水木链:基于可升级智能合约的区块链商业平台

V0.9

2017 年 8 月

摘 要

从比特币诞生到以太坊推出智能合约，区块链技术已经获得了很大的发展。我们研发水木链的目的是更好地满足商业应用开发的需求。相比于 POW(Proof of Work)，DPOS(Delegated Proof of Stake)具有更加优异的性能，并且区块生产者(即“矿工”)的利益总是与持币者一致，便于更好地治理。商业应用需求的多变性，要求智能合约能够安全地进行链上升级，水木链支持这个特性，并且完全兼容以太坊智能合约。水木链将提供友好的 SDK，降低开发门槛，便于开发者快速开发商业应用。

目 录

一、 水木链的设计理念

1.1 区块链背景

区块链的概念首次在 2008 年末由中本聪（Satoshi Nakamoto）发表在比特币论坛中的论文《Bitcoin: A Peer-to-Peer Electronic Cash System》提出。论文中区块链技术是构建比特币数据结构与交易信息加密传输的基础技术，该技术实现了比特币的挖矿与交易。

中本聪认为：第一，借助第三方机构来处理信息的模式拥有点与点之间缺乏信任的内生弱点，商家为了提防自己的客户，会向客户索取完全不必要的信息，但仍然不能避免一定的欺诈行为；第二，中介机构的存在，增加了交易成本，限制了实际可行的最小交易规模；第三，数字签名本身能够解决电子货币身份问题，如果还需要第三方支持才能防止双重消费，则系统将失去价值。基于以上三点现存的问题，中本聪在区块链技术的基础上，创建了比特币。

区块链技术作为比特币的基础性技术，具有高度透明、去中心化、匿名等性质。这些性质体现了分布式自治的理念，逐渐受到拥有创新意识的机构的广泛关注。简而言之，区块链技术是一种使用去中心化共识机制去维护一个完整的、分布式的、不可篡改的账本数据库的技术，它能够让区块链中的参与者在无需建立信任关系的前提下实现一个统一的账本系统。区块是公共帐本，多点维护；链就是盖上时间戳，不可伪造。区块链是一项注重安全和可信度的技术。

1.2 为什么做水木链

随着比特币和区块链的普及，越来越多的技术人员投身于区块链这个新兴的技术领域，也诞生了很多新的加密数字货币，比如有莱特币、瑞波币、NXT、比特股和以太坊等，它们代表着区块链技术在各个角度边界上的突破。但是从行业应用的角度来看，区块链技术还面临比较多的挑战。

目前区块链面临以下问题：

1.现有区块链没有考虑通用商用场景，开发商业应用改造困难。

2.区块链属于新兴技术，底层开发入门门槛高，技术人才短缺。

3.区块链都没有考虑行业管理需求，管理机构监管困难。

4.性能瓶颈，目前大部分区块链平台的性能都比较低，难以满足生产环境的要求。

针对当前区块链的挑战，水木链在技术和理念上进行了大胆创新和融合，在兼容以太坊通用的智能合约技术的基础上提出可升级智能合约的方案，整合比特股高性能交易处理方法，采用 DPOS 共识算法，提供商业友好的区块链应用接口和监管友好的平台机制，致力于打造一个区块链商业应用的生态平台。

1.3 水木链的设计原则

1. 保持以太坊智能合约 EVM 的兼容性

以太坊 Ethereum 是第一个具有图灵完备编程语言的区块链，任何人都能够创建合约和去中心化应用，并在其中设立他们自由定义的所有权规则、交易方式和状态转换函数。EVM（Ethereum Virtual

Machine）在以太坊的实际使用中经受了大量的测试，市面上有许多在 EVM 上运行的智能合约。因此，保持智能合约 EVM 的兼容性显得非常重要，以太坊的开发人员可以很快地转移到水木链上开发，熟悉 Solidity 编程的人员可以继续编写水木链的智能合约。

2. 高性能处理

为了给业界提供生产环境可用的方案，高性能的区块链技术对加密货币和智能合约平台来说是必须的。区块链天生就是单线程的，而单核 CPU 的性能是各种资源中最短缺的、最难扩展的一个方面。水木链设计成能够让这个单线程的执行达到极可能的高效，这是几个必须实现的事项：

a.将关键数据放在内存上，避免同步操作

b.分配索引，减少哈希计算

c.面向对象的数据模式

3. 第三方应用开发易用性

区块链本身是一个相对比较底层的技术，在商业场景的使用上，一般需要比较大的改造。水木链在设计的考虑上，商业通用场景的开发是我们的一个重点。在水木链底层接口上，提供第三方易用的 SDK，方便开发人员根据实际需求定制自己的服务；同时，水木链也提供一个生态平台，上面搭载常见的区块链商业应用场景的服务，有需求的用户可以直接使用，具有开发能力的用户也可以在上面发布服务供第三方使用，形成丰富的应用场景。

4. 支持国密 SM2/SM3 标准

水木链支持可插拔的密码方案，包括以太坊使用的 secp256k1，以及国密 SM2 椭圆曲线公钥密码算法和 SM3 杂凑算法，满足国家密码局的国产商用密码算法标准，使得在金融领域使用水木链开发分布式应用符合国家规范。

二、 水木链的技术设计

2.1 技术架构

水木链是一条以 DPOS 共识算法为基础，可升级智能合约、EVM 兼容的高吞吐量区块链，采用四层结构，如图 2.1 所示。

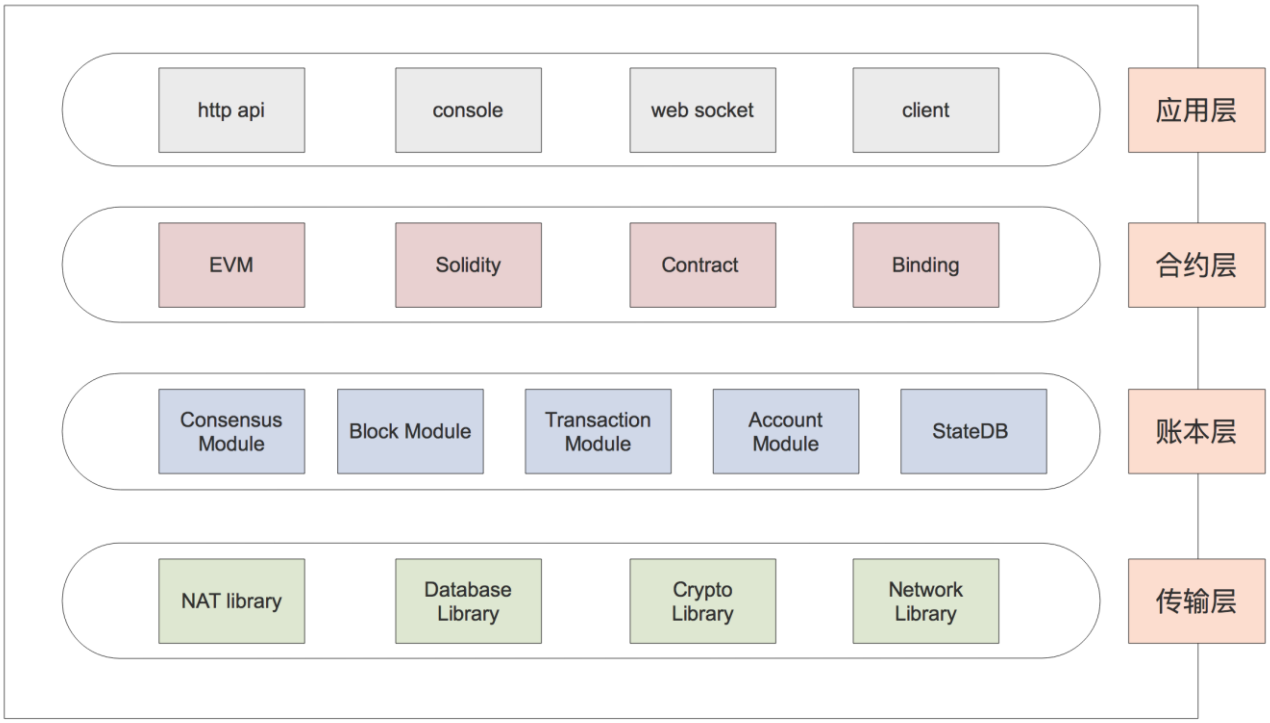

图 2.1 水木链技术架构

1.传输层

水木链的传输层是基于 KAD（Kademlia）协议的 p2p 网络，能高效的传递区块、交易以及其他数据，使得全网节点迅速演进到一致的状态。在处理点对点的连接时，采用了 AES 加密。通过使用 NAT 的方式，利用已经通过验证的节点作为链接桥梁，内网节点也能够参与到水木链的网络中。

2.账本层

水木链在账本层面采用的是账户模型，针对区块包含的交易，采用在内存中进行演化的方式，进行账户状态的更新。区块数据采用链式结构进行存储，所有区块都带有上一区块的指针引用，保证数据不被篡改，采用 Trie 树验证和存储交易。在共识方面，水木链采用的是 DPOS 算法。传统的 POW 算法消耗了太多的计算性能，在实际的商业场景中并不实用。而 DPOS 算法能够兼顾性能的同时，兼顾维护效率，后面会对水木链的 DPOS 进行详细介绍。

3. 合约层

目前水木链在合约层面上提供 EVM 智能合约运行环境，支持部署升级，使用 Solidity 编程。用户在部署好合约代码之后，可以通过使用工具生成比如 Golang 语言的 binding，供应用层调用。在合约层面的设计上，水木链把合约分成两类：

a) 系统合约

创世合约是水木链上预分配地址的合约，在链启动的时候就会部署，将由水木链开发者编写，主要用于开发者对水木链进行功能控制和调整。

b) 普通合约

普通合约是水木链的用户根据实际需要开发编写的 Solidity 合约。

4. 应用层

水木链提供多种形式的接口形式，比如 http 和 web socket 形式， PC、WEB、移动端应用以方便调用合约和交易操作。也可以通过 console 命令行的方法，连接到控台，进行命令操作。我们通过对区块链底层技术的封装，推出 SDK，降低应用层面的使用门槛，也会提供官方客户端，使用水木链提供的标准服务。

2.2 用户模型

在区块链系统中，用户模型是设计之初就需要考虑的数据结构。水木链综合对比了两种典型的用户模型：UTXO 模型和 Account 模型。和其他大多数区块链设计一样， 选择了模型就决定了协议层的实现方式，两种模型各有利弊。

1. UTXO 模型

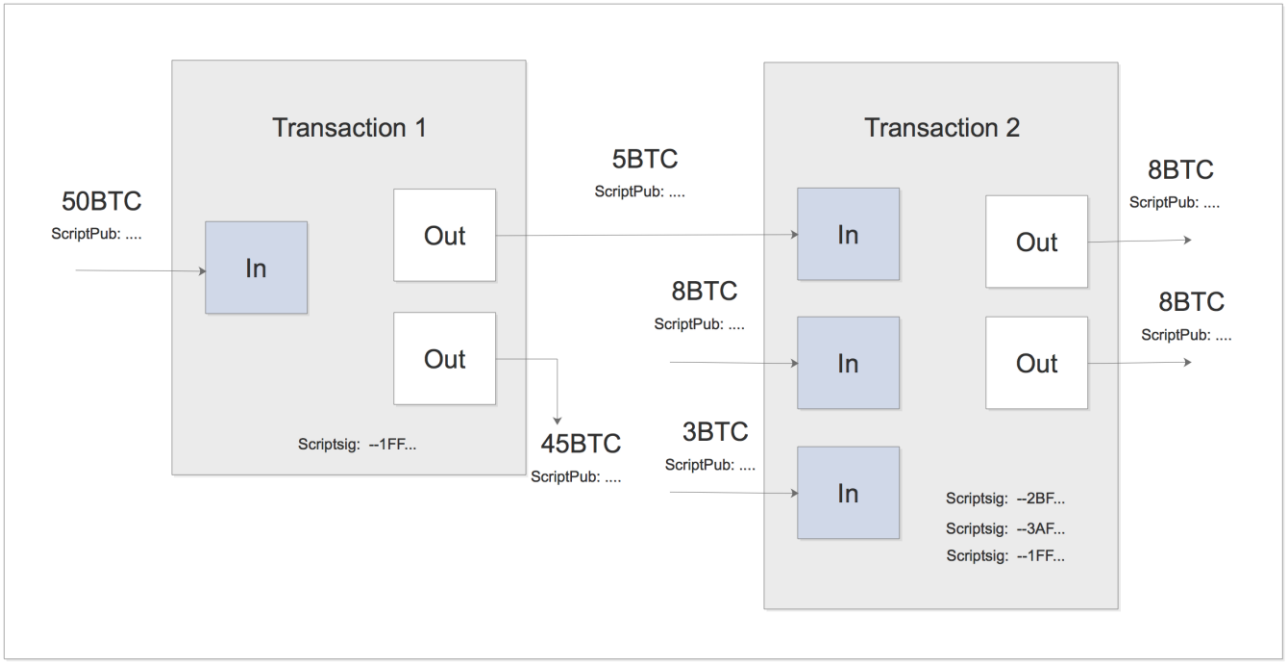

图 2.2 UTXO 模型

在比特币的网络中，交易的基本单位是 UTXO(Unspent Transaction Output)。被某一个交易消耗的 UTXO 称为交易输入，由交易创建的 UTXO 称为交易输出。每个用户的私钥的交易对应着 UTXO 的操作。通过图示的方式，一定额度的比特币就在用户的私钥之间转移，交易费用来源于交易输入和交易输出之间的差值。在转移的过程中，交易链不断消耗 UTXO 和创建新的 UTXO。UTXO 在客户节点存储于一个内存中的数据库，“UTXO 集合”，这个集合检测着所有可用的 UTXO，并不存在一个余额的概念。如图 2.2 所示。

2. Account 模型

以太坊是一个典型的 Account 模型区块链。以太坊的系统中存在着账户体系。账户是一个面向对象的数据结构，为了易于管理账户，引入了世界状态，每一笔交易都会改变这个世界状态。状态就是就是由账户对象和在两个账户之间转移价值和信息的交易构成。

在以太坊的白皮书设计中，账户包含了四个部分：随机数，余额，合约代码和存储空间。通过这个有状态的账户系统来记录账户余额，就像银行的记账方式一样，每发生一笔交易，就有可能对世界状态产生影响。每个账户都有自己的余额，代码和存储，这样就可以调用合约，并且把响应的结果放到存储空间。

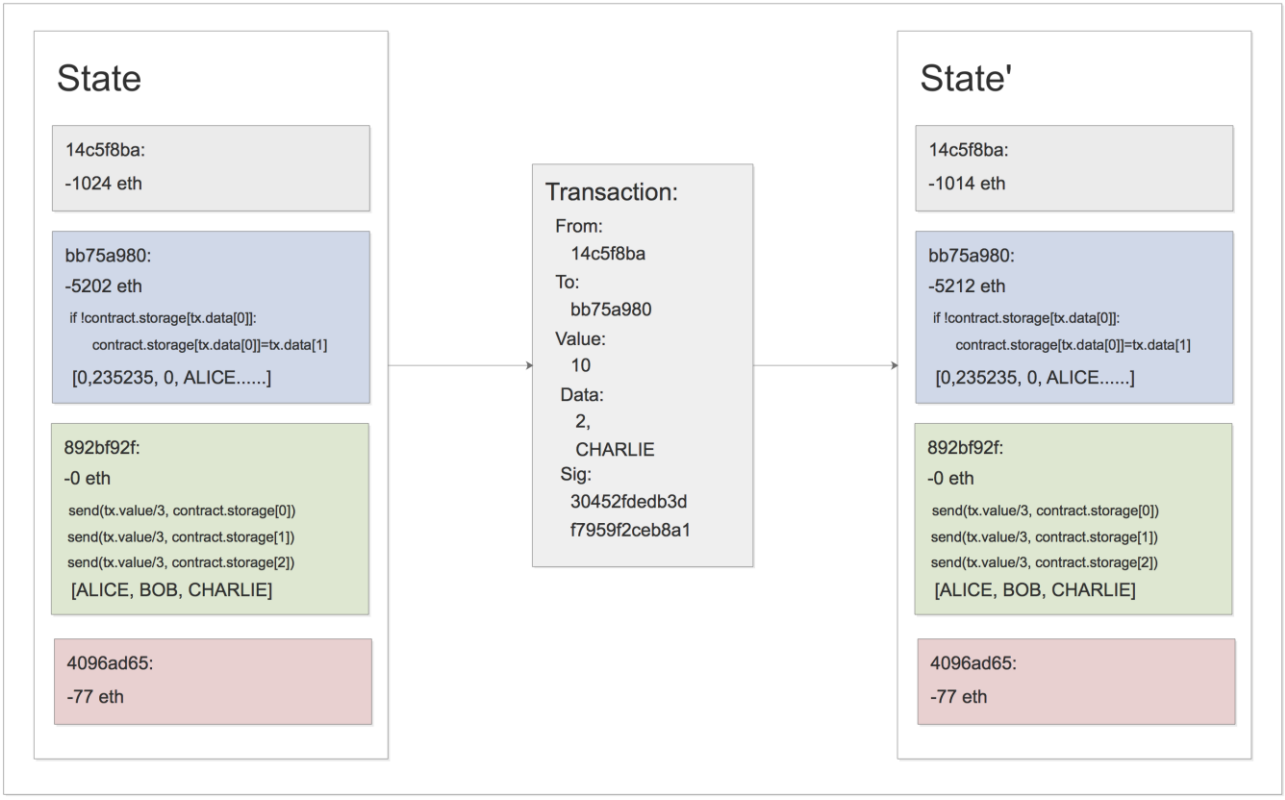

图 2.3 Account 模型

3. 水木链的用户模型

在设计水木链的过程中，兼容 EVM 智能合约是我们的一个主要特性，同时，为了数据易于管理，易于编程，我们采用了 Account 模型。水木链的 Account 模型将会扩展以太坊的账户类型，包含以下部分：

a. 随机数，用于确定每笔交易只能被处理一次的计数器

b. 账户目前的余额，水木币 SMB

c. 账户的合约代码，如果有的话

d. 账户的存储（默认为空）

e. 账户的共识属性，像角色、投票等，用于共识机制

水木币 SMB 是水木链上的主要资源，用于支付交易费用。有两种类型的账户：外部账户和合约账户。外部账户是水木链用户使用的账户，由用户的私钥进行控制。合约账户是由智能合约代码部署之后生成的，用户对合约代码发送一笔签名的交易，合约内部的代码就会被激活，允许它对内部存储进行读取和写入，或者创建其它合约。

交易是水木链上的基本操作事务，账户状态的改变主要是有交易触发的，它主要包含以下部分：

a.随机数，交易计数器 Nonce

b.交易的发起账户 From

c.交易的目的账户 To

d.交易的类型 Type

e.交易的 Amount

f.交易的 Payload

g.交易的费率设定 Fee

h.签名

水木链上的交易类型有两大类：标准原生交易和智能合约交易。原生交易是水木链运行的基础，包括基本的账号管理交易、转账交易和水木链 DPOS 共识运行的交易，包括投票、见证人管理、委员会成员管理等交易。智能合约交易是支持 EVM 智能合约运行的交易，对合约的创建、调用都是通过这种类型的交易来完成。

水木链上的交易会产生一定的费用，这个费用由水木链的见证人节点打包区块的时候来收取，每一笔交易都设定了费率，将会以水木币的形式支付，当交易的发起方账户余额不足以支付费用的时候，交易会失败。EVM 智能合约费用的控制是通过 gas 和 gasprice 来完成，智能合约运行的时候耗费的 gas 会以一定的换算比例换算成水木币来支付。

水木链上的所有账号的状态组成了一个世界状态，类似一个银行内部所有账户的状态。每一笔交易都会修改账号的状态。因为交易都是确定性的输入和输出，对于世界状态的演进来说，每一笔交易的结果都是确定性的。只要根据确定的交易集合，所有节点都能演进到一致的世界状态。

2.3 共识机制

1. 共识算法

所有区块链本质上都是一种由交易驱动的确定性状态机。共识是商定确定性交易顺序和过滤无效交易的过程。有许多不同的共识算法都可以产生等效的交易排序。水木链在考虑共识机制的过程中，综合比较了 POW(Proof of Work)、POS(Proof of Stake)、DPOS(Delegated Proof of Stake)等共识算法。

最有代表性的算法是 POW 共识。比特币和以太坊在区块的生成过程中使用了 POW 机制，一个符合要求的区块哈希由 N 个前导零构成，零的个数取决于网络的难度值。要得到合理的区块哈希需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当节点拥有占全网 n%的算力时，该节点即有 n/100 的概率找到区块哈希。所以当矿工的算力集中到一定程度的时候，POW 共识会变得越来越中心化，对整个区块链网络的影响也越来越大。

POS 算法是在 POW 共识上的改进，基本概念是产生区块的难度应该与节点在网络里所占的股权(所有权占比)成比例。已有几个系统开始运行 POS 共识，比如点点币(Peercoin)和未来币(NXT)。点点币使用一种混合模式，用股权调整挖矿难度。未来币使用一个确定性算法以随机选择一个股东来产生下一个区块，基于账户余额来调整。它们分别解决了谁来生产下一个区块的问题，但没有找到在适当的时间内使区块链具备不可逆的安全性的方法。

在水木链中，我们选取的共识协议的基础是 DPOS。DPOS 在比特股区块链系统上经年累月的可靠运行证明自身是健壮、安全和有效的。DPOS 的核心思想是利用投票系统，网络成员选举出区块链生产者节点，然后生产者节点调度生产。选举过程确保利益相关方最终得到控制。从某种角度来看，DPOS

有点像是人民代表大会制度。如果代表不能履行他们的职责（当轮到他们时，没能生成区块），他们会被除名，网络会选出新的节点来取代他们。正常的情况下，DPOS 比 POW 和 POS 更加高效节能，有更快的确认速度，能够承载更多的交易，并且不会出现矿场权力中心化的问题。

2. 水木链 DPOS

水木链在 DPOS 的设计中，根据节点的职责和功能，全网参与水木链的节点可以分成三种角色：普通成员，区块生产者见证人 witness 成员和区块链理事会 commitee 成员。三种角色在水木链系统中发挥不同的作用。普通成员是水木链的用户，参与水木链的日常使用和交易。见证人是区块的生产者，他们验证交易数据并维护网络安全，获取一定的报酬。理事会成员是水木链的维护中，可以提议修改区块链的动态参数，比如手续费，区块间隔时间以及其他很多参数。这三种角色的区分是通过投票系统来完成的。

在水木链系统中，投票是一种非常重要的特性，关系到网络的安全和稳定运行。参与水木链的普通成员，可以通过投票系统来选取见证人成员和理事会成员。

在选取见证人的时候，每个用户可以投票给他信任的见证人节点。获票数靠前的见证人按既定时间表轮流产生区块，每个见证人分配到一个时间段来生产区块，他们将收到等同于一个平均水平的区块所含交易费的比例作为报酬。水木链里预计每 3 秒产生一个区块，以 21 个区块为一个周期，任何一个时刻，只有一个见证人被授予产生区块。在每个区块周期开始时，21 个区块见证人的顺序会根据块时间导出的伪随机数进行混合，以保障见证人之间的连接分布尽量平衡。

因为见证人节点可以获取报酬，他们将保证近 100%的在线时间来防止被投票罢免，如果见证人错过了太多的区块生产，用户可以撤回他的投票，见证人的排名会靠后，丢失生产区块的资格。通过用户的投票，获得信任度最高的节点总是能获取生产区块的资格，从而能够保障网络的高效运行。

理事会成员是被普通用户投票选举的。理事会成员负责调整水木链整个系统的参数，是一个责任感比较强的职位。理事会成员可以发起调整水木链的提案，经过理事会成员的讨论和投票之后，对结果进行审议，通过的提案按照一定的规则进行代码实施或者参数调整。

3. 投票设计

在水木链的设计中，我们将提供一个钱包客户端。每个钱包有一个参数设置窗口，在该窗口里用户可以管理自己的投票，将自己的选票投向见证人节点和理事会成员，或者是撤回投票。以见证人节点为例，钱包将显示一个状态指示器，让用户知道目前见证人节点打包区块的表现如何。如果他们错过了太多的区块，或者产生了无效的区块，那么系统将会推荐用户去换一个新的见证人。

4. 解决区块链分叉

POW 共识中最佳链是难度最大的区块链，在 DPOS 中则是最长的有效区块链。任何时候，一名见证人错过签发一个区块的机会，该见证人所在的区块链将比潜在竞争对手短。只要用户的交易被见证人的 51%生产出来了，那么你就可以安全地认为你在主区块链上。在防止区块链分叉所导致的损失方面，最重要的事是在事发后第一时间得知消息。因为见证人通过生产区块得到很好的报酬，他们将保持接近 100% 的在线时间来防止因被投票罢免而损失收入。可以安全地认为如果在过去的 10 个区块周期中，有一两个见证人错过生产，则互联网的某些部分可能正发生连接问题，那么用户应该对此警觉并要求额外的确认数。

另外，在水木链上，每个交易都要包括最近的区块头的哈希（TaPOS），这样能够防止分叉的区块链上出现大量的交易，并且系统也能知道用户是否处于在区块链的分叉上。随着时间推移，区块会被越来越多的用户确认，交易也不能被伪造。

2.4 可升级的智能合约

1. 水木链标准原生交易和智能合约交易

在水木链的系统中，存在两种交易类型，标准原生交易和智能合约交易。标准原生交易是水木链上的基础交易类型，包括账号管理、角色创建、转账、投票等内置功能的交易。对于用到 EVM 的部分，我们使用智能合约交易类型，包括合约创建、合约调用和合约升级等。

2. 合约设计

在水木链的设计中，智能合约能够兼容以太坊 EVM 标准 Solidity 智能合约的特性，也支持已部署合约的特定升级。在 Account 模型中，每一个智能合约拥有一个账户，合约的代码和存储的数据 storage 关联到这个对于的账户下面。

合约的代码将会以账户 Code 属性的形式，包含代码的哈希值 CodeHash，存储到 StateDB 中；而合约本身包含的状态数据，也会以 Trie 树元素的形式，存储到 StateDB 中。根据 Solidity 标准，水木链状态数据变量的存储规范：

a. 状态数据以 32 字节对齐

b. 静态类型的状态变量，按照 Solidity 代码中定义的顺序，以“position-value”的形式，从位置 0 开始，依次按照位置存储状态

c. 对于动态类型的数据 Mapping 和 Array，由于它们包含的元素类型和个数是不确定的，采用 SHA3(Keccak-256)函数来计算元素的位置。Mapping 和 Array 本身占有一个 Slot 的位置 p。元素的位置将会依赖于位置 p。对于 Array，元素的起始位置是 Keccak256(p)。对于 Mapping，如果元素的键值是 k，那么元素对于的 value 存储的位置是 Keccak256(k • p)，其中“ • ”是一个连接函数，表示将 k 和 p 拼接成一个 Keccake256 传递的参数。

d.对于 bytes 和 string，如果长度没有超过 31 字节，bytes 和 string 存储在位置 p（一个字节用来存储长度）。如果超过 31 字节，位置 p 用来存储 bytes 和 string 的长度，内容存储的位置是 Keccak256(p)。

3. 合约升级

水木链的智能合约拥有余额的属性，能接受水木币和发送水木币。智能合约的代码、存储和余额都讲作为账户的状态影响着水木链的世界状态。

在实际的智能合约使用中，在部署完之后，DAPP 会通过接口对合约的功能进行集成。由于客观的原因，或许是智能合约存在 bug，或许是接口的使用便捷问题，或是实际的需求发生了变化，用户存在对智能合约进行升级的需求。像以太坊著名的 The DAO 事件，就是因为合约的代码上存在 bug，导致了大量资金被偷窃，后来还引起了以太坊社区的分裂。

所以在水木链的设计中，智能合约除了兼容 EVM，还支持链上的部署升级。在水木链的 Account 模型设计中，智能合约的代码作为合约账号的一个属性，支持在合约创建部署之后，通过发送合约升级交易来进行更新，更新之后保存合约账号地址的一致。用户在第一次部署智能合约的时候，可以根据实际的合约场景，选择支持后续部署升级，也可以选择不可修改。

已部署的合约在区块链上运行一段时间后，会存在合约的状态数据。在升级合约的时候，除了合约本身的代码改动，状态数据的兼容性也是一个需要考虑的问题。这个需要合约的作者在编写 Solidity 升级代码的时候，保持升级后的代码能够读取以前的状态数据。水木链将会提供一个基于 Solidity 编译器原理的状态数据检查工具，通过新旧 Soldity 代码的比较分析，以形式化验证的方式来确认升级之后状态数据的兼容性。

经过代码工具的分析比较之后，合约作者应该在水木链测试网上进行合约部署升级的测试，以检测实际升级过程中是否会发生问题，和升级之后是否会影响现有 DAPP 的接口使用。在测试网运行一段时间之后，确认升级部署没有问题，即可用考虑发布到主网。

由于智能合约的升级会影响当前合约接口的 DAPP，合约的作者不能随意升级智能合约，需要有一个投票的流程。如图 2.4 所示。

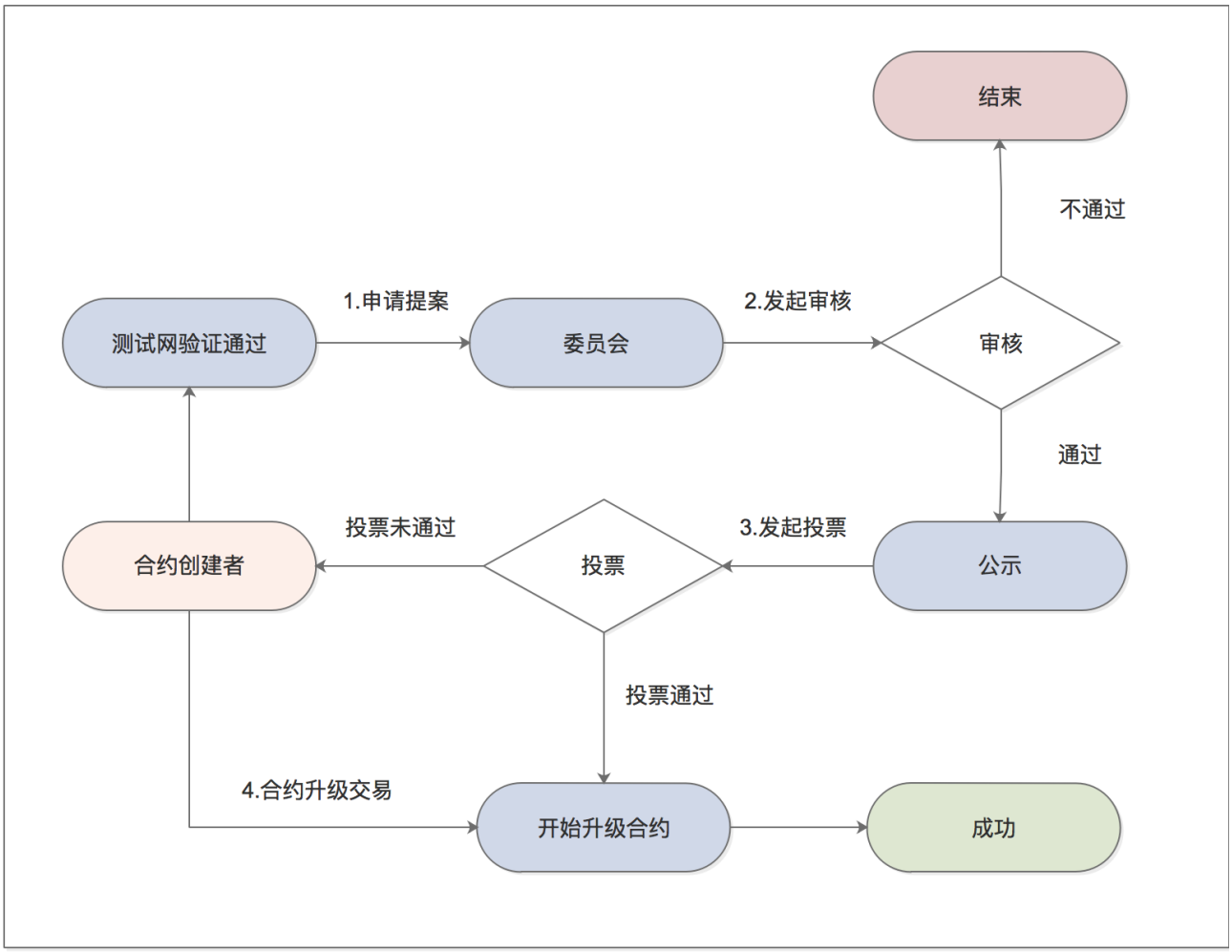

图 2.4 智能合约升级流程

当作者决定需要升级合约的时候，需要发起一个提案给水木链理事会 commitee，并支付一定的水木币作为预付金。理事会成员审核通过之后进行公示这个提案，公示将会收集一定时间内的这个智能合约用户的投票。

如果这个投票满足 80%的门槛值，提案通过，升级操作将被批准。之后合约的作者发起合约升级的交易，在这个交易里包含提案的信息，区块链验证通过之后，如果预付金足够，代码就能完成升级部署，扣除部署手续费后，返还余额；如果预付金不足，代码升级失败，扣除验证手续费后，返还余额。

如果提案没有获得足够的票数，提案被否决，升级操作不被批准。合约作者之前提交的预付金将会直接返回到账户中。

4. 合约的花费

在水木链上用户发起智能合约交易，将会消耗一定量的水木币。我们沿用了 EVM 虚拟机中 gas 的概念。对于一个智能合约，Opcode 的数量，操作和状态变量的 storage，都会影响整个合约的 gas 花费。根据 cost = gas*gasPrice 的换算，具体智能合约交易消耗的水木币依赖于合约本身复杂程度和 gasPrice 的制定。gasPrice 相当于现实世界中的油价，是由水木链的委员会 commitee 设定的全

局参数。用户的智能合约交易越复杂，消耗的水木币越多。同时，每个智能合约能够消耗的 gas 也会有一个 limit。通过这样的经济手段，来约束智能合约交易的行为。

针对可升级智能合约和固定智能合约两种类型，水木链设定了不同的费率。由于可升级的智能合约消耗的 storage 相对多一些，部署可升级智能合约的交易消耗更高的水木币。在真正升级智能合约的时候，流程上涉及的较多的参与方，升级交易的消耗也更高一些。通过这样的经济手段，来约束智能合约发布者的升级行为。

2.5 分布式存储服务

水木链将支持分布式存储服务，参与水木链的节点，可以选择加入分布式存储网络，提供带宽和存储服务获取报酬。水木链分布式存储的目标是为水木链网络提供足够去中心化的存储空间，来保存水木链上分布式应用 DAPP 使用到的数据和文件。

1. 分布式存储

在水木链的设计中，分布式存储服务是一个基于 KAD 协议的 P2P 网络的存储方案，安全可靠，它能够抵御 DDOS 攻击，提供一定程度的容错，并且能够自我维持。对应用户来说，使用水木链分布式存储服务就像使用一般的文件保存服务一样便捷，在预付了一定量的水木币费用之后，上传文件到某个节点，获取文件标识下载链接，就完成的文件的保存。文件被保存到参与存储服务的节点中，只要网络存在，文件就能随时获取。

2. 存储原理

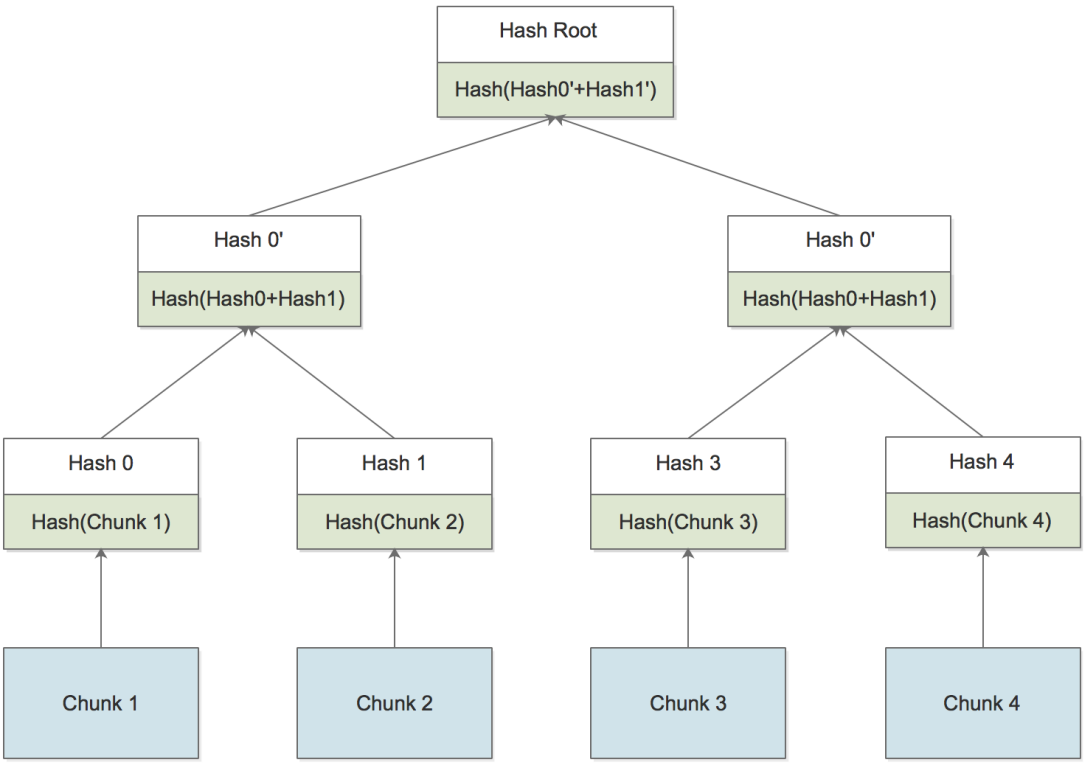

图 2.5 分布式文件块示意图

文件在存储系统中都是通过文件标识来代表的。对分布式存储来说，文件标识要满足以下几个条件：a.标识不冲突，不同的文件数据对应不同的文件标识

b.标识确定性，相同的文件数据的标识一致

c.文件标识在命名空间里面均匀分布

水木链在文件标识的设计中采用了基于哈希 Hash 的方案，SHA3(Keccak-256)函数满足上面提到的几个要求。上传到存储的文件，都会使用哈希来处理内容，产生文件标识。

对于参与分布式存储服务的节点来说，存储服务的基地址（base address）是和用户上传的文件内容最终将要存储的位置相关联的。服务的基地址是通过水木链的节点地址进行 SHA3 哈希得到的，也就是说，基地址和文件标识在一个命名空间里面。

当一个文件被上传到分布式服务时，文件被切成一个一个的小块（chunk）。一个 chunk 的最大尺寸是 4k，每一个 chunk 都有自己的 SHA3 哈希值。组成文件的 chunk 得到的一组哈希值，也被打包成一个 chunk，同样也得到了一个哈希值。这样切割下去，最终，文件形成了一个 chunk 树，一个 root chunk 代表这个文件。这个 chunk 树可以对一块数据作默克尔证明（merkle proof），从而提供完整性校验。如图 2.5 所示。

文件被转换成小块之后，被上传到提供存储服务的节点网络。上面提到，节点的服务地址是 SHA3 得到的，和文件标识一个命名空间，通过 XOR 的基地址运算，每个 chunk 的哈希和节点服务地址 base address 可以算出一个距离。距离每个 chunk 距离最短的节点（会有多个）保存这个 chunk 的内容，一个文件的 chunk 被分布到许多个节点存储。意味着，当一个 chunk 上传的时候，chunk 需要从上传节点传递到存储节点；下载的时候，chunk 需要从存储节点传递到请求节点。这需要对网络节点的查找要求比较高，水木链的存储节点是按照 KAD（Kademlia）协议组成网络，可以提供接近常数时间的节点查找，满足需求。这样，水木链的存储服务组成了一个基于地址的 DHT，参与存储服务的节点提供当前节点所有存储文件块的信息，上传的文件根据 root chunk 分配一个文件标识，对用户来说，这个文件标识就是以后的下载链接。

3. 激励措施

对于提供存储服务的节点，激励总体来源于用户存储文件支付的水木币费用，主要体现在两个方面：存储消耗和带宽消耗。

a.存储消耗

用户在上传文件到网络的时候，文件的各个 chunk 根据 SHA3 的哈希值分布在各个距离最近的节点上。节点存储 chunk 需要消耗一定量的磁盘空间，根据存储消耗量来获得费用。存储消耗的空间越多，节点能够获得的激励也越多。

b.带宽消耗

用户在读取文件 chunk 时，内容需要经过多个节点传递。每个节点会记录相邻节点发送和接收 chunk 的统计，一般来说，提供 chunk 内容服务的节点总体上发送的 chunk 数量是大于接收数量的，而中间的传递节点发送量等于接收量。节点的净发送量越大，表示提供的服务次数越多，能够获取的激励响应的也增加。对于中间的传递节点，他们对存储服务提供了路由的功能，也能获取一定的激励。

4. 水木链命名服务

由于基于哈希产生的文件标识符是一串十六进制字符，在日常的使用中不是很方便，通常的文件名都是使用母语来标识，水木链提供了一个水木链命名服务。水木命名服务的目的是提供一个基于母语的文件标识映射服务，类似 DNS 把域名映射到 IP，这样文件上传到存储服务之后，可以使用一个普通的文件名来标识产生的链接。

水木命名服务是一个基于智能合约的服务，提供接口给存储服务使用。用户基于命名服务可以用普通的名称来获取存储的文件。通过将存储链接组织成 Manifest 文件的形式，水木链分布式存储可以将文件的获取变成服务集合，比如用于文件系统、数据库索引等。

Manifest 文件包含文件路径和对应的内容哈希的 url 链接，因此可以用来对静态资源提供路由，比如图片资源，静态 JavaScript 文件和 css 文件，这样就提供了类似虚拟主机的功能，一个网站的内容都可以存储到分布式存储上，形成去中心化的网站，和传统的 www 网站一样提供服务，不过没有一个完全中心化的服务器。

2.6 跨链资产交易

1. 跨链交易

水木链将通过双向锚定的方式，支持多种数字资产。每种资产都将由一个资产 ID 进行标识，根据不同资产 ID，可以确立该类资产所属类型，并关联到该类资产的操作合约。水木链将能够连接现有的主要数字货币（比如比特币、以太坊），能够完成资产的兑换，同时也不改变原有链的机制。

2. 交易流程

其他公有链资产接入水木链，首先需要完成在资产在水木链上的注册，水木链的验证节点会使用给一个基于协议的内置资产模板，根据跨链交易信息部署新的智能合约创建新的资产。当一种已注册资产由某个公有链转移到水木链上时，水木链验证节点会为用户在创建好的资产合约中发放相应的代币资产水木币，确保这个公有链资产在水木链上仍然能够相互流通。用户使用跨链资产交易功能，主要通过水木链数字钱包的形式进行，以以太坊为例，描述一下公有链和水木链之间资产的转入转出。

a.用户 A 在以太坊上有账户，用户 B 在水木链上有账户，用户 A 需要转入 x 个 ETH 到用户 B。

首先用户 A 使用水木链钱包发起一笔跨链交易请求，并且在以太坊中发起一笔转账交易，交易的接收账户为水木链在以太坊上设置的跨链锁定账户(Locked Account)。水木链的验证节点在收到跨链交易请求后，会在以太坊上验证转账交易是否完成。当转账交易验证通过之后，验证节点将在为用户 A 创建的智能合约资产中发放一定量的水木币，然后将该资产在链上转移到用户 B 的水木链账户。

b.用户 B 在水木链上有账户，用户 C 在以太坊上有账户，用户 B 需要将从用户 A 收到的 x 个 ETH 转出到用户 C。

首先用户 B 使用水木链钱包发起一笔跨链交易请求，并且在水木链中发起一笔 1ETH 等价的水木币转账交易，交易的接收账户为用户 B 对应的智能合约资产。验证节点在收到跨链交易后，将用户 B 智能合约资产转为锁定状态。锁定完成之后，验证节点在以太坊上发起一笔交易，交易的转出方是跨链锁定账户(Locked Account)，接收方是用户 C 的账户；验证节点验证在以太坊的交易确认之后，将用户 B 中的锁定资产清空，资产即完成了转移。

流程如图 2.6 所示：

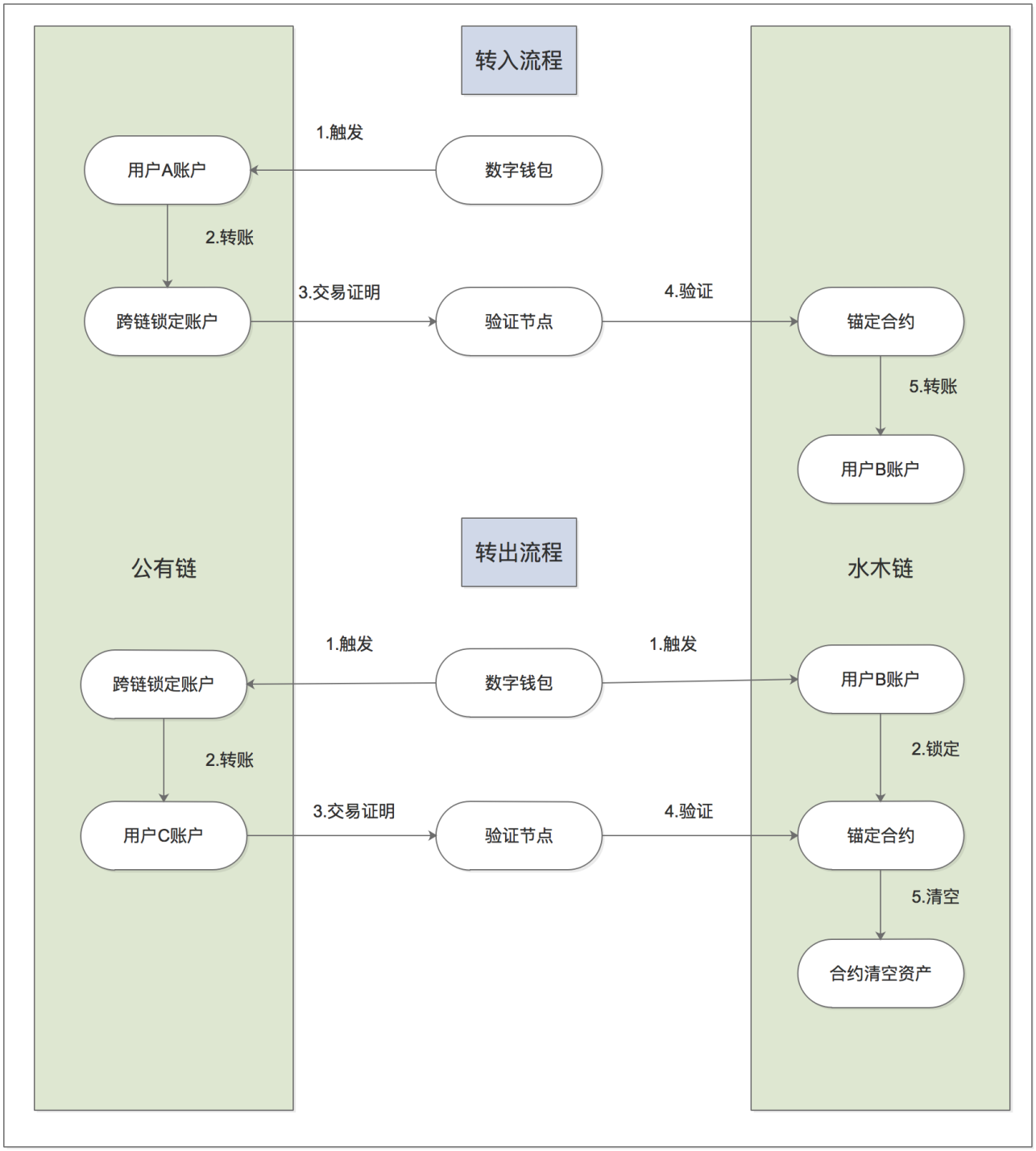

图 2.6 跨链交易流程示意图

对于不同的数字货币，水木链将按照上图所示的规则来处理。新产生的数字货币能够以比较低的成本接入到水木链中，实现资产的转移和流通。

3. 验证节点

在跨链资产交易的过程中，验证节点作为一个业务节点提供服务，它的职责是提供公有链账户和水木链在公有链上的锁定账户之间的交易证明，和水木链上资产的锁定转移功能。根据资产转移的额度，验证节点可以获得相应比例的交易费用作为报酬。通过这样的激励措施，可以提升业务节点的参与活跃度。

2.7 移动端策略

移动端是水木链技术落地的一个重要环节，在主流的手机操作系统 Android 和 iOS 上，水木链都会提供客户端。

在水木链的设计中，轻量级客户端(Light Client)是一个推动区块链移动化的关键点。轻量级客户端是相对全节点而言的，在默认情况下，轻量级客户端使用区块头数据，里面包含交易的默克尔证明（Merkle Proof）。一般情况下客户端不需要处理大量交易，也不存储大量的历史数据，只在某些情况下验证需要的数据以保障正确性。这样轻量级客户端只需要使用少量的存储空间，在手机上也能够运行。轻量级客户端通常情况下是连接到全节点完成关键数据结构的下载，然后基于区块链状态演进的原理，在本地进行验证工作。

为了减少数据存储空间，轻量级客户端依赖的是轻量级的交易存在证明。水木链的全节点通过在导入区块的时候，生成一个增量形式的轻量级数据结构。该结构由当前不可逆区块组成，所有的区块是通过哈希链接起来，通过把哈希链接起来的区块 BlockId 组成默克尔树的形式，最后得到一个 root，形成默克尔证明(Merkle Proof)。轻量级客户端基于这个哈希链默克尔树数据结构，完成轻量级证明。

轻量级客户端能够完成的典型功能包括以下几个：

a.获取特定时刻账号的状态 。客户端不断下载世界状态的节点，直到找到匹配的值。

b.检查某个交易是否被确认。客户端向全节点查询这个交易的区块号，然后下载区块号对应区块里面包含的交易树，检查交易是否被打包。

c.查询某个特定的事件。客户端检查区块头里面的 bloom 过滤器，对潜在匹配的区块，下载交易收据，对比交易的 bloom 过滤匹配，然后检查匹配交易的日志。

除了轻量级客户端，水木链会推出手机数字钱包，支持水木币的管理、交易，并且支持跨链资产转移。同时也会推出 DAPP 浏览器，用于管理和使用水木链上的 DAPP，用户可以在上面使用基于智能合约的服务。

另外，水木链会提供 JSON-RPC 和 WebSocket 接口，第三方开发者可以使用公开的 API 接口，对水木链开发自己定制的 APP。我们也鼓励第三方开发者加入社区，开发普通用户方便使用的区块链 APP。

2.8 可插拔的加密方案

水木链支持可插拔的密码方案，包括以太坊使用的 secp256k1，以及国密 SM2 椭圆曲线公钥密码算法和 SM3 杂凑算法。

SM2 椭圆曲线公钥密码算法是我国自主设计的公钥密码算法，基于椭圆曲线上点群离散对数难题，包括 SM2-1 椭圆曲线数字签名算法，SM2-2 椭圆曲线密钥交换协议，SM2-3 椭圆曲线公钥加密算法，分别用于实现数字签名密钥协商和数据加密等功能。

SM3 杂凑算法是我国自主设计的密码杂凑算法，适用于商用密码应用中的数字签名和验证消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。为了保证杂凑算法的安全性，其产生的杂凑值的长度不应太短，SM3 算法的输出长度为 256 比特，因此 SM3 算法的安全性要高于 MD5 算法和 SHA-1 算法。SM3 算法的压缩函数与 SHA-256 的压缩函数具有相似的结构，但是 SM3 算法的设计更加复杂，比如压缩函数的每一轮都使用 2 个消息字。

通过支持国密 SM2 和 SM3, 水木链的代码将满足国家密码局的国产商用密码算法标准，在各个领域使用水木链开发分布式应用符合国家规范。

2.9 超导数据交易

数据是有价值的，但数据又是一种信息，复制即被拥有。在数据交易的过程中，怎样保证数据的价值和信息的传递同时又不会无端泄漏，是我们要研究的问题。

一个良好的数据交易机制应该满足以下条件：

a. 数据在二者之间直接完成交易，不借助第三方；

b. 交易的过程中不会产生数据泄漏，且交易本身是有迹可循的；

c. 交易的过程中数据的价值得到确认。

超导数据交易技术是满足上述条件的机制之一，专用于数据与数据之间的交换，示意图如下：

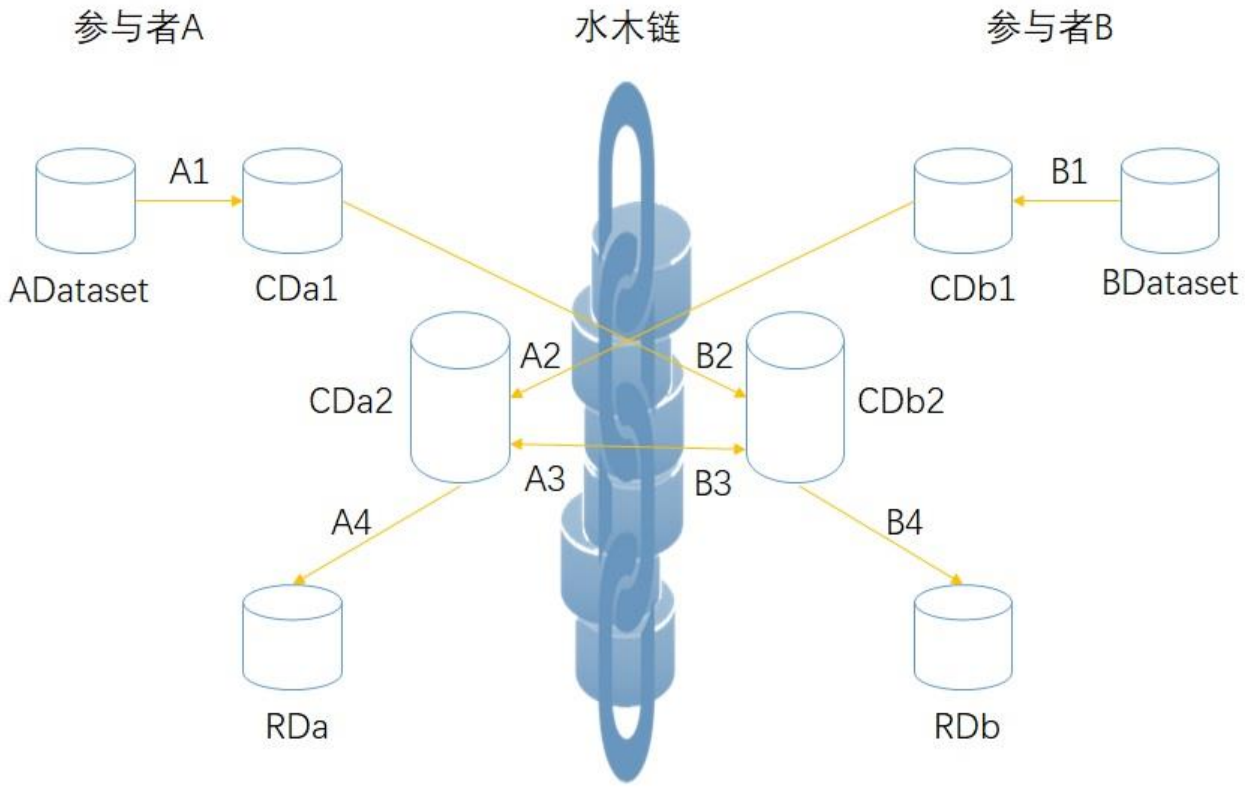

图 2.7 超导数据交易示意图

各步骤含义如下：

A1、B1：参与者 A 和 B 将本地的原始数据 ADataset、BDataset 进行第 1 次加密操作，得到数据集 CDa1 和 CDb1。

A2、B2：使用数据集 CDb1 和 CDa1 进行第 2 次加密操作，得到数据集 CDa2 和 CDb2。

A3、B3：比对数据集 CDa2 和 CDb2，得到交集数据。

A4、B4：A、B 分别得到第 3 步中的交集数据，各自比对本地保留的原文数据索引号，进而得到原文。

在上述步骤中 1 和 2 中，只需要选用合适的非对称加密算法和密钥，便可满足既不在中间过程泄漏数据，也可以得到最后的交集数据。幸运的是我们已经掌握了这样的加密算法。结合水木链，便可以方便地实现点对点的数据交易，同时使用水木贝进行费用结算。

三、 水木链的经济设计

3.1 应用场景

水木链是一条通用的公有链，其技术特点决定了它全面支持去中心化应用(DAPP)。通过经济激励机制的引入以及良好的 SDK，水木链可帮助人们迅速设计、开发商业应用。

3.2.1 P2P 贷款企业黑名单分享服务

在市场活动中，各 P2P 贷款企业出于风险控制的需要，迫切想知道贷款用户是否在其他平台具有贷款记录或是否处于黑名单中。这要求各企业能分享部分用户数据。但无论是央行建立的征信数据库，还是各企业组成的征信联盟，企业都不太愿意相信之，因为这些方式都可能导致自己用户数据的泄露。怎样才能做到既不泄露数据，又能达到分享数据的目的？答案就是水木链提供的超导数据交易技术。

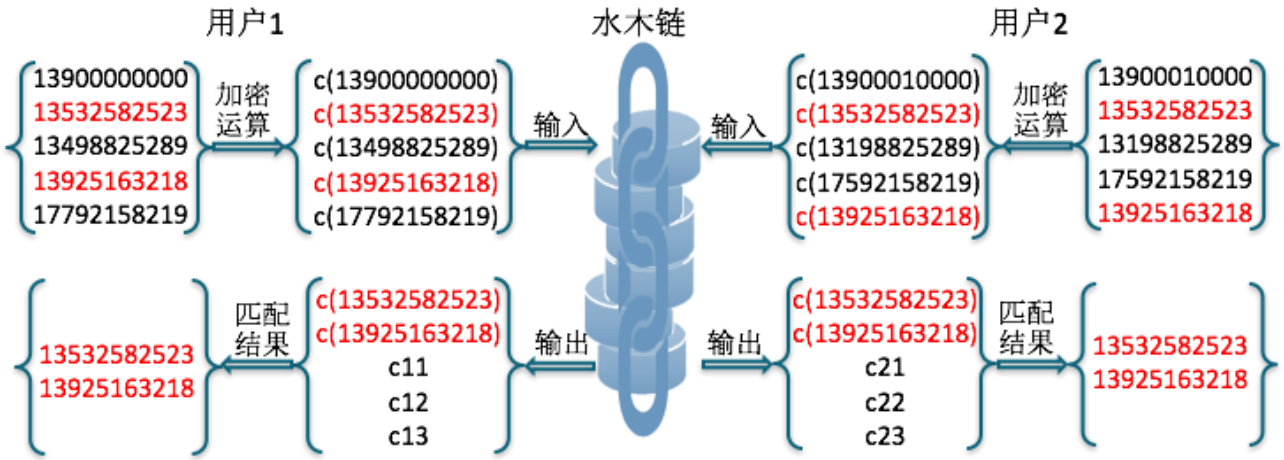

图 3.1 黑名单查询示意图

假设用户 1 拥有的黑名单分别是{13900000000, 13532582523, 13498825289, 13925163218, 17792158219}。用户 2 的一批用户数据是{13900010000, 13532582523, 13198825289, 17592158219, 13925163218}，用户 2 想知道这些用户是否在用户 1 的黑名单中，同时并不愿意泄露所有数据。使用超导数据交易技术完成查询的步骤如下：

a) 用户 1 和用户 2 分别调用服务的加密方法进行非对称加密，同时在本地保留原文与密文的对应关系；

b) 用户 1 和用户 2 分别将密文发送给水木链；

c) 水木链对收到的密文进行多轮运算之后，将中间结果分别输出到用户 1 和用户 2，中间结果包括查询存在的数据对应的密文(图中的 c(13532582523)和 c(13925163218))，以及查询不存在的数据对应的密文(图中的 c11~c23)；

d) 比对 a)中的原文与密文的对应关系，得到存在的数据{13532582523, 13925163218}；而对于查询不存在的数据，其密文是无法解析的，双方都不会泄露这部分数据。

通过上述步骤用户 2 知道 13532582523 和 13925163218 处于用户 1 的黑名单中，用户 1 则知道用户 2 发起了 5 条用户数据的查询，其中 2 条是 13532582523 和 13925163218，剩下的 3 条无法得到原文。

在此模式中，用户 1 根据自己和用户 2 的数据量收取费用，费用均以水木贝进行结算。

3.2.2 数字货币保险箱服务

随着数字货币市场的蓬勃发展，持有数字货币的用户越来越多。数字货币账户具有很高的匿名性和安全性，也正因为此，一旦由于各种原因导致私钥遗失或用户无法操作自己的账户了，就会使得账户中的资产全部损失。这一点与银行账户是不一样的，银行账户无论在法律上还是技术上都有足够的手段找回来。

我们可以搭建一个数字货币保险箱服务，此服务接受有条件的指令，当条件满足时才执行指令。通过智能合约，允许用户指定一个时间点，在此时间点到来之时合约自动将他某个账户中的数字货币转移到其他账户中。在指定时间点到来之前，用户也可以发出取消指令。用户并不需要将数字货币转移到保险箱，只需要将指令提交交给保险箱，并支付足够的 gas。

3.2.3 数字货币抵押贷款服务

数字货币作为一种全新的资产，持有量越来越大，市场对其需求也越来越大。这样一来，基于数字货币的借款业务也会越来越多。数字货币具有非常好的便捷性和安全性，是借款业务中理想的抵押品。机构或个人以水木链为基础设施进行借款，将数字货币抵押在不可篡改的智能合约中，由智能合约完成借款中的利息计算、自动偿付以及违约后的资产处置等。

3.2.4 医疗信息管理服务

现有的医疗 IT 体系中，各医院的信息数据是割裂的、独立的。患者在不同的医院都存有不同的档案，各档案之间的信息完全孤立，A 医院的就诊信息（包括身份特征、疾病情况、治疗方案、用药历史、帐单支付等）对 B 医院完全不可见，从而造成很多医疗资源的浪费。同时，病人的医疗记录和信息都是要求严格保密的，没有一个完善的方案，能够将患者的各项信息数据，安全零风险的进行整合。

通过水木链，可以将医疗数据进行以下几点增强：

统一化：一人一号。每位患者都拥有唯一帐号，所有的历史诊疗信息都存在该帐户当中。

高冗余：多节点备份，防止个人的医疗信息丢失。

无法篡改：医疗数据一旦被篡改，有可能就会造成重大事故。通过区块链的防篡改机制，使得任何更新都会在区块链上留下证据。

权限管理：通过智能合约，对数据访问的权限进行细化，必须获得授权才能访问患者的病患史、用药情况及其他一些个人隐私信息。

通过区块链，使得患者的信息能够跨医院进行流通，从而减少治疗成本，提升痊愈机会。同时，跟医疗相关的支付、保险、科研，由于有了整体的患者信息，也将得到快速的提升。

3.2.5 消费积分管理服务

信用卡积分 、便利店积分、餐馆积分等，目前很多企业都有自己积分的体系，目的不外乎就是为了提高用户对自己品牌的忠诚度，吸引用户多次消费。但是，用户面临着尴尬问题：

1) 积分过于分散，无法聚积到一个体系下，无法换取足够价值的权益。

2) 积分并不是货币，能在商家处兑换的权益非常有限。往往大量的积分，只能换回一些用处不大的商品。

所以积分市场看起来规模很大，其实流动性非常弱，大量堆积在用户的帐号中，成为商家头痛的负债资产。

借助水木链的功能，实现不同商家的积分相互流通、兑换，如图 3.2 所示。用户手中不同商户之间的积分可以在链上自行进行积分间的等比例结算，也可以通过水木币作为中间环节进行兑换，更好的促进积分的流通使用。

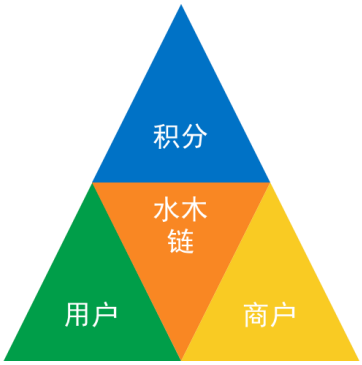

图 3.2 积分流转角色图

3.2.6 用户终端安全

现实当中，每天有成千上万的用户下载安装一些貌似官方的被篡改软件后，突然发现自己的机器（或电脑或手机）中毒了，轻则使得自己的机器运行缓慢、效率低下、出现莫名的广告，重则个人隐私信息泄漏，银行卡被盗用，遭受严重的经济财产损失。究其原因，是由于这些所谓的官方软件，背后被人做了手脚，被一些黑客破解后植入了一些恶意代码，重新打包并以官方软件的方式被用户安装入自己的终端。

借助水木链，可以对所有待下载的软件进行数据哈希计算，并存放到链中。任何用户从第三方网站上下载了软件镜像后，都可以通过水木链比对该软件的哈希是否一致，从而发现该软件镜像是否遭到篡改。

3.2 ICO 方案

3.2.1 水木币 ICO

水木链发行的代币名称为“水木币”，代码为“SMB”。水木币发行总量为 2 亿个，永远不会增发。在水木链上线之前，将以以太坊 ERC20 的形式发行，发行完成之后即可交易。待水木链主网上线之后，参与者按照 1:1 将 ERC20 代币兑换为水木币。

ICO 分配如下：

比例	分配	说明
51%	私募发售 公开发售	用于项目的运营，包括研发、市场、财务、法务等。
25%	创始团队、开发团队以及早期投资人	创始团队、开发团队以及早期投资人在水木链发展过程中做出了技术、人力、财力等方面的贡献，故发放代币作为回报。
24%	商业、学术研究等合作	筛选适合的行业与项目，进行扶持与资助，推动商业落地。

私募发售的代币锁定期为 4 个月，从 ICO 完成之日起算（下同）。

早期投资人持有的代币锁定期为 1 年。

团队持有的代币锁定期满 1 年时解禁 25%，剩余的部分在之后的 3 年按季度线性解禁。

参与 ICO 之前，请确保您了解水木链相关的各种信息以及风险。水木币不是所有权的证明，也不代表控制的权利。团队不对水木币的收益做任何承诺。

参与水木币 ICO 的方法详见官网 https://smchain.io。

3.2.2 基金会治理结构

水木链 ICO 资产由水木链基金会进行管理。水木链基金会（“下称基金会”）注册于新加坡，是一家非营利性的公司。基金会为水木链开源社区筹集、管理数字货币，资助推动项目研发和社区发展的企业、组织或个人。

水木链是基于水木链开源社区的核心项目。项目的技术团队负责水木链交易协议、共识算法、智能合约、官方钱包等功能的研发以及相关技术理论的研究。商业团队负责水木链的市场宣传、产品推广、商业合作伙伴的拓展。运营团队负责人力、行政、法律等日常事务，财务团队负责财务相关事务。

基金会每个月发布一次项目进展报告。每个季度发布一次财务报告。

为了更好地保护参与者的权益，基金会将筹集到的数字货币的 20%作为储备金，在水木币交易市场低迷之时进行公开回购。

基金会将通过微信、QQ、Reddit、Slack、Twitter、网站等方式建立官方的信息发布和交流渠道。

3.2.3 核心团队

刘乐，创始人兼项目负责人

毕业于清华大学计算机系，获得学士和硕士学位。2010 年加入上海证券交易所，2012 年开始研究区块链技术。作为 CTO 于 2015 年联合筹建东吴在线、2016 年联合筹建链石科技。2017 年创立以贝科技，致力于区块链交易协议、共识算法、智能合约等技术的研发，以及区块链在商业领域的落地。刘乐先生具有丰富的创业经验和管理经验。

李中伟，技术负责人

毕业于华中科技大学，获得学士和硕士学位。曾就职于腾讯、思科，多次参与创业。2015 年开始进入区块链领域，对以太坊和石墨烯平台有深入的研究，对区块链体系架构、智能合约、共识算法有较深刻的理解，并成功实施区块链方案到多家银行的基金托管系统。

易强，市场负责人

毕业于湖南大学，获得学士学位。具备 10 年以上用户运营、市场推广经验，曾任达闻营销、大众点评营销总监，服务过大众点评、渣打银行、网易、盛大等大客户，获得广泛好评，也具有丰富的创业经验。

张军，核心工程师

毕业于清华大学计算机系，获得学士和硕士学位。曾长期从事网络安全领域研究，对密码学、密码工程、大规模并发访问有深入研究。长期关注数字货币，具有 2 年以上区块链开发经验。

李阳，核心工程师

毕业于清华大学计算机系，获得学位学位。曾在蚂蚁金服从事支付宝核心交易系统的研发。具有 1 年多区块链开发经验。

沈华虎， 资深工程师

毕业于西安交通大学，获得硕士学位。具有多年软件开发经验，熟悉移动端和后台开发，先后在 HTC、思科、英孚等企业就职，多次创业经验。

马颉， 资深工程师

毕业于中国科学技术大学，获得硕士学位。先后在思科、支付宝、爱奇艺等公司任职，对密码学算法有深入理解，精通架构设计，熟悉主流移动端系统的软件开发。

3.2.4 顾问及投资人

水木链项目从启动到发展的各个阶段中，得到了社会各界的大力支持，在此感谢他们。

田甲

比特基金首席科学家

薛昆

通联数据优矿事业部总经理

陈涛

链石科技首席运营官

3.3 发展路线图

2017 年 3 月开始理论设计，进行概念论证

水木链的起源，来自于给多家银行做区块链的解决方案，当时主要是为了提高单一区块链交易性能和便捷地开发基于智能合约的应用，在这个过程中我们发现了现有区块链在商业应用方面的不足。基于这些经验，我们提出了水木链，在技术和理念上进行了一些创新，融合以太坊通用的智能合约技术，采用 DPOS 共识算法，提供商业友好的区块链应用接口，致力于打造一个商业区块链应用的生态平台。

2017 年 8 月发布白皮书　水木链网站上线，进入 ICO 阶段

经过几个月的准备，我们将概念论证的结果形成了水木链技术白皮书。初期的时候我们将技术白皮书提交至我们的顾问团队及其他业内人士审阅，并获取了许多意见和建议。在这个基础上进行改进后，水木链项目正式公布，发布项目网站并开始进入 ICO 阶段。

2017 年 9 月 ICO 宣传开始 面向特定用户预售代币

水木链启动 ICO 的准备，开始在市场上面宣传和推广水木链，这个阶段开启代币的预售，面向的对象主要是对区块链技术和水木链有一定了解的用户。同时也开始做代币的技术准备，ICO 将通过以太坊 ERC20 代币的方式进行公开销售。

2017 年 10 月正式 ICO 进行代币销售

在经过一个多月的宣传之后，水木链代币将开启代币的销售。参与用户可以通过支持 ERC20 的钱包进行购买，我们也会在合作的众筹平台进行代币的销售。

2017 年 12 月代币开始二级市场交易

水木链将会陆续和主流的交易平台进行合作，登陆交易所进行交易，促进代币在二级市场的流通。对水木链代币感兴趣的用户可以通过各大交易平台的网站和交易所进行操作。

2018 年 Q1 水木链测试网上线

水木链团队将持续推进水木链的开发工作，在实现核心共识 DPOS 算法和可升级智能合约功能之后，水木链的测试网络开始启动，各项开发中的功能将在测试网部署和调试。同时，水木链也会开发源代码到社区，对水木链感兴趣的开发者可以参与进来。

2018 年 Q2 水木链 1.0 上线，实现可升级智能合约功能，水木币 SMB 发行

为了加快水木链的发展，在共识算法稳定测试运行就绪之后，水木链将推出带可升级智能合约功能的 1.0 版本，也会推出水木链钱包应用。持有水木链代币的用户可以通过销毁代币，在水木链的官方钱包应用中获取对应的水木币 SMB。

2018 年 6 月水木链开始合作推广，搭建应用生态

水木链将扩充团队，成立区块链技术研发中心，进行底层研发和商业应用的开发。积极地与各大高校和研究机构进行合作，推广水木链区块链技术，加速商业应用落地。同时，加强与开源社区之间的互动，吸引更多的开发者参与。建立专门的宣传小组，积极参与区块链商业联盟，提高水木链的影响力。

2018 年底水木链 1.5 上线，分布式存储，轻量级客户端，跨链交易

水木链在 2018 年底将实现分布式存储功能，建立起初步的分布式存储网络，支持各种分布式数据应用；也将实现对以太坊跨链交易的支持，用户可以在钱包应用中进行以太坊上的资产和水木链上的资产便捷的交易；发布轻量级客户端，支持主流操作系统。

2019 年 Q2 水木链 2.0 上线，多币种钱包，DAPP 市场，支持多种跨链交易

水木链在 2019 年的主要目标是完善水木链的生态体系，支持更多的分布式应用落地，推出水木链 DAPP 应用市场；实现支持比特币等主流币种的跨链交易，用户在数字钱包中能够便捷操作多种数字资产；持续完善水木链底层技术，研发高级智能合约、虚拟机；推动水木币 SMB 的投融资，与第三方开展合作。

四、 总结

在本文中我们提出了一条为商业应用设计的区块链。自从区块链技术出现以后，在全球范围内出现了推广应用区块链的热潮，但目前也同样面临着许多挑战，传统的公司机构在应用区块链的时候碰到技术改造量大、应用开发难度等问题。水木链设计的目标是降低区块链技术的应用门槛，使得大部分的公司或者机构能够以比较低的代价把对区块链技术引入到现有业务系统的商业应用中去。

我们提出的水木链，是一条支持可升级智能合约的公有链，采用 DPOS 共识算法，低资源消耗，适用于商业应用开发。水木链支持分布式文件存储，满足分布式数据需求。通过水木链可以方便地创建各种开放去中心化、防篡改的 APP，可应用于存证防伪、供应链溯源、物联网、金融交易等多个行业领域。同时，水木链也提出了超导数据交易技术，可以用于行业间用户交换合作的数据，同时不泄露任何隐私，具有广泛的应用前景。我们相信水木链能作为一条基础设施区块链，帮助实现许多行业的分布式商业场景，创建一个更灵活的、去中心化的、多场景需求的区块链应用生态环境。

五、 参考文献

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.
2. Vitalik Buterin. A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper
3. Dr Gravin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. https://ethereum.github.io/yellowpaper/paper.pdf
4. BitShares Wiki: https://bitshares.org/technology/delegated-proof-of-stake-consensus/
5. Solidity Wiki: https://solidity.readthedocs.io/en/latest/
6. Melanie Swan：《区块链：新经济蓝图及导读》
7. BTCRelay: http://btcrelay.org/
8. IPFS. Interplanetary file system. https://ipfs.io/ipfs-p2p-file-system.pdf.
9. Swarm：incentive system for swarm. http://swarm-gateways.net/bzz:/1b5d887cea699d18560ae6dcaf06676f5064f630978b8031d9beb6fbddd82a82/ethersphere/orange-papers/1/sw%5E3.pdf
10. Swarm wiki: https://github.com/ethersphere/go-ethereum/wiki/IPFS-&-SWARM
11. Petar Maymounkov and David Mazieres. Kademlia: A Peer-to-peer Information System Based on the XOR Metric
12. Daniel Larimer. EOS.IO Technical White Paper. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md