《信链白皮书》V0.1.0

谭飞阳
2020

信链，通过区块链技术，为个人、企业与组织提供低廉的信息记录服务，从而达到公证、宣告等作用。

信链生态同时为所有使用者提供免费、方便的信息验证服务，从而达到验证、查询等作用。

注：黄色信息为未定，红色信息为未解决问题，绿色信息为以解决问题。红的与绿色信息都为笔者的自问自答，读者可以选择忽略，不影响了解信链的机制。

背景：

2009 年中本聪发布了比特币，并开设了区块链纪元的起点，同时为世界打开了去中心化系统可行的潘多拉之盒。在随后时间里更多人继承了去中心化的理念，并伴随着以太坊，EOS，超级账本等项目接连出现，整个区块链技术正快速地向着更大众化、更多元和更强大的良性方向发展。在此也致敬所有参与到区块链技术发展中的技术人员、支持者与使用者。

区块链最本质之一的特征就是就是其不可篡改性，这为未来的价值网络铺垫了非常重要基础。但是直至今日，由于多方面的因素，在许多情况下判断信息的真伪依然是低效的、困难的、甚至是不可行的。而信链将能很好的解决这一问题。

现阶段区块链技术在很多方面应用落地依然面临不少障碍，其中之一就是使用区块链的门槛与成本较高。随着区块链技术飞快发展，现阶段无论是开发一套公链还是建造一套企业级联盟链的难度都远低于从前。但即使如此，对于绝大多数的个人与企业而言，区块链技术依然代表着需要投入大量的人力、时间、与金钱。

信链将降低所有需求方对区块链技术的使用门槛，并实现一个区块链能有效解决，并且大量被需求的问题：信息验证。

信链简介：

信链通过区块链技术，为个人、企业与组织提供低廉的信息记录服务，从而达到公证、宣告等作用。信链生态也同时为所有使用者提供免费、方便的信息验证服务，从而达到验证、查询等作用。

信链具备理论上无上限的 TPS 的超高性能，并且具有非常好的可扩展性。

信链社区将作为信链某种形式上的中心存在，但更多的仅仅是表现为一个形式中心，只是为了更高效的解决链以外的问题，且不拥有改变信链的能力。

信币是一种与其他信息一起且默认记录在信链上的一本特殊账本，信币的作用为支付信链上信息的记录。

信链具有两种不同的信息记录方式。一种为不可撤销，一种为可撤销。撤销的机制，主要是用于服务有需要撤销或者跟新的信息，如产权证明等。

信链上的信息将以年作为单位进行储存。用户可以通过选择支付信币的数量来调整信息需要被记录的时间长度。

花费的信币 60%将支付给包装该区块的矿工，20%将支付于参与验证的节点，20%将作为社区运营的费用。

验证者怎么参与？怎么判定、证明是否参与了？怎么支付？

信链实现：

1. 挖矿：

为减少无意义的算力竞争，并最大化 TPS，信链采用 DPOS 作为共识机制。

怎么在 DPOS 机制下，保证节点的设备保持具有一定的竞争关系，从而保证节点的硬件设备标准足够高？对 DPOS 的机制做一定的修改

对所有节点进行评分：

资产*ln（资产保持时间）

全网前 20 的节点将作为超级节点，并具有挖矿的权利。所有超级节点将通过其评分的大小占总评分的比例分配出一段中标哈希值范围用于公平选择挖矿节点。如：

20 个节点，评分分别为：1，2，3……，19，20。总评分 210 分

则：

节点一的中镖哈希范围为：0x00000000000000000000000000000000 ~ 0xffffffffffffffffffffffffffffffff*1/210

节点二的中镖哈希范围为：0xffffffffffffffffffffffffffffffff*1/210 ~ 0xffffffffffffffffffffffffffffffff*3/210

以此类推

每轮区块确认之后，中心节点将对此区块的哈希值，进行签名，签名的哈希取值范围将决定下一个挖矿预选超级节点。

区块出现分叉怎么办？：分叉主要由于网络的不稳定性与恶意节点的恶意操作造成。在信链中的恶意操作动机的可能性：1.增加自己挖矿的概率，获得手续费用。2.针对某节点的运行。3.其他恶意。分叉的情况不可避免会发生。信链将采用一种链的优先级别机制，及若某节点发现网络中存在其他节点的出现则用某种规则对两条链的优先级。选择优先级高的区块；优先级机制怎么设计？

中心节点断开链接怎么办？：备用中心节点，与中心节点同时广播；若中心节点恶意不向中签节点广播结果怎么把？其他节点收到信息之后再次互相广播（广播因含有签名内容无法造假）；若中心节点恶意不接收中签节点的回应信息怎么办？中标节点全网广播，互相再次广播；若由于中签节点恶意或者非恶意，不接收广播怎么办？若全网未收到回应，选择另一个节点；怎么公平选择另一节点？

挖矿的结果，将被全网公布，节点自动收录合法的新区块。

收到多份合法区块广播怎么办？：合法的区块广播需要被当前指定挖矿节点（已确认）的私钥进行签名，所以若收到多份合法广播，则代表挖矿节点私钥丢失，或者挖矿节点发布了两次广播。每次挖矿节点只能发布一次广播。若出现两次广播怎么处理？

2. 区块：

信链中，区块每 30 秒产生一次（考虑各种网络协议的耗时，尽量短一点）。区块信息被分割为区块信息与区块附加信息，区块信息主要保存了一个“文件夹哈希”的信息，区块附加信息则为每一份该区块保存的文件哈希。

每个区块大小最大 37KB。

区块头（32B）：　　前哈希值（16B），哈希值（16B）

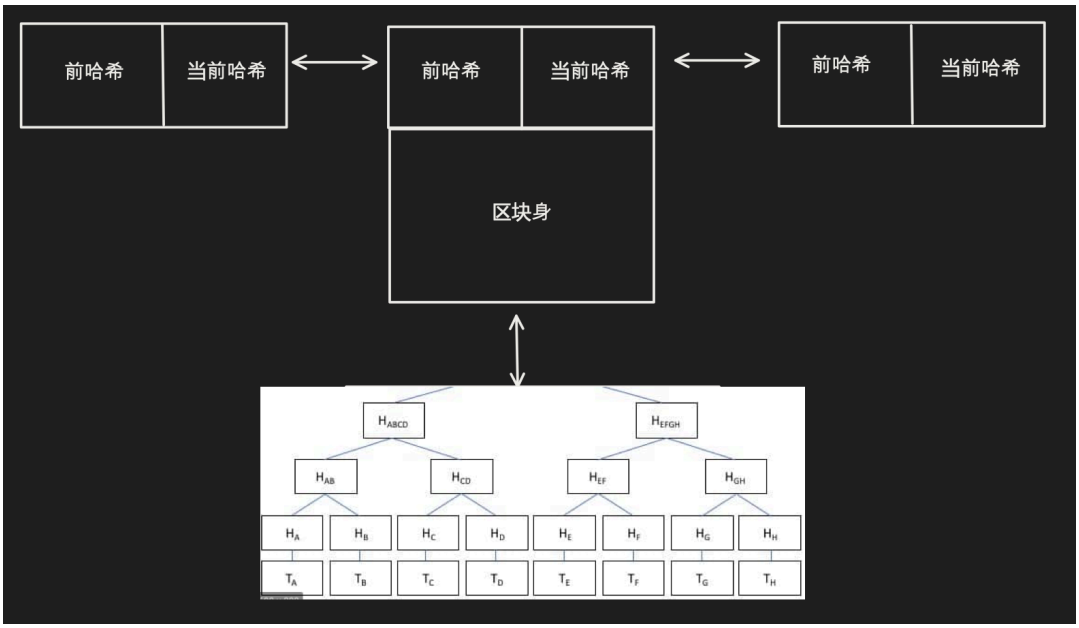
区块身（56B）：　　版本（2B），高度（6B），矿工公钥（32B），文件夹 Merkle Tree 的头部哈希（16B）

区块链仅保留文件夹 Merkle Tree 的头部哈希，文件夹中的内容自身与 Merkel Tree 其他哈希值将保留在区块链之外。文件夹信息

文件（72B）：　　操作序列（1B），操作者公钥（32B），文件哈希（16B），操作者签名（16B），保留（7B）

每个区块链对应的文件夹包含的文件数量为一个可调节的数，根据当前网络繁忙程度决定。

怎么保证挖矿节点不会为了等待更多交易，导致区块生成延迟的风险？



区块链对应的文件夹数量信息：

文件数量	512（2^9）	4096（2^12）	32768（2^15）	524288（2^19）
Merkel Tree 所需哈希	510	4094	32766	524286
总大小	45KB	0.361MB	2.75M	44M
TPS	17+	130+	1000+	17000+

3. 链：

信链信息储存都以年为单位（525600 个区块），每次添加新区块前，都将删除之前第 525600 个区块，并重新打包自动续费的区块。

不断的更新区块能保证过滤掉链中失去意义的信息，使整条链每一个数据都有必要的意义。

信链依然使用前后区块哈希相连的方式成链，其安全性主要来源于挖矿节点签名的不可伪造性，与一定量的工作量证明。

4. 修改后的 DPOS：

为了保证各个节点有一定提升节点硬件的动力，也同时能为修改链增加一定的工作量带来的难度。

每次挖矿节点挖矿，都将通过尝试排列顺序不同的排列方式，最终发布 Merkel tree 头节点必须小于某一个范围才能成为合法区块。该范围将通过某种方式进行调节。

是否真有必要？怎么调节？

5. 世界状态：

信链的世界状态将记录所有文件哈希与该哈希的指引，被取消的文件与它的两个索引也将保存在世界状态，方便某些查询。

信链的世界状态也将记录当前账户资产信息文件，文件贮备了所有拥有币的账号的公钥与余额，该文件的信息将默认存在信链每个区块的 1 号文件里。

6. 信币：

信币将以一种不同于其他数字货币的方式进行储存。所有账号与该账号余额信息将以某种格式记录在一个文字文件里。该文件将作为头号文件记录在每一个区块中。该文件表示次区块之后所有账户的余额信息。并作为世界状态被节点保留。

信币不是一种正统的去中心化数字资产。信币也不是信链的重点，信币更像是一种购买的服务。所以信币将由信链社区统一发布管理回收。信币可以用某种法币作为主体。或者用虚拟货币作为主题。

信币使用：使用记录将保存在每个头号文件里。

信币转帐：信币转帐也将通过某种格式的文件保存在二号文件里。

How？

信币增发/购买：信币将通过某种机制固定数量增发。

什么机制？1 要保障市场稳定之前，投资者有一定的回报。2 要保证，中心不出现亏损。

信币回收：官方某种机制固定数量回收。

什么机制？1 一定程度上保证 2 级市场价格的最低价格。2 保证官方不出现资金问题。

保存不可撤回信息每一年周期需要 1 枚信币，可支付 n 枚信币，自动更新 n-1 次。保存可撤销信息每年周期需要 1 枚信币，同样可支付 n 枚信币，自动更新 n-1 次，可撤销信息需外加 4 枚信币作为保证金，信息到期后将退回全部 4 枚信币。撤销可撤销信息将耗费 1 枚信币，并退回 4 枚信币。

7. 头号文件：
   头号文件即记录信币余额的文件，其记录的内容有
   公钥： ox00000000000000000000000000000001
   当前余额：30.0
   本次交易：-1

8. 二号文件：
   二号文件及记录信币转账记录：
   转账账户公钥：ox00000000000000000000000000000001
   收账账户公钥：ox00000000000000000000000000000002
   转账金额：1
   转账账户签名：ox00000000000000000000000000000003

9. 节点：
   轻节点：用户端，用于验证信息真伪，储存、购买、转帐信币。轻节点只保存链上区块头的信息，轻节点大小每 30 秒增加 32B，满链大小：32M。
   全节点：拥有验证、候选挖矿的权利。全节点保存区块、区块附加信息与当前头号文件与二号文件。全节点大小将取决于信链的繁忙程度。在 1000+TPS 的情况下，全节点每 30 秒增加 45KB，满链大小 45G。
   无限节点：拥有挖开的权利。超级节点将保存所有区块、区块附加信息、头号文件、二号文件。信链社区也将保留完整的无限节点。

10. 用户端：
    客户端：手机 APP，网页，桌面端口。
    每次打开客户端，先更新最新到最新区块。
    验证过程，用户只需要输入需要验证的信息（文字、图片、文件），客户端将发送信息的哈希值以请求验证，验证将发送给 n 个全节点，全节点将寻找该哈希值，若没有返回 false，若有返回区块高度、区块身 Merkel tree 头哈希以外的信息、需要换算出 Merkel tree 头哈希的其他哈希。用户端若收到的回复全为 false 则表明，需要验证的信息不存在，若收到验证信息，则计算 Merkel tree 头哈希，再通过计算该区块哈希，对比本地区块该区块的哈希值，通过则表明需要验证的信息存在。
    如何保证文件、图片等信息不被软件、系统、环境变化而影响？

验证不需要费用。

怎么把任务分配给全节点？怎么选择全节点？怎么奖励帮忙验证的全节点？

11. 信链社区：

信链社区将作为信链的宣传机构、代码管理机构。

信链社区将设置为可置换模式，及信链社区可以在不影响信链运行的情况下被置换。或者能容忍多社区中心的形式。

12. 匿名与实名：

信链，用户可以自由选择创建账户，某账户需要发生交易才能被全网认可。

账户可以自由选择匿名与实名。实名制主要是为账户背后的主体做绑定，大部分信息在有绑定主体的情况下才能有其价值。也为必要的信息提供主体，以防假冒记录。

实名制并不能找回私钥，也不能撤销操作。

匿名性的管理需要一套操作明细。

13. 可置换性：

信链在设计上将在多处使用可插拔式设计，方便部分技术的更换、置换，也保证结构的去中心化

签名方式、hash 方程的使用，这种结构与信链的交互将设置成可替换的模式。即在可行的范围内，用户端、节点可以使用不同的加密方式，信联容忍多加密方程。有利于适应不同国家地区的法规、也能让信链生态去中心化式升级加密方式。

In detail？

信链生态结构的可置换性，使的信链可以容忍更换信链社区，或容忍多信链社区。能容忍不定数量的超级节点存在。

In detail？

14. 信息格式：

被储存的信息，将被建议成某种格式。以避免信息的混乱、唔到与碰撞。

发生碰撞的信息将不能被记录。

优点总结：

可承受的 TPS 非常高，TPS 的最终限制更多来自网络信息传输的速度。

区块大小固定，但可包含的记录信息则可以任意叠加。

本质为服务，不存在政府的抵制与灰色地带。

商业价值可观。

信息可撤回。

使用简易。

应用场景：

需要证明某个信息的真实性：

学校上链毕业证，学生提供毕业证后，用人单位/检查单位可以链上查询

医院上链病人信息，病人提供身份，检查单位链上查询真实性

政府上链财产所有证明，拥有者提供证明，检验方上链查询

产权上链产权证明，拥有者提供证明，检验放上链查询

对外开放的信息（并保证开放后不可串改）：

集体、公益、慈善资金

法文、法规、规章

合约、合同

承若、声明

奖罚

不对外信息：

节点与上链过程并不需要被保存的信息本身。所有被保存的信息本身是不空开的，也是不可通过信链获取的。

信息转跳：

保存信息时，除了通过信息的哈希之外，还有一个默认 7B 的保留大小信息可以自定义。作为信息补全、转接、加密等