近日，Monero的开发者宣布将与无服务器存储协议Arweave合作，正在验证一种新的反ASIC挖掘算法RandomX，一旦审核成功将取代CryptoNight算法。算法替换，直接导致原来的矿机变成了一堆废铁。

Monero，半年一变的算法

Monero是字节币的分叉货币。在那时字节码发布之后，发现82%的货币已经被预挖。在崇尚自由的数字货币世界里，你敢预挖，我就敢分叉，于是社区直接分叉了字节币，门罗币诞生了(2014年4月18日)。

至于字节币，既然字节币团队喜欢提前挖。，剩下的18%也留给他们去挖。门罗币似乎天生追求&quot公平和自由&quot。连团队都可以&#039；我承受不了预挖掘。怎么能承受ASIC矿机？所以为了对付集权的矿霸，门罗币平均每半年硬分叉一次。

门罗币更新算法不是简单的为了对抗ASIC矿机。因为门罗币的挖掘对pc、ipad等终端设备友好，所以被各路黑客盯上了。各种黑客控制其他人&#039；的个人电脑，ipad等。通过木马病毒挖洞。然后攫取利益。这个问题也可以通过算法替换来解决。

历史上门罗币出现过很多monerozero、monerooriginal、moneroclassic等分叉币，但门罗币等社群肯定是很厉害的。目前最受认可的是monero。这叫，你大爷永远是你大爷！

门罗币的出现是为了对抗各种不公正。如果你不&#039；不打，也许门罗就失去了固有的意义。当然，门罗作为混合货币的代表，，不仅对抗集中式算法，对抗黑客病毒，还对抗现实世界&#039；电子货币的匿名审查——。

在比特币中，由于区块链账本的开放性和可追溯性，任何人都可以通过比特币区块链浏览器披露信息。，追查所有与之有关系的比特币账户，所以比特币的匿名性并非无懈可击。

Monero使用环签名和混淆地址来保证匿名性。它的交易不仅隐藏了交易双方的地址你也可以隐藏交易金额。默认情况下，交易细节完全不可见，私密性极强。所谓环签名，就是当一笔交易发生时，系统自动生成几组金额相同的交易。通过这个&quot真假混杂&quot道，你可以&#039；我查不出货币去了哪个地址。

环签名技术，门罗币的隐蔽性

在交易环节，主要涉及到三个数据[发送方][接收方][交易金额]，门罗币对应的三个技术正是从这三个角度。。让&#039；让我们看看门罗硬币是如何通过环签名、混淆地址和环秘密实现匿名的。

戒指签名——发件人，无法追踪

比如，当人们联名写信发表评论时，外界怎么就很难猜到发起者是谁呢？？作者&#039；s的名字可以写在一个环里，每个名字在环里的地位似乎都是对等的，所以很难猜测赞助人是谁。假设A向B发送门罗币，并将混淆交易次数设置为5。转账时网络会自动生成五笔转账交易，除了A发给b的这一笔。另外四个是&quot诱饵交易&quot用来欺骗外界观察者，从而达到隐藏发送者的目的。

混淆地址——接收方，无关性

混淆地址是为了打破输入和输出地址之间的关联，从而隐藏传输之间的关系。。每当汇款人想发起转账时，钱不会直接送到收款人手中&#039；的地址，而是由系统临时生成的地址。比如，A给B转账时，A作为汇款人，给B&#039加了一些随机数；的公钥和私钥来生成唯一的一次性地址。系统会将资金转移到这个临时地址。A和B都能自己看到这个临时地址，但是两个人都不知道地址里的钱是谁的。

那B怎么知道有人给他转了钱，他又是怎么收到钱的？B&#039；的钱包将使用私钥进行搜索。，检查区块链上的临时地址是否有自己的钱。当B&#039；私钥(仅接收方B&#039；他自己的私钥可以)识别他有权要求的临时地址，他就可以使用这笔钱。

环密——A向b转账时交易金额的隐瞒

在RingCT的交易中，A不会直接公开转入网络的金额，而是提供一个数字rct作为交易金额。Rct=随机数，真实交易金额。随机数用于覆盖真实金额，由钱包自动生成。。网络可以使用该rct值来验证交易输入是否等于交易输出的金额，从而确保没有额外的Monero被伪造。但是，对于其他人来说，没有办法知道实际的交易金额。

灰尘侵袭和数据泛滥

显然，门罗硬币的混合是通过创建多个&quot虚假交易&quot同时，然后&quot混淆真假&quot，从而实现隐私保护。这种模式的直接后果是门罗硬币被&quot臃肿&quot。以比特币为例，每一笔交易都是一笔交易；但是在门罗硬币中，每笔交易

至少包括5笔交易(另外4笔交易旨在以假乱真)，这意味着门罗币的数据量将快速增长。

数据快速增长的直接结果就是对所有节点的运行有了更高的要求。以比特币为例。目前的数据已经超过了200g，而且这个数据还在增加。如果这个数据提高到500g、1000g，就算算法反专业矿机，有多少人愿意跑全节点？如果只有几个完整节点在运行那么这个系统必然是集权的。

其中，最可怕的不仅仅是专业矿机，灰尘的攻击也能让门罗币因为臃肿而瘫痪。因为在混币模式下，无论你转1个门罗币还是0.0001个门罗币，都需要匹配四组相同的交易数据，所以尘埃攻击足以把门罗系统变成一个臃肿的系统。

当然，有人会问为什么我们可以&#039；t在硬分叉过程中编辑或合并数据。比如把前一段时间的交易数据剪下来。，或者合并几个小的交易，可以腾出很大的空间。但问题是，这种做法和以现实为中心的机制有什么区别？

防弹协议，让臃肿变慢

为了坚决解决以上问题，Bulletproofs应运而生。Bulletproofs最初由密码学家BenedictBunz和JonathanBootle发表，可以减少事务数据的大小。将交易规模减少到至少80%。

门罗币和比特币一样，使用UTXO交易模式。这意味着区块链通过一个称为未使用事务输出(UTXO)的概念来管理余额。钱包余额由一系列UTXO组成。。每个UTXO是可用于发送给另一个用户的BTC(或XMR)数。每次一个用户向其他用户发送BTC，发送方的一部分UTXO都会被消耗掉，一个新的UTXO会被创建并发送给接收方。使用比特币所使用的UTXO可以被认为已经从现有的全局UTXO组中消失和删除。

因为Monero使用的是环签名，所以无法确定UTXO是否失效。所以，所有曾经存在过的UTXO，不管是不是已经用完了。，都需要在有效的全局UTXO集合中。这是一个庞大且不断增长的数据集，每个挖掘节点都需要对其进行跟踪，如果增长过快，会极大阻碍网络的可扩展性。

在Monero的三种不同机制中，防弹协议主要是针对环形保密链路的。也就是说，防弹协议实际上并没有对门罗币本身的隐私技术做出贡献。协议只保证机密事务中存储的信息不包含任何虚假信息，可以减少数据量。

但显然，Bulletproofs只能减缓门罗币臃肿的数据量，但它可以&#039；不能从根

本上解决数据爆炸的问题。如果随着时间的推移，门罗币所有节点的运行数据越来越大，那么&quot计算能力的集中化&quot目前比特币所面临的。门罗币仍然无法解开。[XY002][XY001]莫内罗存在的问题[XY002][XY001]莫内罗的隐蔽性既是它最大的优点，也是它最大的弱点。隐瞒固然可贵，但也会让犯罪活动逍遥法外，加大监管难度。。莫内罗&#039；混合交易很容易被用于非法金融交易，如洗钱和非法毒品交易。如果很容易利用Monero进行非法金融交易，那么它肯定会被用于这一目的，政府最终将被迫干预。

除了法规问题，莫内罗&#039；美国的隐私保护措施没有那么强。《连线》杂志早些时候发表了一篇关于门罗币隐私弱点的文章，来自不同大学的研究人员指出了门罗币的缺陷&#039；的事务混合算法，这破坏了其不可追踪的特性。。为了解决这些问题，Monero开发人员对Monero进行了定期和持续的改进。但是，隐私不可能一蹴而就，这将是一场持久战。

无可否认。Monero在不牺牲去中心化的情况下将隐私引入加密货币，并使用创新技术确保交易不相关、不可追踪，发送的金额是隐藏的，这一点仍然值得肯定。。目前，莫内罗&#039；美国开发商也在改善可扩展性、黑客和数据滥用的问题，但政府&#039；美国的监管仍然是一个不可忽视的不确定因素。

(作者：诸葛复城，内容来自内容开放平台&quot德德诺。"的链条；本文仅代表作者&#039；s观点，非链官方立场)