

Shadows Network

白皮书 V1.0

关键词

抵押型稳定币：将代币债务化，在 Shadows 系统里，将 DOS 超额抵押铸造出稳定币 xUSD，持有 1 xUSD 等于承担 1 USD 的债务。

合成资产：由智能合约为现实资产构建链上镜像世界，让对标资产价值在链上以债务的形式安全自由流通。

抵押率：合成资产协议的核心数据，保证支撑合成资产的抵押资产能够应对大幅的价格波动，防止系统性风险。

可变债务池：由 DOS 抵押铸造发行的合成资产将以债务方式记账，合成资产价格的变化将影响债务池水平动态变化，所有抵押人的债务总和我们称之为债务池。

债务抵押 (CDO)：Shadows 系统用户将所持有的债务（合成资产）进行抵押借贷，为不同风险偏好的投资人提供更灵活的资金流动性。

债务转换：合成资产的交易本质上是将一种合成资产债务（比如 xUSD）由智能合约执行转换成另外一种合成资产债务（比如 xTSLA）。

摘要

Shadows Network 是基于 Substrate 开发的 DeFi 合成资产发行协议和合成资产交易的底层网络，是 web3.0 价值存储的支柱，将使任何人在任何地方都能够自由的交易链上资产。

Shadows Network 是波卡的平行链，专注于将现实世界金融资产通过协议映射上链，是合成资产发行协议，也是去中心化的合成资产的交易平台和抵押借贷平台。

Shadows Network 系统上的合成资产由原生令牌 DOS 提供底层担保，将 DOS 抵押锁定在智能合约中即可发行合成资产。

DOS 将成为链下资产映射上链的价值连接管道。

Shadows 将支持合成稳定币 (xUSD)，加密货币 (xBTC) 和金融产品 (xGOLD、xTSLA) 等多种合成资产。

Shadows Network 将努力通过参与平行链插槽竞拍成为波卡平行链之一，但是就算到时候没有成功获得插槽使用权，shadows 也会计入平行线程以获得跨链能力。

Shadows Network 由三大模块组成

合成资产发行协议

所有合成资产由 DOS 提供底层价值担保，用户将 DOS 抵押进智能合约中即可生成合成资产，并产生以 DOS 为计价的债务。用户要解锁其 DOS 时，必须先销毁合成资产结算该笔债务。所有合成资产将满足 800% 的抵押率，抵押率低于 800% 时抵押品无法赎回。

Shadows V1 版本支持由 DOS 抵押生产合成资产。

V2 版本将通过跨链支持 BTC，ETH，DOT 做为抵押品，并产生以 BTC 等为计价的债务，抵押率要求最低为 180%。

合成资产交易协议

合成资产价值交换将由交易协议提供支持。

Shadows 交易协议具有以下几个优势：

- 1， 基于债务模型的设计，合成资产的交易本质上是债务的转换，由智能合约执行销毁一种资产（债务），再生产另外一种资产（债务）。这种交易方式，不需要对手盘，也不需要订单簿，不用担心流动性和滑点的问题。让合成资产的交易更加简单、安全和高效。

- 2, 通过合成资产交易, 可以实现在不实际持有该资产的情况下, 实现对该资产的交易。这种交易可以减少资产交换的摩擦, 可以在不同类型的资产间进行快速交换, 比如在特斯拉股票、黄金、比特币等不同资产之间进行快速交换, 因此合成资产可以帮助投资者触及到更大范围的资产。

债务抵押借贷协议



Shadows Network 系统内将有一个借贷池, 用户可将债务 (比如 xUSD) 放入借贷池智能合约中, 进行放贷。借款方出于资金灵活流动性的需求, 将债务 (合成资产如 xTSLA) 抵押进借贷池中, 支付利息并获得贷款 xUSD。

借贷池利率有供需自动平衡, 所产生的利息收益将按照在借贷池出借的 xUSD 所占比例进行分配。

为什么需要合成资产

总有人无法或不愿意持有初始资产, 合成资产满足了我们更多样的需求。对有避险需求的用户而言, 相较于美元, 他们需要区块链上的稳定币 (属于合成资产), 以便于资金流动; 合成资产往往比原始资产具有更多金融属性。比如持有 BTC 是没有利息的, 而持有锚定 BTC 的 xBTC 可以获得持续收益。

合成资产的需求主要源于交易, 通过模拟某种资产获得该资产的风险敞口, 从而获得可能的赚取收益的机会。例如特斯拉公司的股票并非所有国家的人都可以购买。但如果通过合成资产的方式, 用户可以通过购买特斯拉公司股票的合成资产, 从而获得特斯拉股票上涨的收益, 当然同时也会承担下跌的风险。

持有 DOS 权益

持有 DOS 具有以下几个权益:

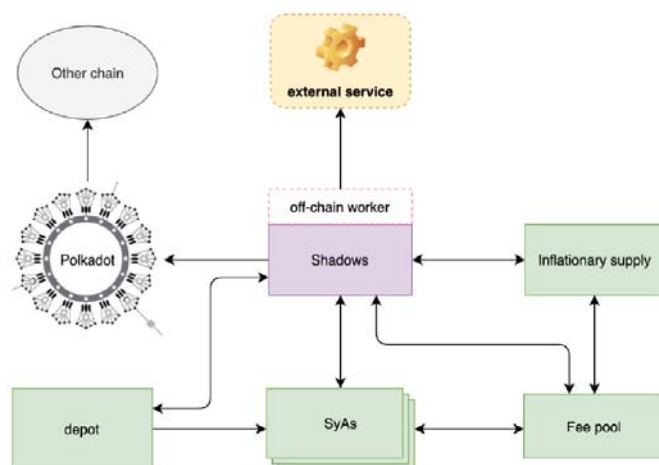
- 1, **发行合成资产:** DOS 是 shadows 系统内生成合成资产的抵押资产, 是进入 shadows 系统的工作令牌。
- 2, **交易奖励:** shadows 交易协议每笔交易产生一笔交易费, 会被存到交易费用池中。交易费用收入每周按照比例分配给符合条件的 DOS 抵押人。

- 3, **抵押借贷**: 用户可用 DOS 合成稳定币 xUSD, 并存入借贷池获得放贷利息收益。借贷池的收益也将按照比例分发给放贷人。
- 4, **合成资产奖励**: 参与铸造成资产的用户可获得 DOS 奖励, 奖励会按照比例每周分发给 DOS 抵押率不低于 800% 的 DOS 抵押人。
- 5, **Staking 奖励**: 用户持有 DOS 并参加 staking 可获得 DOS 奖励, 奖励每周按比例发放一次。
- 6, **销毁机制**: 交易手续费收入和借贷池手续费收入, 将按照固定比例 30% 每周用于销毁, 由智能合约自动执行, 使得 DOS 总量进入通缩模式。
- 7, **系统治理**: DOS 令牌持有者对系统有投票治理权, 比如新功能增加, 协议升级和修复等。

Shadows 工作机制

系统架构

基于波卡的跨链特性, Shadows 系统支持跨链资产合成与交易。



铸造合成资产

用户可以通过 Shadows 合成协议铸造成资产, 由智能合约锁定 DOS 做为底层抵押品, 铸造生成 xUSD, 并且要求抵押率不低于 800%。

用户每一次抵押 DOS 来铸造成资产, 将会产生一笔以 DOS 记账的债务, 并且该笔债务被添加到债务登记簿中, 以 xUSD 存储。

将债务分配给 DOS 抵押人后，Shadows 将向 xUSD 智能合约发出指令发行新的金额，并将新的金额添加到总合成资产的供应量中，然后将新铸造的 xUSD 发放到用户的钱包，更新钱包余额。

当 DOS 的价格上涨时，抵押率会提高，用户所抵押的 DOS 由智能合约执行自动解除锁定。反之如果 DOS 下跌，则抵押率会降低，用户需要增加 DOS 以满足抵押率要求。

债务抵押率 Collateralisation Ratio

用户将 DOS 抵押进 shadows 系统铸造成合成资产，形成以 DOS 为计价的债务，当抵押人将其抵押率维持在 800% 时，可获得 DOS 激励。这种超额的抵押率可确保合成资产有足够的抵押来支撑价格的大幅波动。

当 DOS 或合成资产的价格波动时，会影响到债务池的债务变化，从而每个抵押人的抵押率也会跟着波动。当抵押率低于 800% 时，抵押人将无法获得 DOS 奖励，和领取交易费用奖励，直到恢复抵押率为止。

当抵押率低于规定阈值时，抵押的 DOS 将无法赎回，抵押人可通过销毁部分合成资产或补充 DOS 来调整其抵押率。

动态债务

用户抵押 DOS 创建合成资产时会产生债务。用户的债务会根据网络中合成资产的汇率和供应量变动，增加或者减少。

例如，如果系统中所有的合成资产都是合成黄金（xGOLD），xGOLD 价格下降 50% 时，则系统中的债务将减少 50%，而每个抵押人的债务也将减半。

在另一种情况下，当系统中只有一半的合成资产是 xGOLD，另外一半是 xTSLA，当黄金的价格涨了 50%，TSLA 股票价格不变的情况下，系统的总债务以及每个风险承担者的债务将增加四分之一。

交易对手

所有使用 DOS 进行抵押铸造合成资产承担债务的用户，都是合成资产交易平台的交易对手。抵押铸造合成资产获得激励的同时也承担了系统中的债务波动风险。

我们通过下面一个例子来说明债务是如何计算的，为何 DOS 抵押人是合成交易平台的交易对手：

- 1: 张三和李四抵押了价值 5 万美金的 DOS 铸造了 xUSD，此时网络中的总债务为 10 万美金，张三和李四分别承担了系统中各 50% 的债务。
- 2: 张三将他所持有的 xUSD 全部用于买入 xGOLD，李四则继续持有 xUSD。
- 3: xGOLD 的价格上涨了 50%，则张三的总持仓价值变成 7.5W 美金，其中张三的 2.5 万美金的利润让网络的总债务达到了 12.5 万美元。

4: 张三和李四仍然分别承担网络总债务的 50%，即每人 6.25 万美金。当张三的 xGOLD 的价值减去他 5 万美金的债务，可获利 1.25 万美元；而李四的仓位价值仍为 5 万美金，但他的债务增加了 1.25 万美金，即李四的损失为 1.25 万美金。

交易合成资产

在 shadows 合成资产交易协议里，合成资产的交易主要是跟智能合约交互，没有订单簿，也没有交易对手。合成资产的交易对于 Shadows 系统来说，只是将债务从一种合成资产由智能合约转换成另外一种合成资产，这样用户也不用担心流动性问题。

我们通过下面的例子来描述合成资产交易的过程，以 xUSD 交易 xGOLD 为例：

- 1: 销毁源合成资产 xUSD，并减少该钱包地址的 xUSD 余额，再更新 shadows 系统里的 xUSD 供应总量。
- 2: 根据 xGOLD 的价格计算汇率，确定需要兑换的金额。并收取 0.3% 的交易费用，并将该交易费用以 xUSD 发送到交易费用池，用于给所有 DOS 抵押人激励。
- 3: 剩余的 99.7% 由目标合成资产 xGOLD 的智能合约发行，并更新至钱包余额。
- 4: 最后更新 shadows 系统里的 xGOLD 的供应总量。

系统激励

在系统中有 3 种激励奖励可领取：

- 1: 用户在交易合成资产时收取 0.3% 的费用并发送到交易费用池中，做为 DOS 抵押人的奖励。

交易费用奖励根据每个抵押人已发行债务的比例进行分配。例如，如果一个抵押人发行了 10,000 xUSD 的债务，债务池为 1,000,000 xUSD，该抵押人的债务占总债务池的比例为 10%，此时奖励池有 100 xUSD 的交易费用收入，在派发奖励的时候该抵押人可获得 10 xUSD 的奖励。

- 2: DOS 持有奖励，抵押人可每周领取一次持有 DOS 的奖励，该奖励的来源于 DOS 矿池的产出，奖励的金额也是根据该抵押人所占有总债务池的比例来分配。

- 3: 借贷池奖励，出借人可每周领一次借贷池收益的奖励。例如该抵押人出借了 100 xUSD 进入借贷池，此时借贷池的总规模为 10,000 xUSD，该出借人占有借贷池总金额的 1%，此时借贷池的利息收益为 50 xUSD，在派发借贷奖励的时候该出借人可获得 0.5 xUSD 的出借利息收益。

债务池

Shadows 系统用户在铸造或销毁合成资产时，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。这可以计算 DOS 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。

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。

销毁债务

当用户想要退出系统或减少债务并解锁抵押的 DOS 时，必须先偿还债务。当抵押率低于 800% 时，则抵押的 DOS 无法解锁赎回。

例如：用户抵押 DOS 铸造出 10 xUSD，当他要赎回 DOS 时，必须先销毁 10 xUSD 才能解锁抵押的 DOS 并赎回。在抵押期间如果债务池发生波动，个人债务也会发生变化，则抵押人需要销毁比铸造 xUSD 时更多或者更少的债务。

智能合约销毁债务过程：

- 1: Shadows 智能合约确定抵押人债务余额并将其从“债务登记簿”中删除。
- 2: 销毁所需的 xUSD 金额，并且更新 xUSD 的总供应量以及用户钱包中的 xUSD 余额。
- 3: 通过销毁 xUSD 赎回这些 DOS，并将余额被设置为可转让。

清算机制

如果抵押率降至 800% 以下，抵押人将无法获得交易费用奖励。同时为了避免系统性风险，我们还引入了清算机制。当抵押人的抵押率低于 250% 时，系统将会提示清算风险。如果一段时间内还未增加抵押率，抵押品将会被清算。

这里引入了“deposit liveness period”（补仓活跃期）：抵押人可以在活跃期内（如：4 个小时）追加抵押品来避免清算。活跃期结束后，如果抵押率还是低于 250%，这时候任何 DOS 的持有者都可以对抵押品发起清算，清算成功后，清算人可以从中获取一定的收益。

国库

Shadows 系统内将设置一个国库基金，做为风险基金，以防止发生系统性风险时使用国库基金进行赔偿，以减少系统用户的损失和风险。

跨链

Shadows 将作为波卡平行链（平行线程）运行。所以相对于以太坊和 EOS 的合成资产协议，Shadows 将具有跨链兼容性。有能力提供跨链资产抵押，比如用户可以抵押 BTC、ETH 来铸造合成资产，这是巨大的优势。跨链兼容为我们通往新市场和获得新用户开辟了道路。

链下工作机

Shadows 系统中所有合成资产的价值均需要从链下获取然后提交到链上。常规的做法是通过预言机 (Oracles)。预言机是一种外部服务，通常用于监听区块链事件，并根据条件触发任务。当这些任务执行完毕，执行结果会以交易的形式提交至区块链上。虽然这种方法可行，但在安全性、可扩展性，和基本效率方面仍然存在一些缺陷。

为了使链下数据集成更加安全和高效，我们将使用 Substrate 提供的链下工作机。链下工作机子系统可执行需要长时间运行且可能非确定性的任务(比如 web 请求、数据的加解密和签名、随机数生成、CPU 密集型计算、对链上数据作枚举 / 聚合等)，具体可以参考：<https://substrate.dev/docs/zh-CN/knowledgebase/learn-substrate/off-chain-workers>。

发展规划

- 2021-Q1 Shadows V1 版本上线，支持 DOS 抵押合成资产
- 2021-Q2 参与波卡平行链插槽拍卖，V2 版本上线，支持跨链资产合成与交易
- 2021-Q3 V3 版本上线，支持合成资产抵押借贷
- 2022-Q1 Shadows 系统过渡到 DAO 模式治理
- 远期规划 合成资产（衍生品）期货交易、杠杆交易

官网：www.shadows.link

The end