CChain

区块链技术白皮书

基于区块链的功能性智能合约系统

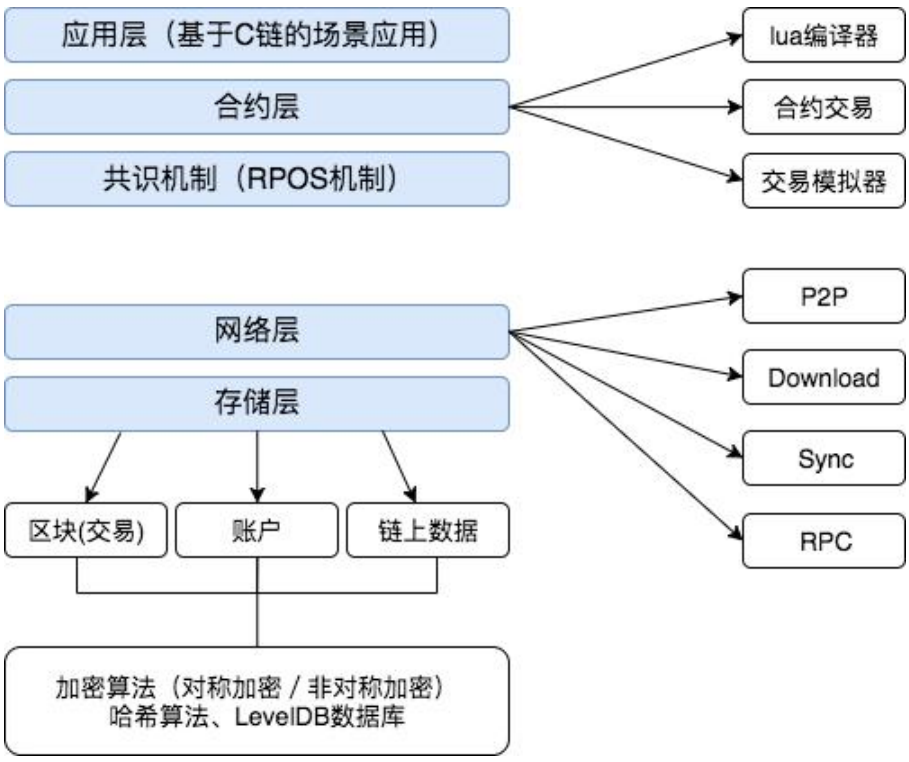
目录

1 概览

C 链定位于是一条区块链功能性智能合约系统底层链，C 链的核心理念是在区块链底层技术的基础上，编辑不同的智能合约，然后将智能合约进行模块化分解，通过构建可视化操作平台，实现不同的智能合约功能。用户可以在 C 链上轻松的通过模块化，搭建自己想实现的基于区块链的智能合约系统。C 链采用了类 BTS 架构，吸收了 BTS 架构底层高并发的设计理念，同时为了更好的应对不同场景的智能合约的编写及测试，C 链实现了自己的一套图灵完备的、执行速度更快、支持链下测试及执行、低成本、有条件升级合约等优势的一套合约机制。

2 CChain 的设计理念和架构

2.1 系统架构



2.2 账户模型和体系

在 C 链系统的账户模型中，根据账户的功能不同可以将账户分为不同的类型。

普通账户

当用户在钱包内生成一个地址时，此时该地址就是一个普通地址，只在本地钱包内可以识别。

注册账户

当用户花费极少数的手续费将普通账户地址注册到区块链上后，该地址就成为了一个注册地址。注册地址与注册账户名存在一一绑定关系，其他用户可以以地址的用户名作为转账方进行转账。

代理账户和出块账户

C 链采用 RPOS 共识机制，因此会有代理账户，代理账户也可以成为出块账户对链上的交易进行打包。

合约账户

当用户编写发布部署合约后，就会产生一个合约账户，这个合约账户也可以进行转账操作。正因为合约有储存金额这样的功能，那么合约可以进行一些众筹的功能。

2.3 共识机制

C 链采用 RPOS(Result Delegated Proof of Stake)的共识机制,这种共识机制保证了在一个产块周期内只能有一个产块代理账户可以对当时的交易区块进行打包，继而该区块会被其他代理节点进行验证，每一个区块与下一个产生的区块都以链表的

形式相连。

RPOS 产块代理机制采用公平的投票机制，确保了每一轮产块代理都是随机公正的，这也确保了每一轮的产块都是透明公开。

相比于以太坊或比特币的 POW 共识机制，POW 采用全网矿工参与的方式来进行打包，其中会有大量的计算会导致打包速度慢，同时采取 pow 方式的挖矿机制由于全网算力不断增大，因此加大了 GPU/ASIC 挖矿芯片更新换代的频率，最后打包也可能会被几大矿池垄断，不适合在场景应用或者类似商业应用中使用，而 C 链的共识机制在执行速度上更快，公平程度上来说相对更好。

2.4 密码学模型

区块链系统内，所有权验证机制的基础是非对称加密算法。常见的非对称加密算法包括 RSA、Elgamal、D-H、ECC（椭圆曲线加密算法）等。

在非对称加密算法中，如果一个“密钥对”中的两个密钥满足以下两个条件：

1、对信息用其中一个密钥加密后，只有用另一个密钥才能解开。

2、其中一个密钥公开后，根据公开的密钥别人也无法算出另一个，那么我们就称这个密钥对为非对称密钥对，公开的密钥称为公钥，不公开的密钥称为私钥。

2.5 智能合约

智能合约作为 C 链系统整个应用的核心，C 链采取模块化、组件化、模版化的功能方式搭建整个平台，根据 C 链平台的设计原则和产品定位的要求，针对智能合约应用场景进行研发，根据不同的应用场景选择不同的功能模块进行组合，以满足

实际的社交服务需求。因此 C 链希望让其智能合约在执行速度上更快、交易手续费更低、测试成本更低。区块链智能合约本身就存在一些天然的优点，例如预指定规则，无法修改、去中心化用户系统、资产合约代币化、合约资产交易等特点。

C 链的智能合约采用相对成熟的 Lua 语言，Lua 语言体积小，嵌入性能更高，非常容易和 C 链的本体实现语言（C++）完美融合。相比于以太坊的合约语言 solidity 而言，Lua 在安全性、代码冗余性方面还是有很大的优势。在 C 链的智能合约体系中，用户可以在链下先进行合约的测试编写及测试，整个智能合约的生命周期包括编写合约、部署合约、注册合约、调用合约。总体来说，C 链的智能合约体系相比以太坊而言，主要有如下几点创新优势：

1. 安全性能更高，体积更小(相应的手续费就会更低)
2. 敏捷开发
3. 零成本合约测试机制
4. 合约编程速度更快，因为有更丰富的内置库
5. 可以销毁合约以及升级合约（有条件）

2.6 验证交易

签名认证：系统在操作需要签名的资源时会检查交易中是否存在所需签名，其中包括普通交易、合约交易，由于采用 RPOS 共识机制，所以会动态的根据交易的执行情况（执行时间、资源消耗等）来去验证交易，达到可信度更高的目的。

2.7 事件

对于普通节点来说，由于在验证接收到的区块的过程中，并不会像代理节点那样执行解释器进行验证，因此对于合约中发生的一些情况缺乏感知能力。因此可以由代

理节点在执行相关的合约中达到的一些特定的关键点（需要产生一个通知信息）的地方产生一个合约事件，事件功能可以用来提升用户对交易以及交易中的一些中间环节的感知能力，并且可以对感知到的状况做一些自定制的反馈，提升可交互能力。（通过本地脚本的方式，或者由用户自行定制的一些方式）。

2.8 合约网关及链间网关

链下面的实际数据通过网关放入区块链，触发链上合约交易的共识。

区块链和类链之间的合约网关：通过其他链上的交易数据达成的共识再由链之间的合约网关负责链之间的数据交换。

3 CChain 的场景应用落地解决方案

3.1 落地应用架构