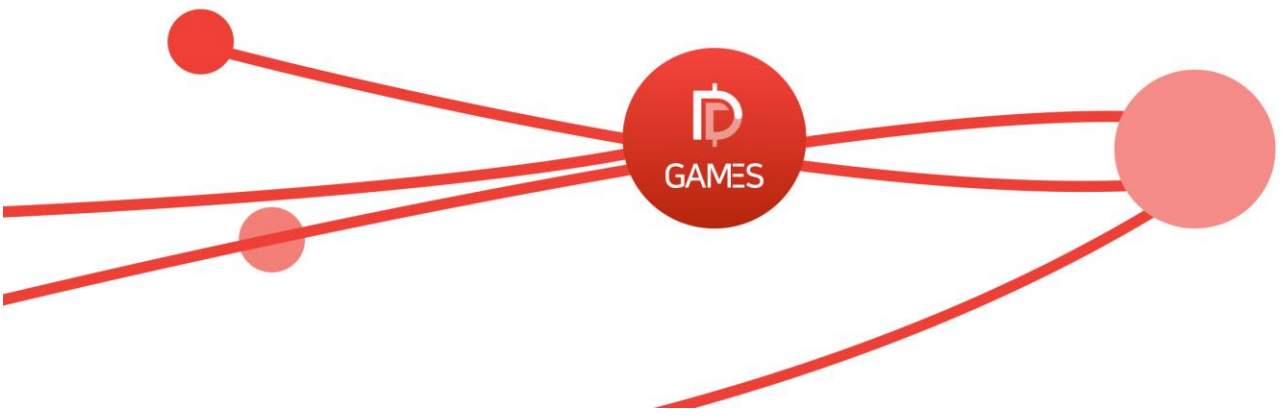
GAMES

去中心化的
自治游戏区块链体系

DGAMES白皮书



目　录

1 摘要

DGAMES（decentralized autonomous organization games）旨在构建去中心化的自治游戏区块链体系，建立一套全新的游戏开发及运行模式。

该体系包括：

- 去中心化游戏服务器框架
- 高效专用子链
- 分布式加密传输协议
- 可视化智能合约编辑器。

DGAMES 为游戏行业带来的期待：一是在性能上支持更为复杂的游戏形式；二是在功能上降低区块链游戏的开发难度。最终形成一个基于区块链的全新游戏分发模式、打造全新的游戏玩法、开创全新的游戏生态。

2 背景

2.1 行业背景

随着区块链技术的迅猛发展，已经快速的融入到社会的各个行业。CryptoKitties（以太猫）的出现，彻底引爆了整个游戏行业，玩客猴、招财猫等一系列区块链游戏产品如雨后春笋般冒了出来。游戏与区块链技术的结合将给整个游戏行业带来了全新的发展契机，其加密算法、共识机制、分布式等特点将构建全新的游戏规则，带来前所未有的游戏体验，致使游戏异常火爆，倍受玩家推崇，从而拥有巨大的发展空间。CryptoKitties（以太猫）的出现只是刚刚开始，可以说是游戏＋区块链规则的简单尝试，它带来的现象，引发我们对整个游戏产业的深思。

动物在幼年时期，通过游戏，学习捕猎生存技巧，保证种族的繁衍。人类的行为活动中，更少不了游戏的存在。在古代，游戏就一直存在并不断发展。如相扑、角抵、投壶、蹴鞠、七巧板、棋类等等游戏为人类的身体素质、社交、协作、教育等领域发挥着不可磨灭的作用。现代的体育竞技，对人类社会政治、经济、文化等诸多领域发挥着积极的影响。

科学技术的不断发展，尤其是计算机技术的日新月异，使游戏行业开启了一个全新的领域。可以说每一次计算机软硬件的革命，都赋予了游戏新的生命。从 1958 年世界上第一款视频游戏“双人网球”问世，到任天堂红白机、Game Boy，再到现在的 PC、手机游戏。电子游戏伴随在我们的成长，已经成为生活不可或缺的一部分。时至今日，CryptoKitties 的出现，使游戏正式拉开了区块链时代的

历史大幕。

2.2 行业痛点

游戏在过去的 30 年间蓬勃发展，从单机游戏到网络游戏再到移动游戏，画面越来越精致，特效越来越炫酷，游戏体积越来越庞大，行业收入屡创新高，但游戏的根本——游戏性却在不断下降。这是行业发展的必由之路，也是不断商业化和中心化发展的必然结果，但这带给游戏玩家的却不是最好的体验和感受。

正是因为上述原因，近年来独立游戏的兴起不断给游戏玩家带来惊喜。很多独立游戏由小的开发团队开发运营，注重游戏价值回归，在游戏性和乐趣上深入挖掘，但这类游戏相对传统的网络游戏吸金能力较弱，大量的用户也不能带给开发团队满意的收益回报，长此以往对行业来说是极为不利的。

同时传统游戏行业的产业链也对整个链条最重要的内容提供方——游戏开发者也并不算友好，大量收益被处于产业链优势方的渠道商及发行商赚走，中小级别游戏开发者乃至部分大型游戏开发团队对此都毫无办法，为了迎合渠道商和发行商的收益要求，无视游戏玩家的权益，竭尽全力、竭泽而渔的攫取玩家的金钱。

2.3 “以太猫（CryptoKitties）”的启示

CryptoKitties（以太猫）的上线带来了区块链游戏的开端，但上线初期大量的交易导致 ETH 公链的拥塞不止一次的发生，且以太猫产品的数据交互形式非常简单，即使如此仍然无法支持较大数量玩家的交易需求，现代游戏对大量数据交互的实时性和便捷性均要求很高，区块链游戏的发展趋势也是从小型产品向大型游戏产品不断发展，这对游戏行业的区块链体系在技术上产生了极高的要求。

3 区块链游戏的要求

3.1 低延时高并发

比特币平均每隔 10 分钟才能产生一个新的区块，每个区块大小只有 1M，仅能记录大约 4000 笔交易，而且一般认为一笔交易被确认 6 次以上才被认定为正当交易。以太坊将确认速度提高到了 14 秒，但是仍然不能满足游戏对于数据处理速度的基本需求。

执行速度快，毫秒级数据确认，为游戏制作、游戏运行提供基础的技术保证。高效的并发请求处理能力，至少百万级 TPS 的数据吞吐量，才能满足大型游戏的运营需求。

3.2 自由扩展

鉴于不同游戏的玩法与机制大不相同，从而需要根据需求自定义功能模块、自由扩展。从架构层要解决负载均衡、数据同步、容错机制、执行效率等问题。

3.3 高可靠性

可靠性（availability），或者说可用性，是描述系统可以提供服务能力的重要指标以及保障用户体验的依托。高可靠的分布式系统往往需要通过复杂的机制来进行保证。

可靠性的两个指标：MTBF（Mean Time Between Failures）和 MTTR（Mean Time to Repair）。MTBF 衡量了系统发生故障的频率，MTTR 反映了系统碰到故障后服务恢复的能力。一个高可用的系统应该是具有尽量长的 MTBF 和尽量短的 MTTR。

3.4 公开透明的游戏环境

游戏的基础规则及关键规则的公开透明，以及游戏资产交易的可靠性往往决定着玩家对游戏的信任。对于用户来说，一个公开、透明、不可篡改的游戏世界，不存在暗箱操作，而且关于装备及道具，用户第一次真正有了虚拟资产的所有权，这对于用户来说极具吸引力。区块链采用分布式加密算法的机制，从根本上解决了上述问题。游戏中的所有策略规则通过区块链智能合约的方式发布执行，所有人可进行查阅，从而实现公平、透明的游戏环境。

3.5 全新的游戏生态

当前的游戏运营模式，主要有付费下载、点卡充值、道具付费等几种主流盈利方式。DGAMES 的到来，将彻底打破当前的游戏收费体系，建立真正免费的游戏模式，为用户创造公平的游戏环境，打造全新的游戏生态体系。

3.6 易上手

多语言支持、模块清晰，提供可视化的游戏规则编辑器。即使没有区块链技术基础的人，都可以自己创建一套属于自己的区块链游戏。

3.7 跨游戏自由交易

对于游戏玩家来说，一旦道具成为资产，交易的需求就随之而来。原来游戏道具的交易路径复杂，且不同游戏间的资产不可流通。如果一个道具，实现了 token 化，不同游戏的道具也将具有交易和结算的基础，其虚拟资产相互之间都可以进行交易，增强虚拟资产的流通性。

3.8 开放自治社区

开放社区带给开发者和玩家全面透明开放的对接通路，对于开发者而言，无需通过传统游戏产业链上的渠道商和发行商就可以直接接触到玩家，可以直击市场第一线，获取最直接的市场反馈，同时带来的更直接的游戏收益体现，收益来自用户的数量及在线时间、用户之间互动交易等游戏性核心硬指标；对于玩家而言，不论是进行游戏来获取收益，还针对某个明星产品的投票推荐获取收益，更有针对某个明星团队的新品支持等获益方式。

4 DGames 的技术架构

DGAMES 的目标是实现一个为未来游戏行业服务的去中心化的区块链平台。

DGAMES 的游戏开发者基于区块链技术的智能合约机制编写游戏策略，通过消耗主链 TOKEN（DGAME）来确认游戏子链（Sub-Blockchain）的身份合法性。任何游戏开发者包括个人、工作室、企业可以通过分布式游戏自治准入机制申请加入 DGAMES，来制作、发布区块链游戏。游戏玩家通过 PoA 确权机制获得主链 TOKEN。玩家在参与游戏的过程中，会根据游戏设置的智能合约策略消耗掉账户中相应的主链 TOKEN 来完成游戏任务或获取游戏虚拟资产。玩家拥有的所有虚拟资产都记录在区块

链网络当中，无法篡改，同时可以通过主链网络与 DGAMES 子链上游戏的多种虚拟资产进行数字化价值交换，交换时需要消耗一定的主链 TOKEN。

我们构想的蓝图整体是以 DGAMES Blockchain 为基础，符合下一代区块链技术前景的多个子链的集合体，所有这些子链通过开放性的功能入口协议实现协作。

4.1 Hash 算法

Hash（哈希）算法是非常重要的计算机算法，它能将任意长度的二进制明文串映射为较短的 Hash 值，并且不同的明文很难映射为相同的 Hash 值。

对称加密算法的加解密过程秘钥相同，优点是加解密效率和加密强度都很高。缺点是参与方都需要提前持有秘钥，一旦有人泄露则安全性被破坏。

非对称加密算法的加密秘钥和解密秘钥是不同的，分别称为公钥（public key）和私钥（private key）。优点是公私钥分开，不安全通道也可以使用，缺点是处理速度较慢，一般比对称加解密算法慢 2~3 个数量级。非对称加密算法主要基于数学问题来保障。代表算法包括：RSA、ELGamal、椭圆曲线、SM2 等。比特币采用了椭圆曲线加密算法，具有较高的安全性，但在加解密计算过程中比较费时。DGAMES 引入了基于离散对数的密码方案，采用此方案可以保留未来扩展的可能性。

4.2 共识机制

区块链系统是一个分布式系统，碰到的首要问题就是一致性的保障。一致性问题是分布式领域最为基础也是最重要的问题。如果分布式系统能实现一致，对外就可以呈现一个完美的分布式网络。如何解决分布式系统中节点可靠性、节点间通讯可靠性等问题是建立分布式网络的基础。共识是保障分布式系统中多个节点之间，彼此对某个状态达成一致结果的手段。

DGAMES 主链采用 DPoS+PBFT 的共识机制。

主网通过 DPoS 的机制，通过网络负载情况，投票选举出背书记账节点，以动态分布式的方式调整主网负载。所有背书记账节点之间将交易信息进行同步，采用 PBFT 算法机制对其打包成块。网络会剔除故障节点和非诚实节点，并重新选举新的节点进行记账，以保证区块信息完整有效。

拥有背书记账权的节点会平权获取网络交易费用的 50%用于记账奖励。

游戏用户通过 PoA（Proof of Activity 用户活跃度）共识机制获得主链奖励。每个参与游戏的用户，拥有游戏签名的证书（Game Digital Signature）和 DGAMES 签名证书（DGAMES Digital

Signature）后，根据用户活跃度证明确权策略来判定用户是否会获得系统奖励的主链 TOKEN。

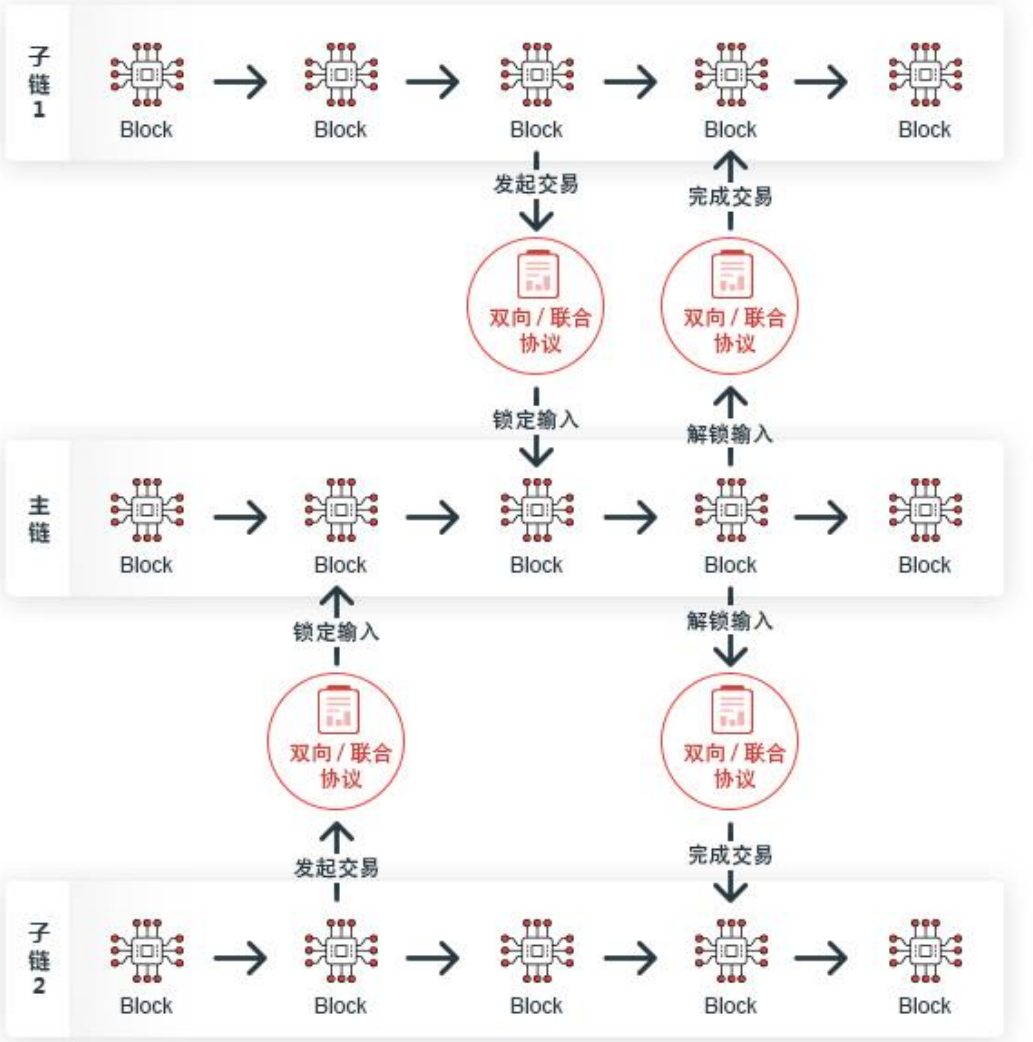
4.3 专用子链

各子链内部采用 PBFT（Practical Byzantine Fault Tolerance，拜占庭容错算法） 。该算法是 Miguel Castro（卡斯特罗)和 Barbara Liskov（利斯科夫）在 1999 年提出来的，解决了原始拜占庭容错算法效率不高的问题，将算法复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行。

对于拜占庭问题来说，加入节点总数为 N，叛变将军数为 F，则当 N≥3F+1 时，问题才有解。PBFT 算法采用密码学相关技术（RSA 签名算法、消息验证编码和摘要）确保消息传递过程无法被篡改和破坏。

4.4 资产流转

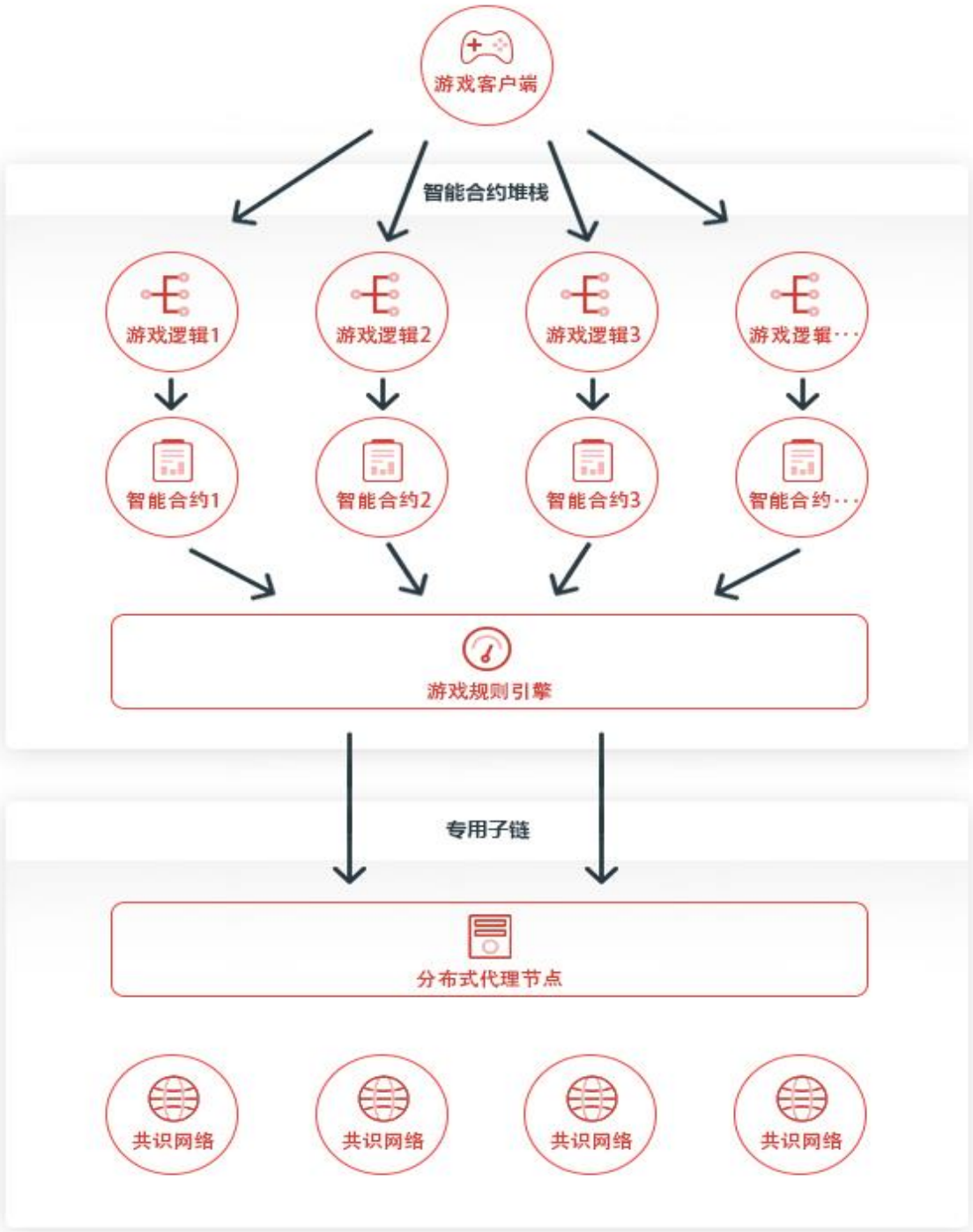
交易的双方拥有不同的子链虚拟资产需要交换时，DGAMES Blockchain 自动建立这笔交易的智能合约，智能合约的建立会消耗双方的主链 TOKEN，交易双方的资产提交到双向/联合协议中进行锁定。当交易双方都在指定时间范围内对要交易的虚拟资产进行签名，则交易资产按照约定进行分配，完成交易，交易双方都将消耗一定的主链 TOKEN。当交易双方没有在指定时间内按照约定对虚拟资产进行签名，则交易失败，虚拟资产返还，未签名方消耗主链 TOKEN。



DGAMES 资产在主链和子链、子链和子链间，通过双向/联合协议，定位包含该交易的区块在区块链中的位置，证明此动作的确发生过，实现子链资产与主链资产的锁定、流转过程。

4.5 去中心化的游戏服务器框架

从区块链的角度出发，专门为游戏设计的去中心化服务器框架，既能满足个人开发者及小型游戏开发团队制作游戏，又可以为专业游戏公司提供成熟的大型游戏开发运营解决方案。



游戏将多个逻辑体系写入到子链的智能合约中，游戏规则引擎对合约进行解释执行。分布式代理节点可以根据需求及业务压力进行多角色拆分及分布式部署。共识网络对业务请求进行共识并写入到区块链上。游戏可以向区块链网络发送请求，通过名称、版本号等来调用指定的智能合约。

游戏规则引擎直接与链结构交互，是极为重要的核心模块。智能合约代码本质上是为了对游戏上

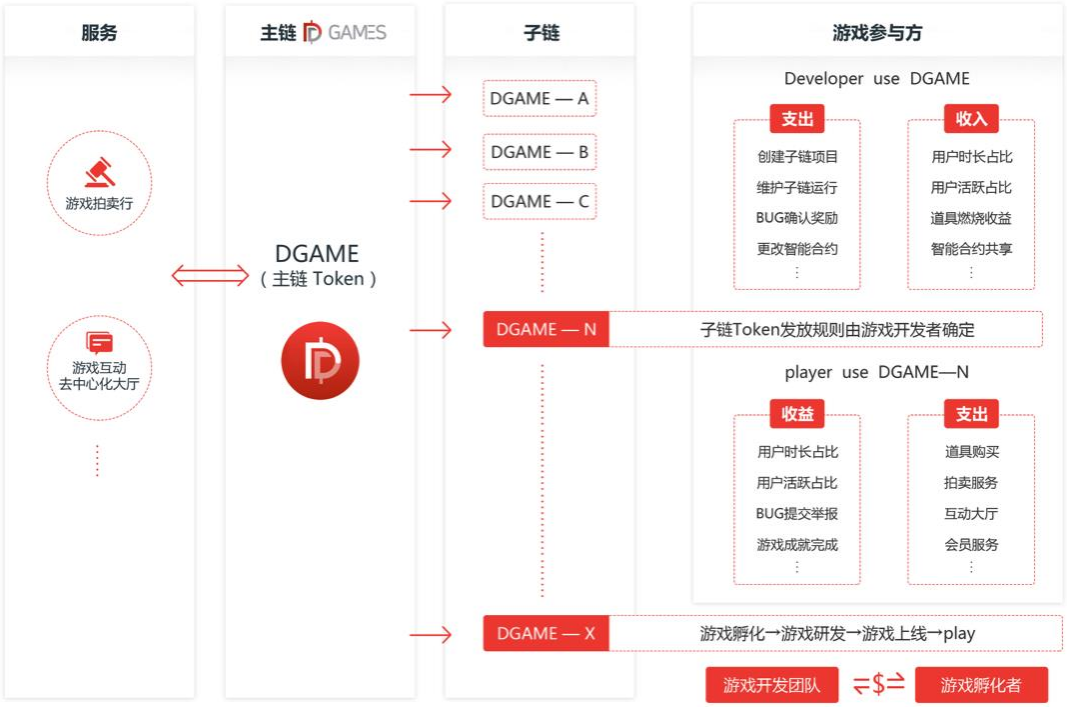
层业务逻辑进行支持。

4.6 可视化编辑器

为了方便开发者开发基于区块链的游戏，DGAMES 提供简单易用的可视化智能合约编辑器（IDE），编辑器能够满足游戏开发的基本逻辑，同时拥有可视化界面，开发者使用此界面可以方便快捷的开发区块链游戏。

5 DGames 带给游戏行业的全新业务逻辑规划

DGames 公链提供主链和子链的同时，还会提供多项公链服务。包括：游戏拍卖行、游戏互动大厅等多项服务，用于建设全新的游戏行业生态。



5.1 DGames 主链

DGames 主链作为游戏链的公用基础设施，可以接入并提供一些最基础的公链服务，如通用拍卖行、去中心化游戏交互大厅等服务。同时，所有的开发者均可接入主链为用户提供多样化的服务。

5.2 每个项目独立的子链

DGAMES 为每个项目提供一条独立的子链，同时提供部分最基础的智能合约。开发者可以自行决定子链 Token 的发放方式。开发者可以自行编写智能合约，也可以将自己独有的智能合约提交给公用的智能合约库供其他开发者使用，最早提供的开发者可以从后续使用该智能合约的开发者那里获取收

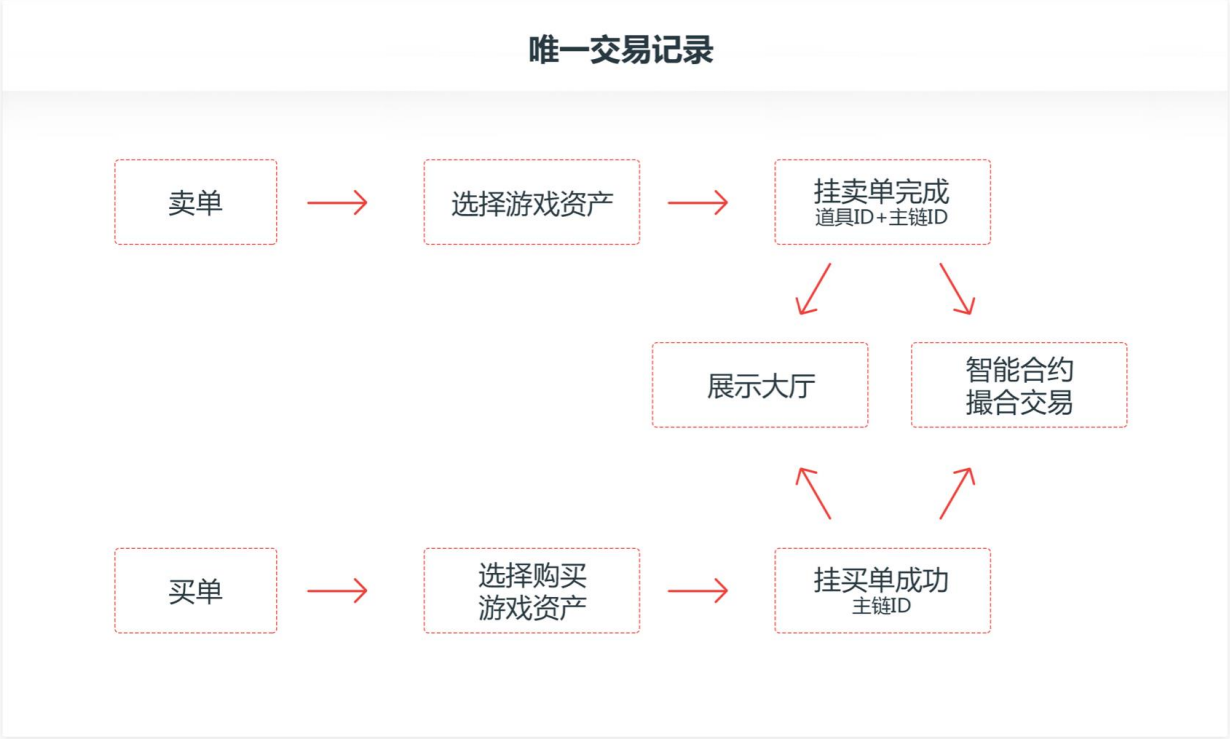
益。

5.3 游戏玩家

游戏开发者将开发的游戏产品提交到任意一个渠道后，玩家就可以通过这些渠道下载并进行游戏。玩家在游戏的过程中，可以通过游戏在线时间、游戏的连续活跃天数、通过游戏的关卡或完成游戏内任务等方式获取 DGames 主链的 Token 奖励。玩家获取的主链 Token 可以用游戏智能合约的燃烧消耗，如完成链上任务、获取链上道具、获取子链 Token 奖励、用户间链上交易等，为用户带来更多的游戏乐趣。

当玩家在游戏内获得成就或稀有道具时，这些成就或稀有道具可以作为玩家终身可展示的标记被记录在 DGames 公链中，使用游戏交互大厅或其它基于 DGames 的公链应用，可以在与其他玩家交互的过程中展现这些成就或稀有道具，更能够通过提交到公链拍卖行进行游戏成就或稀有道具的交易。

玩家从游戏内提交游戏资产到拍卖行的过程中，所对应的游戏资产在游戏中处于被锁定状态，发起者的交易内容和主链 ID 被绑定到卖单，当买方确认购买时自动完成交易过程。拍卖行使用主链 Token 进行交易，交易发起方需要燃烧主链的 Token。交易双方的两个交易动作被打包成一笔交易，正常完成后产生唯一链上的交易记录。通过此方式可以利用主链智能合约撮合交易并增加交易双方的互信程度。



5.4 游戏开发者

开发者在主链上创建了游戏 ID 后，将获得对应的游戏子链。DGames 提供 SDK 给开发者快速开发区块链游戏。SDK 主要包含用户钱包、区块链浏览器接口、子链认证签名、反作弊模块等功能。用户钱包主要提供用户创建账号、转账、查询等功能，区块链浏览器则允许用户以图形化方式查看子链所有链上数据；子链认证签名和反作弊系统给用户资产安全提供完善的保护。

根据玩家在游戏中的行为，游戏开发者可以获取 DGames 主链 Token 奖励，同时开发者还可以获取用户参与链上交互所燃烧主链 Token 的 50%作为收益。游戏玩家在开发者的游戏中进行游戏，游戏时长、活跃度、交互频率、链上道具购买等活动，开发者都会获取主链 Token 奖励。一言以蔽之，游戏做的越好玩，玩家感受到的乐趣性越高，玩家基于链上的互动越多，开发者将获得更多的奖励。

5.5 游戏产品孵化

当某个优秀的游戏团队开发游戏产品之前，可以向公链提交一个产品孵化申请，所有用户都可以查看该团队对于新产品的开发规划，来确定是否对该产品进行孵化。有一个智能合约会定向完成孵化计划，当计划完成时，该项目可以进入开发阶段。项目成功孵化后，孵化用户将在该游戏产品中获得各种奖励。

6 发展线路图

7 DGames 基金会

本项目的基金会成立于 2018 年,称为 DGames 基金会。 基金会致力于 DGames 去中心化的自

治游戏区块链体系架构的研发及落地工作,并促进去中心化游戏的研发。基金会的总体架构如下图图所示,决策委员会下辖技术开发委员会、财务及人事管理委员会、项目运营委员会三个子部门,分别负责技术开发战略的制定和实施监管;财务制度的制定和执行监管;项目总体运营及市场推广的决策及执行等事务。决策委员会成员四年一换届,成员一般由各个子委员会推荐一名代表,加上社区代表、团队成员代表各一名产生。 决策委员会成员五名。各子委员会成员四年一换届,成员一般由具备相关行业杰出能力的人士担任。

8 合作产品

《区块人生》 《怪物行星》 《必有用》 《消消乐》

9 合作伙伴

10 投资机构

11 风险说明:

本项目存在以下方面的风险,请投资人注意:

1. 合规、运营性风险

合规、运营性风险是指 DGames 在认筹资金以及开展业务的过程中违反了当地法律法规,造成经营无法继续的风险。针对合规、经营性风险运营团队采取的避险方 式为: • 运营团队和决策委员会采取分布式运作方式,排除单点风险; • 在开展业务的当地聘请专业律师,在法律框架下设计数位资产发行、数位资产交易、区块链金融、区块链应用等方面业务。

2. 市场风险

市场风险是指 DGames 没有被市场接纳,或者没有足够用户使用,业务发展停滞,没有足够利润支撑。针对市场风险运营团队采取的避险方式为: • 与业界分享 DGames 理念,借鉴同类产品运营经验,并对 DGames 优化改进; • 利用创始团队积累的经验,迅速孵化平台生态并产生利润。

3. 技术风险 技术风险是指底层技术出现重大问题,导致 DGames 平台无法实现预期功能,以及关键数据被篡改或丢失。针对技术风险运营团队采取的避险方式为: • 基于成熟、开源、安全的区块链技术,采用已经被商业客户认可和验证过的构架开发 DGames 系统; • 专案组认筹足够资源后,吸纳更多的行业高端人才加入开发团队,奠定基础,充实力量,借鉴成熟开发经验。

4. 资金风险

资金风险是指专案资金出现重大损失,例如:资金被盗,资金亏损,储备金大幅贬值等。针对资金风险运

营团队采取的避险方式为: • 储备金采取多重签名钱包+冷存储方式由决策委员会共同掌管,在多重签名方式下,当出现 3 名董事同时不能履行职责的情况时,储备资金才会面临风险; • 运营团队有丰富的风控经验, 可以有效的把控专案风险,保护用户根本利益。

11 免责申明

该文档只用于传达资讯之用途,并不构成买卖 DGames 的相关意见。 以上资讯或分析不构成投资决策。本文档不构成任何投资建议,投资意向或教唆投资。 本文档不构成也不可理解为提供任何买卖行为或任何邀请买卖任何形式证券的行为, 也不是任何形式上的合约或者承诺。 相关意向用户明确了解 DGames 的风险, 投资者一旦参与投资即表示了解并接受该专案风险。