Ludos 协议：去中心化游戏生态

Ludos Protocol
A Decentralized Gaming Economy

一、摘要

Ludos 协议是一套去中心化游戏生态的解决方案，由三个部分组成：

- 包含公链和多条游戏侧链的底层协议栈

包含了基于 PoW+PoS 混合共识的公链 Ludos Chain，基于 Plasma 的多侧链和跨链协议，基于状态通道的链下合约交互协议以及跨公链交互协议。

- 面向区块链游戏开发者的工具组

包含了抽象区块链交互接口，游戏数字资产发行上链工具，游戏侧链发行工具，数据持久化工具，透明随机数工具等。

- 去中心化游戏生态 DApp 和经济激励体系

包含了去中心化的游戏资产交易所，游戏数字资产钱包，去中心化的游戏分发体系，公正排行榜和成就体系，游戏 DAICO 和投资协议，以及生态激励和动态调整规则组。

当前区块链游戏面临很多实际问题，诸如公链吞吐量差，智能合约占用资源过多，单个爆款 Dapp 堵塞整个网络，开发门槛较高，生态不开放不收敛等。Ludos 选择不盲目相信和过度依赖未来的技术迭代，理智地选择当前被证实的技术路线，灵活将前沿开源社区的现有技术成果同步到游戏生态，同时认清当前的技术局限，在去中心化和效率间作出合理妥协，并开源核心代码，实现去信任化和高效的游戏生态。

Ludos 利用智能合约实现游戏侧链的管理、生态激励的核心逻辑以及游戏道具货币等数字资产的相关操作。同时，Ludos 协议借助区块链公开透明不可篡改等特性实现虚拟物品和原创内容追踪确权，并做到跨平台地永久记录玩家的游戏成就、排名和战绩，实现玩家游戏成就的终身化。

Ludos 将运用区块链技术和通证经济激励理念重组游戏产业成本结构，为游戏社区增进上下游资源自由流通，为玩家们提供更加公平透明的游戏生态，为游戏厂商带来新的机遇和流量。

二、背景

2.1 游戏市场规模现状

投资银行 Digi-Capital 最近发布的报告显示：全球游戏软件和硬件收入将在 2017 年超过 2000 亿美元，每年以接近 50% 的增速递增，其中软件收入占总收入的四分之三，预计到 2021 年游戏产业收入规模将增至 3000 亿美元。腾讯自开展游戏业务以来，游戏贡献了超过 70% 的利润。这是一个庞大、符合潮流、且仍在快速增长的市场。

其中，PC 游戏、主机游戏、网页游戏以及手机游戏成为最主要的用户聚集领域。得益于智能手机的大规模普及，手机游戏已经成为游戏产业中最重要的市场，手游玩家占游戏用户 86% 以上的比例。

2.2 游戏产业面临革命

2.2.1 游戏产业中心化严重

当前游戏产业中心化严重，利润几乎被巨头垄断，游戏同质化严重，优秀的开发团队生存空间非常有限。好的游戏创意也往往胎死腹中，既没有机会公诸于众进入大家的视线，也难找到可以实现其创意的开发团队和产品策划团队来实现产品，更难遇上靠谱的市场发行团队来操盘整个游戏的生命周期。

2.2.2 传统游戏众筹模式效率低下

传统游戏众筹往往通过 Kickstarter 这样的中心化众筹平台，项目的甄别筛选不够透明高效，募资额度不合理，开发进度不受监控，资金使用情况不够透明公开。最终投资人的利益无法得到保障，潜在未来玩家的信心受挫，从而影响整个游戏产业的健康发展。

2.2.3 游戏数字资产权益不受保障

中心化的游戏运营方出于多种盈利目的，通过创造新的顶级装备，滥发稀有物品，篡改玩家游戏人物属性数据，制造恶性通胀等是普遍现象。玩家手中辛苦所

得的虚拟物品和数字资产无法保值，往往不得不通过增加游戏时间或大量充值的方式来维护自己在游戏中的权益。

2.2.4 跨游戏数据孤岛效应严重

当前，市场对于跨游戏跨平台的资产 / 身份流通没有有效的解决方案，游戏与游戏之间的货币、数字资产、虚拟人物等没有有效的交换和流通方式。玩家在厌倦一个现有的游戏并考虑切换到另一个游戏的时候往往面临一个全部抛弃，另一个从零开始的尴尬境地。市场需要一个去中心化的平台来通过技术手段和共识来实现用户与用户间，游戏与游戏间，平台与平台间的无缝数字资产交易交换。

2.2.5 游戏暗箱操作，无法证明公平性

常见的游戏类型有棋牌、MMO、MOBA、FPS、ACT、策略、博弈等，上述游戏类型中都会存在例如技能触发、伤害输出、伤害防御、洗牌、发牌、道具掉落开奖等游戏场景，这些场景均依赖于随机数值的随机性。游戏开发和运营商通过在服务器上采用黑箱操作的方式来控制此类核心数值，导致游戏可玩性、公平性以及持续运营能力受到影响。

2.2.6 游戏金融系统混乱

1）缺少通用代币，各类游戏的游戏币、充值卡无法兑换，玩家对一种游戏的游戏币投入无法转化到其他游戏，游戏币被锁定在游戏内部无法在游戏之间自由交易。游戏厂商也可以自由设定游戏资产的退出机制，来防止玩家的过度流失。

2）在现有游戏开发和运营体系中，游戏货币的发行毫无依据，造成游戏货币超发滥发。游戏运营商随意操控游戏币，虚拟物品暴涨暴跌，核心算法不公开、不透明、甚至不公正。 游戏运营一段时间后，游戏的公平性、可玩性等问题的原因带来游戏性和竞争性的损失，造成用户流失。

2.2.7 发行推广效率低下

游戏推广渠道一方面连接游戏运营商和开发者，一方面将游戏推荐游戏用户，并从中获取收益。然而玩家的关键游戏数据只存储在游戏运营商服务端处，游戏推广渠道的质量评价和收益获取依赖于对游戏运营商的“信任关系”。游戏推广渠道无法也无从获取真实的推广效率回馈，从而导致游戏渠道推广效率下降，无法进一步优化及转化。

2.3 区块链游戏面临的问题

2.3.1 品类单一不够丰富

区块链游戏普遍模式单一，受限于养宠，挖矿，赌博，市面上充斥 CryptoKitties 竞品以及布洛克城竞品。玩家忠诚度低，流失度高，缺乏复杂而有趣的游戏品类。

区块链游戏往往强调收藏、增值等噱头，刺激玩家从享受游戏本身的乐趣转移到投资赚钱，结果是吸引来了众多不关心游戏的投机分子，而非热爱游戏的忠实玩家。

2.3.2 技术性能低，主链堵塞问题严重

CryptoKitties 堵塞以太坊主网已成笑谈。单个爆款游戏 DApp 堵塞整个区块链网络，占用大量计算资源和数据存储资源成为区块链游戏发展必须突破的难关。

2.3.3 开发门槛较高

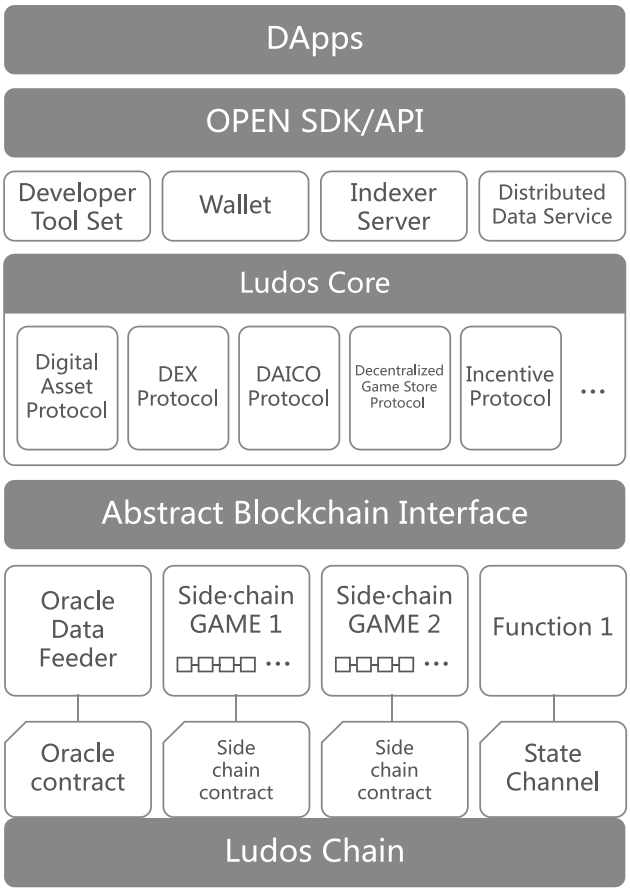
区块链游戏缺乏统一的开发引擎以及成套的开发者工具包，游戏开发者往往需要面对区块链底层技术细节，不能集中精力于游戏本身的开发。Gas 费机制导致区块链游戏应用运行成本昂贵，难以商业落地。

2.3.4 Token 使用场景单一

去中心化游戏平台往往无法为开发者，艺术家和玩家社区构建有效的 Token 激励和社区自治。Token 使用场景单一，经济体系不完善，无法为整个游戏行业提供持久的价值。

三、Ludos 协议和技术架构

Ludos 协议通过基于 Plasma 的多侧链和跨链协议实现主链扩容，同时辅助以基于状态通道的链下合约交互方案，实现游戏资产在主链锚定、合约逻辑运算以及数据存储在主链之外进行的高效底层架构；而游戏研发者可通过 Ludos 提供的工具包来与之进行交互。Ludos 相信，区块链基础设施只有支持大量优质 DApp 在其上流畅运行，才能真正体现它的价值。



3.1. 设计理念

以区块链技术赋能游戏产业，以 Token 经济助力上下游资源高效自由流通是 Ludos 不变的愿景。根植于这一愿景和游戏产业的实际情况，Ludos 将侧链、跨链、智能合约和 StateChannel 等技术融合进现有的区块链架构以改进其在 CAP 不可能三角下的性能表现。

Ludos 的技术架构是开放的、可进化的；团队相信，一切技术最终都是为玩家服务。Ludos 协议包含了一条基于 PoW+PoS 共识的公链，建立多游戏侧链体系，同时研发相关的落地 DApp 和开发工具包，搭建游戏开发者和玩家社区，验证经济体系的可持续性和相关协议的鲁棒性，并不断对协议本身进行更新迭代。Ludos 所有核心逻辑以及游戏运行逻辑将基于智能合约实现，并将所有游戏数字资产，游戏过程中的核心操作和随机数生成结果等关键数据都记录在链上，一切行为公开透明。

关键数据之外的数据，如描述文字、图片、评价、信用等信息将被保存在 IPFS 之上，并与相关智能合约建立链接。如此，Ludos 可以实现更好的可扩展性，并减少不必要的燃费损失。

Ludos 在技术架构设计上有下面 3 个重要的原则：

1）Ludos 力求去中心化和去信任化。

2）Ludos 希望一直能站在巨人的肩膀上。

3）Ludos 会努力保证计算性能和用户体验的平衡。

同时，Ludos 将努力实现下面几个技术目标：

- 游戏和独立场景的 DApp（如去中心化交易所，玩家社区等）将运行在专属且去中心化的区块链上。
- 为开发者提供友好的区块链应用开发接口，使其可以仅关注核心逻辑的开发而不必在意底层技术细节。
- 支持大规模应用（游戏），低燃费，且高吞吐量。
- 侧链应用将可更新，可自治分叉，可共享数据。

3.2. 主链 + 多侧链

Ludos 在设计时充分考虑了游戏场景的高强度交互和高实时性要求的特性，Ludos 协议采用去中心化程度较高的 PoW+PoS 共识主链，配合多条有独自共识机制、安全等级、吞吐量、以及数据存储方式的游戏 / 功能侧链来实现安全和效率的同时兼顾。Ludos 主链将主要被用于侧链根合约的部署、数字资产的发行、交易的结算以及价值的传递，同时主链可以作为纠纷的仲裁者在侧链发生恶意攻击时保证资产可以安全退回，而具体业务（游戏、独立功能）的执行则交给拥有更高吞吐量的侧链处理。

3.2.1 主链共识机制

Ludos 主链采用 PoW（Proof of Work）+PoS（Proof of Stake）的混合共识机制。PoW 也称工作量证明，根据矿工的工作量作为链条随机选取记账人的标准。PoS 也称股权证明，会根据持币者持有数字货币的数量和年龄来分配记账权。PoW+PoS 是一种平衡了矿工和用户角色的混合型共识算法。

- 混合共识的优势

PoS、PoW、DPoS 孰优孰劣是一直争论不休的问题，其各自也有各自被人诟病的缺点：PoW 浪费资源，PoS 容易产生马太效应，DPoS 中心化严重等。

Ludos 相信 PoS 的未来，最终 Ludos 主链将转向纯粹的 PoS 作为共识机制。但是，当前纯粹的 PoS

机制面临着诸如 nothing at stake attack 攻击、有潜在的中心化危险等问题，成功运行的公链鲜有仅依赖传统 PoS 作为共识算法的案例。

Ludos 选择在过渡时期采用 PoW+PoS 作为共识机制：当前，每出 50 个 PoW 块会相应地有一个 PoS 验证，可以最大化矿工和普通用户的共同参与度，使两方都受益。另外，PoS 机制将鼓励 LUD 币的持有者将币留在钱包而不是去交易所卖掉。这将有助于用户关注 Ludos 技术和生态而不是市场波动产生的短期利益。

- 币龄（Coin Age）

Ludos 共识算法的 PoS 部分采用了币龄的概念，其特点为：

每个币每天产生 1 币龄。例如持有 100 个币，总共持有 30 天，此时币龄就为 3000。

如果产出了一个 PoS 区块，币龄清空为 0。币龄越大，获取出块权概率越高，公式为：

$$Hash(block\_header) < coinAge * Target$$

每被清空 365 币龄，将获得年利率个币的利息。如果年利率为 5%（将根据网络情况动态调整以符合持币人的利益），则币龄为 3000 的用户发现区块将获得：

$$3000 * 5\% / 365 = 0.41 \text{ 个币}$$

- 保证金机制

Ludos 通过将保证金机制引入混合共识的 PoS 部分，用于来约束验证者的行为。Ludos 的网络节点必须先缴纳保证金（即锁定保证金）成为“锁定保证金的验证人”后，才可以参与出块和共识形成。

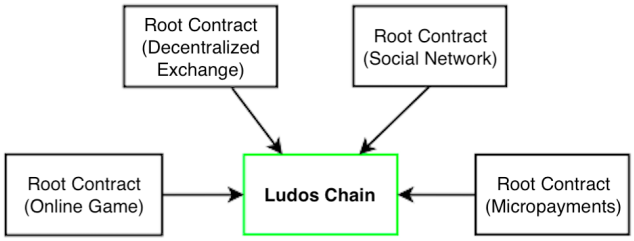
如果一个验证人做出了任何 Ludos 认为“无效”或“恶意”的事情，他的保证金将被没收，出块和参与共识的权利也被取消。

保证金的引入解决了 "nothing at stake"，也就是经典 PoS 协议中做坏事的代价很低的问题。现在有了代价，而且被客观证明做错事的验证人将会付出这个代价。

3.2.2 基于侧链的扩容方案

Ludos 将给出 Plasma 分层侧链协议的一个实现 Ludos Plasma。目标是将功能或游戏的大量智能合约计算转移到侧链上，而不是在 Ludos 主链上执行。侧链可以以相对少节点弱中心化的网络架构起步，同时采用 PoA 或 DPoS 作为共识算法（侧链发行方可以根据实际情况选择最符合需求的共识算法），每秒交易笔数或可以达到数千。

这套扩容方案是一种链下交易的技术，依靠 Ludos 主链底层来实现它的安全性。它允许创建附加在 Ludos 主链上的侧链。这些侧链反过来可以产生他们自己的侧链，他们的侧链也可以产生他们侧链，等等。其结果就是，我们可以在侧链级别执行许多复杂的操作，运行拥有数千名用户的游戏，并且只需与 Ludos 主链进行尽可能少的交互。而这些侧链内部可以更快地操作，且交易费用更低，因为它的操作不需要在整个 Ludos 区块链存留副本。



一个入驻 Ludos 平台的游戏公司如果想研发一个基于 Ludos 的区块链卡牌游戏（如炉石传说），那么他们需要：

1) 在 Ludos 主链上创建相应的数字资产，即卡牌，这些卡牌将符合 LRC721 标准（一种运行在 Ludos 上的虚拟物品协议）。

2) 在 Ludos 主链上创建一套智能合约（Ludos 平台将提供基本模版和自定义接口），作为侧链的根合约（Root Contract）。这套根合约包含了游戏的“状态交易规则”，可以记录侧链状态的 hash，同时包含主链与侧链间转移资产的规则。

3) 使用 Ludos 提供的 baas 接口创建侧链，并依照喜好选择侧链的共识算法（下面详述）。同时选择合适的网络架构以及节点运行方式，启动侧链的运行。

侧链一旦创建并激活，块生产者将定期（新区块产生时）向根合约做出声明。这些声明被记录在根合约所在的 Ludos 主链，作为侧链发生计算的证据。

Ludos 的扩容方案允许扩展基于区块链的数字资产的互动。这些资产需要首先在 Ludos 主链上创建，通过根合约移动到侧链；然后，我们在子链上部署包含所有游戏逻辑和规则的实际游戏应用的智能合约。

当用户玩游戏时，他们只与侧链交互 。例如，他们可以将持有资产（LRC721 卡牌）与 LUD Token 进行兑换，和其他用户互动，而无需直接与主链交互。因为只有侧链上的非常少的节点（即区块生产者）必须处理交易，所以交易费会很低并且操作会很快。

3.2.3 Ludos Plasma 的实现

Plasma Cash 由 Vitalik 和 Karl Floersch 在 2018 年 3 月共同提出，是 Plasma 分层侧链协议的升级和补充，解决了旧版本 Plasma 侧链的扩容问题并有可能缓解挤兑退出（mass exit）的问题。

Ludos Plasma 基于 Plasma Cash 实现了一部分侧链扩容方案。Ludos Plasma 使用户可以将 Ludos Chain 主链上的数字资产（Fungible or non-fungible Token）安全传送至游戏侧链，并在完成交互后安全地退回到主链。同时 Ludos Plasma 提供了 Challenge 期（初始为 3 天），阻断了一切来自侧链用户以及 Plasma Operator 的恶意行为产生实际破坏的可能性。

Ludos Plasma 对存入侧链网络上的 Token 分配唯一的 ID，并使其不可替代（non-fungible）且拥有独立的交易历史。从而使得侧链网络具备如下特性：

- 客户端分片验证

客户端将只需关注其自身持有的侧链上的 Token，进而吞吐量将不受个体用户增加的限制。

- 无需确认

侧链交易将无需进行二步确认，只要主链区块包含了一笔侧链交易，则 Token 即可正常支付出去。

- 支持所有种类 Token

简单支持所有 Token，包括 non-fungible。

- 缓解挤兑退出问题

挤兑退出的问题得到缓解，作恶者将需要为每一个想要偷走的 Token 发起退出请求。

Ludos Plasma 的具体实现包括下面三部分：

1. 部署在 Ludos Chain 主链的根合约。其实现的核心代码（Solidity 语言）如下：

```
contract RootChain {
    address public authority;
    uint public depositCount;
    uint public currentBlkNum;
    mapping(uint => bytes32) public childChain;
    mapping(bytes32 => uint) public wallet;
    mapping(uint => exit) public exits;
    mapping(uint => Challenge.challenge[]) public challenges;
    struct exit {
        bool hasValue;
        uint exitTime;
        uint exitTxBlkNum;
        bytes exitTx;
        uint txBeforeExitTxBlkNum;
        bytes txBeforeExitTx;
    }
    function submitBlock(bytes32 blkRoot, uint blknum)
        public isAuthority;
    function deposit(address currency, uint amount)
        payable public returns (bytes32);
    function startExit(bytes prevTx, bytes prevTxProof,
        uint prevTxBlkNum, bytes tx, bytes txProof,
        uint txBlkNum) public;
    function challengeExit(uint uid, bytes challengeTx,
        bytes proof, uint blkNum) public;
    function respondChallengeExit(uint uid, bytes challengeTx,
        bytes respondTx, bytes proof, uint blkNum) public;
    function isChallengeExisted(uint uid, bytes challengeTx)
        public returns (bool);
}
```

2. 客户端与主链及侧链的交互组件。其退出至主链（Exit）以及提出挑战（Challenge）相关的核心代码（Python）如下：

```
class Client(object):
    def __init__(self, root_chain, child_chain) ...
    def deposit(self, amount, depositor, currency) ...
    def submit_block(self, key) ...
    def send_transaction(self, prev_block, uid, amount, new_owner, key) ...
    def get_current_block(self) ...
    def get_block(self, blknum) ...
    def get_proof(self, blknum, uid) ...

    def start_exit(self, exitor, uid, prev_tx_blk_num, tx_blk_num):
        prev_block = self.get_block(prev_tx_blk_num)
        block = self.get_block(tx_blk_num)

        prev_tx = prev_block.get_tx_by_uid(uid)
        prev_block.merklize_transaction_set()
        prev_tx_proof = prev_block.merkle.create_merkle_proof(uid)

        tx = block.get_tx_by_uid(uid)
        block.merklize_transaction_set()
        tx_proof = block.merkle.create_merkle_proof(uid)

        self.root_chain.functions.startExit(
            rlp.encode(prev_tx),
            prev_tx_proof,
            prev_tx_blk_num,
            rlp.encode(tx),
            tx_proof,
            tx_blk_num
        ).transact({'from': w3.toChecksumAddress(exitor)})

    def challenge_exit(self, challenger, uid, tx_blk_num):
        block = self.get_block(tx_blk_num)

        challenge_tx = block.get_tx_by_uid(uid)
        block.merklize_transaction_set()
        tx_proof = block.merkle.create_merkle_proof(uid)

        self.root_chain.functions.challengeExit(
            uid, rlp.encode(challenge_tx), tx_proof, tx_blk_num
        ).transact({'from': w3.toChecksumAddress(challenger)})

    def respond_challenge_exit(self, responder, challenge_tx,
        uid, tx_blk_num) ...
```

3. 执行主侧链跨链交互的 Oracle 组件，即 Plasma Operator。其核心操作为向主链提交区块，实现代码（Python）如下：

```
def submit_block(self, sig):
    signature = bytes.fromhex(sig)
    if (signature == b'\x00' * 65 or
       get_sender(self.current_block.hash, signature) != self.authority):
        raise InvalidBlockSignatureException('failed to submit a block')

    merkle_hash = self.current_block.merklize_transaction_set()

    authority_address = w3.toChecksumAddress('0x' + self.authority.hex())
    self.root_chain.functions.submitBlock(merkle_hash, self.current_block_number).transact(
        {'from': authority_address}
    )

    self.db.save_block(self.current_block, self.current_block_number)
    self.current_block_number = self.db.increment_current_block_num()
    self.current_block = Block()

    return merkle_hash
```

3.2.4 侧链共识机制

侧链可以拥有它们自己的共识算法。

Ludos 平台默认的侧链共识机制是 PoA（Proof of Authority）。PoA 是一种简单的、依赖于可信验证者（Validator）的共识机制。验证者与 PoW 系统中的矿工类似，它们是接收交易、形成区块并收取交易费的节点。PoA 网络只要有一个验证者就可以正常运行。创建游戏的公司可以运行多个身份公开（identity at stake）的节点，作为侧链的验证者。

创建游戏的公司还可以选择其他如 DPoS、PBFT 等算法作为侧链的共识，以符合自己的节点网络规划。

3.2.5 侧链安全

用户将自己的在主链上的资产发送至侧链，这将产生一系列的安全和信任问题。侧链需要给出相应的审查机制和退出机制，来保证系统的完整去信任化。

Ludos 侧链会定期向主链发送梅尔克证明（Merkle Proofs）作为侧链运行的检查点（Checkpoint）。发送频率可以依据侧链想要的安全级别和费用自由设定，发送的证明越多越安全但要承担更高的费用。

Ludos 为侧链的玩家提供了侧链退出机制（Plasma Exit），即使发生侧链区块生产者试图将侧链的资产擅自移回主链并盗走的情况，玩家依旧可以将资金和资产安全退回到主链上。

Ludos 侧链协议包含如下机制，即欺诈发生时资产不能退回到主链。任何人都可以向根合约发布欺诈证明，尝试表明某区块生产者有欺诈行为。这个欺诈证明会包含前一个块的信息，并且允许我们证明根据侧链规则，当前块（错误块）不是根据前一个块的状态正确产生。如果这个欺诈被证实，那么侧链就会回滚到前一个区块的状态。在此之上，Ludos 侧链协议还有一个处罚机制：任何对错误块签名的块生产者都会损失他们在 Ludos 主链上的保证金。

最后，并不是非要所有的块生产者都要被一个实体（创建侧链的组织）所控制。Ludos 将为新创建的侧链引入玩家、开发者以及其他自治实体，并把区块生产者分布在不同的实体中，即提供共识即服务（CaaS，见 3.2.6）。这种情况下，区块生产者作恶的风险变小，用户不得不把资产转移到主链上的风险也变小了。

3.2.6 共识即服务（Consensus as a Service）

对于刚刚起步的新游戏，其侧链网络可能没有充足的节点来实现共识，甚至遭受女巫攻击。Ludos 平台将为之提供多个可信任的节点来实现侧链网络的共识。CaaS 的节点提供者将来自 Ludos 社区的其他参与者，他们将得到平台给予的相应激励。

3.2.7 跨侧链价值交互

Ludos 并不支持侧链间的直接价值交互，引入主链之外的价值交换渠道（如 Oracle 等）只能导致网络复杂度激增，可用性变差。

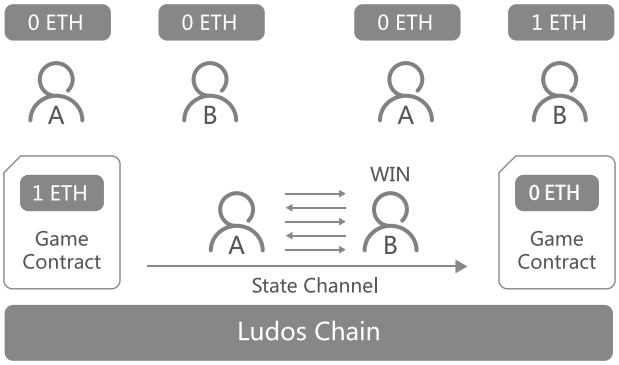
侧链间价值交换，如跨游戏的数字资产交易，都需要先将侧链的资产通过根合约送回主链，再通过主链进行资产交易。这种形式将牺牲一定的效率，且需要多花费交易手续费，但保证了原子交易的可行性，以及资产的安全和系统的简洁。

3.3 状态通道

状态通道是一种进行链下交易和其他状态更新的技术。在一个状态通道内发生的事情保持着非常高的安全性和不可更改性：如果出现任何问题，Ludos 可以选择回溯到链上交易中的上一个保存状态，关闭通道，并释放锁定的资产。

作为状态通道的特殊应用，支付通道的概念已经存在多年，如比特币区块链上的闪电网络。实际上，状态通道不仅可以用来进行支付，还可以用来在区块链上进行任意的状态更新，例如改变智能合约的内部状态。

玩家 Alice 和 Bob 的例子：



Alice 和 Bob 想在 Ludos 上玩一个井字游戏，赢家可以获得 1eth。要做到这一点，最简单的方法就是在 Ludos 主链上创建一个智能合约，它可以实现井字游戏的规则，并跟踪每个玩家的操作。每次当一个玩家进行一次操作的时候，他们向智能合约发起一个交易。当其中一个玩家赢了的时候，就像规则里描述的那样，智能合约就给赢家支付 1eth。虽然上述逻辑是可行的，但是 Alice 和 Bob 正在让整个区块链网络处理这个游戏合约，每次有玩家想要进行操作的时候，他都必须支付 gas 费用，而且必须等几个块被挖出后才能采取下一步行动。这明显多于他们的需求并且效率低下。相反的，我们可以设计一个系统，让玩家尽可能少地在链上进行操作的情况下来做游戏。Alice 或 Bob 能在链下更新游戏合约的状态，并仍然有充分的信心。如果有必要的话，他们可以恢复到主链的状态。我们把这种系统称为状态通道。

应用和限制

状态通道在需要频繁合约交互的应用中非常有用，能切实扩容并提高区块链的承载能力。

Ludos 状态通道机制将有如下的一些限制：

- 依赖于状态的有效性

如果通道参与者在游戏挑战期（期间认为游戏结果不公正的人可以提出挑战）内丢失了网络连接，则可能无法在游戏挑战期结束前做出回应。例如 Bob 为了赢得比赛，伪造了游戏结果，并破坏了 Alice 家的网络，导致 Alice 无法在游戏挑战期访问区块链。在这种情况下，Alice 可以让 Ludos 提供的状态托管网络保留自己的状态副本，并支付一定费用，来保持有效性。

- 仅适合在较长一段时间内做高频率状态更新的 DApp

- 参与的多方在单一合约中需要相对固定

- 通道内操作将默认被隐藏

一切都在参与者之间的通道“内部”发生，而不是广播和记录在链上。只有最初和最后的交易必须公开。

- 状态通道将具有即时终结性

只要游戏合约的参与者多方都签署了一个状态更新，这个状态就可以被认为是最终状态。参与者对此都有很高的信心；如果有必要，他们可以随时“强制执行”将此状态放到主链上。

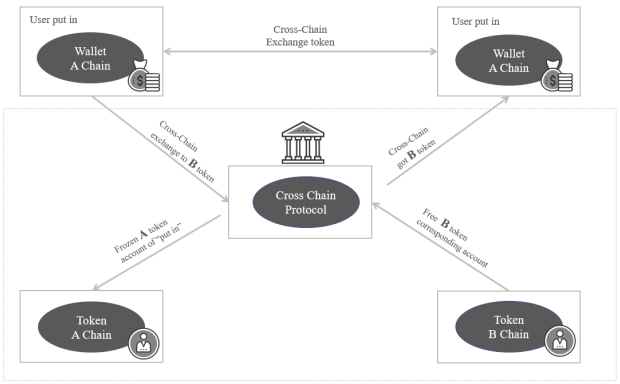
3.4 跨链交互

Ludos 协议要实现的去中心化游戏生态也包含了基于其他第三方公链的游戏和平台，而要进行跨链跨游戏跨平台的资产转移，就需要跨链技术带来的去中心化资产交易能力。另一种情况是，按照游戏的结果以去中心化的方式分发其他区块链网络（如比特币、以太坊）的数字资产或执行跨链智能合约，这都需要 Ludos 具备跨链交互的能力。

目前主流的跨链技术包括：

1）公证人机制（Notary schemes）
2）侧链 / 中继（Sidechains/relays）
3）哈希锁定（Hash-locking）

无论采用哪种技术，其实现方式如何复杂，去中心化跨链资产交易的本质都将如下图所示：



其实现有下面五个步骤：
1. 用户使用 A 链资产向跨链协议发起兑换 B 链资产的请求；
2. 跨链协议锁定用户 A 链资产；
3. 跨链协议锁定等值数量的 B 链资产；
4. 将 B 链资产发到用户 B 链地址，同时拿走用户锁定的 A 链资产；
5. 用户 A 链资产转走，对应获得 B 链等额资产。

Ludos 依赖侧链和中继（Sidechain/Relay）的方式来实现基本跨链功能，同时结合以上三种技术方案的优势来实现真正去信任化的跨链数字资产交易的自动化运作，并在跨链机制上实现以下特性：

1. 便携式资产（Portable assets）：资产可以多链之间来回转移和使用。

2. 满足原子性交换（atomic swap）：跨链资产兑换是安全的而且同步发生的。（不同链上的两位用户可以发起两笔传输交易，要么在两个账本上一起执行，要么两个账本都不执行，即原子性）

3. 带有跨链互通性，具备他链信息和事件的读取和验证能力（Cross-chain oracle issues）：在某些情况下，一个链（如 A 链）的智能合约执行机制可能是依赖另一个链（B 链）的条件触发。所以 A 链要能获得 B 链的所有相关条件状态，即必须具备他链信息和事件的读取和验证能力。

4. 资产留置权（Asset encumbrance）：在某些情况下，相关联的两个链资产同时需要被锁定，如抵押品或者法院强制执行的扣押等。

5. 跨链智能合约（General cross-chain smart contracts）：例如根据链 A 的游戏结果在链 B 上分发数字资产等。

跨链所涉及到的技术点非常多，很多细节实现难度很大，目前牺牲一部分效率验证跨链 SPV 的情况下基本可以实现跨链的去信任化资产转移操作。

跨链智能合约则面临更多的技术难点，Ludos 将可能在多重签名公证人机制（Multi-sig Notary Schemes）以及分布式私钥控制技术（Distributed Private Key Control）方向上投入更多精力，最终实现兼容并包的去中心化游戏生态。

3.5. 其他核心组件

3.5.1 可更新智能合约

Ludos 将通过在链上的智能合约保存核心数据，同时实现平台核心逻辑的自动执行。

这套合约分为两大门类：
1）第一类为 Ludos 平台业务逻辑，包含数字资产发行 / 游戏众筹 / 去中心化交易所 / 激励经济逻辑等。
2）第二类为游戏逻辑模版和数值模型，用于区块链游戏的模块化开发。

Ludos 协议的实现主要表现为成套 Solidity 写成的智能合约。这套智能合约必须是可广泛复用和可更新的，我们为实现这一目标，设计了注册表合约（Registry Smart Contract），用于跟踪版本。
同时，Ludos 将使用“抽象智能合约层”来实现合约代码的部署和升级。所有合约都将有一个封装合约，封装合约将一直指向最新的代码。之前旧版本的合约将被映射在某个版本控制合约中，如果有必要可以直接进行访问。
所有的 Ludos 协议合约将在注册表合约中登记。

3.5.2 前端 DApp

Ludos DApp 将会是一个开源的 React 应用或 JavaScript 应用。它将与以太坊网络、IPFS 网络、索引服务器进行交互。
DApp 将为用户提供一个友好的智能合约交互界面，以承载 Ludos 区块链上的数字资产发行、游戏众筹、去中心化交易所等功能。Ludos DApp 将使用 js-ipfs 来与 IPFS 网络交互，同时使用 web3.js 来通过 MetaMask 等钱包客户端与以太坊网络进行交互。
Ludos 鼓励开发人员可以基于 Ludos 的合约来写出用户体验更好的 DApp。
某个游戏开发人员通过创建游戏资产合约来发行一个新的游戏数字资产，而游戏资产类的信息一般体

积较大，不可能完全保存在智能合约，需要存放在IPFS。上述功能的具体实现过程：

1. 开发人员连入 Ludos DApp（典型的情况是开发者平台）。

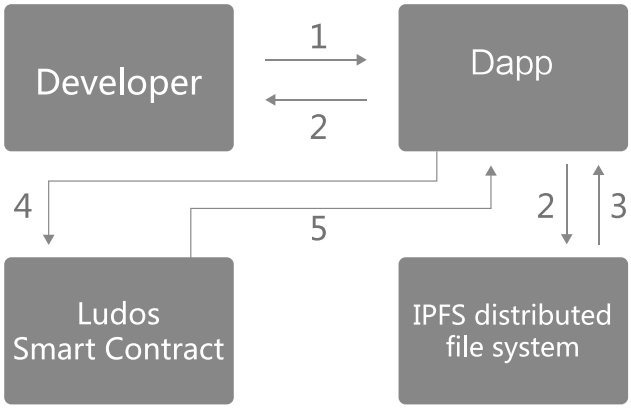
2.DApp 通过与开发者的交互，生成了一个包含了各类基本信息（metadata）的 JSON 对象（样式后面具体有阐述）。DApp 将验证此 JSON 对象是否符合标准样式；如果符合，则上传至 IPFS。。

3.IPFS 返回上传内容的 hash。

4.DApp 将返回的 hash 发送给智能合约工厂。

5. 智能合约工厂生成数字资产并上链保存，然后返回一个 txid。

6.DApp 将监视这条未完结交易，并在交易成功后通知用户。



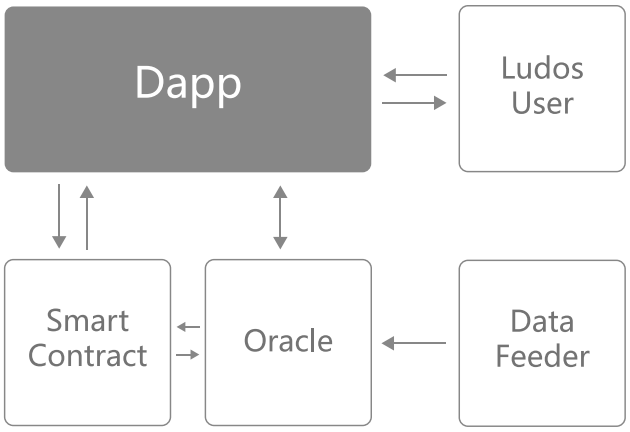
3.5.3 索引服务器

索引服务器是开源的服务器端的应用，它不断读取注册表合约中最新的合约信息，同时从 IPFS 上获取相关合约的文件和数据，并将读取的数据缓存加索引，以便实现 DApp 的快速搜索和条件过滤功能。

索引服务器在网络可扩展方面作用至关重要，Ludos 索引服务器将为平台提供基本的搜索和过滤功能。Ludos 将鼓励开发者分叉源码，开发自己的高效可扩展区块链应用。

3.5.4 预言机（Oracle）

预言机是一种可信任的实体，它通过签名引入关于外部世界状态的信息，从而允许确定的智能合约对不确定的外部世界作出反应。预言机具有不可篡改、服务稳定、可审计等特点，并具有经济激励机制以保证运行的动力。

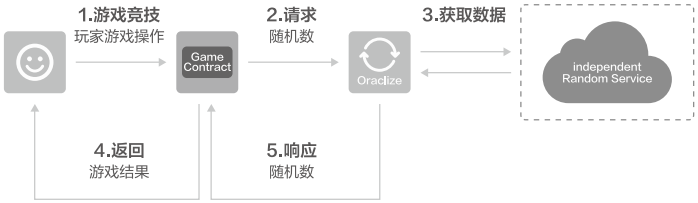


Ludos 体系中在前期会留有一些无法去中心化的环节，如入住平台的中心化游戏，法币支付相关环节，合作伙伴提供的服务，随机数服务，以及跨平台跨游戏的交互等等。这些环节产生的外部数据也需要与 Ludos 主链进行智能合约的交互，继而参与到 Ludos 去中心化体系中来。

例如法币支付的环节，Ludos 点对点支付协议是基于智能合约的多重签名方式；用户使用法币支付购买游戏物品后，区块链本身并没有办法获取支付成功或失败的结果。这时就需要预言机来获取支付结果，并将结果映射到智能合约中，从而完成一次交易。

在绝大部分情况下，一台预言机已经足够；但在处理重大资产时，常常一台预言机并不能保证完全可靠，有人提出了多台预言机的解决方案，比如设置 5 台预言机，如果其中有 3 台或 3 台以上给出的支付结果一致，则向区块链发起一笔携带此结果为备注的交易，从而变相把结果通知给智能合约。这种由多台单一独立预言机组成的多重模型又被称为预言机网络。

3.5.5 公正随机数



随机数是大多数游戏中经常用到的核心参数，例如虚拟道具的掉落、物品的合成结果、伤害输出、伤害防御、技能触发、NPC 的刷新频率等等。随机数计算直接

影响了游戏的公正性和可玩性。

对于区块链这样的确定性系统，实现随机数是十分困难的。因此，Ludos 采用预言机（Oracle）来向链外获取权威的定制化的随机数。

其流程有以下几个步骤组成：

1）玩家向 Ludos 平台上的某个游戏充游戏币并开始游戏，这时直接调用相应游戏的智能合约。

2）智能合约记录玩家信息和充值信息，系统向 Oracle 发起自己自定义模式的随机数请求。

3）Oracle 收到调用请求后，向独立权威的随机数服务获取定制化随机数的数据，避免矿工对随机值的影响。

4）获取到产生的随机数后，Oracle 将得到的数据信息带入到 Ludos 区块链网络中，返回给游戏的智能合约。

5）游戏的智能合约检测返回随机数来源的有效性和数据的有效性之后，将随机数转换为游戏对应的结果。通过智能合约的事件机制将结果回档给用户前端。

3.5.6　零知识证明机制

零知识证明是指一方（证明者）向另一方（验证者）证明一个陈述是正确的，而无需透露除该陈述是正确外的任何信息。

非交互式验证中以 zkSNARKs 算法最为成熟。

Ludos 中零知识证明技术将主要被应用于两个场景：

・游戏资产 / 账号 / 情报等拍卖或交易中的隐私保护

・模版化游戏开发功能中游戏模版的数值设计等知识产权的保护。区块链游戏开发者将只能使用模版而无法获知其内部设计。

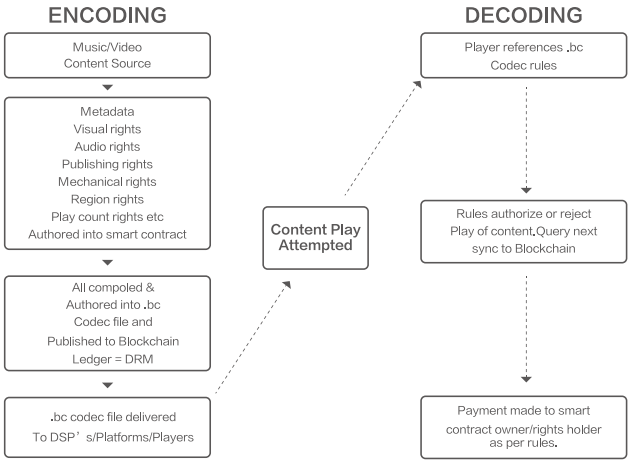
后者的一种实现如下：

设游戏 G，加密后的模版 E，密钥数字指纹 C，数值模版 T，密钥 K。其中：C:=SHA256(K)，E:=Encrypt(K,T)，Proof:=Prove(pk, G, E, C, K, T)。将 <Proof, G, E, C> 作为明文给使用模版的游戏开发商。若 Verify(vk, G, E, C, Proof) 为 true，则：

・T 必须对游戏 G 有效

・E 必须是 T 通过 K 加密得到

・C 必须是 SHA256(K)



3.6 .bc Codec 虚拟物品上链协议

.bc（dot Blockchain） Codec 是使得游戏设计者、平面设计者、音乐家等虚拟内容创作者和艺术家可以利用区块链的智能合约技术来对自己的作品进行定价、属性标注、操作方式描述并最终实现数据上链的成套协议。

Ludos 平台在未来将有许多游戏支持以去中心化的方式拥抱个人设计师和艺术家，尤其是基于 VR 技术的游戏，亟需优质的内容生产者和设计师来为玩家提供新鲜而有趣的 3D 虚拟物品。

设计师可以将自己的作品基于 .bc codec 协议发布至 Ludos 平台，并以自由的方式针对不同游戏设置定价、交易方式、属性、故事等等。最终生成具有唯一性的数字资产上链。

3.7 DAICO 协议

3.7.1 DAICO 的实现方式

DAICO 合约由一个需要募集资金的开发团队发布。DAICO 合约由“贡献模式（Contribution Mode）” 开始，指定一个机制：

每个人都可以将 LUD Token 贡献到合约当中，并得到相应的代币。可以是有封顶的售卖、无封顶的售卖、荷兰式拍卖、互动式的代币发行、KYC 的动态个人封顶售卖或者团队选择的任何一种机制，当贡献阶段结束后，就无法再继续贡献 LUD，初始的代币余额将设定，之后代币可以被交易。

在贡献阶段结束后，合约有一个主要状态变量：tap（单

位：go/sec，go 为 Ludos 货币体系最小单位），初始值为零。tap 决定每秒钟开发团队可以从合约中提现的数量。通过如下实现：

```
tap: num(go / sec)
lastWithdrawn: timestamp  # 将时间值初始化为贡献结束时间
@public def withdraw():
    send(self.owner, (block.timestamp - self.lastWithdrawn) * self.tap)
    self.lastWithdrawn = block.timestamp
@private def modify_tap(new_tap: num(go / sec)):
    self.withdraw()
    self.tap = new_tap
```

同时，还有机制可以让代币持有者通过投票获得解决方案。有两种解决方案：

- 提高 tap 值
- 永久地自毁合约（或者更准确地说，将合约进入 withdraw 模式，剩余的 LUD 可以按比例地提现给代币持有者）

两种方案都可以通过仲裁的多数票决启动（比如：yes − no − absent / 6 > 0）。注意，无法通过投票降低 tap 值。所有者可以自愿降低 tap 值，但是他们无法单方面提高 tap 值。

这样做的目的是，投票者可以给开发团队一个合理而不太高的每月预算，假如团队不断证明其能力，预算可以通过投票提高。如果投票者对团队的开发进展不满意，他们可以完全关闭 DAICO 并取回自己的资金。

3.7.2 博弈安全性

任何投票系统都面临 51% 攻击、贿赂选票和其他博弈上的缺陷。任何 ICO 都面临团队不负责任或者项目仅仅是一个骗局的风险。在 DAICO 中，这些风险都得到了最小化，除非开发者和投票者联合才能产生破坏。

- 51% 攻击以提高 tap − 诚实开发者可以自发降低 tap，或者不提现多余的资金。
- 51% 攻击以自毁合约 − 诚实开发者可以再发布一个 DAICO

注意，两种潜在的 51% 攻击：

1) 将资金发送到攻击者选择的第三方

2) 降低 tap 值将资金永远锁在合约里，在系统中都是不被允许的。

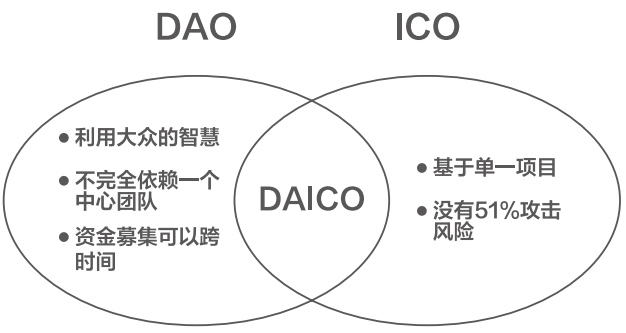
3.7.3 可做尝试的其他玩法

- 将 tap 值设为 usd/sec（每秒多少美元）
- 某个其他加密货币作为募集资金而不是 LUD
- 尝试除了简单投票之外的其他机制

四、基于 Ludos 协议的产品设计

4.1 全球区块链游戏投资孵化生态

Ludos 平台的游戏开发者可以在 Ludos 平台上宣布游戏立项，发布 ICO，获得早期游戏开发资金，并使用户从早期就参与到游戏的开发进程中。获得用户支持的开发商可以便捷地开发并发行自己的游戏。Ludos 平台致力于提供一个让每个开发者都能存活、成长、成功的发布环境。



Ludos 平台遵循 Vitalik（以太坊创始人）提出的 DAICO 模式。任何 ICO 都面临团队不负责任或者项目仅仅是一个骗局的风险，任何投票系统都面临 51% 攻击的问题、贿赂选票和其他博弈上的缺陷。在 DAICO 中，这些风险都得到了最小化。

4.1.1 游戏数字资产和货币发行

如同以太坊社区的 ERC20 和 ERC721，Ludos 可以支持一键发布基于区块链的数字资产（fungible & non fungible）。

4.1.2 游戏众筹和 ICO

有开发和企划能力的游戏开发者可以发行并预售未来游戏中流通的代币，以 ICO 的方式来获取开发游戏必要的资金和资源。

区块链 ICO 行业的乱象丛生，这是大家都看到的事实。Ludos 既反对游戏项目方对融资的滥用和开发进度的不透明，也反对投机者在早期就抛售手中的代币在二级市场抛售，从而使后来的投资者对项目产生不良的预期。

Ludos 相信区块链本身恰恰是解决这一问题的答案：

1）基于智能合约的 DAICO 有效地限制了游戏开发方的行为，迫使其合理使用资金并定期公开开发进度和披露代码。

2）基于智能合约的锁仓 + 自动释放对投资人的行为进行了合理的规制，既保证了投资人的合理收益，也迫使其以长远的眼光来进行投资，做好各种 KYC，间接降低了投资风险。

4.2 虚拟资产确权

Ludos 平台通过智能合约进行游戏中的各类虚拟资产，比如游戏道具、皮肤、宠物等进行独一无二的确权。比如之前火爆的以太坊游戏“以太猫”，其本质是使用 ERC721 协议的 “Non-Fungible Tokens”，非同质代币。“每只以太猫拥有独一无二的基因，每只小猫和繁衍的后代也都是独一无二的。从原理上来看，每只以太猫在区块链平台上都是一条独一无二的代码，因此没有两只外表和特性完全相同的小猫。而且，ERC721 每个代币都有一个独立唯一的 tokenid，例如在 cryptokitties 里就是猫的 ID，独一无二。

Ludos 会将各类虚拟游戏资产通过智能合约的方式存储在底层区块链中，不同用途的游戏虚拟资产采用不同的智能合约协议。每个数字资产都有独一无二的合约协议、所有人和内容描述文件的引用。并且通过智能合约来确认和维护虚拟世界中的地块所有权账本。

4.3 去中心化游戏数字资产交易生态

4.3.1. 游戏币购入

单个游戏的游戏货币作为数字资产上链，总量恒定或有限制地增发。一切交易结算上链，交易记录可审查，可追溯，不可篡改。

4.3.2. 游戏内资产交易

单个游戏的核心资产上链需要上链。其他的装备，临时性的武器、金币等，可以以中心化的方式链下撮合和交易，定期上链结算，并将交易记录打包，将哈希值保存在 Ludos 区块链上。

链上结算和链下 Layer2 高频交易的方式结合，既保证单个游戏的性能，也保证整个主链的网络畅通。

4.3.3. 跨游戏的资产交易

Ludos 去中心化游戏交易所将整合全部基于 Ludos 区块链的数字资产，为平台资产提供二级市场，以用户习惯的直观形式（K 线，下单，交割）为游戏资产提供交易流通性。

游戏的资产原先是孤立于单个游戏的，Ludos 去中心化交易所将为之提供流动性，单个游戏的某个独立的装备也将变得具有投资价值，有眼光的投资者可以从中获取投资收益。

从一个游戏中脱离并决定投入另一个游戏的玩家，也可以在交易所变现自己原有的资产，然后购入新游戏的新资产，并无缝迁移到新游戏中去。

Ludos 去中心化交易所技术上采用链下高频下单撮合，链上交割结算的方式，并不托管用户的数字资产，既保证交易的体验，也保证了个人数字资产的安全。

4.4 去中心化的游戏成就和排行榜

Ludos 将帮助平台上的游戏运营方建立公开透明的竞技激励和排名体系，建立成就和排名奖励协议 LRAP（Ludos Ranking & Achievements Protocol），每个游戏将按照此协议实现自己的具体规则。

4.4.1 LUD ID 系统

每个 Ludos 平台的参与者的钱包地址将自动成为其唯一的 ID 和凭证，与以太坊网络不同的是，Ludos 的钱包地址将具备可实名认证，可追回，可设置权限的特点。

4.4.2 奖池、排名和成就激励协议

单个游戏将设立公开透明并基于智能合约的奖池。

成就的达成和排名数值作为智能合约的Oracle输入，并自动触发奖励分配的逻辑，实现相应数字资产的分配。

4.5 去中心化推广激励生态

与其他平台（Steam，Origin，GOG 等）不同，Ludos 提供了一个开创性的激励和多层次推荐系统，允许玩家在游戏中和社交活动中赚取收入，以及从其他玩家的付款赚取返佣费。通过加 Ludos，开发者将减少其营销费用，并从平台上的其他游戏中获得额外收入。

用户和开发者在给平台产生贡献的过程中，平台会通过奖励代币的形式予以奖励。对于平台贡献者定义以及可能获得的奖励如下：

1）高活跃用户：每天代币消费量的 10% 返还；

2）代理用户 & Room Host：代理用户发展的新用户成为高活跃用户时，代理用户 获得代币奖励；

3）高质量游戏开发商：对提供高质量游戏入驻的游戏开发商，提供代币奖励；

4）帮助游戏开发者做游戏 ICO 发行，提供代币奖励

5）糖果奖励: 平台会针对用户和开发者定期发放糖果，以感谢用户对平台的支持

Ludos 提供游戏社群，直播平台和测评内容发布平台。整合游戏行业现有的参与者，包括优秀的测评师，KOL 和电竞播主等，以去中心化的方式对生态贡献者进行激励，使得优秀的游戏可以脱颖而出，或可成为爆款游戏，带来聚集效应，并使得全部 Ludos 平台的参与者都可获益。

4.6 艺术家社区

4.6.1 艺术作品的上链确权

Ludos 提供基于 .bc Codec 协议的艺术作品数字资产化和一键上链操作。

4.6.2 作品的拍卖和使用权分享

基于智能合约和多重签名钱包的去中心化交易和使用权的分享。

平台将分配第三方的见证者来参与多重签名钱包的建立。三方有两方对交易签名就可以完成一笔数字资产的交易或使用权分享。一旦出现纠纷，则第三方见证者入场，合理地调解纠纷，见证者也可以获取相应的 LUD 代币作为激励。

4.6.3 评价

艺术家将随着自己作品在游戏中实际被使用被喜爱，其自身将获得二级通证 DLV Token，其间接影响艺术家在 Ludos 平台的影响力和身份等级。

4.7 Ludos 开发者社区

Ludos 将为游戏开发者提供支持各个主流平台的 SDK/API，以及多种多样的技术支持和平台化的解决方案。而这都离不开一个强大的开发者社区。

Ludos 将 会 对 Android / iOS / Unity / Oculus / HTC Vive / HTML / Windows / MacOS 等诸多平台的游戏进行广泛的支持，这需要来自世界各地的各个层面的开发者参与进来，一起实现游戏 2.0 和游戏区块链化的革命。

Ludos 将以赠予 LUD Token 和 DLV Token 的方式激励参与到开发者社区贡献代码的优秀开发人员，激励规则和激励目标将由 Ludos 社区进行上层设计和投票表决。

五、Ludos 去中心化游戏激励生态

5.1 生态参与者

Ludos 生态将面向全球的游戏从业者、投资人和游戏玩家，每个参与者都可以通过贡献价值来参与到 Ludos 生态的建设中，共同推动全球游戏产业 2.0 的进化以及区块链技术的应用落地。

参与者角色可分为游戏开发者，游戏发行商，Ludos 社区，投资人，艺术家，游戏玩家，测评师，传播者，其他服务者。

5.1.1 游戏开发者

拥抱区块链技术的传统游戏开发商，或具备游戏策划和研发能力的个人，通过 Ludos 平台以去中心化的方式实现游戏产品的落地，迭代和商业转化。

5.1.2 Ludos 社区

Ludos 社区包括：

- 平台创始团队
- 市场运营团队
- 开发者社区
- 去中心化直播平台
- 去中心化游戏数字资产交易所

5.1.3 投资人

参与 Ludos 平台上游戏 ICO 的投资人。游戏开发者通过发行游戏数字资产及代币来发起 ICO，投资人通过 LUD Token 进行投资并获取相应的游戏数字资产。

该游戏数字资产后续将在 Ludos 平台自由的交易所上线，投资人或将其交易成其他数字资产变现，或转化为游戏玩家，在开发者上线的游戏中使用相应数字资产并获取较高的早鸟优势。

Ludos 的 ICO 公募活动将符合 DAICO 规范，来保证投资人的投资利益。

5.1.4 艺术家

为 Ludos 平台不断输送灵感的艺术家群体，包括平面设计师，3D 设计师，故事线设计师和数值设计专家。Ludos 将通过有吸引力的通证激励手段以去中心化的方式聚集优秀的灵感，以数字资产的形式对艺术家的作品进行上链确权，并保证其拥有自己作品的最终所有权。游戏开发者可以通过支付的相应的 LUD Token 来自由使用艺术家的灵感，一切交易将基于智能合约和多重签名钱包技术。

5.1.5 游戏玩家

所有参与 Ludos 平台游戏的普通游戏玩家。

游戏即挖矿。玩家的任何游戏活动将视为对整个生态的贡献，并以 PoA（Proof of Activity）共识来获取 LUD Token 奖励。普通玩家可以通过充值 LUD Token 来购买平台上游戏的专属数字资产，或在去中心化交易所进行资产间的自由交易。

游戏玩家将自动获取全平台唯一 ID，并可以在专属的 Ludos 钱包中管理和查看当前拥有的游戏数字资产，包括各个游戏的货币(fungible)以及皮肤和装备(non fungible ）等等。

5.1.6 测评师

普通游戏玩家可以通过发表专业的测评文章和打分，来自由切换为测评师的角色。测评师的测评内容和专业意见也将受到整个社区的点评。

优秀的测评文章 / 改进意见将为测评师带来不错的 LUD Token 收益，以及二级信用通证 DLV Token。

5.1.7 传播者

包括平台介绍人，游戏发现者。

平台介绍人

将新玩家带入 Ludos 平台的现有用户，将通过 PoN（Proof of Number）共识接收到平台的 LUD Token 激励。

游戏发现者

为平台上的新游戏打 Call，通过贡献内容，介绍玩法，付费广告等多种形式来为新游戏带来 Ludos 玩家的发现者。

发现者将通过智能合约的获取推广利益，被发现者带入新游戏的玩家的充值收入将有一定百分比送归发现者。推广利益将最多计算 5 层。

5.1.8 其他服务者

参与 Ludos 平台建设和维护的其他服务者，如游戏客服，交易所和直播平台的运维人员，发现 bug 并报告的人员，游戏产品顾问等。

5.2 LUD 数字通证设计

Ludos 将初始发行总量为 100 亿的 LUD Token。

5.2.1 数字通证 LUD 功能

1）交易手续费

任何造成 Ludos 区块链状态发生变化的操作将需要支付交易手续费，以 LUD Token 形式支付给区块验证人。如：

- 账户间发送 LUD Token
- 智能合约的创建，包括状态通道和侧链的建立（基于根合约）
- 智能合约的交互（发生状态改变），如 token 的发送，侧链状态的 hash 更新等

2）流通功能

在 Ludos 生态中全部的费用支付，如广告费，购买游戏，创建游戏等，均通过 LUD Token 进行。为基于 Ludos 区块链发行的数字资产和 token 提供去中心化交易场景下原生的交易媒介。

3）投票功能

治理规则相关的投票，交易所上币和社区中自然发起的投票活动将接受 LUD Token 作为投票的凭证。Ludos 的钱包 App 将包含代币锁仓以及投票的功能，方便 Ludos 用户随时随地参与投票。

4）参与 DAICO

游戏开发商可以发起基于 LUD Token 的 DAICO，参与者将需要购买并捐赠 LUD Token 到相应的合约地址，并获取开发商发行的 token 或在未来游戏中可以使用的虚拟物品资产。过程类似于以太坊上使用以太币 ETH 参与 ICO 并获取 ERC20 token。

5.2.2 二级数字通证 DLV

DLV 的角色将类似支付宝的芝麻信用，其设计原则如下：

- DLV 的持有者将定期得到 LUD 作为固定收益
- DLV 不可自由在账户间转移
- 可锁定 LUD 来获取相应的 DLV
- DLV 反向解锁回 LUD 需要 90 天时间逐渐释放
- DLV 不可被上交易所自由交易
- DLV 代表用户在 Ludos 平台的信用等级和影响力
- 持有 DLV 多的用户将自动得到更多的权益和相关收益

而获取 DLV 的量主要取决于用户在生态中的各种操作和行为，具体计算方法如下：

我们用 $f_s(x)$ 代表 DLV 的获取量

$$f_s(x) = f(x_{act}, x_{tra}, x_{amo}, x_{num}, x_{eva}) = \lambda_1 x_{act} + \lambda_2 x_{tra} + \lambda_3 x_{amo} + \lambda_4 x_{num} + \lambda_5 x_{eva}$$

x_{act} ：用于衡量在整个生态中的行为操作

x_{tra} ：用于衡量在整个生态中的交易次数

x_{amo} ：用于衡量在整个生态中的交易总额

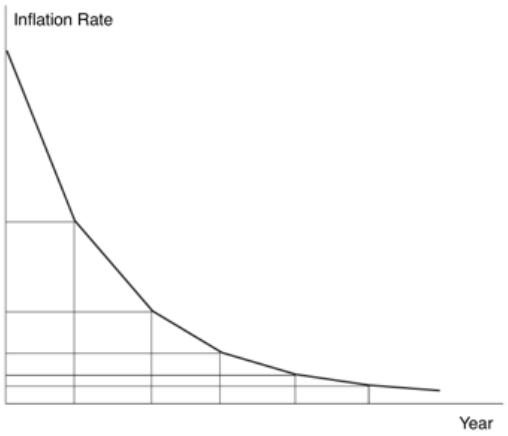
x_{num} ：用于衡量在整个生态与其他生态角色互动的频率

x_{eva} ：用于衡量来自生态系统中其他角色的评价

λ_1，λ_2，λ_3，λ_4，λ_5 为相关比例因子，会根据生态反馈数据进行调整确定。

5.3 Ludos 生态激励机制

Ludos 主网上线之前，社区内部将流通基于 ERC20 标准的 LUD Token，生态激励将使用预挖 100 亿 token 中预留的一部分。Ludos 主网上线后，将进行 LUD Token 向主网的一比一映射，同时开启挖矿奖励和验证人奖励，生态激励也将全部来自于新挖区块的出块奖励（占总出块奖励 70%）。Ludos 此后



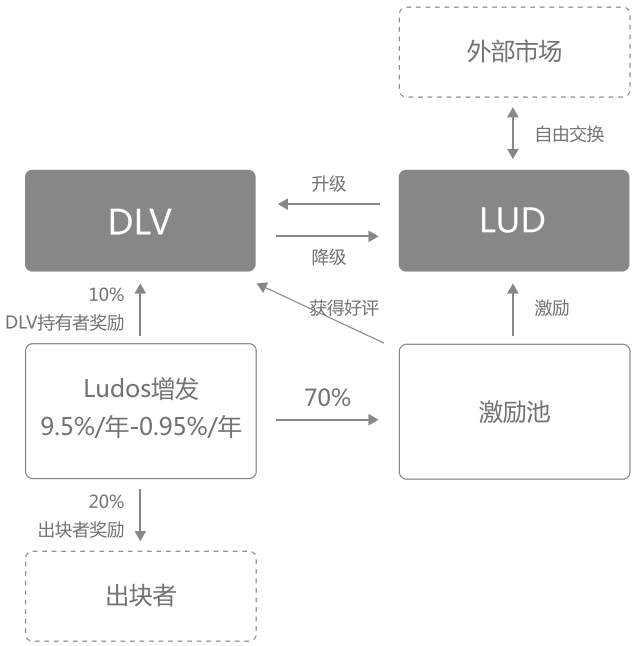
将进入缓慢通胀的阶段，初年通胀率控制在 10% 左右，通胀率在十年时间内逐年递减至 1%，最终总 LUD 币量稳定在 150 亿个左右。

5.3.1 设计理念

每个在 Ludos 贡献了价值的用户都将获取相应的 LUD 作为激励，正向的行为受到鼓励，负向的行为还可能遭到惩罚。平台生态的发展壮大将带来用户对 LUD Token 的极大需求，从而其价值得到提升，LUD 的持有者都将获得平台发展带来的红利和收益。

5.3.2 生态激励分配方案

主网上线后由于加入了矿工的角色，全部出块奖励的 20% 将用于矿工或验证者的收益。另外有 10% 作为 DLV 持有者奖励按比例送出，其余的的 70% 将作为生态激励流入总激励奖池。Ludos 的每个产品模块都将有属于自己的子奖池，而总奖池的资金将按照某套比例流入各个子奖池。



各个子奖池获得奖励的初始比例设计如下：

去中心化游戏分发奖池	25%
开发者社区奖池	15%
内容（艺术家）社区奖池	10%
排行和成就激励池	30%
众筹和新游戏 ICO	5%
推广和广告激励	10%
其他	5%

这个层次的比例设计很难以智能合约的形式来实现动态调整的，Ludos 社区将定期发起投票，来更新这套比例方案，以适应复杂多变的市场，达到动态调整分配比例的目的。投票频率初始设定为 1 月一次。

5.3.3 激励细则

Ludos 委员会按各个奖池给出不同的奖励机制，用户在同一场景将可能触发多个奖池的激励规则。Ludos 将定期发起激励规则调整投票，激励方案将可能动态调整。

1）矿工和验证人

维持 Ludos 区块链底层分布式网络的的正常运转和账本共识的达成将得到激励：

- 超过 2/3 的节点正常运行，获得出块权的正常出块即得奖励
- 超过 2/3 的节点正常运行，未能正常出块的将被判罚小额罚款
- 低于 2/3 的节点正常运行，未能正常出块的将被判罚大额罚款
- 罚款额度与未能正常运行的节点的比例成正比

2）DLV 持有者

DLV 持有即结算币龄，按币龄结算奖励：

- 每周一 0 点清零币龄，分发本周 DLV 持有者奖池的奖励
- 按照币龄占本周总币龄的比值计算奖励

3）游戏分发平台

有效参与或促成分发平台的游戏购买等活动的将得到点数，按点数结算奖励：

- 玩家购买游戏，玩家得 10 点，开发商得 5 点
- 通过分享游戏购买的，分享者得 2 点
- 有效点评游戏者得 3 点
- 按用户本日得点占平台本日总得点数比例计算奖励
- 每日结算，分发本日游戏分发奖池的奖励

4）众筹和 DAICO

- 游戏 DAICO 项目将拥有自己的子奖池
- 发起 DAICO 的游戏开发商和参与 DAICO 活动者都可以获得激励
- 依照开发进度推进研发的开发商将得到激励
- 参与项目方发起的公投等活动的得到激励

5）开发者社区

- 参与 Ludos 议会日常活动以及上层设计和投票，投票成功的将获取奖励
- 参与 Ludos 的技术研发和代码迭代，代码被采纳的将得到相应奖励
- 具体开发项目将有子奖池
- 开发项目的具体激励方案将由项目委员会自行决定
- 开发项目立项以及子奖池具体分配方案将有开发者社区理事会投票决定

6）推广和广告

广告主将向平台支付 LUD，Ludos 平台将依据用户在平台产生的数据向用户精准推送广告。观看广告，以及为 Ludos 带来新的用户和新的影响力的将得到点数，按点数结算奖励：

- 推荐 Ludos 平台并获取有效注册用户，每获取一人得 5 点
- 以指定方式分享游戏者得 1 ~ 3 点
- 以指定方式分享文章者得 3 点
- 开启广告模式（最短一个月）者得 10 点
- 广告模式保持开启，并有效登录并使用平台者，每小时得 1 点
- 按用户本日得点占模块本日总得点数比例计算奖励
- 每日结算，分发本日推广和广告奖池的奖励

7）排行和成就

游戏中的优秀玩家，获取难得的成就以及排行榜名列前茅者将得到点数，按点数结算奖励：

- 活跃度权重高的游戏相关排行和成就将具备更高的加成
- 排行榜前 100 名的用户，第 n 名，将获得（100 × 0.7^n × 活跃度权重）点数
- 成就将按照单个游戏制定的规则代表的权重值以类似排行的计算方式计算点数
- 按用户本日得点占模块本日总得点数比例计算奖励
- 每日结算，分发本日排行和成就奖池的奖励

8）内容社区

提供优质的内容：测评 / 艺术作品等将依据其他用户反馈给予点数，按点数结算奖励：

- 发布有效（游戏测评等）文章者得 5 点
- 有效评论文章者得 1 点，文章作者得 1 点
- 有效回复评论者得 0.5 点，被回复者得 0.5 点，文章作者得 0.5 点
- 发现新内容者（第一评论者）得 5 点
- 按用户本周得点占模块本周总得点数比例计算奖励
- 每周结算，分发本周内容社区奖池的奖励
- 直播等即时内容将按具体流量和活跃度计算奖励，每日结算

9）其他

游戏中的优秀玩家，获取难得的成就以及排行榜名列前茅者将得到点数，按点数结算奖励：

- 造福入住 Ludos 的游戏开发者，包括提供运营和推广相关服务可获得奖励
- 维持平台正常运转的其他关键环节。如客服，交易见证，bug 发现等可获得奖励

六、治理

我们需要考虑一个组织是什么。从结构角度看，组织是不同参与者和实体（例如，人员，其他组织，机器）之间的一组协议。这些协议采用合同和内部规则，正式和非正式协议，准则，流程和程序的形式。总的来说，这本“规则手册”规定了不同组织实体（如管理层，员工，所有者）明确责任，财产权，付款和组织运作的其他要素。他们还定义与第三方，供应商，客户，政府机构和其他利益相关方等实体的关系。

在分布式资产管理的生态中，我们需要基于区块链的智能合约来自动执行的协议，这些协议（即 Ludos protocol）是开放的，安全的，并提供问责制度和透明度。此外，每一方都可以确信承诺会得到真实地保留。因此，我们结合区块链智能合约和中心化的高效管理方式确立了分布式资产管理的治理模式。

——“三权分散式组织”

“三权分散式组织”的治理概念的根本目标是形成去信任化且去中心化游戏生态。

Organization 01
游戏开发者

即拥有游戏设计和研发能力的组织（个人），发起众筹，并运用众筹所得资金，负责游戏本身的设计和运营。

Organization 02
玩家社区

普通玩家和游戏受众。可监督游戏开发者使用资金的流向，以及对游戏的评价推广等。

Organization 03
开发者和艺术家社区

基础设施研发和生态的维护者。

这里必须要提到的是，每一类组织都是分布式的形态，进行相互博弈和共识。组织之间也可以进行转换，组织内共识之后进行组织间共识。组织的转换可以让资源充分在治理过程中体现价值，组织内部和组织间的以此来保证共识的高效性、有效性和安全性。等待区块链的 TPS 到达百万级别，治理的模式可以完全向 DAO 过渡。

Ludos Protocol 的“三权分立”的治理模式既要依托于区块链智能合约，还要依托于中心化的组织（个人），其介于DAO（分散自治组织）和中心化组织之间。

七、核心团队

Joy Hao / 创始人 首席执行官

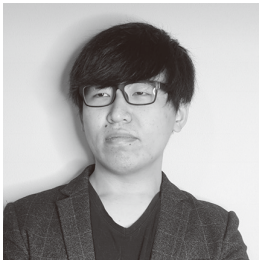
作为区块链行业的早期参与者之一，Joy 女士自 2014 年起便开始专注于区块链科技，并开始在全球布局战略投资。此外，她还曾为数个区块链项目提供过战略咨询。Joy 女士在金融行业有着 8 年的从业经历，精于银行、信托和投资方面的相关知识。

Wilson Wu / 联合创始人

拥有澳大利亚莫纳什大学会计和金融双学位，曾担任FBG One的亚洲业务发展主管，在加入FBG One之前，Wilson是Transintech China的CEO和创始人，Transintech China是一家金融技术公司，为各种金融机构提供固定收益资产管理技术和数据服务。在Transfentech之前，吴先生在中化集团子公司FOTIC（中国对外经济贸易信托有限公司）的小额贷款部门担任董事；在任职期间，管理着价值30亿元人民币的固定收益投资组合。吴先生还曾担任CIFCO（中国国际期货有限公司）的副总裁和交易主管，专攻全球衍生产品市场。

Tai Jin / 联合创始人 首席运营官

卡内基梅隆大学工商管理学、金融学学士；投资分析师、资深区块链投资人。Tai Jin 先生曾任真格基金高级投资分析师，致力于互联网及区块链领域的投资分析。这一经历，让他在区块链、游戏和人工智能方面，获得了丰富的投资经验和独特见解。此外，他在融资、行业研究、投资策略制定及区块链项目运作方面，也有着丰富的经验。



Joe Meng / 联合创始人

北京大学计算机科学学士；资深游戏开发者、创业者 Joe Meng 先生曾任微软亚洲研究院 AI 及传感器网络研究员。此外，他还曾供职于 KLab 株式会社（东京证券交易上市公司），并作为核心开发人员，参与了诸多音乐卡牌游戏的研发。他所开发的热门游戏 Lovelive，在日本应用商店的排名前三。 他在区块链咨询和项目孵化方面有着丰富的经验，并专注于区块链技术落地和去信任系统方面的研究。

Evan Zhang / 联合创始人

Evan Zhang 先生毕业自威斯康星麦迪逊大学，获经济学、应用数学及金融学荣誉学士学位。Evan Zhang 先生曾任花旗银行投资银行部分析师、私募股权基金 SFA 高级分析师。另外，他还曾任美国 Starr 战略控股集团项目经理。他对一级、二级市场的资本运作有着独到的见解，并在科技、游戏和金融服务领域，有着丰富的投资经验。

Rick Zhu / 法律顾问

Rick Zhu 先生毕业自哥伦比亚大学，获法学硕士。此前，Rick Zhu 先生曾任埃克森美孚投资有限公司高级法律顾问。他还曾在数间大学教授编程等课程，并为多个项目提供专业的顾问咨询、合规管理等服务。

Marry Meng / 数据隐私及安全科学家

波士顿大学密码学博士。在相继任职于微软研究院、苹果和亚马逊后，Marry Meng 博士于 2010 年开始研究比特币和区块链。他对云计算环境中的加密协议、区块链及加密货币的相关技术，都进行了深入的研究。他致力于在去信任的环境下，实现大量数据存储时信息曝光的最小化及对隐私的保障。

Jinpeng Zhu / 技术主管

互联网及区块链行业的早期科研人员。Peng 先生曾任日本乐天高级项目经理，负责 EC 仓库及交通系统的设计和开发。此外，他还曾任野村证券交易系统开发团队的主管及安全专家。Peng 先生在交易系统管理、大数据和云计算相关的项目开发方面，有着丰富

Kevin Zhang / 运营总监

Kevin Zhang 先生曾任暴雪娱乐公司游戏研发工程师，并参与开发了其核心产品《守望先锋》。他还曾创办 EZAR，领导团队开发出一款兴趣选择类 App，获天使轮近百万美元投资。Kevin Zhang 先生有着多年海外市场运营经验，熟悉海外市场开发、产品分析及客户挖掘等。

Zoe Zhang / 营销副总裁

重庆大学文学学士。Zoe Zhang 女士是市值 160 亿美金的明星项目波场 Tron 的早期成员和 PR 团队核心领导。此前，她还曾任美国国家地理（中文版）杂志的市场主管。

Sakamoto Yui / 公关总监

Sakamoto Yui 女士毕业于名古屋都立大学，获市场营销学硕士，曾就职于リッチメディア株式会社。Sakamoto Yui 女士是一位资深媒体从业者，有着丰富的媒体资源，与日本多家大型媒体保持良好关系。她在社群运营和公关管理方面，也有着多年的经验。2017 年，Sakamoto Yui 女士进入区块链行业，一直致力于项目孵化、投资并购以及市场推广等相关工作。

Fenny Wang / 高级游戏工程师

Fenny Wang 先生毕业自北京航空航天大学，获计算机学硕士。他曾就职于日本游戏公司 Gumi 株式会社，参与设计及开发了多款倍受玩家追捧手游。Fenny Wang 先生对区块链技术有着多年的深入研究，在游戏区块链技术应用方面，有着充足的实战经验。

Alex Wang / 营销总监

Alex Wang 先生毕业自庆应义塾大学，获商学硕士，并且是高盛奖学金得主及日本政府 Cool Japan 获奖者。Alex Wang 先生曾任日本 Recruit 株式会社大中华区商务拓展总监，并创办了香港华和结控股有限公司。他在媒体方面有着超过 5 年的经验，专攻 ACG（动画、漫画、游戏）领域。他负责过与阿里巴巴、腾讯、携程等大型企业的跨国商务合作项目，其在这方面的丰富经验，让他对中日两国间的商务合作有着深刻的见解。

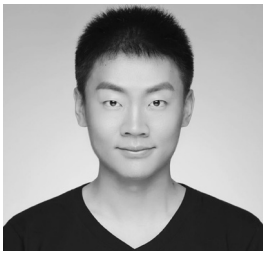
八、顾问委员会

Gregory Wornell / 技术顾问

Gregory Wornell 是麻省理工学院电子工程与计算机系教授，麻省理工学院信号、信息与算法实验室主任。他是信息技术和信息处理方面的世界顶级专家，并曾在信号处理、信息安全、网络通信、统计算法等领域参与了数个重要的科研项目。同时，他和区块链行业有着密切的联系。

大空翼 / 顾问

作为著名的 90 后天使投资人、创业者，有着“梭哈之王”之称的大空翼，对区块链科技有着独特的简介和极高的热情。他曾持有大量 IOTA，并借此实现了 10000 倍的超额回报。他相信，前瞻、雄心和灵感，是区块链行业的基石所在。



Jia Tian / 技术顾问

前百度、阿里巴巴高级开发员；AI 行业资深研发人员现 BitFund.pe 首席科学家。BitFund.pe 是一支由李笑来创立的数字货币基金，自 2013 年开始致力于支持比特币社区。田甲先生同时还是数个区块链科技初创企业的顾问，包括 IOST、DATA、Hydro 等。

Lily Wan / 运营顾问

Lily Wan 女士毕业自耶鲁大学，获工商管理学硕士（MBA）。作为知名区块链基金合伙人，她专注于对区块链技术和加密经济的研究，并投资过多个顶级区块链项目。此前，Lily Wan 女士曾任高盛分析师、大宗商品交易经纪人，YOUNKER CAPITAL 合伙人等。

九、投资者及合作伙伴

SoftBank

VLANE CAPITAL

Fullpay JAPAN

JMODE ENTERPRISE

PUNK Capital

BA CAPITAL

CollinStar

REDNOVA

DDEX

DU CAPITAL

十、路线图

- **2017 年 8 月**
  策划并立项 Ludos
- **2018 年 4 月**
  基金会成立
- **2018 年 Q2**
  Ludos 启动融资
- **2018 年 Q3**
  Ludos 钱包以及测试网络上线
- **2018 年 Q4**
  Ludos 主网上线并进行 token 映射
- **2019 年 Q1**
  多侧链方案测试运行，去中心化交易所上线
- **2019 年 Q2**
  去中心化分发平台上线，支持多侧链功能钱包上线
- **2019 年 Q3**
  多侧链方案和 baas 系统上线
- **2019 年 Q4**
  主链切换至 PoS
- **2020 年~**
  生态体系迭代

十一、免责声明

除本白皮书所明确载明的之外，Ludos 平台不会对 Ludos 或 LUD Token 作任何陈述或保证（尤其是对其适销性和特定功能）。任何人参与 LUD Token 的公开售卖计划及购买 LUD Token 的行为均基于自己本身对 Ludos 以及 LUD Token 的了解以本白皮书的信息。在无损于前述内容的普适性前提下，所有参与者将在 Ludos 项目启动之后按现状接受 LUD Token，无论其技术规格、参数、性能或者功能等。

• Ludos 平台在此明确不予承认和拒绝承担下述责任：

• 任何人在购买 LUD Token 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；

• 任何人在购买 LUD Token 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法付款或无法提取 LUD Token；

• 由于任何原因LUD Token的公开售卖计划被放弃；

• Ludos 的开发失败、推迟或延期，以及因此导致的无法交付 LUDToken 或延迟交付；

• 以太坊或相关区块链原始代码的漏洞、错误、瑕疵、崩溃、回滚或硬分叉等技术问题引起的平台故障；

• 对公开售卖所募集资金的使用；

• 任何参与者泄露、丢失或损毁了数字加密货币或代币的钱包私钥；

• LUD Token 公开售卖的协力厂商平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、解散或关张；

• 任何人对 LUD Token 的交易或投机行为；

• LUD Token 在任何交易所的上市交易或退市；

• LUD Token 被任何政府、主管当局或公共机构归类或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于收到禁止、监管或法律限制；

• 本白皮书披露的任何风险因素，以及与该等风险因素有关、因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。

十二、风险声明

Ludos 开发和运营团队相信，在 Ludos 的开发、维护和运营过程中存在着无数风险，这其中很多都超出了 Ludos 开发和运营团队的控制。除本白皮书所述的其他内容外，每个 LUD Token 购买者还均应细读、理解并仔细考虑下述风险，之后才决定是否参与本次公开售卖计划。

每个 LUD Token 的购买者应特别注意这一事实：尽管 Ludos 开发和运营主体是在日本东京设立的，但 Ludos 和 LUDToken 均只存在于网络虚拟空间内，不具有任何有形存在，因此不属于或涉及任何特定国家。

参加本次公开售卖计划应当是一个深思熟虑后决策的行动，将视为购买者已充分知晓并同意接受了下述风险：

1）公开售卖计划的终止

本次 LUD Token 公开售卖计划可能会被提前终止，此时购买者可能由于比特币 / 以太币的价格波动以及 Ludos 开发和运营团队的支出而仅被部分退还其支付的金额。

2）不充分的信息提供

截止到本白皮书发布日，Ludos 仍在开发阶段，其哲学理念、共识机制、算法、代码和其他技术细节和参数可能经常且频繁地更新和变化。尽管本白皮书包含了 Ludos 最新的关键信息，其并不绝对完整，且仍会被 Ludos 开发和运营团队为了特定目的而不时进行调整和更新。Ludos 开发和运营团队无能力。且无义务随时告知参与者 Ludos 开发中的每个细节（包括其进度和预期里程碑，无论是否推迟），因此并不必然会让购买者及时且充分地接触到 Ludos 开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

3）监管措施

加密代币正在被或可能被各个不同国家的主管机关所监管。Ludos 开发和运营团队可能会不时收到来自于一个或多个主管机关的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何关于本次公开售卖计划、Ludos 开发或 LUD Token 的行动。Ludos 的开发、行销、宣传或其他方面以及本次公开售卖计划均因此可能受到严重影响、阻碍或被终结。由于监管政策随时可能变化，任何国家之中现有的对于 Ludos 或本次公开售卖计划的监管许可或容忍可能只是暂时的。在各个不同国家，LUD Token 可能随时被定义为虚拟商品、数字资产或甚至是证券或货币，因此在某些国家之中按当地监管要求，LUD Token 可能被禁止交易或持有。

4）密码学

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步（例如密码破解）或者技术进步（例如量子电脑的发明）可能给基于密码学的系统（包括 Ludos）带来危险。这可能导致任何持有的 LUD Token 被盗、失窃、消失、毁灭或贬值。在合理范围内，Ludos 开发和运营团队将自我准备采取预防或补救措施，升级 Ludos 的底层协定以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。密码学和安全创新的未来是无法预见的，Ludos 开发和运营团队将尽力迎合密码学和安全领域的不断变化。

5）开发失败或放弃

Ludos 仍在开发阶段，而非已准备就绪随时发布的成品。由于 Ludos 系统的技术复杂性，Ludos 开发和运营团队可能不时会面临无法预测和 / 或无法克服的困难。因此，Ludos 的开发可能会由于任何原因而在任何时候失败或放弃（例如由于缺乏资金）、开发失败或放弃将导致 LUD Token 无法交付给本次售卖计划的任何购买者。

6）众筹资金的失窃

可能会有人企图盗窃 Ludos 平台所收到的公开售卖所获资金。该等盗窃或盗窃企图可能会影响 Ludos 开发和运营团队为 Ludos 开发提供资金的能力。尽管 Ludos 开发和运营团队将会采取最尖端的技术方案保护众筹资金的安全，某些网络盗窃仍很难被彻底阻止。

7）原始代码瑕疵

无人能保证 Ludos 的原始代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能使得用户无法使用特定功能，暴露使用者的信息或产生其他问题。如果确有此类瑕疵，将损害 Ludos 的可用性、稳定性或安全性，并因此对 LUD Token 的价值造成负面影响。

8）安全弱点

Ludos 区块链基于开源软件并且是无准入许可的分布式账本。尽管 Ludos 开发和运营团队努力维护 Ludos 系统安全，任何人均有可能故意或无意地将弱点或缺陷带入 Ludos 的核心基础设施要素之中，对这些弱点或缺陷，Ludos 开发和运营团队无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的 LUDToken 或其他数字代币丢失。

9）“分布式拒绝服务”攻击

以太坊设计为公开且无准入许可的账本。因此，以太坊可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使Ludos系统遭受负面影响、停滞或瘫痪，并因此导致在此之上的交易被延迟写入或记入以太坊区块链的区块之中，或甚至暂时无法执行。

10）处理能力不足

Ludos 的快速发展将伴随着交易量的陡增及对处理能力的需求。若处理能力的需求超过以太坊区块链网络内届时节点所能提供的负载，则 Ludos 网络可能会瘫痪或停滞，且可能会产生诸如“双重花费”的欺诈或错误交易。在最坏情况下，任何人持有的 LUD Token 可能会丢失，以太坊区块链回滚或甚至硬分叉可能会被触发。这些事件的余波将损害 Ludos 的可使用性、稳定性和安全性以及 LUDToken 的价值。

11）未经授权认领待售 LUD Token

任何通过解密或破解 LUD Token 购买者密码而获得购买者注册邮箱或注帐号存取权限的人士，将能够恶意获取 LUD Token 购买者所购买的待售 LUD Token。据此，购买者所购买的待售 LUD Token 可能会被错误发送至通过购买者注册邮箱或注册帐号认领 LUD Token 的任何人士，而这种发送是不可撤消、不可逆转的。每一 LUD Token 购买者应当采取诸如以下的措施妥善维护其注册邮箱或注册帐号的安全性：（i）使用高安全性密码；（ii）不打开或回复任何欺诈邮件；以及（iii）严格保密其机密或个人信息。

12）LUD Token 钱包私钥

获取 LUD Token 所必需的私钥丢失或毁损是不可逆转的。只有通过本地或在线 LUD Token 钱包拥有唯一的公钥和私钥才可以操控 LUD Token。每一购买者应当妥善保管其 LUD Token 钱包私钥。若 LUD Token 购买者的该等私钥丢失、遗失、泄露、毁损或被盗，Ludos 开发和运营团队或任何其他人士均无法帮助购买者获取或取回相关 LUD Token。

13）普及度

LUD Token 的价值很大程度上取决于 Ludos 平台的普及度。Ludos 并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏情况下，Ludos 甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大一部 LUD Token 需求可能具有投机性质。缺乏用户可能导致 LUD Token 市场价格波动增大从而影响 Ludos 的长期发展。出现这种价格波动时，Ludos 开发和运营团队不会（也没有责任）稳定或影响 LUD Token 的市场价格。

14）价格波动

若在公开市场上交易，加密代币通常价格波动剧烈。短期内价格震荡经常发生。该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 LUD Token 交易的二级市场，Ludos 开发和运营团队对任何二级市场的 LUD Token 交易不承担责任。因此，Ludos 开发和运营团队没有义务稳定 LUD Token 的价格波动。LUD Token 交易价格所涉风险需由 LUD Token 交易者自行承担。

参考文献

[1] Baker, Jessi. “Trust in the Digital Age.” Provenance News.October 13, 2016. https://www.provenance.org/news/movement/trus t-digital-age/

[2] 我们把互联网的发展定义为三种：信息互联网即解决信息互通互联的根本问题及基础建设，数据互联网即信息化数据的有效关联，价值互联网即数据的P2P 可信任及区块链化的数据组织再造

[3] https://www-935.ibm.com/services/cn/gbs/ibv/pdf/Unblocking_the_blockchain.pdf

[4] http://www.the-blockchain.com/docs/JP-Morgan-Juno-Distributed-Cryptoledger.pdf

[5] http://www.coindesk.com/jpmorgan-juno-hyperledger-blockchain/

[Other]

- Bitcoin: A peer to peer electronic cash system” at https://bitcoin.org/bitcoin.pdf
- “A protocol for interledger payments” at https://interlegder.org/interledger.pdf
- “Ripple - key feature” at https://ripple.com/technology