



— Social Ecommerce Chain

以社交信任为基础的
下一代电商领域的区块链协议

摘 要

本论文我们分析 Social Ecommerce Chain（一种用于社交电商、P2P 电商、网红电商、内容电商等电商行业的区块链）中所使用的主要技术。SEC 本质上通过分布式记账交易关系和信任背书建立电商和消费者的信任价值网络，引入新的共识算法，实现多项目延展的特性。

一、项目概述

（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。微信体系涉足电商领域的三年时间，市场份额已经占到电商市场总份额的 14%，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，仍旧面临一定程度的繁琐的通关验证程序等，通过区块链技术手段实现跨境产品流转环节中的信任、验证等环节，解决跨境商品真实性验证和追溯等功能的实现，将对全球跨境电商意义非凡。

（五）隐私保护

现有中心化网络可以随意收集用户隐私，个人信息泄露导致个人信息买卖、甚至诈骗等一系列问题，在区块链技术的辅助之下，有助于实现客户信息的技术保护，包括但不限于商品买卖信息等诸多方面。

因此 SEC 是全球第一个以促进电商社交化，以信任为基础的区块链项目，SEC 需要支持大并发及能支撑海量交易的底层建设。SEC 采用的与比特币和以太坊不一样的共识机制和节点算法。

二、SEC 架构概要

（一）基于基础协议交易信任的区块链系统

SEC SYSTEM，将包含协议的完整实现、基础工具和 API 接口。SEC 是一个开源项目，协议遵循知识共享的许可。

基于电商的交互业务逻辑相对简单，但对交易关系形态的变化较多，因此我们在底层基础协议方面提供更多灵活的空间和扩展性需求；但在工具和 API 接口方面，对一致性和安全性保持相对的强耦合状态。根据团队前期的 P2P 电商领域丰富的经验，市场需求非常旺盛，相信这两个方面的考虑会对 SEC 快速的大规模商用提供一定帮助。

（二）SEC 架构概要

SEC 区块链方案的整体架构分成三个层次：（1）SEC Structure ；（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。

整体框架结构如下图：

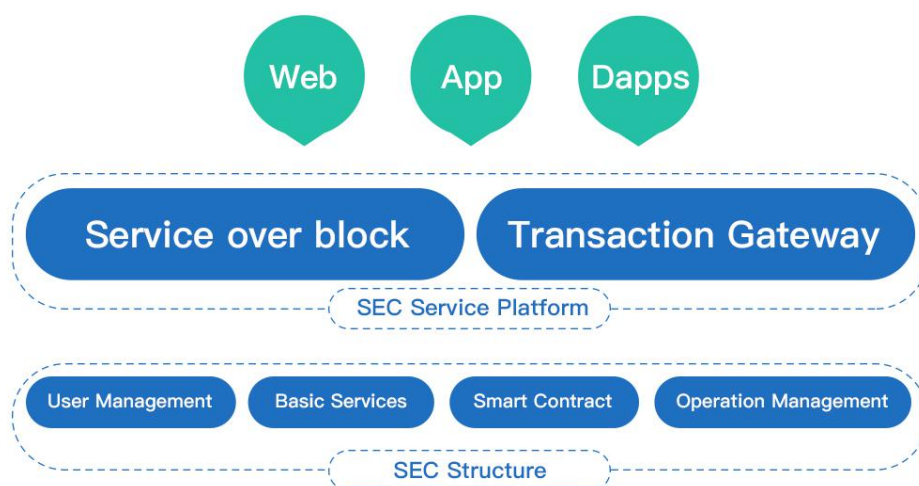


图 1 SEC 基础框架

1、SEC 底层架构

（1）账户管理：负责区块链参与者的身份信息管理，包括维护公私钥生成、密钥存储管理、以及用户身份和区块链地址对应关系维护等。

(2) 基础服务：基础服务部署在所有区块链的节点上，用来验证业务请求的有效性，并对有效请求完成共识后记录到账本上。对一个新的业务请求，基础服务先对接口适配解析及鉴权处理，然后通过共识算法将交易或者合约加上签名并加密之后，完整一致地存储到共享账本上。共识机制可自适应，网络异常或者节点欺骗的情况下具有强容错性。

(3) 智能合约：负责交易的区块链合约的生成以及合约的触发和执行。用户通过简单操作即可完成 P2P 电商合约逻辑，发布到区块链上之后，根据合约条款的逻辑，由用户收款或签名等其他的事件触发执行，完成交易结算等合约的逻辑。

(4) 运维管理：负责区块链发布过程中的部署、配置修改、合约设置以及产品运行中的实时状态可视化的输出，如：告警、交易量、网络情况、节点健康状况等。

2、SEC 服务层

SEC 服务层提供链内链外交易网关和信息服务层的中介。

交易网管协助用户进行链下电商购买操作到链上的交互接口，并提供鉴证服务：让卖家和买家通过一个简单的 API 接口就可以把交易信息等发布到区块链上，让所有记账节点共同为自己作证。在本质意义上是交易信任与买家对交易标的个性化体验差异解耦。SEC 链体系功能实现的是在链内的信任关系机制，因此将链外部的商品标的信息与交易信息分离。在交易关系收敛周期内，如果双方没有进一步的交易完成，则认为双方信任关系解除；而交易关系的收敛周期根据所自然形成的自治域的链的交易速度和广度有关。

信息服务层则抽象底层区块链多种信息，提供上层应用开发框架所需要的底层信息和消息对话机制。

3、SEC 应用层

SEC DAPP 应用服务层提供简单应用开发的框架，应用类型包含了数字资产、共享账本、鉴证证明、产品追溯及所有权交易等基本应用模型。用户可以基于这些应用开发框架进行业务开发。开放区块链底层结构（SEC structure）和应用层（SEC）的能力，协助社区开发新的 SEC 电商应用服务、匹配对应的应用场景，共同维护区块链生态。

4、性能考虑要素

SEC 并非是做电商的基础区块链应用，而作为电商信任基础的底层协议，SEC 将满足复杂的交易关系管理，底层设计成具有可扩展和可伸缩的特性，以实现为广泛的电商场景、创新创业电商公司赋能。

借鉴现有区块链技术，SEC 考虑的关键性能问题包括：

（1）伸缩性（Scalability）：基于 P2P 电商的交易规模，考虑目前移动终端计算能力、带宽变化和存储条件，区块链在处理单个交易的资源方面，需要底层机制在设计的时候考虑到“低耗时”、“低耗能”的处理能力；

（2）开发性（Developability）：考虑到未来电商参与者个体化、公司小型化的趋势，一方面会从工具实现的便捷性方面入手，向使用方提供足够方便的使用工具，满足非程序员人群无需学习就可以上手操作，超越现有电商工具的便利性；另一方面，SEC 基金会会建立开发社区，与所有生态参与者共享电商行业红利。

（3）治理性（Governance）：基础协议需要足够简单，保留能够随着时间进化和适应的灵活性，制定决策能实现高度地包容、合理和透明，来提供去中心化系统的高效领导力。

（4）应用性（Applicability）：是在基础协议公用链和服务层基础上，普通用户就可以便捷的开展去中心化电商应用。

三、SEC 底层区块链平台

SEC 底层架构是一个多域自治的双链并行系统，主链（交易链）负责执行交易、维护交易历史和信任关系信息等；在主链上可以存在全局依赖的动态数据结构，副链（账户和关系链）负责维护账户信息和信用指数。主链用于存储已经达成过信任的交易关系用户信息，并采取异步更新机制。

因 P2P 电商业务逻辑抽象相对简单，因此 SEC 把大部分的复杂性都放在了区块链和 API 上。

（一）SEC 自治域

SEC 是一个涵盖众多独立区块链的网络，多域自治的域，叫做自治域 (Autonomous Area)，即把整个 SEC 网络划分为许多较小的网络单位，频繁的交易关系和信任关系的节点自动生成并收敛在同一个自治域内。SEC 自治域是一种社交关系权益证明加密货币网络，它通过类似路由简单的管理机制来实现网络的改动与更新。SEC 自治域还可以通过连接其他链通过跨链来实现扩展。

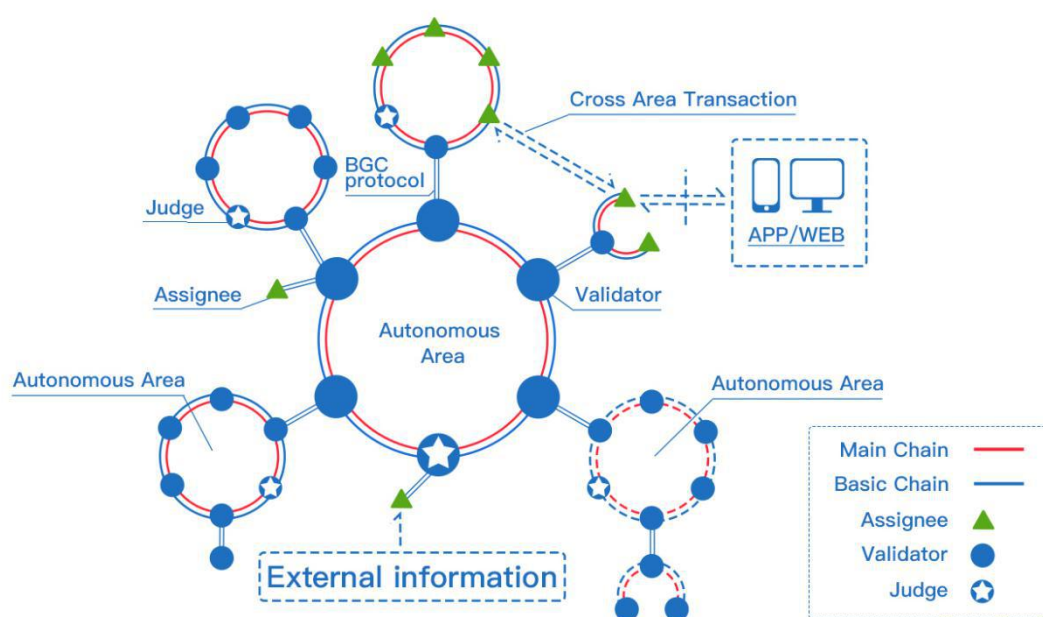


图 2 SEC 架构示意图

通过域间通信（BGC）协议进行交易，BGC 协议就是通过不同域兼类用户数据报协议（UDP）和类传输控制协议（TCP）进行通信。Tokens 可以安全快速在域间转移，两者之间无需体现汇兑流动性。同一自治域内部所有 Tokens 的转移都会通过 SEC 关键节点，它会记录每个自治域所持有的 Tokens 总量。这个自治域会将每个资质与其他故障自治域隔离。

SEC 被设计成一个自治域的集合，可以向外扩展，会有非常大数量的自治域。每个自治域通过相同的网络模式进行平行管理，因此系统具有可伸缩的能力。在 SEC 调度内核支持下运行，是一个类似异步拜占庭容错的安全共识引擎，兼具一致性等

特点，而且在其严格的分叉责任制保证下，能够防止怀有恶意的参与者做出不当操作。采用 SEC 模式，区块链计算可以合并或分开进行，进而实现了负载均衡（load balancing）。

SEC 网络通过 DPOS 机制来运行众多区块链自治域。负责管理众多独立区块链（称之为“自治域”，参考路由协议）。自治域会不断地提交最新区块，这一点可以让自治域跟上每个节点状态的变化，之后信息包就会从一个自治域传递到另一个自治域，并通过发布梅克尔证明（Merkle-proof）来说明信息已经被传送或接收。这种机制叫做“自治域间通信”，或者简称为“Border Gateway Communication”机制。

任何区块都可以自行成为验证人，从而形成非循环图。SEC 自治域是独立的区块链，能够和其他自治域进行 BGC 信息交换。从 SEC 全网络的角度看，自治域是一种双链形成，它可以通过 BGC 信息交互进行 Tokens 和账户信息发送与接收。

设置自治域中心的信任验证人。虽然验证人出现重复而引起的攻击行为会导致 SEC token 数量减少，但是如果自治域中有超过三分之二的选票都出现拜占庭问题，那这个验证人就可以广告无效状态。其他自治域的验证人不会验证或执行提交到其它自治域的交易，SEC 的管理系统可能会通过改善协议，来解决自治域故障问题。比如：在检测到袭击时，可以将有些自治域发起的 Tokens 转移实现紧急中断。

(二) SEC 自治域间通信（BGC）

SEC 最关键的部分之一是跨域通信。因为在自治域之间可以存在某种信息交易，因此是可伸缩的区块链系统。

为了保证最小的实现复杂度、最小的风险和最小自治域架构束缚，这些跨域交易会有个发起方字段，用来辨别自治域的身份。跨链交易使用简单的队列机制解决，该队列用梅克尔树（Merkle tree）来保证数据真实。验证者的任务是把交易从发起自治域的出口队列转移到接受自治的入口队列。

现在我们来查看一个实例假如现在有两个 SEC 自治域，分别是“自治域 1”、“自治域 2”，自治域 1 内一个节点 A 和自治域 2 内节点 D 生成一个交易。为了能够让 Tokens 和信息从一个区块链节点 A 转移到另一个区块链节点 D，需要在接收方区块链节点 C 上发布一个证明，来明确发送方 A 已经发起了交易到指定地点。

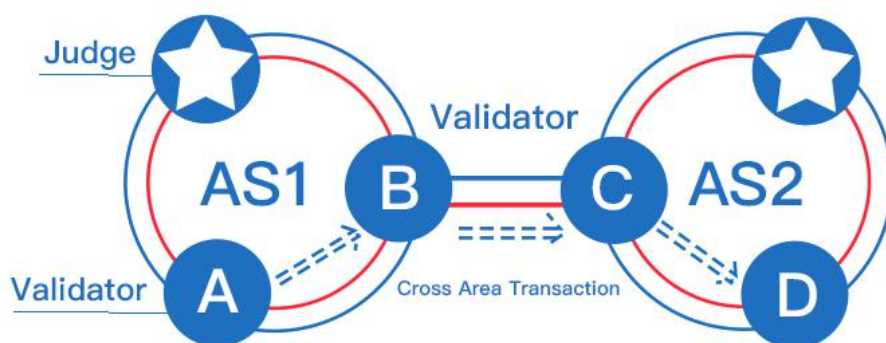


图 3 跨自治域交易示意图

SEC 的自治域可以在保持一致性的前提下，通过优先交易关系链，划分自治域加快交易，自治域域内因长期经常发生交易，因此双链账户信息和交易关系变动有限，进而实现交易的快速完成——针对双向订单交易，及 BGC（跨自治域通信）Tokens 与其他自治域的交易。

(三) SEC Structure 参与方

SEC 有三个基本的角色在维持：受托人 (Assignee)、法官 (Judge)、验证人 (Validator)。在交易信任关系上三者具有相同权限和功能，在打包利益和确权下，三者分工角色不同。

1、 验证人

验证人有最高权限，职责是在 SEC 自治域里打包新区块。验证人需要抵押足够的押金，且必须在高运算能力和高带宽的机器上运行一个节点的客户端。每个区块上，节点都必须准备接收一个已提交的新区块。这个过程涉及接受、验证、再发

布候选区块。验证人的任命是确定性的，但运作逻辑导致的结果实际上很难预测，进而提升了安全性。

不同自治域的验证人一旦都确定性地批准了自己所属自治域的新块，他们就必须开始更新交易队列的状态。也就是从一条自治域的出口队列转移到另一条自治域的入口队列，进而处理已批准交易集合、批准最终的区块、吸收自治域的最终状态。

在共识算法约束下，会惩罚一个没有履行职责的验证人。第一次错误，就会扣留他们的奖励，但如果是重复的错误会扣减他们的押金，会导致他们丧失全部的押金（一小部分烧毁，其余奖励给法官和诚实的验证人）。

验证人唯一有权限可以创建有效的自治域区块。

2、受托人

受托人有两个角色，第一个是受托人是帮助验证人制造有效的自治域内区块的群体。他们会运行一个特定自治域的全节点，他们有自治域全节点的必要信息，可以打包新块并执行交易；受托人群体为了获得更多手续费，竞争性地去收集交易信息，推动信任交易的产生，同样地，去中心化的提名人群体也会允许多个有抵押的参与者来协调和分担验证人的职责。这种能力保证了参与的开放度，有助于成为更加去中心化的系统。

第二个是，受托人为信任传递角色。受托人信息字段中自动 trust index，初始值为 1，当受托人完成交易 TI 值会增加，最高 100。同样如果未完成交易，或卖家售卖假冒伪劣或买家恶意投诉，则 trust index 会减少；当 trust index 减为 0，则账户禁用。Index 越大，根据交易额，交易提交的押金越多。

3、法官

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。法官及时举报并证明至少一个有抵押的参与方存在非法行为，他们就能获得奖励。为了预防由于私钥泄露给法官所导致的过度奖励。法官所

需要的资源相对较少，也没必要承诺稳定的在线时间和大的带宽。法官只需要提交很少的押金，这个押金用于预防浪费验证人计算时间和计算资源的女巫攻击。它是立即可以提现的，但如果监测到一个不当行为的验证人，可能会收获很大的奖励。

四、共识机制

我们选择使用以 DPoS 为基础的共识算法。

在共识上，在有任意网络缺陷的架构下，只要大部分验证人是诚实的，就能提供一种高效的容错算法，可以在大概率层面保证数据的真实性和准确性。

SEC 链在初始时刻即被创建，在应用场景中不断被分发。根据不同联盟链中需求定制平行链的细节功能和平行链所提供的服务和平行链 Tokens 具体信息，不同联盟链之间建立一部分同步共享账本。这些定制信息形成平行链的数据结构，以类似 SEC 交易记录的方式，被记账节点记录在当前时段的区块中。至此自治域将作为一条独立的区块链，记录自治域 Tokens 的交易。

（一）双链共识算法

通过团队成员研发生成的“ Ω 算法”，作为一种严格基于区块链的密码及共识基础而被开发，与现有算法所不同的是：对电商领域所需要的极速共识、安全性、超低算力需求，该算法均可满足。利用双线性映射函数的性质，在不泄露因变量的情况下来验证“函数”有效性，避免一个区块的生成者预测以后生成者的概率时候的天然优势的影响程度，而实际通过网络延迟（即牺牲速度）实现算法有效性。同时构建 DPoS 共识机制，同样通过密码学的方法，通过封装函数非规律性决定下一个区块的生成者，在不牺牲速度情况下，实现共识机制。

算法关键点：（1）为保证完全随机，在区块中引入 X block（第 X 个块）且仅当当前区块的潜伏者在整个网络中被揭晓时才能最终确认，从数学逻辑上阻断入侵阻断可能性。（2）同时构建并发机制，多个潜在的潜伏者所在的区块也完全独立，通过公网进行统一汇集，优先进行区块数据广播，之后进行揭晓环节，从而保证了

篡改失去意义。(3) 算法支持播放器更换机制,从而使任何节点都可以随时被其他节点接管,综合提升算法时效优势、提升经济性。

综上所述,Ω算法涵盖了如下优点:可控制的分叉风险、需要很少的计算量、节点离线容忍度扩容、单向不可逆密钥高安全级、复合验证投票机制。

(二) 权益证明

通过一个更新的股东权益证明(DPOS)结构,验证人严重依赖他们抵押进来的权益。现存验证人的权益会从他们离职的时候开始,这么长的押金冻结期是为了还能惩罚将来的不当行为,直到区块链周期性的检查点到来。不当行为会遭到例如减少奖励等的惩罚,如果是故意破坏网络的完整性,验证人将会损失部分或全部的权益,转移给其他验证人、信息提供者或全部权益持有者(通过烧毁)。例如一个验证人试图同时批准不同分叉上的两个分支(有时也被称为短程攻击),就会被后面的方法鉴别并遭到惩罚。

(三) 区块的打包方式

每条自治域采用不同的包块打包方式,通过BGC协议整合共识。共识完整机制之下,由主要节点进行记账,并用心跳机制保持共识的完整性。

(四) 轻客户端

Ω算法共识算法的好处之一就是它可以开发安全简易的轻客户端,这一点有助于成为手机端社交电商应用的理想工具。轻客户端必须同步运行区块头组成的链,并且找到工作量证明最多的那一条,而SEC轻客户端只需和验证组的变化保持一致,然后验证该交易中大部分的,来确定最新情况。

(五) 网络设计和考虑

我们会基于以太坊devp2p协议系列协议的延续,包含libp2p和IPFS标准,将有效改善隐私性、强健性、延迟及模块化。

在 SEC 网络中，我们专注解决电商交易信任问题，售卖产品的文字、图片或视频信息存储不做考虑，因此基于 devp2p 协议对 SEC 是足够使用的。当然在现在的网络架构和电子商务中，服务器或云服务器都成为垄断性能力，即使简单的云服务器使用，对于普通个体电商参与者都可能成为一种障碍。SEC 基金会，将关注 p2p 网络服务，去中心化算力项目等有助于降低个人搭建 web 应用的项目，当然卖家商品信息存储在中心化机房，并不影响 SEC 网络的使用。

五、账户管理与商业逻辑

(一) 账户管理

1、SEC 提供账户和功能

(1) 用户管理。用户管理主要解决用户身份到区块链地址的映射关系、用户隐私的保密性。

(2) 账户管理。账户管理负责用户的账户管理，包括账户的注册、登录、注销以及账户跟密钥的不相关性处理。账户注册时，将原来用户习惯的用户名、密码等身份信息映射到区块链地址。

(3) 密钥管理。在全托管的模式下，密钥管理系统负责用户密钥跟账户的关联、密钥安全管理和丢失找回。用户密钥在客户端生成，用户可以选择将密钥保存在密钥保险箱或者委托给关联账户的方式以便密钥丢失后找回。为了保证用户账户跟密钥关联关系可靠性，密钥管理系统将关联关系的签名采用多节点链式存储。

(4) 权限管理。权限管理模块负责用户账户、密钥系统、节点加入和退出、数据访问等权限的控制和管理。包括账户委托权限、节点共识权限以及用户数据访问权限等。审计权限是为监管机构提供审计的功能，对访问权限和数据范围做严格的控制，对共享账本上交易不相关性的用户可以做到用户关联。账户委托权限用来控制用户账户委托关系的访问控制。共识权限对参与或者新加入节点进行共识权限管理，访问权限用来管理客户端对区块链上的数据查询权限。

(5)用户信用风控管理。风控模块负责对区块链中用户交易行为进行风险控制，SEC 初始用户采用。

(二)创世用户和用户实例

SEC 网络创世用户均来自社区用户，采用交易方式进入网络，因此进入网络即有双方初步信任值为 1 的信任关系。

用户 A 在 SEC 用户界面设置一条收货后 7 天自动成交的自动合约地址，社交网络/web 电商网页发布产品信息，假设价格 158 元，并留下 SEC 自动合约地址。

陌生用户 B 看到后，手机扫描 SEC 自动合约地址，并付款。因两人并未产生过交易关系，因此肯定处于不同自治域。因此用户 B 通知自治域验证人 C，验证人 C 通过哈希表找到用户 A 所在自治域的验证人 D，并发出交易信息并更新记录。验证人 D 发出已付款交易信息到用户 A 的自动合约地址。

用户 A 看到合约地址状态变化后发货，并更新自动合约发货状态。用户 B 收到货后，可按照原路径更新状态信息，A 自动合约执行。B 没有操作情况下，7 天后 A 自动合约执行。通过自动合约和验证人执行担保交易。

交易完成后，用户 A 和用户 B 形成关系链，并收敛尝试建立自治域，如果网络中有路径符合收敛条件，则双方进入新的自治域，并广播交易信息。

如果用户 B 对该产品认定为商品假冒伪劣产品，向自动合约地址发出不信任后，用户 A 将扣除规定的部分货款，并扣减信任指数。信任指数降为 0，则永久性被网络禁用。

综上所述，该方案使得跨国界、跨平台、跨品类的 P2P 电商市场当中信任传递及社交分享得以实现。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。

该解决方案的第一阶段，我们将会在中国、德国、加拿大和泰国多个垂直商品领域、农业领域、跨境电商生态中落实技术应用，搭建一个完整的初始 P2P 电商信用案例。

六、治理架构

SEC 基金会

SEC 基金会是专门为支持基于 SEC 平台的电商应用项目而创办的一个非盈利性组织。

（一）SEC 基金委员会治理

SEC 基金联盟委员会采用联盟轮值主席方式开展工作，每两年由投票选出轮值主席，轮值主席任职周期为一届、且只能连任一次；SEC 基金联盟委员会设立数个管理中心包括：区块链技术开发中心、区块链商业应用中心、财务管理中心、风控管理中心 和综合事务管理中心。

（二）资金来源与资金管理

1、维持 SEC 项目运作的资金主要来源于原生资产 SEC 币的分批次、风险投资和联盟链会员会费、捐赠等，在需要的时候部分 SEC 会转换为其他形式权益资产，用于项目运营。

2、SEC 通过私募筹集到的加密数字资产及原生资产，将采用冷钱包或转换成其他资产的形式保存，并由专门人员进行资产管理，必要情况下考虑聘请加密资产管理服务商提供资金管理服务，同时可采用多重签名的形式管理私钥。

3、财务管理方面。SEC 基金会财务管理的原则：统筹管理，综合评估使用绩效；勤俭节约，最大化实现财务使用价值。

SEC 基金会资产管理纳入全面预算管理，根据实际运营情况，编制财务收支预算。

年度财务收支预算报自制委员会审议，月度财务预算由执行委员会审议，财务管理中心负责编制和执行，每季度进行披露。

财务报告披露渠道：官网 <https://SECblock.io/>。

SEC 基金会将引入第三方审计，监督项目的财务运作，进行资金审计编制审计报告，审计报告将在年度信息披露公告中体现。并将在每个季度结束后的两个月内披露季度报告，每个会计年度结束之日（每年 12 月 31 日）起三个月内编制并披露年度报告，报告内容包括但不限于 SEC 项目的技术开发里程碑及进度、应用开发里程碑及进度，数字资产管理情况，团队履职情况，财务情况等。

（三）进度及信息披露

SEC 项目发起团队承诺本着勤勉尽责、诚实信用的原则管理和运用项目资金。同时为保护投资人利益，加强 SEC 的管理和高效使用，促进 SEC 项目的健康发展，SEC 项目设置信息披露制度。

SEC 基金会将聘请知名的律师事务所，作为 SEC 项目法律顾问，为 SEC 项目提供数字化资产交易结构设计、运营合规化、法律风控体系设计、海外法律咨询等方面提供全面的法律服务。

SEC 会不定期披露 SEC 项目重要的临时信息，包括并不限于重大合作事项、核心团队成员变更、涉及到 SEC 的诉讼等。希望能通过自身的示范作用，规范私募项目数字资产的管理，增加区块链行业的自律性，提升区块链加密数字资产管理的透明度，维护好区块链行业的长远发展。

SEC 将在官网 <https://SECblock.io/> 披露信息报表。

七、团队介绍

储炆 (Collin Chu)：曾任世界第三大 FinTech 公司项目负责人，20 多年中国及北美银行应用系统、金融软件系统设计和研发经验，新加坡南洋理工大学计算机博士。

陈思宇：毕业于加州大学洛杉矶分校 (UCLA) 计算机系，在亚马逊、百度和独角兽 Procore Technologies，负责过机器学习，大数据挖掘和计算机视觉自动识别相关项目，热爱区块链项目开发。

顾浩 (Oliver Gu)：北美电商论坛主席、国际产能合作中心共同创建人、加中电商高科技联盟共同创建人、加中电子商务高科技峰会共同主席，美国麻省 Bridgewater 州立大学电脑科学硕士。

刘莹 (Rain Liu)：安大略省杰出女性奖获奖人，中加电子商务科技协会会长，Sun 与 IBM 认证加拿大跨国公司高级工程师，加拿大国家电视台、加拿大中文电台、福建漳州电视台前节目主持人兼策划。

八、投资人和顾问

李勍然：SEC 中国区技术负责人，卖座网社交电商 CEO，国内最早期实时 linux 研发者，互联网连续创业者。曾就职中国电信集团，INT 物联网区块链项目团队成员。

陈应魁：卖座网创始人，腾讯早期员工，天使投资人。

王星：卖座网联合创始人，腾讯前 100 名员工，天使投资人。

谭磊：区块链和大数据挖掘专家，北美区块链协会 NASA 发起人、微软总部工作 13 年，美国杜克大学硕士，《区块链 2.0》、《社交电商》等著作和译著。

王勇：国家千人计划专家，加拿大达尔豪斯大学博士学位，CFA 和 FRM 证书持有人，曾任加拿大皇家银行风险部董事总经理。著有金融风险管理专著及风险管理和衍生产品，区块链等译著；同时担任多伦多大学罗特曼管理学院学术顾问，约克大学客座教授。

肖敏：经纬创投合伙人。历任拼音加加总经理，百度 TV 产品经理，天极传媒 IT 事业部总经理，目前主攻互联网、电子商务、无线、软件等领域的投资。

山峰：SEC 中国区电商负责人，区块链资深投资人，电商运营专家，曾在阿里巴巴 B2B 事业部任职，后任阿里服务商培训部、运营部、产品部负责人，深入电商领域九年，服务对接电商企业 5000 家以上。

赵亚甫：广东卓泰投资管理有限公司风控总监；

葛磊：广东广信君达律师事务所合伙人。

九、SEC 分配计划

SEC Tokens 私募方案

关于 Tokens 预售

区块链技术的蓬勃发展也让越来越多的人认识到了加密数字资产的价值。各种虚拟技术的推陈出新，让开发者们以更加灵活的方式构建智能生态体系，而将底层区块链技术具象化的 Tokens，也进一步提升了平台的管理效能；其中，基于区块链技术的电商基础应用，内部信息交互、确定性、时间等内容，通过加密 Tokens 形式解决去中心化信任的问题。

面向电商领域应用的 SEC，对于鼓励投资者参与社区建设、保证平台的有效运行、产生效益进一步向投资者分红等，Tokens 都起到了关键性作用。同时，Tokens 作为项目获取早期开发、项目运营的资金，将为项目的成功带来坚实保证。

此类创新投资及筹资机制已经被广泛应用于区块链产业，是截止目前最为具备可行性及高效的解决方案。

SEC 初始 Tokens 私募计划

SEC 项目持续运作的资金需求为长期均衡分布，本着可持续性、可扩展的方式推进；目前本项目已受到部分优质投资人青睐，并已部分成为基石级投资者。私募阶段，创始团队及战略投资方将释放少量 Tokens；而在项目发展中后期，将更多侧重投资者多元化的发展战略，拟引进包括但不限于电商从业者、风投、虚拟数字产业研发机构及研发人员、个人投资者等。

分配原则

SEC Tokens 的持有者是 SEC 项目最早期投资者。为保护早期支持者的投资利益和项目的健康发展，本次 Tokens 释放小部分币量，其他 Tokens 将被冻结，冻结的系统 Tokens 将在长达 3 年时间内逐步释放，充分保障投资者的利益和投资回报。

SEC Tokens 总量 15 亿枚，但同时设置商家付费购买的增发机制，鉴于电商网络呈现高速增长，那么在商家出资购买情况下，可以按照市场实时价格进行增发，不稀释现有 Tokens 的内涵价值；此次 Tokens 预售量预计在 3 至 6 亿枚。凭借市场效能最高的运作模式，SEC 的早期支持者将有机会在初期参与本项目，投资者参与项目完成 SEC Tokens 的置换，而我们所取得的数字货币将用以支持 SEC 项目的发展。

SEC Tokens 私募兑换基准与方式

此次投资采用 ETH 作为兑换基准，兑换的基准最终以 Tokens 预售结束后一天的 13 时 Bitfinex 的算数平均价为准。募集工作 2018 年 1 月 22 日启动，一个月周期作为募集时间；若提前募集完成，则提前封盘，具体以官网公告为准。

SEC Tokens 分配

SEC 的原生 Tokens 分配方案与基准如下：

表 1 SEC Tokens 分配方案

类型	Tokens 数量	占总量占比	总量占比	说明
天使投资	105,000,000	7%	0.40	天使 50%释放，50%锁定 3 个月；私募无锁定期；均采用白名单制
私募	495,000,000	33%		
基金会 (技术迭代)	150,000,000	10%	0.10	财务披露
商务/战略	300,000,000	20%	0.20	其他私募以及机构融资
创始团队	150,000,000	10%	0.10	3 年成熟期
投资，合作伙伴及社区	300,000,000	20%	0.20	
	1,500,000,000	100%		总量

注：1ETH=11000 个 SEC

表 2 SEC Tokens 软顶和硬顶

类型	软顶	硬顶
私募	19,800 (ETH)	39,600 (ETH)

注：天使轮按照 7%募集

十、资金使用规划

表 3 SEC Tokens 及资金使用规划说明

比例	分配方案	说明
20-40%	天使投资与私募	天使与私募采用邀请制，会提供一定折扣，但存在锁定期要求。
	私募，早期投资人、机构以及早期为 SEC 发展提供资源和技术支持的人	
10%	SEC 项目基金会	用于项目开发，赏金计划等，初始释放 20%，后续每 365 天后释放 33.3%，共分 3 年解冻
10%	创始团队	创始团队和开发团队，初始释放 25%，后续每 365 天后释放 25%
20-30%	投资机构，合作伙伴及社区	初始锁定（其中社区推广、社群运营与奖励，不锁定）
20-30%	其他私募、商业拓展/战略合作	SEC 将会考虑在全球部分国家进行私募；品牌建设、战略合作、挂牌费用等，根据项目进程释放，需提前公示

十一、技术部署以及落地应用

项目计划概述：项目将于 2018 年初完成资金筹集工作，预计在本年度陆续发布具体应用场景及新的项目合作方，此项应用将承载电商行业发展革新之重任，将从电商行业发展红利当中博取利润。

项目对应的市场需求迫切，团队有丰富的互联网和电商运营经验与资源，预计 2019 年 6 月成为用户数量最大的区块链应用之一。目前的项目时间计划如下，因区块链技术方面有一定时间风险，因此准确的技术发布时间会有调整，相应的商务落地应用也会相应调整，以官网公布为准：

表 4 项目初期时间路线图

2017 年 5 月	完成主链的公式算法以及信任算法模型
2017 年 7 月	卖座网社交电商业务模式测试
2017 年 12 月	完成主链网络架构方案设计
2018 年 2 月	主链开发启动
2018 年 3 月	与卖座网社交电商项目技术合作
	3.25 深圳社区千人分享会
2018 年 4 月	基金会技术入股新加坡通证科技，为企业客户提供基于主链的社交电子商城开发
	主链开发底层对等网络协议集，实现专用梅克尔树库及随机数算法
2018 年 5 月	菲律宾马尼拉项目推广会
	完成节点群落分组算法和轮循机制
2018 年 7 月	法国巴黎、德国斯图加特项目推广会
2018 年 8 月	完成群落内 POW 算法
2018 年 9 月	完成客户端钱包开发
2018 年 10 月	全球部署测试节点，完成客户端钱包功能更新
2018 年 12 月	测试网（交易记账和转账功能）上线、测试
2019 年 1 月	SEC 测试网络上线，同步上线浏览器、客户端全节点钱包
2019 年 3 月	Web 钱包、安卓、苹果手机端钱包开发完成

2019 年 4 月	测试网升级、浏览器及各终端钱包优化
2019 年 4 月	主网上线
2019 年 5 月	蜂巢全节点钱包上线，发展节点
2019 年 6 月	生态开发者将推出去中心化的数字货币 OTC 交易应用, 8 月支持 BTC 交易
2019 年 7 月	基金会开发团队升级完成 demo 经济模型，推出社交电商应用
2019 年 8 月	一键定制主链功能开发完成
2019 年 9 月	生态开发团队的众筹投资协作应用
2019 年 12 月	生态开发团队基于主链的直播应用

十二、SEC 媒体与社群

表 5 SEC 媒体与社群列表

名称	地址
官方网站	https://SECblock.io
Telegram 英文群	https://t.me/joinchat/HszcVKwZXyl5LbH8Ywx8Q
Telegram 中文群	https://t.me/joinchat/HszcUiWaWtR5pPmOhDPwg
Twitter	https://twitter.com/SECblock
Facebook	https://www.facebook.com/SecChain
Github	https://github.com/SECblock
微信公众号	SECblock
新浪微博	https://weibo.com/SECblock
Slack	https://secblock.slack.com/
Reddit	https://www.reddit.com/user/SECblock

十三、项目附则

免责声明

本文档只用于传达信息之用途，并不构成买卖 SEC 公司股份或证券的相关意见。以上信息或分析不构成投资决策，或具体建议。

本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖、任何形式证券的行为，也不是任何形式上的合约或者承诺。

SEC 明确表示相关意向用户明确了解 SEC 平台的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意为此承担一切相应结果或后果。

SEC 明确表示不承担任何参与 SEC 项目造成的直接或间接的损失，包括：

- (1) 本文档提供所有第三方信息的可靠性
- (2) 由此产生的任何错误，疏忽或者不准确信息
- (3) 或由此导致的任何行为

SEC Tokens，是一个在 SEC 平台使用的数字加密货币。在写这段文字时，SEC 币尚且不能用来购买相关物品或者服务。我们无法保证 SEC 币将会增值或贬值，那些没有正确使用 SEC 币的人将有可能失去使用的权利，甚至会有可能失去他们的 SEC 币。

SEC 币不是一种所有权或控制权。控制 SEC 币并不代表对 SEC 或 SEC 应用的所有权，SEC 币并不授予任何个人任何参与、控制、或任何关于 SEC 及 SEC 应用决策的权利。

风险声明

- 1、证书丢失导致的丢失 SEC 币的风险

购买者的 SEC 币在分配给购买者之后会关联到购买者的 SEC 账号, 进入 SEC 账号的唯一方式就是购买者选择的相关登录凭证, 遗失这些凭证将导致 SEC 币的遗失。最好的安全储存登录凭证的方式是购买者将凭证分开到一个或数个地方安全储存, 而且最好不要储存在公开场所或者会有陌生人流出现的地方。

2、以太坊核心协议相关的风险

SEC 币基于以太坊协议开发, 因此任何以太坊核心协议发生的故障, 不可预期的功能问题或遭受攻击都有可能对 SEC 币或者 SEC 应用以难以意料的方式停止工作或功能缺失。关于以太坊协议的其它信息 <http://www.ethereum.org>

3、购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥, 即有可能直接控制购买者的 SEC 币, 为了最小化该项风险, 购买者必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

4、司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象, 如果监管主体施加影响则 SEC 应用或 SEC 币可能受到其影响, 例如法令限制使用, 销售, 电子 Tokens 诸如 SEC 币有可能受到限制, 阻碍甚至直接终止 SEC 应用的发展。

5、SEC 应用缺少关注度的风险

SEC 应用存在没有被大量个人或组织使用的可能性, 这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用, 这样一种缺少兴趣的现象可能对 SEC 币和 SEC 应用造成负面影响。

6、SEC 相关应用或产品达不到 SEC 自身或购买者的预期的风险

SEC 应用当前正处于开发阶段, 在发布正式版之前可能会进行比较大的改动, 任何 SEC 自身或购买者对 SEC 应用或 SEC 币的功能或形式(包括参与者的行为)

的期望或想象均有可能达不到预期，任何错误地分析或者底层设计的改变等均有可能导致这种情况的发生。

7、黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断 SEC 应用或 SEC 币功能的可能性，包括服务攻击，Sybil 攻击，游袭，恶意软件攻击或一致性攻击等。

8、漏洞风险或密码学科突飞猛进发展的风险

密码学的突飞猛进的发展或者其他相关科技的发展诸如量子计算机的发展，或将破解的风险带给加密 Tokens 和 SEC 平台，这可能导致 SEC 币的丢失。

9、缺少维护或使用的风险

购买 SEC 币应该被认为是一种对于下一代电商应用开发的支持和投资，而不是一种投机行为。虽然 SEC 币在一定的时间后可能会有相当的市场价值，导致早期投资者产生较大的收益，不过如果 SEC 平台缺少维护或没有足够的应用，这种升值并没有太多的实际意义。

10、未保险损失的风险

不像银行账户或其它金融机构的账户，存储在 SEC 账户或以太坊网络上通常没有保险。任何情况下的损失，将不会有任何公开的组织或者个人为你的损失承保。

11、应用存在的故障风险

SEC 平台可能因各方面的原因故障，无法正常提供服务。

12、无法预料的其它风险

密码学 Tokens 是一种新兴的技术，除了本白皮书内提及的风险外，此外还存在着一些区块链业内以及 SEC 团队尚未预料到的风险。