BENFEN WHITE PAPER

一键发币白皮书

版本日期 7/25/2025

君子务本
本立而道生

Benfen.org

目录

本分链提出“一键发币”功能，旨在为用户提供一个简单、安全、可配置的发行入口，支持包括普通加密代币、稳定币以及RWA在内的多种资产类型，允许任何背景的用户——无论是专业开发者还是非技术人员——都可以安全、高效地创建并发行自己的代币资产。

1. 代币发行原理

本分链采用面向对象模型，代币是封装了自身数据与所有权的独立**“对象”（Object）**，而非账户中的数字。创建代币即通过智能合约（称为 Move 模块）定义并管理一个新的可转移对象。这种设计逻辑清晰，且能通过并行处理提升效率。

为统一资产发行，框架内置了官方 coin 核心模块，为同质化代币提供铸造、销毁、分割、合并等标准函数。任何人皆可调用，无需重复制定标准，确保了生态资产的安全与互操作性。

2. 代币发行的具体流程

在本分链上进行代币创建和发行的具体流程如下：

1. **代币参数配置：**用户首先在发行界面上，配置新代币的核心参数，包括代币名称、代币符号、代币的最小单位、代币在初始发行时的总量等。
2. **定义代币类型：**系统将根据用户输入，自动生成一个专属的 Move 智能合约模块。该模块的核心是定义一个一次性**见证类型（Witness Type）**。此类型是一个空的结构体，不存储任何数据，其唯一作用是作为新代币在全网的“身份凭证”，将此代币与其他所有资产区分开来。
3. **注册代币：**在定义类型之后，系统会部署上述模块，模块中的初始化函数会自动调用官方 coin 模块中的注册函数。这一步会向整个区块链注册新的代币，并生成一个至关重要的**金库凭证（TreasuryCap）对象**。该凭证是未来增发代币的唯一权力证明，将被安全地转移至用户的钱包中。
4. **代币铸造与初始供应：**系统使用用户钱包中的金库凭证自动执行一次铸币操作，按照用户设定的初始总供应量铸造出第一批代币。这批新铸造的代币将以一个代币对象的形式生成，并同样被直接发送到用户的钱包中。

3. 发行代币资产类型

除了常规同质化代币之外，本分链的“一键发行代币”功能也支持加密货币中至关重要的两个资产类型--稳定币和现实世界资产（RWA）。

3.1 稳定币

稳定币是连接数字世界与现实世界价值的桥梁，也是 DeFi生态的基石。用户可以自己发行新的稳定币，但是需要通过与跨链引入的外部主流稳定币建立直接的链上兑换关系，以获得可靠的价值支撑。具体流程如下：

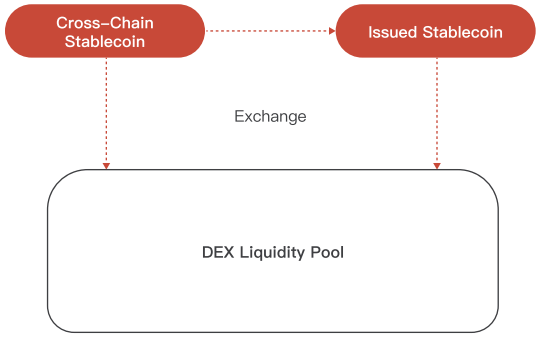

图1：稳定币创建流程图

1. **引入价值储备：**发行方必须先通过 BenFen 跨链桥，将一定数量的主流稳定币作为初始价值储备，从其他公链转移至本分链。
2. **创建流动性池：**在用户使用“一键发行”功能创建出自己的稳定币后，发行方必须在 BenFen 生态内的官方 DEX（BenPay DEX）中，创建一个由“新稳定币 / 外部稳定币”组成的交易对池。
3. **维护价格稳定：**发行方有责任通过管理流动性池来维护其稳定币的价格锚定。BenPay DEX 的价格预言机也会持续获取该交易池的价格信息，提供给生态内其他需要精确价格数据的协议，例如借贷协议、衍生品交易所等。

3.2 RWA

将真实世界资产（如房地产、股票、债券等）通过代币化引入链上，是区块链技术最具潜力的应用方向之一。但是 RWA 资产的核心挑战在于如何确保链上代币与链下资产的权利对应，并满足现实世界的法律和监管要求。BenFen 对 RWA 的发行采取“合规优先”的原则。

- **法律与文件完备性：** RWA 的发行方必须提供完善的法律文件，如资产描述、第三方评估报告、产权证明及投资条款等，用以清晰界定代币持有者的合法权利（如所有权、收益权等）。
- **资产托管与审计：** 发行方也需要聘请具备合格资质的、受监管的第三方机构对 RWA 项目的标的资产进行托管和定期审计。BenFen 也将积极与持牌信托公司、资产管理公司等机构建立合作，确保 RWA 项目链下资产的真实性、完整性和所有权的清晰性。
- **投资者身份认证：** 为遵循全球 AML / KYC 法规，所有 RWA 的发行方与投资者，均需通过 BenFen KYC 等协议的身份验证流程。

4. 使用项目方代币支付 Gas

为了降低用户门槛，本分创新性地允许用户使用白名单内的项目方代币直接支付 Gas 费用，这同时也为生态项目方发行的代币赋予了额外的支付效用，增强了其内在价值和需求。

该机制通过 BenPay DEX 预言机来获取项目方发行代币的公允价格，该价格在每个周期（Epoch）开始时更新一次，并在周期内保持稳定。用户交易时，系统会根据此汇率自动计算并从用户的项目方代币余额中扣除等值的 Gas 费用。

为了预防价格操纵风险，此功能采用基于社区治理的白名单制度。项目方可以提交提案，社区将综合考量项目质量、代币流动性与经济稳定性等因素进行投票。如果提案获得通过，则该代币会被添加到白名单中，可正式用于支付全网的 Gas 费用。

5. 使用赞助交易进行 Gas 代付

此外，本分也推出了赞助交易功能，允许项目方直接为用户支付 Gas 费，以此降低新用户的使用门槛，帮助项目方进行用户拉新、留存以及精准的活动激励。

实现赞助交易的关键，在于其交易结构在协议层面便已经将“交易发起者 (Sender)”与“Gas 费用支付者 (Gas Payer)”明确分离。这种原生解耦的设计，使得赞助交易的实现异常简洁，无需再通过“打包–转发”这类复杂的链下操作来完成，使赞助交易的实现更简洁、安全、快速，且开发成本更低。

赞助交易的具体流程如下：

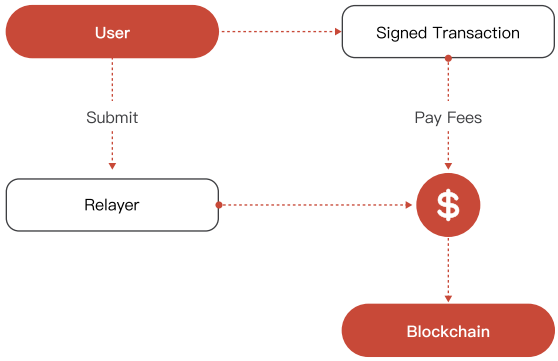

图2：赞助交易流程图

1. **用户构建并签署交易意图：**用户在进行交易时，DApp 会根据用户的意图，构建一个**可编程交易块 (Programmable Transaction Block, PTB)**，这个 PTB 包含了具体需要执行的链上操作，并将交易发起者设置为用户的地址。随后，DApp 会请求用户对该 PTB 进行签名，以确认其同意执行意图。

2. **向赞助方提交请求：**用户完成签名后，包含 PTB 本身及其对应签名的请求数据，将被发送至赞助方进行验证。

3. **赞助方验证请求：**赞助方收到请求后，会执行严格的策略验证，以防范滥用。验证内容可能包括：用户身份、交易频率限制、以及PTB内的操作是否符合赞助范围等。

4. **赞助方封装并为交易签名：**验证通过后，赞助方会为这笔交易添加 Gas 支付信息（例如支付地址、愿意支付的 Gas 单价、本次交易的 Gas 费用上限等），使用自身私钥对完整的交易进行签名，代表赞助方授权从其账户中支付本次交易的Gas费用。

5. **交易提交与链上确认：**这笔包含用户和赞助方双重签名的交易被提交至本分链节点处。节点在执行前会同时验证两个签名的有效性。验证通过后，交易中的操作被执行，Gas 费用从赞助方的账户中扣除，交易完成。