XCoinPay 白皮书

XCoinPay— 区块链支付领域的 PayPal ！

XCoinPay.io

（v1.8 版本）

XCoinPay 团队目前拥有彩色区块链技术专利与数个软件著作版权,XCoinPay 团队的核心成员均来自于区块链业内，拥有深厚的业内资源及背景。

XCoinPay 开发团队在开发上有着诸多技术创新，由 XCoinPay 自主研发的柔支付技术（RouPay）等都是由 XCoinPay 团队自主研发的创新功能。

柔支付技术（RouPay）由 XCoinPay 开发团队自主研发，而基于柔支付技术（RouPay）为底层打造的柔支付网络（RouPay Network），综合运用了 2-of-2 多重签名、锁定时间交易、交易构造延后广播等技术，可以在不需信任的情况，实现区块链资产的零手续费秒速转移，在速度、安全性和隐私性方面，足以媲美闪电网络（Lightning Network）。

注明：因为政策原因，我们下架了关于代币方向的信息，敬请谅解

前言

近些年，加密数字货币市场逐渐火热，加密数字货币有着流通性高、造假成本高、制作成本低、去中心化、账本公正透明、增发成本高等等优点，广受市场追捧，其核心支撑技术区块链（Blockchain）吸引越来越多的关注，被认为是构建下一代价值互联网的核心技术。区块链的发展同时带动了分布式账本技术（Distributed Ledger Technology）的兴起。一般来说，大体认为这两个概念是互通的，指的是同一类技术。但从严格意义上理解，可以认为区块链是分布式账本技术的一种实现方法。

区块链的去中心化理念正在逐渐颠覆传统的货币理念，而且短时间在世界范围内产生了极大的影响力，虽然分布式账本技术的发展非常迅速，但目前整体上还处于早期阶段，技术远远达不到商用要求，部分核心的技术瓶颈没有突破，阻碍了该项技术的大规模应用。其中，以性能瓶颈和跨链通讯痛点尤为突出，区块链技术的高独立性和交易速度极大地限制了数字资产的流通使用空间，各个区块链系统之间互不相连、协议不通，具备有极高的独立性，彼此之间无法进行讯息通信与协同操作，由此每个区块链数字资产的流通与交易也受到了很大的限制，而随着区块链系统的增多，解决不同区块链网络之间的讯息互通与交易速度问题成为了区块链技术发展的的新趋势。

在现有区块链技术中，区块链的处理能力主要受制于共识算法的性能，而共识算法性能又受制于系统节点的规模和单节点的处理能力。在目前的技术水平下，单条区块链性能优化提升的空间非常有限，且存在性能极限，这严重制约了分布式账本技术在大规模、高并发、低延迟的交易型业务场景中的应用。以比特币为例，高额的转账手续费和极慢的速度是很大的弊病，转账速度慢的无法让人忍受，手续费的高昂也让小额交易变得不划算和不可能。可以预见，随着数字经济的高速发展，未来交易的频率和规模会远远超出当前的水平，性能瓶颈是分布式账本技术需解决的首要问题之一。

在支付领域，随着数字货币热度的提升和币应用的增多，对支付的需求越来越高，闪电网络和雷电网络等技术应需诞生，然而闪电网络和雷电网络设计复杂，技术落地难度大，开发周期较长，未来落地实际应用的时间和效果未知。

因此，我们提出了柔支付网络（RouPay Network），一种基于柔性多重签名的分层通道支付网络，使用的是现有成熟技术，原理简单、设计简洁，基于柔支付网络（RouPay Network）可以方便可靠的实现了秒速零手续费的收发数字货币。柔支付网络（RouPay Network）是基于柔支付技术（RouPay）为底层打造的柔支付网络（RouPay Network），综合运用了 2-of-2 多重签名、锁定时间交易、交易构造延后广播等技术，可以在不需信任的情况，实现区块链资产的零手续费秒速转移，在速度、安全性和隐私性方面，足以媲美闪电网络（Lightning Network）。在传统法币世界，用户只需要一个邮箱作为 PayPal 账户，就可以完成世界各国 20 多种法币的高速转账、收款和购物，PayPal 由此也成为了世界级企业。而在区块链行业，尚未有类似产品诞生。而 XCoinPay 的设计理念是打造区块链支付领域的 PayPal。

XCoinPay 对于商家用户和个人用户分别提供了不同的服务，致力于打造区块链支付 3.0 时代，接下来我们将为您详细介绍 XCoinPay 的设计理念、技术构架、DAPP 应用及商用场景等信息。

目录

柔支付网络（RouPay Network）简介

柔支付网络（RouPay Network）—— 一个瞬间、自由、安全的分布式链下支付网络，世界正在进入代币化时代，未来将会有超过数十亿美金的 token 在柔支付网络（RouPay Network）上流动，一场价值网络的革命蓄势待发。

柔支付网络解决了区块链支付的诸多痛点，如速度慢、手续费高和无商业解决方案，让区块链资产自由、免费、零延时进行转移。

柔支付将让区块链支付变的像通讯一样便利，拥有极速、零手续费和完备商业解决方案的特点，并且柔支付网络是金融支付的基础设施，开放、平等、安全，这样一个去中心化的结算网络有望成为实现区块链大规模商用的基础建设设施

柔支付网络的优点：

通用：区块链支付行业的基础设施。

安全：去中心化保管用户资产，绝对安全。

高并发：柔支付网络使用链下清算的方式实现高并发。

极速且零手续费:转账可以实现秒速到账且零手续费!在落地性和实用性方面远超闪电网络。

拓展性强：作为一个区块链支付底层平台，可以衍生出诸多的商业解决方案，具有极大的拓展性和可编程性。

XCoinPay 产品简介

XCoinPay 致力于打造加密数字货币行业的 PayPal，XCoinPay 专注于区块链支付方向，产品布局涵盖有钱包、支付系统和区块链商业解决方案平台，to B 端和 to C 端的产品分别有：

开放平台：

XCoinPay 开放平台（商家版）——提供多种基于柔支付网络开发的区块链支付解决方案。

交易所解决方案：
接入柔支付网络的交易所，用户充值、提现都秒速到账且零手续费，带来极高的流动性

商户解决方案：
面对接受加密数字货币的购物平台的区块链支付解决方案

OTC 解决方案：
场外交易解决方案

开放：
开发者可以提交各种区块链支付解决方案

傻瓜式接入：
商家可以一键接入
更多：敬请期待

手机钱包：

XCoinPay 手机钱包，区块链世界的第一选择。

可以链接的硬件钱包：
XCoinPay 手机钱包可以链接披萨硬件钱包，披萨硬件钱包是 XCoinPay 团队荣誉出品的最安全易用的硬件钱包，点击了解。

去中心化钱包：
XCoinPay 手机钱包包含去中心化钱包，您可以使用去中心化钱包安全储存您的加密数字货币

柔支付网络：
一个瞬间、自由、安全的通用分布式链下支付网络，区块链支付行业的基础设施。

XCoinPay 产品分类

产品	类型	对应图标	安全系数	轻便程度	转账速度	转账手续费	拓展性及可编程性	商业模式	应用场景
披萨钱包	硬件钱包	银行级别的保险柜	五星 绝对安全 冷储存私钥，断绝一切不安全因素	一星 笨重 必须有硬件钱包连接才可以转移区块链资产	一星 慢	一星 有	一星 极差	一星 难以衍生出商业模式	三星 应用场景比较局限 适合长期大额储存区块链资产
去中心化钱包	去中心化钱包	保险柜	三星 比较安全 私钥储存在联网设备上，存在被盗取的可能性	五星 轻便	一星 慢	一星 有	一星 极差	一星 难以衍生出商业模式	三星 应用场景比较局限 适合储存中小量级别的区块链资产
柔支付网络（RouPay Network）	通用分布式链下支付网络	paypal 支付系统	五星 安全系数极高 区块链资产去中心化保存	五星 轻便	五星 秒速	五星 无	五星 具备有极高的拓展性和可编程性	五星 可以衍生出多种区块链商业解决方案	五星 应用场景十分广阔
XCoinPay 开放平台	开放平台	蚂蚁金服开放平台	/	/	/	/	五星 具备有极高的拓展性和可编程性	五星 区块链商业解决方案平台	五星 应用场景十分广阔

一、XcoinPay 核心技术

柔支付技术（RouPay）：使用多重签名技术建立交易通道，实现堪比闪电网络的极速交易

柔支付技术的核心是通过多重签名技术来实现极速交易，其安全度高于零确认，其简单程度和落地性优于闪电网络。

1.1 柔支付技术实现的核心流程

1.收集 A 与 B 各自的公钥生成两柔支付的多重签名地址：

假设 A 是 1Bit 地址的持有者，B 是 1Dog 地址的持有者。公钥在交换公钥的位置后可以生成两个 2-of-2 的多重签名合成地址，即 3CSm 地址和 3Njd 地址。公钥是可以公开的信息，可以主动公开的。也可以在线快速地生成合成地址。

2.A 构造发到合约地址的交易 TX1,及从合成地址锁定时间发回交易 TX2 发给 B：

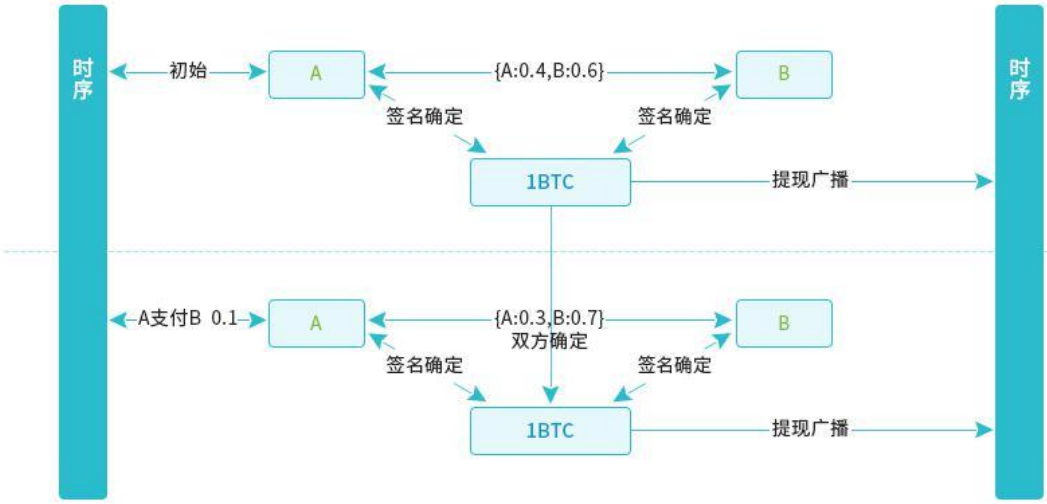
A 用 1Bit 地址的私钥，签名构造一个发向 3CSm 合成地址的交易，只要够造好后得到交易 ID 和位置 n 数据即可，可不先广播发布。然后再由 A 或者 B，最好还是由 A 来构造一个从 3CSm 地址全部币发回 1Bit 地址的的交易 TX2，注意修改下 nLocktime 锁定时间为合理的时间，比如说锁定一年之后。nLocktime， 也被称为 LockTime 或 lock_time，通常被设置为 0，表示交易可随时发送到比特币网络。如果 nLocktime 的值在 1 到 5 亿之间，则表示需要区块高度大于或等于 nLocktime 的区块时才可以写入区块链。如果 nLocktime 的值超过 5 亿，则表示从 197001 月 01 日开始算，加上 nLocktime 秒之后的一个时间点，即 Unix 时间戳，例如 20171 月 1 日是 1483200000，若早于那个时间点，则该交易不会被发送到比特币网路。另外注意 sequence 字段，不能为 INT32 最大值

（0xffffffff），否则会忽略 nLocktime。

3.A 发给 B 交易 TX2 的交易，获得签名后广播 TX1 形成闪电支付的通道把上面的交易 TX2 发给 B，请 B 来确认没问题后用私钥签名会发回。A 在收到来自 B 的签名后，然后用自己的私钥再签名下，看看是否成功。若成功，则可以将之前的交易 TX1 出去，从而形成类闪电支付通道。手里的 TX2 交易保存好，可能等锁定时间过后可能需要广播找回。

其实在一定对 B 信任的基础下 A，可以 A 不用手动构造交易 TX1 不广播，而是直接用币钱包软件发币到 3CSm 地址。然后让 B 来用交易 TX1 的信息来构造一个签名好的带锁定时间的全发回 1Bit 地址交易，并且 B 签名好后发给 A，让 A 妥善保存。一样可以形成类闪电支付通道，对 A 的技术要求会很低，但是需要 B 有足够的信用，而前面的方案是完全不需要 B 有任何信用的。

4. 闪电支付通道中交易的快速零手续费使用，及双向通道实现



建立了类闪电支付通道后，当 A 需要付给 B 币时，那就一个从 3CSm 地址发向 1Dog 地址和 1Bit 地址的一对二交易 TX3。用其私钥签名签名后发给 B。当 B 拿到签名交易 TX3 后，就已经等价于确认拿到币了。而这个速度是仅仅是生成交易和传送字串可以做到秒速的，甚至在一些工具下能做到即时支付。

1.2 柔支付的具体应用

A 向 3CSm 地址转了 0.1BTC 比特币，A 需要向 B 支付 0.02 BTC，那么就构造一个交易 TX3 发向 B 的 1Dog 地址 0.02 BTC 和找零到 A 的 1Bit 地址的 0.0799 BTC，而 0.0001 BTC 作为手续费。A 用私钥签名的后发送给 B，B 收到后再用 B 的私钥签名确认通过确定 A 的签名没有问题，即完成确认收到了 0.02 BTC 的支付，没有必要将这个交易 TX3 广播。可以继续维持类闪电支付通道。

然后过了些日子，再次需要 A 支付给 B 这次 0.03 BTC 时，加上上次的总共是 0.05BTC，

那么再次来构造一个 TX4，这次要发向 B 的 1Dog 地址 0.05 BTC 了，找零到 A 的 1Bit 地址的 0.0499 BTC。在签名好后发送给 B 即可，秒速确认，且因为是链下的不用发送的链上，也没有手续费。

注意可能有人发现了，这个类闪电支付通道是单向的，只是 A 付给 B，那么当需要反向 B 需要付给 A 时怎么办呢？可以再重复上面的步骤再建立 AB 之间的类闪电支付通道，注意互换 AB，且用另外一个 2-of-2 多重签名合成地址 3Njd 地址的来作为类闪电支付通道的主地址，这个地址的主控制权就在于 B 了，可以 B 来签名交易发给 A，来实现 B 付给 A。其实这种用两通道实现双向会更加清晰些。

本质上因为有那笔锁定时间交易 TX2 存在，3CSm 地址上的币是属于 A 的。3Njd 地址上的币是属于 B 的。而在需要类闪电支付时，A 可以签名交易 TX3 重新分配 3CSm 地址上的币将需要付给 B 的币分配给 B，只要拿到签名交易 TX3，就已经是拿到只要在锁定时间之前随时公布即可，没有必要立刻公布而关闭通道，而多次频繁中间双方收发交易仅仅是发送签名的最新交易即可，而这些数据即使第三方拿到也没有什么用，也无法发布广播，因为只有一个签名。

1.3 支付通道的两种关闭形式

A 与 B 之间没有任何类闪电支付交易，在锁定时间到了后，A 可以广播交易 TX2，从而拿回全部在 3CSm 地址上币，从而关闭通道，A 损失的仅仅是锁定时间和一点点手续费，并没有大的损失。下次开启可以只对有可能对其较高频率付款的 B 开通，且尽量将锁定时间设的久些，可以避免这种无使用就关闭地开启类闪电支付通道。

2. A 有通过类闪电支付通道交易多次发给 B 的一些签名交易重新分配 3CSm 地址的币。在锁定时间到来之前，B 对对自己最有利也一般是最新的签名交易，自己再签名之后广播，从而闪电支付通道链上结算成功关闭通道。然后若还有类闪电支付需求可以重复上面的步骤再次开启，并且 2-of-2 多重签名合成地址 3CSm 地址，是不用更换的，可以继续使用。因为再此重复时在 TX1 中的交易 ID，和 TX2 个的交易 ID 都已经变化了，故以前的那些签名都会作废失效的，因此不必担心上次的类闪电支付通道的交易签名，会对这次新的类闪电支付通道产生影响。

二、柔支付网络（RouPay Network） 的核心设计

2.1 多重签名及合成地址生成

多重签名合成地址，以 3 开头的比特币地址收发币，而这种 3 开头的比特币地址则是先生成获得合同脚本，然后对合同脚本进行 hash160 算法后，再对其用 0×05 版本 Base58Check 编码得到的。花费这些合成地址里的币，需要根据生成时设的合同脚本的要求，一般需要多个私钥进行签名，因此也常叫合成地址为多重签名地址。实际上，具体看生成时设的具体的合同脚本，有些脚本可以设为只需要一个签名，而不一定非要进行多次签名。因为其一般是由多公钥合成的，因此命名叫合成地址较好些。多重签名技术 createmultisig 命令生成合成地址，“合同脚本”内容的生成很关键，可以用这个 createmultisig 命令用来生成。这个命令用途应用很广泛很灵活，而具体使用时却很简单，只有必须要输入的两个参数：

一个参数是数字 M，为正整数，要求 M 要不大于下面的参数中的 N。

另外一个参数是长度为 N 的数组，即数组内放有的公钥的数量为 N 个。

具体含义是花费时需要提供 N 个公钥对应的私钥中的任意 M 个的签名即可。若 M=1，那么表示后面数组中的任何一个公钥对应的私钥都可以花币。而若 M=N，则表示必须全部私钥都签名才可以花币。这两种极端情况的中间情况往往较多使用。常用的 2-of-3 的多重签名的合成地址生成方式，就是第一个参数 M 设为 2，在第二个数组参数中，放入 3 个公钥，那么这种生成的合成地址，就是只要这 3 个公钥对应的私钥中的任意两个进行签名，就可以花这笔交易。可在电子商务领域也有较多应用，买家、卖家和平台可以各拿一个私钥，平时买卖双方可以凑够两个签名，而出现争议时可以由平台用其的签名来仲裁决定平币分配。

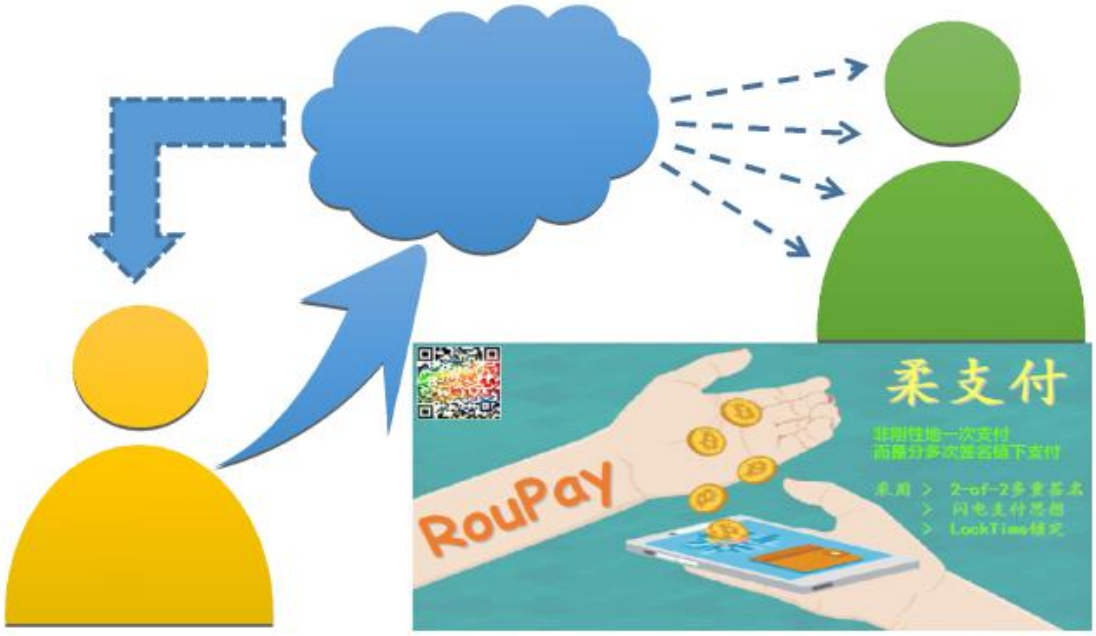
2.2 分配金的签名重分配支付

这个分配金是实现支付通道的关键。具体是采用上面提到的多重签名。具体是生成 2-of-2 多重签名，简单说就是两地址之间达成共识一致都签名时才能交易。参数 M 设为 2，而公钥数组中填写两个公钥。双方达成一致都签名同意时才能动这个 2-of-2 多重签名合成地址里的分配金。闪电网络和雷电网络的通道设计思路都是，由双方共同出一定资金来发到形成分配金，然后给出各多少币的分配方案。然后再签名共同签名更新这个分配方案。同是设计一些机制来作废掉之前的历史分配。最新分配方案与上个分配方案之间的差额，即通道支付的币量。因为仅仅签名，验证正确即可，只需发给对方，不需要在比特币主网络上广播，因此能实现秒速确认。虽然开启和关闭通道需要一定手续费，但通道建立起来后在通道上的交易是完全可以做到免费，或者极低的费用。柔支付网络也是分配金通道，签名来重新分配

的基本原理，但会更加简单易于理解，且易于实施。

2.3 柔支付单向通道建立

简单来说，就是发送者和接收者，发送者把币发到两者的公钥生成地址，然后靠多次签来给接受者的分配比例的越来越高，来实现支付。另外就是有一笔时间戳交易，能在过了时间后，能将分配金的全部币全部归还回归发送者。



这个通道时单向的，只能当 A 需要付给 B 币，且分配给 B 的量会越来越多。当 B 需要向 A 付币时，需要用 3Njd 地址建立个反向的通道。两个通道互动才能双向支付。并且当额度超过是通道会关闭。另外注意需要在 nLocktime 的时间之前关闭柔支付通道。注意修改下 nLocktime 锁定时间为合理的时间 nLocktime, 也被称为 LockTime 或 lock_time, 通常被设置为 0，表示交易可随时发送到比特币网络。如果 nLocktime 的值在 1 到 5 亿之间，则表示需要区块高度大于或等于 nLocktime 的区块时才可以写入区块链。如果 nLocktime 的值超过 5 亿，则表示从 1970 年 01 月 01 日开始算，加上 nLocktime 秒之后的一个时间点，即 Unix 时间戳，例如 2018 年 1 月 1 日是 1514736000，若早于那个时间点，则该交易不会被发送到比特币网路。另外注意 sequence 字段，不能为 INT32 最大值(0xffffffff)，否则会忽略 nLocktime。

1）收集 A 与 B 各自的公钥生成两柔支付的多重签名地址

假设 A 是发送者，B 是接收者，公钥在交换公钥的位置后可以生成两个 2-of-2 的多重签名合成地址，公钥是可以公开的信息，可以主动公开，也可以在线快速生成合成地址。

2）A 构造发到合约地址的交易 TX1,及从合成地址锁定时间发回交易 TX2 发给 B

3）A 发给 B 交易 TX2 的交易，获得签名后广播 TX1 形成闪电支付的通道把上面的交易 TX2 发给 B,请 B 来确认无误后用 1Dog 地址私钥签名会发回给 A。A 在收到来自 B 的签名后，然后用自己 1Bit 地址的私钥签名，检查是否成功。若 TX2 校验成功，则可以将之前的交易 TX1 出去，从而形成类闪电支付通道。手里的 TX2 交易注意保存，等锁定时间过了后可能需要广播出去找回。

2.4 柔支付通道实现双向及跨链

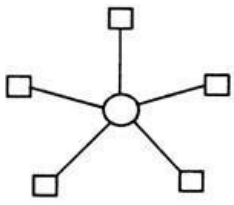
2-of-2 多重签名的等柔支付网络电通道是单向的,，这可能是与闪电网络最大的区别，只能单向的只增不减地从一方向另外一方转币，若想要双方互转，就要通过建立两个相互独立的通道来实现。而闪电网络是可增可减少，完全可任意重新的分配，可增可减，只要有双方签名即可，以时间最新的分配方案为准，之前的任意分配方案将无效。而类闪电支付是没有时间先后顺序的，都是有效。但作为接受方当然会拿币量最多，一般也是最新的自己量最多的分配方案。而发币的发送者因没有收币者的签名的无法发布任何分配版本的。等时间戳到，或者等收币者关闭。

因为只要支持有多重签名，有时间戳交易即可实现柔支付通道，因此可以 A 到 B 是比特币柔支付通道，而 B 到 A 是狗狗币柔支付通道。于是便相当于实现了跨链和安全地币币交易。

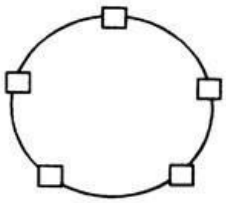
2.5 分层树形拓扑的柔支付网络

网络拓扑方式，第三方支付会是（a）星形，而比特币的点对点是图（c）网状态。

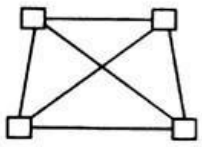
闪电网络估计早期可能椒（b）环形已行程链六，而我们柔支付网裸将会近似于树形。



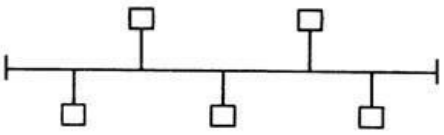
（a）星形



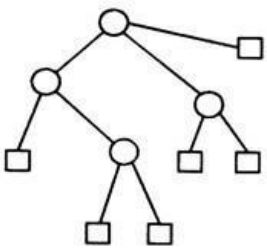
（b）环形



（c）网状



（d）总线形



（e）树形

柔支付的运行原理是发起 2of2 多重签名，在此之后发起一笔全部币回归的延时交易。靠发送交易的签名，逐步增多分配实现单向快速支付。建立两个通道因为只需要将签名后的字串发过去，并不需要广播，进而可以实现快速即时且 0 手续费的交易。

2.6 柔支付网络支付路径设计

根节点将负责跨树枝的交易，因此若仅仅一层就类似于星行网络了，经过 1 个节点。而两层网络，最多中间 3 个节点。而 3 层网络最多是，中间 5 个节点。N 层网络最多 2N-1 个节点，都是先到上一层到根节点。再到目标。若在同一个分支中则不需要向上，类似于域名解析服务。根节点这里可以存储所有的最新数据，切定期的与下层的节点进行结算。

2.7 特殊情况下的应用

柔支付节点出问题的应对：

因为是 2of2 需要双方签名才能动币，因此就算大量节点都出问题都没有了，也并不会造成资金损失。

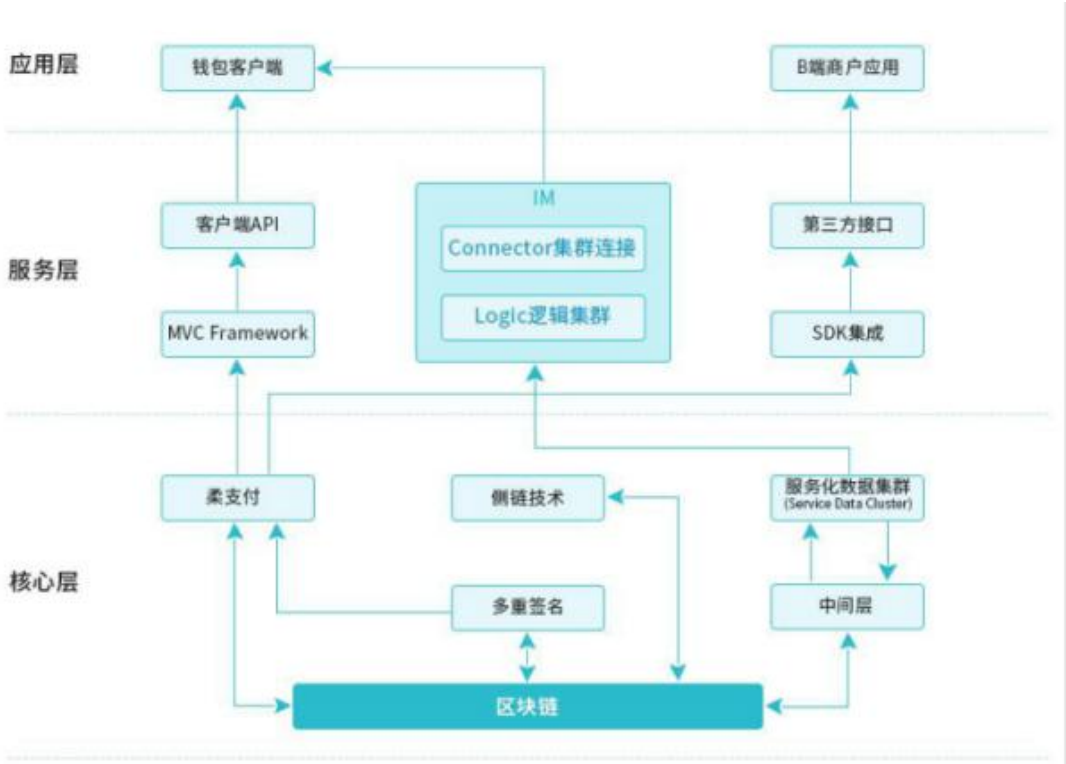
1. A 与 B 之间没有任何类闪电支付交易，在锁定时间到了后，A 可以广播交易 TX2，从而拿回全部在 3CSm 地址上币，从而关闭通道，A 损失的仅仅是锁定时间和一点点手续费，并没有大的损失。下次开启可以只对有可能对其较高频率付款的 B 开通，且尽量将锁定时间设的久些，可以避免这种无使用就关闭地开启类闪电支付通道。

2. A 有通过类闪电支付通道交易多次发给 B 的一些签名交易重新分配 3CSm 地址的币。在锁定时间到来之前，B 对对自己最有利也一般是最新的签名交易，自己再签名之后广播，从而闪电支付通道链上结算成功关闭通道。然后若还有类闪电支付需求可以重复上面的步骤再次开启，并且 2-of-2 多重签名合成地址 3CSm 地址，是不用更换的，可以继续使用。因为再此重复时在 TX1 中的交易 ID，和 TX2 个的交易 ID 都已经变化了，故以前的那些签名都会作废失效的，因此不必担心上次的类闪电支付通道的交易签名，会对这次新的类闪电支付通道产生影响。

三、架构设计

3.1 整体架构：核心层、服务层、应用层

XCoinPay 的整体架构分为三层：核心层、服务层、应用层。架构图如下：



其中：

1.1 核心层

由区块链节点与消息网络组成的区块链部分实现交易数据的广播，经由矿工打包交易录入区块链。其中采用柔支付通道技术，提前开通支付通道，实现快速交易。为 IM 服务提供数据存储。

1.2 服务层

该层针对业务场景，采用 MVC 架构，分离处理客户端与 B 段商户业务：针对钱包客户端，提供对应的 API 接口；针对 B 端商户应用，提供集成 SDK，方便第三方对接调用。针对 IM 部分，该层提供对应的处理逻辑，承载应用层 IM 的读写与核心层数据集群的交互。

1.3 应用层

该层向终端用户提供基于分布式账本的应用服务，如币种数字资产的钱包、交易、第三方应用对接 SDK 写入交易等。

3.2 总体架构设计

总体架构包括 5 个层级，具体内容如下图 1 所示：

各层级说明如下

用户端：该层重点是移动端，支持 iOS/Android 系统，接入客服系统。

用户端 API：该层依据不同业务类型使用 TCP 协议、HTTP 协议，为移动端提供 iOS/Android 开发 SDK。H5 页面，提供 WebSocket 接口。

接入层：该层主要保护海量用户连接、攻击防护，整流海量连接成少量 TCP 连接与逻辑层通讯。

逻辑层：该层负责 IM 系统的核心逻辑实现，例如：群聊、单聊、朋友圈、等等。

存储层：该层负责缓存或存储 IM 系统相关数据，主要包括用户状态、消息数据、文件数据等。

3.3 数据存储格式采用 Protocol Buffer，database 选择 MoogoDB

Protocol Buffer 是一种轻便高效的结构化数据存储格式，在.proto 中定义消息格式，使用 protocal buffer 编译程序，直接生成目标文件，便于多端同步，另外该目标文件在各大平台之间均可运行，解决跨平台问题。

Protocol Buffer 有如 XML，但更小、更快、更简单，在解析速度与占用空间上具有性能好效率高的特性。Protocol Buffer 不需要解析后再进行映射，直接序列化反序列化直接对应应用程序中的数据类。MoogoDB 可以将热点数据加载到内存，在大数据量是，查询效率优势明显,MoogoDB 采用 BSON 的方式存储数据,对 JSON 格式数据具有非常好的支持性，方便平台之间对接 MoogoDB 数据库的分片集群负载具有非常好的扩展性以及非常不错的自动故障转移。

四、彩色区块链专利技术

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106529924 A
(43)申请公布日 2017.03.22

(21)申请号 201610864109.9

(22)申请日 2016.09.29

(71)申请人 马龙
地址 528311 广东省佛山市顺德北滘镇美的翰城11座1503

(72)发明人 马龙 周朝晖 曾舜斌

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
代理人 张大威

(51)Int.Cl.
G06Q 20/06(2012.01)
G06Q 20/38(2012.01)

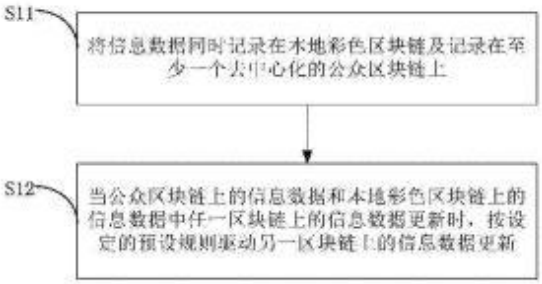
权利要求书1页 说明书7页 附图3页

(54)发明名称

彩色区块链的管理方法及管理系统

(57)摘要

本发明公开一种彩色区块链的管理方法及管理系统，彩色区块链的管理方法包括：将信息数据同时记录在本地彩色区块链及记录在至少一个去中心化的公众区块链上；当公众区块链上的信息数据和本地彩色区块链上的信息数据中任一区块链上的信息数据更新时，按设定的预设规则驱动另一区块链上的信息数据更新。上述彩色区块链的管理方法，通过将信息数据同时保存在彩色区块链及公众区块链上，降低了使用公众区块链和建立基于区块链的资产信息管理系统的技术门槛和安全维护成本，使彩色区块链对应的项目能更加专注项目本身的应用开发，因此，上述彩色区块链的管理方法能高效灵活地应用于各细分具体领域。



9924 A

本彩色区块链技术的申请的专利已经公开，可以通过专利号在各专利官网查询下载。

CN201610864109.9 一种彩色区块链的管理方法及管理系统，彩色区块链的管理方法包括：将信息数据同时记录在本地彩色区块链及记录在至少一个去中心化的公众区块链上；当公众区块链上的信息数据和本地彩色区块链上的信息数据中任一区块链上的信息数据更新时，按设定的预设规则驱动另一区块链上的信息数据更新。上述彩色区块链的管理方法，通过将信息数据同时保存在彩色区块链及公众区块链上，降低了使用公众区块链和建立基于区块链的资产信息管理系统的技术门槛和安全维护成本，使彩色区块链对应的项目能更加专注项目本身的应用开发，因此，上述彩色区块链的管理方法能高效灵活地应用于各细分具体领域。

五、团队与顾问

核心成员：

赵世达　CEO

毕业于上海工程技术大学，资深互联网从业者，持有申报软件著作权两项，设计、运营过一系列互联网产品，产品涵盖有手机 APP、自媒体网站、电商平台等，对区块链、数字货币发展密切关注，积极探索区块链落地应用。由于区块链的技术启发，设计过基于哈希算法、不可作弊的彩票抽奖系统。

马　　龙 CTO

武汉大学硕士、清华大学 iCenter 特聘讲师、亚洲区
块链 DACA 协会特聘讲师、巴比特资讯专栏作家、巴比特意见领袖、IDGUI 导航平台、8Doge 币应用创始人、施比爱 CTO&联合创始人、论坛版主。知名的作品有：脑口令钱包工具，新币产量减半倒计时，币域名平台，EW 留言，彩色区块链等。

CARLOS CHOONG　COO

CARLOS CHOONG 是马来西亚华人，在香港金融公司工作多年，也在美国、英国生活和工作过，海外关系广泛，CARLOS CHOONG 在传统金融领域有丰富经验，同时也是比特币老玩家，在马来西亚首都吉隆坡拥有大型矿场。

顾问：

周朝晖　顾问

复旦大学毕业，中国狗狗币协会副会长、DACA协会与清华大学 iCenter 特聘讲师、世界区块链基金会（WBD）研究员、施比爱（shibe.io）创始人、Joomla 开源建站系统资深协作者和专业咨询师。2003 年起参与国际开源软件的协作，深谙开源项目和去中心化自治组织的运作机理。目前正在深入区块链的应用。

主编：《如何投资数字货币》（电子工业出版社）、《狗狗币：最宝贵的人生财富》（免费电子版）

参编：《区块链开发讲义》在编：《2 分钟投资全球区块链项目》、《比特币全球电商平台 OpenBazaar》

黄连金　技术顾问

著名区块链专家

美国 ACM Practitioner Board 委员

中国电子学会区块链专家委员

Well-known Blockchain Expert
ACM Practitioner Board Commit Member
Chinese Electric
AcademyBlochchain Expert
Committee Member

FAQ:

柔支付网络是否安全？

答：柔支付网络是去中心化的，任何开发者和管理团队都无法挪用户资产。

柔支付网络（RouPay Network）的发展前景如何？

答：1） 柔支付网络（RouPay Network）打造的是底层区块链，底层区块链最有发展前景的。而 XCoinPay 的切入领域是区块链支付领域，支付领域是市场的绝对刚需。

所以 XCoinPay 的发展前景非常广阔，未来可预见到很多用户、商家、交易所将接入柔支付网络（RouPay Network）这样的安全去中心化的支付系统。

柔支付网络（RouPay Network）和闪电网络及雷电网络相比，优势在哪里？

答: 闪电网络和雷电网络对区块链资产更具有针对性，闪电网络主要是支持比特币和莱特币等等，而雷电网络用来支持以太坊，就灵活性而言，闪电网络和雷电网络很难全面的支持多币种，而柔支付网络（RouPay Network）兼备良好的可扩展型和可编程性，可以轻松支持多币种，并且作为一个区块链支付底层平台，柔支付网络（RouPay Network）可以衍生出诸多的商业解决方案，具有极大的灵活性、拓展性和可编程性。

XCoinPay 关心比特币和以太坊的扩容问题吗？

答：其实 XCoinPay 并不是特别关心比特币和以太坊的的扩容问题，因为使用柔支付网络（RouPay Network）可以完美解决这些问题，并且带来扩容后的效果。
打个比方，现在的比特币和以太坊就好像两条非常堵车的公路，大家都在讨论扩建公路来解决堵车的问题，而柔支付网络（RouPay Network）直接提供了飞机航班来解决问题，因此 XCoinPay 并不太关心比特币和以太坊的扩容问题，只关心飞机航班的建设。

作为一个区块链底层平台，柔支付网络（RouPay Network）的特性是什么？

答：柔支付网络（RouPay Network）具有极大的可拓展性和可编程性，基于柔支付网络（RouPay Network）可衍生出多种商业解决方案。

XCoinPay 和 bitpay 有何不同？

答：BitPay 是针对收取区块链资产的商户提供解决方案，但是 BitPay 提供的是链上解决方案，这种解决方案受限于比特币网络的速度和手续费，有很大的弊端。例如，BitPay 近期宣布由于比特币确认速度慢和手续费高昂的原因，BitPay 将不再支持比特币的交易。因此随着时代

的发展，BitPay 的链上解决方案不会是主流，柔支付网络（RouPay Network）提供的链下清算方案，速度快且零手续费，因此将成为主流的解决方案。

柔支付网络（RouPay Network）和瑞波和恒星有什么差别？

答：恒星和瑞波致力与发展线下网关、跨境汇款和协议类产品，而柔支付网络（RouPay Network）则完全不同，柔支付网络（RouPay Network）作为一个区块链底层平台，可以在上面建立各种商业应用。

柔支付另外还能解决哪些问题？

答：柔支付网络将是扩容之争的最终解决方案

市场和用户最终会接受 XCoinPay 吗？

答：现在的市场和用户，需要一定时间去接受这种链下清算系统的概念，因为目前用户已经习惯使用去中心化钱包去储存和发送区块链资产，但这有很多痛点—去中心化钱包虽然安全，但是相当笨重—速度慢而且费率高，而且去中心化钱包将像传统意义的保险柜，很难衍生出区块链商业解决方案。
柔支付网络（RouPay Network）作为新一代的区块链支付网络，特性是轻快、免费，而柔支付网络（RouPay Network）和去中心化钱包一样安全，因为柔支付网络（RouPay Network）也是去中心化的，市场需要时间去接收这样的一个新型支付网络。
另外柔支付网络（RouPay Network）兼备良好的可扩展型和可编程性，可以轻松支持多币种，并且作为一个区块链支付底层平台，柔支付网络（RouPay Network）可以衍生出诸多的商业解决方案，具有极大的灵活性、拓展性和可编程性。
但我们仍然认市场需要时间来接受这样的一个强大的工具，所以我们会向市场推广柔支付网络（RouPay Network）的概念，并打造柔支付网络（RouPay Network）的品牌效应，让更多的用户和商家接收和使用柔支付网络（RouPay Network）。

交易所接入柔支付网络，有什么好处？

中心化的交易所存在很多痛点，充值和提现都走链上支付的形式，速度缓慢且费率高昂，所以柔支付网络（RouPay Network）可以解决这个问题，交易所接入柔支付网络（RouPay Network）后，将有很多意想不到的好处

零费率：交易所接入柔支付网络（RouPay Network）后，交易所将不再有充值和提现的费率，用户可以省掉这笔钱，因为所有的充值和提现全部通过柔支付网络（RouPay Network），而通过柔支付网络（RouPay Network）转移区块链资产是零手续费的

速度极快：交易所接入柔支付网络（RouPay Network）后，用户通过柔支付网络（RouPay Network）向交易所充值或者是提现是秒速到账的，对于一部分交易者，这会让他们可以迅速操作，而不错过行情。

交易所将不再有“钱包维护中，禁止提币”的通知，因为交易所使用的清算系统是柔支付网络（RouPay Network），柔支付网络（RouPay Network）是基于区块链的，7x24 小时运转，不会停机。

当交易所普遍接入柔支付网络（RouPay Network）后，用户在 A 交易所购买的加密数字货币，可以瞬间转移到 B 交易所卖出盈利，得益于柔支付网络（RouPay Network）带来的极高的流动性，各大交易市场的价格会趋于一致，这也是一个市场趋向成熟的表现。

柔支付网络（RouPay Network）有哪些商业模式？会变革哪些领域？

答：柔支付网络（RouPay Network）将首先变革支付方式和交易所。
支付方式：用户使用柔支付网络（RouPay Network）进行转账和收款，可以实现瞬间、秒速、零手续费，这将变革现在普遍使用的链上支付方式。

交易所现有的模式根深蒂固，柔支付将如何变革交易所？

答：首先，我们难以说服大型交易所使用柔支付网络（RouPay Network）。因此，初期我们将把与中小型交易所的合作作为突破口，中小型交易所接入柔支付网络（RouPay Network）后，柔支付网络（RouPay Network）将为中小型交易所带来大量流量和交易，而与中小型交易所的合作，也将为柔支付网络（RouPay Network）带来用户数量的爆发性增长，直到整个市场都广泛接收柔付网络的概念和产品，然后大型交易所将不得不接入柔支付网络（RouPay Network）。

如果有的交易所始终拒绝接入柔支付网络（RouPay Network）呢？

用户去一个商店购买商品，用户拿出了手机打开了 paypal：“我将用 paypal 付款，如果你不支持 paypal 支付，我会去其它商店购物”
同理，现在看似不可撼动的交易所，将在这场革命中被革新——如果某些大型交易所拒绝变革，那么将成为陨落的巨头。

针对中心化交易所存在的种种痛点，有一种解决方案是去中心化交易所，那么去中心化的交易所和柔支付网络（RouPay Network），哪个更具优势？

答：现阶段，去中心化的交易所受限于区块链的高并发问题，普遍存在产品体验差、速度慢等等问题，去中心化交易所的技术现在非常不成熟，短期内不会成为主流的解决方案。
而从用户层面来看，交易所的核心竞争力是产品体验和服务，去中心化的交易所在这两方面都是弱项，很简单，你想象一下无人餐厅就知道了，没有良好的服务，那么没有人愿意来就餐。

柔支付网络（RouPay Network）的使用流程是怎样的？

答：跟传统的使用方式相同
充值：用户将充值区块链资产到柔支付网络（RouPay Network），就可以使用秒速收发区块

链资产。
转账：在柔支付网络（RouPay Network）内转账是秒速并且零手续费的，并且可以使用通用

地址功能—输入对方的通用地址便可以转账任何区块链资产
提现：用户发起提现申请，中间没有任何人工审查，提现速度只受限于比特币网络速度
优势：操作简单，无需任何操作门槛，用户易于接受。

你认为柔支付网络（RouPay Network）将会被市场广泛接受吗？

答：回顾历史可以预知未来，一个去中心化的、高效且安全的区块链支付系统必将是历史发展的必然产物。

随着柔支付网络（RouPay Network）的市场知名度和用户数量的提升，柔支付网络（RouPay Network）将以星火燎原之势，颠覆区块链支付和变革交易所的现有模式——因为，柔支付网络（RouPay Network）给用户带来了极大的安全保障和更好的用户体验，就像 PayPal 刚面世的时候，通过用户的口口相传，以极高的用户体验和产品粘度，PayPal 成为了主流支付方式，我认为，同种情景也会发生在柔支付网络（RouPay Network）这个产品上

使用 XCoinPay，对用户有哪些好处？

1.用户将区块链资产充值进柔支付网络（RouPay Network）后，收发区块链资产将是秒速并且零手续费的，而用户的资金并没有第三方掌控，因为柔支付网络（RouPay Network）是去中心化的，用户不用担心资金安全问题
用户使用 XCoinPay 将会有多种选择—可以同时使用去中心化钱包和柔支付网络（RouPay Network），并且用户可以使用所有接入柔支付网络（RouPay Network）商家和交易所

参考文献

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system

[2] 马龙，《柔支付：基于 2-of-2 多重签名实现的类闪电支付》

[3] 马龙，《你应知道的币地址和私钥的一个重要秘密》

[4] 朱立，《详解最近大热的闪电网络、雷电网络和 CORDA》

[5] 英国政府首席科学顾问报告,《分布式账本技术：超越区块链》

[6] 马龙，《如何能做到比特币快速确认到帐？》

[7] 《闪电网络非常伟大，但它也面临各种类型的问题》

[8] printemps 《闪电网络：比特币网络的飞跃》

[9] Vitalik Buterin,Ethereum:A Next--Generation Smart Contract and Decentralized Application Platform。

[10]Blockchain Technology Market by Provider, Application, Organization Size,Vertical, and Region 。

[11]David Schwartz, Noah Youngs, and Arthur Britto. The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 5, 2014.

[12]Economist Staff. "Blockchains: The great chain of being sure about things". The Economist, 18 June 2016.

[13]Juan Benet. "IPFS - Content Addressed, Versioned, P2P File System"

[14]Popper, Nathan (2016-05-21). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". New York Times

[15]《The future of financial infrastructureAn ambitious look at how blockchain can reshape financial services》