信链白皮书

作者：黄立峰

version 0.8.1

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）：

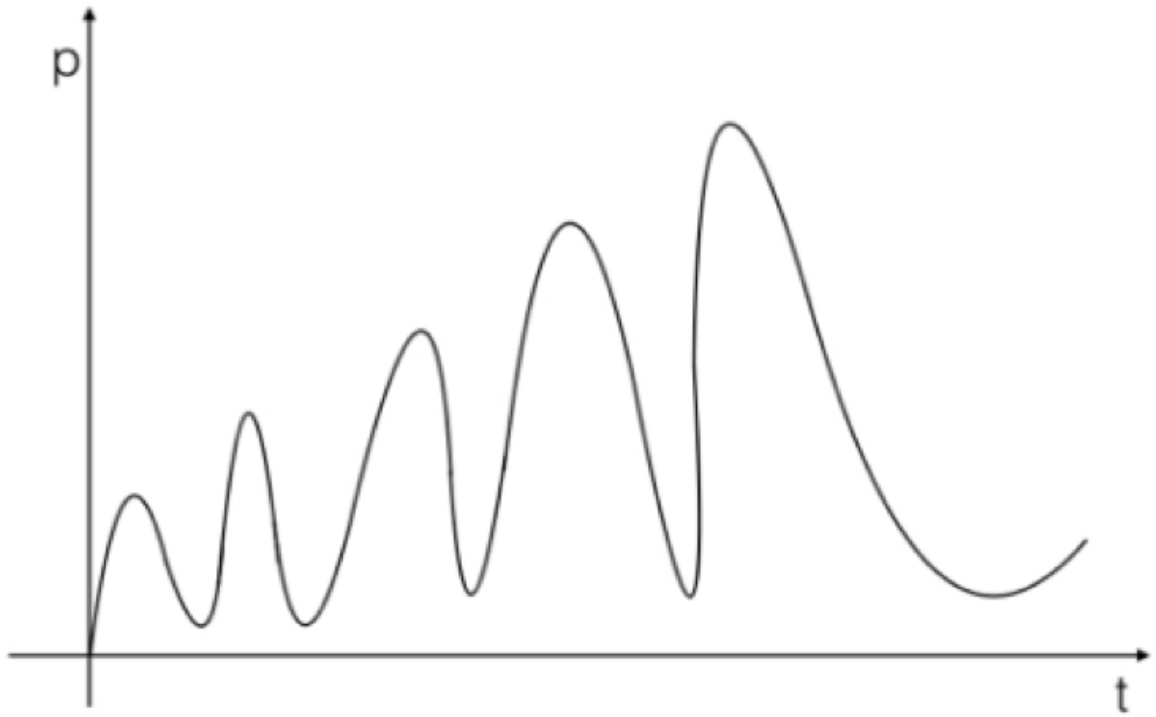

图 2 比特币的价格走势预测

而理想的价格走势应该如下：

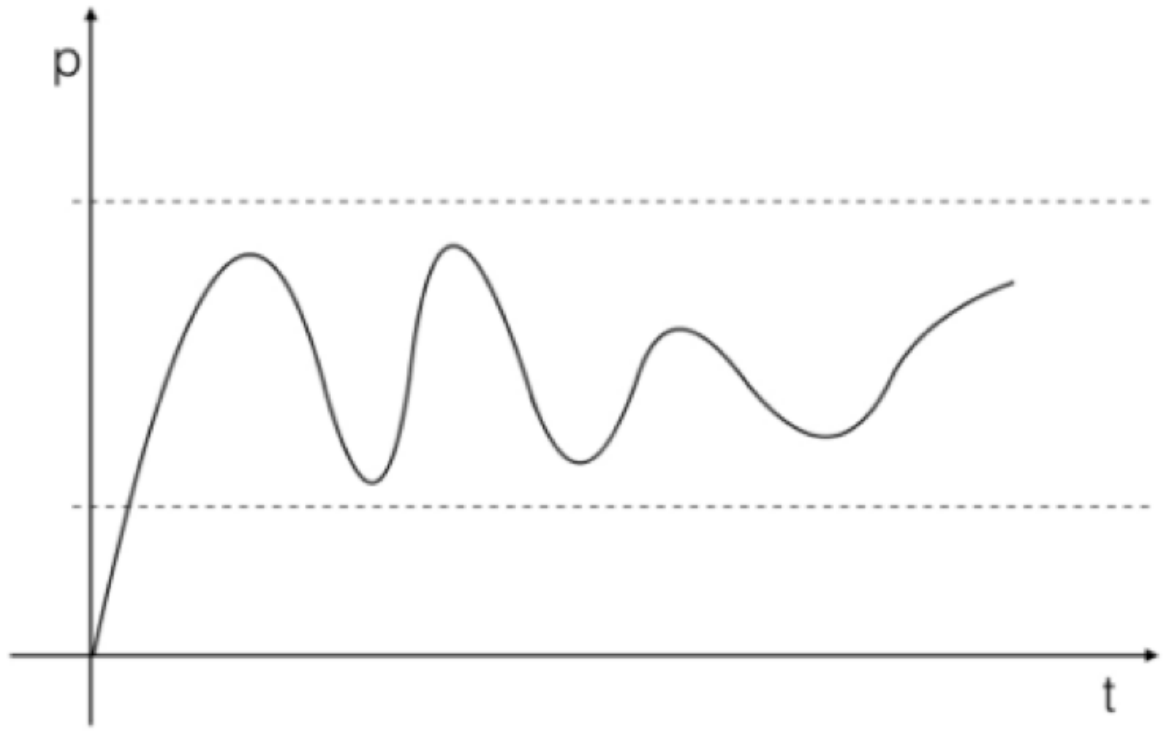

图 3 理想的价格趋势

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。

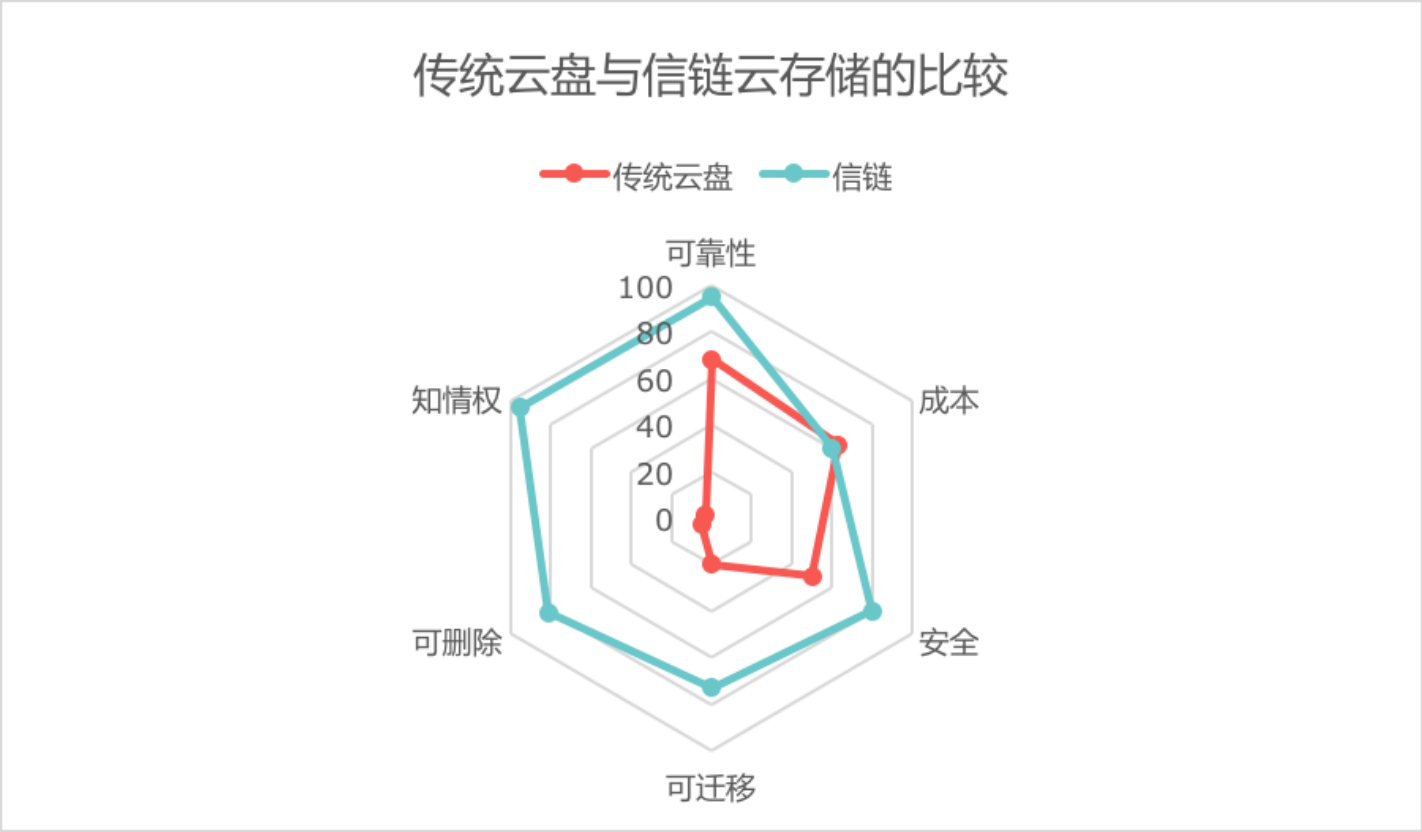

图 4 传统云盘与信链云盘的比较

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。

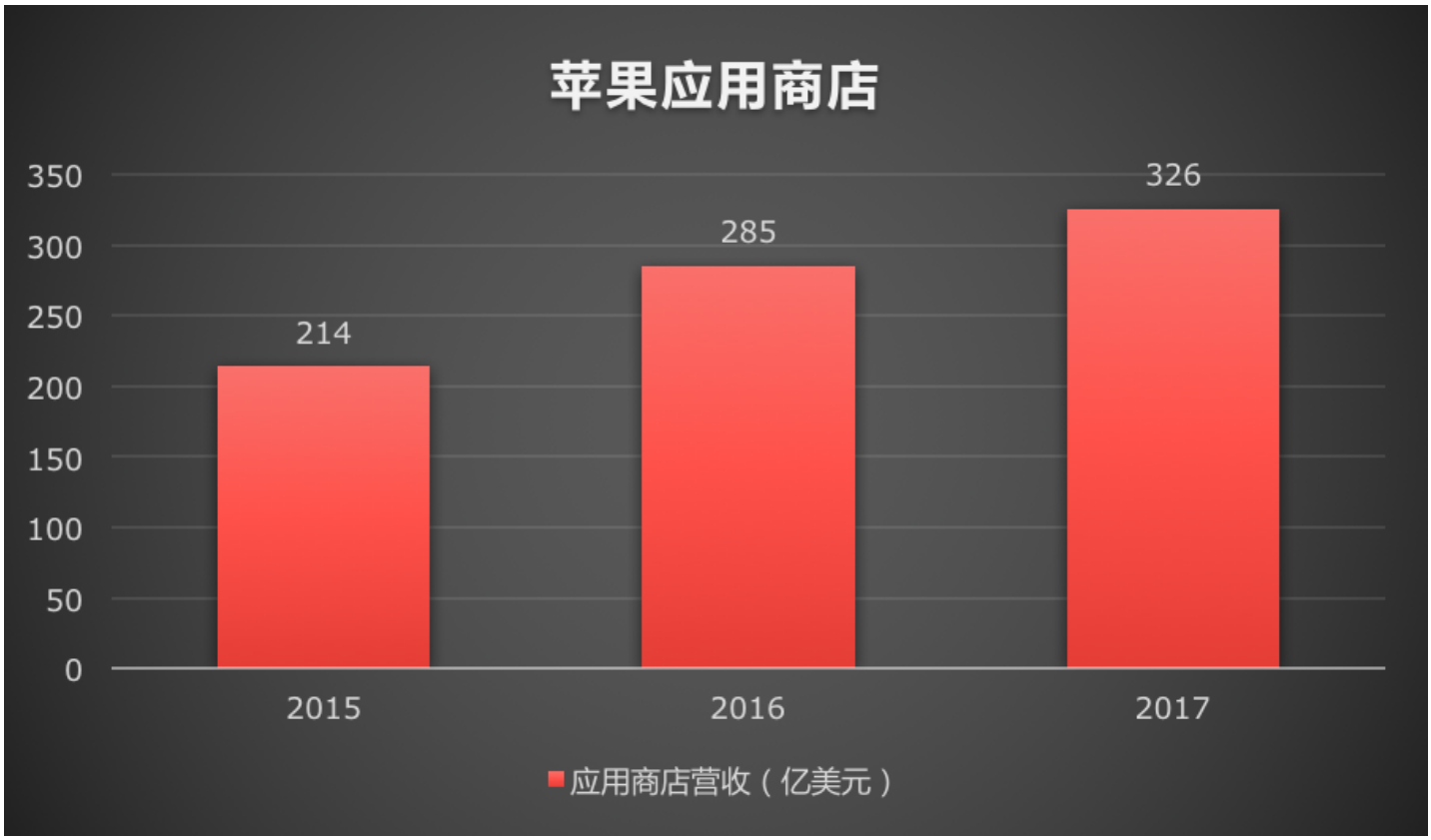

图 5 苹果应用商店营收

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。

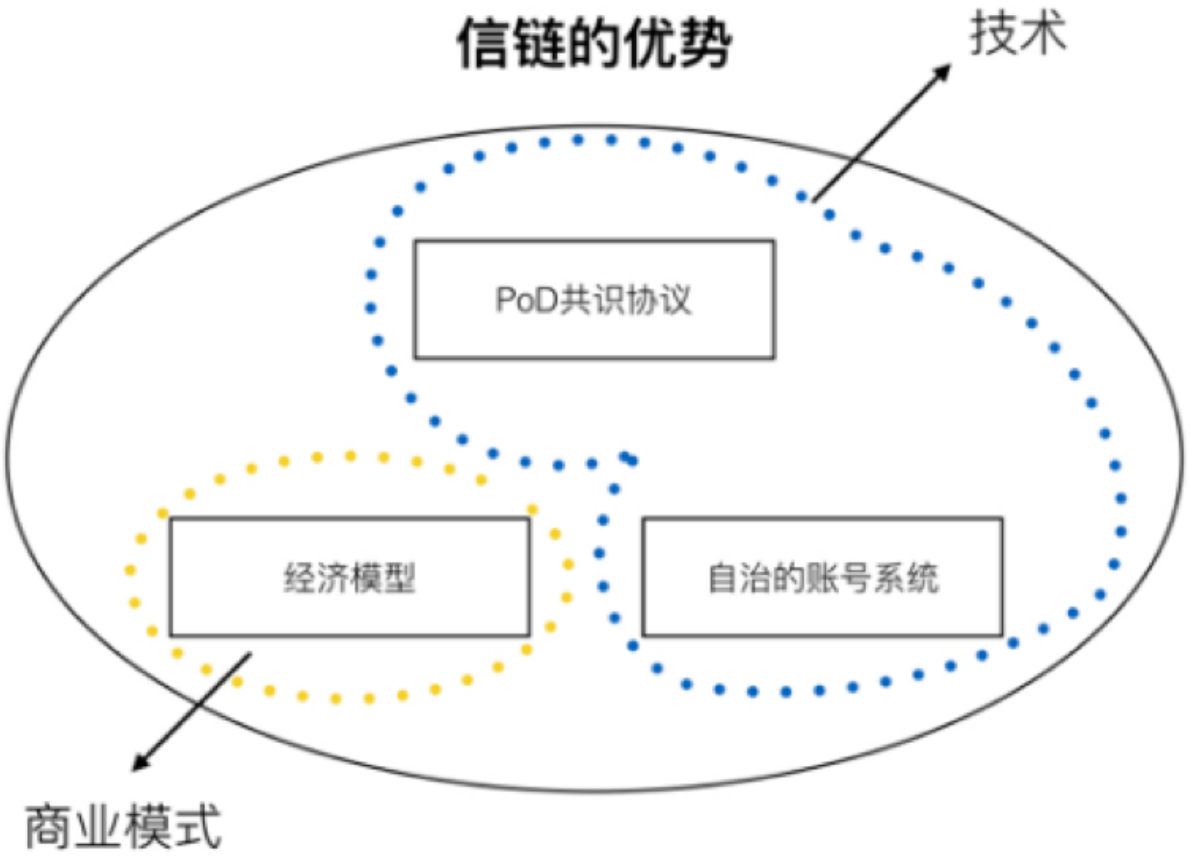

图 6 信链的优势

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：

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。

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；

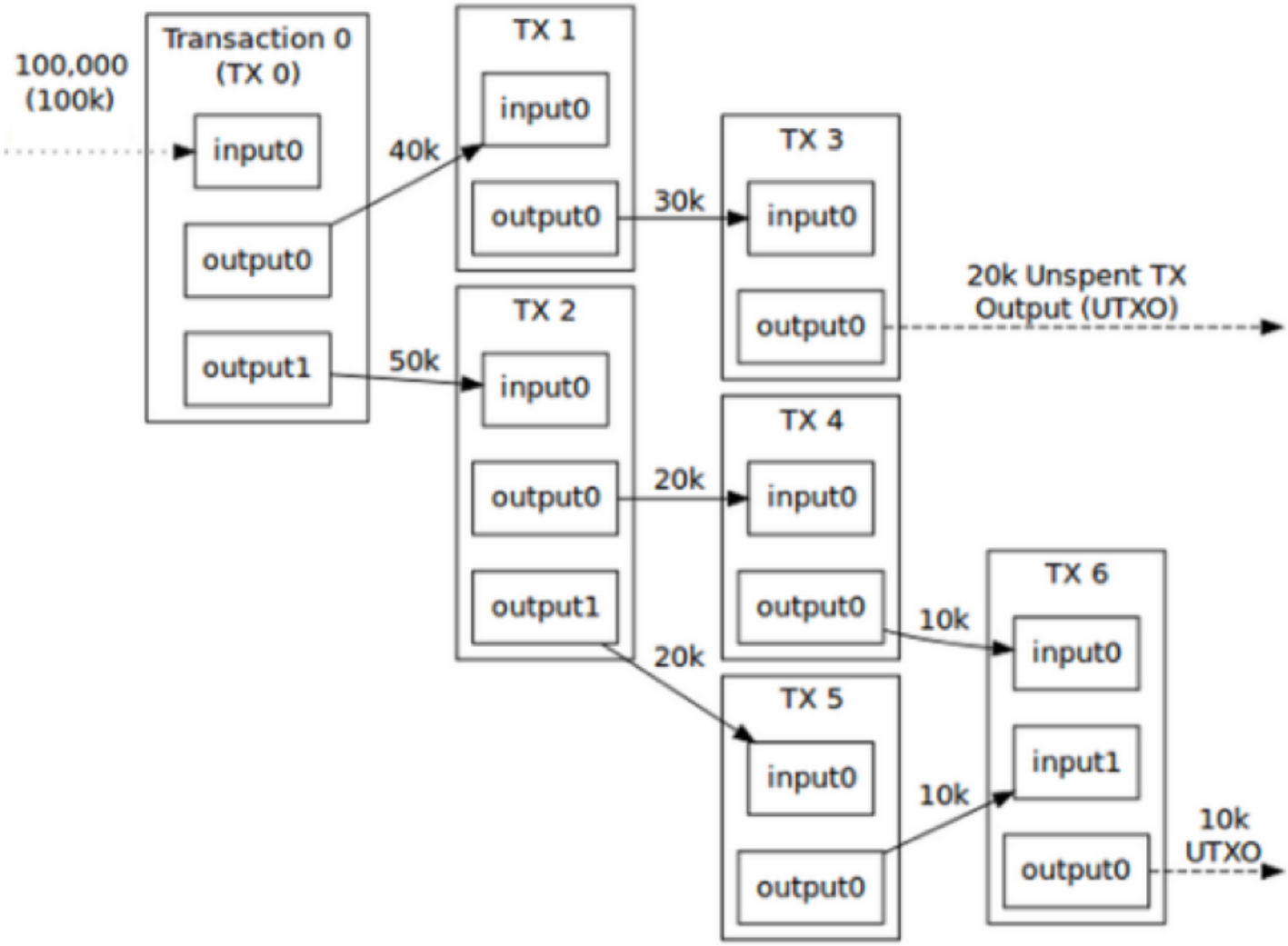

图 9 UTXO

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。

3.1.2 PoD共识算法

共识算法是区块链的核心算法或协议，我们有我独创的PoD（Proof Of Data）共识算法。共识算法是区块链的核心算法或协议，区块链网络从机器的角度来说，其三个物理构成要素分别是：算力、存储、带宽；PoW算法本质上是对用户贡献的算力进行经济激励，而我们的算法是对用户贡献的存储和带宽进行经济激励。比特币是第一种把共识算法与经济激励相结合的成功应用，经济激励对维护整个网络的长期安全可靠稳定的运行、对整个比特币生态圈的良性循环具有不可替代的作用，而我们的算法只从激励的角度来说与PoW算法完全不一样，是一种全新的算法或协议。

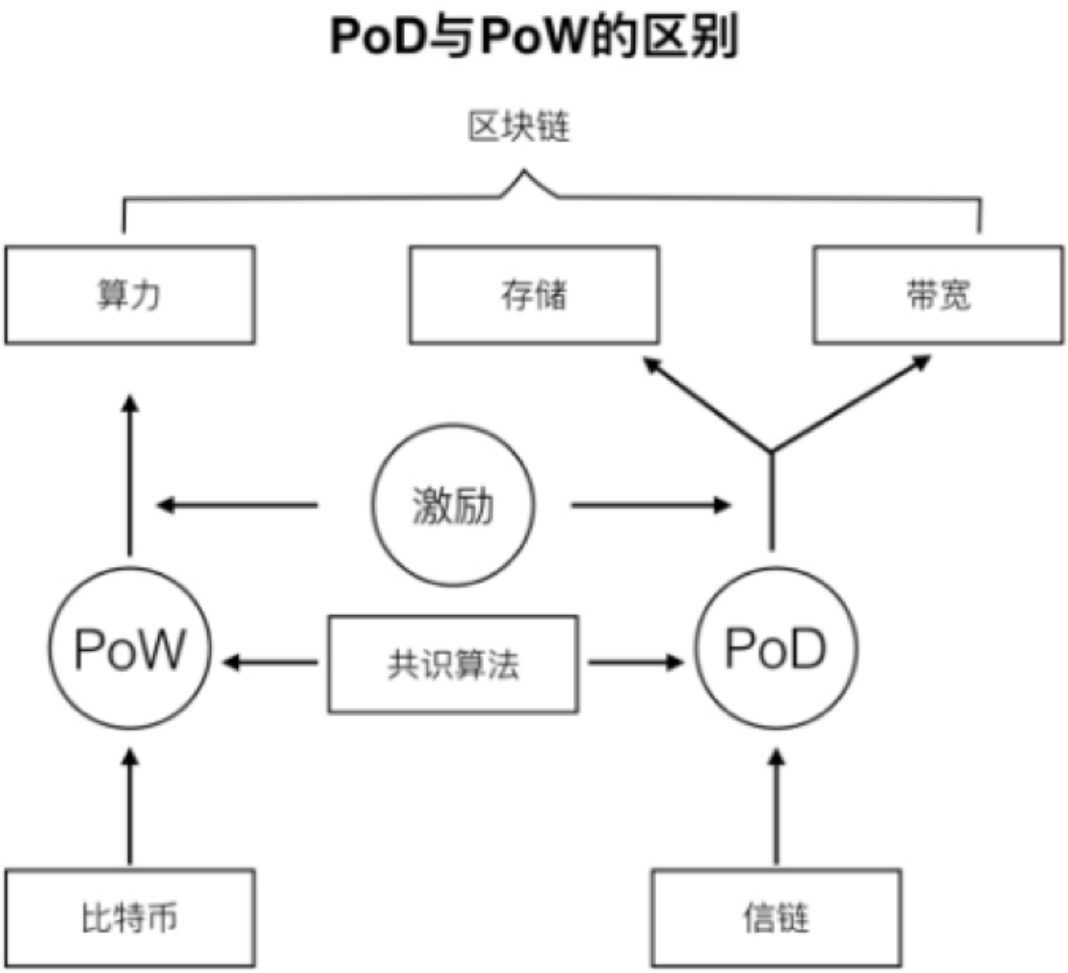

图 10 PoD与PoW的区别

我们的PoD算法无需挖矿，用户只需要存储指定的数据（通常是账本数据）并在线一段时间，就有机会获得相应的经济激励。

算力是一种线下资源，任何人只要有足够的金钱，就可以购买到足够多的算力，从而可以实现算力垄断，可以很轻易的发起51%攻击，这对整个网络的安全是一种潜在的隐患。

而存储和带宽都是线上资源，是无法垄断的，举个例子来说：假如我有1G的数据需要存储，用户A贡献了10G的空间，那我们只对其给予对应于1G空间的经济激励，多出来的9G空间是不起作用的；同理，对带宽资源也是一样的道理。这样就可以真正做到多劳多得、按需激励的效果。

3.1.3 公私钥及地址生成方案

信链的地址系统分为两种，实名地址和假名地址，实名地址与真实世界中用户的某个属性一一对应，如用户的邮箱地址、身份证号码、或者某个生物特征ID；每个用户有且仅有唯一的一个实名地址，但是可以有很多的匿名地址，而且用户可以随时弃用自己的某个匿名地址，所以说匿名地址相当于用户的一个假名，可以用于隐藏用户的真实身份。为了很好的保护用户的隐私性，保障用户在绝大部分情况下都不会泄露自己的实名地址。

信链的私钥、地址生成方案基本上遵循BIP 0032，也就是分层决定性钱包地址方案:

```
实名地址 = DoubleHash（根公钥）
假名地址1 = DoubleHash（子公钥1 + P），P是用户选择的一个随机字符串；
```

这样用户的每个假名地址都能够很轻易的从用户的根私钥生成，而且很容易验证，但是却无法从假名地址反推出其对应的根私钥，也就无法与实名地址进行关联。

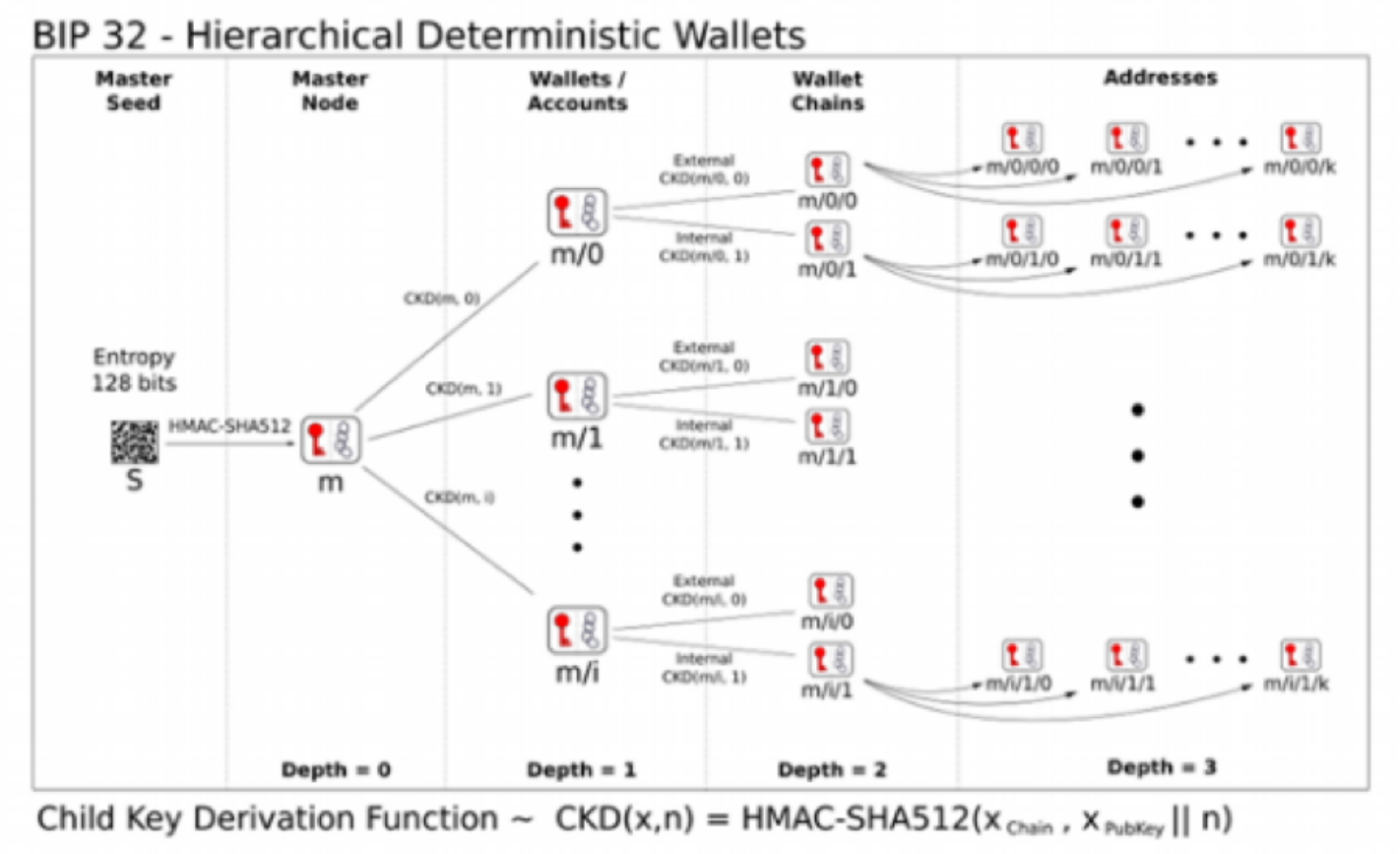

图 11 分层确定性钱包地址方案

3.1.4 用户自治的账号系统

信链将会同时支持实名账号和假名账号，以匹配不同的用户需求。匿名账号的交易记录、账号余额都是公开可查的；实名账号的交易记录、账号余额是保密的，只有交易相关方可以查询。实名账号可以实现更多人性化的易用服务，比如账号密钥重置功能。 而假名账号则可以用来保护用户的交易记录、账号余额等信息不被泄露。

采用该模型，其隐私性不会低于ZCash、达世币等专注于隐私保护的特殊币种，却具有更好的用户友好性。

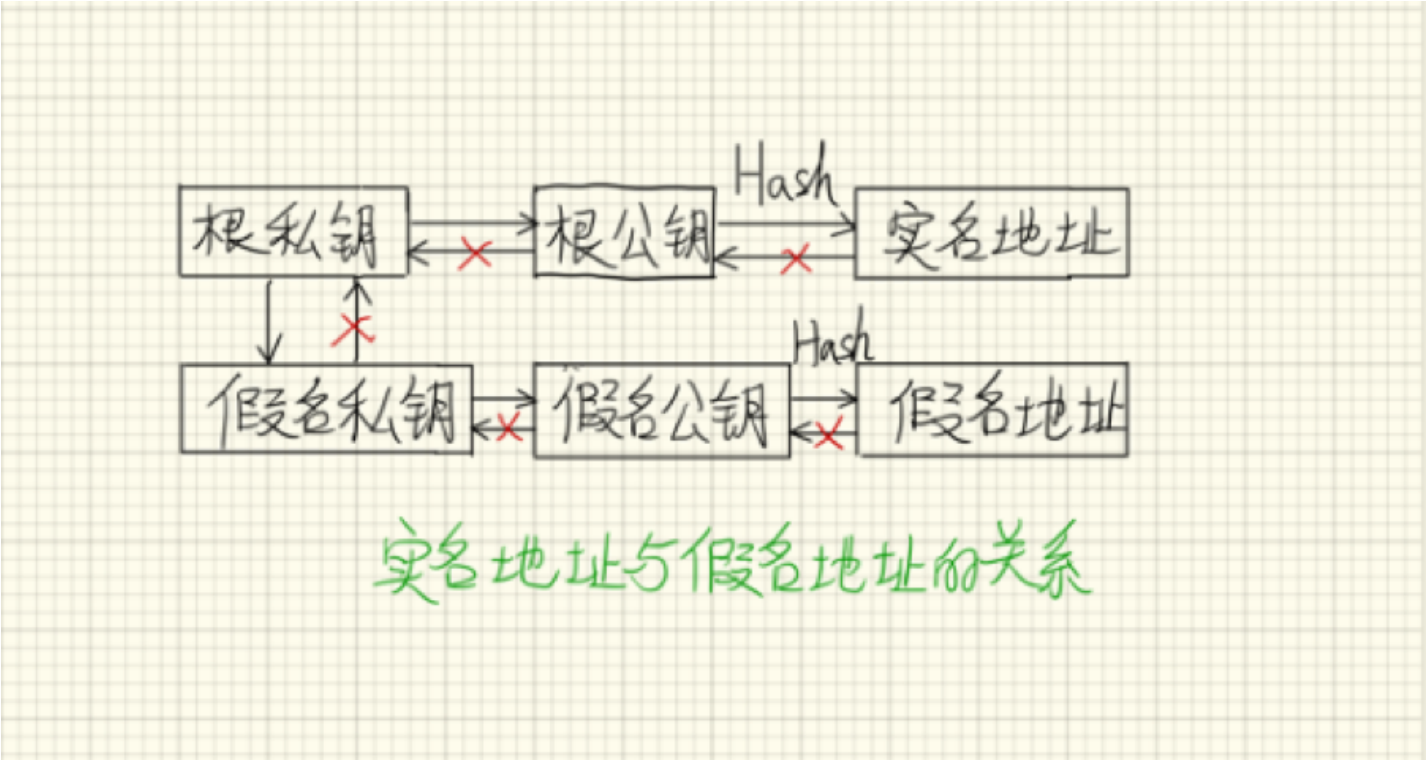

图 12 实名地址与假名地址的区别

3.1.5 信链的保密交易

因为同时支持实名账号和假名账号系统，信链得以实现高度隐私的保密交易，其流程如下：

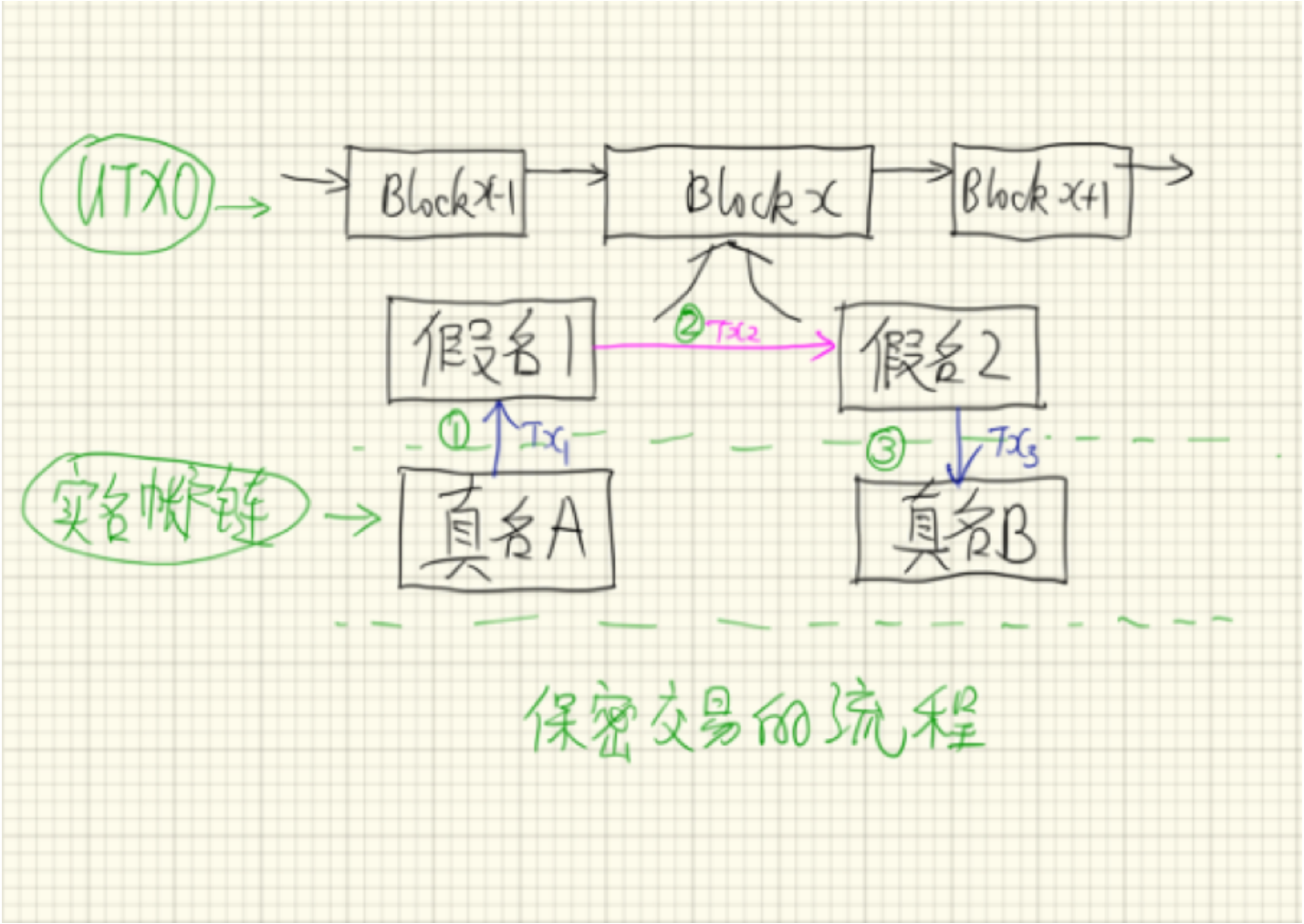

图 13 信链保密交易的流程

上图中Tx1和Tx3都是保密的交易，Tx2是公开的交易，Tx1和Tx3的数据保存在账号链上，只有交易相关方才能查询到这些交易；Tx2的交易保存在核心的交易链上，其数据是公开可查询、可验证、可回溯的。

3.2 信链的经济模型

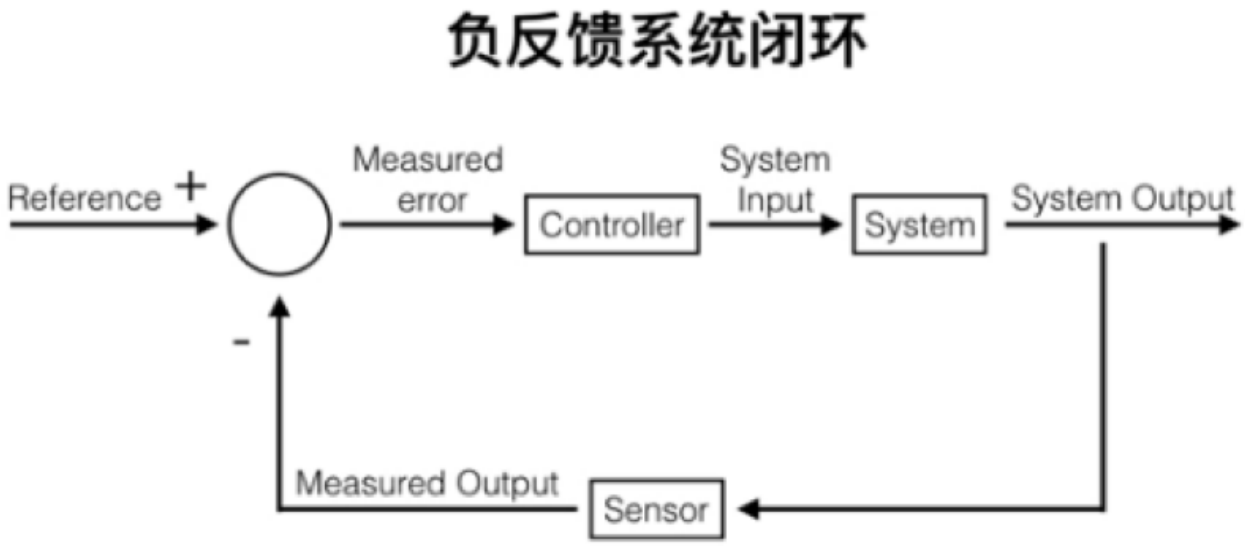

图 14 负反馈系统

从控制论的角度来看信链的经济模型，可以发现信链的经济模型是一个负反馈系统，负反馈系统的一个最重要的特性就是其是趋于稳定的，而比特币的经济模型则是一个正反馈系统，也就是说是无法稳定运行的。

信链币将会通过ICO的方式发行，信链币与比特币在产品特性上的最主要差别就是信链币的总量是根据当前用户数来确定的，而比特币的总量是固定的。

信链币的ICO中，股东通过某种被广为接受的硬通货比如（比特币、ETC、或人民币、美金）换取信链股，信链币的发行方共识互联网络科技公司将会设定一个最低的目标用户数（常数，比如100万用户），那么计算公式如下：

- 其中Ue代表当前信链平台的有效用户总数；
- 其中S代表信链股的总数；
- 我们将Ue * k / Umin 称为信链指数Idx；

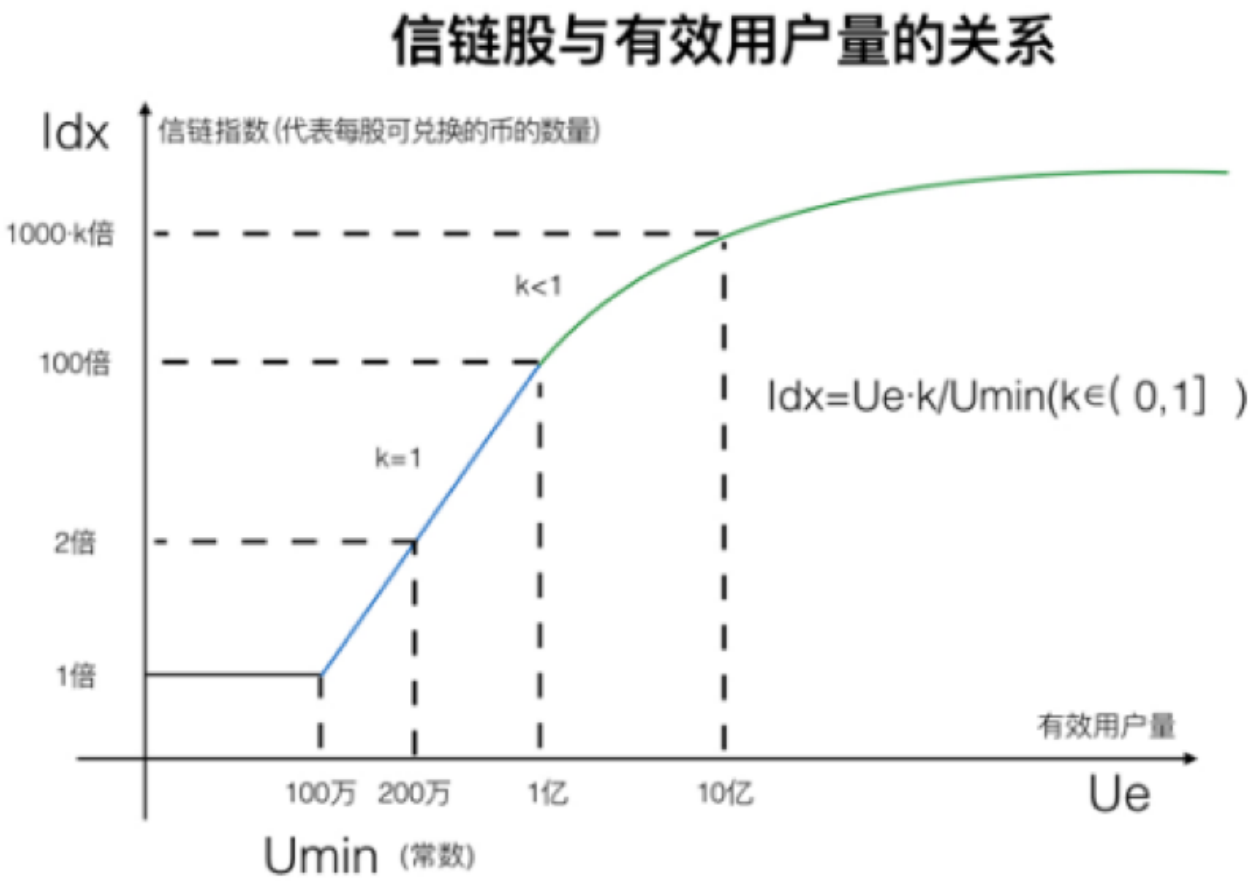

图 15 信链股与有效用户量的关系

3.3 信链的产品

3.3.1 产品功能

信链与比特币的产品功能对比图可以很清楚的看出信链在产品上已经大大超越了比特币。

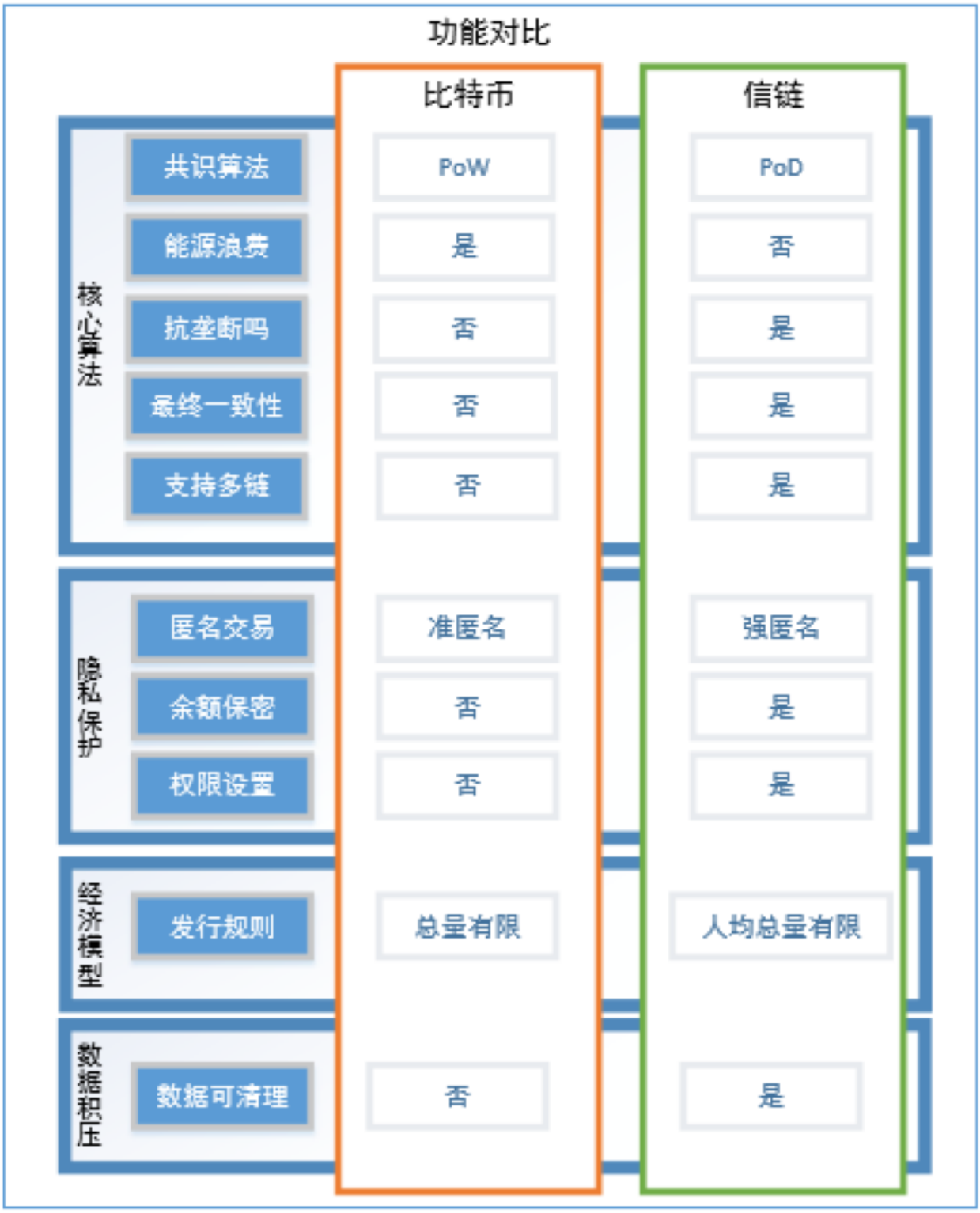

图 16 比特币与信链的比较

4 信链平台的应用场景

4.1 数据安全与隐私保护

痛点：现有的云盘无法保障个人的数据被遗忘权（或数据删除权）、数据可迁移权、数据使用知情权；

凯文凯利说过所有的生意都是数据的生意，马云说过数据就是生产资料，这些都充分说明掌握数据所有权的重要性，在数字化时代每个人都应该掌握自己生产的数据的所有权，主要包括数据被遗忘权（或数据删除权）、数据可迁移权、数据使用知情权；

区块链解决方案：将每个人自己生产的数据放到自己指定的空间中，只有自己能够决定何时删除、何时修改、何时交易自己的这些数据；这些数据存储空间必须不被任何大的机构所控制，但是也不限制任何愿意善意提供服务的商家提供这些存储空间。

4.2 知识产权保护

信链可以用于进行知识产权的保护，尤其适合数字化内容的保护，比如艺术品、音频、视频等。这里面蕴含着巨大的市场空间，因为有数据显示互联网上80%以上的流量是音视频流量，国内的视频网站就有好几十家，现有的DRM技术基本上无法很好解决各种盗版的问题，而区块链是一种很有前途的数字化内容产权保护技术。

4.3 会计记账

痛点：行业标准复式记账法过于复杂，效率低，已经几百年没有改进了。

复式记账法（Double entry bookkeeping）起源于13~14世纪的意大利。借贷记账法“借”、“贷”两字，最初是以其本来含义记账的，反映的是“债权”和“债务”的关系。复式记账法对于每一笔经济业务，都要以相等的金额在两个或两个以上相互联系的账户中进行登记，系统地反映资金运动变化结果的一种记账方法。

区块链解决方案：我们正在研发的基于区块链的协同单式记账法（Collaborative single entry bookkeeping）所取代，因为基于区块链的记账将可以做到更加高效和简单。这必将是一种颠覆性的创新，涉及到几乎所有的行业、企业，虽然这可能会是一个比较漫长的过程，但是趋势是不可逆的。

4.4 去中心化的搜索引擎

2009年全球搜索引擎市场规模达339.0亿美元，2015 年全球的搜索引擎市场规模达到 815.9 亿美元。目前，全球搜索引擎用户达18.57亿，中国搜索引擎市场用户有5.66亿，占到了全球的30%。但从收入看，中国2015年的搜索引擎收入102.36亿美元，只占到了全球的12.5%，小于GDP在全球的占比16%，中国的搜索引擎市场收入规模还存在很大空间。

但是中心化的搜索引擎带来的各种弊端显而易见，最主要的就是缺乏监管，其通常的商业变现模式是付费广告，但是广告效果通常是由搜索引擎提供商自己说了算的，这种过度中心化的商业模式一定会被不那么中心化的商业模式所替代的，我坚信只有削弱过于强势的搜索引擎提供商的中心地位才能真正更好的为客户服务。或许有人会认为增加一些竞争对手可以降低强势搜索厂商的中心化地位，可是如果不从根本上变革搜索引擎的商业模式，这只是前驱狼，后继虎，并无法从根本上改变搜索引擎厂商一家独大的状况。基于区块链技术或许有可能实现去中心化的搜索引擎。

4.5 互联网广告

痛点：互联网广告行业的造假非常严重，一方面是中心化的商业模式带来的问题，一方面是技术上没有更好的解决方案。

区块链解决方案：区块链技术的出现将会给互联网广告行业带来很多变化，例如一定程度的去中心化或许将带来行业商业模式的变化。

商业前景：互联网广告是谷歌、百度最主要的收入来源，谷歌更可以说是世界上最大的互联网广告公司。2016年，中国网络广告年度市场规模为2769亿元，同比增长率为29.7%，略有放缓。但从整体发展来看，网络广告市场仍将保持较快的增长水平，预计在2019年将超过5000亿，2016-2019年的复合增长率仍将在25%以上。

图 17 2011-2019年中国网络广告市场规模及预测

4.6 去中心化的评价系统

现有互联网的电子商务、新闻网站、广告系统都对用户评价、评分系统有着严重的依赖，甚至已经成为了其商业模式不可分割的一部分，俗称为“水军”的造假行为司空见惯。区块链与小微支付相结合或许将可以很好的解决其中的一部分问题，任何人要发起评论、浏览文章都必须支付一定的费用，这样将抬高造假的成本，将会遏制水军现象。同时也能给内容生产商带来更加便捷、高效的盈利途径。

4.7 清洁能源

痛点：太阳能、风能（陆上、海上）、水电等清洁能源发电成本较低，其很大一块成本是并网输送上。 解决方案：信链独特的PoD算法本质上可以视为将电能转换成了对数据的存储、分享能力，如果清洁能源生产商能够就近将自己生产的电能现场转换成信链币，那就可以节省大量的并网输送成本，而且其不受电网高低峰值的价格波动，可以常年不间断的获取商业利润。

4.8 商业积分或客户忠诚系统

痛点：传统线下或线上商业场景中，VIP卡、积分卡等通常都可以大大提高消费者对商家的忠诚度、活跃度，但是往往不同商家发行的积分卡无法互通，导致对用户的体验非常差。 解决方案：基于区块链的商业积分系统在技术上将更加容易发展成一种通用积分系统，而且区块链技术因为其数据不可篡改、去中心化、自证其信等特点，可以给相应的积分系统增加可信度。

4.9 游戏

痛点：很多游戏里面都有各种游戏币、游戏积分、道具，又或者各种抽奖等活动，这些在中心化的系统里面通常都有造假、无法取信于人的问题。 解决方案：区块链技术能够很好的解决这些问题。

4.10 保险

保险行业通常都会有大量资金沉淀，如果高效、透明的管理这些资金，成为保险行业能否盈利、甚至是能否生存下去的关键问题，区块链技术将为保险行业提供一种更好的工具来解决这些问题。

4.11 企业协同

多个企业或同一企业内的不同部门之间的数据共享将会大大提高企业的整体运营效率，降低成本，例如企业财务数据的协同，协同记账，有可能完全重造整个会计、审计行业的规则，虽然这将会需要比较漫长的过程，但其趋势是不可逆的。

4.12 太空

信链在太空中的的一个很大的应用场景是太阳能的充分利用，因为太空中具有取之不竭的太阳能，可是因为空间站上的电能或太阳能无法远距离传输到地球上，其多余的能源只能是白白浪费，如果能够在空间站上将太阳能不断的转换成信链币，那将会创造无限的财富。

远途太空旅行中需要的各种无人值守的空间站也会需要信链的技术实现经济上的激励，不管对人还是对机器，都会需要一个能够自行运作的无人值守的经济系统，毕竟在茫茫太空中没有人能够及时找到足够的人来维护经济秩序，只有信链技术能够做到自证其信，无需任何第三方的信用。

4.13 供应链管理

痛点:核心企业虽然是供应链中的主角，但其对供应链的掌控能力有限，当其将管理范围向上下游扩展的时候，将导致成本的急剧上升和效率的大幅下降。同时，核心企业的影响能力也有限，遇到势均力敌的供应商时，话语权也不强。

就拿供应商来说，一般优秀的企业最多能管理1-2级供应商，因为随着产业分工的不断细化，供应商的数量呈指数级增长，超过核心企业的管理能力。比如微软surface产品的供应链，一级供应商在5个以内，二级供应商就超过200个，三级供应商则多达数千个。

因此，核心企业一般都将管理下级供应商的工作交给一级供应商去做，这样的模式导致信息不对称且有延迟，核心企业无法实时掌控货物的流通，其中也有做假和被篡改的风险。更有甚者，由于关键技术和渠道被掌握，核心企业可能会受制于一级供应商，想要更换难度很大。

区块链解决方案:区块链能够围绕核心企业搭建一条包括制造商、供应商、分销商、零售商、物流公司、终端用户等在内的联盟链，将资金流、信息流、货物流都记录在链上不可篡改，值得一提的是，货物流上链可以结合物联网技术，简化协同工作。 这样一来，区块链就能够实时记录并共享供应链各环节的最新进展，核心企业得以穿透式地实现对供应链的掌握，及时地了解订单的生产、质量、运输等情况，将供应链透明化可视化。透明化的实时管理能够降低企业的库存成本，给企业应对突发事件的即时支持，也为审计提供了便利。

5 ICO发行规则

5.1 ICO简介

本次ICO的标的物是信链股，信链股的总量为10亿股，此次众筹出让比例占总股份的30%，也就是3亿股，剩余的信链股将在今后几年逐渐售卖出去，没有参与ICO的信链股将处于冻结状态，其对应的权益不会被分配，也不会在市场上进行销售、转让。 此次ICO信链股的分配比例如下：

- 投资人：70% * 3亿 = 2.1亿股，
- 信链团队：20% * 3亿 = 6000万股，
- 前期推广费用：10% * 3亿 = 3000万股。

我们制定的政策策略就是用良好的激励机制让股东持续贡献自己的资源，并能从中获取相应的利益，做到能者多劳，多劳多得。 我们的经济模型中最大的创新就是可以实现随着信链网络有效用户数的增长，自动给股东们进行分红，类似股票市场上的高送转，但是投资人随时可以变现这些分红。

5.2 ICO投资人如何获利

假设某投资人掌握的信链股可兑换的信链币的总数为B，则信链股的市场价值计算公式如下：

```
V = P * B
```

- V代表信链股的市场价值；
- P代表信链币的单价；
- B代表信链币的数量；

从上面的公式可以看出，持有信链股后主要有两种盈利途径：

1. 随着信链币的单价的上涨而获得总价值的上涨；
2. 随着可兑换的信链币的数量多上涨而获得总价值的上涨，也就是随着信链有效用户数的增长而增长；

以上两个因素同时起作用，而且是乘积效应；

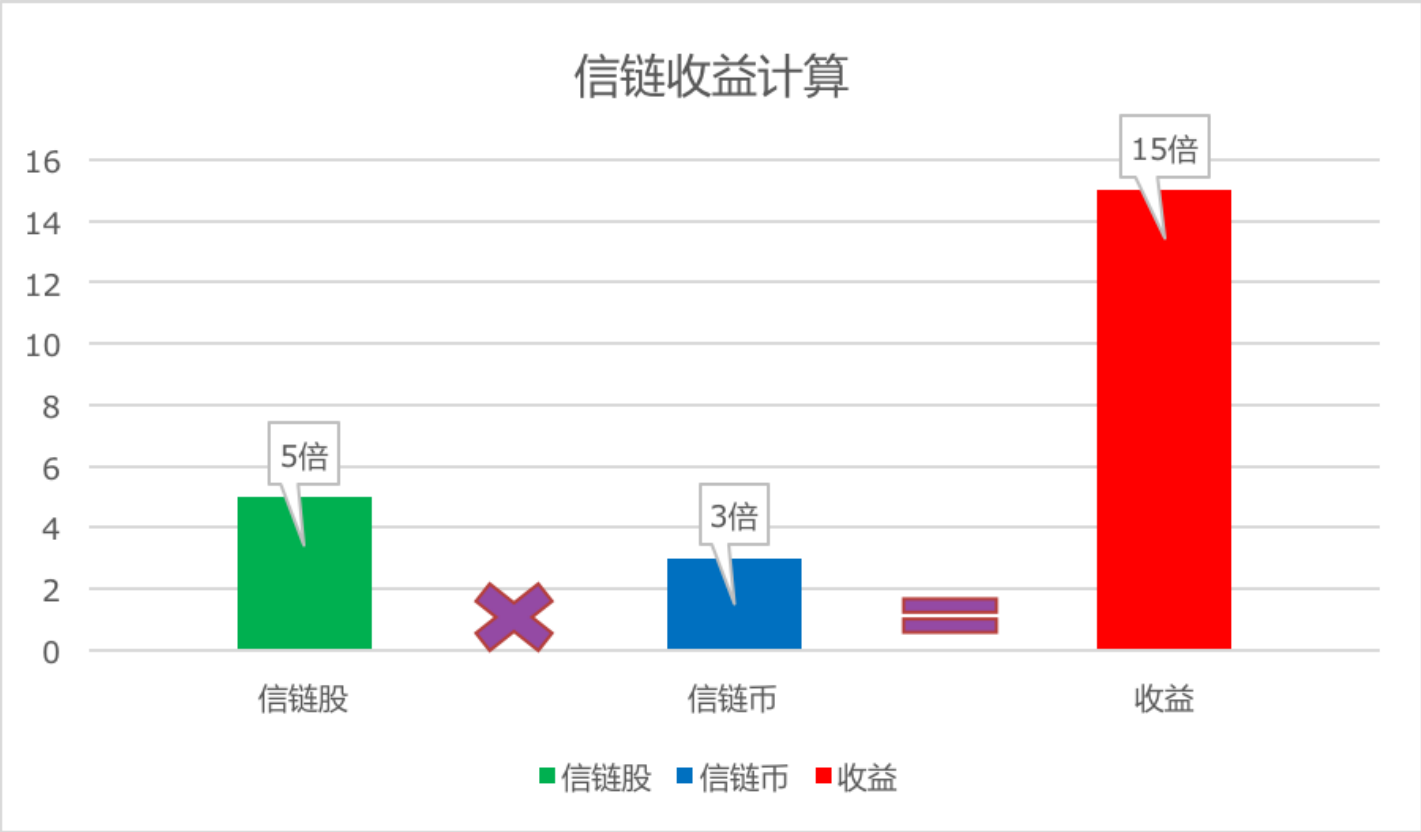

图 18 信链收益计算

5.3 ICO股东额外好处

称为ICO股东并且只有称为股东，才能参与用户拉新激励计划（具体即推荐一个新用户加入信链网络，将获得一定的信链币的激励），该激励计划在早期只会对ICO股东开放，并且在后期会保持对ICO股东的政策倾斜，例如优先成为经销商或代理商等。

只有ICO股东才有可能成为信链基金会的成员，参与到信链网络的管理当中；并且可以通过为信链提供运行所需相关硬件、软件、运维服务，获得固定的信链币的回报。

5.4 ICO投资人收益试算

假设一个投资人最初花费1000元购买一份信链股，最初该信链股可以兑换10000个信链币，每个信链币在公

开市场上可以兑换0.1元人民币，那么此时投资人持有的信链股等值是：

```
1 * 10000 * 0.1 = 1000元人民币。
```

那么当信链网络的有效用户量达到500万的时候，则一股可以兑换20000个信链币了，而此时信链币的价格因为需求的上涨，变成0.2元人民币了，那么此时投资人持有的信链股的价值是：

```
(500/100) * 10000 * 0.2 = 10000元人民，也就是涨了10倍。
```

5.5 锁定期

投资人获得的信链股都会被锁定一年时间不得进行交易，或兑换成相应的信链币，锁定期结束后，按照前面说明的规则将信链股兑换成信链币，然后可以在公开市场上对信链币进行交易流通。