uPlexa 磐石 (音译)

运用和激励物联网设备的大规模计算能力，建立基于浏览器的区块链匿名支付系统。

声 明:

您正在查看的是于 2018 年 11 月 26 日完成的磐石（uPlexa）项目白皮书版本。 未来白皮书可能会对业务、技术和法律模型作进一步更改和完善。 请访问 uPlexa 网站以获取本白皮书的最新版本。

目录

4 前言和愿景

工作原理

5 物联网模型（核心功能）

6 费用和近零拥塞模型(NZCM)

7 磐石（uPlexa）近零拥塞模型应用程序接口（ NZCM API）

8 电子商务简介

9 匿名服务支付

技术说明

10-11 物联网的可行性和收益率

12-18 CryptoNight 算法概述

19 总结

前言和愿景

磐石（uPlexa）是一个专注于利用物联网和匿名算法的点对点（p2p）电子支付系统。uPlexa 利用改良的 CryptoNight 算法，建立了自己的区块链，其目的是将物联网设备作为一个整体连接在一起，提供基于匿名的支付服务，特别是为互联网和电信服务提供商提供匿名支付服务，它同时也支持基于匿名的电子商务。 据不完全统计，2018 年全球物联网设备数量超过 90 亿件，2020 年有望达到 200 多亿件。

和比特币一样，磐石（uPlexa）也是一个点对点(p2p)电子支付系统，但是 uPlexa 同时支持匿名支付服务和有利可图的物联网交易挖矿。磐石（uPlexa）不仅具有抗专用集成电路（ASIC resistant）的特性，而且还致力于成为物联网挖矿最有利可图的硬币，用户可以利用物联网设备一定比例的空闲资源进行挖矿。uPlexa 区块链可以通过 web 浏览器直接访问和挖矿，完全不需要下载任何外部资源。当然，桌面和手机应用程序也会提供下载。

2017 年 12 月，我们看到所有加密货币中使用最多的是比特币。当时比特币还没有准备好被如此海量的用户群所使用，导致网络拥堵严重，交易确认速度慢，费用高。磐石（uPlexa）打算通过使用近零拥塞模型(NZCM)来有效地解决这些问题。近零拥塞模型（NZCM）利用物联网设备的计算能力，形成强大的哈希率（hashrate），同时随着网络交易量的增加，微支付的费用也会增加，进而减少微支付。任何不被认为是小额支付的支付总是会有相对较低的费用。近零拥塞模型还将使用 uPlexa API，以便为 uPlexa 高级用户开展脱链事务。这些只是近零拥塞模型的几个简单的层，更多详情，请详细参阅第 6 页关于近零拥塞模型的内容。

匿名和隐私是加密货币领域最大的争议点之一。uPlexa 使用 CryptoNight 算法以确保私人交易不可被追踪。通过使用 uPlexa，我们的目标是将匿名性引入互联网和电信服务提供商支付系统以及电子商务领域。我们将通过与互联网和电信运营商合作，并推出支持匿名交易、支持匿名店主、杜绝存储和销售个人隐私信息等目的的电子商务平台，以此来实现目标。

工作原理——物联网模型（核心功能）

磐石（uPlexa）使用了 CryptoNight 算法的修改版本，以提供毋庸置疑的安全性和匿名性。在审核了默认的 CryptoNight 算法之后，我们很快意识到如果使用默认 CryptoNight 算法，物联网设备挖矿既不可行也无利可图。因此，我们对修改了算法，使物联网设备挖矿更加有利可图。与其他支付系统不同是，我们的主干网络将由全世界数十亿的物联网设备提供算力支撑。

我们的核心目标是通过使用物联网设备合理的闲置资源进行挖矿，从而获得 uPlexa 收益，以帮助支付运行物联网设备的电费。这些设备在发达国家可能听起来并不多。然而，大多数物联网设备在发展中国家制造，那里的人们也更容易买得起。例如，东南亚等地区的个人拥有智能电视、智能冰箱、智能汽车和其他多种移动设备。如果他们能够获得足够的利润，或者至少能够覆盖一部分运行成本，他们的处境就会好得多，因为每月的电费可能高达他们收入的 20%。

我们计划支持大多数(如果不是所有的话)物联网设备，通过为每种设备开发专门的软件，利用物联网设备闲置的 CPU 的资源来进行 uPlexa 挖矿。为防止用户物联网设备的过度使用，用户可自由调整具体参数，我们也将设置上限。我们将支持的设备是：

- 台式电脑和笔记本电脑
- 移动电话及平板电脑
- 智能电视
- 智能厨房设备（冰箱、烤箱、咖啡机、炉灶等等）
- 智能汽车
- 树莓派
- 服务器(数据中心和服务器集群)
- 其他正在开发的物联网设备

工作原理——费用及近零拥塞模型（NZCM）

为了消除严重的网络拥塞并保持极低的费用，我们决定创建一个称为近零拥塞模型(NZCM)的模型，它具体包括以下几层:

- 利用大规模物联网应用的能力
- 利用磐石（uPlexa）近零拥塞模型应用程序接口（NZCM API）进行链下交易
- 不鼓励非常小金额的小额交易
- 小额交易的收费比例更高

随着当前大量物联网设备及物联网技术的广泛普及，我们相当有信心磐石（uPlexa）将获得大量的网络支持，为区块链提供动力。同时，另一个积极的因素是，在发挥 uPlexa 的主要用途时，通过使用近零拥塞模型应用程序接口（NZCM API）将可以使大部分交易中在链下完成而不必在实际的区块链中进行。

近零拥塞模型应用程序接口（NZCM API）将允许网站管理员、应用程序开发人员和公司在 uPlexa 中信任他们的用户，而用户可以选择挖矿以换取特定的服务、应用程序或业务。当用户选择使用 NZCM API 为特定公司挖矿时，该公司将充当矿池。这些矿工将使用同一个钱包挖矿，比如一家在线电子商务商店的钱包。所有挖矿所得的硬币都被发送给公司而不是单个矿工。然后 uPlexa 通过 API(而不是区块链本身)记账给平台上的单个用户。因此，当用户在公司平台上使用挖矿所得的 uPlexa 时，不需要通过区块链处理交易，而是通过其平台数据库直接进行处理。

磐石（uPlexa）的用途主要用于互联网和电信供应商的匿名支付以及电子商务。因此，小额交易不是我们优先考虑的事项。我们希望未来通过 CryptoNight 闪电网络来支持 uPlexa 和其他 CryptoNight 小额交易。无论如何，由于 uPlexa 不直接支持小额交易，因此我们为 uPlexa 发送的数量设置了最小限制(当前为不少于 1 个 uPlexa)。这个最小限制以后可以在任何既定时间通过分叉进行更改。对于 5 个 uPlexa 以下的小额交易，将会进行弹性收费。因此，当网络中充斥着小额支付时，如果您发送的 uPlexa 小于 5，那么此类小额交易的费用将比标准支付增加两倍。这样做法的的初衷是在消除网络攻击同时减少 uPlexa 的小额支付。至少 uPlexa 目前不是致力于于小额交易的加密货币(< 0.15 美元)

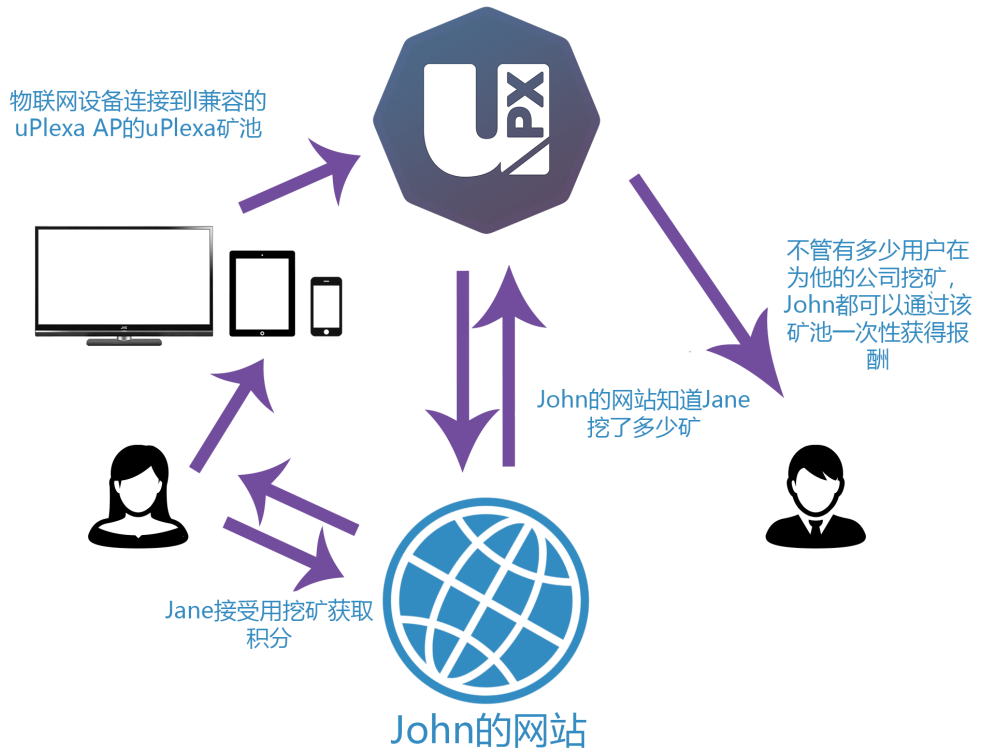
磐石（uPlexa ）近零拥塞模型应用程序接口（NZCM API）

通过使用 uPlexa API 能够实现更少的链上交易，帮助减少网络拥塞，进而降低公司和项目的费用。

工作原理

例如，johnswebsite.com 的所有者 John 想要为他的用户提供一个信用系统，以便他们购买商品、服务或捐款。他可以要求用户将他们的物联网设备连接到他的在线网站上，通过挖矿获得 uPlexa 币。作为回报，用户使用 uPlexa API 的获得特定积分。一旦用户挖掘了足够多的 John 积分，用户就可以在 John 的网站上购买商品，或者使用其中的一些积分打折。

在挖矿的过程中，所有挖到的 uPlexa 都只会发送到了一个钱包里，那就是 John 的钱包，当然，uPlexa API 跟踪记录了每个用户及其贡献的哈希值。因此，当用户 Jane 希望进行购物时，这个金额是通过 API 从用户余额中直接扣除的，而不是从她的钱包到 Johns 钱包进行单独的交易。



电子商务简介

全球电子商务行业总收入的达 2.3 万亿美元以上，预计到 2021 年将超过 4.88 万亿美元。来源 https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

磐石（uPlexa）团队将推出自己的电子商务平台，该平台将广泛地支持多种加密货币和法币，并将 uPlexa 作为网站管理员及其客户的私有、安全和匿名的交易网关。我们的网站管理员将不会实行实名认证（KYC），他们将通过 uPlexa 获得匿名支付。网站管理员也可以用 uPlexa 为他们自己的商店购买其他东西，如软件开发服务、插件程序和美工设计。

磐石（uPlexa）电子商务系统在用户运营的商店盈利之前，都不会向用户收费。也就是说，商店是免费的，直到你开始赚最少三倍于每月的商店费用，也就是 29 美元/月的基本商店费用。如果您超过 29 美元，我们将每天支付。否则，每两周付款一次。

我们团队在电子商务行业工作过，从 BigCommerce 到 Wordpress (WooCommerce)，再到 Shopify。我们将重点专注私人定制和匿名电子商务体验，也胜过其他现有的电子商务系统，特别是会认真听取客户建议和投诉，这一点是其他公司一直忽视的。可以说，如果不进行重大的升级和修改，上述的这些系统是很难适应将来的发展，我们已经有了许多改进和提升现有电子商务系统的创意，其中一些目前正在研发中，以投入现有商店使用。

总而言之，磐石（uPlexa）在电子商务领域的第一要务是为客户提供加密数字货币服务并提升服务体验。

匿名服务支付

磐石（uPlexa）最终将在匿名支付和服务提供商之间架起一座桥梁。这将通过与发展中的初创公司建立多重合作关系来实现，这些初创公司将允许用户在不使用 KYC 的情况下为其服务付费，同时将 uPlexa 作为一种可选的支付方式。

为什么服务支付应该是匿名的?

- 匿名提供隐私保护，防止间谍程序窃取你的私人信息
- 帮助保护您的数据不会被出卖给他人用作推销或其他目的
- uPlexa 是一种全球通用货币，所以在外旅行时支付其他国家的服务而无需支付“旅游”费用，因为他们不知道你是谁
- 避免让其他公司知道你在付钱给谁，或者你可能要收购哪家公司
- 保密你的商业供应商
- 避免来自网络服务提供商或监视你数据的员工的敲诈
- 用自己的账户支付家庭成员的服务费用
- 黑客将无法追踪到你的电话号码，也无法用你的个人信息来劫持你的手机访问权限盗取你的在线账户

磐石（uPlexa）的匿名功能远远超出了基本代码，进入了大公司的视野，影响了关于 KYC 和匿名的策略。最困难的挑战是找到愿意为其系统和服务提供安全和匿名选项的公司和合作伙伴。因此，我们将重点关注战略合作伙伴关系，同时也将奖励那些帮助 uPlexa 实现其真正潜力的人。

物联网的可行性和收益率

磐石（uPlexa）将为大量物联网设备提供挖矿服务，从智能手机、平板电脑到智能电视，甚至智能汽车。这些都是通过运行我们的挖矿软件来完成的。uPlexa 挖矿软件利用了一组特定的故障保险设置，确保只使用设备部分的空闲资源，防止设备过热和响应速度降低。在我们的测试中，uPlexa 挖矿软件需要的 CPU 资源比平常使用的应用程序(如手机摄像头、Facebook 和 Netflix)要少。

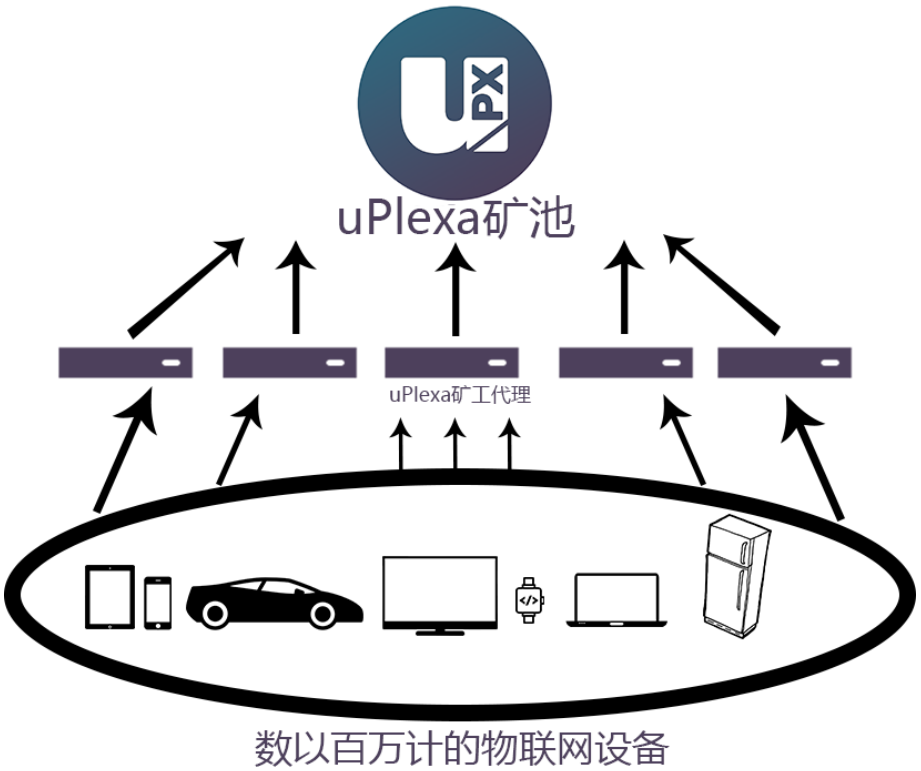
计算

标准智能手机：CPU 满载工作时算力约为 28H/s 或 35%的 CPU 使用率时算力约为 10H/s

标准笔记本电脑在满载工作时算力约 45H/s 或在 35%的 CPU 使用率时算力约 16H/s

使用 35%的 CPU 算力中值为 13H/s。如果 Alice 有 15 个设备，她有算力 13 * 15 = 195H/s

CryptoNight 叉状矿池技术结合先进的代理协议，从而大大减少矿工与矿池的连接数，使 uPlexa 挖矿成为现实并实现轻量级。使用我们的软件，我们能够在 5 个 Amazon m5.2xlarge 实例和 2 个 Amazon m4.16xlarge 实例(一个用于矿池，一个用于共享验证和工作负载平衡)上接受超过 200 万个并发连接。



矿工收益率

矿工的盈利能力涉及到我们对 CryptoNight 协议的修改版本，以提供最盈利且匿名的物联网挖矿方式。CryptoNight 协议具有相当强的 ASIC 抗性，尽管如此，为了避免有人在我们的平台上利用 ASIC 挖矿，将来我们可能会对整个网络进行强制硬分叉，当然硬分叉既不会扰乱网络也不会有风险。

我们的算法的目标，是以用户每一美元挖矿硬件的成本为依据，尽可能地平衡 GPU 和 CPU。物联网挖掘背后的理念是让世界各地大量的物联网设备连接起来，这将有助于减少挖矿的集中化，同时也为我们的矿工通过持续帮助处理 uPlexa 区块链上的交易而获得稳定的利润流。

有了磐石（uPlexa）项目，人们可以将物联网设备直接连接到任何一个 uPlexa 公共矿池来进行挖矿并获利。他们也可以选择连接到公司或网站/游戏池，以便在该平台上获得相应的积分奖励。

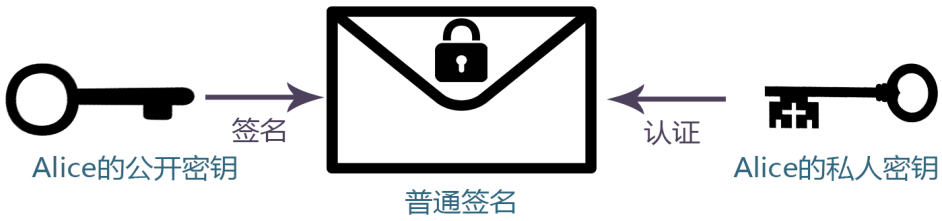
技术原理——CryptoNight 概述

CryptoNote 算法

CryptoNote 算法是在开源许可的，磐石（uPlexa）采用并兼容它，因为它构成了一个可靠的、经过良好测试的加密货币核心的基础。它与 Monero(加密货币前 10 名)和 bytecoin(加密货币前 15 名)的核心区块链技术相同。

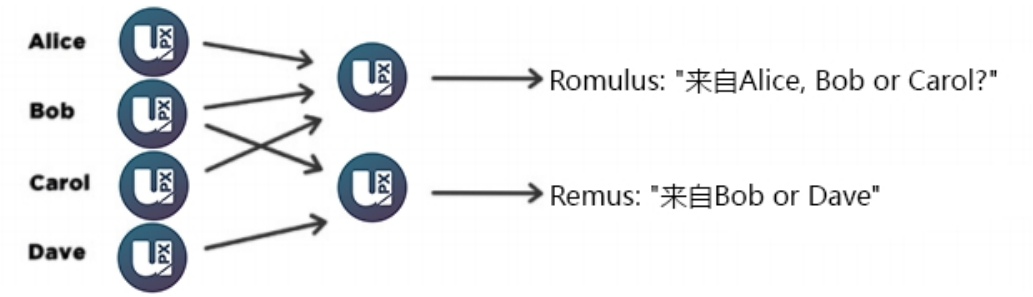
不可追踪的支付

普通数字签名（例如（EC）DSA，Schnorr 等）验证过程会涉及签名者的公开密钥，这是一个必要条件，因为签名实际上证明作者拥有相应的秘密密钥，但这并不总是充分的条件。



环形签名是一个更复杂的方案，实际上可能需要几个不同的公钥进行验证。 环形签名的情况如下：我们有一组人，每个人都有自己的私钥和公钥， 环形签名证明的是给定消息的签名者是该组的成员。 它与普通数字签名方案的主要区别在于，签名者只需要单个秘密密钥去签名，但验证者无法确定签名者的确切身份。 因此，如果您遇到 Alice，Bob 和 Carol 公钥的环签名，您只能声称其中一个人是签名人，但您无法确定具体的他或她的身份。

这个概念可以用于通过使用环签名中的其他成员的公钥将数字交易发送到网络，不可追踪，这将用于交易。 这种方法证明，交易的创建者有资格花费在交易中指定的金额，但他的身份与他在其签名中使用的公钥的其他用户无法区分。

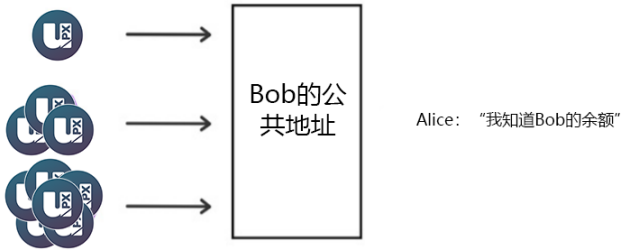


不可追踪的交易

应该指出的是，外围交易并不限制你花自己的钱。 您的公钥可能出现在许多其他人的环形签名中，但这只是作为一个混淆的因素（即使您已经使用了相应的密钥来签署自己的交易）。此外，如果两个用户使用相同的公钥集创建环形签名，然而签名也是不同的（除非使用相同的私钥）。

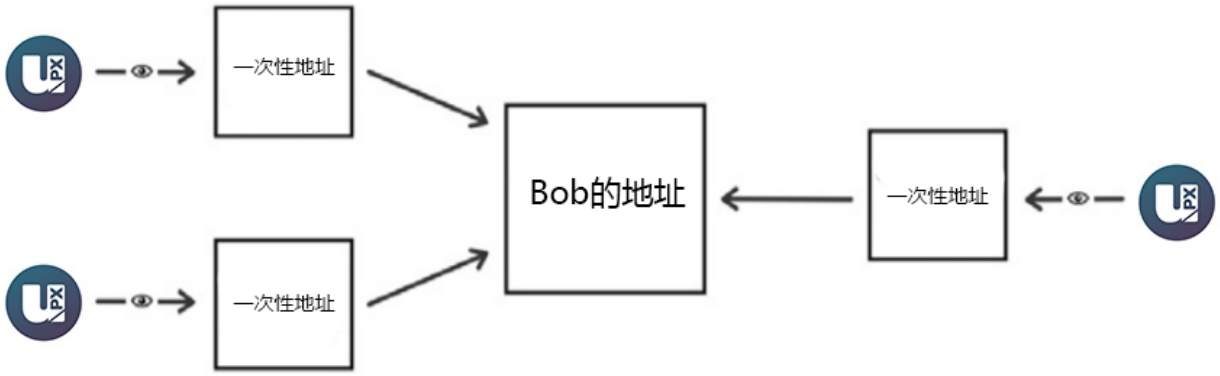
不可链接的交易

通常，当你发布公开地址时，任何人都可以检查你所有的交易，即使它们隐藏在环形签名之后。 为了避免交易链接，您可以创建数百个密钥，并将其发送给您的支付方，但这剥夺了您使用单个公开地址的便利。



uPlexa CryptoNote 通过为每个 p2p 支付自动创建从单个公钥派生的多个惟一一次性密钥来解决这个难题。解决方案在于对 Diffie-Hellman 交换协议进行巧妙的修改。使他它本来就允许双方从其公钥生成一个公共密钥。在我们的版本中，发送方使用接收方的公共地址和他自己的随机数据来计算支付的一次性密钥。

发送方只能产生密钥的公开部分，而接收方只能计算密钥的私有部分;因此，只有接收方可以在交易提交后释放资金。他只需要对每个交易执行一个公式检查，就可以确定它是否属于他。这个过程涉及到他的私钥，因此没有第三方可以执行此检查或发现发送方生成的一次性密钥与接收方唯一的公共地址之间的链接。



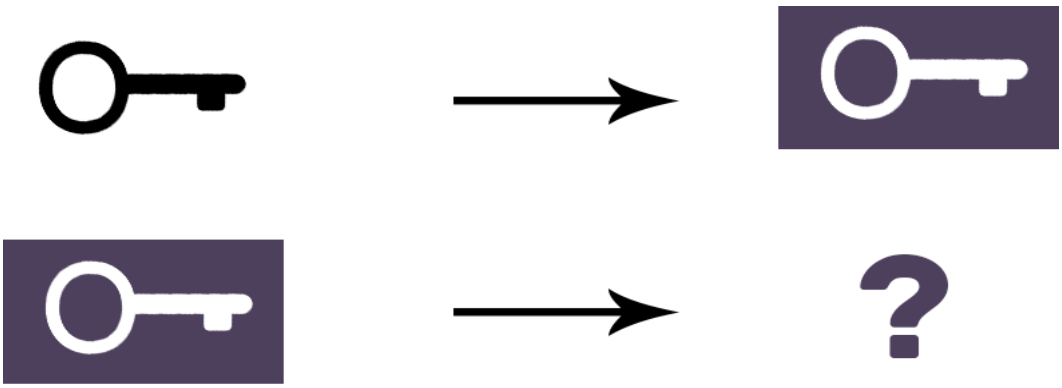
我们协议的一个重要部分是发送方对随机数据的使用。即使发送方和接收方对于所有事务都是相同的，它也总是会产生不同的一次性密钥(这就是为什么称为一次性密钥的原因)。而且，即使它们是同一个人，所有一次性密钥也绝对是惟一的。

双花问题的解决

完全匿名是否会产生双花问题，发送方将同一款项花费了多次？当然这是不可能的，这与任何支付系统都不允许双花，问题可以解决如下：

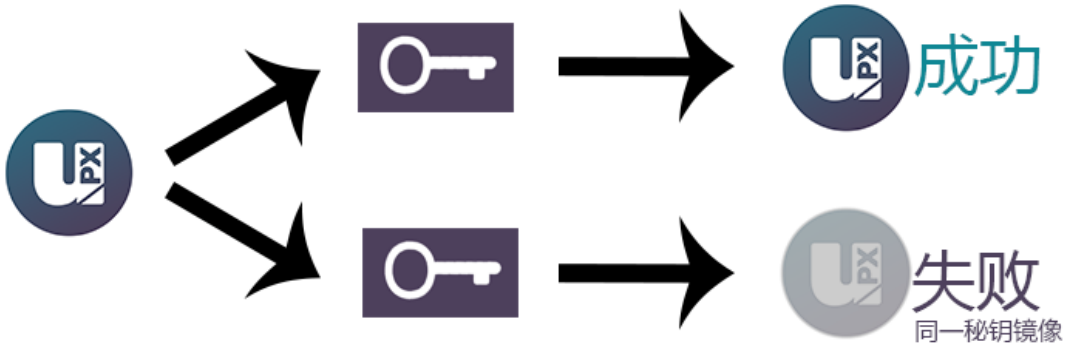
环形签名实际上是一类具有不同特征的密码算法。uPlexa CryptoNote 使用的是修改过的可跟踪环形签名版本。事实上，我们将可追溯性转换为可链接性。该属性限制签名者的匿名性，如下所示：如果他使用相同的私钥创建了多个环形签名（外部公钥的集合是无关紧要的）， 这些签名将被链接在一起，这就表示存在双重花费企图 。

为了支持可链接性，uPlexa CryptoNote 在签名时引入了一个由用户创建的特殊标记，我们称之为密钥镜像。秘钥的密码单向函数的值，在数学上它实际上是这个密钥镜像。单向性意味着只给出密钥镜像是不可能逆推出私钥的。另一方面，在计算上不可能发现碰撞（两个不同的私钥，其具有相同的密钥镜像）。使用任何公式，除了指定的公式，将导致无法验证的签名。所有考虑的事情，密钥镜像是不可避免的、明确的，而且是私钥的匿名标记。



秘钥镜像通过单向函数

所有用户保留所使用的密钥镜像（与所有有效交易的历史记录相比，它只需要很少的存储空间），并立即拒绝具有重复密钥映像的任何新的环签名。 它不会识别不正常行为的用户，但它可以防止任何由于恶意的意图或软件错误导致的双重支出企图。

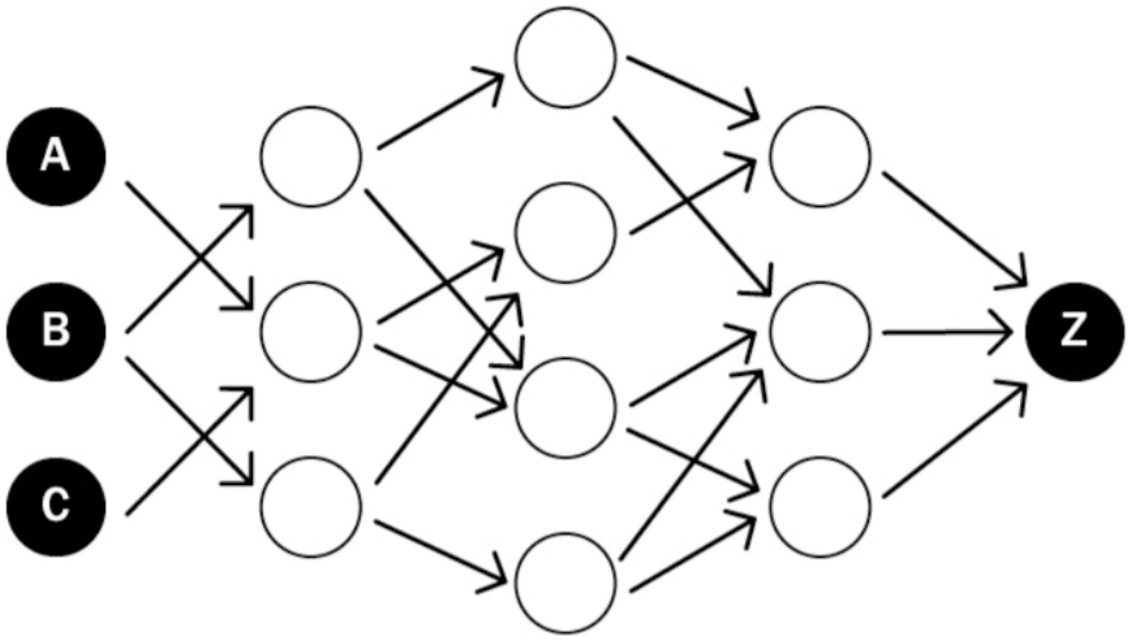


区块链分析抗性

有很多学术论文致力于分析比特币区块链。它们的作者跟踪货币流动，识别硬币的所有者，确定钱包余额等。之所以能够进行这种分析， 是因为地址之间的所有交易都是透明的：交易中的每个输入都引用唯一的输出。此外，用户经常重复使用旧地址，多次接收和发送货币，这更加简化了分析师的工作。还有会无意中发生情况：如果您有公共地址（例如捐款），那么您一定会在许多输入和交易中使用这个地址。

uPlexa CryptoNote 旨在减轻与密钥重用和单输入到单输出跟踪相关的风险。付款的每个地址都是唯一的一次性密钥，从发送方和收件人的数据派生。它可能出现两次 256 位哈希冲突的概率。一旦您在输入中使用环形签名，就会产生不确定性：哪个输出已经花费了？

尝试绘制边缘上的输出和交易中的地址的图形，将会获得一个树：没有任何循环的图形（因为不存在使用相同的秘钥/地址两次）。此外，由于每个环形签名都会产生歧义，从而可能有数十亿个图形，。因此，您不能确定哪个可能的发件人的交易路径来到地址。根据环形的大小，您有可能从“1/2”到“1/1000”概率中猜到。且每一次交易都会增加熵值，并为分析师带来额外的障碍。



标准的 CryptoNote 交易

标准的 CryptoNote 交易是由白皮书介绍的以下序列生成的。

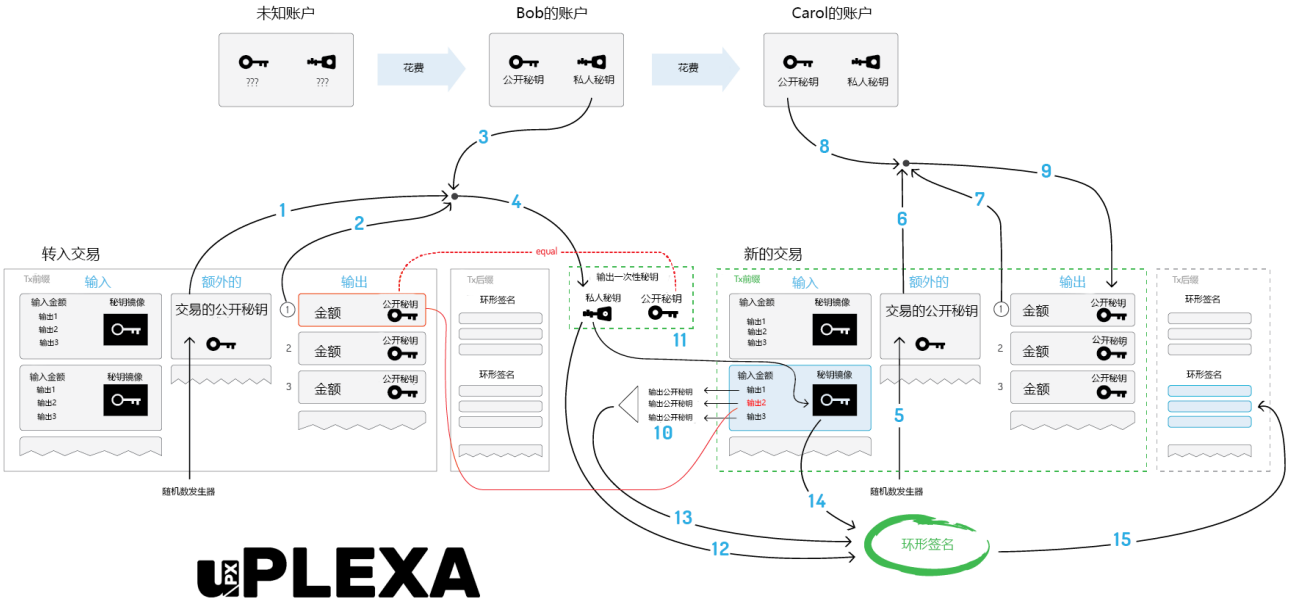
Bob 决定花费一个输出，发送到一次性公钥。 他需要 Extra（1），TxOutNumber（2）和他的账户私钥（3）来生成他的一次性私钥（4）。

当向 Carol 发送交易时，Bob 会随机生成其 Extra 值（5）。 他使用 Extra（6），TxOutNumber（7）和 Carol 的账户公钥（8）获取她的输出公钥（9）。

在输入中，Bob 将他的支出链接隐藏到外围密钥集（10）中。

为了防止重复使用，他还打包了密钥映像，该映像来自他的一次性私钥(11)。

最后，Bob 使用他的一次性私钥（12）、所有的公钥（13）和密钥映像（14）来签署交易。 他将结果的环形签名附加到交易末尾（15）。



自适应范围

一个去中心化的支付系统不能依赖于某个人的决策，即使这个人是核心开发者。代码中的硬常数和魔术数字阻止了系统的演变，因此应该被消除（或者至少被削减到最低限度）。每个关键限制（如最大块大小或最小收费用金额）应根据系统以前的状态计算得出。因此，它总是自适应地、独立地变化，允许网络自行发展。

uPlexa CryptoNote 的有以下参数，可自动为每个新块调整：

1、难度。我们的算法的总体思路是计算节点在最后 720 个块中执行的所有工作，并将其除以它们花费的时间来完成它。工作的度量是每个块的相应难度值。时间计算如下：对所有 720 个块的时间戳进行排序，并排除 20%的异常值，剩余 600 个块的值是对应于 80％相应块的时间。

2、最大块大小。设 MN 为最后 N 个块大小的中值。那么接受块大小的“限制”是 2 * MN。它避免了块状膨胀，但如果需要的话，仍然允许限制随时间缓慢增长。交易大小不需要明确限制，它被块的大小限制。

平缓释放

数字货币总量的上限计算如下：

MSupply = 264 − 1 原子单位

这是一个基于实施限制的自然上限，而不是像“N 个币对每个人都应该足够”这样的直觉。 为了使发射过程更顺畅，uPlexa 的 CryptoNote 使用以下公式进行区块奖励：

BaseReward = (MSupply − A) >> 18

其中 A 是先前产生的货币量。 它提供了货币供应的可预测的增长，没有任何断点。

总结

uPlexa 致力于为电子商务和服务提供商支付提供免费实用的匿名加密电子货币。这些实用程序将建立在大规模物联网计算能力和链下交易的基础层之上。

参考资料：

Cryptonote white paper:
https://cryptonote.org/whitepaper.pdf

Cryptonote Inside:
https://cryptonote.org/inside

Bitcoin white paper:
https://bitcoin.org/bitcoin.pdf

Statistica: IoT Connected Devices 2015-2025:
https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

PRISM (surveillance program):
https://en.wikipedia.org/wiki/PRISM_(surveillance_program)