印链白皮书 2.0

重庆印链科技有限公司

2017 年 4 月

目录

正文

一、印链对区块链的理解

随着比特币进入大众视线，区块链技术的魅力也被越来越多的人发现和认可。其突出的去中心化、去信任化和数据不可篡改特性，将会颠覆许多传统行业，目前区块链技术处于初级阶段，其应用范围还十分狭窄，印链致力于打破这种局面。

区块链的本质是一个一致的分布式数据账簿，印链在项目开发过程中，对区块链技术有了更深层次的理解。结合 p2p 技术和共识机制，基于印链公有链的应用开发，就像在传统数据库上面开发一样简单，结果就是印链能为各种应用尤其是商业应用提供底层协议支持。印链的技术和业务，将会为区块链行业带来突破性的发展。

二、什么是印链？

印链是由重庆印链科技有限公司发起，并主导开发的一个定位于区块链商业应用底层平台的公有链项目，印链的初衷是利用区块链技术打击假冒产品，为品牌商家提供最具公信力的技术以保护商家的品牌形象。印链项目于 2016 年 12 月正式启动，截至 2017 年 4 月，印链已完成区块链底层设计和开发，完成通用的防伪溯源业务流程，基于印链公链的第一个应用防伪溯源应用平台也已发布公测，所有人均可体验！

三、印链为什么更适合发展商业应用？

区块链人才短缺，底层技术门槛高，多数应用需要建立在某一个已经搭建好的底层平台上，印链为这些应用提供了另一个选择。

比特币和以太坊、lisk 等平台没有考虑实际的通用商用场景的需求，商家需求契合底层困难，应用与商家产生业务逻辑同样困难。还有很重要的一点，不符合商业监管的需求。

印链是第一个专业的商用区块链应用生态平台，从底层架构身份认证管理分级系统，签订双私钥的多重签名注册绑定管理。这一系统结合管理中介和印链拟订开发的高级仲裁系统一起，满足去中心网络的去中心监管和政府准入性商业级监管要求。

四、印链的创新之举

(一)　共识创新

印链由已注册的重庆印链科技有限公司创造，独创了创新的 POC-Proof of Credit 信用共识机制（后文有详细介绍，在此不赘述）。

(二)　账户系统创新

为适合商用，印链在底层接入了独家认证分级管理体系，为不同的角色配备不同的权限和功能，使商家和其他角色账户可以自然的形成模式组合，实现多种商业模式。

(三)　系统代币信用双价值中介

除了代币 INS 印股，节点还可以在共识中积累和获得另一个数据流：信用值。印链首次创造性的把信用值作为管理中介引入区块链，构成印链的双中介机制。

(四)　交易模型创新

不同于其他区块链项目只有转账、双重签名等简单交易类型，印链创造性的在底层的基础上嵌入了很多交易模型，这些模型自助完成更复杂的商业活动。如：验证返币交易模型，悬赏合约模型，信用保证金模型以及拍卖竞价模型等。

(五)　模式创新

印链将采用全局资产白名单和应用白名单支持架构，使发行资产可以在协议合约、应用、底层网络多个层面管理和监管资产。从而实现了类似现实企业资产的发行、破产清算、应用上线，资产安全等全面功能。

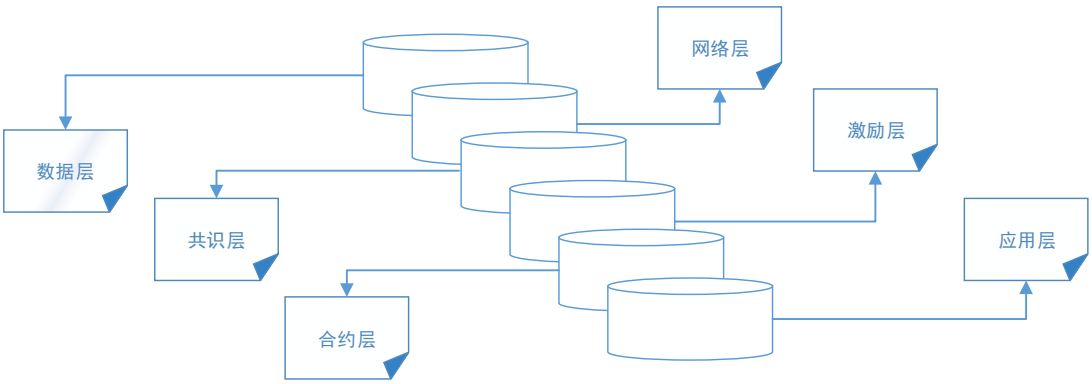
(六)　技术整合创新

印链努力将区块链与本行业及其他行业先进技术进行整合，例如与重庆科技学院合作使用微小二维码技术。会陆续添加虚拟机，高级智能合约，高级仲裁，隔离验证等新技术。

五、印链的技术架构

印链包括了数据层、网络层、共识层、激励层、合约层、应用层共六层基础

模型。



(一) 数据层

印链的区块数据采用链式结构进行存储，所有区块都带有上一区块的指针引用，保证数据不被篡改。印链采用 sha256 函数对数据进行哈希散列，采用 ecc 非对称加密算法进行身份认证，采用 aes 加密算法加密私钥，采用 Merkle 数验证和存储交易。

(二) 网络层

印链的节点交互用的是 nio socket，用 dns 方法和程序内置方式加载种子节点。所有节点启动后会进行自检，处于公网下的节点会主动上报自己的 ip 和端口到网络中，其它节点会对其上报的信息进行验证，如果验证通过，所有节点会将可用节点的 ip 地址和端口存储到本地，下次启动会直接连接无需再次探测；若验证多次不通过（会有一个规则，每 10 分钟探测一次，当失败次数超过曾经成功连接次数的 10 时，会触发），该节点可能已经下线，将从存储队列里面删除。当连接节点数量过少时，会主动向已连接节点询问获取更多可用节点。

印链通过打洞穿透的方式，让处于内网的节点间能进行互联互通，利用已验

证通过的节点作为连接桥梁，帮助处于 nat 背后的节点握手并完成连接。

(三)　共识层

印链没有采用现有的共识机制，是因为印链的商业定位，会成为用户流量和 tps 最大的公有链，同时在商业环境中找到一个价值纽带，poc 就此而生。这也算是印链的一种”硬创新”，在兼顾性能的同时，兼顾维护效率，下面会有 poc 详细的介绍。

(四)　激励层

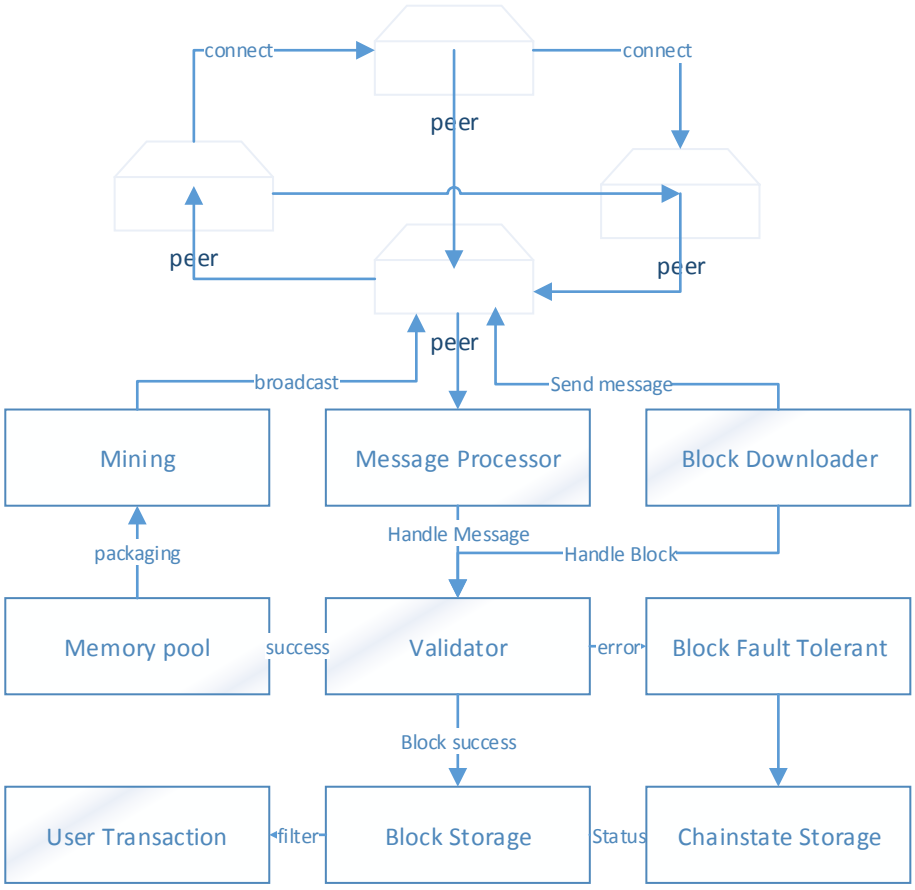
印链的代币有 10%用于共识奖励，因为印链独特的共识机制，性能不受节点数量的影响，所以印链的共识节点没有设置上限，并且是动态变化的，任何人都可以随时加入赚取奖励。

(五)　合约层

目前印链的合约层仅是简单的脚本代码，防伪码的验证脚本、共识保证金的赎回脚本，都是一个个小小的智能合约。印链的定位是商业应用平台，故印链会采取与其它智能合约平台不同的方式进行公有链生态整合和促进成型。印链会招募第三方团队基于印链打造更多接地气、具有实用性的落地应用项目，前端的受众人群将会是普通大众，进而为印链积累沉淀大批用户。印链计划于 2018 年开发图灵完备的虚拟机，以提供更高的灵活性，前提是印链有一定庞大的用户基数之后，在这之前印链的目标和方向非常明确。

(六)　应用层

印链前期会在底层提供通用的应用协议，以开发不同的落地项目，尽快让区块链普惠大众。目前已开发完成通用的防伪溯源协议，实际上这套业务协议的适用范围远远不止防伪溯源，后面有详细的介绍。



印链框架图

六、信用体系

(一)　什么是信用体系?

印链的信用体系是系统对参与系统者的反馈过程。因为印链团队认为，获得系统嘉许的不该是既得利益者的不劳而获（pos），也不该是弱肉强食的强者恒

强（pow）,系统的朋友是活跃于系统，真心为系统贡献的劳动人民。因此,印链引入信用体系，实现这一理念。

(二)　印链为什么需要信用体系?

这里只分析一个最重要的原因，印链是一个商用的区块链底层平台。既然商用，节点的行为类型会比以往的其他区块链公链多很多。因此，需要用有效的办法规范节点的行为，形成稳定的秩序，适合商用的同时可以避免链上的权限被人滥用，造成垃圾数据膨胀。

印链的代币需要流通，因此不适合作为规范节点行为的中介。因此印链提出代币与信用的双中介体系。顺应印链的商业落地和用户流量路线，设计信用体系作为规范用户行为的一种管理和价值纽带。

(三)　印链的信用体系

基于区块链的信用体系，有可能会掀起大的浪潮。印链的信用体系结合商业性质，已有初级雏形。信用作为规范用户端行为的准则，不能变现和流通，是用户良好行为习惯的一种体现。

信用的用途包括但不限于参与共识、转账手续费打折、修改别名、转让商品、申请高级仲裁、参与商家有针对性的活动等等。印链目前已实现利用信用参与共识、共识违规信用处罚、修改别名消耗信用、转让二手商品消耗信用。信用作为整个系统的价值中介之一，会陆续利用其纽带作用开发更多用户行为准则。

信用的获得：信用作为和代币平行的价值中介，其获得不需要实际利益上的代价，仅仅是遵守系统规则，保持良好的用户习惯，即可获得。目前已实现的信

用获得方式是用户 24 小时内转账，后期会加入更多合理的信用获取来源方式。

七、POC 共识机制

任何区块链项目，都需要共识机制使分布在全球各地的对等节点、对数据的状态达成一致性。印链旨在开发一套高效、可自我维护的共识系统以适应印链的商业定位，POC 共识由此而生。

POC 的全称 Proof of Credit，中文名信用共识机制，简称 POC。

印链的 POC 共识机制解决了 POW 的性能问题，解决了 POS 的权益不均问题，解决了 DPOS 的违规处理效率问题。

那么 POC 到底是什么样的呢？

POC 是基于印链信用体系基础上，使用信用准入，利用现有区块链账簿唯一性和确定性，协调各节点进行单点广播权限确定和可验证的系统。

(一) 共识准入

作为一条公链，共识节点涵盖了用户端，必须规范用户行为，才能使整个网络按照协议稳定安全的运行。POW 利用算力竞争规范节点，POS 利用持有代币数量和币龄规范节点行为，DPOS 利用投票选举受托人，这几种目前流行的共识，原理上除了 POW（其实 pow 的难度调节也是利用的已有账簿）之外都是利用账簿的确定性进而选出具有单点广播权限的节点。所以只要根据链上账簿数据确定性，进行共识集合顺序出块即可。

印链的共识门槛是信用达到一定值，即可参与。这种准入方式有一定的难度需要时间累积信用，作为开源公链，攻击者很有可能利用很长的时间做准备，发起一次对网络共识的攻击。

所以印链引入经济制裁机制杜绝这种情况的出现，因为攻击者发起攻击获得的收益并不会比损失大，这就是在信用准入的基础上增加保证金机制作为辅助。

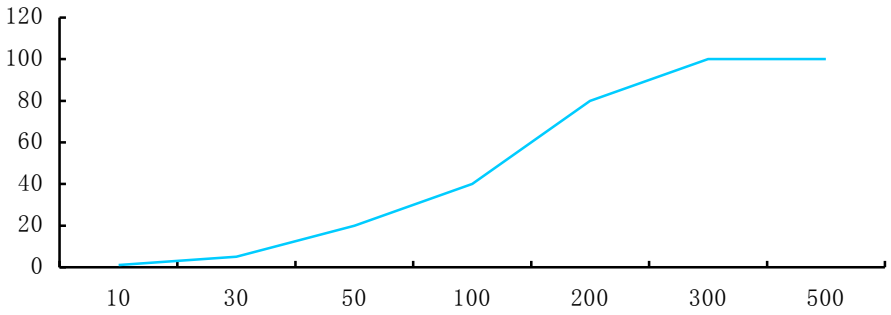
有人说：直接提交保证金不就行了，信用准入是多余的！原因是共识的情况极其复杂，有的情况是不适于经济制裁的，比如共识节点电脑死机，网络掉线，若没有信用准入，那么系统无法甄别并排除这类节点，若统一采用经济制裁的方式，势必将大批用户拒之门外。另外，信用保证系统的权力不被大量持币者垄断。信用作为底层的价值中介之一，日后会有更加广阔和重要的用途。

(二) 浮动保证金机制

因为印链的共识无需节点之间频繁来回的通讯即可达成共识（下面有介绍），所以印链的性能是不受共识节点多少影响的，100 个节点和 1000 个节点的性能几乎一样。故印链采用创新的浮动保证金机制来平衡共识节点的收益。

印链网络通过当前共识节点数和一个线性增长算法，来动态计算当前参与共识所需保证金。

```
recognizance = maxRecognizance * ((Math.log(size/Math.log(2)) * size) / Math.log(maxSize/Math.log(2))
```



从上面的保证金计算公式可以看出，参与共识所需保证金，随着共识节点数量的增加成线性增长，当共识节点数量达到最大数量时，保证金也达到最大值。

(三)　全网效验

任何节点的共识申请和退出，都会被全网进行严格的效验。

1. 信用的效验

当任何节点申请成为共识节点时，其它节点都会首先验证该节点的信用值，若发现信用值低于准入门槛，那么该节点的该次请求会被丢弃。

2. 保证金的效验

任何申请共识的请求，都必须提交相对应的保证金。和转账的不同之处在于，提交的保证金接收方是一个智能合约脚本，该脚本对保证金的赎回进行了强制的规范。全网不止会对申请共识请求的信用和保证金做效验，还会对赎回智能合约脚本做效验，对保证金的安全作了最高级别的定义。

3. 保证金的赎回效验

印链的共识协议有经济制裁制度，故节点提交的保证金，并没有采用传统冻结的方式；系统运行过程中，一旦发现有严重违规的节点，任何诚信节点可罚没该违规节点的保证金。节点的保证金实际上提交到了一个智能合约脚本，处于无

主状态，为保证这部分资金的安全，任何退出共识或者处罚请求，都会被严格的效验，效验规则里面包含了严格的效验协议，任何人想领走别人的保证金，那是不可能的事，任何人想罚随意没别人的保证金，那也是不可能的事。

4. 制裁效验

印链的每一个区块头部，都有出块人的签名，所以当有人试图作恶，必然会留下密码学证据，以便追责。

当共识节点超时出块，或者由于死机掉线等非人为因素不能出块时，全网能监控感知，并在第一时间将该节点降级为普通节点。这种情况虽然没有密码学证据，但依然需要提供全网其它节点能对其效验的证据。

任何节点要对其它节点实行制裁，必须提供合理的或者带有密码学的证据，这样才会被全网其它节点效验并接受。

(四) 确定单点广播权限

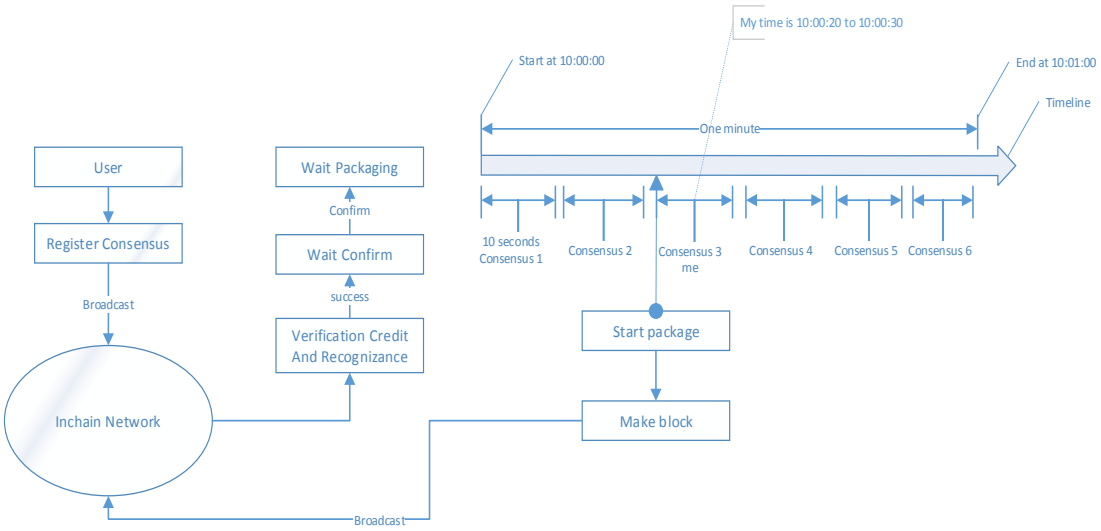
结合前面几小节提到的理论知识，本小节将提供更全面的 POC 运行原理和细节。

先做几个名词解释：

- **共识节点**：达到信用准入门槛并成功申请共识的节点
- **共识轮次**：所有共识节点轮流出块的完整时间段，称为一个共识轮次。每个共识轮次都有开始时间戳和结束时间戳，上一轮次的结束时间为当前轮次的开始时间，所以节点必须按照这个时间规则进行下去，否则任何的改动都会被全网排斥。在每个共识轮次中，所有共识节点有且只有一次广播区块的权力。

- **共识顺序**：在一个共识轮次中，每个共识节点出块的顺序，叫做共识顺序。在印链的共识中，每轮的顺序都是随机变化的，根据当前轮次的开始时间戳（也就是上一轮的结束时间戳）与共识节点账户、通过算法排序决定。所有节点（包含非共识节点）必须遵守这个规则，才能正常运行，任何哪怕是细微的改动，都会导致改动的节点被全网排斥。
- **共识时段**：在确定了共识顺序之后，每个节点都被映射到一个时间段上面，这样自然就确定了单点广播权限，这个时间段也有开始时间和结束时间，间隔是区块出块时间，称为共识时段。
- **区块权限验证**：每个区块头部，都有当前轮次的开始时间、共识节点的时段信息、共识节点的签名，通过这些信息对区块的合法性进行验证。

POC 完整的运行流程：



1. 申请共识
2. 效验信用和保证金
3. 申请包含进区块，被确认
4. 等待当前共识轮次结束

5. 当前共识轮次结束，下一轮共识开始，下一轮变当前轮

6. 确定当前轮次共识人数

7. 初始化当前轮次共识顺序，各自节点计算出自己的共识时段

8. 接收新块，并进行区块权限验证和容错监控，等待自己共识时段的到来

9. 到了自己的共识时段开始时间，开始打包区块

10. 打包程序从内存池中获取新交易并验证

11. 预估到了自己的共识时段结束时间，停止打包

12. 询问容错监控器是否有违规需要处理，发放信用

13. 验证区块交易数据

14. 广播区块到全网

15. 继续接收新块，并进行区块权限验证和容错监控，等待下一轮开始

(五) 容错监控与处罚机制

区块链系统是非常复杂的系统，不单因为底层技术的复杂，更因为其运行的环境极其复杂，尤其是公有链。使用习惯、网络环境、人为破坏等都有可能影响系统的正常运转。区块链的共识机制，能有效的解决这些因素带来的影响。

对于印链的 POC 共识机制来说，节点的任何动作，都会被全网其它节点监督。印链创新的共识会对以下这些情况做出相应的处罚，整个系统会自身调节、维护稳定。

1. 不出块，扣除一定的信用值，并降级为普通节点。

2. 不按时出块或者网络同步延迟等非人为因素，会根据全网其它节点的选择作决定，若下一区块引用了这个块，那么正常相安无事；若下一区块丢弃了该

块，那这个块将会成为孤块，其面临的结果是信用处罚并降级为普通节点。

3. 非共识节点胡乱广播区块，验证不通过，直接丢弃。
4. 同一时间段广播多个块，属于严重违规类型，会被没收保证金并信用拉黑。
5. 打包双花交易，属于严重违规类型，会被没收保证金并信用拉黑。
6. 从链上的旧块处尝试分叉系统，所谓的双花攻击，属于严重违规类型，会被没收保证金并信用拉黑。

4、5、6 这三类严重违规类型，全网可监控，并有密码学证据，任何诚信节点只需提交包含其签名的一个或多个区块头信息即可行驶处罚权力 ,没收该节点的保证金到社区基金账户，并扣除该节点 999999 点的信用值，被处罚的节点永久无法再次作恶。

(六) POC 共识机制的优势及不足之处

优势：

1. 节能：不过多占用系统 CPU 和内存资源。
2. 高效：节点之间无需额外的网络通讯即可达成共识。
3. 稳定：系统能自身调节运行状态，高效自维护。
4. 安全：超过 50%的容错率。
5. 创新：第一次引入双价值中介机制（信用与代币）。

不足之处：

和所有公有链一样，允许分叉，可能需要检查点。但 POC 是短期分叉，容错检测器一般会在 2 个块左右的时间内解决。

(七)　POC 总结

POC 的最大亮点是及时的处理作恶情况，系统自身高效的维护，虽然在技术实现上的难度非常大，但是印链团队做到了。

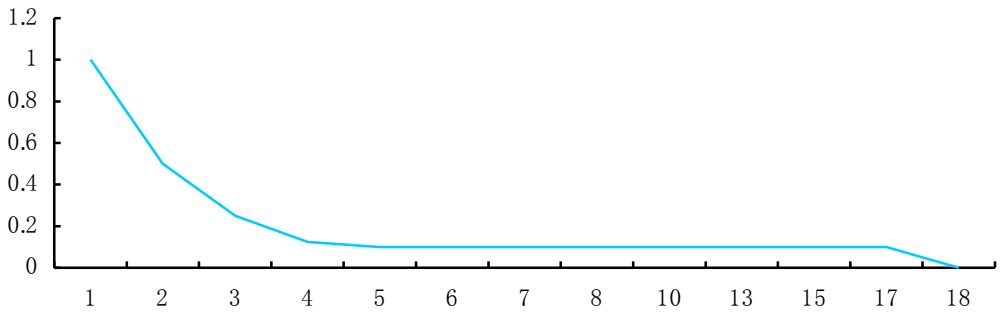
团队已有持续优化完善的方案，使 POC 不断完善以满足持续增长的商业需求。

1. 节点之间通讯，引入先进的压缩技术。
2. 优化新区块同步到全网的流程。
3. 实现隔离见证技术，减少新区块广播大小。

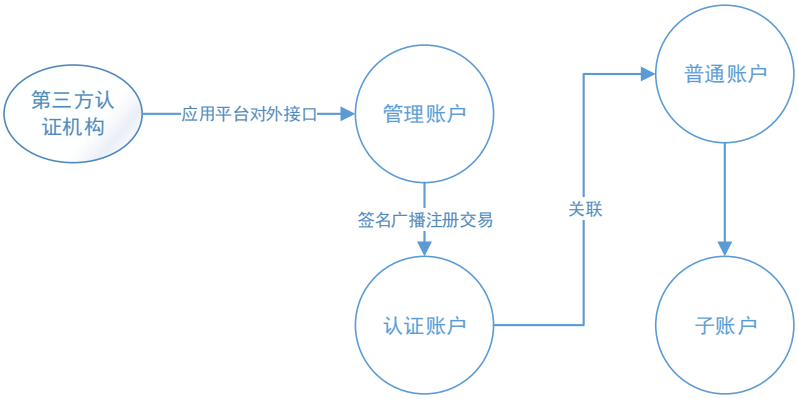
通过以上 3 点优化改进，能大大提高整个网络的 TPS。

八、激励机制

和其它公有链一样，印链对共识节点有奖励政策。奖励部分是总量的 10%，通过新块的 coinbase 交易逐步分发。印链的区块出块间隔时间是 10 秒，第一年每个块产出 1INS，以后每年减半，直到达到每个块 0.1INS，以后保持这个值。印链的共识奖励部分，大概 17 年分发完，后面会逐步强制要求商家建立节点维护网络。



九、账户分级认证系统



印链系统账户分为管理员账户、认证账户、普通账户、子账户。

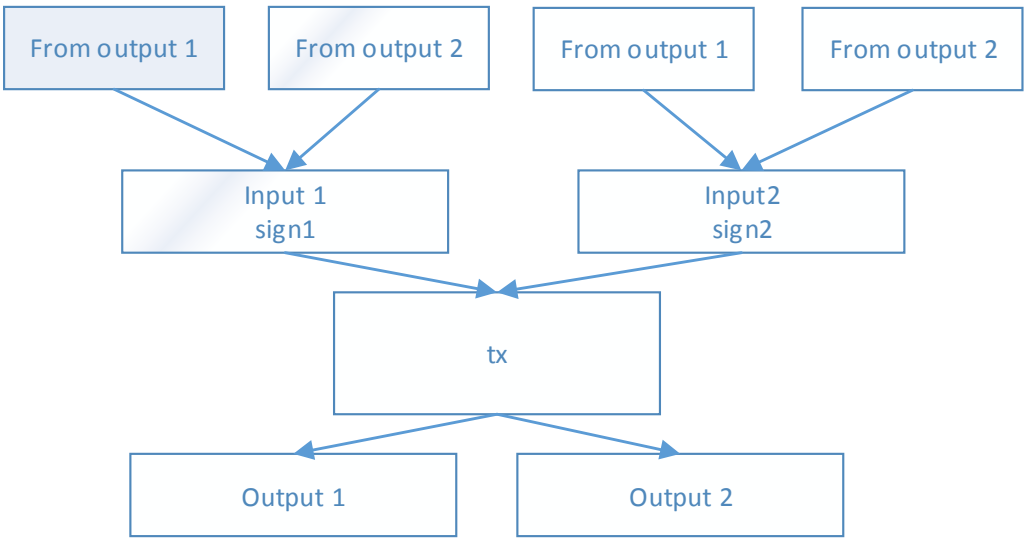
管理员账户：仅仅是多一个注册商家的权限，其它方面和认证账户没有区别。

认证账户：无规矩不成方圆，印链前期会充当商家接入审查者角色，后面适当的时候，与第三方专业认证机构合作，把这部分权限通过接口的方式移交出去。所有认证账户，必须由管理员账户签名之后，才会被印链网络接受。

普通账户：印链的广大用户群体，所使用的账户。包括印链客户端的基本功能、验证商品、转让商品等功能。

子账户：认证账户可关联普通账户为其子账户，关联之后子账户可为认证账户生产的商品添加溯源流转信息。

十、改进的 UTXO 交易模型

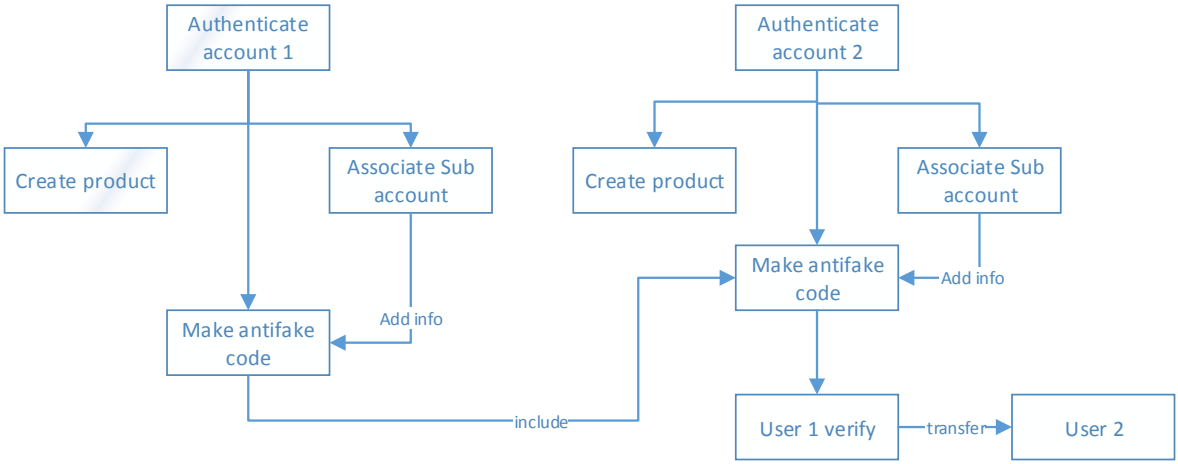


印链的交易模型，大部分采用的是 UTXO 模型。结合印链的账户系统，改进了 UTXO 模型以提高效率和减少交易大小。

改进详情：合并同一账户的多个交易输入引用，采用一个签名。

十一、专为商业应用而设计的通用底层协议

印链的底层为商业应用而设计，目前已完成的一套应用协议，能适应众多业务场景。



1. 认证账户资料和商品资料的灵活性，使用通用的 key value，能录入任何形式的资料信息。
2. 认证账户创建商品。
3. 认证账户生成指定商品的全网唯一身份 ID（在系统里面叫做防伪码）。
4. 认证账户关联子账户。
5. 认证账户关联的子账户对商品唯一 ID 关联流转信息（流转溯源信息）。
6. 认证账户在生成商品唯一身份 ID 时，能引用其他商品的全网唯一身份 ID。（形成来源溯源）。
7. 普通账户对商品唯一 ID 的验证。
8. 普通账户对商品验证后的归属权进行转让。

以上业务流程协议，在印链客户端（钱包）里面已实现，并通过 PRC 的方式，对所有第三方开放。

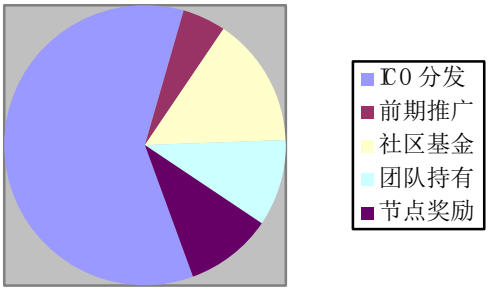
目前印链团队已开发出基于印链网络的第一个应用 – 防伪溯源应用平台的核心功能。

印链的这套底层应用协议，适用的范围远远不止商品的防伪溯源，基于这套协议，能开发诸如《基于区块链的中小企业员工打卡系统》、《基于区块链的快递内部管理系统》等等。

十二、印链的商业应用及落地规划

印链的商业应用及落地规划，请参考《印链白皮书第二版--商业应用》。

十三、印链的代币参数与分配



印链具有自己的系统代币：印股（INS），总量 1 亿。

ICO 分发：60%；

前期推广：5%；

社区基金：15%；

节点奖励：10%；

团队：10%；

说明：前期推广部分若有剩余，则转入社区基金（假设剩余 1%，则社区基金为 16%），由社区掌管，管理办法见《印链社区白皮书》；

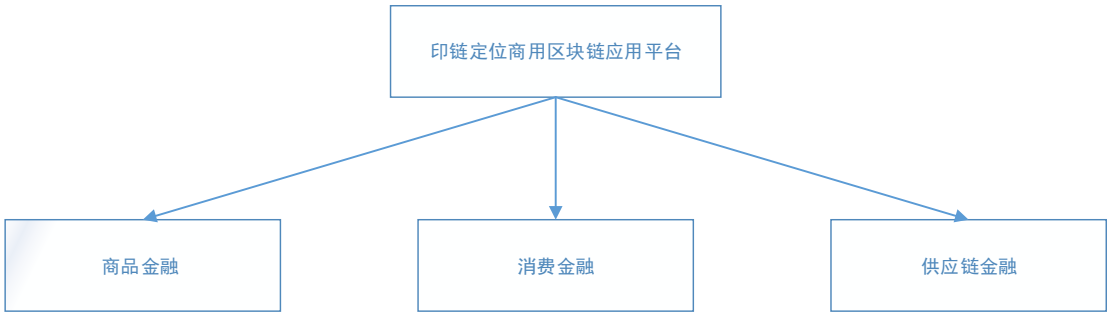
团队持有部分正式上线时技术锁定两年；

节点奖励分发，具体见《节点奖励细则》。

十四、印链的发展路线图


2016年11月
发布印链白皮书1.0版
官网架设
2016年12月
启动资金ICO
5.8%代币
2017年1月
注册重庆印链科技有限公司
与重庆工艺美术协会达成战略合作
2017年2月
印链微信小程序
印链商家工具
2017年3月
底层完成、钱包内测
多家企业合作
重庆科技学院战略合作
多家风投机构来访
2017年4月
印链白皮书2.0、印链官网改版
艺术品应用宣讲
钱包公测、防伪溯源应用测试
推广宣传、联系平台
2017年5月
正式ICO
扩建技术与市场团队
2017年6月
1、扩充团队、成立重庆区块链技术研发中心，进行区块链底层研发
2、成立印链商业联盟，招募第三方团队开发应用
3、筹建重庆区块链协会及相关事项
4、防伪溯源平台继续开发完善
5、钱包全面测试。
2017年7月
1、社区1.0网站，社区基金、社区建立运作。
2、确认印股交易平台
3、试运营印链防伪溯源平台
4、招商加盟、各方合作
5,、建立政府合作公关小组，需求政府合作
6、组建国际化宣传小组、为印链国际化铺路
7、深化防伪溯源应用
8、钱包深化测试，准备主网正式上线
2017年8月
1、印链主网上线
2、印股上线国内交易平台
3、建立上海分公司，宣传推广，市场全面化。
4、为加盟商家提供商品金融服务
5、开发手机APP、轻钱包、区块浏览器。
6、深化微信小程序，充分结合印股，让大众认识并使用虚拟加密货币。
2017年10月
加速防伪应用市场拓展
研发印链艺术通应用
研发为印链提供资源服务的联盟链（由于商业机密、暂时保密更多细节）
2017年12月
进一步扩大市场，增加商家和用户
上线各大交易平台
研发印链资产通应用
启动A轮融资计划
2018年
1、继续开拓防伪、溯源、艺术、商品金融市场。
2、配合第三方团队开发物联通，知识通等应用及运营。
3、推动印股的投融资和第三方应用合作及 企业联盟、政府合作等工作。
4、进入区块链金融市场。
5、底层技术的持续完善；研发高级众筹系统底层协议等。
6、适当时机研发高级智能合约，虚拟机。
7、技术储备和创新持续进行。

十五、印链的终极目标



印链的目标是三年内代币市值最少达到 30 亿。

三年内上线 10 个以上落地应用、累积百万级别用户、上千家商家。

四年内防伪溯源应用盈利。

七年后公司上市。

总结

大环境：

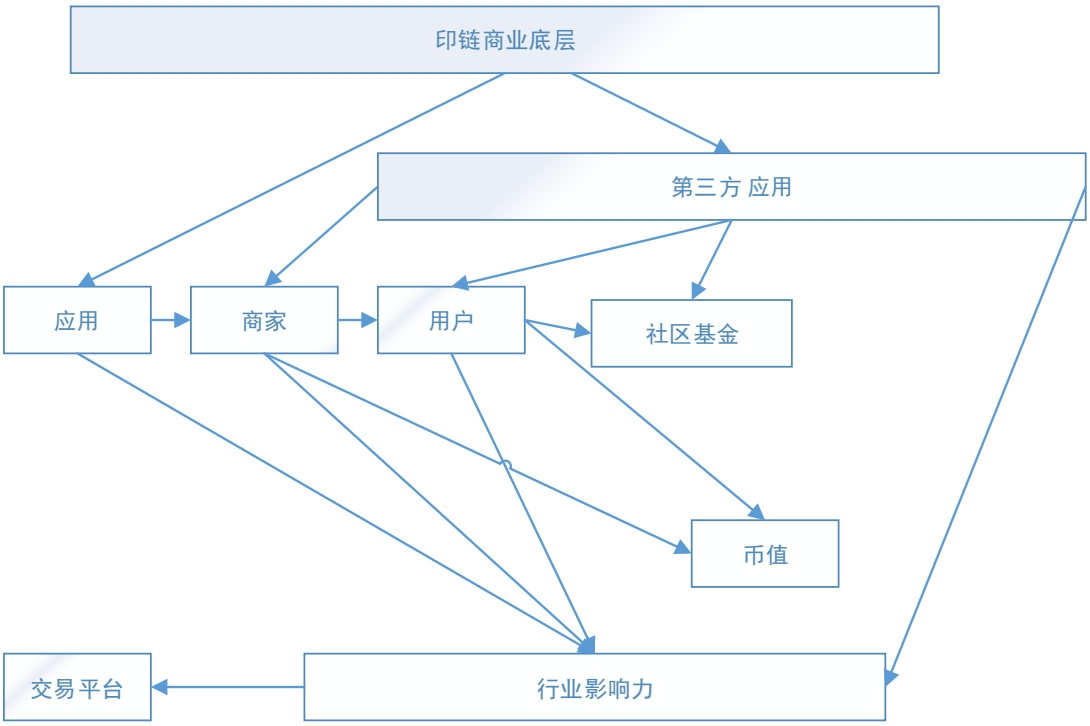
区块链风口，公益性质，国际扶持，中国市场，互联网经济深入人心，企业转型压力大。

团队：

正规，自律，诚信，认真，踏实，目光长远，战略清晰，发展有序。技术实力强，理念先进。

方向：

生态系统建设



生态系统图

印链具有清晰的行业认识，完整的战略计划，高效的执行团队，开放的发展态度。欢迎各行各业商家加盟，有识之士共建生态大业。