公开▲

白　　皮　　书

技术文件名称：一种完全去中心化和闭环的区块链群生态系统

技术文件编号：

版　　本：1.6

目 录

1 摘要

CES: one perfect decentralized and closed cycle block chain Crowd Ecological System，一种完全去中心化和闭环的区块链群生态系统，下文简称“本生态“或“本生态系统”。

CES 通过设计一个基于云计算全新的技术架构，能够承载各行各业的区块链，形成一个不依赖任何外部条件就实现完全去中心化和闭环的区块链群生态系统。本生态将尽量去除命令行的操作方式，在各个环节提供适合所有用户的图形化操作。

区块链已经解决了信任问题，本生态将着重解决信用、认证、公证和支付问题。

CES 有 9 大创新点：

1) 全新的技术架构，承载着各行各业共生共荣的区块链群；
2) 完全去中心化（仅指底层区块链，不包括上层应用）和闭环的区块链群生态系统；
3) 首创的多次分片多次共识的共识算法，TPS 达到大规模商业化要求；
4) 首创的双重密钥保护机制，账户资产更安全；
5) 生态内自带的支付链支持法币-法币、法币-数字货币、数字货币-数字货币交易，不再依赖任何外部交易所；
6) 共享的商业生态（共享用户、市场、技术、应用解决方案），并存在巨大的优势吸引开发者开发基于本生态的应用和智能合约；
7) 整个区块链群生态系统中通用的和唯一的账户与数字货币（token 除外）；
8) 数据区分对待，引入零知识证明算法保护需要保护的隐私数据；
9) 能快速的开发行业链并发行自己的 token，不再有“空气币”；

2 术语、定义和缩略语

2.1 术语和定义

表 2.1 术语和定义

术语	英文	含义
架构	Architecture	也叫体系结构
云计算	Cloud Computing	云计算
实例	Instance	类实例化（instantiated）后的实体

2.2 缩略语

表 2.2 缩略语

缩略语	英文	含义
API	Application Programming Interface	应用程序接口
APP	Application Program	特指传统的中心式应用程序
BaaS	Blockchain as a Service	区块链即服务
BFT	Byzantine Fault Tolerance	拜占庭容错算法
DAPP	Decentralized Application Program	分布式应用程序
DAO	Decentralized Autonomous Organization	去中心化的自治组织

缩略语	英文	含义
DPoS	Delegated Proof of Stake	委托权益证明算法
EIP	Ecosystem Improvement Proposals	生态系统改进建议
EOS	Enterprise Operation System	区块链商业操作系统
ETH	Ethereum	以太坊
IaaS	Infrastructure as a Service	基础设施即服务
ICO	Initial Coin Offering	首次币发行
IPFS	Inter Planetary File System	星际文件系统
KYC	Know Your Customer	了解您的客户
LCV	Light Client Validation	轻客户端验证
PIN	Personal Identification Number	个人识别码
PBFT	Practical Byzantine Fault Tolerance	实用拜占庭容错算法
PaaS	Platform as a Service	平台即服务
SPV	Simplified Payment Verification	简单支付验证
TPS	Transaction Per Second	每秒交易数

3 背景

区块链技术自诞生以来，就受到很多企业和人员的大力支持，大家都向往那个完全去中心化、公开透明、数据不可篡改、可溯源的、社区共同决策的理想世界。但是经过Bitcoin，ETH，EOS，区块链技术虽然在一步一步的进步，但是仍然存在各种问题。

3.1 区块链目前问题

1) 性能有限，达不到大规模商业化的要求；
2) 链与链之间没有关联性，无法共生共荣，反而经常出现恶性竞争；
3) 逐利资金喜欢自己重新搭建新链进行 ICO，或仅仅只是发行“空气币”，各种各样的区块链泛滥成灾；
4) 严重依赖于外部交易所，而且绝大部分交易所却是中心化的，安全性低，这与区块链的初衷相违背；
5) 没有形成商业化和闭环的区块链生态系统；
6) 共识机制仍需进一步完善和完全去中心化；
7) 跨链和侧链技术不成熟；
8) 没有丰富的应用；

3.2 区块链 APP/DAPP 的要求

3.2.1 支持上亿级用户

大规模商业化需要处理上亿级日活用户所产生的数据，因此支撑大量用户至关重要。

3.2.2 用户使用简单方便

大规模商业化意味着大多数的用户都是普通百姓，文化程度一般，这就要求商业化

的模式和各种用户操作，都必须简单方便，适合普通大众，便于全球推广。

3.2.3 用户使用无痛感

俗话说“羊毛出在羊身上”，任何的成本，最终都会无形的转移给消费者。但是区块链技术极大的降低了成本，用户只需要支付极低的无痛感的交易手续费。

3.2.4 轻松升级和漏洞修复

应用需要灵活地通过新功能来增强应用程序，及解决运维过程中的 BUG。

3.2.5 低延迟

良好的用户体验要求不超过几秒钟的可靠反馈，过长的延迟会影响用户体验。

3.2.6 顺序性

有些应用程序的命令执行必须有先后顺序。

3.2.7 并发性能

大规模应用需要在多个 CPU 和计算机之间划分工作负载，或多个服务节点间实现负载均衡。

3.2.8 快速接入

应用希望区块链底层能提供多种开发语言的 API，供其快速接入。

3.2.9 场景多样化

应用只需要基于本生态提供的一套 API 开发，就能使用各行各业的区块链提供的功能，大大丰富了应用场景。

4 CES 生态系统

4.1 约束和准入制度

本生态会详细的制定约束和准入制度，全生态的链、应用和用户都需要遵守。

4.1.1 约束制度

如禁止黄赌毒、禁止 token 上任何外部的交易所等等。这部分后续细化。

4.1.2 准入制度

4.1.2.1 进驻链

公有链一般需要具备影响力大和用户量多，或具有公益性质，例如户籍登记，工商登记，房产登记，医疗服务，知识产权，慈善公益等等。公有链需要申请，纯商业的公有链允许在一段时间里具有排他性。而联盟链和私有链则无要求，当一个联盟链或私有链达到一定的影响力，则可以申请上升为公有链。

本生态对所有进驻链不收取任何费用，公益链还可以得到技术支持。

4.1.2.2 进驻应用

本生态自带一个应用商城，允许开发者发布自己的分布式应用（DAPP）和中心式应用（APP），以及智能合约，而且基本是免费的，只要他们都遵守本生态的自治规定。

4.2 技术架构

4.2.1 基于 C2I 的模块封装

本生态中的所有模块都将采用 C2I 的封装模式。

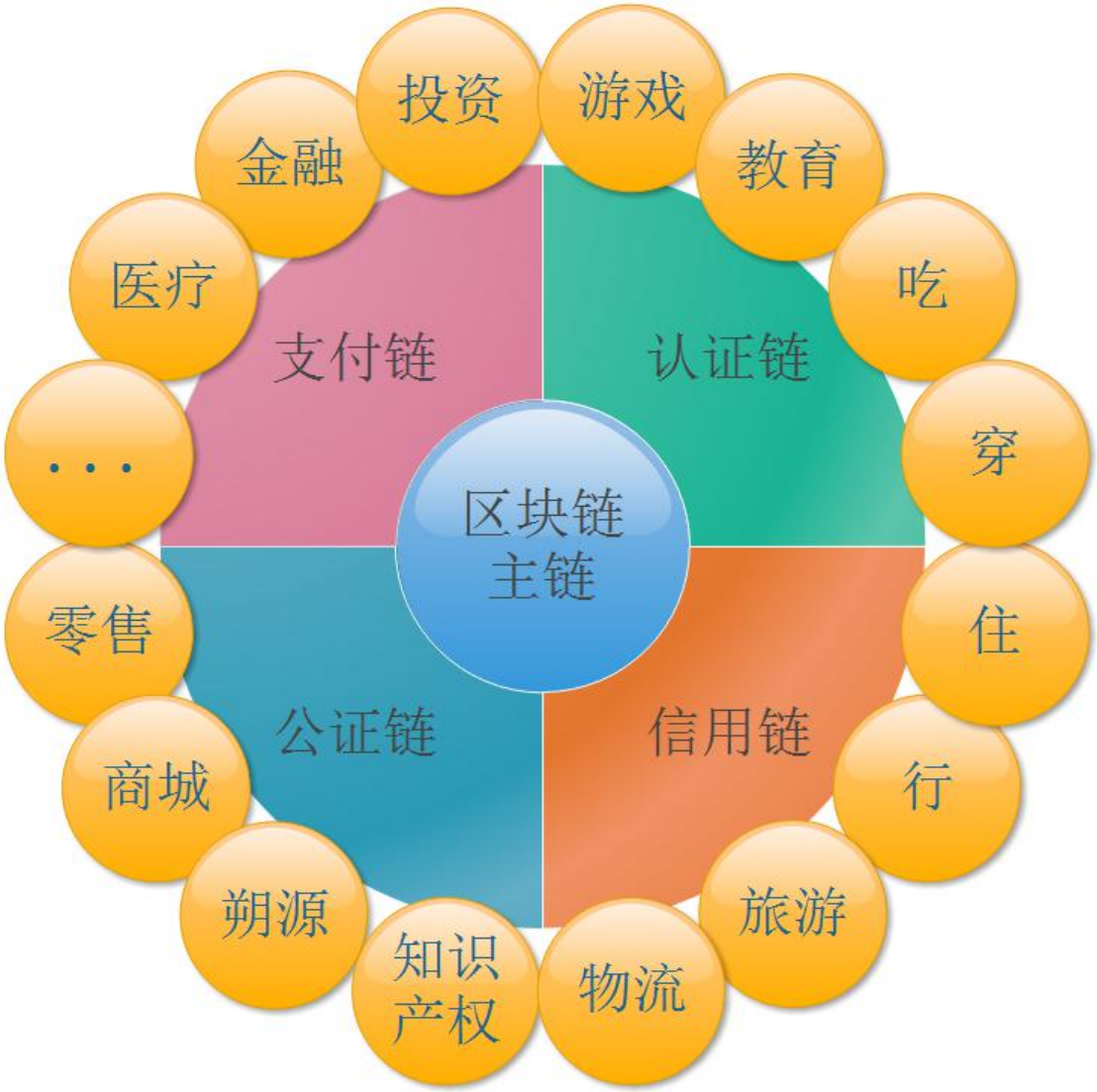
C2I：Class to Interface，Class is Derived from Interface。源自于六大设计原则中的依赖倒置原则和接口隔离原则，再结合五大创建型模式、桥接模式、类继承，是实践中得到的最佳模块封装形式。

C2I project：

https://github.com/sunnygood/CEN-XFS

4.2.2 生态系统模型图

以主链（账户）、支付链、认证链、信用链、公证链为核心，再结合各行各业的行业链，形成一个相互依赖、共生共荣的区块链群生态系统。

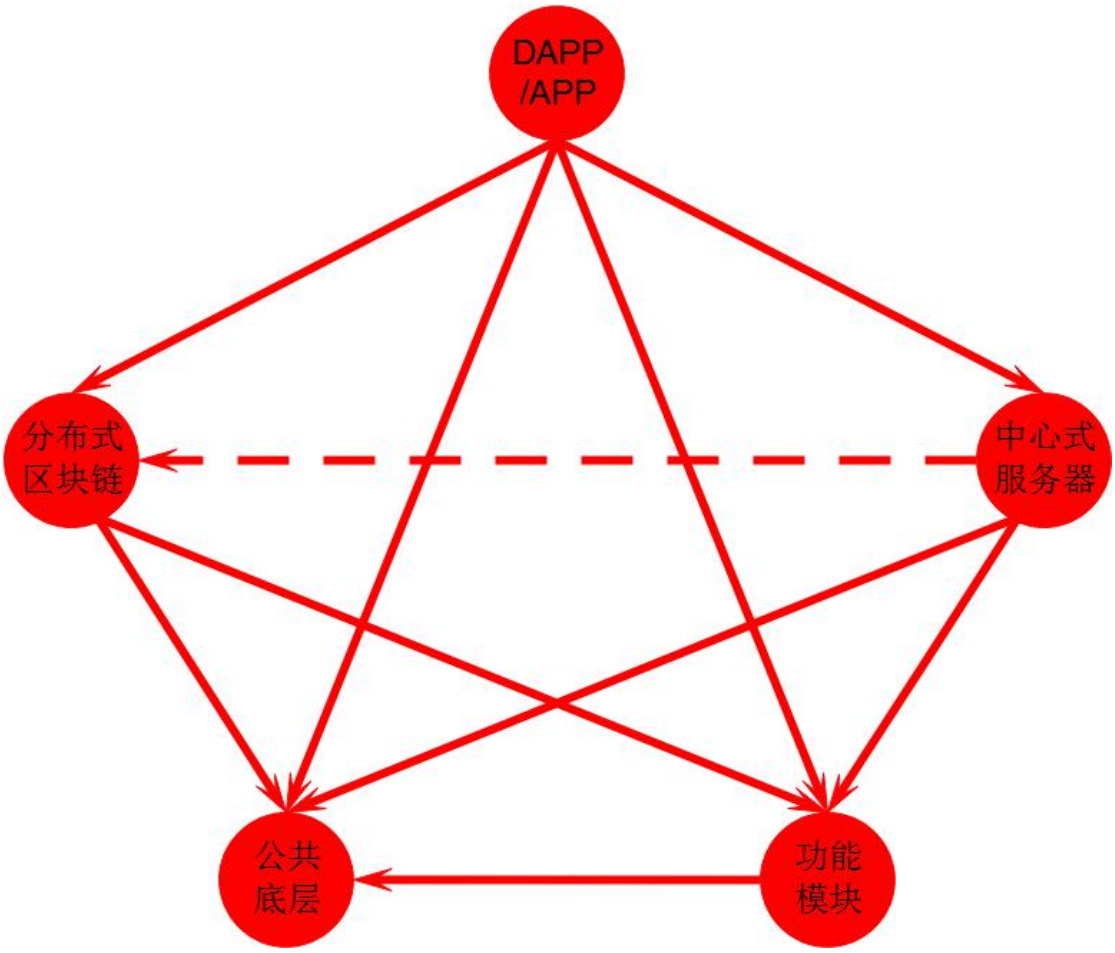


4.2.3 生态系统五角星架构图

当今世界现存的绝大部分应用都是由 APP 层、功能模块（业务）、中心式服务器、公共底层这当中的若干（1～4）部分组成。

而自从区块链诞生以来，区块链都是由 DAPP 层、功能模块（业务）、分布式区块链、公共底层这四部分组成，人们多认为只有 DAPP 才能参与到区块链生态。但是由于 DAPP 分布式的特点，有相当大一部分行业难以实现 DAPP，再加上开发人员参与度不高，造成区块链应用的匮乏。

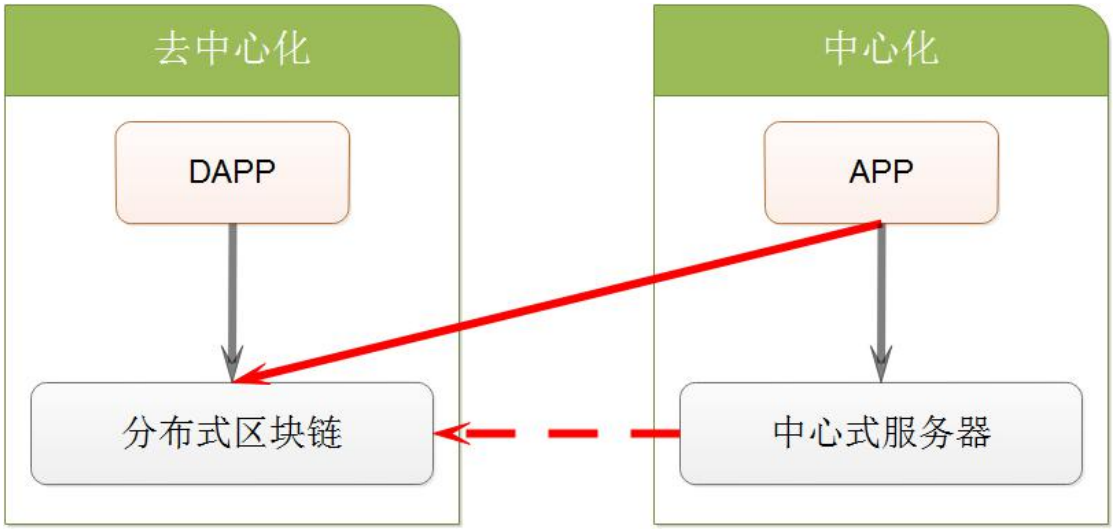
正因为如此，本生态引入五角星架构，只要 APP 使用部分的行业链，就可以把去中心化的区块链、中心化的服务器融合在一起，得以利用现存的大量资源，极大的丰富了生态。



4.2.4 应用模型图

本生态系统只追求分布式区块链的完全去中心化，而对于应用，可以是去中心化的分布式 DAPP，也可以是中心化的 APP，这由开发者决定。

如下图所示：左边是完全去中心化的分布式区块链生态，右边则是当今世界占据极高比例的中心化应用生态。正是通过下图红色箭头的这种方式，中心化 APP 接入部分链即可（如主链、支付链、认证链、信用链、公证链、溯源链等），这样就能把当今世界现有的主流应用都包含到本生态中，丰富了应用生态。



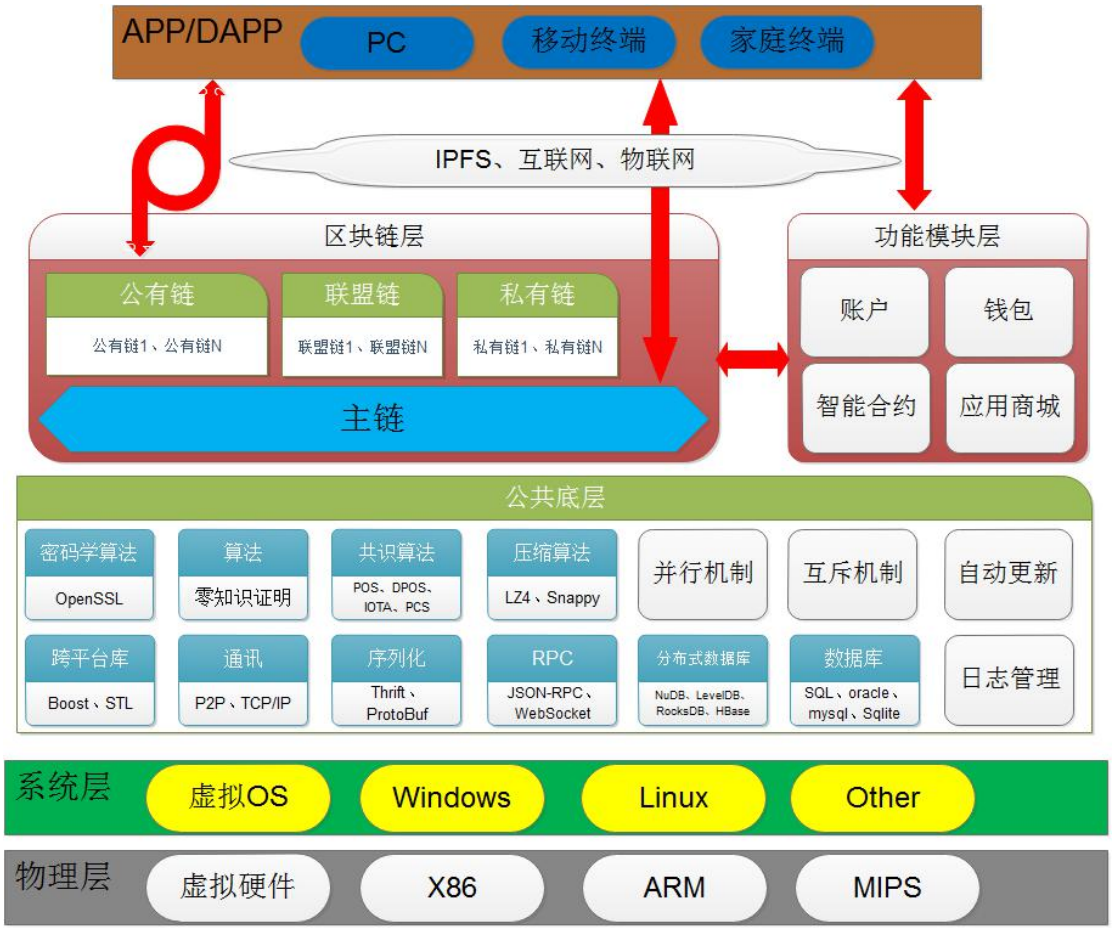
4.2.5 区块链

4.2.5.1 层次架构图

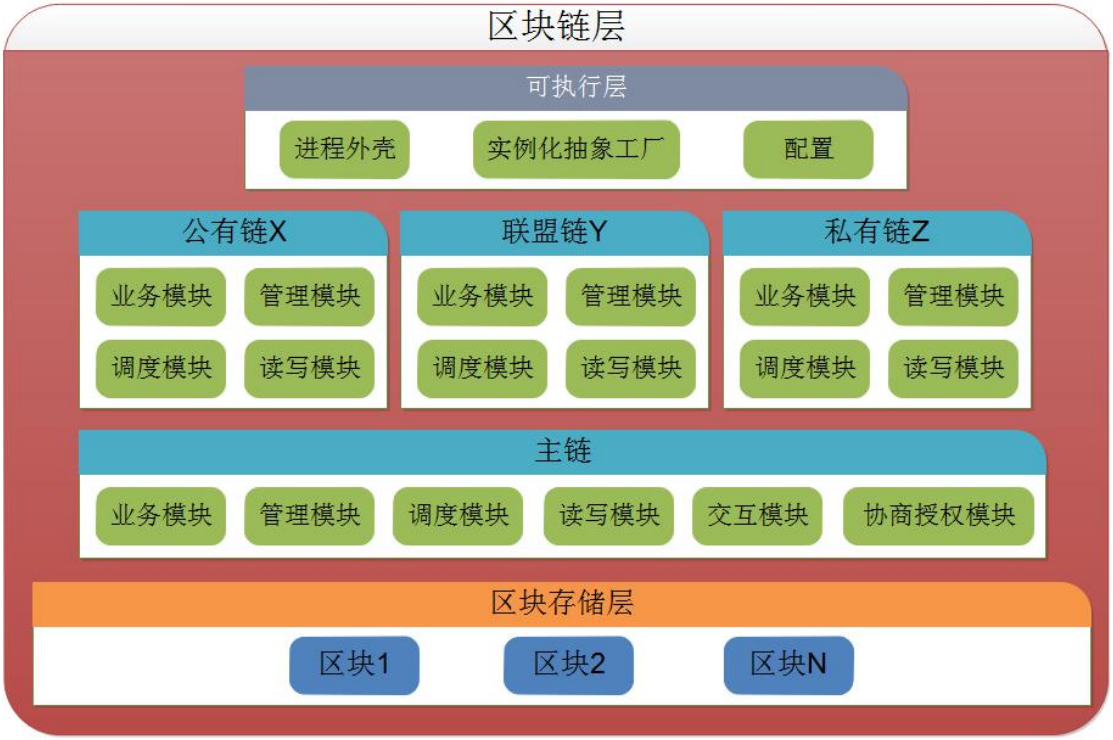
如下图所示，本生态通过设计一个结合云计算的全新的区块链技术架构，能够承载各行各业的区块链，形成一个不依赖任何外部条件就实现了完全去中心化和闭环的区块链群生态系统。本生态系统的区块链层可以做到所有链并行运行，实现互联互通。

在这个生态系统中，应用可以是中心式 APP 也可以是分布式 DAPP，如本生态自带的应用商城和社区治理网站就是中心化的。他们通过 IPFS、互联网、物联网等连接到区块链服务节点中使用区块链的各种功能，享受区块链完全去中心化、公开透明、数据不可篡改、可溯源、维护成本低、所有人共同治理等各种优点。

本生态系统各行各业的区块链，他们共享用户、共享市场、共享技术、共享应用解决方案，他们之间是共生共荣的关系。

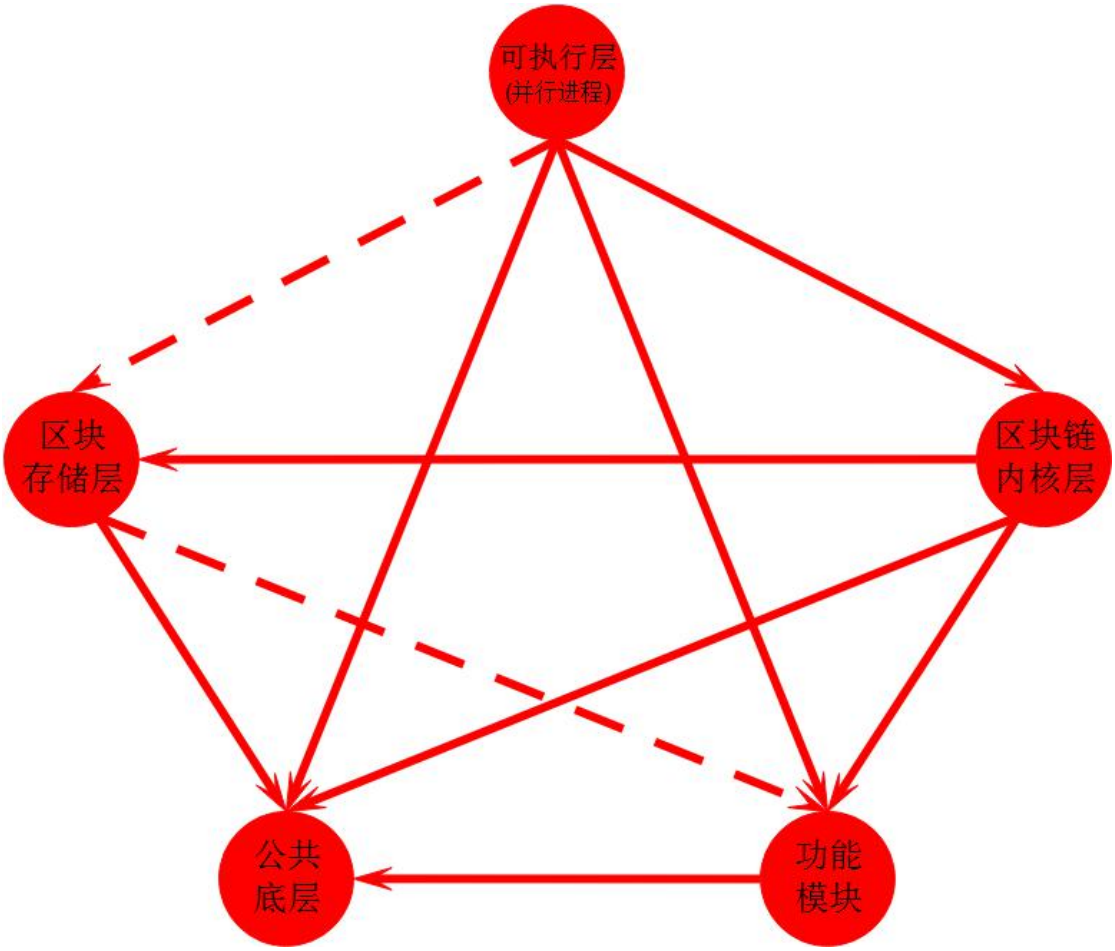


这是承载各行各业区块链的核心技术架构。这个架构按照层次划分为可执行层、副链（公有链、联盟链、私有链）、主链、区块存储层这四个层次。

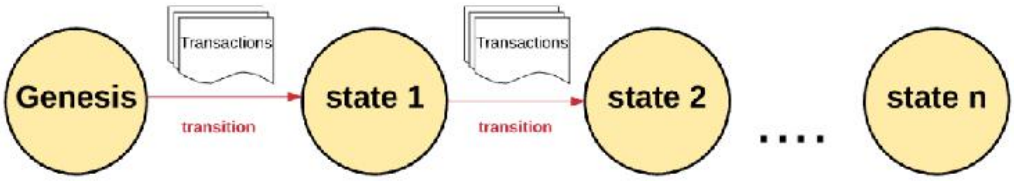


4.2.5.2 五角星架构图

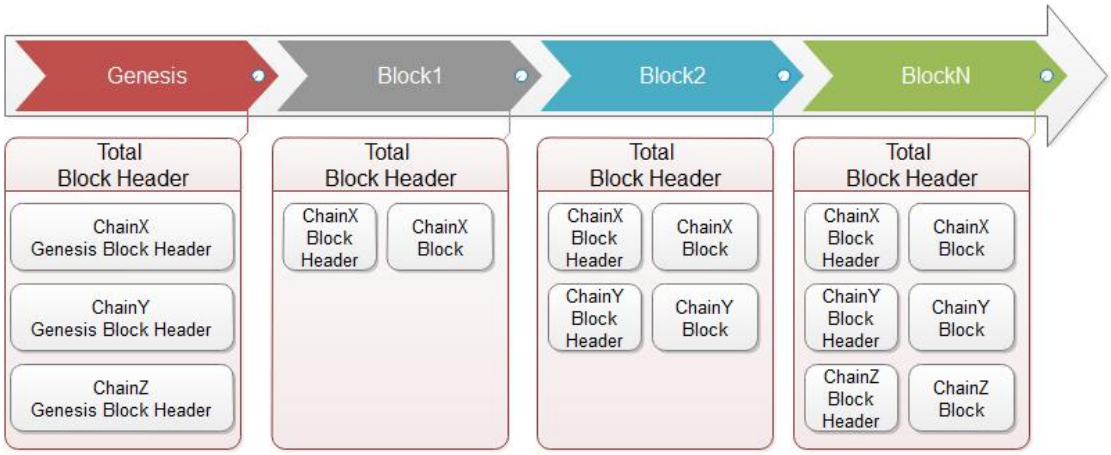
每条区块链也可以采用五角星架构，如下图所示，分为可执行层、区块链内核层、区块存储层、功能模块、公共底层。



4.2.5.3 数据库状态图



4.2.5.4 区块存储图

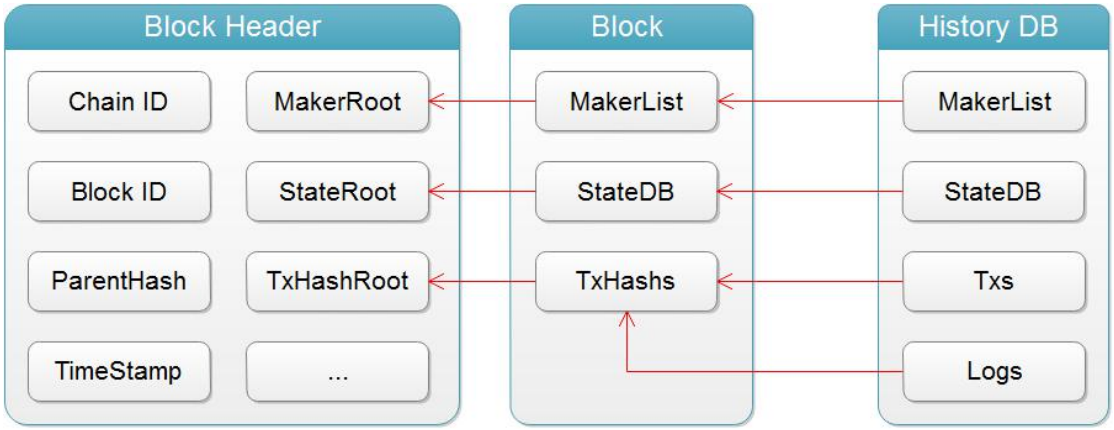


4.2.5.5 隔离见证

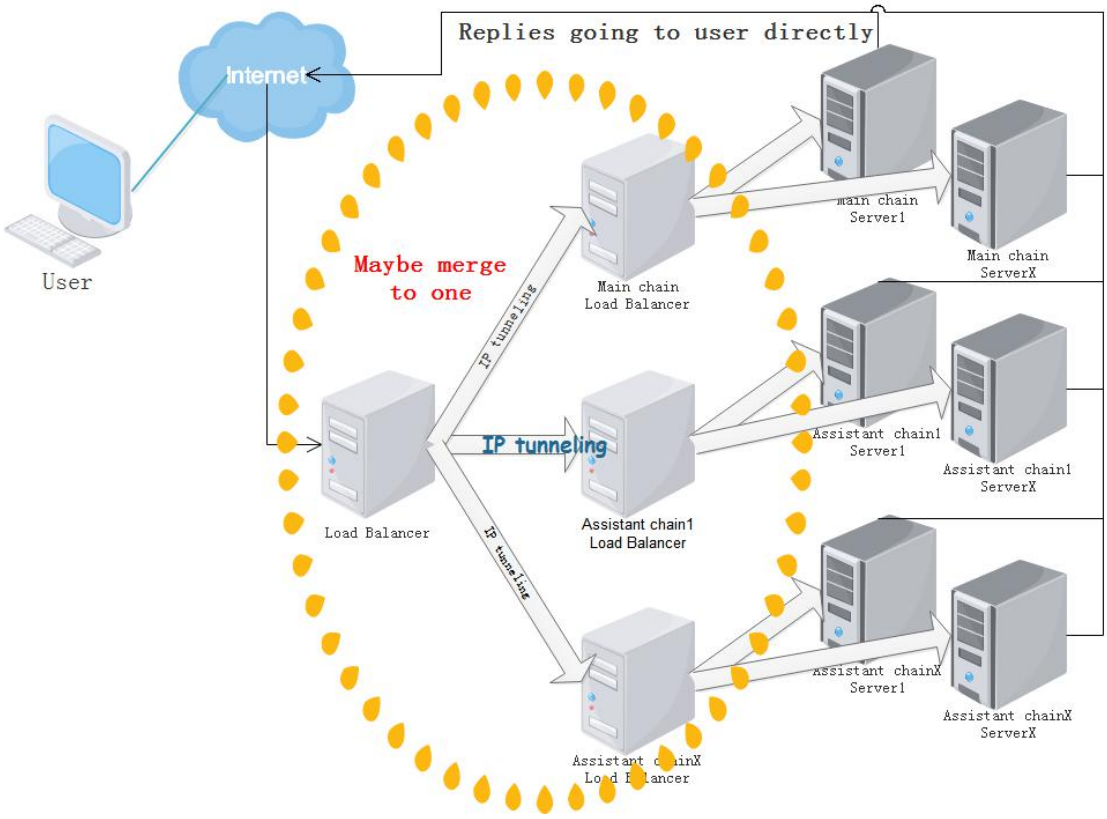
隔离见证的概念是指：一旦区块链完成不可逆交易后，交易签名便会无关紧要。因此，即使签名数据被缩减，当前状态仍可有效导出。由于签名占据了多数事务的大量数据，隔离见证可显著减少磁盘存储空间和同步时间。

相同概念也可使用到整个区块存储中：一旦交易不可逆转地记录在区块链上，区块里仅需永久存储数据库状态和导致状态变迁的交易哈希，而交易明细和交易日志将按服务节点配置的保留时间暂时存储。所有的数据库状态、交易明细和交易日志，都保存在数据节点的历史数据库里。

也可以这样理解，每条链都存在两条并行的区块链，一条是存储数据库最新状态的状态链，一条是存储所有数据的历史链，历史链仅存在于数据节点中。所有的服务节点都需要同步状态链，不需要同步历史链，除非他自己请求同步。



4.2.5.6 网络扑拓图



4.3 商业生态

本生态坚持做实业，目标是改变世界上每个用户的生活方式。本生态的各个链之间的商业生态是相互依赖的，许多业务是由多条链协同完成的。我们担负着把整个群生态推广到全世界，因此每条链的链交易手续费（类似 Bitcoin 的矿工费）都转入贡献基金。

4.3.1 主链

管理账户、数字货币、智能合约、和副链之间的交互等等。智能合约只能发布到主链上，但是能与副链交互。

4.3.2 支付链

支付链是央行、银行、支付公司、交易所、货币兑换公司的有机结合体。支持法币-法币、法币-数字货币、数字货币-数字货币交易，实现转账（同币种），汇款（跨币种），货币兑换（同账户），小额的快捷支付，信用预支付等业务功能。

4.3.3 信用链

追踪账户的信用值。交易分为奖励、扣除、定期自生长三大类。

4.3.4 认证链

认证账户的法人身份，根据与每个国家的合作程度，采取户籍登记或 KYC 审核。本链将采用密码学算法和零知识证明算法保护所有的隐私。

4.3.5 公证链

证明行为、事实、合同、遗嘱等各种形式事务的真实性、合法性。本链将采用密码

学算法和零知识证明算法保护所有的隐私。

4.3.6 行业链

各行各业的行业链集合。

4.3.7 小额快捷支付（移动支付）

支付链推出遍布世界每个角落的小额快捷支付，支持各种法币和数字货币交易。

4.3.8 守护神和守护精灵

在信用链上推出守护神和守护精灵，他的悟性能提高**信用增长因子**，他的基础属性则会叠加到主人的信用值中。

守护神需要主链辅助，全部或部分副链配合（仅指公有链），因为他的仙法有些是适用于所有链的。守护精灵的魔法仅适用于信用链。一个账户可以拥有多个守护神和守护精灵，他们的仙法和魔法效果可以叠加，但是悟性和基础属性不能叠加。后续还会和支付链的信用预支付功能相结合。至于 UI 效果展现和其它功能，暂定和钱包相结合，也有可能专门开发一个应用。

4.3.8.1 守护神

守护神在整个生态系统中是独一无二的，由神话人物和历史名人组成。每个守护神都拥有自己独特的仙法。基础属性待定，悟性范围是 60～100，即提高 60～100 倍信用增长因子。关联项的合理性、不能影响区块链本质、不损害用户利益、伦理道德、尊重名人、需要关联的进驻副链等，守护神必须满足这些规定要素才能推出，每个要素都不能牵强附会。守护神仅由拍卖获得，无婚配功能，但是神能创造万物，由其创造的守护精灵都是首代的。如果完全是由进驻链设计的守护神，拍卖后的 80%收益归其所有。

如果以下表格中的问号都不能解决，那么本生态就只有两个守护神。

人物	性别	悟性	仙法	影响链	仙法特点	合理性说明
赵子龙	男	81	七进七出	全部链	1、免所有的交易手续费； 2、交易立即被处理； 3、没有一段时间内的交易数量限制；	1、不损害用户利益； 2、很多链都有高矿工费立即被处理的机制； 3、有些链采取该机制只是为了防止 DDOS 攻击； 综上，能满足规定要素。
诸葛亮	男	95	草船借箭	主链 支付链	1、无抵押和利息，最高能融币 1000 万，期限为 1 年；	类似于证券行业的融资融券，由保稳基金担保，没有损害用

					2、全部归还后就可以再次融币； 3、在融币期间不能出售该守护神； 4、到期后不能归还本币，则冻结账户，并回收该守护神重新拍卖；	户利益； 综上，能满足规定要素。
鲁班	男	89	？	？ 建筑链	？	？
女娲	女	96	？	？	？	？
爱因斯坦	男	95	？	？	？	？
丘比特	男	79	？ 爱情之箭	？ 爱情链 婚介链	？	？
雅典娜	女	85	？	？ 艺术链 公证链	？	？
上帝	男	100	？ 上帝之手	？ 证券链	？	？
？	？		？	？	？	？

4.3.8.2 守护精灵

守护精灵由精灵、哺乳动物（如猫、狗、熊猫、龙、凤凰等）组成，各自拥有不同的魔法，如龙吟、凤鸣，魔法仅影响信用链，而且施展后不一定每次都有效。基础属性待定，悟性范围是 2～20（出生时随机产生）。同种类的异性可以婚配生育。获得途径有拍卖、部分初始账户赠送，以及繁衍和守护神创造。每个物种仅推出公母各 1000（暂定）的初始数量。

4.4 数字货币

主链和所有公有链统一发行同一种数字货币，这种币可以在本生态系统中的所有链（包括主链、公有链、联盟和私有链）中流通。每条公有链限定发行总量为 **2.1** 亿个数字货币，这些币都是用来奖励在生成区块时做出贡献的节点。公有链不允许预发行数字货币，只有主链才能预发行 **10** 亿个币，用于主链和公益性公链开发，和保持本生态系统的可持续发展。

公有链能预发行自己的 token，联盟链和私有链也可以发行自己的 token（预发行或区块奖励），但是这些 token 只能在自己的链中流通。也就是说整个生态系统中只有一种数字货币和 N 种 token。

在本生态中，这种数字货币和 N 种 token 任意两者之间就能自由交易。本生态自

带的支付公链可以进行法币交易、法币-数字货币交易、币币交易，不再需要任何外部的交易所。我们将坚持数字货币不上外部的交易所（不主动上，被动则保留权利），而禁止 token 上任何外部的交易所，目的是限制纯粹以 ICO 为目的的 token。

要作为一种全球性流通的稳定的数字货币，必须具备以下几个要素：

- 流通盘要适当，不能太大也不能太小；
- 价格不能太高，要和物价相对持平；
- 价格要在一段时间里保持相对稳定，不能大涨或大跌；
- 需要好的流通性，要在全球范围内大力推广和运营；

假设本生态有 **1** 条主链，**N** 条公有链，**M** 条联盟或私有链，那么整个生态的数字货币总量 **Y**（单位：亿）为： **Y = 10 + 2.1 *（1 + N）**

数字货币的发行价是 **1.68** 元（CNY），主链预发行的 **10** 亿个币使用计划为：

4.4.1 保稳基金

总额度为 **6** 亿个币。这是担保和平稳基金。这部分币将会放入一个独立账户中，做到每一笔交易都是公开透明、可追溯的。

- 给本生态的业务作全担保或部分担保，总额度不超过 3 亿个币。
- 当币价大涨或大跌的时候，将动用平稳基金稳定币价。

4.4.2 贡献基金

初始额度为 **2** 亿个币，这部分币保留在创世账户里，并在社区公开全部的支出。后续拍卖优质账户名称、拍卖守护神和守护精灵、交易手续费等得到的币将转入本基金。

本基金用于奖励给当下或今后对本生态作出贡献的团体或个人。如密码学算法、零知识证明算法、压缩算法、数据库、通讯、Boost、序列化等各个领域，或提出 EIP 和 bug 的，还有整个创始团队，以及运营最好的进驻链和应用，“运气差”的候选生产者节点。

这是一种可持续化的奖励机制，类似于上市公司的分红，半年一期，在主网上线后启动第一期分红。这部分的奖励方案后续再细化。

4.4.3 赠送奖励

总额度为 **1** 亿个币，**送完则止**，拍前一定要注意智能合约的币余额。

本生态以智能合约的方式公开拍卖 **2** 万个**初始账户**，底价都为 5 个 ETH，时间为 187 天。前 97 天买的都赠送 3500 个币，剩下的时间都赠送 2000 个币。前 37 天买的还加送一个**守护精灵**。对于拍卖价超过 5 个 ETH 的部分，每满一个 ETH 再额外赠送 800 个币。即如果首月你以 5 个 ETH 买下，你将获得一个初始账户和守护精灵和 3500 个币；如果首月你以 8.9 ETH 买下，你将获得一个初始账户和守护精灵和 5900 个币（3500 + 800 * 3）。合约结束后，拍卖价最高者（仅一个，价格相同者，以拍卖时间早的优先），加送一个**守护神**。

初始账户都拥有挑选账户优质名称（长度 2 至 10）的专享权利。名称如有一样者，则按照拍卖价高、购买时间早的优先原则执行，落选者需要重新挑选。这些账户都是主网上线时就已经创建好的初始账户，对比一下 EOS 账户的拍卖价格，相当于白送。请

查看“账户”这一章获取更多介绍。

初始账户是优质账户名称爱好者追求的目标，而守护神是财富自由者的游戏，不建议没有物质基础的用户参与。一个 ETH 账户只能拍一个初始账户。

智能合约地址：

https://etherscan.io/address/0x54850c1601826b3958b25bd995efc26a52044c0a

4.4.4 进驻链奖励

总额度为 **5000 万**个币。前 20 个进驻的公有链，每个链可以申请奖励 100 万至 1000 万个币。

按照用户量的多少、链的影响力和对生态的贡献力来评估奖励额度，送完则止。

本生态欢迎现有的各行各业的孤链加入，一起创建共生共荣的区块链群生态系统。

4.4.5 进驻应用奖励

总额度为 **4800 万**个币。前 500 个进驻应用商城的 APP 或 DAPP，不管是中心化的还是去中心化的，不管是 PC 端还是移动端，每个可以申请奖励 1 万至 200 万个币。

按照用户量的多少、应用的影响力和对生态的贡献力来评估奖励额度，送完则止。

很多现有的中心化应用，如微信、淘宝、京东、抖音、绝地求生、王者荣耀等，只要接入本生态的主链、认证链、信用链、公证链、支付链或其它的任意一个或多个链，就可以参与到本生态中来。

4.4.6 空投奖励

总额度为 **200 万**个币。

加入官方的 Telegram（或中文版 BiYong）后，并在下面 4 个贴中的任意一个回帖（回复 Telegram 的用户名或手机号）的自然人，每人奖励 5 个币，不能重复领取。如需 ETH 的本生态 token，还可以留下 ETH 的账户地址。

巴比特（限前 10 万人） https://www.8btc.com/

bitcointalk 中文区（限前 5 万人）

https://bitcointalk.org/index.php?topic=5063573.new#new

bitcointalk（限前 15 万人） https://bitcointalk.org/

reddit（限前 10 万人） https://www.reddit.com/

Telegram: https://t.me/cesfans

BiYong: https://0.plus/cesfans

白皮书：

GitHub: https://github.com/sunnygood/CES/tree/master/whitepaper

官网：

4.5 生态治理

每条链都应该有自己的社区来管理本链的事务，本生态的社区只管理本生态所有链需要遵守的规章制度和行为准则，和主链事务，我们不干预每条链自己的事务。

本生态的钱包会自带投票表决功能，按照持币比例投票，全民共同决定所有事务。主链有以下事务：

4.5.1 冻结和解冻账户

有时候，某个智能合约表现异常或不可预测，不能按预期执行；应用程序或帐户可能会发现一个可被利用的漏洞。当这些问题不可避免地发生时，本生态有权冻结这些账户。而当这些账户恢复正常后，则可以解冻。

4.5.2 更换账户法人密钥

只要经过认证链的法人认证，就可以更换法人密钥。

4.5.3 组织 EIP 投票

在社区定期发起 EIP 投票，用户也可以在钱包客户端里投票。

4.5.4 进驻链资源分配

在社区分配并公布进驻链的标识 ID 等资源。

4.5.5 兑现贡献奖励

在社区收集贡献清单，定期兑现贡献奖励，并把奖励情况公布在社区专栏里。

4.5.6 紧急变更

如需修复严重 BUG 或损害用户的安全漏洞时，进行的紧急变更。

4.6 模块管理

4.6.1模块发布

整个生态系统的模块都需要附带签名才能发布。

4.6.2模块校验

程序能自动校验每个模块的签名是否正确，验证其是否合法和被篡改。

4.6.3模块更新

分为软更新和硬更新。

4.7 节点分类

4.7.1 按性能分类

4.7.1.1 主干节点

这种节点能自动部署全部公有链；其需要非常庞大的 CPU 运算能力、内存、存储空间、带宽等资源，建议用 IaaS 来搭建。

4.7.1.2 树干节点

部署了部分链的节点（包含主链），根据部署链的个数，来决定选择 IaaS 或普通服务器来搭建。

4.7.1.3 树枝节点

只部署单个副链的节点（包含主链），这种节点一般是该链自己搭建的，仅服务本链，用普通的服务器即可。该节点多是联盟链或私有链的节点。

4.7.2 按功能分类

4.7.2.1 查询节点

检查命令格式、处理查询命令的服务器，这种节点一般是需要淘汰的旧服务器，或由公司、个人搭建的临时服务器。

4.7.2.2 交易节点

检查命令格式、处理查询命令、处理交易命令、共识交易并生成区块的服务器。这类节点需要绑定账户，用以领取区块奖励。对应 6.2 节列表中的候选生产者和生产者。

4.7.2.3 数据节点

存储数据库状态、交易数据（交易明细）、交易日志和其它分析数据等历史数据的服务器。数据节点只有很少的数量。所有的数据节点会组成一个集群，复盘所有数据，分析数据的正确性，一旦发现异常数据，将会提交所有数据节点共识，一旦确认数据异常，将会处理提交该数据的节点。

5 分片技术

本生态解决共识效率低的方法是在共识算法中引入分片技术，来提高所有区块链的可扩展性，实现高吞吐量。本生态将划分成 16（暂定数）个片区，以发起账户为标的，那么所有的交易就分为同片区交易和跨片区交易两种；同区交易将以各区自己的共识结果为准，会立即被打包；而跨片区交易则需要所有片区一起共识，会存在一定的延迟。采用了分片技术，既提高了共识效率，也减少了传输的数据冗余（很多数据将不再采取广播的方式传输），TPS 比现有的区块链至少能提高几十倍，甚至成百上千倍（和分片片区的数量存在抛物线关系），本生态的 TPS 目标是 3 万左右，完全可以支撑大规模商业化的需求。要知道，VISA 的 TPS 才 2 万多而已。

共识算法的分片方案有以下 3 种：

5.1 按地域分片

账户和服务节点都按地域（或按时区或其它）分片。此种算法实现简单，但是有一点点中心化的味道，具体请查看 6.1.1 节。

5.2 由算法半随机分片

账户或服务节点当中的一个按地域（或按时区或其它）分片，另外一个则由共识算法随机分片，如账户名称哈希分片、节点 IP 哈希分片。此种算法相对折中，具体请查看 6.1.2 节。

5.3 由算法全随机分片

账户和服务节点都由共识算法随机分片。此种算法最为复杂，具体请查看 6.1.3 节。

6 共识算法

本生态采用 X 次分片 Y 次共识的共识机制（X，Y = [1, N)，此处先以 1 次分片 2 次共识来介绍）。这是基于分片技术完全去中心化的共识算法，即带分片的贡献证明算法（Byzantine Fault Tolerance-Proof of Contribution with Sharding，BFT-PCS）。

根据这种算法，只要满足一定的能力要求，任何节点都可以成为区块生产者，其中软件版本、交易处理速度和交易处理总量是硬性指标。贡献证明的依据是工作量证明，已经正常处理了 10 万笔交易的节点，总比才处理了 10 笔交易的节点可靠些。共识不以交易的顺序性为依据，而以写入区块的时间（first-to-block）为依据。

6.1 算法实现

6.1.1 BFT-PCS(A)

本算法的账户和服务节点都已经按地域分成 16（暂定）个片区，步骤大致如下：

1、根据交易处理总量、网速、CPU、内存、存储空间等评估出节点的能力指标；

2、当能力指标达到预定阀值的节点把必须同步的信息都同步后，就可以被添加到候选生产者列表；如果掉线或其它原因造成不同步，将会被暂时移除出候选生产者列表；

3、每条链的第一个生产者列表，由创世区块的创世账户所绑定的节点产生，后续则由上一轮的第 4 个生产节点（第 16 * ¼个）随机产生；

4、生产者列表的产生方法是：

第一步从 16 个片区各自的候选生产者列表中抽取 4 个（暂定）节点；如果某个片区的节点数为 0，则不抽取节点，该片区交易都以跨片区处理；如果只有 1 个节点，则不抽取替补节点；除非节点数不够，否则是不允许自己抽取自己的；

第二步把第一次从各片区抽取的 16 个节点设置为各片区的预定生产节点，后面抽取的节点设置为为替补生产节点；

第三步把生产者列表广播到全网。

5、在第 8 个生产节点（第 16 * ½个）的生产时间段内，检查下一轮生产者列表是否存在作弊，如果作弊则把生成该列表的节点加入到黑名单；并由本生产节点重新生成；如果合法则所有节点都需要存储下一轮的生产者列表；

6、当生产者列表中有预定生产节点不能正常工作，将会立即由替补节点补上，如果替补节点也不能正常工作，那么该片区将会被跳过，由下一个片区节点继续生产区块；

7、按照生产者列表的固定顺序，依次由生产节点连续生产 4（暂定）个区块，每一秒产生一个区块；以发起账户为标的，发起账户不是本片区的交易将会被转发到其片区的服务节点处理；在一个区块共识过程中，先共识同片区交易，再共识跨片区交易。每个片区的节点（或仅由该片区 1 预定 3 替补节点）仅共识自己片区的同片区交易；然后只由 16 个预定生产者一起共识跨片区交易。16 个预定生产者中的同片区的交易立即被打包进区块，而跨片区交易则需要他们一起共识通过后才打包进区块；一个区块的绝大部分时间都用于共识跨片区的交易，但是达成共识的交易量却远远少于同片区的；

8、每一轮的总时间为 64 秒（16 * 4），每轮结束后，由本轮最后一个生产节点把本轮产生的所有奖励币平均分配给生产者列表中的所有节点。

9、按照步骤 3 产生的下一轮生产者列表开始新的一轮共识；

6.1.2 BFT-PCS(B)

假设服务节点已经分片，账户由算法分片，该算法步骤和 A 差不多，在此省略。

假设账户已经分片，服务节点由算法分片。步骤大致如下：

1、同 A；

2、同 A；

3、同 A；

4、生产者列表的产生方法是：

第一步把候选生产者列表中的节点随机分成 16（暂定）个片区；如果节点数不足的时候，有多少个节点就分成多少片区，此时存在一个节点分片对应多个账户分片；

第二步从 16 个片区各自的候选生产者列表中抽取 4 个（暂定）节点；如果只有 1 个节点，则不抽取替补节点；除非节点数不够，否则是不允许自己抽取自己的；

第三步把第一次从各片区抽取的 16 个节点设置为各片区的预定生产节点，后面抽取的节点设置为为替补生产节点。

第四步把所有节点的分片结果和生产者列表广播到全网。

5、在第 8 个生产节点（第 16 * ½个）的生产时间段内，检查下一轮生产者列表是否存在作弊，如果作弊则把生成该列表的节点加入到黑名单；并由本生产节点重新生成；如果合法则所有节点都需要存储下一轮的分片结果和生产者列表；

6、同 A；

7、同 A；

8、同 A；

9、按照步骤 3 产生的下一轮分片结果和生产者列表开始新的一轮共识；

6.1.3 BFT-PCS(C)

本算法账户和服务节点都由算法分片，如根据账户名称哈希分片、节点 IP 哈希分片。步骤大致如下：

1、同 A；

2、同 A；

3、同 A；

4、生产者列表的产生方法是：

第一步同 B；

第二步同 B；

第三步同 B；

第四步把所有账户随机分成 X 个片区（X=节点分片）；

第五步把所有账户和节点的分片结果、生产者列表广播到全网。

5、同 B；

6、同 A；

7、同 A；

8、同 A；

9、同 B；

6.2 算法特点

本算法的节点功能权限分类如下：

角色		检查命令（格式等） 处理查询命令	处理交易	共识	生产区块	奖励币
查询节点		√	×	×	×	×
候选生产者		√	√	×	×	×
生产者	预定	√	√	√	√	√
	替补	√	√	√	未知	√

本算法具有极高的随机性和未知性，做到完全去中心化，也杜绝了作弊的可能性。如果一个节点被全网认定为不可信任或作弊者，将会被添加到黑名单，从此该节点不会再被添加到候选生产者列表。该节点所绑定的账户也会受到相应的惩罚。

理论上，本生态的区块链不会经历任何分叉，因为在区块生产过程中，生产者是合作而不是竞争关系，而且生产者是可追溯的。如果出现分叉（非硬分叉），则意味着这是人为故意制造的分叉，共识将自动溯源并切换到合法的链上。

共识算法中增加拜占庭容错机制。基于多重签名，通过允许所有预定生产者签署区块，一旦 11（按 16 个片区计算）个生产者签署了一个区块，则这个块被视为不可逆的，不可逆的共识可以在 1 秒内可达成。 如果拜占庭式的生产者签署了两个相同时间戳或相同区块高度的区块，那么算法会自动把该节点添加到黑名单。

6.3 交易确认

本共识算法中，将加入异步拜占庭容错算法(aBFT), 可实现更快的不可逆性。

由于交易写入区块的速度不一致，同分片的交易 1 秒就可以得到不可逆的确认，跨分片的交易需要 1~4 秒才可以得到不可逆的确认。但这对用户来说是可接受的。

7 账户

账户类型分政府单位、组织、公司、个人和初始账户这五种类型。帐户的可读名称长度为 2~10 个字符，由字母和数字组成。在整个生态链中，账户是通行的唯一凭证。

账户名称由创建者自由选择。政府单位、组织、公司账户必须经过认证链认证才能注册，这 3 种类型都自带后缀。个人账户不强制认证，但是这样丢失密钥后就没有任何途径可以修改法人密钥和 PIN。自由创建的账户长度只能是 10 个字符，其它长度的只能由拍卖获得，上线后拍卖获得的账户不属于初始账户；初始账户是特殊的个人账户，这些账户都是元老级的，只能在众筹阶段的智能合约里拍卖获得。

- 政府单位以.gov 为后缀：china.gov，usa.gov
- 组织以.org 为后缀：abc.org
- 公司以.cl 为后缀：google.cl，apple.cl，icbc.cl
- 普通个人账户：oneperson9，abcdefg123，1234567890
- 初始账户和拍卖的个人账户：games，love，god，baby，money，coin

7.1 操作和处理程序

每个帐户可以将结构化的操作发送到其他帐户，并且可以定义脚本来处理收到的操作。系统为每个帐户提供自己的专用数据库，只能由自己的操作处理程序访问。操作处

理脚本还可以将操作发送到其他账户。消息和自动操作处理程序的组合是智能合约的方式。

为支持并发执行操作，每个账户同样可以在数据库内定义任意数量的范围。区块生产者将以这样一种方式来安排事务，即对存储器访问范围没有冲突，因此他们可以并发执行。

7.2 基于角色的权限管理

一个账户里，最多可以有五级的权限管理。这五级角色分别为法人、管理级、使用级、合约级、旁观级（不可执行交易，示例是绑定服务节点）。系统提供了一种自定义式权限管理系统，可以对帐户进行细粒度、高级别的控制，确定每一种角色可以做什么和什么时候做什么。

认证和权限管理必须标准化，并与应用程序的业务逻辑分开，这是至关重要的。这使得开发工具能够以通用方式管理权限，并为优化性能提供巨大空间。

每个帐户都可以通过其他帐户和私钥的任何加权组合来控制。这创建了一个分层的权限结构，真实反映了权限的组织方式，并使得多用户对账户的控制比以往更容易。允许帐户定义与其他账户和密钥的组合方式，并且把这个组合以特定类型的消息发送到另一个账户。

7.2.1 权限映射

允许每个帐户定义其它账户与自己的账户角色之间的映射。例如一个公司账户，可以把员工的账户映射到对应的角色中，通过此映射，这些员工可以作为公司帐户使用者，使用公司账户为其分配的所属资金，但是他们仍然使用自己的密钥来签名。

7.2.2 并发权限评估

系统首先会检查是否存在权限映射，一旦识别出映射，则使用多签名阈值和对应角色相关联的权限来验证签名权限。如果不存在映射，那么它会遍历父类权限，最后遍历所有者的权限。

权限评估过程是“只读”的，并且对事务所做的权限更改直到块结束才会生效。这意味着所有交易的所有密钥和权限评估可以并发执行。此外，这意味着可以快速验证权限，而不需要重新启动昂贵的应用程序逻辑。最后，这意味着交易权限可以在接收到待处理的交易时进行评估，而在应用它们时无需重新评估。

从整体来看，权限验证占验证交易所需计算的很大一部分。让权限验证成为一个只读与可并发化的过程可以显著提升性能。

当重播区块链以从动作日志重新生成确定性状态时，不需要再次评估权限。因为事务包含在已知的状态良好的区块中，可以让其跳过这一步骤。这极大减少了重放区块链时消耗的计算量。

7.3 双重密钥保护

本生态将采用另外一种椭圆曲线算法，除了私钥之外，将增加用户密码 PIN（长度为 4-12 的数字），采取特殊机制由 PIN 计算生成 PIN Block，而 PIN Block 共同参与签名和验签的计算，这样只有私钥和 PIN 都正确，签名才能验证通过，交易才能成功。

用户只要把私钥和 PIN 分开存储，或者 PIN 完全不存储，只留存在记忆中，这样就极大的增强了安全性。别人就算盗取了您的私钥，也无法盗取你的资产。

私钥和 PIN 是同等重要的，用户必须都要保管好。

7.4 被盗帐户恢复

为用户提供了账户被盗时恢复其帐户控制的方法，前提是其经过认证链认证。

- 私钥不可找回，私钥被盗取或丢失后，只有通过法人认证，才可以重新设置法人的公钥，否则该账户只能丢弃。
- PIN 可以根据旧 PIN 重置（类似银行修改密码），如果忘记 PIN，则需要通过法人认证才可以重置。

8 脚本和虚拟机

脚本语言和虚拟机的细节是特定于实现的细节，这些细节大多独立于技术的设计。任何语言或虚拟机都可以与 API 集成在一起，这些语言或虚拟机具有足够的性能，并且具有确定性和正确的沙箱效果。

8.1 明确的指令架构

所有账户间发送的指令都是通过区块链共识状态模式来定义的。该架构允许在二进制和 JSON 表示形式中无缝转换。

8.2 定义数据库的架构

数据库状态也使用类似的模式进行定义。 这确保了所有应用程序存储的数据都可被解释为人类可读的 JSON 格式，但以二进制的效率进行存储和操作。

8.3 通用多索引数据库 API

开发智能合约需确定的数据库模式来追踪，存储和查找数据。开发人员通常需要对多个字段进行排序或索引的相同数据，并保持所有索引之间的一致性。

8.4 身份验证与应用程序分开

为了最大化并行机会和最大限度地减少与事务日志中重新生成应用程序状态相关的计算债务，将逻辑验证分为三部分：

1. 验证 Action 是否内部一致;
2. 验证所有先决条件是否有效;
3. 修改应用程序状态。

验证 Action 内部的一致性是只读的，不需要访问区块链状态。这意味着它能以最大并行度执行。验证的先决条件（如所需的平衡）是只读的，因此也可以从并发性中受益。只有修改应用程序状态才需写入权限，并且必须按顺序处理每个应用程序。身份验证是验证可以应用操作的只读过程。事实上，应用程序在做这项工作，实时两项计算都需要执行，但是一旦交易包含在区块链中，就不再需要执行认证操作。

8.5 代码与实例分开

智能合约都采用模块化的方式开发。一个相同的智能合约模块，在区块中只会存储一份，把智能合约的代码与执行实例分开，有利于提高代码的复用率，也有利于减少区

块的存储空间。

开发者上传智能合约代码到应用商城，供用户浏览，并把编译后的模块发布到区块中。当用户使用该模块后，需要一次性支付开发者预设置的费用。因为发布和直接使用的费用差不多，加上发布需要审核，这样既能保护开发者的权益也能鼓励用户使用现有的模块。

8.6 WASM

WASM 是构建高性能 Web 的最新标准，通过少量适配就可以被明确定义和沙箱化。它已经得到业界的广泛支持，目前主流的浏览器都已经支持 WASM。

本生态系统将采用 WASM 来构建智能合约，开发语言为 C++。

我们将提供基于 C2I 架构的智能合约接口模块和适配模块，让任何语言开发的 APP/DAPP 都可以直接和智能合约交互。

9 应用程序确定性的并行执行

区块链共识取决于确定性（可重现）的行为。这意味着所有并发执行都不能使用互斥体或其他锁定基元。如果没有锁定，必须有一些方法来保证并发执行的帐户不会产生非确定性结果。

在区块链中，一旦执行并发操作，区块生成器需要将消息传递到独立的线程中，以便进行并发评估，但是生成计划的过程无需确定。这意味着区块生成器可以利用并发算法安排交易。

并发执行还意味着脚本生成新消息时，它不会立即发送，而是在下一个周期中发送。无法立即发送的原因是接收方可能会在另一个线程中主动修改自己的状态。

9.1 最小化通信延迟

延迟是指一个帐户将消息发送到另一个帐户并收到响应的时间。目标是使两个帐户能够在单个区块内来回交换消息，而不必在每个消息之间等待 1 秒。为了实现这一点，系统将每个块分为周期（cycle）。每个周期分为线程（thread），每个线程包含交易列表。每个交易包含一组要传递的消息。该结构可以可视化为树状结构，其中各层按顺序并发处理。

区块

区域（分片）

周期（顺序）

线程（并发）

交易（顺序）

消息（顺序）

在一个周期中生成的交易可以在任何后续周期或区块中传送。区块生产者不断把周期添加到区块中，直到达到最长的执行时间，或者没有新生成的事务要交付。可以使用区块的静态分析来证明在给定周期内，两个线程内不包含修改同一个帐户的交易。只要一直保持这种静态分析机制，就可以通过并发运行所有线程来处理区块。

9.2 只读消息处理

某些帐户可能能够以通过/未通过的方式处理操作，而不必修改其内部状态。在这种情况下，只要特定账户的只读消息处理程序包含在特定周期内的一个或多个线程中，这些处理程序就可以并发执行。

9.3 多账户原子交易

有时最好确保动作被多个账户以原子方式交付和接受。在这种情况下，两个操作都放在同一个交易中，两个账户分配至同一个线程，消息按顺序执行。

9.4 上下文无关操作

上下文无关操作仅涉及需要用到交易数据的计算，而不涉及区块链状态。例如，签名验证是一种仅需交易数据和签名以确定签署事务的公钥的计算。签名验证在区块链必须执行的计算中，属于最昂贵的单个计算之一，但由于此计算是上下文无关的，因此可并发执行。

上下文无关操作与其他用户操作类似，只是它们无法访问区块链状态来执行验证。这不仅使系统能够并发处理诸如签名验证等所有上下文无关操作，更重要的是可以实现通用签名验证。

10 与区块链节点通信

10.1 交易延迟

与区块链通信时，应用必须 100%确定交易已不可逆后，再视该结果为最终结果。

10.2 完整性证明

在区块链底层，每个账户都拥有自己独立的流水号。在命令中增加账户的流水号，可以证明帐户的所有指令均已被处理，以用户的操作频率来看，交易都是按序处理的。