BENFEN WHITE PAPER

本分公链

版本日期 02/02/2026

『新一代现实世界支付公链』

君子务本
本立而道生

Benfen.org

目录

免责声明：本白皮书中的任何内容都不构成销售的要约，或购买任何代币的邀请。本分仅发布本白皮书以接受公众的反馈和意见。如果本分将出售任何代币（或未来代币的简单协议），它将通过确切的发售文件进行，包括披露文件和风险因素。这些明确文件预计还将包括本白皮书的更新版本，该更新版本可能与当前版本有很大不同。

本白皮书中的任何内容都不应被视为或阅读为本分业务或代币将如何发展，或代币的效用或价值的保证或承诺。本白皮书概述了当前计划，这些计划可能会在其自行决定的情况下发生变化，其成功将取决于本分控制之外的许多因素，包括市场因素和数据和加密货币行业等因素。关于未来事件的任何声明都仅基于本分对本白皮书中描述的问题的分析。该分析可能被证明是不正确的。

1. 本分的愿景和使命

自比特币问世以来，它被定义为点对点的数字现金系统。区块链分布式账本技术由比特币构建而来，经历了令人瞩目的演进，并对多个领域产生深远的影响。作为首个也是最广为人知的加密货币，比特币具备去中心化、安全和透明等优势。但极端的价格波动，也严重制约了其作为交易媒介和价值存储的潜力。

稳定币作为 Web3.0 世界最重要的应用之一，它的出现在一定程度上解决了这个问题，其相对稳定的价格使其成为区块链领域最主要的支付手段，也是 PayFi（Payment Finance，是指在区块链和加密货币领域中，将支付功能与金融服务相结合的一种创新技术和应用模式）浪潮中不可或缺的中坚力量。然而，中心化、不透明、缺乏公链的原生支持等问题在一定程度上限制了稳定币更大规模的推广和应用。

因此，我们决定打造**本分 —— 新一代现实世界支付公链，采用 Move 语言构建，具备安全、低成本、可扩展等技术优势。内置原生锚定币BUSD，用户可直接使用稳定币支付 Gas，大幅降低使用门槛。BUSD 作为 BenFen 公链生态的核心资产， 1:1 锚定美元，由跨入的 USDT/USDC 在链上铸造而成。链上原生支持跨链，并通过多种生态应用，覆盖真实支付场景。本分致力于构建开放的支付网络，连接跨境支付、电商平台与线下商户，推动多元应用生态发展。**

作为首个原生支持稳定币支付 Gas 费的公链，本分围绕稳定币，基于市场的需求，打造了完整的闭环生态，包括但不限于去中心化金融 (DeFi) 服务、资产跨链服务、支付解决方案、借贷以及现实世界资产代币化 (Real World Assets, 简称 RWA) 等。开发者亦可以借助本分强大的去中心化技术与丰富的底层金融服务，基于安全的 Move 语言快速开发各种生态应用。

本分的架构设计确保了本分链、DEX、稳定币和生态应用之间能够相互促进，形成一个层层驱动的飞轮。这不仅提高了整个网络的效率和可靠性，还为链上应用的广泛采用提供了坚实的基础，从而推动了区块链技术在更广泛场景下的应用和发展。通过这样的综合性设计，本分旨在成为领先的区块链生态系统，为用户和开发者提供一个全面、高效、安全的区块链服务平台。

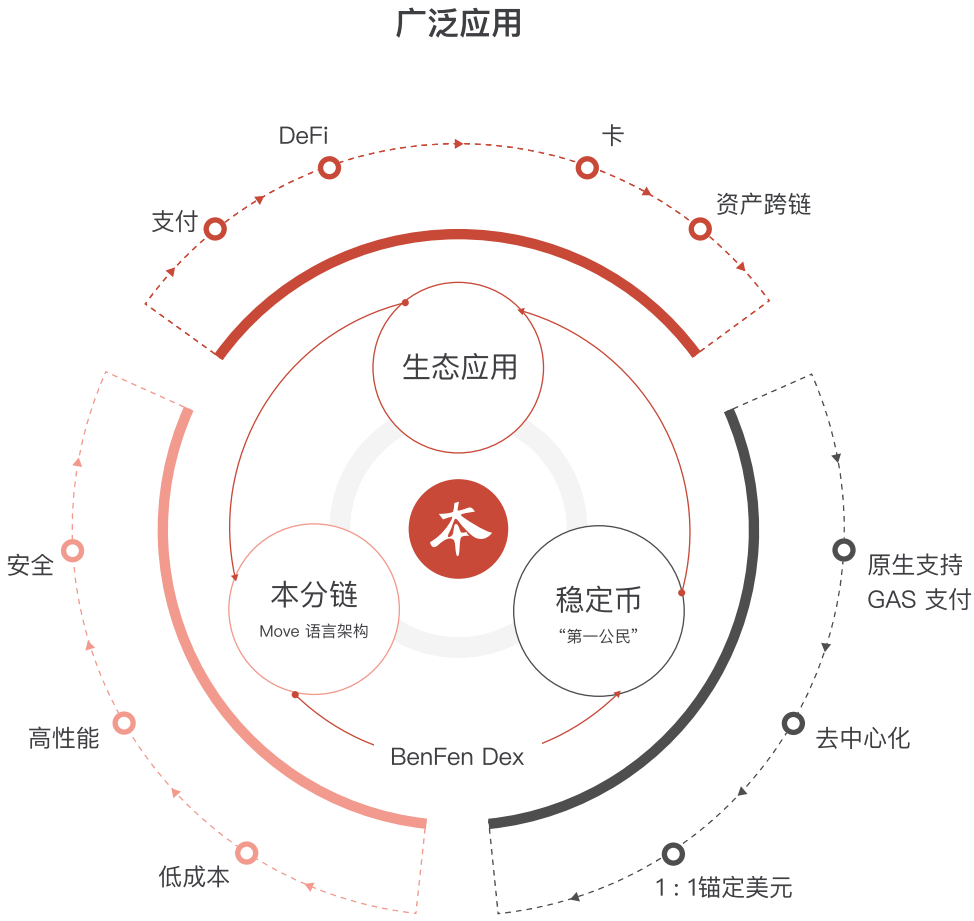

图1: 本分生态系统

2. 重点名词释义

为方便读者能更好更便捷的理解全文，我们现将重点名词释义罗列如下：

- **BUSD**：BUSD 是由USDT/USDC跨链1:1铸造而成的美元锚定币。用户可将 USDT 或 USDC 跨链转入，并按 1:1 比例自动兑换为 BUSD；同样也可将持有的 BUSD 按 1:1 比例兑换回 USDT或 USDC 并跨链提取。
- **BFC**：BenFen Coin（BFC）是本分链网络的原生代币，通过权益质押机制保障整个网络的安全。同时，它也可以被用于支付链上交易的 Gas 费用，并为节点提供持续的经济激励。
- **BenFen DEX**：BenPay DEX 是本分链内置原生的自动做市商模式的去中心化交易所（AMM DEX）。

3. 本分公链

本分链基于 Move 语言构建安全、高性能、高可用性的底层区块链，在保证安全性的同时，实现了亚秒级延迟和每秒数万笔交易的高吞吐量，且显著降低了交易的平均成本。

3.1 安全性

Move编程语言最早在 Facebook 的 Diem 区块链项目中亮相。作为一种专注于数字资产的智能合约编程语言，Move 语言具有很多安全性优势：

- **类型安全性：** Move 具有严格的类型系统，可以在编译时捕获许多常见的错误，例如类型不匹配和空指针引用，从而提高代码的安全性。
- **资源生命周期管理：** 通过资源（Resource）概念来管理资产，这些资源具有严格的生命周期管理，确保资源只能按照预期的方式使用和传递，避免了许多安全漏洞，如重入攻击和资源泄漏。
- **权限控制：** 允许开发人员在代码中定义访问资源的权限和约束，从而实现对资源的细粒度控制，防止未经授权的访问和潜在的安全风险。
- **不可变性：** 鼓励使用不可变数据结构和函数式编程范式，从而降低了代码的复杂性，并减少了许多安全漏洞的可能性，如状态篡改和意外副作用。
- **形式化验证：** 提供形式化验证工具，可以对智能合约进行静态分析和验证，帮助开发人员发现并修复潜在的安全问题，提高了代码的可靠性和安全性。

3.2 高性能与共识机制

当前，区块链领域面临两大核心挑战：在保持低延迟的前提下实现高吞吐量，并确保共识协议的长期稳定性。为了克服这些挑战，本分链采用了一项创新性的方法，将基于 DAG 的共识和无共识方法相结合。这一方法不仅成功实现了亚秒级延迟和每秒数万笔交易的高持续吞吐量，还同时保持了对复杂合约的支持、生成检查点以及跨纪元重新配置验证者集的能力。

本分链采用了一种巧妙的方式来处理不同类型的交易对象，以达成上述目标。当具有私钥的用户创建并签署用户交易时，交易将被发送至本分的每个验证者。这些验证者会执行一系列的有效性和安全性检查，然后将已签名的交易返回给客户端。客户端会收集来自大多数验证者的回复，从而形成

交易证书。一旦证书组装完成，用户将其发送回所有验证者。验证者会检查证书的有效性并将收据发送给客户端。对于仅涉及用户拥有对象的交易，可以直接处理交易证书，而不必等待共识引擎的介入（通过快速路径直接处理）。所有证书均采用基于 DAG 的共识协议进行处理，由本分链的验证者执行。共识协议确定证书的总顺序，验证者会检查并执行那些涉及共享对象的证书。客户端能够收集来自大多数验证者的回复，并将它们组装成有效证书，用作交易结算的证明。最后，每个共识提交都会形成一个检查点，确保网络的长期稳定性。具体流程如下图所示：

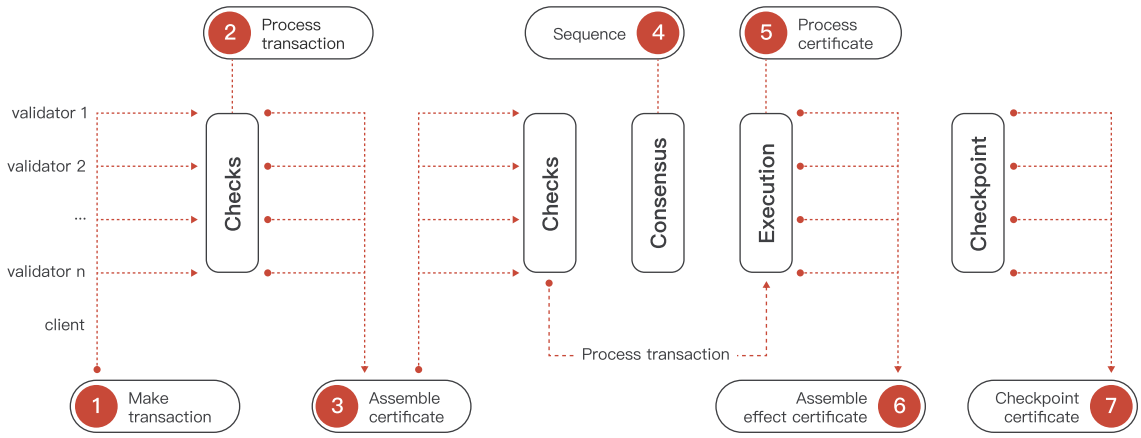

图2: 本分链流程图

经过上述流程的优化处理，本分链能够确保非常低的交易延迟，每笔交易的处理时间维持在0.5秒以下，并且实现每秒处理数万笔交易的高吞吐量。这意味着用户可以期待快速的交易确认和高效的区块链操作。

此外，本分还表现出卓越的健壮性。即使在某些验证节点出现故障或停止运行的情况下，系统仍能够持续稳定运行。这种容错性是确保区块链网络可靠性的关键因素之一，有效地减轻了单点故障对整个系统的影响，从而提高了系统的可用性和稳定性。这使得本分链在各种情况下均能维持高性能和可靠性，为用户提供卓越的区块链体验。

3.3 高可用性

本分链的高可用性体现在用 Move 语言编写的合约具备可验证性，并能实现模块化设计和开发，大大降低了链上开发的难度。

3.3.1 可验证性

为了降低链上计算开销并提高安全性，Move 定义了一套规范语言称为 Move Specification Language。这是一种用于描述程序正确运行方式的规范语言，通过前提条件、后置条件和不变式等规范来定义程序的行为。这种规范语言的设计旨在降低链上计算开销并提高安全性。

一旦程序被用 Move Specification Language（MSL）描述，并且规范被定义好，接下来的步骤是将 Move 程序和规范转换为 Boogie 程序，这是一种具有形式化语义的中间验证语言。通过 Move to Boogie 编译器完成这一转换过程，将程序和规范转化为 Boogie 语言的表示形式。

最后，使用形式验证领域的自动定理证明求解器来验证程序是否符合规范。这些求解器能够分析 Boogie 程序，检查其中是否存在违反规范的情况，从而验证程序的正确性和安全性。通过形式化的方法进行验证，可以更全面地检查程序的行为，并且提供更高的保证水平。

3.3.2 灵活性

依托模块化设计、高级抽象能力、自定义数据结构、灵活的权限控制和跨平台兼容性等特性，本分链具有较高的灵活性，能够满足各种不同的区块链应用开发需求，提供更多的选择和可能性。

- **模块化设计：** 支持模块化设计，允许开发人员将代码模块化为可重用的组件，从而提高了代码的可维护性和可扩展性。
- **高级抽象能力：** 提供丰富的高级抽象能力，如资源（Resource）和事务（Transaction），使得开发人员能够更轻松地表达复杂的逻辑和业务需求。
- **自定义数据结构：** 允许开发人员定义自定义数据结构和类型，从而更好地适应不同的应用场景和需求，提高了灵活性和可定制性。
- **灵活的权限控制：** 支持灵活的权限控制机制，开发人员可以根据需要对资源的访问权限进行细粒度的控制，从而实现更安全和可信的智能合约。
- **跨平台兼容性：** Move 语言设计时考虑了跨平台兼容性，可以在不同的区块链平台上运行，从而为开发人员提供了更广泛的选择和灵活性。

3.3.3 标准库

作为通用且安全的智能合约平台，本分链提供了经过形式验证的智能合约标准库。该标准库包含了40多个常用的功能模块，包括账户、转账、交易、事件、错误处理、数学计算、向量操作等。

3.4 zkLogin

本分创新性的引入 zkLogin 的设计， 为用户提供了一种基于第三方授权的地址生成和交易签名的方式。

能够更好的帮用户实现以下 6 种需求：

- **交易便捷：**zkLogin 可以使用户使用第三方登录 OAuth 的方式生成本分地址，以及在本分链上进行交易。
- **安全自主：**OAuth 提供商仅通过临时公钥生成 JWT，并无法获取用户的临时私钥，即除用户外，无其他人或组织能得到地址公私钥的完整信息。
- **双重验证：**zkLogin 是一种双重验证，即由 OAuth 服务商提供的 JWT，以及用户或其他 salt 服务商提供的 salt；单独盗取用户的 OAuth 账户无法掌控用户的地址。
- **隐私保障：**通过链上数据并不能得知用户的 OAuth 账户身份。
- **灵活选择：**用户可选择多种 OAuth 中的任意一种。
- **原生签名：**zkLogin 为本分原生支持的特性，交易验证发生在公链层而非合约层，最大程度满足高性能低成本交易。

3.4.1 生成地址流程

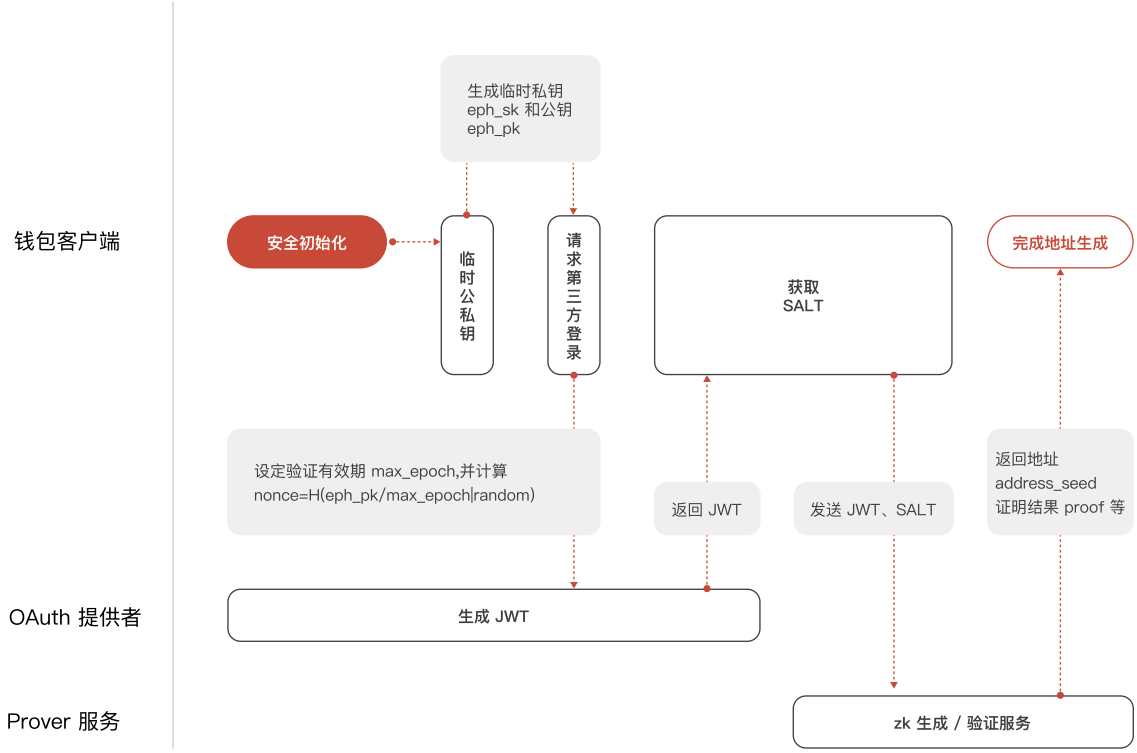

图3: 生成地址流程

3.4.2 验签交易流程

图4: 验签交易流程

3.5 GAS 费用

Gas 费用是用户在链上执行交易或智能合约时支付的费用，主要用于奖励验证节点，并维护区块链网络的安全性和稳定性。本分链通过 Move 编程语言的高效性、基于对象的存储模型、高效的共识机制、以及动态 Gas 定价等多方面的创新，显著降低了链上交易的平均 Gas 费用。

本分链的 Gas 费用定价模型为：

```
Total_gas_fees = computation_units * reference_gas_price + storage_units * storage_price
```

其中包含计算交易产生的计算费用和存储费用，它们分别通过将计算或存储单元乘以相关价格计算得到。具体来说：

- **参考价格（reference_gas_price）：** 每个验证节点在每个 epoch 提交他们愿意处理交易的最低报价。本分链会按照每个验证节点提交的报价自动排序，并选择按质押比例计算的2/3位置处的价格作为参考价格。当用户提交的 Gas 价格高于参考价格时，差异视为支付给网络的小费，支付小费可以使用户获得更高的优先级。
- **计算单元（computation_units）：** 不同的交易需要不同数量的计算时间进行处理和执行。本分链通过将每个交易以计算单位的形式度量，将这些变化的操作负载转换为交易费用。
- **存储价格（storage_price）：** 此价格通过治理提案设定，并不频繁更新。
- **存储单元（storage_units）：** 本分链根据交易中的每个存储单元计算存储费用，每个字节的数据等于 100 个存储单元。

另外本分链的存储机制在事务删除先前存储的对象时提供存储费用返还。因此，用户支付的净 Gas 费用等于Gas 费用减去与数据删除相关的返还：

```
Net_gas_fees = computation_gas_fee + storage_gas_fee-storage_rebate
```

本分链不仅支持使用原生代币 BFC 支付 Gas 费用，还允许用户使用本分原生稳定币 BUSD 进行支付。这样，用户即使仅持有稳定币也能轻松在本分链上进行交易等活动，不过需要注意的是，当用户选择使用稳定币支付 Gas 费用时，将会收取很小比例的交易磨损费用，以确保稳定币能够兑换到足够的 BFC 来支付 Gas 费用。

4. 原生稳定币

基于本分的愿景，本分推出本分链上的原生核心稳定币 BUSD。其中，BUSD 通过与 USDT、USDC 等主流美元稳定币锚定，实现刚性兑付以及价格的稳定；与其他稳定币系统相比，本分稳定币系统的主要创新特性包括：

- **刚性兑付：**本分稳定币通过跨链桥实现与 USDT、USDC 等主流稳定币的 1:1 刚性兑付。
- **稳定币作为“第一公民”：**本分从公链层面赋予稳定币“第一公民”的身份，用户可以直接采用稳定币进行 Gas 支付。

4.1 稳定币生态

4.1.1 本分生态内稳定币循环

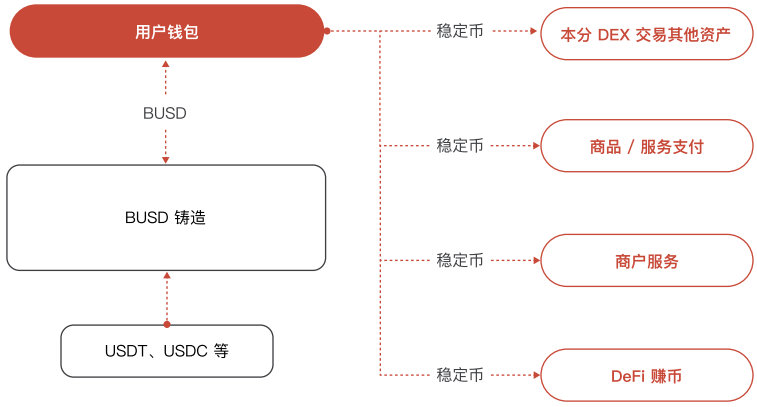

图6: 生态内稳定币循环图

4.1.1.1 稳定币支付 Gas

在当前已知的主流公链体系中，进行交易或者使用其生态系统中的去中心化应用（DApp）通常要求用户先持有该公链的原生代币以支付 Gas。这一要求对于推广和使用 Web3 应用而言，会带来不小的成本和操作复杂性。同时，原生代币价格的波动也可能给用户带来经济压力。

为解决这一问题，本分设计并实施了一项新的机制，允许用户使用本分支持的稳定币来支付 Gas 费用，这样用户即使在没有持有本分平台币（BFC），仅持有稳定币的情况下，也能轻松地发起交易、使用和开发 DApp。

不同于以太坊的 Gas Station Network（GSN）方案，本分的稳定币支付 Gas 方案不需要用户增加代码逻辑或接入 GSN 的 SDK，也不涉及 GSN 方案中可能引发的中心化问题，例如中间服务器（Relay Servers）导致的单点故障。相反，本分采用了内置的稳定币服务，当用户提交一笔交易并选择使用 BUSD 作为 Gas 费用时，系统会自动帮助用户完成 Gas 费用的支付。用户无需关心这一过程，也无需执行额外的操作或重新发起交易。

此外，该方案还具备良好的扩展性。本分允许用户使用任何代币来支付 Gas 费用，只需接入相应的代币兑换平台即可实现。这项创新方案为用户提供了更便捷、更高效、以及更经济友好的数字资产交易环境，同时提升了去中心化应用生态系统的可用性和用户友好性。

4.1.2 PayFi 生态中的稳定币应用

全球支付体系长期以来受到传统支付基础设施僵化与银行系统割裂的制约。这导致跨境资金转移普遍存在成本高昂、延迟严重及流程繁琐等问题，尤其对于新兴市场的用户而言，这些壁垒极大地限制了其参与全球经济活动的机会。

PayFi（Payment Finance，支付金融）正是在此背景下应运而生的一种创新范式。它通过融合区块链技术，将高效的支付功能与复杂的金融服务相结合，从根本上重塑全球价值流转的方式。PayFi 旨在通过以下几个核心优势，系统性地解决传统金融系统中存在的问题。

4.1.2.1 PayFi 核心优势

- **全球可访问性与普惠成本：** PayFi 彻底摆脱了对传统银行系统的依赖。任何人，无论身处何地，仅凭一个数字钱包即可接入全球金融网络。同时，由于区块链的低成本与实时清算能力，其支付成本远远低于传统金融体系，让普惠金融成为现实。
- **无需信任：** 通过智能合约，所有交易和金融协议都能自动执行，无需昂贵且低效的中心化中介。这不仅保证了执行的公正性，而且所有规则和交易记录都在链上公开可查。
- **可编程性：** PayFi 不仅仅是支付通道，更是一个可编程的金融平台。用户可以基于智能合约，为资金流转设定复杂的条件，例如自动化的薪资发放等。这种灵活性为创造全新的金融产品和商业模式提供了无限可能。

- **无缝的生态兼容：** PayFi 与主流数字资产生态（特别是稳定币）无缝集成，为用户和商家提供了稳定、可靠的交易媒介。通过降低技术门槛和解决价格波动的核心痛点，它极大地推动了加密支付在真实商业场景中的普及与应用。

4.1.2.2 本分链稳定币的角色

想要实现这样的愿景，必须依赖一种全新的、更加稳定、高效且值得信赖的稳定币，在整个 PayFi 生态中承担价值流转的核心角色。这个稳定币不仅需要在链上和链下世界中高效地完成发送、接收和结算等流程，还要具备广泛的适用性，支持各种金融需求。

本分链的稳定币 BUSD ，正是为 PayFi 生态量身打造的理想解决方案。它结合了 Move 语言的安全特性，能够在流转环节达到安全性远高于通过合约实现的其他稳定币，可以更稳定并且更高效的适应各类新型的金融需求。另外，本分链的稳定币还能够在极低的成本下完成资金流动。无论是在跨境支付、消费者金融，还是供应链金融等场景中，用户都能体验到前所未有的资金流转速度和低交易费用，实现资金的最大时间价值，这也是 PayFi 生态应用带给用户最大的价值。

4.1.2.3 PayFi 应用场景

当前以及未来，本分稳定币集群将在 PayFi 生态中发挥核心价值，广泛应用于各种链上与链下的金融场景。

- **资产交易：** 稳定币作为价值锚定的交易媒介，可以规避加密资产价格波动带来的风险。用户可以通过 BenPay DEX平台使用稳定币作为核心交易对，安全、高效地完成各类数字资产的流通。
- **DeFi 生态：** 在抵押借贷、流动性挖矿等 DeFi 协议中，用户可通过为 BenPay DEX 等应用提供稳定币流动性，成为生态的建设者并获取持续收益。
- **RWA（Real World Assets）资产：** 现实世界中的资产，例如不动产、应收账款、房屋抵押贷款等，可以借助稳定币作为清算和支付工具，实现链上融资与资产证券化。
- **跨境支付与贸易：** 企业和个人可以通过 BenPay 等应用，借助本分稳定币的低手续费和高稳定性，实现秒级到账的跨境结算，规避传统支付网络中的延迟和中介成本。
- **日常消费支付：** 用户可以将 BUSD 充值进 BenPay Card 卡中，像使用传统银行卡一样在全球使用，满足各种支付场景的需求，打破了数字资产与现实消费的壁垒。

- **薪酬支付：** 特别适用于自由职业者、远程团队、DAO 组织等全球协作模式，链上透明记录以及按小时或实时流支付（stream payment），减少汇率波动影响和高额国际转账费用。

通过这些场景的深入拓展，本分稳定币可以推动区块链支付在更广泛的金融科技应用场景中落地，成为 PayFi 生态实现全球化、规模化的重要支柱，连接链上金融创新与链下真实世界的资金需求，为用户带来真正可用、可信、可持续的金融体验。

5. 一键发行代币

目前，链上发行代币通常需要开发者编写和部署智能合约，涉及复杂的技术流程、安全审核和高昂的 Gas 费用，对于大多数非技术用户而言门槛极高，尤其在涉及稳定币或 RWA 等相对敏感资产时，更需要专业的合约模板与风控机制支持。因此，本分链提出“一键发行代币”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。

5.1 代币发行原理

本分链采用的面向对象（Object-centric）模型，与以太坊等基于账户的模型有着本质区别。在该架构下，代币并非账户中的数字，而是封装了自身数据与所有权的独立**“对象”（Object）**。因此，创建代币的过程，即是通过智能合约（称为 Move 模块），来定义并管理一个具备可转移性的全新对象。这种设计不仅使资产的转移、销毁等操作逻辑更为清晰，还能通过并行处理技术大幅提升执行效率。

为简化并统一资产发行，BenFen 框架内置了名为 coin 的官方核心模块。该模块为所有同质化代币提供了标准的结构与行为（如铸造、销毁、分割与合并），允许任何人调用其标准函数来创建代币，无需重复制定标准，从而确保了整个生态系统中资产的安全性与互操作性。

5.2 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。

5.3 发行代币资产类型

除了项目方发行的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领域--稳定币和现实世界资产代币化（RWA）。

5.3.1 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：

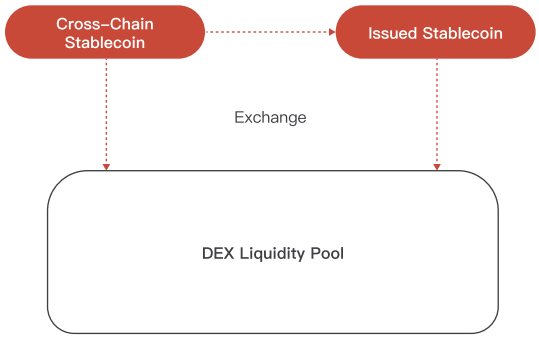

图7：稳定币创建流程图

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：**发行方使用“一键发行”功能创建出自己的稳定币后，必须在本分生态内的官方 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。

一键发行稳定币的功能可以广泛应用于多种场景，以下是一些具有代表性的实用场景：

1. **本地化支付和结算：**企业或平台可发行与特定法币锚定的本地稳定币，用于本地商户支付、员工薪资发放、结算等，避开跨境支付中的汇率损耗和清算延迟。
2. **Web3 项目资金管理：**创业团队可发行特定法币锚定的稳定币进行早期融资、营运支出与员工激励，保证资产稳定、避免价格剧烈波动带来的财务风险。
3. **供应链金融/应收账款代币化：**企业可将应收账款等债权类资产锚定为稳定币发行，实现应收账款代币化，从而提升融资效率和流动性，实现资产的链上拆分、转让与变现。
4. **品牌专属代币或平台币：**企业、DAO、游戏、社交平台等可以快速发行自己的稳定币作为内部结算单元，避免资产波动影响经济系统稳定，提升用户交易意愿与资金留存。

5.3.2 一键发行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，是区块链赋能实体经济、释放万亿级资产流动性的核心方向。作为实现“新一代现实世界支付公链”愿景的关键支柱，本分链基于 Move 语言在安全性（资源模型）与可编程性上的原生优势，构建了标准化的 RWA 代币协议。该协议将法律合规、资产验证与生命周期管理等复杂流程编码为可自动执行的智能合约，旨在提供高效、合规、一键式的发行与管理体验，确立了可扩展、透明、可信的通用标准。

依此标准发行的 RWA 代币，是特定实体资产（如金融票据、大宗商品、不动产收益权）所有权的链上直接映射。其设计内嵌三大核心特征，构成了可信的基石：价值锚定（以持续、可验证的链下审计为支撑）、自动成本计提（通过透明的链上管理费机制实现）与双向兑换（保障自由流通与最终赎回实体资产的权利）。

所有参与方均须通过本分链的 KYC/AML 身份验证，确保发行与交易符合全球合规要求。在此合规前提下，协议通过以下智能合约机制实现资产的数字化发行与管理：

资产验证与审计

发行前，发行方必须完成并提交链下资产的第三方验证证明，该证明的关键摘要（哈希）将上链存证，构成发行的先决条件：

- **存在性证明：**提供资产仓单、托管机构记录或法定权属文件。
- **价值证明：**依据公开市场价格、资产净值或第三方估值报告确定资产公允价值。
- **审计报告：**由合格机构出具，内容须包括审计日期、覆盖范围、资产估值及有效期限。

代币发行

在资产验证通过后，发行方可发起发行。智能合约将强制执行以下规则：

- **硬性上限：**累计发行代币的总价值不得超过最新审计报告确认的资产净值。
- **发行记录：**每一笔发行动作均与特定的审计报告版本关联，并永久记录在链上。

管理费机制

管理费为项目方可选配置机制。启用后，代币在持有期间会自动累积管理费，该费用按时间比例计算。用户钱包显示的余额为扣除应计费用后的“净值”，市场交易价格则反映底层资产价值与管理费计提的综合影响。此机制以透明、自动化的方式，为发行方提供了覆盖持续运营成本的一种可行途径。

赎回与流通

- **赎回：**持有者可发起赎回请求，相应的代币将被销毁，发行方按智能合约约定的规则进行线下资产交割。
- **流通：**代币可自由转账，RWA 作为优质资产将流入本分生态的 DeFi 与 DEX 协议，提升整体资本效率与收益机会，赋能 BUSD 等生态资产。

透明度与可验证性

链上公开记录所有关键信息，任何用户均可独立验证：

- 当前有效的审计报告信息（机构、日期、覆盖价值）。
- 代币流通总量及其对应的资产价值。
- 管理费费率及累计计提情况。
  这确保了**“发行量 ≤ 审计资产价值”**的等式始终成立，且所有操作历史可追溯。

本分为多类现实资产上链提供了通用解决方案，典型应用场景包括：

1. **房地产代币化：**房产拥有者或开发商可通过“一键发行”功能，将一套房产或商业地产映射为链上的 RWA 代币。用户可进一步细分所有权（如 1 套房拆为 10 万个份额），进行融资、分红、交易或作为抵押使用。
2. **商品资产上链：**黄金、白银、石油等大宗商品可以在链上以代币形式代表仓单、保单或存储凭证，实现跨境价值转移与链上结算。比如贵金属经销商可一键发行锚定黄金的 RWA Token，实现快速交割和对冲。
3. **艺术品与收藏品投资：**通过一键发行，将高价值艺术品或收藏品的所有权切割为多个代币，普通用户也能参与投资，降低门槛并提升流动性。

4. **音乐/影视/IP 收益权：**创作者可以将音乐、影视、IP 等未来收益权一键发行为 RWA 资产，出售部分收益权换取早期现金流。比如一个音乐人发行“未来5年收入权”的代币，粉丝和投资者可参与分润。

5. **应收账款与发票资产：**企业可将应收账款、发票凭证通过 RWA 功能一键代币化，实现链上融资、转让、流通。

5.4 使用项目方代币支付 Gas

在传统区块链中，用户发起任何交易都必须使用原生代币（如 ETH 或 BNB）来支付 Gas 费。这为用户制造了显著的进入障碍——在与应用交互之前，他们必须首先通过特定渠道获取原生代币。为了优化用户体验，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。这不仅让用户的链上交互过程更无缝，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。

为了防止整个网络受到流动性差、价格易被操纵的代币的攻击，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，申请将其代币加入 Gas 费支付列表白名单。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。如果提案获得足够赞成票通过，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。

5.5 使用赞助交易进行 Gas 代付

在支持用户使用项目方代币支付 Gas 费用的基础上，本分进一步提供了赞助交易功能。赞助交易允许项目方直接帮助用户支付交易所需的 Gas 费用。这可以极大地降低新用户的使用门槛，帮助项目方更高效地吸引和留存用户。同时，项目方也可以选择性地对特定类型的链上交易进行赞助，以实现精准的用户激励和生态引导。

本分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。因此，它也极大地降低了开发成本，并显著提升了交易的安全性、速度和透明度。

赞助交易的具体流程如下：

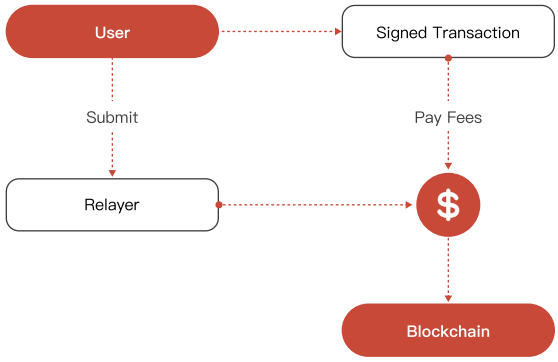

图8：赞助交易流程图

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。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。

6. 隐私账户和隐私支付

链上数据的透明性是一把双刃剑。对于金融应用而言，交易金额、账户余额等信息的完全公开，不仅会泄露个人隐私、暴露商业机密，更会阻碍大规模、合规的金融业务在链上落地。

为解决这一痛点，本分链在 Move 虚拟机层面提供了原生支持，实现了“数据可用不可见”的隐私账户与隐私支付体系。 用户的资产在存入隐私账户后，其真实余额在区块链上被完全屏蔽；在隐私支付过程中，外部观察者仅能捕捉到加密的交互记录，而无法得知具体的交易金额。这套机制确保了资金流转的机密性，从底层重构了金融流转的隐私范式，为各类复杂金融场景提供了必需的安全底座与合规基础。

6.1 核心技术

基于 FAST MPC 和监管介入的保密交易系统架构，本分链隐私支付系统创新性地融合了区块链技术 （Block Node）、快速多方计算 （FAST MPC） 以及监管合规机制 （Regulator），以实现在分布式网络中资产转移的“数据可用不可见”，同时提供极佳的交易处理速度和较低的计算成本。

关键技术组件

1. 区块节点 （Block Node）

区块节点作为分布式账本系统的核心，负责交易的验证、共识和存储等功能。所有交易（无论是 Plain Tx 还是 Confidential TX）都需要经过这些节点处理。

2. 快速多方计算 （FAST MPC）

FAST MPC这是系统实现隐私保护的核心技术。MPC 允许参与方在不泄露各自输入数据的前提下，共同计算一个预定的函数。“FAST”强调了该 MPC 方案针对性能和效率进行了优化，以满足区块链高吞吐量的要求。 MPC 模块在 Block Node 内部运行，主要职责是处理 Key_shard（密钥分片）和 User Private Meta Data，用于生成或验证保密交易。

3. 密钥分片 （Key_shard）

这是实现数据安全和监管介入的关键元素，由FAST MPC模块产生。用户的私有元数据被加密或分割成多个密钥分片，分别由不同的实体（如 Block Node 和 Regulator）持有。并且只有将来自不同来源的 Key_shard 汇集（如 Block Node 的分片和 Regulator 的分片），才能访问或解密核心的 User Private Meta Data。

在此基础上，本分链在下一阶段将引入更加去中心化的 SMPC（Secure Multi-Party Computation）方案，将信任从有限的验证节点分散到更广阔的节点网络中，大幅提升系统的去中心化程度和抗单点故障/审查的能力。最终，本分链将引入全同态加密（FHE）方案，允许在加密数据上进行任意计算而无需解密，从而让隐私计算演进至真正的零信任模型，彻底摆脱对可信中间方的依赖。

6.2 隐私交易的具体流程

一个典型的隐私资产从诞生到使用的完整生命周期，主要包括以下三个核心阶段：

6.2.1 隐私资产的创建：从充值开始的一步式隐私化

本分链在架构上进行了改良，将隐私选择前置。用户在充值时即可决定是否将代币充值为隐私形式，无需多步操作，体验更流畅。

1. **发起隐私充值或隐私代币转换：**用户在钱包中选择充值代币时，即可勾选“充值为隐私代币”选项。此外，用户也可通过钱包发起一笔“资产加密”交易，指定希望转换为隐私形式的代币和数量。
2. **资产锁定：**交易经网络确认后，一个特殊的智能合约会自动将用户转换的代币进行锁定，作为即将创建的隐私资产的价值支撑。
3. **价值分片：**网络验证节点接收到该数值后，动用其内部的共享密钥和加密算法，将这个数值转换成一组独特的、无规律的数据分片。
4. **凭证生成：**系统为用户创建一个新的“隐私资产”对象，并将这组新生成的数据分片存入其中。
5. **完成：**交易上链后，用户的公开代币被锁定，同时获得了一个等值的、以加密分片形式存在的隐私资产，这笔资产的真实价值在链上不再可见。

这种“充值即隐私化”的机制，消除了用户获取隐私资产的门槛，使隐私保护成为上链操作的默认选项，而非复杂的附加流程。

6.2.2 隐私支付

当用户 A 希望向用户 B 支付一笔隐私资产时，流程如下：

1. **构建交易：** A 的钱包创建一个交易，指明收款方为 B 并设定具体的支付金额。之后它会向一个可信的验证节点发起授权请求，请求将支付金额处理成临时的加密分片。

2. **提交网络：**钱包将执行交易所必须的信息打包成一笔交易并提交至网络。交易内容中会包含 A 的当前余额分片、B 的当前余额分片，以及上一步获取的、代表交易金额的加密分片。
3. **后台运算：**网络验证节点接收到这笔交易后，会利用共享密钥，对这三组分片进行解密和运算，之后将结果再重新加密成新的加密分片。
4. **状态更新：**计算会产生两组全新的数据分片——一组代表 A 减少后的新余额，另一组代表 B 增加后的新余额。随后，系统将这两组新分片分别更新到 A 和 B 的隐私资产对象中。
5. **完成：**交易上链后，价值的转移便已完成。对于任何其他链上用户而言，他们只能看到 A 和 B 的隐私资产对象里的数据发生了变化，但具体的交易金额无从得知。

6.2.3 查看或取回资产

当用户希望查看自己的真实余额，或将隐私资产换回公开代币时，流程如下：

1. **发起请求并签名：** 用户通过钱包向一个可信的网络节点发起请求。这个请求中附带了由用户钱包私钥生成的数字签名，用以证明其所有者身份。
2. **身份验证：** 节点收到请求后，会验证签名的合法性，确认请求者为该隐私资产在链上记录的合法所有者。身份验证主要用来防止其他用户的未授权访问。
3. **链下还原：** 验证通过后，该可信节点会从链上读取用户的加密分片，并在其本地内存中，使用共享密钥将这些分片还原为用户可读的真实余额数值。
4. **安全返回或赎回：**
   - **查看：** 该真实余额会通过一个安全的加密通道，被发送回用户的钱包前端进行显示。
   - **赎回：** 用户可以授权一笔交易，在链上销毁其持有的隐私资产凭证。一旦网络确认销毁，最初被锁定的等量公开代币便会自动释放，返还给用户。

6.3 核心特点与差异化优势

6.3.1 双层合规设计

- KYC **身份基础：**与合规服务商合作，为企业用户提供链下认证并生成凭证。这不仅是所有高级金融活动的信任锚点，也为 AML/CFT 提供了制度基础。
- **协议层可审计隐私：**基于**门限解密机制，**系统预设了监管介入接口。仅在获得合法司法命令且多方协作时，才能恢复特定交易历史。这实现了“默认隐私，选择性披露”，让企业在审计中无需披露每笔交易细节即可向税务机关验证合规性。

6.3.2 极致用户体验与零 Gas 费模型

本分链致力于降低隐私功能的使用门槛：

- **操作无感化：**隐私转账步骤与普通转账完全一致，隐私保护在后台自动运行。
- **原生赞助交易：**协议层支持角色分离，项目方或商户可直接为用户代付 Gas，实现用户的零 Gas 费体验。
- **原生稳定币架构：**稳定币作为链层“一等公民”，不依赖脆弱的智能合约逻辑，为隐私支付提供了更坚实的安全基石。

6.3.3 高性能与生态可扩展性

- **秒级确认：**优化后的密码学套件支持 1,000+ TPS 的隐私交易处理能力，满足高频商业需求。
- **全维度隐匿：**保护范围涵盖交易金额、发送/接收方地址及资产类型，从根本上切断链上数据分析的可能性。
- **批量化操作：**原生支持企业级批量发薪、空投等场景，将效率与私密性完美结合。

7. BenPay DEX

BenPay DEX 不同于其他公链上第三方的 DEX，而是本分链构建在系统底层的原生去中心化交易所。BenPay DEX 不仅是本分链的核心交易平台，也是本分稳定币发行和流通的重要前提。

7.1 BenPay DEX 特点

BenPay DEX 有着常规 DEX 所具备的资金池（Liquidity Pool）和自动做市（Automated Market Making，简称AMM）的模型设计。对于每笔交易，BenPay DEX 会对交易的用户收取 0.1% 的手续费（以 BUSD 的形式），其中50%用于激励流动性提供者，剩余的50%用于增加协议储备。

除此之外 BenPay DEX 还拥有以下几个关键优势：

1. **交易便利性：**稳定币提供了一个相对稳定的价值存储，使得用户可以在不担心剧烈价格波动的情况下进行交易。
2. **集中流动性提供：**BenPay DEX 引入了集中流动性（Concentrated Liquidity）的概念，允许流动性提供者（LPs）在价格范围内而不是整个价格区间内提供流动性。
3. **促进生态系统发展：**一个健全的 DEX 可以吸引更多的用户和开发者加入本分公链的生态系统。稳定币作为交易的基础，可以促进更多的去中心化应用（DApps）和服务的开发，从而推动整个生态系统的增长和繁荣。

7.2 BenPay DEX 的内置 Oracle 系统

BenPay DEX 的内置 Oracle 系统（区别于上文提到的汇率预言机），在本分平台中担当着至关重要的角色，其任务是提供准确且实时的资产价格信息，以确保交易市场的公平性和透明性。BenPay DEX 的内置 Oracle 系统充分利用了 CLAMM 框架和 Move 编程语言的优势，为用户提供了高效且安全的交易服务。通过加强价格信息的真实性、准确性和稳定性，构建了一个可信赖的数字资产交易生态系统，有助于确保市场的健康运作，提高用户对平台的信心和参与度。以下是 Oracle 系统的主要特点：

- **TWAP（时间加权平均价格）机制：**BenPay DEX 的 Oracle 系统采用 TWAP 计算方法，不仅仅依赖瞬时价格。TWAP 通过对一段时间内的价格进行加权平均，有效地平滑价格波动，减少了短期操纵和异常波动对价格的影响，以保障价格的稳定性和可信度。
- **价格滑动窗口：**Oracle 系统采用价格滑动窗口技术，持续更新价格数据。这确保了最新且最相关的价格信息始终可用，同时有效地防止了价格延迟或混淆。
- **防操纵机制：**
  - **冷却时段：**每次 Oracle 系统进行价格更新后，都会设定一个冷却时段，在此期间不允许再次更新。这有效地限制了频繁价格变动可能带来的操纵市场风险。
  - **价格偏离阈值：**如果新价格与当前价格相差过大，超出了预设的阈值，该价格数据将不予接受，以确保价格的稳定性和合理性。
- **透明性承诺：**BenPay DEX 坚决承诺，所有价格更新和 Oracle 系统的活动都是公开和透明的。这意味着任何人都可以验证价格数据的准确性和真实性，以确保平台的透明度。

8. BenFen Bridge

BenFen Bridge 是连接本分链与多条主流公链的跨链桥。它不仅支持不同链上原生资产的互通，还支持将来自多条公链的 USDT、USDC 等主流稳定币，跨链铸造为本分链的核心稳定币 BUSD。

为兼顾安全性、效率与广泛的兼容性，BenFen Bridge 既包括基于智能合约的 BenFen 原生跨链桥，也包括通过节点网络实现的比特币 、Solana 等异构链的跨链。其中，基于智能合约的原生跨链桥保障了资产在 EVM 兼容链之间的去中心化转移；而对于比特币、Solana 等非 EVM 兼容的异构链，则通过高效的节点网络实现跨链，确保了更快的处理速度。

目前，BenFen Bridge 已支持包括比特币、以太坊 、Solana、TRON、BNB Chain、Optimism、Base 在内的多条公链以及 L2 资产的双向跨链。我们正积极开发针对 Solana 和 TRON 的去中心化跨链方案，并计划在未来持续扩展，接入更多主流公链，构建一个无缝、互联的区块链生态系统。

8.1 原生 BenFen Bridge

本分链上的原生跨链桥 BenFen Bridge 是一种安全、去中心化且具备可扩展性的跨链聚合解决方案。它采用当前最广泛使用的“锁定与铸造”机制：当以太坊等公链的原生资产跨链时，BenFen Bridge 会将这些资产锁定在以太坊上的智能合约中，并根据资产流入或流出的方向，在本分链上相应地铸造或销毁对应资产。

作为本分链的原生模块，BenFen Bridge 无需引入额外的信任机制——为本分链提供安全性的验证节点，也同时为 BenFen Bridge 的跨链安全提供保障。此外，BenFen Bridge 的运行逻辑将内置于本分链的核心代码中，实现原生集成与一致性安全。

8.1.1 BenFen Bridge 关键组成

- **BenFen Bridge 委员会：**为了继承本分链的安全性，BenFen Bridge 委员会或者 Bridge Node 网络与本分链的活跃验证者一致。节点负责观察、验证、签署跨链事件。除此之外节点还会签署 Solidity 和 Move 合约升级批准和紧急治理请求。
- **BenFen Bridge 智能合约：**包括 EVM 链上的 Solidity 合约和本分链上的 Move 合约，负责处理资产的锁定、铸造和销毁等操作。

- **全节点：**在 EVM 链和本分链上运行的全节点负责监听跨链事件或提供验证信息来保证跨链事件的合法性，为 BenFen Bridge 节点和客户端提供支持。
- **跨链客户端：**客户端是用户与 BenFen Bridge 进行交互的接口，客户端会提交格式正确的交易信息并收集 BenFen Bridge 节点的签名（签名节点的质押资金需要超过 1/3）来帮助用户完成跨链操作。

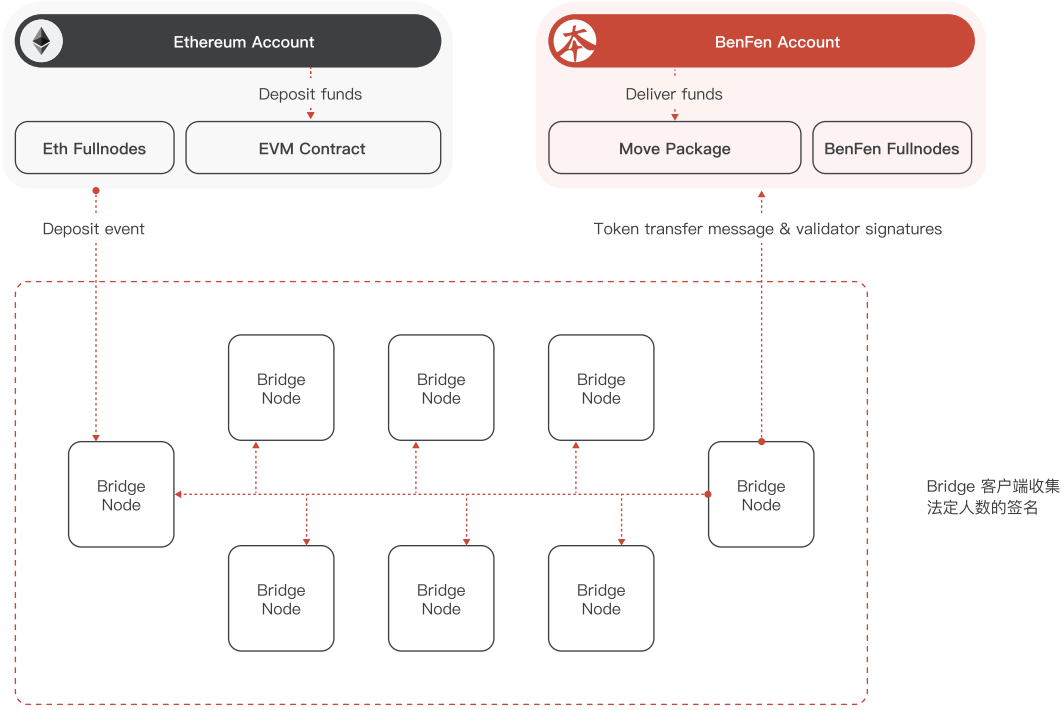

图9: BenFen Bridge 结构图

8.1.2 链跨流程

以用户通过 BenFen Bridge 实现从 EVM 链跨链至本分链的过程为例，整个流程可划分为以下几个步骤：

1. **发起跨链请求并锁定资产：**用户通过 EVM 链上部署的 BenFen Bridge 合约发起跨链操作，明确指定跨链币种、数量、目标链（BenFen）以及接收地址。Solidity 合约收到请求后，将对应的用户资产锁定，并将交易信息记录上链，触发跨入事件。
2. **事件监听与验证：**BenFen Bridge 节点网络实时监听来自 EVM 链上的跨链事件。一旦捕获到用户的跨链请求，Bridge 节点将对事件的有效性和签名进行验证，并准备在本分链上构造对应交易。

3. **构造目标链交易：**验证完成后，Bridge 节点在本分链上构造一笔跨链资产铸造或转账交易。该交易将按照用户请求，将等值资产发送至用户指定的本分链地址，并保留跨链原始信息以便追溯。

4. **多签确认与广播执行：**构造完成的交易将由多个 Bridge 节点共同签名，当节点签名数量达到预设阈值（默认75%）时，交易将被正式提交至本分链并执行，完成跨链资产的最终释放，用户即可在目标链上收到对应的资产。

用户从本分链将资产跨链到其他 EVM 链的过程相反，需要在本分链发起跨链操作，合约会销毁资产并生成交易凭证。Bridge 节点网络监听到销毁事件后会验证并共同签署一份“领取证明”。用户可以在目标 EVM 链使用证明发起**“领取”（Claim）**操作，合约验证证明有效性后，会解锁最初被锁定的资产并发送给用户。

8.1.3 风险防范措施

为了进一步确保跨链桥的安全性，BenFen Bridge 还采取了多项措施以降低风险：

- **重放保护：**为了避免重放攻击，每个跨链交易都会包含一个随机数（nonce），如果随机数之前已经被使用过，跨链交易将会失败。

- **跨链最终性确认：**为了减少 EVM 链可能的重组风险带来的影响，EVM 链的交易在其区块最终确定（≥2 个 epoch）之前不会被视为有效，这意味着 EVM 链到本分链的跨链交易需要大约 13 分钟来结算。但是本分链到 EVM 链的交易不受此影响，可以在几秒钟内完成。

- **委员会管理：**每个活跃的验证者都是跨链委员会的一员，委员会会在本分链的每个 epoch 变化后刷新，验证者也会轮换其签署认证或批准的密钥，这将在下一个 epoch 生效。委员会的信息也会存储在EVM 链合约中，每个本分链周期开始时，EVM 链合约中的信息也会同步更新。更新需要超过 1/3 的投票权。

- **合约升级：**本分链上的合约需要至少 2/3 的验证者批准才能进行升级，EVM 链上的合约需要至少 1/2 的验证者批准才能进行升级。

- **紧急暂停：**面对意外的灾难性事件或者故障时，可以使用紧急暂停，所有的操作都将停止，直到被解除。启动紧急暂停的门槛会设置的相对较低，确保紧急事件出现时能快速制止损失。要解除紧急暂停，同意的质押资金需要超过 1/2。

- **限额保护：**BenFen Bridge支持多种灵活的限额措施，包括单笔、不同方向、累计24小时、以及根据金额阶梯限制等，达到用户使用便捷和 Bridge 金库安全的平衡。

8.2 基于节点网络的跨链

对于支持图灵完备智能合约的 EVM 兼容链，BenFen Bridge 可通过原生 BenFen Bridge 实现完整的跨链流程，全程自动化、无需信任中介，具备高度的可组合性与安全性。然而，对于比特币等不具备图灵完备性的异构链，无法依赖智能合约完成链上逻辑验证和状态转换。为实现与此类链的资产跨链，BenFen Bridge 引入了第二种机制 —— 基于节点网络的跨链方案。该方案通过多节点监听、签名和审核相结合的方式，在确保安全性的同时，实现了对非合约链资产的安全跨链。

在这种跨链方式中，BenFen Bridge Node 扮演跨链中继器（Relayer）的角色，负责监听、签名与转发比特币与本分链之间的跨链交易事件。用户可通过该桥实现比特币与本分链映射资产的双向流转。

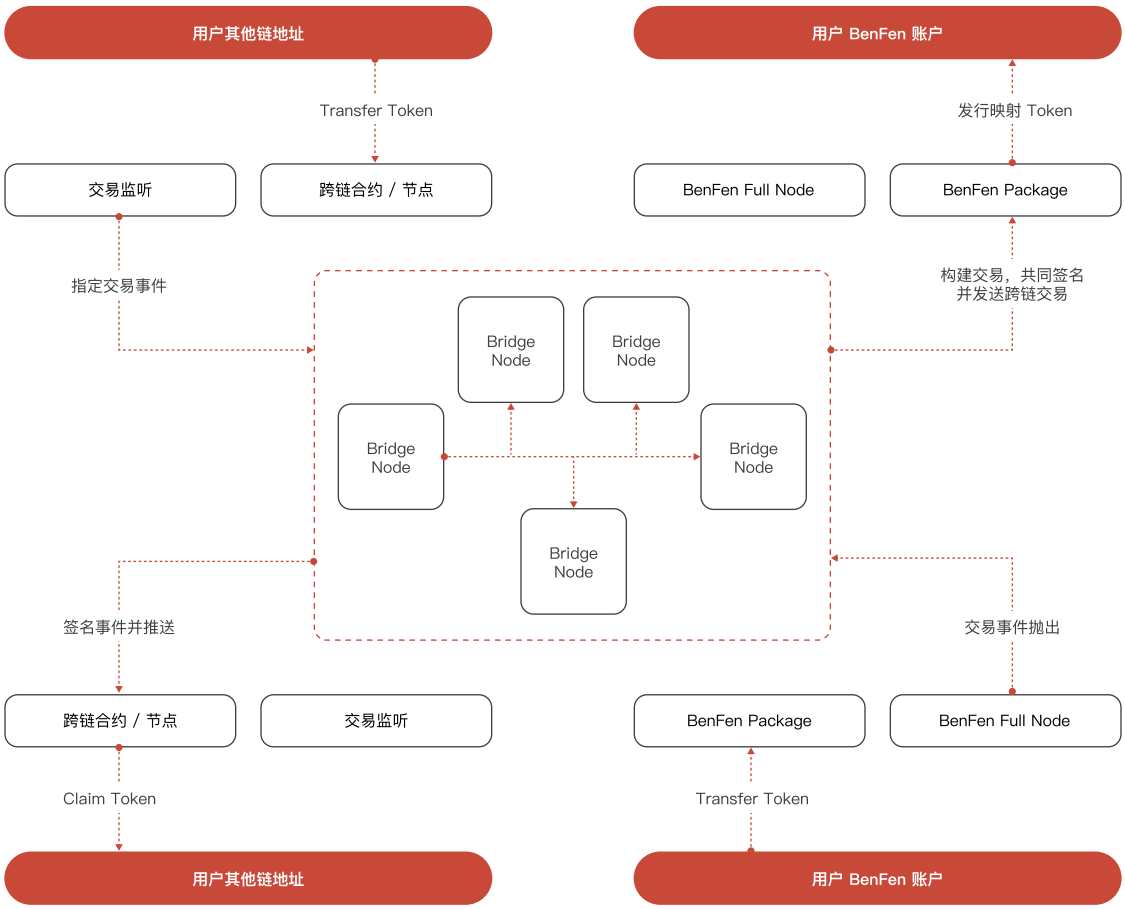

图10: 节点网络跨链流程图

8.2.1 跨链流程

当用户希望将原生 BTC 跨链至本分链并获取映射资产 bBTC 时，流程如下：

1. **发起转账：**用户在比特币网络向跨链服务提供的指定 BTC 地址发送一定数量的 BTC，并在交易中附带目标链（BenFen）、目标地址以及转账金额。
2. **事件监听与确认：**交易达到所需确认数后，链上产生交易信息，Bridge Node 网络检测到相关交易事件，并提取交易内容，准备在本分链上触发映射资产铸造。
3. **构建并签名跨链交易：**Bridge Node 构造在本分链上铸造 bBTC 的交易，并在多节点签名达到阈值后，发送至本分链进行上链确认。
4. **资产到账：**交易执行完成后，用户本分链地址上会收到铸造的等量映射资产 bBTC，跨链过程至此完成。

当用户希望将手中持有的 bBTC 赎回为原生 BTC 时，跨出流程如下：

1. **发起销毁请求：**用户在本分链调用销毁函数，销毁指定数量的 bBTC，并填写跨出目标链（Bitcoin）及接收地址。
2. **生成跨链证明：**本分链上的销毁交易被 Bridge Node 网络监听并提取，节点共同生成销毁证明文件，并进行多签验证。
3. **服务验证与审核：**跨链服务接收到签名完整的证明文件后，进行有效性验证。为进一步提高安全性，该过程还包括一次人工审核环节。
4. **BTC 释放：**审核通过后，系统从 BTC 储备地址向用户指定的比特币地址发送等量 BTC，完成跨链。

9. 本分生态

本分致力于构建全球领先的稳定币金融基础设施，其核心目标是通过原生稳定币系统、链上身份认证、以及高性能基础设施，为支付、交易、借贷等金融活动提供无摩擦、低门槛的支持。围绕 BenFen 公链，生态内逐步发展出包括 BenPay、BenPay DeFi 赚币、BenPay Card、BenPay Lending、BenPay DEX、BenPay 商户服务、BenPay Shop 等多个子模块，形成统一入口、模块化拓展的金融应用矩阵。

9.1 BenPay：Web3 稳定币金融超级应用

BenPay 是本分（BenFen）生态的核心金融应用平台，集成链上支付、非托管借贷、交易撮合等多项功能，定位为“**BenFen 链上超级应用**”。

BenPay 作为本分生态的主要用户入口，基于 BenFen 公链构建，充分利用其亚秒级出块性能、低 Gas 成本和原生稳定币支持，为用户提供**一体化、多功能、安全合规**的金融体验。其目标是消除用户在使用稳定币资产进行消费、借贷等操作时的链间割裂与操作壁垒，构建一个更高效、开放的全球支付与金融服务网络。

BenPay 平台目前包括以下子模块：

9.1.1 BenPay DeFi 赚币：

BenPay DeFi 赚币是本分生态中为用户提供的直通多链头部DeFi协议的统一入口。它的核心是解决用户在探索和参与去中心化金融时面临的操作复杂、壁垒过高等痛点。

作为连接用户与去中心化金融世界的关键入口，BenPay DeFi 赚币在设计上重点优化了交互流程与资产管理机制，其主要优势包括：

- **完全掌控资产：** 用户的资产始终存储在个人钱包中，平台不托管、不触碰资金，全程由用户自主管理。
- **严选头部协议接入：** 所有可部署的协议均经过安全性、稳定性等多维筛选，保留行业头部的优质协议。
- **灵活赎回机制：** 支持随时赎回资产，资金流动性强，避免传统锁仓带来的使用限制。
- **零 Gas 负担：** 任何链上操作通常都需要支付Gas费，但在 BenFen 公链上，平台将为您代付投入与赎回的 Gas 费用，用户无需额外支出。
- **安全审计保障：** BenFen 公链核心智能合约已通过权威安全机构 慢雾科技（SlowMist） 的全面审计，确保系统安全与合约稳定。

9.1.2 BenPay Card：链上稳定币支付卡

BenPay Card 是本分生态中用于实现链上稳定币原生支付的重要工具，旨在推动加密资产在现实世界中的无缝流通与普及。卡片服务完全构建于本分（BenFen）公链之上，依托链上身份、原生稳定币与钱包授权机制，用户可使用 USDT、USDC 等主流稳定币跨入至BenFen链稳定币（BUSD）消费，覆盖线上与线下的主流支付场景。BenPay DeFi 赚币是本分生态中为用户提供的直通多链头部DeFi协议的统一入口。它的核心是解决用户在探索和参与去中心化金融时面临的操作复杂、壁垒过高等痛点。

BenPay Card 采用自托管模式，卡片访问权限由用户通过链上钱包签名授权完成，确保资产控制权始终归属于用户自身。卡片开通无需质押代币或预存资产，申请流程合规、简洁，具备较强的普适性与可拓展性。

在支付体验方面，BenPay Card 实现链下法币支付与链上稳定币资产的自动结算映射，用户资金可在充值后即刻用于消费，无需额外兑换操作，减少支付路径中的摩擦。系统支持多链稳定币资产的充值与提取，当前已覆盖 Ethereum、Solana、Tron、BSC、Polygon、Arbitrum、Optimism、Base、Avalanche 等主流网络，进一步提升资产流动性与用户可达性。

为加强用户资产安全性，BenPay Card 集成卡片冻结控制、链上授权验证与加密数据传输机制，支持在无需暴露敏感信息的前提下完成交易身份验证与权限控制，确保操作安全。

BenPay Card 作为 BenPay 支付生态的重要一环，提供了连接链上资产与现实消费的原生支付桥梁。它的推出不仅提升了稳定币的使用效率与场景广度，也进一步推动本分生态在支付金融（PayFi）领域的落地与普及。

9.1.3 BenPay Lending：去中心化借贷协议

BenPay Lending 是 BenPay 平台下的去中心化借贷协议，采用“撮合周期”设计，每轮借贷周期匹配借款人和出资人，形成稳定利率。用户可通过抵押主流加密资产（如 BTC、ETH）借出稳定币（如 USDT），平台合约全程无托管，链上清算与风控机制完善。

特性亮点：

- **周期撮合，利率可预测；**
- **多抵押品支持；**
- **链上透明风控机制；**
- **还款路径灵活，适配不同用户资产配置偏好。**

9.1.4 BenPay 商户服务

BenPay 提供面向商户的稳定币支付解决方案，支持多链 USDT、USDC 及 ETH 等主流资产的收款接入。商户可通过 API 快速生成收款地址，接收用户链上转账，并通过 webhook 回调实时获取支付状态。可支持 Ethereum、Tron、BSC、Polygon、Arbitrum、Optimism 等主流网络，适用于数字商品、电商平台与 Web3 服务等场景。系统具备高可靠性监听能力，帮助商户实现链上支付自动化和流程可控化。

9.1.5 BenPay 链上红包

BenPay 还创新性推出了链上红包功能，允许用户通过链接或二维码方式发送稳定币的数字红包，适用于社群分发、用户激励和社交互动。

9.2 技术基础与生态支撑

BenPay 所有服务模块均构建于 BenFen 公链之上，并由以下核心能力支撑：

- **高性能 Layer-1 架构：**采用 Move 语言构建，提供高吞吐量和低延迟性能；
- **稳定币系统：**BUSD 由锁定主流稳定币资产铸造，1:1 刚性兑付，稳定性强；
- **zkLogin 非托管钱包：**支持通过 Google / Apple 账户创建链上身份，降低新用户门槛；
- **原生跨链桥：**BenFen Bridge 支持与 BTC、ETH、BSC、Polygon、Optimism、Solana 等主流链的互操作性；
- **稳定币 Gas 机制：**平台原生支持用稳定币支付 Gas 费，简化用户体验。

9.3 合规与安全性保障

BenPay 由注册于美国的金融科技实体运营，持有美国财政部金融犯罪执法网络（FinCEN）颁发的 MSB（Money Services Business）牌照（注册号：31000260888727），具备合规从事虚拟资产交易和预付账户服务的资格。同时，链上核心智能合约已通过第三方安全机构 SlowMist 的审计认证，保障用户资产和协议安全。

9.4 总结

BenPay 不仅是本分生态中的关键金融应用，更是推动稳定币支付与 DeFi 普及的“超级入口”。其多功能集成的架构设计、自托管用户控制模式、对稳定币的深度优化及对传统支付场景的良好兼容性，使其具备成为下一代全球化支付平台的潜力。

未来，BenPay 将持续拓展其服务边界，涵盖更多资产类型与支付场景，加速稳定币在全球主流金融体系中的落地应用。

10. 治理

10.1 BenFen DAO 和链上治理

本分已经成功实现了一个开放、透明、包容和公平的在线治理 DAO 系统，旨在协助用户维护其权益。通过我们的 DAO 系统，任何用户都可以低成本地发起链上提案，积极参与任何链上事务的投票，参与社区治理，以保护和捍卫自己的权益。

去中心化治理在区块链领域扮演着至关重要的角色，我们设计的链上治理机制包括管理群组提案、用户投票、决策制定和执行等多个关键流程，这些流程以智能合约的形式嵌入到系统模块中，以确保治理的完整性和透明度。此外，合约开发者也能够通过重用模块中的治理机制，更好地满足其合约开发需求。

本分的 DAO 系统为用户提供了一个强大的工具，使他们能够积极参与决策过程，确保其权益得到充分保护。这一创新性的设计有望进一步推动社区参与，促进区块链生态系统的成熟和发展。它为用户提供了更多的话语权，有助于共同构建更加可信赖和健全的区块链生态系统。

10.2 工作原理和提案状态

1. **[pending]**：任何用户可以通过质押 token 后，发出提案， 提案进入公示期 [pending]， 用户可以在公示期间对提案进行审核和讨论；
2. **[active]**：公示期结束之后， 提案进入投票期 [active]，在投票期间， 任何用户可以通过将自己持有的代币锁定到投票池中之后，再去对提案进行投票支持或者反对；
3. **[defeat]**：投票期结束之后， 如果反对的票大于支持的票，或者支持的票少于系统设定的阈值1000万票，提案就失败；
4. **[agree]**：投票结束之后， 如果提案没有失败， 就需要等待管理员群组设置提案执行时间，如果此时提案还没有设置执行时间， 提案处于通过待设置执行时间状态；
5. **[queued]**：如果提案通过并且设置了待执行时间， 提案处于待执行状态；
6. **[executable]**：如果提案已经满足了执行时间的间隔要求，此时链上模块会捕获拦截对应的提案信息，并根据数据和逻辑状态自动执行提案效果；
7. **[executed]**：如果提案已经执行完成， 提案会变成已经执行完的状态。

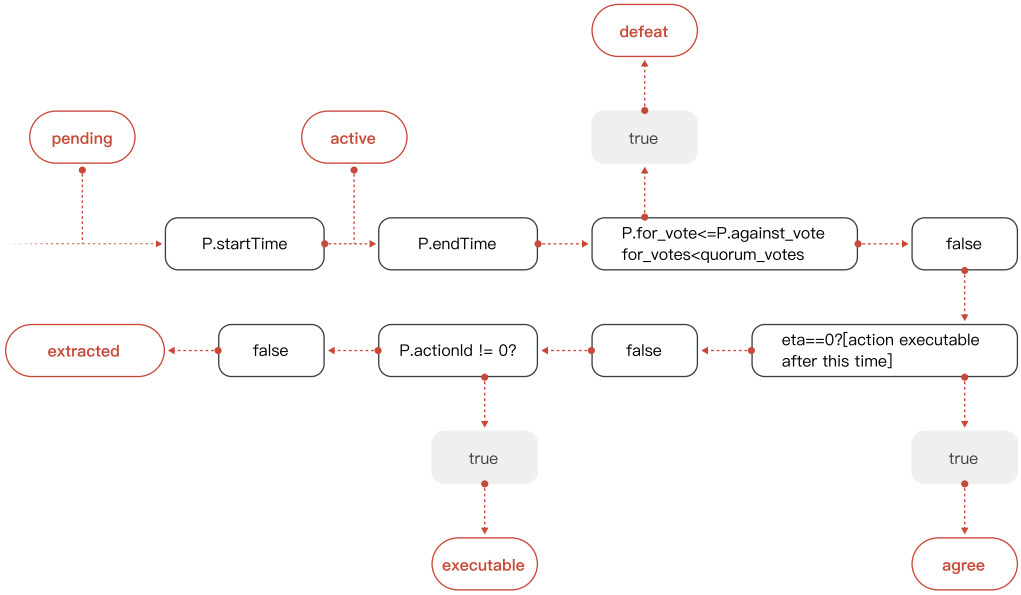

图11: 工作原理和提案状态示意图

10.3 DAO 系统设计说明

我们基于 Move 语言设计了一个强大的 DAO 系统，这个系统充分利用了形式化验证、前提条件、后置条件和不变式等语言规范，从根本上提高了库的安全性和可靠性。

为了降低用户参与门槛，我们采取了极具包容性的措施，任何用户只需将代币质押到投票池中即可参与投票，其投票权将与质押的代币数量成正比。在安全性方面，更高级别的操作需要管理员群组权限，而管理员群组则需要满足一定的条件才能进行扩展。

我们特别注重系统的灵活性，通过可配置的 DAO 参数和阈值，以适应各种不同的需求和情境。此外，将 DAO 的模块部署到 DApp 层面，使普通用户能够充分利用 DAO 系统，从而提高了系统的民主性和参与度。

这一全面的设计为用户提供了更广泛的参与和决策权，有助于实现更加开放、民主和包容的治理体系。同时，形式化验证和安全性措施保证了系统的可靠性和用户资产的安全，为社区提供了稳定和可信赖的治理环境。

11. 未来发展路线

11.1 分层网络

当前，解决区块链可扩展性问题主要采用两种思路，一层扩展（Layer1）和二层扩展（Layer2）。一层扩展受到不可能三角的限制，难以在安全性和可扩展性之间找到平衡。尽管本分在一层已经取得了显著的性能提升，例如交易确认速度，但在某些情境下，需要更快的确认时间和更好的可扩展性。因此，本分的设计中，一层主要负责安全性，而二层则负责扩展性，它们有机结合以解决区块链可扩展性问题。这种分层思路已经成为公链领域的共识，比如以太坊采用了 Rollup 发展路线。一层和二层的主要职能如下：

- **一层的主要职能：**
  1. 通过增强共识机制（如 dPoS、DAG 等技术），在确保安全性的前提下提高一层的容量，以最大程度地利用一层网络。
  2. 提供资产定义、发行和流通，以及一层和二层之间的资产流转功能。
  3. 为二层提供仲裁机制，确保二层的安全性，利用一层的安全机制来支持二层。
- **二层的主要职能：**
  1. 将一层交易分流至二层，使一层不再需要关注二层交易的细节或状态更改。
  2. 提供监督机制，使二层不同角色之间可以相互监督。
  3. 提供证据保全功能，当用户对二层交易产生争议时，可以仲裁至一层解决。

11.2 本分二层方案概览

11.2.1 状态通道

通用的状态通道包括支付通道，不过支付通道的状态限定在资产方面。通用状态通道试图扩展状态的概念，可以适用于应用中的任何状态。状态通道的核心思想是通过双方监督，将双方之间的状态变化从链上迁移到链下，等到通道关闭时进行链上清算（或者可以优化为定期清算）。这相当于将多次交易中的状态变更合并成一次，从而降低了交易成本，提高了整体的交易容量。通道内的状态变更成本极低，因此支持高频交易或需要频繁互动的互联网应用，例如游戏。

尽管理论上状态通道的参与者可以是多方，但由于状态通道中的每个变更都需要所有参与方的共同

确认，因此难以扩展到多于两个参与方，这也限制了其应用范围。

11.2.2 RollupChain

RollupChain 是目前流行的二层解决方案，将二层的数据直接提交到一层区块链中，一层的区块只记录二层的交易数据，但不执行。用户需要时可以在一层找到数据并构建证明，以确保资产的安全性，尤其在需要挑战运营方时。尽管 RollupChain 也受到一层容量的限制（因为其交易也需要占用一层区块链的容量），但仍然显著提高了性能和可扩展性，是当前更容易实施的解决方案。这种方案通常被称为 Optimistic Rollup。

另一种解决方案引入了零知识证明，其思想与 Optimistic Rollup 类似。但由于引入了零知识证明，可以减少取款等待时间，并理论上可提供更短的处理时间。如果需要挑战，挑战在一层执行的难度较大，一层只需要提供验证零知识证明的能力。这种方案通常被称为 ZK Rollup。

关于本分的二层设计具体方案将在未来发布的本分二层设计白皮书中详细阐述，这里只描述了一层设计中对二层的考虑。

12. 展望

本分，作为新一代现实世界支付公链，旨在有力地应对当前区块链技术和应用面临的挑战，提高其易用性并推广使其能被广泛采用。通过在共识机制、智能合约编程语言、稳定币经济模型、社区治理等方面的改进，本分增强了安全性和性能，使其更适合当前去中心化金融的应用场景。同时这些改进也为未来架构奠定了基础，以满足高性能低延迟的 DeFi 的运行需求。通过链上治理机制，本分确保了其链的持续演进和生态构建能力。

相比传统公链，本分在性能和安全性方面表现更出色，稳定币也为用户提供了全新的交易和储值选择。此外本分通过打造原生的去中心化交易所（DEX），降低用户使用门槛，提升用户体验，进一步增强了去中心化金融平台的能力。

我们坚持以用户价值创造为核心，通过不断的研究、创新和改进，致力于将本分打造成一个高度安全、高性能、可扩展、易用性强且可广泛应用的去中心化金融平台，为用户、开发者和商家创造更多的机会和价值。

13. 参考文献

1. Y. Zohar. (2020). Move Prover. Retrieved from https://www-cs.stanford.edu/~yoniz/cav20.pdf

2. Wikipedia contributors. (n.d.). Decentralized autonomous organization. In Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Decentralized_autonomous_organization. Note: APA suggests providing a retrieval date for sources that may change over time, like Wikipedia.

3. Mysten Labs. (n.d.). Why we created Sui Move. Medium. Retrieved from https://medium.com/mysten-labs/why-we-created-sui-move-6a234656c36b. Note: Author(s) and publication date are missing; “Mysten Labs” is assumed to be the author; “n.d.” denotes “no date.”

4. Move Language Team. (n.d.). Move Spec. Retrieved from https://github.com/move-language/move/blob/main/language/move-prover/doc/user/spec-lang.md. Note: The specific authors of the GitHub document are not listed, and publication date is not provided.

5. Singh, S. F., Michalopoulos, P., & Veneris, A. (2023). DEEPER: Enhancing Liquidity in Concentrated Liquidity AMM DEX via Sharing. In Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1–5). Dubai, United Arab Emirates. https://www.eecg.utoronto.ca/~veneris/23cryptox.pdf

6. Blackshear, S., Cheng, E., Dill, D. L., Gao, V., Maurer, B., Nowacki, T., Pott, A., Qadeer, S., Rain, D., Russi, S., Sezer, S., Zakian, T., & Zhou, R. (2019). Move: A Language With Programmable Resources. Retrieved from https://developers.libra.org/docs/move-paper.

7. (2022). DAG meets BFT. Retrieved from https://decentralizedthoughts.github.io/2022-06-28-DAG-meets-BFT/.

8. Danezis, G., Kokoris-Kogias, E., Sonnino, A., & Spiegelman, A. (2021). Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus. CoRR, abs/2105.11827. Retrieved from https://arxiv.org/abs/2105.11827

9. Guerraoui, R., Kuznetsov, P., Monti, M., Pavlovic, M., & Seredinschi, D.-A. (2018). AT2: Asynchronous Trustworthy Transfers. CoRR, abs/1812.10844. Retrieved from https://arxiv.org/abs/1812.10844

10. Spiegelman, A., Giridharan, N., Sonnino, A., & Kokoris-Kogias, L. (2022). Bullshark: Dag bft protocols made practical (full paper). arXiv preprint arXiv:2201.05677. Retrieved from https://arxiv.org/abs/2201.05677

11. Dill, D. L., Grieskamp, W., Park, J., Qadeer, S., Xu, M., & Zhong, J. E. (2021). Fast and Reliable Formal Verification of Smart Contracts with the Move Prover. CoRR, abs/2110.08362. Retrieved from https://arxiv.org/abs/2110.08362

12. Optimism Community. (n.d.). Rollup Protocol. Retrieved from https://community.optimism.io/docs/protocol/2-rollup-protocol/#moving-from-op-mainnet-to-ethereum. Note: Author(s) and publication date are missing; "Optimism Community" is assumed to be the author; "n.d." denotes "no date."

13. Liu, Y., & Tsyvinski, A. (2018). Risks and Returns of Cryptocurrency. August 2018. *Note: The exact format of a working paper citation can vary. If this is an article, include the journal title, volume.