

ForTube

DeFi 借贷市场

白皮书 V1.0

摘要： ForTube 是基于原力协议 DeFi 技术组件开发的 DeFi 平台，致力于为全球加密数字资产爱好者提供去中心化的借贷服务，ForTube 支持全球绝大部分热门资产，用户可随存随取、随借随还。

目录

1 FORTUBE 简介	1
1.1 DEFI 技术组件.....	1
1.2 代币化协议.....	1
2 FORTUBE 的 DEFI 技术组件	1
2.1 基础组件 APEC.....	1
2.1.1 设计理念.....	1
2.1.2 架构图.....	2
2.1.3 技术构架.....	2
2.1.4 资产安全.....	3
2.2 扩展组件 BEAMS.....	4
2.2.1 区块链的局限性.....	4
2.2.2 设计理念.....	4
2.2.3 BEAMS 架构图.....	5
2.2.4 技术架构.....	5
2.3 金融组件.....	6
2.3.1 DeFi 金融安全三定律.....	6
2.3.2 GEL.....	6
2.3.3 CALM.....	6
2.3.4 MAK.....	6
3 FORTUBE BANK	7
3.1 设计思路.....	7
3.2 利率模型.....	8
3.3 利率计算.....	8
3.4 健康指数.....	8
3.5 资产分区.....	9
4 FORTUBE BOND	9
4.1 债券信用评级.....	9
4.2 BOND TOKENS.....	10
4.3 债券清算.....	11
4.4 债券交易市场和债券衍生品.....	11
4.5 BOND 模块社区治理.....	12
5 公链生态建设	13
5.1 以太坊 2.0.....	13
5.2 币安智能链.....	13
5.3 波卡.....	13
5.4 其他公链.....	13
6 FORTUBE 的治理代币	14
6.1 FOR 代币用途.....	14

6.1.1 参与 ForTube Bond 评级投票.....	14
6.1.2 参与 ForTube 的治理.....	14
6.2 FOR 代币分配计划.....	14
6.2.1 社区生态建设.....	15
6.2.2 基金会.....	15
6.2.3 战略投资者及社区捐赠.....	15
7. 研发路线图.....	15
参考文献.....	16

1 ForTube 简介

ForTube 是原力协议开发的去中心化金融服务平台，包括 ForTube Bank 和 ForTube Bond 两大模块。ForTube Bank 是算法驱动的加密数字银行，支持随存随取，随借随还。ForTube Bond 是一站式加密数字债券发行和投资平台。

ForTube 基于原力协议开发。原力协议是在主流区块链系统上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。

1.1 DEFI 技术组件

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。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。

1.2 代币化协议

在 DeFi 技术组件的基础上，可进一步开发债券融资协议、货币借贷协议和去中心化稳定币协议。

- **债券融资协议:** 固定期限、固定利率的数字货币借贷服务;
- **币币借贷协议:** 由算法驱动的活期、可变动利率的代币存借服务;
- **去中心化稳定币协议:** 加密资产储备型去中心化稳定币协议。

2 ForTube 的 DeFi 技术组件

2.1 基础组件 APEC

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

2.1.1 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

2.1.2 架构图

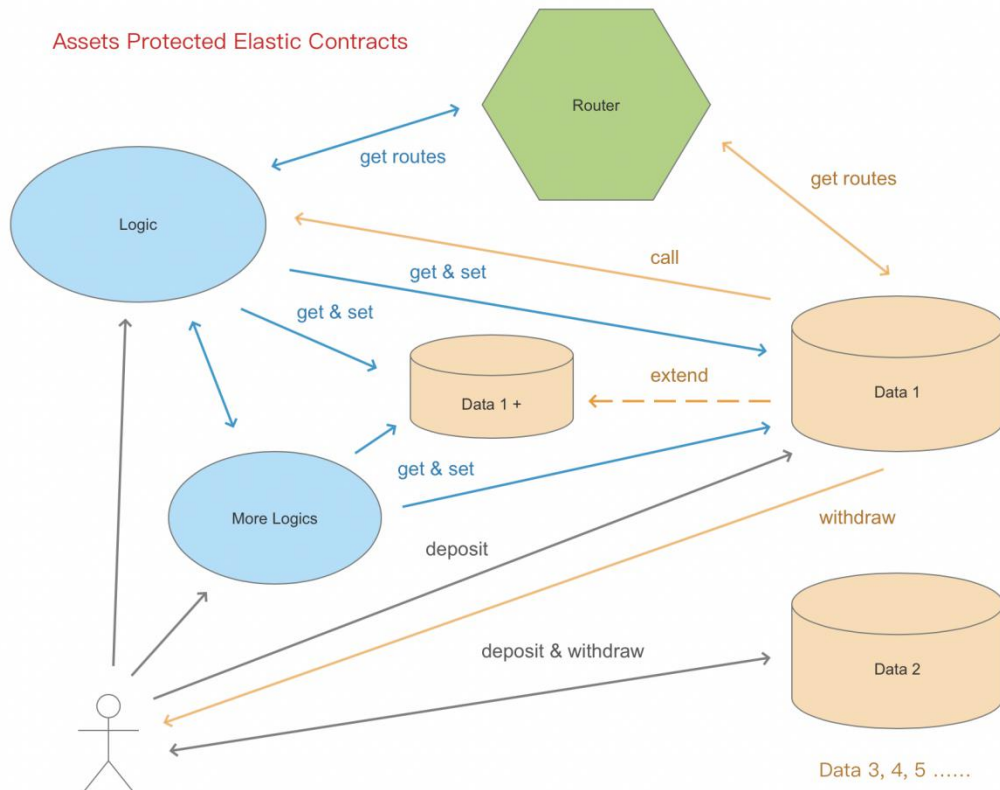


图 1 APEC 技术架构图

2.1.3 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，非必要不使用数据扩展机制。

2.1.4 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 and 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)。

2.2 扩展组件 BEAMS

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

2.2.1 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。

2.2.2 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

2.2.3 BEAMS 架构图

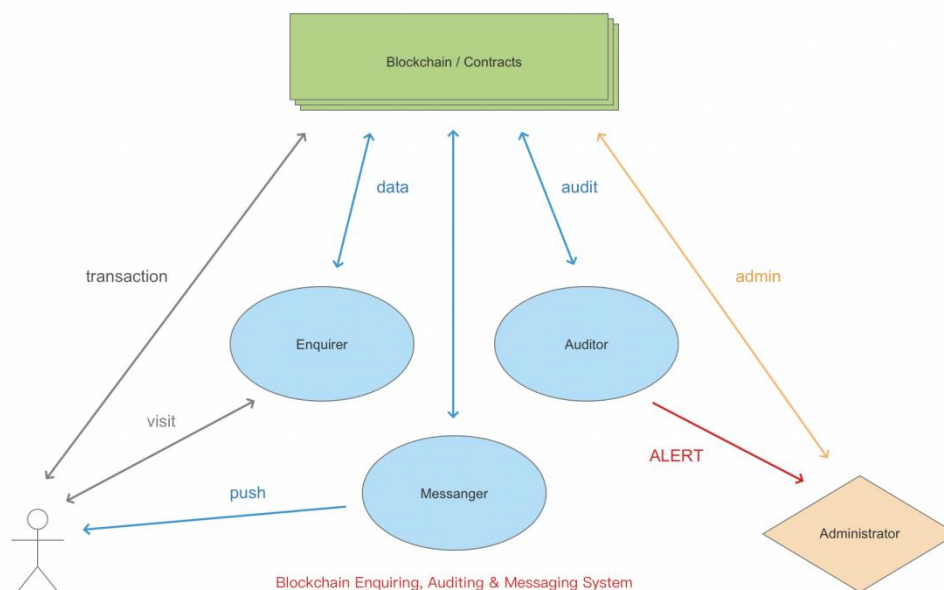


图 2 BEAMS 技术架构图

2.2.4 技术架构

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

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。

2.3 金融组件

2.3.1 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。

2.3.2 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。

2.3.3 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。

2.3.4 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。

3 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。

3.1 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。

ForTube Bank 的几个核心概念：

存币：用户通过 Bank 的“存币”功能，将平台支持的数字资产转给智能合约托管，获取利息收入。用户进行“存入”操作时，存入的资产会先偿“该种资产”的借款（若有），资产净额可获得存款利息；

取币：用户对某种代币的“可取数量”，包含对该种代币的“存入数量”，以及以其他存款资产为抵押担保的“可借数量”。若取出后产生负债，将产生借币利息；

最大借存比：借款和存款价值的比例，代表特定抵押的最大借款能力。例如，如果最大借存比为 75%，则价值 100 的存款，以此为抵押最多可借出 75。

最大安全可借：假设用户 i 资产存款价值为 V_i ， $V_i = i \text{ 数量} \times i \text{ 价格}$ ，该资产最大借存比为 F_i ，则用户的最大借款能力为 $\sum (V_i \times F_i)$ 。若用户按最大借款能力

借出，则面临被清算的风险，因此，我们将用户最大剩余可借乘以一个小于 1 的系数 MAX（比如 0.8），即最大安全可借 = $\sum (V_i \times F_i) \times \text{MAX}$ 。

3.2 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（即使用率），其公式为：

$$x \text{ (使用率)} = \frac{\text{资产的借出总额}_a}{\text{特定资产剩余可借总额}_a + \text{特定资产的借出总额}_a}$$

设借款利率为 y ， y 和 x 的关系可以用如下函数表示：

$$y = \text{最低借款利率} + \text{斜率} \times \text{使用率}$$

相对应地，存款利率 SIR 公式为：

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

其中，

x = 资产 a 的借出比率；

y = 资产 a 的借款利率；

s = 调整比率， $0 \leq s < 1$ ，一般可取 0.2。

3.3 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 t_0 ，还款时刻为 t_1 ，则到期应还本息和为

$$BA \times \frac{r_{t_1}}{r_{t_0}}$$

存款利率和利息计算公式类似。

3.4 健康指数

与一般的质押借贷不同，ForTube 的各种资产支持互相作抵押进行借贷，因此单个资产的质押率和清算线等策略已经不适用。因此，ForTube 引入健康指数这个概念。健康指数是一个用来反映用户的债务健康程度的数值，这个数值越高，被清算的可能性越低，资金的安全状态越高。

健康指数 H 定义如下：

$$H = \sum (V_i \times F_i) \div \text{Debt}$$

当用户按最大借款能力借出时， $H=1$ ；若价格波动使得 $H < 1$ ，用户资产将被清算。

当用户按最大安全可借借出时， $H=1.25$ 。

因此，

当 $H > 1.25$ ，表明用户债务相对安全；

当 $1 \leq H < 1.25$ ，表明用户债务处于预警状态，用户应该增加质押物或者偿还部分债务；

当 $H < 1$ 时，用户资产处于被清算状态。

3.5 资产分区

目前，ForTube Bank 包括以太坊资产区和币安智能链资产区。以太坊资产区不仅支持 ETH、HBTC、WBTC、USDT、USDC、DAI 等主流资产，也支持 YFI、UNI、LINK 等热门 DeFi 资产。币安智能链资产区同样支持 LTC、EOS、BCH 等传统经典资产和 YFI、YFII、DOT、FIL 等创新型资产。未来，ForTube Bank 将根据资产类别开放稳健资产区（仅支持 BTC、ETH、USDT、USDC 等稳健资产），全球新兴资产区（全球热门潜力资产）等。

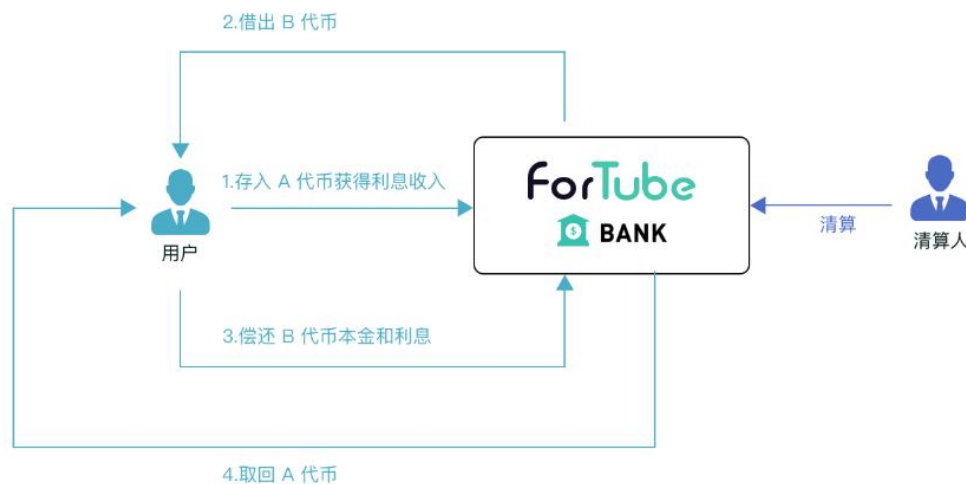


图 3 ForTube Bank 价值流向

4 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 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。

4.2 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。

4.3 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-Discount) 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

$$CCR \leq 70\% \times TCR$$

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

$$AC \times Price \times Discount \geq CD$$

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

$$AC \times Price \times Discount \geq CD$$

时，

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

剩余质押物数量 (AC-X)，发债人可取回。

4.4 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。

4.5 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。

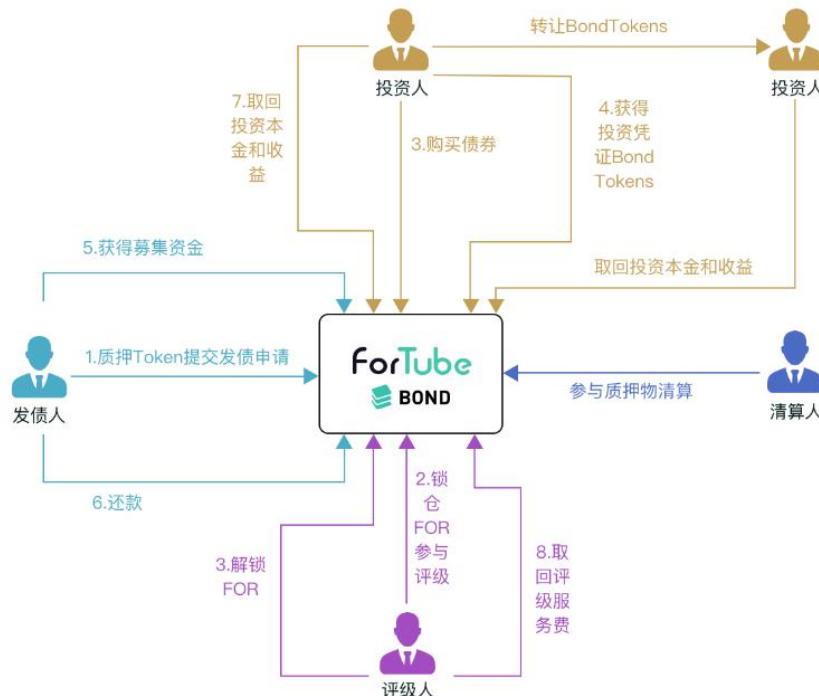


图 4 ForTube Bond 价值流向

5 公链生态建设

当前，ForTube 已在以太坊上线了 ForTube Bank 和 ForTube Bond，在币安智能链上线了 ForTube Bank，市场规模跻身全球借贷平台前列。

5.1 以太坊 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。

ForTube 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 Bank 等智能合约将仍能获得 ETH 挖矿奖励，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 币安智能链

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。ForTube 将继续在币安智能链生态体系中发力，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。随着波卡系统的完善和逐步上线，ForTube 将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。

5.4 其他公链

随着 DeFi 受到加密世界的认可，各大公链都纷纷宣布了自己的 DeFi 生态发展计划，ForTube 未来将与更多的公链进行合作，支持不同公链的 DeFi 生态发展，满足 ForTube 平台用户的多样化需求。

6 ForTube 的治理代币

ForTube 的治理代币为 FOR，用户可通过 FOR 代币参与 ForTube 的治理，ForTube 团队将追求 ForTube 治理的完全去中心化，通过全体 FOR 持币人的努力，将 ForTube 建设成优秀的 DeFi 基础设施。

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，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 ForTube 的治理

ForTube 平台治理将由 FOR 长期爱好者参与，参与治理可获得平台手续费奖励。将 FOR 锁定到 ForTube Staking 合约可获得治理投票代币 GFOR，GFOR 按 FOR 锁定数量的一定比例发行，GFOR 仅能用于治理投票，并在用户赎回 FOR 时被销毁。被投票选中的提案可以修改和调节 ForTube Bond、ForTube Bank 的系统关键变量。



图 5 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。

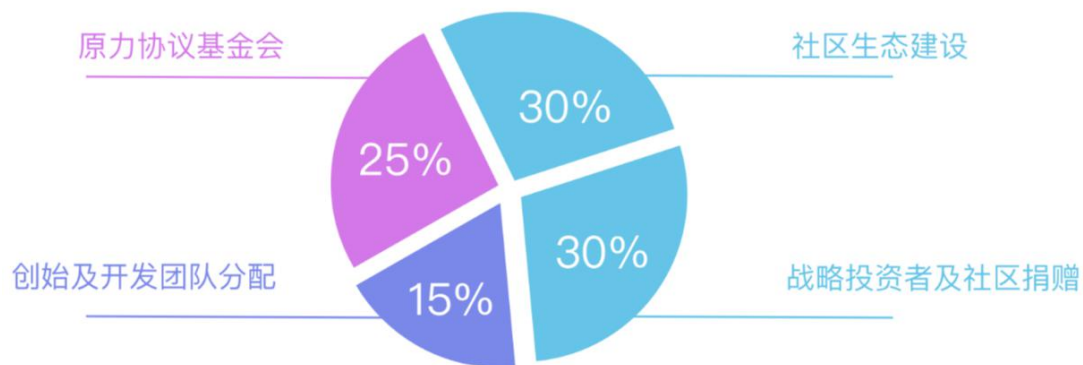


图 6 FOR 代币分配情况

6.2.1 社区生态建设

社区生态建设包括但不限于: 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 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, 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

- 2020 年 3 月, 推出加密数字债券 DApp — ForTube Bond;
- 2020 年 6 月, 将借贷、债券集成至 ForTube, 形成一站式 DeFi 平台;
- 2020 年 9 月, 同时在以太坊和币安智能链上发布 ForTube Bank V2.0;
- 2021 年 6 月, 与其他公链合作 ForTube 业务, 如 Polkadot、Cosmos 等;
- 2021 年 12 月, 推出实体企业加密债券试点业务。

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

Federal 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

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>