiernan 在 2013 年就提出了基于哈希时间锁 (Hashed Timelock Contracts)[**ACCS**] 的 ACCS(atomic cross-chain swap，原子交叉交换) 协议，然而该协议直到 2017 年 SegWit(Segragated Witness Consensus，隔离见证) 扩容方案 [**SegWit_activation**] 的正式启用，才终于结束了它不能被真正实行的历史。SegWit 使交易延展性 (transaction malleability) 问题得以被修复，同时也使得 Poon's and Dryja 闪电网络 [**lightning_network**] 具有了能够被安全地在比特币区块链上执行 [**BTC**] 的可能性。IPFS(InterPlanetary File

System，行星文件系统) 是一个内置了版本控制的分布式文件系统，它通过内容寻址超链接，从而在区块链上进行高效的数据存储 [**IPFS**]。

第一部分 技术基础

2 理论基础

从技术角度上看，AtoX 区块链可以被看作是一个“标记状态转移系统 (labeled state transition system)，其“状态”被记录在共识分类账上。下文对其进行的解释并非深入到全部细枝末节，只是区块链技术广袤海洋中的小小一粟。

2.1 密钥和签名

AtoX 区块链使用由 [**FIPS-186-4**] 定义的经典 ECDSA 算法 (Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法)，采用被 [**Secp256k1**] 提出的，业已广泛应用在诸如比特币区块链和以太坊区块链等主链结构的 Secp256k1 参数。我们定义**密钥**为一个整数 $d \in [1, n-1]$，其中 n 满足 Secp256k1 标准。公钥则根据私钥 d，被一个**公钥生成函数**

$$PK : [1, n-1] \to \mathbf{Z},$$

所生成。因此**公钥**的形式为

$$Q \coloneqq PK(d)。$$

交易地址进一步根据公钥 Q 被生成，但由于生成该地址可以被看作完备定义的映射，因此为了表达简便，我们在这里就简单地假设交易地址等于公钥。

2.2 交易

基于比特币交易系统构架和绝大多数加密货币至少都有着与其同样的交易功能这一客观事实，我们把“交易”的概念按照下文的方式构建。

令 $v, l \in \mathbf{N}_0$。我们把 v 称为**版本号** (version number)，把 l 称为**时间锁** (TimeLock)。版本号显示了交易满足的是哪项交易标准。它的存在方便了新标准的引入，同时使旧版本的保留和向后兼容有了可能。时间锁的用途将会在后面的章节里阐述。定义**输入** (input) 为数组

$$inp = (PrTX, ind, ScrSig),$$

其中 $PrTX$ 称为**资金来源** (previous transaction reference)，ind 称为**输出索引** (output index)，$ScrSig$ 称为**签名脚本** (Signature script)。令 $1 \leq n \in \mathbf{N}$。**输入列表** (list of inputs) 则可记为一个 n-元数组 $I = I_{1 \leq i \leq n}$，这里的 I_i 是一个输入，对于所有 $1 \leq i \leq n$ 成立。定义元组

$$out = (PKS, amt),$$

为**输出** (output)，其中我们把 PKS 称为**公钥脚本** (PubKey script)，amt 则称为**金额** (amount)。令 $1 \leq m \in \mathbf{N}$，**输出列表** (list of outputs) 则被定义为 m-元数组 $O = O_{1 \leq j \leq m}$，其中每一个 O_i 都是一个输出。现在，我们就可以把**交易** (transaction)τ 构建为一个 5-元数组

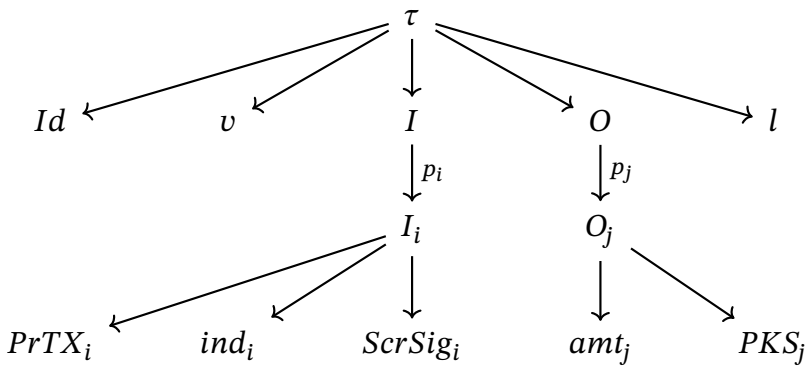
$$\tau = (Id, v, I, O, l),$$

其中

$$Id = H(v, I, O, l)$$

是单射 **TXID 生成函数** (TXID generation function)H 的值域，是一个加密散列函数。把输入列表和输出列表中的第 i 个分量上的投影记为 p_i，交易这一

概念的构成，就可以借助下图的结构进行理解：



定义 τ 的**输入集** (set of inputs) 为

$$Ins_\tau := \{x_{1\le i\le 3} | x_i = p_i(p_j(p_3(\tau))), 1 \le j \le n_\tau\}。$$

注意，Ins_τ 的每一个元素，都是上文定义的输入。定义 τ 的**输出集** (set of outputs) 为

$$Outs_\tau := \{y_{1\le i\le 2} | y_i = p_i(p_j(p_4(\tau))), 1 \le j \le m_\tau\}。$$

同样地，$Outs_\tau$ 的每一个元素也都是上文所定义的输出。我们把

$$\Lambda := \{\tau | \tau 是一个交易\}$$

记为**交易空间** (space of transactions)。令 $SCRSIG$ 表示所有签名脚本的空间。那么 PKS 则是一个二元函数

$$PKS : SCRSIG \to \{0, 1\}。$$

在后面的section 3中，我们将使用该二元函数以指定和例举各种交易。

2.3 标记状态转移系统

在上一节的基础上，我们便可以把标记状态转移系统 $(S, \Lambda, \to)$ 定义为一个满足下面性质的系统。即 $(S, \Lambda, \to)$ 满足：

1. S 是一个由一系列状态构成的集合，集合的每一个元素 $s \in S$ 都是由数组 (Id, O) 构成的有限集，其中 Id 是一个 TXID，O 是一个输出列表。

2. Λ 是一个交易空间。

3. $\rightarrow \subseteq S \times \Lambda \times S$ 是一个由标记状态转移函数构成的集合。集合的确切表达为

$$\rightarrow := \{(p, \tau, q) \in S \times \Lambda \times S | \, (p, \tau, q) \text{ 满足以下三个条件。}\}$$

   (i) 存在一个 (有限) 子集 $U \subseteq p$，对于这个子集存在一个一一映射 $f : U \rightarrow Ins_\tau$ 对于所有 $u \in U$ 满足

$$p_1(u) = p_1(f(u))$$
$$p_2(u) = p_{p_2(f(u))}(p_3(H^{-1}(p_1(u))))$$

   换句话说，τ 种的引用 (reference) 都引自于 p 中的元素。

   (ii) 等式

$$(p_2(p_2(u)))(p_3(f(u))) = 1$$

   对于全部 $u \in U$ 成立，即输入脚本的签名必须包含于 $p_2(p_2(u))^{-1}(1)$ 之内。

   (iii) 不等式

$$\sum_{u \in U} p_1(p_2(u)) \geq \sum_{1 \leq i \leq m_\tau} p_1(p_i(p_4(\tau)))$$

   成立。即 τ 输出量的总量必须小于 U 中输出的总量。

   (iv) 等式

$$q = (p \setminus U) \cup \{(Id, O_j) | Id = Id_\tau, O_j \in Outs_\tau$$

   成立。这意味着在 Ins_τ 中引用的 p 的元素被与 τ 的输出相对应的元组替换。

本文将使用 $p \xrightarrow{\tau} q := (p, \tau, q) \in \rightarrow$ 来表示集合 $\rightarrow \subseteq S \times \Lambda \times S$ 的元素。

3 脚本

现在我们来构建各种 $ScrSig$ 和 PKS 函数。对于标记状态转移函数 $p \xrightarrow{\tau} q \in \rightarrow$，$p_3(Ins_\tau)$ 中的输入脚本必须位于 PKS 的 1 次逆像中。这些输入脚本和 PKS 函数都终将由代码来定义和实现，一系列具有实用价值的协议便可以被这些代码构架并实现出来。需要注意的是，尽管以下示例仅仅用比特币 Script 语言编写，但是由于比特币脚本本质上代表了用 Solidity 语言 (以太坊脚本语言) 所编写的脚本的一个子集，因此以下的每个语句也都同样适用于 Solidiyt 脚本。

3.1 多重签名合约

令 $1 \leq n, m \in \mathbf{N}$。*$n$-$m$-多重签名合约*，或者说 **$n$-$m$-多重签名**就是一个具备如下形式的 PKS 输出：

$$PKS(y) = \begin{cases} 1, & \text{若 } m \text{ 个签名中的 } n \text{ 个有效,} \\ 0, & \text{其他。} \end{cases}$$

一个 2-2-多重签名 PKS 可以在脚本中这样实现：

```
2
< Q_1 >
< Q_2 >
2
OP_CHECKMULTISIG
```

与之相应的 $ScrSig$(另一个引用包含上述 PKS 的输出的交易) 则可以写成：

```
OP_0
< sgn_Q_1 >
< sgn_Q_2 >
```

3.2 哈希锁合约

哈希锁合约 (HashLocked contract)，简称 *HLC* 是一个具备以下 PKS 形式的输出

$$PKS(y) = \begin{cases} 1, & \text{若 } H(y) = H(x), \\ 0, & \text{其他}, \end{cases}$$

其中 H 是加密散列函数。下面是一个比特币 script 语言中哈希锁合约 *PKS* 的例子：

```
[HASHOP]
< H(x) >
OP_EQUAL
```

在这里[HASHOP]既可以是OP_SHA256也可以是OP_HASH160。相应的 *ScrSig* 是单行代码：

```
< x >
```

3.3 哈希时间锁合约

哈希时间锁合约 (Hashed TimeLock contract)，简称 **HTLC** 是一个具有非零时间锁的交易 τ，即 $l_\tau \geq 0$，此外还应有至少一个输出具有 PKS 形式

$$PKS(y) = \begin{cases} 1, & \text{若 } H(y) = H(x) \text{ 且时间锁定期满}, \\ 0, & \text{其他}, \end{cases}$$

其中 H 是加密散列函数。比特币脚本中的 HTLC 结构可以写成：

```
OP_IF
[HASHOP]
<digest>
```

```
OP_EQUALVERIFY
OP_DUP
OP_HASH160
<seller pubkey hash>
OP_ELSE
<num>
[TIMEOUTOP]
OP_DROP
OP_DUP
OP_HASH160
<buyer pubkey hash>
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```

这里[TIMEOUTOP]或者是
OP_CHECKSEQUENCEVERIFY，或者是OP_CHECKLOCKTIMEVERIFY。

4 跨链闪电交易

AtoX 区块链的核心功能之一就是跨链闪电交易。为了阐释该功能，我们首先来就跨链闪电交易的两大基本理论基础，即原子跨链交易和闪电网络分别展开讨论。

4.1 原子跨链交换

原子跨链交换 (atomic cross-chain swap) 简称 **ACCS**，是一份旨在实现把属于两个不同区块链上的代币进行交换目的的协议。本文所使用的 ACCS 协议是被 Noel Tiernan 首先提出的 [**ACCS**]。

假设 $(S,\Lambda,\rightarrow)$ 和 $(S',\Lambda',\rightarrow')$ 是两个不同的区块链。交易方 P_1 想要把自己在区块链 $(S,\Lambda,\rightarrow)$ 上的 $0 \leq n \in \mathbf{N}$ 个代币与交易方 P_2 在区块链 $(S',\Lambda',\rightarrow')$ 上的 $0 \leq m \in \mathbf{N}$ 个代币进行交换。为此，每个交易方都要在格子的持币区块链上生成两个交易：P_1 生成 $\tau_1,\tau_2 \in \Lambda$，$P_2$ 生成 $\tau_3',\tau_4' \in \Lambda'$。令 $0 \leq 2c \in \mathbf{N}$，设 $x \in \mathbf{Z}$ 是由 P_1 生成的一个加密随机整数。在不考虑手续费、交易 Id 和交易版本号的情况下，由 P_1 和 P_2 生成的上述四个交易框架如下：

$$
\begin{aligned}
I_{\tau_1} &= P_1 \text{ 资金来源} \\
O_{\tau_1} &= (n,(sgn_{P_2},x||sgn_{P_1},sgn_{P_2})) \\
l_{\tau_1} &= 0 \\
I_{\tau_2} &= ((Id_{\tau_1},0,(sgn_{P_1},sgn_{P_2}))) \\
O_{\tau_2} &= (n,sgn_{P_1}) \\
l_{\tau_2} &= 2c \\
I_{\tau_3} &= P_2 \text{ 资金来源} \\
O_{\tau_3} &= (m,(sgn_{P_1},x||sgn_{P_1},sgn_{P_2})) \\
l_{\tau_3} &= 0 \\
I_{\tau_4} &= ((Id_{\tau_3},0,(sgn_{P_1},sgn_{P_2}))) \\
O_{\tau_4} &= (m,sgn_{P_2}) \\
l_{\tau_4} &= c
\end{aligned}
$$

需要注意的是，交易双方需要把 τ_2 和 τ_4 进行互换，以便确保输入都包含必要的签名。τ_1 和 τ_3 再由交易方提交给两个交易各自所属的区块链。此后，如果 P_1 公开 x 并生成一个花费 τ_3 输出的交易，P_2 则也可以通过同样的操作花费掉 τ_1 的输出。否则，交易双方也可以通过分别推送 τ_2 和 τ_4 来找回各自的资金。下面是 τ_1 输出脚本的一个代码示例：

```
OP_IF
// Refund for Q_1
```

```
2 < Q_1 > < Q_2 > 2 OP_CHECKMULTISIGVERIFY
OP_ELSE
// Ordinary claim for Q_2
OP_HASH160 < H(x) > OP_EQUAL < Q_2 > OP_CHECKSIGVERIFY
OP_ENDIF
```

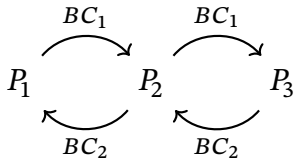
τ_2 的退款交易代码是一个输出映射到 P_1 地址的 2-2-多重签名输入脚本。

4.2 闪电通道

Poon 和 Dryja 在文章 [**lightning_network**] 中描述了“闪电网络”的概念，闪电网络的具体实行详情参见 [**BOLTS**]。简而言之，交易双方开放一个所谓的“闪电通道”，并且在闪电通道上冻结双方区块链上一定数量的资金作为交易基金。各交易方通过“闪电通道”生成脱链交易，以重新定义基金中各方所占有的份额。通道通过 HTLCs 被连接在一起，并且速度能够达到即时交易的程度。尽管交易各方都关闭各自的通道 (对每个通道都执行双侧关闭) 是更加经济的操作，但是单方进行单侧通道关闭也是完全可以的。

4.3 跨链闪电交易

通过在脱链闪电通道中发布原子跨链交换，跨越不同区块链上的闪电网络来实现价值交换就得以实现了。这使得跨链闪电网络的交易速度可以与中心化交易相媲美，而无需第三方作为起到资金缓存作用的交易平台介入。下图为 P_1，P_2 和 P_3 的三方交易示意图，其中 P_1 和 P_2 在两个不同区块链上开放闪电通道，并通过通道彼此连接，P_2 和 P_3 在上面的两个闪电网络上通过各自的通道被连接。



5 交易委托簿

建立在 IPFS 上的去中心化的脱链委托交易簿，是一个用于检索和共享 IPFS 对象的 P2P 系统。IPFS 使用 Merkle DAG 系统以确保所有被永久存储的数据都具备唯一性和防篡改性。

5.1 IPFS

IPFS 对象可以被看作是一个元组 (d, l)，其中 d 代表一个**非结构化二进制数据** $(\leq 256\,\text{kb})$，l 代表一个**链接结构数组**。链接结构是 3-元数组 (N, H, S)，其中 N 表示**链接名**，H 表示 **IPFS 对象的哈希**，S 表示 **IPFS 对象大小**。超级节点为每个交易储存以下三个文件，这些文件将持续被更新：

1. 一个包含交易委托簿的文件。只有有效交易委托 (详见下文) 才能被写入交易委托簿，部分执行的委托将被更新，而执行完毕的委托将被删除。

2. 一个将会被持续重写的，包含被成功执行的交易委托的文件。它将起到计算汇率的作用。IPFS 就像 Git repository 一样随着时间来跟踪版本，因此以往的汇率可以被从文件历史记录中其取出来，并汇聚在一起形成历史汇率表或者历史汇率图线。

3. 一个包含跨链闪电网络中当前活跃闪电节点列表的文件。

如果某个交易方 P_1 希望将区块链 A 上的 $0 \geq c \in \mathbf{Q}$ 枚代币兑换成区块链 B 上的代币，并向交易委托簿推送了一个交易委托，一下的步骤将会按顺序被执行：

```
Test, if P_1 is connected to a registered BC_A lightning node
Test, if P_1 is connected to a registered BC_B lightning node
Test, if P_1 is connected to a registered AtoX lightning node
```

```
Test, if P_1 has at least m coins on BC_A
Test, if P_1 paid its order book fees
```

交易委托簿的 Snapshots 会被存储在 AtoX 区块链上。

6 节点种类

我们在跨链闪电网络中区分四种对象类型，即用户、普通节点、备选节点和超级节点。

首先我们对通常意义上的“跨链钱包”做出概述（我们的跨链钱包以 Atox Swapp App 的形式呈现），然后对上述四种对象进行解释。

6.1 跨链钱包

钱包 (wallet) 是一个实现确定性功能的软件，这里的确定性功能则是指将加密货币的私钥映射到对应的公钥和地址。应用这些功能，钱包可以在给定私钥的情况下，重建出相应的地址，并通过添加尚未花费的交易输出量，方便地向拥有该私钥的个人显示出该地址可用的资金数量。钱包还可以重建储存在区块链上的该地址的支付历史。

虽然闪电交易的开仓和平仓交易被储存在各自的区块链上，但是基金再分配合约却由于是脱链合约的缘故，并不会被储存在区块链上。这意味着如果个人丢失了仍然开放着的闪电通道上的脱链交易历史记录 (例如储存交易历史的物理设备损坏)，那么这条闪电通道上的基金会被冻结，直到另一个交易方单向关闭这条通道为止。如果交易双方都丢失了各自的脱链历史记录，基金将永远丢失。因此，个人应该尽可能只和受信对象进行通道连接。这里的受信对象，指的是其被信任采取了例如拥有物理备份等安全设施。

跨链钱包 (multiwallet) 是多个钱包的集合，并同时具备发起跨链闪电

交易的功能，这个功能使得连接到子钱包地址的资金可以被交换。跨链钱包给人以“所有的资金都可以在一个地方进行管理”的直观感受。对于相对保守的个人而言，这样一种兼并跨链闪电交易功能的跨链钱包，可能会带来更多“货币换货币”的真实感受，而不是像股票交易那样的“代券交易”。对于喜欢冒险的个人而言，跨链钱包通过展示历史汇率和用户感兴趣的各种指标等功能，提供交易平台的体验。

从表面上看，我们的跨链钱包似乎和其他跨链钱包并无不同。然而，我们跨链钱包中的货币交换不是由任何中心化交易执行的，因而我们的技术对于终端用户来说极大地提高了安全性：私钥全部掌握在用户自己手中而不存储在“可被黑客攻击”的交易服务器。恶意方唯一盗取资金的方法只有通过获取用户的私钥，类似传统银行业务里窃取 PIN 码。

使用跨链钱包的用户需要向跨链闪电网络支付对应交易额百分之 0.2 价值的手续费。

6.2 用户

用户 (user) 用户是能够向跨链闪电网络发起交易的对象。用户可以是通过跨链钱包 APP(例如 AtoX Swap App) 与跨链闪电网络交互的人。用户也可以是连接到跨链闪电网络的交易算法实例，通过发出跨链闪电交易自动执行交易。

6.3 普通节点

普通节点 (regular node) 是为用户充当跨链闪电网络接入口的物理设备。由于我们不使用 POW(proof-of-work) 机制，普通节点因而并不需要具备巨大的计算能力。但是普通节点需要拥有稳定并且强大的互联网连接，因为它将被用作闪电网络的顶点，应该能够连续启动和运行，以充当用户间跨链闪电交易的中间人。普通节点至少应该连接至一个超级节点，超级节

点概念将在后文进行解释。作为整个网络的基础设施，普通节点获得的奖励来自以下两个方面：

1. 闪电交易手续费：这部分手续费由普通节点自己任意设置，可以随意高（或者更有可能是比较低）。闪电网络选择交易双方之间“阻力最小路径”，并以此确保手续费保持在合理的均衡状态下。换句话说，如果一个普通节点把自己的手续费设置得过高，它则不会被闪电网络选择为闪电交易中间人，因此也就赚取不到任何手续费。从另一角度来看，比较低的手续费也足以能保证节点运行成本（例如网络成本和电力费用）。请注意，由于普通节点只需要具备最低级别的硬件配置，电力成本和生态环保方面的影响会比基于 POW 的机制低好几个数量级，其副作用之小和低廉的手续费甚至不堪匹配（现实中无论各行各业，低价导致的往往是巨大的副作用）。

2. 从与之连接的超级节点处获取区块奖励分成。分成额度可以由超级节点自己设置。和交易手续费的平衡体系类似，普通节点更有可能去连接分成额度高的超级节点，所以区块奖励分成数额最终也会达到合理的均衡状态。对于超级节点来说，尽可能地被更多的普通节点连接是至关重要的，其重要性将在后文里解释。

6.4 备选节点

备选节点 (entitled regular nodes) 备选节点是拥有参选超级节点资格附加权的普通节点。为了防止试图在跨链闪电网络上建立恶意子网络的行为，我们出于安全考虑人为地设置了这一门槛。备选节点将会从至少持有 10000 枚 AXC 的，过往表现最突出的普通节点中选出。席位限定为 70 个。

6.5 超级节点

超级节点 (supernode) 超级节点也是物理设备，除了充当普通节点外，还负责验证 AtoX 区块链上新交易的完整性。跨链闪电网络的超级节点席位限为为 35 个。与普通节点类似，超级节点的奖励来源为：

1. 闪电交易手续费。与普通节点和备选节点没有区别。

2. 区块奖励。超级节点提出 AtoX 公共分类账的下一个 snapshot(即提议下一个将被添加至 AtoX 区块链的区块)。如果该区块被其他超级节点接受，它就会被写入分类账，同时成功生成该区块的超级节点将以 AXC 代币的形式获得奖励。超级节点与连接到它的普通节点们分享区块奖励。连接到某个超级节点的全部普通节点以及他们所完成的交易事务，计为这个超级节点的“贡献”，而超级节点成功生成出下一个区块的概率，则是由他的“贡献”占整个跨链闪电网络的百分比所决定的。因此对于超级节点来说，设置合理的区块奖励分享机制，吸引越多普通节点与之连接，也就越有利于其自身提高贡献百分比，从而提高获得区块奖励的概率。

7 区块奖励

区块奖励来源于两个方面。

1. 每个区块的固定奖励。它为整个系统产生新代币。

2. 以往的跨链闪电交易所收取的 AXC 手续费。超级节点因此会自然而然地被激励优先处理手续费较高的交易。

请注意，我们的共识机制与被严厉批评的传统 POW 挖矿的区别非常之大，但是我们的区块奖励机制却与之类似，因为这种奖励机制已经通过检验并且运行良好，已经被证明完全足以达到预期结果。这种奖励机制还蕴藏着

一个含义：以 AXC 形式被支付的交易手续费将会被分配给参与了交易进程的节点们。

7.1 RPCA

许多加密货币采取 **POW**(proof of work) 共识机制。这种方法通过限制首区块散列哈希的允许值集，人为地提高了生成新区块所需要的计算能力。POW 浪费了大量电能 (参考 [**energy_consumption**] 和fig. 1，可以用 [**energyconsumption2**] 中的数据可视化)。常见的替代方案是 POS 共识机制；然而，这种共识机制还会被以下两个方面诟病。首先，对特定版本的 POS 区块链进行投票不需要任何资源，因此也没有机会成本。这意味着，理性的矿工应该简单能轻而易举的看到每一个竞争分支上进行开采，以便最大化他们获得多开采回报。第二，存在“主体性薄弱”的问题。这个概念是指第一次上线的节点必须向可信资源请求有效链的哈希值是多少。这完全破坏了区块链的可信度，许多人认为区块链是区块链技术的“杀手级应用“。所有运用 POS 共识算法的区块链都有这个问题。

因此，我们的应对方法类似于 RPCA 共识机制。它不被认为是 POW 或者说 POS，而是围绕着网络中受信任节点之间的“投票”机制。为了保证网络的正确性和一致性，所有节点每隔几秒钟就应用一次 RPCA。一旦达成共识，当前的分类帐会被认为是“关闭”的，并且成为最后关闭的分类帐。假设这种共识算法是成功的，并且网络中没有分叉，那么网络中所有节点维护的最后关闭的分类帐将是相同的。这意味着这种经常挖矿是没有必要的，RPCA 是迄今为止实现交易确认最有效的方法，比 POW 和 POS 更为有效。

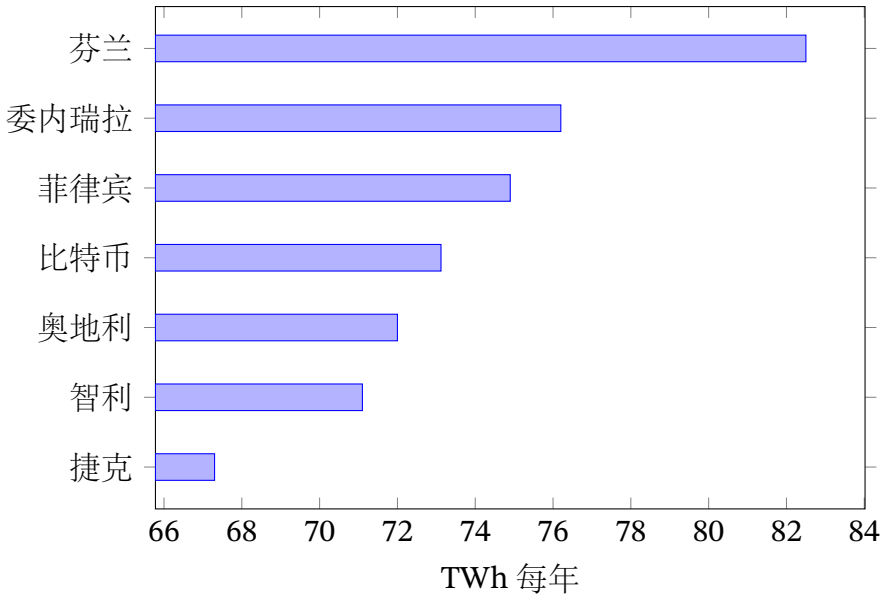


图 1: 2018 比特币能源年消耗。

第二部分 投资者需知

本文的这一部分为考虑建立 AtoX 节点的潜在投资者和个人提供需要了解的信息。

8 AXC 分配

尽管有时被批评为“不纯”，AtoX 区块链依然实现了超于常规的初始区块奖励：AXC 总量的百分之十。选择这种比例目的在于在尽可能多的缔约方之间快速分配 AXC。换句话说，从第一个区块开始，就会有相当数量的人个人可以开始使用 AXC 了。AXC 的总量为 2×10^{11} 枚。初始区块奖励将

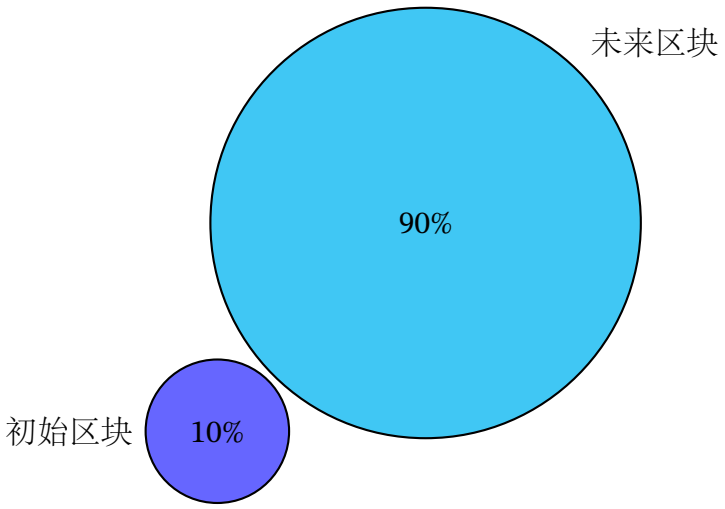


图 2: 初始区块奖励和未来区块奖励。

如fig. 3进行分配。投资者可以投资于 AtoX 的初始节点布局，总额度为初始区块奖励的 55%。为了平等地保护投资者和 AtoX 区块链创始团队的权益，初始区块奖励在 24 个月内不可以花费。投资 c 枚 AXC 的日回报 r 设定为

$$r(c) \coloneqq c \cdot d(c),$$

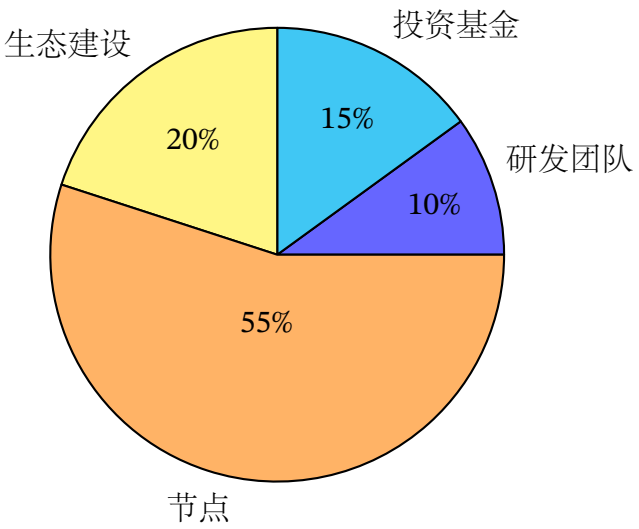


图 3: 初始区块奖励分配。

其中 d 定义为

$$d(c) := 2c \times 10^{-9} + \begin{cases} 0 & \text{若 } c < 2.5 \times 10^7, \\ 0.2 \times 10^{-2} & \text{若 } 2.5 \times 10^7 \leq c < 5 \times 10^7, \\ 0.225 \times 10^{-2} & \text{若 } 5 \times 10^7 \leq c < 1 \times 10^8, \\ 0.25 \times 10^{-2} & \text{其他。} \end{cases}$$

日回报将从初始投资后的第 11 个月开始，每月减少 5%，并在 2 年以后完全停止发放日奖励。Figure 4展现了最初投资 5×10^5 枚以上 AXC 的基准年回报 $c + r(c) \cdot 365$(线性缩放，因为只有冻结的 AXC 会产生回报)。此外，投资人每成功推荐一位 Atox Swap 跨链钱包用户，初始投资的年回报率将增加 0.5% (最高 15%)；被推荐使用跨链钱包的客户每投资 1 百万枚 AXC，推荐人初始投资的年回报率增加 1% (最高 15%)。被推荐用户使用 AtoX Swap 时，将会购买 AXC 以支付交易手续费，初始区块奖励将会给其推荐人发放被推荐人首次购买 AXC 数额的 5% 给作为奖励。同样地，如果被推荐用户 AtoX Swap 内资产超过 100$，其推荐人也会收到来自初始区块奖励的 99 枚 AXC 作为奖励。Table 1 展示了奖励系统规则。

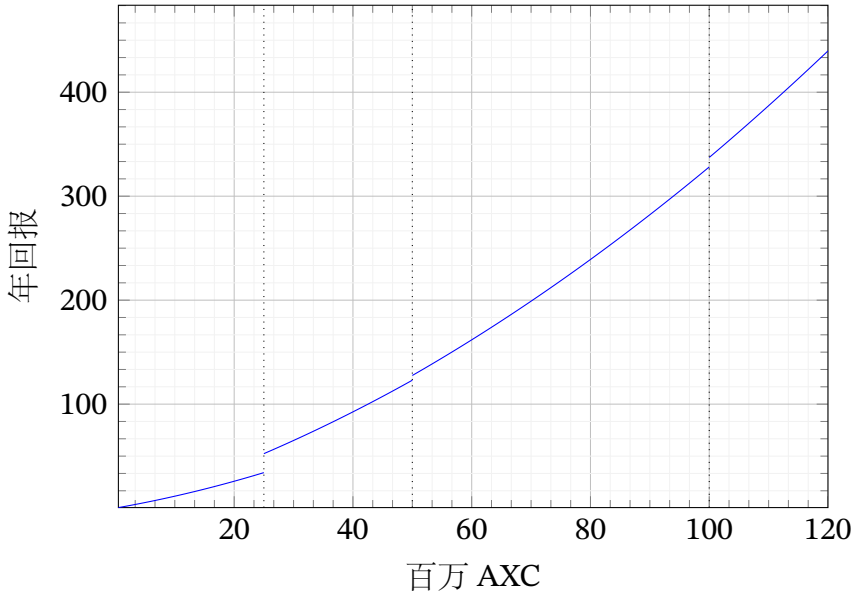


图 4: 初始投资超过 5×10^5 枚 AXC 的基准年回报。不包含推荐奖励和第 11 个月起日回报递减。

AXC 发行价格 $0.02		
AXC(百万)	奖励 AXC(百万)	**日**回报
100	15	0.25%
50	5	0.225%
25	1.25	0.2%
0.5-25	0	0%
每增加 50 万 AXC 投资 + 0.002% **日**回报		
每推荐一位用户 + 0.5% **年**回报，最高 15%		
被推荐用户每增加 1 百万枚 AXC 投资 + 1% **年**回报，最高 15%		
+ 5% 被推荐用户首次支付交易手续费的**一次性**奖励		
被推荐用户跨链钱包资产超过 100$，+ 99 枚 AXC **一次性**奖励		

表 1: AXC 奖励体系。

9 市场趋势

在下面的部分，我们分析了各种市场趋势和市场发展。

9.1 比特币主导地位下降

自从 2009 年比特币区块链启动后不久，“加密货币”就成了比特币的代名词。在比特币获得最初的成功之后，各式各样的 Altcoin(术语，指比特币外的所有加密货币) 也随之应运而生。然而与比特币相比，它们的市值仍然微不足道。瑞波币和以太坊改变了这红模式：区块链社区注意到，可以构建不同的加密货币用以处理不同的特定任务，例如支付、智能合约、ICO、证券、实用令牌等等。随着密码市场的发展，比特币的主导地位开始动摇，而 Altcoin 的市值变得越来越高，加密货币也随之从这种发展中越来越多地获益。如今，用户们期望的是快速、安全、快速、大额的加密货币交易。

9.2 Altcoin 市场的增长

2018 年中旬，2018 年中旬，Altcoin 市值突破了 2500 亿美元大关。随着加密货币市场规范化的出现，传统资产管理公司也具备了投资这一市场的可能性，因此由于资本的流入趋势，加密货币市值上升的趋势有望继续下去 [**cryptomarketcap**]。Chris McCann 将加密货币市场的发展过程和早起互联网发展进行了比较 [**earlycrypto**]：

> 尽管我们已经看到加密货币、令牌和 *DApp* 用户的大幅增加——如果把它的轨迹和互联网的增长进行比较，我们仍然只是相当于处在 *1994* 年。

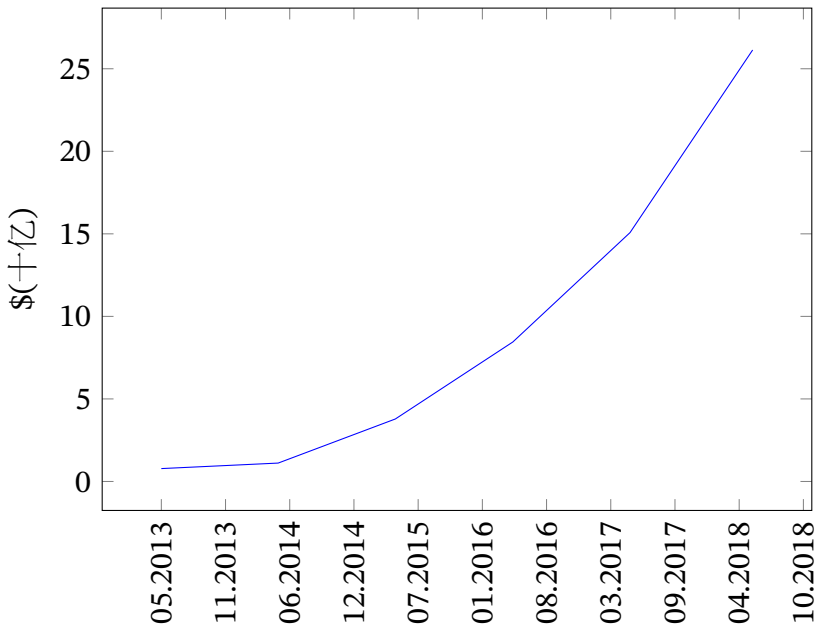


图 5: Altcoin 总市值随时间变化。

9.3 闪电网络增长

自启动以来，比特币闪电网络中的节点数量大幅度增长。随着闪电通道和容量 (通道上的冻结资产) 的增加，通过闪电网络来进行大额资金运送有了可能性。以太坊的等离子体 (Plasma) 以非常相似的方式运作 (甚至是由同一个团队开发的)。闪电网络和二级解决方案依然注定是要主打小额支付的，因为它能够高效、频繁地处理小额支付而不对主区块链造成任何负担。关于闪电节点的增长，参见fig. 6，关于闪电通道的增长，参见 fig. 7 。

9.4 日交易量增长

随着 altcoin 数量的不断增加和全球市值的持续增长，加密货币交易所的日交易量也在不断上升。在价值曲线波动比较大的时候，2018 年中期 24 小时内的交易量已经超过了 220 亿美元，参见fig. 8。

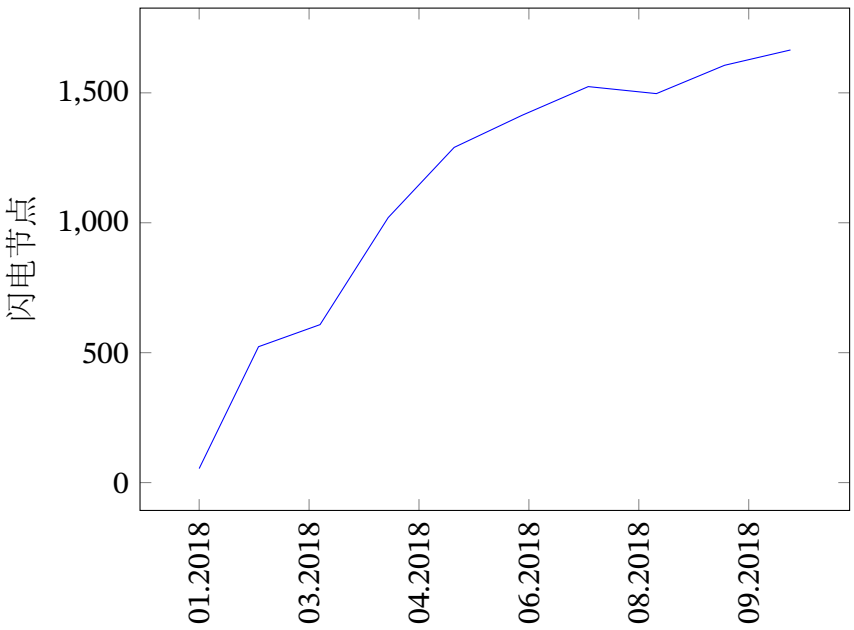


图 6: 闪电节点数量随时间变化。

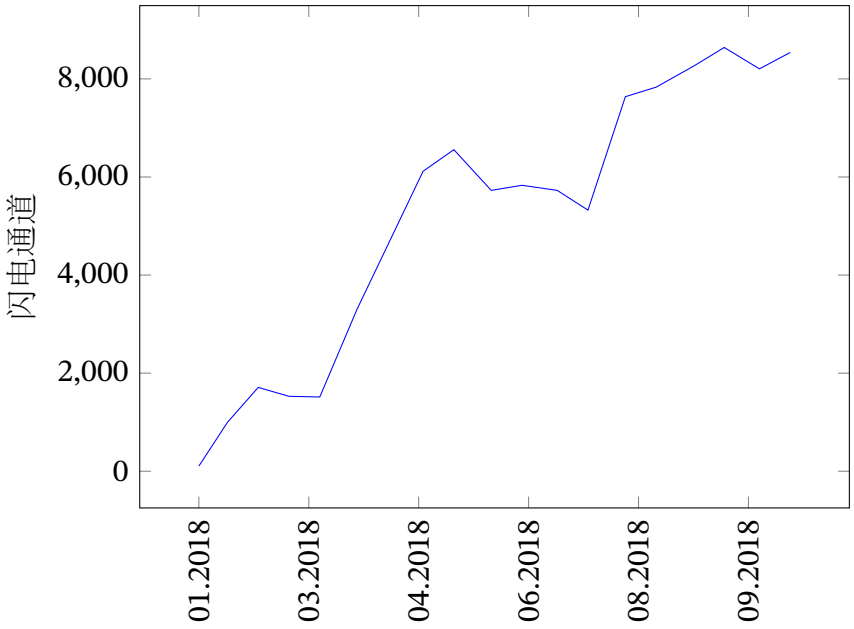


图 7: 比特币闪电通道数量随时间变化。

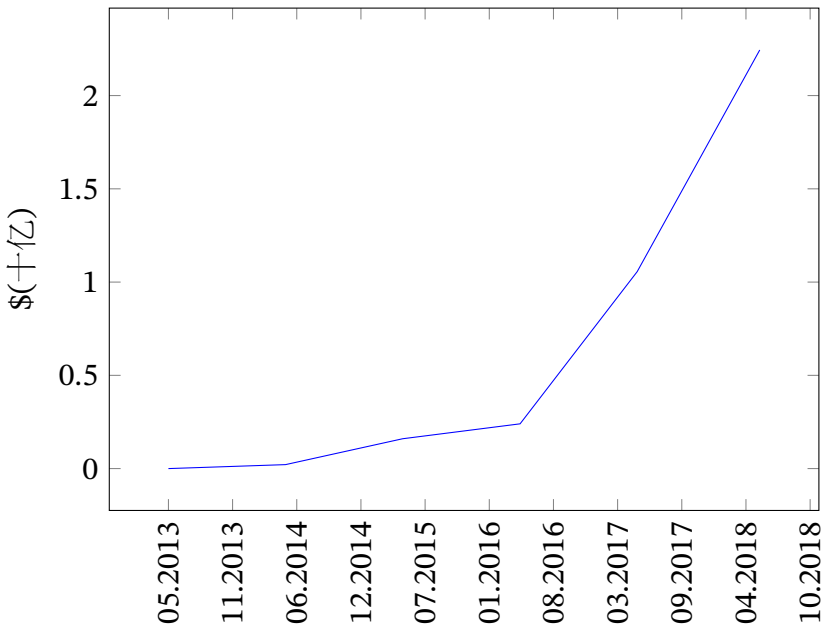


图 8: 加密货币日交易量随时间变化。

10 黑客攻击

本节将会围绕黑客攻击加密货币的方法、案例以及对策展开讨论。本节将分析最常见的黑客攻击策略，并编汇收集被公开发布过的关于安全问题的信息，以及罗列出存在记录的黑客事件清单。清单上的全部内容都来源于可靠新闻并附有来源注释。这些信息将有助于加密货币持有用户和交易平台制定交易系统防御措施，以反抗黑客攻击。

10.1 黑客攻击方法

与人们的普遍认知相反，绝大多数黑客攻击都是以社会工程 (social engineering) 的形式完成的。Social engineering 是指利用欺骗手段来操纵个人，使其无意间泄露可以被用于欺诈目的的机密或个人信息。下面提供的交易黑客攻击列表将证明，黑客绕过系统制定的安全措施的方法通常都是以这种手段实现的，实际上很少需要使用中断加密的方法。一些 social engineer-

ing 黑客的普遍形式是:

手机/电子信箱劫持; 通常情况下，黑客利用从社交媒体检索到的个人信息，冒充目标，并从受害人的移动电话运营商获得新的手机 SIM 卡，或者重设受害人电子信箱密码。这就使得黑客能够访问所有类型的账号、获得各式各样的信息，而黑客所盗取的信息中，就有可能包含加密货币交易所员工的信息。

网络钓鱼; 作为迄今为止最常见的盗取他人账户的方式，许多人都采取了防范措施，或者受到账户平台的反钓鱼保护。然而在 2014 年 7 月，这种钓鱼技术被成功用于从 Cryptsy 窃取 950 万美金 (见下文)。网络钓鱼经常要求人们在看上去合法合规的网站上登录他们的账户，从而获取登陆数据。鉴于钓鱼网站和钓鱼邮件的无处不在，有人在一个漫不经心的时刻上当受骗只是时间问题。

恶意软件; 2015 年 1 月，多名比特股员工被骗将恶意软件下载到了他们的工作电脑上，损失共计 520 万美元。该技术还会利用目标的兴趣爱好来诱使他们下载恶意软件。

防御 social engineering 黑客; 世界上极少有数据库是没有经过加密的。由于中断此类加密是几乎不可能的，因此攻击这些数据库就必须要致力于获取用于解密数据库的私钥或者密码。因此，大多数交易所被黑只可能是由于糟糕的信息安全协议导致的。大多数情况下，包含交易所客户全部私钥的加密数据库密码只掌握在几个关键员工手中，这些员工就可以成为低成本 social engineering 攻击的目标。这种类型的数据泄漏不仅在中心化系统中非常常见，而且也是造成系统最大损失的关键点。

总结性地说，加密货币本身很少被黑，但是它们的核心协议或者共识机制却是有可能受到损害的。这几乎总是设计不当的共识机制和中心化系

统的最终结局——人为失误造成的严重损失。

从下面列出的黑客攻击、fig. 9中的钱包客户端和去中心化私钥系统的情况可以推断，将资产存储在离线冷钱包里以及多签名身份验证，是最重要的黑客资金盗取防御措施。

10.2 交易所黑客攻击事件时间线

2011 年 6 月

Mt. Gox，875 万美金; 早期规模最大、最重要的加密货币交易所，同时也是第一个已知的加密货币交易所黑客受害者。这起事故的原因——我们必须假设——是由于其低标准的安全措施导致的。当时总部位于日本的 Mt. Gox 没有使用任何一种版本控制软件，这意味着任何一位程序员都可能出于意外而撤销同事的全部工作，如果他们恰好在同一个文件上编辑代码。就在黑客攻击前不久，比特币交易所引入了一个新测试环境，因此旧版本的软件更改已经被推送到交易所客户，并处于未经测试的状态。[i]

2011 年 10 月

Bitcoin7，5 万美金; Bitcoin7——当时全球第三大 BTC/USD 交易所——成为了俄罗斯黑客组织的目标。10 月 5 日，该交易所网站向用户发布了一条信息，称“攻击本身不是仅仅针对 bitcoin7.com 服务器，而是对于属于同一网络的其他网站和服务器也都采取了行动。最终黑客们成功突破了整个网络，并导致随后对 bitcoin7.com 网站的严重破坏。”最初的突破无论发生在哪个层面，都能让黑客们接触到网站的热钱包。黑客攻击后不久，Bitcoin7 便永远地关门大吉了。[ii]

2012 年 3 月

Bitcoinica，22.8 万美金; Bitcoinica 是利用名为 Linode 的网络主机发动黑客攻击的最突出受害者之一。Bitcoinica 的 CEO 周同在最初表示损失了 1 万枚 BTC 后，向 Ars Technica 承认实际上丢失了 4.3554 万枚比特币，所有这些币全都存放在 Linode 服务器上的未加密热钱包里。[iii]

2012 年 5 月 **Bitcoinica，8.7 万美金；**第一次黑客攻击后 10 周，Bitcoinica 又一次被盗取了一笔资金。这一次不仅是丢失比特币，甚至 Bitcoinica 用户数据库也遭到严重破坏。姓名、电子信箱地址、密码和其他敏感数据全部被盗，尽管这些信息被存储在具有不同加密方案的独立数据中心的独立服务器上。[**iv**]

2012 年 7 月 **Bitcoinica，30 万美金；**第三次攻击令 Bitcoinica 再次丢失了客观数量的比特币。然而，关于黑客是内部监守自盗的传言永远无法被证实。[**v**]

2012 年 9 月 **Bitfloor，25 万美金；**截至 2012 年 9 月，总部位于纽约的 Bitfloor 是以美元做交易的第四大交易所。在攻击中，黑客获得了交易所钱包密钥的未加密备份。此备份是在 Bitfloor 创始人 Roman Shtylman 进行手动升级并将数据存入磁盘上的未加密分区是创建的。被泄露的钱包钥匙被用于清空 Bitfloor 上的大量热钱包。[**vi**]

2013 年 5 月 **Vircurex，16 万美金；**一个人为错误导致了 1454 枚 BTC，225.263 枚 TRC 和 23.400 枚 LTC 被盗。根据 2013 年 5 月 Vircurex 的报告，黑客获得了他们托管服务商的 VPS 控制账户的登录凭据，然后成功请求到了所有服务器的重置根密码。[**vii**]

2013 年 6 月 **Picostocks，13 万美金；**6 月 10 日，Picostocks 的发言人在 bitcointalk.org 论坛上透露，多个账户是使用相同的密码操作的，这就给黑客提供了进入交易所钱包的许可。[**viii**]

2013 年 11 月 **Picostocks，300 万美金；**同年 11 月，Picostocks 又被盗取了一笔大得多的金额。由于此次被黑的一部分钱包是冷钱包，无法被通过互联网访问，因此黑客有可能是内部人员。[**ix**]

2014 年 2 月 **Mt. Gox，4.6 亿美金;** 这是有史以来第二大的加密货币交易所黑客攻击。鉴于相对较小的加密货币市场，这是影响力最大的攻击事件。“危机战略草案”中显示，黑客多年以来一直在利用同一个 bug 针对该公司进行研究。“危机战略草案”泄露后，Mt. Gox 承认损失了 4.6 亿美元 [**x**]。来自该公司内部的事后资料报告称，他们曾经使用的源代码可以说是“一塌糊涂”[**xi**]。自 2011 年 6 月的黑客攻击以来，Mt. Gox 的安全措施似乎并没有得到充分加强。

2014 年 3 月 **Cryptorush，57 万美金;** BlackCoin 发布了他们区块链的一个新分叉，其中产生了一个 bug 使得 BlackCoin 的所有者能够兑现币他们实际拥有的资金更大的金额。官方声明的副本现保存在 bitcointalk.org 论坛上。[**xii**]

2014 年 3 月 **Poloniex，6.4 万美金;** 一个类似的 bug，利用交易被安排发生在同一时刻，从而提取多于超过钱包内实际存储的金额，以达到从 Poloniex 上盗取资金的目的。[**xiii**]

2014 年 3 月 **Flexcoin,，60 万美金;** 在对加密货币存储服务提供商进行攻击后，所有的热钱包全部被清空。黑客进入 Flexcoin 系统的手段，目前尚不清楚。[**xiv**]

2014 年 7 月 **Cryptsy，950 万美金;** 这一严重的黑客攻击事件，直到发生两年后该公司宣布破产的时候才被公开。在最初针对技术问题的一番指责过后，Cryptsy 据称在破产前成为了网络钓鱼的攻击目标，并被迫暂停了交易。[**xv**]

2014 年 8 月 **BTER，165 万美金;** 尽管 BTER 通过谈判，使黑客归还了部分被盗资金而减少了他们的损失，但一位开发者声称问题完全在于交易所本身，而黑客攻击造成的损失本身是可以避免的。[**xvi**]

2014 年 10 月 **Mintpal，130 万美金;** Mintpal 的黑客攻击情况以及其随后的破产原因依然不清楚。2017 年，Ryan Kennedy 因欺诈和洗钱罪名被带到英国法院，并在黑客攻击后得到了交易所，这引起了人们对其内部人员的怀疑。[**xvii**]

2015 年 1 月 **796Exchange，23 万美金;** 即使将服务器迁移到高度安全的云端站点，也无法保护当时交易量最大的交易所避免被黑客成功攻击。在发现了系统弱点之后，黑客们能够欺骗客服部门，让他们把比特币发送到错误的钱包里。796Exchange 的总裁 Nelson Yu 告诉 cointelegraph.com，”准确地说，钱包系统在这次事件中一点也不受影响。资金盗取发生在基金的交易过程中。” [**xviii**]

2015 年 1 月 **Bitstamp，520 万美金;** 2015 年的 Bitstamp 黑客劫案是众多复杂的网络钓鱼攻击中一个很好的例子。多个员工被锁定，并通过利用他们的兴趣爱好信息被诱骗下载恶意软件。通过这种手段，攻击者获得了对两个服务器的访问权，其中包含 Bitstamp 热钱包的密码。[**xix**]

2015 年 2 月 **BTER，175 万美元;** 黑客针对 BTER 的第二次攻击尤为重要，因为这次他们袭击的目标是 BTER 的冷钱包。他们是如何做到这一点的，至今仍然是个谜。[**xx**]

2016 年 4 月 **Shapeshift，23 万美金;** Shapeshift 的黑客攻击时为数不多的，可以追溯到该公司一名员工的黑客攻击之一。在盗取了 13 万美金之后，他们把敏感信息卖给了一名黑客。据信，黑客制造了第二笔盗窃，金额为 10 万美金。[**xxi**]

2016 年 5 月 **Gatecoin，214 万美金;** 这次黑客攻击是一个久经考验的策略的转折点。攻击者似乎改写了系统，使其将存款转账储存在热钱包中，而不是应该存放的冷钱包中，以此增加了后来被盗走的金额。[**xxii**]

2016 年 8 月 **Bitfinex，7 千 7 百万美金;** Bitfinex 使用 BitGo 的多签名钱包系统，被许多人认为是极其安全的。然而，黑客一定是设法获得了私人钱包的钥匙以及 BitGo 的 API 的关键点，直到今天仍然留下了许多关于攻击性质和过程的问题。[**xxiii**]

2017 年 2 月 **Bithump，1 百万美金;** 黑客成功地获取了超过 3 万名 Bithump 用户的个人信息。数据泄露是该公司一名员工的私人电脑被黑客攻击的结果。然后，这些信息被用来进行欺诈通话，以窃取用户的身份验证代码。[**xxiv**]

2017 年 4 月 **Youbit，530 万美金;** 之后被称为"Yapizon" 的韩国交易所的四个热钱包被成功攻击并清空。被盗金额相当于公司总资产的 36%。[**xxv**]

2017 年 2 月 **Youbit, "全部资产的 17%" [xxvi];** 在 Youbit 发生的第二起黑客抢劫案迫使交易所宣布破产。这两起袭击事件都是邻国朝鲜的间谍机构所为，但这些说法无法核实。[**xxvii**]

2018 年 1 月 **Coincheck，5 亿美金;** 由于安全手段不足，Coincheck 成为了这一大规模黑客抢劫案的轻松目标。交易所不进将其客户的资产存储在热钱包中，而且也没有用已经成为行业标准的多签名身份验证起来保护这些钱包。[**xxviii**]

2018 年 2 月 **Bitgrail，1.87 亿美金;** 人们对意大利 Bitgrail 在今年 2 月向当局提交的黑客攻击了解甚少。根据交易所自己的说法，造成损失的具体日期甚至无法确定。自然地，对 Francesco Firano 本人作为 CEO 策划盗窃资金的指控不断上升，但是没有任何证据可以证明这一点。Firano 试图将责任推卸给 BitGrail 使用的 Nano 令牌区块链背后的开发者。[**xxix**]

2018 年 6 月 **Coinrail，4 千万美金;** Coinrail 时另一个在被黑客攻击后不得不关闭的交易所。尽管该公司 70% 的资产都存放于冷钱包中，但黑客仍然盗走了 4 千万美金。[**xxx**] 这一事件标志着韩国交易所在几个月内第三次被黑客攻击，这意味着加密货币交易所黑客们集中在亚洲。

2018 年 9 月 **Zaif，6 千万美金;** 总部设在日本的 Zaif 措手不及，因为黑客从他们的热钱包偷走了 6 千万美金。该公司只有通过与 Fisco 合作才能生存，而 Fisco 制服了 4.45 亿美金的被盗金额，以获得交易所股权的大部分份额。[**xxxi**]

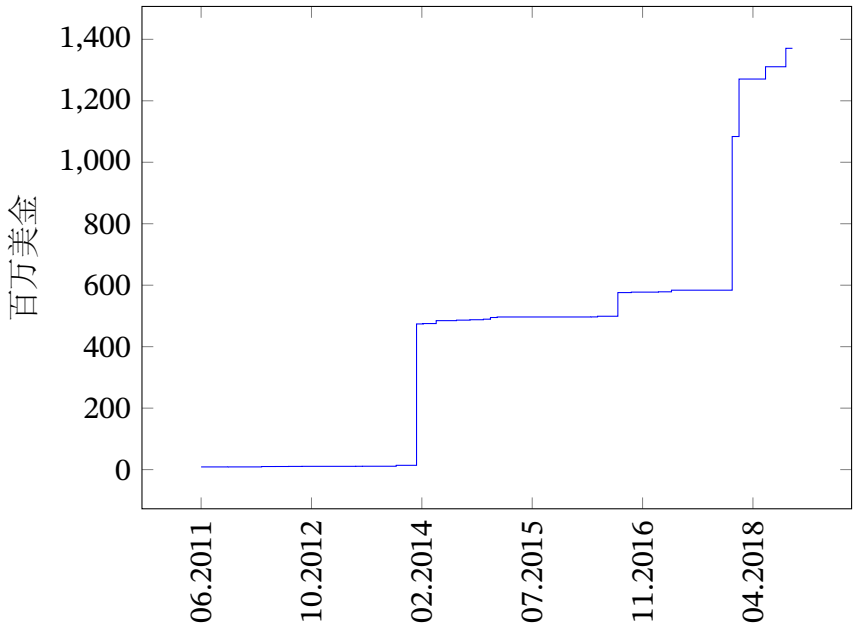


图 9: 加密货币交易所黑客攻击损失金额总量。

总结 通过观察这些黑客，可以总结出一些有趣的信息:

1. 大多数成功攻击的加密货币交易所的事件，发生在总部设于亚洲的公司身上。

2. 上面提到的绝大多数黑客攻击的都是被集中管理的热钱包。

3. 被列举的许多攻击事件都是由于人为错误导致的，即数据未在加密情况下存储、更新在没有质量保证的情况下推送、伪装成客户的黑客没有被发现，或者交易所员工成为网络钓鱼目标。

通过使用客户端钱包，和在私钥上进行多重签名身份验证，真正的去中心化加密货币交易所大大降低此类黑客攻击成功的可能性。除此之外，这也让公司员工更加难以实现从内部挪用资金。