Cocos BlockChain Expedition

去中心化应用与数字资产的生产、管理和流通平台

技术白皮书

Version: 1.1.3
Date: May 30, 2019
Prepared by: 陈昊芝、尹健辉、杨小龙、刘冠群、王哲

更新记录

更新日期及版本号	更新内容
2018.05.20 v1.0.1	增加平台经济体系部分描述
2018.05.22 v1.0.2	增加概要中的技术特性部分描述； 增加 2.7.9 链内的可信随机过程描述；
2018.05.31 v1.0.3	修改 2.7.5 事务的并发处理机制； 修改 2.7.6 委托型事务机制与随机过程实现；
2018.07.12 v1.0.4	更新 3.5 COCOS 的使用分配中的代币用途示意图
2018.07.31 v1.0.5	更新封面封底品牌 Logo
2018.10.11 v1.1.0	1. 增加 2.2 可迭代更新的智能合约系统； 2. 增加 2.4 跨越世界的道具穿越； 3. 修改 2.5 铁匠铺机制； 4. 修改 2.7 道具资产流通平台； 5. 修改 3.1 实现游戏规则上链； 6. 修改 3.3 支持同质和非同质数字资产的跨链承兑网关； 7. 修改 3.4.1 改进的非同质数字资产数据结构； 8. 增加 3.4.6 合并多个操作确保事务的原子性； 9. 修改 3.6.4 在语法级别支持共识任务； 10. 修改 3.6.5 合约的优先共识； 11. 修改 3.6.7 链内的可信随机过程； 12. 修改 3.6.10 标准化的非同质数字资产； 13. 修改 4.1 区块链为游戏行业带来的本质改变； 14. 修改 4.5 COCOS 的使用分配； 15. 增加 3.7 关于防止 BP/开发者作弊的设计； 16. 全文用语修订(弱化交易属性)； 17. 修改 5 团队构成； 18. 修改 6 总结； 19. 增加 3.9 增强的资产权限系统； 20. 修改 3.4.1 改进的非同质数字资产数据结构； 21. 修改 3.6.7 委托型事务机制； 22. 增加 3.6.8 内源可信随机过程的实现； 23. 修改 3.6.11 标准化的非同质数字资产；
2018.10.31 v1.1.1	1. 增加第 2 章项目优势和技术优化； 2. 增加第 7 章合作机构与投资机构； 3. 修改第 3 章业与运行设计； 4. 修改第 4 章技术架构；
2019.01.18 v1.1.2	1. 增加 4.5.12 既定规则设计工具
2019.05.30 v1.1.3	1. 去掉团队成员介绍； 2. 去掉合作伙伴介绍； 3. 修改部分字母名称及数值；

我们的愿景

让数字世界的内容资产化，内容生产者可以与内容消费者建立一致的价值体系。

陈昊芝

发起人, Cocos BlockChain Expedition

摘要

项目目标

本文描述了一个用于在区块链生态上开发、运行、管理和流转去中心化应用及应用内资产的平台—Cocos-BCX Expedition（简称“Cocos-BCX”或“平台”）的设计思想与技术实现原理。该平台包括（1）支持多种操作系统、多种区块链环境的应用开发框架，（2）完全脚本化、组件化和数据驱动的应用开发工具，和（3）一个面向高性能应用、基于石墨烯技术框架改进的区块链系统及相关功能组件。能够支持开发者进行面向区块链环境的去中心化应用、混合架构应用的编程、调试与发布。同时，平台整合了包括基于区块链的分布式用户账户系统、钱包和数字资产流通平台，可以实现应用内资产的脱链永久保存及跨链使用。

第一阶段目标

由于游戏是最早、最大的区块链应用领域之一，我们以该行业中开发者和用户的需求作为项目初期版本的设计出发点。本文所探讨的技术、产品、经济体系设计与用例均基于游戏这一应用场景。

目录

1. 项目背景

1.1. 区块链生态与数字资产是经济发展方向之一，具备价值基础

2009 年以来，针对区块链和数字货币的讨论逐步从技术延伸至经济、社会和政治等多个领域。公众开始关注区块链对社会发展的影响，以及数字货币在世界经济活动中的作用。在全球科技进步存在瓶颈、资源消耗上升、人口老龄化、地缘政治冲突加剧等背景下，部分地区或行业范围内由政府主导的生产力组织方式有可能发生变化。与之对应的货币体系也可能从“政府-法币”变为“非政府生产力组织者-多种共识通货”。我们认为，以区块链技术和经济机制为基础的去中心化社会形态是未来一段时间内部分地区、人群和行业生产秩序变革的产物。区块链经济生态和数字货币的存在具备价值基础。

相比传统物理资产，数字资产在区块链机制上的生命力更强。在数字经济中，人是生产力的绝对主导因素，数字资产的生产、使用和分配行为能够在区块链上形成闭环，对中心化资源支配者的依赖度降低。另一方面，去中心化后的数字内容可以依赖单个或多个区块链生态存续，并被公开、公允地定价，成为真正具备独立物权的“数字资产”，并衍生出新的商业模式和社会价值。

在不同类别的去中心化应用中，游戏是制作模式最成熟、商业化程度最高、开发者和用户基础最深的场景之一。在本项目的第一阶段，我们将围绕它进行研究与开发，解决区块链游戏领域存在的问题。

1.2. Cocos-BCX 希望解决的问题

我们希望向游戏开发者提供易用、完善的区块链游戏基础设施，包含可视化的开发套件和链上生态环境，开发者无需关注区块链技术的实现，即可直接以图形化的方式，低门槛、快速高效的完成区块链游戏的开发。

我们希望向游戏玩家提供一个数据透明、规则透明、不会发生后台操纵道具掉率、恶意诱导消费的公平、公正、公开的游戏环境，希望游戏玩家的资产能够长时效、安全、去中心的保存。

同时，我们希望通过区块链承载的数字资产经济模型，帮助开发者和玩家实现更好的利益一致性：我们帮助开发者将其生产的内容资产化，使其在资产的使用、管理和流转过程中持续获得收益，并提供便利、去中心的游戏分发渠道；我们帮助玩家将其消耗时间与精力形成的数据和消费获得的道具转化为可以安全存放和流通的资产，让玩家拥有将其管理和商业化的权利。

1.3. 区块链游戏的四个发展阶段

1.3.1. 使用同质资产做游戏“金币”的结算

这一阶段的区块链游戏使用区块链系统中的数字资产作为游戏中“金币”产出的结算载体。这一阶段的典型代表是以太坊系统的 ERC20 同质资产标准。

该标准在如今的区块链项目中已经众所周知。很多的项目同质资产都会基于以太坊网络的 ERC20 标准进行制作，基于 ERC20 协议发行的数字资产容易交换和兼容，并且能够在 dApps 上行使应有的功能，资产的持有人可以完全控制资产并且跟踪其流通的任何地址、任何数量，而且这些资产可以用于不同项目和平台，同质资产的流通路径可在区块链浏览器中查询。

这一阶段的区块链技术主要解决如下几个问题：

- 游戏“金币”产出量和流通的透明化；
- “金币”的跨游戏流通；
- “金币”兑换通道的多样化。

该阶段的代表作：Candy Shooter 和 Candy 游戏平台。

Candy Shooter 是 Candy.One 平台的一个 STG 游戏，类似于多年前的“雷电”游戏。其游戏“金币”即为 Candy。每次开始游戏时，用户需要支付 100 Candy 作为门票。用户控制一个小飞机射击所有的“敌人”并且保证自己不会被对方的子弹打到，每一关卡会有一个大 Boss，击败大 Boss 将会获得更多的“游戏金币”奖励。

当用户生命耗尽或全部通关后，游戏便会结束。结算系统会根据用户在游戏内获取的各种“游戏金币”（以及其他赞助商同质资产）的数量，按照特定比例换算成 Candy，而这些同质资产（含 Candy 在内）同样被 Big.One 和其他数字货币流通平台接纳，并可在各自的应用场景中使用。

图 1-3-1 Candy Shooter 游戏画面

这一阶段的数字资产是同质化的，只能表达积分、金币类的数值，用作游戏结果的结算。

1.3.2. 游戏“金币”和道具的自由兑换

以 ERC20 为例，它只能用于发行可替代性通证（Fungible Token），用其来代表各种可替代性事物，其决定在流转或使用过程中同等或相似类型的物品或数量是否可以完全互换。因此，项目资产本身只具有单一价值媒介的作用（例如证券、积分、数字资产等）。

但是，在现实生活中，还有一些事物是不可替代的（任何带有唯一属性的人、事、物，例如一件文物等）。而这些事物也可以被数字资产代替，但是其价值无法通过 Fungible Token 衡量，因此，在以太坊的改进计划中（EIP）的代号 721 项（ERC： Non-fungible Token Standard #721），就提出了新的“非同质” 数字资产标准——ERC 721 标准。而 BCX-NHAS-1808 是 COCOS 应用中适用于去中心分布记账式网络的非同质数字资产标准。非同质数字资产可以在任何流通平台中使用，但是它们的价值取决于和每个资产相关联的独特性及稀缺性，例如游戏中的装备、道具和高等级账户。

前一阶段很火的以太猫是非同质数字资产标准的例子。每一只猫都是一个“具备独特基因的生物”，而非同质化的货币，并且，每一只猫都不能进行拆分，永远都是完整的个体。当然，每只猫都会拥有自己的标签、价格等等独特属性。展开来看，除了以太猫之外，特殊的游戏道具或者任何具有一定收藏价值的物品，都可以对应一个资产来表明其身份信息。并且非同质数字资产在某种程度上就是唯一的，不可分割、不可拆分。

在这一阶段中，不论是游戏中的道具、装备、玩家账号，其价值体现都可由非同质数字资产表达，游戏内的所有广义资产流通行为（包括但不限定于道具流转、资产流通、道具掉落等场景）最终都以数字资产（同质和非同质）的形式结算，特定的游戏内容（例如 MOD）甚至可以单独作为一种数字资产发行流通。

正因为游戏中的内容有了一个统一标准的价值载体，使得所有和区块链系统对接的游戏内容具备了可以流通的基本价值体系，因此和链对接的游戏具备了跨平台流通能力，对于玩家而言，可通过同质和非同质数字资产完成一组游戏资产到另一组游戏资产的迁移。

相对第一阶段，本阶段把道具作为非同质的唯一标识放在区块链的记录中，道具、金币的产量、流通路径是透明的，但游戏的运行规则是在链外执行的，道具和金币的生产逻辑仍在暗箱中，需要变通的解决。Cocos-BCX 已经实现本阶段的全部特性，正在尝试下一阶段的解决方案。

1.3.3. 关键规则上链运行

在这一阶段，链上游戏所需的基础设定及关键规则将以合约或其他便于公开的形式写入区块中，供全网见证，保证游戏规则和产出逻辑的公正公开。例如扭蛋中的道具出现概率、RPG 地图上的遇敌设定、开宝箱掉落设定、发牌规则等游戏的数值逻辑，都将会写入链中，实现规则的公开、透明、不可篡改，保证游戏的公平性，增强用户体验和玩家群体信心。

这一特性有效解除了玩家群体对游戏运营舞弊的担忧，能够提高玩家群体的信心并吸引更多玩家参与游戏，更加利于社区的建设与发展。

合约的运行和见证是需要时间的，如果以 SLG 游戏地图中的宝箱刷新逻辑为例，则可以归纳两种运行思路：

- 所有宝箱内容在地图载入时一次性的在合约中生成

  此模式下，合约在场景载入时一次性执行，网络压力较小，运行时除了记录道具的获取外，无需执行其他耗时操作，可以带来更加流畅的游戏体验，但缺点在于灵活性较差，缺乏普适性，无法对地图场景内的剧情上下文做响应；

- 每一次开箱子行为即时运行合约生成内容

  此模式下，合约在每一次开启宝箱时执行，即时演算道具的产出逻辑，合约运行次数多，链网络压力大，但合约使用和运行灵活，能够和地图场景内的剧情上下文相关联。

此阶段的区块链游戏已有较多规则和数据在链上执行，用户增长将导致链网络的压力剧增。在没有新的突破前，这一阶段的技术只能适用于敌我回合中有 Cool-Down Time（冷却时间）的游戏。去中心和性能是矛盾的，高性能的共识以及合约虚拟机是下一阶段的主要任务。DAG 等延时较小的技术可能成为突破口，但离终极的解决方案仍有距离。

1.3.4. 游戏整体上链运行

游戏整体上链是行业最终形态，游戏的全部逻辑代码在链环境中执行，并由去中心化的分布式网络承载和存储数据，在这个场景下，游戏即是合约本身，游戏的运行需要可信、高效、极小延迟的集成运行环境与轻量级的用户节点，目前业界尚无决定性的技术方案。

以太猫的设计初衷是游戏整体上链运行，但由于以太坊网络的吞吐性能的问题，无论是数据交互还是内容承载都受到极大限制，最终以太猫选择了妥协的做法：“数据链上交互，游戏链外运行”的策略-即上一阶段的“关键规则上链”。

Cocos-BCX 下一阶段的思路为：

1. 玩家拥有轻量级的全节点环境；
2. 服务栈在区块链环境中运行；
3. 游戏引擎作为节点的基础设施之一；
4. 提供包含引擎、可视化 IDE、链网络交互接口的联合开发/调试环境；
5. 节点间具备一组异步共识任务，用以确保引擎环境的可信，该共识有可能基于引擎关键函数目标代码的特征码判别；
6. 游戏代码（合约）由引擎控制的安全虚拟机执行，该合约的关键数值运算的部分可能采用“可信执行环境”方案，和合约主体分开执行；
7. 合约的关键过程被临近或相关节点（如同一个副本中的玩家）们共识见证。

2. 项目优势和技术优化

2.1. 技术目标

Cocos-BCX 将打造一个完整的多平台游戏运行环境，最大程度地为游戏开发者提供区块链游戏的开发便利性和完善的生态环境，同时，将为游戏用户带来全新的游戏体验，和超越以往的游戏形态—用户将拥有游戏资产的自主权、游戏环境将最大可能的公平、公开、公正。

为了达到以上目标，Cocos-BCX 将提供包含且不限于如下技术特性：

1. 带有区块链系统互操作接口的多平台游戏运行环境；
2. 基于 DPoS 改进的高速共识，和委托见证模式；
3. 包括高效链网络与高速合约虚拟机的测试链；
4. 支持同质和非同质数字资产的跨链承兑网关；
5. BCX-NHAS-1808 非同质数字资产标准；
6. 增强的资产权限系统；
7. 能够跨块持续执行的智能合约；
8. 原子化的事务操作；
9. 支持语法级别的共识任务；
10. 支持委托的事务机制；
11. 小范围共识和随机数；
12. 支持内源可信随机过程；
13. 支持极小的链上事务确认周期；
14. 支持链内精确定时器、支持 Standby 模式，带有心跳支持的合约运行模式；
15. 防止 BP/开发者作弊的事务验证机制。

同时，提供包含且不限于如下的功能：

1. 去中介资产（道具）操作接口；
2. 非同质资产流通平台的范例；

3. 玩家自治和铁匠铺机制的支持；

4. 可视化 IDE（含游戏程序和合约的可视化编辑）；

5. 完整的钱包、用户系统和区块链浏览器；

6. 可迭代更新的智能合约系统。

目前，Cocos-BCX 测试链的理论吞吐量可以达到 100,000 tps，实际吞吐接近 5,100tps，出块时间为 3 秒，即每 3 秒完成一次全网信息广播。Cocos-BCX 的实际吞吐量在完成可由合约设定的分区共识、多链联合和“见证委托”后将得到进一步提高，足以支撑大部分游戏的关键逻辑上链运行，“极小延迟事务确认”技术将进一步提高资产流通过程的体验。

Cocos-BCX 测试链附带的钱包直接集成资产流通平台，用户可根据流通平台的游戏数字资产与主链基础货币的兑换率评估游戏金币、道具和账号的价值。

Cocos-BCX 被 COCOS Creator 可视化游戏编辑器直接支持，Creator 产出的游戏能够直接在 Cocos-BCX 的区块链运行环境中运行。

2.2. 优越的技术亮点

Cocos-BCX 项目有诸多技术亮点，包括可迭代更新的智能合约系统、铁匠铺机制、道具嵌套组合、支持多链和资产铆接的承兑网关、改进的 DPoS 共识机制、可视化的合约编辑器、高效链网络与高速合约虚拟机、多链挂接和防止 BP/开发者作弊的事务验证机制、Cocos-BCX 经济体原理设计、支持多种数字资产流转的资产流通平台等。下文会对此部分技术功能作详细阐述。

Cocos-BCX 项目基于游戏产业的市场痛点，结合区块链技术发展机遇，提出了打造数字世界里内容生产者与消费者价值一致的愿景体系。基于大的技术框架体系下，每个技术环节与组织有很强的针对与逻辑基因，并且在此基础上提出众多模块化、改造化的技术方案或机制。

2.3. 不可能三角的优化

“不可能三角”代表着区块链系统中难以同时兼顾的三种特性，Cocos-BCX 同样无法同时在这三点上都做到最强，但通过诸多的设计，我们已经让“不可能三角”的边长尽可能的缩短了。

（1） 去中心化

- 改进的 DPoS 机制

  我们在传统 DPoS 共识机制基础上改进共识算法，所有的活跃见证人在 DPoS 共识算法的见证人预定算法中具有相同的出块预定概率，这保证了所有见证人的出块概率和获取出块奖励是一致的；

- 低分叉风险

Cocos-BCX 使用 DPoS 共识机制，不需要矿工使用矿机进行挖矿，可以有效避免中心化算力对整个基础链的影响，进而降低分叉风险。在 DPoS 机制下，若有见证人想要通过投票进行分叉，则需要保证 1/3 以上的见证人都同时违背机制才有可能；

- 轻量级节点

  轻量级节点本质上是一个具备与链互操作能力的环境，与全节点不同，轻节点不需要同步全网数据，取而代之的是同步运行必须的合约信息与环境数据，这样的设计可大幅减少节点同步的数据量和同步时间，使链上游戏端软件具备实际使用的容量、时间成本可行性。

（2） 安全性

玩家自制和资产安全，由于区块链网络公开、透明的特性，玩家在游戏中所获得的数字资产信息可以通过区块链浏览，并且针对游戏资产安全提供保障机制：

- 资产操作权限

  游戏内道具所有权及处置权仅归玩家所有，物品销毁的操作仅能由用户自己授权处理；

- 链内关键操作原子化

  资产流通、资产创建等重要行为被提交至流通平台或铁匠铺，流通或制作过程中所有操作被视为一次不可分割的原子事务；

- 可扩展的多步验证

  除去区块链事务验证密码以外，游戏商将提供进一步的二次密码验证以及随机码验证等，进一步提高玩家资产安全性；

- 现代密码学的保障

  Cocos-BCX 链系统使用常见的现代密码学技术 ECC（椭圆加密算法）进行加密，保障区块链信息安全；

- 防止 BP/开发者作弊的事务验证机制

  Cocos-BCX 方案中设计了一套针对 BP 和开发者可能作弊环节的事务执行、消息传递、运行机制，防止 BP/开发者有作弊行为；

- 可迭代更新的智能合约系统

  Cocos-BCX 可以提供链上游戏智能合约的逻辑更新、漏洞修复等，从而保证了智能合约的安全性与适时性。

（3） 拓展性

项目顶层设计的强拓展性，通过游戏引擎、开发环境和 Cocos-BCX 游戏链建立了一个去中心化游戏制作与游戏经济运行的整体解决方案，构建了一个商业生态体系，目的是连接全球的游戏生态。其中主要的生态环节有：开发者、用户、创作内容、关键生态环节和区块链系统等。

项目顶层设计的强拓展性包括：多平台游戏集成运行环境、区块链交互接口、支持同质/非同质资产和多链铆接的承兑网关、多链挂接、对已有区块链系统的优化和扩展。

拓展性从顶层设计构建了多样化、多元化的生态，以及后续的可能性，其次通过多平台游戏集成运行环境、区块链交互接口等至少 5 种技术或方案，从而扩大了项目的融合边界。

3. 业务与运行设计

3.1. 完整的钱包和区块链浏览器

Cocos-BCX 项目向多种运行平台提供数字资产钱包，包括 Android、iOS 及 Windows 等操作系统，确保主流运行环境下的用户均可以参与资产流转。通过数字资产钱包，用户可以将所有的游戏数字资产和通过承兑网关导入的 ERC20 资产存储在其中，更加方便在游戏金币流通平台完成资产出让和购入。另一方面，Cocos-BCX 对数字资产钱包进行了金融级别的算法加密，同时会结合运行平台的 KYC 认证服务，确保用户存储在钱包中的数字财产安全。

Cocos-BCX 在钱包中直接提供区块链浏览器功能。区块链浏览器是浏览区块链信息的主要窗口，每一个区块所记载的内容都可以从区块链浏览器上进行查阅。每一个独立的区块链系统都有对应的区块链浏览器。Cocos-BCX 提供一个完整的、带有查询和跳转功能的区块链浏览器，例如当用户在游戏中产出一件珍惜级别的道具资产时，对应的游戏道具数据就会在主链中产生，用户可在区块链浏览器中查询到对应的事务信息，Cocos-BCX 的区块链浏览器支持原子操作的查阅。区块链浏览器可以让用户更加透明的了解自己的资产分布，所有的数据在链上记录，真实不可篡改。

3.2. 可迭代更新的智能合约系统

以 Ethereum 为代表的智能合约体系，其智能合约一旦定义发布后就无法再修改，难以满足链上游戏逻辑更新、漏洞修复对合约系统的需求，因此我们在设计合约系统时针对游戏合约需要更新、漏洞修补等场景的需求做出了可迭代更新的合约系统设计。

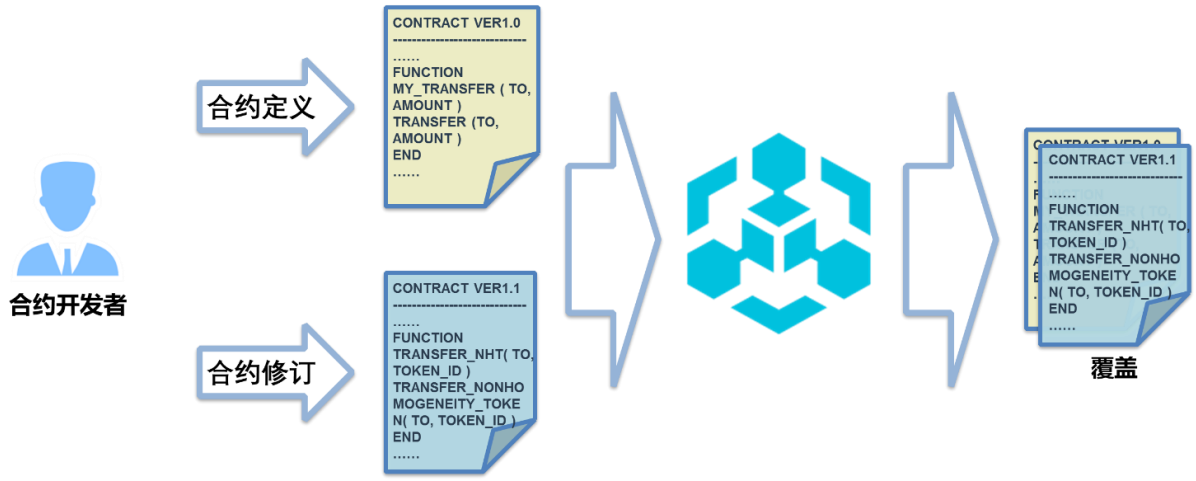


图 3-2-1 智能合约迭代更新

当合约开发者将定义的合约发布至链网络后，系统允许具备此合约开发者权限的用户使用修改后的合约更新此合约，虽然旧的合约仍然存在（确保合约的公开和公正性），但链上的合约地址的内容将被新的合约数据覆盖，多合约应用无需更新引用关系。

3.3. 声明世界观

当下游戏体系中，许多道具设计都是泛用，为了减少重复设计、增加游戏开发效率以及趣味性，Cocos-BCX 引入了世界观的概念，世界观相同的游戏资产和道具可以进行互通。区块链游戏的世界观是一种用于区分故事设定、角色/道具/规则设定和效用范围的标识，游戏道具在世界观遵循统一的世界规范，世界观相同的游戏资产和道具能够通过支付迁移费用在本世界观下的不同游戏世界中迁移、互通，即游戏道具的“穿越”。

在 Cocos-BCX 设计中，世界观中定义了一类非同质数字资产的使用场景、流通规则、定制登记，以及世界观的基本信息即世界观 ID 以及世界流通代币符号等。

以“型月世界”（TYPE-MOON）为例，其世界观是统一的——每作有相同的世界观，并且在不断完善它。其作品包含：

- 同人作品发售的月姬；
- 作为个人小说出版的空之境界；
- 作为商业化第一作的 Fate/Stay Night；
- Fate/Stay Night 的 fan disc Fate/Hollow Ataraxia；
- 剧情格斗游戏 Melty Blood 系列。

一个世界观内的各作品中的人物、道具、设定体系通常是通用的，现实中也常有数个厂商共同在一个世界观中开发各类作品的情况。

Cocos-BCX 允许游戏开发者在创世时声明世界观，允许世界观有自己的治理委员会（和共识委员会），未来还将允许世界观具备自己独立的链环境。

3.4. 跨越世界的道具“穿越”

世界观相同的游戏资产和道具可以在本世界观下的不同游戏世界中互通，例如图 3-4-1 中的游戏 B 的道具，可以进入游戏 A 与游戏 C 的世界中进行使用。

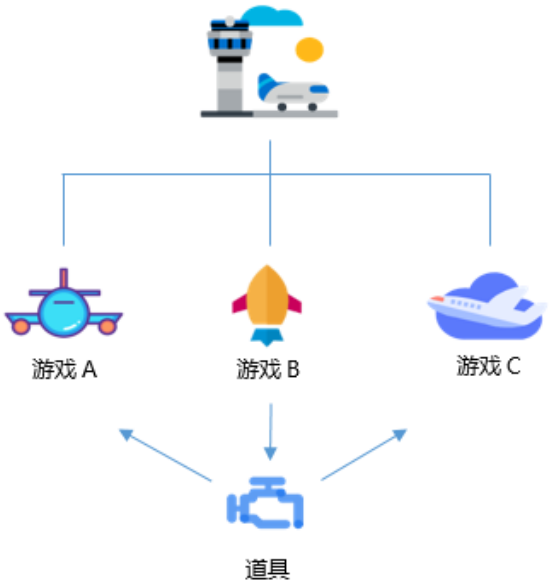


图 3-4-1 支持相同或相似世界观的不同游戏道具流通

游戏道具在世界观遵循统一的世界规范，能够通过支付迁移费用在本世界观下的不同游戏世界中迁移，即游戏道具的“穿越”；道具是一种用于链上游戏的非同质数字资产，道具的“穿越”即同一世界观下的资产在不同游戏应用的过程；不同游戏对该资产的修改会存储在游戏各自的域数据中，游戏间的数据在默认的设置下互不干涉，能且仅能修改自己的域数据。

图 3-4-2 一个链上游戏资产在世界观内不同游戏世界中迁移的示例

3.5. 铁匠铺机制

“铁匠铺”的本质是一系列具有道具、装备制作权限的帐号和一系列合约，作为所有游戏世界的核心功能之一，铁匠铺可由游戏厂商管理，亦可由玩家公会、设计师工作室经营。玩家可通过铁匠铺，将金币和材料合成为道具（或直接求购道具）。铁匠铺创造道具的过程公开透明，与游戏中的其他道具一样具有唯一性，能够从区块链浏览器中检索和查询。

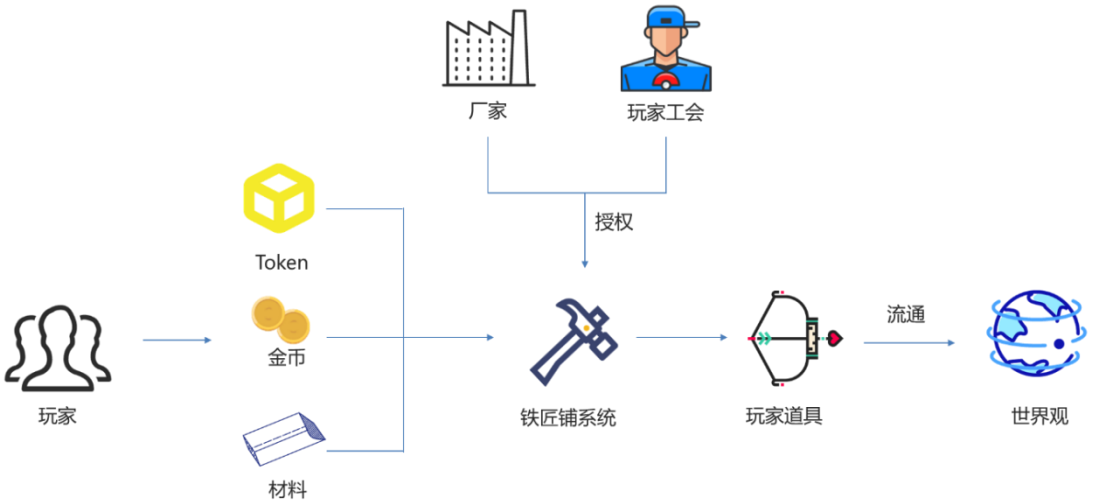


图 3-5-1 铁匠铺锻造资产及资产流通

铁匠铺机制中，合并多个道具操作为一个原子操作，以确保事务的原子性，事务中的所有操作只会同时成功或同时失败。此外，在“玩家-铁匠铺-玩家”的整个过程中，核心部分包含：玩家提交素材给铁匠铺，铁匠铺将制作完成的游戏道具交给玩家，两者合起来可视为一个完整的事务。两步行为信息都将在链上存在，确保用户的资产流转信息真实可靠不可篡改，保证玩家发布流通的材料、游戏金币等数字资产不会像以往中心化的游戏系统一样出现暗箱操控，数据丢失等情况，能够切实保护玩家利益。

铁匠铺拥有以下特性：

- 具有道具、装备制作权限的帐号和一组合约；
- 铁匠铺是独立于游戏的道具产出点；
- 铁匠铺的道具具有唯一性；
- 道具生成、设置道具属性、变更道具所有权到用户等合并为一个原子操作；
- 铁匠铺由世界观管委会（厂商、玩家公会、设计师联盟）管理。

Cocos-BCX 允许向铁匠铺授权世界观下的道具产出权限。例如胜利与誓约之剑，可以有亚瑟传奇世界观的版本，亦可以有 TYPE MOON 世界观的版本，两者可在各自的世界中跨作品流通，使用统一的世界观的同质资产进行该世界观下的资产流通标准。

3.6. 道具嵌套组合

游戏中装备道具可能是由多个组件、物品组合而成的，Cocos-BCX 设计中，区块链游戏的非同质数字资产，即道具也具备能够嵌套包含的特性。

每一个道具都可以由多个道具组成，父级资产可以包含一个或多个子级资产，子级资产又可以包含其他的子级资产，例如图 3-6-1 中的道具“红色彗星”由子级道具“引擎”、“机轮”、“武器”组成，而子级道具“引擎”和“机轮”又分别由子级道具“燃油”、“滤清器”和“齿轮”、“轮胎”组成。

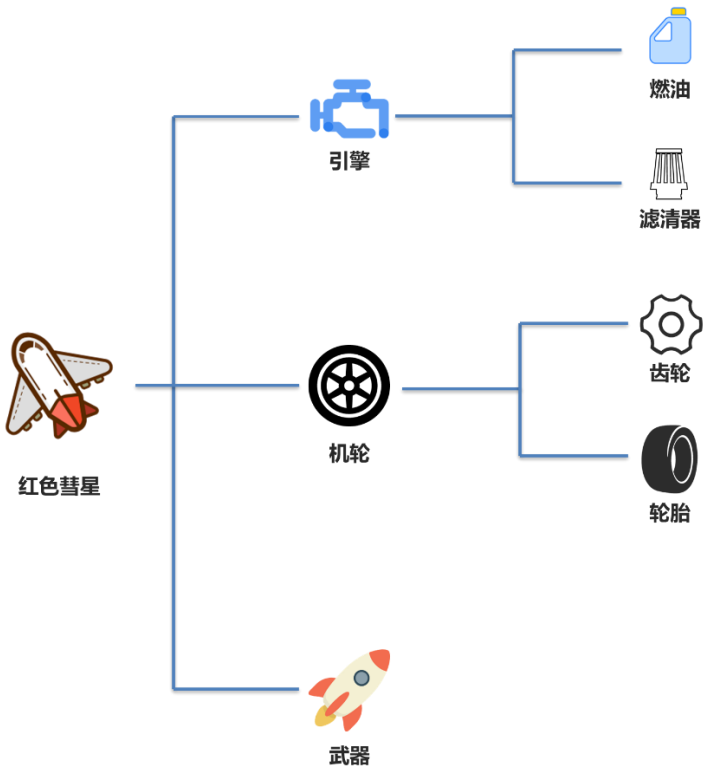


图 3-6-1 道具嵌套组合

3.7. 道具资产流通平台

Cocos-BCX 项目中，道具买卖主要由两个函数实现：

道具的求购是一个多步合成的原子操作，在支付费用的同时完成用户账户游戏道具数据的更新，如果账户资产数据更新动作中任一个动作不被主链区块认可，则整个求购事务将被回滚。

对于道具的出让，Cocos-BCX 提供的函数并不能直接变更特定资产的所有权，而是向 OTC 资产流通平台（中心或去中心）发起出让资产的请求。原则上讲，链内只允许用户对自己的资产发起主动操作，而不应被任何第三方控制，例如平台对实际资产的托管、代管出让。OTC 资产流通平台需记录本函数执行成功时生成的 orderObejct 请求对象。（在发起前可调用 getItems 函数，列出用户道具，以便用户选择出让）当求购请求抵达时，实质是请求的点对点匹配。

与传统的游戏交易平台不同，Cocos-BCX 的去中心数字资产流通平台并不存在中介机构，一方面提高了双方完成流通的效率，一方面能够让原本支付给中介机构的费用直接支付给了卖方，达到卖家多获益、买家少消耗的效果。

玩家可以在道具流通平台完成“游戏金币”和游戏中道具资产等非同质资产的出让和求购行为。在整个流转过程中，为了更加高效的帮助用户完成流转服务，平台将采用智能合约进行自动撮合。

流通平台将对接多平台运行的游戏数据，由于具备最佳的兼容性和可定制特性，游戏厂商可以灵活设计自己的链上游戏存储结构，并将游戏数据对接到流通平台，用户可以方便的在流通平台查询到多种游戏的金币和道具资产。为游戏内的资产流通提供强有力的支持。

用户在授权登录流通平台后，可以选择将自己的游戏道具资产以请求的方式提交至流通平台，符合要求的购入请求和出让请求将被系统自动撮合，内容不局限于游戏内货币等同质资产，也涵盖道具、装备、游戏数据等非同质资产。

完成发布请求后，请求信息将被写入链上。游戏内对应的资产也将被同时冻结。

一个典型的资产流转过程如下图所示：

图 3-7-1 数字资产流转过程

3.8. 一个道具流通平台的实例

流通平台中可以完成 COCOS、独立发行的“游戏金币”（同质数字资产）与道具资产（非同质数字资产）的自由流通。

流通平台中游戏金币的兑换服务主要包括使用 COCOS 与各种游戏金币相互兑换、不同游戏间金币的互换、流通等服务，其中不同游戏金币的价格由其对应的 COCOS 比值决定。流通平台能够在提高游戏行业流转率同时给不同游戏金币的价值提供一个统一的评估依据。

流通平台中的游戏内容流通则主要用于 COCOS、金币与游戏道具资产的互换、流转。由于游戏道具数据的高度自定义性，不同的游戏道具的数据结构可能不一致，故接入游戏内容流通平台的游戏内容需由游戏厂家授权并提供解析方法。

用户在游戏内容流通平台上提交求购、出让请求时，请求对应的游戏内容（金币或道具等）将被锁定，暂时无法在游戏内继续使用。请求中包含出让人的账户 ID 以及出让的资产信息，当请求完成时，系统自动完成所出让非同质资产的所有权转移，并且向出让人获得求购人支付的资产。在请求发起到完成的过程中，双方数字资产的转移操作将被合并为原子操作，即请求内双方的动作将被打包成一项事务，这些动作的状态具有一致性，事务正常完成将产生唯一链上可查的事务 ID。其流程参见图 3-8-1 所示。

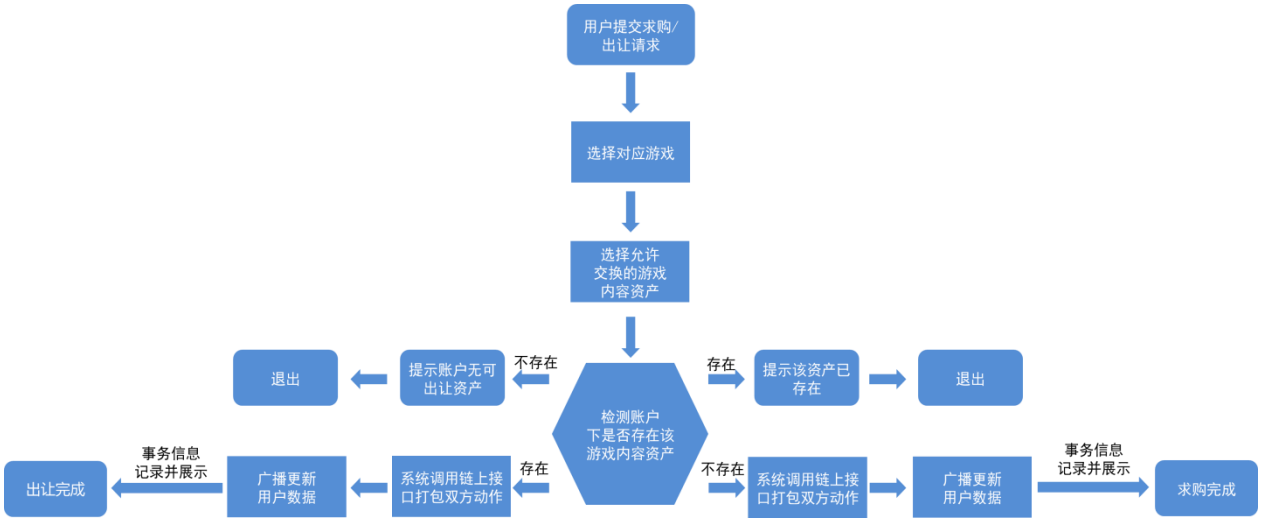


图 3-8-1 游戏内容请求/匹配流程

3.9. 增强的资产权限系统

3.9.1. 细化资产权限和链内操作以支持更多业务形态

Cocos-BCX 中设计资产权属分离，细化现有的资产权限系统，分别设计使用权与所有权：使用权决定用户是否具备资产的大部分操作权限，所有权决定用户是否具备资产的实际归属权和关键操作权，某些特定操作在进行时可能需要所有者与使用者共同签名。

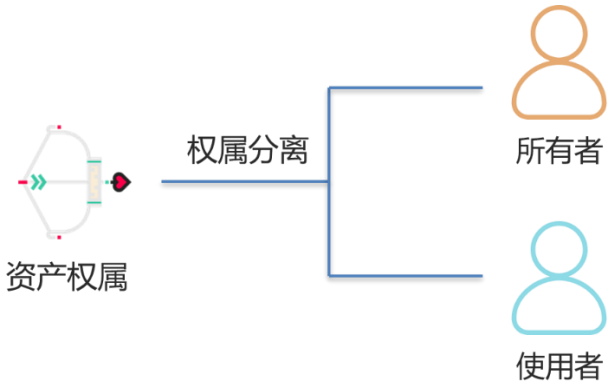


图 3-9-1 资产权属分离

链内操作细化，Cocos-BCX 链提供能够被合约调用的，能转移所有权和使用权的操作；提供能被合约调用的且能创建一个定时任务的操作；创建定时任务的操作时能够指定到期时会执行的任务（如调用一个合约函数）。

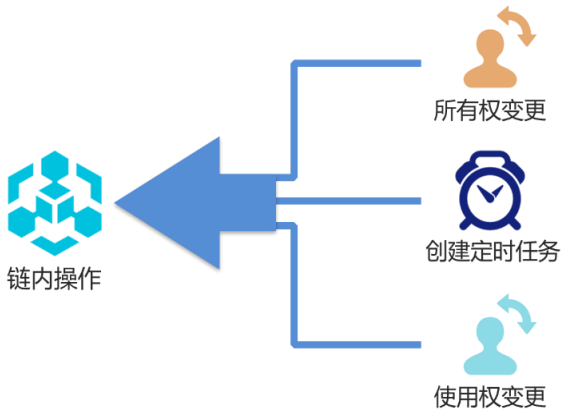


图 3-9-2 细化链内操作

3.9.2. 通过合约与新增 OP（操作）实现新型业务模式

改进的 Cocos-BCX 链新增了多种原子操作和数据结构用于实现可能的新型业务，结合自身合约系统，开发者能轻松实现传统链/合约系统无法做到的业务逻辑，例如资产租赁、抵押、典当等。

租赁

在合约中定义租赁业务各流程的函数，在达成租约时，合约函数通过组合权属变更 OP 和一般交易 OP 实现交租、权限变更等行为，利用链的定时任务 OP 定义租期达到时收回使用权等业务行为。

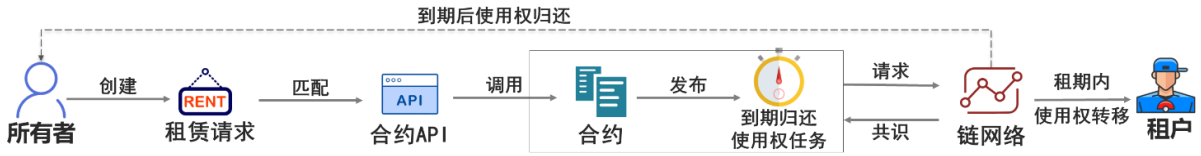


图 3-9-3 资产租赁过程示意图

抵押

在合约中定义抵押业务各流程的函数，在达成抵押行为时，合约函数通过组合权属变更 OP 和一般交易 OP 实现支付抵押款、所有权变更等行为，利用链的定时任务 OP 定义抵押到期时收回使用权或期限内赎回时转还所有权等业务行为。

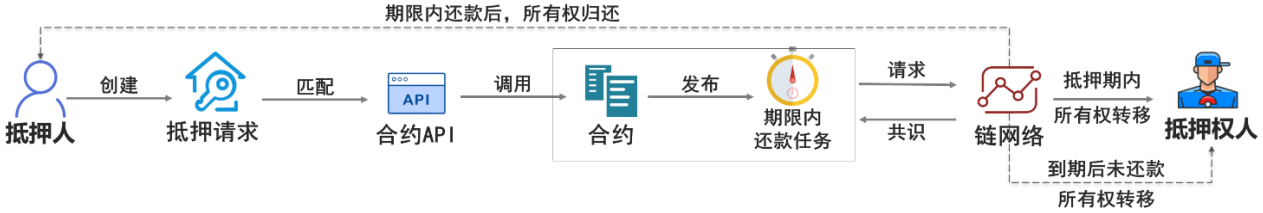


图 3-9-4 资产抵押过程示意图

典当

在合约中定义典当业务各流程的函数，在达成典当约定时，合约函数通过组合权属变更 OP 和一般交易 OP 实现支付典当款、使用权变更等行为，利用链的定时任务 OP 定义典当到期时收回所有权或期限内赎回时返还使用权等业务行为。

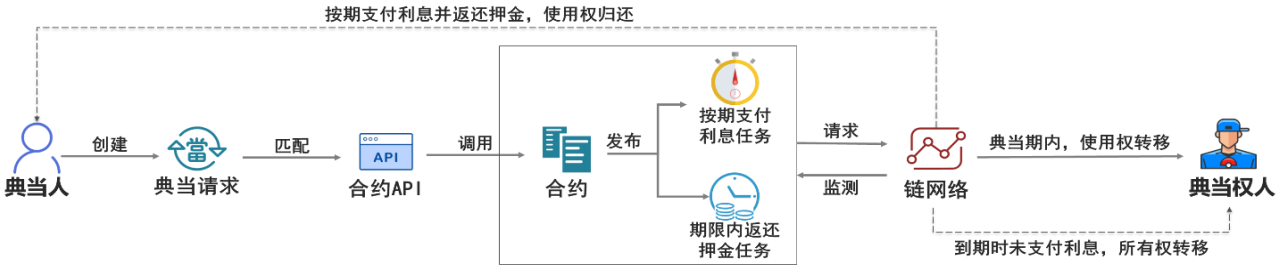


图 3-9-5 资产典当过程示意图

3.10. 玩家自治和资产安全

Cocos-BCX 公开节点工具包，游戏开发商、运营商、玩家公会、设计师工作室等均可成为节点，并参与理事节点选举。

由于区块链网络公开、透明的特性，玩家在游戏中所获得的数字资产信息可通过区块链浏览器被任何人查阅到。而在游戏世界中，拥有高价值非同质资产的帐号往往成为盗号者、黑客勒索的首选目标。Cocos-BCX 对玩家账号的资产安全非常重视，针对游戏资产安全提供以下安全保障机制：

- 操作权限制

  游戏内道具所有权及处置权仅归玩家所有，物品销毁的操作仅能由用户自己授权处理；

- 关键操作原子化

  发生资产流通、资产创建等重要行为时，请求被提交至流通平台或铁匠铺，在完成流通或这制作的过程中的所有操作被视为一次不可分割的原子事务，即这些过程中的参与行为均需被同时共识认可才被视为通过，如果其中任意一个操作不被链网络认可，则整个操作过程将被回滚，避免发生异常的事务过程；

- 可扩展的多步验证

  除去区块链事务验证密码以外，游戏商提供进一步的二次密码验证以及随机码验证等，进一步提高玩家资产安全性。

3.11. 可视化的合约编辑器

Cocos-BCX 项目向开发者提供的可视化合约编辑器，编辑器从用户友好的角度简化设计，将合约常用的功能、方法等以图形化的方式展现给用户，即使是不具备脚本编写能力的使用者也能够根据需要便捷地完成合约编辑；此外，面向具备脚本编写能力的进阶使用者，合约编辑器也提供更详细的高级编辑模式，为使用者提供充分发挥的途径。

可视化编辑器是一种以图形界面辅助使用者完成快速开发的编辑工具。以按键精灵为例，软件将大部分常用方法以快捷方式展现在工具栏，用户通过简单拖放、点击和填写参数等动作即可完成一段脚本代码的编写和插入。

4. 技术架构

4.1. 集成链交互游戏运行环境

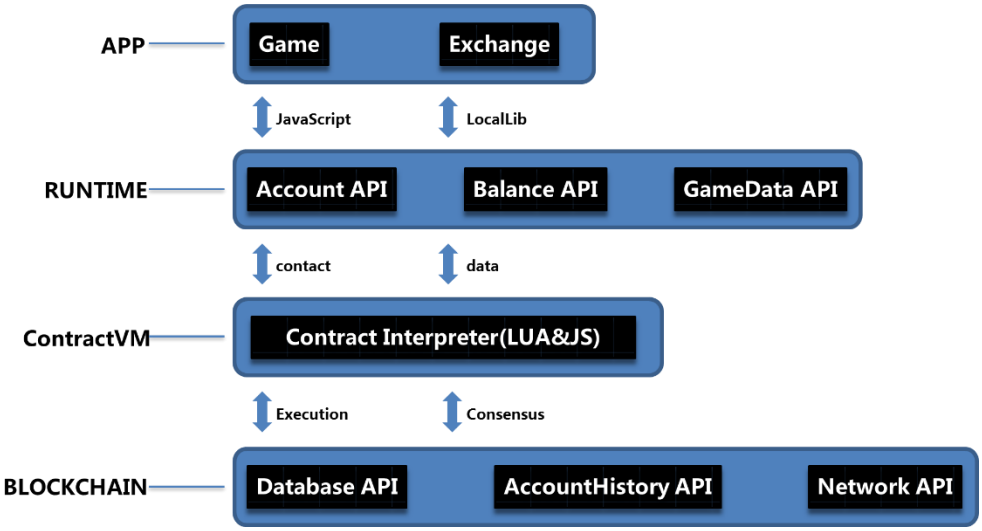


图 4-1-1 Cocos-BCX 链上游戏、应用的运行环境架构

4.1.1. 多平台游戏集成运行环境

Cocos-BCX 认为未来的区块链游戏的运行环境应具备以下的特征：

- 一致和完善的链互操作接口；
- 向下透明的承接方式；
- 封装的原子操作；
- 多平台兼容。

为了简化开发者的使用过程，Cocos-BCX 设计了一套可适配多种类型 APP 的集成运行环境，以及配套的互操作接口。和 Cocos Creator 结合，简化游戏程序和区块链的对接过程，使链内交互工作对开发者透明化，让传统游戏的开发者也能无门槛地开发或迁移区块链游戏。

Cocos-BCX 链上游戏运行 SDK 被集成到 Cocos 引擎 Runtime 中，对游戏提供完整的链交互接口，游戏开发者基于 Cocos-BCX SDK 完成游戏内容向区块链网络的接入，链交互过程透明化、结构化，游戏开发团队不再需要投入研发力量用于适配链网络和不同设备。

同时，运行环境将兼容原生 Android、iOS 和 PC Web、移动 H5 等系统和环境。运行环境内的游戏将具备原生的跨平台能力，实现链上游戏在多个平台无障碍运行的特性。

4.1.2. 区块链交互接口

Cocos-BCX 提供链交互的开发环境，以便开发者能够通过这套环境便捷地与链交互。

Cocos-BCX 的区块链交互开发环境提供兼容多种工作平台的开发组件，包括适配 Android、iOS 系统的 SDK，适配前端 web 应用的 javascript 库，以及适配后端应用的 python、PHP 库等。

开发者能够使用这些开发环境开发自己的区块链软件，实现数据交互，诸如用户注册、用户信息和资产操作、用户游戏数据操作等功能。链上数据接口允许用户在链上存储同质或非同质资产数据，并且为了提供最佳的兼容性和可定制特性，区块链系统不会强制要求资产数据以明文方式存储，游戏开发者可以更灵活的设计自己的链上数据存储结构，以便这些信息可以更为安全地通过游戏客户端和市场的插件解析。

目前链交互开发环境主要提供同质、非同质数字资产和道具查询、转移、所有权变更、事务提交、提议与表决等功能的封装。

4.2. 支持同质/非同质资产和多链铆接的承兑网关

Cocos-BCX 中，同质、非同质资产和智能合约是分离的。可以预见的，Cocos 的网络中会存在大量的、持续发生的事务，需要尽可能降低资产解析和流转的运算成本，更容易实现非同质资产的跨链承兑，并且“资产和合约分离”是更安全的设计。

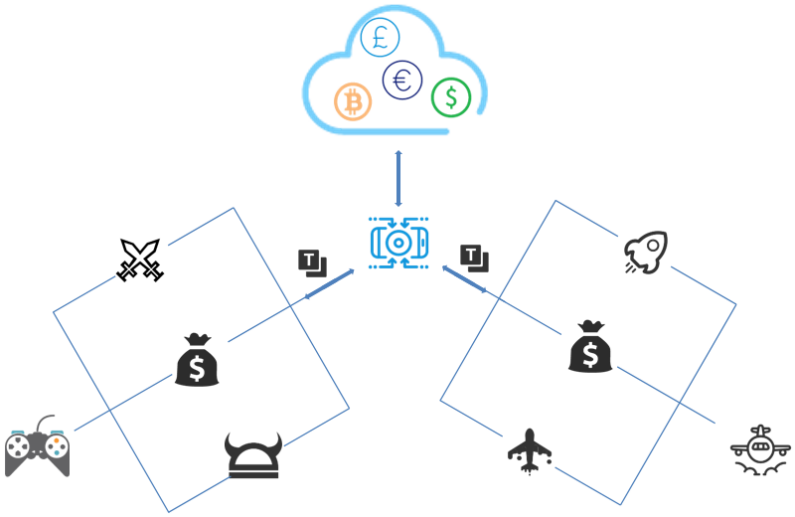


图 4-2-1 承兑网关

Cocos-BCX 提供一套承兑网关用于游戏金币和道具的自动化承兑，在统一的价值衡量体系下，实现链上不同游戏、不同平台间内容的平滑过度，可用于承兑的内容包括游戏金币、游戏装备数据等。

4.2.1. 游戏数字资产的承兑

游戏数字资产与以太坊 ERC20 数字资产承兑如下图所示：

图 4-2-2 ERC20 数字资产承兑关系

游戏金币支持通过承兑网关与其他联盟链以及独立链进行资产转移。

4.2.2. 游戏非同质资产的承兑

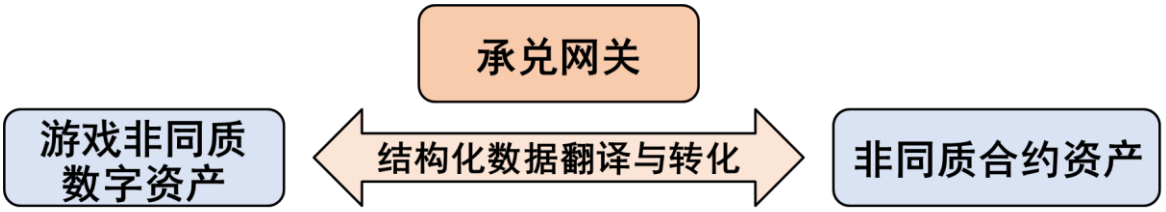


图 4-2-3 Cocos-BCX 与 ERC721 数字资产承兑关系

BCX-NHAS-1808 是 Cocos 应用中适用于去中心分布记账式网络的非同质数字资产标准，具备资产与合约分离的特性以及可扩展、可自定义的数据区域，可兼容其他非同质资产标准。

ERC875 和 ERC721 数字资产标准都是以太坊针对非同质数字资产的标准协议。在某种程度上，ERC875 更像是 ERC721 的“简略缩水”升级版。ERC721 创建了非同质数字资产的标准先河，其随后更新的 ERC841 和 ERC821 都是在其上某部分进行的优化修改；而 ERC875 标准则更加简单直接。其定义的函数包括 name 、symbol、balanceOf、transfer、transferFrom、totalSupply、ownerOf、trade。对比 ERC721 标准，ERC875 的函数更加简单。

通过进一步扩展承兑网关支持的数字资产技术，网关将能够在未来支持以 ERC721、ERC875、BCX-NHAS-1808 为代表的非同质复合型合约，承兑网关对游戏道具与非同质合约的承兑类似于一个专用编译器，通过对结构化数据的翻译和转换，实现非同质合约到链内游戏道具的双向承兑，兼容更多类型的链内外道具流转，提供更丰富的游戏内容和用户体验。

4.3. 对已有区块链系统的优化和扩展

4.3.1. 改进的非同质数字资产数据结构

非同质数字资产是一种应用于分布式记账网络中的数字资产类型，资产实例具备唯一性，通过对非同质数字资产结构的优化可以使其更加灵活地服务于区块链网络游戏。

Cocos-BCX 重新设计数据结构，增加自定义数据存储，以容纳可能的游戏数据和扩展内容。同时也相应调整共识、见证、出块等关键流程，以匹配新的数据结构。BCX 中的道具数据，只在生成和属性变动时在块数据中作完整记录，普通的事务和流转时，则仅记录哈希指针，确保块数据的体积不会因长期的事务过快的增长。

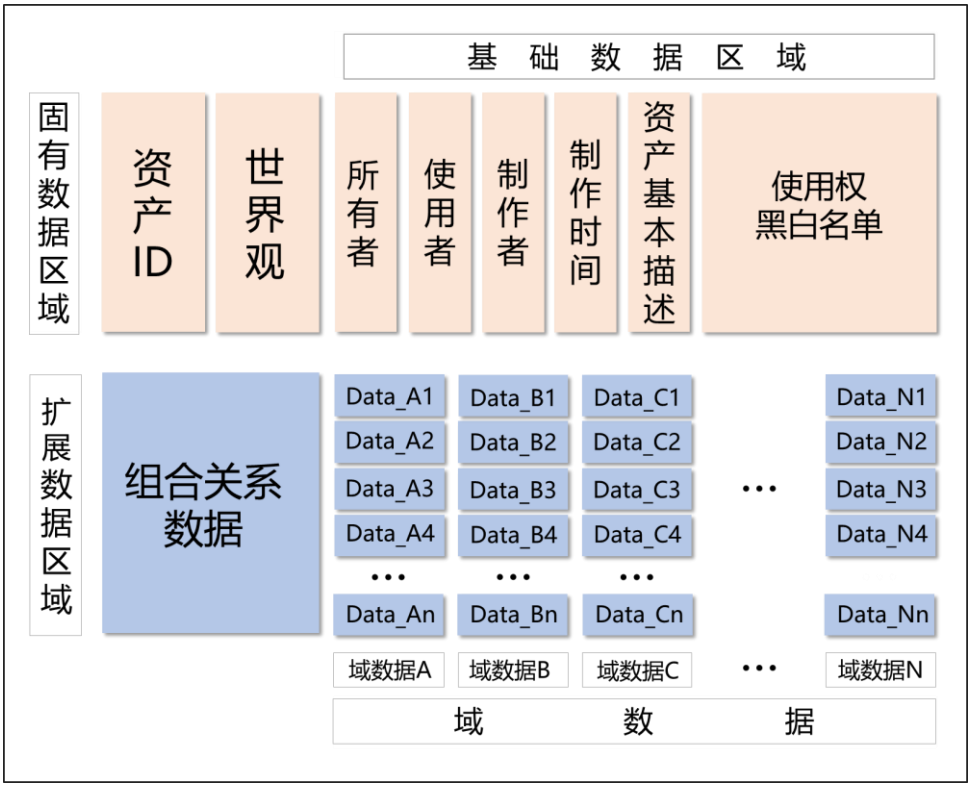


图 4-3-1　非同质数字资产各部关系与数据结构图

区块链网络中非同质数字资产数据结构分为固有数据区域和扩展数据区域。

其中固有数据区域存储非同质数字资产的基本信息，包括资产 ID、世界观申明和基础数据区域三部分。资产 ID，即资产实例在分布式账本网络中的唯一标识，是该资产在被访问、查询、修改时的唯一凭据；世界观申明，包括世界观 ID 以及该资产生效和支持的游戏类型、世界，以及此资产在网络中流通需要使用的世界流通货币类型；基础数据区域又分为资产基本描述、制作时间、制作者、所有者、使用者、使用权黑白名单等信息。

扩展数据区域是为非同质数字资产属性扩展设计的功能板块，包括组合关系数据和域数据两部分。组合关系数据描述资产组合、嵌套和从属关系。扩展数据区域支持非同质数字资产属性扩展，数据单位称为域，是该资产支持的世界观内游戏具体业务数据的存储区域，不同的游戏或者其他业务实体在域数据拥有专属的域标识和数据区，并且数据区相互隔离，每一个域绑定若干个仅对自己负责的合约，域数据以域标识和数据的键值对形式存储，代表该资产在具体游戏内的数据如攻击值、防御值、耐久度等。

此外，分离的使用权和所有权设计，使得基于链权限系统的租赁、抵押、典当等复杂金融模式的业务设计具备了可行性。

Cocos-BCX 中非同质数字资产标准 BCX-NHAS-1808 与其他以太坊非同质数字资产标准相比，具备很多优势：具备资产与合约分离的特性以及可扩展、可自定义的数据区域，可兼容其他非同质资产标准。

特性 \ 资产	ERC-721	ERC-1155	ERC-998	BCX-NHAS-1808
唯一性	合约资产之间各不相同	合约资产之间各不相同	合约资产之间各不相同	合约资产之间各不相同
数据扩展性	支持自定义的数据类型	支持复数组自定义的数据类型	支持自定义的数据类型	支持多个可扩展的自定义数据域
嵌套组合	无原生的嵌套设计	无原生的嵌套设计	支持资产的嵌套组合等关联方式	支持资产的嵌套组合等关联方式
权限控制	与同质资产相同的权限设计	以白名单方式控制资产访问权限	与同质资产相同的权限设计	以扩展域数据控制资产访问权限
与合约的关系	数据存储在合约数据库中	数据存储在合约数据库中	数据存储在合约数据库中	资产数据与合约分离，独立存在于链网络中

图 4-3-2 现行的非同质数字资产标准对比

4.3.2. 资产与合约的数据分离

同质、非同质资产和智能合约数据在链上的存储是分离的。

Cocos-BCX 的网络中会存在大量的、持续发生的事务，需要尽可能降低资产解析和流转的运算成本，资产与合约分离可以实现合约的单独解析执行以及必要结果上链的操作。

在资产与合约数据存储分离的设计下，资产拥有者具备该资产的全部权限，资产的操作仅能由拥有者的授权完成。可以避免因资产合约不分离而出现通过修改合约内容而破坏资产属性或者调用他人资产的情况发生，并且不考虑合约因素的制约则更容易实现非同质资产的跨链承兑，因此资产和合约分离是更安全的设计。

4.3.3. 改进的 DPoS 共识机制

Cocos-BCX 测试链的共识层采用 DPoS 共识算法。

DPoS 算法通过预定见证人和规定时间槽位来推测区块的生产者以及出块时间，通常时间槽位间隔为 5 秒，在实际使用过程中为了更快的网络广播速度以及更大的网络吞吐量而将时间槽位间隔设置为 3 秒，如果预定的见证人在规定的时间槽到来时，因为网络原因或者设备硬件故障没有正常的出块，则该时间槽位不会出块，网络将等待下一个时间槽位到来选择另一个预定见证人进行出块。

Cocos-BCX 中，所有的预定见证人都由所有的持股人从见证人中投票选举，预定见证人统称为活跃见证人，活跃见证人数量通常为 11-101 个。所有的活跃见证人在 DPoS 共识算法的见证人预定算法中具有相同的出块预定概率，这保证了所有见证人的出块概率和获取出块奖励是一致的。石墨烯投票更新时间通常为 24 小时，但出于安全性、稳定性、公平性的考虑，项目初期网络投票更新时间通常较短，可能为 12 小时甚至更短。

特性	POW	POS	DPOS
更高的吞吐效率	✗	✓	✓
更快的确认速度	✗	✗	✓
高效且低能耗	✗	✓	✓
社群激励机制	✗	✓	✓

图 4-3-3 现存共识机制优劣势对比

在 DPoS 算法中通过预定见证人和规定时间槽位来推测区块的生产者以及出块时间，主链的活跃见证人总是多于支链，故此主链区块高度一定高于支链，同时全网投票机制避免了见认证人集中化，保证了网络的安全性，不同见证机制之间的优劣对比如图 4-3-3 所示。

4.3.4. 使用现代密码学保障的安全性

现代密码学技术是一门基于数学原理的密码学技术，目前已经广泛应用于互联网领域的多种行业，常见的对称加密技术包括 WiFi 使用的 AES 加密，以及不对称加密算法（公私钥密码体系）RSA、ECC 等，其中 ECC（椭圆加密算法）是区块链领域常用的加密算法。这些算法通过数学原理设计出一种不可接受解算消耗的加解密体系来防止加密被攻破。在没有正确获得密钥的前提下，对此类加密算法的破解尝试均会因为计算量过大导致实施时间过长（通常需要花费近百年的时间用于尝试破解/猜解密钥体系）而失去破解行为的价值。

ECC 算法全称 Elliptic curve cryptography（椭圆曲线加密算法），于 1985 年由 Neal Koblitz 和 Victor Miller 分别提出。

4.3.5. 低分叉风险

在比特币和以太坊网络中的工作量证明机制下，矿工遵循相同的机制，当矿工同时挖出了两个区块时，就出现了分叉现象。在遵循“最长链”原则的共识机制下，分叉的链会在 6 个区块后，短的链就会被废弃。但是当矿工不遵循同样的机制时，就会出现两种会产生深远影响的分叉结果，软分叉和硬分叉。相对而言，软分叉就是区块链系统的旧版本与新版本的区别，当原有旧系统完全升级后，软分叉现象就会消失；硬分叉是原本同一区块链主链的矿工，选择采取不同的共识机制进行挖矿，同一条主链将会被分成同源但却分离的两条链。2016 年 7 月份的“The DAO”事件就是最著名的以太坊网络硬分叉案例。而当以太坊分叉为以太坊和以太坊经典后，其对应原有主链的算力就会降低，进而对整个主链网络的安全性产生重大影响。

Cocos-BCX 使用 DPoS 共识机制，不需要矿工使用矿机进行挖矿，可以有效避免中心化算力对整个基础链的影响，进而降低分叉风险。在 DPoS 机制下，若有见证人想要通过投票进行分叉，则需要保证 1/3 以上的见证人都同时违背机制才有可能。与此同时，用户也可以通过票选罢免活跃见证人来降低可能的分叉问题。相比较比特币和以太坊网络的 PoW 共识机制下的高分叉风险，Cocos-BCX 的分叉风险更低，可以有效保证游戏开发者和用户的数据安全。

4.3.6. 多链挂接

除跨链承兑网关外，Cocos-BCX 将在未来支持更加直接的多链挂接方案，例如，在下一阶段的升级中，Cocos-BCX 将支持使用 IPFS 存储大段的合约与一些游戏数据。

4.3.7. 合并多个操作确保事务原子性

区块链游戏的道具制作是原子性的，道具制作者根据玩家提交的需求和材料、资产打造道具，打造完成后，道具转移给玩家。在这一过程中包含一系列操作(OP)：数字资产生成、设置道具属性、变更资产所有权到用户等，为了保证过程中所有操作结果的一致性，我们将这一系列操作合并为了一个事务，即一次原子操作，事务中的所有操作只会同时成功或同时失败。

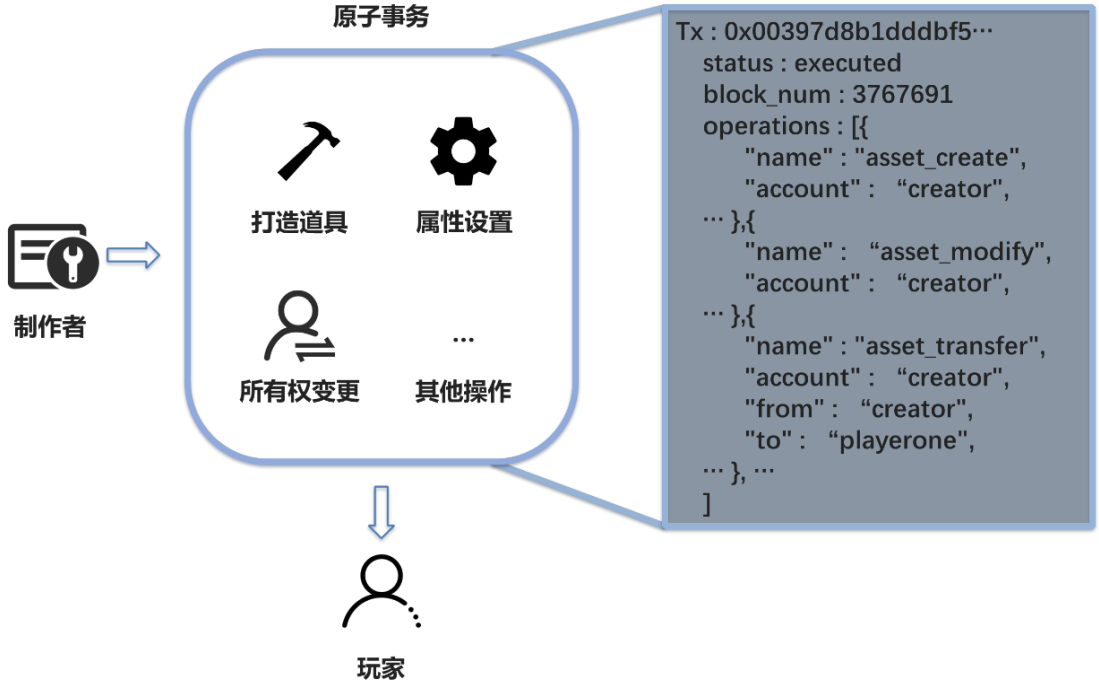


图 4-3-4 多操作原子合并示意

原子合并的另一个应用是 Project BCX 的去中介资产流转，目的是让卖家多获益、买家少消耗。去中介流通平台本身不存储用户的资产数据，而仅作为点对点请求的撮合媒介，游戏厂商可以灵活的设计自己的游戏资产数据结构，可流转的内容不局限于游戏内的同质资产，也涵盖道具、装备、游戏数据等非同质资产。用户在游戏内容流通平台上提交出让请求时，请求对应的游戏资产（金币或道具等）将被锁定，暂时无法继续在游戏中使用，直到取消本次请求。请求包含出让人的主链 ID 以及出让资产的内容，当出让请求达成时，系统自动完成资产所有权的变更，并且向出让人转移购入请求人支付的资产，完成整个流转请求。

发生资产流转行为时，出让/求购以请求的形式提交至流通平台，资产转移与资产的所有权变更被视为一次不可分割的操作，即双方的行为均需被共识认可，如果任意一方资产变更动作不被主链区块认可，则整个事务将被回滚。即在整个流转过程中资产的所有权变更或资产转移等行为将打包在一笔事务内，两个动作的状态具有一致性，事务正常完成后将产生唯一链上可查的事务 ID。

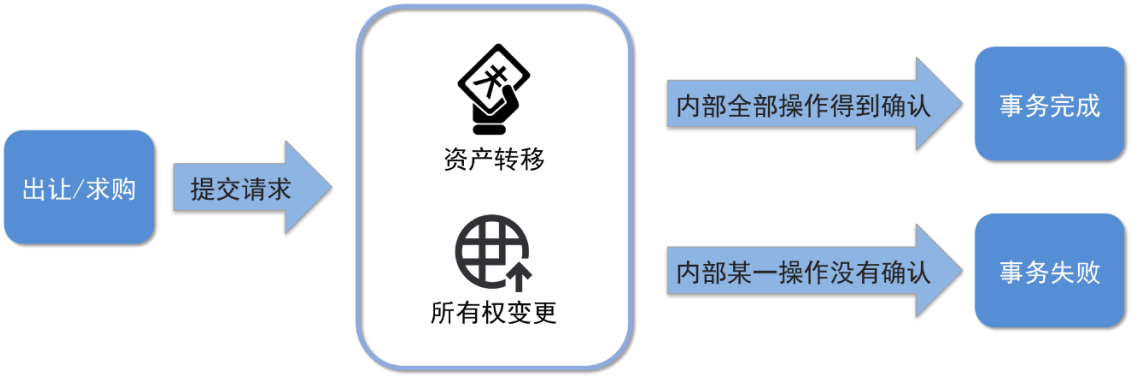


图 4-3-5 原子事务状态判定机制

4.4. BCX 测试链：高效链网络与高速合约虚拟机

Cocos-BCX 拥有足够的高并发处理能力。

目前的绝大部分联网游戏，当用户规模达到一定程度时，其服务器需要在短时间内进行大量的数据处理，而在现有的以太坊网络中是无法实现的。

Cocos-BCX 采用改进的 DPoS 共识，理论吞吐量约 10 万 TPS，其高并发处理性能在合理的数据管理模式设计下足以支持现有游戏的开发与正常运行，基本满足大型联网游戏在平台中的运营诉求，保证用户的游戏体验与现有的中心化游戏几乎没有区别。

由于大规模网络游戏的数据交互频率非常高，DNF 曾创下 60 万人同时在线的记录，Steam 游戏平台更有 1420 万人同时在线的惊人数据。如果每一个在线用户提交数据的行为都视为发起了一次共识申请，Cocos-BCX 的极限吞吐能力不足以支撑这样级别的处理请求，开发团队按见证速度的需求设计了不同的见证委托模式（Delegation Templates），使单一见证委托人不用对所有运行中的游戏作同时见证和处理，而是专注于对复数个同类型游戏作见证和计入区块的工作。并且，在这一模式下，不同游戏的数据提交/见证是相对异步的过程，每一个游戏会选择适合的委托模式，而异步模式下的数据验证则可以通过链上数据库服务来完成，即用户在链上验证并完成数据存取。这一过程非常高效，足够支撑大规模游戏场景下的玩家数据操作。

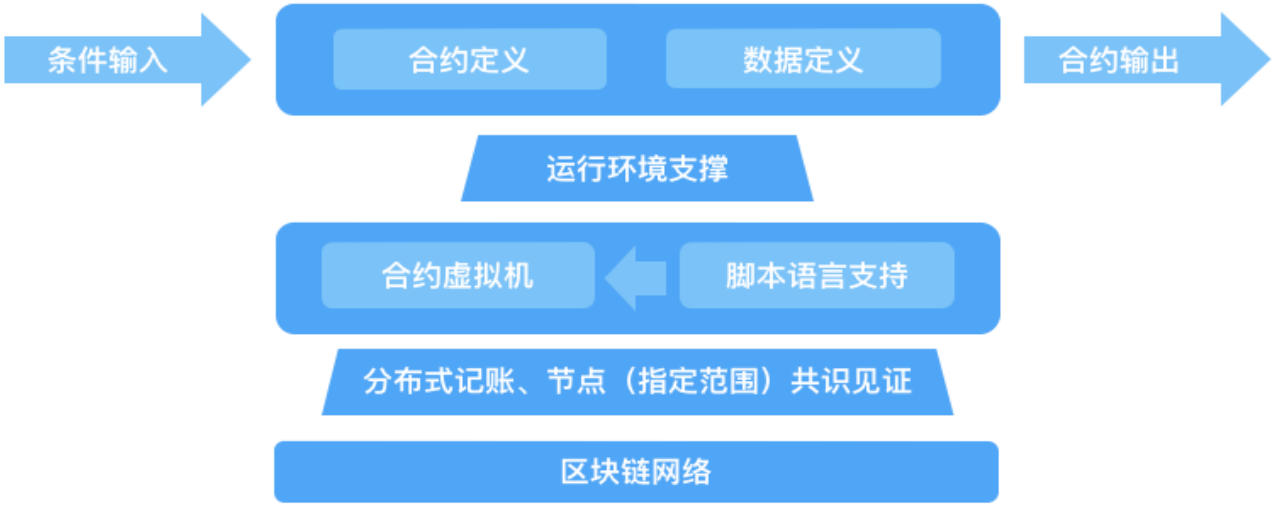


图 4-4-1 Cocos-BCX 的合约

合约是一段可以自动执行的程序，同时作为系统参与者，按照环境的基本规则（编译器规则）执行预设的任务，合约可以定义输入和输出，能够接受和存储价值，同时向外发送信息和价值。智能合约是以“不信任原则”为前提设计的，每一个节点均认为彼此不可信任。由于区块链的分布式保存特性，链上的每一个节点均保存有同样的合约执行代码，合约的运行结果由全网算力共同见证，并通过全体表决形式决定运算结果是否被认可。Cocos-BCX 的合约支持见证委托的定义。

为了保障合约执行的效率足以向用户提供足够良好的游戏体验，Cocos-BCX 重新设计了一套针对链上游戏场景的基于 LUA 的高速合约虚拟机方案。不同于现有区块链的合约虚拟机方案，除了通过大幅定制和优化现有的区块链运行环境及合约虚拟机的执行效率外，Cocos-BCX 的虚拟机使用与游戏 SDK 相同的语言和 API 系统，并提供链和游戏执行环境的互操作接口，这将彻底改变区块链合约环境单一、灵活性差、定制能力差的现状。智能合约的应用场景将不再限于作为货币描述，而是开始能够接纳更多与游戏直接相关的内容，包括可能的诸如：基础规则、设定、单位、场景、甚至地图等。改进后的虚拟机不仅支持更为复杂和灵活的合约形态，并且将大幅度提高现有智能合约的运行效率。

4.5. 链上游戏的分布式记账体系深度开发

在上文中我们提到链上游戏的最终形态是实现游戏整体逻辑的上链运行，但现有的区块链技术尚不满足承载游戏完整逻辑所必须的最低限度特性，其中最为关键的几点包括：

- 节点数据同步的数据量与时间成本

  只有完整节点具备执行合约的能力，但完整节点存储有全网的所有事务数据，其数据量之大显而易见，且新建一个节点时同步这些数据的时间消耗也非常惊人；

- 游戏逻辑完整上链需要能够支持大型合约

  若实现游戏完整逻辑上链，那么合约本身将包含游戏的全部后台逻辑，合约将可能变得非常大，甚至超过一般区块的块大小，而在现有区块链技术的设计下，无法被块容纳的合约是永远无法运行并得出结果的；

- 合约持续执行

  游戏逻辑完整上链则意味着一个游戏应用在结束前，游戏合约将会持续运行，也即是游戏合约的运行时间是远大于出块周期，跨块执行的，现有任何区块链技术都无法支持这样的合约运行模式；

- 事务执行延迟

  游戏完整上链意味着链上处理了所有游戏中可能会执行的事务，其中不乏要求高速响应的部分，而传统区块链的事务响应取决于出块行为，而最快确认速度也受限于出块周期限制，难以满足游戏合约对事务即时响应的需求；

- 随机过程无法共识

  链上随机过程规则由智能合约描述，而合约的过程是公开的，若需要产生无法被第三方推算的随机结果，则需要合约运行时有节点的噪声参与这一过程的输入，但不同节点的噪声不可能一致，即其他节点无法通过再次运行这份合约来验证这次随机过程的结果是否正确，最终导致无法完成共识；

- 链内实现的定时器与心跳

  定时器与心跳机制是所有链上合约、游戏内容实现定时运行、自动运行、条件运行的前提条件，而这一特性的时候背后还隐含了时间同步、同步防伪等过程，这对现有区块链技术来说是完全空白的区域；

- 数字资产权限

  传统区块链数字资产记录在合约数据区域内，资产不能脱离合约，因此合约所有者有权修改数字资产数据，可能导致资产拥有者受到损失。

针对这些问题，Cocos-BCX 提出了对现有的分布式记账体系进行深度改造的设想，提出了下述的多种特性、机制设计，以最终实现链上游戏能够具备实际落地运行的目标：

- 减少数据量和时间成本；
- 在语法级别支持共识任务；
- 合约持续执行；
- 极小的事务延迟执行；
- 链内可信随机过程；
- 链内实现定时器与心跳；
- 非同质数字资产数据结构中增加权限观念。

4.5.1. 轻量级节点

在 Cocos-BCX 设计中，轻量级节点（下文简称为“轻节点”）本质上是一个具备与链互操作能力的环境，与全节点不同，轻节点不需要同步全网数据，取而代之的是同步运行必须的合约信息与环境数据，这样的设计可以大幅减少节点同步的数据量和同步时间，使链上游戏端软件具备了实际使用的容量、时间成本可行性。

Cocos-BCX 开发的游戏整体以合约形式在轻节点上本地化运行，但合约中标识出需要共识的部分将被单独拆分为一个或多个子合约发布至相关节点进行共识（详细介绍见 4.5.4 在语法级别支持共识任务），这样的设计能够让巨大的游戏合约以更具效率、几乎无延迟的方式运行，分别处理合约的共识与非共识部分也能够在尽可能保障用户体验的前提下保持与传统区块链一样，数据具有可靠性。同时，对于轻节点的验证也不再像传统区块链一样进行过程和结果的验证，而是对节点运行环境和输入数据的验证（可信执行环境验证），进一步提高了整体的运行效率。

4.5.2. 合约的持续执行

通过轻节点的方式，游戏整体作为一个合约运行的设想得到了实现可能，本地运行的游戏合约能够长期、持续地在轻节点中运行，这一过程与出块周期或块大小都无关，与之相关的仅是游戏合约中包含共识的子合约内容。

游戏合约与子合约根据语法级别的共识优先级标识，在持续运行的同时也不断完成关键步骤的验证和同步，实现了游戏合约持续运行以及结果共识见证的机制。

4.5.3. 合约会话机制

链上提供会话建立接口，该接口在合约公共数据区建立一个具有有效限制的用户会话列表，会话区间的用户将有权限向同会话区间的其他用户推送事务，其他用户收到数据变动通知时，可及时获取对应数据。

4.5.4. 在语法级别支持共识任务

Cocos-BCX 提出了让合约在语法级别支持共识任务的设计，通过特定的关键词修饰脚本的共识优先级，使合约解释器能够识别并在运行全文扫描时将有标记的需要共识的合约部分拆分出形成子合约发送至链网络的相关节点进行共识，共识优先级别从低到高包括不需共识、正常共识、即时响应、立即确认等。

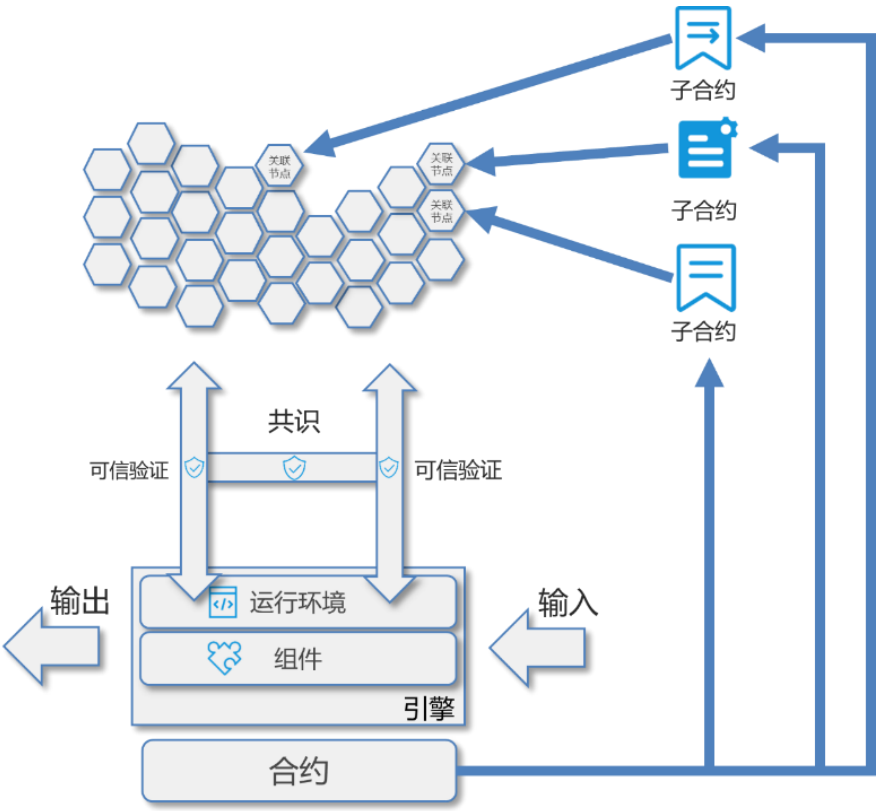


图 4-5-1 轻节点与合约拆分运行原理

合约整体在本地执行，到达需要共识的部分时，根据语法级别的优先级标识来确认共识方法，不同优先级采用不同共识步骤，游戏合约的运行更加流畅，可能发生的阻塞等待更低、时间更短。

被标记为优先级最高的立即确认的合约主体的运行过程与共识过程是两个相对独立的异步过程；被标记为即时响应的合约部分，事务在提交的同时，节点会立即回复信息被提交的回执，即事务 hash 值(Tx ID)；正常共识的合约事务则按区块链事务执行的正常流程被执行；被标记为不需共识的合约内容仅在轻节点上运行。

此外，需要被共识的合约部分是拆分后以子合约方式分发执行的，这些子合约内容应该具备完整的上下文关系和无额外依赖的设计，以便在其他节点上也能正确的得到结果。

4.5.5. 合约的优先共识

Cocos-BCX 设计链上处理所有游戏中需要共识的事务，其中不乏要求高速响应和即时确认的部分，而传统区块链的事务响应取决于出块行为，而最快确认速度也受限于出块周期限制，难以满足游戏合约对事务即时确认的需求。

- 事务的快速异步确认

合约支持语法级别的共识标记，合约运行时，被标记为立即确认的事务将被抽出并立即广播，当任意节点收到后会立即运行该过程得到结果并广播运行结果，同时本周期的出块人将把广播的结果存入结果池，当相同的结果数量达到判定通过的阈值时，出块人立即广播事务确认的结果并将此事务写入出块缓存，整体流程如图 4-5-2。

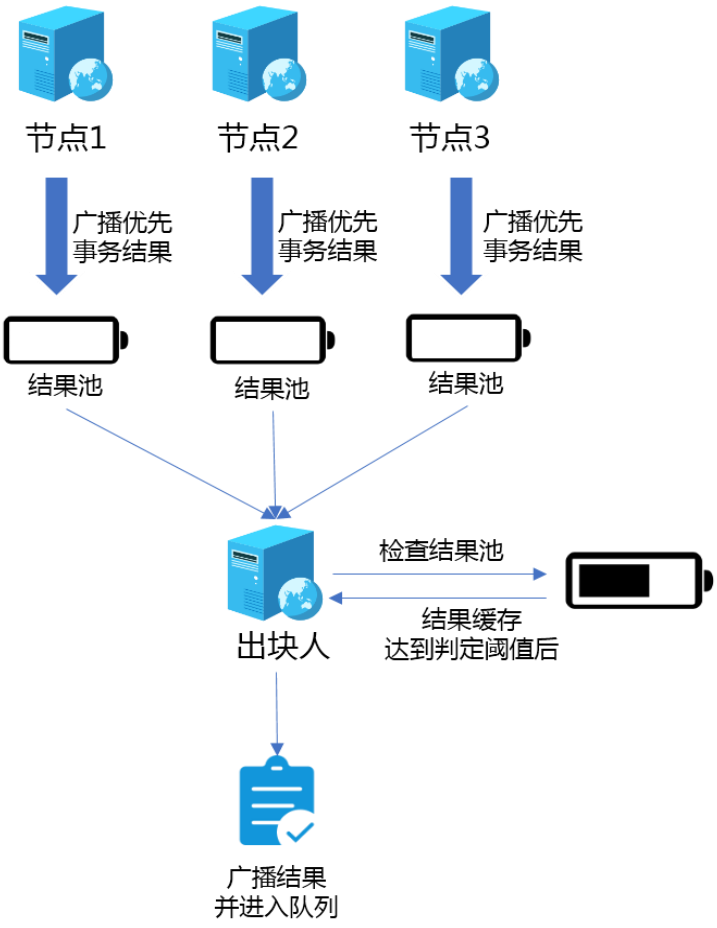


图 4-5-2 异步共识下数据处理示意图

在这个设计下，节点会在第一时间完成事务提交、处理、广播，而区块生成与事务执行过程成了相互异步的操作，达到事务的快速异步确认。

- 即时响应

Cocos-BCX 设计中，优先级标记为即时响应的合约，当用户向节点发出事务请求，节点将立即向网络发出事务广播，并同时向用户返回事务 hash 值。在这个设计下，其实事务最终记录周期与传统设计并没有太大差异，但事务的响应却几乎是没有延迟的，节点会在第一时间完成事务提交，大幅提高了事务的响应速度。

进一步的，用户可通过事务 hash 值跟踪事务状态，同时事务信息将更新到用户历史事务数据表中动态向用户推送，用户不必等待事务在链网络中验证、应用之后的回调再响应。我们借鉴了以太坊的 hash 跟踪特性，并在此之上加入了用户事务动态推送的机制。

4.5.6. 极小延迟的事务响应

传统区块链的事务执行确认是在节点接收到区块数据，完成事务内容解析，运行并得到正确结果验证通过写入块数据时确认的，当一个事务被提交时这个事务实际进入了 pending 队列，而此时事务仍并未执行，直到下一个出块周期，这样的机制导致事务始终无法更及时地得到响应和处理。

- 优先级共识

Cocos-BCX 在语法级别对事务增加了优先级标识的设计，当事务被标记为立即确认时节点会在第一时间完成事务提交、处理、广播，而区块生成与事务执行过程变成了相互异步的操作，达到事务的快速异步确认；即时响应为另一种共识优先级，在这种模式下事务的响应却几乎是没有延迟的，节点会在第一时间完成事务提交，大幅提高了事务的响应速度。

- 分区见证

为了进一步提高节点利用率和处理效率，Cocos-BCX 在委托见证的基础上提出了分区见证的设计，即某些节点专注处理特定类型的合约请求，其原理如图 4-5-3 所示。

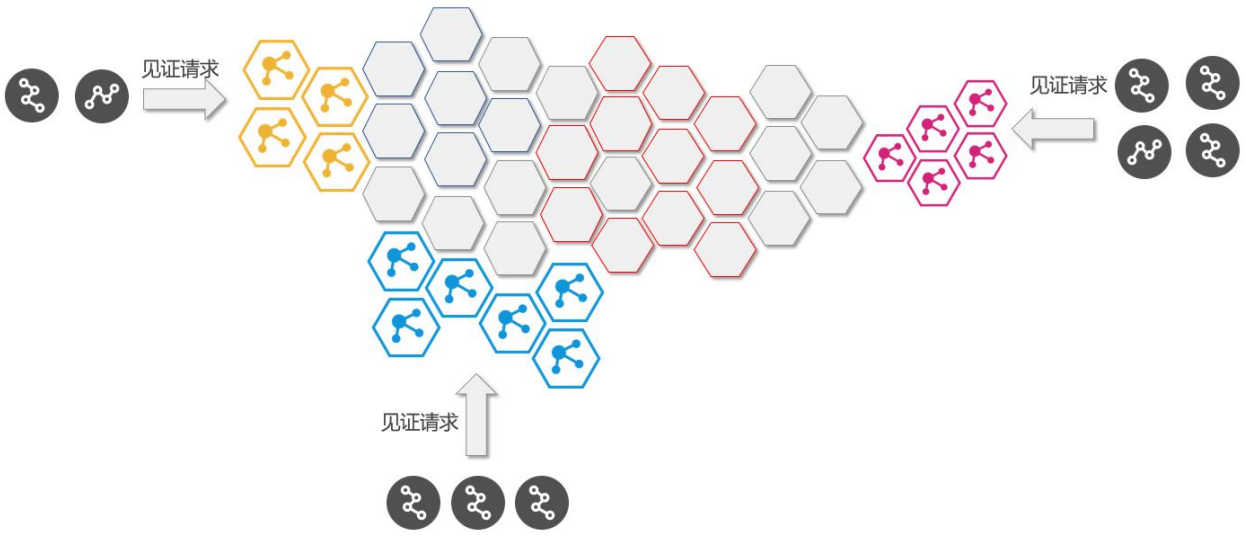


图 4-5-3 合约的分区见证机制

分区见证在游戏行业应用的意义在于能够针对不同请求类型针对性优化相关节点的处理能力，例如对浮点运算集中型请求重点加强核心算力，对结构数据处理集中型请求重点加强存储 IO 能力等，最终达到整体的效率、效益最优配置。

4.5.7. 委托型事务机制

委托型事务主要用于处理随机性高，不同节点执行会产生不同结果的事务类型（如产生一组随机数），但此类型事务仅限于非个人数据关联的事务请求。合约中的共识标记允许定义需要委托参与共识的节点簇 （节点组） 名称，指明事务需要由哪一类节点处理。当数量只有一件时（N=1），被指名的节点簇会随机选择簇内任意一个当前在线的节点分配处理该事务，例如处理随机事件；当委托节点数量大于一件（N>1）或为一个簇时，被指名的簇内的多个节点将被分配至处理该事务。通过可信执行环境认证的受托人收到委托事务之后，会验证事务的可行性并执行委托，完成后将事务结果加密并打包向链上广播。

指定委托节点簇名的设计出发点有两个：一是出于安全性的考虑，只指定委托节点簇名，簇内随机选择节点处理事务，委托方不知道所委托的具体节点，这样可很好地防止作弊；二是从运行可靠性出发，指名节点簇可保证簇里分配事务到当前在线的节点。

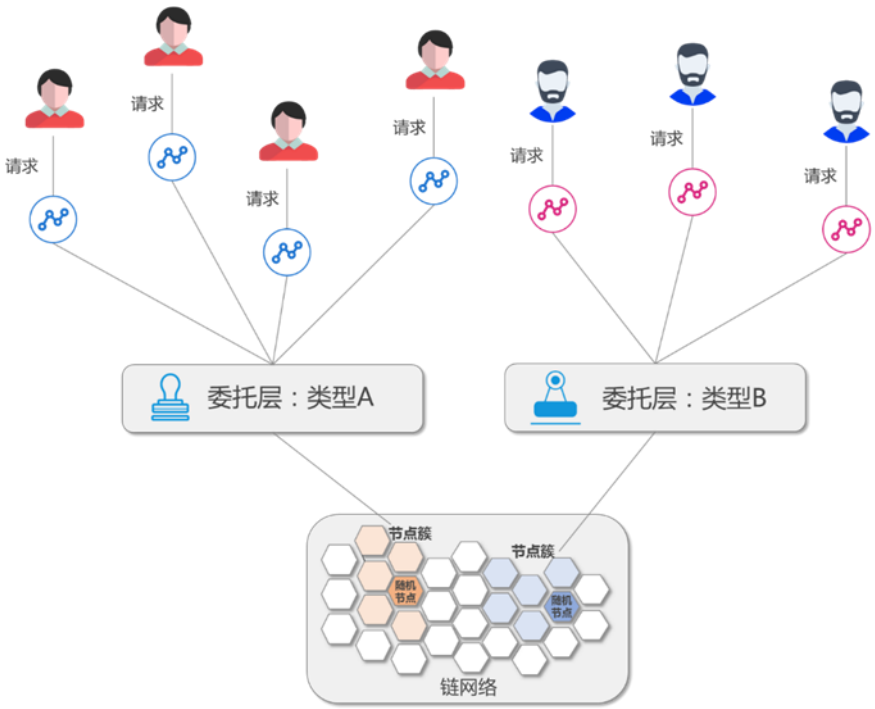


图 4-5-4　基于委托的分区共识

4.5.8. 内源可信随机过程实现

外源随机指随机过程的不确定性因素发生在区块链系统以外，内源随机则反之，外源随机无法保证随机因素的生成过程是能被链系统信任的，因此链系统如何实现合理的随机，其实就是要解决如何保证随机过程及结果可信的问题。

- 实际完成随机过程执行的节点不应知晓此随机信息被使用的场景和对象，以免这部分信息被利用在作弊行为上；
- 随机过程在调用其的业务行为结束前不应被链上公示，以免进行中的业务过程因随机过程的公示失去公正性（例如一局斗地主中各方手牌的构成等）；
- 内源随机过程应具备抵抗 BP/开发者作弊的特性。

目前 Cocos-BCX 已经成功在链内实现了可信的随机过程，并将随机过程调用以接口的形式供合约开发者调用。只需在合约中以一般开发的方式调用 random 函数即可获取内源的随机数据。

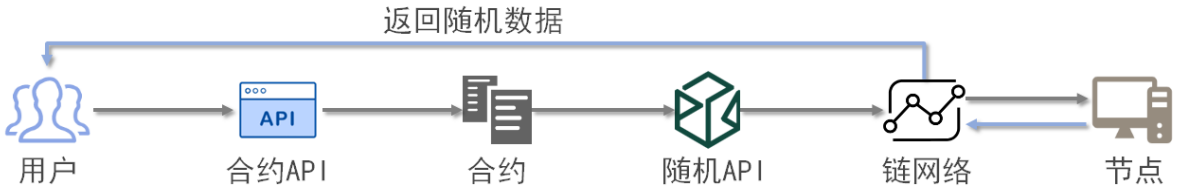


图 4-5-5　链内可信随机过程

4.5.9. 链内的可信随机过程

区块链游戏规则上链能否具有实际应用价值与能否在链上实现随机过程密切相关。通过研究发现，完整的链上随机过程需要解决一个关键问题：链上随机过程规则由智能合约描述，而合约的过程是公开的，若需要产生无法被第三方推算的随机结果，则需要合约运行时有节点的噪声参与这一过程的输入，但不同节点的噪声不可能一致，即其他节点无法通过再次运行这份合约来验证这次随机过程的结果是否正确，最终导致无法完成共识。

要解决这个问题，我们提出了三种可实施的方案：

方案一

- 在区块链动态数据区维护一个或若干随机数据池，出块人将随机过程的结果包裹在区块的加密数据段中并且加密过程的代码以闭源、不公开的形式发布。此时，所有节点将拥有同一套随机数据池。随机数据池的数据结构呈管道形态，具有读端和写端的封装，且仅允许符合规则的读写端访问，具有先进先出的特性。
- 因为区块链的所有节点事务处理具有一致性，应用在申请随机过程结果时可从随机数据池中读取。在该随机过程产生、分配机制下，过程与结果的安全性能够满足区块链网络对随机过程的安全性需求：
  - 任意一种访问（读、写）行为都将导致随机数据池发生变化且无法复原；
  - 写入随机数据的行为由动态加密函数库完成，且函数库闭源、不公开；
  - 随机数据的生产者无法获知此次随机过程的结果将放入随机数据池的位置以及这一随机过程将会被谁使用；

这一随机过程的实现方案适用于链网络对事务处理顺序具有一致性的场景，例如 RPG 游戏中玩家开启地图宝箱获取随机道具的过程。

方案二

- 通过委托机制，允许部分事务委托至某可信节点簇完成处理，节点簇中随机分配当前在线的可信节点执行事务，可信节点完成处理后记录随机过程结果，并由通知或轮询机制让委托方获取结果。
- 因为该方案基于链事务委托机制，对链的改动会小于方案一，但要保证方案的可行性，应满足以下需求：
  - 受托方应通过可信执行环境验证，确保自身可信；
  - 受托方运行随机过程并发布结果时，应采用同样具备安全性的加密函数库完成；
  - 加密数据的传递需通过“零知识证明”或其他可靠证明方案证明受托方身份并能够被委托方识别，确保委托方得到的数据不是由第三方伪造。

此随机过程实现方案适用于事务具有多方参与但仅需要同一批随机结果的应用场景，例如棋牌游戏中每一局的洗牌顺序等。

方案三

- 当前的区块生产者接收到随机事务，通过随机函数生成一个随机结果并将随机过程与随机结果通过加密函数加密写入区块数据，并打包发送到全网，其余普通节点接受该随机结果并应用，以此完成随机事务的共识。

这一随机过程的实现方案已经完成，适用于游戏中的抽奖场景等，如掷骰子产生一个随机结果。

4.5.10. 定时器和心跳

几乎所有的游戏与应用都需要实现在线检测，而在 Cocos-BCX 设计区块链游戏时，为了解决用户的状态检测与持续的会话机制，提出了定时器与心跳的概念。

在区块链网络中实现定时器首先需要实现时间同步机制，而传统的时间同步机制通常是由外部授时或信任中心实现的，而在区块链去信任的逻辑下，外部授时或信任中心都存在无法自证的缺陷，因此链上时间的同步只能由链内完成。

Cocos-BCX 提出的时间同步方案是：利用块数据时间戳，出块节点在发布块时即等效的进行了时间同步广播，各节点收到块广播后完成时间同步操作，最终全网在一个块同步周期中完成了一次时间同步过程。

基于这个设计，Cocos-BCX 提供两种形态的定时器技术支持：

- 定时器以块周期为最小计时粒度，按照预先设定的计时目标工作，由区块数据时间戳为标准时间计数，可认为是全网统一的计时标准，计时器可以在任意网络区域、时区以同样的计时规则正常执行；
- 采用与内源可信随机过程类似的消息传递机制，以委托方式将定时器所需参数提交至随机节点，并由该节点上的实现层执行定时器的初始化与到期通知等行为。

心跳与定时器相近，其心跳的时间脉冲同样来自于区块的时间戳，一个心跳周期中，节点/端会提交自己的连接更新信息，如果发现某一周期没有特定的端/节点更新信息，则证明这个端/节点掉线，定时器和心跳为用户状态检测和未来的会话机制提供了应用基础。

4.5.11. 标准化的非同质数字资产

非同质数字资产扩展数据区域支持非同质数字资产属性扩展，是该资产支持的世界观内游戏具体业务数据的存储区域。非同质数字资产中扩展数据区域的结构设计非常灵活，允许游戏或其他业务场景对其进行扩展。随着游戏增加，资产在不同的游戏中迁移时域数据必然逐渐追加，若追加太多则会影响区块链链运行效率，同时为了防止合约恶意写入大量数据导致用户资产数据冗余，因此我们增加资产合约权限控制观念：

- 用户有权删除但不能修改该资产中某一个域的数据，可减少数据冗余的同时防止如自定义增强版的道具等作弊行为；
- 合约能且仅能修改自己所负责的域数据。合约可以读取非同质数字资产扩展数据中所有数据，但是修改权限仅限于当前合约所处的域中。例如在区块链游戏世界中，合约可以读取《风暴英雄》和《魔兽世界》的相关资产数据，但是《风暴英雄》中“霜之哀伤”不会在《魔兽世界》中被“灰烬使者”真正斩断，而只是在《魔兽世界》呈现“斩断状态”。

4.5.12. 既定规则设计工具

在真实的游戏应用场景中存在这种情况，用户认可某款游戏公开的规则并选择参与，在游戏开始之前开发者临时修改合约代码更改游戏规则来使自己受益，或者将众筹的资产转移之后不再为用户提供游戏服务，这些行为都会给用户带来资产损失，既定规则设计工具就是为防止此类现象而开发的。游戏开发者可以选择使用针对区块链游戏的既定规则设计工具来设计区块链游戏以增加用户的信任，其原理是由智能合约实现将一定数量的同质资产锁定，并且设置解锁的条件、时间以及数量，合约代码中加入资产在锁定期间内不能对游戏规则代码进行修改的工具函数，资产在锁定期合约代码无法进行任何修改，因此游戏只能按照最开始设定的规则进行。

4.6. 防止 BP/开发者作弊的事务验证机制

BP 作为全网的事务处理与通信核心，能够先于一般节点获知最近事务的处理结果，因此对于某些具备时效性或机密性的信息，BP 拥有较一般节点更高的优先权，因此具备了从信息获取方面作弊的可能，例如提前获知一个随机过程的结果并利用合约提前预测运行结果等，这对链上的游戏无疑是不公正的，也是不安全的。

开发者在这里包括链网络的底层开发者以及合约开发者等一切有能力进行一定程度链交互/改造能力的个人或组织，开发者具备深度解析/控制链内信息的能力，并且有理由相信开发者能够通过阅读代码等方式获知传输过程中可能会使用的加密/隐蔽通信技术细节从而使之能够针对性的设计代码从而以非法方式获知这部分信息(随机过程、敏感信息数据等)。

因此BCX方案中设计了一套针对BP和开发者可能作弊环节的事务执行、消息传递、运行机制，将在下文中简要介绍。

4.6.1. 动态加密传输

为防止敏感信息在广播传输过程中被监听并解析，BCX 链网络通信针对这类信息增加了使用动态加密的安全通信方式，如图 4-6-1 所示。

图 4-6-1 动态加密传输机制

以随机种子的产生为例，当一个随机种子被产生后，生产者将把一段与时间、块高度、其他噪声输入等相关的动态数据作为 AES 密钥加密这段随机种子信息并广播加密后的信息。由于所有的节点拥有同样的动态密钥生成算法，因而可以正确的解出种子信息，而非法窃听的第三方无法解出，保证了敏感信息在传输过程中的安全性。

4.6.2. 防止自定义节点接入网络

保证信息的传输安全并不能防止节点开发者通过修改程序来达到输出收到并解密后的信息，因此本方案中设计了一套身份验证机制用以防止修改后的节点程序接入链网络，如图 4-6-2 所示。

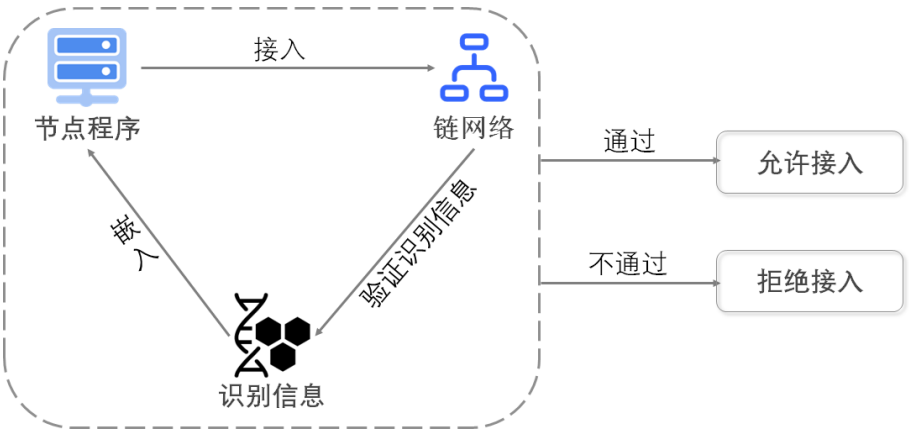


图 4-6-2 节点接入验证机制

BCX 节点程序将在发布时内嵌一个不包含在公开源代码中且与版本号关联的验证信息，当节点试图连接链网络和其他节点时，其他节点将会验证这一信息是否与链网络中记录的校验信息一致，并会主动拒绝无法通过验证的节点连接，防止修改后的节点程序连入链网络进行恶意行为。同时二次开发者也可以通过自定义源代码中的这一身份验证信息，发布属于自己的链网络，并将同样具备防止非官方节点接入的特性。

4.6.3. 隐藏过程变量

由于合约自身是一套图灵完备的状态机系统，因此固定的输入一定会得到固定的输出，并且在事务机制下将结果广播至全网同步，而如果广播的信息是一系列行为的中间过程，则可能导致一些不适宜被获知的过程变量被公开。因此本方案针对这类情况，提出了使用隐藏过程变量的合约执行逻辑，如图 4-6-3 所示。

通过合理的合约设计，将涉及敏感数据的过程变量放在同一个操作(OP)过程中执行，由于执行过程在执行节点内存中完成，最终广播的是操作结果，因此过程变量在整个周期中是被隐藏的，不会存在暴露的风险。

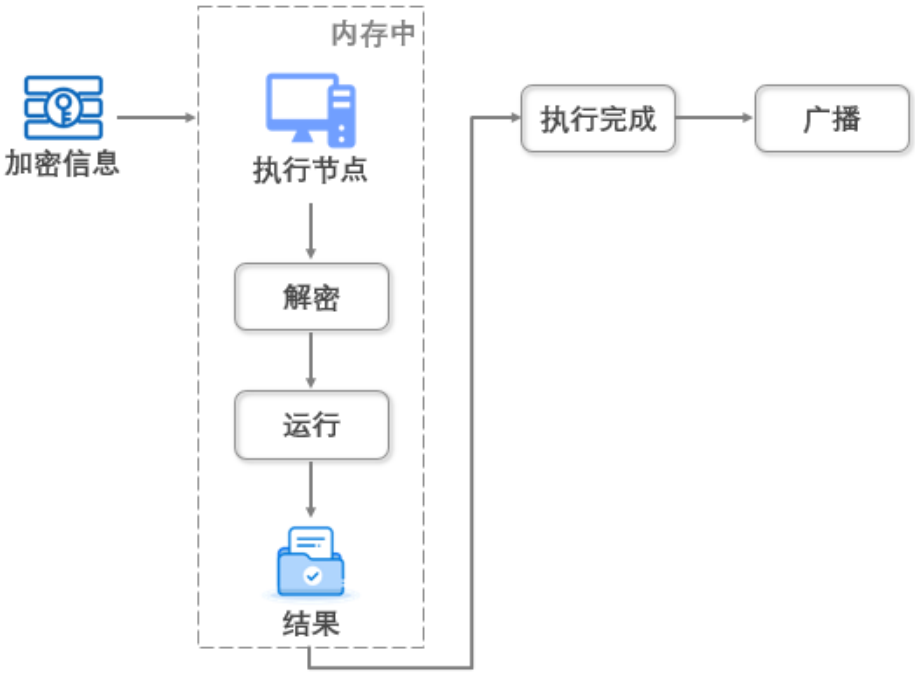


图 4-6-3 过程变量隐藏机制

4.6.4. 带有执行身份验证的合约机制

为了防止恶意的开发者通过测试性调用合约接口来预测合约的可能输出，本方案的合约系统中增加了执行身份验证机制，即合约特定的接口需要具备授权的账户才能够执行，如图 4-6-4 所示。

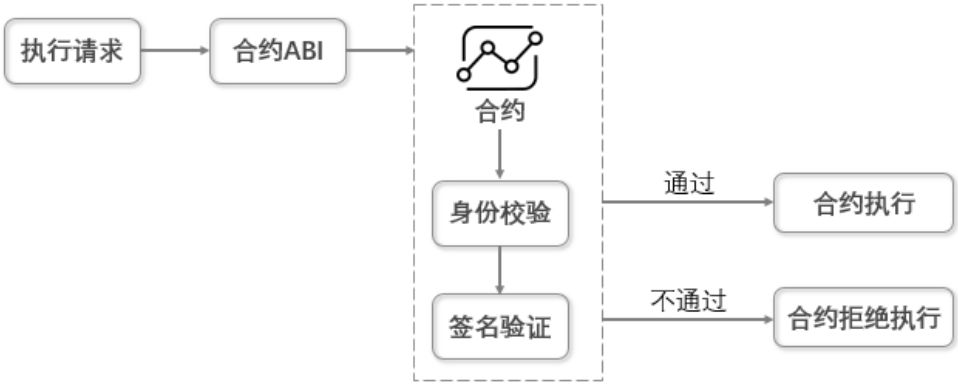


图 4-6-4 带有执行身份验证的合约机制

当合约收到执行请求时，会验证请求信息中的签名信息，与合约中规定的执行者权限验证，验证通过的执行者请求才会正常执行合约函数，否则合约将直接结束，并且不会返还请求者支付的费

用，在这套机制下， 即便开发者知道链与合约的代码，了解执行过程和原理，也无法恶意调用特定的接口，保证了合约无法被随意调用推测其执行结果。

4.6.5. 敏感过程通过内部可信环境执行

对于在一定时间内持续敏感的信息或操作过程(例如一场牌局)，本方案允许阶段内的执行逻辑在 TEE(Trusted Execution Environment, 可信执行环境)机制保障下以黑盒模式运行，平时链网络通过 TEE 保障机制对这些黑盒环境发起周期性的挑战/验证以保证环境的可信，并在需要执行持续性敏感过程时随机选择一个其中一个环境运行，过程执行完成后将向链上提交足以回溯执行过程的记录信息与结果信息，以保证链网络上记事的公正、公开、透明。其原理如图 4-6-5 所示。

图 4-6-5 敏感过程内部执行机制

在这一机制的保障下，开发者与 BP 均无法参与黑盒过程的执行，因此可以有效的避免两者从中作弊的可能，结合上述各个保障设计，可以让 Cocos-BCX 以可信、可靠、安全的执行环境运行所有支持的业务过程。

5. 平台经济体系

5.1. 区块链为游戏行业带来的本质改变

从使用体验的角度，“区块链游戏”和普通游戏对玩家并无区别。然而，区块链可能对游戏市场起到根本性影响。游戏行业现行的商业逻辑是“付费获取服务”，即用户付出金钱、时间和行为数据以单向开支的形式交换游戏体验。但基于区块链机制上数据公开、不可逆、永久存续等特点，游戏内的道具可被用户管理和转移，从体验服务转变为体验资产。我们认为，“付费获取服务”与“求购和使用资产”对于开发者、发行者和玩家是截然不同的价值诉求，会相应形成不同的行为和商业模式。这些潜在的改变可以被归纳为：

1. 资产属性。资产是由过往经济活动形成，被某方控制并可获得未来所产生的经济利益的资源。游戏内容在区块链上具备了成为资产的两个特性：（1）技术保证的稀缺性，区块链环境中的内容供应量可以被限制，具备了价值；（2）技术保证的所有权和所有权流通，用户对数字内容的所有权无法篡改，并可以通过代币转移。数字内容具备了被拥有的权利和权利流动机制，真正成为资产。

2. 商业模式与资产定价模型。以一款中国市场评级为 B 的动作角色扮演（Action RPG）移动游戏为例：发行者选择游戏产品、测试、上线并进行不超过数天的集中推广；开发者为在有限时间内转化用户进行支付，在数小时游戏时间后开始设置收费点，并预期多数账户的生命周期不超过 75 天；大量玩家在明知游戏大概率运营不超过 12 个月的情况下，被迫在游戏体验和付费间进行抉择。开发者、发行者和玩家三者的博弈鼓励短期利益最大化，一定程度上降低了游戏的整体体验。将该游戏视为资产，其价值没有实现最大化。多年以来，发行商在上述现象中受到较多的非议，被认为是导致行业瓶颈的原因。新的技术（例如 HTML5）和商业模式（例如独立发行）被作为削弱传统发行商议价能力的尝试，但收效有限。

   我们认为以上问题的关键不在于发行商所处的行业位置，而是传统商业模式与游戏资产价值最大化存在根本矛盾。从长远看，开发者、发行商、用户三者的利益诉求截然不同。开发者作为创作者，产出一款可行产品具备偶然性，因此希望该款游戏的总价值最大；发行商直接面对用户，最大利益来自其一定时间内的投入-产出经济性，单款游戏的总价值不是第一考虑（如图 18 所示）；用户希望支付的金钱、时间与隐私数据和游戏体验匹配。从表面看，开发者和用户的利益高度一致，“去中介”能够实现两者的最大收益。但从实际操作角度，内容开发和用户运营是不同的专业领域，大量开发者直接运营用户并不现实。因此，在现有的商业模式下，开发者和发行商仅在一定时期内拥有共同的利益诉求，导致游戏资产价值无法最大化。

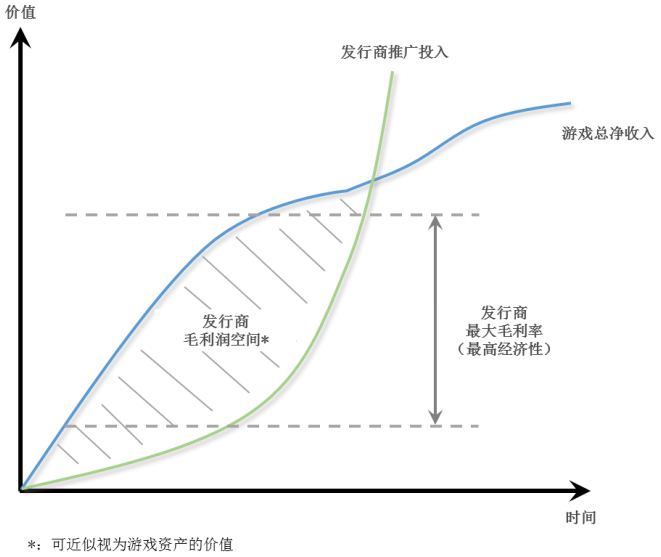


图 5-1-1 传统游戏商业逻辑示意

在区块链环境中，由于游戏资产的收益可以通过其价值反映且实现流通，以上的问题可能从两个角度被大幅度缓解甚至解决。首先，开发者、中介和用户共同通过数字资产享有游戏的利益，三方的目标高度统一，其行为趋向推动游戏价值的最大化；其次，不同的持币中介可以在持有根据自身的经济性对游戏进行更充分的推广。例如，在游戏的不同阶段，中介可以根据自身的投入-产出经济性求购数字资产、进行推广并获得收益。投入-产出效益低的中介可以出让数字资产、退出推广，新的中介评估经济性、求购数字资产，并继续推广。每个阶段的用户、中介与开发者利益都可以相对达成一致，直到游戏资产的生命周期结束。

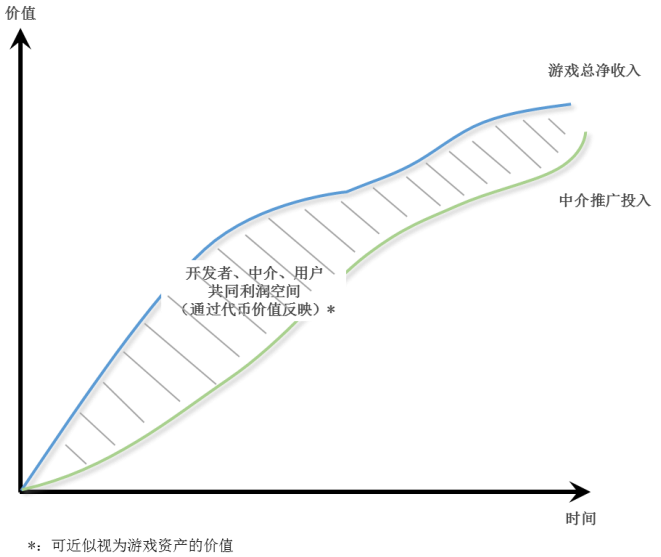


图 5-1-2 区块链游戏商业逻辑示意

我们认为，在区块链游戏的产业变革中，形式上的“去中介”不是目的，“利益一致、资产价值最大化”是最终的目标。“中介”作为用户运营的专业性和角色将长期存在，无论是以机构还是个人形式。

综上所述，“区块链游戏”可以被更准确地定义为“使用区块链技术、具备区块链经济机制的游戏”。从经济角度看，本文 1.3 节中所阐述的区块链游戏发展路径也可以被视为市场各方参与资产定价、利益逐步统一的四个阶段，是商业模式变化推动开发者和用户的结果，势必给游戏行业带来根本变化。

以上的资产化路径也适用于游戏以外的广义数字资产，我们将在 Cocos-BCX 平台的后续发展中对更多类别的资产进行支持。

5.2. Cocos-BCX 经济体的设计原理

通过提供底层公链、数字产权管理、资产流通平台等一套完整的功能组件，Cocos-BCX 平台承载了开发者所创造的游戏资产价值。随着更多的游戏、游戏内资产被生产、管理和交换，平台的经济总量持续膨胀。

Cocos-BCX 基于石墨烯标准的技术和治理架构设计，拥有 DPoS 共识机制对应的经济属性。平台具备非挖矿、委托共识、低分叉可能、可定义资产流通成本等特性，开发者与用户可以将主要资源投入数字资产本身的创造与交换中，系统资源的整体消耗成本低。

在真实的商业环境中，参与方的经济行为和心理既存在宏观规律又有微观离散性。我们认为 Cocos-BCX 的经济、治理、产品和技术规则设定应充分考虑和兼容各类行为的复杂性与不完美。平台仅提供最小可行、灵活的工具与规则，帮助和促进参与者根据各自的利益进行高度自由的经济活动与社区治理。各个生态角色在无需互信的前提下形成博弈关系和自激励机制，从而提升行业的整体效率和价值。同时，全球游戏开发者社区拥有长期的历史，具备成熟的价值观。我们希望最大程度地将该价值观反映到经济体系的设计中，即：

- 独立生存：平台自身拥有清晰的商业模式，能够稳定存续；
- 自治与共识：社区与子社区（例如同一世界观下的生态）逐步建立共同决策机制，并最终按照共识原则运行，建立以参与者投票为基础的发展决策体系；
- 共享：社区产生价值中的一部分作为共同财富，用于社区的生存和竞争力提升；
- 自我进化：建立奖励机制，未来鼓励成员对社区的技术和经济机制持续提出挑战。

5.3. COCOS 数字资产：全域、广义去中心化数字资产的原生定价媒介

为实现上述的设想，我们创建了平台资产 COCOS 作为平台生态经济活动的流通媒介和治理凭证。

除作为 Cocox-BCX 的价值交换载体和社区参与证明以外，COCOS 将有可能作为基础定价资产，对数字资产生态起到关键的作用。大量去中心化数字资产未来将以不同标准存在于多个区块链生态中，跨越链生态的资产定价媒介有存在的必要性。基于以下原因，COCOS 能够成为区块链生态数字资产原生的定价媒介：

1. Cocos-BCX 平台在底层技术、共识机制、应用功能等方面原生支持全域、同质/非同质去中心化数字资产的交换。COCOS 具备成为基础定价媒介的技术基础；
2. 在 Cocos-BCX 平台上的资产创造过程中，生产行为（例如委托共识出块）和生产要素（例如从平台应用商店求购游戏内的设计素材）均以 COCOS 作为原生的定价媒介。所产出资产的 COCOS 价格体现了对生产成本与利润的价值确认，而非名义标价。COCOS 具备成为基础定价媒介的经济基础；
3. Cocos-BCX 平台支持和鼓励同一世界观、相关世界观下的资产流通，在全域数字资产间建立了真正的用户使用价值联系，而不仅代表资产间的名义兑换率。COCOS 具备成为基础定价媒介的流通基础。

基于 COCOS，开发者和用户可以对不同链生态、世界观内容、技术标准的数字资产进行评估、比较、流通和管理。同时，COCOS 作为原生和基础的定价媒介，是未来区块链行业进行数字资产金融产品和衍生品开发与流通的必要条件。

5.4. COCOS 数字资产的基本使用模型

平台数字资产 COCOS 具备三个作用：（1）平台生态内的价值交换媒介、（2）Cocos-BCX 公链的委托共识权益份额代表、和（3）平台社区参与和贡献的衡量。COCOS 从平台共识工作贡献奖励（例如出块）、开发者产出资产的过程中产生，并通过游戏内货币和道具、资产流通平台传导至用户。用户和开发者也通过平台数字资产的流通设施对 COCOS 进行交换。

作为平台的价值交换媒介，COCOS 可用于支付社区内的资源消耗、兑换平台功能、消费和实现数字资产流通，以及支付跨链生态的消费和资源交换（例如通过平台发布以太坊应用需要的 GAS 等）。

作为 Cocos-BCX 公链的委托共识权益份额代表，COCOS 的持有者直接参与共识代理投票。具体的投票机制请参考本白皮书中“4.3.3 改进的 DPOS 共识机制”部分。

作为平台参与度衡量证明，COCOS 可作为未来社区事项的投票权代表和完成平台任务的激励手段。例如使用 COCOS 作为赏金征集开发者，针对平台的特定功能进行开发或优化。

在平台的第一阶段，我们发行基于 ERC-20 标准的 COCOS Token，数量设定为 100,000,000,000（一千亿）枚，总量维持不变，最小计量单位为 10^{-18} COCOS。在我们推出自有公链后，持有 ERC-20 COCOS 数字资产的用户可根据凭证获得等量的自有公链 COCOS 币，同时其 ERC-20 Token 将被回收。

5.4.1. COCOS 的获取方式

参与者在 Cocos-BCX 平台中拥有相同的身份权限。无论是普通游戏玩家，亦或是开发者都可以充分使用平台功能创造出属于自己的数字资产，并通过这种方式获得收益。

COCOS 的获取方式包括但不限于：

1) 价值创造：包括（A）创造数字资产行为的贡献，即开发游戏、制作道具。针对单一的数字资产（包括游戏、应用、游戏/应用内道具），平台激励的发放量与参与者创作的该资产价值成正比、与 Cocos-BCX 平台的存续时间和系统总资产价值成反比，激励总量设有上限；和（B）创造数字资产价值的贡献，即创造资产到达一定的收费与资产流通规模可获得 COCOS。针对单一的数字资产（包括游戏、应用、游戏/应用内道具），激励发放量与开发者创作的该资产总资产流通量成正比，激励总量不设上限；

2) 平台贡献奖励：为 Cocos-BCX 社区做出贡献的用户可获得 COCOS。初期，我们以开发者社区的历史贡献度（对 Cocos 引擎的代码贡献积分、在线社区互动积分等）进行 COCOS 发放。后期，平台将采用赏金任务、免费资产（例如无偿赠送开发者的游戏人物形象）等多种形式，激励开发者对平台进行新功能开发、升级、错误修改、测试等社区行为。此部分将从平台基金会的资产预留和平台分成部分拨出，激励总量不设上限；

3) 资产流通：出让在游戏中获取的道具资产获得 COCOS。该部分的激励与游戏玩法和经济体系相关，由游戏开发者与市场规律决定，平台原则上不做规则和数量限制；

4) 行为激励：在 Cocos-BCX 平台、社区及平台游戏内的多种有效行为将按照一定的贡献度兑换成 COCOS。例如，用户注册平台账号、参与社区各类互动以获得 COCOS。平台通过分析访问有效性、信息完整性、行为合理性等维度，确认用户行为是否有效，并进行 COCOS 的发放激励。该部分的激励数量与互动内容（如发帖、点赞、回复等）成正比、与平台总用户量、平台存续时间成反比，激励总量设有上限；

5) Cocos-BCX 公链共识工作贡献奖励。

5.4.2. COCOS 的消耗及应用场景

COCOS 的使用场景包括但不限于：

1) 从第三方开发者兑换开发资源（例如游戏角色形象等）；

2) 从平台处兑换开发功能组件等增值服务；

3) 从游戏内或资产流通平台中求购游戏金币和道具资产。基于平台的资产权利管理机制，道具在其完整生命周期内的每一次流转均向开发者缴纳一定的费用；

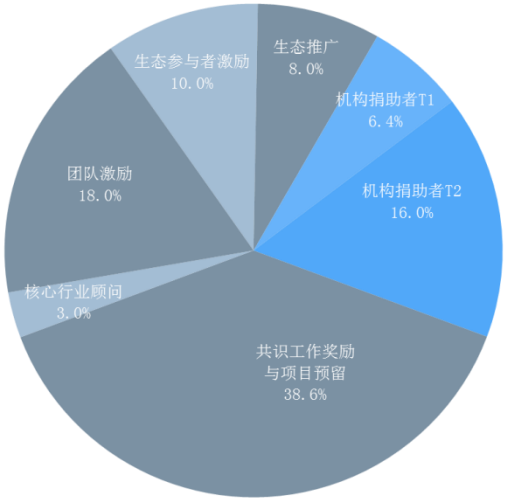
4） 在社区发布悬赏任务，发起和参与社区事务的投票。

在每一次 COCOS 的流转行为中，平台将抽取一定比例的费用，并将其锁定为社区的共同财富。在一定时间后，平台将释放使用该部分财富用于生态建设的资源。

5.5. COCOS 的使用分配

在初始状态，我们建议将 82%的 COCOS 拨备用于各种方式的平台社区建设，其中包括但不限于见证人出块奖励、平台生态开发者的激励、全球社区建设、营销和推广、行业联盟、生态投资、研究、财务与法律合规等。使用该部分 COCOS 的使用包括通过共识工作贡献换取、无偿赠送、赠送换取服务、赠送换取其他数字资产等。

18%的 COCOS 拟用于激励本项目的发起团队。我们预计全球区块链游戏行业在未来 3 年内将有突破性发展，并希望项目的商业和社会价值在 3 年内得到验证。因此，激励部分将予以锁定，在数字资产生成后的每年末发放并解锁 1/3，在 3 年内发放完成。



用途	占比	说明	锁定条件
生态参与者激励	10%	对用户和开发者参与生态内使用、推广、研究与开发行为的激励	视业务情况
生态推广	8%	为在业内推广项目，建立项目的市场地位所进行的战略级别代币交换、资源支持	视业务情况
机构捐助者T1	6.4%	对企业、机构与相关行业捐助者的回报	1. 55%生成后发放、解锁 2. 15%生成二个月后发放、解锁 3. 15%生成四个月后发放、解锁 4. 15%生成六个月后发放、解锁
机构捐助者T2	`16%	对企业、机构与相关行业捐助者的回报	
共识工作奖励 与项目预留	38.6%	项目的长期发展资源储备，	视业务情况
核心行业顾问	3%	对项目做出重大贡献的技术、商业等领域顾问的激励	按贡献 逐步释放
团队激励	18%	团队在项目研究、开发、持续维护付出时间和精力的激励	生成后每年末发放并解锁33% 三年解锁完毕
总计	100%		

图 5-5-1 数字资产用途示意

6. 投资机构

6.1. 投资机构

Cocos-BCX 投资机构包含 NGC、币安、INB 资本、Dfund、500Startups、BlockVC、OK Blockchain Capital、一粟资本、雄岸基金、ONTology、FreeS FUND、NODE Capital、共识资本、哈希资本、NEO Capital、 Ticker Capital、合约资本、君物资本、糖果资本、浩方创投、BMETA Capital、BYTE Capital、敏捷资本、 InsurFun、BA Capital、共识实验室、TOKENMANIA 和拜占庭资本等。

Cocos-BCX 投资机构数量非常多，且一类机构居多，有非常强的机构后盾实力。

7. 总结

我们认为数字资产是最符合区块链经济本质的资产类别，拥有广阔的发展前景。游戏作为巨大的市场，是区块链大规模应用的第一步。

为帮助开发者大规模在区块链环境中生产资产提供条件，我们推出一个应用开发和数字资产管理与流通的平台。该平台支持大规模数字内容的创建、区块链机制的集成，以及数字内容资产化、管理和流通的必要组件。

截止 2018 年 8 月末，我们已经实现了主要产品模块的内测版本开发，并推出了我们的非同质化数字资产标准 BCX-NHAS-1808。


COCOS BCX