PKC(私钥链)白皮书

一个真正实现价值存储的区块链网络

上海零圈信息科技有限公司

发布日期：2019-1-10 V1.0

目　　录

一、区块链技术简介

2008 年 10 月 31 日,Satoshi Nakamoto(中本聪)提出了比特币的白皮书，从此我们迎来了区块链的世界。至今为止，比特币一直践行着”A Peer-to-Peer Electronic Cash System”(一个去中心化电子现金系统)的初衷.用密码学和代码捍卫了用户财产的安全，并且经受住了时间的考验。为区块链行业开创了一个良好的篇章。

而以太坊基于比特币的思想,更近一步,为用户提供了一个具有图灵完备的代码运行平台。虽然比特币基于堆栈的脚本系统也可以编写出较为复杂的应用，例如多重签名、时间锁、支付通道，但是相较于以太坊的 EVM 与 Solidity 还是欠缺了可读性与可扩展性。以太坊的出现使得区块链的可扩展性得到了提升。

区块链本身不是一个全新的技术，而是一些已有的技术的组合，使用了包括密码学、Bittorrent 的 p2p 网络、Hashcash 的 Proof of work 工作量证明、Unspent Transaction Ouput （未花费输出）、Merkle Tree 梅克尔树等， 产生了一个公平公正、解决信任的创新模式。

二、区块链技术挑战

运用区块链技术的去中心化、公平自治的系统，正在引起越来越多的研究人员以及用户关注。区块链的公平公正，规则透明，使得越来越多的基于区块链之上的应用场景被开发且应用。其金融属性，以及智能合约技术能解决社会中不公开不透明等问题，并且重建社会的信任机制。在区块链技术的蓬勃发展、应用场景不断产生的今天，用户对区块连技术的诉求正在逐渐的增加，我们关注到了现有区块链技术的缺陷:

1.私钥丢失。 据区块链显示数据统计目前 BTC 的私钥至少造成了约 400 多万个 BTC 永久丢失,更用户带来了非常巨大的损失.并且其他加密货币(eth,eos)同样存在着大量的私钥忘记或者丢失的情况,私钥的丢失给用户带来了无法估量的损失。

2.私钥复杂。 目前私钥的主流协议比如, BIP39(助记码), BIP32,BIP44 (分层规则钱包)虽然在一定程度上可以简化私钥的生成和记忆,使用助记词可以扩展

生成无限多个钱包的私钥/公钥配对.但是对于普通用户来说,记忆大于等于 12 个单词还是非常有难度的.私钥复杂的问题使得普通用户很难使用区块链钱包。

3.算力集中化。 据矿池数据统计比特币目前大约 70%的算力都来自中国，当在区块链系统中控制了足够多的算力时很容易发起攻击,虽然无法剥夺走用户的个人财产,但是可以发起 DDOS 拒绝服务攻击和 double spend 双重支付自己手里的币。使区块链不再是一个相对公平的去中心化平台。

4. **安全**。目前市面上的区块链项目,例如比特币所使用的脚本,以太坊所使用的 Solidity,都遭受过非常多的攻击,本质是因为语言系统是非常复杂的,没有办法开发出不包含 bug 的语言系统.区块链底层应该足够简单,保留最基础的功能,hard code 到程序中,简单到不可能有错误.而不是像现在的区块链项目一样过度设计,埋下了很多安全的隐患。

5.性能。目前市面上的去中心化区块链项目,例如以太坊,消耗了大量的计算资源,并且性能缓慢，其原因是系统设计的太过于复杂,把合约与货币设计到了一个系统内，系统设计应该遵循模块化原则:一个事物只做一件事情,并把它做到最好。合约应该不在链上计算,而是在链下通过多方签名得到最后的状态后再通过模块之间的协议与货币系统进行交互并且同步到链上。

三、PKC（私钥链）的设计原则

面对上述的技术缺陷和挑战，我们要设计一个简单、高效、公平、安全的区块链系统。

模块化设计： PKC（Private Key Chain）遵从模块化原则,一个事物只做一件事情,并把它做到最好。PKC 采用最小化设计方式,从比特币中提取最常用的脚本操作符,并硬编码到程序中。提供最简单并常用的的功能来实现底层货币系统。并把合约功能设计到另外一个系统中,采用时间锁,双向锚定等技术完成模块之间的交互,提升安全程序与性能,大大减少问题发生的概率。

存储理念设计: PKC 可以提供少量珍贵,隐私,机密绝密等极其重要数据的加

密存储。借助于区块链的存储即永不丢失的特性，给用户提供有价值的信息或者索引的存储接口,收取高额的管理费用,这样可以减少垃圾信息的攻击(粉尘攻击),具体费用估算是不低于磁盘的硬件价格，然后随着市场需求来自动定价，形成一个自循环的经济模型。

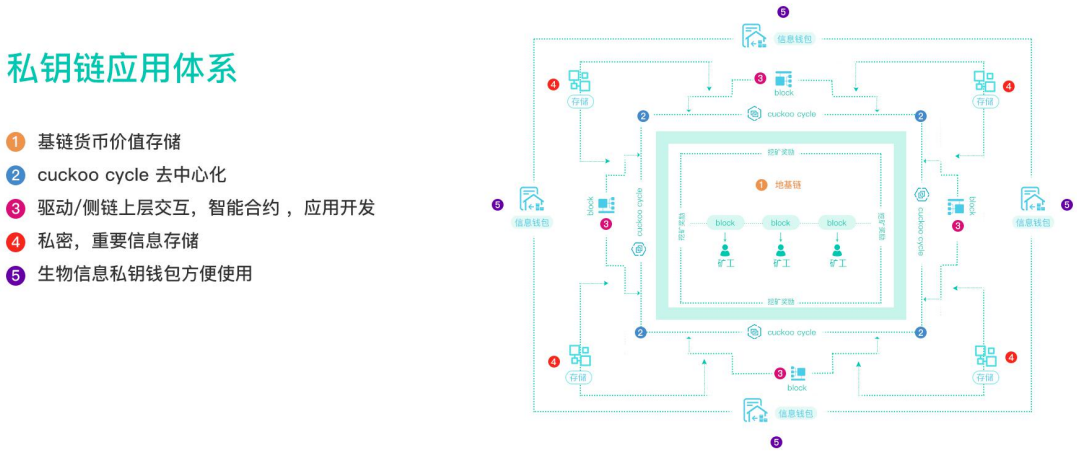
工作量证明设计: PKC 遵从”A Peer-to-Peer Electronic Cash System”的初衷，使用了荷兰计算机科学家 John Tromp 的基于图论的工作量证明算法 cuckoo cycle 帮助解决现在大多数区块链项目的中心化问题，使得计算难题依赖于内存访问延迟而不是哈希函数计算能力,很大程度上限制了 ASIC 高性能挖矿设备的产生，使用普通计算设备,CPU,GPU 也可以挖矿，保证了公平公正，同时也防止了算力过于集中而产生的操控行为。

私钥系统设计: PKC 结合生物识别技术,将私钥映射成传统的 id+password 的方式多中心加密存储,生物信息提供便捷支付功能，使得 PKC 不但拥有区块链的安全性,更具备传统软件的便捷支付方式，让普通用户也能很好的使用区块链系统。

基于上述设计原则,我们试图构建一个简单,高效,公平,安全的区块链系统。下文我们将描述技术的细节。

四、模块化智能合约

我们认为在区块链系统中,数字货币应当作为底层基础,如同 OSI(Open System Interconnection Reference Model)五层模型一样,层层之间分工明确,上层与下层之间用明确的协议接口来完成调用,每一层做好它应该做好的事情。例如OSI 的网络层只负责 IP 数据包的传输,而上层传输层可复用网络层的传输接口来实现 TCP 链接,重传机制,拥塞控制,或者 UDP 的面向数据包的协议.在我们的系统中也是如此,最底层的地基只做货币应该做好的事情,复杂的功能通过标准的协议交给上层来把控。图示：



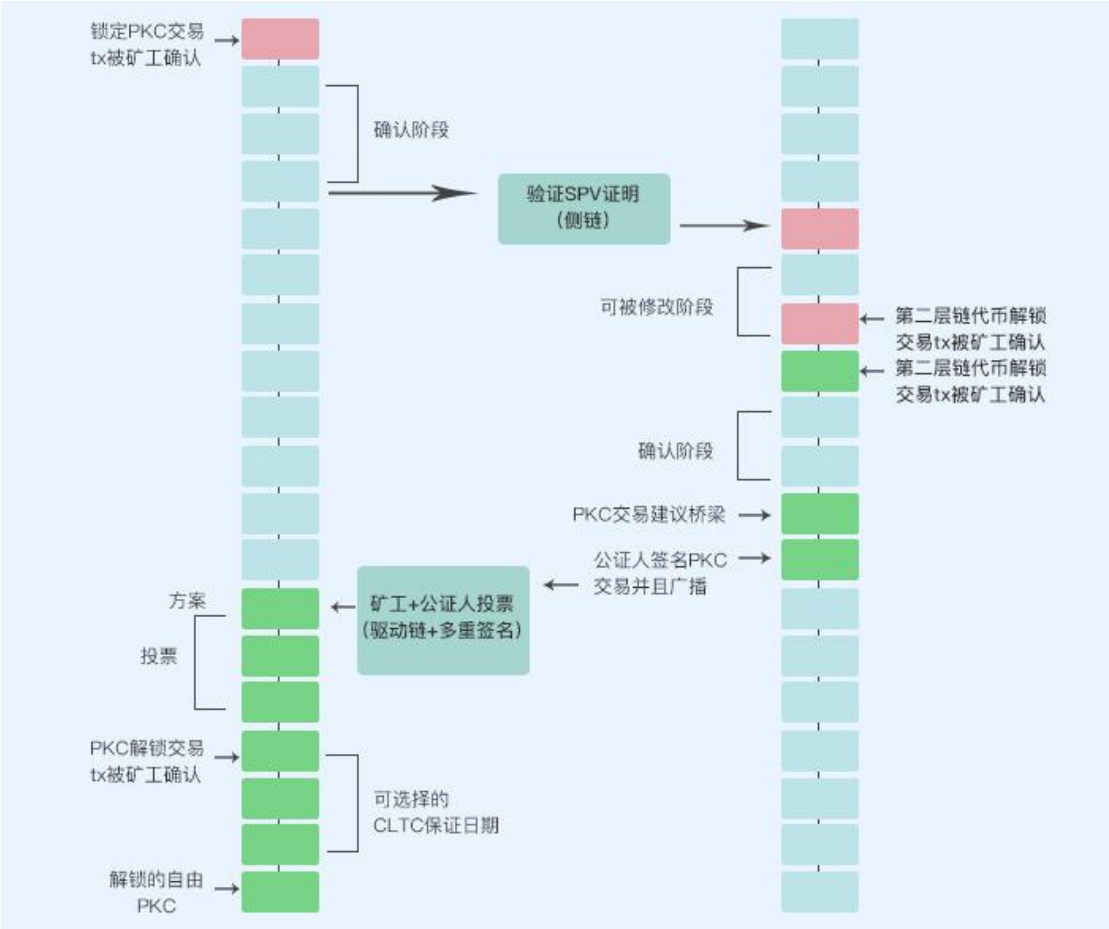
（一）地基链

我们提出了地基链的概念,其提供最小化的关于货币所应该具有的基本功能,例如转账,时间锁定,多重签名,支付通道等.并且使用硬编码,抛掉诸如以太坊的EVM 或者比特币的脚本，可以大幅的减少代码量,以及系统的准确性，将接口的标准定义为 KIP (PrivatekeyChain Improvement Proposals)。

（二）侧链+驱动链混合智能合约

对应智能合约应用层,我们将设计成地基链的上层应用。之所以选择侧链+驱动链的混合方案是因为地基链是货币层,其安全程度比之上层应用来的更为重要,因为上层应用不发行货币，货币转移到其他系统时可以使用侧链的技术,而把货币从上层系统转移到地基链时,需要考虑到安全性,所以我们应用了驱动链的技术。

驱动链允许矿工们投票决定何时解锁数字货币和将解锁的数字货币发送到哪里.矿工使用 coinbase 中的字段来实现投票,越多的诚实矿工参与投票,安全性就越高。



五、存储系统

区块链虽然可以永久的保留数据，但是其并不是解决类似互联网上的海量数据、大量图片和视频的存储，PKC 的存储系统只存储有价值的信息或者索引，并为此收取高额存储费用。

（一）隐私和安全

我们会提供存储的接口，需要用户输入复杂的密钥组合，将信息对称加密存储，然后打到区块链的块体中，可以存储小型数据量，安全级别高的数据。用户凭借私钥可以索引到所有链上存储的数据。

六、工作量证明

(一) Bitcoin 工作量证明的实现与问题

区块头:

```
int32_t nVersion;
uint256 hashPrevBlock;
uint256 hashMerkleRoot;
uint32_t    nTime;
uint32_t nBits;
uint32_t nNonce;
```

HASH 出块规则将随机变化

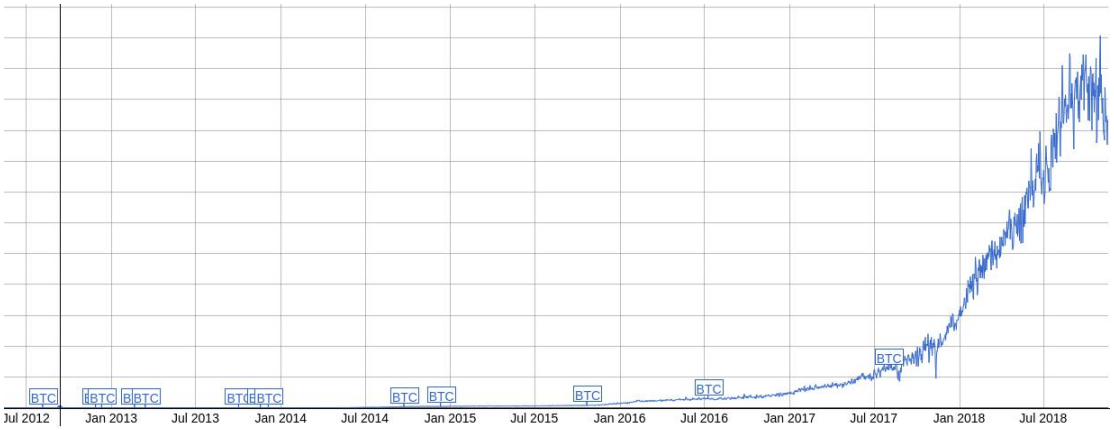
1. Coinbase 的交易数据变化以达到 hashMerkleRoot 的变化，总共 8 字节的随机源
2. nNonce 4 字节的标准随机源头
3. nTime 时间值（单位秒）

也就是允许矿工每秒尝试 2^96（*79228162514264337593543950336)*次产生不同的随机数达到如下规则:

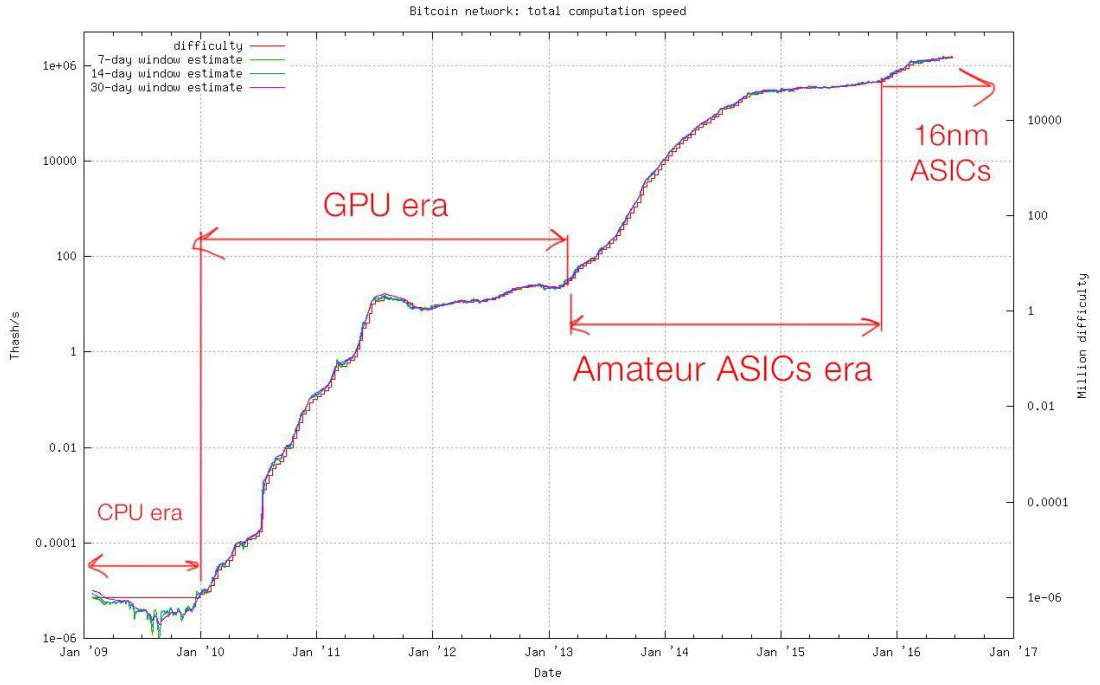
SHA-256(header) < (nBits 生成的 Target)

而在面对这样一道难题,普通的通用 CPU 并不是专用挖矿设备(ASIC)的对手:

1、平均每秒计算 hash(SHA-256)次数:



2、军备竞赛:



当 ASIC 产生之后会加剧中心化发展,因 ASIC 芯片掌握在少数人的手中，维护交易网络公平的工作量证明变成了少数 ASIC 制造商的装备竞赛以及数据中心的部署竞赛(部署在节省电费的地方)

中心化之后会产生两个严重的问题:

1. 当权者使用分叉手段实现双重支付,也即是把自己的资产通过分叉调整多次花费。
2. 拒绝服务攻击,阻止特定的交易打包,使得交易网络瘫痪,击跨交易网络

（二）PKC 的工作量创新

采用荷兰计算机科学家 John Tromp 的基于图论的工作量证明算法 cuckoo cycle（https://github.com/tromp/cuckoo）改进这一问题：

```
int32_t nVersion;
uint256 hashPrevBlock;
uint256 hashMerkleRoot;
uint32_t nTime;
uint32_t cuckooBits;
uint32_t cuckooNonce;
std::vector<word_t> cuckooNonces;
```

工作量算法证明的算法的一个问题在于如何控制求解的难度,因为我们要保证稳定的出块时间 1 分钟，而矿工的中途加入或者是退出都会带来全网算力变化而引致出块时间的变化，因此我们要寻找一种合理可行的调整难度控制出块时间的方法。

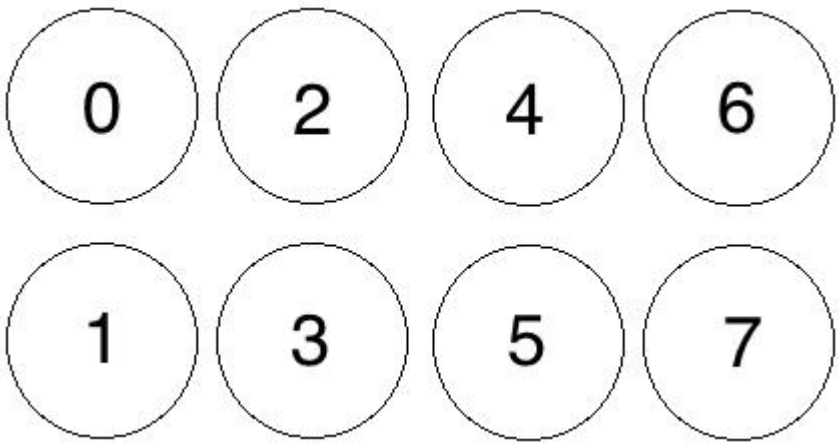
我们将 cuckoo cycle 图搜索算法与 sha256 相结合，当寻找到图的解后，通过 sha256 结果点的集合 cuckooNonces 与 blockheader，验证是否小于 cuckooBits 生成的 Target 来判断是否寻找到正确的答案，cuckooBits 作为了难度调整的限制。

cuckooNonce 与 hashMerkleRoot 以及 nTime 作为生成图的随机源. 每秒可产生 2^96 (79228162514264337593543950336)次产生不同的图

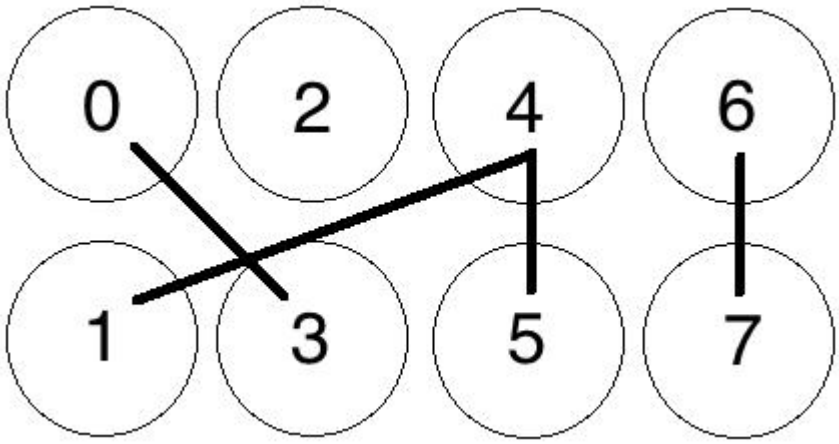
（三）图搜索的原理阐述与优点

利用区块头数据生成二分图,如果二分图符合指定规则即表示找到了问题的答案.

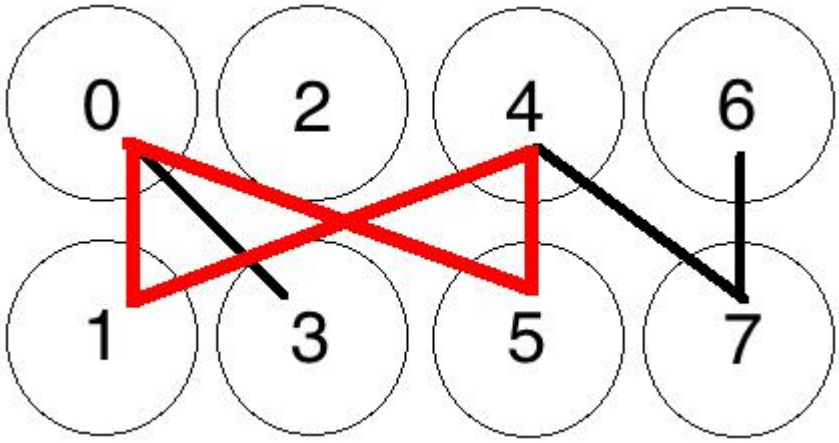
1、只有节点,没有边,所以没有环路



2、随机添加一些边,有边,没有环



3、有环[0-5-4-1-0]



Cuckoo cycle 与 SHA256 hash 算法不同的特点是将计算密集型任务变成了内存访问延迟密集型任务.使得普通的民用 PC 机,平板电脑,智能手机,甚至是树莓派也能加入到挖矿工作中.减缓中心化的趋势,技术更能够保障用户的财产。

七、私钥系统

（一）生物信息技术

PKC 参考了目前的主流私钥规则,BIP39,38,32,43,44. 在其之上,添加了一些创新的思考,将私钥的规则映射成私钥命名系统,提供账户与密码,以及采取生物信息，将 12 个单词的助记词或者 32 字节的私钥(64 个 16 进制数字)转换成较短的用户名+密码,并且通过生物信息验证环节,极大的提升了数字货币钱包的易用性,同时也不失去可用性。

PKC 提供私钥托管服务,将用户的私钥以多中心的方式加密存储,保障了用户财产安全，并且通过生物信息技术,使得私钥无法被穷举破解。

八、研发团队

吴奇骏

系统设计

上海交大EMBA
荷兰商学院MBA
携程 技术经理
爱代驾 创始人

茹云峰

合伙人
区块链技术总监

比特币研究员
中国系统架构师大会 主讲嘉宾
超级课程表 CTO
新浪微博 架构师
阿里巴巴 技术专家

龚国春

区块链工程师

胜科金仕达 区块链工程师
证券系统研发架构师

张后富

区块链工程师

云形控股 技术总监
一唐技术 区块链工程师
昆山炫生活 区块链专家
万城金控有限公司
联合创世人及技术总监

冯超

区块链工程师

携程 高级工程师
爱代驾 技术经理
舜凯 总架构师
主要研究分布式系统
以及应用密码学

吴学杰

后端架构师

携程 高级工程师
考拉秀 架构师
淘金子 架构师

梁治文

区块链工程师

经济学硕士
高级工程师
12年IT行业从业经验
精通PHP，JAVA，C，
Python,MySQL,Oracle,redis

周威

前端技术经理

币达 资深前端工程师
一米辅导 前端工程师

张威远

区块链工程师

藏龙卧虎网络科技 创始人
蜗牛说平台 合伙人
朗源 高级开发工程师

黄俊生

区块链工程师

GO高级工程师

李志强

APP开发工程师

Android 资深开发工程师
Android 钱包高级工程师

朱超

APP开发工程师

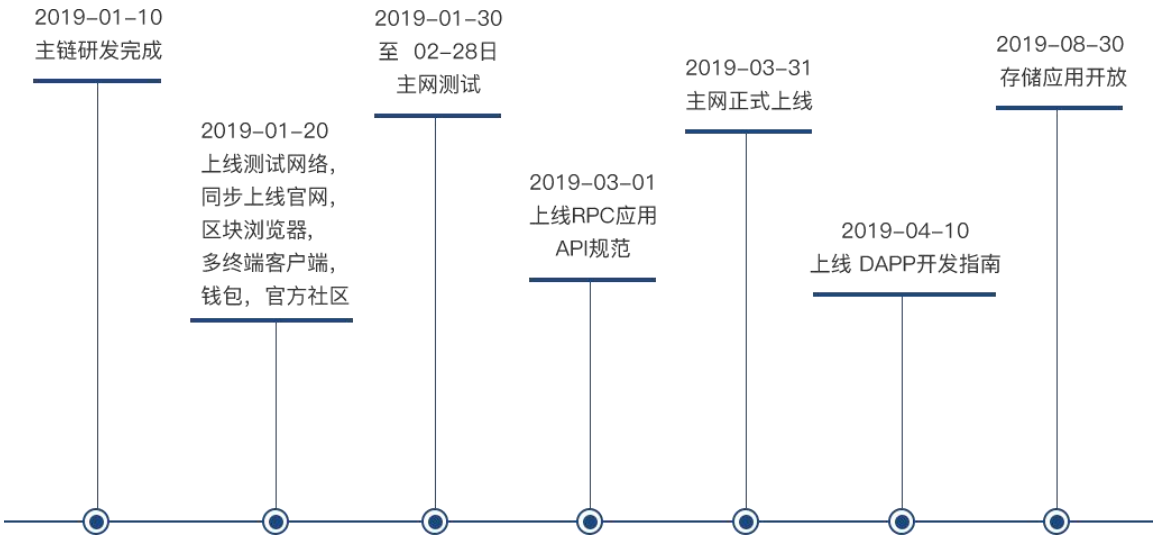
IOS资深开发工程师
IOS钱包高级工程师

张瑞

APP开发工程师

IOS资深开发工程师
IOS钱包高级工程师

九、时间线



十、引用文献

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System.2008

[2] Giulia Fanti. Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees.2018