下一代高性能区块链游戏平台

纯分布式、安全可靠、高效易用

Version 0.1.0

2019 年 2 月

摘 要

以比特币、以太坊为代表的区块链技术正以燎原之势构筑一个更加公平、透明、可信的新型价值互联网世界。然而，目前尚未有任何一个区块链共识机制完美兼顾了“去中心化、安全性、可扩展性”这三者在实践中遭遇到不同程度的技术瓶颈。如何实现这一突破并将区块链技术带入大规模商业应用，是 Kaleido 矢志探索的目标。

Kaleido 定位于高性能区块链游戏应用平台，其核心共识机制引入一种基于可验证随机算法的全新公共账本协议——Algorand，旨在实现区块链底层链较高程度的安全性、去中心化以及分布式应用的高性能扩展，为突破“不可能三角”提供一种新型技术解决方案。我们基于 VRF 随机算法设计了一种纯分布式的区块链游戏架构，充分利用区块链公开账本、密码学验证机制、P2P 可信网络等技术实现真正去中心化的应用开发，赋游戏予区块链公平、透明、可信等特性，同时，基于任何节点均可自由进出的 Algorand 共识算法机制以及针对游戏合约设计的权限合约机制，使得游戏复杂度和体验度均能达到目前中心化服务器的水平。

经实践测试，我们构建的基于系统合约的权限合约机制，可有效抵御 DDoS 攻击，并且代替用户交付 gas 费用，使得不持有链上 token 的用户也能参与到 dApp 中来，这一创新型技术设计能极大地拓展 dApp 的增量用户，易于创造裂变式传播，点燃市场，使得面向亿级用户的区块链落地应用，真正成为可能。

目 录

1　Kaleido 设计背景

1.1　市场痛点

（1）现有的基础设施是区块链大规模落地的最大瓶颈

自 2008 年比特币诞生以来，区块链作为一种基于 P2P 传输的分布式公共账本技术，在节点无须互相信任的分布式系统中实现去中心化的点对点交易，从而为解决中心化机构普遍存在的高成本、低效率、数据储存不安全、不可信等问题提供了解决方案，并且引入价值传递和分配机制，开启了价值传输网络的序幕。

在区块链的底层基础——公有链当中，比特币掌控了 PoW（Proof of Work）共识机制的绝对优势，10 年来全球逐渐强大的算力为这一系统的安全和稳定保驾护航，但算力呈现中心化垄断趋势，低性能、高能耗的特性也不适宜大规模商用，基于此，PoS（Proof of Stake）共识机制被提出，以参与者的经济权益代替算力工作量证明，从而平衡性能的短板，其中，以 EOS 为代表的 DPoS（Delegated Proof of Stake）则试图以牺牲去中心化为代价更进一步提升系统性能，然而近期层出不穷的黑客攻击事件则暴露出安全上的短板。

由此可见，在区块链的核心共识机制设计上，存在一个“不可能三角”，目前尚没有任何一个已经落地的共识机制很好地平衡“性能、安全和去中心化”三者的关系。但区块链技术想要实现大规模商业应用，就必须同时满足这三项要求。

在应用落地进展上，目前基于以太坊，EOS 等公链的智能合约开发的 dApp 大部分为游戏。因为智能合约是在链上的公开账本，所以游戏的操作需要在链上完成。受限于链上智能合约的操作性能和成本，目前区块链游戏的复杂度并不高，体验也不够好，但大型游戏的运行追求高并发、零延迟，需要在交互性方面做到高度流畅和灵敏，然而现有的公链性能远远无法满足这一要求。

另外，现有公链对于开发者的准入门槛过高。ETH 开发 dApp 的成本虽仅为开发合约的费用，但 TPS 远远达不到大规模商用的要求；而 EOS 开发者则需要购买底层技术资源并且承担运行成本，并且配套工具、编程语言等因素都导致开发难度相较于 ETH 更大，因此 ETH 的游戏类型相对 EOS 多元，EOS 的应用目前基本只有博彩类游戏。但鉴于很多 dApp 需要高 TPS 支撑，很多应用开发者只能选择 EOS，为两弊相权取其轻，并非两利相权取其重。

（2）现有区块链游戏对区块链圈外玩家门槛过高

一方面，使用 dApp 需要下载专门的钱包，预先充值数字货币，消耗资源且步骤繁琐，还涉及到私钥的保存与安全，这对于不熟悉区块链的大多数受众而言，市场教育成本十分高昂；另一方面，在依托某些公链如以太坊的游戏中，链上交互活动大部分需要消耗交易费，对于玩家而言游戏成本过高，非常影响体验。这些都在一定程度上导致目前区块链游戏 dApp 活跃度低、用户覆盖量少、难以形成规模效应，阻碍区块链技术的商业落地进程。

目前区块链游戏的优势特性并不直观，体验也未能与传统游戏相比，为了吸引用户，只能采用击鼓传花模式进行传播，带来的最大问题是后劲不足，游戏生命周期非常短暂，且这种模式只局限于币圈投机用户，无法扩展到圈外体量更加庞大的传统玩家。

（3）传统游戏对开发者和玩家的弊端明显

传统游戏运行在中心化服务器上，存在严重的技术安全风险，第一，在中心化服务器上运行的游戏有随时停运的风险，无论对于游戏开发者还是玩家，都是投入成本的巨大损失；第二，中心化服务器游戏经常面临黑客、DDoS 等技术攻击；此外，传统游戏厂商的巨头垄断趋

势明显，小型优质游戏开发者出头困难，收益难以保证，游戏开发对于他们而言投入巨大、风险极高。

另一方面，互联网游戏时代，游戏玩家和开发者往往是站在对立面的，中心化游戏中的游戏机制、数值算法不透明，虚拟资产例如装备、皮肤、坐骑等的归属权并不属于用户，而是归属游戏厂商，只允许现实资产向虚拟资产单向流动，这导致传统游戏内在价值的封闭和不流通。此外，游戏内经济体系也因为虚拟货币的不断增发而存在恶性通货膨胀倾向，玩家利益得不到应有的保障。[1]

1.2 Kaleido 解决思路

就应用场景而言，最契合区块链技术的必然是原生数字化领域，而非与现实发生巨大联系的，并且区块链多适用于：交流效率低、信任成本高的领域（特点多见于产业链条长、环节众多）；对真实性、共识有极大需求的领域（多见于不透明、黑箱操作）；以及长尾流量、资源分散、生态参与者之间利益不均衡的领域（需要完善激励措施）。电子游戏产业毫无疑问就是同属原生数字化的区块链走向大众的一个重要引爆点和切入口。

据相关数据统计，2018 年全球游戏市场规模高达 1379 亿美元，全球

[1] 参考资料：火币区块链研究院《火币区块链产业专题报告：游戏篇》。

游戏玩家超过 23 亿，占世界总人口的 1/3[2]，其中中国占了全球游戏市场超过 25%份额，达到 379 亿美元，整个亚太游戏市场则超过 52%，达到 714 亿美元。游戏用户群体年轻，对新鲜事物接受度更高，正好符合区块链这一新技术的特性，有望在未来形成强大的融合力。

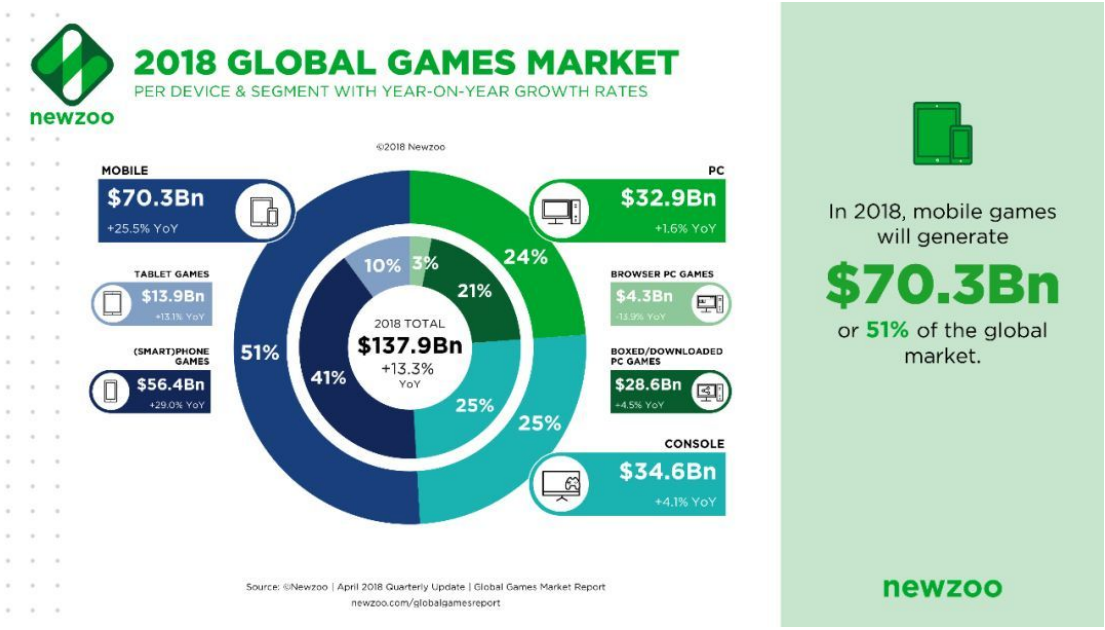

图 1.1 2018 年全球游戏市场

更重要的是，游戏上链带来的透明、公平、可信，将大大改变传统游戏规则、数值不透明、黑箱操作等一系列中心化作恶的风险，通过技术和 token 燃料重构游戏产业链上各参与者之间关系，让游戏厂商与

[2] 数据来源：游戏市场研究公司 Newzoo《2018 全球游戏市场报告》。

玩家社区的利益高度一致，玩家重获更纯粹的游戏体验和链上游戏资产所有权，忠实玩家便会自发地去维护游戏的平衡性，引入更多创新玩法和体验，帮助厂商获取用户，延长游戏的生命周期。这种基于公平透明的机制和共建共荣的社区共识，带来的必将是整个游戏业态的繁盛。

综合以上对区块链现存问题和传统游戏业态的认知，我们针对游戏领域构建了一个区块链 P2P 技术网络架构，这种架构使得复杂游戏能在区块链上得以真正落地。该架构充分利用公开不可篡改账本技术、密码学验证机制、P2P 网络来实现真正去中心化游戏应用的部署，且性能优异，让游戏的复杂度和体验度得以到达目前传统中心化服务器的程度，同时，大大提高链上游戏的公正、透明和安全性。

解决思路概述如下：

（1）Kaleido 引入了一种从纯 PoS 机制升级而来的全新共识算法：Algorand。这种算法结合了 VRF 和 PBFT 的优势，并创设了随机抽签选举的方式以实现更大程度的公平性和去中心化，旨在建立一个低能耗、高速度、民主化、可拓展性好且分叉率极低的分布式账本，解决现有区块链共识算法中的“不可能三角问题”。节点参与无需任何许可，任何人拥有设备都可作为节点参与记账，并且不需要耗

费太多的计算资源，该算法下各个节点均是对等的，能轻易扩展到百万节点上，而目前已有的基于 PBFT 的共识算法只能应用在几十到几百个节点的联盟链上。Kaleido 测试网的 TPS 目前稳定在 3000 左右，平均 2 秒出块，一旦出块即交易最终确认。预计主网上线以后，目标 TPS 最高将到达 5000。

（2）Kaleido 极大地扩展了链上功能，设计出一种新的 dApp 应用开发模式。除了与以太坊开发环境兼容，继承了以太坊对开发者的友好之外，我们还扩展了更多链上功能：除了公开账本之外，我们还提供了自动组建 P2P 应用网络的功能，使得应用程序能直接在链上建立可信的 P2P 网络，并且在这一网络中完成消息的交换和传递，从而使各节点之间的应用数据能公平、公开地传输和调用，这将极大地扩展链上应用的落地场景。

（3）Kaleido 通过公开的双加密账本，极大地保障了游戏数据的高度隐私性。尽管区块链加密账本技术实现了交易主体的匿名性，但要实际应用到游戏行业，其一大挑战是交易内容（包括交易额、交易时间等）的隐私性。无论是以太坊还是比特币，链上的交易内容和账户余额均对所有人公开，而对于游戏行业的开发者和玩家来说，他们对于游戏交易数据上链更为敏感，并不希望交易内容被公开。基于此，Kaleido 特别设计了一种双加密账本机制，通过将同态加密和零知识

证明等技术应用到现行智能合约上，实现了两种公开的加密账本，一种是对应 ERC-20 token 的加密 token 合约，另一种是基于游戏应用的加密结算账本，从而保证系统数据的高度安全和用户隐私保护。

（4）Kaleido 针对游戏合约，实现一种基于系统合约的权限合约机制。通过这种权限合约机制，dApp 可以有效控制合约的访问账户，从而增加抵御 DDoS 攻击的可能。同时，通过这个机制可以实现由合约账户代替用户交付 gas 费的机制，使得没有链上 token 的用户也能参与到 dApp 的体验中来，这样可以极大拓展 dApp 用户的覆盖面，从而让真正面向普罗大众的区块链应用成为可能。

1.3 Kaleido 设计原则

区块链要实现大规模商业应用，就必须满足“去中心化、安全、性能”三者的高要求，从这一初衷出发，Kaleido 旨在构建一个安全性高、去中心化程度高、支持超大规模应用的分布式信任网络，其设计中遵循的原则如下：

（1）真正的纯分布式网络

基于 Algorand 的 VRF+PBFT 算法逻辑，每个新区块均由一个独立委员会投票产生，而这个委员会从所有用户集合中随机抽签产生，在

委员会的选举上，引入 VRF 可验证随机函数，使得每一轮共识委员会以及区块提议者的选举都完全不可预测，且区块提议者及委员会成员在每一轮的共识过程均不相同。各个节点都拥有参与加密抽签和产生新块的权利，抽中的权重与账户余额成正比，这一点与 PoS 类似，但 Algorand 去中心化程度优于现行 PoS 机制的设计在于：(1) token 持有量只影响被抽中作为委员会或出块提议者的概率，并不决定最终产块的权力；(2) 共识过程中会抽取多个区块提议者，最终确认块基于 VRF 的 Proof 来选取，保证了 leader 的公平性和不可预测；(3) 节点参与也无须任何许可，任何人拥有设备都可作为节点参与记账。

经测试实践，基于 Algorand 算法的 Kaleido 去中心化程度要高于任何 DPoS 公链以及大部分 PoS 公链。

（2）极高的安全性

如果一个系统能够可验证地抵御拜占庭节点攻击、双花攻击、女巫攻击、拒绝服务攻击，那么我们可认为这个系统的安全性足够高。

在 Kaleido 网络中，共识过程的 Pure PoS 并不会通过用户的代币价值决定抽签的概率，而是根据各个账户的余额数量来选定中标用户，这样可有效避免攻击者伪造多个身份增加其被选中的概率，从

而发动女巫攻击；其次，VRF 加密抽签算法使得所有参与共识的用户均是秘密得知身份，投票广播后身份被暴露，敌手虽然可以马上腐蚀他们，但是他们发送的消息已经无法被撤回，且消息生成后，用于签名的一次性临时秘钥会立刻被丢弃，使得敌手在该轮无法再次生成任何合法消息，极大地增强随机性及不可预测性；再者，对于一个区块的公证，需要随机选出多轮委员会成员直至达到共识，且每一轮次的委员会成员均进行替换，这样能使权利随机地分散到全网内的各个节点，使得攻击者对全网作恶和控制的可能性大大降低。

在 Kaleido 的网络中，只要全网诚实节点拥有代币权重大于 2/3，那么主链就可避免分叉以及双花的可能性。

（3）低能耗、低分叉率、高性能

Kaleido 所运用的共识机制使得不管系统中有多用户，大约每 1500 名用户中只有 1 名会被系统挑中执行长达几秒钟的计算，并不占用计算资源，普通个人计算机也可参与产块。

每一次仅有且只有一个拥有最高优先级区块被公证，也意味着几乎不会发生分叉，区块的产出即意味着交易信息完成最终性。Kaleido 共识协议每隔几秒就能完成对区块的验证，造成非常低的延迟。

Kaleido 的共识过程采取一种超快速拜占庭协议（Byzantine Agreement，BA*），加密随机抽签的快速性以及小范围委员会成员公证区块的方式，在保障网络安全的基础上，都将为 Kaleido 带来高吞吐量。目前 Kaleido 测试网的出块速率是 2 秒/个，TPS 达到 3000 左右，预计主网上线后到达 5000 左右，这足以支撑游戏市场的应用需要。

（4）高度隐私保护

比特币、以太坊中尽管交易主体匿名，但交易金额、交易时间、交易地址等这些数据在网络中是公开的，任意攻击者能够通过追踪、分析这些记录，从而大几率破解交易主体身份。游戏对交易金额等数据的隐私性要求特别高，因此在解决账户的数据存储安全和隐私保护上，Kaleido 通过将零知识证明(ZKPs)和同态加密技术应用到智能合约，实现了两种公开的加密账本，一种是对应 ERC-20 token 的加密 token 合约，另一种是基于游戏应用的加密结算账本，从而隐匿了交易双方身份和交易金额，保障用户账户的高度安全和隐私保护。

（5）低门槛开发、大规模落地

Kaleido 公链所有设计的最终目标是要指向大规模商业应用落地，因此在提高链的性能与安全、降低开发部署应用的难度、降低普通用户的参与门槛三个原则上进行了一系列技术探索并取得初步成果。首先，底层共识算法为实现高吞吐量和高安全度奠定了坚实根基；其次，对于开发者而言，我们提供了相对现有公链而言更为完备的开发环境，所有具备基本编程知识的开发人员均可在链上部署更个性化和更多种类的应用；对于无任何区块链基础的普通用户而言，参与使用 Kaleido 上的应用并不需要下载钱包、交付 gas 费用等，体验上与目前 App 并无太大分别，学习门槛几乎为零，但又能让用户享受到分布式应用的公平透明，且用户对游戏资产拥有真正的所有权。

以上技术实现都让一款千万级甚至更大用户量的区块链落地应用成为可能。

2 Kaleido 技术解决方案

2.1 Kaleido 整体协作架构

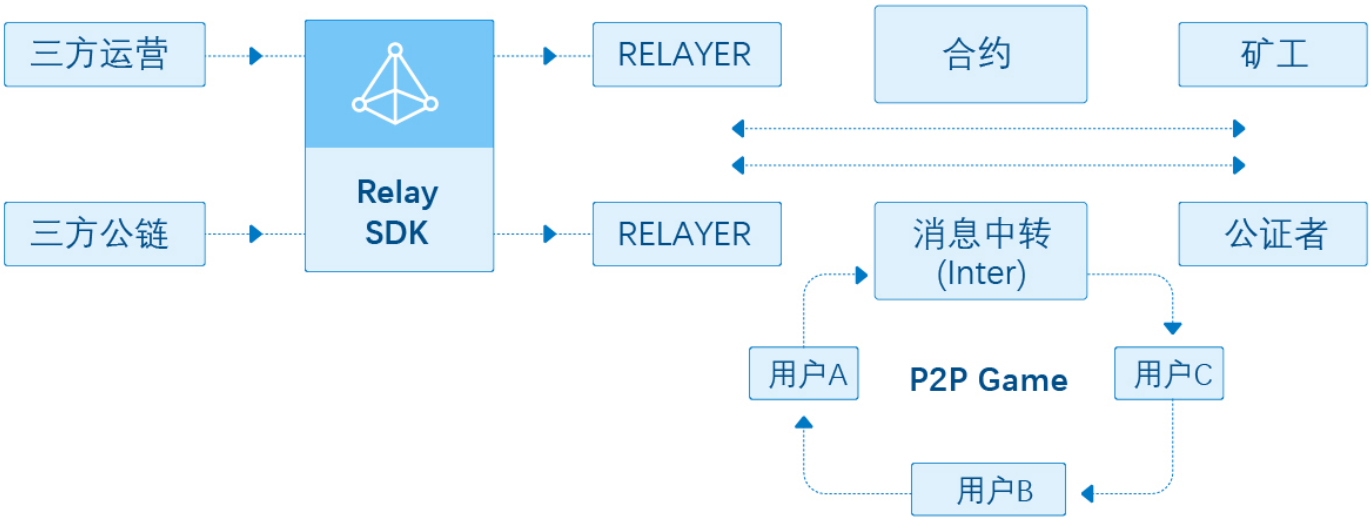

图 2.1 Kaleido 整体协作架构图

链上角色介绍：

- Relayer， 作为独立的功能单元存在，在第三方公链（如 BTC、USDT）接入时起到授权和校验功能，负责协助主链将第三方价值对接到主链的合约中
- 合约，包括 token 合约和游戏合约等，第三方链可以创建 token 合约， 并在此基础上创建游戏合约
- 矿工，负责主链上的区块验证、打包等工作，实现基于 Algorand 的共识流程
- 公证者，作为独立功能单元，可以通过提交签名消息数据来公

证消息，通过公证来驱动游戏合约，从链上获取公证脚本对用户的公证请求进行处理

- 消息中转，作为独立的功能单元存在，通过智能路由随机选择游戏的消息中继，负责 P2P Game 网络的消息传递，同时根据签名对用户进行校验

2.2 Kaleido 基本技术单元

图 2.2 Kaleido 基本技术单元示意图

- 侧链：负责链下 P2P 网络的组建、消息的传递、提供游戏脚本执行的环境、提供 P2P 网络和 Game SDK 的 API 接口，对中转者和公证者提供对应的功能
- 主链：基于 Algorand 共识算法，提供区块数据的存储、链上系统合约的访问接口、合约层的访问接口，包括链上合约的权限控制等

- 合约层：提供链上合约的执行环境、游戏脚本的访问读写功能、合约和链下 P2P 网络的交互

3 Algorand 共识机制

自比特币诞生至今，区块链的伸缩性/可拓展性，或称为区块链的性能，一直是制约区块链技术走向实际应用的瓶颈。产学研各方对于公链的共识机制、协议、算法都进行了众多研究和探索，但却仍然没有一个很好的方案能破解“不可能三角”这个额难题，系统的安全性、去中心化和性能，三者只能取其二。

PoW 机制能耗高、性能低； PoS 机制牺牲了一定的去中心化；Hash 图与 DAG 更多是解决一致性问题而非准确性；PBFT 又过于中心化。这些共识机制都从三角中取其二进行强化，难以从全局突破最优解。

在 Kaleido 中，我们采用了一种全新的共识机制 Algorand，它由美国图灵奖得主、麻省理工学院计算机教授 Silvio Macali 最早提出，是一种基于随机抽签选举的快速拜占庭共识协议（a fast Byzantine agreement protocol with leader election），基于纯粹股权证明（Pure Proof of Stake）和实用拜占庭算法（Practical Byzantine Fault Tolerance，PBFT）改进而来，不仅解决了拜占庭算法中心化的问题，还支持真实的互联网环境，在异步不可信的网络环境中

也能安全和高效地达成共识，真正实现了一种纯分布式的共识网络。

另外，我们使用自主实现的超高速可分区容错拜占庭共识算法（Super-Fast and Partition Resilient Byzantine Agreement）`Algorand Agreement`替换原有的工作量证明（PoW）共识算法`ethash`，此外还独立架构了区块共识加速网络，大幅提高链的整体性能。

3.1 Algorand 共识算法优势

经过实践测试验证，Algorand 共识机制具有如下优点：

Algorand 是目前已有共识机制当中能攻破“不可能三角问题”的最优解，在保证去中心化（Decentralization）、安全（Security）的同时，给整个网络赋予了强大的可扩展性（Scalability），极大地拓展了区块链的应用范围，dApp 开发者得以专注于链上应用的开发和部署，更好地提升使用体验。

在去中心化程度上，Algorand 通过 VRF（Verifiable Random Function，可验证随机函数）将出块提议者和选举委员会投票者、验证者的选举随机化，利用二项分布的线性叠加特性来保证公平性，这

种设计使得任何可联网设备包括小节点和散户均可成为节点参与共识记账。每一轮区块均由新的独立委员会选举产生，即每一轮的区块提议者、投票者、验证者均用 VRF 加密抽签，增加了随机性和不可预测性。在任意分区容错的特性下，恶意节点即使操控网络，将其进行分区并维持任意长时间，该协议也仍然能确保安全性，即所有诚实节点的共识结果也仍然是一致的，共识结果不会被恶意节点所影响。

在安全性的保障上，委员会轮番替换的设计在一定程度上保证系统安全性；另外，所有参与共识投票的用户都是秘密得知身份，即使投票后广播暴露身份，但消息无法撤回且临时秘钥立刻丢弃，攻击者无法进行任何腐蚀；Pure PoS 机制不通过代币价值而是账户余额数量来衡量抽签权重，能有效避免女巫攻击，只要诚实用户总权重超过 2/3，就能避免双花和分叉；这一算法具备任意分区容错的特性，即使网络被恶意节点操控，被分区且维持任意长时间，在网络分区恢复后也能快速恢复共识协议继续出块，使得攻击成本非常高。无论是用户级别、协议级别还是网络级别受到攻击，都可以安全抵御。

Algorand 具备极高的可扩展性。基于 VRF 的抽签程序功耗很低且在本地运行，节点之间不需要沟通，正常情况下只需两步即可达成共识，数学证明的零分叉交易确认机制使得交易一旦入块，就可以快速并可信地获得确认，大大缩短了交易确认时间，且消除了链的

分叉可能性。在不做分片等优化的情况下，目标 TPS 能到达 5000，这一吞吐量足以满足目前大多数应用的需要，在保持高性能的同时还能安全稳定地扩展到亿级用户。

Algorand 专为分布式网络设计的特性，非常契合商业应用落地的需要。它大大降低了共识层用户的参与门槛，只要持有 token，就可以参与到链的产块流程和共治社区中来。

3.2 Algorand 共识流程执行

Algorand 基于 gossip 网络运行一种经改进的高速拜占庭投票协议（BA*）。类似 PBFT 的预准备、准备、提交三个过程，Algorand 协议也有“发起提案”、“预投票”、“确认”三个投票过程，此外增加了“下一轮”投票。相比 PBFT，Algorand 改进的地方主要有以下几点：1）基于时钟频率来运行，而不是时间点，解决了公开网络中时间难以精确同步的问题；2）允许将前两步投票并行执行，缩短了投票所需的时间，使得正常情况下，只需要两步投票时间就能达成共识；3）异常情况下，增加的“下一轮”投票能使得本轮投票的有效信息传递到下一轮，提升了下一轮达成共识的概率，多轮投票的概率累积下来，就能极大地提升达成共识的概率。

（1）基本概念

节点（Node）

我们把用户设备上运行的一个客户端进程称为节点。在 Kaleido 网络上存在三种类型节点：

- 挖矿节点：执行共识出块流程，又分为提案者和投票委员会成员两种角色，具体职能下面会详细阐述。
- 非挖矿全节点：不执行挖矿，提供加速或业务访问服务，同步链上所有数据的节点，一般为普通服务器或 PC 等。
- 轻节点：主要是链上游戏的各种客户端或者钱包等，他们不保存区块和交易，通过连接全节点接入网络。

挖矿节点/矿工（Miners）

挖矿节点简称矿工，是运行共识算法的节点，运行在 gossip 网络上，为链持续产生新的区块。根据具体职能分为：

- 提案者（Proposer）：负责给出区块提案，每轮次均抽签替换，在 Kaleido 网络中极大概率最多有 26 个。
- 投票委员会成员（Committee Member）：以组协作方式工作，对提案矿工所给出的区块做有效性验证，按照算法逻辑投票决定共识区块，每轮次均抽签替换。

需要注意的是，每一个挖矿节点是根据持有的投票权重，随机抽签决定是否能以某种角色参与某一轮共识，挖矿节点只能通过提高持有的投票权重来增加中签概率，但无法影响自己成为哪一种角色。

公钥，用户和拥有者（Keys，Users and Owners）

一般情况下，公钥和用户其实是等价的，而拥有者一般是表示拥有这个钱包的使用权，即拥有这个公钥对应的私钥，当一个公钥 j 付款给另一个公钥 i 后，可以理解为用户 i 加入了系统。

无需准入和需要准入的系统

(Permissionless and Permissioned Systems)

如果一个公钥可以随意加入系统，一个用户可以拥有多个公钥，则这是一个无需准入的系统，否则便是一个需要准入的系统。

（2）假设要求

系统要正常运行，需要有一定的假设要求：

- 系统在无需准入和需要准入的环境下都能正常工作，在需要准入的环境下表现更好
- 系统中存在诚实用户和恶意用户，诚实用户遵守预定规则和行为指引（主要指拜占庭协议），并能完美地发送和接收信息，

恶意用户的行为违反任何预定规则，即拜占庭错误

- 系统在无需准入的环境中，2/3 以上的金额（Money）属于诚实（Honest）用户，在需要准入且一人一票的环境中，2/3 以上为诚实用户

（3）目标

理想情况下，Algorand 共识协议的最终目的为：

1、一致性（Consistency），即所有诚实节点得出的结果相同，且符合共识协议；

2、终局性（Liveness），即所有参与共识的诚实节点，最终可以达成一致性结果，即要不都发生共识，要不都不发生共识。

（4）铸块流程

- VRF（Verifiable Random Function）可验证随机函数

Algorand 维护了一个非常安全可靠的随机数 VRF，随机性由具备随机特征的哈希算法提供，安全性由链上的机制来保证，即要求更新随机数的挖矿节点的公钥在更新前已经写入区块链。

VRF 提供了一个随机数据生成方法，函数的输出由随机结果和随机

证明组成，由于它包含生成者的私钥签名，验证者可以通过公钥确认该随机数的合法性。

用户输入一特定参数（seed）+ 私钥，就会得到独一无二的随机输出和证明，简单示意图如下：

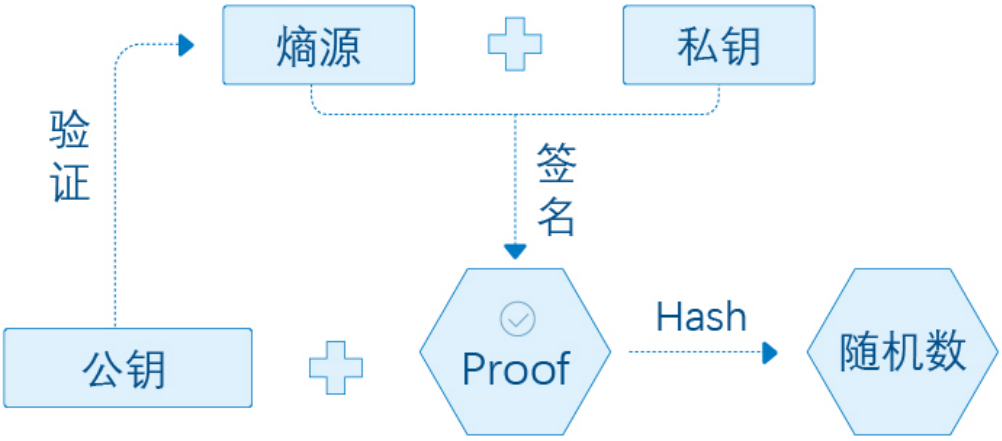

图 3.1 VRF 生成流程示意图

- Algorand 两步共识：

1、区块提案者出候选块；2、通过 BA*算法达成共识

Algorand 是一种纯 PoS 共识算法，参与共识的每个节点都有权重（Weight），该权重和账户的余额成正比。每个节点使用上一个区块中的随机数作为种子，自行执行随机抽签算法，从而得知自己是否将要参与具体某一步投票协议。抽签结果会生成抽签证明，可由任意节点校验。投票时，需要带上自己的抽签证明和签名，以表明自己的投

票权。这一机制确保了每一轮参与共识的节点数不会随着区块链分布式网络的增大而增加，从而使得共识协议能始终高效运行。

由以上共识流程，可以得出 Algorand 共识机制有如下特性：

1、分叉可能性极低；

2、所需计算量极少；

3、链上生成一个区块的延迟近似于在网络中完成区块广播的延迟；

4、不要求网络节点 7*24 小时在线（Lazy Honesty）。

3.3 Token 流转模型

Kaleido 共识算法的特性决定了需要有足够庞大数量的矿工才可以保障底层系统的稳定性和安全性，因此，Kaleido 的设计必须体现对矿工的经济激励，让他们的付出有所获益，从而推动底层生态系统的良性发展。另外，Kaleido 公链的生态繁荣度至关重要，包括游戏开发者、玩家、战略合作方等在内的所有为生态做出积极贡献的参与者，都应该获得与贡献相匹配的激励。

因此，Kaleido token 流转模型设计须遵循以下原则：

1、前期在保证底层链安全性的基础上，尽可能地吸引大量优质矿工进入底层生态参与共识出块，矿工基数足够庞大可以保证 2/3 为诚

实节点这一条件的实现，满足系统稳定安全运转的大前提；

2、让所有为链的安全与性能做出贡献的矿工，根据自身付出的劳动获取相应的报酬，可预期、可审计、可追溯、公平公正又不可篡改；

3、作为区块链应用开发的底层平台，token 的流动性包括产出、使用、消耗对于推动整个生态的良性运转至关重要，作为燃料剂的 token 应更多地引导生态参与者使用和消费，而非囤积和炒作。

基于以上原则，Kaleido token 流转经济模型如下：

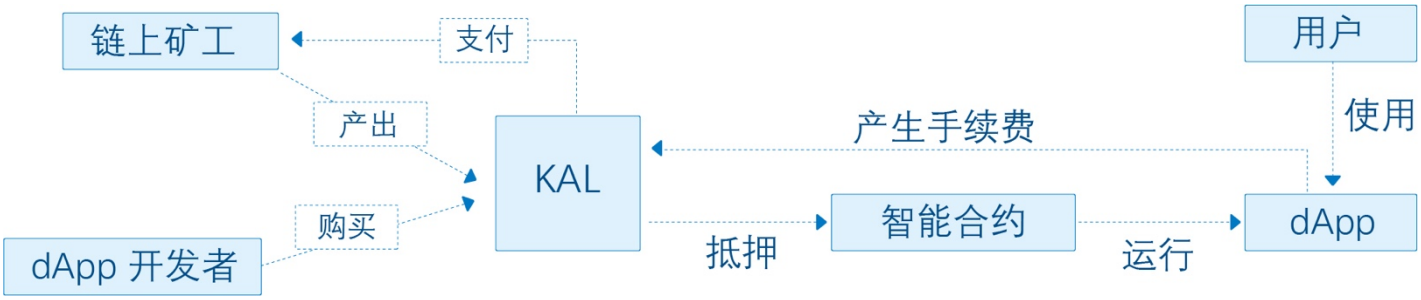

图 3.2 KAL token 流转图（(KAL 为 Kaleido token 缩写）

4　可信 P2P 网络

4.1　P2P 网络通信机制

交易吞吐量和延时是最重要的交易性能指标，影响区块链的交易性能包括广播通信、信息加解密、共识机制、交易验证机制等几个环节，作为区块链的核心技术之一 P2P 网络，其通信的效率对性能产生的影响非常大。

传统的 P2P 网络采用的是基于 tracker 或者 DHT 机制实现的匿名消息互联，为网络增加随机性。由于节点之间不可信任，所以消息中重要数据都采用 hash 校验，通信请求数据时使用数据的 hash 来进行请求和检索，但是对于消息的发出者并没有校验，这应用在游戏的逻辑里并不合适，因为应用和游戏通常是根据参与者的消息来驱动状态改变的。

我们实现的 P2P 网络采用基于 Notify 的广播机制，在 P2P 网络里面所有节点都会收到全部消息，这些消息均带上自己的签名，所以各个用户都可以验证网络里面的消息，同时结合链上状态可以对 P2P 网络里的用户进行鉴权，从而确保所建立的链下 P2P 网络是可信的。另外 Notify 机制保证了各个节点是完全对等的，使得单个节点可以

校验所有应用逻辑。

5　基于可信 P2P 网络和智能合约的游戏脚本驱动框架

Kaleido 通过将可信 P2P 网络和链上合约结合起来，可以搭建更多复杂的去中心化应用。链上账本是各个应用的数据和状态切换机制，P2P 网络链下交互则作为链下扩展，负责完成游戏逻辑和达成链下共识。在可信的 P2P 网络里通过密码学的零知识证明以及签名可信数据的方式，能够扩展到更多一直通过中心化服务器来完成的可信数据交互。

6　公开的加密账本实现

区块链公开账本应用在游戏行业的一大挑战是隐私性，无论是以太坊还是比特币，链上的交易和账户余额是对所有人公开的，而游戏行业对于数据的隐私度要求甚高，对于游戏交易数据上链非常敏感，因此，我们针对游戏行业设计了一种隐私度更高的加密账本实现机制。

6.1　同态加密

同态加密是指能够通过对加密后的密文直接计算得到原始数据密文

的加密算法。同态加密算法可以在不透露原始信息的前提下将计算委托给第三方，使得基于隐私数据的云计算得以实现。能实现所有算法（加法和乘法）的同态加密算法被称为全同态。拥有全同态特性的加密算法由 IBM 提出，但全同态算法由于当前算力的限制，暂时不能应用到实际商业场景中。对于一个加密账本来说，只需要具有同态加法特性的同态加密算法就可以实现账本的加密和运算。

我们选择了一个具有同态加法的加密算法来实现加密账本，并将加密运算放到链下 API 实现，账本（即合约）中只进行数据运算（即转账）和验证，如此设计便可实现一个在现实场景中得以应用的加密账本。

6.2 零知识证明

仅通过一个基于加法的同态加密算法还不能实现一个高度公开公正的加密账本，因为公开账本的数据需要通过多方提交，很难确保提交的数据是有效且不是故意作弊的，如此一来，如果要实现一个任何人都可以参与并且数据正确的加密公开账本，难度系数便倍增。

我们使用零知识证明来确保参与者所提交数据的有效性和正确性，确保账本转账等交易数据是有效和准确的。在实际转账过程中，要求参与者提交数据有效性和正确性证明，通过使用零知识证明使得转账交易中的加密数据可以被验证。

7　基于智能合约的权限控制合约机制

阻碍区块链 dApp 大规模推向普罗大众的一大门槛是要求用户必须要持有指定的链上 token，而获得 token 的主要途径就是去交易所用法币进行交易兑换，目前区块链应用的用户基本上是持有各个项目 token 的币圈用户，再加上 dApp 体验度差，基本难以扩大数量和规模。但是，如果区块链作为一项革命性的技术创新最终要实现大规模落地，则一定要让用户在不需要任何技术知识或资金门槛的前提下，也能便捷地参与应用体验，享受技术红利，如此方能真正体现区块链的价值。

因此，在 Kaleido 上部署的应用必须是不需要用户提前去了解专业知识或通过法币事先买卖交易，就可以直接使用的区块链应用，如同当今的互联网应用一样。

以太坊上的 gas 机制有效的保护了以太坊的安全，通过让调用者付出 gas 的代价有效的控制了 DDoS 的攻击，但是同时也因矿工会根据交易的价格高低进行选择，导致了一种通过发送高价的交易来阻塞正常交易的攻击手法。因此，我们实现了一种能够控制交易类型和验证交易有效性和权限的机制。

8　Kaleido 应用场景

在不实行分片并行的情况下，Kaleido 的 TPS 设计目标在 5000 左右，这个量级已经足够处理目前大部分中小型商业应用，但在处理大型游戏 dApp 上仍有不足。我们计划在 2019 年下半年加入 layer2 分片并行计算框架，进一步把 TPS 提升到 30000 左右，我们认为这一量级足以支撑目前为止 99%的商业化应用，且 Algorand 共识机制对用户访问数量没有限制，Kaleido P2P 网络开放式的用户访问机制足以支持大规模用户使用。

作为聚焦游戏、同时支持其他更多分布式应用的公链平台，Kaleido 第一阶段的落地应用场景瞄准全球游戏市场。从上一次互联网科技浪潮的趋势来看，信息互联网最早的爆发式增长点在游戏，到了价值互联网时代，我们认为在杀手级应用的爆发点当中，游戏同样必然是其中一个。

为了验证 Kaleido 的落地可行性，创始团队基于公链环境开发了一款华人世界普及面最广的游戏——斗地主，这将是全球首款基于纯分布式区块链网络的斗地主。从 Demo 测试来看，体验和交互都与在中心化服务器上运行无异，同时，整个游戏过程从押注、发牌、对弈到最终结算均上链，不存在单方控制结果的情况，并且能做到

事后的回溯审计，使得比赛结果等信息不可篡改，再加上基于 Algorand 共识机制，可以公开游戏规则，这就保证了游戏过程的透明以及公平性，且玩家拥有游戏资产的所有权确权保障。

9 Kaleido 年度发展规划

- 2019 年 2 月：测试网及游戏 Demo 持续优化；游戏生态搭建；首批合作伙伴对接
- 2019 年 3 月：Kaleido 应用开发者配套工具上线：测试网、游戏 demo 测试版、开发者文档；游戏社区生态搭建；合作伙伴对接
- 2019 年 4 月：Kaleido 主网正式上线；矿工激励计划敲定并上线；游戏正式 Demo 上线；第三方游戏开发者进驻部署
- 2019 年 5 月：线上游戏正式版上线；启动大规模游戏玩家推广；游戏 SDK 开发文档上线；加密账本上线
- 2019 年 6 月： 第三方游戏发布及运营；BDN 上线测试网；完整第三方开发文档公布
- 2019 年 7 月：举办大型线上赛事；对接业内强资源战略合作
- 2019 年 8–9 月：完整 layer2 方案上线；链分片 Sharding 方案验证; BDN 正式方案上线
- 2019 年 10–12 月：链分片 Sharding 方案发布；存储解决方案发布；完成虚拟机优化

10　结论

我们经过初步研发和实践测试，设计并论证了一个下一代高性能区块链游戏平台的落地可行性。融合 VRF 可验证随机算法和实用拜占庭容错算法（PBFT）而改进的共识算法机制 Algorand 是实现去中心化、安全、性能三者的基础，在此之上我们构建了可信 P2P 网络、基于 P2P 网络和智能合约的游戏脚本驱动框架、两种公开的加密账本以及权限控制合约机制。在落地应用场景上，我们早期将深耕游戏市场，并且为技术底层、中间层和生态层设计了通证经济模型，通过 token 燃料剂推动各个齿轮间的咬合和运转。

下一步，Kaleido 将持续升级优化底层基础设施，并着力于生态的搭建，实现生态内价值的流通闭环。在游戏这一高价值市场机会中，我们相信基于区块链 P2P 分布式网络的游戏不仅仅能为玩家带来更加公平透明的纯粹游戏体验和游戏资产确权，其革命性的意义更在于为生态各参与方建立一种更加强大的信任纽带，让游戏开发商、运营商、玩家在充分满足各自需求的基础上，基于共同的利益诉求形成强大共识，从而为整个游戏生态赋予共建共荣的生机与前景。

未来，Kaleido 公链将从游戏领域向更多的应用领域扩展，剑指区块链界的 Linux 系统。

参考文献

[1] S, Nakamoto. Bitcoin: *A Peer-to-Peer electronic cash system*. http://www.bitcoin.org/bitcoin.pdf, May 2009.

[2] *Bitcoin Computation Waste*, http://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-502013.

[3] BitcoinWiki. *Proof of Stake*. http://www.blockchaintechnologies.com/blockchain-applications.

[4] Ethereum Foundation. *Ethereum,2016*: https://www.ethereum.org.

[5] Jing Chen, Silvio Micali. *ALGORAND*. In arXiv report http://arxiv.org/abs/1607.01341 Version 9.

[6] Yossi Gilad, Rotem Hemo Silvio Micali, Georgios Vlachos, Nickolai Zeldovich. Algorand: *Scaling Byzantine Agreements for Cryptocurrencies*. In SOSP '17.

[7] Silvio Micali, *Byzantine Agreement, Made Trivial*. http://people.csail.mit.edu/silvio/SelectedScientif

[8] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. *Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults*. In Proceeding 26th Annual Symposium on the Foundations of Computer Science, IEEE,1985:383~395

[9] Silvio Micali, Salil Vadhan, and Michael Rabin. *Varifiable Random Functions*. In FOCS'99.

[10] S. Goldwasser, S. Micali, and R. Rivest. *A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attack*. SIAM Journal of Computing, 17, No. 2, April 1988, pp. 281-308

[11] S. Micali. *Fast And Furious Byzantine Agreement*. Innovation in Theoretical Computer Science 2017. Berkeley, CA, January 2017. Single-page abstract.

[12] B. Chor and C. Dwork. *Randomization in Byzantine agreement, in Randomness and Computation*. S. Micali, ed., JAI Press, Greenwich, CT, 1989, pp. 433-498.

[13] D. Dolev and H.R. Strong. *Authenticated algorithms for Byzantine agreement*. SIAM Journal on Computing 12 (4), 656-666.

[14] M. Castro and B. Liskov. *Practical Byzantine Fault Tolerance, Proceedings of the Third Symposium on Operating Systems Design and Implementation*. New Orleans, Louisiana, USA, 1999, pp. 173–186.

[15] M. Pease, R. Shostak, and L. Lamport. *Reaching agreement in the presence of faults*. J. Assoc. Comput. Mach., 27 (1980), pp. 228-234.

获取项目详情：info@kaleidochain.io