shuang-guo Update whitepaper.md f8cd9fe on Nov 26, 2017

3 contributors

289 lines (164 sloc) 21.2 KB

公信宝区块链技术和应用白皮书 (V2.0.0)

I. 摘要

> 大数据时代已经来临，万物互联的时代也已不远，人类社会生产、获得和处理数据的能力已经远超过去。通过对数据的合理应用，我们对世界的认识、对商业和社会活动的规划，对需求的响应，对人与人的协作都将会提升到一个新的高度。

近几年来，随着互联网的高速发展和信息技术的普及应用，各个行业和机构所产生的数据呈爆炸性增长，对于全社会来说，这是一个在不断膨胀的巨大宝库。但是在数据量呈几何级数增加的同时，巨头对数据的垄断和机构间信息孤岛的情况也亟待破局。“将数据交换起来”，这背后蕴含着巨大的生产效率提升空间和商业价值。

数据，是未来最重要的生产资源，不但规模巨大，且将随着人们行为的变迁而不断流变，成为我们测量、理解一个时代商业和社会的关键，它也将是全行业的标配；而区块链技术，是未来世界最重要的基础技术之一，它构建了一个让所有参与者都可以共同维护的可信价值互联网。而它作为一个传输价值的信任网络，能够让数据这项最重要的生产资源，在流通中的成本降至最低。

可以说，区块链这项未来最重要的底层技术，与数据这项未来最重要的社会资源结合在一起，能够释放出极大的商业价值、社会价值。公信宝的使命和愿景，就是构建于此。我们已经开发了一系列基于区块链和数据的应用产品。其中，最底层的就是我们的公链——公信链（GXChain），公信链 = 区块链 + 大数据。

公信链的定位，是基于区块链建立一个可信任的全领域数据交换价值网络，让各个领域的数据都可以非常自由、相互信任、极度高效地共享交换，让数据逐渐远离垄断，信息不再有孤岛，让数据为商业和我们的生活提供更高的价值。

II.GXChain

1.GXChain 基础介绍

GXChain（公信链）是公信宝团队打造的一条数据交换公有区块链，是公信宝数据交易所的底层链，不仅支撑着公信宝数据交易所高频的数据交易交换，还支持开发者开发应用。在公信链上开发应用，不仅可以利用区块链的技术特性，还可以获得各行业多维度数据的支持，做出非常落地于民生的有价值应用。

已经开发出来并上线的应用，证明了公信链在商业上的可用性，基于 GXChain 的第一个企业级应用——公信宝去中心化交易所，已经在 2017 年 9 月 24 日正式商业化落地。 而第二个基于 GXChain 的应用，面向大众的个人信用管理工具（公信宝 DApp），也将在今年发布测试版。

2.GXChain 的共识机制

公信链使用 DPoS 和 PoCS 来实现区块链记账和数据交换的共识机制。
DPoS(Delegated Proof of Stake) 机制，源自于 Graphene，中文名叫做股份授权证明机制（又称受托人机制），它的原理是让每一个持有代币的人进行投票，由此产生 101 位代表，我们可以将其理解为 101 个 (可无限扩展) 超级节点或者矿池，而这 101 个超级节点彼此的权利是完全相等的。从某种角度来看，DPOS 有点像是议会制度或人民代表大会制度。如果代表不能履行他们的职责（当轮到他们时，没能生成区块），他们会被除名，网络会选出新的超级节点来取代他们。

PoCS(Proof of Credit Share) 机制，是公信链自主设计开发的共识机制，中文名叫做信用贡献证明机制 (又称共享交换平衡机制)，用来解决数据体量悬殊企业之间的共享交换不平衡问题。

联盟成员每完成一笔数据交易，则计算一次 PoCS，贡献比根据买卖次数计算，并参与数据交易手续费的计算。PoCS 低的联盟成员，将会付出比基准手续费更高的费用换回数据，PoCS 高的联盟成员将会付出比基准手续费更低的费用换回数据。

PoCS 和交易手续费实现原理的**伪代码**如下：

```
if ((total_sell + total_buy) >= pocs_threshold) {

    pocs = calculate_pocs(total_sell, total_buy);

    fee = scale_fee(pocs, data_transaction_base_fee);

} else {

    fee = data_transaction_base_fee;
}
```

pocs：贡献比，一个联盟成员在一个联盟中有且只有一个贡献比。

total_sell：当前账户卖数据的总次数。

total_buy：当前账户买数据的总次数。

pocs_threshold：产品阈值，若当前账户买卖总次数大于等于此阈值，才启用贡献比参与最终手续费的计算。

data_transaction_base_fee：不考虑贡献比的基准手续费，即全局参数中操作的手续费。

calculate_pocs：根据买卖数据次数计算 PoCS。

scale_fee：根据 pocs 调整交易手续费。

3. 为什么选择 DPoS 共识机制

现有区块链项目的主要共识机制为 PoW 和 PoS，少部分项目采用修改后的 BFT（拜占庭容错）的共识机制，BTC 就是 PoW 机制下最成功的加密货币。PoW 机制虽然已经成功证明了其长期稳定和相对公平，但在现有框架下，采用 PoW 的 “挖矿” 形式，将消耗大量的能源。其消耗的能源只是不停的去做 SHA256 的运算来保证工作量公平，并没有其他的存在意义。而目前 BTC 所能达到的交易效率为约 5TPS（5 笔 / 秒），以太坊目前受到单区块 GAS 总额的上限，所能达到的交易频率大约是 25TPS，与平均千次每秒、峰值能达到万次每秒处理效率的 VISA 和 MASTERCARD 相差甚远。

PoS 机制下较为成熟的数字货币是 Peercoin（点点币）和 NXT（未来币），相比于 PoW，PoS 机制节省了能源，引入了 “币天” 这个概念来参与随机运算。PoS 机制能够让更多的持币人参与到记账这个工作中去，而不需要额外购买设备（矿机、显卡等）。每个单位代币的运算能力与其持有的时间长成正相关，即持有人持有的代币数量越多、时间越长，其所能签署、生产下一个区块的概率越大。一旦其签署了下一个区块，持币人持有的币天即清零，重新进入新的循环。在 PoS 机制下，因为区块的签署人由随机产生，则一些持币人会长期、大额持有代币以获得更大概率地产生区块，尽可能多的去清零他的 “币天”。因此整个网络中的流通代币会减少，从而不利于代币在链上的流通，价格也更易受到波动。由于可能会存在少量大户持有整个网络中大多数代币的情况，整个网络有可能会随着运行时间的增长而越来越趋向于中心化。相对于 PoW 而言，PoS 机制下作恶的成本很低，因此对于分叉或是双重支付的攻击，需要更多的机制来保证共识。稳定情况下，每秒大约能产生 12 笔交易，但因为网络延迟及共识问题，需要约 60 秒才能完整广播共识区块。长期来看，生成区块（即清零 “币天”）的速度远低于网络传播和广播的速度，因此在 PoS 机制下需要对生成区块进行 “限速”，来保证主网的稳定运行。

为了让处理效率能有质的突破，DPoS 机制应声而出。DPoS 机制要求在产生下一个区块之前，必须验证上一个区块已经被受信任节点所签署。相比于 PoS 的 “全民挖矿”，DPoS 则是利用类似 “代表大会” 的制度来直接选取可信任节点，由这些可信任节点（即见证人）来代替其他持币人行使权力，见证人节点要求长期在线，从而解决了因为 PoS 签署区块人不是经常在线而可能导致的产块延误等一系列问题。DPoS 机制通常能达到万次每秒的交易速度，在网络延迟低的情况下可以达到十万秒级别，非常适合企业级的应用。因为公信宝数据交易所对于数据交易频率要求高，更要求长期稳定性，因此 DPoS 是非常不错的选择。

IV.GXChain 的特点

高性能和可扩展性

公信链是一条拥有高并发处理能力的公链，每 3 秒出一个块，拥有每秒高达 10 万笔交易的处理能力，考虑到今后链上业务不断上涨的可能性，公信链支持横向扩展，这样可以迅速扩张每秒交易处理能力，并不需要分叉来达到共识。

参数动态调整

公信链不需要分叉就可以修改系统参数，通过共识投票的方式实现区块大小、出块速度、手续费等全局参数的动态调整。

例如：目前每 3 秒出一个块，可以动态调整参数到每秒出块；目前区块大小是 2M，可以动态调整成大区块，如 8M。

数据提供

在公信链上开发的去中心化数据交易所支持很多领域的数据交易和交换，企业和个人开发者可以交易获得和使用这些数据。

BaaS 服务

公信链还提供一些如存储和验证类 BaaS(区块链即服务：Blockchain as a Service) 接口的支持，开发者根据丰富的 BaaS-API、数据交易 API、原生 API 开发出充满实际价值意义的区块链应用。

基于公信链的应用开发

与其他公共区块链相比，基于公信链开发的应用拥有各行业的数据支持，让开发者做出更有实际价值的商业应用。

数字资产发行

公信链上有数字资产的发行标准，允许开发者自由发行和流通应用。

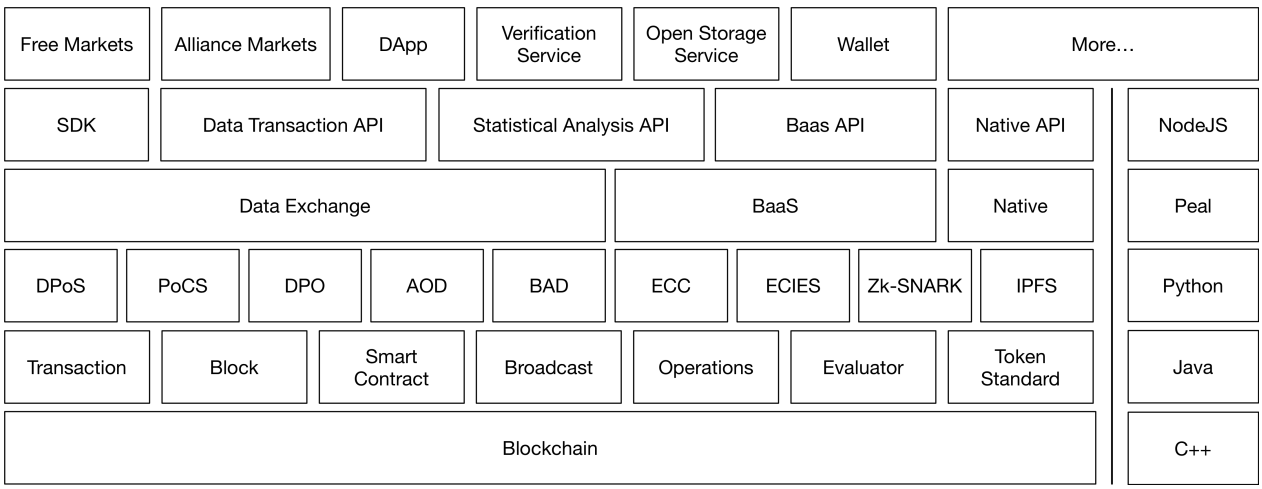
代码开源

公信链以及相关代码已经在 Github 上完全开源。

开源地址 https://github.com/gxchain

V.GXChain 技术架构

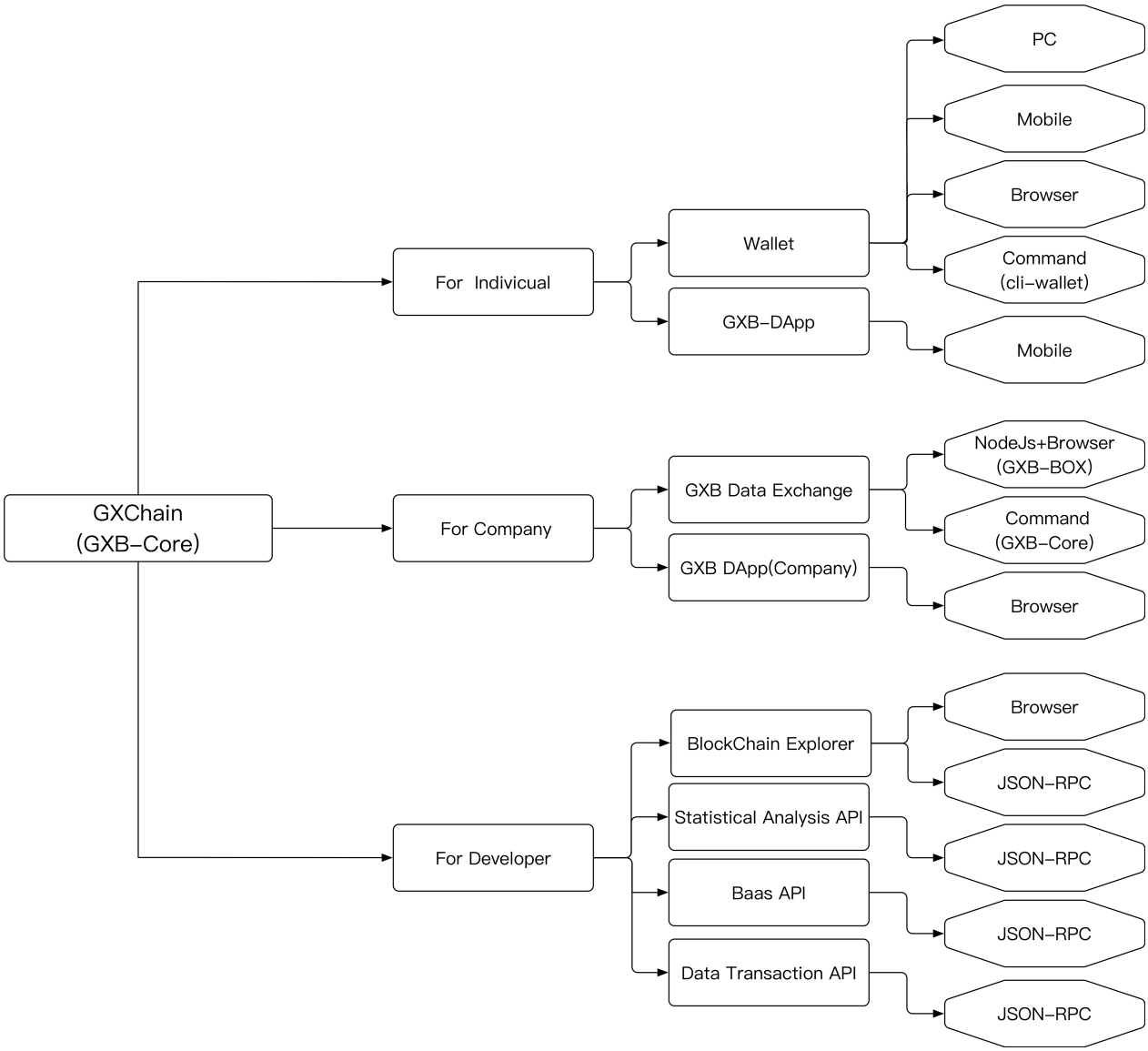
公信链技术架构如下图所示：



VI.GXChain 应用架构

公信链在面向个人用户、企业用户、开发者三个方向上规划了丰富的应用和服务。

应用架构如下图所示：



1. 面向个人用户的

钱包

钱包用来管理在公信链上发行的数字资产，目前我们开发了 4 种不同环境的支持，分别是 PC 版、移动版、浏览器版、命令行版。

PC 版
支持 Windows32bit 及 64bit、Linux 桌面、MacOSX 版本。

移动版
支持 ios 和 android 双系统，除了可以保管数字资产，移动版还实现了交易所行情对接，未来还将和数字资产交易所打通。

浏览器版
非常轻量化的在线使用，支持了 PC 版所有功能。入口 https://wallet.gxb.io

命令行版
操作相对复杂，是提供给专业用户使用的，例如数字资产交易所的工程师，建议具有命令行使用经验和相关技术背景的用户使用。

钱包下载地址

https://gxs.gxb.io/#downLoad

公信宝 Dapp

这是公信宝官方工程师在公信链上开发的一款让个人用户使用的信用管理工具，可以实现面对面信用验证和个人信息所有权管理等功能。其中面对面信用识别功能是在得到对方的授权同意后，通过公信宝数据交易所查询他的个人数据 (个人的数据包括但不限于健康病历、交通出行、教育培训、工作经历、兴趣爱好、征信记录等)，从而轻松实现面对面信用识别，此功能将广泛应用于招聘、相亲、租赁、二手交易、贷款、场外交易等需要个人信用数据作为风控依据的领域。
更多介绍请看详细的**公信宝 Dapp 白皮书**
zh/gxbDapp-whitepaper.md

2. 面向企业用户的

去中心化数据交易所

公信宝团队在公信链上开发了一个去中心化数据交易所，数据交易所具有不缓存数据、保护个人隐私、保护数据版权、有效遏制造假以及支持双向匿名交易等特点。面向的典型客户为互联网金融领域的网络贷款、汽车金融、消费金融、银行等企业以及有数据交换需求的政府部门、保险、医疗、物流等政企部门，以去中心化思维解决了各个行业的数据安全交换和流通等环节中一直没有解决的诸多核心问题。并可以为全社会所用，广泛使用于公民的学习、工作、生活等各种应用场景中，让数据释放应有价值，提升社会协作效率。

更多介绍请看详细的**去中心化数据交易所白皮书**

zh/dataExchange-whitepaper.md

公信宝 Dapp 企业版

公信宝 Dapp 是非常适合应用于个人用户在求职面试、租赁、二手交易、场外交易等场景中的信用识别，我们考虑到未来很多应用场景的业务流程都需要企业参与或主动发起，所以在产品线上规划了一个面向企业用户的 web 程序，企业可以轻松发起请求，经由个人用户授权同意，企业可以查询到个人授权的数据，直至完成业务流程。

3. 面向开发者的

公信链支持开发者调用开放的 API 来开发应用，分别是数据交易 API、BAAS-API、原生 API、统计分析 API。
数据交易 API：
经过开发者认证后，安装 GXB-BOX 后，点对即此 API 将允许开发者付费调用公信宝去中心化数据交易所的数据接口，丰富应用的实用价值。
BAAS-API：
公信链整合了 IPFS 技术，初期 BAAS 将提供业务数据存储、对象存储和验证服务，开发者可以将应用的数据存储到公信链之上，实现数据储存账本公开和过程校验。
原生 API：
可以调用命令行钱包中很多区块链原生 API，将直接访问区块链账本记录和发送交易。
统计分析 API：
官方向开发者开放区块链上的数据统计分析服务 API, 有利于开发者做一些计算和展示功能。 **区块浏览器 API:** 区块 l 浏览器实现了区块、交易记录和账户信息的功能, 同时提供了网页和 API 两个两种方式进行查询, 不同的用户可以根据不同的需求进行选择。

https://block.gxb.io/#/

更多细节和内容可关注开发者社区论坛 https://forum.gxb.io/

VII.GXC 和 GXS 的用途

资产介绍及用途

它们的定义分别是这样的：
公信币 (GXC) 是商户在公信宝数据交易所的买卖数据的结算记账数字货币，和人民币 1:1 锚定，价值不变，确保购买数据成本稳定。
公信股 (GXS) 是公信宝在公信链上发行的数字货币，不仅具有流通价值，同时还是基于公信链应用的必需加密数字货币。
简单来说，GXC 是公信宝数据交易所里的数据交易支付 Token，针对有买卖数据需求的客户而发行，客户需要支付 GXC 才可以购买数据；而 GXS 是公信宝在公信链上发行的 Token，它可以在数字货币交易所交易流通，它的应用价值主要体现在以下几个方面：
1. 在公信链上开发、认证应用、使用链上服务（例如链上转账的矿工费）需要支付或燃烧 GXS，GXS 是作为链上应用运行唯一使用到的 Token。
2. 随着公信宝合作的客户和数据源越来越多，数据交易所的交易量越来越大，公信宝就可以收到更多的佣金，团队会定期拿出佣金收入的 10% 按照当时二级市场的价格回购 GXS 并销毁。
3、在选举产生见证人时可作为选票使用。（暂未开通）

分发机制

GXS 的总量为 1 亿股，总共分为 ICO 份额、私募份额、公信宝基金会份额三部分，详细分配情况如下：

公信股（GXShares）总量： 100,000,000 股

公众 ICO 计划总额：39,000,000 股，占 39%。公众 ICO 实际发行总额为 2451 万股，未完成原计划 ICO 份额的公信股目前处于冻结状态

私募总额：10,000,000 股，占 10%，用于发放给最早期的私募投资者

公信宝基金会持有：51,000,000 股，占 51%

公信宝基金会持有的股为限制流通股，以年为单位释放，第一年最多释放数额占公信股总额的 6%（即第一年释放 6,000,000 股），用于推广计划（聘请顾问、人才招募、社区建设以及 ICO 推荐人奖励、宣传推广等），以后每年最多释放 5%。基金会持币账号对全社会公开，并在其官网公布资金使用计划、使用用途等，接受社会监督。

回购机制

公信宝将用数据交易所佣金收入的 10%，回购二级市场上发行的公信股（GXS）。回购的公信股将转移至销毁账户进行销毁。我们将确保整个过程的公开透明：回购记录将在第一时间公示，届时用户也可通过公信宝区块链浏览器查询，这个过程将持续到销毁 ICO + 私募发行的公信股总量（共 3451 万股）为止。

回购销毁的周期：公信宝数据交易所上线后，第一年以每 3 个月为周期，第一次回购将发生于 2017 年 12 月。公信宝将用数据交易所佣金收入的 10% 回收代币销毁；第二年，以每 2 个月为周期，回收代币销毁；第三年，以 1 个月为周期回收代币销毁。GXS 总量不会增发，回购销毁后流通量会逐渐减少。

公信宝的回收代币销毁账户为：null-account，这是一个初始账户，没有任何人可以掌握其私钥并动用账户里的资产，具体可用公信宝区块链浏览器查询。浏览器地址：https://block.gxb.io

关于数据交易所的交易量、交易额及佣金收入数据，您可以登陆公信宝网页钱包进行查询，具体方法如下：
1、登陆公信宝网页钱包：https://wallet.gxb.io
2、点击左上角的 “浏览” 按钮。
3、点击 “统计” 按钮，即可查询数据交易所的交易数据。

七. 团队主要成员介绍

黄敏强 创始人 CEO

香港财经学院 MBA 、山东科技大学 计算机学士
前汉鼎宇佑 (股票代码 300300) CTO
前汉鼎宇佑金融服务公司 总经理
前浙大网新互联网 副总经理
在数据交换、互联网金融、区块链领域工作和研究十余年，从 2012 开始研究数字货币和区块链，参与并发起多个区块链项目，同时也是超级马拉松、越野跑、山地自行车等耐力运动爱好者。

涂国君 联合创始人 VP

湖南大学 计算机学士
先后在 3 家上市 IT 公司担任高管职务
创建过多家科技公司，拥有超过 21 年互联网、支付、信息安全、大健康等行业的从业经验，区块链深度研究者。

王成 CTO

国内顶尖数据技术专家
前 51 信用卡架构师，曾任职国内著名互联网公司如阜博通、51 信用卡、大树网络并快速成为核心人物、主导角色。
在金融垂直领域衍生数据采集，清洗和挖掘有相当丰富经验。

徐若淞 CMO

复旦大学物理学学士
曾供职于华为技术、中国移动及同盾科技， 在数据领域、信贷风控领域有丰富的行业经验。

许潇鹏 运营总监

6 年市场营销经验，历任浙江广电集团、思美传媒、网易市场负责人，负责过大量产品和各种行业的品牌传播和市场活动，对互联网营销、品牌策略经验丰富。

吴立宇 产品经理

原网易高级产品经理，曾先后在同花顺、微贷网等公司负责产品设计工作。深耕互联网金融行业，在 C 端和 B 端产品上均有丰富的产品经验。

蔡鑫 日本社区经理

日本大阪大学无线通信专业硕士，曾在某国内知名通信公司海外市场担任技术工程师并负责项目管理。精通日语，英语，可听说韩语，擅长不同文化间的沟通和跨国技术项目拓展。

蓝昊翔 PM & 区块链开发工程师

前端技术专家，精通 Node、iOS，熟悉最前沿的前端技术和服务端技术，同时熟悉区块链的开发，擅长应用层的实现。曾任 51 信用卡、大树网络前端开发主程。和王成一起设计了一套如今被行业广泛模仿的前后端交互数据挖掘架构模式。

张俊杰 区块链开发工程师

全栈工程师，擅长 UI 设计，前端开发，后端开发；精通 node.js，python，负责过某外企、国内知名互联网金融公司前端开发架构工作，参与过基于区块链应用的开发工作。

朱礼廷 区块链开发工程师

数学学士和计算机硕士，拥有丰富的 P2P 网络开发经验，熟悉区块链技术开发，精通 C/C++ Python、Shell，曾就职于 Vobile 阜博通担任资深开发工程师。

屠家华 区块链开发工程师

精通 C++ 编程开发，熟悉前沿技术和 golang，前海康威视综合安防平台核心开发人员，作为项目经理和核心开发，完成多个版本的发布。

徐磊 区块链开发工程师

全栈工程师，熟悉各种前端技术，具备跨终端的前端开发能力和拥有数据可视化产品设计开发经验，精通 PHP、Node、Python，曾任浙报集团、房产销冠核心前端开发工程师。

尧俊 服务端工程师

资深 java 工程师，前大树网络核心开发工程师，拥有丰富的互联网开发经验，对于大数据采集、分析、挖掘有相当丰富的经验。

沈冬明 服务端工程师

资深 java 工程师，前典典养车核心开发工程师，拥有丰富的互联网开发经验，同时对安卓开发也有很深的研究。

叶狄武 服务端工程师

后端开发工程师，有丰富的数据采集开发、数据建模经验，实现了组件化的数据采集服务。