

信链白皮书

1 概述

1.1 我们正在失去对个人资料的控制

痛点：首先我们正在失去对个人资料的控制，其次大公司控制了个人数据，占山为王的数据孤岛开始出现，而这两点正在阻碍数据在更大范围内的共享和协同，阻碍共享经济的更进一步发展。

目前，许多网站的商业模式，都是向用户提供免费的内容，从而换取用户的个人资料。不过，为了换取网站的免费服务，大部分人似乎并不介意一些个人信息被网站所收集，包括但不限于社交、搜索引擎、广告、电商、云存储、游戏等。我们的数据被保留在这些公司的数据库中，这些信息完全游离于我们的视线之外。我们不能直接控制这些数据，我们也无权选择何时与谁分享，一旦数据分享出去，我们就已经失去了这些个人资料的控制权。我们甚至往往没有办法向这些公司反馈我们不愿意分享的数据。而数据的集中，也导致了包括政府在内的组织滥用这些数据，我们甚至都不知道这些数据在被如何使用中。

欧盟早就有过关于个人数据安全保护的立法，俄罗斯、日本、美国、我国等都有跟进。这些法律里面明确规定了个人对其数据应该享有**数据可迁移权**、**数据可删除权**、**数据使用知情权**，这些法律法规如果能够得到执行将会很好的保护所有用户的数据安全和个人隐私。

1.2 如何夺回个人资料的控制权？

在区块链技术出现之前，要很好的实现数据安全保护的三个权利可以说是难上加难，基本上是不可能的。而因为区块链所具有的数据不可篡改、去中心化、自证其信、非对称加密等特点将可以很好的实现这三个权利。

虽然区块链技术可以解决这些痛点，但是目前现有的区块链技术、商业模式上并不够成熟，无法大规模的应用于绝大多数的场景，所以改进现有的或发展新的区块链技术就成为的当务之急。

那么现有的区块链技术究竟有哪些问题呢？接下来的章节将会先详细讲解一下现有区块链的技术、商业模式的问题，然后再介绍我们自己的技术、商业方面的解决方案。

1.3 现有区块链面临的问题



图 1 现有区块链面临的问题

1.3.1 技术问题

比特币的技术问题大部分都是其核心算法PoW带来的，其问题主要有：

1. 并发交易量有限，只支持7笔交易不到，完全无法支持大规模应用
2. 交易确认时间比较长
3. 数据累积问题严重
4. 隐私保护不足
5. 不支持小微额交易
6. 算力容易被垄断，存在51%攻击问题
7. PoW算法需要不断挖矿，浪费能源
8. 对大部分普通人来说操作不够友好，很容易导致遗忘密钥，或导致被黑客攻击。

1.3.2 经济模型的问题

从系统控制论的角度来说，比特币是一种非线性的复杂金融系统，其价格与用户量的关系是一种典型的正反馈关系，而正反馈只会导致系统不稳定，也就是说随着用户量的增长，其价格长期来看将会不断上涨，但是没有任何一种商品的价格能够长期维持在上涨通道中，这就导致中短期来看，比特币的价格将会不断的处于剧烈的波动当中，其价格曲线大概会是这样（价格波动过大）：

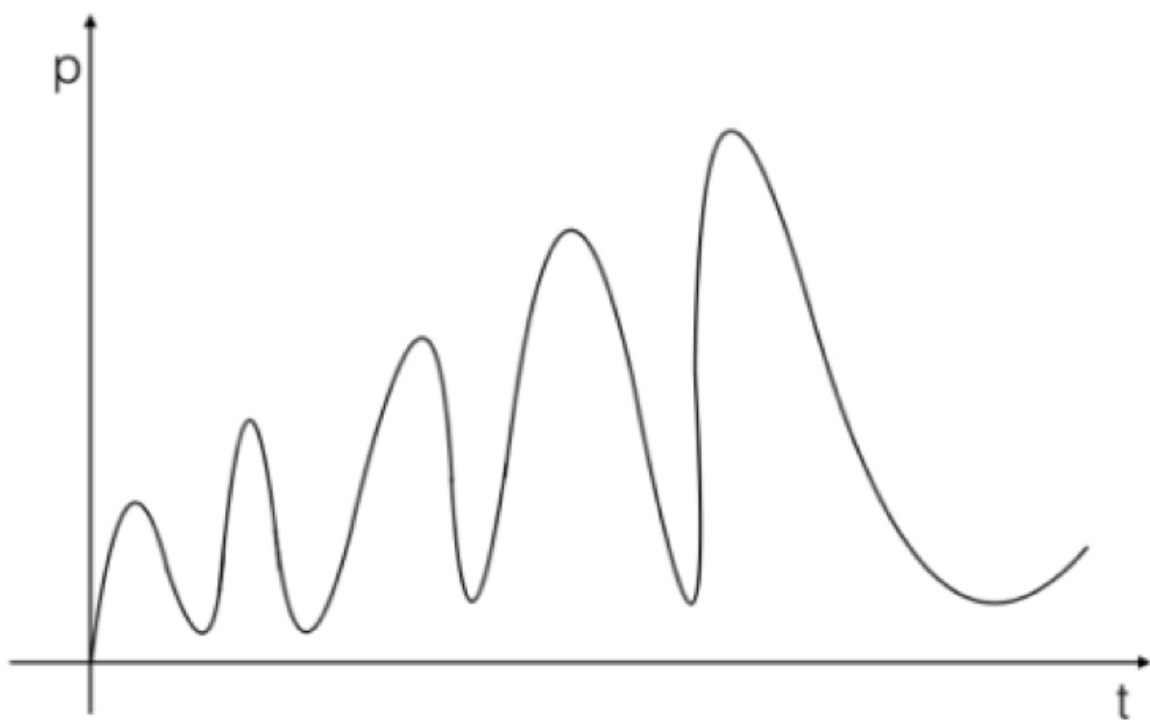


图 2 比特币的价格走势预测

而理想的价格走势应该如下：

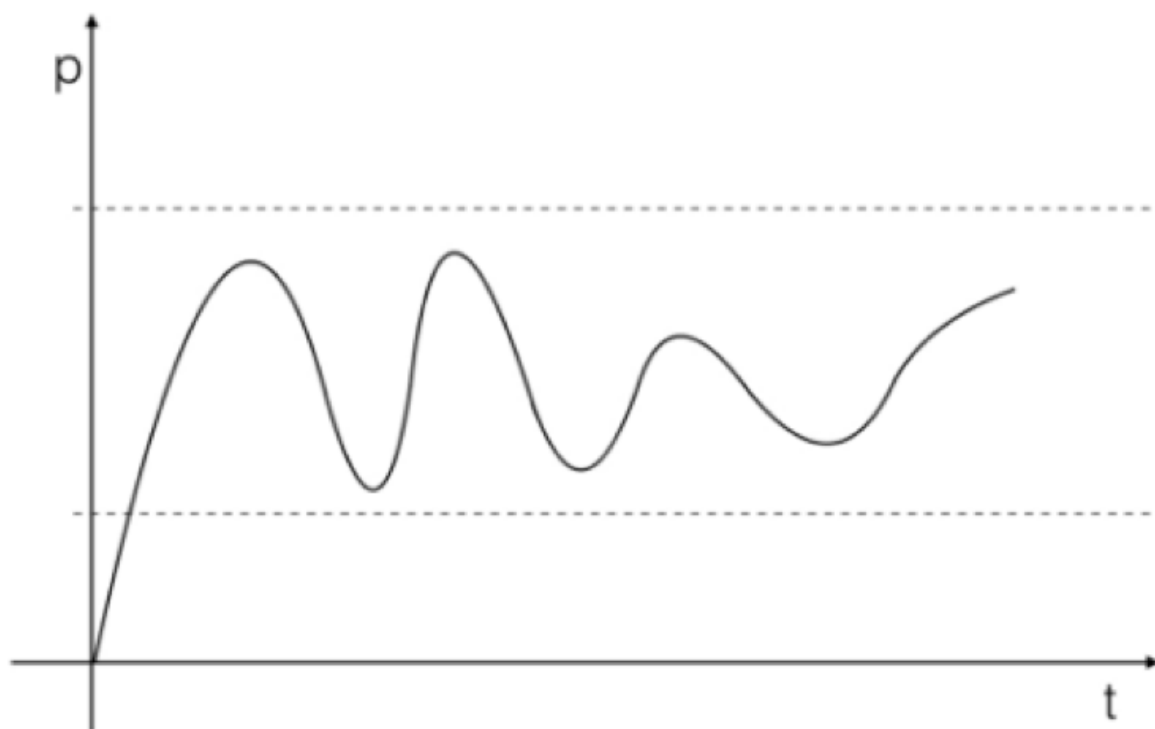


图 3 理想的价格趋势

加密货币的使用者可以分为两种不同角色：投资人和普通用户，投资人角色肯定是希望该币的价格可以一直上涨，而且上涨的越快越好；普通用户却是希望其价格在一定时间内保持稳定。

1.4 我们的解决思路？

为了不依赖于任何的底层数据存储服务提供商，我们采取经济激励的方式鼓励用户贡献自己的空闲存储资源，这样可以通过市场手段来自动调节数据存储空间的供给，让供需获得匹配；

同时提供一个数据存储控制层，用算法来决定某块数据将存储在哪里，但是用户自己可以根据自己的喜好选择数据存放空间，但是系统会自动为用户进行选择最佳的数据存放空间，大部分时候用户无需为此烦恼。

让用户自己来控制怎样存储，用户可以选择自己控制自己的数据，可以在任何时候删除自己的数据，可以在任何时候把自己的数据迁移到任何地方，只有获得用户自己的许可，任何第三方才能使用用户自己的数据。

下图可以很好的看出我们的云盘产品与传统云盘的区别：我们提供的是具有更高安全性、可删除、可迁移，具有数据使用知情权的云盘。

传统云盘与信链云存储的比较

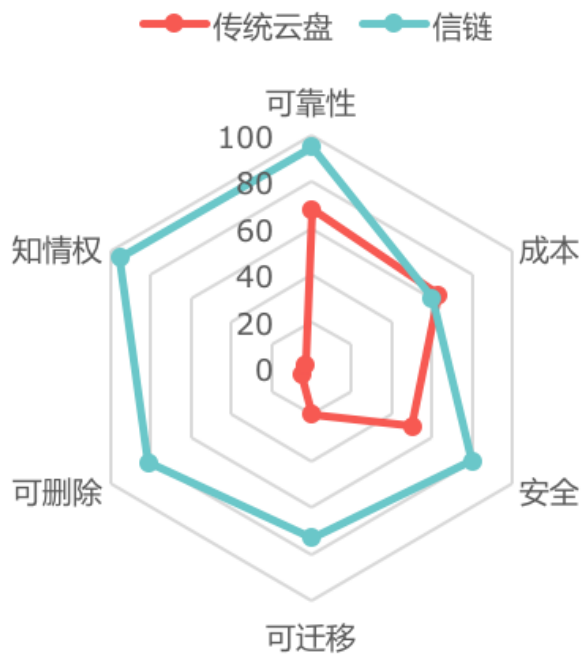


图 4 传统云盘与信链云存储的比较

1.5 怎样赚钱？

我们的平台的商业模式类似苹果公司的应用商店模式。主要有三种盈利途径：

1. 作为应用商店运营方我们采取与开发者进行分成的模式获取收益；
2. 在应用商店中向开发者收取广告费，SDK使用费等；
3. 作为开发者，开发相关应用，直接向消费者收取费用。

下图是苹果应用商店最近三年的营业收入，而区块链之上可以构建更加丰富的各种互联网应用，可以说这里面蕴含的市场机会至少是几百亿甚至是千亿美金级别以上的机会。

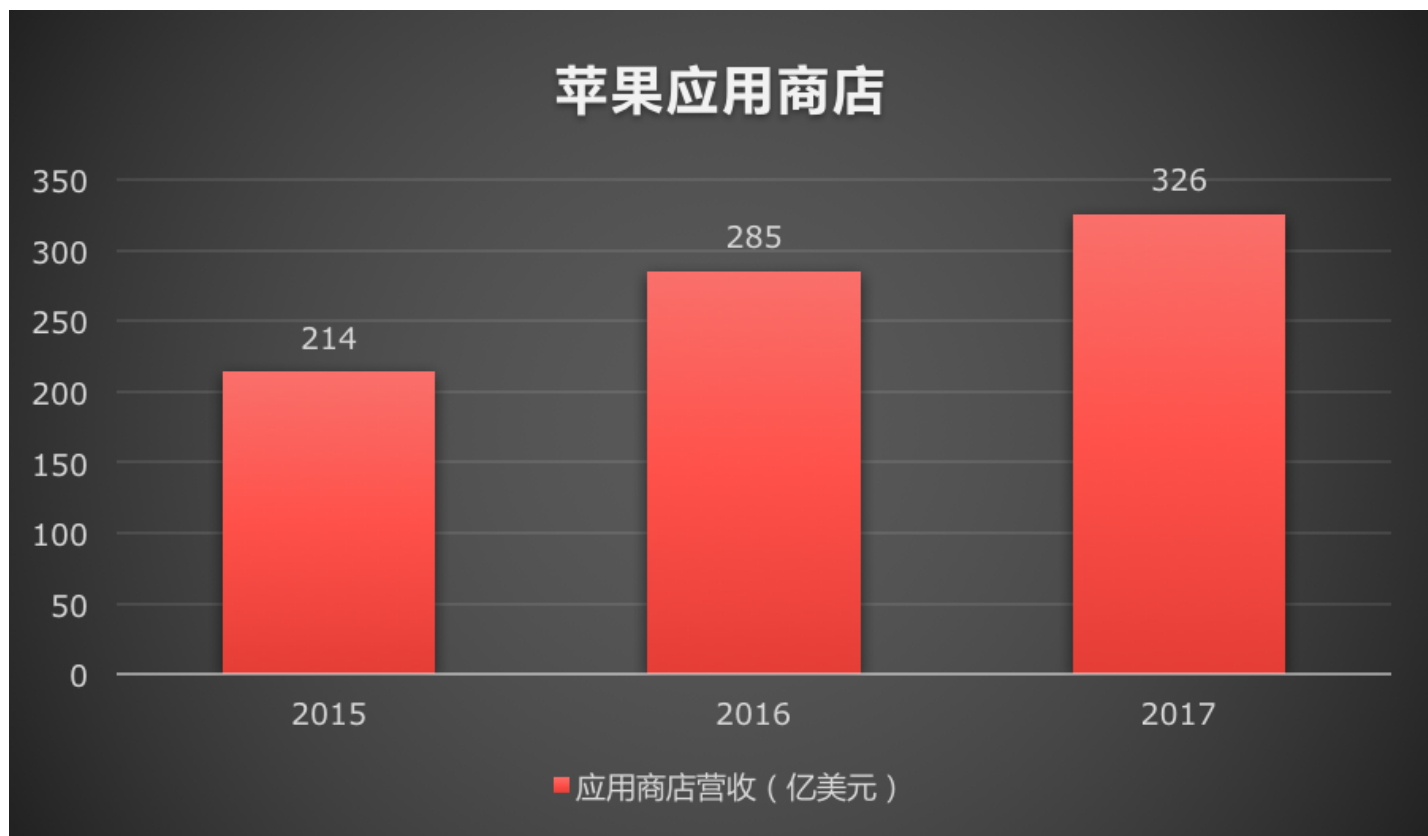


图 5 苹果应用商店营收

2 信链简介

2.1 我们的定位

云存储领域的Uber，我们不提供云存储服务，我们只提供数据管家服务，因此我们可以视为一种存储中间件，自动化的帮助用户将自己的数据存储在各个底层存储服务商那里。

另外信链还是一个下一代区块链技术平台，一个价值交换、传输网络平台，任何第三方应用都可以基于信链的SDK进行开发。

2.2 我们的理念

用区块链连接全世界的人和机器，保护每个人的数据所有权；因为信链，信任无忧。

3 信链的技术和产品

信链相比于比特币、以太坊的最大优势在于以下三点，分别是：

1. 创新的PoD共识算法，比特币的共识算法本质上是对用户贡献的算力进行激励，而我们的共识算法是对用户贡献的存储和带宽进行激励。

- 2. 独特的经济模型：价格波动没有那么巨大的系统，内建的激励机制可以很好的激励股东自愿自发的贡献自己更多的资源促进整个生态的发展。
- 3. 自治的账号系统可以让普通用户自己控制自己的身份、数据，无需依赖任何第三方机构。

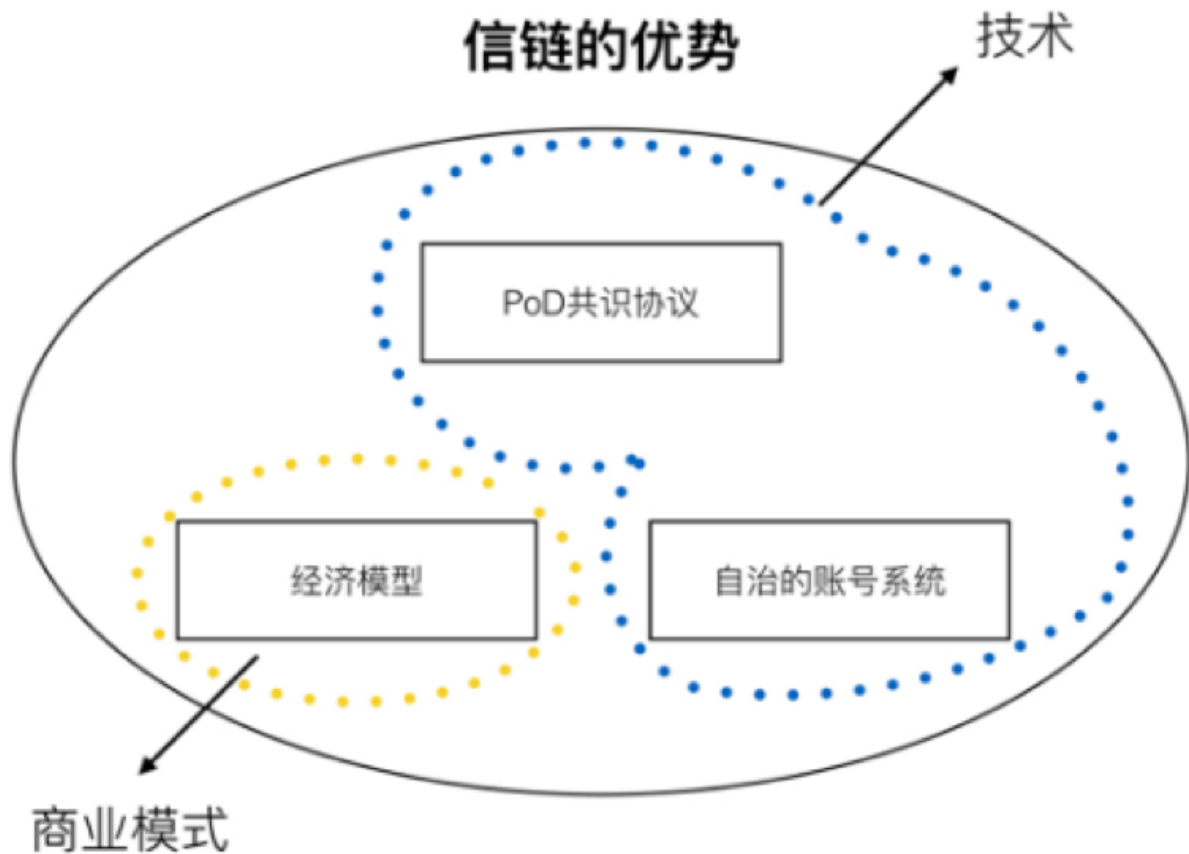


图 6 信链的优势

3.1 信链的技术

3.1.1 信链的架构

信链的网络节点可以是用户家里的个人电脑，可以是Aws、Azure、UCloud、阿里云等任何云计算服务提供商的主机，只需要安装信链的客户端，连上网络，就可以通过信链网络连接彼此，形成一个p2p网络。下图是信链的整体架构图：

信链架构全景图



图 7 信链架构全景

信链采用的是多链的架构，由一条核心链和多条侧链组成，下图中L0和L1层是完成系统主要功能的功能层。

信链分层图



图 8 信链架构分层图

信链的核心帐本层，也就是L0层，采用源自比特币的UTXO结构来对交易进行组织、记录，账本上的所有交易公开可查，可追溯。是一条交易链，采用UTXO结构。采用UTXO结构的好处是：

1. 同一个区块上的多笔交易可以并发执行；
2. 所有历史交易都可以被很方便的回溯，方便审计、校验；

L1层是系统服务层，包括账户管理、名称解析、权限管理、多链管理等功能。

L2层是上层应用配套的侧链，通常是由第三方开发商来注册建立、维护，每个上层应用都可以申请自己的链，这些应用链的数据既可以是公开的，也可以是私有的，创建者可以通过权限来控制其他用户的查询和读写权限。