原力协议白皮书

（新版草稿）

目录

1. 背景

1.1. 当前全球金融存在的问题

金融是现代经济的血脉，推动着社会各个行业迅猛发展。但是，金融追逐利益和规避风险的天性致使全球金融服务极不平衡。

- 2008 年，因银行审贷失职，以次级抵押贷款引发历史以来全球最大金融海啸；
- 收益最大化原则促使金融机构明显偏好于服务大型企业和中产消费群体，中小企业融资难问题十分普遍；
- 以发薪日贷为代表的掠夺性贷款，以及高利贷、欺诈骗贷等问题严重；
- 世界银行报告显示，全球约 17 亿成年人没有银行账户；
- 国际货币基金组织(IMF)估计，在 2018 年有 11 个国家的通胀率达到了 20%甚至更高。

针对全球金融存在的问题，世界主要国家、经济体以及国际组织对当前的金融监管体系进行了反思，并针对其弊病提出了各种改革方案。比较有代表性的包括国际清算银行主导的巴塞尔协议和金融市场基础设施原则（Principles for Financial Market Infrastructures，简称 PFMI）。联合国于 2005 年提出普惠金融概念，“以可负担的成本为有金融服务需求的社会各阶层和群体提供适当、有效的金融服务，小微企业、农民、城镇低收入人群等弱势群体是其重点服务对象。”同时，科技也成为推动金融变革的强大动力。

1.2. 从 FinTech 到 DeFi

金融科技的发展历程

金融科技起源于金融机构信息化建设，科技公司为金融机构提供技术服务。这是“金融科技 1.0”。这一阶段，金融科技的目的是实现办公和业务的电子化和自动化，从而提高业务效率，科技公司通常并没有直接参与公司的业务环节。

2008 年全球金融危机后，金融科技进入了新的发展时期。一些科技公司开始涉足传统金融服务的某些领域，开始与传统金融公司展开竞争。到 2014 年，以 Lending Club IPO 成功为代表，大量金融科技公司成功闯入金融领域，金融科

技产业逐渐壮大。在这个阶段，科技公司搭建在线业务平台，以去中介化为主要特征，利用互联网或者移动互联网实现金融业务中的资产端、交易端、支付端、资金端的互联互通，实现信息共享和业务融合，其中最具代表性的包括互联网的基金销售、P2P 网络借贷、互联网保险。我们可以称之为“金融科技 2.0”。

目前，以大数据、人工智能和区块链为典型代表的新技术正在推动“金融科技 3.0”的发展。其中，区块链技术最具颠覆性。

分布式金融(DeFi)

2014 年，以太坊诞生，区块链技术开始逐步引起全球金融和科技行业的注意。2015 年 12 月 Linux 基金会在主导发起 Hyperledger 项目，截止 2019 年 7 月，成员数达 270 余家，包括金融，银行，物联网，供应链，制造和科技行业的领头羊。传统金融和科技巨头也纷纷尝试数字货币区块链应用，2019 年 2 月 14 日，JP Morgan 宣布推出稳定币——JPM Coin；2019 年 5 月 18 日，Facebook 发布加密货币项目 Libra 白皮书，联合数十家知名金融机构和在线商户，计划推出基于加密货币的支付系统。2019 年 8 月，中国人民银行宣布即将推出央行数字货币。

我们认为，只要利用到区块链分布式账本技术的金融服务都可以统称为分布式金融（Decentralized Finance， DeFi），包含以下两个方面：

第一、纯分布式账本技术应用，即无币区块链应用。对于金融行业来说，区块链技术中的分布式存储、数据不可篡改、不可抵赖、可追溯等特性，与金融行业对信息和数据安全，交易数据溯源等业务的需求高度契合。因此，区块链技术在金融行业的典型应用场景包括贸易融资、供应链金融、资产证券化、跨境支付与清算等等。

第二、包含数字货币的区块链应用。该类应用主要依托智能合约，使用数字货币或上链资产等通证化的加密数字资产开发产品，产品类型包括借贷、稳定币、交易所、预测、保险、期权等。

1.3.分布式金融的前景和机遇

当前，全球加密数字货币市值约 2000 亿美元，而最高时达 8300 亿美元。然而同链下资产相比，这仅仅是沧海一粟。链下数字资产和实物资产的通证化是区块链技术发展的重要方向。我们相信，随着越来越多的资产转移到区块链上，分布式金融将成为未来的主流。

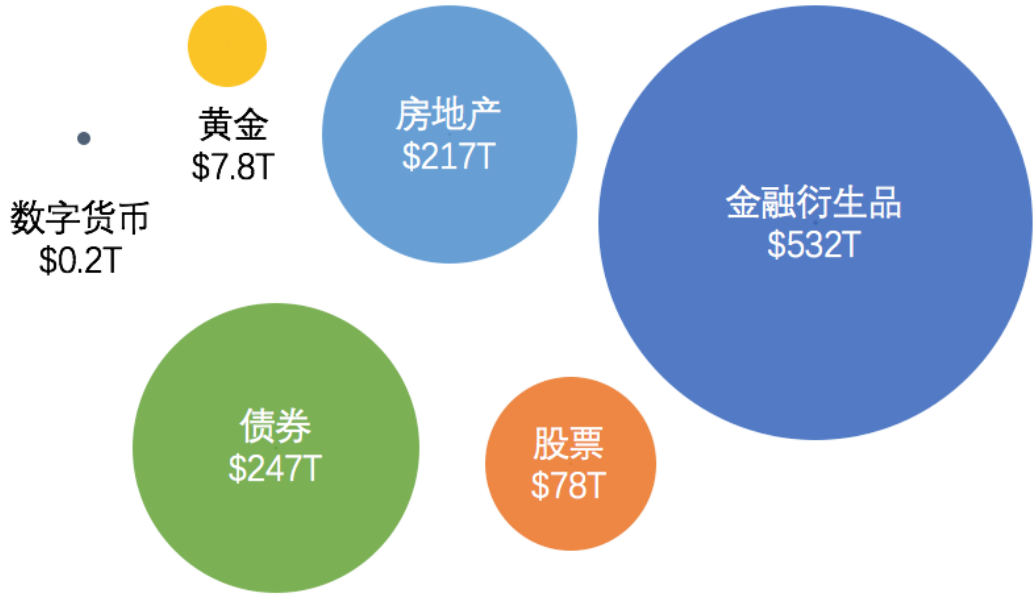

图 1 各类资产规模对比

1.4. 分布式金融面临的问题和挑战

目前，借鉴传统金融，分布式金融领域出现了一些新的尝试，诸如交易所、借贷、债券、金融衍生品、量化投资等。但普遍存在市场较小，体验较差，开发难度大等问题。面对复杂的区块链技术，很多市场参与者望而却步。分布式金融广阔的发展前景与区块链技术的不成熟之间存在着巨大的鸿沟。

具体而言，分布式金融从技术角度存在如下的问题：

- 隐私保护和数据共享存在矛盾
- 数字资产无法实现有效跨链流通
- 金融产品规则复杂，合约构建难度大
- 缺乏可靠的预言机将链上链下数据和计算资源打通
- 缺少一条能够真正承载金融应用的专属公链

2. 我们的定位

传统金融在企业早期融资服务、普惠金融服务、中小企业金融服务等方面十分欠缺，在网络借贷、跨境贸易、供应链金融、资产证券化等方面也存在明显的提升空间。而正好，区块链技术具有解决传统金融问题和不足的潜力，极有可能

在金融行业推动深刻变革。在此背景下，原力协议看到分布式金融的广阔前景，立志于搭建加密数字金融的基础设施，推动人类开放金融和普惠金融事业的发展。

原力协议是一个开源的分布式加密数字金融开放平台，向加密数字金融服务应用开发者提供基于跨链技术的解决方案。原力协议将基于当前主流公链及原力协议金融公链，通过对加密数字金融业务通用模块的抽象和封装，以 SDK 及 API 的形式对外提供服务。

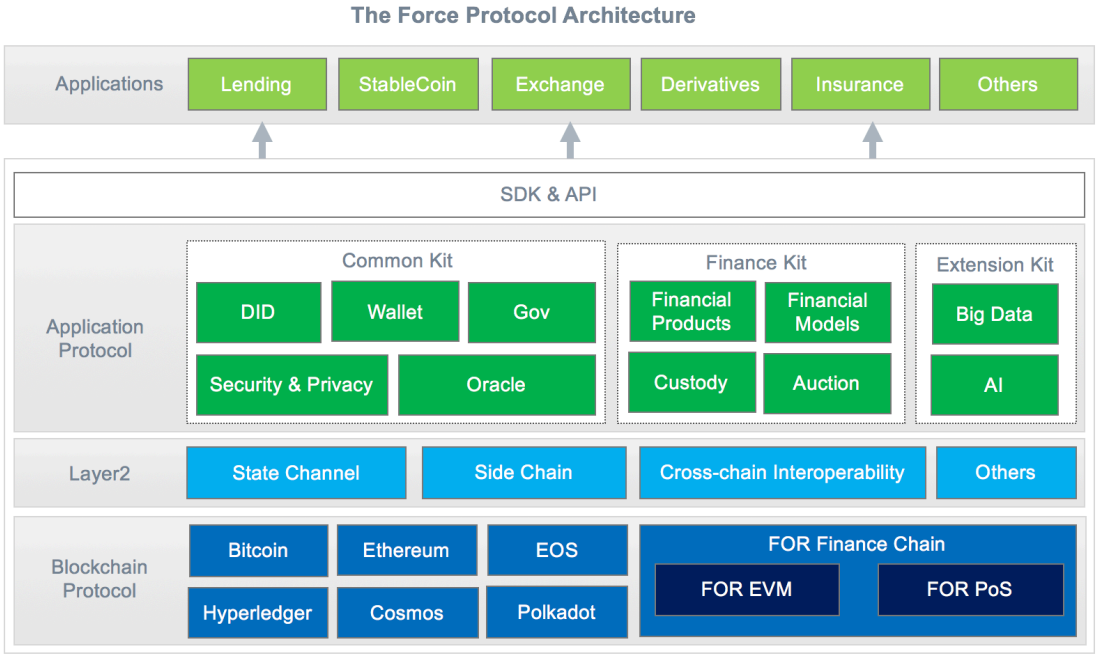

图 2 原力协议系统架构图

具体而言，原力协议致力于区块链技术协议开发，具体如下：

区块链协议层

当前，区块链技术还缺乏统一标准，各区块链生态也具有一定开发者和用户，为了更好的提供技术服务，原力协议首先将在主流公链和联盟链开发应用协议层以及孵化去中心化金融应用。支持的区块链平台包括 Bitcoin、Ethereum、EOS、Hyperledger、Cosmos、Polkadot、RSK、ETC 等等。同时，原力协议将设计适合金融业务的共识协议，并结合 Layer2 层对扩展性和跨链互操作的支持，提供安全、可靠、高性能的金融区块链解决方案。

应用协议层

应用协议层向应用层封装网络通信，协议编解码，异常处理等细节，暴露友好的面向对象的功能接口，应用服务面向接口编程，专注于实现业务逻辑，而不需要承担区块链底层技术实现的开销。

金融业务种类繁多，规则非常复杂，通过对金融业务的抽象，原力协议在协议层设计基本组件、金融组件和扩展组件三部分。

- 基本组件：分布式数字身份、钱包、安全与隐私保护、治理和预言机。
- 金融组件：金融产品、金融模型、资产托管、拍卖。
- 扩展组件：大数据、人工智能。

应用层

通过使用原力协议 SDK 及 API，加密数字金融应用开发者可以开发如下去中心化应用。

- 借贷：零售银行借贷，P2P（点对点借贷），消费分期。
- 稳定币：数字资产抵押模式
- 交易所：中心化交易所、去中心化交易所
- 金融衍生品：期货、期权、互换、CDS、TRS 等。
- 保险：寿险、财险、意外险等。
- 债券：零息债券、付息债券等。

3.应用协议层

3.1.基础组件

3.1.1.去中心化身份标识（DID）

当前，拥有公链的主网账号（如 ETH 和 EOS 的区块链账户）就可以使用很多去中心化应用。但是，对于很多金融应用场景，按相关法律要求，特别是在反洗钱及反恐融资方面，身份认证是必须的。传统方案中，我们进行 KYC 时已经向平台方提供了身份信息，存在身份信息泄露的风险。因此，原力协议将结合生物识别技术和密码学算法，引入去中心化身份标识(Decentralized Identifier，DID)，确保用户身份数据隐私和安全。原力协议身份认证协议将遵循 W3C 标准，也会寻求同 MicrosoftDID、Sovrin、uPort 等项目合作。

3.1.2.钱包

钱包是用户区块链账户的管理工具。账户是数字资产流动的起点和终点，是交易、清结算、核算的基础。因此，账户具有举重轻重的作用。根据不同的场景，原力协议提供支持多链的钱包解决方案，包括:

- HD 钱包：HD 钱包支持多币种，且只需备份种子助记词，提高了操作简易性及兼容性。
- 中心化钱包：为降低用户教育成本，早期接触数字货币用户更容易接受中心化数字货币钱包。

3.1.3.安全与隐私

账户交易的隐私保护是金融应用的一项基本需求。技术上，可以采用数据脱敏、零知识证明、安全多方计算、环签名、群签名、盲签名等密码学方法，对数据进行高强度的加密保护。信息加密及解密授权可确保所有数据均由其拥有方自行加密上链，并可将解密权限仅授权给其认可的参与方;零知识证明则能够更进一步在第三方无需解密链上密文、数据拥有方不泄露敏感信息的前提下，实现对部分链上信息进行验证和判断，提高全流程效率。交易隐私方面，为了实现交易发起者对任何人不可追踪,可以使用环签名技术将交易发起者隐藏在一组账户集

合中；使用智能合约交易时，可以通过一次性账户技术将智能合约账户和原生账户进行隔离。

3.1.4. 治理

投票是社区或者合作联盟进行治理的一种重要机制。原力协议将提供一个投票表决和执行表决结果的通用功能，确保投票的安全性，透明度和普适性。治理有两个过程：第一、治理投票，目的是提供一种解决方案，比如引入新的预言机或者修改系统某个参数。第二、执行投票，目的是改变系统的状态，如实际改变某种质押物的风险参数。

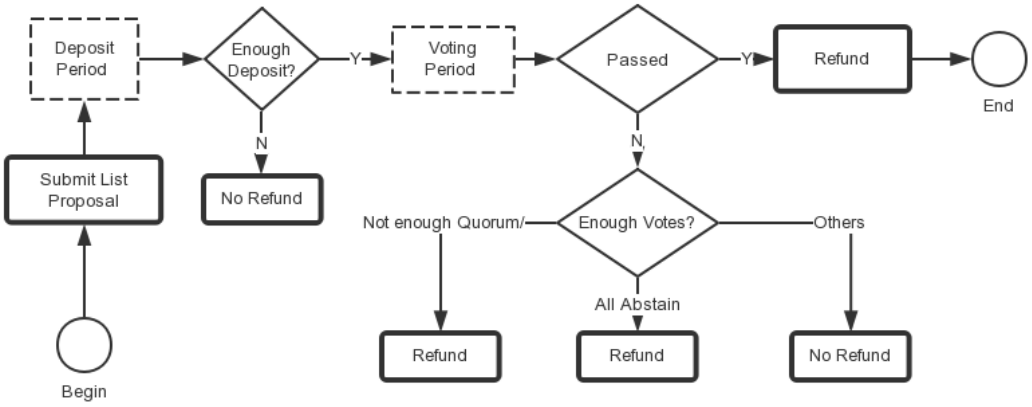

图 3 投票流程

3.1.5. 预言机

把金融合约实现为区块链上的智能合约，合约状态的判断不可避免需要使用到链下系统里的信息。这种链下业务流程和链内智能合约相结合的模式，需要一个实现链上链下数据打通的渠道，就是预言机。

对于预言机来说，最重要是怎么确保预言机本身是可信的，没有篡改数据。预言机一般有两种模式：中心化预言机及去中心化预言机。中心化的预言机存在单点失效的问题和数据信任问题；而去中心化的预言机有更好的稳定性和可靠性，但一般存在性能问题。

基于此，原力协议提出中心化和去中心化预言机并存的方案，即通过一定奖惩机制引入多数据源服务节点，鼓励数据源节点提供有效的数据上链服务，所有忠实的节点都将会得到原力协议代币奖励，反之，非正常的数据源节点将可能丢

失抵押给原力协议的代币。此外，考虑当前现实商业环境，对于部分可信第三方权威机构提供的数据，原力协议也支持直接采用中心化的对接方式实现。

3.2. 金融组件

3.2.1. 金融产品

金融产品具有复杂的业务属性和规则，这为智能合约的设计带来一定挑战，下表列举了主要的金融产品的要素和规则。

表 1 常见金融产品的要素和规则

金融产品	要素和规则
借贷	币种、利息、期限、还款方式等。
债券	币种、面值、付息期、偿还期、票面利率、发行人等。
期货	标的资产、合约大小（数量和单位）、交割时间、交割价格等。
期权	标的资产、数量、行权价、行权时限、类型（欧式或美式）等。
互换	币种、头寸、期限、固定利率、浮动利率等。
保险	宽限期、受益人、保费、保额、理赔条件等。

为了实现具体的金融业务，原力协议将参考金融行业通用标准，根据各金融产品的特性梳理数据结构，提炼出一系列可复用的产品规则条款，以供应用开发者使用。这样的标准包括基本条款、选择性条款和条件性条款。

- 基本条款：特定金融合约的必填项，如借贷产品的币种、利息、期限、还款方式等。
- 选择性条款：金融合约可选配置项，如债券产品是否可提前赎回、是否可转债等。
- 条件性条款：满足某种特定条件时执行，如债券产品中可设定当市场利率低于某个设定值时，发债方有权强制赎回债券，以降低融资成本。

3.2.2. 资产托管

根据不同的场景，加密资产托管模式包括智能合约、交易专户和多签账户等模式。原力协议将同各主流资产托管服务提供商进行合作，整合技术接口，为交易所、基金、借贷平台、资管服务平台及 OTC 交易商等提供便捷资产托管服务。

3.2.3. 金融模型

金融产品通常会涉及一些复杂的计算，同时需要动态监控市场和风险要素的变动情况，因此原力协议将提供一系列数学和金融模型服务。

- 数学模型：概率统计、方差分析、回归分析、时间序列等；
- 定价模型：根据最新数据动态计算金融产品价格，保障交易准确。
- 风控模型：依据风控模型输出风险分析结果，主要包括市场风险、信用风险、投资风险、流动性风险、交易对手风险等。

3.2.4. 拍卖

拍卖在现实生活中是处置资产的一种常见形式，公开叫价竞购确保了公平公正性。在去中心化金融应用中也经常存在着处置加密数字资产的场景，因此原力协议将提供一套实用的组件。

拍卖组件的实现将遵循最小化损失原则，即寻求处置最少的加密资产和获得最优处置价格。因此，拍卖的方式包括以下三种：

- 正向拍卖：固定质押物，出价高者中标；
- 反向拍卖：固定出价，要求质押物数量少者中标；
- 先正后反拍卖：先固定质押物，当出价达到预期价格后转为反向拍卖，即固定出价为预期价格，降低质押物数量，要求质押物数量少者中标。

3.3. 拓展组件

3.3.1. 大数据

数据是现代金融分析的基础。随着量化分析、机器学习等在金融领域的深入应用，数据被誉为“流动的黄金”。原力协议基于分布式架构，提供 ETL 加工清洗、数据分析及报表服务、数据可视化等一站式的大数据解决方案。

3.3.2. 人工智能

原力协议将集成人工智能技术，包括机器学习、知识图谱、自然语言处理、

计算机视觉(如人脸识别)等，为金融行业的各参与主体、各业务环节赋能，突出AI技术对于金融行业的产品创新、服务升级、流程再造的重要作用。

4. 金融公链协议

4.1. 金融公链架构

原力协议将开发针对金融服务的区块链分布式账本网络，将金融需求考虑到区块链底层平台的设计当中，构建开放金融服务的基础设施。

原力协议金融公链设计将遵循如下的思路：

- 针对金融市场的需求增强权限管理、安全控制、隐私保护、监督/监管等能力；
- 实现 3000+TPS，满足生产系统大吞吐高并发性能需求；
- 兼容 EVM，充分利用以太坊生态资源；
- 解决跨链互操作问题。

在深入比较了当前主流公链的优缺点后，考虑基于 Tendermint Core 和 Cosmos SDK 开放原力协议金融公链。以下为原力协议金融公链架构。

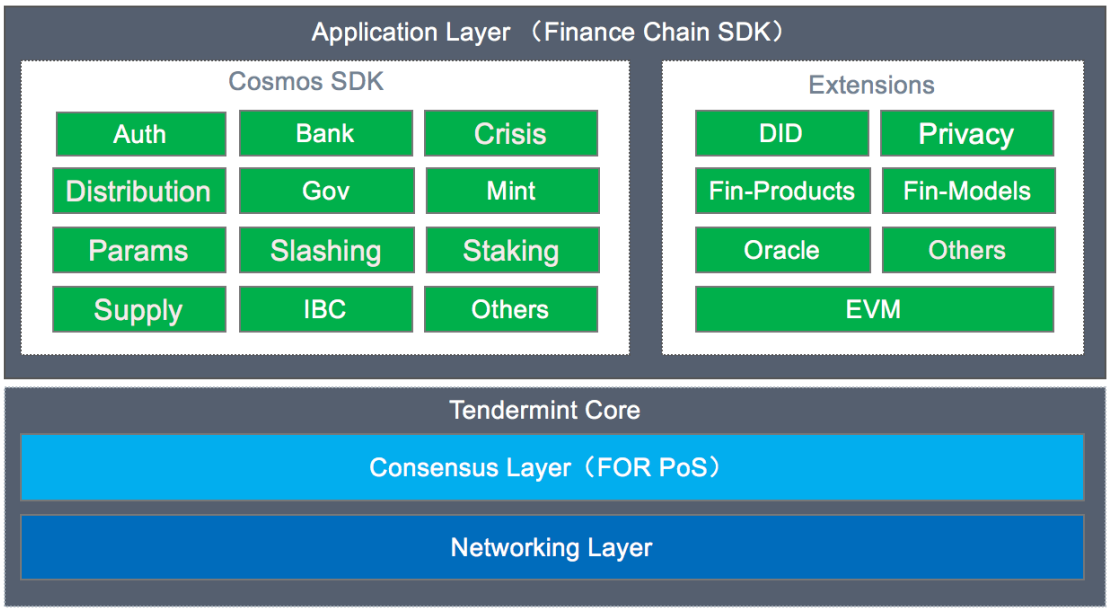

图 4 原力协议金融公链架构

金融公链分层架构

- 网络层：负责传播交易以及与共识相关的信息。
- 共识层：使节点能够就系统当前状态达成共识。
- 应用层：负责更新交易状态（即处理交易）。

Cosmos SDK 提供的有如下模块：

- Auth：多资产账户模型
- Bank：转账相关

- Crisis: 系统紧急情况处理
- Distribution: 在验证人和委托人之间分配手续费
- Gov:治理模块
- Mint: token 增发模块
- Params: 系统全局参数处理
- Slashing: 对作恶节点进行惩罚模块
- Staking: Proof of staking 模块
- Supply:代币供应管理模块
- IBC：跨链模块

原力协议控制模块：

- DID:去中心化身份标识
- Privacy：隐私保护
- Fin-Products:金融产品
- Fin-Models:金融模型
- Oracle:预言机
- EVM:以太坊虚拟机

4.2.共识机制

原力协议在综合考虑了各共识协议的优缺点后，首先基于 Cosmos 的 Tendermint 做为共识协议，后续随着对业务的升级，会将金融特有的一些特性加入到共识中去，提升业务能力。Tendermint 主要包含两个主要的技术：区块链共识引擎和通用的应用接口。共识引擎被称为 Tendermint 核心模块，确保相同的交易在每个机器中都按照相同的顺序被记录下来。应用接口被称为应用区块链接口(ABCI)，让交易可以被任何编程语言编写的程序处理。

假设少于 1/3 的验证者是恶意节点或者未能正常运行，Tendermint 保证安全永远不会被破坏。也就是，验证者（2/3 以上）永远不会在同一个高度提交冲突的区块。因此，基于 Temdermint 的区块链永远不会分叉。

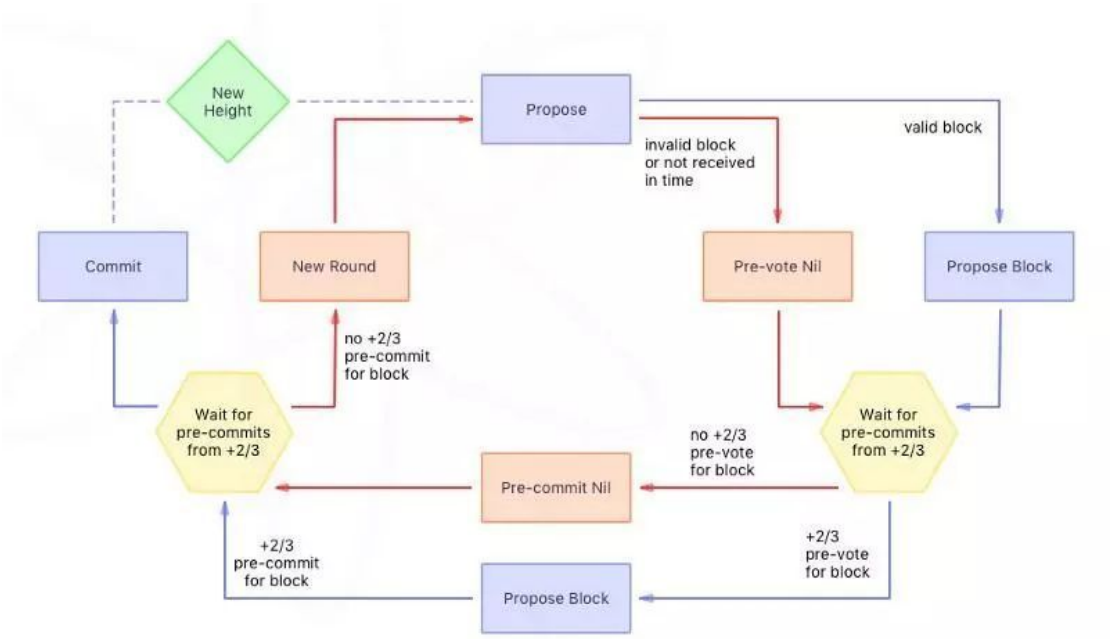

图 5 Tendermint 共识过程

4.3.智能合约

Cosmos 本身不支持智能合约,于是Cosmos 官方开发了 Ethermint。Ethermint 是一款非常快速的 POS 区块链,并整体兼容以太坊 Ethereum。原力金融公链将集成 Ethermint 模块到自己的系统中，以兼容支持 Solidity 的公链或联盟链，如 Ethereum，ETC 和 RSK 等。随着 EVM 的更新，以及合约编程语言的进步，原力公链将始终追踪业内进展，将具有前瞻性的进展集成到系统中。

将 Ethermint 集成到原力金融公链中，有助于复用现有的以太坊工具，如 Dapptools 系列开发工具、web3j、web3js 以及 truffle 等。原力协议基于以太坊开发的应用层协议各组件也可兼容复用。

4.4.跨链解决方案

跨链数字资产的管理是当前业内的一个主要研究方向,这样的尝试包括公证人机制（Notary schemes)、侧链/中继（Sidechains/relays)、哈希锁定（Hash-locking)、分布式私钥控制（Distributed private key control）等。

其中，公认证机制不够去中心化；哈希锁实现较为简单，在闪电网络等支付通道中得到应用，但因为不能实现跨链资产转移，应用场景受限。分布式私钥控制方案使用安全多方计算和门限秘钥共享技术实现，该方案不需要双向锚定，无

需修改原有链机制，具有一定合约开发工作量，是原力协议的备用方案。

目前，中继机制是最主流的跨链解决方案，Cosmos 和 Polkadot 两个项目都采用该技术，但该技术的实现非常复杂。原力协议金融公链基于 Cosmos SDK 开发的主要目的之一便是使用 Cosmos 的跨链通讯协议（Inter-Blockchain Communication， IBC），以实现资产跨链功能。

5. 应用案例

5.1. 网络借贷联盟

网络借贷是指利用互联网发放贷款的业务，其中涉及到众多参与方。

图 6 网络借贷业务参与方

对此，原力协议提供的方案是搭建联盟链，联盟成员严格准入，所有成员节点同步更新数据。

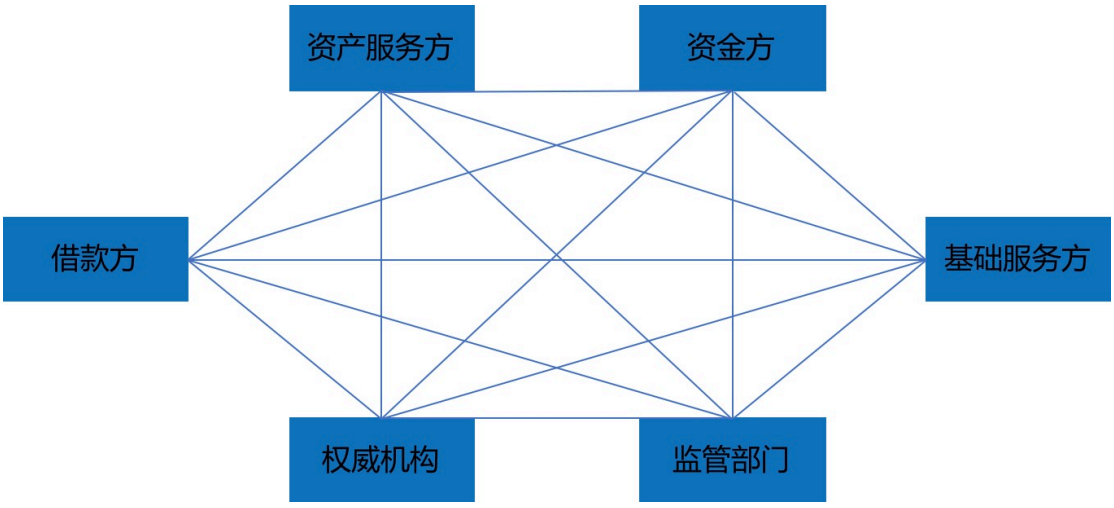

图 7 网络借贷联盟链

区块链不可篡改、信息记录可追溯的特性，使得所有通过共识验证成功上链的数据，都无法因个别参与方的意愿，在其他参与方不知情的情况下被修改。这将大幅降低参与方伪造数据作恶的意愿，同时提升审计检查的效率。

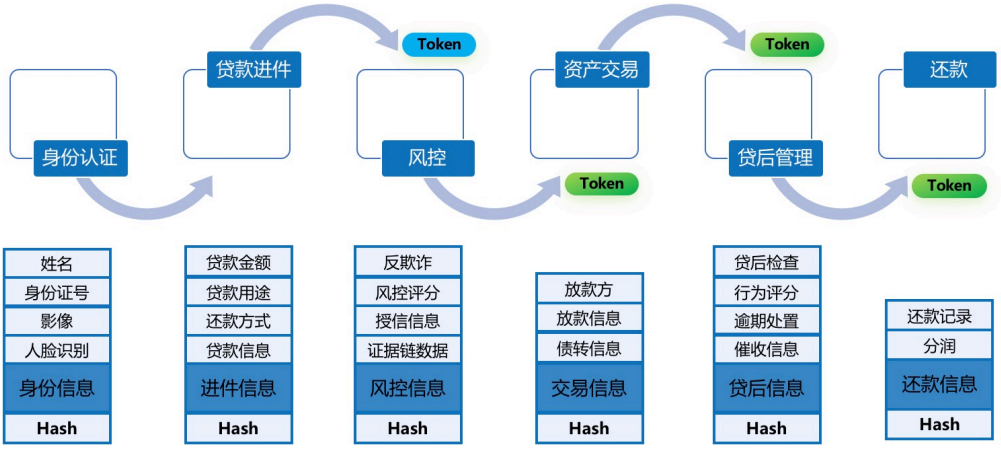

图 8 网络借贷信息上链

同时，在标准化环节中引入智能合约的应用，在满足条件时自动触发执行相关业务，在提高自动化程度，增加效率的同时，也能在一定程度上规避信用欺诈风险和操作风险。这样，就可以建立一个稳定透明的借贷互信生态，让所有参与者都能合作共赢。最重要的是，该方案对监管友好。

5.2. 去中心化借贷——币币贷

币币贷是在以太坊公链上开发的去中心化借贷应用，支持点对点质押借贷，质押资产由智能合约保管。

表 2 币币贷去中心化借贷产品介绍

要素	规则
借币币种	USDT(ERC-20)、DAI 等
质押币种	ETH、BNB、FOR、BAT、HT、MKR、LRC 等
质押率	180%（=质押币市值/借币市值）
补仓线	150%
平仓线	120%
日利率	万 1 到万 8，借币用户自主设置
借款期限	7、14、30、60、90 天，借币用户自主选择
最低借款数量	10 USD 起
手续费	日手续费率万 0.5（以页面提示为准），向借币用户和出借用户双向收费。借币者还款时支付手续费，出借者出借时支付手续费。质押率到达 120%时将被平仓，其中 5%质押币将转给借币订单来源渠道，5%作为币币贷平仓费用，110%转给出借人。

订单有限期	若订单在 5 个自然日内未成交，订单将被系统取消。

借币用户向智能合约质押数字货币，自主设定借款利率和借款期限即可创建借款订单。每笔借款订单将进入币币贷共享订单薄，该共享订单簿向所有币币贷合作伙伴开放，来自任何合作伙伴的出借用户可以选择其中任意一笔借款订单进行出借。

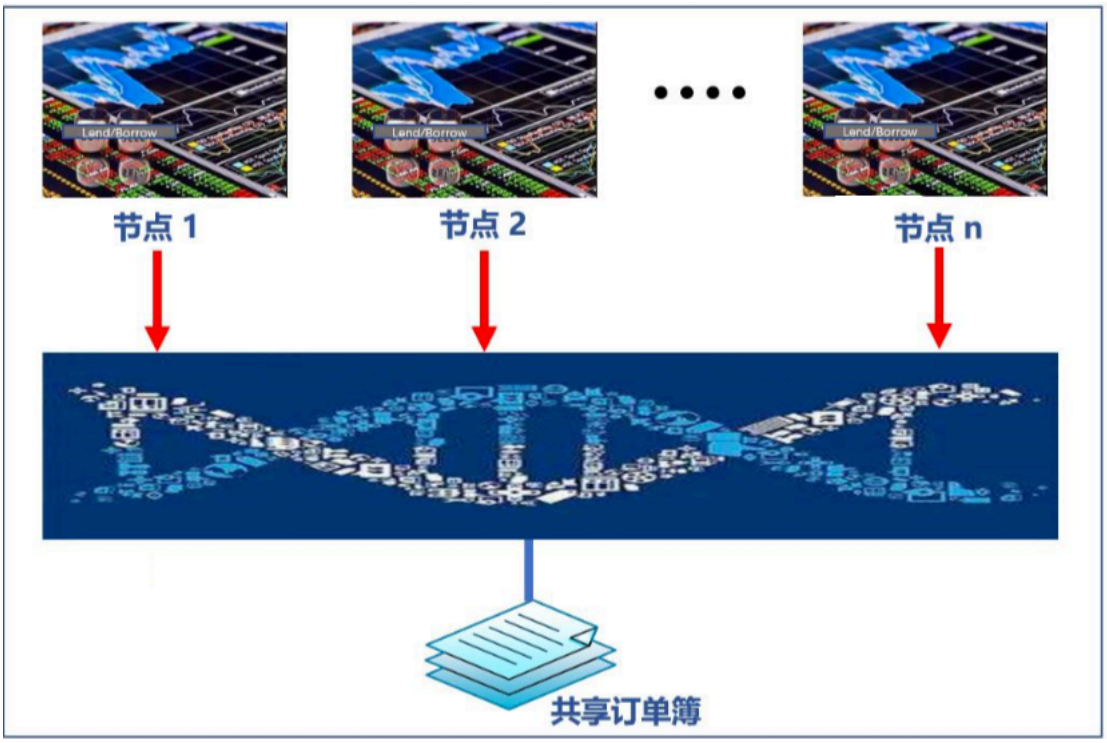

图 9 共享订单薄

币币贷通过合作节点搭建全球借贷网络，实现全球借贷资源共享。所有合作节点可以享受手续费分润。

平台合作节点：数字货币钱包、数字货币交易所及其他流量平台等

区域合作节点：区域性金融机构和个人（需符合当地法律法规）。

【概念图待设计】

图 10 币币贷借贷网络

5.3. 去中心化稳定币——Qian

Qian 是数字资产质押发行的稳定币，这种模式的原理是在区块链的智能合约上抵押数字资产，从而发行锚定法币价格的数字货币。在这种模式下，每一个发行出的稳定币，背后都有对应的数字资产进行抵押，比如 BTC、ETH 等目前主

流的数字货币。但由于这些数字资产本身价格波动较大，因此一般要通过超额抵押以及强制清算等风控机制保证每个价值 1 美元稳定币，背后至少存在价值 1 美元的抵押物，可以在清算的过程中获得。相较于同样有抵押物的法币储备模式，Qian 主要优势在于体现了区块链的去中心化思想，质押物锁定在智能合约里，公开透明，无法被挪用或冻结，没有任何人或者机构可以直接控制稳定币的发行。

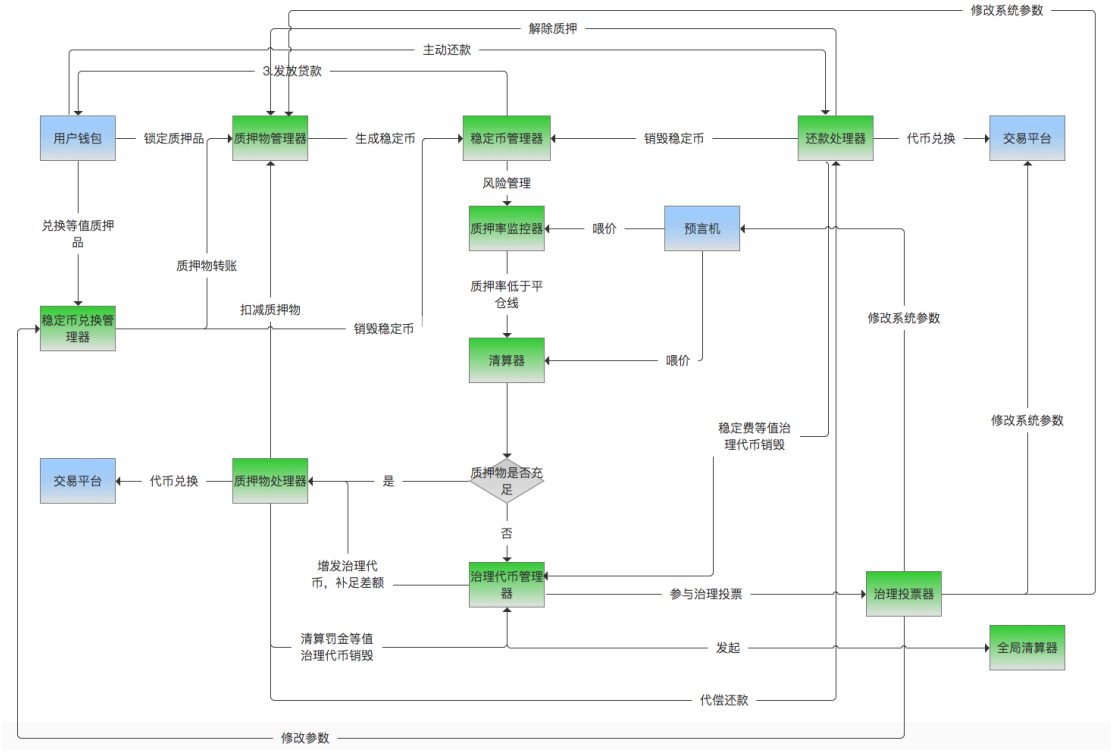

图 11 QIAN 系统架构图

QIAN 的基本要点

- QIAN 以加密资产为底层支持资产；
- QIAN 1:1 锚定美元，但逐渐会脱离这种锚定；
- QIAN 系统优先在 RSK 和以太坊上发行，后续开发对接更多主流币种的跨链功能；
- QIAN 系统致力于实行完全的去中心化，但这将是一个渐进的过程；
- QIAN 系统基于原力协议开源框架开发，是原力协议生态系统的一部分。

稳定机制

- 超额加密资产支持；
- QIAN 持有者可以按锚定价格赎回等值质押品；
- 精选资产组合，降低系统性风险；
- 动态利息调整机制，维持和调整生态的发展和稳定；
- 风险缓释金机制。

6.研发路径

2018 Q2～Q3

项目启动，白皮书设计，官网上线。

2018 Q4

借贷智能合约和交易系统开发，币币贷 1.0 平台上线。

2019 Q1～Q2

分布式加密数字金融服务协议设计，白皮书更新。

2019 Q3～Q4

基于以太坊的分布式加密数字金融服务协议开发完成，币币贷 2.0 上线。

2020 Q1～Q2

原力协议稳定币发行，启动原力协议公链开发。

2020 Q3～Q4

原力协议公链上线，基于原力协议公链的加密数字金融服务平台 1.0 版上线。