最难忘的精彩电影是什么？《西虹市首富》自然能排上名次，那个突然继承大笔财产的中年大叔，简直完胜了小鲜肉们。

最近，圈子里又沸腾了同样一个关于财产的资讯。加拿大加密货币交易公司Quadriga CX创始人因患克罗恩病，年仅30岁，突然死亡，大笔财产留给了自己的妻子。

不幸的是由于交易所冷钱包的私钥只有当事人知道，导致冷钱包被锁死，价值1.45亿美元的代币全部丢失。

有趣的是，这位创始人一直非常关注加密货币的安全性，在价值1.45亿美元的代币中，有比特币、莱特币、以太币和其他数字代币。

他在参与运营工作期间，不仅仅是笔记本电脑、电子邮件、邮件系统统统加密，为了遭受黑客的攻击，还将“大多数”数字代币转移到了冷钱包中，或者保持离线状态。

冷钱包与离线交易再次因为安全问题，出现在了我们的视野中。究竟冷钱包的离线交易有什么安全性可谈呢？

一、离线签名发展近况

这不是第一次出现离线签名，在数字资产风靡全球之时，主流的加密数字资产BTC、ETH就已经可以进行离线签名操作，并受到很多数字资产爱好者的追捧。

在不具备互联网条件下，能够进行转账交易，将会催生这个市场更加迅速的发展，以及全球化的普及。

我们现在的生活状况，离不开网络，网络的发展也从2G快速成长到4G，伴随2019年的到来，5G市场让运营商、手机厂商等众多行业为之疯狂。

从目前的情况来看，失去网络功能，意味着失去了人们日常生活中的所有能通过网

络来实现操作的功能，比如交易功能、购物功能等等。

但是，对于加密数字资产市场来说，离线功能恰恰能带来一种全新的趋势。

就在最近，一家比特币技术公司正在研究如何通过卫星来实现全球范围内的比特币网络广播，一旦有了这种全球范围内可以使用和被动接收的数据流，也就实现了离线功能，所有人都能随时随地的进行交易。

据相关报道显示，这种交易功能可通过短讯服务、网状网络甚至是二维码来完成。而这一切离线操作几乎是零成本，也避免了很多因为网络问题导致交易过程不及时的问题，同时，还不会受到互联网供应商的监控，距离实现去中心化更近了一步。

可以说，离线状态下的交易方式正在逐渐得到整个市场的推崇。

二、什么是离线签名？

那么，在2018年出现的离线签名，究竟是什么意思呢？

我们从字面上来理解很简单，就是在不联网的情况进行签名，随后将签名后的原始数据放在网络上进行广播，从而达到交易的目的。

也就是说，当时的离线签名并没有完全摆脱网络，只是单纯在签名这一步骤上，可以离线完成，最后的交易过程还是得依托网络。

那么，有人提出了质疑，明明可以在线签名，为什么还需要离线？

这其中最主要的原因在于保护用户的私钥安全。频繁被黑客攻击的加密数字资产市场，也有很多是由于私钥被盗，从而引发的恶性事件。

从目前的互联网技术上来看，安全问题的确存在诸多漏洞。而选择将私钥在离线状态下进行签名，极大程度上保护了冷钱包地址和私钥安全。

因此，有很多为了确保账户安全的玩家们，对火热的BTC、ETH进行了深入研究，并选择离线签名的方式，来管理数字资产。

其中，最为常见的两种离线签名的方法有两种，一种是使用Armory处理离线交易签名，二是手动进行签名。

我们以第二种手动进行签名方法为例，在整个操作过程中，需要两台电脑，一台完全脱离网络，也就是专门用来持有钱包并可以给交易签名的电脑；另一台电脑需要连接网络，主要用来创建未签名交易的可视钱包。

再按照离线签名的方法安全发起交易，由于联网的电脑不能进行交易签名，因此即便是被黑客入侵，也不会导致数字资产被盗。

三、升级中的“离线签名”

伴随近几年来区块链技术的发展，人们对于早期数字资产跨境交易的实践应用，均在广泛进行研究应用。可以说，离线签名为随后离线状态下进行加密数字资产的交易也奠定了深厚的基础。

正如文章开始所介绍的，目前已有公司正在探索离线状态下进行比特币交易，具体可操作性表现在哪呢？

通过卫星访问比特币网络，在实现去中心化上具备了一定优势；

通过简单易用的网状网络设备进行本地网状网络的连接，实现交易，直接获取实时数据，不影响交易速度。

实现钱包来验证区块的过程，提高私钥、冷钱包的安全性，确保交易安全。

仅凭以上三点，让我们对离线状态下进行加密数字资产交易有了期待，或者说，对于更安全的交易方式有了保障。

中年大叔再次激情演绎了《飞驰人生》，我们又不禁一番感叹，不过索然无味的人生，就是执着于信仰。

此时此刻，谁也不知道下一个比特币十年，会发生怎样翻天覆地的变化，但对于它的价值应用，仍然有不少信仰者们在期待一次次惊喜来临。