OMNI Protocol

1 简介
- 1.1 基本概念
- 1.2 符号定义

2 协议架构
- 2.1 代币池(Pool)
- 2.2 桥适配器(BridgeAdapter)
- 2.3 代币池管理器(PoolManage)
  - 2.3.1 权益化代币(oToken)
  - 2.3.2 债务化代币(dToken)
  - 2.3.3 交互模块(Action)
  - 2.3.4 注册模块(Register)
  - 2.3.5 治理(Govern)
  - 2.3.6 再投资模块(Reinvest)

3 协议风险
- 3.1 借贷风险
  - 3.1.1 清算许可
  - 3.1.2 资产分层
- 3.2 跨链消息协议
- 3.3 流动性风险

4 协议合约

5 交互
- 5.1 充值
- 5.2 提现
- 5.3 借贷
- 5.4 还款
- 5.5 跨链
- 5.6 清算

6 展望

7 总结

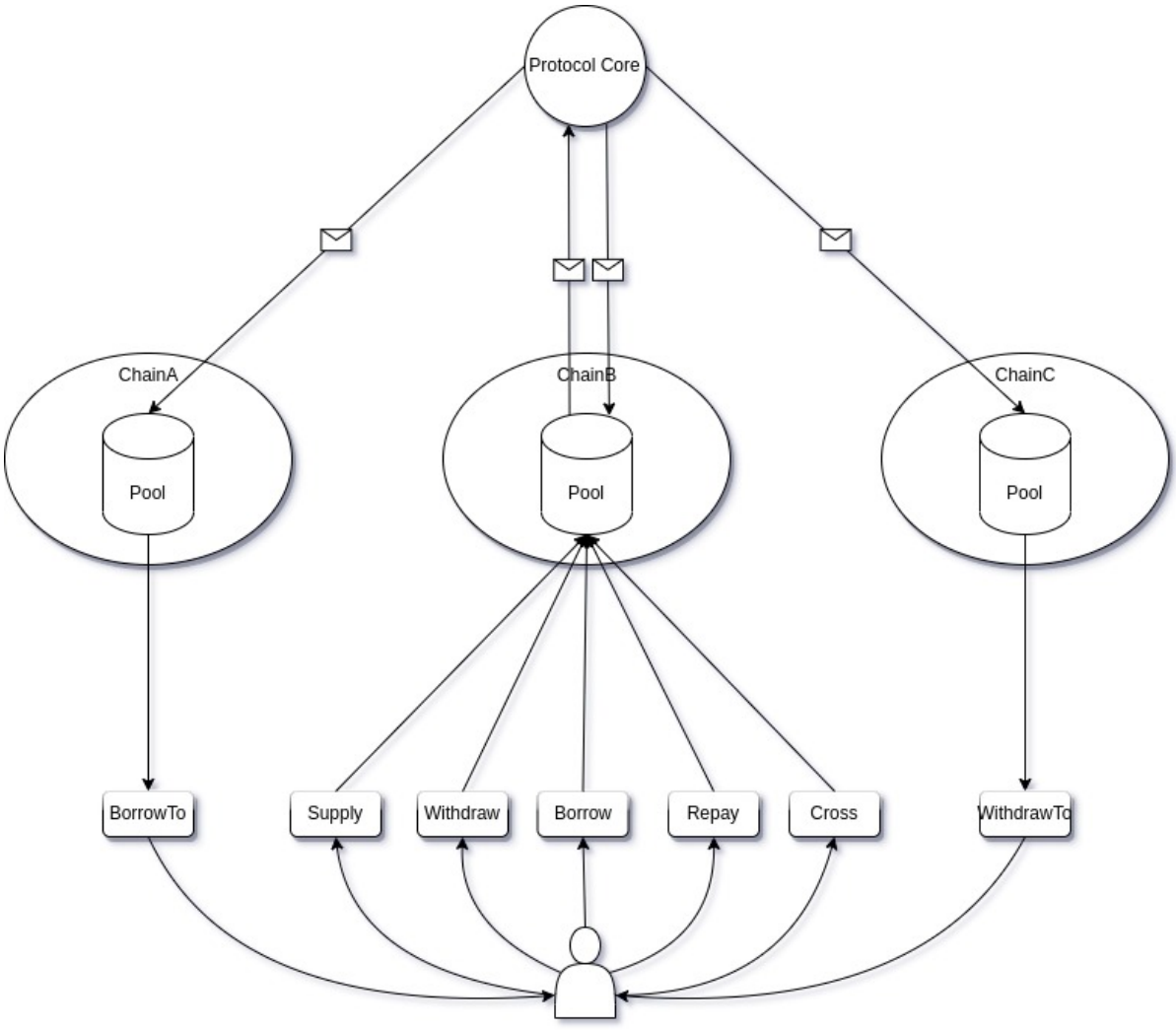
1 简介

随着区块链公链数量的不断增长，用户对全链操作的需求日益增长。跨链消息协议成为新的热点，过去单链DeFi的逐渐饱和，这些都标志着全链时代的到来。为了满足全链时代区块链发展以及用户的需求，协议借鉴Aave借贷协议以及跨链消息协议设计出了全链借贷协议。全链借贷协议是专门为全链而设计的协议。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，全链借贷协议所有的借贷操作可以在任意链进行。全链借贷协议不再依赖于单链的流动性，并且支持使用协议流动性进行跨链交换。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。全链借贷协议由跨链消息传递协议和借贷协议组

成，跨链消息传递协议主要负责传递不同链之间的消息，而借贷协议则负责处理用户的操作消息。在全链借贷协议中，用户可以在任意链进行存款和借贷。一方面，用户在某条链上进行存款时，会为该链提供流动性，该流动性不仅可以用于借贷也可以用于跨链以及其他操作；另一方面，用户可以利用协议的流动性在任意链进行借款和跨链，他们付出的利息和跨链手续费会分发给流动性提供者。

1.1 基本概念

全链借贷协议由一个协议核心以及多个流动性池组成，每条链上都有专门的流动性池，协议核心负责管理所有链的流动性。通过桥接器，协议核心能使用跨链消息协议与每条链上的流动池进行交流。用户通过与每条链上的流动池进行交互就能使用协议进行存款、提现、借贷、还款以及跨链。



1.2 符号定义

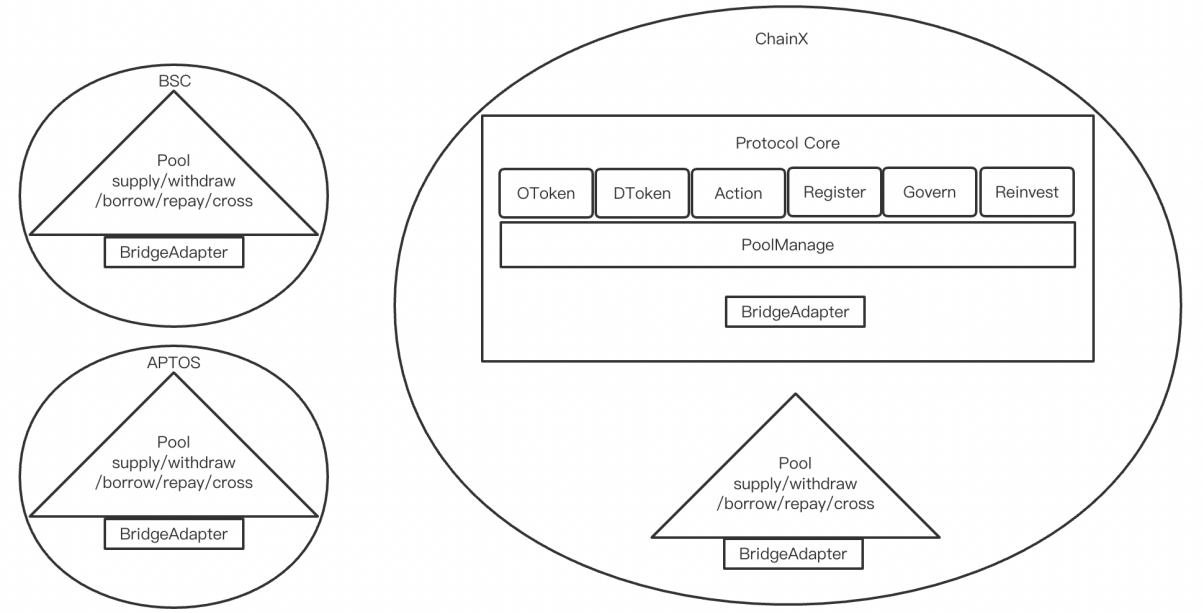
Variable	Formula	Description
T	-	Current number of seconds

Variable	Formula	Description
T_l	-	Timestamp of the last update of the reserve data
ΔT	$\Delta T = T - T_l$	Delta time
T_{year}	$T_{year} = 365 * 24 * 60 * 60$	Number of seconds in a year
L_c	-	Current amount of liquidity available in the reserve
D_c	-	Current amount of debt in the reserve
U_c	$U_c = \frac{D_c}{D_c + L_c}$	Representing the utilization of the deposited funds
$U_{optimal}$	-	The utilization rate targeted by the model, beyond the variable interest rate rises sharply
BR_b	-	base variable borrow rate, Constant for $D_t = 0$
BR_{slope1}	-	Constant representing the scaling of the interest rate versus the utilization, when $U_c < U_{optimal}$

Variable	Formula	Description
BR_{slope2}	-	Constant representing the scaling of the interest rate versus the utilization, when $U_c >= U_{optimal}$
RF	-	Treasury Interest Factor
BR_c	$BR_c = \begin{cases} BR_b + U_c * BR_{slope1} & U_c < U_{optimal} \\ BR_b + BR_{slope1} + \frac{U_c - U_{optimal}}{1 - U_{optimal}} * BR_{slope2} & U_c >= U_{optimal} \end{cases}$	Current borrow interest rate
LR_c	$LR_c = BR_c * U_c * (1 - RF)$	Current liquidity interest rate
BL_t	$BL_t = (\frac{BR_c}{T_{year}} + 1)^{\Delta T} * BL_{t-1},\ BL_0 = 1$	Cumulated borrow index
CL_t	$CL_t = (\frac{LR_c * \Delta T}{T_{year}} + 1) * CL_{t-1},\ CL_0 = 1$	Cumulated liquidity index
CF	-	Collateral coefficient $[0, 1]$. A coefficient used to prevent the downside risk of collateral prices
BF	-	Borrowing coefficient $[0, 1]$. A coefficient used to prevent upside risk of loan prices
CS_c^t	-	Represents the liquidity of the token t on the c chain at the current moment
EDR	-	Expected distribution ratio of token liquidity on different chains

Variable	Formula	Description
TR	-	The threshold of the EDR
SoT_t	-	Used to represent the number of scaled oTokens owned by the user at time t. $SoT_0 = 0$
oT_t	-	Used to represent the number of oTokens of owned by the user at time t
SdT_t	-	Used to represent the number of scaled dTokens owned by the user at time t. $SdT_0 = 0$
dT_t	-	Used to represent the number of dTokens of owned by the user at time t

2 协议架构



2.1 代币池(Pool)

代币池是协议的资金池，负责托管各个链上的各种资产。代币池是无状态的，用户的状态统一由协议核心(Protocol Core)管理。这种方式使得代币池非常的简单，新公链可以快速加入协议，有利于实现全链生态目标。同时代币池是无状态的，保证用户的充值，提现，借贷，还款行为可以在不同链上分开进行，极大提高了用户操作的灵活性。代币池的主要特征:

- 代币ID：各个代币池中的代币以$(chainId, tokenId)$作为在协议中的唯一标识，方便不同代币的统一管理。
- 用户Lending相关操作: 用户通过代币池的充值、提现、借款、还款接口与协议交互，实现全链Lending。
- 用户Swap相关操作: 用户通过代币池的跨链接口以及不同链上的DeFi协议，实现全链Swap。

2.2 桥适配器(BridgeAdapter)

桥适配器是跨链消息协议的适配器。通过适配跨链消息协议(如LayerZero)，实现协议消息的跨链传输。为了实现不同公链消息的通用性，协议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。

桥适配器也是协议和跨链消息协议的桥梁。桥适配器会接收来自代币池或代币池管理器的跨链消息，生成事件和消息编码，将编码后的数据通过跨链消息协议发送出去。同时也接收来自跨链消息协议的跨链消息，解码消息并生成事件，将跨链消息传递到代币池或代币池管理器。当跨链消息的目的链就是当前链时，跨链消息会直接传递到代币池管理器。

2.3 代币池管理器(PoolManage)

代币池管理器是不同链上代币池的统一管理者，包括代币池的代币分类，流动性管理等。同时通过桥适配器接收来自不同链上代币池的跨链消息，利用交互模块更新用户和资产的协议状

态。作为代币池的管理者，代币池管理器实现的主要功能有：

- 管理代币种类：对不同链上的代币进行分类。分类是将不同链上相同代币映射到同一类(如USDT)。每一类在代币池管理器中对应一个ERC20影子代币。影子代币帮助管理代币(如USDT)在整个协议中的全局状态。举个例子，理想情况下影子代币的总供应量代表着当前时刻不同链上代币池的托管代币数量总和。同时影子代币会作为协议核心的实际托管资产，帮助实现Lending的相关操作。
- 期望分布比(EDR)：用来管理代币池流动性。代币池管理器除了通过影子代币维护代币全局状态，同时还会记录同一类代币在不同链上的流动性。期望分布比指的是同一类代币在不同链上的期望分布。可以通过治理来手动设置，未来也可以通过合适的算法自动适配。CS_c^t用来表示c链上代币t在当前时刻所拥有的流动性。TR用来表示阈值(如0.2)。通过设置不同的阈值且c链代币t的流动性满足下列公式时：协议会抑制甚至禁止消耗c链代币t流动性的行为。同时鼓励增加c链代币t流动性的行为。鼓励的方式包括免除手续费，计提利息奖励，国库奖励，治理代币奖励等。

$$\frac{CS_c^t}{\sum_c CS_c^t} <= EDR * TR$$

- 管理用户地址：为了满足协议的全链生态目标，对于非EVM链(如APTOS)上进行任何操作之前需要进行地址绑定。地址绑定是将用户的EVM地址和非EVM地址进行绑定。
- 管理行为状态：用户通过代币池的交互行为，代币池管理器会通过桥适配器接收到跨链消息并处理。处理结果会被代币池管理器通过存储或事件来记录行为状态。行为状态的记录便于对用户交互行为进行轨迹跟踪，进而保证用户交互行为被协议完整处理。

2.3.1 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，1:1映射代币池管理器中的影子代币。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：

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

$$oT_t = SoT_t * CL_t$$

2.3.2 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：

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

$$dT_t = SdT_t * BL_t$$

2.3.3 交互模块(Action)

交互模块用于接收来自代币池管理器的协议消息，根据用户行为利用协议模块更新协议状态。交互模块会根据用户行为检查行为有效性。如用户借贷时，交互模块会通过预言机获取抵押品价格，并检查抵押品价值是否满足借贷要求。通过有效性检查，交互模块会更新权益化代币，债务化代币的协议状态，包括更新借款利率BR_c、流动性利率LR_c、借款指数BL_t以及流动性指数CL_t。

2.3.4 注册模块(Register)

注册模块主要用于引入新链和新代币。注册模块需要通过治理获得超级权限才能完成相关操作。通过注册模块添加新链时，如果是EVM链只需要部署相同的Pool合约即可，如果是非EVM链，则需要按照协议重新开发相应的代币池合约并部署。部署完成后在注册模块将新链上的代币ID写入代币池管理器的相应分类下，完成新代币的注册操作。后续添加该链新代币只需重复类似的操作。注册模块同时会实现其他需要超级权限的行为，诸如预言机合约地址，利率策略合约地址的管理。

2.3.5 治理(Govern)

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，待治理代币发行规则确定后，逐步过渡到去中心化治理，最终完全由社区进行治理。

2.3.6 再投资模块(Reinvest)

再投资模块用于提高用户资金的利用率，避免闲置资产过多，通过将闲置资金存入外部协议(如Aave)为用户赚取二次收益。再投资模块将利用链下预言机更新并维护支持的外部协议收益率。用户通过协议投资外部协议时，协议会帮助用户承担M1(如20%)的风险，获取的收益协议收取M2(如10%)。M1，M2可以通过治理进行设置。$M1 > M2$，可以用于Aave等广泛认可的协议，从而吸引Aave用户；$M1 < M2$，可以用于某些高收益但认可度不高的协议。用户在本协议充值时，如果外部协议的收益率高于本协议且流动性充足，将用户资金和一定比例的协议资金存入外部协议，记录用户投资状态。用户在本协议进行提现或借贷时，如果流动性不足或外部协议收益低于协议，就从外部协议取回资金。进行外部投资有更高的收益，同时也必然地存在更多地风险，为了保证协议和用户资金安全，每一种外部协议，都有用户资金和协议资金投资上限，避免过多的风险暴露。

再投资模块与协议的全链生态目标有很高的契合度。通过协议实现了全链生态资金的聚合，而再投资模块进一步将闲置资金导入优秀的外部协议。协议引入新链和新代币的简洁性，能够帮助快速高效的完成资金的聚合。而再投资模块除了主动发现优质项目(如Aave)外，也可以通过外部申请的方式完成。因此，再投资模块可以成为全链资金和全链生态项目沟通的桥梁。对于再投资模块，协议需要做的是合理平衡外部协议的风险和收益，保证协议整体运行的安全性。

3 协议风险

协议是存在风险的。在DeFi项目中，对协议存在的风险必须保持足够的谨慎。相比于第一代DeFi借贷协议Compound和Aave，本协议引入了足够多的功能特性和灵活性。享受这些便利的同时，不可避免的带来了额外的风险。本协议的风险主要有资产价值波动带来的破产风险和外部跨链消息协议引入的消息传递风险。

3.1 借贷风险

3.1.1 清算许可

协议采用超额抵押来规避资产价值波动带来的破产风险。和其他DeFi协议相同，破产风险考虑了借款人抵押品价值下降导致资不抵债出现的坏账。不同的是，协议同时考虑借款人负债价值上升带来的破产风险。为了降低系统破产风险，协议引入抵押品下跌风险系数CF和负债价值上升风险系数BF。用户资产价值必须满足下述条件，否则会被清算。

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

3.1.2 资产分层

在第一代DeFi借贷协议(如Aave)中，为用户提供了少数流动性最好的ERC20代币的借贷能力。这些协议依赖许可上市系统保护用户免受波动性资产的风险。同时导致波动性资产的借入借出仍有大量未满足的需求。为了解决新资产上市的无许可问题，目前的解决方案有孤立的流动资金对和孤立的流动性池。

孤立的流动资金对顾名思义是孤立的超级抵押品对：用户每次只能用一种特定的抵押品接到另一种资产，同时用户需要为不同的孤立对分别提供流动性，造成了极端的流动性隔离。

孤立的流动性池是本协议采用的方案。通过将资产分层，分隔流动性的同时实现了风险的隔离。这是在孤立流动性资金对和单一流动性池中间权衡的一种解决方案。资产层级2～4层，不同层级可以有独特的设计满足风险控制需求。目前，资产分为普通资产和高风险资产两层。普通资产流动性池是协议的基石，针对的是传统流动性最好的代币。保证普通资产池的流动性，能够有效提升协议抗风险的能力。高风险资产池针对的是波动性高的资产，通过债务上限控制高风险资产池最大风险。分层资产的主要特性：

普通资产：普通资产既可以用于抵押，也可以用于借贷，没有任何限制。当由于抵押品价格下行和负债价格上行资不抵债出现坏账时，会利用国库中存留的储备金进行赔付。普通资产大部分情况下表现比较稳定，出现坏账的情况较少。储备金的累积速度远超坏账累积速度，能够保证协议正常运转且不断提高协议的抗风险能力。

高风险资产：波动无法预估的高风险资产。此类资产作为抵押品或负债容易暴涨暴跌，导致坏账。为了满足高风险资产的可用性，同时降低系统风险：

- 高风险资产无论作为抵押品或负债，风险均由借贷双方承担。出现坏账，不会利用国库储备金赔付。这是由协议初期抗风险能力弱决定的。
- 高风险资产作为抵押物或负债必须用单独子账号来进行风险隔离。
- 高风险资产有更高的借款和贷款利率，抵消用户承担的风险。
- 高风险资产作为抵押品，负债必须是稳定币。负债稳定币有借出上限，控制高风险资产下行总风险不会超过借出上限。
- 高风险资产作为负债，抵押品必须是稳定币。抵押品稳定币有存入上限，控制高风险资产的上行总风险不会超过存入上限。

3.2 跨链消息协议

协议利用外部跨链消息协议进行消息的传递。跨链消息协议是目前资金被盗的重灾区。然而，协议对跨链消息协议的安全性有很高的要求。为了满足协议的要求，首先会挑选目前认可度较高的跨链消息协议（如LayerZero）。同时，为了实现分散风险，可以依赖多个跨链消息协议。通过多次确认消息的正确性，保证消息传输的安全性。

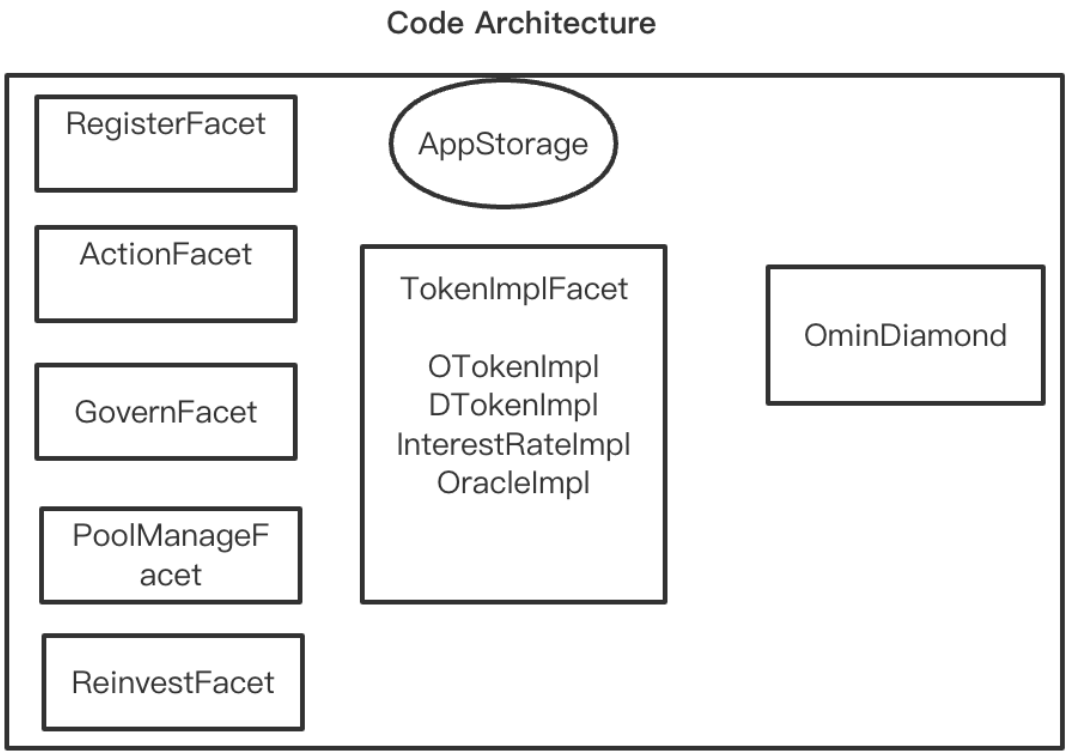
3.3 流动性风险

相比于通常的流动性池枯竭风险，全链流动性完全枯竭可能性较小，但单链流动性枯竭可能性很大。单链流动性枯竭会导致用户无法在该链上提现和借贷资产，虽然用户仍可以从其他链进行提现和借贷资产，但总的来说与用户的期望不符。协议通过期望分布调整不同链之间的流动

性。当该链的流动性小于协议期望分布时，阻止用户进一步消耗流动性的行为，鼓励用户增加流动性的行为，从而消除单链流动性风险。

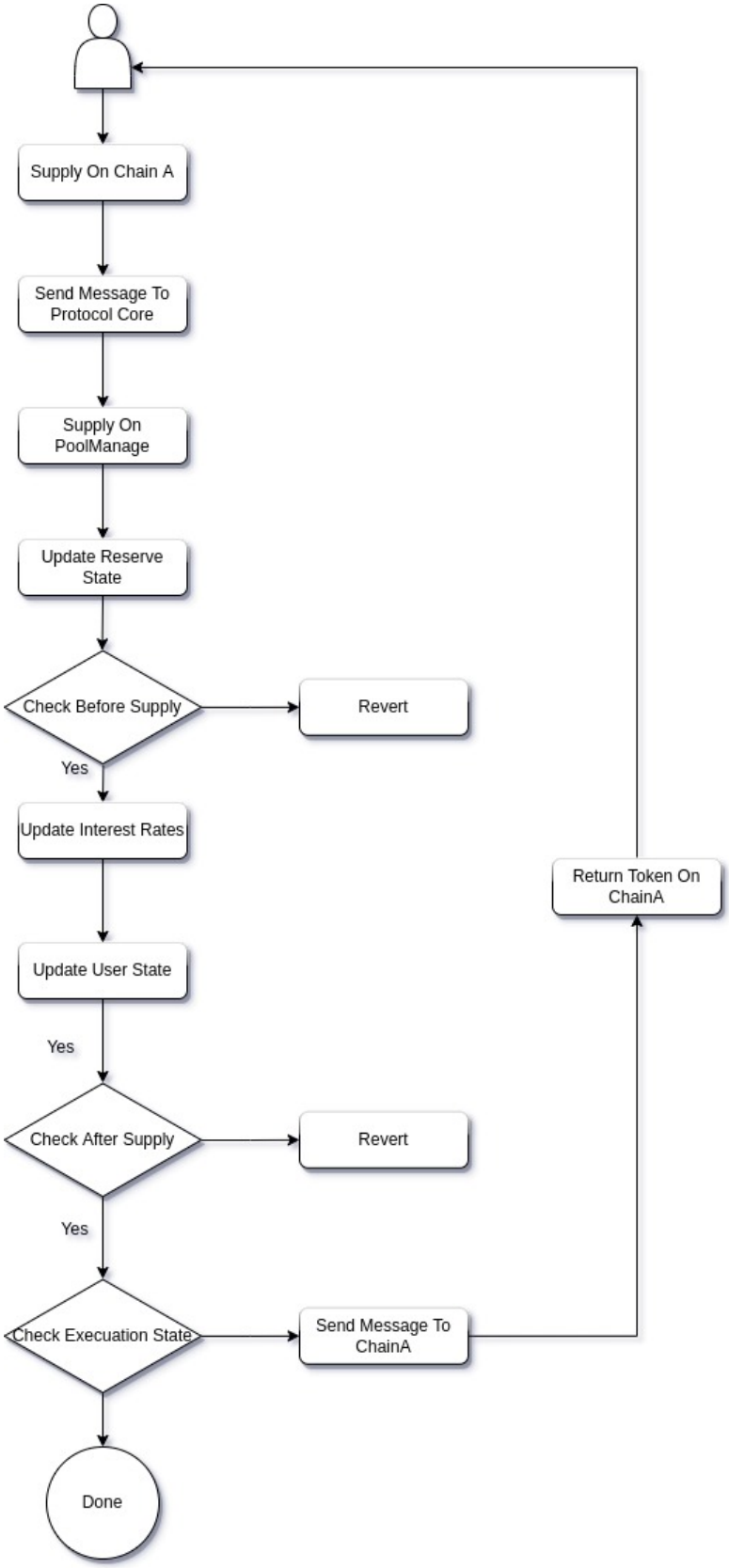
4 协议合约

协议核心采用EIP2535协议构建合约代码，所有数据统一存储在AppStorage中，所有交互行为通过Facet实现。用户操作通过OmniDiamond代理合约对协议核心进行delegateCall调用。协议合约采用如下架构的好处有：1）存储和交互行为完全分离；2）交互行为合约非常容易升级；3）通过OmniDiamond代理合约统一调用，合约升级不会对前端应用产生任何影响。

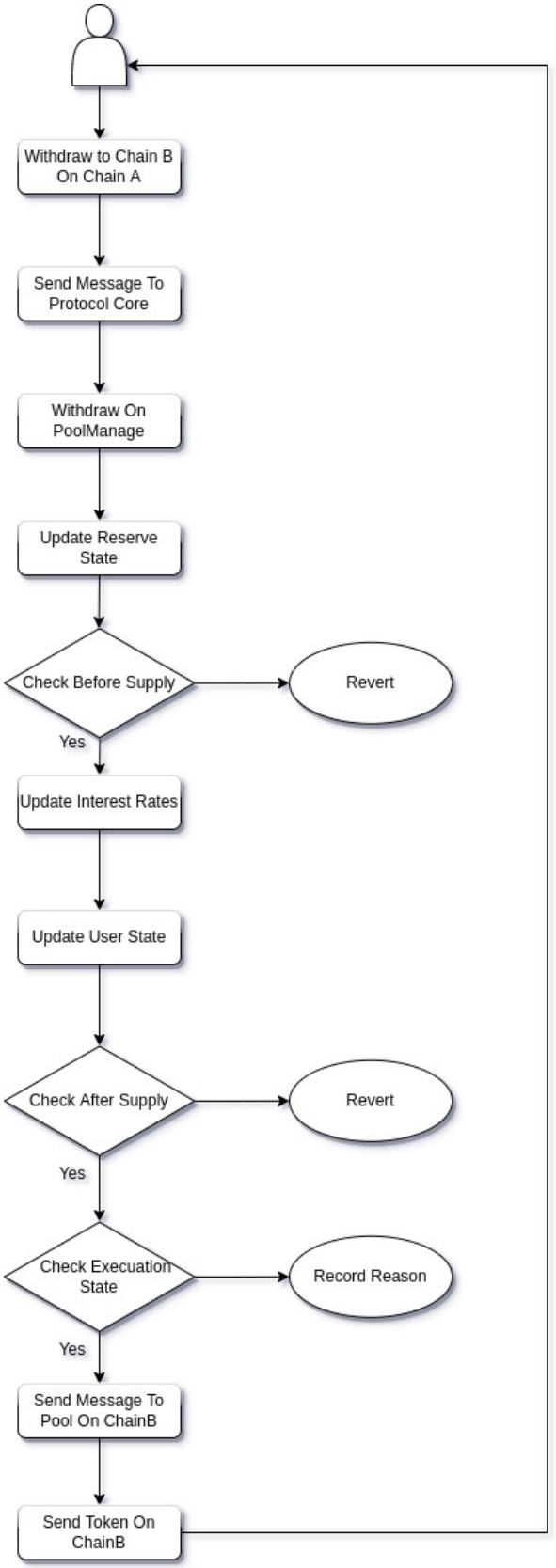


5 交互

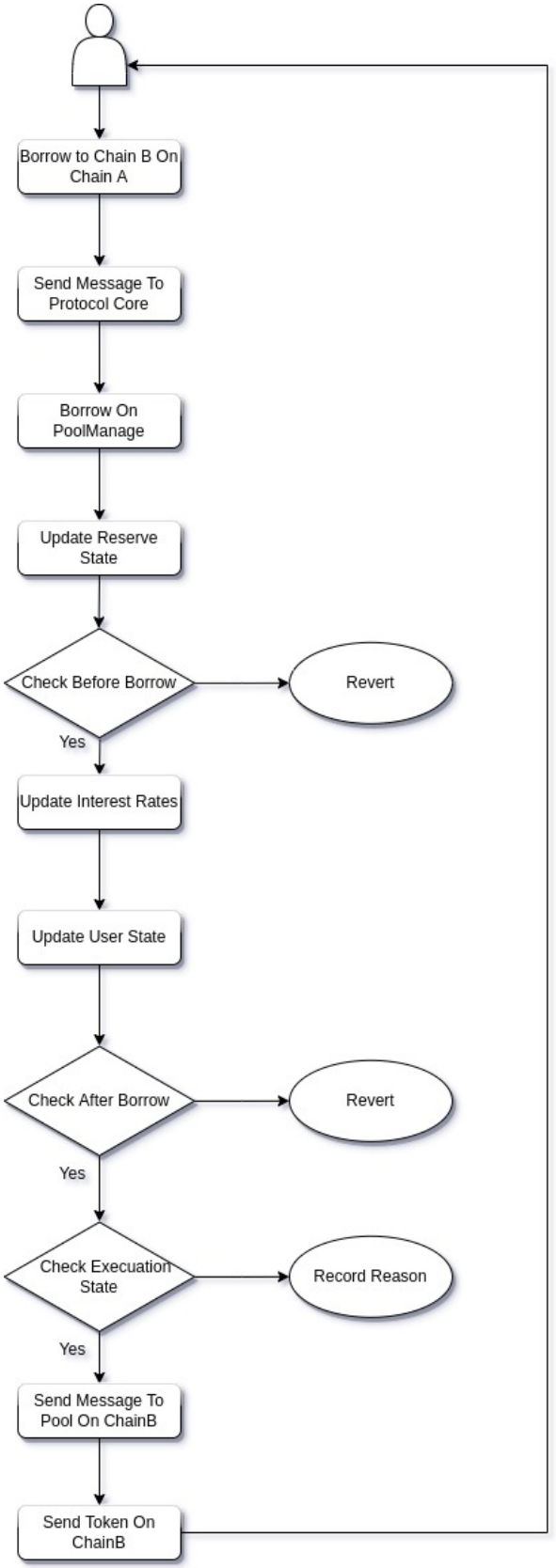
5.1 充值


Supply On Chain A
Send Message To Protocol Core
Supply On PoolManage
Update Reserve State
Check Before Supply
Revert
Yes
Update Interest Rates
Update User State
Yes
Check After Supply
Revert
Yes
Check Execuation State
Send Message To ChainA
Return Token On ChainA
Done

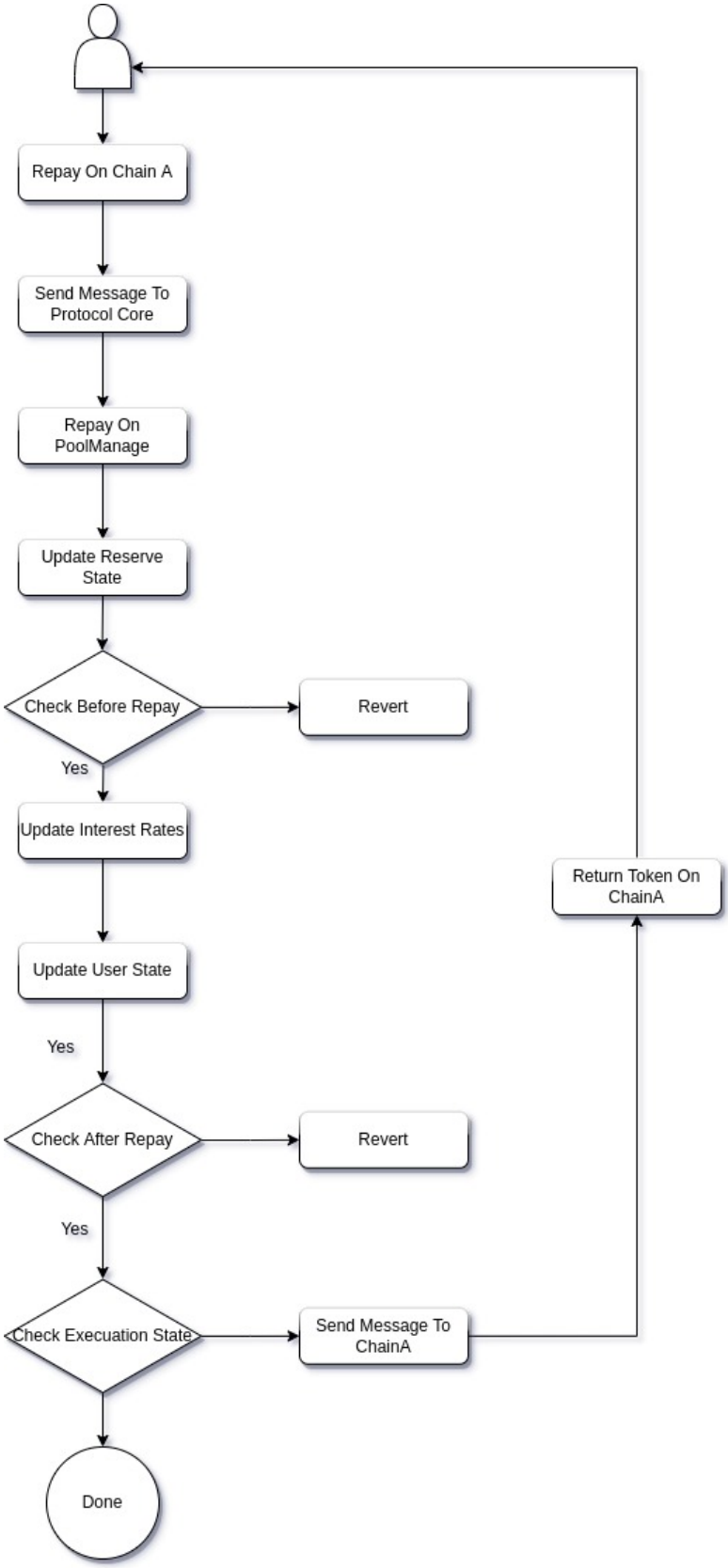
5.2 提现


Withdraw to Chain B On Chain A
Send Message To Protocol Core
Withdraw On PoolManage
Update Reserve State
Check Before Supply
Revert
Yes
Update Interest Rates
Update User State
Check After Supply
Revert
Yes
Check Execeution State
Record Reason
Yes
Send Message To Pool On ChainB
Send Token On ChainB

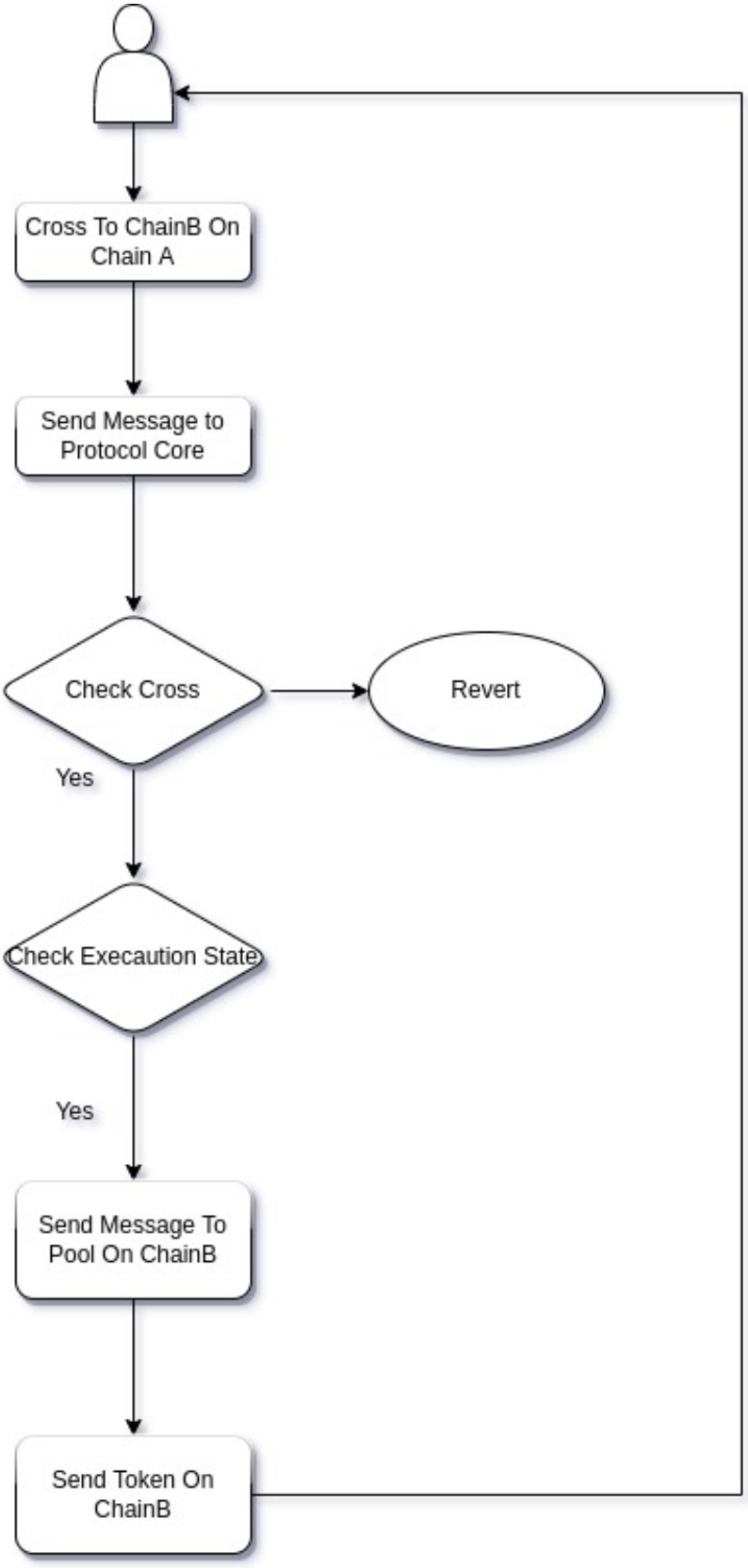
5.3 借贷


Borrow to Chain B On Chain A
Send Message To Protocol Core
Borrow On PoolManage
Update Reserve State
Check Before Borrow
Revert
Yes
Update Interest Rates
Update User State
Check After Borrow
Revert
Yes
Check Execeution State
Record Reason
Yes
Send Message To Pool On ChainB
Send Token On ChainB

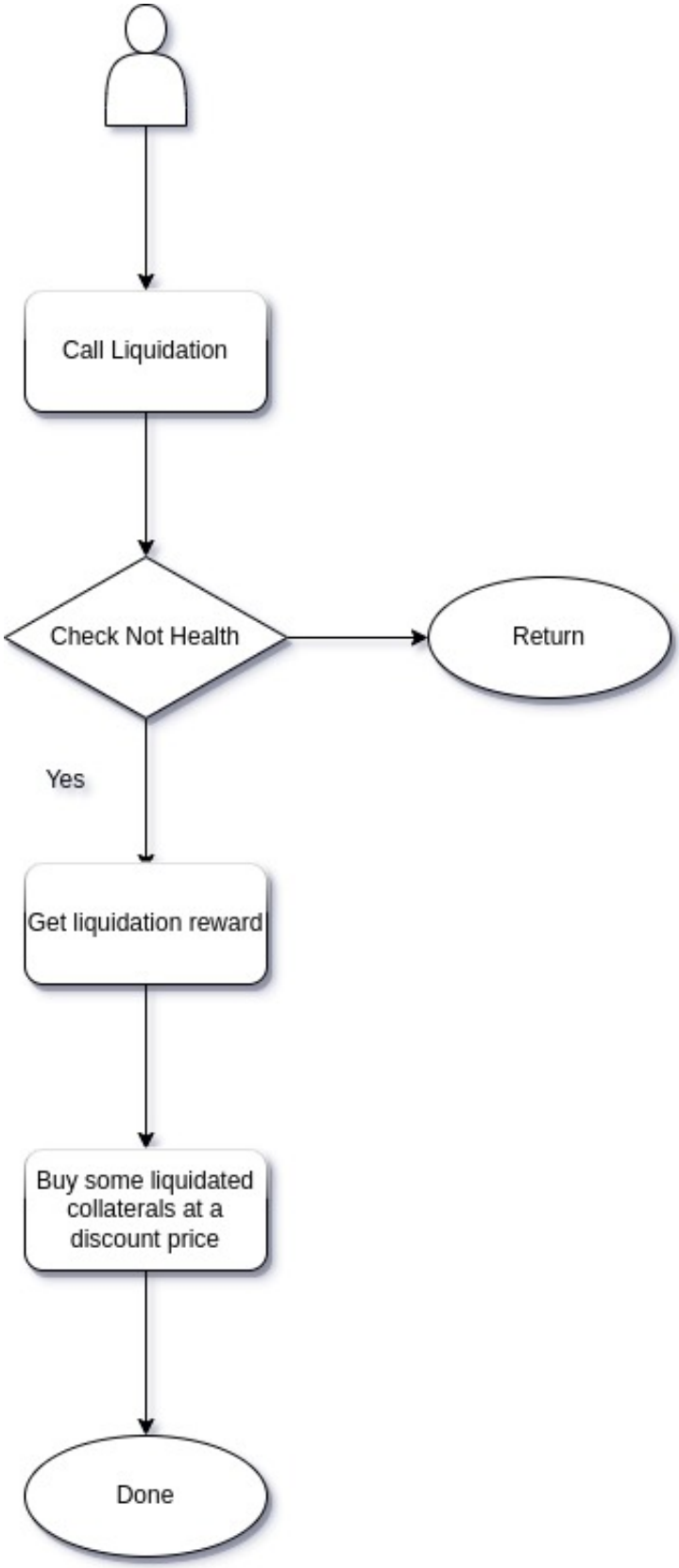
5.4 还款


Repay On Chain A
Send Message To Protocol Core
Repay On PoolManage
Update Reserve State
Check Before Repay
Revert
Yes
Update Interest Rates
Update User State
Yes
Check After Repay
Revert
Yes
Check Execuation State
Send Message To ChainA
Return Token On ChainA
Done

5.5 跨链


Cross To ChainB On Chain A
Send Message to Protocol Core
Check Cross
Revert
Yes
Check Execaution State
Yes
Send Message To Pool On ChainB
Send Token On ChainB

5.6 清算


Call Liquidation
Check Not Health
Return
Yes
Get liquidation reward
Buy some liquidated collaterals at a discount price
Done

6 展望

协议的设计实现了代币的全链借贷和兑换，同时不可避免的存在一些可以改进的地方。风险控制是开发过程及未来永远需要关注和改进的部分。协议应该尽可能规避风险，控制最大风险规模和预定制风险补救方案。协议是全链生态的，可以进一步做一些有趣前沿的工作。代币的全链借贷和兑换向NFT市场的横向扩展；权益化代币进一步抵押和应用的纵向挖掘等都是未来可以探索的方向。

7 总结

协议借鉴了Aave的一些优秀设计，同时融合代币池以及跨链消息协议形成了全新的全链借贷协议。全链借贷协议通过全链流动性池进行借贷以及跨链操作，相比于现在的DeFi应用已经是走在了最前沿的道路上。这迈出了全链时代的第一步，为全链时代的发展奠定了良好的基础。全链借贷协议通过恰到好处的设计将流动性池进行了统一，为借贷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。