Magellan Network

--去中心化跨链网络协议

白皮书

2019.06

目录

1. 背景

1.1 什么是区块链

2008 年 11 月 1 日，一位名为中本聪（Satoshi Nakamoto）的密码朋克在一个秘密讨论群“密码学邮件组”中发表了一篇题为“比特币：点对点现金电子现金支付系统”的署名文章。一次人类历史上最伟大的数字货币实验正式开始。

从此，“比特币”与“区块链”两个概念逐渐进入人们的视野。未来的十年，这两个词将引发一场技术革命和思想革命。但现在，人们认为：嗯，又一个异想天开的疯子。

严格意义上说，区块链的发展并不是随比特币的出现而开始的，区块链也是完全不同于比特币的一个概念。不过比特币的出现把原来鲜有人关注的区块链推到了世人面前。

关于区块链的定义，不同的人从不同角度做出过诠释。从技术的狭义角度定义，区块链特指的是一种数据结构：

“区块链是一种数据结构，即通过哈希指针构建的链表。”

“狭义上讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改、不可伪造的分布式账本。”

不同于一般的数据结构，区块链具有两个标志性的特征：单向

性和唯一性。

单向性是指在区块链上的数据区块排布具有固定顺序，只能单向延伸。这种顺序往往是按照时间进行排列的，因此每块数据都打有时间戳。处于时间序列后部的人仅能沿区块链对之前的数据进行追溯和查找，但无法进行添加或销毁。

唯一性是指区块链上记录的数据与区块链的数据结构一一对应。链接后一区块与前一区块的哈希指针以哈希函数为基础，而哈希函数具有完美的安全特性：隐秘性和约束性，即任意两个不同的输入不会产生相同的输出，通过输出无法反推输入。利用哈希函数的这两个特性，可以使得一个区块链中的哈希指针仅对此区块链中的数据有效，而对其他区块链毫无价值。另外，对数据进行改动会导致之后区块链上所有的哈希指针发生变动。

拥有这两个特征的区块链因此具有了能应用于现实的重要特性：数据不可篡改。任何企图对数据的改动或增减都会导致区块链的数据结构发生改动。只要保证区块链的头部数据不可篡改，全链的数据就是真实可靠的。

1.2 区块链的演进

行业内倾向于把公链划分为三代，依据的是共识机制和实现的功能。以比特币为首的应用于加密货币领域的区块链项目为第一代公链，他们的典型特点是依赖于原始的工作量证明机制。各种加密数字

货币要么在比特币基础上增强了匿名性，要么只是更改了比特币的参数，典型项目包括比特币、莱特币、门罗币、达世币等。这一代公链只能完成交易信息的链上记录，最大的应用就是加密货币，而且往往受到效率低、耗费能源的指责。

以以太坊为首的加入智能合约功能的区块链项目称之为第二代公链，典型项目有以太坊、EOS、NEO、波场等。他们的共同之处在于都将智能合约开发作为重要的公链功能进行开发，而且往往采取新的共识机制，如 POS 权益证明机制、DPOS 授权股权证明机制等。

第三代公链通常是指采用 Casper、DAG、混合共识等更新一代共识机制的区块链项目，如 IOTA、Zilliqa、TrueChain 等。

现在区块链所面临的诸多问题中，区块链之间彼此隔离是区块链技术普及的一个重大阻碍。这就造成了区块链系统的资产被困于自己的系统内，无法产生链间分工和协作。

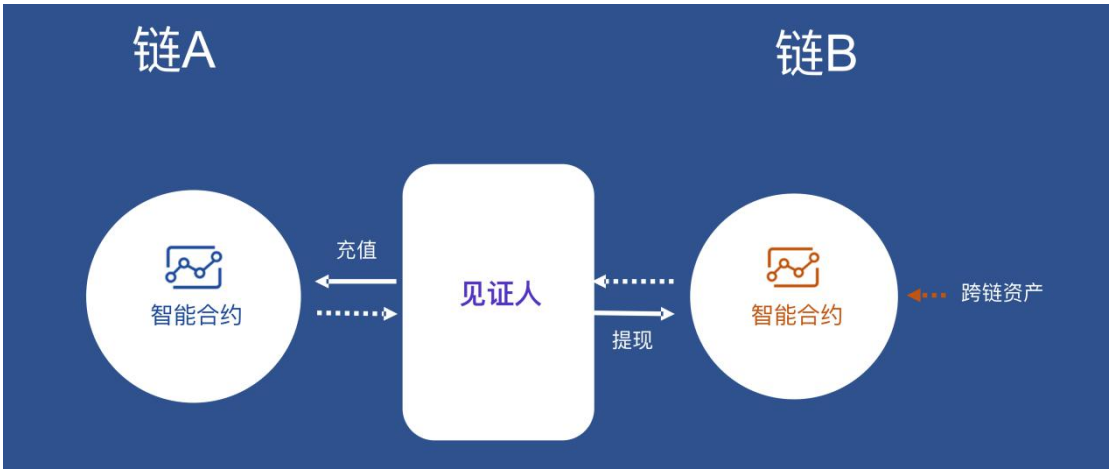
跨链技术作为区块链之间通信的一个桥梁，无论是对于公有链还是私有链来说，都是实现价值互联网的关键，其必要性早已成为大家的共识。既然跨链必须做，那如何做、怎么实现，就成为目前很多项目和学者探索的问题。

2016 年 9 月份，以太坊的创始人 Vitalik 在一份给 R3 提供的跨链技术报告里提出了三种跨链的方案： 公证人模式、侧链中继模式以及哈希锁定模式。这也是最常用的跨链方式：哈希锁定、见证人、侧链中继。

哈希锁定

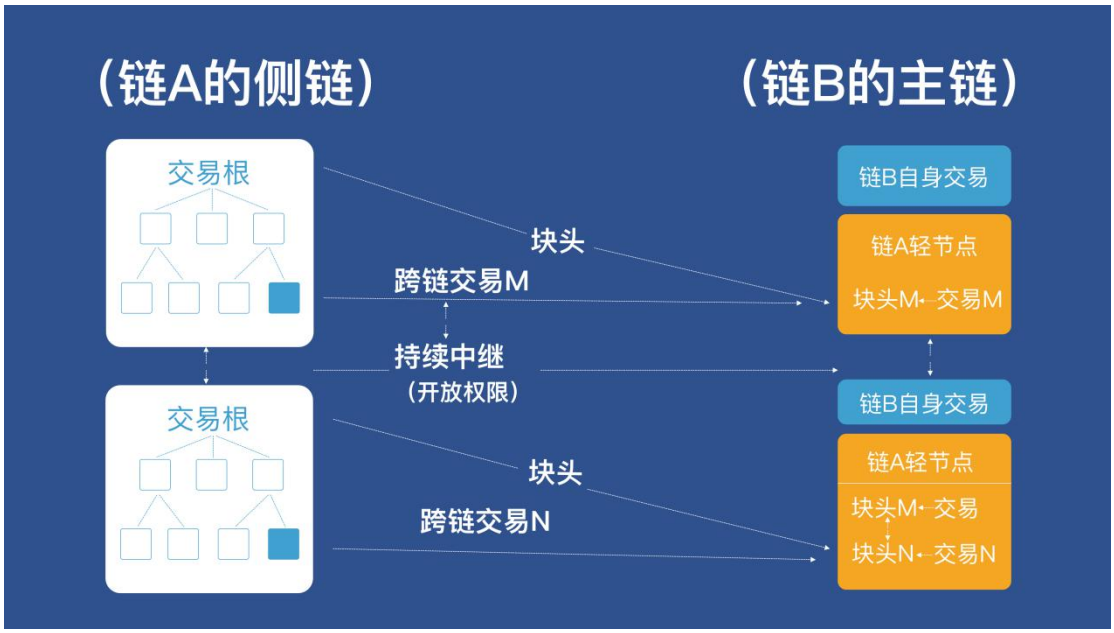
哈希锁定是最简单的跨链方案。AB 双方商定好兑换比例和解锁密码，然后双方就在各自的链上先后锁定资产，再到对方的链上先后解锁资产，所有操作都要在特定的时间窗口内完成，任何一步没有及时完成都会导致交易失败，所以安全起见整个过程可能要持续几个小时。大部分带有跨链、分层、链下扩容标签的项目都是用的这个方法，但是这样的用户体验是非常糟糕的。

见证人



见证人是最易理解的跨链方案。链 A 想知道链 B 上发生的事件，就要指定一些他的用户，让他们把链 B 上发生的事情各自独立地转发过来，这些人就叫见证人。其实就是我们常听说的 Oracle 预言机系统，链 A 以少数服从多数的态度信任转发过来的离散数据。这样链 B 的一个跨链交易需要这些人在链 A 上重复发送，而且要求所有见证人是中心化才做，是可信的，跨链数据无法从数学角度验证。

侧链中继



只有侧链才是最正统的跨链方案。中本聪在设计比特币的时候就设计了轻节点逻辑，任何人不需要知道全链所有的数据，仅获得所有的块头，然后根据交易根验证每个块内发生的交易，甚至还可以验证交易执行过程中的事件和任何账户的最新状态。所以侧链数据的安全性来源就是主链的出块节点，也就是 POW 或 POS 的共识协议，如果没有人可以伪造分叉链，那就没有人可以伪造跨链数据。

2. 概述

Magellan Network 基于侧链中继的方式 ,在链上集成了轻节点功能，实现了去中心化的跨链，而且所有节点均可验证跨链交易的有效性。

Magellan Network 作为 TrueChain 的侧链，采用双向轻节点协议，原生的支持与 TrueChain 的跨链，更加高效且无需信托节点托管。同时，Magellan Network 通过去中心化的方式将链间资产进行统一转化，任何链只要建立与 Magellan Network 的连接，就可以与所有 Magellan Network 连接的链进行资产互通，支持将其他主链上的资产转到 Magellan Network 上面或者转到 TrueChain 或者与 Magellan Network 建立跨链的主链上面。

Magellan Network 的 APOS 机制，根据用户跨链充值的 BTC、TRUE、ETH 等多种数字资产作为权益证明，尽力使节点规模化、平民化，使用 APOS 算法建立起首个可以长期参与共识的区块链网络。

3. Magellan 跨链协议

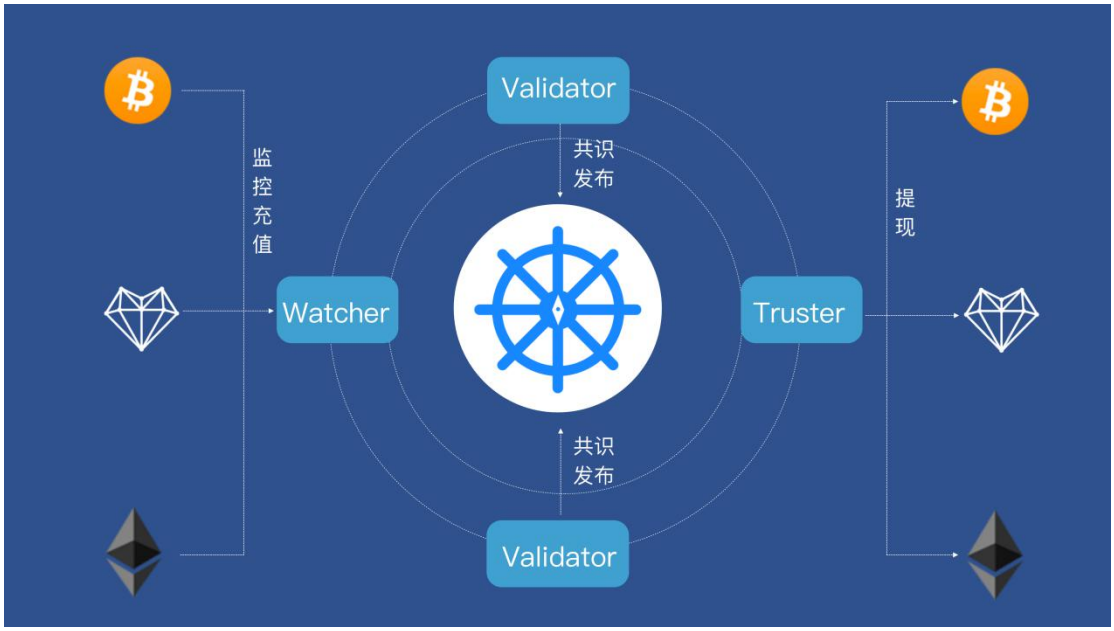
Magellan 跨链协议主要负责主链和侧链也就是 Magellan Network 的协议通信。它要实现把主链资产转移到侧链，在侧链上发币；也要实现把侧链资产回兑到主链。另外，还有很重要的一点就是，在双向锚定过程中保证资产安全。

主要包括角色：

Validator：通过质押跨链资产成为 validator，作为 APOS 委员会成员，负责跨链协议的共识以及链内交易共识处理。Validator 将从主链上转移的资产校验并共识，并在 Magellan 上发币；并对提现申请校验共识，批准资产提现到原有主链。

Trustor：通过质押跨链资产成为 Trustor。Trustor 负责资产从 Magellan Network 转回主链，用于处理已经批准提现资产的回兑交易签名。如果 Trustor 作恶，将由 Valiator 对其做出惩罚。

Watcher：负责监听主链的跨链交易，可适配不同的主链资产，如果有 Validator 或者 Trustor 作恶，也可以进行举报。



具体流程来说，用户要完成一笔跨链交易，首先用户把主链资产发送到主链上的特定地址。

该特定地址是多重签名地址或者多重签名合约，由所有 Trustor 共同管理。多重签名地址、合约的好处是，可以保证资产被安全的锁定在该地址上。根据多签算法而定，当所有或超过 2/3 的 Trustor 签名才能解锁该资产。

一旦用户把主链资产发送到特定地址后，监听链上交易信息的 Watcher 就会监控到该主链交易，然后它会把这笔交易的信息发送到 Magellan Network，信息包括了主链交易的 txid、特定地址的 address、交易金额、Magellan Network 上相应的地址等。

在收到信息之后，Validator 会通过 txid 来验证交易的真实性和

准确性，当所有 Validator 达成共识，确定交易不会被撤销，会在链上保存这笔跨链交易的信息并进行发币。这样完成了资产从主链向侧链转移的过程。

举个例子，代币从 BTC 转移的基本流程：

首先 BTC 链上向特定的多签地址转入一定数量的 BTC，Watcher 节点会监控到该笔跨链交易，当确定交易不会撤销后，会将该笔交易的信息广播给 Validator 节点，所有 Validator 对交易内容进行校验，如果校验通过，会将该跨链交易上链，并释放相应代币。

如果用户想把自己的资产从 Magellan Network 转移到主链呢？

用户首先需要在 Magellan Network 发起回兑请求。发起回兑请求之后，Watcher 把监控到的信息发送给 Validator，Validator 验证该交易是否真实和准确，通过 POS 委员会来达成共识。如果共识达成，则 Trustor 会发起主链交易，解锁用户的部分代币。同时，validator 会在链上保存相关信息。

举个例子，从 Magellan Network 把代币回兑到 BTC 的基本操作：

> *首先在 Magellan Network 合约发起赎回交易上进行代币燃烧，watcher 监控相应赎回交易，并通知 Validator。Validator 校验该交易并达成共识，如果通过则通知 Trustor 节点，Trustor 创建释放 BTC 交易并收集其余 Trustor 对该交易的签名，如果签名足够，则发送交易到 BTC 链，转移 BTC 到用户。*

Magellan 协议要求跨链的主链能够支持多重签名的地址或合约。比如 TRUE、ETH 通过智能合约可以实现多签合约的支持，而 BTC、BCH 等链是原生支持多签签名地址。

多签地址或者合约由 Trustor 节点进行管理，Truestor 节点也会进行换届。每一届 Trustor 会生成多签地址或更新合约，每次换届后，对于多签地址，老地址的资金会转入新地址，而对于多签合约，则将多签合约的签名者更新为新的 Trustor。Trustor 需要质押资产，其资产由 Validator 进行管理，并对作恶的 Trustor 进行惩罚。

用户可以实时查看系统的跨链资产发行和储备量，没有任何节点可以单方挪用。

总的来说，就是在主链上锁定一定数量的代币，然后根据锁定代币在侧链发行新的代币。反过来，就是侧链上进行回兑，销毁一定数量代币后，在主链上解锁相应数量的代币。主链和 TRUE 通过去 Magellan Network 实现双向锚定。

4. 共识算法 APOS

Magellan Network 采用新型的委托资产权益证明（APOS）模式进行 validator 的选举。APOS 通过质押的模式进行 validator 选举，但是质押的不是本币，而是跨链资产。

现有 POS 和 DPOS 模式都是通过质押本链币进行权益证明，但是通常初始账户拥有大量 stake，对小额持币者很不友好。APOS 模式使用跨链资产进行质押，保证了足够去中心化与公平。

Magellan Network 的整个模型分为 2 个阶段：

1. 在 Magellan Network 运行的初始阶段，需要质押跨链资产 TRUE、BTC 等作为资产证明。节点需要质押一定量的跨链资产才能作为 Validator 参与共识出块。同时其他用户也可以通过质押跨链资产并委托给 Validator 参与共识，同时分享参与共识的收益与损失。

2. 在 Magellan Network 平稳运行到一定阶段后，通过链上投票，启动质押 Magellan Network 本币 VICT 作权益证明，即同时支持跨链资产和本币的质押。链外资产和 VICT 的质押按照一定比例进行折算。如果在运行过程中资产价值发生变化，可以通过链上投票，更新折算比例。

5. 技术特点

去中心化跨链实现

Magellan Network 通过侧链中继方式，在链上轻节点方式实现跨链交易的校验，通过 APOS+PBFT 方式实现跨链共识，并通过 PBFT 实现跨链资产的释放，实现了真正的去中心化的跨链交易。

高效的 WASM 虚拟机

Magellan Network 支持智能合约，使用 WASM 作为虚拟机。WebAssembly，简称 WASM，是一种以安全有效的方式运行可移植程序的新技术。WASM 具有性能高效、存储成本低、多种语言支持的有点，基于 WASM 虚拟机合约功能会更加高效、方便。未来跨链轻节点的实现也会基于 WASM 实现。

安全的随机数模型

在链上合约运行过程中，随机数的随机性关系到很多服务和游戏的公平性，但是目前区块链还没有很好的方式提供安全的随机数。

一些区块链依赖区块哈希（block hash）来产生随机性。因为区块哈希值不可预知、随机性很强，但在所有节点上都是相同的。然而，如果区块奖励少于矿工操纵区块哈希所能获得的奖励，那对他们来说，操纵哈希值在经济上是完全理性的。更严重的是，在权益证明

（PoS）系统中，由于生成一个区块几乎不需要计算时间或能量，矿工（验证者）可以很容易地连续生成数千个区块，直到获得一个他们喜欢的哈希值，然后提交这个哈希值。

在 Magellan Network 当中，validator 在共识出块过程时，会首先有多个 validator 广播一个随机数的 hash，等出块时再将这些随机数拼成一个完整的随机数，保证了随机数的安全。

链上治理

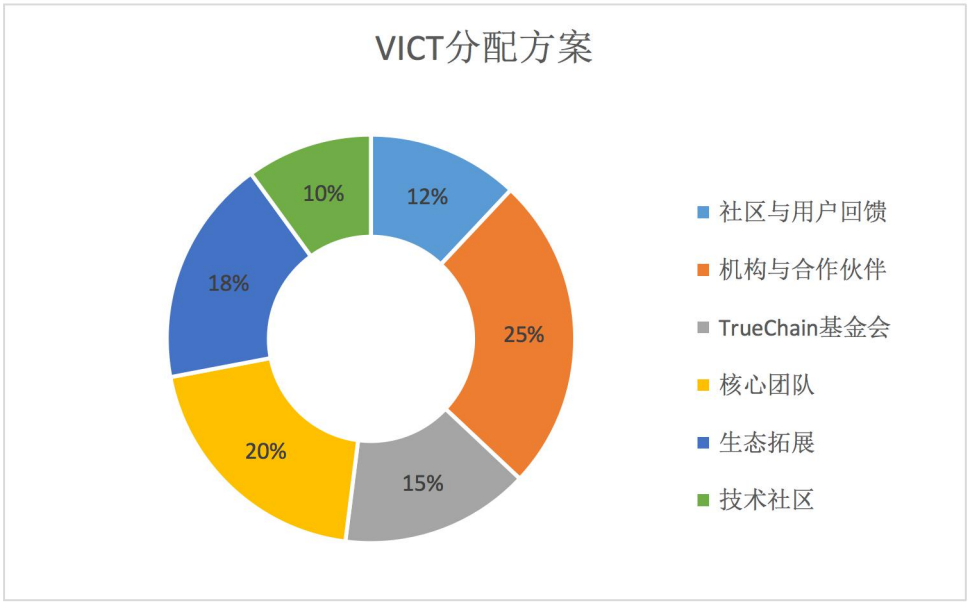
区块链治理是一个各方面相互协调的过程。目前的治理方式主要有两种：链下治理和链上治理。与链下治理相比，链上治理的规则是嵌入到区块链协议层里的，对于谁参与治理，怎么参与，怎么实施，都有着明确的定义和裁定。

Magellan Network 采用链上治理的方式，所有协议改动必须通过全民公投，拥有更多投票的人将拥有更多话语权。每个治理流程经过提案、公投和计票实施，如果提案得到了足够多的支持，就会按照机制实施提案。

6. 激励模型

为了纪念麦哲伦大航海航行中的“维多利亚号”探险船，Magellan Network 上发现的币为 Victoria，缩写为 VICT，初始发行 100 亿枚。分配方式如下：

- 社区与用户回馈 12%
- 机构与合作伙伴 25%
- TrueChain 基金会 15%
- 核心团队 20%
- 生态拓展 18%
- 技术社区 10%



7. 应用生态

资产跨链

Magellan Network 作为 TrueChain 的侧链，通过侧链中继方式为 TrueChain 提供了跨链服务，同时整合了多链资产，使它们可以享受同等的智能合约服务。最简单的就是扩充了 BTC、ETH 等的应用能力，在原有链上只能进行每秒几笔到十几笔的转账操作，但映射到 Magellan Network 后，可以提升了交易吞吐量和响应速度，还极大的降低了交易成本，并且能够发挥基础货币的优势，参与到多种 DApp 服务内。

跨链相关 DApp

Magellan Network 基于新一代通用 WASM 智能合约技术，可以开发部署各类 Dapp。开发者可以使用任何能够编译成 WASM 的语言进行开发，可以开发部署各类 DApp，尤其是跨链相关应用，比如稳定币与去中心化交易所应用。

更多经济模型和应用场景

在 Magellan Network 广泛的跨链支持和强大的合约等完善技术生态支持下，社区开发者后续开发的各类应用可以自由设计经济模型和应用场景。比如以 BTC 或者一系列数字资产为抵押的稳定币，以 ZCASH、GRIN 等为媒介的隐私支付系统，以及各类游戏或高阶金融衍生品服务等。

8. 项目路线图

2019.Q4 主网上线,支持 TrueChain 的跨链

--主网上线，支持与 TrueChain 的跨链，并使用 TRUE 以及 TrueChain 上面的稳定币作为跨链资产实现 APOS。

2020.Q2 支持 BTC、ETH 资产跨链

--支持 BTC、ETH 资产跨链，并通过链上投票，启动 VICT 作为权益证明。

2020.Q4 完成与 Cosmos 和 Polkadot 生态对接

--完成与 Cosmos 和 Polkadot 的对接,打通主要跨链生态。

2021.Q2 链上资产撮合交易协议

-- 开展链上资产撮合交易协议的开发以及更多生态应用。