区块链权益证明的高效金融架构

摘要

为将区块链资产资金融化，最大程度地提高共识效率和促进链上应用程序使用，我们提出一种区块链解决方案。我们建立了一个金融渠道，将区块链资产转化为灵活可交易的金融产品。本文对比了传统金融产品，探讨区块链抵押资产的含义，验证在程序中操作抵押资产的金融影响。通过我们的财务渠道，个人既可以从权益奖励中受益，也可以通过参与区块链应用程序获得收益。节点运营商可以发行衍生品，在一定期限内通过衍生品出售抵押资产。因此，该财务协议为首例允许用户同时通过抵押和应用两个途径获得收益。基础资产衍生品的发行使区块链更加灵活，从而促进区块链行业的金融化进程。

引言

抵押资产的总价值已从 7.41 亿美元增至 47 亿美元，总增长率为 533%。随着新型 PoS 网络的兴起以及现有区块链向 PoS 的迁移，预期资产总值会进一步增长。但是，权益证明要求投资人将其资产在一定时期内在区块链内锁定，不能投放允许短期内交易盈利的二级市场。

所有类型的区块链目的都是为了创建一个数据库系统，各方可以以去中心化的方式共同维护和编辑数据库，任何一方无法进行中心化控制。在区块链经济中，去中心化操作会影响代币代理人的的商业动机和操作惯例。在标准的权益证明系统中，越多人持股，就有越多的代币处于非流通状态。这看似有利于代币价格上涨，但多数情况下，流动性不足会阻碍整个金融网络的发展。

充足的流动性对于支撑金融网络而言是十分必要的。流动性不足会影响需求，因为此种情况下一旦出现需求的小幅上涨趋势，就可能导致价格急剧上升，甚至可能超过应用程序买家所能承受的最大倾向范围。如果交易对价格的影响过大，退出系统的成本也会增加，最终影响数据提供方的收益。由于交易买卖引起的价格变动称为滑点，滑点的起伏不定是各方都不希望的结果。

我们计划创建一个连接协议层和应用程序层的财务渠道。PoS 代币持有者可将本地代币存入权益合同并获得与原代币具有同等价值的合成代币。持有人可以使用合成代币在二级市场上交易，也可进入链上应用程序，例如 defi。持有人通过自由使用代币，实质上就是在权益证明链上的抵押池中通过已经抵押的代币获得报酬。相反，对于正在运行具有大量抵押资产的抵押节点运营商，他可以通过我们的财务渠道进行抵押拍卖，发行由自己抵押资产做保的金融衍生产品。衍生产品采用代币形式，拍卖竞标者可以在应用程序或交易中自由使用这些衍生代币。

我们的金融渠道建立在 Polkadot 上，由基层开发者开发后连接到平行链。财务层是一个包含了各种金融模型优化智能合约层。智能合约在 polkadot 区块链上运行，可以加强合约性质，以一种编程和自动算法的形式促进货币和有物品价值所有权的交易。即使在某些

情况下，智能合约需要由中心化数据端执行，去中心化的共识记录也可以使合约和执行方面的摩擦相对减少。智能合约可以提高某些意外情况的合约约束力和执行力。

金融架构

权益衍生品发行：

我们提出一种权益拍卖机制，在此机制中，利益相关者可以拍卖所抵押的资产。买家可以竞标拍卖的一部分，即一部分的抵押资产权益。买家也可以大量购入，生成以抵押为基础的衍生工具。治理方面，首先将验证资产抵押方的有效性以及拟发行衍生品的抵押资产的数量。衍生产品合约的定价由发行人确定，但我们有一个基准框架，可为发行人设定要价提供参考。我们首先定义股份合同的特征，如下所示：

每个抵押合同的标准符号：

•权益年回报率：$k\%$;

•抵押期：T;

•到期时间：τ;

•合约大小：C（一般情况下，假设 C=1）；

•当前代币价格：S。

•抵押合同的当前价值：$V = S * (1 + k\%)^{\tau/T}$。

如果市场上有 n 个合约交易，所有符号都用 i 标记。假设 0=τ0<τ1<⋯<τn，则代币的（连续复合）返回率应为时间[τi-1]，τi 上的分段常数 ri。这些回报率应满足

$$\begin{cases} e^{r_1*\tau_1} = \frac{(1+k_1\%)^{\tau_1}}{V_1/S} \\ e^{r_1*\tau_1}e^{r_2(\tau_2-\tau_1)} = \frac{(1+k_2\%)^{\tau_2}}{V_1/S} \\ \vdots \\ e^{r_1*\tau_1}e^{r_2(\tau_2-\tau_1)}\cdots e^{r_n(\tau_n-\tau_{n-1})} = \frac{(1+k_n\%)^{\tau_n}}{V_n/S}. \end{cases} \tag{0.1}$$

因此我们得到

$$\begin{cases} r_1 = \frac{1}{\tau_1}[\tau_1 \ln(1+k_1\%) - \ln(V_1/S)] = \ln(1+k_1\%) - \frac{\ln(V_1/S)}{\tau_1} \\ r_2 = \frac{1}{\tau_2-\tau_1}[\tau_2 * \ln(1+k_2\%) - \tau_1 * \ln(1+k_1\%) - \ln(V_2/V_1)] \\ \vdots \\ r_n = \frac{1}{\tau_n-\tau_{n-1}}[\tau_n * \ln(1+k_n\%) - \tau_{n-1} * \ln(1+k_{n-1}\%) - \ln(V_n/V_{n-1})] \end{cases} \tag{0.2}$$

现在，如果要评估具有到期时间和收益率 k%的抵押合同，则其价值应为：

$$\begin{aligned} V &= e^{r_1*\tau_1}e^{r_2(\tau_2-\tau_1)}\cdots e^{r_i(\tau_i-\tau_{i-1})}e^{r_{i+1}(\tau-\tau_i)} \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(e^{r_{i+1}(\tau_{i+1}-\tau_i)}\right)^{\frac{\tau-\tau_i}{\tau_{i+1}-\tau_i}} \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(\frac{(1+k_{i+1})^{\tau_{i+1}}}{V_{i+1}/S} / \frac{(1+k_i)^{\tau_i}}{V_i/S}\right)^{\frac{\tau-\tau_i}{\tau_{i+1}-\tau_i}} \\ &= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(\frac{(1+k_{i+1})^{\tau_{i+1}}}{(1+k_i)^{\tau_i}}\frac{V_i}{V_{i+1}}\right)^{\frac{\tau-\tau_i}{\tau_{i+1}-\tau_i}} \end{aligned}$$

在此定价指导下，发行人可以评估其衍生产品的当前价格并公开拍卖抵押资产。

ETF 的发行：

我们还提供获得多种 pos 奖励的合成金融投资产品，该产品可以通过一种最简单方法，让用户选择最优质的的权益证明协议下进行长期交易。持有人持有的每一枚代币都可以获得抵押资产的最优回报。我们会根据市值和日交易量筛选 POS 资产的资质，然后通过抵押率和奖励率等因素对这些资产进行排名。然后，我们将筛选出排列前三位的代币作为合成组合，并每月进行市值加权和重新评估。

共识和协议：

我们使用基于 Polkadot 的权益证明共识算法，该算法是一种混合共识模型，用于区块创造，而不用于确定区块的最终性质。我们的网络具有多种类型的节点：勤奋节点、挖掘节点和权益代理节点。勤勉节点除具有区块生成功能外，还具有投票和渠道维护的权利。当勤奋节点达到投票阈值时也将成为区块生成节点。挖掘节点生成区块，在投票方面更具吸引力。权益代理节点从块生成节点筛选得出。勤奋节点，挖掘节点和权益代理节点必须具有相同的网络访问环境和计算功能。尽管勤奋节点不需要产生区块，但是有必要创造真实节点来传输规律性的交易数据。节点的区块创造、区块丢失、节点掉落或其他恶意行为将受到惩罚，同时扣除节点的自抵押资产和用户所等待的奖励。利益主体节点将获得额外的利益收益；违反收益合同的条款将受到相应的惩罚。罚金将转入议会资金，随后进行全民公决决定如何处理。

节点注册和应用程序向所有用户开放。设置节点服务器后，即可开始运行。我们使用一点一票模型来防止暗箱操作。所有用户都可以使用 BNC 进行节点投票选举。为保证网

络稳定运行，同步节点和块生产者节点需要支付相同的成本。因此，同步节点和块生产者节点将获得相同的收益。权益代理节点将成为我们多链生态系统的重要组成部分，负责产生生态系统的收益。除大宗节点的收入外，权益代理节点还将获得收益产生的股息。

运行环境作为链的重要组成部分，比智能合约更底层。运行环境由各种运行时模块组成。运行时区块包括帐户、余额、抵押、智能合约、交易过渡、治理和共识等模块。模块可以彼此独立，同时允许模块相互调用。该链的大多数代码逻辑都在运行时环境中运行。

运行环境允许每个运行模块独立升级，而它的一个重要功能是没有硬分叉升级。现有区块链系统升级时，由于每个节点的运行版本不一致，存在造成整个链条硬分叉的风险，严重影响了整个生态系统的健康发展以及节点和用户的利益。每次升级模块，我们都会生成两个版本：本地版本和 WASM 版本。当运行时环境确定更新的模块的版本与当前本地版本一致时，为获得最快的运行效率请直接运行本地版本代码。

用户通过跨链将资产锁定在主链内，这部分资产经过签订多重托管合同，托管合同由多个见证节点共同管理。通过去中心化治理机制，见证节点由各节点参与方投票选出并定期轮换。同时，当主链托管合同持有的资产太大时，可以将其拆分为多个托管合同，出于安全性考虑，会引入更多的托管节点组进行托管。

保险与安全：

通过存入我们的平台代币并指定某些关键参数（例如基础资产、预购价、到期日等），期权程序开发者可以制造称为 oTokens 的任意可替代期权代币。出售 oTokens 代币使开发者赚取溢价，最终通过自有的抵押资产创收。然后，买家可以购买这些 oToken，这些

oToken 在 0x 或 Uniswap 等交易所进行交易，从而确保市场流动性。除此框架所支持的可互换、可自由交易的 ERC20 期权合约之外，买家还可以特别关注存款保险的保护性看跌策略（例如，保护代币市场的用户，如复合货币用户免受黑客入侵和流动性危机影响）以及保护用户避免 DAI 价值崩溃风险。我们还考虑其他一些情况，比如希望提供风险保护期权卖方可以采取措施，使用一种不同于与以行使价计价的资产（例如美元）的另一种抵押类型（例如 ETH）。

财务审计：

审计师采用区块链技术上策略是互补和调整性的，因为在处理多审计师共同参与的交易项目时，越多审计师采用区块链技术，那么审计的损失代价就越小。但如果审计客户宁愿冒着被查办的风险还是倾向谎报数据的话，此时客户往往宁愿选择不用区块链技术的审计师，即使这类审计师的收费更低。因此，如果其他审计师没有使用该技术，那么审计师往往同样不会使用，因为不仅利润上不划算，还可能造成客户丢失，最终不如传统审计师。但总体而言，区块链有三个有利于审计的技术特征：（i）去中心化：区块链的点对点设计，无需受有信用度的数据中心的要求限制；（ii）加密性：零知识证明支持加密通信，保护数据隐私；（iii）不可篡改：一旦审核员通过联合区块链请求信息，任何审核员或外部黑客都很难有意修改或删除该信息，除非能够做到修改联合区块链上绝大多数的节点信息。我们将建立去中心化的财务审计系统，以监督权益拍卖的权益交易人拍卖完成后的活动。

经济原理

我们拥有用于金融渠道的本地代币。此种代币可为我们的渠道获取链上价值。我们的代币的主要功能如下：

服务：我们提出一种代币锁定奖励模型，该模型使用户可以通过锁定代币来奖励协议贡献者，而无需花费自身代币。此过程类似于锁定代币：原理是由加盟者根据已签署的条款将其锁定在代币中。衍生产品发行人必须就所需的代币和时间长度进行协商，允许我们的财务渠道为其协议作公开记录。一旦确定条款，衍生产品发行人就会按照其协议条款将交录入区块链。我们将此交易称为协议交易。衍生发行人需要抵押一定数量的平台代币以获得拍卖许可。

ETF 发行：我们将分配平台代币池来发行权益 ETF。我们新发行的代币价值将紧跟通过算法管理的透明化 POS 代币配餐。由我们新发行的代币跟踪的基础资产产生的奖励将用于回购和销毁。

保险：保险的概念来自过去，人们集中资源来保护彼此抵抗所有人所面临的风险。我们意识到，我们可以在一个平台上建立一个共同体，在此平台上，个人只需要信任系统，而无需信任每个人。此举目的是为我们的用户提供更简单、透明、可访问且更优惠的财务保护措施以防范风险。我们的平台代币将有一组保险资金池来为链上活动提供保护。我们提供衍生品担保业务，为权益人和权益购买方防范价值存储的过程的黑客入侵风险。

购回及销毁：我们将通过财务渠道的运营从交易和服务中产生费用收入。所有收入将用于回购代币，我们将回购的代币销毁，作为所有代币持有者的权益保障。