XCoinPay 白皮书
XCoinPay—区块链支付领域的 PayPal！
XCoinPay.io
（v1.7 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）和 MHT 技术（Matching hedge Technology 匹配对冲技术）等都是由 XCoinPay 团队自主研发的创新功能。

柔支付技术（RouPay）是由 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）。

柔支付网络的优势在于：

1、底层技术成熟：柔支付网络（RouPay Network）的底层技术是基于成熟的多重签名技术、时间戳交易技术和交易冷签名技术等技术建立起来的柔支付通道。

2、兼容性好：支持绝大部分主流币种，甚至像狗狗币这种已经较久没有核心维护更新的币种，只要是数字货币，一般均可以支持实施柔支付网络（RouPay Network），且可以实现跨链跨币种支付，不需要核心钱包做任何调整。

3、灵活应用：可将柔支付网络（RouPay Network）技术集成到目标币的核心钱包中。

4、安全且简洁：柔支付网络（RouPay Network）相比闪电网络来说，使用的底层技术已经大规模应用，足够安全，且柔支付网络（RouPay Network）的设计简洁，应用落地性高。

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

一、XCoinPay 简介

XCoinPay 致力于打造区块链支付领域的 PayPal，XCoinPay 开发团队自主研发了包含柔支付技术（RouPay）在内的诸多核心技术，显著地解决了现有区块链系统的传输低效问题，基于自主研发的柔支付技术（RouPay）和 MHT 技术（Matching hedge Technology 匹配对冲技术）等多种技术，XCoinPay 打造了全新的区块链资产支付网络—柔支付网络（RouPay Network），使用柔支付网络（RouPay Network） 可以实现区块链资产的零成本极速支付，同时 XCoinPay 将各类数字资产的区块链支付通道集合成 sdk 接口，打造各种应用于区块链支付场景的开放工具，提供给商家和企业，最终打造基于区块链金融的开放生态系统。

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）和 MHT 技术（Matching hedge Technology 匹配对冲技术）等关键功能都是由 XCoinPay 自主研发的创新功能。

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且秒速确认，在速度、安全性和隐私性方面，足以媲美闪电网络（Lightning Network）。

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，前期 XCoinPay 私募了大概 3659 个 ETH 以及数百万人民币，投资者包含业内知名人士和一家私募投资机构。

XCoinPay 隶属于香港 XCoinPay 公司（HONGKONG XCOINPAY TECHNOLOGY LIMITED），XCoinPay 公司是一家成立于香港的金融科技公司，香港对区块链行业有着积极的政策支持，XCoinPay 公司立足于世界金融中心香港，使用区块链技术服务于全世界用户。

二、XCoinPay 概述

1. XCoinPay 理念：致力于打造开放、全面的区块链支付生态系统

XCoinPay 致力于打造开放、全面的区块链支付生态系统，XCoinPay 面对商家用户和个人用户提供了不同的服务及产品，面对商家用户，XCoinPay 提供了 XCoinPay 商用平台（Commercial platform），可以实现一键接入 XCoinPay 支付以及跨境支付解决方案等。面对个人用户，XCoinPay 提供了移动 DAPP 钱包、基于 RSA 算法加密的通讯模块、场外担保交易、极速交易等为加密数字货币用户定制的诸多功能。

2. XCoinPay 自主研发了柔支付技术（RouPay），可以实现零成本和极速转账

XCoinPay 自主研发了“柔支付技术（RouPay）”，柔支付技术（RouPay）使用了时间戳交易和 2-of-2 多重签名技术等多种成熟技术，使用柔支付技术（RouPay）可以实现即时支付，即时到账，并且零手续费，所以使用 XCoinPay 发送比特币（或者其它加密数字货币）可以极速到账且零手续费，给用户带来全新的支付体验，而且不同于中心化地数据库技术实现的链下钱包，柔支付技术是去中心化的，用户的资产完全掌握在用户自己手中，可以在区块链上进行查询通道，不会被平台动用，绝对安全。

和普通数字钱包高额的转账旷工费和极慢的转账时间相比，XCoinPay 通过自主研发的柔支付（rouPay），可以实现用户与用户之间的零手续费、秒级的数字资产转移，带来区块链支付 3.0 时代！

3. XCoinPay 使用了通用地址，一个通用地址可以接收和发送 95%的加密数字货币

通用地址的出现，可以帮用户免去管理多个币种地址的烦恼，就像拥有一个 paypal 账户，就可以收发全球 20 多种各国法币一样便捷。

通用地址由用户自定义，可以是某个主流数字资产的币地址，也可以是一个 ID 号、邮箱或者手机号，使用通用地址可以便捷的接收和发送以及维护管理自己的区块链资产。

4. XCoinPay 自主研发了 MHT 技术（Matching hedge Technology 匹配对冲技术），可以实现跨链交易。

XCoinPay 通过自主研发的 MHT 技术（Matching hedge Technology 匹配对冲技术），可以满足不同用户间在多种币种之间进行自由地相互转换和支付，甚至在能良好的配对对冲且都有建立柔支付通道下，可以实现秒速且零手续费的实现跨链交易。

本跨链协议实现的跨链是开源的公开地协议，用户之间只要遵守此协议，甚至不需经过 XCoinPay 平台即可实现，从而保证跨链能公开公正和足够地去中心化。

三、XcoinPay 核心技术

1. 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。

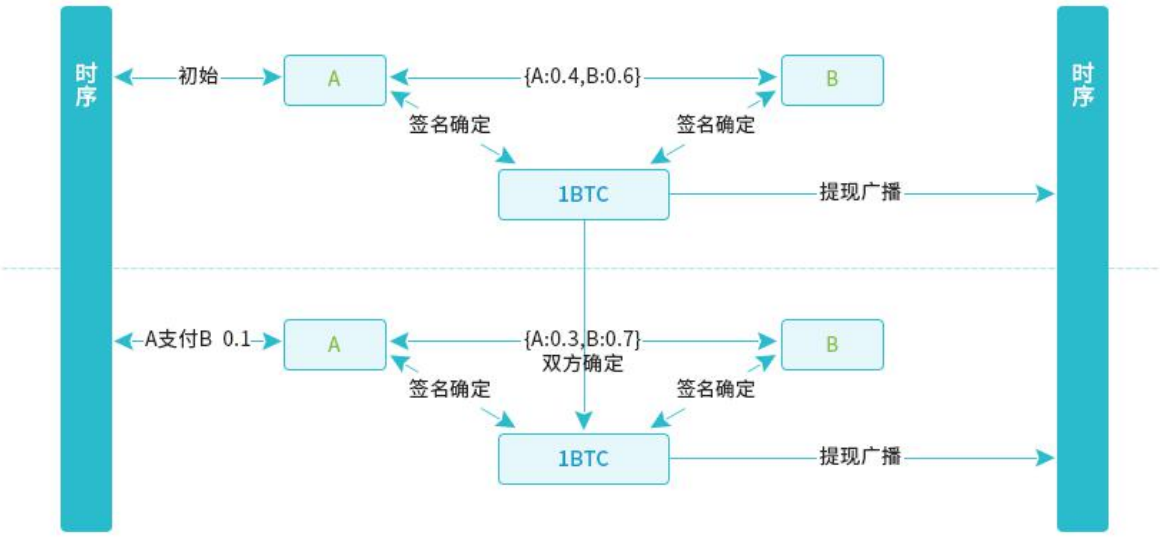
nLocktime, 也被称为 LockTime 或 lock_time, 通常被设置为 0，表示交易可随时发送到比特币网络。如果 nLocktime 的值在 1 到 5 亿之间，则表示需要区块高度大于或等于 nLocktime 的区块时才可以写入区块链。如果 nLocktime 的值超过 5 亿，则表示从 1970 年 01 月 01 日开始算，加上 nLocktime 秒之后的一个时间点，即 Unix 时间戳，例如 2017 年 1 月 1 日是 1483200000，若早于那个时间点，则该交易不会被发送到比特币网路。另外注意 sequence 字段，不能为 INT32 最大值（0xffffffff），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

若 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 0.05 BTC，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

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。

2.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 版本的 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

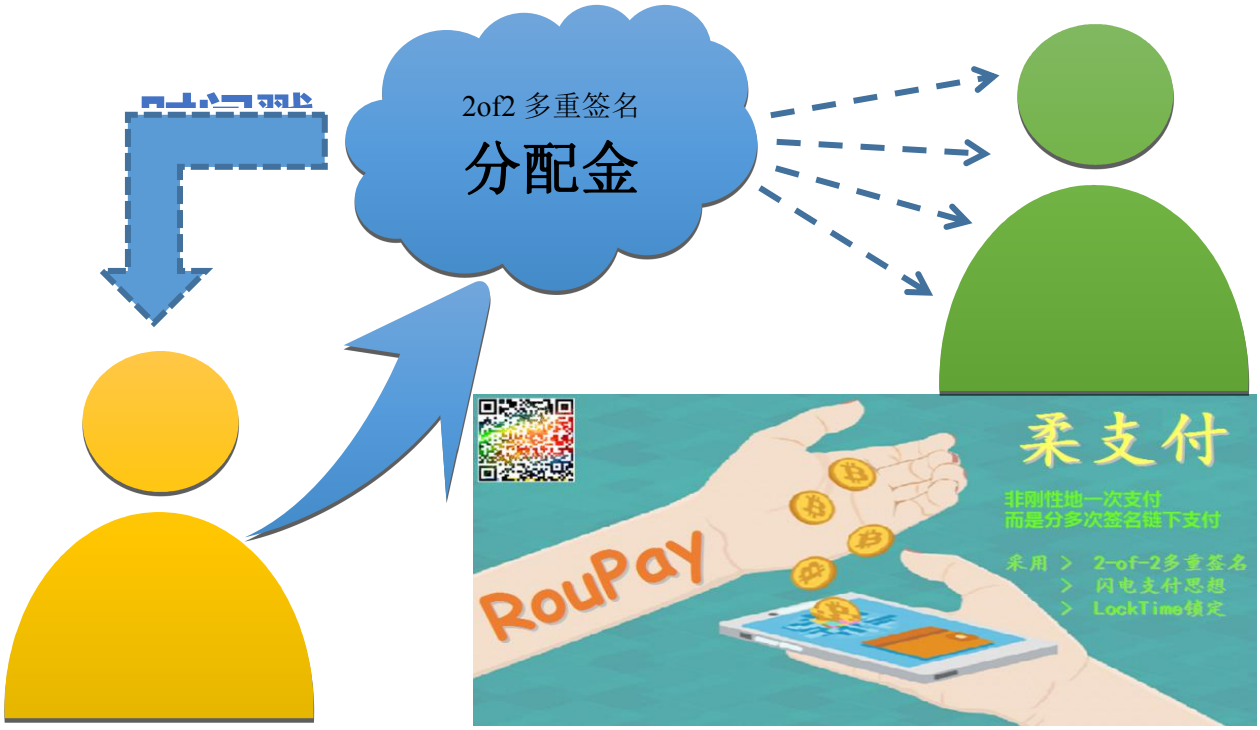
这个分配金是实现支付通道的关键。具体是采用上面提到的多重签名。具体是生成 2-of-2 多重签名，简单说就是两地址之间达成共识一致都签名时才能交易。参数 M 设为 2，而公钥数组中填写两个公钥。双方达成一致都签名同意时才能动这个 2-of-2 多重签名合成地址里的分配金。

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。

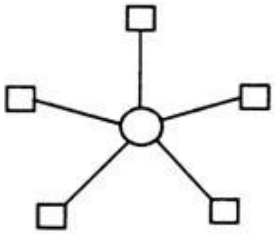
2.4 柔支付通道实现双向及跨链

这 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。

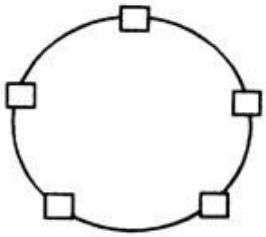
因为只要支持有多重签名，有时间戳交易即可实现柔支付通道，因此可以 A 到 B 是比特币柔支付通道，而 B 到 A 是狗狗币柔支付通道。于是便相当于实现了跨链和安全地币币交易。

2.5 分层树形拓扑的柔支付网络

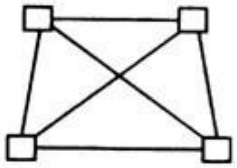
网络拓扑方式，第三方支付会是（a）星形，而比特币的点对点是图（c）网状态。闪电网络估计早期可能椒（b）环形已行程链六，而我们柔支付网裸将会近似于树形



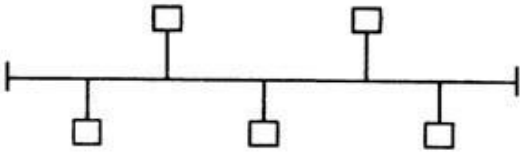
（a）星形



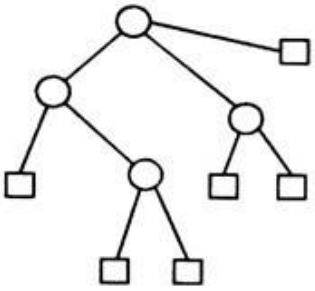
（b）环形



（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。

2.8 使用使用 MHT 技术（Matching hedge Technology 匹配对冲技术）可以实现跨链交易

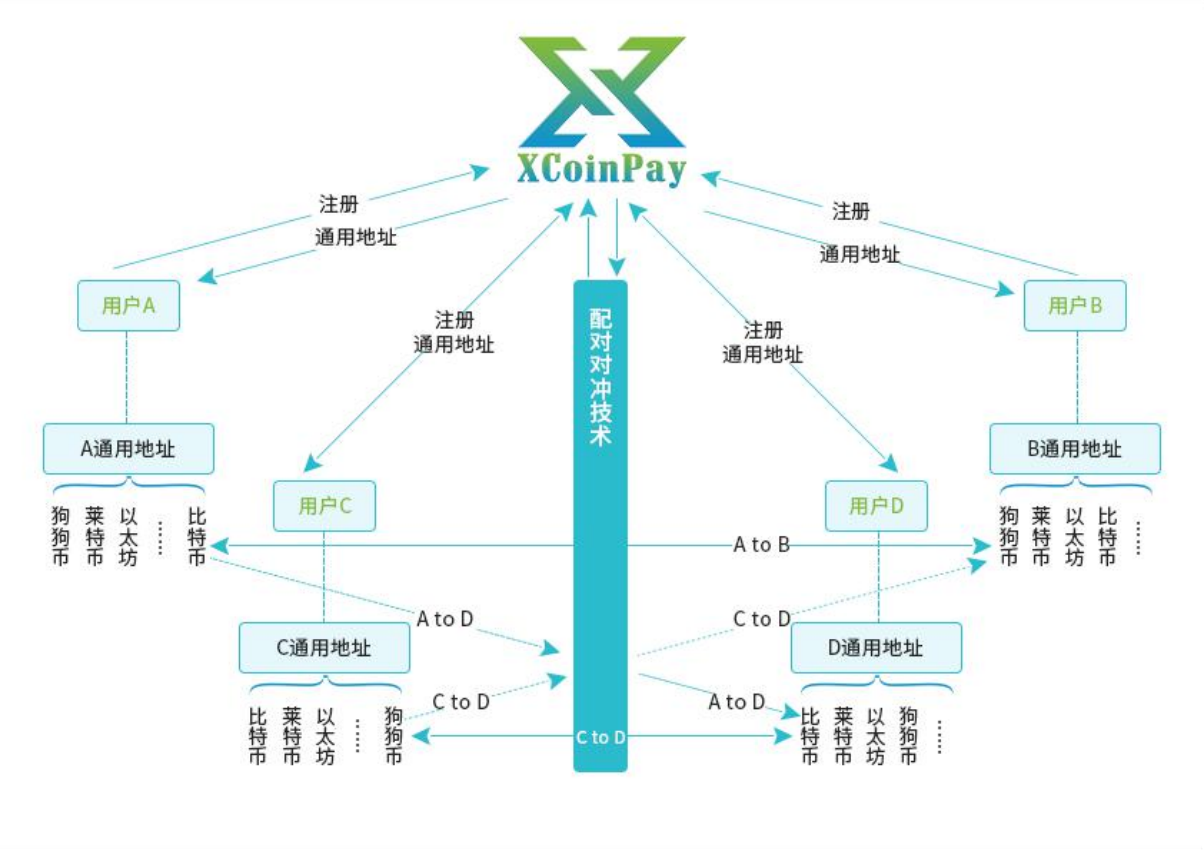
XCoinPay 钱包客户端连接用户与柔支付网络（RouPay Network），柔支付网络（RouPay Network） 作为中间层链接各个用户。

具体案例：以狗狗币与比特币跨链交易为例，具体流程如下：

I 用户经过通用地址技术获取自己在柔支付网络（RouPay Network） 的通用地址，狗狗币与比特币地址是一一对应的。

II 单用户情境下，A 用狗狗币付 B 的 btc，XCoinPay 锚定最新交易数据，在 XCoinPay 上通过构建柔支付通道，多重签名技术，完成交易，并分别广播交易到对应的区块链系统。流程图如下图所示：

III 多用户情景下，采用配对对冲技术，A 用 btc 付 B 的狗狗币，同时可能有人 C 用 doge 付 D 的比特币。因此可以匹配对冲过去，A 付 D，C 付 B。



3. 通用地址：一个通用地址可以接收和发送 95%的加密数字货币

3.1 传统地址生成原理

一般区块链的地址生成需要经历如下过程：

I 随机选取一个 32 字节的数作为私钥，该数介于 1～0xFFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4141 之间

II 使用椭圆曲线加密算法计算私钥对应的非压缩公钥。

III 计算公钥的 SHA-256 哈希值，假定为 A

IV 计算 A 的 RIPEMD-160 哈希值，假定为 B

V 在 B 前加上地址版本号，结果值假定为 C

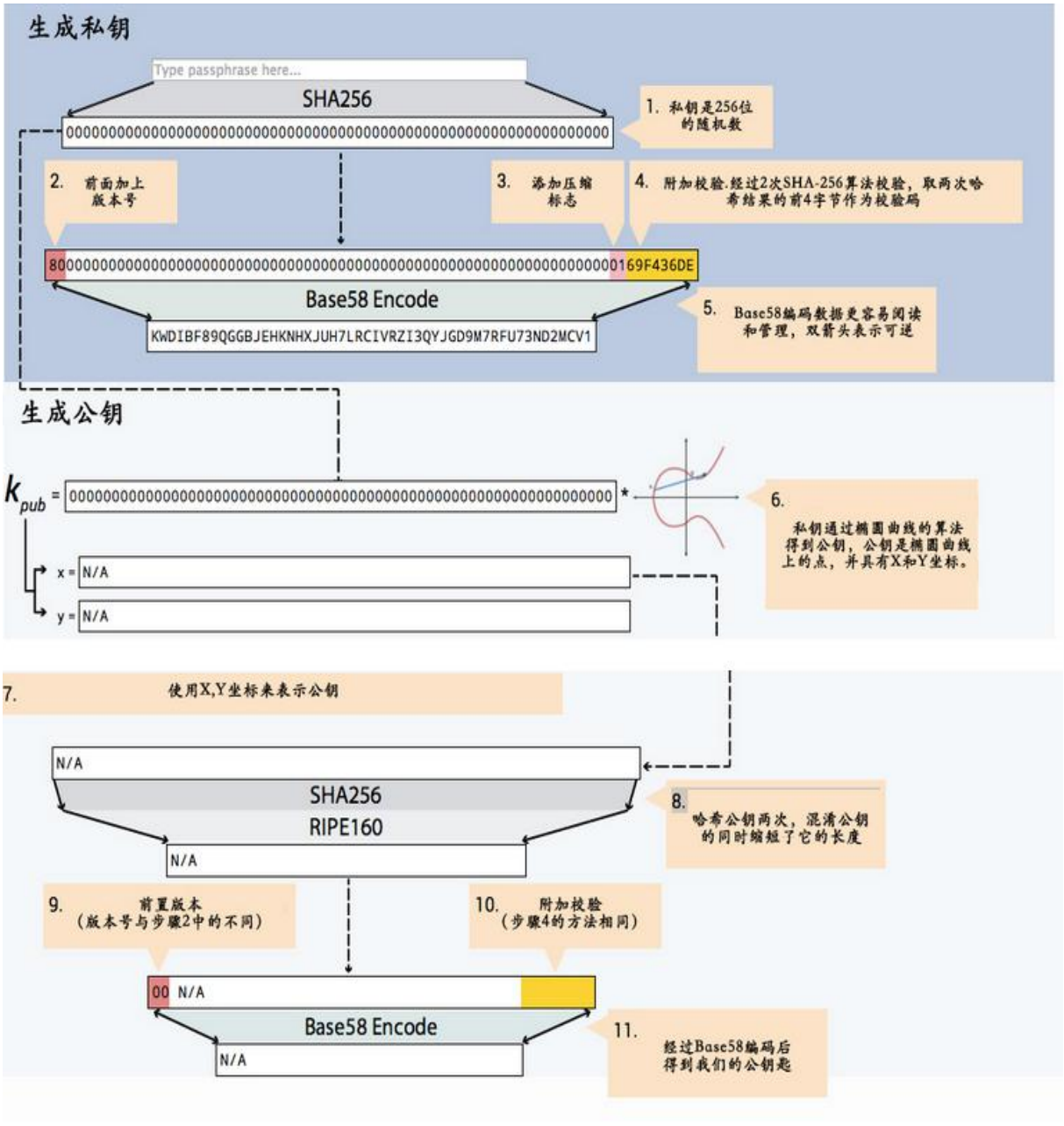
VI 计算 C 的 SHA-256 哈希值，假定为 D

VII 计算 D 的 SHA-256 哈希值，嘉定为 E

VIII 取 E 得前 4 个字节，把这 4 个字节加载 C 后面，作为检验，结果值嘉定为 F

IX 用 Base58 表示法变换一下 F，所得结果为 G,其中 G 就是最常见的比特币地址形态。

具体流程图如下：



3.2 具体案例：地址之间的相互转化

以太坊、基于以太坊的代币、比特币、以及市面上的主流币种的币地址的公钥，以及对其 SHA-256 和 RIPEMD-160 后得到的 40 十六进制的数都是一样的，各个币地址之

间的区别，是在如上图 2.1 中 9 序号所示的前置版本区域不同，比如：比特币该区域是 0x00，狗狗币是 0x1E，莱特币是 0x30。

明白这个流程后即可实现币地址之间的相互转化。以转为狗狗币为例，在流程 11 所示的任意其它币地址进行 Base58 的反向编码，去掉前两个十六进制的版本号和后 4 字节地校验码，按照需要转添加成对应币种的前置版本 0x1E 以及计算加上附加检验，再经过 Base58 Encode 即可得到对应的狗狗币地址。

3.3 通用地址的设计及应用

1）币地址 Base58 decode，解码成十六进制

2）去掉前两个十六进制版本号和后面校验

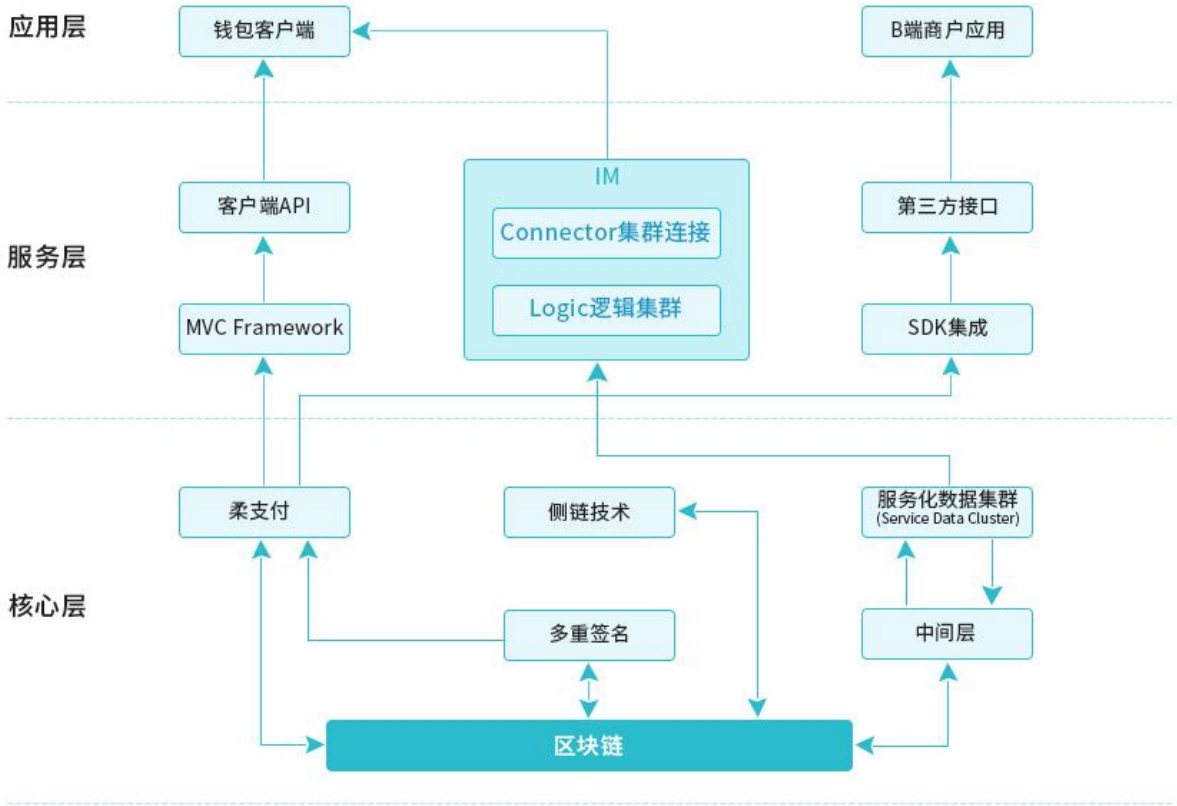
3）遍历各个版本号，使用 Base58Check 进行有校验的编码。

4）满足 Base58Check 的校验的币地址都是币系统支持的，可用来收币。

四、架构设计

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。

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：

2.1 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。

2.2 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。

五、XCoinPay 产品

1. XCoinPay 移动钱包，基于柔支付技术（RouPay）和通用地址等技术的颠覆性区块链钱包

面向个人用户，XCoinPay 提供 DAPP 钱包，XCoinPay 移动钱包专属为加密数字行业的用户而打造，基于柔支付技术（RouPay）和通用地址等技术打造的 XCoinPay 移动钱包，XCoinPay 移动钱包可实现以下诸多功能：

1.1 仅需要一个私钥和一个通用地址便可以方便管理区块链资产

1.2 收发比特币（或者其他加密数字货币）是秒速到账并且零手续费

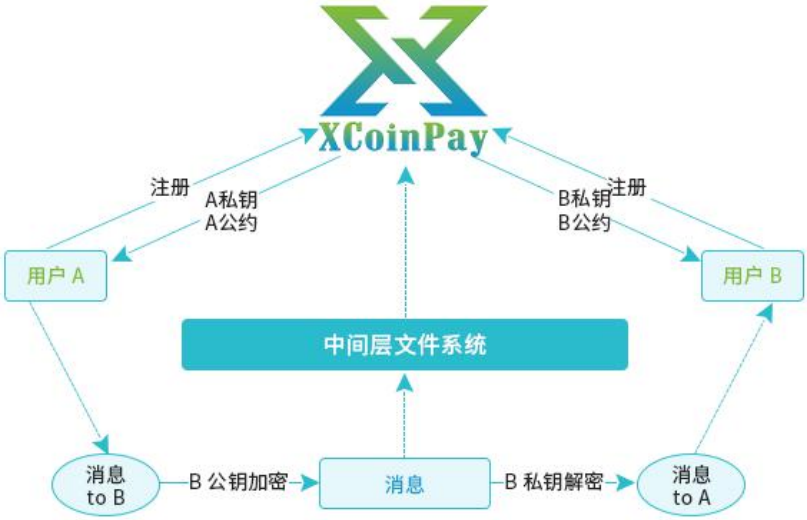
1.3 支持绝大部分主流加密数字货币

1.4 基于 RSA 算法加密的通讯模块，实现绝对私密的信息通讯

XCoinPay 手机钱包内置了加密通讯功能，基于 AES 算法加密，使用公私钥原理构建高效、可信且安全的加密通讯服务，所有你发送的信息都通过 AES 算法加密，保证了用户的数据和隐私，XCoinPay 内置的加密通讯功能将为加密数字用户提供绝对隐私的通讯服务。

普通的 IM 通讯都存在一个中心系统来管理用户账户，安全性问题依赖于可靠的或合格的证书。在这种模式下，如果证书颁发机构有一定的网络硬件位于用户服务器与目标服务器之间，将能随意对看似安全的通信进行有针对性的 man-in-the-middle 攻击。

解决方式：XCoinPay 在传统的服务端技术基础上，XcoinPay 会为用户生成一对公钥和私钥，其中公钥和私钥是由 RSA 算法生成的，并是唯一对应的，保证数据安全。通讯过程中消息从 A 传递到 B，A 的消息内容采用 B 的公钥进行加密，消息发送过去之后，B 用自己的唯一私钥解密消息内容，这样子整条消息在系统的各个环节中对除 B 以外的所有用户都是不可见的。消息模式如下图。



1.5 实现基于智能合约的场外担保交易

XCoinPay 手机钱包可实现基于智能合约的场外担保交易，即交易双方将币打到通道，由智能合约来担保并开启换币通道，其会 7*24 小时无休息地在线，且实现秒速的进行兑换，手续费也几乎为零。

1.6 可定制的智能合约小游戏

基于智能合约的可参数化定制的特点，让用户自定义填写参数，来实现合约游戏的建立，完全不需要有任何编程语言技术门槛，用户只需要填写参数即可，整个流程完全去中心化技术实施，而且使用智能合约能保证游戏的公平与公正，游戏最终结果可验证，技术流程图如下：

2. XCoinPay 商用平台（Commercial platform）：全渠道支持、全平台支持、全场景支持

面对商家用户，XCoinPay 提供 XCoinPay 商用平台（Commercial platform），XCoinPay 商用平台（Commercial platform）提供了传统支付级别的 SDK，并且提供了沙箱环境供测试，SDK 支持传统 web 端、app 以及线下商铺接入。

XCoinPay 商用平台（Commercial platform）提供移动端和 PC 端的全支付场景支持，包括 IOS、Android、HTML5，满足商户多重经营场景需求，为用户经营场景多样化提供支持，商家可以使用 XCoinPay 商用平台（Commercial platform）来零成本地接受全世界用户的数字货币支付。

2.1 商家一键接入 XCoinPay 支付

全世界的商家可以一键便利接入 XCoinPay 提供的 SDK 到自己的网站、app 中，就可以接受全世界用户的跨国付款，全平台 SDK 让商家最小化接入支付的时间与人力，用户只需要支付加密数字货币，就可以迅速购买异国的商品，XCoinPay 提供的服务是

实时而且手续费低廉的，而使用区块链作为资金通道可以实现即时、安全，商家可以通过 XCoinPay 商用平台（Commercial platform）提供的商户管理后台管理这些支付渠道的所有订单。

2.2 跨境支付解决方案

在传统的跨境支付中，往往面临转账手续费高昂、结算周期长、到账速度慢、转账额度限制、资金冻结等风险，这些风险常常给企业用户经营带来不必要的损失，跨境支付在传统金融体系下难以有突破点，而区块链提供的无摩擦、实时高效的去中心化支付网络，是解决跨境支付痛点的有效工具。

六、XYT 代币（XCoinPay Token）

XYT 代币（XcoinPaY Token）为标准的 ERC20 代币，XYT 总量 5 个亿，总量固定永不增发，XYT 代币为应用型代币，XYT 代币在柔支付网络（RouPay Network）中的主要用途：

1、作为防止粉尘交易攻击收的微量交易手续费。

2、搭建柔网关节点时的信用担保金和结算服务费。

3、各种数字货币币种在跨链柔支付时的中间换算币。

XYT 代币的分配：

额度及数量	用途	状态	备注
6.3%	早期私募	已结束	私募投资锁定半年，锁定地址已经公布在白皮书内。机构控股公司股份，未占代币份额
62%	售卖硬件赠送	已结束，即将开启空投	/
8%	创始团队及顾问所持	/	锁定半年，锁币地址已经公布在白皮书内
6%	社区推广、个人打赏以及第三方合作、交易所合作等	/	/
17.7%	陆续分发给活跃以太钱包地址	/	/

公示地址：

团队及顾问所持代币的钱包地址：

0x1AE242dE666125f7f8ea2bb55E533214BF29FE29

私募钱包地址：

0x74467850Bcbd00264d1FD7a108a7E3DdF83961b4

截止到 2018 年 5 月，这两个地址上的 XYT 代币都不会被挪动。

注：

*交易：XYT 代币将于 2018 年 1 月在 AEX.com 开盘交易，具体时间延后公布。

七、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)

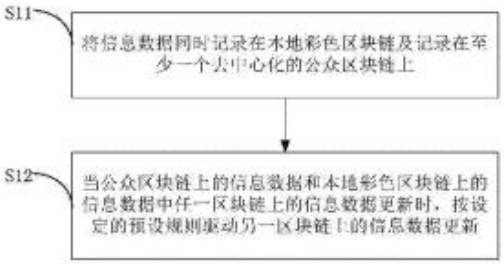
权利要求书1页 说明书7页 附图3页

(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。

八、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。

欧阳克星 COO

曾担嘉田传媒集团高管，在互联网推广运营领域拥有 10 年以上从业经验，对互联网运营及市场营销策划有深刻的理解，曾主导过多家大型平台运营规划及市场活动，在电商、金融 app、移动互联网行业运营推广方面具有多年丰富的实战经验。

CARLOS CHOONG 首席海外关系官

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。

Daniel 海外运营总监

Daniel 持有语言学士学位，精通数门语言，Daniel 曾经在美国、英国、意大利、德国、阿拉伯联合酋长国和中国生活过，访问过 30 多个国家，海外关系丰富，同时 Daniel 是 BTT 论坛上面的活跃用户，他翻译过很多技术文档，在 BTT 论坛上面拥有很多粉丝。

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 Academy Blochchain Expert Committee Member

联系我们

FAQ:

❖ **XCoinPay 的目标是什么？**

XCoinPay 的目标分为两个：市值和应用价值，在市值方面，我们将努力推动 XCoinPay 的市值进入全球数字货币市值排行榜前 50，给广大投资者带来回报，这是我们的目标，XCoinPay 团队将为此不懈奋斗。

在应用价值方面，我们将基于柔支付技术打造为支付而生、新一代的区块链资产支付网络，显著地解决现有区块链的传输低效问题，用户使用 XCoinPay 可以实现零费用、极速发送区块链数字资产，同时获取至少 40 万+活跃用户。

❖ **XCoinPay 跟 imtoken 有什么不同？**

XCoinPay 更像 paypal，而 imtoken 更像支付宝，因为 imtoken 主要支持 ERC20 代币，而 XCoinPay 则支持多种加密数字货币。

❖ **XCoinPay 跟瑞波有什么区别？**

瑞波的偏重点是瑞波协议和银行服务，而 XCoinPay 的偏重点是打造跨链功能和极速低成本转账系统，从而打造加密数字行业的 PayPal。

❖ **项目落地性如何？**

项目落地性很高，我们描绘的不是遥远的未来，而是不久后的一个实用系统。

❖ **XYT 代币什么时候可以交易？**

XYT 代币将于 2018 年 1 月开盘交易，具体时间延后公布。

❖ **XYT 代币上线哪个交易平台？**

将首发 AEX.com，后期会上线更多一线平台。

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》