金色财经近期推出Hardcore栏目，为读者提供热门项目介绍或者深度解读。

匿名是比特币的特性之一，但是匿名不等于隐私，所以加密货币业研发人员做出了很多努力来增强比特币的隐私性。CoinJoin是其中一项技术，已经有一些钱包如Wasabi，Samorai和JoinMarket在提供混币服务，但这项技术要求混币需求者同时在线并有交互行为。现在JoinMarket贡献者Adam“waxwing”Gibson提出了一项新的混币技术SNICKER。本文编译自bitcoinmagazine。

人们对比特币隐私的需求日益增长，SNICKER可能是比特币隐私下一个工具。

按照中本聪的白皮书，隐私是比特币协议的设计目标，但如今，区块链分析通常可以破坏用户的隐私。这是一个问题。举例来说，比如比特币用户可能不希望人们知道他们的钱花在哪里，他们的收入如何或拥有多少比特币，企业可能不想将交易的详细信息泄露给竞争对手。

幸运的是，比特币开发研究人员正在提出越来越多的解决方案来保护用户隐私。其中一个“比特币隐私”捍卫者是Adam“waxwing”Gibson，他以对JoinMarket的贡献而闻名，JoinMarket是一种允许用户混币的协议，并为混币服务者提供经济奖励。

最近，Gibson提出了一个新想法：SNICKER(Simple Non-Interactive Coinjoin with Keys for Encryption Reused，可复用加密密钥的简单非交互式Coinjoin)。现在已作为比特币改进提案(BIP)草案提交，SNICKER将允许无需任何同步或交互而完成混币，这意味着用户无需沟通或同时在线。

CoinJoin

到目前为止，SNICKER基于知名的比特币混币技术CoinJoin。一些最受欢迎的混币解决方案在使用CoinJoin技术，包括Wasabi钱包(ZeroLink)，Samorai钱包(Whirlpool)和JoinMarket。

CoinJoin本质上是将多个交易混合为一个交易的工具。假设Alice想向Carol支付一枚比特币，而Bob要向Dave支付一枚比特币。Alice和Bob可以合作创建一笔大交易，在这笔交易中，他们均花了一个比特币(总共两个)，而Carol和Dave则各自获得了一个比特币。区块链间谍将无法辨别是哪个付款者向哪个收款者付的款，从而使所有人的隐私受益。

然而，实际上，比特币交易数量的隐私经常被泄漏。如果Alice想向Carol支付一枚比特币，而Bob想向Dave支付两枚比特币，则很明显，通过比对发送和接收的数额

很容易看出谁在向谁支付。

这就是为什么CoinJoin常被用于混币的原因。Alice和Bob不向别人付钱，而是向自己发送了一个比特币。通过将其合并为一笔交易，区块链间谍无法分辨是谁退回了哪枚代币：这些代币混合在一起，从而保护了Alice和Bob的隐私。

CoinJoin混币器如今工作的不错，但是它们有一个缺点：它们需要交互。仅当所有参与用户都签署了整个交易时，CoinJoin交易才有效，但要签署整个交易，参与用户必须首先向其添加所有比特币和新的接收地址。这通常意味着他们需要传递好几次交易，并且通常要求他们同时在线。

对于许多用户来说，这样的要求有点困难，这就是CoinJoin交易不是很常见的原因之一。这些要求正是SNICKER可以解决的。

SNICKER版本1

本节中描述的协议是SNICKER的第一个版本。这个版本比其他版本更容易理解，但必须注意，实际上它不是协议的最佳版本，也不是最有可能实现的版本。(稍后会提供更多有关替代版本的信息。)

SNICKER版本1的工作方式如下：

假设Alice想混合一个比特币，这体现在区块链上未花费的交易输出(UTXO)。她要做的第一件事是将比特币重新发送到她的同一个地址。没错，在此版本的SNICKER中，她正在重复使用地址，这违反了比特币的最佳做法。但这很方便：它公开标记了此UTXO为(可能)用于混合。

顺便说一句，这并不意味着Alice不能使用此比特币。它仍然在她的钱包里，随时可以使用。如果有人注意到，它只是被标记了。

Bob也有一枚比特币要混合。(实际上，数量不必相等，Bob至少需要拥有Alice的数量。)Bob不认识Alice，但他确实知道像Alice这样的用户在那里标记了他们的UTXO可以用来混合。因此，Bob扫描区块链以查找潜在的匹配项。他找到Alice的UTXO，可能还找到了更多匹配的UTXO，包括误报(并非所有重复使用的地址都真正可用于混合)。但是，为简单起见，现在让我们假设Bob只找到一个匹配：Alice的UTXO。(稍后我们将回到其他可能的匹配和误报。)

通过匹配，Bob现在获取与重用地址相对应的公钥。这完全有可能，因为地址被重用了：通过第一次使用它，Alice在区块链上发布了该公钥。(UTXO一旦被花费，公

钥就会在区块链上可见，而地址始终可见。)

此时，Bob拥有了Alice的UTXO(因为她标记了它)和她的公钥(因为她从地址中花费了一次)。

现在，Bob使用Alice的公钥并将其与自己的私钥(用于他要混合的比特币)结合起来，以创建“共享密钥”。从字面上看，这是密码学书籍中最古老的窍门，因为只有Alice和Bob可以生成它：Bob用他的私钥和Alice的公钥，Alice用她的私钥和Bob的公钥(对应于他要混合的比特币)。

因此，现在Bob有了Alice的UTXO和她的公钥，以及一个“共享密钥”(因为他是用Alice的公钥和他的私钥生成的)。

Bob以新的方式使用“共享密钥”。他用它来数学上“调整”Alice的公钥。这种调整实际上会创建一个新的公钥。除了……没有人拥有私钥。

有趣的是，由于加密技术的魔力，Alice也可以发现经过调整的公钥对应的调整的私钥！如果她使用相同的“共享密钥”调整原始私钥，则调整后的私钥将对应于调整后的公钥。

换句话说，Bob可以为Alice生成一个新的公钥，从而为Alice生成一个新的比特币地址，只有Alice可以使用。即使她现在不知道！

因此，Bob现在有了Alice的UTXO和她的公钥，一个“共享密钥”以及一个新的Alice比特币地址(使用她的公钥和“共享密钥”生成)。

这几乎足以创建有效的CoinJoin交易。具体来说，Bob接受了Alice的UTXO，并为自己的比特币添加了UTXO，因此有两个输入。然后，他添加了Alice的新地址和自己的地址作为输出(以及费用和其他一些详细信息，比如需要时提供自己的找零地址)。然后他签署了交易。

现在唯一缺少的是Alice的签名。

送达Alice

最后一步送达Alice，实际上比听起来容易，但需要最后一招。

Bob可以简单地将几乎完成的CoinJoin交易发布到某个地方，以供Alice查找。例如，在专用于SNICKER用户的公告板上；最好是使用Tor隐藏服务或者以其他方式为

发布者提供匿名的地方。

但是，如果使用纯文本格式，这仍然不是理想的选择。如果监控者监视公告板，他们可以轻松查看哪些输入属于提议者(在此例中为Bob)，以及哪个输入属于接受者(在此例中为Alice)：签名者是提议者。这本身可能泄漏隐私。但是，如果Bob提出更多提案来混合不同的比特币，那就更糟了。在那种情况下，例如，监控者可能能够将所有不同的UTXO连接到Bob，因为他那批发布的交易同时发布在公告板上。

因此，Bob改为用Alice的公钥加密CoinJoin交易！这样，只有Alice可以解密交易，而监控者则无法得到任何东西。

在将加密交易发布到公告板上之后，Bob完成了他需要做的所有事情。如果他愿意的话，他可以在网上消失。

该Alice了

由于现在对CoinJoin交易进行了加密，因此引入了最后一点复杂性。虽然Alice知道在哪里寻找交易信息(在SNICKER公告板上)，但她不知道要寻找什么：公告板上的所有CoinJoin交易看起来都是一团加密的信息。

只有一种方法。Alice需要尝试使用她的私钥来解密所有软件包，希望其中一个是有用的。

但是当Bob加密的一团信息变成CoinJoin交易时，Alice拥有完成混币所需的一切。她使用她的私钥和Bob的公钥(包含在他的输入中)来生成共享密钥，然后她可以用来创建新的经过调整的私钥。在检查新密钥对应于她在输出中的新接收地址之后，她签署交易并将其广播到比特币网络。

Alice和Bob的币混在一起了，即使他们从未互动过，也不需要同时在线。

尽管该过程在文字上看起来有些费力，但请记住，所有过程都可以通过软件进行抽象，翻译成笔记本电脑或手机屏幕上的几个按钮，甚至完全自动化。

SNICKER版本2

到目前为止说明的SNICKER是该提案的第一个版本。Gibson已经提出了第二个版本，其他变种也在讨论中。

第二个SNICKER版本与此类似，但是避免了重用地址的需要，只是稍微复杂了一点

。

在第二版SNICKER中，Bob不会从重用地址获得Alice的公钥。相反，Bob从创建Alice的UTXO的同一笔交易的输入中获取公钥。Bob假定该交易中的至少一个输入是由Alice自己创建的，并且她仍然拥有这些输入的私钥。

Bob做出这个假设是因为，Alice的UTXO甚至被更清晰地标记为可以用来混币，并且只有当Alice控制与输入相对应的私钥时，它才会被清晰地标记。SNICKER BIP没有指定如何进行初始标记，但是建议某些钱包(如JoinMarket钱包)可以正确地显示此类信息。另外，Alice可以在公告板上简单地发布一条消息宣传她的UTXO。

但甚至可以更好，一旦开始使用SNICKER，查找新的匹配项将变得更加容易。这是因为识别SNICKER交易本身并不容易，并且现有的SNICKER用户可能希望再次混币。换句话说，在初始引导阶段之后，未混合的比特币将与先前混合的比特币混合，从而产生更多的混币，而这些混币又可以用于更多混合。

挑战与机遇

如上所述，SNICKER BIP仍只是草案，尚有待审核和可能的改进。(自从Gibson在博客文章中首次公开提出该想法以来，它已经在某些方面发展了。)现在已经提交了该提议以使其成为BIP，因此可以对其进行标准化，并且在钱包之间相互兼容。

SNICKER还面临一些未解决的问题和挑战，尽管这些似乎都不是无法克服的。例如，其中包括应选择哪些UTXO作为匹配项，尤其是如何限制误报的数量。除了重复使用的地址外，潜在的匹配项的解决方法有按数量、UTXO的使用期限或所用钱包的特定类型过滤。

但是，正如本文前面提到的，即使存在多个匹配项(包括误报)，这也可能只是一个小问题。要约人(“Bob”)可以简单地为所有要约人创建候选交易。即使这些提议发生冲突(因为Bob对所有人都使用同一个UTXO)，这仅意味着第一个做出回应的taker(第一个“Alice”)完成混币，其他潜在的taker会发现他们为时已晚，但没有造成什么伤害。对于误报，也不会造成任何实际伤害，Bob的要约只会放在公告板上，被永久忽略(或直到被删除)。

但是，垃圾邮件可能是一个特别重要的问题。由于公告板将托管加密的数据信息，因此不可能过滤掉“伪造”提交的交易，攻击者发布乱码来破坏SNICKER协议。Gibson在他的BIP草案中提出了一些解决此问题的方法，但是这会带来新的折中，例如需要费用来提交交易。

另一方面，SNICKER还提供了一些迄今为止为简单起见而遗漏的优点。这样的好处之一是，要约人可以在taker的输出中增加一些资金，从而增加接受该混币交易的经济动机。也可以同时与两个以上的用户进行SNICKER混合，尽管这样做会更加复杂。

正是由于该协议是非交互性的，Gibson认为，与其他一些隐私技术(例如JoinMarket)相比，SNICKER在钱包中的实现相对容易。到目前为止，Electrum钱包已经对采用该提案表现出了兴趣，尽管实际实施可能还有很长的路要走。

有关SNICKER的更多信息和背景，请参阅BIP草案(https://gist.github.com/AdamISZ/2c13fb5819bd469ca318156e2cf25d79)，关注bitcoin-dev邮件列表讨论或阅读Gibson提案(略过时)的博客文章(https://joinmarket.me/blog/blog/snicker/)。

原文：SNICKER:How Alice and Bob Can Mix Bitcoin With No Interaction

地址：https://bitcoinmagazine.com/articles/snicker-how-alice-and-bob-can-mix-bitcoin-with-no-interaction

来源: 金色财经

关注同花顺财经微信公众号(ths518)，获取更多财经资讯