CoinEx 智能合约链

白皮书

CoinEx Smart Chain

目录

动机 01

CSC简介 01

设计原则 02

共识与验证节点 02

- 基于权益的质押 (Proof Of Staked) 03
- 验证节点 03
- 安全 04
- 收益 04

代币经济学 04

- 原生代币 04
- 其他代币 05

展望 05

动机

自 2013 年 Vitalik Buterin 首次提出以太坊， 自此智能合约进入人们的视线。从以太坊诞生至今八年间，智能合约诞生、发展，逐步繁荣，吸引了大量关注，如今以太坊已是最为成功，最为广泛使用的智能合约平台。随着各种 DApp 应用，尤其各种 DeFi 应用层出不穷， 以太坊低吞吐量， 低交易数及高额手续费等问题也进一步凸显， 即“慢”且“贵”。目前， 有不少平台在解决以太坊“慢”和“贵”等方面做了一些工作，但在拥有较高的交易吞吐量及较快的交易速度的同时，都或多或少在去中心化上做了一些妥协。

CoinEx 致力于为区块链世界构建基础设施，秉承去中心化、无需许可原则，推出 CoinEx 智能合约链 （简称： CSC）。CSC 在支撑高性能交易的基础上， 实现对 EVM 的完全兼容； 同时采用 pos 模式，任何人只要愿意，都可以通过质押进入排行成为节点，无需任何许可。

CSC简介

CoinEx 智能链： CoinEx Smart Chain（CSC）是 CoinEx 公链团队为去中心化金融打造的一条去中心化、高效率公链，可为开发人员提供高效且低成本的链上环境，以运行去中心化智能合约应用程序 (DApps) 和存储数字资产。

CSC 具有以下特点：

（1）完美兼容以太坊生态： CSC 基于以太坊虚拟机（EVM）构建， 开发者可以使用成熟的开发工具，轻松的移植 Dapp 到 CSC 上，用户也可轻松接入 CSC 网络。

（2）极高效率和低交易费： CSC 使用 POS 共识协议，实现秒级出块时间，支持

极高的 TPS，同时保持低廉的交易费。

（3）出块节点无需许可： CSC 最多支持 101 个出块节点， 根据 CET 质押数量排序确定，无需中心化机构审核，网络更加去中心化。

设计原则

CSC 的设计遵循以下原则：

1. 以太坊兼容：

以太坊是第一个实用的、被广泛使用的智能合约平台。现在提到智能合约，第一反应就是以太坊。以太坊已经有相对成熟的应用、社区及工具链，可以说是一个相对完整的生态。 CSC 选择与现有的以太坊兼容， 这意味着以太坊上几乎所有的 DApp、 生态系统组件和工具都可以直接或者只需要做很小的更改就能迁移到 CSC。

2. 基于 POS 共识：

基于权益质押（PoS）的共识更环保， 在确保比 PoW 共识具有更好的性能（即出块时间短，交易处理容量高）的情况下，便于社区灵活管理，同时不失去中心化的原则。

共识与验证节点

基于以上设计原则，CSC 的共识协议是为了实现以下目标：

1. 出块时间比以太坊时间短，约 3 秒

2. 尽可能与以太坊兼容

3. 基于质押的链上治理机制
4. 支持最多 101 个出块节点，节点无需许可

基于权益的质押 (Proof Of Staked)

尽管工作量证明（PoW）已被证明为实现去中心化网络的实用方案，但它对环境并不友好，而且还需要大量参与者来维护网络安全。

以太坊及一些其他网络在不同的场景中使用权威证明（PoA）或其变体，包括测试网络和主网。PoA 为 51% 的攻击提供了防御，更有效的防止一部分拜占庭节点作恶。但 PoA 协议因不如 PoW 去中心化而被批评，因为验证人拥有极大的权力，并且容易产生腐败和遭受安全攻击。其他区块链，如 EOS、Cosmos，引入了不同类型的委托权益证明（DPoS），允许代币持有者投票选举验证人节点。它让网络更加去中心化，有利于社区管理。

结合 PoS 及 PoA 的特点，CSC 采用 PoS 作为底层共识机制，并结合 PoA 的出块机制，采用的方案为：
1. 区块是由有限数量的验证节点生成的
2. 验证节点轮流以 PoA 方式生成区块，即验证节点的出块概率是一样的，类似于以太坊的 Clique 共识引擎
3. 验证节点集合是基于质押的链上治理选出和淘汰，而无需任何许可
4. 任何人都可以给自己信任的节点进行质押

验证节点

在网络启动的创世块阶段，一些受信任的节点将作为初始验证节点集合运行。为了进行权益质押管理，网络启动之后会部署验证节点管理系统合约。开始出块后，任何人都可以通过调用系统合约质押 CET 参与竞选验证人。

根据质押数量， 排名前 101 的节点将成为下轮验证节点集合， 这样的选举和淘汰每 200 个块进行一次。按 3 秒出块时间计算，验证节点将每 10 分钟更新一次下轮验证人集合。

安全

由于采用 PoA 的出块机制，网络超过一半的 N/2+1 验证人是诚实可信的，网络通常可以安全、 正常地工作。CSC 的可用性依赖于 PoS 共识中验证节点集合中的每个节点，当轮到其出块时，他们能够及时生成区块。

但由于一些原因，验证节点可能错过出块时机，比如硬件、软件、配置或网络方面等问题。这种不稳定运行将损害网络的性能， 并给系统带来更多的不确定性。为了保证网络的稳定性，CSC 引入惩罚机制，内部维护惩罚合约，负责记录每个验证节点错过的区块。一旦指标超过预定义的阈值，该验证节点将被罚没部分质押资产。

收益

验证节点的收益主要来源两个方面： 挖矿奖励与每个区块内的交易手续费。收益根据验证节点质押占总质押的比例进行分配。

由于验证节点是以相同的概率轮流生成区块（如果它们保持 100% 在线），验证节点的收益只与其质押 CET 占比有关。

代币经济学

原生代币

CoinEx Token （CET） 作为 CoinEx 业务生态的用户增值服务权益体系， 是 CoinEx 智能合约链的原生代币。它于 2018 年 1 月推出， 曾基于以太坊 ERC20 协议发行，在 CSC 主网上线后将迁移至 CSC 上。

CET 在 CSC 上运行的方式与 ETH 在以太坊上运行的方式相同，主要作用为：

1. 验证节点的出块奖励
2. 支付在 CSC 上转账与合约调用的燃料费
3. 支付在 CSC 上部署智能合约的手续费
4. 对选定的验证节点进行权益质押

其他代币

由于 CSC 是兼容以太坊的， CSC 上支持的 ERC20 合约被称为 “CRC20” 合约。CRC20 通过添加更多的设置来“增强”已有协议， 这些设置可以对外披露更多的信息，比如代币单位、精度。

展望

对于 CoinEx 智能链的未来， 很难在当下就盖棺定论， 因为它一直在升级进化。CoinEx 致力于产品开发和服务， 为区块链世界的基础设施做出自己的贡献， 而 CSC 只是其中的一小步。

未来 CSC 将在提供针对以太坊及其未来升级版本的兼容性的同时， 不断提升区块链的吞吐能力、优化更易用的区块链客户端、完善更安全的托管服务和更全面的代币跨链服务。同时丰富的去中心化应用也是我们未来将大力支持的方向。