



Social Ecommerce Chain

社交电商链
以社交信任为基础的下一代电商领域区块链系统

<https://secblock.io>

> 欢迎阅览

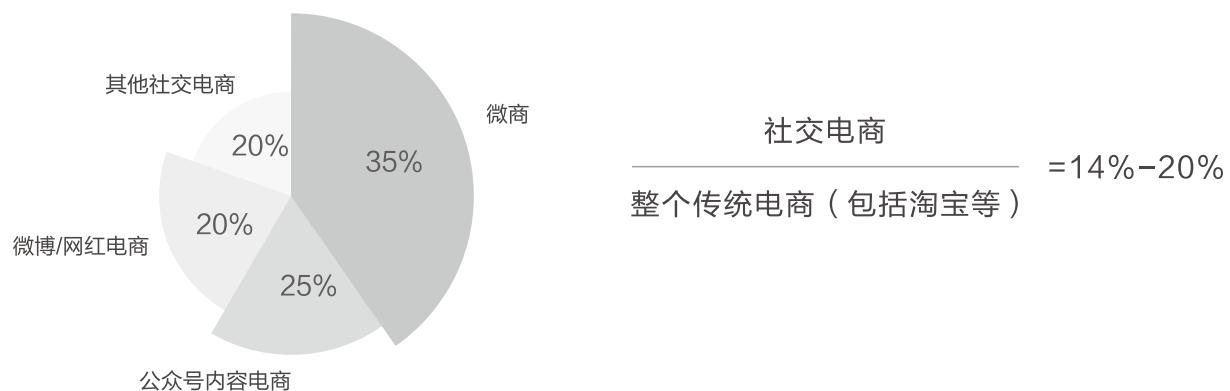
目录

01	导读	Page 04
02	SEC 系统分层与模块	Page 06
03	账户及信息管理	Page 07
04	SEC系统架构	Page 09
05	SEC区块数据结构	Page 10
06	SEC加密算法	Page 11
07	交易记录数据的结构及其上链流程	Page 12
08	P2P网络架构	Page 13
09	SEC区块链栓链结构及自治域定义	Page 14
10	自治域内角色和交易	Page 15
11	共识机制	Page 16
12	奖励机制	Page 17
13	SEC网关及智能合约的设计	Page 20
14	区块链基础术语解释	Page 21
15	全球技术部署	Page 22

导读

(一) 电商背景

过去未去，未来已至。电商形态已经发展到了新的转折点。电商正快速走向移动化、碎片化、社交化。Ebay、亚马逊、阿里巴巴均为电商领域的佼佼者，中国大陆地区电商行业更是在互联网浪潮中实现了电商领域长达17年的爆发式发展。虽然电商领域的绝对销售量仍保持增长态势，但中国电商领域领军企业的阿里电商体系正不断遭遇到社交电商、网红电商、内容电商等多种电商模式的竞争，市场竞争氛围异常激烈。以微信、微博社交用户为基础的电商形态发展迅猛，服装类网红电商异军突起，不断涌现出年销售额超10亿人民币的单一品牌。社交电商三年时间，已经占据电商14-20%的市场份额，体现出新一代电商的潜力与优势。



基于微信在中国市场的用户量，中国大陆市场的社交电商等模式创新和市场容量都领先全球。网红电商、内容电商、微信朋友圈电商三者业务模式从本质来看，有着异曲同工之妙，都是基于个人品牌、熟人圈子建立信任关系，然后再通过内容展示吸引用户成交，这也是目前为止最先进的产品生产零售形态。以网红电商为例，网红先通过产品展示，获得粉丝购买数量预测，然后再进行工厂定量生产、进行销售。从样品展示到完成单品主要销售周期，资金的流转效率跟原有生产零售模式比是数量级的差别。

传统电商形态基于PC设备时代，伴随智能终端的发展进而逐步过度到以APP等移动端作为载体的移动智能时代，信息技术的深度发展，正进一步给个体赋能，新一代电商正在快速起步阶段，更大数量级的市场还没有被激发。比如中国很多农户的农产品缺乏有效的信息传递及信任机制，无法以合

适的价格出售给消费者。举一反三，解决信任基础及更有效的传播途径两个核心问题，是新一代电商发展的契机；综上所述，构建新一代电商信任机制作为新一代电商的有效支撑。

(二) P2P技术用于电子商务的历史

此前很多人致力于将P2P技术应用于电子商务，如Lightshare就在P2P网络上开展电子商务。P2P电子商务模式中，用户拥有更为灵活的通信交易模式，在网络中的每个用户节点都可能相互访问到彼此，并直接发生交易，它正作为一种新型的电子商务发展起来，但信任风险是P2P电子商务发展的主要障碍。

(三) 正在重构的电商客户关系管理

随着用户时间的碎片化，大多数品牌已经在通过社交平台诸如facebook、twitter、微博等渠道进行品牌宣传和用户关系维护，不少中国的中小电商正在把消费者从其他电商平台，引流到微信个人号，把微信当做客户关系管理工具使用。

而区块链技术支持之下的电商将重新定为P2P电商模式，重新定义“客户关系管理”；间性关系的全程管理，必然走向买方与卖方、买方与买方的间性关系全程管理。最终，间性关系就是新一代的信任机制的建设核心。

(四) 跨境电商正快速崛起

纵观2017年，全球跨境电商消费额进一步增长，全球购模式进一步得到夯实，且未来仍具备高速增长潜力。跨境商品在物流仓储，跨境流通的过程中，消费者对大量中小品牌无认知，不信任，中小很难形成规模销售，因此通过区块链技术手段实现跨境产品流转环节中的信任等环节，将对全球跨境电商意义非凡。

SEC系统分层与模块



SEC以社交信任为基础的下一代电商领域的区块链协议

SEC 区块链方案的整体架构分成三个层次

1. 底层是SEC的主链系统
2. SEC 服务层作为中间层，提供交易网关作用，用于链内和链外 WEB 协议等的交互
3. 上层是 SEC 应用服务层，提供 api 接口，并提供 web 应用开发和DAPP 开发框架和底层应用能力。

SEC系统分层与模块

SEC区块链首先是一个去中心化的系统，任何数据都将是公开透明可追溯的且不可修改的，我们不存在用于储存交易信息的服务器。其次加密机制确保了用户私钥和地址的高安全性，同时对交易信息选择性加密，又保护了用户交易过程中的隐私。



SEC系统分为五层结构。由下往上数据层作为第一层。在该层中保存了区块数据，链式结构以及数字签名。并且哈希的生成，梅克尔树以及非对称加密的计算也由数据层负责。网络层位于第二层。由数据层产生的区块数据交由网络层，并在P2P的网络中进行传输。并且区块数据的可靠性也由网络层确认。第三层共识层中定义了SEC系统中的共识算法。SEC系统的共识机制采用类DPOS。激励层位于模型的第四层，在该层中定义了Token的发行机制，以及产生新区块时的奖励机制。最顶层是智能合约层。该层位于SEC网关中，智能合约存放于该层中。

账户及信息管理

SEC提供账户以及功能管理分为

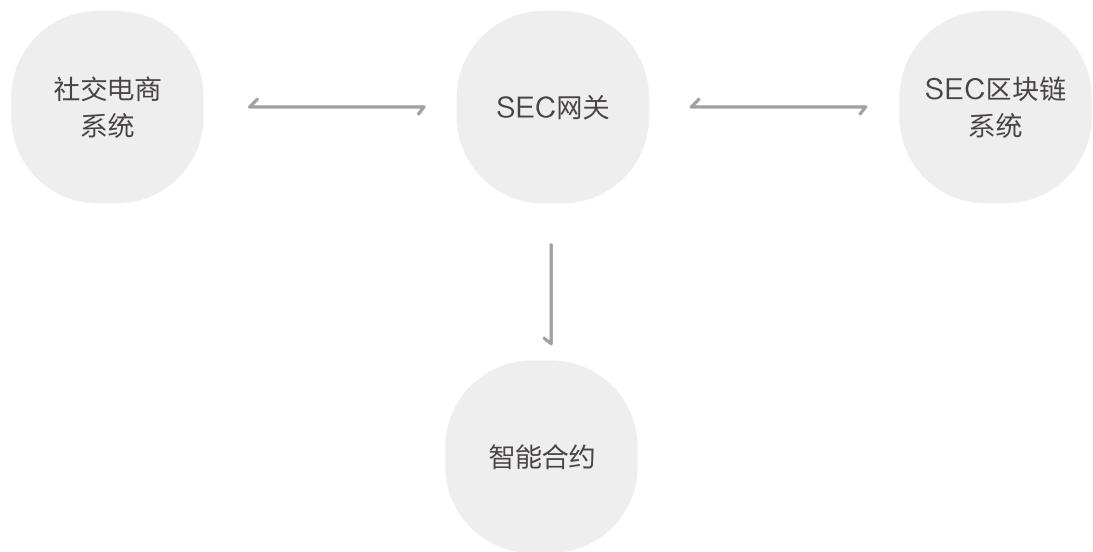
- > 用户管理
- > 账户管理
- > 密钥管理
- > 权限管理
- > 用户信用风控管理

SEC的目标是

SEC拟实现跨国界、跨平台、跨品类的P2P电商市场当中信任的传递及社交的分享。它将是一个基于电商应用场景的全新底层构架平台：去中心化、开放、安全、高效。在生态系统中，参与方通过分享行为及分享有效性可以得到合适的Tokens 奖励，商家也可以在享受技术服务的同时降低平台入驻成本及信息处理的可变成本，一举多得。区块链和电商这两个领域存在着快速发展的红利。

SEC 作为透明、开放的系统，希望可以促进全球电商的发展，通过分享经济方式去驱动社交电商重塑，形成一个有效的去中心化市场。

SEC系统架构



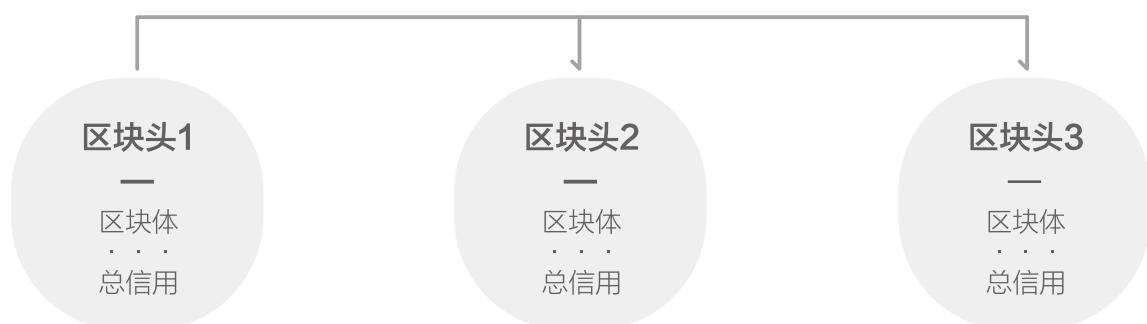
在我们的设想中，社交电商系统与SEC区块链系统，相对独立，之间只通过SEC网关进行通讯。SEC区块链系统只存储由社交电商系统发出的完成交易后的交易记录数据以及在分享完成后交易记录数据。SEC网关在构想中由智能合约集合实现，用来实现SEC网关的智能合约在这里定义为系统级智能合约，此智能合约的执行无需消耗Gas。系统级智能合约搭建在各个超级节点上（见P2P网络架构）。系统级智能合约包括如下种类和功能：

- > 对完成交易后的交易记录数据进行验证并上链
- > 对通过分享者完成的交易进行验证并上链
- > 完成对假冒伪劣商品的处罚
- > 完成对虚假交易的处罚

SEC 区块数据结构

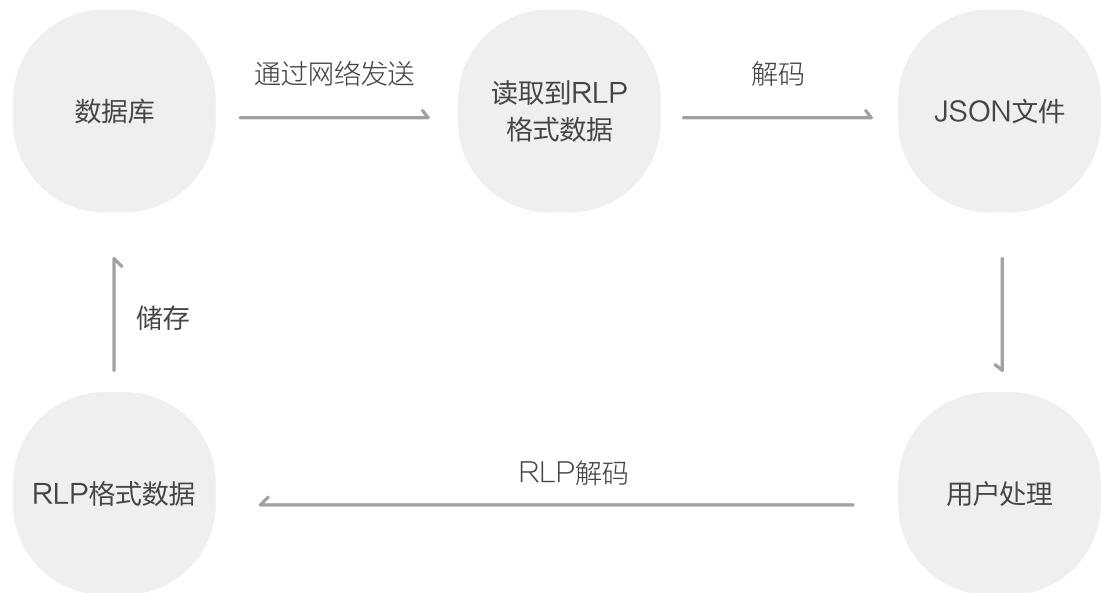
在这个项目中，我们将使用 JSON 格式+RLP 编码的方法来处理和存储区块的信息

在交易链区块中的交易记录之后记录当前商品最新信用值（总信用值），如此确保区块中最底部的数据永远为商品最新总信用。通过这种机制，DAPP 和各个节点可以通过极少的资源消耗拉取对应商品的信用情况，也解决了SEC轻节点拉取商品信用值的问题。



JSON 是一种轻量级的数据交换格式，有简洁和清晰的层次结构，易于人编写和机器解析，并有效地提升网络传输效率。RLP 编码可以嵌套任意长度的二进制数组，专门用于列表结构的数据处理，结构清晰简洁，仅仅靠分析短短几个字节长度的前缀，就可以很清晰的了解数据结构。

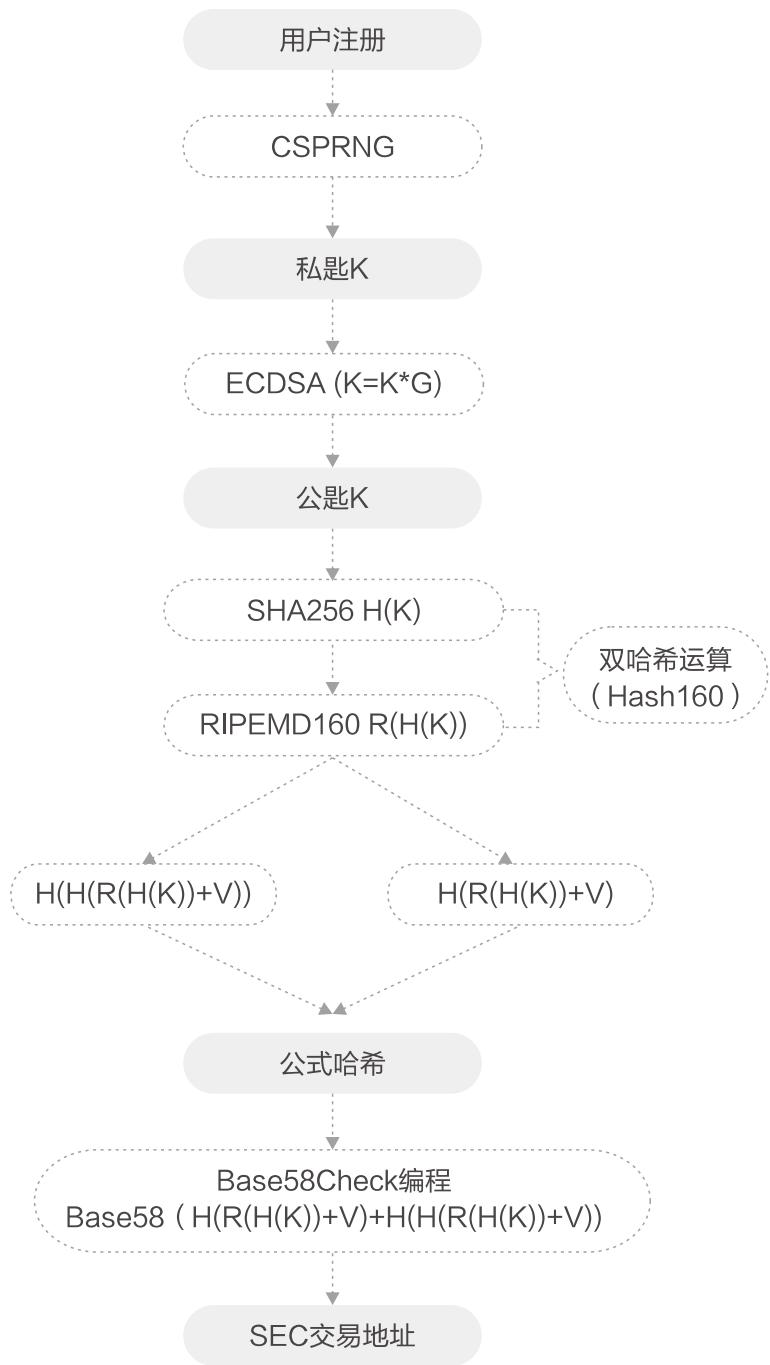
具体流程图如图



SEC 加密算法

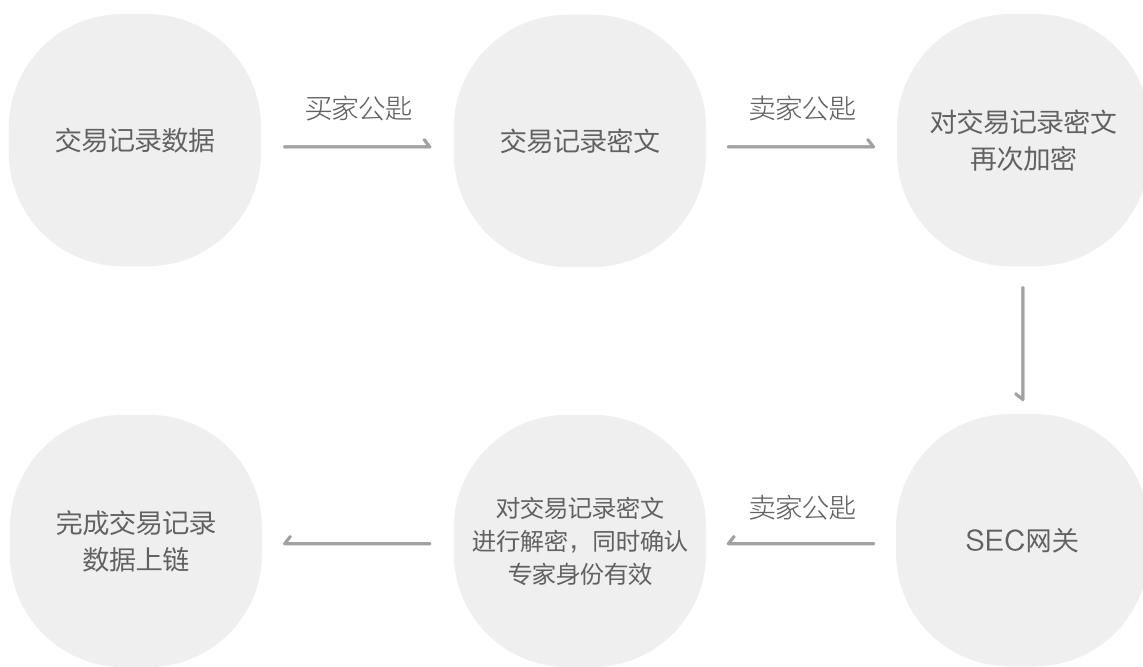
采用非对称加密方式中的椭圆加密，其加密算法为 secp256k1。也正是比特币所用的加密法。椭圆加密的工作效率远高于非对称加密 RSA 算法，达到同样级别的安全强度，RSA 所用的字符长度约是椭圆加密字符长度的 6 倍多。因此椭圆加密大大降低了对整个系统的运算负荷。以目前的技术来看，可以说是椭圆加密算法不可逆。当用户注册了以后，产生随机数 k 做为用户私钥，用椭圆曲线乘法单向加密函数 ECDSA (k)，得到用户公钥 K，此时，使用一个单向加密哈希函数 Hash (K) 得到用户 SEC 交易地址。其中私钥的生成是第一步也是最重要的一步，我们此处建议使用密码学安全的伪随机数生成器 (CSPRNG)。通常情况其长度为 256 位，是一个二进制数，以 64 位十六进制示，每个十六进制占 4 位。

用户注册以及交易地址产生结束后，用户向本自治域的验证人发送“握手请求”，若验证人在线并响应，发送给验证人用户的公钥 K 和 SEC 交易地址。公钥做为私钥和 SEC 交易地址的桥梁，其重要作用是验证交易的真实性，可通过运算正推验证发送交易的地址是否和该公钥生成的地址一致；公钥也可验证私钥的签名，用来验证该交易是否使用了正确的私钥签名；私钥生成公钥是成对出现，公钥可以生成对应的唯一地址，因此就可以确认了该地址发送的交易是否使用了对应的私钥。



交易记录数据的结构及上链流程

交易记录数据的主要内容为：卖家地址、买家地址、交易记录和交易状态。其中的交易记录需要在上链之前进行加密，交易记录内容储存商品名称和商品价格。



1. 交易记录数据中的交易记录首先会用买家公钥进行加密，生成交易记录密文，此密文会在之上被存储在自治域的交易链中。

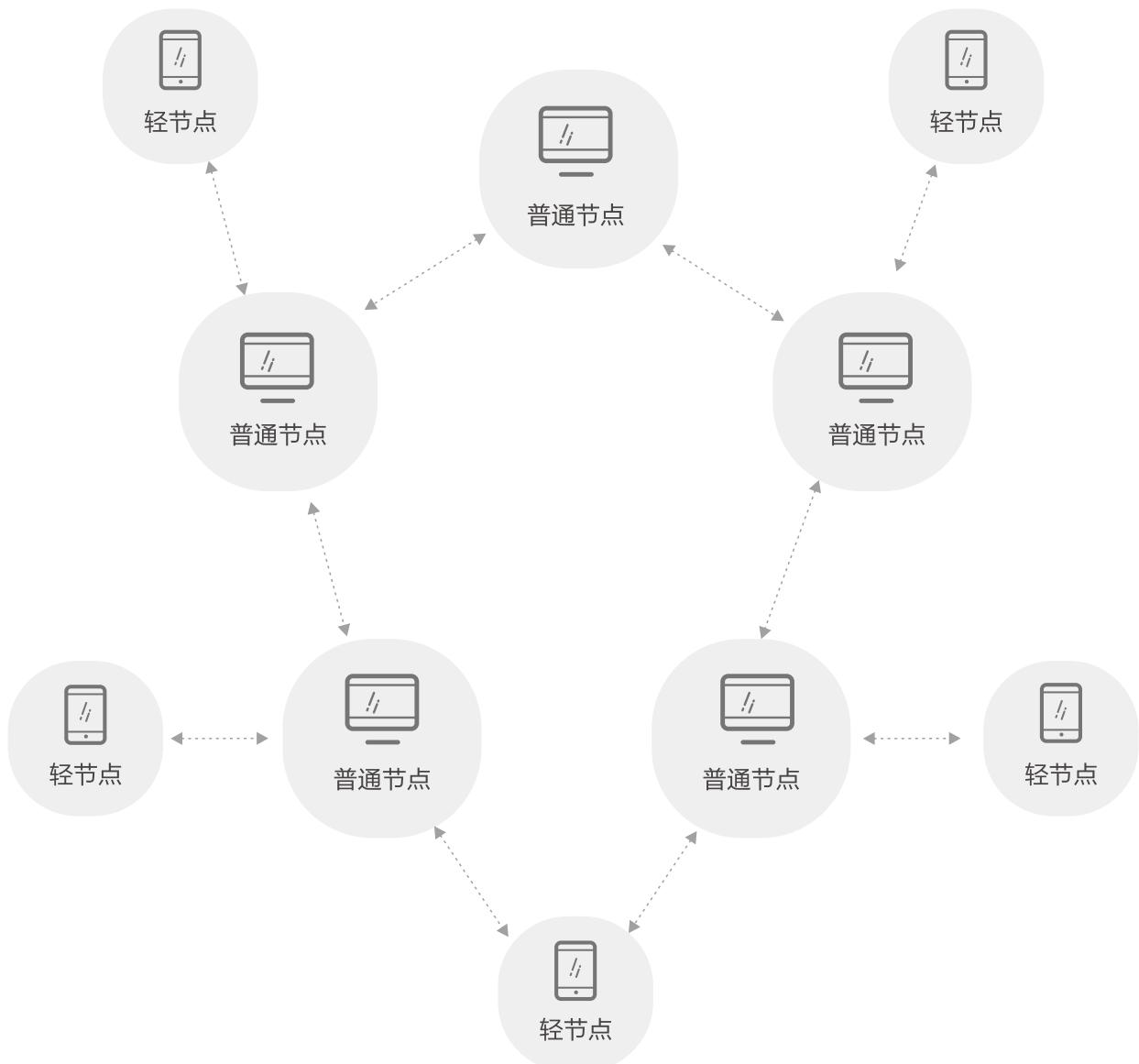
2. 在第一步生成的交易记录密文再次使用卖家私钥进行加密，并发送至SEC网关。
3. SEC网关中的系统级智能合约会用卖家公钥对二次加密的交易记录密文进行解密，如果可以解密，则可以确定此交易记录的真实性（确实由卖家生成并发出），完成对交易记录真实性的验证。
4. 在完成验证后由对应轮循内的负责节点封装上链。

通过此流程上链的交易数据本质上只能由交易相关的卖家和买家进行解密后查看，与此交易无关的其它结点无法查看这次交易的具体内容，只能知道发生了交易。实现了链上交易记录的保密性及匿名性。

P2P网络架构

SEC 区块链系统网络为一个类似于 Skype 及 KaZaA 的结构化分布式网络，是第三代 P2P 网络。此 P2P 网络由 SEC 轻节点、SEC 节点组成。

- > SEC 轻节点：一般为手机客户端，只与 SEC 节点进行连接，数据从 SEC 群落拉取。
- > SEC 节点：一般为 PC 客户端，负责连接其他节点，同步交易数据。家庭网络可胜任。



SEC 区块链双链结构及自治域定义

SEC 区块链采用双链平行结构，分为交易链和 Token 链，交易链可分自治域，每个自治域包含一个自己的交易链；Token 链为一条独立的主链。

交易链

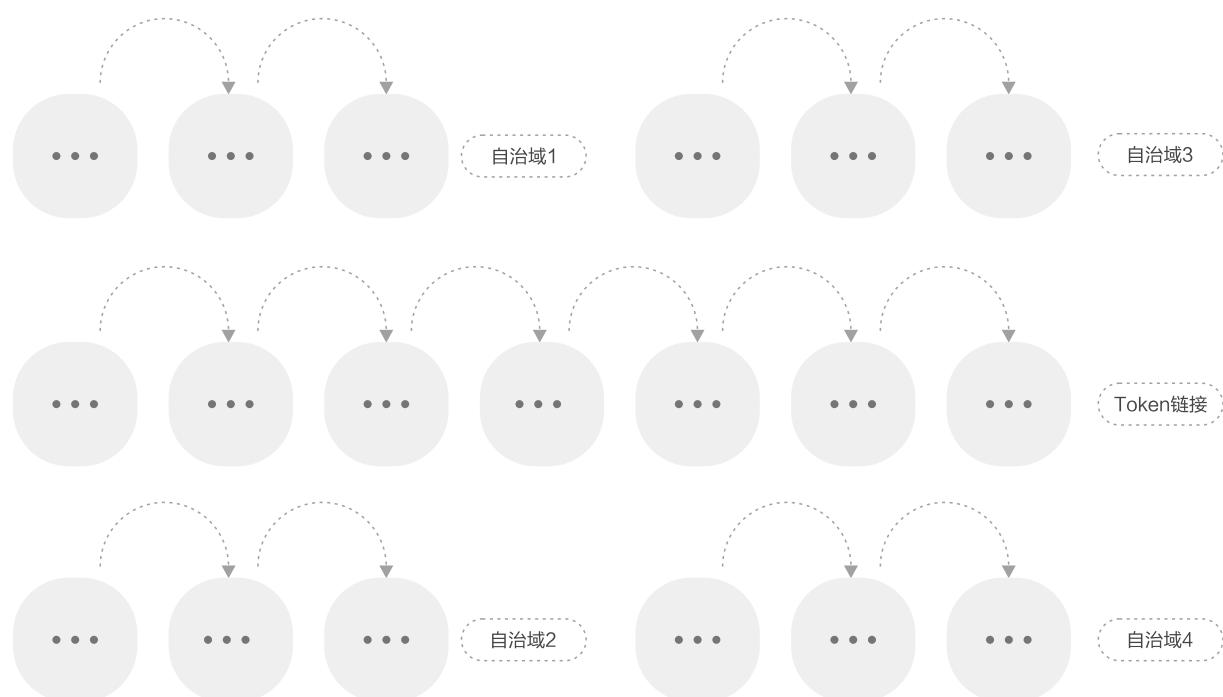
只用来存储交易信息及对应商品的信用值

Token链

用来记录用户得到的 Token 奖励、转换 Gas、实现 Token 转账与记录、支持智能合约系统，类似比特币的主链及以太坊的主链。

自治域

按一个商品进行划分（待选）；或者按一个品类的商品进行划分（待选）

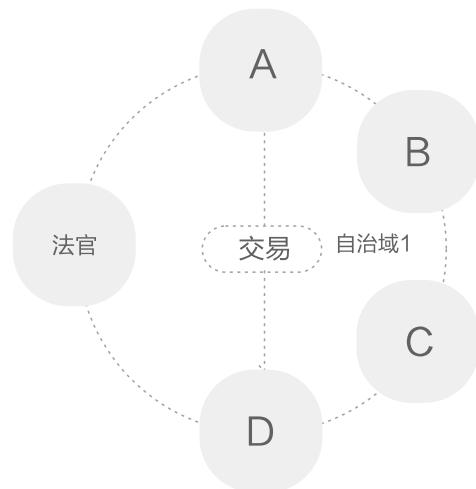


自治域内角色和交易

当 A 与自治域内的其他用户 D 交易时，此条交易信息并签名，之后将一段时间内所有的交易信息发送给 B，B 验证并确认所有交易信息的真实性，并将此次的所有交易信息封装上链，记录在区块中。验证人 B 通过创建新的区块获得系统奖励，奖励额度见共识机制算法。自治域内，用户的管理由验证人和法官共同负责，法官监督自治域的交易。

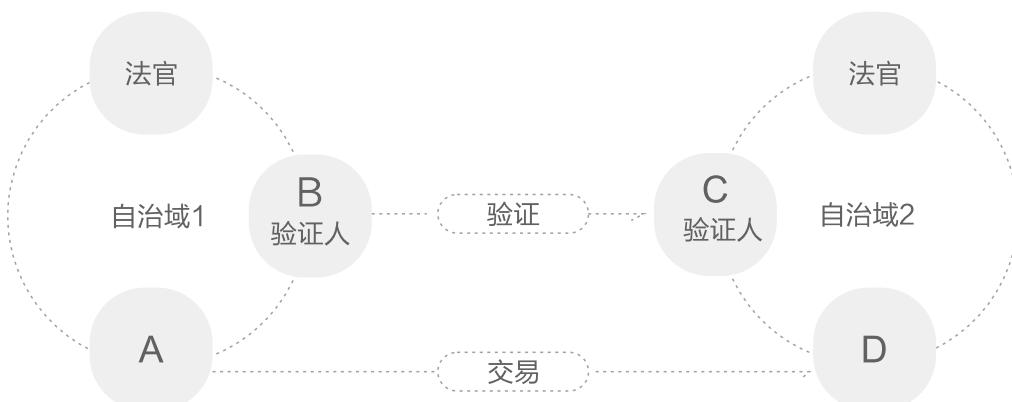
验证人有最高权限，职责是在SEC自治域里打包新区块。

法官并不直接和区块打包的过程相关。他们是独立的“赏金猎人”，激励他们的是一次性的大额奖励。

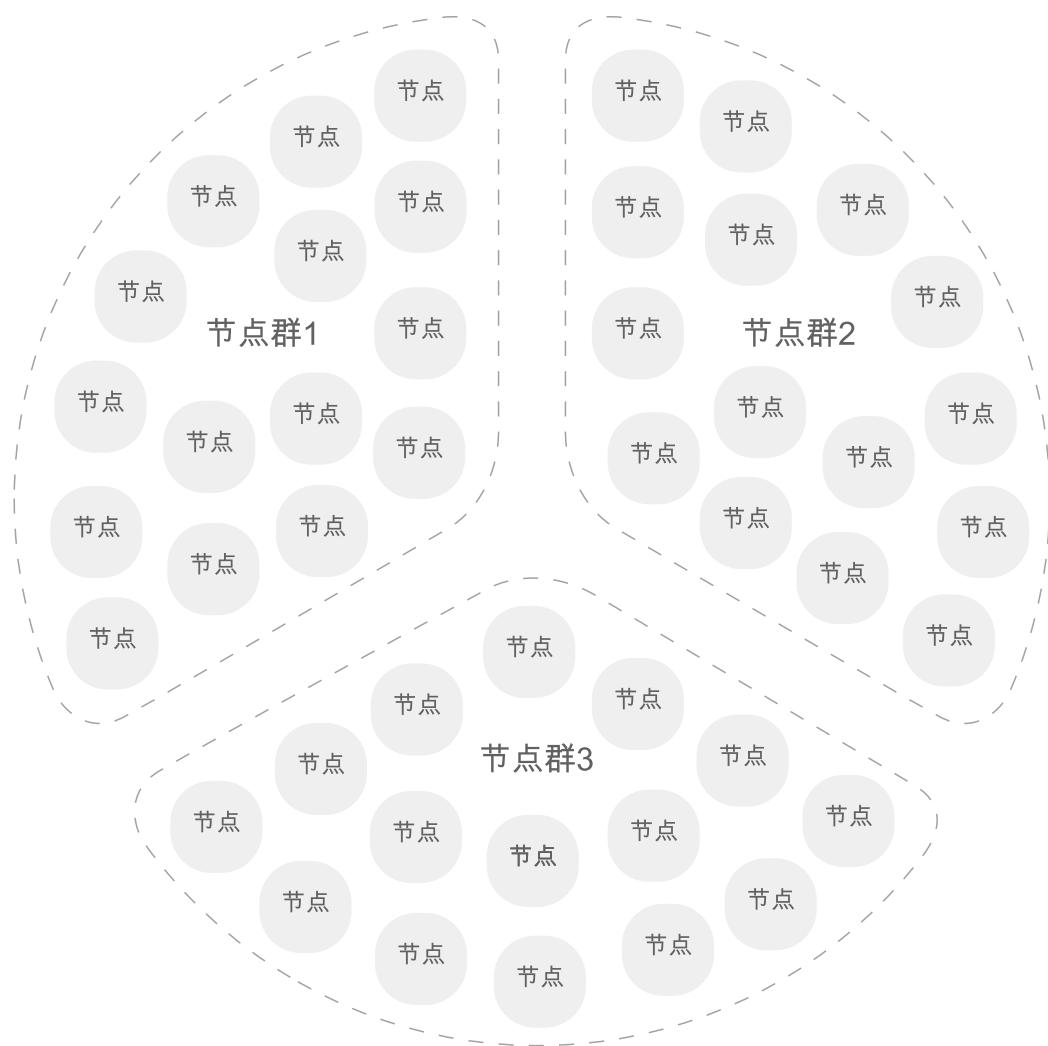


所有的用户信息都会记录在Token链中，Token 链即为跨链交易的介质链。当A与自治域外的用户D交易时，验证人将会在Token链中寻找D的位置，将交易记录储存在相应区块链中。交易链上信息由智能合约打包写入。

自治域以商品为单位划分，每个自治域中都会储存信用度，顾名思义是评判商品信用的判据，并且此行为由该自治域验证人管理，每个节点用户拥有状态，验证人可确定状态。



共识机制



我们的共识机制采取了节点群间DPOS与节点群内POW结合的方式。

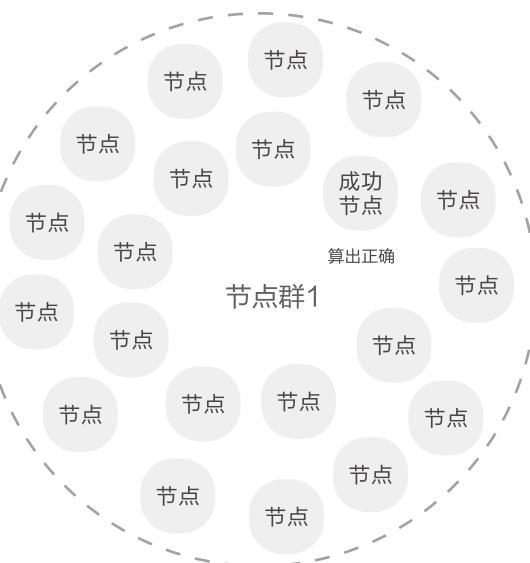
在网络层面上只由SEC轻节点与SEC节点组成，在逻辑层面上由数量庞大的自治域组成，每个自治域又包含一条交易链。每一笔在社交电商中完成的交易会被储存在对应的交易链中。为了满足对数量庞大的交易链的维护（如交易数据包打包验证上链，每一条交易链新区块的生成），并且又不使用超级节点以避免可能带来的中心化问题及超级节点成本问题，所以在这我们使用了节点群落的概念。

节点群落由SEC节点构成，从本质上说，节点群落实现了超级节点的功能，解决了对大量交易链维护所需的算力问题以及Token链新区块生成问题。

共识机制

节点群落生成的具体流程如下

1. 假设我们的系统由10个节点群落组成，节点群落标号1到10
2. 每个普通节点给自己的每一个相邻节点生成一个1到10的随机数，这个过程称为投票
3. 每个普通节点会得到来自相邻节点的投票，获得的最多的点数就为这个节点所在的节点群落标号
4. 获得相同节点群落标号的普通节点，属于同一个节点群落通过上述机制，划分每个节点群落，同时避免了投票作弊。在每个轮循完成后，系统会自动再次进行节点群落的重新划分。



Token链新区块生成及交易链的维护

由上述1到10个节点群落轮换生成Token链上的新区块，并轮换对交易链进行维护，在这里有点类似于DPOS机制。一次完整的轮循为一个周期，一个周期结束后，重新进行新的节点群落划分及开始新的周期。

被轮换到的节点群落内部进行POW机制，各个节点竞争一个生成Token区块的机会，生成Token区块的节点获得Token及Gas奖励。

上述的POW机制无需设置很困难的题目，目的只是为决出一个可以生成Token区块的节点，另外可以相对保证这个普通节点的机器性能较高，可以胜任数据打包的任务，这个节点完成对Token链上的数据打包及上链。

在节点群落内的各个普通节点，由于共同维护了系统的正常运作，即使没有竞争成为节点群落内矿工节点，也可以获得少量Token奖励。

由于节点群落包含了很多普通节点，这些普通节点大概率包含了系统内全部的交易链，这些交易链由在被轮循节点群落内的所有普通节点共同维护。

共识机制

通过此流程上链的交易数据本质上只能由交易相关的卖家和买家进行解密后查看，与此交易无关的其它结点无法查看这次交易的具体内容，只能知道发生了交易。实现了链上交易记录的保密性及匿名性。

当SEC TOKEN链出现分叉时，即由于网络延时等原因出现两个不同区块拥有同一个父区块的现象时，我们采取与比特币相似的方法，即承认较长链的方法来解决分叉问题，具体的步骤如下：

1.假设群落1的两个用户A和B在相近的时间完成了POW，并将结果广播给了群落2，则群落2会有部分用户根据用户A的结果计算，剩下的根据用户B的结果计算。

2.假设群落2基于A结果计算的用户C首先计算出了结果，其他群落2的用户没有计算出结果，则C将该结果全网广播，同时群落3的用户开始基于C的结果进行计算，此时：

a.由于群落2的用户C已经计算出了结果并进行了广播，因此群落2将停止接收从群落1发送来的位于用户C上链区块之前的新区块上链计算请求。

b.若在C用户广播之后，位于群落2的恶意用户D仍基于A的结果计算，并于C广播10秒钟后算出同样符合要求的POW结果并广播，此时由于群落3已经在基于C的结果计算，因此D的广播会被绝大部分节点忽略。

c.若群落3有恶意用户D的同伙E，则为了确保在群落3用户D的结果会被更早计算出来，则群落3用户的算力要超过51%（由于C的结果已经被计算过一会儿了，因此甚至需要超过51的算力）

由于当一个群落计算出POW结果并广播后，该群落就不再接受前一群落的新区块信息，因此当两条分叉的链相差超过两个区块后，短的链就会被完全否定。

d.当然，从概率上来说，即使恶意用户D的同伙E节点的算力很低，节点E仍有不低的概率先于基于C结果计算的节点完成POW计算（当C发布时间与D相仿时，概率约等于节点E占群落3的算力百分比）

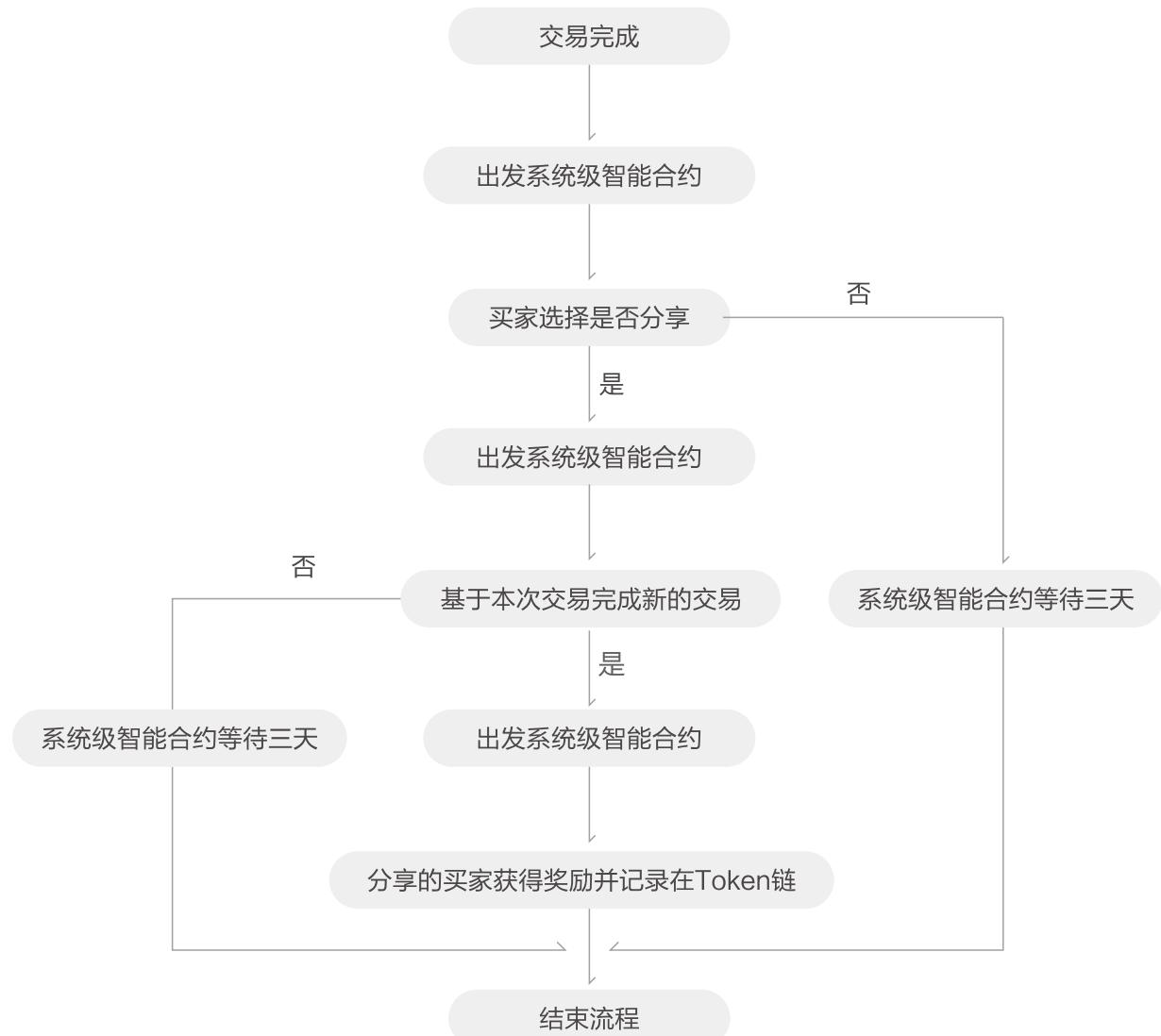
这种情况下的分叉是被允许的，该机制可以保证链无法被从很早的区块被硬分叉，这种段分叉是合法并无法防止的。同时，即使恶意节点D的区块被承认了，另一条基于C的短链上的交易也不会被取消掉，而是会回到交易池中等待下次区块打包。

3. 假设群落2基于A结果计算的用户C，基于B结果计算的用户D（或基于A结果计算的用户D，处理相同），也在相近的时间完成了POW，并将结果广播给了群落3，则将重复上述步骤。

4. 如上述2.c所述，当最长链的长度超过第二长的链两个区块后，可以知道：若最长链的长度为n，则之前n-1个区块的交易信息被确认并无法被更改。

奖励机制

当买家和卖家完成一笔交易后，交易记录智能合约将会拉取交易记录到交易链中（具体流程见交易记录数据的结构和其上链流程），然后对应的买家可以选择是否分享该商品到社区，如果进行分享则会触发SEC奖励智能合约，在当买家分享的链接被另外的买家触发并完成购买行为，则前一位买家获得对应奖励（即SEC Token），其奖励的额度与商品价值挂钩；如果没有进行分享或者分享后没有发生购买行为，则SEC奖励智能合约将会在三天（72小时）后自动失效。两个智能合约均为SEC区块链系统级智能合约，存储在创世区块，用户无需编写，由系统自动生成。



SEC网关及智能合约的设计

智能合约分为用户方智能合约以及系统级智能合约。用户方智能合约可由用户自行定义交易的行为方式。系统级智能合约由SEC系统直接提供。我们将SEC的所有系统级智能合约的集合定义为SEC网关。SEC系统级智能合约保存于交易链中。

SEC系统级智能合约主要应用于针对买家的分享行为奖励。当卖家与买家之间的一笔交易完成时，卖家节点会在SECVM环境中运行智能合约。该智能合约会为此次的交易信息生成区块并且开始对买家的分享行为进行监听。

买家的分享事件如下定义

当卖家A与买家B之间的交易成功后，买家B可选择分享此次购买的商品给买家C。如果买家C通过买家B的分享与卖家A之间成功进行交易，那么买家B便会通过此分享行为获得系统的奖励。

分享行为在区块链上的实现如下

系统智能合约在卖家A和买家B交易成功后会对买家B的分享行为进行监听。当买家B分享此次交易购买的物品后，智能合约会对分享的事件生成区块并加入到交易链中。此时买家B还无法获得系统给予的奖励。当买家C通过买家B的分享与卖家A达成交易，卖家A节点上的智能合约便会监听到该交易事件。此时，通过智能合约，系统会去链上验证买家B的分享行为是否存在。验证通过分享行为的Id以及交易的状态进行确认。

如果存在，那么C与A之间通过分享所达成的交易事件也会上链，并且给予买家B奖励。

如果节点A宕机

使得和节点A在同一自治域内的SEC节点也是P2P网络上相邻节点。在这里，假设他们为B和C节点。

A节点运行智能合约时，它会把每条信息用自己的私钥签名。

A节点会给B和C节点发心跳包，周期为每10秒，心跳包中包含着智能合约运行的最近状态和数据。如果心跳包中断，B和C开始运行合约，当检测到分享行为，他们都会广播该信息，由信息收集者甄选，同时信息也要分别用他们的私钥签名，此举可以避免个别恶意节点借此机会攻击。

当A节点重新上线，A会重新发送心跳包，当B和C检测到来自于10次的心跳后，会中断自己的运行，当同时收集到A，B，C关于同个交易ID的信息时，以A签名的信息为准。

区块链基础术语解释

● 区块链

区块+链=记录+验证，比特币的核心技术，是一个去中心化的分布式账本。

● 分布式账本

不同于传统数据库技术的数字化所有权记录（因不需要中央管理员或中央数据存储）；这种账本能在点对点网络的不同节点之间相互复制，且各项交易均由私钥签署。

● 节点

保存账本副本的共识网络或服务器的成员或系统，并可担任不同角色，如发出、验证、接收和通知等。概括而言，节点可被视作虚拟机实例。

● 共识机制

区块链或分布式账本技术应用的一种无需依赖中央机构来鉴定和验证某一数值或交易的机制。共识机制是所有区块链和分布式账本应用的基础。目前的主流共识机制有POW（工作量证明）、POS（股权证明）和DPOS（股权委托证明）。

全球技术部署



SEC在开发伊始便确定全球技术部署的战略，依托投资团队在社交电商行业内丰富的运营经验及全球范围内的优质资源，我们将把核心技术团队在亚洲、北美洲以及欧洲进行全面部署。



SEC项目着眼全球市场，并计划在多伦多、
硅谷、上海、慕尼黑以及澳大利亚进行项目推广，
与当地品牌开展商务合作和用户推广。预计
2019年6月成为用户数量最大的区块链应用之一。



中国深圳：SEC项目总部



德国：主链开发团队



美国硅谷：运营团队



加拿大多伦多：应用层DAPP开发团队



COPYRIGHT ©2017 SEC TECHNOLOGY CO, LTD.ALL RIGHTS RESERVED.