Aurora（AOA）极光链白皮书

摘要

Aurora（AOA）极光链——采用 DPOS+BFT 共识机制与光速合约，如同来自遥远的 “太阳之风”，链接游戏、大数据、人工智能、物联网等各行业，打造极光般绚丽多彩的世界！独创应用智能隔离技术，多链并行横向扩展，安全无限提升 TPS，引领区块链世界的爆发，让世界耀眼发光！

Aurora（AOA）极光链在技术上不断的升级以完成自己的使命：DPOS+BFT 共识机制，快速共识基础上最大程度降低分叉风险；P2P 立体网络，通过网络分层的方式，实现快如闪电安全通信；独创应用智能隔离技术，Pending 区智能调控，保障应用间互不影响；多链并行，横向扩展的方式多条链并行处理，无限提升 TPS；多资产发行，简化资产发行流程，提供和主链币同等级别的处理速度和扩展能力；可升级区块链，全新技术保障在指定的高度自动升级；集群自组，可以使用户在不存储任何区块链数据的情况下，验证交易的真实性，降低用户存储成本。

Aurora（AOA）极光链致力于提升速度，定位于为应用而生的区块链，解决区块链难题并且保证立即可用。将链接区块链与各个行业，促进应用落地，构建多彩区块链世界！

目录

第一章　Aurora（AOA）极光链产生的背景

区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

区块链的诞生，标志着人类开始构建可以信任的互联网。区块链引人之处在于，能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除了中介的干扰，既公开透明又保护隐私，既共同决策有保护个体权益，这种机制提高了价值交换的效率并降低了成本。

第二章　Aurora（AOA）极光链的使命

Aurora （AOA）极光链坚持打造多彩的区块链世界，连接区块链与各行业，加速区块链应用落地。

其核心含义如下：

1. 专注于与行业深度结合

区块链目前最大的应用是发行数字资产，而 AOA 极光链独辟蹊径，多与其他行业做深度结合，不仅仅是数字资产，更多的在应用上链、规则上链上做深入的尝试。为应用而生，促进应用的上链，连接各行各业。

2. 专注于做最完善的合约

合约是区块链与其他行业结合的纽带，没有合约，就不能结合；区块链对合约的支持度，一定程度上反映了区块链与其他行业结合的深度，只有底层丰富、自由度高、代码完善的合约才能满足各行各业的需求。

3. 专注于提升速度升级技术

区块链的交易吞吐量（TPS）一直是为人诟病的话题，也是其他行业不敢与区块链结合的最大问题，AOA 极光链一直不断的提升交易处理速度，消除其他行

业对区块链的担心。

4. 专注于解决区块链难题

AOA 极光链致力打造可升级区块链，并实现在指定高度自动升级功能。同时通过集群自组技术，降低用户的存储成本。解决应用上链面临难题，加速区块链生态搭建。

5. 保证立即可用

AOA 极光链注重理想于现实的结合，效率与实用并存，AOA 主链可深度对接各类应用，加速区块链应用落地。

第三章　Aurora（AOA）极光链的技术实现

1. DPOS+BFT 共识机制

1.1 DPOS

因为 DPOS 共识机制具有交易速度快，TPS 高等特性，越来越多的区块链使用 DPOS（Delegated Proof of Stake）共识机制。AOA 极光链也采用 DPOS 共识：

当 AOA 余额大于 500 万时，该地址可以申请成为代理候选人；

代理候选人地址内的余额如果小于 500 万，则自动撤销候选人资格；

每一个拥有 AOA 的地址都可以给代理候选人投票，票数最高的前 101 位候选人自动成为打包交易的代理节点；

每一个地址最多可以给一个候选人投 1 票，最多投 101 票，投 1 票需要锁定 1 个 AOA，取消投票后解锁 AOA。

1.2 BFT

1）在 DPOS 机制上增加 BFT，这样可以有效的防止分叉问题，出块后不需要等待 N 个确认数，提高处理速度。

2）建立 P2P 立体网络，节点之间建立基于 UDP 的广播网络，代理候选人之间建立基于 TCP 的长连接，通过上层网络，代理之间可以快速实现 BFT 机制，提升 BFT 共识速度。

3）区块头信息中增加代理状态 ROOT 树，标记每个块代理状态，实现快速验证。

2. 智能合约

智能合约是跨领域法律学者尼克·萨博（Nick Szabo）提出来的，其定义是“一个智能合约是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议。”

智能合约是在区块链数据库上运行的一段计算机程序，可以处理信息，接收和发送价值。

AOA 采用 EVM 虚拟机和 Solidity 开发语言实现智能合约，以后将会支持基于 Java、go、C++等语言开发的智能合约。

3. P2P 立体网络

节点之间建立广播网络，代理候选人之间建立直连，通过上层网络，代理之间可以快速实现 BFT 机制。用网络分层的方式，实现更快速安全的通信。

4. 智能应用隔离

每一笔通过验证交易都会进入 pending 区进行处理，代理节点每隔一段时间将 pending 区的交易进行打包。智能应用隔离主要实现以下功能：

1）从宏观上，将合约从手续费、流量、类别等多维度进行区别，动态控制每类交易进入区块链的行为，实现相对公平性，并达到部分合约的拥堵不影响其他合约的顺利进行。

2）从微观上动态调整，实时监控每个合约，根据实际情况进行智能调度与干预，提高区块链效率同时，保护区块链不受攻击。

5. 多资产发行

简化资产发行流程，提供和主链币同等级别的处理速度和扩展能力。提供标准的代币流程包括简化并且规范化发行 Token 的方式和流程；通过多资产发行 Token，可以直接在合约中使用，不需要引入其他合约。

6. 多链并行技术

多链可以极大的解决交易性能问题，由于受到加密算法，网络传输的限制，单链性能总是有上限的，通过在多链上建立 P2P 立体网络，实现链与链之间的跨

链共识，横向提高区块链的 TPS，只要动态增加链的数量，就能无限增加区块链的处理能力。

7. 可升级的区块链

当前区块链一旦发布，就很难升级，只能强制采用硬分叉的方式升级，这种方式阻碍了区块链的快速发展。通过 LLVM 编译器，将区块链代码和合约脚本处于相同位置，将区块链升级版本放入区块链上，共识通过，达到一个指定高度，所有的客户端开始自动升级。

8. 集群自组

任何节点只要打开自组功能，网络中的一些节点形成一个集群组合，这个集群组合就能参与网络中交易验证和存储，降低用户的存储成本。而只要帮助别人验证交易，就能获取额外的奖励，这是一种类挖矿机制。

9. 抗量子攻击技术

量子信息的奇妙特性，使得量子计算具有天然的并行性。例如，当量子计算机对一个 n 量子比特的数据进行处理时，量子计算机实际上是同时对 2n 个数据状态进行了处理。正是这种并行性使得原来在电子计算机环境下的一些困难问题，在量子计算机环境下却成为容易计算的。量子计算机的这种超强计算能力，使得基于计算复杂性的现有公钥密码的安全受到挑战。

目前可用于密码破译的量子计算算法主要有 Grover 算法和 Shor 算法。对于密码破译来说，Grover 算法的作用相当于把密码的密钥长度减少一半。而 Shor 算法则可以对目前广泛使用的 RSA、ElGamal、ECC 公钥密码和 DH 密钥协商协议进行有效攻击。这说明在量子计算环境下，RSA、ElGamal、ECC 公钥密码和 DH 密钥协商协议将不再安全。

国际上，抗量子密码研究主要集中于基于格密码（Lattice-basedcryptography）、基于编码（Code-basedcryptosystems）的密码系统、多元密码（Multivariatecryptography）以及基于哈希算法签名（Hash-basedsignatures）等领域。

目前，没有量子算法可以借助量子计算机对格密码进行破解，而且，格密码系统在最坏情况假设条件下依然具备安全性。基于格加密的核心问题是最短向量

问题（ShortestVector Problem, SVP），即在各系统内找到最短的非零向量。AOA 将采用格密码算法，以对抗即将到来的量子计算攻击。

10. 跨链通信

区块链通信目前还是处于孤岛状态，网络孤立性阻碍了不同区块链之间的协同操作，限制了区块链的发挥空间，AOA 极光链会支持跨链通信协议和其他跨链技术，保证价值互联网的自由联通。

11. 不一样的挖矿机制

在比特币网络中，挖矿节点通过完成工作量证明算法的验算，将交易记录独立打包进新区块，从而获得比特币奖励。挖矿的核心就是对贡献进行奖励，从而激发社区成员的参与兴趣。

在 AOA 极光链中，任何一件对 AOA 极光链社区有贡献的事都可以获得奖励，从代码更新、bug 发现到优化建议、知识分享等等，只要被社区成员认可，即可获得奖励。挖矿机制前期不会写在区块链底层，会先在社区进行广泛到试用、优化，直到规则完善之后适时更新到区块链底层。

12. AOA Token 及手续费

AOA 是 AOA 极光链系统里的代币，是 AOA 极光链系统正常运行的必要保障。正常情况下 AOA 手续费为 0.0001，只有当发生类似攻击行为时，出于系统保护，AOA 手续费会涨到很高，从而直接拒绝攻击。

AOA 发行总量 100 亿，其中早期社区 26%，投资人与合作机构 34%，基金会 40%，用于日常运营、核心团队奖励、社区开发者奖励与生态建设。

第四章　Aurora（AOA）极光链的应用场景

1. 游戏行业应用

1.1 游戏代币区块链化

游戏使用区块链代币作为游戏币进行生产、交易和结算。代币可以在不同的游戏之间进行转换，代币的持有人可以完全控制自己的游戏代币，实现了开放型

经济体系。

1.2 游戏数据区块链化

游戏中的道具、角色、装备通过非同质的 Token 去定义和表达，这个 Token 代表了所有权，玩家可以脱离游戏去交易。道具和角色的区块链化，让游戏进一步开放，而游戏的开发者、运营方、发行方，也需要重新定义自己在游戏中的位置，以使自己的游戏能应付开放所带来的冲击。最终游戏会变得社区化，由游戏玩家和游戏厂商来共同决定一件装备的生产、消耗规则，有助于延长了游戏的生命周期，回归游戏的本质。

1.3 游戏规则区块链化

游戏的规则进行区块链化，这样使得任何一个道具、装备的产生都是完全透明化的，游戏开发者或者运营者都不能进行更改。这种完全透明的方式给了游戏用户极大的诱惑力，但对游戏开发者有一定的挑战。

2. IOT 物联网行业应用

目前的物联网生态体系，依赖中心化的网络管理架构，所有的设备都是通过云服务器连接。在去中心化的物联网中，区块链是发生互动的设备间促进交易处理和协作的基础框架，网络上的每个设备都可以作为一个独立、微型的商业主体运行。

3. 人工智能、航空航天等高科技应用

在人工智能、航空航天等高科技领域，数据的安全性与协同性一直以来都是相互制约的难点。当前采用的中心化数据网络，在跨地域、多节点的体系内协同方面存在着不足。同时，不同数据网络体系之间的协同，以及基于协同而产生的诸如价值交换、联合研发、技术创新之类的诉求，也对技术的革新提出了迫切的需求。区块链技术在此方面提供了全新的可能。

4. 供应链领域应用

区块链数据在交易各方之间公开透明，会在整个供应链上形成一个完整且流畅的信息流，确保参与各方及时发现供应链系统运行过程中存在的问题，并针对性地找到解决问题的方法，进而提升供应链管理的整体效率。

第五章　Aurora（AOA）极光链发展规划

2018.3　　AOA 极光链上线，同步上线智能合约平台

2018.5　　升级智能应用隔离服务及立体网络，进一步提升安全性和速度

2018.12　　多链并行服务成熟，集群自组技术及升级区块链技术完善，实现 30 家应用与区块链合作

2019 以后　实现抗量子攻击，安全快速多彩的区块链世界建成

第六章　网址与联系方式

官网: www.aurorachain.io

Email: official@aurorachain.io