DeGate 白皮书 1.0

1. 概述

DeGate 是真正由 DAO（Decentralized Autonomous Organization，去中心自治组织）拥有和控制的、基于以太坊 Rollup 二层网络的去中心化交易协议，由社区共建、共治、共有。DeGate 以“公平启动”的方式诞生，没有人获得免费的 DG 代币。DeGate 的功能模块包含自动化做市商交易、订单簿交易、杠杆现货交易、跨层桥接、法币兑换通道、初始代币分发平台。DeGate 协议的治理由双层 DAO 机制组成：Home DAO 和 Council DAO，其中 Home DAO 是 DeGate 协议的直接拥有者和控制者，并获得协议产生的收入；Council DAO 受 Home DAO 委托，负责日常运行的决策和执行。

2. 背景

截止 2021 年 2 月 16 日，Uniswap 累计交易量达到 1000 亿美元。根据 Coingecko 的数据，2021 年 2 月 16 日 Uniswap 的 24 小时成交量为 11.5 亿美元，在全球所有交易所中排名第四。这样的成绩足以验证 Uniswap 的“产品市场契合度”，它的成功也开启了去中心化交易所（Decentralized Exchange，以下简称 DEX）的繁荣时代。在 Uniswap 的带动下，自动化做市商（Automated Market Maker，以下简称 AMM）模式已经成为以太坊一层（Layer 1，以下简称 L1）上的主流交易模式。

难以想象，Uniswap 的上述成绩是在以太坊 L1 上极其拥堵的基础设施条件下完成的。随着基于以太坊 Rollup 二层技术（Rollup 技术的综述参考："An Incomplete Guide to Rollups"）的逐步成熟，以太坊有望在 2021 年获得至少两个数量级的吞吐量提升，这样的基础设施巨变极大可能将重构原有生态，并孕育新机会。DeGate 正是在这样的背景下诞生。

3. DeGate 的功能

DeGate 是一个综合性的去中心交易协议，其目标是建设成为以太坊上现货流动性最好的 DEX。DeGate 将会部署至以太坊上最大的 Rollup L2 网络，并致力于成为 L2 网络的交易枢纽。目前重点考察的 L2 网络为：Optimism、 Arbitrum 和 zkSync，但并不排除其他。

3.1 DeGate DEX

DEX 是 DeGate 协议的核心，其他功能则强力支持 DEX。DEX 分为 3 个子模块：**AMM 模块、订单簿模块、杠杆交易模块。**

3.1.1 DeGate AMM 模块

AMM 模块将采用目前最广泛应用的恒定乘积算法（x*y=k），并通过虚拟额度（更多信息请参见 此文）的方式来抵御交易抢跑。AMM 中的各项参数均由 Council DAO 来确定，包括但不限于交易费率、虚拟额度值、Home DAO 提成比例、流动性挖矿相关参数等，其中，交易费率预计将显著低于目前 L1 上的 AMM。

AMM 资金池不设 Admin Key，即任何人无法以任何形式挪用用户的做市资金。由于 DeGate 协议的去中心化特性，任何人均可利用 DeGate AMM 交互界面的开源代码，自行部署交互界面后接入 DeGate AMM 协议。

3.1.2 DeGate 订单簿模块

DeGate 订单簿交易模块将采用链下挂单、链上撮合的模式，以消除“订单上链”带来的交易效率的损失和订单上链所需的费用。虽然订单在完成撮合之前并未上链，但是由于附带了用户的数字签名，其他人并无法篡改订单的内容，因此该模式在大大提升交易效率的同时，又保留了“无需信任”的特性。

订单簿交易的资金不设 Admin Key，即任何人无法以任何形式挪用用户的挂单资金。由于 DeGate 协议的去中心化特性，任何人均可利用 DeGate 订单簿模块的交互界面的开源代码和订单传导节点（Relayer）的开源代码，自行部署交互界面和订单传导节点后接入 DeGate 订单簿协议。

3.1.3 DeGate 杠杆交易模块

杠杆交易一直都是加密资产交易领域的核心需求之一，DeGate 杠杆交易模块将使用户能够以去中心化的、且用户体验优良的方式满足这一需求。在杠杆交易的过程中，用户将不会感受到“借贷”这个动作单独存在，而是在用户交易的过程自动完成。例如，用户将价值 100 美元的代币 A 加杠杆后兑换成 150 美元的代币 B，用户的杠杆账户中将呈现：（1）价值 150 美元的代币 B 的资产，（2）价值 –50 美元的代币 A 的负债。这些资产和负债实际上都保存于外接的去中心化借贷协议中，同时，DeGate 中的交易界面将告知用户强

制平仓的清算价格等信息。

DeGate 杠杆交易模块本身针对用户的交易资金不设 Admin Key，即在 DeGate 协议内任何人无法以任何形式挪用用户的挂单资金和待交易资金；DeGate 杠杆交易模块计划对接外部的去中心化借贷协议，因为用户杠杆交易后的资产实际上保存于外部的借贷协议中，所以资产的处置权在于外部去中心化借贷协议的智能合约代码，Council DAO 将仔细审查对接的去中心化借贷协议，包括该借贷协议中是否存在针对资金安全的 Admin Key，以及审查 Admin Key 的潜在风险如何被处置。对接外部去中心化借贷协议属于重大决策，最终的选择将由 Home DAO 通过 DG 代币投票决定。

由于 DeGate 协议的去中心化特性，任何人均可利用 DeGate 杠杆交易模块的交互界面的开源代码，自行部署交互界面后接入 DeGate 杠杆交易协议。

3.2 DeGate Bridge

DeGate Bridge 是通过交易市场的方式实现的跨层资产转移的快速通道，首期将实现 L1 与 L2 之间的快速兑换通道，之后视情形考虑开通不同 L2 之间的快速兑换通道。首期的 Bridge 将通过中心化托管资产的方式实现，被托管的资产的安全性由 Home DAO 自身持有的净资产作为担保；当以太坊上 L2 出现成熟的预言机服务后，DeGate Bridge 将转向以去中心化的方式实现资产的桥接。

下面将以中心化方式托管资产的 DeGate Bridge 和 Optimistic Rollup L2 为例，说明 L1–L2 Bridge 的工作原理。

DeGate Bridge 的工作原理与 Curve 协议的原理类似，都采用在价格 1：1 附近更加平缓的 AMM 曲线，只不过 Bridge 的 2 个资产池分布在 2 个不同的状态机中，即 L1 和 L2。对于 Optimistic Rollup，资产从 L1 转移到 L2 是实时完成的，而从 L2 转移到 L1 则有相当长的延时，预计延时 7 天。由于时间价值的折现，通常情况下同一资产在 L2 上的价格会略低于 L1。

举例，Alice 希望将 1 L1 ETH 转换成 L2 ETH，我们假设：

- 1 L2 ETH = 0.995 L1 ETH
- DeGate Bridge 费率 = Curve 费率 = 0.04%
- Gas 价格 = 100 Gwei

经由 Optimistic Rollup 原生通道：

- Alice 发送 1 L1 ETH
- Alice 为 L1 上的交易支付 ~45,000 gas
- 交易被处理后，Alice 立即收到 1 L2 ETH
- 最终，Alice 支付了 1.0045 L1 ETH，获得 1 L2 ETH
- L2ETH / L1ETH = 1 / 1.0045 = 0.9955

经由 DeGate Bridge 通道：
- Alice 发送 1 L1 ETH
- Alice 为 L1 上的交易支付 21,000 gas
- 约 5 分钟后，Alice 从 DeGate 收到 1 / 0.995 * (1 – 0.04%) 数量的 L2 ETH
- 同时，DeGate 向 Alice 收取这笔 L2 交易的费用： x gas — 非常低，可忽略不计
- 最终，Alice 支付了 1.0021 L1 ETH，获得 1.0046 L2 ETH
- L2ETH / L1ETH = 1.0046 / 1.0021 = 1.0025

在这个示例中，Alice 节省了 ~0.7% 的资金，代价是额外等待 5 分钟，以及信任 DeGate Bridge 的托管式运营（今后将转为去中心化）。

下面我们反转方向，让 Bob 转换 1 L2 ETH 成为 L1 ETH：

经由 Optimistic Rollup 原生通道：
- Bob 发送 1 L2 ETH
- Bob 在 L2 上支付的 gas 费用很低，可忽略不计
- 7 天后，Bob 在 L1 上领取 1 L1 ETH，并为此支付 ~61,000 gas
- 最终，Bob 支付了 1 L2 ETH，获得 0.9939 L1 ETH

经由 DeGate Bridge 通道：
- Bob 发送 1 L2 ETH
- Bob 在 L2 上支付的 gas 费用很低，可忽略不计
- 约 5 分钟后，Bob 从 DeGate 收到 0.995 / 1 * (1 – 0.04%) 数量的 L1 ETH
- 同时，DeGate 向 Bob 收取这笔 L1 交易的费用： 21,000 gas
- 最终，Bob 支付了 1 L2 ETH，获得 0.9925 L1 ETH

在这个示例中，Bob 支付 ~0.14% 的额外成本，将原本 7 天的等待期缩短到 5 分钟。过程中 Bob 同样需信任 DeGate Bridge 的托管式运营。

这里有必要说明，为什么 DeGate Bridge 不一开始就以去中心化的方式实现，让 L1 和 L2 上的资金池都由智能合约来托管呢？原因是非常技术性的：L1 和 L2 分别是独立的状态机，L1 的状态可以通过原生的通道立即传递给 L2，且 L2 可以完全信任该消息，因为 L2 本身的安全性都是依赖 L1 的；而反过来却不可以，也就是说，基于 Optimistic Rollup L2 的状态通过原生的通道传递给 L1 的时候，L1 不能立即信任该消息，而是要有一定的等待期，等待期是为给潜在发生的挑战留足时间，以此来制止和纠正 L2 上潜在的作弊。

由此得出结论：DeGate 的去中心化实现，依赖于从 L2 向 L1 上传递准实时消息的可靠成熟的预言机，当这样的预言机出现后，DeGate Bridge 将能够启动去中心化的升级，届时 DeGate Bridge 也将获得去中心化产品的特性：

（1）Bridge 资金池不设 Admin Key，即任何人无法以任何形式挪用用户的做市资金；

（2）任何人均可利用 DeGate Bridge 的交互界面的开源代码，自行部署交互界面后接入 DeGate Bridge 协议。

DeGate Bridge 作为 L1–L2 的快速通道，将为 DeGate DEX 业务提供有力支持。

3.3 DeGate Fiat

DeGate Fiat 是一个支持 L2 上的稳定币与法币之间兑换的平台，其用户体验与 DeFi 应用类似，以区块链地址的方式登录。

DeGate Fiat 将对接合规的“兑换机构”，兑换机构在其所在国家 / 地区持有合规的金融牌照。DeGate Fiat 作为纯信息服务商，不以任何形式持有用户和兑换机构在交易中的资金和资产。根据兑换机构所持的金融牌照的要求，用户将会需要提供真实的身份信息，某些时候还需要提供“资金来源”等符合反洗钱法律要求的信息。

DeGate Fiat 作为 L2 与法币之间的直接通道，将为 DeGate DEX 的业务提供有力支持。

3.4 DeGate Launch

DeGate Launch 是一个去中心化的首次代币发行平台，与中心化发行平台最大的区别在于：DeGate Launch 将只作为信息展示的工具来服务代币发行方和普通用户，这也意味着，将不会有中心化的运营者充当裁判员进行审批。有时候裁判员也会下场成为运动员，你懂的。

DeGate Launch 将保有 DeGate 系列去中心化协议的一贯特性：

（1）DeGate Launch 协议不设 Admin Key，即任何人无法以任何形式挪用用户的资金；

（2）任何人均可利用 DeGate Launch 的交互界面的开源代码，自行部署交互界面后接入 DeGate Launch 协议。

4. DG 代币

DG 是 DeGate 的原生代币，总量为 10 亿，100% 由 Home DAO 初始拥有。

19.8% 初始融资，Home DAO 以 99 万美元的价格出售给创始团队，该部分 DG 代币分 4 年线性解锁。未解锁部分的 DG 代币除无权自由转移外，享受完整的代币权益。初始融资后，创始团队成为与 DeGate 生态利益一致的实体。

44% 运营激励池，运营池的资金预计绝大部分将用于流动性挖矿，以此使 DeGate 获得市场竞争力。预计 4%（4000 万枚）DG 代币将用于向币乎和 MYKEY 的使用权代币 KEY 的持有者开放兑换，首期兑换 2%（2000 万枚）DG 代币，剩余 2%（2000 万枚）的兑换时间和方式由 Home DAO 决定，兑换所得的 KEY 由 Home DAO 拥有和处置。开放 DG 与 KEY 之间的兑换，是为了吸引币乎和 MYKEY 的已有用户群以快速扩大 DeGate 的社区规模，构建初始共识。另外，其他运营相关的开支也由该池支付，例如奖励有贡献的社区成员等。

20% 融资池，出售此资金池中的 DG 代币来获得 DeGate 运转所需的资金。该部分 DG 代币既可以在公开市场上出售，也可以私下出售给组织或个人，私下出售的价格应以公开市场的价格为基准。融资所得归 Home DAO 所有。

9% 商务拓展资金池，用于激励生态中的其他从业方与 DeGate 展开紧密合作，该部分资金既可以以即时兑付的形式支付给合作方，以换取合作方的服务或商品；也可以以远期期权的形式供合作方购买，使得合作方长期与 DeGate 保持利益一致。商务拓展资金池产生的收益归 Home DAO 所有。

5.2% 预备池，由 Home DAO 按需灵活调配。

2% 用于 DG 代币的做市，以增强 DG 本身的流动性。首期做市投入 1%（1000 万枚）DG，做市的起始估值与出售给创始团队的估值保持一致，即 500 万美元总估值。剩余 1%（1000 万枚）的做市 DG 代币预计将于初始做市开始之后的若干星期内投入做市。该部分代币的所有权以及做市所得均归 Home DAO 所有。

5. 治理

世界唯一不变的，就是变化本身。对于 DeGate 而言，快速做出改变以适应环境的能力至关重要。治理则决定如何变化。

5.1 共识原点

尽管 Home DAO 有权针对 DeGate 的几乎一切做出改变，但是以下初始共识作为社会契约不应被轻易改变，我们称之为共识原点。

- Home DAO 对于由 DeGate 协议的自身过失引起的损失对外承担 100% 的赔付责任；
- 杜绝多数币的暴政，例如，以明显不合理的方式剥夺少数派的合法权益；
- 采用双层 DAO 的治理机制，使得治理模式兼具稳定性和灵活性。

5.2 双层 DAO 机制

DeGate 协议的治理由双层 DAO 机制组成：**Home DAO** 和 **Council DAO**。双层 DAO 机制是为了让 DeGate 协议保持稳定性的同时，兼具决策灵活性。

5.2.1 Home DAO

Home DAO 是 DeGate 协议的直接拥有者和控制者，并获得协议产生的收入，收入通常转换为 DG 代币的形式保存于 Home DAO 账户。Home DAO 通过 DG 代币投票选举产生 Council DAO 的成员，Home DAO 将定期或不定期授权 Council DAO 以一定数额的资金预算，由 Council DAO 代为行使财政权。Council DAO 的智能合约受制于 Home DAO，即 Home DAO 有能力冻结 Council DAO 并提取 Council DAO 的资金，即罢免 Council DAO，并设立新的 Council DAO。

Home DAO 通过 DG 代币对议案进行投票来制定决策，Council DAO 和 DG 代币持有者均可发起议案，后者发起议案有最低支持的 DG 代币数量要求。重大事务应由 Home DAO 直接裁决，重大事务的范围将在经过社区广泛讨论后在《DeGate 治理白皮书》中明确表述，或者 Council DAO 认为关系重大而需要 Home DAO 直接裁决的事务。重大事务交由 Home DAO 直接裁决，有利于 DeGate 协议保持稳定性和一贯性，并取得外界的信任。

5.2.2 Council DAO

Council DAO 受 Home DAO 委任，在 DeGate 协议中直接在代码层面拥有部分控制权，以及掌握 Home DAO 授予的预算资金，负责 DeGate 的日常运行。Council DAO 的成立，是为了使 DeGate 协议在激烈的市场竞争中获得快速应变的能力。非明确规定由 Home DAO 进行的决策均由 Council DAO 完成。

Council DAO 理事会成员由 DG 代币持有者选举产生。理事会成员以一人一票的民主方式制定 Council DAO 的决策，预计刚开始的成员数量为 5 人或 7 人，随着 DeGate 的业务扩大，理事会席位应适度增加。理事会成员应由德才兼备者担任，并由 DeGate 协议向他们支付报酬。

在运作模式上，Council DAO 既可以直接雇佣员工，也可以将事务承包给外部组织完成。

5.3 治理基础设施的建设

在 DeGate 的治理中，将实实在在地践行“**代码即法律 & 法律的执行**”，所有的权利和控制都将完全依赖代码，因此，治理模块所涉及的代码容不得任何差错。正因如此，治理基础设施的建设将是长期的，从最初的以多签合约的方式暂行 DAO 的权利和职能，到最后完全将权利和控制以代码的方式实现，中间是一个逐渐完善的过程。

本白皮书只对治理机制做结构性的描述，关于治理基础设施的具体功能和参数设置，将需要通过广泛的社区讨论来确定，并后续形成**《DeGate 治理白皮书》**。