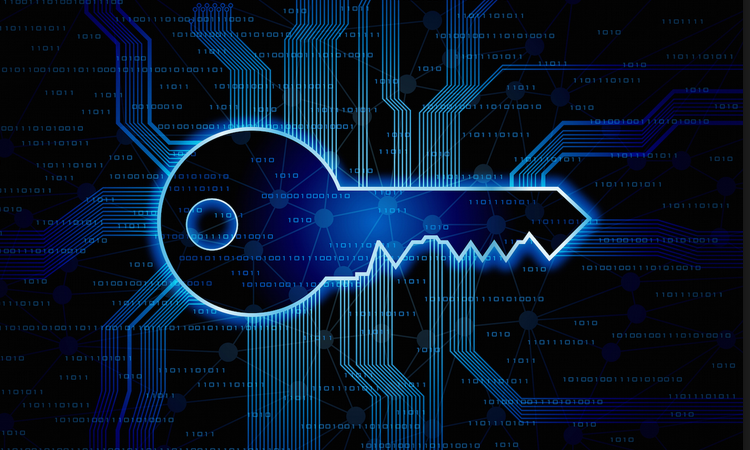
比特币多重签名的现状

[**面神护法**](http://www.8btc.com/author/1163)**2015-12-03 10:25 发布在**[**币头条**](http://www.8btc.com/featured)**,**[**技术指南**](http://www.8btc.com/how)[**4**](http://www.8btc.com/the-state-of-bitcoin-multisig#comment)**4303**

在本文中，我将回顾多重签名的历史，介绍多重签名在比特币网络中的使用情况，以及展望多重签名将如何改变未来。



什么是多重签名？

多重签名是一种允许多个公钥共同签署一笔比特币交易的技术。比如说，使用多重签名技术，爱丽丝，鲍勃和查理可以共同监管一个比特币，这样，要动用该比特币，至少需要他们之中的两个人的同意。

比特币发布之初，币只可以通过一个公钥进行存储。这意味着，无论是谁，只要获悉了与该公钥匹配的私钥，就能够支配该公钥名下的比特币。

对于一个可靠和安全的系统来讲，免疫单点故障是（单点故障意味着，若此处出现故障，则全系统停止运转）一条基本的原则。而在这里，这条原则没有受到尊重，因为：只要私钥丢失或者泄露，即意味着失去比特币合法所有者的身份。

对此最早的解决方案，是一种叫做秘密片段的密码学方法。它将一条私钥分解成独立的几个部分（称为片段），一定数量的片段（少于总数）组合起来就可以重建原私钥。通过这种方式，一个私钥片段的丢失或者泄露并不会危害到比特币的安全。

然而，这种方法未能很好的与比特币软件兼容：你必须使用额外的工具来创造或者合并私钥片段。而且，为了使用比特币，你不得不将大量的片段放在一起，这意味着，免疫单点故障的初衷还是未能得到很好地实现。

其实解决方案一直包含在比特币核心代码之中，从一开始就存在，只是没有标准化：有两个脚本操作允许对普通的比特币公钥进行多重签名。这样的话，多重签名交易时需要验证的不同的私钥无需处于同一空间，相比于使用单一的私钥或者加密片段的方法，系统安全性可以得到很大的提升。

一个比特币改进协议（BIP11）将这种类型的交易标准化，并将秘钥的最大数量限定为3个。在2011年12月20日，BIP11被纳入比特币核心代码，2012年1月下旬，首个BIP11类型的交易出现在区块链上。

多重签名与向脚本哈希支付（P2SH）

尽管因为有了BIP11，多重签名在2012年早期已经成为可能，但是多重签名大规模接受却要感谢另一种类型的交易：向脚本哈希支付，或简称P2SH。这种新的交易类型，可以采用任意的脚本来验证交易。在此之前，只能严格的使用特定的脚本来验证交易。

由于可以使用任意的脚本，多重签名脚本中可以使用的秘钥的最大数量，从BIP11类型多重签名接受的3个，提升到P2SH脚本允许的15个压缩秘钥和相应签名。

最重要的是，P2SH增加了一种新的比特币地址模式。在BIP11之下，简单的向某人提供一个多重签名地址，与他进行交易，你必须精确的告诉对方如何给你的多重签名设置打币：秘钥分别是什么，需要多少才能验证交易，怎样发起多重签名……

P2SH将使用多重签名的难度降低到与使用单一公钥相当的水平上。使用这种新的技术，大量的在线钱包和软件迭兴，同时提升了比特币网络的安全性。

多重签名的现状

如今，已有多于六千五百万的比特币交易使用了多重签名技术，其中绝大部分使用的是P2SH。这表明，在多重签名被接受的过程中，P2SH起到了至关重要的作用。

如今，多于百分之十的比特币使用的是P2SH地址（其中大多数使用的是多重签名），不夸张的说，在过去的两年中，多重签名在比特币生态系统中占据了非常重要的位置。

在多重签名的使用案例中，显现出两种最流行的使用方式：

1. ·2-3 多重签名，约110万个地址的4690万比特币交易使用了这种方式。
2. ·2-2 多重签名，约26.1万个地址的1330万比特币交易使用了这种方式。

有意思的是，最忙碌的10个P2SH地址（即接受和发送比特币最多的地址）中，前4个使用的是2-2多重签名，其交易量占据了全部使用2-2多重签名交易量的80%。同时这也意味着，2-3多重签名是最常用的多重签名设置。

2-3多重签名常用个用法是，一个用户生成两个密钥：一个保存为备份，另一个存放在钱包内；剩下的一个秘钥由钱包服务商生成和保存。支付比特币时，用户和钱包服务商共同签署交易。如果用户或者钱包服务商丢失了秘钥，备份的秘钥就可以动用，转移资金。但是钱包服务商却不能私自动用用户的资金。

最新进展？

新发布的比特币核心0.11.2介绍了一种新的脚本操作：[OP\_CHECKLOCKTIMEVERIFY](https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki)。简称CLTV

新的支付方式允许交易输出在未来的某个时间点之前不可使用。虽然使用简单的交易设置，交易锁定时间就可以实现类似的功能，但是CLTV可以与其他的脚本指令结合，比如多重签名和算法操作，进而可以创造复杂的交易合约。

比如，你可以创造一个2-3多重签名输出，设置当达到某个日期之后，获得一个签名。CLTV指令是通向比特币更加复杂的应用的一步。

另一个重要的正在成型的进展是支付通道。支付通道允许一方与另一方进行重复的微支付，但是只公开第一个和最后一个交易，这样就能避免避免给区块链带来太大负担。这种理念的一些变形，比如闪电网络，扩展到允许用户通过支付通道的网络，进行安全的比特币交易，而不用将每一笔交易公布在区块链上。

结论

所有这些创新，使得多重签名的角色，在比特币网络更加复杂和迷人的应用中，愈加重要。

有的人认为，比特币死了，但是在过去的两年中，我看到新用法的暴增和多重签名带来的新理念，这无疑证明了，比特币活得好好的。