XCoinPay 白皮书

XCoinPay— 区块链支付领域的 PayPal ！

XCoinPay.io

（V2.4）

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）。

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）是一个瞬间、自由、安全的分布式链下支付网络

柔支付网络（RouPay Network）是潜力巨大的二层支付网络，柔支付网络（RouPay Network）采用了树状网络的拓扑模式，可以在维持足够高去中心化度地前提下，能通过网络简洁地提升网络效率和增加网络生态的扩展能力，降低摩擦提升运行效率，从而建立起一个完善的支付网络生态系统。

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（RouPay Network）可以解决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（RouPay Network）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（RouPay Network）是一个崭新的区块链支付网络，基于柔支付（RouPay）技术为底层打造，使用柔支付技术可以达到速度快、操作安全、去中心化等优点。未来使用柔支付网络（RouPay Network）可以实现零费用、极速发送区块链数字资产，柔支付网络（RouPay Network）致力于提升区块链支付领域的用户体验，打造革命性和颠覆性的区块链支付网络，成为区块链支付领域的 PayPal。

比特币的高额转账手续费和蜗牛般的到账速度实在让人无法忍受，而关于是否要扩容以提升交易速度的问题，社区意见不一，争吵了很久，但不能否认的是，比特币的高额转账手续费和极慢的到账速度极大地影响了比特币的发展，直接导致了分裂出了更大区块的 BCH。

相比传统的支付系统，比特币支付系统的每秒交易量上限是 7 笔，而 visa 的平均每秒交易量百万，支付宝峰值接近千万，如何提升比特币的交易速度，成了一个棘手的难题。

从技术层面上看，交易处理能力和区块链数据容量似乎是一对无可调和的矛盾，通俗来说，如何提升比特币的转账速度而又不在比特币区块链上做太多改动，似乎成了一个鱼和熊掌不能兼得的难题。

为了解决这个问题，闪电网络的创始人 Joseph Poon 提出了闪电网络的概念，以提升区块处理交易的效率，不可否认的是，闪电网络的理念非常了不起，社区甚至认为：“闪电网络”的论文（The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments）对比特币的重要性仅在中本聪的创世论文之下，排名第二。

从技术角度来说，闪电网络的本质是使用了哈希时间锁定智能合约来安全地进行确认交易的

一种机制。首先，所有未确认的闪电网络交易都是基于现有的已确认的资金交易的。这些资金已经在比特币网络上多重签名地址中得到了的确认，未确认的闪电网络交易就是基于这些已确认的交易的。

在这种大背景下，XCoinPay 的开发团队自主研发了柔支付技术（RouPay），柔支付技术（RouPay）综合地运用了 2-of-2 多重签名，锁定时间交易，和交易构造延后广播等等技术，实现了可以在不需相任的情况，完成建立类闪电支付通道，进行免手续费且秒速确认的链下交易。

从技术层面上简单来说，柔支付技术（RouPay）聪明的利用了现阶段已经非常成熟了的多重签名技术，能在交易时实现链下的安全且去中心化的类闪电支付，可以实现区块链资产的瞬间零成本转移。

可以想象，使用柔支付网络（RouPayNetwork）可以完成比特币的瞬间零成本转移，带来的交易速度甚至媲美传统支付工具，这样的产品将是区块链支付领域的“杀手级应用”，而柔支付网络（RouPayNetwork）相比闪电网络来说，柔支付网络（RouPayNetwork）短小精悍，而且更简洁、更容易落地。

柔支付网络（RouPayNetwork）可以显著地解决现有区块链的传输低效问题，未来使用柔支付网络（RouPayNetwork），可以实现零费用、极速发送区块链数字资产，从而成为区块链支付领域的“杀手级应用”

柔支付网络技术原理阐述

1.柔支付的诞生及通道原理

1.1 多重签名确保币资产安全

多重签名是主流币种普遍支持的技术。也是二层网络应用如 LN 闪电网络和 RN 柔支付网络等底层的关键基础技术。

技术简单理解即像是给币资产上了多把锁，需要多方通过私钥共同解锁币才可以转移移动。也就是说，平台仅仅只有一把钥匙，没有用户的签名同意下，是无法独自地动币的。这即是与传统的完全平台掌握币的第三方链下钱包的最大的不同之处。

靠多重签名技术，能从区块链层面保证用户对其币的一半的控制权。进而能避免平台卷币跑路的情况。当然具体的多重签名技术，是允许有多个的，另外也可以指定收集其中任意多少个签名即可转移。即可以有多种多重签名模式，其中较常用的是 2-of-3 模式和 2-of-2 模式的多重签名。

1.2 即时零手续费的柔支付

有些人想要进行硬分叉扩容，背后的深层次原因不明，但直接原因是为了解决要么手续费高，要么确认时间久的问题。在比特币的设计模式下两者不可兼得的，付足够高手续费即可及时地在下个区块即较大概率确认满而未堵，而若想节省手续费只付低手续费，就要接受需要较久时间才能确认的可能。硬扩容是一个解决方案，但是其同时又带来另外的风险：若区块过大可能会提高全节点运行门槛使全节点中心化。

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。

柔支付 RouPay 技术具体见下方的参考文献 2，核心钱包会在授权下自动帮两用户，建立了一个柔支付通道，逐步进行签名支付，不会立刻在区块链上进行广播。另外以通过建立两个通道相互对冲的形式实现双方对等进而降低信任，通过自发的成为中间支付中转，从而实现陌生人之间的柔支付。任何人都可以成为中间的环节，从而可以实现去中心化。

图 1 柔支付技术原理示意图

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 开头地址的持有者，B 是 1Dog 开头地址的持有者。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，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

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，获得到交易 ID 和位置 n 数据即可，先不广播发布。

再由 A 或者 B(最好还是由 A)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 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 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，例如北京时间 2018 年 1 月 1 日 0 点是 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。

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

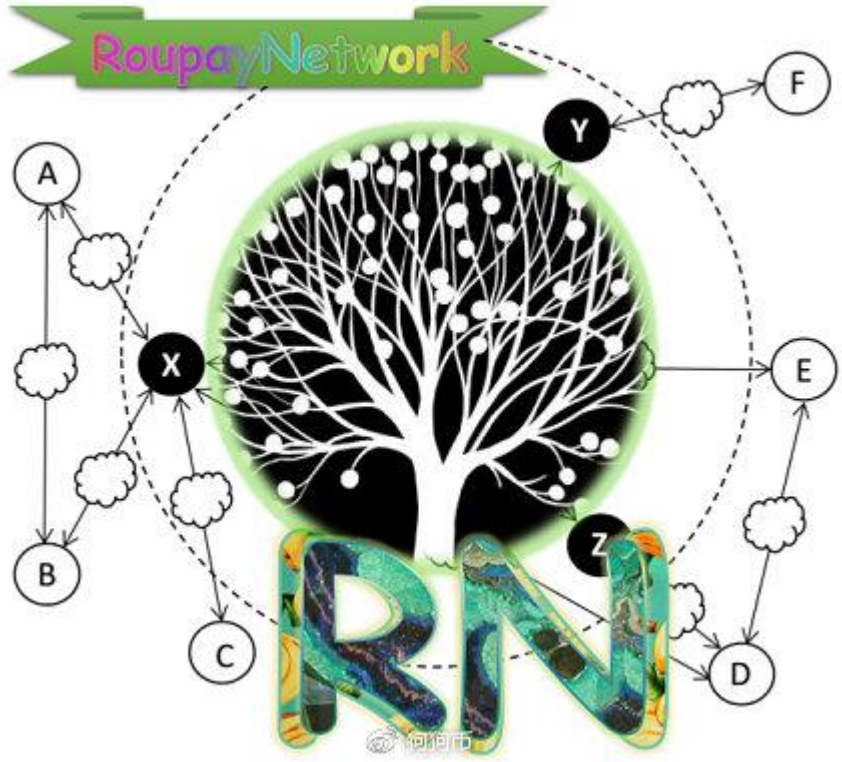
把上面的交易 TX2 发给 B，请 B 来确认无误后用 1Dog 地址私钥签名会发回给 A。A 在收到来自 B 的签名后，然后用自己 1Bit 地址的私钥签名，检查是否成功。若 TX2 校验成功，则可以将之前的交易 TX1 出去，从而形成类闪电支付通道。手里的 TX2 交易注意保存，等锁定时间过了后可能需要广播出去找回。

如果 A 对 B 有一定信任的基础下，A 可以不用手动构造交易 TX1 不广播，而是直接使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，A 注意妥善保存。同样可以形成类闪电支付通

道，该方式对 A 的技术要求很低，但需要 B 有足够的信任，而前面的流程方案是完全不需要 B 有任何信任的。

4）闪电支付通道中交易的快速零手续费使用

建立了类闪电支付通道后，当 A 需要付给 B 币时，那就从 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，就等价于确认拿到币了。方案仅生成交易和传送字串，可以做到秒速且 0 手续费。且在整合到核心钱包或一些钱包中时，能自动判断，从而能做到即时支付。



1.3 柔支付通道实现零手续费秒速确认

支付应用是各个币种都有的基本功能，但由于区块链本身需要全球同步共识的特性，并非都做好。一种思路是自己主链进行优化，但优化在提升支付效率的同时会造成去中心化度的降低很难两全。而另外一种思路就是在主链之上构建支付通道进一步形成二层网络。例如知名的 LN 闪电网络，这是很好的思路。我们 RN 柔支付网络也是同样的二层网络。

关于支付通道的建立，技术上和闪电网络类似，都是对多重签名地址中的币，进行不断地新分配方案签名替代旧分配方案，而新旧分配方案之间的差额作为通道支付额。不同之处在于 LN 闪电网络是双向通道，需要较复杂的构架和，而 RN 柔支付网络是单向通道。

虽然这个是 RN 柔支付网络的白皮书，但柔支付技术的诞生却在数年前。当时比特币主链已经有较大的交易处理压力，作为终极解决方案的 LN 闪电网络已经提出并且热议中。结合闪电网络的思想以及时间戳锁定交易的技术，首次于 2016 年 11 月 7 日公开发布在币圈知名的巴比特 www.8btc.com/2-of-2-multisig 文章受到广泛好评。当时临时取名“类闪电支付”的技术，最底层和闪电网络一样都是基于对 2of2 多重签名分配币的刷新签名再分配，然而不同之处在于巧妙地通过时间戳返回交易，构建了可逐渐缓慢多次支付的单向支付方式，即两者间建立了柔支付通道。

1.4 用户间建立的柔支付通道及形成双向通道

上面提到的柔支付通道是单向的，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。注意需要在 nLocktime 的时间之前关闭柔支付通道。

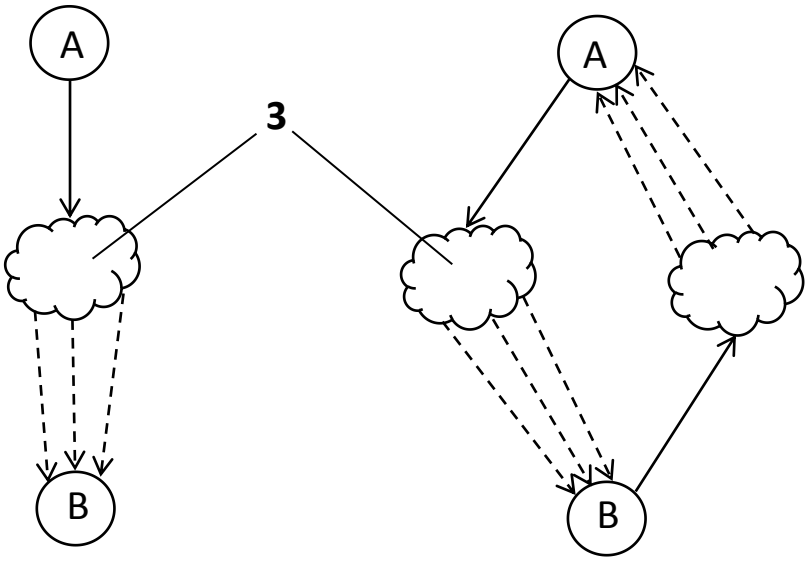


图 2 用户 A 与用户 B 之间建立的柔支付通道

因为原理层是单向的，而实际的支付需要中有可能需要双向，因此需要将单向拓展为双向。方法也很简单，A 到 B 建立个通道，B 到 A 再建立另外一个通道即可。

用户 A 与用户 B 之间建立 A->B 和 B->A 的双向柔支付通道。

第一步：扫码或网络连接或者直接内置，获得对方地址公钥，生成两个 2of2 多重签名分配地址。

第二步：构造自己发向分配地址和从分配地址延时回自己的两个交易，发送给对方。

第三步：签名后发给对方，收到验证后可广播自己发向分配地址的交易，形成双向通道。

一种多重签名的柔性区块链支付方法，其特征在于，包括以下步骤：

发送方将数字资产存放在需要多重签名才能支付的区块链多重签名地址中，且接受方签名同意将多重签名地址中的部分或全部币在某时间戳或区块高度后转回发送方 ,发送方通过区块链发送数字资产到上述多重签名地址中，开启柔支付通道；

发送方签名分配多重签名地址中发送方和接受方占有的币量，并将签名好的字串发给接受

方作为柔支付通道内实现的柔支付；

接受方验证签名是否正确来确认收到柔支付币量，之后可选择增加自己签名后区块链广播关闭柔支付通道或者不广播继续维持柔支付通道的开启状态。

区块链多重签名地址为 2of2 模式多重签名地址，需要发送方和接受方都签名才能动用所述区块链多重签名地址中的数字资产。

区块链多重签名地址为 2of3 模式多重签名地址，除了发送方和接受方外还有第三方，需要收集发送方、接受方和第三方中的任意两者的签名即可动用所述区块链多重签名地址中的数字资产。

第三方可以视为发送方或者接受方中的一方，即可有不只一个发送方或不只一个接受方。某时间戳或区块高度 ,具体可由发送方或者接受方来选择设定。柔支付通道内签名好的支付字串，可以交给平台进行管理维护防止丢失。

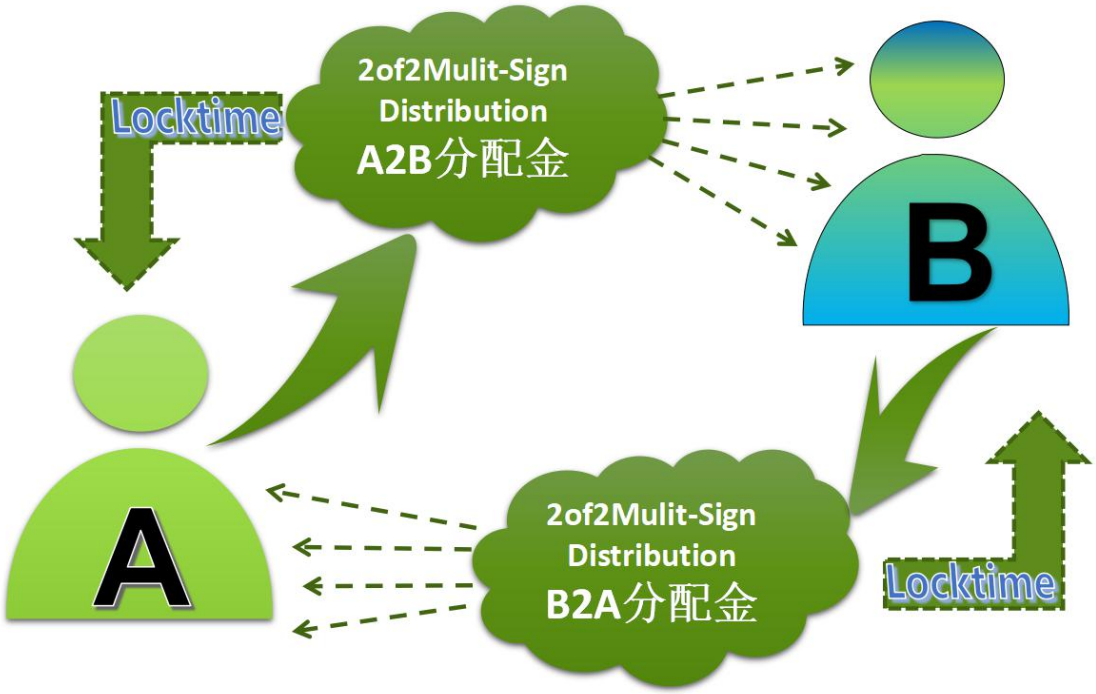


图 3 柔支付通道原理示意图

上图是 A 与 B 之间的柔支付通道的原理的示意，即 A 将币资产发到 A2B 多重签名的地址中作为分配金，然后在分很多次，逐渐增多的分配给 B 越来越多的币。而为了防止 B 一直不关闭通道，还有个时间戳锁定 Locktime 的交易将分配金转回给 A。而这个 Locktime 即通道的截止时间。B 需要在通道结束前关闭通道。

1.5 LN 闪电网络和 RN 柔支付网络通道比较

LN 闪电网络和 RN 柔支付网络都是属于二次网络技术，因此有很多地方可能相近，为了避免混淆，列表说明下底层的闪电通道和柔支付通道之间的区别。

表 1 闪电支付通道与柔支付通道对比表

	LN 闪电支付通道	**RN 柔支付通道**
依赖技术	多重签名、SW 隔离验证、CSV 延迟	多重签名、时间戳 Locktime
刷新签名方式	额外构建惩罚交易并签名作废旧分配	单向增多，天然地旧分配作废
使用次数	可理论无限次地不断刷新支付	分配金多少影响最大次数
时间限制	随时在 CSV 延迟其间决定是否可惩罚	只需关注 Locktime 确定时间
可支持币种	比特币 BTC、莱特币 LTC	几乎各种主流数字货币
实现难度	需要复杂地很多很多步实现困难	简单，使用几个现有接口即可

通过上表对比可以看到 RN 柔支付网络在底层相对于 LN 闪电网络是有一定优势的，其更加简洁，时间戳和分配币币量可根据需求随意设更加灵活，易于在各币种的区块链上具体落地应用。并且对主链矿业会更加友好，较少出现一直处于开通状态而不关闭通道的情况，可以有利于主链矿业，进而可得到矿业较好地支持。

RN 与 LN 的相同点：

1）整体原理和构架相同，都是底层多重签名建立通道签名实现刷新分配，上层形成网络路径实现陌生人间快速结算。

2）资金的安全均不依赖于中心，这是与第三方链下钱包的重要区别。即就算所有的节点网关全部都关闭或跑路离开，只要自己做好了签名的本地备份，便都不会损失任何币。

3）都不建议大额资金使用。定位的均是高频小额的日常场景，大额财富储值应去区块链主链。LN 是较严格的限制大额，而 RN 主要是在柔支付网关那限制，主要看各柔网关愿意给多大的额度。

RN 与 LN 的不同点：

1）在底层 RN 通道是单向通道，若想收发需要建个收通道再建个发通道。而底层的 LN 通道的是双向通道，即一个通道可以即能收又能发。

2）RN 通道有时间戳，靠时间戳的返回交易和不断增加的分配比例来实现刷新签名。而 LN 通道是靠构建惩罚交易，来作废之前的签名分配比例。

3）RN 支持的币种更多，因为原理底层柔支付并不需要 SW 隔离验证技术，因此很多没有这种技术的区块链均可接入柔支付网络。

4）网络拓扑结构不同。上面已经介绍了，RN 是树状结构网络，而 LN 是网状结构网络，任何两个 LN 节点都是平等的。虽然去中心化度更高，但进行连接时会更复杂，常有无法连接的情况发生。

5）技术门槛不同。要运行 LN 节点需要精通大量知识，而若基于钱包，其实和差别并不大。而 RN 可以将签名后的字串保持本地，即只要会签名和广播即可掌握运用柔支付网络。更加安全和实用。

从对比中也可以看出，柔支付网络 RN 的优势，首先门槛低

2.柔支付网络及跨链技术

2.1 柔支付网络系统的分层树形拓扑构架

网络拓扑方式，中心化的各第三方支付都是（a）星形，而比特币的点对点闪电网络 LN 定位高度去中心化的二层网络为图（c）网状态。而柔支付网络会近似于树形（e）拓扑。

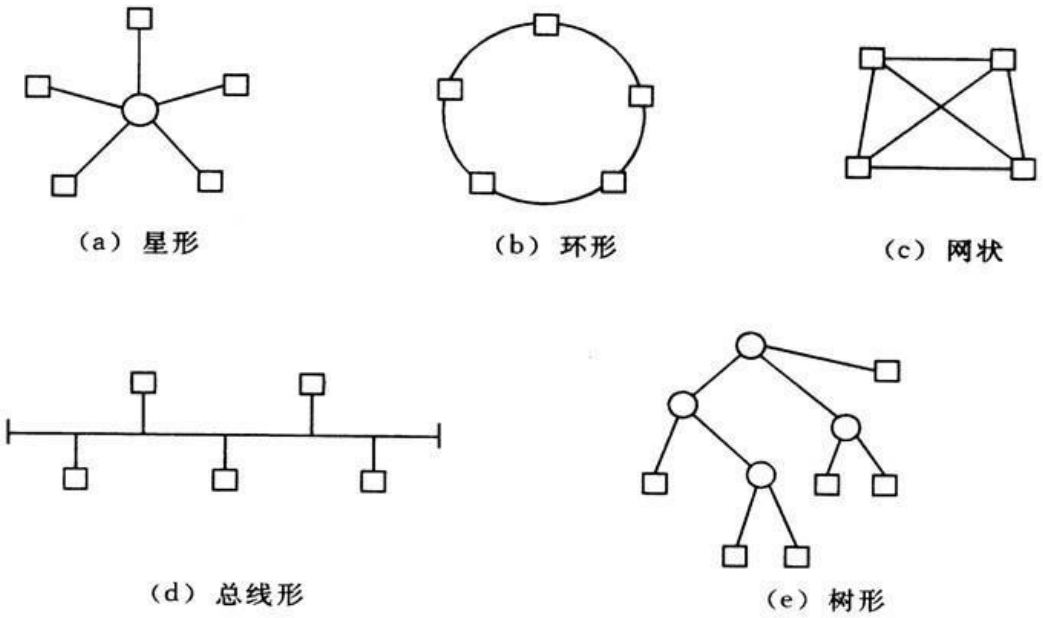


图 4 常见的网络拓扑图

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。

各个柔网关及其用户就像是很多局域网，要实现全球的互联，需要一个中转根节点。采用树状拓扑模式。中转根节点是树根树干，而各柔网关是各个分支，而用户就是树叶。一般分三层即可，若系统过于庞大而中转根节点较吃力时，可以考虑四层或更多层，即柔网关下面可分一些子柔网关。不过一般还是维持三层会更简洁高效些。这种构架下任意两人最多中间中转三次即可

柔支付。例如图中 A 想柔支付付给 F，可以通过 A 付 X，X 付 T，T 付 Y，Y 付 F 实现。注意要减少最好杜绝柔网关之间相互连接 ,否则会路由情况增多而增加系统的复杂度和稀释中转根节点的地位，甚至演变成点对点的网状网络。

2.2 柔网关与用户间建立的柔支付通道

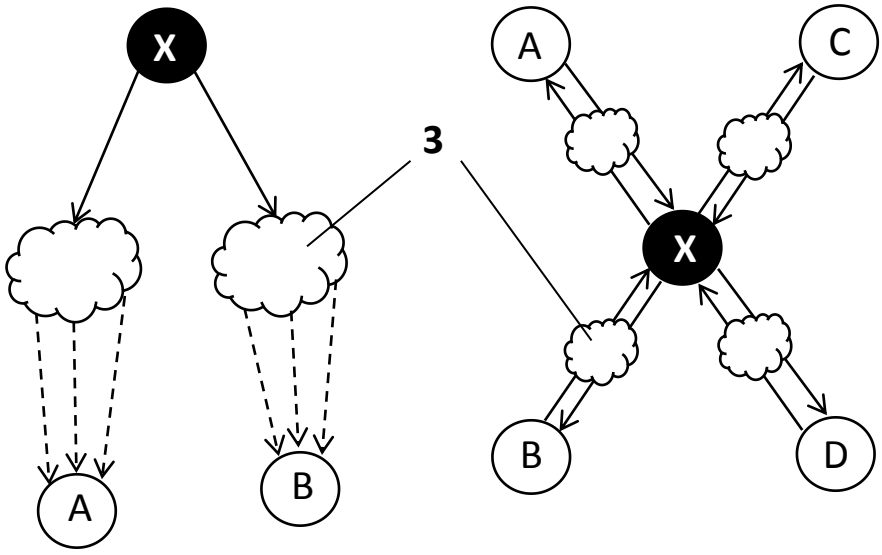


图 5 柔网关 X 与用户 ABCD 间建立的柔支付通道

要先建立有柔支付通道，才能进行柔支付，而若任意两人柔支付都先建立一下通道会很复杂不便。因此有个特殊的柔支付节点，称为柔网关节点，他们同时会和很多用户节点之间建立柔支付通道。

如图 3 所示意例子，若 A、B、C、D 四个用户都与柔网关 X 建立了双向柔支付通道，那么可以通过柔网关的中转可以轻易实现这四个用户间的任意收发柔支付。例如 A 要支付给 D，那么 A 先支付给 X，X 再支付给 D 即可。柔支付可以中间收取少量地手续费作为服务回报，也可以免费的提供中转服务来吸引更多用户来建立柔支付通道 ,毕竟柔支付通道内的柔支付本身的支

付成本就是几乎为零。柔网关连接的用户越多其价值越大。

交易平台，钱包平台，矿池，资讯社区平台甚至知名个人等等都可以成为广义的柔网关，只要能有足够多的人愿意与其建立柔支付通道。

2.3 柔节点间建立柔支付网络

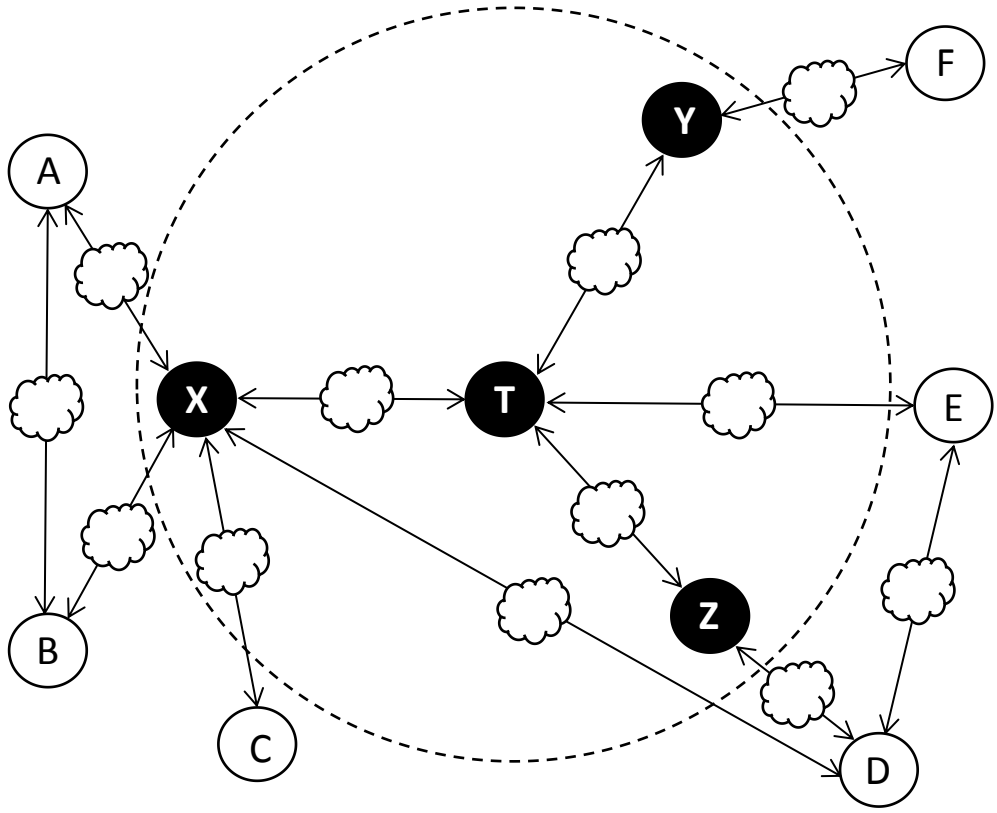


图 6 中转根节点 T 与各柔网关 XYZ 以及用户 ABCDEF 间建立柔支付网络

具体中转根节点、各柔网关及用户间建立起网络。各个柔网关及其用户就像是很多局域网，要实现全球的互联，需要一个中转根节点。采用树状拓扑模式。中转根节点是树根树干，而各柔网关是各个分支，而用户就是树叶。一般分三层即可，若系统过于庞大而中转根节点较吃力时，

可以考虑四层或更多层，即柔网关下面可分一些子柔网关。不过一般还是维持三层会更简洁高效些。这种构架下任意两人最多中间中转三次即可柔支付。例如图中 A 想柔支付付给 F，可以通过 A 付 X，X 付 T，T 付 Y，Y 付 F 实现。注意要减少最好杜绝柔网关之间相互连接，否则会路由情况增多而增加系统的复杂度和稀释中转根节点的地位，甚至演变成点对点的网状网络。

柔支付节点相互之间建立双向或者单向柔支付通道；

通过柔支付通道使节点之间建立连接，形成一定拓扑形状的柔支付网络。

各节点之间相互平等，任意节点之间都有可能连接，从而形成网状拓扑形状的高去中心化的柔支付网络。

节点分为中心节点和用户节点，所有用户节点与中心节点相连接，用户节点之间不连接，从而形成星型拓扑支付网络；

中心节点可以为一个或者多个，若为多个中心节点相互之间相互连接形成一个整体。

节点分为中转根节点，柔网关节点和用户节点；

中转根节点与柔网关节点，以中转根节点为中心星型拓扑连接，一般仅有一个，且在出现特殊情况时，可共识认可下将某个柔网关节点升级为中转根节点；

柔网关节点，有多个，与用户节点和中转根节点相链接，但各柔网关节点相互之间一般不连接。

用户节点，一般可与柔网关节点连接，也可以直接和中转根节点连接，用户节点相互之间也可以直接连接；

从而形成分层树状拓扑的柔支付网络。

柔支付通道是较简单的技术，将现有技术的进行组合，于是早期直接公开给大家使用。然而单纯柔支付通道是较难有较好应用场景的。这便像众多闪电节点建很多闪电通道构成闪电网络一样，由很多柔支付通道构建形成了 RN 柔支付网络。这个由通道形成 RN 网络的技术是较核心

技术。为了保护知识产权避免山寨，我们于 2018 年 3 月递交了发明专利申请《多重签名的柔性区块链支付方法、装置及电子设备》专利申请号 CN201810260125.6。即将简单的柔支付通道，扩展到柔支付的网络生态。

中华人民共和国国家知识产权局

100084

北京市海淀区清华园清华大学思源院商业楼 301 室
北京清亦华知识产权代理事务所（普通合伙） 张润(010-82886568)

发文日：
2018 年 03 月 27 日

申请号或专利号：201810260125.6　　发文序号：2018032702209010

专 利 申 请 受 理 通 知 书

根据专利法第 28 条及其实施细则第 38 条、第 39 条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日、申请人和发明创造名称通知如下：

申请号：201810260125.6
申请日：2018 年 03 月 27 日
申请人：马龙
发明创造名称：多重签名的柔性区块链支付方法、装置及电子设备

经核实，国家知识产权局确认收到文件如下：
说明书摘要 每份页数:1 页 文件份数:1 份
权利要求书 每份页数:2 页 文件份数:1 份 权利要求项数： 10 项
说明书 每份页数:11 页 文件份数:1 份
发明专利请求书 每份页数:5 页 文件份数:1 份
说明书附图 每份页数:3 页 文件份数:1 份
专利代理委托书 每份页数:2 页 文件份数:1 份

提示：
1. 申请人收到专利申请受理通知书之后，认为其记载的内容与申请人所提交的相应内容不一致时，可以向国家知识产权局请求更正。
2. 申请人收到专利申请受理通知书之后，再向国家知识产权局办理各种手续时，均应当准确、清晰地写明申请号。
3. 国家知识产权局收到向外国申请专利保密审查请求书后，依据专利法实施细则第 9 条予以审查。

审 查 员：自动受理　　审查部门：

200101
2010.4

图 7　RN 柔支付网络专利申请受理通知书

因为有专利的保护，因此我们柔支付网络的搭建技术，不用作为技术秘密，而也可以直接的向币圈公开细节。进而在技术公开透明下，可以很好的一起参与到 RN 柔支付网络中，专利并不会限制加入柔支付网络生态的柔网关们，而是保护它们。避免的仅仅只是在明确原理后搭建的自己作为根网关的山寨柔支付网络。若不能打通连接成一个大的统一的柔支付网络，将不利于发挥网络优势。

另外柔支付网络技术还在较早期，也会是有很多新的细节技术在不断的优化完善中，因此维护网络的统一避免分裂非常关键。专利保护知识产权的目的仅在于避免分裂和山寨，并不会限制，反而鼓励和保护越来越多的项目加入到柔支付网络生态中。

上图示意图可以看到 RN 柔支付网络的结构，虽然不是中心化的星型网络构架，但也和完全点对点的比特币主链网络 LN 闪电网络等不同，RN 采用了树状网络的构架。分为根网关节点，

柔网关节点和用户节点三层，就像一棵大树的树根，枝干和树叶。各类节点有自己的定位，有机地构造成一个高效地柔支付网络系统 ,从而可以都接入 RN 网络的陌生人之间可以高效地进行柔支付。极大地扩展了柔支付的应用场景。

用户节点，即 RN 柔支付网络的用户，可以是个人，也可以是商家或应用。其目的是进行高效快速且近乎 0 手续费的柔支付各种加密数字货币。其有两种选择，一是和柔网关建立柔通道从而接入柔支付网络，另外一个是直接和根网关建议柔支付通道。

柔网关节点，是 RN 闪电网络的重要构架和贡献者，往往需要服务器或者硬件矿机来成为可以提供用户节点接入的特殊节点。当然对于柔网关节点的贡献，RN 柔支付网络系统会回报一些币，就像比特币矿机维护比特币网络获得比特币一样。

根网关节点，理论上是从众多的柔网关节点中选出的特殊柔网关节点，若根网关节点意外断网崩溃，有必要下可以很快选出另外一个柔网关节点作为新的根网关节点，从而实现高度的去中心化。其不仅仅处理用户节点的柔通道建立和柔支付，更加重要的是与各个柔网关节点建立通道，处理跨网关的柔支付请求。将来柔支付网络越来越庞大后，其可能减少与用户节点的直接建立通道，转向专注于联系各各柔网关，处理跨网关柔支付。

注意这个树状拓扑的 RN 柔支付网络是禁止柔网关节点之间建立柔支付通道进行直接跨网关结算的。若允许一些柔网关将可以不再与根网关建立通道，最后整个网络变成错综复杂的 P2P 点对点网络，和 LN 闪电网络相近了，而进而带来的是支付时路由的复杂和低效，而将失去柔支付网络现有的最多仅三个中间节点，路由清晰明确的优势。

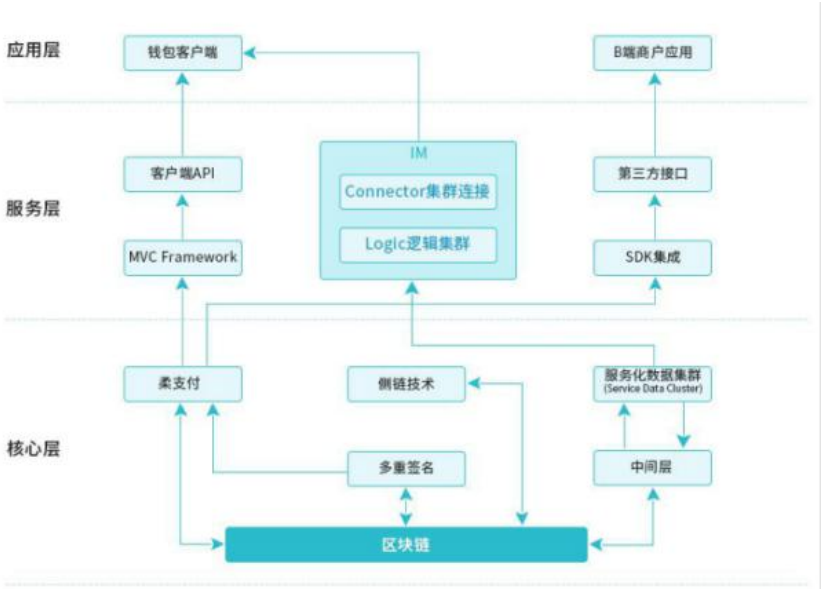
注意虽然根据底层的原理，柔支付靠多重签名保证自己的币量绝对安全。但是为了确保柔支付的支付成功率和确保树状拓扑的落地，以及跨网关结算的更高效进行，需要对柔支付的柔网关节点有一定的门槛要求，即抵押一个币到柔支付根网关，作为柔网关的信用担保。这也是用途之一。随着将来 RN 用户增多，进而柔网关节点增多，需要的总的柔网关担保币也就越来越多，

进而形成需求。最后整个 RN 网络的各种应用收益，也会与柔支付币的持有者进行利润分红，来回馈柔支付网络支持者和币持有者。

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。

3.柔支付生态整体分层架构

XCoinPay 的整体架构分为三层：核心层、服务层、应用层。架构图如下：



3.1 区块链核心层

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。

最核心层，本质上是各种区块链，对这些区块链的二层网络应用，基于区块链自身的多重签名和时间戳交易的应用。核心安全度等同于此区块链本身的安全度。

核心层的主要任务是保护用户的区块链币资产安全，以及能通过柔网关通道技术实现对数字资产的签名刷新重分配。

3.2 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。

服务层主要是的应用场景，包括各接口的接入，各柔网关的担保费用，以及各种集成框架模块的使用，提供一键建立柔支付通道服务等。

服务层主要是为简化柔支付应用直接使用核心层的使用门槛，能以更加方便易用的方式向应用层提供服务。以及整合各种资源来构建柔支付网络生态。

3.3 RAPP 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、竞拍、币找回、红包、交易、第三方应用对接 SDK 写入交易等。

应用层有大量的 RAPP。可以由 DYX 来提供具体的应用服务支持。详细可以见下面章节对 DYX 应用代币的主要应用描述。

应用层面向的是各种各样的可以向用户提供各种具体服务的应用。也欢迎各种现有的 DAPP 甚至常规 APP，及其开发者们入驻加入柔支付网络生态，成为 RAPP。越来越多的 RAPP 将成为柔支付网络生态的重要价值来源。

4.柔支付网络 DYX 代币应用

为了在生态中引入柔支付网络(RouPay Network)RAPP 应用激励，XCoinPay 将在柔支付网络(RouPay Network)的基础上发行二层代币 DYX，DYX 主要在柔支付网络(RouPay Network)中用作节点激励、跨网关支付等作用，DYX 作为与柔支付网络深度结合的应用层的原生代币，有众多具体的应用相结合的应用场景，下面只是列举其中的一部分有可能的应用场景，随着柔支付网络的发展会越来越多用途的，DYX 在柔支付网络生态中的应用大致有以下几点：

4.1 在 RAPP 调用消耗 RN 资源的操作中消耗

RN 柔支付网络，会在核心层和服务层为 RAPP 们提供丰富的接口服务，虽然理论上是可以免费使用的。但是若免费，将来有大量 RAPP，甚至有些 RAPP 在大量刷量下，对柔网关提供太高的性能要求，而不利于柔网关的增多和去中心化度提升。

因此在需要消耗柔网关资源的 RAPP 操作中，将消耗 DYX。即 DAPP 的开发运营者需要储备些 DYX，部分作为给柔网关们类似于手续费地感谢打赏。部分可直接销毁消耗掉，以减少流通中的 DYX 币量。

4.2 开启建立 RAPP 柔支付应用的担保

为了提升 RAPP 的整体质量，以及减少骗局应用增加用户体验和服务质量。因此对新接入柔支付网络的 RAPP ,会以代币 DYX 的形式冻结一定的担保币。这些币会推出流通领域 ,当 RAPP 违规时，有可能有扣除部分 DYX 以补偿可能的用户损失。

当然担保币量的多少，和想接入柔支付网络是多种因素决定的。首先是 RAPP 应用的性质，

若仅仅只是游戏类，并没有太高额的币，那可以少冻结些。而涉及资产类的 RAPP 如丢失私钥找回区块链币资产应用，可能就要多冻结些。另外是 RAPP 本身运营主体的实力和历史信用表现，若表现好和有实力的应用，完全可以少冻结些。这个冻结币量多少是协商决定且公开的，有些 RAPP 应用，为了表达自已的信誉，也可以主动要求多冻结些币。最后当应用下架时，是可以退还解冻这些冻结币的。在 RAPP 应用需资金周转时，也可以考虑申请适度降低冻结币量。

4.3 新币种接入 RN 柔支付网络的币投票

只要币种直接支持或能通合约间接支持多重签名技术和时间戳交易 ,那么即可接入柔支付网络，门槛很低。主流的币种几乎都可以接入柔支付网络(RouPay Network)。也会主动的将重要的币种直接接入柔支付网络，但为避免资源的浪费，其它币种需要经过投票。

投票币种可以用 DYX，任何人都可以发起任何币公开的投票，即将 DYX 发到币种对应的黑洞地址，永久销毁烧掉，烧地越多相当于投票越多。而柔支付网络(RouPay Network)会不定期地将 DYX 销毁燃烧投票多的币种加入柔支付网络。预计未来将可能会是 DYX 的重要应用之处。

4.4 在签名和校验签名等消耗资源操作中燃烧

类似于 ETH 在以太合约中运行合约时的燃烧是近似的，不同的是 ETH 是以手续费的形式又给矿工了并没有真正的烧掉。而 DYX 会在各个需要消耗资源的柔支付操作中，直接将 DYX 完全燃烧销毁。对单个操作量很少，但是若柔支付量很多时将会是很大的一个燃烧量。

4.5 建立柔支付通道的建立费用

用户想接入柔支付网络实现几乎所有币都能实现几乎零手续费的秒速确认，一般来说，是需要有一个主链上币发到多重签名地址的交易的，而此交易需要此币种的交易手续费，而各币种会有高有低不一样，且收多种币会很难以计算，因此统一的收等价值的 DYX。即首次接入柔支付网络的新用户，以及柔支付通道到期或通道额度用完需要新开启通道，都需要 DYX 来应用。这个视申请开通的币种及此币当前繁忙程度及是否需要紧急建立等等多因素决定的，有时会需要较多的 DYX，且部分是给网关节点作为收入，部分是完全燃烧掉。

5.DYX 发布与分配细则

DYX 是一种基于 Ethereum 实现的合约代币，DYX 总共发行 1000 亿，永不增发，DYX 合约地址：0x042f972ac93404f0fcbe4e3a0729f0b395232106

DYX 分配计划如下：

1、20%将用于 xcoinpay.io 的打折模式中，打折模式信息请登录官网 XCoinPay.io 查看

2、20%归属创始团队和开发团队所有，作为团队的发展经费资金

3、10%用作资源方合作资金，用作重大资源方合作

4、10%用作接受机构投资的份额资金

4、30%由 XCoinPay 基金会代持，作为 XCoinPay 的基金会发展备用金，用于后续基金会的建设备用金

5、 5%用作预备空投资金，后期预备空投给活跃地址

6、 5%用作市场发展激励资金，用于 XCoinPay 的市场的推广运营，例如空投奖励、群主激励等

比例	分配方案	备注
20%	用作打折抢购模式中	打折模式信息请登录官网 XCoinPay.io 查看
20%	创始团队和开发团队所有	作为团队的发展经费资金
10%	资源方合作资金	用作重大资源方合作
10%	机构进入资金	预留接受机构投资的份额资金
30%	基金会代持，作为 XCoinPay 的基金会发展备用金	用于后续基金会的建设备用金
5%	预备空投资金	后期预备空投给活跃地址
5%	市场发展激励资金	用于 XCoinPay 的市场的推广运营，例如空投奖励、群主激励等

6.XCoinPay 荣誉—中国区块链风云榜项目奖

7.XCoinPay 团队持有申报的两项区块链专利

目前 XCoinPay 团队持有申报区块链专利两项，公开资料如下：

专利名称	申请时间	原文链接	号码信息
一种多重签名的柔性区块链支付方法及网络系统	2018.03.05	http://www.xcoinpay.io/public/file/patent.pdf http://roupay.com/CN201810260125.6.pdf	清亦华卷号：PIDE3181370 分类号：H04L29
彩色区块链的管理方法及管理系统	2019.09.29	http://www.xcoinpay.io/public/file/administration.pdf	申请公布号：CN106529924A

7.1 申报区块链专利 1：一种多重签名的柔性区块链支付方法及网络系统

简介：本申请提供一种多重签名的柔性区块链支付方法及网络系统，通过发送方多重签名地址中发送有延迟返回的待分配数字资产形成柔支付通道，接受方可以验证签名是否正确来通过通道确认收到柔支付，并将这些通道有机的整合建立成柔支付网络，从而实现任意两陌生人间不需直接建立柔支付通道，解决了现有的区块链支付效率低、灵活性差，且十分繁琐，成本高的问题 。

PIDE3181370

中华人民共和国国家知识产权局

100084

北京市海淀区清华园清华大学照澜院商业楼301室
北京清亦华知识产权代理事务所（普通合伙） 张润(010-82886568)

发文日：

2018年03月27日

申请号或专利号：201810260125.6　　发文序号：2018032702209010

专利申请受理通知书

根据专利法第28条及其实施细则第38条、第39条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日、申请人和发明创造名称通知如下：

申请号：201810260125.6
申请日：2018年03月27日
申请人：马龙
发明创造名称：多重签名的柔性区块链支付方法、装置及电子设备

经核实，国家知识产权局确认收到文件如下：
说明书摘要 每份页数:1页 文件份数:1份
权利要求书 每份页数:2页 文件份数:1份 权利要求项数： 10项
说明书 每份页数:11页 文件份数:1份
发明专利请求书 每份页数:5页 文件份数:1份
说明书附图 每份页数:3页 文件份数:1份
专利代理委托书 每份页数:2页 文件份数:1份

提示：

1. 申请人收到专利申请受理通知书之后，认为其记载的内容与申请人所提交的相应内容不一致时，可以向国家知识产权局请求更正。
2. 申请人收到专利申请受理通知书之后，再向国家知识产权局办理各种手续时，均应当准确、清晰地写明申请号。
3. 国家知识产权局收到向外国申请专利保密审查请求书后，依据专利法实施细则第9条予以审查。

审 查 员：自动受理　　审查部门：专利局初审及流程管理部

200101
2010.4

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路6号 国家知识产权局受理处收
电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

(15)

	检索过程和检索结果	
贵司卷号：ML-2018-001	清亦华卷号：PIDE3181370	
专利名称	一种多重签名的柔性区块链支付方法及网络系统	
发明点及解决的技术问题简述	本申请提供一种多重签名的柔性区块链支付方法及网络系统，通过发送方多重签名地址中发送有延迟返回的待分配数字资产形成柔支付通道，接受方可以验证签名是否正确来通过通道确认收到柔支付，并将这些通道有机的整合建立成柔支付网络，从而实现任意两陌生人间不需直接建立柔支付通道，解决了现有的区块链支付效率低、灵活性差，且十分繁琐，成本高的问题 。	
分类号	H04L29/	
关键词	多重签名　　区块链支付　　区块链	
检索式及文献数量	多重签名　AND 区块链支付	0
	多重签名 AND 区块链	4
	区块链支付 AND 区块链	9
接近的对比文献列表	对比文件 1：CN 107038578 A - 一种基于区块链的数据交易平台中多重签名交易信息处理方法 对比文件 2：CN 107682331 A - 一种基于区块链的物联网身份认证方法 对比文件 3：CN 107370606 A - 一种基于区块链的微博多重签名方法	

说明书摘要

本发明公开了一种多重签名的柔性区块链支付方法、装置及电子设备，其中，方法包括：将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道；获取发送方分配的至少一个分配信息，并根据至少一个分配信息生成对应的至少一个重分配柔支付签名；根据至少一个重分配柔支付签名将待分配数字资产柔支付至对应账户。该方法可以通过将待分配数字资产发送到区块链的多重签名地址上，并通过建立柔支付网络，而实现双方不需要直接建立柔支付通道便可以实现柔支付，不但有效保证支付的可靠性和安全性，而且具有支付成本较低、确认时间短、灵活性较高等优点，有效提升用户使用体验，且简单易实现。

权利要求书

1、一种多重签名的柔性区块链支付方法，其特征在于，包括以下步骤：

将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道；

获取所述发送方分配的至少一个分配信息，并根据所述至少一个分配信息生成对应的至少一个重分配柔支付签名；以及

根据所述至少一个重分配柔支付签名将所述待分配数字资产柔支付至对应账户。

2、根据权利要求 1 所述的多重签名的柔性区块链支付方法，其特征在于，还包括：

在将发送方发送的待分配数字资产存储于区块链的多重签名地址中之前，获取所述接收方签名的延时转回签名，并根据所述接收方签名的延时转回签名关闭所述柔支付通道，以将所述多重签名地址中的部分或全部待分配数字资产在预设时间戳或预设区块高度后转回所述发送方；或

根据所述接收方签名的分配信息发送的区块链广播关闭所述柔支付通道，按所述分配信息进行分配所述待分配数字资产。

3、根据权利要求 1 所述的多重签名的柔性区块链支付方法，其特征在于，所述区块链的多重签名地址为 2of2 模式多重签名地址或者 2of3 模式多重签名地址，以在所述发送方和所述接受方均签名，或者所述发送方、所述接收方和第三方中任意两方签名后，支付所述待分配数字资产。

4、根据权利要求 2 所述的多重签名的柔性区块链支付方法，其特征在于，还包括：

7.2 申报区块链专利 2：一种彩色区块链的管理方法及管理系统

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。

(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)

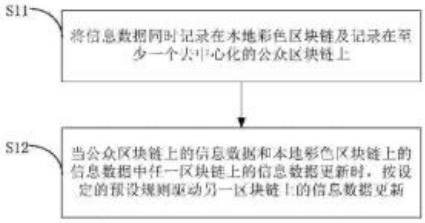
权利要求书1页 说明书7页 附图3页

(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。



CN 106529924 A

1.一种彩色区块链的管理方法，其特征在于，包括以下步骤：

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；

当所述公众区块链上的所述信息数据和所述本地彩色区块链上的所述信息数据中任一区块链上的所述信息数据更新时，按设定的预设规则驱动另一区块链上的所述信息数据更新。

2.根据权利要求1所述的彩色区块链的管理方法，其特征在于：所述公众区块链的数量为单个，所述公众区块链为比特币区块链。

3.根据权利要求1所述的彩色区块链的管理方法，其特征在于：所述公众区块链的数量为单个，所述公众区块链为竞争币区块链。

4.根据权利要求1所述的彩色区块链的管理方法，其特征在于：所述公众区块链有两个或多个链，所述预设规则为所述两个或多个链均相应地发生所述信息数据改变更新时，驱动所述本地彩色区块链上的所述信息数据进行更新。

5.根据权利要求1所述的彩色区块链的管理方法，其特征在于：所述公众区块链有两个或多个链，所述预设规则为所述两个或多个链中的任意一个或几个链的所述信息数据改变更新时，就会驱动所述本地彩色区块链上的所述信息数据进行更新。

6.根据权利要求1-5任一项所述的彩色区块链的管理方法，其特征在于：所述本地彩色区块链的具体记录所述信息数据的方式是用私有区块链的形式进行记录。

7.根据权利要求1-5任一项所述的彩色区块链的管理方法，其特征在于：所述本地彩色区块链的具体记录所述信息数据的方式是用服务器数据库的形式进行记录。

8.根据权利要求1-5任一项所述的彩色区块链的管理方法，其特征在于：还包括步骤：

将由所述本地彩色区块链和所述公众区块链共同记录的所述信息数据，按照信息的类别进行分类标识。

9.根据权利要求8所述的彩色区块链的管理方法，其特征在于：所述信息的分类标识的具体方式是通过指定不同的颜色来进行区分标识，以序号、颜色名称、颜色编码、公众区块链名称和/或公众区块链数量的组合来区分命名信息记录系统。

10.一种彩色区块链的管理系统，其特征在于，包括：

数据记录系统，用于记录彩色区块链的信息数据和记录公众区块链的信息数据，所述彩色区块链的信息数据同时记录在所述公众区块链上，所述公众区块链为去中心化的区块链；

管理发行平台，用于管理和发行所述彩色区块链，当所述公众区块链上的所述信息数据和所述本地彩色区块链上的所述信息数据中任一区块链上的所述信息数据更新时，按设定的预设规则驱动另一区块链上的所述信息数据更新；及

资产流通平台，用于提供彩色区块链币的交易流通，当所述交易为冲提币时，所述资产流通平台与所述彩色区块链对接以更新所述彩色区块链的所述信息数据。

8.XCoinPay 团队所编写的书籍—如何投资数字货币

8.1 主编 —XCoinPay 团队顾问周朝辉

8.2 副主编—XCoinPay 团队 CTO 马龙

9.团队与顾问

团队核心成员

赵世达　CEO

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。

团队顾问

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

FAQ

什么是 XCoinPay？

答：XCoinPay 是一个区块链底层金融平台，内置的柔支付网络（RouPay Network）能实现去中心化的链下秒速转移区块链资产

柔支付网络（RouPay Network）是 XCoinPay 的内置的区块链底层支付网络，柔支付网络（RouPay Network）是一个链下支付系统，柔支付网络（RouPay Network）使用链下清算的方式实现高并发，柔支付网络（RouPay Network）是新一代的链下清算平台，同样支持多币种，使用柔支付网络（RouPay Network）可实现秒速、零手续发送和接收区块链资产，而基于柔支付网络（RouPay Network）这个区块链底层支付网络，可以衍生出多种区块链商业解决方案。

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：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。

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。

柔支付另外还能解决哪些问题？

答：柔支付网络将是扩容之争的良好的解决方案

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）。

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

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

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。

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。

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。

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。

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》