Omni Protocol

1 简介

Omni Protocol是以各公链的单币池为核心，以Wormhole, Layerzero等跨链消息协议为桥梁，以Sui公链作为结算中心的全链流动性聚合结算系统。各公链的单币池允许任意链上的用户为协议提供流动性。跨链消息协议负责将单币池互联互通。Sui公链作为结算中心，为协议带来了安全，并发，低手续费的良好特性。基于Omni Protocol协议，我们将开发多种金融应用。我们将在全链单币池的基础上开发全链借贷应用，该应用可以满足不

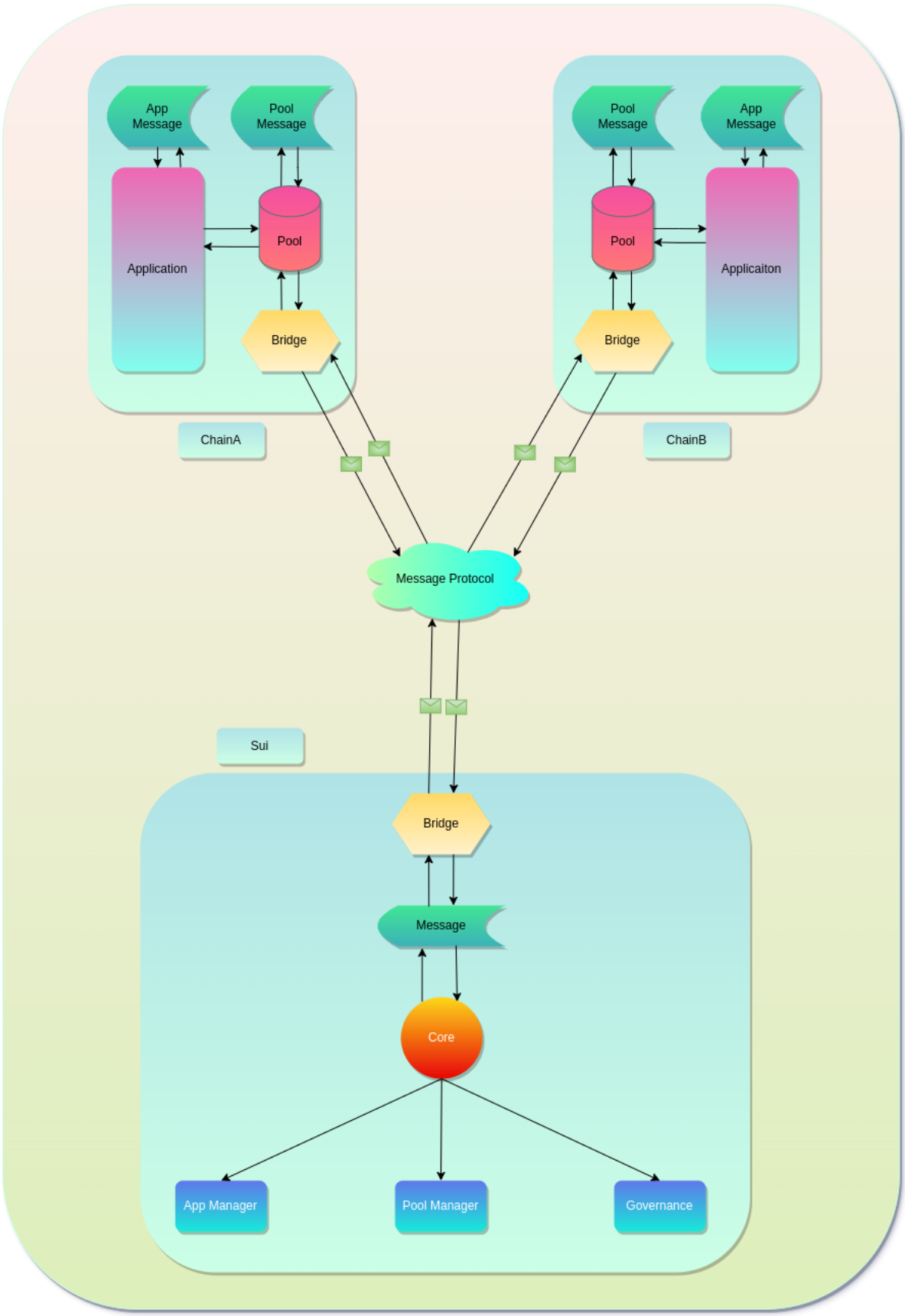
同链上用户的存款借款需求。相比于Aave协议在单链提供流动性进行借贷并借用第三方跨链桥进行跨链，全链借贷所有的借贷操作可以在任意链进行，这极大地增加了借贷协议资金利用率，并且用户能够对链无感知地进行借贷操作。我们将开发新型Dex应用，不同于传统AMM的地方是，允许用户提供单边流动性进行单边做市。新型Dex应用可以实现高效跨链Swap，低滑点和减少无常损失。同时相比于Stargate稳定币跨链桥，新型Dex应用允许非稳定币跨链交换，进一步聚合全链资产流动性。基于单币池全链借贷，我们可以一步扩展到NFT全链借贷，满足非同质化资产的抵押借贷需求。我们也可以将Omni Protocol接入已经上线的OmniSwap和其他Web3应用，作为全链流动性的入口。Omni Protocol的初衷是建立一个全链流动性聚合结算系统，足够的扩展性允许我们将全链流动性引入到不同的Web3应用。

1.1 动机

从Web3智能合约编程兴起以来，各种公链层出不穷。从最初的以以太坊为代表的Evm系公链，到当下以Sui, Aptos为代表的Move系公链。这种现象导致流动性出现相当程度的割裂。目前55%的流动性聚集在以太坊上，剩下流动性分散在其余公链。割裂的流动性导致不同公链用户难以进入新公链。需要用户找到Dex换取新公链的代币，并使用代币桥换跨链。不同的代币桥有不同的用户界面，用户需要学习，浏览，使用而且价格也不便宜。同时拥有不同公链资产的用户，难以找到合适的项目赚钱超额收益。

为了解决上述问题，我们提出了Omni Protocol。拥有不同公链资产的用户可以将流动性提供给协议，轻松赚取更高的超额收益。出现新公链，Omni Protocol的易扩展性，为第一时间接入提供时间保证。一致的用户入口，带来更优秀的操作体验。

2 协议架构


App Message
Pool Message
Application
Pool
Bridge
ChainA
Pool Message
App Message
Pool
Applicaiton
Bridge
ChainB
Message Protocol
Sui
Bridge
Message
Core
App Manager
Pool Manager
Governance

2.1 流动性层

2.1.1 单币池(Pool)

单币池是协议的核心。用户提供的流动性，由单币池负责托管。单币池本身是无状态的，用户的状态由协议核心的代币池管理器聚合管理。这种方式使得代币池非常的简单，带来了极大的可扩展性，有利于新公链快速接入协议。同时，用户的操作可以在不同链上分开进行，极大提高了用户操作的灵活性。用户可以在A链向协议充值赚取收益，在B链上提现提取收益。单币池的主要特征:

- 资产ID：不同公链的资产在协议中有唯一ID，不同公链的同类资产使用相同ID统一管理（如Evm和Optimism上的USDT）
- 用户充值：允许用户向单币池发起充值，单币池负责编码用户地址，资产地址，资产数量，再通过桥完成协议负载的投递，实现用户的入金操作
- 用户提现：允许用户向单币池发起提现，单币池负责编码用户地址，再通过桥完成协议负载的投递，实现用户的出金操作
- 用户充值和提现：允许用户在一笔交易中完成充值和提现操作，Dex应用中的Swap操作可以看作一次充值T1资产，提现T2资产的操作

2.1.2 桥(Bridge)

桥负责接收来自单币池的消息，并利用Wormhole，Layerzero跨链消息协议完成消息传输。桥只允许单币池和协议核心的调用。单币池接收用户出入金操作并编码地址和数量，为协议提供了用户出入金的安全保障。

桥是不同跨链消息协议的适配器。为了实现不同公链消息的通用性，协议将制定统一的消息规范。其中消息属性的类型满足数值统一转换成64位整数，地址统一转换成字节类型，其他数据也统一用字节类型表示。桥接收到单币池消息完成类型转换后，会调用不同的跨链消息协议接口完成消息传输。

2.1.3 单币池管理器(PoolManage)

Sui结算中心的单币池管理器是不同链上单币池的统一管理者，负责单币池的资产分类，资产流动性管理等。通过单币池管理器可以全局透视不同链上单币池的资产分布。单币池管理器拥有一个动态跨链费算法，通过不同链上的可用流动性和期望流动性，激励单币池流行性自动再平衡。如果单币池的可用流动性低于期望流动性，跨链费用变高。如果单币池的可用流动性高于期望流动性，跨链费用变低。

2.1.4 应用管理器(AppManage)

Sui结算中心的应用管理器负责管理协议支持的应用。Omni Protocol引入新应用，需要通过应用管理器获取权限并分配应用ID。协议中的每一个应用拥有唯一ID。用户可以通过应用ID自主选择想要使用的应用，为协议提供流动性，也可以根据协议推荐算法进行自动选择，让用户拥有较低的学习成本和良好的用户体验。应用管理器负责应用的冻结和下架，用于应对紧急情况。应用管理器负责制定或更新不同公链应用层接口使用的消息库。

2.1.5 治理(Governance)

治理是协议可持续发展的最重要模块之一。通过去中心化链上治理，协议能持续升级和优化，并为协议参与者带来给多收益。治理模块采用DAOStack的思想，通过治理代币和声誉系统在链上进行共同治理，治理范围包含整个协议。早期由开发团队代理治理，治理代币发行后，逐步过渡到去中心化治理，最终完全由社区进行治理。治理代币的发行规则将在不久的未来确定。

权限管理涉及整个协议的所有权限。单币池管理器相关的权限，需要单币池管理器通过治理才能引入新的资产，更改动态跨链费算法参数。应用管理器相关的权限，需要应用管理器通过治理才能引入新的应用，冻结应用。通过链上治理，让治理代币持有者共同发展完善协议生态。

2.2 应用层

2.2.1 全链借贷

以Aave为代表的借贷协议，提供了对少数流动性最好的代币的借贷能力。在去中心化的金融世界里，Aave提供了无信任和无许可的良好特性。经过时间证明，去中心化的借贷能够运行的很好，但同时目前的借贷协议也存在大量未满足的需求。Aave仅仅满足了流动性最好的资产借贷能力，对于其他资产的借贷有待进一步扩展。Aave是单链模式的。虽然通过代币桥实现了跨链抵押借贷，但是需要各公链部署Aave协议，成本高且用户操作复杂。

利率模型

储备金：借贷协议中，极少数情况下借款人抵押品的价值可能会低于其负债的价值，在这种情况下，借款人的能力被称为无力偿还。无力偿还的借款人被清算后，会出现剩余的负债被认为是坏账。如果坏账出现累积，贷款人可能一下子都来提取资金以避免成为坏账的承担者。为了减少这种风险，遵循Compound的做法，协议提取一部分利息积累成储备金。如果出现坏账，利用储备金进行偿还，只要储备金的积累速度高于坏账，就能避免贷

款人成为坏账的承担者。提取成为储备金的利息比例称为储备金系数，记做RF。不同的资产有不同的RF 。RF取值在0和1之间，可以通过治理来进行调整权衡。

资金利用率：资金利用率是当前借贷资金和供应资金的比例。U_c代表资金利用率，D_c代表借贷资金，L_c代表剩余资金。

$$U_c = \frac{D_c}{D_c + L_c}$$

借款利率：Aave和Compound使用静态线性利率模型来决定协议的借贷成本。简单来说，当从池子里的借贷需求增加或者供应减少，利率上升，而当供应增加或者借贷需求减少，利率下降。BR_b代表基础借款利率。$U_{optimal}$代表最佳资金利用率。BR_{slope1}代表当前资金利用率低于最佳资金利用率时，利率与利用率的比例关系的常数。BR_{slope2}代表当前资金利用率高于最佳资金利用率时，利率与利用率的比例关系的常数。BR_c代表当前借款利率。

$$BR_c = \begin{cases} BR_b + U_c * BR_{slope1} & U_c < U_{optimal} \\ \\ BR_b + BR_{slope1} + \frac{U_c - U_{optimal}}{1 - U_{optimal}} * BR_{slope2} & U_c >= U_{optimal} \end{cases}$$

流动性利率：流动性利率是贷款人提供贷款应获利息的利率，资金来源于借款利率，用LR_c表示。

$$LR_c = BR_c * U_c * (1 - RF)$$

累积借贷指数：表示随着时间的累积，借款人应付利息的累积指数。ΔT 代表当前时间到上一次更新的间隔时间，T_{year}代表一年时间，单位为秒。

$$BL_t = (\frac{BR_c}{T_{year}} + 1)^{\Delta T} * BL_{t-1},\ BL_0 = 1$$

累积流动性指数：表示随着时间的累积，贷款人应获利息的累积指数。ΔT 代表当前时间到上一次更新的间隔时间，T_{year}代表一年时间，单位为秒。

$$CL_t = (\frac{LR_c * \Delta T}{T_{year}} + 1) * CL_{t-1},\ CL_0 = 1$$

利率模型参考了目前Aave和Compound的成熟做法进行建模，不同的地方是储备金系数RF所获得的利息会成为一个特殊的借款人，加入累积流动性指数从而自动获得利息，进一步增加协议抵御坏账风险的能力。

权益化代币(oToken)

权益化代币oToken是存款人存款后收到的衍生代币。权益化代币oToken会随着CL_t的增加而自动累积，增加的数量代表存款用户所获得的利息。SoT_t 用来表示用户在t时刻拥有的scaled oToken的数量。m用来表示用户存款/提现数量为m的代币。oT_t用来表示用户在t时刻oToken的数量。权益化代币oToken的数量由SoT_t和CL_t共同决定，如下所示：

用户存款：

$$SoT_t = SoT_{t-1} + \frac{m}{CL_t}$$
$$oT_t = SoT_t * CL_t$$

用户提现：

$$SoT_t = SoT_{t-1} - \frac{m}{CL_t}$$
$$oT_t = SoT_t * CL_t$$

债务化代币(dToken)

债务化代币dToken是借款人借款产生的债务。债务化代币dToken随着BL_t的增加而自动累积，增加的数量代表借款用户所要付出的利息。SdT_t 用来表示用户在t时刻拥有的scaled dToken的数量。m用来表示用户借款/还款数量为m的代币。dT_t用来表示用户在t时刻oToken的数量。债务化代币dToken的数量由SdT_t和BL_t共同决定，如下所示：

用户借款：

$$SdT_t = SdT_{t-1} + \frac{m}{BL_t}$$
$$dT_t = SdT_t * BL_t$$

用户还款：

$$SdT_t = SdT_{t-1} - \frac{m}{BL_t}$$
$$dT_t = SdT_t * BL_t$$

清算

清算是当用户的负债价值和抵押品价值不满协议规定的超额抵押要求时，用户抵押品会被清算来偿还用户负债。

风险调整：不同于传统借贷，仅仅考虑用户抵押品价值降低带来的坏账风险。协议同时考虑负债价值上升带来的风险，通过BF(大于1)将负债价值提升来抵御这种风险。CF(小于1)用于降低抵押品价值。当用户的抵押品价值$TotalCollateral$和负债价值$TotalDebt$不满足如下公式时，会被清算。

$$TotalCollateral * CF >= TotalDebt * BF$$

抗MEV能力：在传统借贷中，清算的激励方式是将借款人的抵押品以固定百分比的折扣提供给清算人，通常在5%-10%之间。清算人是有利可图的，但是不抗MEV，因为矿工和跑在前面的人可以窃取清算人的交易。为了限制这种形式的MEV，协议允许流动性提供者有资格获取折扣，矿工和其他人没有折扣。

清算成本：在传统借贷中，清算通常需要利用外部流动资金来处理。这种方式的确定导致清算人不能以理想的价格进行清算。造成这种情况的原因包括滑点，价格波动，手续费等。协议的全链单币池，允许清算允许通过闪电贷的进行清算。清算人仅仅需要支付Gas成本。

软性清算：在传统借贷中，清算人一次性清算的债务是固定的，目前是0.5，即清算人一次性允许清算人清算一半的债务。这种方式的缺点是如果较小的清算可以使债务恢复健康，那么清算一半的债务是过度的且不公平的。因此，本协议将采用软性清算模式，每次允许清算的债务不超过使违约者恢复正常所需的金额（加上一个额外的安全系数）。这意味着轻微违约的借款人清算的债务少于一半，严重违约的借款人超过一半。

资产隔离

为了满足长尾资产的借贷需求，对于长尾资产允许用户在隔离模式下进行借贷。不同于普通资产，用户必须进入隔离模式，长尾资产只能用作抵押品，只能借入稳定币资产且存在债务上限。通过债务上限可以对风险进行良好的控制，从而避免长尾资产的价格波动导致坏账急剧增多。

总的来说，全链借贷应用借鉴了Aave和Compuond协议中的成熟做法，同时针对它们的不足进行了相应的改进。相比Aave和Compuond：对于用户来说，可以实现一键在A链上存入B链上借出操作，降低了用户的学习成本。对于清算人来说，降低了清算陈本，减少了MEV。对于协议来说，提高了抗风险的能力。

2.2.2 PMM

PMM是主动做市商算法，来源于DODO协议。相比于传统的AMM，PMM允许用户进行单边充提，非常契合我们协议的全链单币池。将PMM构建在全链单币池基础之上形成的新型Dex应用，用户将拥有更低的滑点，做市商将拥有更低的无偿损失。不可避免的PMM引入更高的算法复杂度，但是算法逻辑构建在Sui上会有效降低额外手续费消耗。

边际价格

边际价格P是当前状态下的瞬时价格，用来表示多少个quote token可以买一个base token。B_0表示做市商的base token总充值，Q_0表示做市商的quote token总充值。B表示当前资产池的base token总数量，Q表示当前资产池的quote token总数量。i是由预言机提供的市价， k是一个在 0 到 1 范围内的参数。

$$P = \begin{cases} i * (1 - k + k(\frac{B_0}{B})^2) & B < B_0 \\ \\ \frac{i}{(1-k+k(\frac{Q_0}{Q})^2)} & Q < Q_0 \end{cases}$$

从边际价格公式可以看出，k为0时，边际价格恒等于预言机提供的市价，无滑点，资金利用率高。k为1时，退化为传统的AMM，必须按照当前价格比例同时冲提两种资产，滑点高，资金利用率低。当池子中的资产数量B和Q偏离B_0和Q_0时，会导致当前价格高于和低于外部价格，促使套利者套利，使得B和Q回归目标数量B_0和Q_0。值得注意的是，当系统处于不平衡状态时，预言机的价格变化会带来盈利或亏损。如当base token短缺且预言机价格base token上涨，多余的quote token价值低于base token回归到平衡状态的价值，做市商就会出现亏损。因此对于边际价格波动大的base token和quote token，需要设置一个较大的k，减少做市商出现亏损的风险。

平均价格

如下公式，对边际价格积分，可以得到平均价格P。通过平均价格P，可以得出交易者想买卖一定数量的base token和quote token时，需要支付的token数量。

$$P = \frac{Q_1 - Q_2}{B_2 - B_1} = i * (1 - k + k * \frac{B_0^2}{B_1 * B_2}) = \frac{i}{1 - k + k * \frac{Q_0^2}{Q_1 * Q_2}}$$

回归目标

B_0和Q_0是回归目标，将B_0和Q_0代入平均价格公式，求解二元一次方程可以得出

$$B_0 = B_1 + B_1 * \frac{\sqrt{1 + \frac{4 * k * \Delta Q}{B_1^2 * i}} - 1}{2 * k}$$

$$Q_0 = Q_1 + Q_1 * \frac{\sqrt{1 + \frac{4 * k * \Delta B * i}{Q_1^2}} - 1}{2 * k}$$

做市商充值base token时B_1上涨b，B_0上涨幅度更大，因此做市商一旦充入资金，会导致所有base token做市商盈利，协议会提供充值奖励做市商，奖励主要是由让系统偏离平衡状态的交易者支付的，quote token遵循同样的规则。反之，做市商提现，会让所有的做市商遭受亏损，因此提现需要支付一定的手续费。手续费等于这笔引起的做市商的亏损总和，并被分配给还未提现的做市商。

总的来说，新型Dex应用利用PMM算法，让用户可以在任意公链充值资产进行单边做市。同时灵活的参数配置，可以带来更低的滑点，减少无常损失，以及更优秀的用户体验。

2.2.3 NFT借贷

NFT 借贷，是指借款人通过在平台将其 NFT 作为抵押品，去借出加密货币，由贷款人或平台为借款人提供资金流动性。NFT借贷目前主要有三种模式，分别是点对点、点对池和抵押债仓。在点对点NFT借贷模式中，借款人与放款人直接进行匹配，借款人申请某个时期内的贷款，放款人提供不同的利率条件，最终由借款人选择利率条件完成借贷；在点对池NFT借贷模式中，用户可以将NFT的投资组合进行抵押，并以可变利率获得USDT等其他代币，这就类似于Compound借贷；在抵押债仓NTF借贷模式中，用户将一类NFT抵押品抵押创建保险库后，就可以铸造稳定币，这种模式来源于MakerDAO，实现方式基本一致。目前NFT借贷中，NFTfi，BendDAO和X2Y2占据了绝大部分市场。其中，NFTfi和X2Y2是点对点借贷模式，BendDAO是点对池借贷模式。点对点和点对池借贷从同质化代

币借贷衍生而来，具有很多的相似之处。不同的地方在于，NFT的唯一性，导致同类型的NFT价值是不同的，需要考量更复杂的使用场景。

点对点模型

点对点模型是对于平台列出的NFT，借款人进行自主设置金额，期限，年利率等，经借贷双方同意后，达成交易。点对点模型优势是支持低流动性资产和长尾资产，劣势是资金利用率低下。

点对池模型

点对池模型是借款方从资金池借款，而贷款人事先将资金存入池中来获得收益。点对池模型存在三大主体：借款人、平台和贷款人，平台充当借贷蓄水池的作用，并作为借款人和贷款人的对手方。作为借款人，通过平台将合适的 NFT 捆绑到一个独特的 NFT，作为单一的抵押品单位且无法用于任何交互行为。随后根据标的的地板价和平台规定的抵押比率从借贷池中借出加密货币；贷款人通过把 加密货币存入借贷池提供流动性赚取利息。当因标的地板价大幅下跌使借款人的健康因子小于1是，触发清算。点对池的优势是提高了时间效率并且通过资金池分散了风险，劣势是不利于低流动性资产和长尾资产，并且同样面临资金利用率低下的问题。

Omni Protocol将同时支持点对点模型和点对池模型实现全链NFT借贷。通过融合两种模型的优势，使用户拥有更多的选择，支持长尾资产的同时带来更高的时间效率。

2.2.4 OmniSwap

OmniSwap是通过聚合各公链流动性，实现一键跨链Swap。OmniSwap通过将不同的公链的Dex和代币桥进行有效组合，寻找最佳路由，为用户带来更优秀的Swap体验。目前，OmniSwap已经上线支持以以太坊为首的EVM公链和Aptos公链，利用Stargate和Wormhole代币桥，组合不同公链的Dex实现一键Swap。

当前的OmniSwap是对单链Swap的有效改进。然而，将OmniSwap融合进Omni Protocol，可以拥有更高的资金效率。通过利用PMM构建的Dex应用，使大部分的跨链Swap得以在协议内完成，并且可以有效利用PMM算法的优势，为用户带来更低滑点，更低gas的操作体验。

2.2.5 其他项目

Web3世界一直在不断的发展，日新月异。金融和非金融的Web3应用层出不穷。Omni Protocol将留下足够的扩展空间，满足这些Web3项目的对接需求。将这些Web3应用引入Omni Protocol协议，项目方可以有效获取各公链的用户和资金流动性，促进Web3项目的发展。用户拥有更多的选择，发现更多的价值和乐趣。

2.3 消息层

应用消息

应用的消息对于不同的应用是独立的，需要经过应用层编码传给流动性池。应用消息由不同应用自定义消息的解码和编码，并配合Sui协议核心使应用消息进入到各自对应的结算逻辑中。

流动性池消息

流动性池消息主要包含资产相关的用户地址，资产地址，资产数量等。流动性池消息采用统一的格式，在应用消息的基础上进行统一编码，最终进入到桥中。这种方式是为了对协议资产进行统一管理，保障协议资金的安全。

跨链协议消息

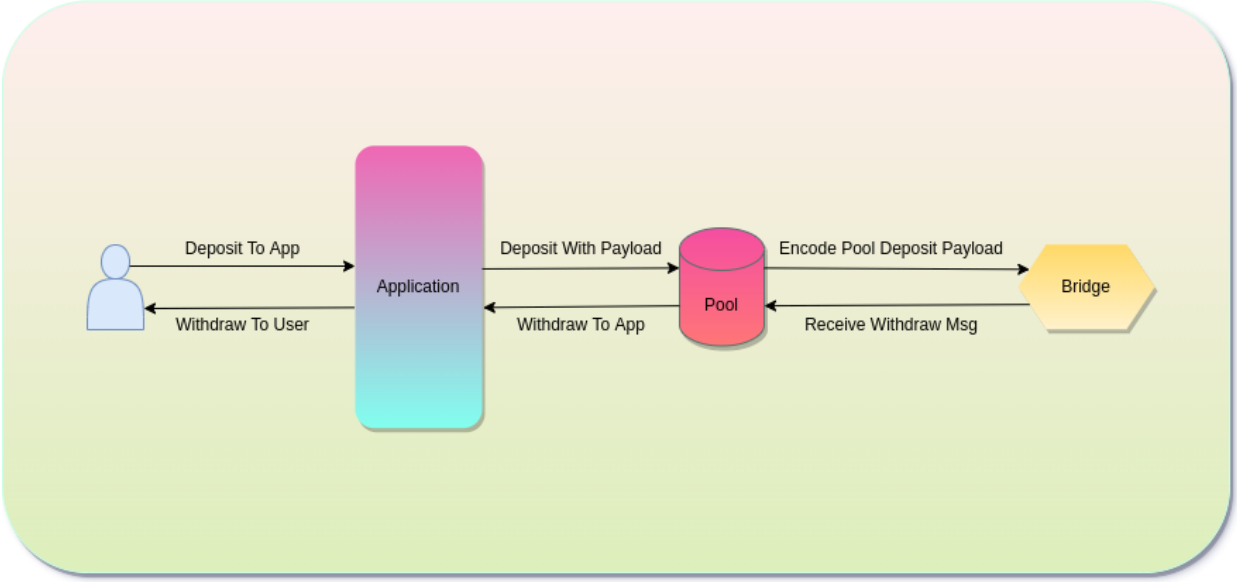
针对不同的跨链消息协议，具有不同的跨链协议消息。跨链协议消息是消息层的最后一层，包含应用消息和流动性池消息，打包好后最终通过跨链消息协议在桥之间传播。

3 协议合约

协议合约有三个部分，分别是单币池、消息协议桥、协议核心。

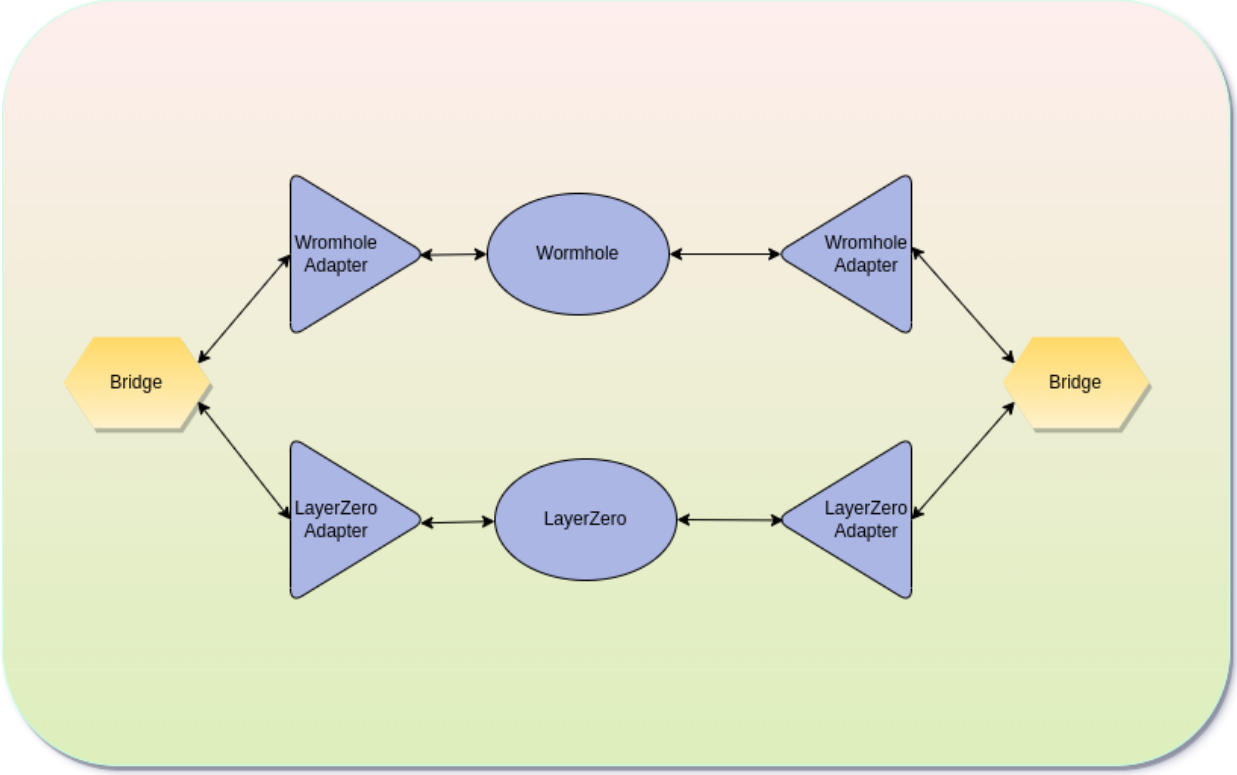
3.1 单币池合约

单币池需要对外提供充值的接口，以及对消息协议桥提供提现的接口，并且要对来自应用的消息进行打包再发送给桥。



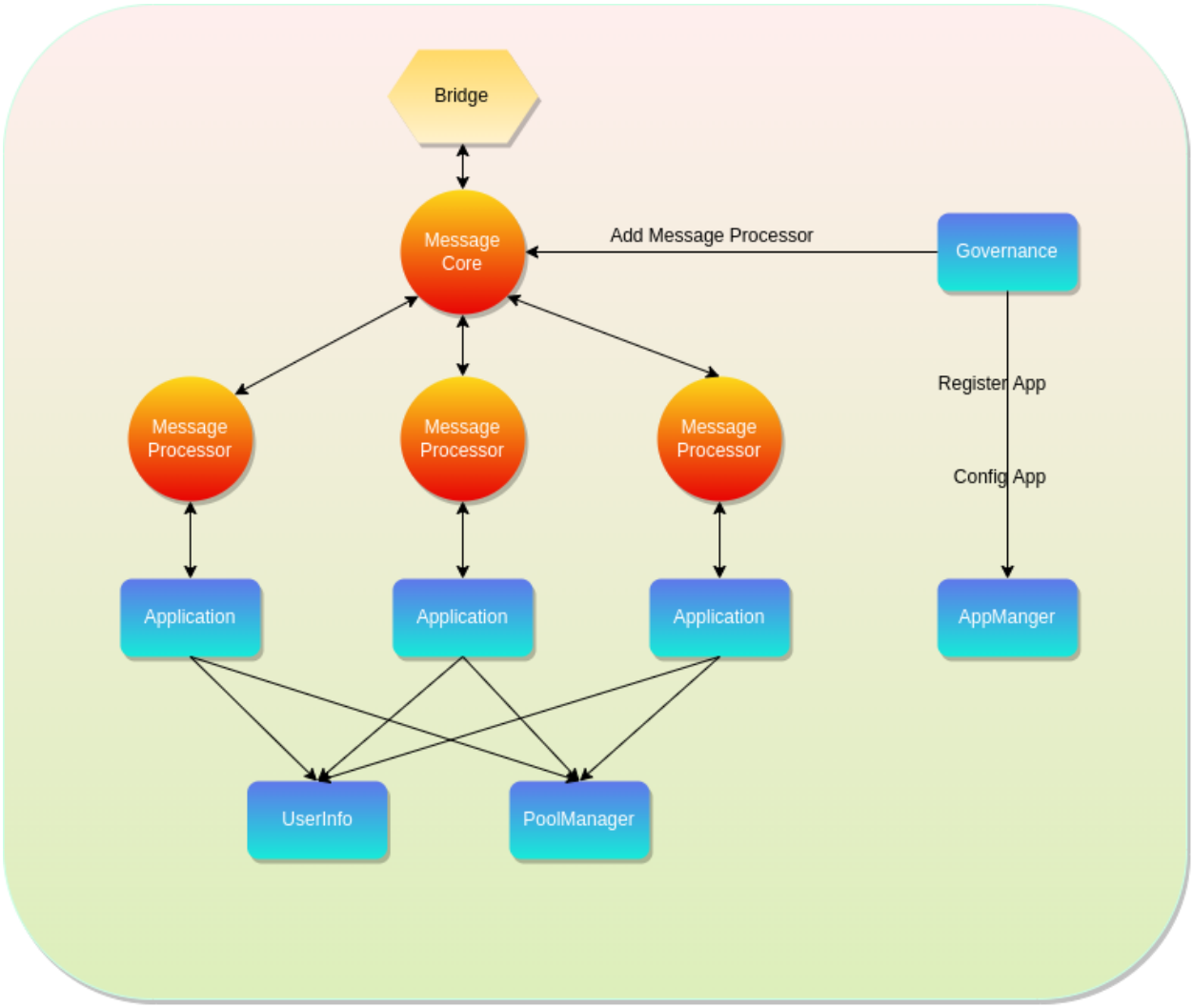
3.2 消息协议桥合约

消息协议桥需要根据接入的消息协议进行兼容，只负责消息的传递。



3.3 协议核心合约

协议核心分为3个部分，分别是消息处理、应用逻辑和治理。第一部分是消息处理，消息处理主要负责将消息进行解码并分发到相应的应用逻辑合约，同时也要负责将不同应用的消息进行编码发送给消息桥；第二部分是应用逻辑，每个应用逻辑都对应着相应的应用消息，并对协议的用户信息和单币池进行相应的更新；第三部分是治理，治理需要对协议全局的权限进行控制和管理，包括对Bridge的授权、消息类型的添加和应用的权限设置等。



4 展望

全链流动性协议是一个可扩展的协议，旨在聚合所有链上的流动性，并将流动性提供给应用。应用可以通过协议使用来自任意链上的流动性。对于开发者，在协议上层构建应用，让开发者能将更多的精力用在应用的创新上，不再需要关注链和流动性不足的问题，大大降低了开发者的门槛，也给予个人开发者更多的机会；对于想要赚币的流动性提供者，他们拥有了提供流动性的统一入口，不再需要去针对每个应用学习，极大地减少了用户的学习成本，同时也降低了添加流动性的门槛。对于用户，他们拥有了全链的未来，因为基于协议的应用都是全链的，用于可以使用任意链上的应用进行交互，而不需要去换某条链上的代币才能使用该链上的应用。我相信，未来的Web3用户使用Web3应用一定不会困难，只需要在一个应用上就应该能操作大部分DeFi应用，最终做到Web2用户就是Web3用户。全链流动性协议的未来就是Web3的核心，这里聚集着Web3的大部分资金和应用，是Web3金融体系的基础。

5 总结

全链流动性协议提供了一个为应用聚合流动性的方式，同时也给应用提供了使用全链流动性的机会。基于协议构建的应用会自然而然地聚合流动性，也能顺其自然地使用全链流动性。当前的DeFi应用主要都还是在各自的链上各自发展，就算有跨链其效果也不是很大，流动性主要还是聚合在原链上。并且对于每个团队他们想要在其他链上进行发展都比较困难，不管是开发上还是资源上，最根本上的原因是没有一个统一的协议支持他们。假如把DeFi应用比作企业，链比作国家的话，那么现在的全链流动性协议就是进行经济全球化的基础，应用通过我们的全链流动性协议可以更好地在全链进行发展，而不仅是困在一条链上。全链流动性协议通过恰到好处的设计将流动性池进行了统一，为借贷等各种DeFi应用提供了全链的操作便利，解决了当下链与链之间的孤岛困境。迈出了全链时代坚实的一步，为全链时代的发展奠定了良好的基础。