原力协议

加密开放金融服务协议

白皮书 V6.0

摘要：针对当前加密开放金融领域存在的问题，原力协议提出了包括 DeFi 技术组件和多个代币化协议在内的解决方案，向全球用户提供安全、普惠、创新、透明的加密开放金融服务。

目录

1 背景

以太坊智能合约是一项伟大的发明，它使区块链不再仅仅只是一种电子现金系统，而是具备了逻辑处理能力的图灵机。但是，基于资产安全等多种考虑，以太坊智能合约从一开始就被设计为不可修改不可升级的机制，这就对基于智能合约的应用开发提出了严峻的挑战。

首先，程序员都有可能犯错，特别对于合约中的复杂逻辑，更有可能存在无法轻易察觉的问题，即使历经严格反复的逻辑检查和代码审计，仍然无法确保所有代码都正确无误。潜在问题的改正和错误代码的修复，势不可免。其次，现实世界是瞬息万变的，用户需求也不可能一成不变。一个产品无论在事先考虑得多么周密和详尽，在经过运营尤其是大规模运营之后，总会发现已实现需求中的问题，以及亟待实现的全新需求。这就要求智能合约是可持续迭代和升级的。

自从第一个去中心化 DApp 上线以来，数据和资产安全问题就始终是影响甚至毁灭 DApp 的最关键因素之一。层出不穷的资产安全事件，持续震动着整个业界。如何最大化地提升区块链应用的系统安全性，全力保护好用户资产，已经成为横亘在每一个 DApp 开发运营团队面前的首要问题。

2 原力协议定义

原力协议是基于主流区块链系统搭建的加密开放金融服务协议，由一套 DeFi 技术组件和多个代币化协议组成。原力协议致力于向全球用户提供安全、普惠、创新、透明的加密开放金融服务。

2.1 DeFi 技术组件——“The Force”

针对以太坊 DApp 开发中存在的诸如合约不易升级迭代、数据结构固化、链上交互速度慢、用户体验差、缺乏必要基础设施、安全问题突出等问题，原力协议提出基础组件、扩展组件、金融组件等三大 DeFi 技术组件，合称为“原力”。最终目标是让以太坊金融服务类 DApp 能够接近传统互联网产品的开发迭代速度、用户体验，并保留其安全特性。

- **基础组件：**APEC，即 Assets Protected Elastic Contracts，资产安全的弹性智能合约。
- **扩展组件：**BEAMS，即 Blockchain Enquiring, Auditing & Messaging System，区块链查询、审计和消息系统。
- **金融组件：**GEL，即 Global Emergency Lockdown，全局紧急闭锁；CALM，即 Cooperative Automatic Lockdown Mechanism，协同自动闭锁机制；MAK，即 Multisig Admin Keys，多重签名的管理员密钥。

2.2 代币化协议——“ForTube”

在 DeFi 技术组件的基础上，原力协议将债券融资协议、货币借贷协议和去

中心化稳定币协议集成，形成 ForTube 加密开放金融服务平台，ForTube 将为个人和企业用户提供加密数字资产的投资、融资和交易服务，满足不同用户的加密数字金融需求。

- **ForTube Bond**：债券融资协议，固定期限、固定利率的数字货币借贷服务；
- **ForTube Bank**：货币借贷协议，由算法驱动的活期、可变动利率的代币存借服务；
- **QIAN**：去中心化稳定币协议，致力于成为加密数字领域具有影响力的稳定币项目，QIAN 稳定币可用于投资 ForTube Bond，也可以存入 ForTube Bank 获取利息。

上述三种协议互相促进，业务间具有较高的关联性，可以形成聚合效应，有利于业务的协同发展。

3 DeFi 技术组件

3.1 基础组件 APEC

基于 Solidity 语言的 APEC 平台是 DeFi 协议的主要基础组件，APEC 即 Assets Protected Elastic Contracts，资产安全的弹性智能合约。

3.1.1 设计理念

APEC 作为链上（On-Chain）核心架构，基于 Solidity 智能合约，并且在坚守去中心化和资产所有权的前提下，对合约开发中的不便之处进行了调整和优化。

APEC 的核心理念是资产安全和组件弹性，主要包括以下 3 个方面的特性：

- 资产安全，Assets Protected
- 逻辑可升级，Logic Upgradable
- 数据可扩展，Data Extensible

3.1.2 架构图

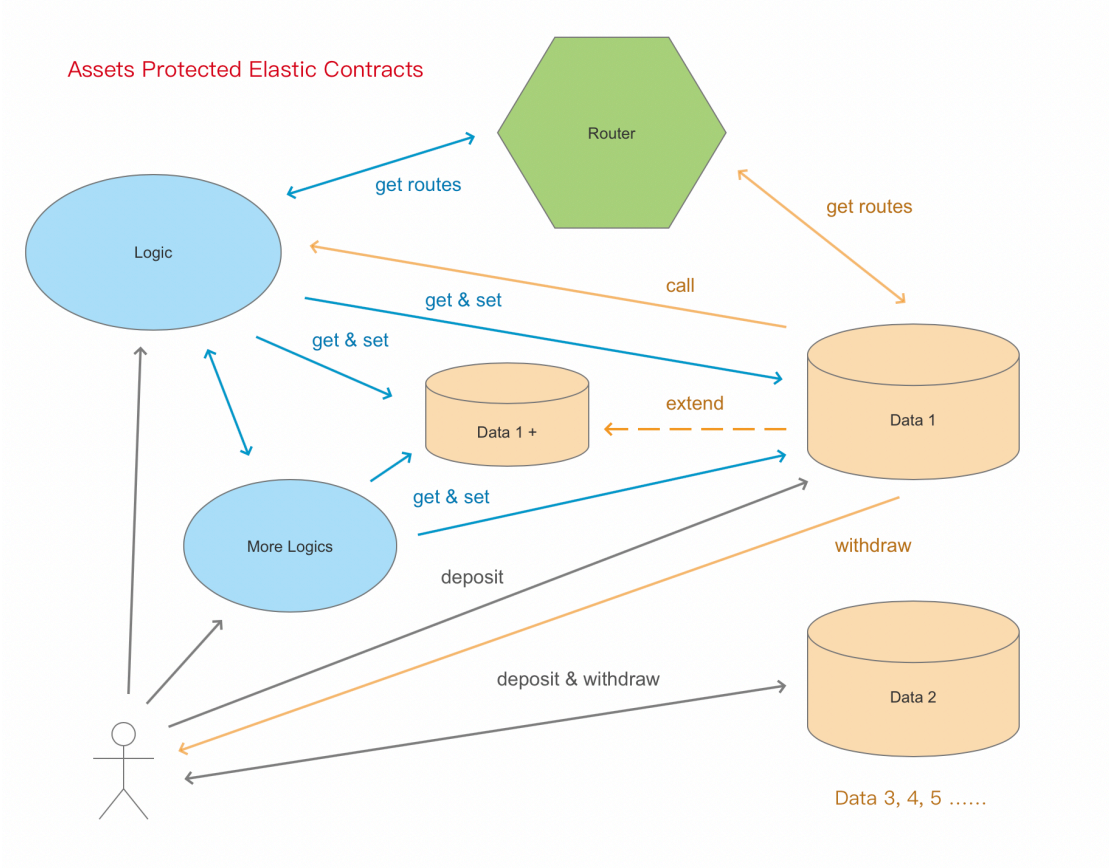

图 1 APEC 技术架构图

3.1.3 技术构架

APEC 在整体上可分为 3 大模块：

- 数据（Data）：把经典合约结构的数据部分独立出来，做成一个或一组数据合约，用于存储数据，对外只暴露必要的读写接口。
- 逻辑（Logic）：逻辑合约负责纯粹的业务逻辑，不含业务数据。
- 路由（Router）：业务逻辑所需要读写的字段数据，可根据数据模块和字段名称从路由表中查询，再根据定位结果进行访问。

路由表

路由表是一个独立合约，内含一个路由对照表，存储逻辑合约和数据合约地址的路由映射，可随系统升级持续更新。

合约系统在整个部署后，各个逻辑合约的地址就会被存储到路由表中，外部请求可访问路由表，获取逻辑合约的地址映射并调用其接口。数据合约也可以通过查询路由表获取逻辑合约地址，进行业务逻辑的调用或回调。

对于每组数据，都会有一个属于自己的独立的数据合约，数据合约的地址将会在创建时被自动存储到路由表中。逻辑合约在访问指定的数据之前，也会首先从路由表中获取数据合约地址，再通过地址读写数据合约。

逻辑可升级

逻辑合约不存储资产，不含业务数据，因此就不存在资产安全和数据迁移等问题，所以它是可升级和可插拔的。逻辑合约的新版本在经过测试和审计后，即可部署到链上。

部署新合约时会同时更新路由表合约中的映射表数据，更改路由表中该逻辑合约的地址映射指向，以供其它合约或应用前端查询和调用。

数据可扩展

作为一个可迭代升级的应用，它的数据结构往往也要求是可迭代的。但出于数据所有权和资产安全的考虑，数据合约不可升级。我们采用的解决方案是扩展。如果业务上需要添加新字段，这些字段会被存储到一个全新的数据合约中。同时，这个新数据合约的地址和内含的字段名称，会被添加和更新到路由表中，业务逻辑通过查询路由表，获取新字段的地址路由进行读写。

数据合约的扩展，应该是节制和有限度的。一味地增加新的数据合约，会提升整个系统的复杂度和运行效率。数据扩展机制只是把数据结构迭代的需求从不可能变为可能，不鼓励频繁和随意地使用这个机制。

我们在设计和使用数据结构时，仍然需要遵循合约的经典设计原则和最佳实践，设计充足和弹性的数据结构。对于数据的扩展，应始终保持克制的态度，非必要时不使用数据扩展机制。

3.1.4 资产安全

如果逻辑合约可升级，数据合约可扩展，那么随之而来的问题就是，用户的数据所有权和资产安全是否能得到保障。

众所周知，对于传统 DeFi 应用而言，用户的所有资产都被锁定在合约里。智能合约，特别是代码开源的合约，通过代码公开的形式向用户保证，除了用户自己，没有其它任何人或程序可以染指用户锁定在合约中的资产。更进一步地，合约的不可修改性使得合约一旦部署就不会有代码的变动。

APEC 采用了职责分离的方式解决了在可升级架构下的合约资产安全问题。

业务合约是可修改和升级的，数据合约则秉承经典合约的理念，不可修改升级。在初始化时，每份数据集合会自动生成一份初始数据合约，这个合约一旦部署到链上就不可再修改其代码逻辑。

- **数据合约会在内部维护一个用户地址和资产详情的映射表。**该映射表在数据合约内部，只提供用户资产的入账和出账两个接口，其它任何接口都无权写入和更新该资产表。
- 用户入账交易，直接发往数据合约地址，调用其入账接口。用户资产锁入合约后，**在资产映射表中记录该用户的地址和其资产详情**。然后再调用逻辑合约，处理和记录业务逻辑。

- 用户在出账交易时，仍然是直接调用数据合约上的出账接口，**合约将校验用户的地址是否存在于资产映射表中**，然后调用逻辑合约，计算出账数额，最后把资产直接转账给用户的请求地址。
- **任何不在资产映射表中的地址，出账接口将不响应其资产请求。**在逻辑上保证了任何一份出账的资产，都属于当初投资入账的原始地址，确保了用户对投资资产的所有权和用户资产的安全。即使是运营团队自己，也无法篡改和冒领用户的任何锁定资产。

通过数据合约严格的所有权约束，保证了用户资产的所有权和安全性，使得 APEC 的安全哲学秉承了智能合约的一贯理念：超越了“不要作恶”（Don't Be Evil），实现了“无法作恶”（Can't Be Evil）。

3.2 扩展组件 BEAMS

BEAMS 即 Blockchain Enquiring, Auditing & Messaging System，区块链查询审计和消息系统。

3.2.1 区块链的局限性

区块链对现实世界几乎是完全割裂的，它无法主动向链下推送消息，如果智能合约的逻辑出现问题或受到攻击，现实世界是无法被动感知的。因此我们需要持续地监控合约的运行，严格地审计合约中的数据和资产，在出现问题时第一时间发出告警，尽最大可能保证应用的安全。

对用户而言，区块链交互体验天然的不友好。区块延迟导致的异步反馈，频繁而大量的链上数据读取和业务模型重建，链上和链下的消息割裂，都造成了体验上的缓慢甚至交互上的混乱。

3.2.2 设计理念

上述问题的存在，促使我们去构建一个连接链上和链下的系统，持续监控合约的运行，审计数据和资产，加快产品的响应速度，使响应速度的波动曲线趋向平滑，让不可避免的异步反馈更加顺滑和流畅。各种由条件触发的状态提醒和消息推送，可以让用户在使用 DeFi 应用解决金融需求之外，获得更为人性化的产品体验。

BEAMS 是与合约紧密配合的链下（Off-Chain）系统，其核心理念主要包括以下 3 个特性：

- 查询，Enquiring
- 审计，Auditing
- 消息，Messaging

3.2.3 BEAMS 架构图

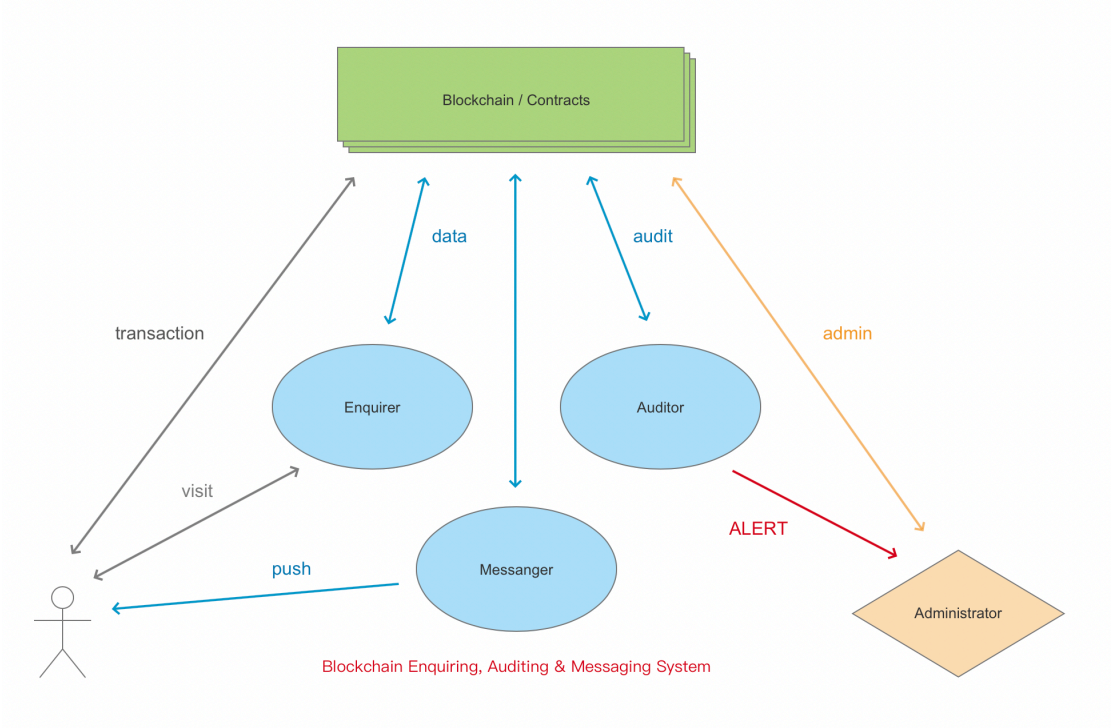

图 2 BEAMS 技术架构图

3.2.4 技术架构

BEAMS 由 3 个模块构成，查询(Enquirer)，审计(Auditor)和消息(Messanger)。

BEAMS 采用基于链上事件（Event）的轮循机制，监控链上合约状态和数据的变化，基础数据将会存储在数据库中，通过接口提供给前端界面。合约数据的变动会实时并行审计，并将异常情况即时上报给系统管理员。同时对抵押物价值变化和清算等状态进行持续计算，必要时主动向相关用户推送各种形式的通知和告警。

数据查询

涉及资产变动的核心交易，都会触发自定义的链上事件。查询系统持续地监控新事件的产生，并根据事件内容去查询相应的合约数据。数据合约向外部提供暴露数据的只读接口，查询系统按照数据模型的要求，从合约中读取相关数据。

读取到的数据都将被整理和聚合到 BEAMS 的数据仓库，并记录其数据变动情况。数据仓库作为整个系统的数据核心，将通过后端 API 接口向前端提供准实时的数据缓存，向消息模块提供计算和触发的所需数据。审计模块也会使用这些数据对链上合约的状态转移和数据变动进行复核和审计。

审计风控

审计风控模块将持续监控每个合约的状态和数据的更改，对于涉及到的资产变动，审计风控模块会使用独立并行的逻辑对资产变动情况进行二次复核，如果出现异常，则实时通知系统管理员进行处理。

审计风控模块会使用资产总量、变动逻辑、状态校验等不同的复核方式从各个方向对合约数据进行实时审计，以提升审计的准确性。审计模块可以对异常情况进行评级和告警，风控模块在判断为极高风险的场景下甚至将有权对链上合约的运行情况进行干涉和管理。

审计风控模块还将担负统计分析的职责，对用户的订单记录，历史收益，资产变化曲线，平台的实时收益指标，历史收益曲线等系统运营数据进行统计和分析，预测和控制风险点，并为产品运营方向提供数据参考。

消息推送

为了提升由于区块链特性导致的异步反馈的用户体验，消息推送模块将在用户使用流程的各个环节起到重要的作用。特别是在涉及到用户自身利益的提醒通知和警示消息等方面，缺乏基础设施的区块链更需要消息推送系统来配合工作。

在页面一侧，消息推送模块将优先使用 Websocket 长连接模式，通过前端页面和用户建立双向实时链路，在各个需要执行链上交易的环节，监控链上交易执行情况，交易结束后，向用户推送交易结果和链上状态。

而对于资产清算、收益发放、赎回提醒等消息，则由消息推送模块对合约数据进行持续的监控和分析，达到触发条件后，可以使用包括邮件和短信在内的各种方式，实时对用户推送提醒通知和告警信息。

3.3 金融组件

3.3.1 DeFi 金融安全三定律

DeFi 安全哲学可以概括为层级防御理念的 **DeFi 金融安全三定律**：

- 保护平台安全，不受攻击和入侵
- 如果受到入侵，保护资产安全
- 如果资产不再安全，把损失降到最低

DeFi 金融安全体系是一个多层次全方位的体系。去中心化是核心，是基础，但并不是唯一和全部。一个具备良好可扩展性，能够应对未来可能存在的千万数量级用户，安全可靠具有完备风控能力的开放金融应用，如果仅仅依靠去中心化的基础设施，是不可能建设成功的。

3.3.2 GEL

GEL 即 Global Emergency Lockdown，全局紧急闭锁。

在 DeFi 体系，所有涉及到资产变动的智能合约接口上，都有全局紧急闭锁开关。如果合约出现问题，可以手动或自动触发紧急闭锁，禁止所有的出入账调用，保护合约内锁定的资产安全。

3.3.3 CALM

CALM 即 Cooperative Automatic Lockdown Mechanism，协同自动闭锁机制。

CALM 是链下风控机制，采用金融级风控标准，使用独立的高可用主从热备集群，7x24 小时不间断运行。CALM 每 5 秒检查一次合约状态，对合约内所有的金融资产进行严格的记账和对账，一旦发现可能的资产风险，将立即自动触发全局紧急闭锁，禁止受波及资产的所有出入账接口，把资产损失降至最低。同时通知管理人员，启动运营团队快速反应机制，人工介入和排查问题。

3.3.4 MAK

MAK 即 Multisig Admin Keys，多重签名的管理员密钥。

DeFi 采用管理员密钥机制，管理员可使用密钥设置各级权限，如合约路由的更新，预言机的喂价权限，全局闭锁标志位的设置权限，等等。管理员密钥可以添加、删除和更新下级权限，在下级权限密钥泄漏时，可迅速更换密钥。

为了规避管理员密钥被盗和遗失的风险，我们采用了多签机制。目前使用的是 3-2 多签，随着平台锁定资产的增加，我们还会逐步提升至 5-3 甚至 7-5 机制。

以 3-2 多签为例，合约中保存 3 个管理员密钥，在进行诸如更换管理员密钥等最高安全等级的操作时，必须使用至少 2 个管理员密钥，同时进行多重签名，该操作才可被执行。

管理员密钥的多签机制保证了：

- 如果某个管理员密钥泄漏，攻击者使用这个密钥也无法完成高权限等级的操作。而平台管理员可以使用多签机制将泄漏的密钥删除，使之失效。
- 如果某个管理员密钥遗失，可使用剩余的管理员密钥添加新的管理员密钥，并删除遗失的密钥。
- 管理员密钥多签才能生效的机制，使每一个高等级的权限操作都依赖于集体决策和执行，有效地防范了内控风险，进一步保护了资产安全。

4 代币化协议

4.1 债券融资协议——ForTube Bond

加密数字债券（Crypto Bond）是以 token 形式发行和记账的新型债券，既能为持有加密资产的团队或个人提供融资服务；也能给加密货币市场补充固定收益产品，满足部分投资者的需求。ForTube Bond 将为加密数字债券提供整套解决方案，包括信用评级、债券发行、债券清算、债券交易等。

4.1.1 债券信用评级

受限于目前加密金融服务仍然不成熟，不适合中长期债券发行，当前加密数

字债券产品类型将以短期债券为主。加密数字债券发行采用注册制，不需要任何中心化机构审核和批准。债券发行人提交的发债基础信息将由 ForTube 平台自动进行必要的形式化校验，发债信息由 ForTube 社区投票确定信用等级后，债券即可正式发行。

债券信用评级（Bond Credit Rating）是对债券违约风险的评测，为用户的投资决策提供参考，ForTube 平台采用如下债券信用评级表。

表 1 债券信用评级表

评级	含义
A-1	为最高级短期融资券，还本付息风险很小，安全性很高。
A-2	还本付息风险较小，安全性较高。
A-3	还本付息风险一般，安全性易受不利环境变化的影响。
B	还本付息风险较高，有一定的违约风险。
C	还本付息风险很高，违约风险较高。
D	不能按期还本付息。

ForTube 平台债券信用评级由社区评级和专业评级组成。社区评级由原力协议生态代币 FOR 的持有者执行，评级人了解债券信息后，将 FOR 锁仓至相应等级，评级结束后即可取回 FOR 代币。专业评级由专业信用评级机构或专业人士执行，成为专业评级人需要向 ForTube 运营团队提交申请，提供能够证明其专业能力和资质的材料。最终评级结果将由社区评级和专业评级共同确定，社区评级权重为 60%，专业评级为 40%。参与评级将获得评级服务费，评级服务费按同等比例分配。

4.1.2 BondTokens

债券信用评级完成后，加密数字债券即可发行。每份债券以 ERC-20 格式发行，我们称之为 BondTokens，BondTokens 是投资债券后获得的投资凭证。每种类型的 BondTokens 都有自己的 ERC-20 合约，包含了该债券的所有必要信息和相关操作。BondTokens 可任意转账，但是不可分割，其票面价值通常为 100 USD。谁持有 BondTokens，谁即是该债权债务关系中的债权人，拥有 BondTokens 即可在 ForTube 平台兑付本金和收益。

表 2 BondTokens 主要信息

债券信息	举例
发债人	以太坊地址
债券信用等级	A-3
发行量	1,000,000 DAI
票面价值	100 DAI
发行份数	10,000 份
息票利率	15%
债券期限	30 天
债券起始日	2020-02-01
债券到期日	2020-03-02
是否可赎回	否
是否可回售	否

BondTokens 是一种新型的加密数字资产，不同质押资产、不同到期日、不同利率、不同信用等级的 BondTokens 可满足加密数字资产市场的多样化需求，成为其他创新金融应用的基石。

4.1.3 债券清算

若债券底层质押资产出现大幅贬值或者发债人未按时还款时，会涉及到质押资产的清算。ForTube 平台当前采用折价清算模式，即清算人可以按折扣价格兑换质押物。

为方便计算，设定如下参数：设定目标质押率为 TCR，当前债务总计 CD，当前质押率 CCR，折扣率 Discount，质押物当前价格 Price，清算前质押物剩余数量 AC。其中折扣率（1-Dicount）为对清算人的清算奖励。

债券存续期内清算

债券存续期内，当质押物价值下降 20%后，系统将向债务人发送补仓提醒，当质押物价值下降 30%后，系统触发质押物处置，系统将清算部分质押物，使得质押率回到初始值。

当

$$CCR \leqslant 70\% \times TCR$$

时，计算清算质押物数量 X，以及清算债务额 Y

$$Y = X \times Price \times Discount$$

其中 X 的计算过程如下。若质押资产不能清偿债务，即

$$AC \times Price \times Discount < CD$$

时，全额清算

$$X = AC$$

当质押资产能够清偿债务，即

$$AC \times Price \times Discount \geqslant CD$$

时，清算后质押率需等于目标质押率 TCR，即

$$TCR = \frac{(AC-X)\cdot Price}{CD-X\cdot Price\cdot Discount}$$

求解 X，得

$$X = \frac{AC\cdot Price-TCR\cdot CD}{Price\cdot(1-TCR\cdot Discount)}$$

逾期未还款清算

债券到期后，若债务人未能还款，系统将触发质押物处置，系统将清算部分质押物以偿还所有债务和手续费，剩余质押物返还债务人。

若质押资产不能清偿债务，即

$$AC \times Price \times Discount < CD$$

时，全额清算

$$X = AC$$

当质押资产能够清偿债务，即

$$AC \times Price \times Discount \geqslant CD$$

时，

$$X = \frac{CD}{Price\cdot Discount}$$

剩余质押物数量（AC-X），发债人可取回。

4.1.4 债券交易市场和债券衍生品

为方便债券持有人提前退出投资，收回本息，ForTube 平台未来将推出债券二级交易市场。债券持有人可在系统给定的参考定价上自由设定转让价格和转让数量。投资人可查看债券基础信息、信用评级信息、预期收益等。投资人支付投资款项后即可获得相应债券的 BondTokens，到期后即可在平台兑付本息。随着 BondTokens 的流行，ForTube 平台将继续推出更多功能以支持各种债券衍生品，包括：

- 债券回购（包含逆回购）；
- 可赎回债券（指债券发行人可在债券到期日前赎回已发行的债券）；
- 可回售债券（指债券持有人可在到期日前将债券回售给债券发行人）；
- 其他符合业务需求的债券衍生品。

4.1.5 Bond 模块社区治理

ForTube 致力于推动去中心化（或多中心化）债券发行和结算，系统权限及核心参数在将来会交由社区管理。但是，在项目初期，为了快速推动项目开发和平台发展，系统权限和参数将由 ForTube 开发者维护。ForTube 开发者将秉持公正和透明原则，对系统的任何改动都将及时告知社区。当前，由 ForTube 开发者维护的系统参数包括但不限于：

- 支持的加密数字资产及其质押率、最大可发债数量、清算折扣等；
- 债券发行基本参数，如息票利率、债券期限、发行费用、评级服务费等；
- 时间参数，如信用评级期限、债券发行期限、还款宽限期等；
- 债券信用等级设置；
- 可信预言机喂价程序。

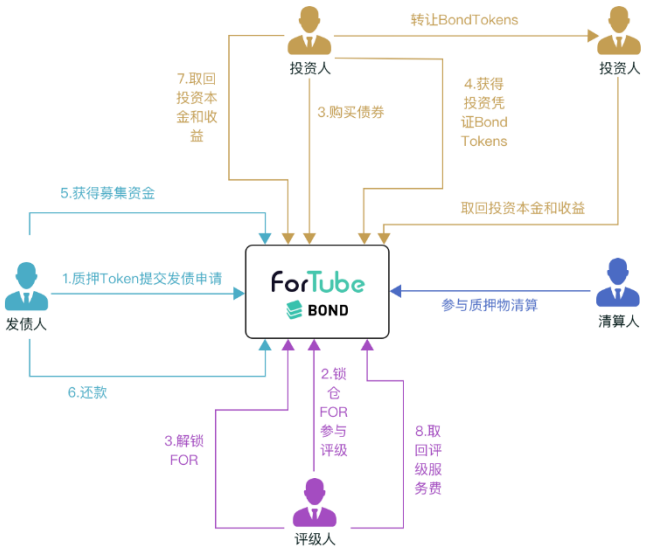

图 3 ForTube Bond 价值流向

4.2 加密货币借贷协议——ForTube Bank

ForTube Bank 是一个加密数字货币存借协议，支持随存随取，随借随还。通过部署在区块链系统上的自动程序（智能合约），出资方可以无摩擦地快速获得资金收益，有资金需求的借款方在提供合适的抵押物之后就可以快速便捷地获得财务支持。

4.2.1 设计思路

ForTube Bank 支持用户将其数字资产存入智能合约获得利息收入，同时获得贷款额度，用户可以在贷款额度内借出其他数字资产。不管是存款还是贷款，用户不需要关注借款期限，随时取回或者还款。

当借款人的未偿还借款超过其抵押物限定比例时，系统将扣押用户资产，进入清算流程。此时，允许套利者调用清算合约，按照一定的折价比例置换扣押资产。由于不同的数字资产在市场规模、流动性、价格稳定性等方面存在区别，其质押率、清算折扣等会有差异，产品相关信息如下表。

表 3 Bank 产品信息表

要素	规则
支持币种	USDT(ERC-20)、USDC、DAI、ETH、WETH、HBTC、IMBTC、QIAN 等
质押率	150%
清算折扣	95%
平仓线	用户存币资产之和小于所有借币资产乘以对应质押率之和时，可对用户借币资产进行平仓
借款年利率	1.5% ~ 20%
存款年利率	0 ~ 18%，存款年利率由借款年利率和使用率决定，计算公式：借款年利率 × 使用率 × 0.9
合约中每一币种用户可借最大数量	=［（所有存币资产之和 - 所有借币资产乘以对应质押率之和） ÷ 对应币种最小质押率 ］÷ 对应币种价格

页面中每一币种用户可借最大数量	= 合约中每一币种用户可借最大数量 ×（1 - 币种清算折扣）

4.2.2 利率模型

ForTube Bank 采用一套算法控制的利率模型，基于供求关系的变化，利率自动调节，从而调节借贷总规模、资金供应量等因素。

对于借贷资金的调控，Bank 遵循以下原则：当借贷资金池内的资金借出量较低时，借贷利率上涨的速度较低，以促进借款人从资金池借款；当借贷资金池内的资金借出量较高，甚至接近饱和时，借贷利率上涨的速度较快，带动存款利率增加，以促进存款人向资金池内存入更多资产。通过算法调节，确保整个借贷资金池的发展和增长处于健康的范围。

对资金借出量进行量化，我们引入参数 x，代表资产 a 的资金借出比例，其公式为：

$$x = \frac{\text{稳定币的借出总额}_a}{\text{稳定币剩余可借总额}_a + \text{稳定币的借出总额}_a}$$

设借款利率为 y，y 和 x 的关系可以用分段函数表示如下：

$$\begin{cases} y = x^e + 0.015\,; & if \quad 0 \le x < \dfrac{3-\sqrt{5}}{2} \\ y = \left(\dfrac{3-\sqrt{5}}{2}\right)^{e-1} x + 0.015\,; & if \quad \dfrac{3-\sqrt{5}}{2} \le x < \dfrac{\sqrt{5}-1}{2} \\ y = \left(\dfrac{3-\sqrt{5}}{2}\right)^{e-1} - (1-x)^e + 0.015\,; & if \quad \dfrac{\sqrt{5}-1}{2} \le x \le 1 \end{cases}$$

如公式所示，ForTube Bank 将利率的变化分为了三个阶段：

- 第一阶段，为了刺激初始阶段的借贷量上涨，利率增长模型近似指数曲线，这也符合自然增长规律；
- 第二阶段，通过积累一定量的借款额，利率的增长速度进入了稳定期，其图形为一定斜率的直线；
- 第三阶段，由于借出的资金量已经较多，借贷利率的增加速率会加快，以适当的控制资金借出速度，促进存款量增加，利率增加的速度会逐渐逼近一个极值，这一阶段的利率变化接近于修正指数曲线。

相对应地，存款利率 SIR 公式为：

$$SIR_a = x \times y \times (1 - s)$$

其中，

x = 稳定币 a 的借出比率；

y = 稳定币 a 的借款利率；

s = 调整比率，0 ≤ s < 1，一般可取 0.1。

4.2.3 利率计算

存款年化利率和借款年化利率将转换成每秒利率，采用连续复利计算。假定 R 为借款年化利率，则每秒利率 r 的计算公式为：

$$r = \frac{R}{365 \times 24 \times 60 \times 60}$$

所以，t 时刻的利率：

$$r_t = r_{t-1} \times e^{r \times \Delta t}$$

其中，Δt 是指 t-1 时刻到 t 时刻的时间间隔。

因此，假定用户借款金额为 BA，借款时刻为 t0，还款时刻为 t1，则到期应还本息和为

$$BA \times \frac{r_{t1}}{r_{t0}}$$

存款利率和利息计算公式类似。

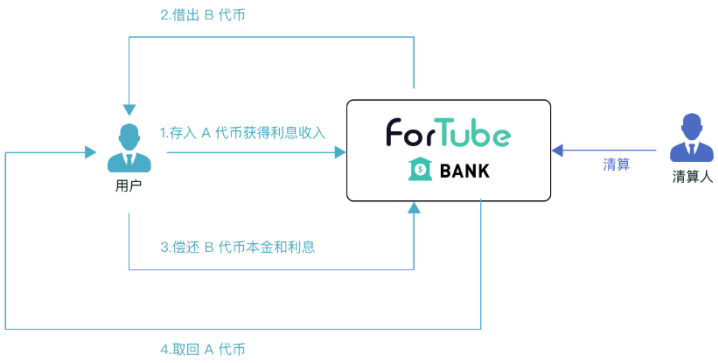

图 4 ForTube Bank 价值流向

4.3 去中心化稳定币协议——QIAN

QIAN 同“乾”和“钱”。在《易经》当中，乾卦代表天，代表宇宙万物运转的规律，是最崇高的精神和正向能量。遵循这个重要的涵义，我们将去中心化稳定币协议命名为 QIAN。QIAN 致力于创造一种人人皆可平等、自由、便捷参与的稳定币系统，让每个人都享受无差别和无歧视的金融服务。

4.3.1 QIAN 的设计理念

持有加密资产的用户，只需要将超额的加密资产锁定到 QIAN 的智能合约，就可以获得等价于法定货币的 QIAN 稳定币，不需要支付任何利息。稳定币 QIAN 被视为智能合约对加密资产持有人的货币交换证明，我们将这一机制下的智能合约命名为 CSA（即 Currency Swap Agreement，货币互换协议）。

持有 CSA 无利息成本

作为流动性提供者，持有 QIAN 的 CSA 不需要支付任何利息，相反有可能获得来自于智能合约的利息作为额外收入，这将刺激债权人长期持有 QIAN 的 CSA，使 QIAN 有了被用于跨境支付、消费支付、资产交易、借贷活动等各类经济活动的可能。无需持有成本，QIAN 才有可能真正的参与加密开放金融生态的发展过程，与同样无需持有成本的法币担保型稳定币共同发展，服务不同需求的用户。

支持闪电贷

目前已知闪电贷（Flash loan）是一项安全的技术，任何拥有资产的智能合约，都可以选择对外提供闪电贷服务，通过收取一定量的借贷利息，可以利用自身资产增加更多的收益。目前已经在以太坊 DeFi 生态中出现了闪电贷的聚合类工具，通过将支持闪电贷的智能合约的流量进行聚合，可提供更强大的闪电贷服务。QIAN 的智能合约将支持闪电贷，锁定在 QIAN 智能合约里的加密资产可以获得额外的收益，QIAN 系统的运营者将定期用获得的收益在市场上买入 FOR 代币，FOR 作为 QIAN 智能合约收益的价值贮藏载体，将被锁入保存 QIAN 系统收益的智能合约。

风险控制

在 QIAN 的设计中，我们遵循如下的风险管理规则：

首先，QIAN 2.0 秉持超额储备原则，用户在使用 ETH 等加密资产生成 QIAN 时，需要满足一定比例的启动充足率，锁定加密资产的价值与生成 QIAN 的价值比例至少要大于 120%。

其次，为了增加 CSA 内锁定资产的安全性，避免在极端行情下产生爆仓，同时兼顾加密资产的利用率，QIAN 将根据加密资产市场价格的变化速度，引入波动率因子，调控 CSA 的资产锁定倍数。当价格进行单边上涨或下跌时，波动率上升，系统将上调 CSA 的启动充足率。在市场较为平稳的时期，波动率下降，系统将下调 CSA 的启动充足率。这种设计将有效的减轻市场波动对 CSA 锁仓资产的影响，鼓励用户在市场平稳的状态下进行 CSA 锁仓，增加锁仓资产的安全性。

第三，当市场行情暴跌时，用户的 CSA 充足率会下降，在下降过程中，CSA 有预警状态和冻结状态两种变化。例如，某用户持有 ETH 的 CSA，当其储备资产充足率下降到 150%（ETH 的预警线）附近，QIAN 系统将会提示用户补仓。此时，如果行情继续暴跌，用户来不及进行补仓，CSA 的充足率继续下降，当低于 120%以下时，智能合约将会冻结用户的 CSA，直到用户补充锁定资产到安全水平以上才进行解冻。用户在补充锁定资产之前，将不能通过自己的地址发起对于锁定物的赎回。

第四，处于冻结状态的 CSA 可能被清算，允许非 CSA 持有者用 QIAN 按照所有处于冻结状态 CSA 所生成 QIAN 的数值赎回冻结合约当中的资产，这部分内容将在后续平滑套利机制章节详细阐述。

极端行情之下，QIAN 系统内某几种或全部储备资产的充足率可能低于 100%，导致 QIAN 的内在价值支撑不足。如果此时 CSA 持有人普遍没有意愿补充锁定物，而且底层储备资产的市场价格在一段时间内都没有恢复，这将会在 QIAN 系统形成储备缺口（债务）。在这种情况下，系统会在整体储备充足率持续低于某一水平，且经过一定的观察期之后，启动全局债务拍卖。

在全局债务拍卖里，系统将解冻由 The Force Protocol 基金会所提供的治理代币 FOR 并对外拍卖，拍卖所得的收益将用于弥补整个系统的储备资产充足率。

总结而言，QIAN 的设计优势如下：

表 4 QIAN 的设计优势

对比项	QIAN 2.0	DAI
发行机制	货币互换	抵押借贷制
CDP 持有成本	无成本，潜在正收益	成本中到高
CDP 持有风险	中低风险	中高风险
抗极端行情能力	强，待检验	弱，已暴露
抵押资产是否有收益	正收益	负收益
对新技术的支持	强	待观察
生态支持	完善中	较完善
是否有最终购买方	有	有

目标市场	DeFi、实体经济中的跨境支付、消费支付、资产交易、借贷活动等各类经济活动	主要局限于DeFi
汇率对标的法定货币	人民币	美元

4.3.2 锁定物管理

QIAN 由用户向智能合约锁定加密资产生成，初期的底层资产将以 ETH、ERC-20 版本的 BTC 等加密数字货币为主，待系统稳定运作一定时期后，将考虑纳入具备共识的线下资产 token 等加密资产作为发行抵押物。

对于每一种加密资产，系统配置的核心参数包括：

- **市场价格波动率 Vol_i**：由于加密资产的高频交易特性，QIAN 系统将借鉴目前国际市场上常见的，反映期权价格波动的指标 RV（Realized Volatility），定义加密资产 i 的波动率为 Vol_i。在系统上线初期，Vol_i 将根据预言机的报价间隔进行更新，稳定币和期权的概念不同，通过近期的已实现波动率即可有效调控底层资产的风险，因此 Vol_i 不涉及对未来波动率的预测。
- **启动充足率 $Q_{i,0}$**：受到每种加密资产市场价格波动的影响，$Q_{i,0}$ 处于动态的变化中，在 QIAN 系统上线初期，$Q_{i,0}$ 将根据预言机的报价周期进行更新；
- **当前资产充足率 $Q_{i,t}$**：$Q_{i,t} = \frac{Pledged(i,t)}{QIAN_i}$；
- **最低充足率 $Q_{i,min}$**：加密资产 i 的 CSA 低于某个比例时将触发冻结；
- **预警充足率 $Q_{i,alarm}$**：$Q_{i,alarm} = \frac{Q_{i,0} + Q_{i,min}}{2}$，CSA 低于某个比例时将触发预警，提示用户为了保持健康的充足率，需要向 CSA 补充更多储备资产，但用户如果不补充，也能正常进行 CSA 的赎回操作；
- **最高铸币量**：指该类加密资产在系统中所能铸造 QIAN 的最大量；

其中，$Pledged(i)$ 为当前锁定的加密资产 i 总体价值，报价来自预言机，定期更新。

对于特定的加密资产 i，设其可铸币量为 H，则有

$$0 < H \leqslant \frac{Pledged(i) \times Price(i)}{2}$$

其中，$Price(i)$ 为当前加密资产的市场价格（来自预言机）。

对于系统整体，核心参数包括：

- **全局资产充足率 Q_{total}**：$Q_{total} = \sum_{i=1}^{n} Q_i \times \frac{QIAN_i}{QIAN_{total}}$
- **全局最低充足率 Q_{min}**：初始阶段，要求 $Q_{min} \geq 90\%$，后续会通过社区治理流程进行调整。
- **债务拍卖观察时间 $T_{auction}$**：当 Q_{min} 出现后，距离全局债务拍卖开始的时间。

4.3.3 价格波动缓冲机制

设计理念

当前的主流加密资产质押型稳定币缺少基于波动率指标对平仓和抵押操作进行调整的机制，导致在面对极端行情时，稳定币系统不能有效缓冲市场波动对于质押资产的影响，在面临 2020 年 3 月 12 日类似的市场暴跌时，就容易产生质押资产损失，从而影响整个稳定币系统的均衡性。

因此，在设计 QIAN 系统时，我们综合考虑了价格、波动率和时间等因素对底层储备资产的影响。在 QIAN 稳定币系统引入波动率参数，旨在让资产价格对稳定币均衡性的扰动降低，从而能够最大化的维持系统的整体均衡。

波动率指数

QIAN 将引入波动率指数 V_i，作为衡量底层储备资产波动率的重要指标。任何资产的价格都会有涨跌，当价格加速上涨或者下跌时，随着回报率的加速上升或下降，稳定币的底层储备资产 V_i 增加，质押风险逐渐的积累增大。此时通过增加启动充足率 $Q_{i,0}$ 和暂缓清算操作，可以有效的缓冲价格波动对底层储备资产安全性的冲击。当稳定币的底层储备资产价格变化速度逐渐趋于平稳，此时 V_i 下降，质押风险得到释放，通过降低 $Q_{i,0}$ 和恢复清算操作，可以让发生偏离的 QIAN 价格得以回归。

每日间 RealVol

在传统衍生品市场，收益率，或称为已实现波动率（Realized Volatility，RealVol），尤其是每日间的 RealVol，已被广泛接受作为期权波动率指数（例如 RVOL 和 RVOV 等）的基础计算参数。由于加密货币的交易特殊性，需要对传统市场的每日间 RealVol 公式进行再设计，以作为稳定币储备资产 i 波动率计算的基础参数。

每日间 RealVol 公式从传统的标准差公式开始，并在几个关键的方面进行了修改：

- **年化系数：**RealVol 将年化系数设置为一个常数。由于加密市场 7×24 的交易特性，实际的交易天数应该修正为自然年的天数。由于存在月份的天数变化，最好是有一个近似的常数，而不是有几种确切但不同的数值，因此在系统上线初期，我们将年化系数定为 360。
- **更加易读的表示：**RealVol 的结果通常是一个小于 1.00 的值。我们选择将 RealVol 的结果乘以 100，以使数值达到更直观的“百分数衡量”结构。例如，一种加密资产回报率的年化波动可能是 0.20。通常情况下，我们会把这个数字乘以 100，作为 20.00 来传播。

每日 RealVol 公式

$$R_t = ln\frac{P_t}{P_{t-1}}$$

其中：

R_t = t-1 至 t 之间的连续复合收益率（Continuously Compounded Return）

ln = 自然对数

P_t = 当日 t 时的基准价（"收盘价"，根据预言机报价源确定具体时刻）

P_{t-1} = 紧接 t 日前一天的基准价（"收盘价"，根据预言机报价源确定具体时刻）

$$Vol = 100 \times \sqrt{\frac{360}{n}\sum_{t=1}^{n} R_t^2}$$

其中：

Vol = 日间已实现波动率

360 = 一个常数，代表一年中大约的交易天数。

t = 代表每个交易日的计数

n = 测量时间框架内的交易天数

R_t = 按公式计算的连续复利日收益率。

实时 RealVol 公式

由于加密货币的持续交易特性，我们在得出每日间 RealVol 之后，需要进一步计算实时 RealVol。我们将以 30 天为周期，进行实时 RealVol 的计算。

RealVol 每日公式中描述的所有设计元素都与 RealVol 实时公式相同。要将每日值转换为实时值，需要从 RealVol 每日公式开始，然后合并当前的基础价格和加权方案。这样做可以在整个交易日内提供连续的更新，并向 CSA 持有者提供有用的实时指示，以实时了解最新的 30 日内，每日已实现的波动性。从

本质上讲，即使我们处于新的最近一天（“今天”）内任一时刻，VOL 也能衡量出 30 天的恒定已实现波动率。

举例来说，如果在当天（n + 1）的交易时间已经过了 80%，我们将使用最新的底层资产实时价格（Underlying Real-time Price，URP）来从昨天的 URP（n）中的对应（80%）部分计算当前日的收益（n + 1）。然后，取计算周期内的第一天，并将该天的收益率加权 20%（100%-80% = 20%）。通过这种方式，我们仍然可以得到 30 天内在任何时间点上实现的波动率的权重，即使实际上有 31 个回报--第 1 天的权重为 20%，第 31 天的权重为 80%，第 2 天至 30 天的权重为 100%。

注意：虽然当日的部分回报是自加权的，因此不需要额外的协同因子，但仍然需要计算当日的自加权部分，以便将适当的剩余权重应用于第 1 天的全日回报。为了计算出当日的权重，每天的当日时间要取到最接近的一分钟。由于一天有 1,440 分钟，所以在 RealVol 实时公式中使用当前时间和一天中的秒数来计算要应用到第 1 天的权重。

当一天的时间等于今天的收盘时间(n+1)时，现在第 n+1 天的权重为 100%，而第 1 天的权重为 0%。因此，由于其权重为 0，原来的第 1 天的收益率从计算中删除。原来的第 2 天现在变成了新的第 1 天，所有其他的日子也被重新编号。RealVol 实时公式在这个时间点（我们的例子中是中国标准时间每日 0 点收盘）简化为 RealVol 每日公式。在市场收盘后的瞬间，我们开始一个新的交易日，回报率被重新编号，这样又只有 30 个回报率，新的交易日的加权回报率为第 31 天。

$$\mathrm{Vol_R} = 100 \times \sqrt{\frac{360}{n}\left[\frac{1{,}440 - m}{1{,}440}R_1^2 + \sum_{t=2}^{n} R_t^2 + \mathcal{R}_{n+1}^2\right]}$$

其中：

1,440 = 一天中的分钟数

n+1 = 今天

m = 从最近一次收盘时间(第 n 天)开始，截至当日的最接近时刻(n+1)的分钟数

R_1 = 计算周期内第一天(第 1 天)的回报(从第 0 天收盘到第 1 天收盘)

R_{n+1} = 部分回报（使用当前的相关价格和前一天的相关参考价格的回报）。

注：为了澄清，花体"R"表示部分回报，其他所有回报均为全日回报。

启动充足率 $Q_{i,0}$ 和 $Vol_{i,R}$ 的关系

如果不加任何调节因子，始终保持 $Q_{i,0}$ 为一个固定值（例如 150%），则在市场波动的情况下，新开仓用户将暴露于极大的风险之中，在拥有了实时波动率因子后，我们可以将实时波动率的变化值与启动充足率建立如下关系式：

$$Q_{i,0,n} = 120\% + e^{(Vol_{R,i,n} - Vol_{R,i,n-1})}$$

其中：

n = 当前时刻

i = 特定资产种类，例如 ETH

$Vol_{R,i,n}$ = 当前采样点资产 i 的实时波动率

$Vol_{R,i,n-1}$ = 上一采样点资产 i 的实时波动率

上述关系式反映了波动率本身的变化值，及其对 $Q_{i,0}$ 的调节作用。我们将通过 QIAN 系统的运作对该公式进行持续检验，如果发现上述公式存在不足之处，原力协议项目团队保留通过社区治理程序进行修改的可能性。

4.3.4 加密资产平滑套利清算机制

QIAN 系统将根据 Vol_R 的值决定是否开启套利机制，系统鼓励在市场波动较低的情况下进行清算，以减缓市场短期恐慌情绪对 QIAN 系统稳定性的冲击。

在任意时间 t(i)，对于充足率 $Q_{i,t}$，QIAN 系统会存在以下几种 CSA 状态：

- 正常合同 CSA(normal)，$Q_{i,t} > Q_{i,alarm}$
- 预警合同 CSA(alarm)，$Q_{i,min} < Q_{i,t} \leqslant Q_{i,alarm}$
- 冻结合同 CSA(frozen)，$Q_{i,t} \leqslant Q_{i,min}$

对于不持有 CSA 的套利者，其赎回行为可能会导致 CSA 持有人的锁定资产减少。为了兼顾公平和效率，对于平滑套利清算的参与者而言，其在时刻 t(i) 可赎回资产的来源，将被限制在 CSA(frozen)。

在套利过程中，套利者将从储备资产 i 的整体冻结资产当中套利，具体来说，假设在 t 时刻，QIAN 系统有 100 个处于冻结状态的 CSA，这些 CSA 一共生成了 100,000 QIAN。此时，任意一个或 n 个套利者可以用不大于 100,000 QIAN 的清算资金，按照出资额大小，从清算合约里获得部分/全部冻结资产。在清算过程里，持有 CSA(frozen) 的所有用户都会按其被冻结资产占冻结 CSA 内总资产的比例分担损失。

所有处于 CSA(frozen) 中的储备资产都可以被套利者赎回，为了使自己不受损失，CSA(frozen) 的持有人必须抢先补充自己 CSA 里的储备资产，使其脱离冻结状态。无论是套利者的赎回操作还是 CSA(frozen) 持有人的补充锁仓，都能够有效的提升 QIAN 的资产储备充足率，让 QIAN 在储备资产不足的情况下尽快价值回归。

这种清算机制的设计既可以促使所有 CSA(frozen) 的持有者补充储备资产，也平滑了冻结资产的清算速度和数量，尽可能的减缓和减少单个用户所受的损失，因此，我们将这一机制命名为平滑套利清算。

当 QIAN 系统支持多种加密资产时，平滑套利清算机制将变得复杂。理论上，套利者可赎回系统中的任何一种符合清算条件的储备资产，各储备资产之间不存在清算的先后顺序。当套利者赎回加密资产时，系统实时动态呈现各加密资产的可赎回量。套利者在可赎回量的范围内赎回加密资产，将不会大幅改变整个系统加密资产的分布情况。

各种加密资产的可赎回量始终处在动态变化中，当质押资产 i 已经达到最大赎回比例 R_i 后，客观上提升了系统的整体储备充足率，此时质押资产 i 的套利操作受到最大赎回量的影响而暂停，由于 QIAN 是一个多抵押系统，对其他质押资产的套利活动仍将继续。

4.3.5 债务拍卖

在极端情况下，系统的全局资产充足率 Q_{total} 可能不足 100%，如果市场环境持续低迷，此时的清算套利过程将可能会不顺利，套利者的套利意愿不足。此时，系统内的储备资产价值不足，将产生整体债务。为了维持 QIAN 系统的内在价值，系统将解锁（unlock）治理代币 FOR 并通过拍卖的形式补齐整体各储备资产的差额，让系统的整体充足率回到安全线以上，恢复 QIAN 在极端行情下的内在价值。

对于债务拍卖的参与者而言，吸引他们参与债务拍卖的原因，是被解锁的 FOR 将以低于市场价的形式折价进行拍卖，在 QIAN 的债务拍卖中，会引入最大折价率 Δr。Δr 的初始值设置为 70%，具体数值将由社区充分讨论后通过投票进行修改。参与债务拍卖的 FOR 总量为：

$$\text{FOR total value in debt auction} = \frac{\text{Debt balance}}{\Delta r}$$

FOR 的拍卖中，起拍价

$$p(\text{start}) = \frac{\text{market price(FOR)}}{\text{market price(i)}} \times \Delta r$$

拍卖参与者以资产 i 作为报价和结算标的，最终成交价 i(final) 为：

$$i(\text{start}) \leqslant i(\text{final}) \leqslant i(\text{market})$$

拍卖所得的资产 i 将用于弥补系统债务差额，若有剩余，则会锁定到拍卖盈余合约，以备未来所需。

4.3.6 全局清算

虽然我们长期看好加密资产的发展，但是我们也必须要正视这样的一个现状：加密资产仍然处于整体发展的早期，市场暴涨暴跌时常出现，在过往的市场记录中也曾出现过长达数年的熊市。

虽然 QIAN 稳定币有着一系列的稳定机制，但是仍然有可能在发生市场极端行情并且市场长期低迷的情况下，即使通过债务拍卖也仍然无法弥补整个系统的储备资产充足率。如果发生了这种情况且持续一段时间，将意味着整个 QIAN

稳定币系统丧失了内在价值的支撑，我们在这种情况下，将通过社区治理的流程，探讨是否进行全局清算并且关闭 QIAN 稳定币系统。一旦社区治理通过了 QIAN 稳定币系统的关闭议案，则将会启动全局清算。

在全局清算状态下，QIAN 稳定币系统将会首先冻结所有 CSA，关闭 CSA 的生成功能，其次关闭预言机喂价，并且以最后一次预言机喂价的价格作为系统全局清算的参考报价。此时，系统状态再次发生改变，以最后一次预言机报价为准，持有 CSA(normal) 的用户将能够优先向合约赎回自己的锁定资产，系统将处理这部分用户的资产赎回操作。在 CSA(normal) 的持有用户赎回资产完成之后，系统内如果仍然存在储备资产的剩余，则将允许 CSA(alarm) 的持有用户进行赎回。

在全局清算状态下，用户是否能够拿回全部锁定资产，不受到损失，这是不确定的。能够全额赎回锁定资产的概率，依次为 CSA(normal) ＞ CSA(alarm)，不同的底层储备资产的数量、市价等因素会对赎回成功的概率形成综合影响。

4.3.7 QIAN 系统治理

QIAN 系统的主要参与者包括 QIAN 铸造者，QIAN 持有者及治理代币 FOR 的持有者。系统治理的目的在于平衡所有参与者的利益关系，在一定权衡和取舍的基础上，维持系统的稳定和持续健康发展。

QIAN 铸造者在系统中主要承担的风险是储备资产价格下跌，系统锁定后导致的赎回风险，享受的利益包括获得流动性、价值贮藏、风险对冲等功能。基于对行业中类似方案的研究，我们认为，在合理的风险范围内，QIAN 的铸造应该是被鼓励的，这有利于 QIAN 系统的发展，所以我们设计了可调整的利息机制。QIAN 持有者的核心诉求在于其汇率稳定性，因此我们设计了汇率稳定调节机制。

FOR 持有者将是整个系统最后收益或风险的承担者，平台的管理是通过 FOR 持有者进行投票确定的，被投票选中的提案可以修改 QIAN 平台的内部管理变量，这些变量包括但不限于：

- 增加新的储备资产
- 选择可信任的预言机
- 调整利息
- 调整闪电贷利率
- 风险参数：每种储备资产的债务上限、初始锁定比例、可赎回上限、预警线等。

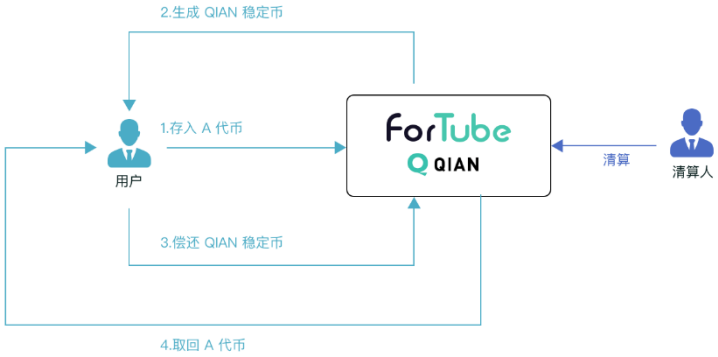

图 5 QIAN 价值流向

5 生态扩展

当前，原力协议已基本完成以太坊上的 DeFi 技术组件，以及债券融资、货币借贷、去中心化稳定币等代币化协议的开发。未来，我们将扩展这些代币化协议至其他区块链系统，包括 ETH2.0、币安链和波卡等。

5.1 Ethereum 2.0

ETH 2.0 是新一代以太坊。它是一个完全不同的项目，在区块链的架构上采用了全新的思路。ETH 2.0 的目标是提高以太坊的可扩展性、安全性和可编程性。不同于 ETH 1.0 只能达到 15 TPS 的吞吐量，ETH 2.0 每秒可处理上千至上万笔交易，同时不用降低其去中心化程度。

ETH 2.0 是一个巨大的飞跃，它的分片技术将有可能使得主流链锚定币成为可能，那它事实上将成为一个连接所有区块链的跨链系统。如果 ETH 2.0 做到了这一点，再结合它的高并发事务执行能力和 PoS 特性，也将成为跨链平台的典范。

原力协议将会充分利用 ETH 2.0 在技术上的巨大优势，第一时间随着主链的升级，把当前应用平滑迁移到最新的稳定版本上，紧跟以太坊升级的步伐，引领 DeFi 金融平台业务模型和技术升级的发展趋势。

另外，基于以太坊 2.0 的 POS 特性，用户的 ETH 资产锁定到 QIAN、Bank 等智能合约将仍能获得 ETH 挖矿奖励，QIAN、Bank 等合约在未来可以形成类似于矿池的功能，同时继续提供原有的金融服务，让用户的 ETH 资产进行最大化利用，创造更多的价值。

5.2 币安链及币安智能链

币安链（Binance Chain）是一个由社区驱动的区块链软件系统，由全球各地的开发者和贡献者组成。它是一条专注转账和交易区块链资产的公链，着重于性能、易用性和流动性。是一条为 DEX 量身打造的交易公链。币安链推出了 BEP2 代币标准，可在其上发行自定义的代币。尤其是币安链已支持主流代币锚定币，如 BTC、ETH、XRP、BCH、LTC、TRX。这些锚定币再配合币安链基于 Cosmos 的跨链特性，就给原力协议的跨链 DeFi 金融应用提供了无限想象空间。

2020 年，币安链的开发团队发布了通过并行链扩展币安链功能的方案：币安智能链。该方案在保留币安 DEX 的高性能撮合的前提下，实现对开发者友好的智能合约功能。

结合币安链的秒级事务和高 TPS 特性，BEP2 主流锚定币，以及币安智能链的 EVM 兼容性，原力协议在以太坊上的 DeFi 应用可以无缝拓展到币安链和币安智能链生态体系中。届时，基于币安链生态，通过主流代币的价值互换，高并发的金融交易，兼容良好的虚拟机，ForTube 将会成为重要的跨链 DeFi 金融平台。

5.3 波卡

波卡是一个允许不同区块链以一种无信任成本的方式传输消息、数据、价值的平台。可以同时共享它们的独特功能和安全性。简单来说，波卡是一种可扩展的异构多链技术。波卡是独立跨链技术的引领者，它的中继链、平行链和转接桥理念，可能将成为通用跨链技术事实上的标准。通过波卡跨链体系，主流链将会通过跨链机制进行良好的代币价值互换和事务协同。

原力协议将会对波卡进行持续深入的研究和实践，基于波卡体系进行原力协议应用的原型验证和适应性开发。随着波卡系统的完善和逐步上线，原力协议将考虑把 ForTube 体系逐步拓展到波卡生态中，在跨链金融应用赛道上保证持续的竞争领先地位。

6 原力协议生态代币

6.1 FOR 代币用途

6.1.1 参与 ForTube Bond 评级投票

社区评级人持有原力协议生态代币 FOR 即可参与债券信用评级。投票人了解债券发行信息后，将 FOR 锁仓至投票等级，评级结束后即可解除 FOR 锁定。

专业评级由专业信用评级机构或专业人士进行。成为专业评级机构或个人需要向 ForTube 运营方提交申请（后期审批权将会被移交给 ForTube 社区），提供能够证明专业能力和资质的材料，并向系统锁仓 100 万 FOR 代币。锁仓代币在评级期间以及所评级项目存续期间不可取回。

6.1.2 参与 QIAN 的稳定性调节

通过闪电贷，锁定在 QIAN 智能合约里的加密资产可以获得额外的收益，QIAN 系统的管理委员会将定期的使用获得的收益在市场上买入 FOR 代币，FOR 作为 QIAN 智能合约收益的价值贮藏载体，将被锁入保存 QIAN 系统收益的智能合约。当 QIAN 系统认为需要激励铸币者以提升 QIAN 的流通量时，系统会支付利息给新创立 CSA 的用户，支付的利息以 FOR 代币的价值进行计算，发放的利息也是 FOR。

6.1.3 参与 QIAN 的全局债务拍卖

在极端情况下，QIAN 系统的全局资产充足率可能不足 100%，如果市场环境持续低迷，套利者的套利意愿不足，进而导致系统内的储备资产价值不足，将产生整体债务。为了维持 QIAN 系统的内在价值，系统将解锁（unlock）治理代币 FOR 并通过拍卖的形式补齐整体各储备资产的差额，让整体充足率回到安全线以上。

6.1.4 参与 ForTube 的治理

ForTube 平台的治理是通过 FOR 持有者投票进行的，被投票选中的提案可以修改和调节 ForTube Bond、ForTube Bank、QIAN 的系统关键变量。

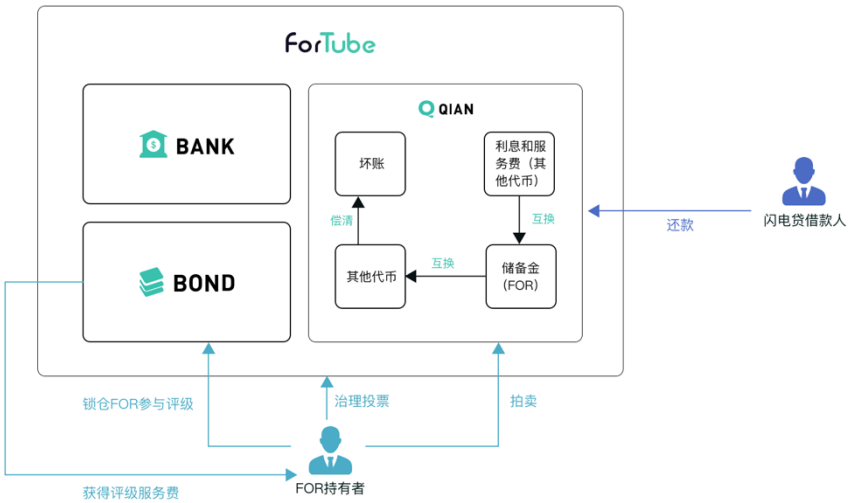

图 6 FOR 代币功能

6.2 FOR 代币分配计划

FOR 代币总量 10 亿，永不增发。在原力协议发起团队主导下，将会有 85% 的 Token 用于社区建设和社区捐赠计划，其中社区生态建设占 30%，原力协议

基金会占 25%，战略投资者及社区捐赠占 30%。剩余 15%的 Token 将为原力协议创始团队和 ForTube 开发团队预留，作为他们在项目初期做出贡献的奖励，以及作为后续新团队成员的激励。分配给团队的 token 锁仓 3 年，首次公开交易后 12 个月释放 30%，24 个月后释放 30%，36 个月后释放 40%。FOR 代币分配比例如下图所示。

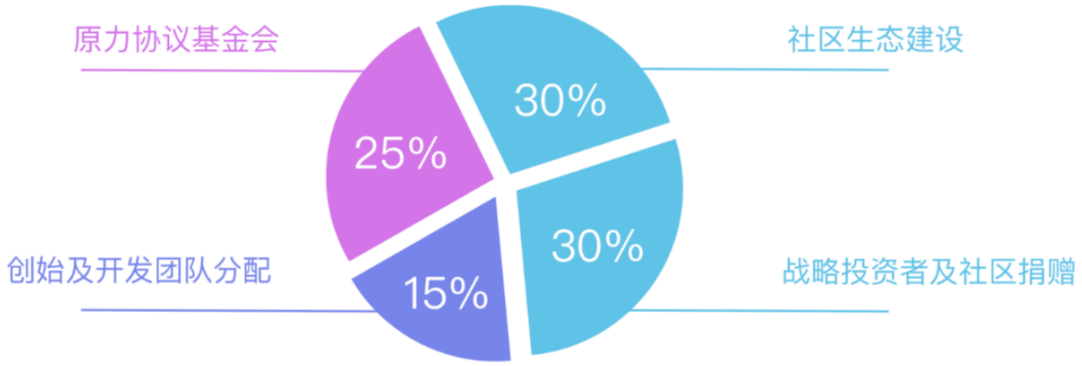

图 3 FOR 代币分配情况

6.2.1 社区生态建设

社区生态建设包括但不局限于:原力协议区块链应用(ForTube)生态治理和激励、开发者社区建设、商业合作和产业合作、市场营销推广、学术研究、教育投资、法律法规等。

6.2.2 原力协议基金会

我们已经在新加坡注册非营利性原力协议基金会，该基金会主要任务是负责原力生态的搭建和运营、开发战略方向的制定、FOR 代币发行及管理等，公开透明地管理由代币捐赠而获得的资金。

6.2.3 战略投资者及社区捐赠

根据项目发起及运营需求，我们将会预留 30%的代币回馈战略投资者及社区成员的资助。基石轮投资由团队创始成员们自筹资金完成，出于对项目的长期看好和自我激励，团队决定在基石轮所投入的资金对应的 FOR 代币永不解锁。

7. 研发路线图

2018 年 6 月，项目启动，白皮书设计，官网上线；
2018 年 12 月，推出中心化点对点借贷产品—币币贷；
2019 年 2 月，推出基于 EOS 的试验性借贷 DApp；
2019 年 4 月，项目代币 FOR 在公开市场开放交易；
2019 年 6 月，上线基于 Ethereum 的点对点借贷 DApp—Pawn；
2019 年 11 月，在 Pawn 内上线 Bank 借贷功能；

2019 年 12 月，上线去中心化稳定币 QIAN，支持 Ethereum 网络；

2020 年 3 月，推出加密数字债券 DApp — ForTube Bond；

2020 年 6 月，将借贷、稳定币、债券集成至 ForTube，形成一站式 DeFi 平台；

2020 年 7 月，稳定币 QIAN 2.0 上线；

2020 年 9 月，推出 DeFi 应用安全协议组件；

2020 年 12 月，与其他公链合作 ForTube 业务，如 Binance Chain、Polkadot 等；

2021 年 3 月，在无法获得银行服务的东南亚地区用户中推广 QIAN 的使用；

2021 年 6 月，推出实体企业加密债券试点业务；

2022 年 3 月，QIAN 稳定币开放技术联盟成立，发展 QIAN 稳定币全球合作伙伴。

参考文献

An Introduction to Smart Contracts and Their Potential and Inherent Limitations [EB/OL].https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

Implementation of Smart Contracts Using Hybrid Architectures with On- and Off-Blockchain Components [EB/OL].https://arxiv.org/pdf/1808.00093.pdf

Robert Leshner and Geoffrey Hayes. Compound: The Money Market Protocol [EB/OL]. *https://compound.finance/documents/Compound.Whitepaper.pdf*

MakerDAO. The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System [EB/OL].*https://makerdao.com/en/whitepaper*

Wikipedia. Federal Reserve [EB/OL].*https://en.wikipedia.org/wiki/Federal_Reserve*

Wikipedia. United States Treasury security [EB/OL].*https://en.wikipedia.org/wiki/United_States_Treasury_security*

Fedreal Reserve Bank of New York. How Currency Gets into Circulation [EB/OL].*https://www.newyorkfed.org/aboutthefed/fedpoint/fed01.html*

Wikipedia. Quantitative easing [EB/OL].*https://en.wikipedia.org/wiki/Quantitative_easing*

Wikipedia. 香港外匯基金 [EB/OL].*https://zh.wikipedia.org/wiki/香港外匯基金*

MBA 智库·百科. 货币发行制度 [EB/OL].*https://wiki.mbalib.com/wiki/货币发行制度*

香港金融管理局. 强方兑换保证 [EB/OL].*https://www.hkma.gov.hk/gb_chi/news-and-media/insight/2005/05/20050519*

香港金融管理局. 外汇基金资产负债表摘要及货币发行局帐目 [EB/OL].https://www.hkma.gov.hk/gb_chi/news-and-media/press-releases/2018/04/20180430-4/

潘攀（北京大学金融法研究中心）. 港币的发行及其稳定机制 [J]. 金融法苑, 1999, 14（总第二十六期）: 52 页

朱孟楠. 香港外汇基金的发展及投资策略的选择 [J]. 国际经济合作, 1997, No.6: 39~42 页

Prashant Bhayani & 谭慧敏（香港首席投资策略师）. 为何我们不担心港币联系汇率制度 [EB/OL].*https://wealthmanagement.bnpparibas/asia/cns/news/hkd-peg.html*

瞿新荣. 美联储重启扩表，美元发行的逻辑与油价 [EB/OL].*https://www.guancha.cn/QuXinRong/2019_10_13_521093_s.shtml*

中信期货研究员 姜沁. 美国国债的规模管理体制、发行体制以及流通管理体制 [EB/OL].*https://finance.sina.com.cn/money/forex/forexroll/2018-10-19/doc-ifxeuwws5814324.shtml*

中国金融期货交易所. 美国国债期现货市场研究报告 [EB/OL].*http://yjs.dwfutures.com/uploadfiles/2013/8/20130806142789838983.pdf*

DAppTotal. 稳定币 [EB/OL].*https://dapptotal.com/stablecoins*

CEIC. 中国香港特别行政区 外汇储备 [EB/OL].*https://www.ceicdata.com/zh-hans/indicator/hong-kong/foreign-exchange-reserves*

CEIC. 中国香港特别行政区 货币供应 M1 [EB/OL].*https://www.ceicdata.com/zh-hans/indicator/hong-kong/money-supply-m1*