



# 金融启示录项目白皮书

Revelation Project White Paper  
(V1.0)

# 目录

1. 去中心化自治组织 RevelationDAO	4
1.1. 提议投票和执行投票	4
2. 颠覆传统金融的 DeFi 革命——Revelation 协议	5
2.1. Revelation 的组成	6
2.2. Revelation 将持续推动去中心化金融	6
2.3. Logo 设计理念	7
3. 旧世界的金融将被遗忘	9
3.1. 传统的中心化交易所有着无法突破的瓶颈和弊端	9
3.2. 未来公链、基于公链的去中心化交易所都会是热门领域	10
4. 金融启示录将揭开未来金融的新纪元	10
4.1. 治理令牌 RDAO	11
4.2. UNC 稳定币	12
4.2.1. UNC 具有以下特质：	13
4.2.2. UNC 的生成	13
4.2.3. 与 Revelation 资金保险柜的交互方式	14
4.2.4. 高风险 Revelation 资金保险柜的清算	14
4.2.5. Revelation 协议拍卖	15
4.3. 去中心化银行 Defibank	16
4.3.1. 当前区块链资产的弊端	16
4.3.2. Defibank 可以革旧立新	16
4.3.3. Defibank 里的核心概念	17
4.3.4. Defibank 核心逻辑	18
4.4. RevelationSwap 去中心化交易所	19
4.4.1. AMM (Automated Market Revelation)	20
4.4.2. RevelationSwap 的流动性激励	23

4.4.3. RevelationSwap 的架构	24
4.4.4. RevelationSwap 有着其他交易所无法比拟的优势	24
4.5. 去中心化金融衍生品 Rebirth	26
4.5.1. RDAO 抵押	27
4.5.2. RDAO 持有和交易的激励措施	27
4.5.3. 铸造，销毁和抵押率	27
4.5.4. 抵押人，债务人和交易对手	27
4.5.5. UNC 挂钩	28
4.5.6. rTokens 对 RevelationSwap 交易所的有力支持	28
4.5.7. 铸造 rTokens	28
4.5.8. 智能合约处理 rTokens 交易时的步骤	29
4.5.9. 申领费用	29
4.5.10. 销毁债务	30
4.5.11. 债务池	30
4.6. 孵化器（Group wisdom）	32
4.7. 金融启示录的整体架构	32
5. 风险及免责声明	33
5.1. 技术风险	33
5.2. 政策风险	34
5.3. 免责声明	34
6. 项目总结	35

## 1. 去中心化自治组织 RevelationDAO

RevelationDAO 发行一种名为 RDAO 的治理型令牌，全世界范围内持有该令牌的人均可参与 RevelationDAO 项目治理，而由 RDAO 的持有者构成的 RevelationDAO 则是在以太坊区块链上创建的开源去中心化自治组织，也是 Revelation 协议的启蒙和发起人。RevelationDAO 团队的成员都是独立的市场参与者，并非受雇于 Revelation 基金会，他们通过提议和执行投票的方式，来维持项目的运行与发展，RevelationDAO 的最终目标是解散团队，实现完全的去中心化自治。

投票机制是 Revelation 去中心化治理流程中关键的一环，RDAO 持有者有权投票决定每种担保物的风险参数（Risk Parameter）以及能够维持 Revelation 持续发展的各种决策。Revelation 治理的灵活性使得 RevelationDAO 社区能够调整 DAO 团队框架，基于现实情况和新兴挑战来提供整个生态系统所需的服务。

在 RevelationDAO 中，团队的成员被划分为不同的角色。例如，治理协调员（Governance Facilitator）主要负责主持沟通和治理流程；风险团队（Risk Team）成员则是通过金融风险研究和起草关于引入新型担保物和管理现有担保物的提案来支持 Revelation 治理等。

通过由提议投票和执行投票组成的科学型治理系统，RDAO 持有者可以管理 Revelation 协议及 UNC 的金融风险，从而确保协议的稳定性、透明性和高效性。RDAO 投票权重与投票者存在投票合约中的 RDAO 数量成正比。换言之，投票者在合约中锁定的 RDAO 代币数量越多，其拥有的决策权就越大。

### 1.1. 提议投票和执行投票

Revelation 的治理流程包括提议投票（Proposal Voting）和执行投票（Executive Voting）。其中提议投票的目的是在进行执行投票之前，先在社区内形成一个大致的一致。这有助于确保治理决策是经过仔细考虑，且在进入投票流程之前就已达成一致的。执行投票的目的则是批准/驳回对系统状态的更改。

任意以太坊地址都可以部署有效的提议合约。从技术层面来说，Revelation 治理里的每一类投票都是由智能合约管理的。提议合约（Proposal Contract）是通过编程的方式写入了一个或多个有效治理行为的智能合约，提议合约只能执行一次，一旦执行了，它就会立即对 Revelation 协议的内部治理变量进行更改，并且在执行之后，该提议合约就不能再度使用。

RDAO 代币持有者可以通过投批准票来选出有效提议（Active Proposal），获得赞成票最多的以太坊地址的提议会被选为有效提议，有效提议会获得 Revelation 协议的内部治理变量的管理权限，然后修改这些参数。

当前 Revelation 治理里面拥有治理权的管理人员拥有的权限如下：

- 上架新的 UNC 市场；
- 对每个代币市场的利率模型进行升级；
- 提取 UNC 准备金；
- 选择新的管理员、或者一个 DAO 组织来管理社区；
- 引入新的担保物类型，并为其设置一组风险参数；
- 修改、乃至增加一种或多种现有担保物资产类型的风险参数；
- 触发紧急关停；
- 升级系统；

总之 Revelation 协议治理机制的设计目标是尽可能灵活化，并具备可升级性。如果 Revelation 系统在社区的引导下成熟起来，那么从理论上来说，提议合约的形式也会变得更高级，比如一个提议合约可以绑定多项提议。不过，这些改进仍待 RDAO 持有者共同决定。

## 2. 颠覆传统金融的 DeFi 革命——Revetation 协议

DeFi，全称为 Decentralized Finance，即“去中心化金融”或者“分布式金融”。

“去中心化金融”，它是与传统的中心化金融相对的，指建立在开放的去中心化网络中的各类金融领域的应用，目标是建立一个多层面的金融系统，以区块链技术和密码货币为基础，重新创造并完善已有的金融体系。

区块链+金融，这是多数人对 DeFi 的理解。DeFi 是为了解决传统金融弊端诞生的，在降低中心化机构的组织作用和中介费用、消除了地域和金融监管限制等方面，已经初步开始展现出无可替代的作用。此外，DeFi 类应用的存款利率不错，对于长期持币的用户和偏好投机者中有很强的吸引力。甚至在那种无法在行情的波动中争取收益的特殊时期，币圈用户在 DeFi 平台理财的需求得到提升，借贷盘活了存量资金，还吸引了一定的外部资金。

具体来说，DeFi 一般是指基于智能合约平台（例如：以太坊）构建的加密资产、金融类智能合约以及协议。目前来讲，DeFi 的业务以抵押借贷为主，这也导致了很多朋友形成了“DeFi=借贷”固有思维。但 DeFi 是一个极具潜力的金融市场，它能形成一个相对完整闭环的生态系统，有望成为加密史上继比特币之后的第二个突破。它之所以能在很短的时间内爆火，究其原因，不仅是由于其自身具备了传统金融所不具备的优势，而且与时代和当下金融发展的大环境有着密切的关系。正是在 DeFi 运动飞速发展的大时代背景下，Revelation 协议应运而生。

Revelation 协议（全称“Financial Revelation”），也即“金融启示录”，它是以太坊上专业的一站式 DeFi 应用平台，由去中心化组织 RevelationDAO 发起和管理。

## 2.1. RevelationDAO 的组成

Revelation 协议致力于成为以太坊用户最广泛使用的 DeFi 应用平台。它将推出：RevelationSwap 去中心化交易所、UNC 稳定币，治理令牌 RDAO，去中心化金融衍生品 Rebirth，去中心化银行 DeFibank, 去中心化孵化器（Group wisdom）等功能及组成部分，旨在打造去中心化金融综合体（经济体），建立一个多层面的金融系统。

## 2.2. Revelation 将持续推动去中心化金融

Revelation 协议将直击传统中心化金融的痛点，并且有效解决传统中心化金融中透明度低、信任成本高等诸多问题。它可以将信任在机器和代码上重建，使用户无需任何可信任中介机构的担保即可放心的操作；任何人都有访问权限，没人有中央控制权；所有协议都将是开源的，因此任何人都可以在协议上合作构建新的金融产品，并在网络效应下加速金融创新。

Revelation 协议将以区块链技术和密码货币为基础，重新创造并完善已有的金融体系，在资金追逐可以炒作的热点中，Revelation 既有市场潜力，又有实际应用，并且由于金融本身是区块链最容易落地的应用方向，因此它必然会成为当前时代区块链领域最优落地场景，结合最新最具代表性的技术，它必将推出一场颠覆传统的史诗性 DeFi 革命。

## 2.3. Logo 设计理念



它以生命自由和颠覆传统金融弊端为目的，是一条任重道远的革新之路，亦是不断自我斗争和自我超越之路，在这个改变外部并不断自我进化的过程中，自由意志是它源源不断的动力，所有人的行动追寻和遵从光明的引导。

## 设计组成



Bible



Savior



Wing

**Revelation** 的 logo 是自由意志的体现，呼唤光明与信仰的指引，由代表启示与引导的圣经，为人类献身而获得重生的救世主，为追寻光明与自由展翅高飞、搏击长空的雄鹰化作的羽翼主要元素构成。

### 圣经——人类光明最后的指引。

圣经中的最后一部预言，叫做《圣经启示录》（**Book of Revelations**）。在所有预言里，圣经启示录可能是对于人类最后这段时期讲得最准确、最详细的。《启示录》是一本成全的书，是神从万世以前所预定要成全的事情的最终应验，里面包含了无数的含义，它虽然是一部预言书，但它的中心内容还是救赎的计划，对世人具有警戒、劝勉的作用，时刻提醒人们不要偏离教训。创世纪指明了救赎计划的开始，启示录则预言了救赎计划的完成。

金融启示录亦是如此，在 **Revelation** 治理规则的引导下，由来自世界各地的 **RDAO** 持有者组成的 **RevelationDAO**，通过提议投票和执行投票的方式所形成的去中心治理规则网络，正如启示录对的预言一般，只要我们坚固我们的信心，只要我们的信仰永不动摇，必能在启示录的指引下得到救赎，最终到达成功与理想的彼岸。

### 耶稣——伟大的救世主、光明的预言者

他为全人类而死，亦为全人类复生，必要于世界穷尽的审判之日在荣光中降临、建立荣耀的天国、给善带来最后的胜利。

金融启示录不仅是一种机遇，更是一种化茧成蝶颠覆自身的挑战。世界的变革必然伴随着挑战，而每一个挑战、每一个横亘在我们面前的难关，都是打开自我成就之门的

钥匙，在对传统的金融桎梏发起挑战并坚持努力之后，Revelation 必然能够站上金融革命之路的巅峰。



### 羽翼——鹰击长空、振翅高飞

自由本应是与生俱来的特权，然而现实却令它可悲的变成一种奢侈。在这个越来越容易让人感受到失望的现实时代中，人们越来越需要勇气的力量。

雄鹰是勇敢与力量的象征，而羽翼则是它与现实斗争的武器，它是一种自由意志的体现，以自己的意志为主导，以羽翼为舟，以信念为剑，追寻光明，摒弃黑暗，必将于高空翱翔，俯视那些依旧只甘于懦弱最后只得卑微的化身为蝼蚁一般的生命。



金融启示录想要完成引导颠覆性的革命，不仅需要光明的引导，还要有勇气与坚持。待到冲破阴霾升上云端的那一刻，前路必定铺满金色的光芒。到了那个时候，自由不再是奢侈，每个人的人生，都可以如展翅的雄鹰，在云端之上向着彩虹自由的翱翔。



### 3. 旧世界的金融将被遗忘

去中心化交易所，顾名思义，去掉传统交易所一切可去的中心化环节，资金在用户钱包地址或者交易智能合约中，由用户完全控制。当用户发起交易时，交易所执行智能合约来完成交易，资产划转在链上完成，所有交易记录链上可查，公开透明。

去中心化交易所跟一般中心化交易所最不一样的地方，就是交易行为发生在区块链上，以数字资产的借贷交换为例，两者不一样的地方在于：

中心化交易所：在交易所本身的数据库中增减用户资产字段。

去中心化交易所：在区块链上直接交换，加密货币会直接发回使用者的钱包，或是保存在区块链上的智能合约。这样直接在区块链上交换的好处在于交易所并不持有用户大量的加密货币，所有的加密货币会储存在区块链上使用者的钱包或由智能合约管控，因而能够极大程度的提高隐私性，并且排除任何暗箱操作的可能性。

#### 3.1. 传统的中心化交易所有着无法突破的瓶颈和弊端

##### （1）传统的中心化交易所需要高昂的上市费用

目前，绝大多数交易平台收取高昂的数字资产上线费用，此举导致交易平台在选择上线数字资产时倾向于利益最大化币种，从而间接损害了投资者手中优质币种的价值。

##### （2）传统的中心化交易所资产保护措施不够完备

在过去的十一年里，已经发生了太多起中心化交易所被黑客攻击的事件，就连大名鼎鼎的 Mt.Gox 和币安也无法幸免于难。直到现在，黑客的偷窃尝试也从未停止，每天都有黑客在试图通过各种方法寻找入侵中心化系统的漏洞，毕竟动辄数以十亿计的交易量，并且其中大多数储存在交易所的服务器上，这无疑是诱人的蜜罐。

##### （3）中心化交易所稳定性不足

目前现有的中心化交易平台大量存在技术架构落后、系统不稳定的问题，高峰期经常宕机。这些都让用户无法及时、有效地进行交易等各种操作，投资时效性差致使投资受损，极其严重地影响到用户的利益，成为影响交易市场发展的瓶颈。

##### （4）中心化交易所缺乏流动性

中心化交易所呈现出一种状态，在其上数额特别巨大的订单很难匹配。即使是最繁荣的活跃期，对于传统的中心化交易所来说，想要撮合成交一笔数额巨大的订单也不是一件容易的事情。

中心化交易所呈现出的另一种状态是：市场碎片化——但并不是去中心化的，全球资产被划分成若干个主要市场，却没有任何一家在交易量上特别领先，这最终将导致流动性问题。

#### （5）中心化交易所上的用户面临高风险

传统的交易所的弊端很明显，例如：潜在的操作问题、市场操纵、硬件故障、等待时间过长、拔网线.....甚至是交易量上升也能引发各种潜在问题。

#### （6）中心化交易所缺乏信任与透明

发生在中心化交易所上的交易进程和实际成本都不透明，手续费往往还很高，由于高峰期的订单不能得到有效管理，通常会高于已经公布的费用并且会有更多的延误。同时，有些中心化交易所甚至还能进行违法的提前交易。

#### （7）缺乏有经验的用户

市场充斥着纯粹的投机者，根本不知道处理加密货币的安全途径。

综上所述，由于中心化交易平台的种种不足，用户对去中心化交易平台的强烈需求已经出现,传统的中心化交易平台必将被 DeFi 运动引领的去中心化金融所取代，这是顺应经济发展的必然趋势。

### 3.2.未来公链、基于公链的去中心化交易所都会是热门领域

就目前的形势，区块链领域的很多从业者及投资者都十分看好去中心化交易所，未来公链、基于公链的去中心化交易所都会是大家抢占的领域。对交易所而言，当流量不再是通过有吸引力的项目获得的时候，有自主技术服务能力来扩展自己的用户边界的去中心化交易所一定会是未来交易行业中的热点。

随着以太坊公链为主的 DeFi 运动逐渐渗透到其他公链和领域，去中心化交易所不管从范围还是质量上都已经发生了很大的变化，即将改变金融和其他大宗商品的交易和融资方式，**Revelation** 将使用链下匹配引擎将中心化平台的速度及功能与去中心化交易所的非托管好处结合在一起，提供安全的自我托管和无边界金融，通过完全的链上透明，可以减少机器人、中间商以及中心力量的无须信任的交易流程，并允许各种玩家无须信任的参与进来，具有极强的生命力及发展潜力。

## 4. 金融启示录将揭开未来金融的新纪元

**Revelation** 协议即金融启示录，将建立一个不受中心化权力机构或管理者影响的公共基础设施，并在全球范围内采用。

下面，本白皮书将从通俗易懂的角度讲解构建在以太坊区块链上的 Revelation 协议六大组成模块，它们分别是：治理令牌 RDAO、去中心化稳定币 UNC、去中心化银行 Defibank、去中心化交易所 RevelationSwap、去中心化金融衍生品 Rebirth、孵化器 Group wisdom。

## 4.1. 治理令牌 RDAO

RDAO 是 Revelation 协议发行的治理令牌，我们已经知道 Revelation 协议由去中心化自治组织 RevelationDAO 发起和组建，而 RevelationDAO 又是由 RDAO 的持有者组成，这些 RDAO 的持有者是整个金融启示录的受益者，以持有 RDAO 数量为基准来执行对等的投票治理权。

RDAO 还是基于智能合约的通缩令牌，可与任何不受信且社区驱动的加密货币协同工作。RDAO 的每笔交易都会带来套利机会。交易吸引了流动性，而流动性又持续的增加交易。在流动性波动的过程中，RDAO 都会进行通缩对冲，其中每笔交易都销毁 1% 的交易额就是 RDAO 的核心算法之壹。

Revelation 治理令牌 RDAO 可以看做是纯治理型 DeFi 令牌，RDAO 的价值则主要通过治理来捕获：RevelationDAO 组建后，RDAO 持有者可以投票决定各个 DeFi 协议的重要参数，比如 Revelation 协议是否进行分红、Revelation 协议分红比例、Revelation 协议交易手续费率、UNC 稳定币债仓利息、UNC 稳定币爆仓罚金等，还包括可以投票决定各类提案，如 RDAO 销毁方案、DeFi 协议逻辑调整、DeFi 协议开发计划等。RDAO 持有者由于有决定 DeFi 协议重要参数的权利，因此将成为 Revelation 的决策参与者，并且从治理中收益。

只要 RDAO 持有者还有权投票批准可以在 Revelation 协议上用作生成 UNC 的担保物并投票制定风险系数。另外，一旦用户通过 RevelationSwap 生成稳定币 UNC，则意味着用户对系统有了一笔债务，需要归还 UNC 并支付稳定费，才能取回 Defibank 中锁定的担保物，因此在偿清贷款时，除了还回相应数量的 UNC，还需附加一部分费用，这部分费用可视为贷款利息，目前，该笔费用必须用治理型令牌 RDAO 来支付。

Revelation 在以太坊主链发行 RDAO 令牌，发行总量为 2.1 亿枚，Swap 预售发行 10%，当预售发行的 2100 万代币兑换完成以后，后续将采用质押挖矿和流动性挖矿奖励的方式来对剩余的部分进行开发，矿池总量 1.575 亿枚，以以太坊每个区块产出约为 5 枚，每日总计产出约为 28800 枚，计划约 15 年挖完，具体分配规则如下：



图：Revelation 分配规则

其中总量的 10% 即 2100 万枚 RDAO 为流动性挖矿奖励为：生成稳定币（UNC）奖励 500 万枚；RevelationSwap 做市奖励 500 万枚；Defibank 存币、贷币奖励 500 万枚；去中心化金融衍生品 Rebirth 合成资产奖励 500 万枚；孵化器 Group wisdom 的孵化贡献奖励 100 万枚。

开发团队所得的 5% 部分 (1% 用于早期初始流动性创建)，4% 锁仓三年，第四年开始每年解锁 20%。

## 4.2. UNC 稳定币

区块链技术提供了前所未有的机会，可以用来很好的解决公众对功能失调的中心化金融系统的不满和不信任。通过将数据分布到计算机网络中，该技术可以让任意团体中的每位成员都享有透明性，不受中心实体的控制，由此诞生出无偏袒、透明且高效的免许可型系统，它可以改善当前的全球金融和货币结构，更好地为公众利益服务。

比特币就是为此而创建的。但是，虽然比特币从许多方面来说都是一种成功的密码学货币，它却并不是一种理想的交换媒介，因为它的供应量是固定的，而它的投机性又造成了价格的波动，使其无法进一步发展成为主流货币。然而，UNC 的优势却能弥补比特币的这一致命短板，这是因为 UNC 的设计目标就是将价格波动性降至最低。

UNC 是一种去中心化且中立的资产担保型加密货币，其价格 1:1 软锚定美元，是一种以太坊上的，旨在维持价格和货币功能的去中心化抵押型稳定币。其发行是去中心化、无偏见、一视同仁的。由于波动性低，UNC 能够抵御恶性通货膨胀，并为全球范围内的任意个体提供经济自由和机会。

UNC 的生成、访问和使用门槛都很低。用户通过使用 Revelation 协议来创建智能合约并存入资产来生成 UNC，这个过程既是 UNC 进入流通领域的过程，也是用户获得流动性的过程。此外，用户也可以从中介或交易所处购买 UNC，或者更简单一点，只

要愿意接受 UNC 来支付，那就能得到 UNC。但无论是用户自己生成的、买到的还是收到的 UNC，用起来都跟别的加密货币没有区别：用户可以将 UNC 发送给其他人，用它来购买商品和服务，甚至可以通过 Revelation 协议功能，把 UNC 转入储蓄账户。

#### 4.2.1. UNC 具有以下特质：

##### （1）UNC 是一种价值贮藏物

价值贮藏物指的是能够保值的，不会随时间流逝而大幅贬值的资产。UNC 是一种稳定币，其设计使其在波动巨大的市场中也能保证价格稳定。

##### （2）UNC 是一种交换媒介

交换媒介指的是一切可代表价值标准、被用来促进商品或服务的出售、购买或交换（交易）的事物。在全世界不同类型的交易中，都能使用 UNC 稳定币来达成交易。

##### （3）UNC 是一种记账单位

记账单位是一种标准化的价值度量衡（软锚定美元），被用于商品和服务的定价。目前，UNC 的目标价格是 1 USD（1 UNC= 1 USD）。

##### （4）UNC 是一种延期支付标准

在 Revelation 协议中，UNC 还被用来清偿债务，正是这一优势使得 UNC 更为出众。

#### 4.2.2. UNC 的生成

UNC 的创造、价值背书以及价格稳定，都是通过存入 Revelation 资金保险柜的担保品资产来实现的。担保品资产指的是由 RDAO 持有者投票纳入协议的数字资产。

只要经过 RDAO 持有者的批准，任何基于以太坊的资产都可以在 Revelation 协议上用作生成 UNC 的担保物。在许可某种资产成为担保品时，RDAO 持有者会选择具体的风险参数，稳定型资产一般选择较为宽松的风险参数，风险型资产可能要选择较为严格的风险参数。在做出上述以及其他决策时，RDAO 持有者都是通过 Revelation 去中心化治理流程做出的决定。

这些经过批准的担保品资产，可以存入使用 Revelation 协议生成的 Revelation 资金保险柜智能合约来生成 UNC。用户可以通过多种用户界面来访问 Revelation 协议并创建资金保险柜。创建资金保险柜并不复杂，但是生成 UNC 即意味着用户对系统有了一笔债务，需要归还 UNC 并支付稳定费 RDAO，才能取回资金保险柜中锁定的担保物。

资金保险柜本质上是非托管型的，用户可与资金保险柜和 **Revelation** 协议直接交互。只要担保物的价格不低于最低必要水平（即清算率 **Liquidation Ratio**），用户都可以享有对该担保物完整且独立的控制权。

### 4.2.3. 与 **Revelation** 资金保险柜的交互方式

#### Step1: 创建资金保险柜并锁入担保物

用户通过 **Revelation** 门户界面上的入口来创建 **Revelation** 资金保险柜，并锁入特定类型和数量的担保物来生成 **UNC**。存入资金之时，该资金保险柜即被视为有担保的。

#### Step2: 通过有担保的资金保险柜生成 **UNC**

将担保品资产锁入一个资金保险柜之后，该资金保险柜所有者便可使用任意非托管型密码货币钱包来发起、确认交易，生成出一定数量的 **UNC**。

#### Step3: 偿还债务并支付稳定费

若想取回部分或所有担保物，资金保险柜所有者必须部分或全额偿还他所生成的 **UNC**，并支付 **UNC** 未偿还期间不断累积的稳定费。稳定费只能用 **RDAO** 支付。

#### Step4: 取出担保物

在偿还了 **UNC** 并支付了稳定费之后，资金保险柜所有者可以将全部或部分担保物退回自己的钱包。在完全偿还了 **UNC** 并取出所有担保物之后，资金保险柜就会空置下来，以待其所有者再次锁入资产。

在这些交互的过程中，至关重要的一点是，不同的担保品资产需分置在不同的资金保险柜中。因此，一些用户会拥有多个资金保险柜，采用的担保物类型和担保品率各不相同。

### 4.2.4. 高风险 **Revelation** 资金保险柜的清算

为了确保 **Revelation** 协议中始终有充足的担保物来为未偿还债务背书（未偿还债务即以目标价格（**Target Price**）计算的未偿还 **UNC** 的总价值，任何根据 **Revelation** 治理规定的参数被判定为高风险的 **Revelation** 资金保险柜都会通过自动化的 **Revelation** 协议拍卖流程来清算。**Revelation** 协议的判定依据是比较清算率与该资金保险柜当前的担保品价值-债务比率（**collateral-to-debt ratio**）。每种资金保险柜类型都有各自的清算率，都是由 **RDAO** 持有者基于不同担保品资产的风险状况投票决定的。

### 4.2.5. **Revelation** 协议拍卖



通过 **Revelation** 协议的拍卖机制，如果在系统无法获得担保物价格信息的情况下，依然能对高风险的 **Revelation** 资金保险柜进行清算。在进行清算时，**Revelation** 协议会取出被清算的资金保险柜中的担保物，并使用协议内一个基于市场的拍卖机制将其卖出。这被称为担保品拍卖（**Collateral Auction**）。

通过担保物拍卖获得的 **UNC** 会被用来偿还资金保险柜内的债务，其中包括清算罚金（**Liquidation Penalty**）。

如果担保物拍卖上获得的 **UNC** 足以清偿资金保险柜内的债务，并足够支付清算罚金，该竞拍会转换成反向担保品竞拍（**Reverse Collateral Auction**）以尽可能地减少担保物的出售数量，剩余的担保物则会物归原主。

如果担保物竞拍获得的 **UNC** 不足以清偿资金保险柜内的债务，那么其亏损部分就会变成 **Revelation** 协议的负债，由 **Revelation** 缓冲金（**Revelation Buffer**）中的 **UNC** 偿还。如果缓冲金中没有足够的 **UNC**，**Revelation** 协议就会触发债务拍卖（**Debt Auction**）机制。

具体拍卖流程为：

当某个大额资金保险柜的质押率跌至最低阈值以下时，拍卖清算商（**Auction Keeper**）检测到这一现象并对该资金保险柜启动清算程序。

每个清算商都可以有自己的竞拍策略（**bidding model**）。竞拍策略中包含担保物的竞标价，这个竞标价不可拆分，只能设置为竞拍的总价，发起清算的清算商将自己竞拍策略中的代币价格作为担保物拍卖第一阶段的起拍价，在该阶段，投保者使用 **UNC** 来竞拍固定数量的担保物，价高者得。

当清算商设置了竞拍价，并决定用 **UNC** 竞拍清算负债的资金保险柜里的担保物时，这部分 **UNC** 会从资金保险柜引擎转移到担保物竞拍合约内。等到某一笔充进担保物竞拍合约的 **UNC** 能够偿还系统债务并支付清算罚金，担保物竞拍的第一阶段就结束了。

为了用自己竞拍策略中的价格买到担保品，清算商还要在担保物竞拍的第二阶段提交报价。这一阶段的目标是在市场竞争的情况下，将尽可能多的担保物归还给资金保险柜的所有者。在这一阶段，清算商要使用固定数量的 **UNC** 去竞拍尽可能少的 **ETH**。本次竞标获得的 **UNC** 会从资金保险柜引擎转移到担保物竞拍合约内。等到投标期结束，竞标截止之后，该竞拍管理者中标，取得担保物，到了这个时候，担保物竞拍才算彻底结束。

总结来说，**Revelation** 协议采用超额抵押与爆仓清算的风控机制，基本上凡是持有以太坊的人都可以生成 **UNC**，等同于通过质押以太坊获得低息贷款。流通中的每个 **UNC** 都是由超额资产背书的，且担保物的价值会高于 **UNC** 债务的价值，而且所有 **UNC** 交易都在区块链上公开可见，可以规避市场波动，以足额抵押物为每个 **UNC** 提供价值支撑，进而它可以进一步满足用户的杠杆交易、获取流动资金等多种需求。

UNC 稳定币的特质决定了它的发展潜能，它将成为去中心化金融事业的基石，成为 Revelation 协议中至关重要的一环。

### 4.3. 去中心化银行 Defibank

Defibank 区块链银行是一个可以通过借贷双方的需求，依据算法自动调节存款和贷款利率的借贷工具，平台上提供的利率可以反映出大众对协议的信任，用户可以将自己持有的以太坊注入到这里，从而无需依赖任何中心实体就能从协议中借出一笔美元价格稳定的贷款。然后，用户就可以把这笔 UNC 借给那些不想通过质押以太币借 UNC 的人来赚取利息。

Defibank 可以按一个区块（约 15 秒）为一次计息，能够避免 P2P 借款组合下匹配难、体验差、门槛高、市场流动性不足等各类问题，从而减少借贷双方的摩擦成本，同时让用户的数字资产真正展现其应有的时间价值。

#### 4.3.1. 当前区块链资产的弊端

当下区块链资产是存在弊端的，主要体现在以下两个主要问题上：

##### （1）借贷机制极为有限，导致资产错误定价

比如说一些没有实际价值的代币因为不能借到，没办法对其做空，反而会导致该类代币价格虚高，从而产生与其实际价值极不对等的现象。

（2）无论是在交易所内还是在交易所外，都存在着巨额的存储成本和巨大的波动风险，所以无论是将数字资产存在交易所还是自己的钱包，都没有一个自然利率可以用来消除这个成本。

难道真的没有办法去消除这些令人生厌的弊端吗？Defibank 正是答案。

#### 4.3.2. Defibank 可以革旧立新

Defibank 是建立在以太坊上，存款和借款供需双方关系通过算法来计算利率的资金池模式。存款者直接向 Defibank 存款，获取浮动的利息收益，而无需和对手方协商到期日、利息率抵押物等。





图：Defibank 的核心架构

在 Defibank 上，用户可以通过去中心化的系统，无偿借用以太坊代币，却能摒弃现有方法的所有缺陷，使适当的货币市场发挥作用，并创建一种安全的正收益的方法来存储资产。

### 4.3.3. Defibank 里的核心概念

要想理解 Defibank，首先需要了解一下它里面的一些核心概念，如：底层资产（Underlying Asset）；dToken；兑换率（Exchange Rate）；使用率（Utilization Rate）；借款利率（Borrow Rate）；存款利率（Supply Rate）；抵押率/抵押因子（Collateral Factor）；准备金（Reverse）；准备金率（Reverse Factor）；清算（Liquidation）；关闭因子（Close Factor）等等。

**底层资产（Underlying Asset）：**用户提供到 Defibank 的资产如 ETH/BTC 等为底层资产。

**dToken：**用户抵押底层资产后，系统会根据一个兑换率来给用户返还一定数量的 dToken，如用户存入 ETH 则会反还 dETH，另外当用户需要提取底层资产的时候也需要用到 dToken 去兑换。

Defibank 目前有两种类型的 dToken：DErc20 和 DETH，其中 DErc20 封装的是 ERC-20 资产，而 DETH 则封装的是以太坊。

**兑换率（Exchange Rate）：**这个概念所指的是 dToken 和底层资产的兑换比例，当没有任何人存入资产生息时，会有一个 initial Exchange rate，兑换率随着时间的推移会不断增加，由于资产借款人应计利息，所以它的计算公式等于：

$$exchangeRate = \frac{underlyingBalance + totalBorrowBalance_a - reserves_a}{dTokenSupply_a}$$

**使用率 (Utilization Rate) :** 每个市场  $a$  的利用率  $U$  将供给和需求统一为一个变量:

$$U_a = \text{Borrows}_a / (\text{ash}_a + \text{Borrows}_a)$$

**借款利率 (Borrow Rate) :** 借款利率受到使用率影响

$$\text{Borrowing Interest Rate}_a = 2.5\% + U_a * 20\%$$

**存款利率 (Supply Rate) :** 存款利率的计算需先得到借款利率，和借款利率一样，都是每个区块计算一次，同一个区块的放贷人对于相同的资产获得相同的放贷利率。

**抵押率/抵押因子 (Collateral Factor) :** 针对不同的资产，Defibank 内有着不同的抵押因子，抵押因子的范围是 0-1，代表用户抵押的资产价值对应可得到的借款的比率，为零时则表示该类资产不能作为抵押品去借贷其他资产。

相对与大市值资产，小市值资产的抵押因子会相对较低，因此同样的抵押资产，能借到的资金更少。

**准备金 (Reverse) :** 准备金是协议本身的权益，以便为其运作提供资金。准备金也构成了 cash 的一部分，可用于贷给市场上的借款人。借款人的一小部分利息计入协议，而它是由准备金率决定的。

**准备金率 (Reverse Factor) :** 准备金率定义了应计入准备金的一小部分利息。

**清算 (Liquidation) :** Defibank 中的清算是指当某个用户抵押资产价值小于借款价值时，清算人可以代替被清算人归还一部分欠款，同时清算人可以得到被清算人抵押物 (dToken) 的一定百分比奖励。这个机制可以激励套利者迅速介入，以减少借款人的风险，同时也可以消除 Revelation 协议的风险。

**关闭因子 (Close Factor) :** 在清算过程中，清算人可以帮助贷款人还掉的债务最大比例，在 0~1 之间，这个因子可以被连续调用，直到用户借款订单处于安全状态。

#### 4.3.4. Defibank 核心逻辑

Defibank 的核心逻辑。

我们已经知道整个 Defibank 上活动的参与者有：放贷人、借款人、清算者、社区成员、开发者。

放贷人 (Suppliers) / 借款人 (Borrowers) 存入资产到 Defibank 的货币市场 (Money Market)，放贷人/借款人存入的资产为底层资产 (underlying asset)，Defibank 智能合约按照兑换率发放对应底层资产的 dToken 到用户账户中。计算公式为：

$\text{dToken 数额} = \text{存入底层资产的数额} / \text{兑换率}。$

其中，放贷人存入的资产，既可以享受放贷利息，也可以随时提取。

借款人存入 dTokens 作为抵押资产后，可以从 Defibank 借款，借款上限为抵押资产价值\*抵押因子，其借款上限=SUM (抵押因子\*dToken\_i 余额\*兑换率\*价格)，SUM 表示对所有抵押资产从 1 到 N 的求和。

借款人借出的是底层资产。

借款人还可以先作为放贷人存入抵押资产，然后选择将资产作为抵押物，这样之后，借款人实际上可以享受自己提供抵押物进入资金池的利息，可以一定程度减轻贷款的利息支付。

借款利率由 Defibank 智能合约根据市场对资金的供需关系实时确定，同一个区块内，所有借款人的借款利率相同。Defibank 按照区块数为单位累积借款人利息 (Accrue Interest)。

借款人抵押资产价值同借款价值的比例被称为健康度，如果借款人抵押资产价值低于借款价值，健康度会小于 1，这个时候会发生清算。其中，抵押资产价值=SUM (抵押因子\*dToken\_i 余额\*兑换率\*价格)，SUM 表示对所有抵押资产从 1 到 N 的求和，再将其转换为 ETH。而借款价值则=SUM (借款数额\*价格)，转换为 ETH。清算人地址不能是对应借款地址，即自己不能为自己清算。

通过上述这些设计规则，任何以太币持有者都能够利用构建在以太坊区块链上的 Revelation 协议以免信任的方式来赚取利息。等到多质押 UNC 实现之后，还可以直接实现更多样化的密码学资产投资组合，从而以更多样的方式生息。每个客户都可以根据自己的需求，选择最适合自己的产品。这些产品都可以有深度的共享，并共享相同的风控能力，也正是这些优势，使得 Defibank 在初期就具备强大的竞争能力。

#### 4.4.RevelationSwap 去中心化交易所

基于 Revelation 协议搭建的 RevelationSwap 是一个去中心化交易所，旨在促进 ETH 和 ERC20 代币数字资产之间的自动兑换交易。用户可以自由存入代币进行兑换和提取，不需要中心化交易所的注册、身份验证和提取限制等繁琐而不安全的环节。它的交易对手并不是其他交易用户，而是跟代币池进行交易，并且 RevelationSwap 有自动做市的模型来计算交易价格。

去中心化交易所是 DeFi 生态中非常重要的一环，由于去中心化交易所的完全去中心化、透明、开放的特性，尤其受一些开发者和极客用户的喜欢。RevelationSwap 也可

以被认为是一个 DeFi 项目，因为它试图利用去中心化协议来让数字资产交易过程中彻底实现去中介化。同中心化交易所（CEX）相比，它对于偏好个人安全和隐私管理的用户来说，拥有更高的价值。不仅如此，它在功能上也越来越丰富，越来越有想象力。

#### 4.4.1. AMM

**RevelationSwap** 在做市商自动化的模块应用上，利用既定算法替代人工报价，去掉了中心化的撮合与清结算，在去中心化的领域内可以做到极致的便利。

我们知道“做市商”指的是传统的由“人”或“组织”构成的实体。做市商是流动性的来源，高流动性的市场需要做市商，也反过来会吸引规模化的做市商参与。他们不同于普通交易者，他们是风险中性的，一手持有筹码，一手持有现金，当人们需求增长开始从做市商手里购入筹码时，做市商的库存会变少，现金增加；而当人们对市场不看好开始将筹码抛给做市商时，做市商会积累更多的库存，现金减少。由于自身资本是有限的，在做市商认为两边库存不平衡后，便会对报价做出调整。如果手上筹码过少，则考虑提高报价珍惜筹码，如果手上筹码过多，则会考虑降低询价以尽快卖出。因此，存货变化是市场需求变化的结果和价格的指标，并进一步影响价格和供需。

而自动化做市协议（AMM）从根本上做的事情，正是用流动性池存货变化这面镜子，来模拟价格变化。每个人都可以加入流动性池子，只需要将指定两种资产存入即可，系统即可通过一种复杂的数学算法建立起来的叫做恒定乘积的模型得出资产价格。这种数学模型听起来复杂，但实际原理很简单，它所模拟的东西和前文所描述的个体做市商的行为是一样的——在总资本一定的情况下，保证两边库存的平衡。如果出现失衡，则调整价格。

自动化做市与传统做市相比，区别在于做市商是根据自身判断调整价格变化幅度，而自动化做市模型是按照预设好的数值，每笔交易后，由于库存的变化，自动化做市模型会给交易资产赋予新的价格，如果价格偏离市场价格，会出现套利机会，套利者可以按照偏离的价格成交，获得差价回报的同时将缺少的资产补足进池子。自动化做市就如同一个特殊的自动售卖机，只要有人买走商品，该商品的价格就会提高，且取的越多，价格飙升越快，直到做市商和套利商补货。

因此与传统做市商的盈利模式稍有不同，这种模式下是套利商赚差价，做市商分红。自动化做市真正去掉的环节，不是做市本身，而是和任何区块链应用一样——去中介。然而，中介和信用本是一体两面，没有做市商赚差价的市场，就如同失去搬运工的自然水，达不到最好的流动。

#### Revelation 中的 AMM

普通的交易所都会有限价订单的概念，一般的做市商提供流动性都会设定价格，而这些在 **RevelationSwap** 都没有。在 **RevelationSwap**，做市商只需提供代币资金，剩下的都可以通过机制来解决。

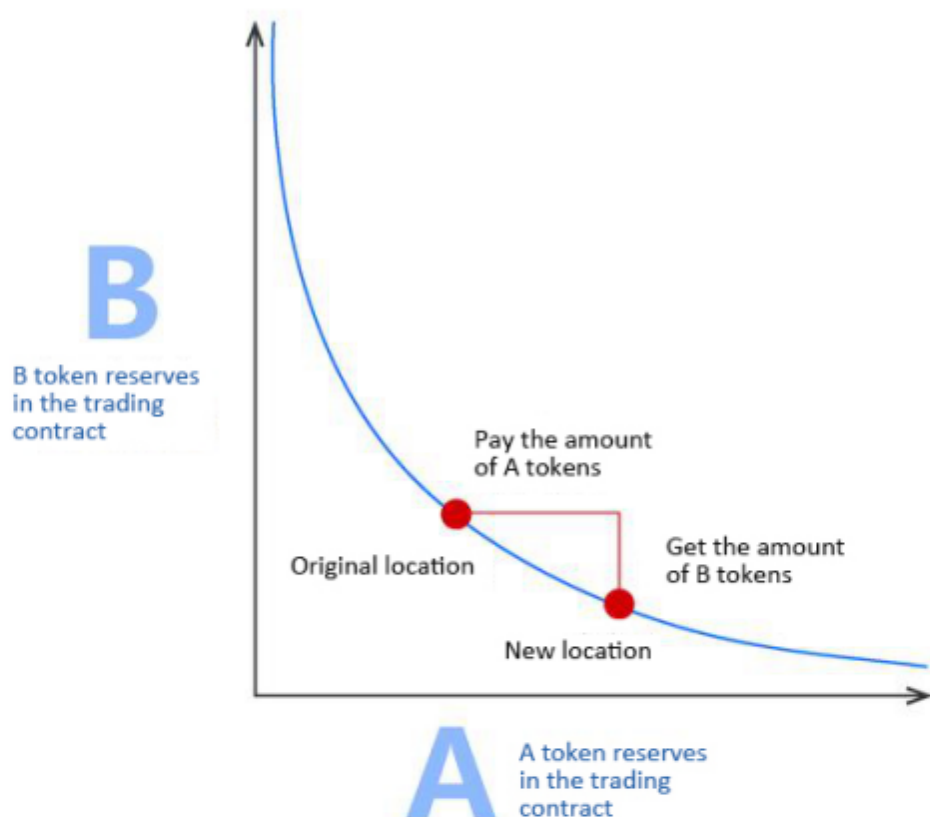
在 **Revelation-swap** 里，做市商也并非真正意义上的做市商，他们大多是普通用户，使用自有资金，继而根据其存入资产占资金池的比例获得份额，分得交易手续费。换句话说，**Revelation** 做市过程实际上是参与一种特殊自动售卖机的众筹，实时分得利润。他们是现代做市商，不需要自有资本，只需用现金借来数字资产，或者用数字资产借来现金，以达到两边的平衡，并最大化资本边界。他们用自己的资产负债表连接各个市场，赚取差价。

普通的交易所需要交易对手，做市商通过设置买入价和卖出价，一是为市场提供流动性，二是可以获得交易的利差。这些设置的价格形成了限价订单。当然这些订单可能成交，也可能不会成交。如果交易所将所有人的订单都集中到两个大型的池中，交易者不会愿意，他们不希望自己的订单跟其他人的订单混在一起。

而 **RevelationSwap** 要做的就是将代币混在一起，同时做市商无须指定其希望买入和卖出的价格，这源于 **RevelationSwap** 自动做市商的设计，它的特色之一就是将每个人的流动性集中到一起，然后根据算法进行做市，也就是说它本质上是基于算法的自动做市服务。**RevelationSwap** 会有一些预定义的规则，根据这些规则它会向用户提供兑换代币的报价。自动做市的规则可以有多种，**RevelationSwap** 采用的是其中一种基于“**Constant Product Market Maker Model**”的变体。它有一个特点很有意思，理论上，它可以提供无限的流动性，可以有很大的订单规模，且不用担心流动池很小。

我们将之称为恒定乘积公式，其公式是  $X*Y=K$ ，其中  $X$  是 ERC20 代币， $Y$  是 ETH， $K$  是常数。

对于 **RevetationSwap** 而言，对应的则是 ERC-20 代币和 ETH 的交易合约中 ETH 和该 ERC20 代币的流动性池的储备量。在这个公式中，该 ERC-20 代币和 ETH 的兑换汇率，将始终处于此公式结果曲线上的某一点。



使用此公式，如果以 **RevetationSwap** 中的交易合约举例，则代表该交易合约储备有  $x$  数量的 A 代币和  $y$  数量的 B 代币。这个合约将始终保持乘积恒定，也就是说  $x * y$  得到的  $k$  值不变。

任何人都可以通过有效改变做市商在  $x * y$  曲线上的位置来进行买入或者卖出代币。

横轴代表卖出的 A 代币的数量，纵轴代表买入的 B 代币的数量。

假设 B 代币是 ETH，而 A 代币是任意一种 ERC20 代币，我们可以通过  $x * y = k$  的公式来理解一下它们的功能：

如果用户决定买入大量 A 代币，那么将导致 A 代币的紧缺，并且导致 ETH 数量的增加。这时用户购买的行为导致了把汇率移动到了  $x * y = k$  曲线上的另一个点。红点将向左移动，也就是买入 A 代币的价格会变得更贵。

我们也可以将 **RevetationSwap** 的交易合约中的 ETH 和 A 代币的相对供应理解为 A 代币的供需关系，这种供需关系决定了 A 代币与 ETH 之间的汇率。

综上所述，第一个为交易合约提供流动性的充值操作，并不取决于交易汇率。而是反过来，后面的交易汇率，将取决于第一次为交易合约提供流动性的这个充值操作充值



了多少 ETH 和 ERC20 代币，用第一个流动性提供者认为的等值，来反映 ERC20/ETH 的兑换汇率。如果这个汇率和市场对比过高或者过低，套利交易者都会很快把差距抹平，直到市场恢复正常水平。

这里还有一个概念需要清楚，就是每次兑换之后，会产生新的流动池，同时也会产生新的常数。原因是每次交易后产生的手续费会重新回到流动性资金池中，这样手续费会在完成代币价格兑换计算后重新添加到资金池，这样常数在每次交易后稍为变大一些，可以为流动性提供者提供系统性的盈利。

在 **RevelationSwap** 里，除了 ETH 和 ERC20 代币可以进行兑换之外，ERC20 代币之间也可以实现兑换，且不必存在单独的资金池。其兑换的方法是通过 ETH 完成兑换，因为 ETH 是所有 ERC20 代币的通用交易对，它可以成为不同 ERC20 代币之间进行交易的媒介。

从数学模型的角度，**RevelationSwap** 可以看做对以往的算法做了一次线性变化，把原曲线投影至一个新的坐标系中，进而可以实现超低滑点、超高流动性以及闪兑等功能和优势。正因为有了上面这种独特的设计规则和算法，使得 **RevelationSwap** 与其它 AMM 机制的去中心化交易所相比，拥有超低的滑点，可提供近乎无限的流动性，并极化资金利率。

#### 4.4.2. **RevelationSwap** 的流动性激励

「流动性提供者」是一个金融术语，指的是帮助一个金融市场提高流动性的个体。

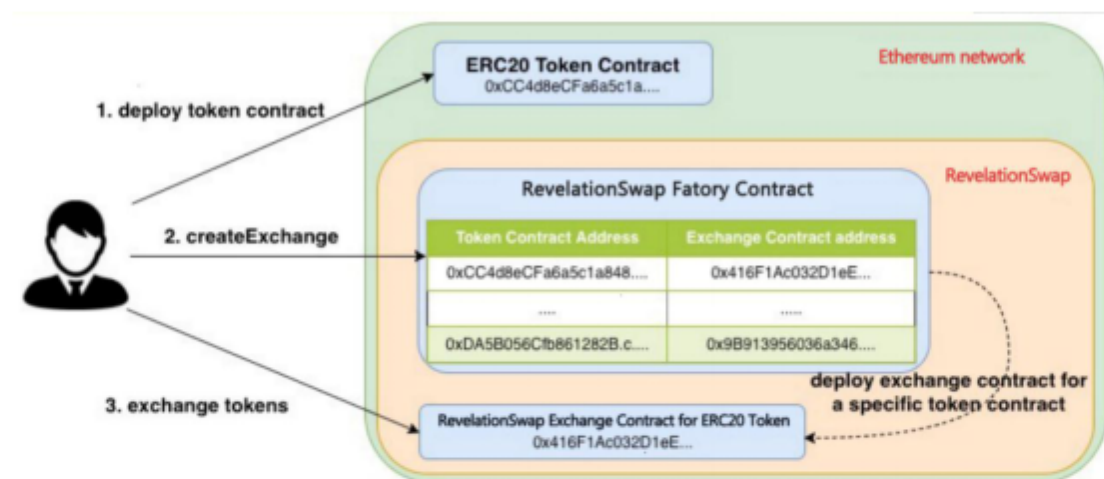
一个拥有越高流动性（市场深度越大）的交易所，其使用者就越能在短时间内以稳定的价格完成大额资产的交换，使用者的交易体验当然就越好。反之，在一个流动性不足的交易所，则很有可能因为一笔大额的交易便会导致币价的剧烈波动。在大部分的交易所中都有流动性提供者或做市商（**market maker**）这样的角色存在，做市商会在买、卖两个方向上挂单，让想要交易的使用者只需要跟做市商的订单搓合就能完成交易，而不需要等待拥有相反需求的交易对手出现，市场流动性就能提高。

在 **RevelationSwap**，流动性提供者要做的事情是：替一个 ETH - Token 交易对增加 ETH 与 Token 的储备资金，准备金越多，ETH  $\rightleftharpoons$  Token 的交易价格就越稳定，该 Token 的流动性就越高。

但如果“替一个交易对增加流动性”这件事不能带来利益，应该很少人会自愿这么做，所以 **RevelationSwap** 的做法是采取一定的激励措施：一旦用户在 **RevelationSwap** 里成为了流动性提供商，就可以获得收益。收益是通过流动性池的代币来捕获。**RevelationSwap** 从每一笔 ETH  $\rightleftharpoons$  Token 交易中抽取「流动性提供者费用」0.3 % 分给流动性提供者。用户提供了流动性，就可以获得该流动性池的代币，根据代币流动性池的规模大小，用户获得相应份额的流动性池代币。

这样一来逐利的人们就会自愿为 **RevelationSwap** 增加流动性以赚取被动收入，交易者也能享受到更好的交易体验，达成双赢。

### 4.4.3. RevelationSwap 的架构



RevelationSwap 依赖于 3 个合约：ERC20 合约，Factory 合约以及 Exchange 合约。其中：

ERC20 合约：ERC20 币对应的合约，符合以太坊 ERC20 协议

Factory 合约：使用该合约创建并部署 ERC20 币的 Exchange 合约

Exchange 合约：用户兑换币使用的合约

通过这个架构，Revelation 可以有效而快速的支持 ETH（以太币）与 Token 之间、Token 与 Token 之间的快速兑换。

### 4.4.4. RevelationSwap 有着其他交易所无法比拟的优势

交易所的核心环节是充值、下单、订单撮合、资金结算、提现等等，传统的中心化交易所（CEX）中，上述所有的环节均由交易平台本身撮合完成。CEX 的交易流程类似银行，用户把自己的虚拟货币资产转入到交易所，在交易所的背书下完成币币交易，最后再把资产提取到自己的钱包。在交易所开户需要通过 KYC 认证，即上传自己的 ID 等个人资料。

而 RevelationSwap 的交易流程会简化很多，省去了 KYC 和“转入”、“提币”的步骤，用户使用自己的地址（在 RevelationSwap 上申请，或者导入自己的钱包，但用户都掌



握私钥)与 Revelation 的智能合约地址交易。用户自始至终都握有地址和密钥,资产完全掌握在自己手中,上述所有环节都置于链上,由智能合约执行全部操作,这样用户的交易过程就无需任何可信任的第三方做担保。

RevelationSwap 在以下方面有着良好的设计:

### (1) 易用性 (ease-of-use), 支持闪兑

在 RevelationSwap 中,使用最多的功能应该是代币之间的币币兑换交易了,Revelation 的特色之一正是可以提供支持的币种间实现两两闪兑交易。

RevelationSwap 闪兑是去中心化代币兑换协议与自动做市协议 (AMM),协议通过恒定乘积算法实时提供兑换价格,用户可以实时完成代币兑换。

在中心化交易所里无法直接交易的交易对,用户最少需要两次交易,例如用户想用 TokenA 兑换 TokenC,但是 TokenA 和 TokenC 之间没有直接的交易所,这个时候,用户就需要先把 TokenA 兑换成 TokenB,再用兑换所得的 TokenB 来完成和 TokenC 的兑换,这样的两步操作在 RevelationSwap 却是可以一步完成交易 (虽然系统可能需要转换,但在用户看来就是一步交易) 的。

使用 RevelationSwap 这种交易形式,会比订单撮合模式速度更快,因为它是基于兑换池的人机交易,节省了撮合时间。很显然,对于用户来说,RevelationSwap 会更加便捷。而且 RevelationSwap 支持的币种间可以实现两两闪兑交易,交易对明显比中心化交易所更丰富。

由于 RevelationSwap 是基于以太坊的,所以在 RevelationSwap 中只能交易以太坊上的加密货币资产。目前 RevelationSwap 支持的币种大概在 150 种左右,以太坊上的主流资产基本都可以在上面进行交易。

除了代币兑换,用户还可以自由创建兑换市场,也可以选择加入已创建的市场成为做市商,为市场提供流动性 (按比例存入两种代币),做市商根据流动性占比,自动赚取交易用户所支付的手续费。在 RevelationSwap 交易所上买卖币时,你只要决定好卖出的币种、买入什么币、买或卖的数量是多少,送出交易后,在交易上链后就能立即取得你应得的币。

### (2) gas 使用效率 (gas efficiency)

RevelationSwap 交易消耗的 gas 量将会是以太坊上的几家主流交易所之中最低的,也就代表在 RevelationSwap 交易要付的矿工费最少。这主要得益于它相对简单的做市机制:它不是采用挂单撮合机制来完成交易,而是根据合约中储备的资金量算出当下的交易价格,并立刻从资金池中取出对应的金额传给使用者,整体的运算量相对较少。

### (3) 抗审查性 (censorship resistance)

抗审查性体现在 RevelationSwap 上架新币的门槛:

在 RevelationSwap 上架新币没有门槛，任何使用者都能在 RevelationSwap 上架任何 Token。这点即使在众多去中心化交易所之中也是少见的，大多数的去中心化交易所虽然不会像中心化交易所那样向你收取上市费，但还是要申请上市、通过审查后，运营团队才会让您的 Token 可以在他们的交易所上交易。

但在 RevelationSwap，任何使用者只要发起一个 createExchange 的交易，就能让一个 Token 上架到 RevelationSwap 的交易对中，上架后也没有人能迫使它下架。

#### （4）零抽租（zero rent extraction）

在 RevelationSwap 的合约设计中，没有人有任何特权，即使是开发团队也不会从交易中抽取费用。

由智能合约驱动的去中心化交易所是交易者们最后的隐私保留地，RevelationSwap 以去中心化版本运作，具有无价的金融合约，没有中心运营者，通过链上价格流来确保偿付能力。不仅可以为用户省去以往中心化平台上必须经历的繁琐操作，还可以帮助用户消除中心化交易所“拔网线”、暗中操纵价格、交易量造假和跑路带来的风险，且所有的交易记录都在链上可查。

随着 DeFi 模式的盛行，去中心化交易所已经初步显示出了时代发展趋势的必然性，在不远的将来，极可能有数百亿甚至上千亿美元的传统资产将转换为数字资产，交易平台的交易产品和交易方式将变得更加多样化，交易平台市场总体交易规模也将有可能达到今天的数百倍，甚至数千倍。而 RevelationSwap 无疑是这个行业内的佼佼者，由于 Revelation 协议自身的优势，保守估计，RevelationSwap 在不远的未来，至少能够占据整个市场五分之一的份额。

### 4.5.去中心化金融衍生品 Rebirth

用户可以基于 Revelation 协议发行合成资产 rTokens，rTokens 由 Revelation 网络通证 RDAO 担保，只要将 RDAO 在智能合约中锁定，即可发行合成资产 rTokens。抵押池模型使用户可以直接使用智能合约在 rToken 之间执行转换而无需交易对手。这种机制也可以帮助解决去中心化交易所遇到的流动性和滑点问题。

Revelation 当前支持合成法定货币，加密货币（多头和空头）和大宗商品。

当前有四类 rTokens 可用：法定货币，大宗商品，加密货币和反向加密货币。我们的法定货币 rTokens 包括 UNC 等。大宗商品 rTokens 包括合成金和合成银，均以盎司为单位。我们的加密货币 rTokens 包括 rBTC，rETH 等，未来将加入更多种类。而 Inverse rTokens 则反向跟踪加密货币的价格，这意味着当 BTC 的价格下降时，rBTC 的价格就会上升。

系统会根据用户的贡献，将产生于 RevelationSwap 交易所中的交易费用按比例付给 RDAO 持币者，从而鼓励用户持有 RDAO。在这里，RDAO 的价值来源于使用网络的权利，和收取因 rToken 交易而产生的费用。

### 4.5.1. RDAO 抵押

当 RDAO 持有者使用其 RDAO 作为抵押品进行抵押时，便会生成 rTokens。rTokens 目前有 750% 的抵押率支持，但是将来可以通过 RevelationDAO 社区治理机制提高或降低其抵押率。RDAO 抵押人在创建 rTokens 时会产生债务，要退出系统（即解锁其 RDAO），必须通过销毁 rTokens 来偿还该债务。

### 4.5.2. RDAO 持有和交易的激励措施

RDAO 持有人被鼓励以多种方式持有 RDAO 和铸造 rTokens。

#### （1）交易奖励。

每当有人将一种 rToken 交换为另一种 rToken 时（即在 RevelationSwap 上交易），会生成交易奖励。每笔交易产生 0.3% 的交易费，会被存到费用池中。RDAO 抵押人每周可以按比例申领费用池中的 RDAO 作为交易奖励。

#### （2）持有奖励。

协议的通胀政策产生 RDAO 持有奖励。RDAO 的总供应量将会逐年上升，通胀率将逐年降低。如果这些 RDAO 的抵押率不低于目标阈值，则会按比例分配给 RDAO 抵押人。

### 4.5.3. 铸造，销毁和抵押率

以上机制可以激励 RDAO 抵押人将其抵押率（Collateralisation Ratio）保持在最佳水平（目前为 750%）。这样可以确保 rTokens 有足够的抵押来支撑大幅价格冲击。如果 RDAO 或 rTokens 的价格波动，则每个抵押人的抵押率也会波动。如果降至 750% 以下，他们将无法申领交易奖励，直到他们恢复抵押率为止。他们可以通过铸造 rToken（如果它们的比率高于 750%）或销毁 rToken（如果它们的比率低于 750%）来调整其比率。

### 4.5.4. 抵押人，债务人和交易对手

RDAO 抵押人创建 rTokens 时会产生“债务”。根据网络中 rTokens 的汇率和供应，该债务可以独立于其原始铸造价值而增加或减少。假设系统中的 rTokens 全都是合成比特币（rBTC），那么当 rBTC 价格减半时，系统中的债务也将减半，这时每个抵押人的债务也将减半。再假如系统中 50% 的 rTokens 是 rBTC，而 BTC 的价格翻了一番的话，系统的总债务以及每个风险承担者的债务都将增加四分之一。

这样一来，所有 RDAO 抵押人就成为了所有 rToken 交易所的交易对手；抵押人承担系统中全部债务的风险，当然，他们也可以选择在该系统外部进行对冲，以规避这种风险。所有抵押人通过承担此风险，使得 Revelation 上能够产生交易，从而获得系统产生的交易奖励分成。

#### 4.5.5. UNC 挂钩

UNC 挂钩对一个功能良好的系统至关重要，因为交易者需要 UNC 与其他加密资产之间的流动性和稳定性，才能从交易中获利。UNC 在公开市场上交易，因此有可能跌破与美元同等的水平。这个时候就需要采取激励措施，以确保挂钩的价格偏差最小，同时使 RDAO 持有者有动力去通过套利纠正价格偏差。

保持 UNC 挂钩的主要机制是，RDAO 抵押人创造了债务，并出售了他们铸造的 rTokens 后，通过将 UNC 以低于其面值的价格回购并销毁以减少债务，达到套利的目的。还有其他保持此挂钩的方法，包括提高抵押率，从而减少 rTokens 的供应以适应需求。对于未能保持 UNC 挂钩的情况，引入清算是另一种选择。这些方案都需要 RevelationDAO 投票通过之后才能实施。

#### 4.5.6. rTokens 对 RevelationSwap 交易所的有力支持

合成资产可以在无需持有某种实际资产的情况下，提供对这种资产的交易。合成资产有一系列优势，包括减少在不同资产之间切换时的摩擦（例如，从股票到合成黄金），扩大某些资产的可触及性，以及抗审查。

rTokens 是跟踪实际资产价格的合成资产。它们使持有者无需自己持有实际资产或委托任何托管人，就可以在以太坊上交易各种资产类别。

rTokens 的这些优异特性，对于 RevelationSwap 无疑是最有利的助益，它使得 RevelationSwap 比中心化交易所和基于交易簿（order book）的去中心化交易所更加具备优势。没有交易簿意味着所有交易都是根据智能合约执行的，称为 P2C（点对智能合约）交易。RevelationSwap 交易所的 dApp 将通过预言机（Oracle）提供的价格信息为资产分配汇率，从而运行资产转换。这提供了相当于系统抵押品总量的无限流动性，零滑点和无审查的上链交易。

#### 4.5.7. 铸造 rTokens

RDAO 持有者可以通过 Revelation 智能合约锁定其 RDAO 作为抵押品来铸造 rToken。RDAO 持有者铸造 rTokens 的步骤是：

（1）Revelation 智能合约检查 RDAO 抵押人是否可以用这些 RDAO 来铸造 rTokens，要求其抵押率低于 750%。

(2) 他们的债务被添加到债务登记簿中。债务是新铸造的 **rToken** 金额，并存储在 **XDR** 的 (**Revelation Drawing Rights** 提款权) 中。**XDR** 使用一篮子货币来稳定债务的价值。这些货币价格通过价格预言机在推送上链。

(3) 将债务分配给抵押人后，**Revelation** 智能合约将指示目标 **rToken** 智能合约发行新的金额，将其添加到总目标 **rToken** 的供应量中，然后将新铸造的 **rTokens** 分配到用户的钱包。

(4) 如果 **RDAB** 的价格上涨，则抵押人一部分相应的 **RDAB** 将自动解除锁定。例如，如果一个用户锁定了 100 美元的 **RDAB** 作为抵押品，并且 **RDAB** 的价值翻了一番，那么他的 **RDAB** 总数 (总价值: 200 美元) 中的一半将被锁定，另一半则被解锁。当然，如果他愿意，还可以将多余的未锁定 **RDAB** 抵押以创建更多 **rTokens**。

#### 4.5.8. 智能合约处理 **rTokens** 交易时的步骤

智能合约处理 **rToken** 交易时涉及的步骤，以从 **UNC** 到 **rBTC** 为例：

(1) 销毁源 **rToken** (**UNC**)，包括减少该钱包地址的 **UNC** 余额并更新 **UNC** 的总供应量。

(2) 确定兑换金额 (即根据每种货币的价格计算的汇率)。

(3) 收取交易费用，目前是决定取交易金额的 0.3%，并将费用发送到费用池，用于所有 **RDAB** 抵押人申领。

(4) 剩余的 99.7% 由目标 **rToken** (**rBTC**) 的智能合约发行，并且更新钱包余额。

(5) 更新 **rBTC** 总供应量。

由于系统将债务从一种 **rToken** 转换为另一种 **rToken**，因此不需要交易对手进行交易。另外，由于不需要交易簿或撮合交易，**rToken** 之间的流动性是无限的。债务池中的债务变化也不需要记录，因为源 **rToken** 销毁的价值已经在目标 **rToken** 中被铸造出来了。

#### 4.5.9. 申领费用

通过 **Revelation** 智能合约交换 **rToken** 时，将收取 0.3% 的费用并将其作为 **XDR** 发送到费用池中，以供 **RDAB** 抵押人申领。申领费用 (也称为 **rToken** 交易奖励) 时，抵押人也可以申领他们的 **RDAB** 持有奖励，即持有 **RDAB** 可以获得额外的 **RDAB** 奖励。抵押人申领费用时，智能合约的流程如下：

(1) 费用池检查当前是否有可用费用，以及抵押人是否有资格申领费用。

(2) 发行对应的 UNC，并销毁费用池中等价 XDR。更新抵押人钱包地址的余额和费用池的余额。

(3) 此外，从 RDAO 持有奖励智能合约中，按比例分配托管的 RDAO 到抵押人钱包地址。

申领能够得到的费用是根据每个抵押人已发行债务的比例分配的。例如，如果一个抵押人发行了 1,000 UNC 的债务，债务池为 10,000 UNC，并且在收费期内产生了 100 笔费用，那么该抵押人有权获得 10 UNC，因为他们的债务占债务池的 10%。相同的比例分配机制也用于 RDAO 持有奖励。

#### 4.5.10. 销毁债务

当 RDAO 抵押人想要退出系统或减少债务并解锁抵押的 RDAO 时，必须先偿还债务。最简单的例子是：如果抵押人通过将 RDAO 锁定为抵押品来铸造 10 UNC，那么就必须销毁 10 UNC 才能解锁那些 RDAO。但是，如果在抵押期间债务池发生波动（其个人债务也会随着发生波动），则他们可能需要销毁比铸造时更多或更少的债务。将债务减为零的过程如下：

(1) Revelation 智能合约确定其债务余额并将其从“债务登记簿”中删除。

(2) 销毁所需的 UNC 金额，并且更新 UNC 的总供给以及用户钱包中的 UNC 余额。

(3) 这些 RDAO 余额被设置为可转让。

#### 4.5.11. 债务池

当 RDAO 持有者铸造或销毁 rTokens 时，系统会通过更新“累积债务增量比率”，来跟踪债务池（以及每个抵押人的债务）。这可以衡量 RDAO 抵押人上次铸造或销毁时，其债务在债务池中所占的比例，以及由其他抵押人进入或离开系统而引起的债务变化。系统使用这些信息来确定每个抵押人在任何未来时间点的债务，而不必实际记录每个抵押人的债务变化。

通过更新“债务登记簿”上的“累积债务增量比率”，系统可以跟踪每个用户的债务百分比。系统使用如下公式计算新债务对债务池的引入变化的百分比，并将其添加到债务登记簿中：

新铸造的债务（现有总债务 + 新债务）

然后，抵押人的铸造/销毁操作，包括其债务发行数据和编号，将被记录到债务登记簿中。由以下公式计算得出在债务池中的占比，将被记录下来：



抵押人债务占比 = (新债务 + 现有债务) / (之前债务池总量 + 新债务)

上述计算得出的，保存在债务登记簿中的累积债务增量比率，加上债务的相对时间（编号），就可根据任何用户上次铸造/销毁时引起的债务池占比变化，来计算此用户在任何未来时间点的债务池占比。

每次产生或销毁债务时，我们通过相加每个 **rToken** 智能合约中代币的数量乘以当前汇率，来重新计算债务池：

总发行债务 = 总铸造 **rTokens** ("XDR")

这样就可以计算当前债务池，并包含在更新后的“累积债务增量比率”中，以便我们知道每笔“债务登记簿”条目中债务的大小（以 **rTokens** 为单位）。

当抵押人偿还债务（即通过销毁他们铸造的 **rTokens**）以解锁其 **REV** 抵押时，系统将基于销毁的债务金额相对于债务减少后的系统债务总值的百分比变化来更新累积债务增量。

这是用户铸造新债务的逆运算：

抵押人新的债务比 = (现有债务 - 将销毁的债务) / (债务池 - 将销毁的债务)

这是用于计算更新的累积债务增量的公式：

增量 = 将销毁的债务 / (债务池 - 将销毁的债务)

如果抵押人将所有债务销毁，则其在债务登记簿中的债务发行数据将被设置为 0，且其不再属于债务池。

目前，**Revelation** 系统中所有合成资产的价值均由一个自动将资产价格推送上链的预言机确定。它使用具有多种来源的算法来为每种资产形成合计价值。它目前由 **RevelationDAO** 团队运行，但计划在未来将其去中心化。

未来多种 **rTokens** 将被添加到系统中，以为 **RevelationSwap** 会提供更多的实用性。而且 **Revelation** 完全支持，并开始成为以太坊上越来越多的 **DeFi**（去中心化金融）运动的一部分。其中非托管贷款是该生态系统的重要组成部分。因此，**Revelation** 计划集成开源贷款协议以提供 **UNC** 贷款，从而允许用户借贷 **rTokens** 并在 **RevelationSwap** 上进行交易。这将是一种吸引用户使用平台的令人兴奋的新方法。

**Revelation** 计划在将来能够使用户在 **RevelationSwap** 上建立合成资产头寸。该功能的许多方面尚未最终确定，但预计它将使用与 **RevelationSwap** 自动做市商算法类似的自平衡机制，该算法将限制每个头寸的总未平仓权益，因此可以限制 **RDAO** 抵押人的风险和未平仓合约总额，并且借入利率会根据当前未平仓合约进行调整。该系统还将鼓励交易者通过向重新平衡头寸的交易者支付一定比例的费用来平衡系统中的风险。目前

已经有许多加密资产的衍生品交易平台受到交易对手流动性的限制，**Revelation** 系统的独特设计意味着它可以在该领域抢夺并占据较大的市场份额。

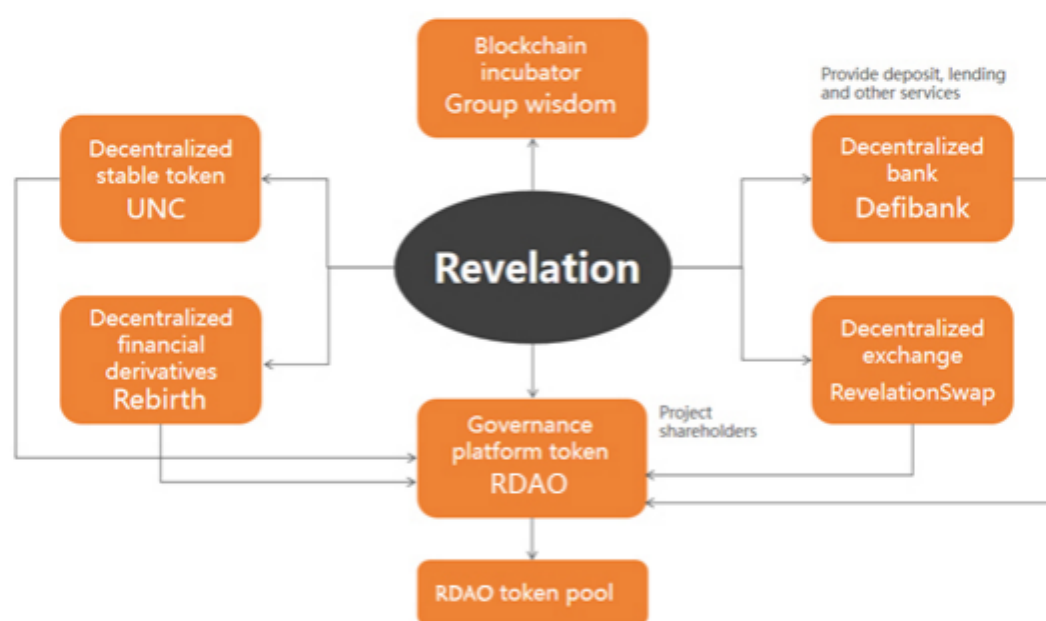
随着 **Revelation** 机制的进一步改进、新功能的升级，以及新的 **rTokens** 交易对的加入将大大增加该平台的实用性。同时，进化到去中心化的治理流程还将减少系统风险，并提高项目的长期可行性。

## 4.6. 孵化器（Group wisdom）

金融启示录下设隶属的（**Group wisdom**），是一个致力于从空间建设、投融资服务、专业技术平台、内部管理等各方面进行创新突破的孵化器平台，它被用以专门发掘和培植富有市场潜力的 **RevelationDAO** 生态项目，可以有效地帮助其降低风险和成本，提高成功率，促进成果转化。从而，随着这些小微却极具市场潜力的创新成果不断被转化，**Revelation** 生态得以不断完善，并被确保向着健康稳定的方向发展，时刻保有竞争力以及在整个同类市场上的超前性。

**Group wisdom** 是金融启示录的重要组成部分。

## 4.7. 金融启示录的整体架构



图：Revelation 模块化设计

Revelation 协议的各个模块之间的关系如图：

**Revelation** 协议是由去中心化组织 **RevelationDAO** 发起和创建的，通过 **Revelation** 治理来进行链上的去中心化的投票治理的一站式 **DeFi** 应用平台，**Revelation** 协议由世界各地的治理型令牌 **RDAO** 持有者管理。**Revelation** 治理通过由提议投票（**Proposal**



Voting) 和执行投票 (Executive Voting) 组成的科学型治理系统, 可以让用户使用经过 “Revelation 治理 (Revelation Governance)” 批准的资产作为担保物来生成 UNC, UNC 是以太坊上的去中心化抵押型稳定币。通过抵押以太坊发行稳定币 UNC (1:1 锚定美元) 可满足杠杆交易、获取流动资金等多种需求。

RDAO 持有者相当于 Revelation 项目的投资人, 可以管理 Revelation 协议及 UNC 的金融风险, 从而确保该协议的稳定性、透明性和高效性。在通过 Revelation 治理及 R 对市场的调控平衡作用下, Revelation 协议逐渐演变和进化, 进而形成了金融启示录下的六大模块: 治理令牌 RDAO、去中心化稳定币 UNC、去中心化银行 Defibank、去中心化交易所 RevelationSwap、去中心化金融衍生品、孵化器 Group wisdom。

这六大模块之间是相互促进, 互为助益的, 它们共同构成了金融启示录的健康闭环生态, 使得建立在以太坊上的 Revelation 协议, 在自由金融属性赋予它蓬勃生命力的情况下, 能够向着健康有序的方向稳步的进化和发展, 为投资者提供安全的、去中心化的抵押、存款、借贷等服务以及其他一些新鲜的有特色的划时代的尝试。

金融启示录有望改善不透明的金融环境、应对经济危机, 构建透明化的金融系统, 向所有人开放, 且无须许可, 不用依赖于第三方机构, 通过其上提供的丰富有趣的规则, 通过各种不同的资产、合约以及协议, 可以组装出新的项目, 给用户源源不断地提供新的产品和服务。并且由于孵化器 Group wisdom 的存在, 在 Revelation 的成功和发展的过程中, 能够不断孕育出极具市场竞争力的新模块、新模式, 令 Revelation 生态可以不断的在发展中获得进化, 在进化中趋于完美, 从而为用户提供更加丰富多彩、与时俱进甚至是超前于时代的实用性功能和解决方案。

## 5. 风险及免责声明

### 5.1. 技术风险

与执行团队非常重视资金安全, 智能合约已经通过安全公司的多重审计, 但是仍然不能保证合约是 100% 安全的, 未来可能出现无法预知的突发事件: 比如 DeFi 协议安全漏洞、黑客攻击等, 一旦出现此类突发事件, RevelationDAO 将紧急关停 DeFi 协议, 避免或减少损失。我们将保持审慎原则, 未来将推出 Bug 赏金计划, 尽量消除可能存在的安全漏洞和潜在风险。

### 5.2. 政策风险

未来不排除可能因为政策原因停止运营, 因此 RevelationDAO 计划最终目标是实现社区完全自治。

### 5.3.免责声明

本白皮书只用于传达信息，并不构成投资金融启示录项目的相关意见。

本白皮书不构成也不理解为提供任何买卖行为，也不是任何形式上的合约或承诺。一旦参与项目即表示了解并接受该项目风险，并愿意为此承担一切相应后果，明确表示不承担任何参与 **Revelation** 项目所造成的直接或间接的损失。

除本白皮书所明确载明之外，维优运营团队和基金会不对 **Revelation** 作任何保证（尤其是对其适销性和特定的功能）。

任何人参与 **Revelation** 的行为均基于自身对 **Revelation** 的知识和本白皮书信息的理解。所有参与者将在 **Revelation** 项目启动之后按现状接受 **Revelation**，无论其技术规格、参数、性能或功能，维优运营团队和 **Revelation** 基金会在此明确不予承认和拒绝承担下述责任：

（1）任何人在参与 **Revelation** 项目时不能违反任何国家的反洗钱、反恐怖主义融资或其他监管法律；

（2）任何人在参与 **Revelation** 项目时违反本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法付款或无法提取，责任由本人承担；

（3）**Revelation** 的开发失败或被放弃，以及因此导致的无法交付 **Revelation**；

（4）任何人在参与 **Revelation** 项目时发生投机行为；

（5）任何人与第三方平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；

（6）**Revelation** 被任何政府、准政府机构、主管当局或公共机构归类到禁止、监管或法限制范畴；

（7）**Revelation** 的第三方平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作等不当行为、失误、疏忽、破产、清算、解散或歇业；

（8）本白皮书披露的任何风险因素，以及与该风险因素导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响；

（9）任何国家限制或禁止参加此类项目的投资人。

## 6. 项目总结

**Revelation** 作为以太坊上专业的一站式 **DeFi** 应用平台，以提高全球价值流通效率为使命，利用去中心化的力量，将充分发挥 **DeFi** 更加透明、更加公平、更加便捷的特点，为用户提供安全专业、方便易用的 **DeFi** 协议，为去中心化金融发展贡献力量。

我们有办法使加入 **RevelationDAO** 的各个成员形成紧密的联系，以形成更为庞大更为系统的治理结构，最终目的是实现近乎完美的去中心化自治体系：其中有生态、有分型结构、有逻辑、有去中心的链上配合与分工、治理.....如果用形象化的语言来进行描述的话，这个系统结构就象是自然界的超级生物体系，您可以将整个 **Revelation** 想象成一个巨大的蜂箱，那么每个成员就象是其中的蜜蜂，他们在已经制定好的规则下，只需按照既有体系进行运作，只需要做好自己对应的任务和角色，如此之后，最终展现出来的会是令人叹为观止的杰作。

当下，我们周围的加密网络正在与日俱增，且发展的速度一日千里，它是一种超国家规约，可以突破国界的限制，在全球范围内影响和规范人类活动，它可以提供一个互通的、共享的国际基础，允许世界各地的人不用聚集在一起，也可以完成互动共同做出决定，他们甚至可以在链上去中心化的完成共享企业，共享资源等传统模式下无法轻易实现的便利，进而可以实现去中心化治理，去中心化收益，最终实现这项工作的真正关键部分。

在不久的将来，会有越来越多的人加入到这个行列中来，**RevelationDAO** 的最终目标是实现完全的去中心化，由全人类的共识决定 **RevelationDAO** 是什么样子，这是一件伟大而神圣的事业，最终会实现颠覆性的金融革命，为每一个参与者的金融平等与财富自由做出努力，进而最终创造出理想的金融世界。