虎符智能链：易扩展、高性能公链

背景

交易所是天然的区块链世界的枢纽，不同链的资产通过中心化的方式进行着极高频率的交换。对比于挖矿，ICO 以及其他投资机会，早期参与的用户都是通过中心化的交易所接触到区块链世界。随着区块链基础设施的完善，公链上的应用渐渐成为区块链入门的第一站。

中心化的交易所在交易环节中是一个不可替代的角色，基于交易所的流量能够自成一套生态体系。但是这种体系的生态是封闭式，无拓展性的。而作为开放式的以太坊，其生态土壤异常繁荣，项目方和用户都可以无授权匿名的进入区块链世界，公链的拓展性和开放性给予了项目本身以极大的未来发展空间。币安于 2020 年 9 月 1 日上线币安智能链，发展到现在只有短短不到一年时间，生态繁荣度已经有赶超以太坊的趋势。

虎符智能链介绍

HSC 是一条去中心化高效节能公链，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。

HSC 是虎符集团立足区块链生态资源，基于虎符技术和新项目挖掘优势，构建的开放友好区块链平台。HSC 生态联盟为多链 Dapp 提供全方位支持服务，帮助开发者更好服务用户需求，提供低成本与高效能并存的优质链上体验。

HSC 采用 PoSA 共识机制，每个参与节点拥有相同的权利，它可以让开发者自由构建去中心化应用，包括 DeFi 产品、DAPP、数字资产等。此外 HSC 通过跨链模块，可以简单高效地实现各区块链的价值互联互通，从而共同构建生态系统和增值系统。

HSC 旨在促进基于区块链技术的大规模商业应用程序的开发，HSC 生态联盟共建开放共生生态，致力于拓宽区块链世界并带来更加完整的生态闭环。

HSC 生态

虎符智能链是一个规模庞大的分布式操作系统，全世界范围内有成千上万的节点平稳地运行在遍布全球的服务器和终端之上。虎符智能链的强大离不开应用软件的支持，虎符智能链生态的繁荣离不开社区开发者的追随。虎符生态系统中拥有包括 DeFi、DAPP、NFT 等板块在内的众多优秀的应用。如钱包、区块链浏览器、DEX、借贷、预言机、NFT 交易市场等。

HSC 生态共建计划

生态资本

虎符联合联盟伙伴设立 HSC 生态资本，为潜力项目注资、提供流动性等支持，在联盟生态实现资本利得，再次投资 HSC 生态，实现商业闭环。

生态联盟

虎符生态联盟伙伴包括但不限于交易所、钱包、资本、媒体、项目社群等区块链行业伙伴，旨在为 HSC 开发者提供项目全生命周期的全方位扶持，助力项目成功。

Hoo Smart Chain（HSC）设计逻辑

虎符智能链采用高度抽象的模块化设计思路，将系统划分为基础网络、数据库存储、共识算法、交易处理机、虚拟机、应用层接口等几个核心模块。

Hoo Smart Chain 公链上线后，任何开发者都可以便捷的在 HSC 链上构建去中心化项目，另外 HSC 后期会逐步开放若干创新性的服务。

设计逻辑

1、从技术上来讲，HSC 不属于二层解决方案，是以太坊的侧链。大多数 HSC 的技术功能以及业务功能由 HSC 团队开发。

2、可兼容包括以太坊、BSC、HECO 等当前主流公链。以上公链具有相对成熟的应用以及社区。因此行业内的大多数成熟的 DAPP、生态系统组件和工具可以和 HSC 相适配。HSC 节点将进行硬件规范以及 HSC 的功能运行。

改进方案

根据当前行业面临的问题，HSC 将在以下几个层面进行改善
1、区块确认 3 秒，比包括以太坊、BTC 在内的主流区块链都快
2、HSC 的手续费用充当区块奖励，手续费用以 HOO 结算和支付。
3、引入 Staking 机制，设立 HSC 联盟支持项目方和开展节点竞选。

Hoo Smart Chain（HSC）特点

共识机制：PoSA
TPS：500+
出块时间：3 秒

特点：

1、高吞吐量
高吞吐量是通过改善 HSC 中的 TPS 实现的，HSC 区块确认时间为 3 秒，日常使用实用程度已经超过比特币和以太坊。
2、可扩展性
基于良好的可扩展性和高效的智能合约，应用程序可以在 HSC 中有更多部署方式，HSC 可以支持大量的用户。
3、高可靠性
HSC 具有更可靠的网络结构，用户资产，内在价值，并且更高程度的分权化共识带来了改进的奖励分配机制。

PoSA

共识机制种类大不相同，包括 Proof-of-Work（PoW）、Proof-of-Authority（PoA）、Proof-of-Stake（PoS）。PoW 通过算力进行挖矿来维护网络，PoA 采用验证人机制，不过这被一部分人认为 POA 去中心化的程度较低。HSC 将采用的 PoSA 共识机制，此机制融合了 PoA、PoS 的特点，其中：

1、验证者数量有限，区块由一定数量的验证者验证后产出

2、验证者轮流产生区块，类似于 PoA 的产生方式

3、可以通过 Staking 成为验证者参与 HSC 的治理

跨链技术

跨链技术原理的利用对于区块链行业至关重要，通过 HSC 跨链技术可以使用户资产自由流通，优势包括：

1、用户可基于 HSC 搭建数字资产、去中心化金融产品

2、HSC 链上项目、资产可自由稳定地流通、并且比当前行业内的各大公链更加高效、便捷、以及成本低廉。

3、HSC 可承担区块链资产中转站的角色，通过资产跨链桥，将各公链资产映射到 HSC，在链上锁定资产后，在 HSC 生成对应数量的 Token

虎符虚拟机（HVM）

虎符智能链实现的虚拟机全面兼容以太坊虚拟机，方便开发者移植现有的 DAPP，不仅降低了开发者的学习成本，并且由于虎符智能链 PoSA 共识算法天然的优势，大幅提高了 DAPP 的运行效率，同时运行成本大幅降低。

虎符智能链的虚拟机还进行了诸多优化，使得 DAPP 的运营成本大幅降低，同时开发了许多新特性来支持智能合约的业务逻辑，比如在智能合约中支持批量验签、在智能合约中支持合约地址的判断等。

1、轻量级

HVM 采用轻量级的虚拟机构架，旨在节省运行空间，减少资源耗费及保证系统性能。

2、稳定、安全性

HVM 采用了严谨的设计规范，低粒度的底层操作码，保证了每个计算步骤的精确性，最大程度消除产生歧义的空间。 同时出于安全性的考量，HVM 的转账与运行合约均不需要消耗代币，只会消耗带宽，避免了针对类似以太坊 gas 消耗模式的攻击。在保证了每个操作计算步骤的确定性的同时，也保证了带宽消耗的稳定性。

3、兼容性

目前，HVM 能完美兼容以太坊 EVM，并在未来兼容更多主流的 VM。因此，以太坊上的智能合约，能直接运行到 HVM 上，无缝对接现有的开发者生态，提高开发者的开发效率。开发者无需学习新的编程语言，就能用 Solidity 等主流编程语言在熟悉的 Remix 环境中进行智能合约的开发、调试、编译，将极大缩减开发成本。

4、开发人员友好性

HVM 的带宽消耗模式减少了合约的开发成本。让开发者可以把更多精力放在合约代码的逻辑本身。同时，HVM 提供了对开发者友好的一站式的部署、触发、查看智能合约的接口。

模型设计与机制

账户模型

HSC 采用账户模型。账户的唯一标识为地址 address，对账户操作需要验证私钥签名。项目方可以发布并创建智能合约，也可以调用他人发布的智能合约，也可以对节点进行投票等等。HSC 所有的活动都围绕账户进行。

资源模型

虎符智能链设计了一套完善的资源模型，并支持资源模型参数的动态调整，这是一个非常优秀的反馈调节机制，比如当链上交易繁忙的时候，交易手续费用使用费用会变的较高，当空闲时，这些资源的成本会随之降低。另外还为用户设置一定量的免费资源配额。
同时支持用户通过冻结 HOO 的方式来获取相应数量的投票权，用户通过为节点投票可以获得相应的奖励。

链上治理和投票机制

虎符智能链设置了科学高效的激励机制，促进区块链的自我繁荣，节点有权利生产区块，打包交易，并获取相应的区块生产激励，同时节点还可以获得选票奖励。

系统参数可以通过社区的治理进行调控，包括：
1、HSC 系统合约的参数都是灵活的，如跨链转移费用，中继器奖励金额等，这有利于生态的良好运行
2、HSC 上的 Stake / Slash / Oracle 模块的参数
所有这些参数由 HSC 验证程序集根据其 Staking 通过提议投票过程一起确定，这样的过程都将在 HSC 链上进行。

治理设计原则
1、统一的界面，对这些参数感兴趣的合同仅需要实现相同的接口。
2、可扩展，添加新的系统合同时，无需修改任何其他合同。
3、失败容忍度，验证者可以投票跳过错误的建议并继续。
4、多路复用，现在我们使用参数 gov，但是将来会有更多的治理功能。

投票流程：
1、选票
HSC 中设定持有 HOO 就可以拥有选票的权利。
2、投票过程
HSC 设定对候选人的投票是一笔特殊类型的交易，节点可以通过生成一笔投票交易对候选人进行投票。
3、统计票
每个维护期内，统计一次候选人的票数，将获得票数最多的候选人作为下一个出块周期的记账人。

激励机制

为了保证区块链系统安全高效地运行，虎符智能链设定激励模型用于鼓励更多的节点加入到 HSC 网络中，从而扩大网络规模，对于记账人当他们完成出块任务，给予相应的 HOO 奖励。HSC 设定 witness 每生产一个被固化的区块，就会获得一定的 HOO 奖励；对于所有记账人，每个 Epoch 的维护期会依据得票率的多少分配固定的奖励。并且激励的数量是透明的，激励的发放过程是完全去中心化的。

代币经济

Hoo Token

HOO 是 Hoo Smart Chain 的原生资产，HOO 在 HSC 链上的作用相当于 ETH 在以太坊上的作用。不过，HOO 在 HSC 上流通过程中，并不会像以太坊链上一样需要消耗巨额的手续费。

HOO 在 HSC 上的功能包括但不限于
1、HSC 手续费
2、通过质押 HOO 提供流动性获得收益
3、作为跨链质押资产

HSC Token 标准

HSC token 是通过 HSC 链上发行的标准代币。HSC 完全兼容以太坊 Ethereum、BSC、HECO 标准，因此 HSC 链同样可支持 ERC20 Token、BSC Token、Heco Token。用户可在虎符交易所内部或者 HSC 跨链桥进行链间互换。

共识机制

HSC 采用 PoSA 共识机制，具有交易成本低、交易延时低、交易并发高等特点，支持最多 21 个验证人节点；

名词解释

验证人：负责对链上交易进行打包出块；
活跃验证人：即当前负责打包出块的一组验证人，上限为 21 个。
Epoch：以区块为单位的时间间隔，目前 HSC 上 1epoch = 200block，每个 epoch 结束的时候，区块链会与系统合约交互，进行活跃验证人更新；

系统合约

HSC-contracts
目前验证人的管理，均由系统合约完成，目前的系统合约有：
Proposal 负责管理验证人的准入资格，管理验证人提案和投票；
Validators 负责对验证人进行排名管理、质押和解质押操作、分发区块奖励等；
Punish 负责对不正常工作的活跃验证人进行惩罚操作；
区块链调用系统合约：
每个块结束的时候，会调用 Validators 合约，将区块中所有交易的手续费分发给 active validator;
发现 validator 没有正常工作的时候，会调用 Punish 合约，对 validator 进行惩罚；
每个 epoch 结束的时候，会调用 Validators 合约，根据排名，更新 active validator；

质押

任何账户，都可以对 validator 进行任意数量的质押操作，每个 validator 的最小质押量是 100000HOO。
如果想取回已质押的 HOO，需要按照如下操作进行：
发送调用 Validators 合约，发送针对某一个 validator 的解质押(unstake)的声明交易；
等待 86400 个块之后，调用 Validators 合约，发送提取质押(withdrawStaking)的交易，将所有在此 validator 的质押取回；

惩罚措施

每当发现验证人没有按照预先设定进行出块的时候，就会在这个块结束时，自动调用 Punish 合约，对验证人进行计数。当计数达到 24 时，罚没验证人的所有收入。当计数达到 48 时，将验证人移除出活跃验证人列表，同时取消验证人资格。