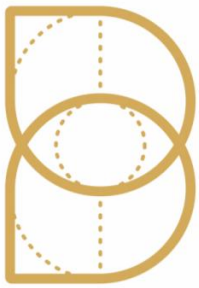


BRAHMAOS

TECHNICAL WHITE PAPER

VERSION 1.0

http://brahmaos.io/
@BrahmaOS
@brahma_os
https://medium.com/brahmalabs

摘要

Brahma OS 是一种承载去中心化网络的操作系统，它通过解构已有服务并使用各类去中心化服务和组件得以实现，确保用户可以安全、无障碍的使用区块链之上的服务和应用。

内容

背景

区块链技术是通过 2008 年诞生的比特币让人们所认知，自此之后，开发者和企业家都在不断的尝试这一技术，期望将其用于更广泛的生产中，来解决不同行业的技术痛点。

而区块链技术从根本来讲并不是为已有公司架构中企业解决技术痛点的技术，更多的它是在处理一种可以自我治理、无中心的价值网络，通过激励制度来维持一个网络的安全、持续运转。

以太网络通过提出智能合约的架构，为不可停止的应用带来了可能性。而 2017 年短短的一年中，便在以太网络之上出现了诸如 Kyber Network, 0x Protocol, Radian Network 等具有革命性的技术方案和实现，它为未来带来了一个完全无中心的应用生态的前景和期望。

同时，诸多的其他可承载应用的公链也在不断涌现，比如 EOS，ADA 等。

作为承载用户最多，花费时间最长的手机等电子设备，却仍然运行着依赖中心服务的 OS，从用户账户系统，到个人数据的备份，再到 OS 之上的应用构建逻辑，显然，现在已有的 OS 并没有为区块链未来的应用提供完备的基础土壤。

去中心化操作系统的需求

有别于当前已经运行的 iOS 和 Android OS，去中心化 OS 需要从设计之初就完全摆脱中心服务器的设计架构 ,从基础服务到上层应用构建皆是如此。在确保 UI/UX 层面尽可能维持使用习惯的同时，更多关注在去中心化服务能在 OS 中发挥的作用和体现的价值。

数据隐私

当个人在使用 OS 时 ,无论是用户有意生成的数据还是无意间操作产生的数据，都是有价值的。

这类数据构成人工智能分析的基础 ,被称为事实数据。同一份事实数据 ,在数据挖掘算法不断优化之后 ,可以生成丰富和不同的用户画像。而我们如今所已知的所有个性化服务 (如网购推荐、好友推荐、语音识别等) 均依赖用户事实数据所生成的用户画像 , 也因为有了成千万上亿用户的数据构建起了 Facebook, Google 这样的商业帝国。

但用户在中心化服务的商业闭环中 , 除了贡献行为和事实数据 , 并没有得到经济上的回报 , 甚至于这类数据会被二次、三次的贩卖。从某种意义上讲，现如今，系统和 App 厂商的商业模型很大程度上建立在无经济回报的使用用户隐私数据的基础之上。

在 Brahma OS 中 , 隐私问题将从根本上解决 , 窃取和剥削用户隐私数据的行为将变得难以进行。

无障碍网络通信

无论是区块链还是现有的互联网经济中,网络通信连接都是需要先觉解决的内容。而如何无障碍的访问网络上的给类数据在很多时候成为了关键性问题。

当我们提到网络通信时，我们大多时候在说终端如何连接到广域网络。当前的结构中，终端设备通过连接到元网络（即自己可直连的局域网络），而元网络再通过路由器、交换机提供不同元网络或上层网络的互相连通。其中，连通元网络间关系的大多是当前的运营商。

这其中，我们可以抽离出两层：元网络、路由器。

元网络内的终端节点是可以构成对等网络的，也就是说，任何一个元网络内的节点下线，不应该引起元网络内通信的不可达。这并不是我们关注的核心点，因为它的连通性相对而言并不难解决，关键的问题出现在路由器的角色中。

在当前的网络通信中，我们必须信任也只能信任“路由器”角色，但事实上它不仅仅可以完整的拦截和窥探元网络间通信的数据、协议、走向，甚至它可以对此作出行为，比如篡改、拒绝服务等等。

在当前可用的网络通信中，OS 终端用户面临着两个巨大的问题:隐私暴露、无障碍通信的不可保障。

因此，在 Brahma OS 中，我们预期构建一个可对等连接的 OS 网络，从数据传输层面通过协议混淆确保通信数据的加密和不可识别，另外从路由角色的设定上构建可自治的连通网络。

去中心化存储

时至今日，大多的 OS 为用户提供了“云存储”的功能，用户在不同设备只需要登录同一账号便可以访问相同的数据。这为个人带来便携的同时，也为个人数据安全带来了隐患。

从 Dropbox 漏洞导致用户个人数据丢失，到 iCloud 账号大量遭受黑客攻击泄漏诸多明星裸照的事件，已经反映出一个明显的问题：当前的中心化云存储架构中，安全只是被攻破时间长短的问题，也就是说，其存在系统性的不可规避的风险。

而去中心化的链上存储恰恰从设计之初就解决了这一问题，以 IPFS 为例，没有可被攻破的单一服务器或可被追查的一组服务器，所有的数据被切分多份，随机存储于网络的不同节点，整个网络由存储网络的矿工为其提供存储和传输的安全和高效。

Brahma OS 在构建存储服务时，会直接使用去中心化网络服务，当前我们并不保证一定使用 IPFS，同时还会对比 Sia, Storj, MadSafe 等其他可能的去中心化存储技术方案。

密码学资产的管理

资产管理是钱包应用层需要完成的功能，而我们从 OS 的角度深入的考虑这一需求。

在可以预见的未来，密码学资产很多时候并不再依赖于中心化交易所，中心化交易所从现在的投机性买卖变为对接区块链资产与法币资产的角色，而密码学资产的兑换可以使用去中心化服务直接完成。

当前，在以太坊的主链之上，我们已经可以直接使用 0x 协议构建交易 relayer 来提供撮合服务，有趣的是，这一协议可以连通所有其他构建的 replayer，也就是说，它不单单可以提供单一应用内的流动性，它可以直接提供所有使用这一协议的 replayer 间的资产流动性。

另一个可行的方案是 Kyber Network，它与 0x 的差别是其本身就是一个去中心化交易所，OS 可以直接接入这一服务，无需自行构建 replayer 角色就可以直接帮用户完成资产兑换。

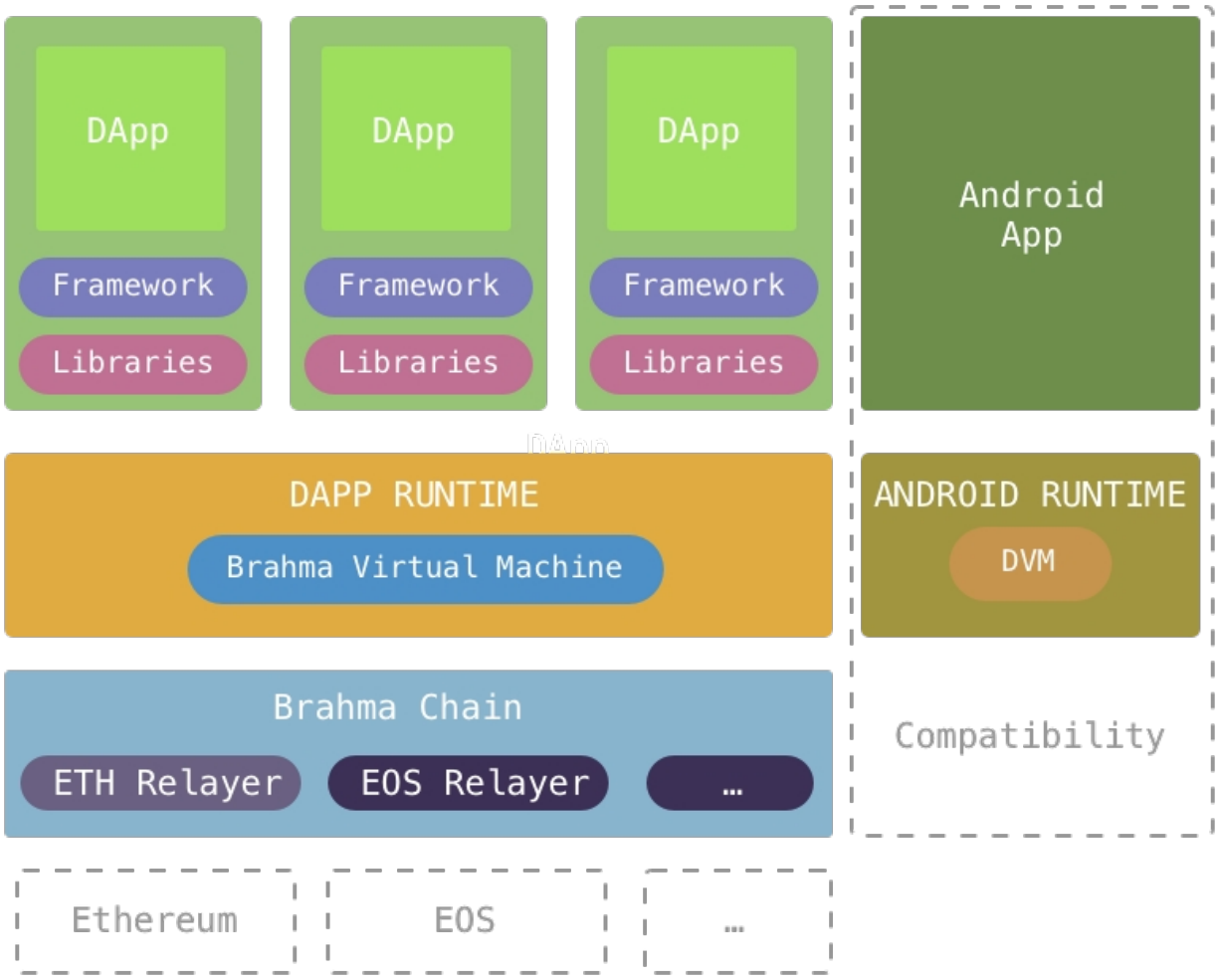
相对于已经有可选方案的兑换服务而言，构建 OS 层面的支付服务更为关键。Brahma OS 将成为诸多 D-App 的载体，比如游戏、社交、媒体等 D-App 需要一个用户可以快速使用的土壤，在 D-App 内的所有消费也将是在链上（链下的快速交易最终也需要回归链上，只是延迟发生）完成，整个过程中，从 D-App 发起支付请求，到最终用户完成交易，与任何中心无关。

自治的经济系统

在过去的一年中，以太坊之上出现了层出不穷的具有巨大潜力的技术突破，这些突破正在不断拉近区块链与现实用户的距离。

Brahma OS 初期通过集成诸如 IPFS，Kyber Network, 0x 等技术方案，并提供自治无障碍网络通信和上层应用服务基础，随着跨链技术及 Brahma OS 主链的上线，我们将构建起以 Brahma OS chain 为基础，连通 ETH，EOS，ADA 等其他主链的完整生态。

架构



分层设计

Brahma OS 使用分层设计方案，将 Chain、Runtime、Framework 等逐一分层。并且为了考虑到 Android 原生应用的兼容性问题，从 Virtual Machine 单独区分，从而使得 Android App 和 DApp 的运行时环境完全隔离，保证了 Android App 即便存在危险的行为也不能获取到 DApp 的信息。

Brahma OS 为 DApp 独立设计了 Brahma Virtual Machine(BVM)，用于执行 DApp 的运行和关联的 Framework 和 Libraries 的运行。

Brahma 独立的 Chain 作为 Brahma OS 的主链，起着 Chain Context(链间上下文)的作用，预期通过 Chain Relayer 作为中间角色，来连通其他的应用链（如 Ethereum，EOS 等）。

共识算法

作为独立的区块链，Brahma OS Chain 的共识算法对于安全性至关重要，当前我们主要考虑采用两种可能的方案：DPoS 和 DAG。

DPoS 由 Bytemaster 最初提出并在 BitShares、Steemit 及 EOS 中应用，它主要的特点是较高的 TPS (TX per second) 和较低的共识维护成本 ,同时相比于 PoW 共识的竞争机制 ,DPoS 更倾向于 Witness node 间合作的方式来达成共识。

DAG 是图论中的一种图IOTA 最初尝试使用 DAG 来替代已有的 blockchain 结构，用于提供一种通过数学证明，而非共识机制保证的价值传输网络。在 IOTA 之后，又有 Byteball 等其他项目对 DAG 提出了改进和应用。DAG 的主要特点在于可以更高并发的处理交易请求，因为没有了 block 结构，因此不存在 TPS 的限制。

兼容性与安全性考虑

我们相信去中心化 OS 最终会替换掉当前的中心化 OS ,但是这不仅仅需要时间和精力，还需要用户学习的过程，因此我们在设计之初，会坚固兼容性并考虑到安全性因素。

因为已有的 Android OS 已经相对完整因此我们考虑在进行 Brahma OS 相关内容研发的同时如 Brahma Virtual Machine、Brahma Chain 等，兼顾已有 Android OS 的运行，在 OS 层面提供 Dalvik Virtual Machine 为 Android 已有的 App 提供运行时环境。

这样，既保证了兼容性，又从运行时的层面直接隔离了 Android App 与 DApp 之间交互的可能性，从而避免了 Android App 窃取密钥、偷取 DApp 信息的可能性。

身份

在任何系统中，身份都是不可规避的首要因素，也是人机进行逻辑、功能性交互的前提。

Brahma OS 中，身份不再依赖于基于中心化服务的账号系统，而是直接使用区块链的公钥作为用户身份的标识,连接整个去中心化服务体系。

关于“我”

之所以会抛弃中心化服务的账号体系，很大程度上来源于我们对于“我”这一身份在整个网络架构中的认知。

在现在已有的中心化账号体系中,终端用户需要在中心化的服务商那里进行注册，拿到一个分发的身份，授权用户登录到系统中，再进行后续操作。这带来几个问题（现在已经凸显）：

- 在不同的账号系统间切换时，“我”的数据并不天然互通
- “我”在不同账号里是冗余且并不互备的
- “我”的行为产生的所有事实数据和用户画像被中心化的服务商无成本轻松获取

以上几个问题总结来说就是，“我”在当前已有的中心化网络中是被授权访问，且无条件的在被剥夺行为数据。

当一个账号泄漏了密码或服务商被黑客攻击,甚至是服务商贩卖用户个人数据时，“我”便变得对这件事情无能为力。

身份的作用与价值体现

基于对于“我”，即身份，的认知我们不难发现，身份作为接入到系统的准入标识，背后关联着一整套的商业逻辑。

而构建在中心服务商之上的身份，彼此之间是隔离、冗余、无交叉、不安全的，而用户身份又恰恰是当前互联网经济的重要资源和壁垒。

所以，在 Brahma OS 中，如何将身份的价值回归给身份所有者本身便显得至关重要了。

通过上面的阐述，可以知道，身份在一个完备的系统中起着两种作用：

- 获取账户系统授权
- 访问和操作账户系统的标识

在 Brahma OS 中，身份还具有其他用作：

- 资产的标识
- 用户画像的标识
- D-App 匹配用户画像的标识

Brahma OS 预期提供给用户可选择机会，通过 OS 层面在本地收集用户的事实数据，并训练其本地 AI 进行用户画像的完善，当 D-App 的主体需要使用这些用户画像时，其直接支付费用给用户，确保最终收益归 OS 所有者本人，而非任何中间角色。

去中心化存储的意义

相比于直接使用其他中心化的云存储方案 ,用户的身份相关数据使用去中心化存储会带来更大的价值。

先说下使用中心化云存储方案的几个弊端：

- 中心化系统存在系统性安全风险
- 云存储服务商之间并不共享身份信息
- 任何一个中心化云存储服务商被攻破都会威胁其他服务商

而去中心化的存储方案 ,恰好在设计之初就规避这类问题。即便是单一用户因为个人行为或其他原因导致密钥被盗窃 ,带来个人数据的泄漏 , 也不会造成整个系统中其他用户数据的丢失 , 甚至于都不会产生丝毫的关联。

同时 ,用户身份不再是被商业巨头榨取的来源。所有因为使用用户身份及画像支付的费用 ,都会回馈给用户本身。从一开始便规避了用户数据需要集中存储和处理的问题。每个人持有着自己的数据 ,离散的分布在去中心化存储的网络中 , 不再有人 (机构) 可以监视个人数据的去向、内容 , 也无法在中间劫持数据。

这将为个人的数据隐私、行为自由、价值回归带来诸多的可能性 , 是重塑现有商业模式的基础。

网络

网络的连通最终将是无障碍进行。

网络角色

在 Brahma OS 的网络层，我们通过分离不同的角色，来确保网络的连通性和相应的自治经济构建。

其中，我们会区分出元网络节点和路由网络节点两类。

元网络的构建

元网络是一个局域网络的最小单元。

在元网络内，不同节点之间是彼此对等，彼此间连通不需要额外的流量成本，所以元网络的构建主要发生在小范围内，甚至是近距离直接通过蓝牙等协议完成设备间互联。

Brahma OS 之间可以互联构建元网络，并以此为最小单位向外扩散。在元网络内传出数据时，应用层协议本身会做诸多的混淆措施，会对数据做分片、加密等处理，从而确保数据在元网络内的传输不会泄漏数据内容。

路由

路由扮演着连接不同元网络及连通到上层广域网络的角色。

多个路由本身也可以形成一个元网络的结构。它们为不同的元网络之间提供数据交换的服务。这边可以形成一个无中心的流量市场。

Brahma OS 中，连通不同元网络的节点作为路由节点，它们为不同元网络之间及元网络与广域网间的互通提供流量交换，因此作为路由节点的设备也会在一定程度上获得网络连通中的经济回报。

应用基础

Brahma OS 集成给类去中心化服务的目的，是为之上的应用提供可以基础，让 D-App 开发者可以不必过多的考虑如何接入去中心化服务，只需要关注在如何构建应用逻辑。

运行时环境

Brahma OS 运行时环境作为 Native D-App 的运行沙盒环境。

运行时环境需要确保几点：

- 完全隔离
- 执行效率
- 去中心化组件的调用环境

其中，完全的隔离为 D-App 提供安全的运行空间，这里的安全不单单是指单一 App 本身的数据不会被侵犯，同时也指与其他 App 之间运行是彼此隔离。

作为 Native 运行的 App，执行效率至关重要，这直接关系到用户体验的好坏。在系统的线程优先级层面，Brahma OS 会优先处理与用户交互相关的事务，而网络、IO 相关的执行则并行多线程在后台运行。

应用结构

Brahma OS 之上的 D-App 应该会包含两个关键部分：Brahma OS 服务组件、UI 组件。

我们在此更多讨论和关注服务组件。

去中心化服务组件

如上文所提到的，以太坊之上的诸多去中心化服务正在不断推出，而对于开发者而言，如何快速、符合最佳实践方案的对接这些服务至关重要，它不仅仅影响到 D-App 的开发进度，同时也影响着用户的资产安全等问题。

因此，Brahma OS 预期为开发者提供：

- 便于快速集成的组件 SDK
- 丰富的文档
- 最佳实践的接入 Sample
- 积极参与的开发者社区

比如，当一个 D-App 中用户需要使用 ETH 购买某个道具时，他不再需要繁琐的跳转到钱包发起交易，而是直接在游戏内调用 Brahma OS 的支付组件，为用户展示请求支付的具体信息，用户的认知也将从过去发送交易的逻辑中变为使用支付的逻辑，为更广泛的密码学资产使用场景带来了可能性。

D-App Store 的可能性

Brahma OS 除了在技术上带来诸多的突破，还在为未来可能的新生态带来另一个巨大的可能性，D-App Store。

D-App Store 不同于当前当前我们已知的给类 App Store 或 Google Play，我们预期它不是一个中心化的运营主体，而是一个由用户直接参与运营和筛选的去中心化集市。

其上可以构建和尝试很多新的商业模式，比如 D-App 的收益可能可以直接与评分用户或推荐用户直接关联，不再存在中间的角色剥夺 D-App 主体的收入。

而且，因为用户身份的数据不再是分裂在不同的中心系统中，所以不同的 D-App 之间可以基于同一个用户身份作出更为人性化的定制，甚至于从 D-App Store 时这些数据就已经起到作用，而开发者可以通过付费给 D-App Store 的推荐系统，来寻找到符合其目标群体的用户，这些用户不但会直接收到收益（事实上用户会认为他们什么都没做就收到了代币），而且还会促进 D-App 的高转化率。

总结

Brahma OS 踏入了一个全新的、密码学货币至今从未被触及过的领域。它将作为连通终端用户和区块链网络的核心角色 ,它不仅仅集成了已有的诸多去中心化服务 ,还为其上的开发者提供了便于快速构建应用的底层架构和一个完整的生态系统。它代表了区块链技术从探索到蓬勃发展的重要进步。

技术路线图

Phase 1 Token 兑换

2018 Q1

- Token 兑换分发

Phase 2 MVP

2018 Q2-Q4

- 移除 Android 的中心化服务组件
- 确定去中心化组件的细节开发时间表
- 接入以太坊网络
- 适配关键机型
- 初步运行测试 Brahma OS

Phase 3 DEX Integration

2019 Q1

- 集成去中心化代币兑换服务
- 测试中心化代币兑换
- 确认中心化代币兑换组件的封装

Phase 4 Decentralized backup service

2019 Q2-Q3

- 集成去中心化存储服务
- 测试中心化存储服务
- 封装去中心化存储服务和组件

Phase 5 Brahma blockchain research

2019 Q4

- 设计共识模型与虚拟主机运行模型
- 测试对比共识方案

Phase 6 Brahma blockchain testnet

2020 Q1 - Q2

- 测试 Brahma 链共识机制
- 测试 Brahma Virtual Machine
- 部署 Brahma testnet

Phase 7 D-App 及 Brahma D-App Store

2020 Q3 - Q4

- 重构上层 D-App 架构
- 完善 D-App 开发架构方案
- 完善开发者去工具链
- 设计并实现 D-App Store 架构及集成分发方案

Phase 8 D-App 开发者社区构建

2021 Q1

- D-App hackthon
- 扶持优秀开发者
- 核心开发者技术沙龙

Phase 9 生态构建与基金会

2021 Q2 - Q4

- 基金会投资 D-App 及核心组件项目
- 与更多行业洽谈商业合作
- 增强 Brahma OS 影响力
- 启动 Brahma OS DevCon 计划

代币兑换

- 预期软顶：3w ETH
- 预期硬顶：6w ETH
- 总发行量：3,000,000,000
- 出让比例：40%
- 其余比例用途：待定

团队介绍

Bella Liu

联合创始人

- 12年互联网经验。
- 6次创业经验，杰出的产品经济设计能力。
- 曾在顶尖互联网公司担任要职。
- 近几年在国际项目中具有丰富的资产投资运营经验。

Lorna Chen

CMO

- 曾就职于摩根，纽约梅隆银行，东京三菱银行。
- 英国特许会计师。
- 爱丁堡科学硕士和剑桥大学法学院商学院EMBA。

Steven Hu

CTO

- 具有10年以上电信及互联网行业架构设计与研发管理经验
- 负责可编程虚拟化路由器团队的架构设计工作
- 参与最早期分布式架构设计
- Consumer BG，先后负责IM系统以及云笔记系统的研发管理和设计

Elaine Shehu

技术顾问

- 德意志银行与区块链相关项目的IT战略前负责人
- 在开发基于云的平台方面已有12年多的时间。
- 伦敦大学计算机科学硕士学位。

Marinos Tsokas

顾问

- 雅典联合技术经济系统硕士学位
- 英国剑桥大学工商管理硕士
- Ex-CMO，沃达丰区块链项目 - 营销和商业开发负责人
- 屡获殊荣，商业专业敏锐，成功推动商业改进并促进客户参与度
- 商业上精明的专业人士，成功推动商业改进并促进客户参与度

Trevor Smith

OS架构师

- 在爱丁堡大学取得博士学位
- 少数几位在IOS和Salesforce上工作的初级IOS开发人员之一。从事iOS和Android App计算机算法的早期原型,目前正在分散式区块链技术研究工作中。

Srikanth Bodla

DNA 图像主管

- 解决方案架构师/项目负责人，拥有强大的商业智能和数据仓库背景，
- 在成功交付端到端解决方案，解决问题和要求由优良的记录，对新兴技术Qlikview，大数据，SAP Hana，SAP BI / BW充满热情。

Xingchu Liu

工程师领导

- 德克萨斯A＆M大学博士，清华大学硕士和学士学位。
- 优异的的领导者和创新者，在分析学应用，商业智能，机器学习，数据挖掘和人工智能领域以及在零售，电子商务，技术，批发，制造和分销等多个行业中也具有深厚专业知识的
- 在分析决策支持解决方案的设计，开发和实施方面拥有超过12年的经验。

Shu Collins

经济模式

- 英国牛津大学统计学硕士学位。
- 在汽车，游戏，科技，娱乐和数字保险行业拥有超过10年的数据科学，有机器学习和人工智能方面的工作经验。

- 曾在多家财富500强公司 ,或英国天然气公司 ,苏格兰皇家银行等IPO公司领导过数据科学项目，擅长区块链应用和加密货币领域。

KJ

研究院

- 12年分布式数据库系统和P2P网络架构设计经验
- 研究方向包括区块链能力，数据碎片和生态系统。
- 在技术和研究方面有丰富的经验。

团队责任

Ocean Lu

负责用户画像 Team，机器学习，深度学习及算法研究。

对用户标签进行封装。

Martin Wang

负责分布式协议优化，网络层协议对接 os。

对存储内容进行安全封装。

Kevin Lee

负责无网络技术实现，优先改造无网络协议，优化性能。

并嵌入 os

KJ

主要研究优化链结构，基于链上的算法设计与实现。

Steven

带领 10 人团队，负责 os 的底层系统实现，将各层解构。

并对 os 各层协议进行整体研发嵌入。

Han

负责 Dapp 架构设计与研发，为上层接入提供整体 API。

体系设计与实现。

Sheng

负责安全防攻击及安全加固。

为整体 os 在协议层，传输层安全做架构设计与研发。

David Silva

负责 OS 产品的功能设计和接口协议的开发。项目优先级调整

JAsmall

os 交互设计师专家。为主框架人机交互提供解决方案及实施。

Ouy

负责支付体系的设计与研发。

对接链上各支付协议并安全快速。

Kaiko

负责视觉效果，UI 设计师。