China Blockchain Conference

中国原创的公链模式探索

——兼论EcoBall区块链操作系统设计与实现

胡振生

个人简介

胡振生

- 20+年软件开发管理工作经验
- 夸克链科技创始人
- EcoBall思想理论体系设计者
- 武汉大学-夸克链联合研究中心副主任

申报区块链发明专利25项，20+年软件设计与开发管理工作经验，设计多款区块链行业应用解决方案（物联网、文旅、健康、游戏、积分、钱包、交易所、区块链矿机等）


1、公链及其体系设计
2、高并发处理实现
公有链
面向千万DAPP应用
3、去中心化分布式存储
4、token经济与监管
5、共建共享

China Blockchain Conference

1、公链及其体系设计

公链

公链是公有区块链（PublicBlockChains）的简称，又称公有链。

公链是区块链基础技术设施，是区块链世界的“操作系统”，它支撑起区块链大规模商业化工程级应用。

公链为成千上万区块链应用DAPP搭建起分布式数据存储空间、网络传输环境、交易和计算通道，利用加密算法保证网络安全，通过共识机制和激励机制实现节点网络的正常运行。公链需要提供API接口供开发者调用，以开发符合公链生态的应用。

公链是构建人类社会可信价值互联体的基石。

EcoBall（ABA)区块链操作系统设计

EcoBall（ABA)是我们受托设计开发的一款兼容性区块链操作系统，EcoBall（ABA)公链平台+EcoBall联盟链平台，其目标是构建人类社会可信价值互联体：

第一阶段目标是Platform级产品：真正实现区块链大规模商业化工程级应用，满足不同场景DAPP落地应用的需要。

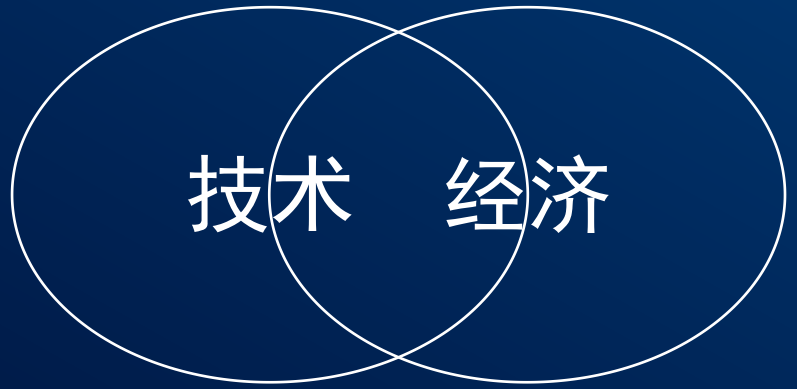
第二阶段目标是BlockChain Operating Systems，真正意义上的区块链操作系统。

因为区块链是全新物种，只有在区块链实现大规模落地应用后，我们那时设计的区块链操作系统才是符合需要的产品。我们用已知的PC互联网时代的OS思想去设计一个全新物种的OS，有悖科学方法论原则。

EcoBall（ABA）公有链平台+EcoBall（LBALL)联盟链平台

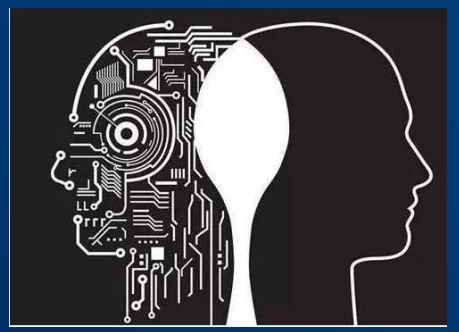
EcoBall（ABA)区块链操作系统设计

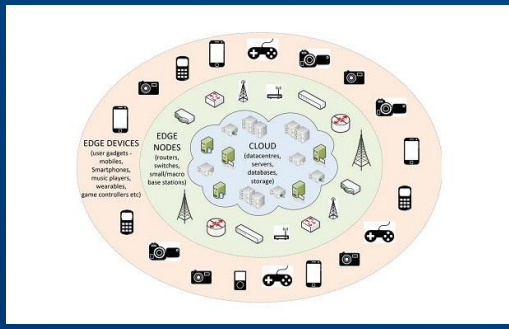
EcoBall（ABA)是复杂系统科学体系，在思想理论体系和顶层架构设计中，除了考虑跨链通信、点对点传输、高并发处理、共识机制、加密算法、分布式数据存储、可扩展性、体系安全等基本技术元素以外，同时必须考虑其有机组成部分的Token奖罚机制、社群自组织管理机制等经济、社会属性元素的实现，同时在公链领域可操作的监管技术实现方式的考量。



区块链上的云计算 – 云计算作为区块链的应用场景

应用场景

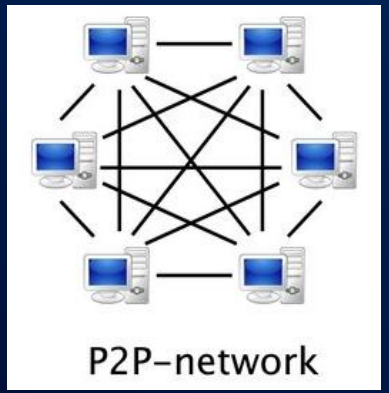




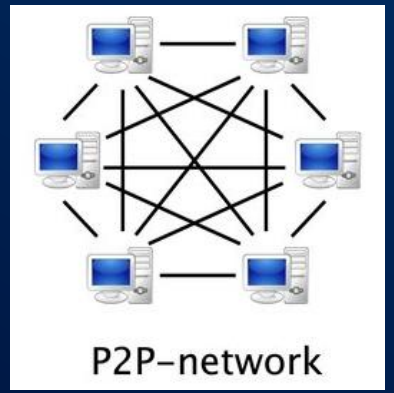
价值网络

区块链激励层　　去信任　　去中心化　　自组织

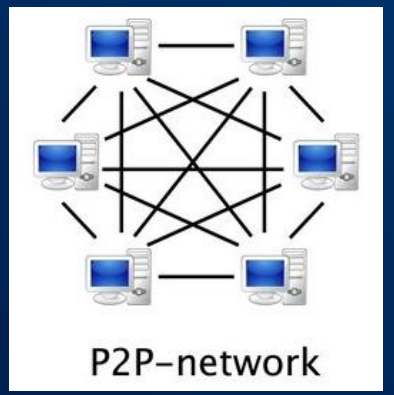
资源层



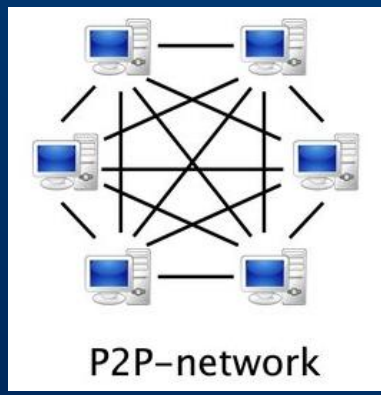
计算节点网络



存储节点网络



AI节点网络



边缘计算节点网络

支撑全产业DAPP大规模应用

EcoBall联盟链场景

EcoBall（ABA）公有链场景

China Blockchain Conference

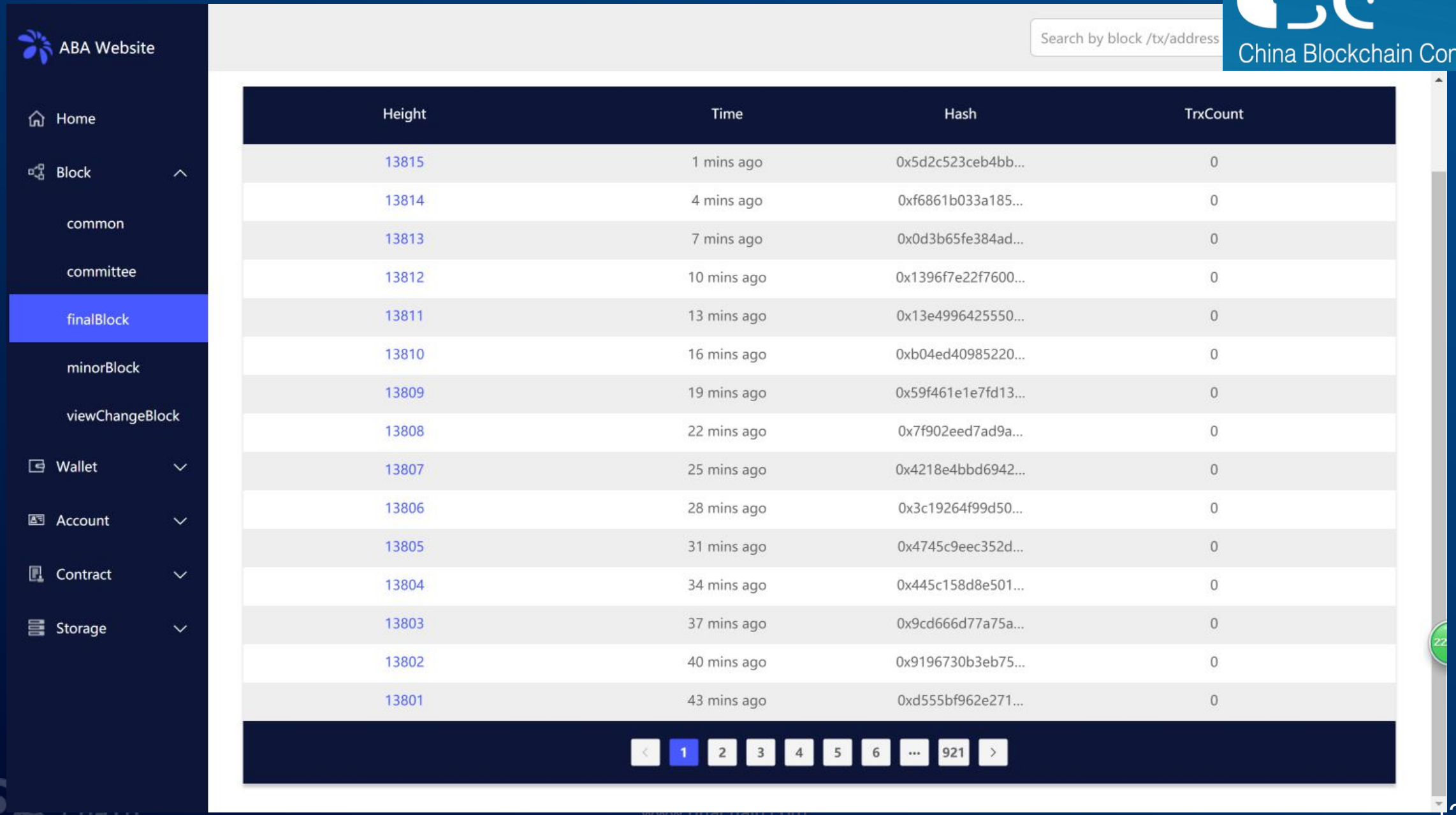
2、高并发处理实现

分片技术举措

分片技术策略:

全网无数逻辑子网，分区间可并行执行。

2018-11-15日，EcoBall平台分片技术成功内测，成为业界第一个在分片技术上运行智能合约的公有链平台。（见程序运行截图）


ABA Website
Home
Block
common
committee
finalBlock
minorBlock
viewChangeBlock
Wallet
Account
Contract
Storage
Search by block /tx/address
Height
Time
Hash
TrxCount
13815 1 mins ago 0x5d2c523ceb4bb... 0
13814 4 mins ago 0xf6861b033a185... 0
13813 7 mins ago 0x0d3b65fe384ad... 0
13812 10 mins ago 0x1396f7e22f7600... 0
13811 13 mins ago 0x13e4996425550... 0
13810 16 mins ago 0xb04ed40985220... 0
13809 19 mins ago 0x59f461e1e7fd13... 0
13808 22 mins ago 0x7f902eed7ad9a... 0
13807 25 mins ago 0x4218e4bbd6942... 0
13806 28 mins ago 0x3c19264f99d50... 0
13805 31 mins ago 0x4745c9eec352d... 0
13804 34 mins ago 0x445c158d8e501... 0
13803 37 mins ago 0x9cd666d77a75a... 0
13802 40 mins ago 0x9196730b3eb75... 0
13801 43 mins ago 0xd555bf962e271... 0
1 2 3 4 5 6 ... 921

融合性共识机制

多共识机制结合:

EcoBall采用融合性共识机制与策略：EcoBall主链采用ABABFT、VRF（可验证随机函数）、DKG&TBLS（阈值签名）、TPOS(阈值POS)等相结合的共识机制，兼顾平台的安全和效率。

$$\langle hash,\pi\rangle \leftarrow VRF_{sk}(seed)p = \frac{\tau}{W} j \leftarrow 0\text{While } \frac{hash}{2^{hashlen}} \notin \left[\sum_{k=0}^{j} B(k;w,p), \sum_{k=0}^{j+1} B(k;w,p)\right) doj \text{ ++ Return } \langle hash,\pi$$

$$\text{If} VerifyVRF_{pk}(\pi,seed,hash) then\text{Return } 0p = \frac{\tau}{W} j \leftarrow 0\text{While} \frac{hash}{2^{hashlen}} \notin \left[\sum_{k=0}^{j} B(k;w,p), \sum_{k=0}^{j+1} B(k;w,p)\right) doj \text{ ++ Return } j$$

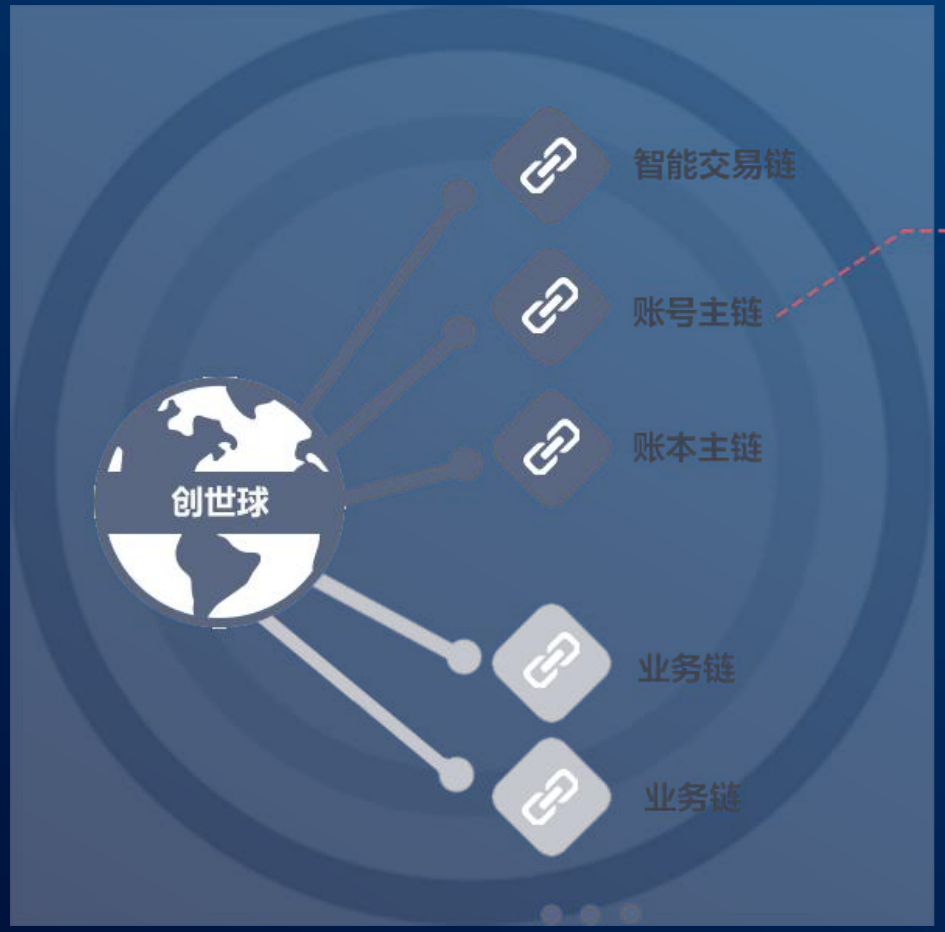
多平台主链与业务主链技术策略

EcoBall采用多平台主链并行：

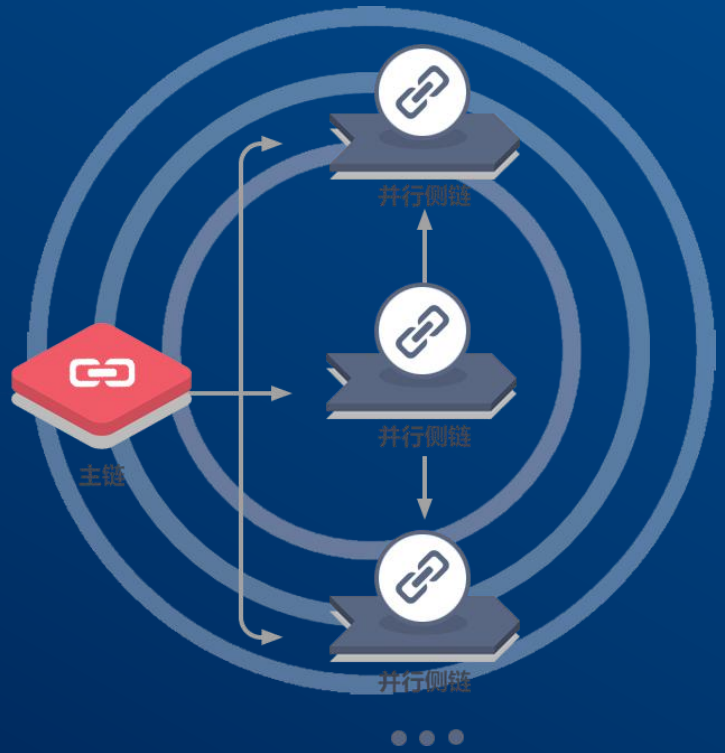
EcoBall通过设置功能主链（交易主链、账号管理链、账本链），各主链功能独立且信息共享，通过功能独立，从而提高每条链的吞吐量及出块速度。

EcoBall采用多业务主链并行：

EcoBall提供一键生成业务主链功能，支持百万业务主链并发运行，每条业务主链逻辑独立互不影响。



生态球关键主链



China Blockchain Conference

3、去中心化分布式存储

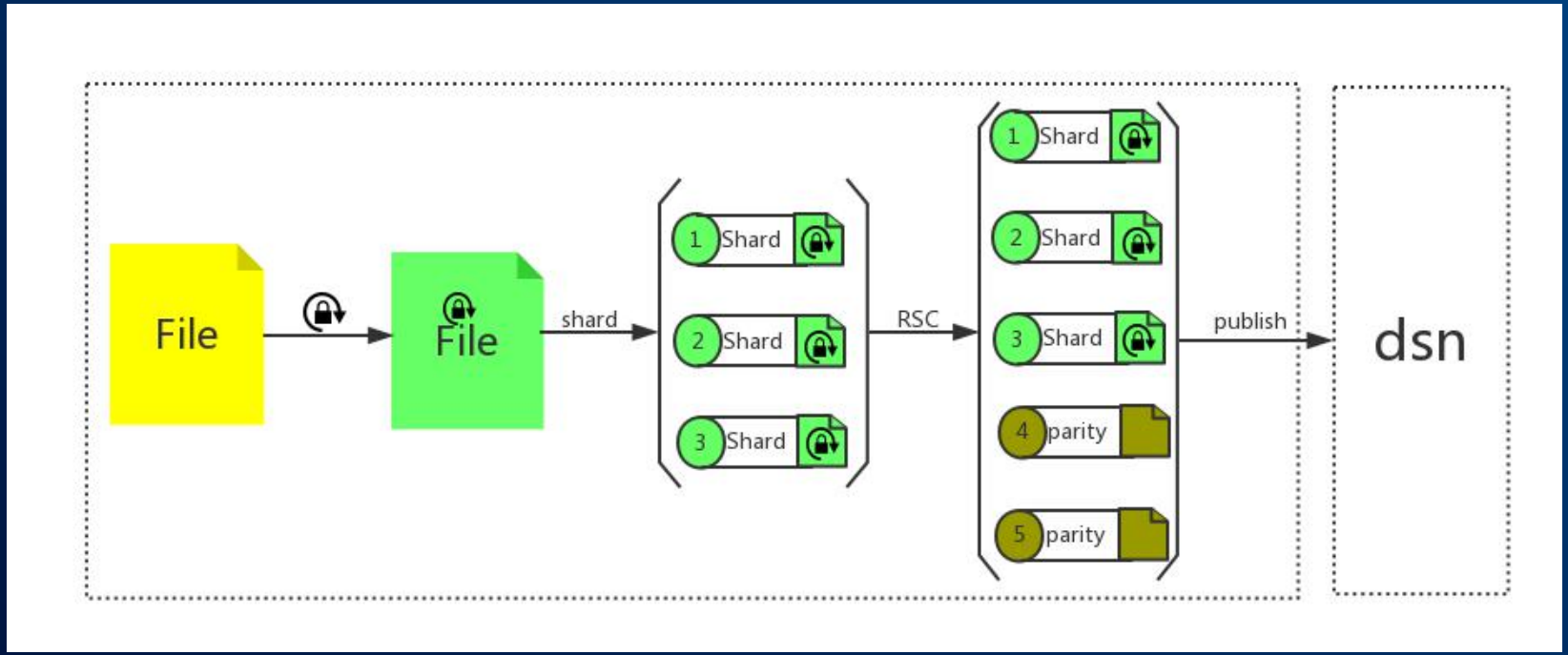
分布式存储技术

Ecoball DSN是去中心化的、安全的存储系统。DSN不仅存储DAPP的重要数据，包括用户的照片、视屏、文档等各种数据，还可以存储区块链的区块、交易等数据。

Ecoball DSN是一台永不停机的、高效的服务器。数据被存储在多个节点上，保证了用户在任何时间和任何地点都可以检索数据，也避免用户数据丢失。

Ecoball DSN技术在IPFS基础上进行改造的产品：对数据进行加密及冗余编码，引入存储激励、带宽激励等激励机制。

保存在IPFS上的数据都是“裸露”的，不安全；数据没有经过冗余编码，一些“冷数据”容易丢失；Ecoball DSN对数据进行加密及冗余编码。

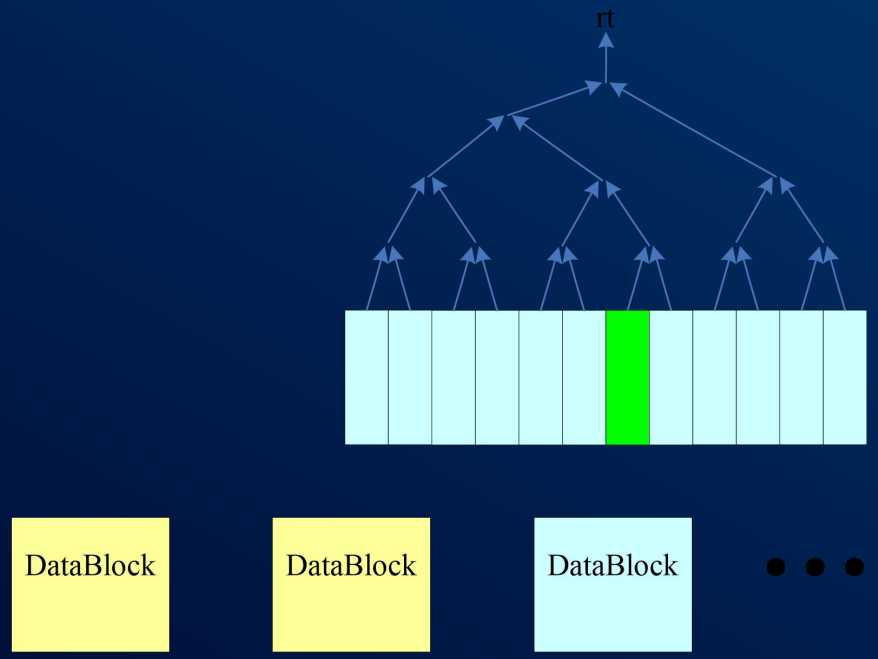

File
File
shard
1 Shard
2 Shard
3 Shard
RSC
1 Shard
2 Shard
3 Shard
4 parity
5 parity
publish
dsn

对IPFS改造

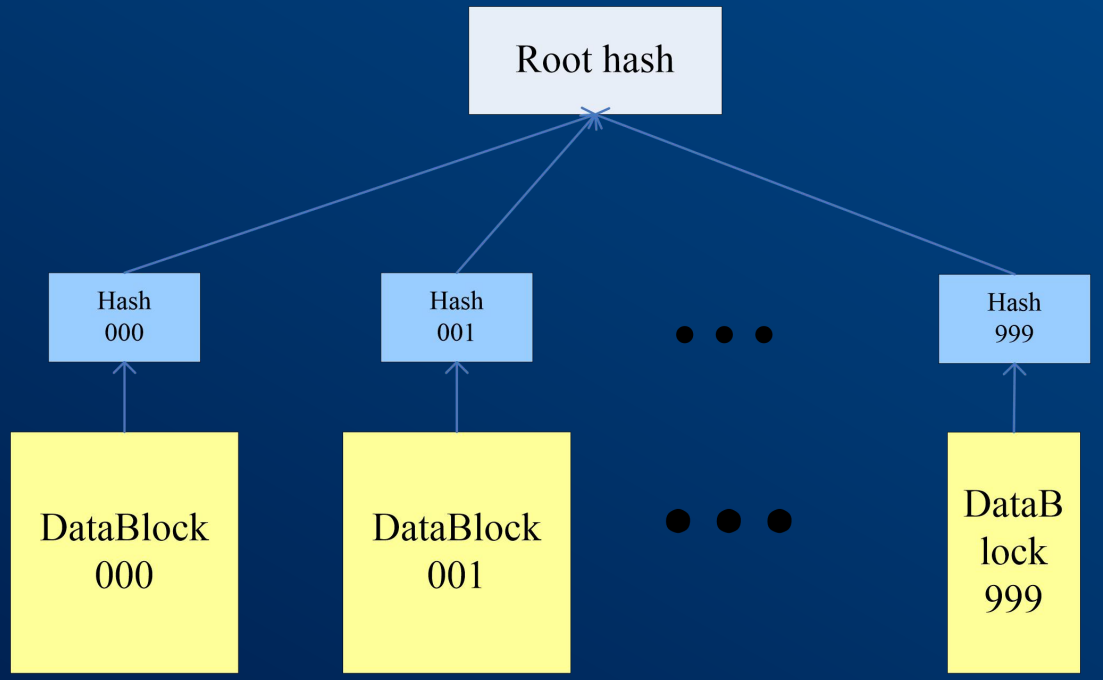
存储与宽带激励

$$r := \frac{t}{T} * \alpha + U * \beta + O * \gamma$$

基于Merkel tree的存储证明算法



数据被切分成多块存储到不同的节点上



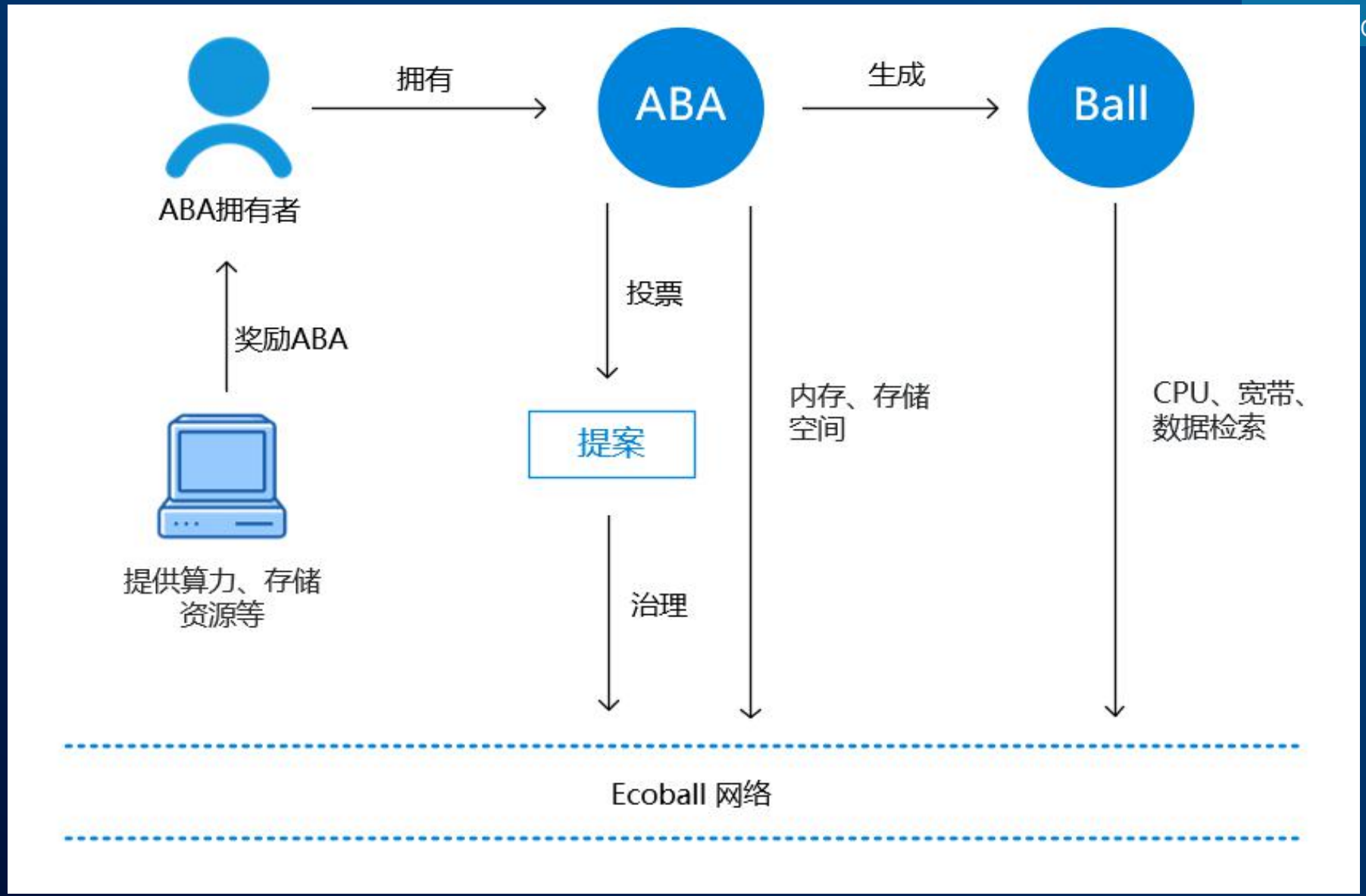
4、token经济与节点经济

双通证模式，以EcoBall（ABA)为例

EcoBall设计ABA与Ball双通证的经济模式：

ABA——是EcoBall生态治理和收益权标志，是权益型通证。一方面，ABA持有者可接收由系统生成的Ball，可使用ABA购买内存、存储空间等消耗型资源，可通过参与EcoBall 网络建设（提供算力、存储、带宽资源等）来获得ABA奖励。另一方面，ABA持有者可参与EcoBall网络重大决策的投票，促进EcoBall生态环境健康发展。

Ball—— 是EcoBall 生态功能型通证，是EcoBall经济体内非消耗型资源的流通通证。算力(CPU)、带宽、数据检索以及其它资源的使用需要抵押一定数量的Ball。Ball不设发行总量，而是通过抵押ABA按一定比例生成，可进行交易流通。


拥有
ABA
生成
Ball
ABA拥有者
投票
奖励ABA
提案
内存、存储
空间
CPU、宽带、
数据检索
提供算力、存储
资源等
治理
Ecoball 网络

节点经济

EcoBall网络由去中心化的节点网络系统支撑运行。

超级节点：EcoBall的核心节点，承载核心交易的切割分片、分片任务打包、网络配置、系统纠错等任务。

主节点：EcoBall多种业务功能的承载主体，负责分片交易任务的记录、打包并回传给超级节点，并承载全网存储业务和存储内容检索业务。不同的硬件配置和网络状态，对业务的支持效率略有不同。常规个人或商用电脑、个人或企业NAS、网络服务器等都可以参与区块主节点。主节点数量不限，受系统调节算法影响，不同的硬件和网络性能、地理位置对产出效率都有影响，可以对主节点进行合理调节。

轻节点：EcoBall网络业务的承载主体，负责组网优化和数据传输，总体数量不限，基于网络动态激励，引导轻节点合理分布。

EcoBall区块链网络云系统
支撑整个EcoBall系统及在其之上创建的成千上万的DAPP应用

全网算力、分布式存储、内容检索、
通信宽带流量

云NAS

私人云盘
PT/BT内容分发

生态业务

网络加速
版权内容（电视、音乐、游戏）分发
物联网、广告分发、家庭物联网

私家云路由节点

PN节点、存储、分片节点

云节点

China Blockchain Conference

5、共建共享

开发者联盟、社区自愿者

公链本质特性，决定了它必须依靠社会社群的全员力量共同建设，并通过可量化的Token奖惩经济技术手段保障了贡献者的成果分享。

技术开发者联盟和社区自愿者协会是常见的两种形式。

知识产权

发明专利
40个

软件著作权
27项

发明专利

1. 异构平行区块链及其技术实现，编号201810525202.6。
2. 一种区块链智能协同交易模式，编号201810525204.5。
3. 一种高性能共识算法实现，编号201810740356.7。
4.一种新型区块链区构造及其共识算法，编号201810746597.2。
5.一种非主链区块自增长方法技术，编号201810779968.7
6.工作量算法难度叠加方法...
7.以太坊发布智能合约时指定地址的方法...

软件著作权

1. 夸克链以太坊系列本地签名安全钱包软件（Android）（简称BiBouse），登记编号2018SR660724。

2. 夸克链以太坊系列本地签名安全钱包软件（IOS）（简称BiBouse），登记编号2018SR665831。

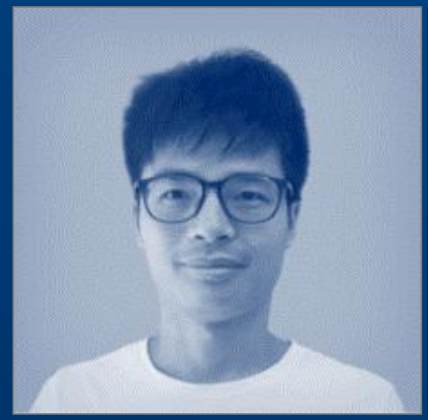
主要核心研发成员

雷志斌
(首席科学家)

美国布朗大学电子工程学博士
香港应用科技研究院创新研发总监
香港科技大学兼职教授
香港中文大学博士生导师

陈华毅
区块链架构师

硕士
华为10年工作经验
两款大型区块链系统设计经验
5项区块链技术专利



吴小龙
区块链架构师

中科院硕士
7年腾讯分布式开发经验
原美图区块链架构师
EOS社区代码贡献者

王旭
首席算法工程师

中科院博士
仿真视觉追踪发明人
3项专利拥有者
1项著作权拥有者

胡原
区块链算法工程师

高级算法工程师，留法硕士（华中科技大学），7年互联网与区块链研发工作经验，数学和算法功底深厚，对共识算法有深入的研究

国家、地方政府支持

中国科技产业化促进会

夸克链科技(深圳)有限公司、大唐教育发展控股(深圳)有限公司：

来函收到。经研究，中国科技产业化促进会同意作为"2018年（首届）区块链联合发展国际论坛"的支持机构，并组织相关学者和专家参加此次论坛。

此函。

中国科技产业化促进会

2018年08月27日

一带一路国际合作发展基金管理委员会

支 持 函

夸克链科技（深圳）有限公司、大唐教育发展控股（深圳）有限公司：

经研究，管理委员会同意支持并参与你公司于2018年10月在深圳举办的2018年（首届）区块链联合发展国际论坛。

"一带一路"国际合作发展专项基金由一带一路研究院、中国国际人才交流基金会建立和管理。

此函。

一带一路国际合作发展基金管理委员会

2018年8月20日

1. **国家科技部**
   +
   国家发改委一带一路研究院
   发文支持区夸克链科技承办"区块链联合发展国际论坛"

2. **国家网信办**
   公司及夸克链科技北大课题组，一同受邀参加"网信办《区块链信息服务管理规定（征求意见稿）闭门研讨会》。

3. **"一带一路"国际商协大会**
   夸克链科技应邀作主题演讲

4. **广西自治区常委**
   邀请夸克链科技参加广西民营数字经济建设座谈会。

学术合作

区块链金融课题研究

点对点通讯网络课题研究

区块链联合实验室

共识算法课题研究

联盟链应用课题研究

行业合作

walton

ZTE中兴

湖南卫视

芒果tv

万润科技
MASON TECHNOLOGY

DTT 大唐电信

东方晨旭
EASUNRISING

SMART VALOR

战略支持

杨东

区块链“共票理论”创建者
人民大学法学教授、博导
国家互联网金融安全技术专家委员会委员
夸克链联合实验室主任

何德标

国家密码学专家，
武汉大学教授、博导
夸克链联合研究中心主任

窦尔翔

北大教授、博导、
经济学博士、金融学博士后
“塔福域理论”创建者
夸克链课题联合组长

Marc Ryser

美国经济学博士
瑞士持牌律师
夸克链法律顾问

丹尼尔 陈
(Daniel Cheng)

联合国工业发展组织官员
夸克链国际事务顾问

China Blockchain Conference

谢谢聆听

THANKS FOR YOUR LISTENING!

www.quachain.com