OmiseGO

去中心化交易和支付平台

Joseph Poon OmiseGO Team

joseph@lightning.network omg@omise.co

2017 年 6 月 17 日

摘要

OmiseGO 正在搭建一个具备去中心化交易、流动性提供机制、清算信息网络和资产支持的区块链网关。OmiseGO 不属于任何一方。相反，它是一个开放的分布式验证节点网络，网络内的验证节点将约束所有参与者的行为。它使用协议代币机制来创建股权证明区块链，以便在参与者之间实现市场活动。这个高性能的分布式网络允许不同资产类别间的交易——无论是由法币支撑的发行方，还是完全去中心化的区块链代币（ERC-20 类别以及本地化的加密数字货币）。跟几乎所有其他去中心化交易平台不同，该分布式网络在无需可信任的网关代币的前提下，允许不同区块链间直接进行去中心化交易。此外，市场利差将显著下降，并通过去中心化监管以及市场活动透明度的提高来鼓励市场保障。上述过程通过使用智能合约以及协议代币保证委托交易账本配对的正确性。这是使用以太坊担保清算活动以及通过使用以太坊智能合约来保证历史交易数据的新结构。

1 介绍及问题阐述

区块链的主要作用是解决网络参与者间的多边协议之间的协调问题。通过确保透明度，保障以及执行，我们可以有效达成多方共识，而这在以前是不可能实现的。当网络内参与各方发现业务不仅透明化，而且运行机制无法轻易改变，那么它们会更愿意进行协调。参与者显然更能确保，任意一方很难通过改变业务流程或利用信息不对称来强行收取暴利益租金。换句话说，任何单个参与者都更乐意使用业务流程和机制本身不属于任何其他单个参与者所拥有的系统。

支付处理商，网关和金融机构之间存在着基本的协调问题。例如，银行的客户希望在另一个网络上支付商家。过去，建设一个在支付网络和机构之间兼容的支付系统是一项浩大的工程。

这个过程通常是通过建立一个管理交易的交换所，即使用与中央交易对手清算中心或者银行往来帐户的通信网络，例如 FedWire，CHIPS，SWIFT，消费者银行卡支付网络，NSCC / DTCC，OCC 和 ACH。这些网络服务于不同的角色和功能，包括本地/国家支付，国际支付，信贷，股票/资产交割和衍生工具。这些中心化网络允许控制实体随意更改机制，在信息成本，尽职调查和所有各方之间的合同执行的过程中导致交易成本大幅度上升。

我们认为，目前使用新型支付平台来颠覆数字支付存在着广阔的新兴市场（例如 Venmo，支付宝等）。这些网络对于跨网络的交易具有重大的意义，因为它们通常需要承担显著的与交换设施相互信任的间接成本。缔约方不愿意使用中央交易对手，因为任何一方都不希望听从对方，并且使用银行往来帐户需要参与者之间制定合约。虽然较大的网络有足够的动力保护自身的网络影响，但我们相信大多数机构都希望能够提供电子钱包服务，并且这些服务需要多方参与者之间进行更多的协调。这些中等规模的参与者将能够实现网际价值交换，以便在可用性方面有足够的网络影响。这些基础设施和参考前端使网络效应被编码到这个网络中，使得新的电子钱包用户可以立即创建高级网络设施。

区块链允许社会将全世界的业务流程从单中心公司转化为开放的、去中心化的计算网络。[1][2] OmiseGO（OMG）是一个将市场流动性，交易委托账本配对执行、清算中心保管以及可扩展支付去中心化的网络。这将有助于解决新兴电子钱包支付网络间进行支付的问题。

通过将这些传统上放在一个单一公司中的商业流程进行转化，我们有可能在一个高性能的开放网络中为电子钱包提供商提供一个完全的交换方法。

2 设计方法

最终状态要求是拥有法币价值的电子钱包平台去中心化机制的一个架构。电子钱包代币将能够在去中心化、公共的以太坊[3][4]区块链上使用以太币（或者其它去中心化加密数字货币）作为交换媒介以达到最大效率。我们相信这将为去中心化加密数字货币赋予更多的价值和使用意义，因为它为许多电子钱包平台提供了用处。

由于该网络的一个核心功能是实现电子钱包间的交易。OmiseGO 必须拥有

一个区块链账本，以保持每个电子钱包服务（或任何用户/节点）的总体资金余额。这个账本必须能够跨多类资产/商品记录资金。但是，仅仅拿着一个账本对于交换来说是不够的。这种机制还必须允许这些资产/商品进行交易。

为了进行交换，它需要在公开公共市场上的交易者间放置一个命令。这需要一个去中心化的交易委托账本和交易引擎。这个交易引擎内置于OMG区块链中。当匹配的订单获得了大多数验证节点的确认，订单将被发布并进行匹配。该流程将作为每个区块的一部分来执行。这产生了一个单方拥有的非监管的去中心化交易，其中，此电子钱包平台可以在无需信任某一中心化实体的前提下，与其他电子钱包平台进行交易。

然而，直接进行电子钱包代币交换并不可取的，因为这会很复杂。在没有单一偏好的情况下，我们有必要在流动市场使用加密数字货币。通过将以太坊与智能合约[5]绑定（或将类比特币代币绑定清算中心），我们可以将以太币锁定到OMG 区块链的活动上，以便基于以太坊或其他加密货币的电子钱包创建一个流动市场（如果每一对都与 ETH 进行交叉，在低货币波动的情况下，差价将小得多）。对于需要非常小的差价的活动，可能会出现一些电子钱包代币将被用作交叉；然而，由于程序裁决相关的协调和信任优势，我们有必要使用去中心化代币，如果有必要，也可以使用其他电子钱包代币。但为了不影响短期的智能合约交易率浮动比率，我们主要使用 ETH（例如 HTLC 清算所，流动性供应和 OMG 链执行）。通过允许加密数字货币支撑电子钱包平台，所有电子钱包间的交易活动
都是公平的。

这意味着锁定的资金需要更大的流动性，而对于低价值的交易活动（例如大量的小额支付），OmiseGO 去中心化交易可能不太可取。

两个不同电子钱包之间的每一笔付款不是必须使用去中心化交易来执行。我们可以设想，电子钱包将储备一些其他电子钱包的代币，用于流行方向的小额转帐。诸如闪电网络等架构允许在电子钱包记录余额以促进快速支付的前提下发生链下支付。我们允许跨比特币[7]和以太坊[8]付款，因为这些过程都可以轻松地移植到 OMG 链上，对电子钱包余额进行记录。

借助去中心化交易，加密数字货币（例如 ETH）匹配，交易委托账本和没有全面监管的清算所的信任，OmiseGO 区块链架构允许电子钱包间进行交换。

2.1 基于去中心化流动中心通道

这个结构还有一个额外的好处，那就是允许一个去中心化的流动资金池被用于各种加密货币的支付通道，比如比特币（某种程度上，以太坊也可以）。

对于区块链上单独的代币支付而言，我们有必要在不影响基础链的前提下，扩展底层的区块链活动，以减少验证/挖掘节点的计算压力。因此，使用闪电网络是必须的（或者使用闪电网络通道的类似架构）。然而，闪电网络面临着对资本的网络效应的巨大压力，因此我们希望避免流动资金池集中到单一可信赖的实体手中。通过使用与去中心化清算所相同的机制，我们可以创建一个闪电网络中心，该中心不属于任何单一个体，并且支持更复杂的智能合约（例如，以太坊，ERC-20 的代币等）。对于具有简单智能合约的货币，网络中的任何节点（例如比特币网络）都可以作为进入 OMG 链池的网关，并与任何其他参与者交叉。这将大幅减少 OmiseGO 链的许多在线活动，同时也鼓励去中心化。

我们认为可以通过利用确定性/已知的一致性规则来将利益链条去中心化的方式来减轻流动性集中的自然网络效应。

特别是对于以太坊（以及其他拥有全功能的智能合约脚本的区块链）而言，所有参与者都将通道设置为一个行使单一资金池功能的 ETH 智能合约。 OMG 链的链状态反映了参与方当前的余额。这将允许任何参与者在此网络上提供流动性，这些流动性可以根据 OMG 链共识规则来进行分配（如果这个结构在健壮的测试/验证之前已经成功，那么早期我们会添加一些限制以防止区块链从加密数字货币处吸收所有的剩余流动性）。因此，这些资金可用于 OMG 链上的任何流动性活动。

3 区块链概述和机制

上述机制需要大量的活动（和大量的状态数），而且在这个时候并不适合让所有的活动都发生在以太坊主链上，但是，这个结构将把交易活动绑定在公共以太坊链上，其中，合约执行的输入由 OMG 链提供。

我们正在建立一个挂钩到其他区块链来进行跨代币/资产类别的交易。这个过程主要由以太币来支持。从任何单一链条的角度来看，我们正在建立一个可扩展的区块链，其合约状态由 OMG 链本身的活动绑定。其他链条的活动可以通过类似与 BTC 中继[9]的形式以跨链提交证明的形式进行链间连接，这个过程可以

提交到以太坊处。OMG 链验证了该活动所有参与者的行为（包括其他链条上的活动）。换句话说，OMG 代币的作用是提供计算和执行。代币本身作为其在该区块链上的活动的保证金，不正确的活动将导致代币/保证金在 OMG 链上销毁。通过创建一个具有深度执行力的定制链，我们可以构建一个系统，在这个系统中，其共识规则对于高性能活动是最优的。

该设计优化了快速执行和清算，但是结算速度会较慢。未来的迭代可能包括 OMG 链的分片技术，但是对于初始迭代，我们将假设具备高吞吐的区块传播量。

拥有 OMG 代币，实际上是依照协商一致的规则，购买验证此区块链的权利。交易费用，包括（但不限于）用于支付，交换，清算和结算所的资金，将给予无故障的验证节点执行保证金抵押的合约状态。

这些代币将根据从网络中导出的费用获取价值，也意味着承担向链上用户提供验证的义务和成本。这些代币必须具有价值以防止低成本攻击，并且对于推动网络的执行时非常必要的。

在我们的路线图上，我们可能允许将验证授权委托给第三方，而在需要重新授权之前，每一次可以减少有限的数量（该安全模型的完整机制尚未确定）。

因为这将被设计为一个高性能的系统，因此我们需要一条证明连接区块链。我们期望这个系统能够处理大量的交易，这样我们只要把最终的结果传输到以太坊就可以了。清算和结算都在 OmiseGO 区块链上发生。共识规则将通过股权证明网络执行。作为网络共识规则的一部分，我们要求所有 OMG（Omise GO）验证节点也同时运行以太坊网络来并行验证，从而使以太坊成为区块链间验证的首要保障。

我们同时假设存在如以太坊/ ERC-20 来进行担保或者退款的机制，BLS 签名方案（或 Schnorr）将在不久的将来用于以太坊。对于加密数字货币，这些代币是非监管的，而是锁定在智能合约中（不像其他交换平台，比如 Ripple，需要可信的网关来代表底层）。它也不依赖于所谓的集中验证集合（例如 Ripple）。

OMG 区块链负责管理在以太坊上的执行顺序的匹配和管理执行。OMG 上的活动确保验证节点的活动也可以通过本地以太坊智能合约在以太坊区块链上执行。对于比特币和类比特币系统，我们允许通过闪电网络上的清算网络来进行交易。区块链通过提交证明在该网络上执行活动。虽然不如以太坊网络那么强大，

但它允许在无需全节点验证的情况下协调OMG链上的几近即时的清算和结算活动。为了安全性，我们期望在未来让不允许区块链重组的节点进行部分验证，支持重组的区块链上的简单的 SPV 验证不允许在此网络中执行。

共识机制和安全属性的详细描述请见 Exonumia Labs 的 Joseph Poon 即将在 2017 年夏季发表的（目前正在撰写）的论文。论文的创作（以及随后由 OmiseGO 使用的实现方式）可能对未来的许多开源代币协议区块链项目有用，并且可能为新链提供新颖的构建比如为分布式数据处理以及区块内金融活动创建激励机制。我们希望 OmiseGO 及其分布式交易，在帮助提供基础技术/基础设施的过程中，能起引导及核心作用，这些基础技术/基础设施可以引发和构建整个协议代币生态系统。 OmiseGO 的初始版本可能会使用 Tendermint 共识的一些内容。

3.1 轻客户端验证

虽然 OmiseGO 被构建为能够处理许多交易的高性能网络，但是有必要为部分验证以及外部智能合约的执行提供轻客户端证明。

每个区块所提交的交易的 merkle 树以及最近交易状态将被包括。任何节点可以通过下载最近的区块状态提交数据和这段时间的任何区块来获取当前状态。

由于最近的区块状态包括最新状态的树，客户无需下载整个链条就可以得到查看最近的提交数据。请注意，我们必须有足够的经济激励措施来阻抗重放和停机攻击；OMG 链设计为以保证金形式阻止区块重组，但不提供围绕区块确认需求的保证。与目前的 SPV Bitcoin 验证实现类似，在审查风险方面，我们需要给予全节点一定的信任。从交易量角度来考虑，我们不认为已提交的布隆地图可以满足去中心化交易。轻客户端可以验证到有效数量的验证节点已经处理了交易。此外，它还可以从全节点获取任何部分数据。由于 OMG 链智能合约的结构，我们推荐客户端同时验证以太坊链上的活动。

4 电子钱包

虽然 OmiseGO 支持付款，但它并不是只能作为在特定电子支付提供商（EPP）之间的支付处理商。我们认为一个 EPP 不存在协调一致的问题，协调问题主要存在于 EPP 之间。然而，由于 EPP 之间交易的需要，支付活动可以通过区块链进行。该区块链允许 EPP 在 OmiseGO 上进行代币发行。这个过程不仅支持平台上由法币支撑的法定数字货币，也支持其它的资产类别（如顾客积分）。OmiseGO 是一个允许任何人发行资产的开放系统，但由个人用户（或代表用户的 EPP）来

确保正确的发行/审计。这是通过创建附加到允许发行的脚本（使用私钥）来实现的。一种替代方法是在以太坊上发行ERC-20代币，把它们锁定在智能合约中，并在OmiseGO链上管理，就跟现在大家在OmiseGO链上对现有的ERC-20代币（REP，GNT等）进行管理一样。

在默认配置中，我们假定为了便于使用，EPP将代表用户直接保管资金。这跟现在的许多全担保钱包（比如Coinbase）或者其它中心化交易一样。这将允许EPP在自己的网络中进行零费用交易，因为这并不构成区块链活动。然而，用户也可以直接在EPP退款或者在OmiseGO链上交易它们发行的代币（比如法币）。不过如果这笔交易不是在 EPP 的链上担保账户发生的话，那么可能会产生链上交易费用。这样的话，我们就能够支持去中心化传输，同时满足一部分 EPP 的需要，因为它们可以在自己的网络上实现零费用交易。EPP可能提供一个类似于托管加密货币钱包的中心化软件，这将大量减少部署时间，只有跨网络的支付会有EPP基础设施托管。第三方在未来可能会开发出一个可以在链上记录EPP余额的去中心化钱包。

通过将电子钱包打造成区块链的一部分，我们可以在OmiseGO上直接使用去中心化货币以及协议代币与由法币支撑的代币进行交易。

4.1 电子钱包合规性

传输限定将要求代币发行方按照发行政策以证书形式来发行代币（并非去中心化货币）。EPP在对证书签名之前可能需要验证KYC，一些限定包括只能向证书持有者传输的限制以及流量控制（单一账户传输的流量限制以及某次特定代币发行的最大账户余额）。这些规则不适用于无需遵从这些约束条件的代币，也不适用于去中心化货币。EPP有责任保证它们发行的代币是否获得许可以及是否合规。

5 去中心化交易

电子钱包间交易平台的核心是去中心化交易。这不仅支持了EPP发行代币，也支持了去中心化货币间的交易。

对于电子钱包间交易而言，去中心化交易是最理想的。因为他们有不同的底层价值体现，即使在相同的底层中进行交易，也有可能会有不同的交易对手风险和成本。电子钱包A不同于电子钱包B，即使它们的支撑结构是相同的。因此，

要实现正确的市场操作，一个流动性的市场是非常必要的（即使汇率差非常小）。

去中心化交易一开始会使用一个批量拍卖结构，每一个回合都会进行交易匹配。当然，也有可能买入某一个特定的回合（区块高度）或者每一个回合留下一个开放的订单，直到该订单被填充。批量拍卖允许订单被放置，并且在特定间隔时间一次执行。这种结构允许在去中心化网络中提供更高的保证和性能。订单可能会留在交易委托账本上，但执行速度可以快到足以与 EMV 银行卡终端相媲美（需要更多与共识机制相关的研究）。如果特定用例遇到不便之处，则 EPP 负责记录希望支持快速交易的其他 EPP 的余额（可能会收取较高的利差）。这种形式可用于小型日常采购，而较大价值的购买活动将通过去中心化交易进行。

尽管我们希望能够进行低时延、高频次的执行，但是在去中心化网络中存在这样的障碍。单点执行是命令匹配的一个必要功能。如果没有执行单一“引擎”的命令，那么这个网络内的单个对象就有可能遭受女巫攻击。如果某个节点在很多地方同时执行同一个命令，那么就没有发生真正的订单承诺。我们可以很容易地对网络进行女巫攻击并假装自我执行。此外，由于存在不可信任的执行场所，我们不可能在智能合约创建外部使用的代码，而这恰恰是这个网络的必要功能。该网络的目的是设计成为卓越的高价值交易和结算平台（而不是大量低价值网络）。

另一个低延迟快速执行的替代方案是引入外部中心化场所。然而，这将引起对单个实体执行信任的问题。随着交易流动性自然趋于中心化（远远高于支付中心化），那么就会存在重大的信任/协调问题，最终看起来就像现在的加密数字货币交易（唯一的区别在于它是非监管的）。然而，这种结构并没有解决参与者并不想在单一受信任的供应商进行交易的重大协调问题。OmiseGO 去中心化交易的目标是拥有透明的、已知的执行行为。我们认为，受信任的非监管执行是作为去中心化执行引擎的补充的一个可信的选择，OmiseGO 可能会在未来很好地支持这些平台。成熟的去中心化交易在一个非监管的信任执行环境中，有益于将其用作智能合约的去中心化预言机。

这种去中心化交易是按高性能设计的，其中订单在股权证明网络上进行传播。当足够数量的参与者拥有区块确认的顺序，那么订单将被置于交易委托账本上。特定批处理点的订单是所有订单的运行计数，在批处理执行点之前不执行（所以

在账本中订单是相匹配的）。最初的配置包括透明的订单，但是可以做一个类似虚线框架的结构，在这个架构中，订单是盲目放置的，然后不再接受订单。发出订单的参与者负责生成盲钥匙，并在一定时间后执行。初始版本将使用完全透明的系统（批处理执行格式会有效减轻部分敌对行为）。

最终，交易都将在单个“引擎”上执行，即股权交易去中心化交易，但确保执行规则是透明和可行的。

5.1 以太坊交易

考虑到效率和安全问题，OMG 需要对以太坊公共链上进行全节点验证。我们可以在以太坊区块链上创建一个合约，该合约锁定了由 OMG 链条件决定的资金。这些资金现在已经被捆绑和锁定，其活动由 OMG 链执行。当订单执行时，系统会提供一个证明来解锁以太坊那边的资金。

这种结构假设 Schnorr 或 BLS 签名未来可用于以太坊。交易跟踪 OMG 链的活动，并且在传递到以太坊链上付款之前满足达成一定程度的成熟度约束。资金仍然可以在 OMG 上结算，并持续更新余额。只有在以太坊上进行支付时，才进行最终的传输。OMG 链强制执行以太坊链上的支付行为。在非对抗环境中，我们可以使用类似闪电的结构，用户可以直接提供付款而无需证明。如果付款在一定的区块成熟度后没有争议，则不需要区块证明/计算。
如果支付行为与 OMG 链中的状态不匹配，那么任何人都可以提供证明，发送方的余额将被削减。通过这种方式，以太坊链的算力和带宽效率得到显著提高。

这个 OMG 链上的结构适用于以太坊、类以太坊链以及使用担保智能合约的满足 ERC-20 的以太坊发行代币的交易。

5.2 与其它产品的对比

交易是金融活动的一个基本方面。毫无疑问，一定有人尝试用不同的方式来搭建加密数字货币交易结构。

中心化全监管加密数字货币交易（如 Poloniex）性能极高，但也依靠对单一方的信任来负责任地进行监管，并诚实地执行订单。

像 Ripple（XRP）这样的网络依靠所谓的可信任的验证节点来达成共识，这个博弈理论上聚集在一个不变的集合上。此外，Ripple 的交易功能依赖于在自己的平台上交易发行的资产（与监管选择有关的重大问题）。如果不创建发行网关，

以太币及比特币的去中心化交易是不能实现的。

许多使用 EVM 智能合约的去中心化交易平台主要依赖于两种方式：要么直接在链上执行任务（这迫使以太坊网络上的所有东西都不支持跨区块活动），或者他们在没有单一执行工具的前提下链下执行任务。OMG 链正是为执行跨链（比如 ETH-BTC）交易而设计的。在整个交易过程中，我们无需为使用基于本链加密数字货币的全监管发行资产。

5.3 比特币清算中心

另一方面，对于比特币和类比特币系统而言，我们可以创建一种系统。在这个系统中，我们可以将资产从外部与清算中心系统绑定在一起，由此实现 BTC 和其它类似的区块链进行交易。

本质上，这种结构是将清算中心作为一个预言机运行[10]，其中的活动都绑定在 OMG 链上并由 OMG 链负责执行，以实现与类比特币区块链的去中心化交易。上述流程参照了 Tier Nolan [11]在基于外部交易执行工具进行快速去中心化交易的研究。

清算中心用于确保支付发生在比特币区块链上。我们使用清算中心而不是 SPV 证明，是为了防止由比特币矿工产生的不符合共识但 SPV 证明有效的区块来攻击外部系统的对抗性激励（对自己的链条进行重组攻击的成本是昂贵的，但外部攻击比较便宜）。

对于类比特币系统，该系统要么需要进行可延展性修复（例如隔离见证），要么是仅在透明地址上可用的 P2SH / BIP-66 / CLTV / CSV 组合。

清算中心是必需的。因为目前不可能在比特币上执行复杂的合约状态。这些清算中心负责通过生成原像和哈希值来披露比特币（或类比特币）的链上活动。这些哈希值将被提交至清算中心所负责的活动，并进行绑定。如果他们释放不正确的原像，或拒绝透露 OMG 链的原像，任何人都可以提供渎职证据，此时，清算中心将会被削减。

需要注意的是，这要求清算中心既要有比特币资金储备，也要有可用于在 OMG 链上进行绑定的资金。至于保证金，其数额只能存留到资金可以在比特币上进行清算和结算，所以理想情况下不需要极高数额的资金。

清算中心运营着一个闪电通道，但他们不仅在通道中拥有自己的资金，还有

预期在 OMG 链上流动的资金的数倍金额的 ETH 储备（例如，3 倍预期流动资金以应对汇率浮动）。

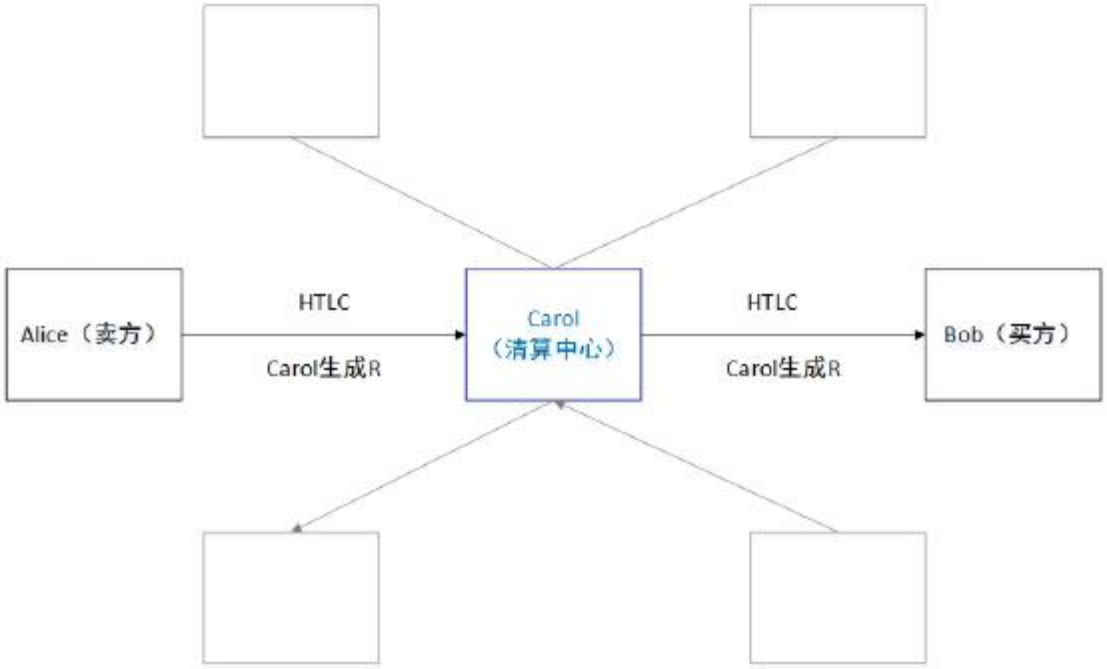

图 **1**：Alice 和 Bob 有一个闪电网络通道与 Carol，即区块链上的清算中心相连。支付原像 R 由 Carol 生成，并且原像的释放由 OmiseGO 链上的绑定承诺来执行。

假设 Alice 希望出售比特币，而 Bob 希望购买比特币，他们都有向 Carol 清算中心开放的通道。这三者都在 OMG 链上，并指定Carol 为可接受的清算中介。请注意，如果双方均指定某一清算中心为可接受，则可能会在多个清算中心之间进行转账，而且交易只能在交易参与者指定可接受的清算中心的交集中进行。

Carol 这一清算中心根据 OMG 链以及智能合约中的共识规则将以太坊上的资金锁定在智能合约中。Carol 提供了一个已签名的证明，并对 H（它是由 Carol 的原像 R 生成的，这时只有 Carol 知道）进行哈希。她提供哈希 H，在她负责的 BTC 中具有相应的价值，并签名。这可以用作 OMG 链上的证明（如果 Carol 出现故障，则可以使用以太坊智能合约）[12]。

当 Alice 想要出售比特币时，她将根据 Carol 提供的 H 值创建一个 HTLC 支付内容。同样地，当 Bob 想要接收比特币时，Carol 根据自己提供给 Bob 的 H 值发布 HTLC 内容。

这些 H 值在 OMG 链上与特定人物相关联，那么此时，资金就可以进行去中

心化交易。

当交易在OMG去中心化交易中心执行时，例如Alice要卖出BTC兑换ETH，而Bob用ETH购买BTC，该交易现在在OMG链上进行清算。每个人现在都有履行交易的责任和义务。

Carol负责释放与Alice和Bob在OMG链上所执行的交易相关的H的原像R。Bob可以使用这些信息来提取比特币链上的资金，而Carol现在有权从爱丽丝处提取资金。

如果Carol拒绝在相关时段内将原像R释放到OMG链上，她的资金将被削减，她的ETH将转移给Alice和/或Bob。（以惩罚的方式来减轻汇率波动，并防止Carol作恶）。

如果Carol不正确地释放了她不应该释放的R值，那么任何一方都可以将证明提交到区块链上，此时Carol将被处以罚款，并将交易清算合约锁定的与H值相关的资金给予证明提交方。

清算中心可能不需要直接与参与者（Alice，Bob）相连，他们可以通过路由网络支付，这样的话，他们可以实现资本效率最大化。

清算中心有权为各种使用自身来进行的活动收取费用。

我们需要去相信清算中心能够执行支付，但我们可以对他们的活动信任最小化（因为他们的活动都绑定在OMG链上）。

值得注意的是，这种结构对于通过外部化接合的 HTLC 快速超时也十分有用，也是实现以分钟测量的极速超时来构造支付的方式。它不需要清算中心锁定比特币，只需要绑定由清算中心所执行的信息的释放过程。这个结构的进一步解释将在另一份单独的文件中进行阐释。

请注意，这仅仅是可能的。因为OMG链很大程度上不提倡重组。

最终的结果就是我们能够在比特币之外进行去中心化交易。我们相信这是一个新颖的结构，因为比特币网络上的参与者的活动是由一个外部去中心化的交易中心经由以经济激励方式来驱动的建立在比特币上的清算中心来执行的，并且通过外部条件强制释放原像可以让比特币用于协议代币区块链。

5.4 智能合约实时数据更新

将最近交易执行的 VWAP 定期在 OMG 区块链上进行计算和公布作为共识

规则。

它将允许外部合约使用交易执行价格和数额的 Merkle 树 SPV 证明，甚至可以在智能合约中创造更大的可行性。

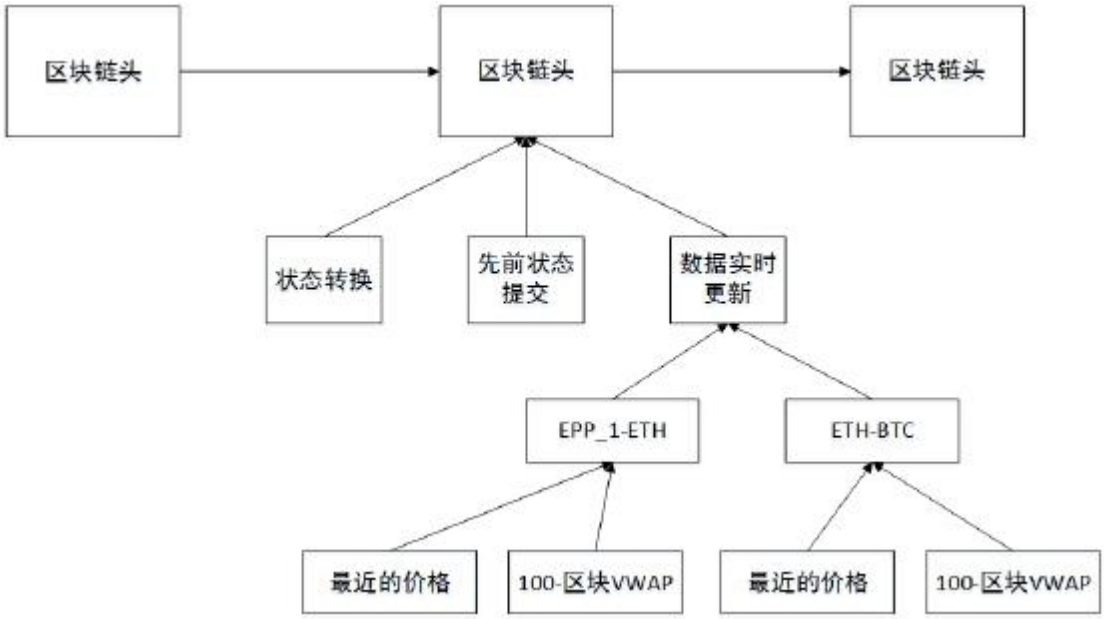

图 **2**：实时数据的定期提交将在 OmiseGO 区块链中记录。人们可以通过区块链头中的 merkle 根提交信息来进行外部验证。交易数据来源包含最近交易价格，交易量和各种 VWAP 条件（各种时间和/或区块数）等常用交易对。

任何交易所的主要功能都不仅是管理交易委托账本和执行，而且还有一个供第三方系统使用的数据供应。它允许第三方系统使用这些信息，并让参与者在一个地点上净化活动。由于汇率/定价机制的基础对于所有（智能）合约来说都是必要的，因此访问该系统可以让这些外部合约的参与者使用交易中心作为实时数据更新的途径，从而在执行中有更大的保证和透明度。合约参与者将被允许基于行为认知创建合约，并获得去中心化合约服务。如果参与者使用 OmiseGO 链上的价格预言机供应作为智能合约定价的基础，他们可以通过在 OMG 链上下订单获得更好的执行保证。这将为 OMG 链创造更卓著的网络效应以彰显其对智能合约更好的应用。

6 闪电流动性供应商

网络资本流动性的中心化压力一直是人们担心的问题。许多人担心闪电网络可能集中在少数节点上，这些节点将允许租金提取。闪电网络旨在避免这种具有大量流动性的节点的租金提取。但是，拥有良好连接节点也有一些好处。

我们可以在构建类似于上述部分所提到的清算中心机制，节点可以将活动绑

定在 OMG 链上，并且 OMG 链可以充当具有大量流动性的单个闪电中心。

对于 ETH 和类 ETH 通道，我们可以直接将其锁定在智能合约中。

对于基于 BTC 的通道，这是可能的，但通道参与者的活动是由在 OMG 链上 ETH 支持的保证金来执行的。支付将被发送到 OMG 链上的参与者，而外部活动将通过该链上的承诺来执行。

为了防止太多资金被分配到这个系统中，OMG 平台在成熟之前需要进行限制。这样就可以建立一个巨大的流动性池，从而激励资金用于清算中心和去中心化交易。

7 OmiseGO 代币的经济学意义

交易费用将在 OmiseGO 链上产生。验证节点通过验证该区块链的活动来获取费用。

支付和兑换费用将用于支付此网络上的活动费用并激励诚实的活动。

担保会产生成本。那些在这个网络上代表他人的担保可能会收取费用，例如清算中心。

8 限制

这个网络是一个开放的网络，准确的交易活动要求去中心化交易中心的获取最终公共，哪怕是盲承诺/盲投标。虽然现在可以通过 SNARKS 进行新的密码学处理，但是对于大批量的交易网络来说，目前还是太慢，并且面临资源密集的问题。我们目前正在对性能和速度进行优化。因为这是一个本地匿名网络（带有可选的代币发行 AML / KYC 结构）。

其他链的 SPV 验证被认为是不安全的，没有因为它们的区块链没有阻止重组。对于允许重组的链，要么需要对该链进行全节点验证，要么需要建立 HTLC 清算中心。它假定以太坊会为最终结果创造更高的可靠性和保障（当前的权益证明研究）。

这些技术都是全新的且尚未经过测试。我们会尽全力建设，使其在对抗环境中具有最大的安全性。我们正在搭建这些机制的安全模型，这些机制需要使用人类行为的真实用例来正确理解。当链之间交互时，很难回滚错误。所以我们在进行去中心化跨链活动时，如无必要，尽可能不要在该链产生交易。初始版本在对抗性设置中可能不够稳健，我们建议降低风险值，因为随着软件的开发，攻击（尤其是拒绝服务攻击）会随着时间的推移而得到解决。设计的性能和其对现实世

界的影响还有待研究观察。

目前还不清楚这个网络的长期价值参与者可以得出什么结果，而且这一领域的竞争会带来影响，作为验证者参与也并没有什么保证，因为这是个在技术上仍处在探索中的领域。

任何一次清算转账（但尚未结算）的总价值必须低于验证节点担保的总价值。我们也可以绑定额外的数额，但是如果代币的总价值足够高，那就没有必要了。我们有必要对系统固有的执行机制进行建模。

执行这个愿景最终是 OmiseGO 团队的责任，本文的作者虽不是团队成员，但主要负责供技术指导及架构。

9 结论

随着电子钱包平台的普及，孤岛网络正在成为一个问题。这种情况创造了一个独特的机会实现法定代币去中心化网络交易，以及加密数字货币的交叉兼容性。

为了建立这个去中心化交易网络，它不仅需要一条非常适合已发行代币支付和交易的区块链，而且还需要支持这些活动的去中心化交易中心，以及制定行之有效的流动池的激励措施。

最终，这些发行的代币可能越来越接近于完全去中心化（包括用户拥有的钥匙），最大限度地发挥个人的代理权。我们可以通过在支付交易的业务流程中创建透明度，以及从单个受信任者中移除业务流程本身的所有权来实现。OmiseGO 希望我们的股东——从个人到发行方——拥有更好的社会金融机制保障。

10 致谢

感谢 Piotr Dobaczewski 为本文所作出的贡献，还有 Rick Dudley 和 Vitalik Buterin 对本文的投入以及反馈。

11 许可证

参考文献

[1] Fred Erhsam.Blockchain Tokens and the dawn of the Decentralized Business Model.https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f .

[2] Fred Erhsam.Tokens,Why How. https://www.youtube.com/watch?v=rktHO5R8Y9c.

[3] Ethereum.Ethereum.https: //ethereum.org.

[4] Gavin Wood.ETHEREUM:A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.http://szabo.best.vwh.net/ formalize.html,Feb 2015.

[5] Nick Szabo.Formalizing and Securing Relationships on Public Networks.

http://szabo.best.vwh.net/ formalize.html,Sep 1997.

[6] Joseph Poon and Tadge Dryja. Lightning Network. https://lightning.network/lightning-network-paper.pdf ,Mar 2015.

[7] Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf,Oct 2008.

[8] Raiden. Raiden Network. https:// raiden.network/.

[9] Joseph Chow.BTC Relay. http://btcrelay.org/.

[10] Bitcoin Wiki. Using external state. https://en.bitcoin.it/wiki/Contract#Example_4:_Usi ng_external _state.

[11] Tier Nolan. Re: Alt chains and atomic transfers. https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949.

[12] Ilja Gerhardt and Timo Hanke. Homomorphic Payment Addresses and the Pay-to-Contract Protocol. http://arxiv.org/abs/1212.3257,Dec 2012.