

Number Chain

白皮书

二〇一七年十二月

目 录

第一章、 背景介绍	3
1.1 区块链：第四次工业革命	3
1.2 区块链的特点	4
1.3 全球娱乐游戏市场	5
1.3.1 传统游戏产业困境与现行的游戏产业链	5
1.3.2 游戏产业的前景与现状	5
1.3.3 现有游戏产业存在的问题	5
1.3.3 解决方式	7
第二章、 Number Chain 简介	7
2.1 什么是 Number Chain?	8
2.2 平台描述及愿景	8
2.3 NUBC 的平台优势	8
2.4 应用场景	10
2.5 NUBC 社区与用户	12
第三章、 技术架构	12
3.1 平台框架	13
3.2 区块链的功能说明	14
3.3 技术特点	16
3.4 技术说明	17
第四章、 Number Chain 的生态圈	17
4.1 网络节点	17
4.2 NUBC 的云平台	18
4.3 DAPP 的开发者	18
4.4 NUBC 的生态联盟	18
第五章、 Number Chain 发展历程与规划	18
第六章、 代币简介	19
6.1 NUBC 代币说明	19
6.2 NUBC 获取途径	19
6.3 NUBC 发行方式	19
6.4 资金使用说明	20
6.5 分配方案	20
第七章、 NUBC 基金会及组织架构	21

-----Number chain -----

7.1	基金会	21
7.2	组织架构	21
第八章、团队与顾问		23
8.1	团队成员与顾问	23
8.2	联系方式	24
第九章、投资机构		25
第十章、法律事务与风险提示		26
10.1	法律事务	26
10.2	风险提示	26

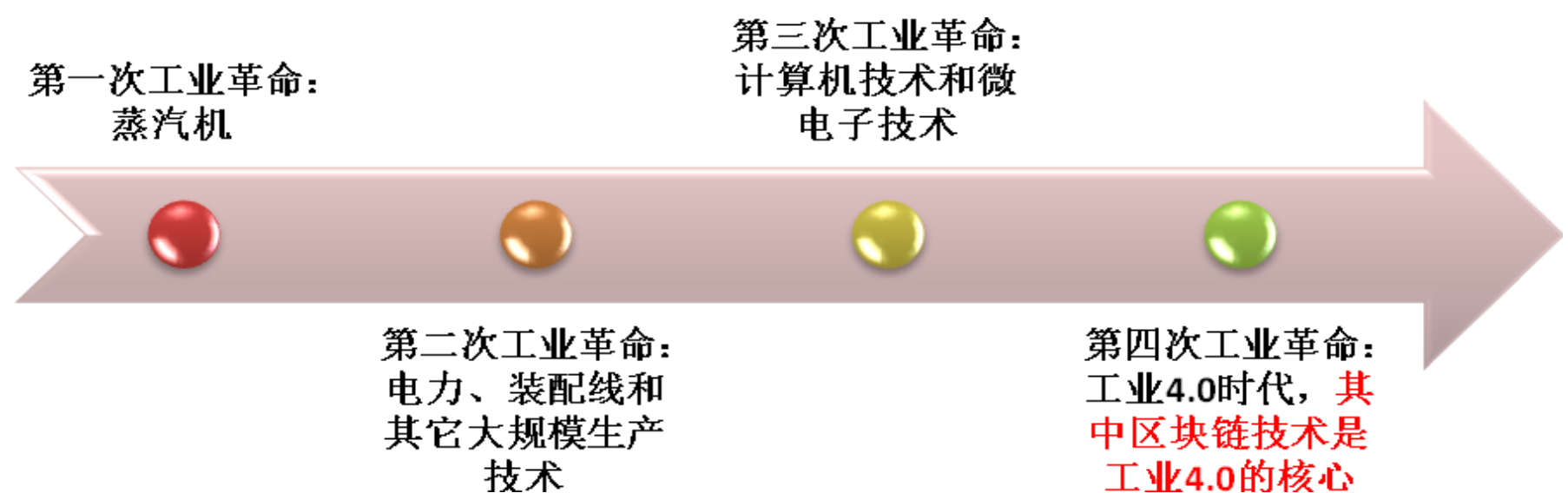
第一章、简介

1.1 区块链：第四次工业革命

正如世界经济论坛创始人和执行总裁 Klaus Schwab 所言，“第四次工业革命的一个主要特征就是它不是改变我们所做的事情，而是改变我们自己。”

蒸汽机推动了第一次工业革命。然后电力、装配线和其它大规模生产技术，带来了第二次工业革命。紧接着，计算机技术和微电子技术推动了第三次工业革命。

现在，惊人的创新，包括物联网、基因工程、3D 打印、人工智能、无人驾驶汽车、机器人和智能设备将带来第四次工业革命，工业 4.0 时代。



图：工业革命的历程

区块链是工业 4.0 的核心

第四次工业革命带来了人类前所未有的全方位改变。本质上，这次革命正在改变人类本身。

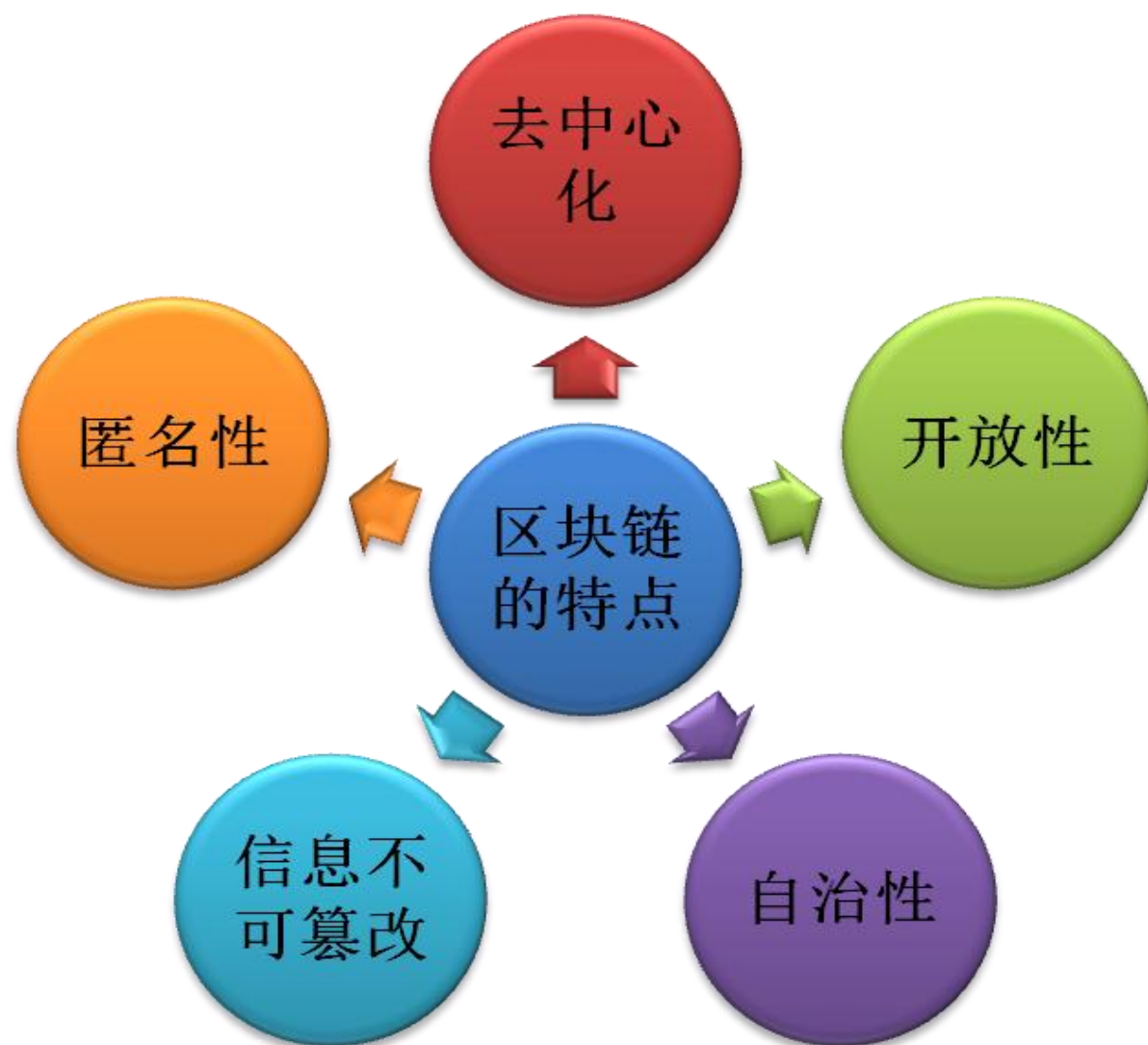
第四次工业革命正在深刻地改变着我们周围的所有事物，甚至是我们的生活方式。本次革命有望在所有工业领域创建更高的效率、为人类带来最大的福利。然而，第四次工业革命要想取得成功，必须要有一个开放、无国界的支付协议。这个协议就是比特币和区块链。

比特币及其潜在的区块链技术是另外一项重要的技术创新。确实，如所言，“区块链是第四次工业革命的核心。”

这些新技术也在巨大地影响着经济和工业。例如，比特币的出现揭露了银行系统和法币是如何的不合时宜。

1.2 区块链的特点

区块链是一种共享的分布式数据库技术，也是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。尽管不同报告中对区块链的一句话介绍措辞都不相同，但以下 5 个技术特点是共识性的。



图：区块链的特点

1. 去中心化

由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。

2. 开放性

系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

3. 自治性

区块链采用基于协商一致的规范和协议（比如一套公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

4. 信息不可篡改

一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中超过 51% 的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

5. 匿名性

由于节点之间的交换遵循固定的算法，其数据交互是无需信任的（区块链中的程序规则会自行判断活动是否有效），因此交易对手无须通过公开身份的方式让对方自己产生信任，对信用的累积非常有帮助。

1.3 全球娱乐游戏市场

全球娱乐游戏市场作为一种新型的娱乐方式，必将成为一个潜力无穷的新兴产业。娱乐是人类永远的需求，尤其是随着人们闲暇时间和可支配收入的增加，对娱乐的需求将更加旺盛。

1.3.1 传统游戏产业的困境与现行的游戏产业链

游戏的质量主要取决于研发商所开发的内容和发行商所提供的运营服务，然而，渠道商和结算通路却占据了绝大部分利润，位于源头的发行商和研发商能获得的收益非常有限，而且需要承担最高的风险，这亦正是游戏产业链的不健康和不完整的根源，埋没了大量优秀的游戏，同时亦浪费了研发商和发行商的资源。

在游戏研发领域，一方面是中小型 CP 因为资金压力无法实现对游戏品质的提高和 IP 的追求，空有好的创意却很难实现，或者在实现之前就被迫放弃；另一方面却是众多中小型发行商为找好游戏四处奔波却求之不得。

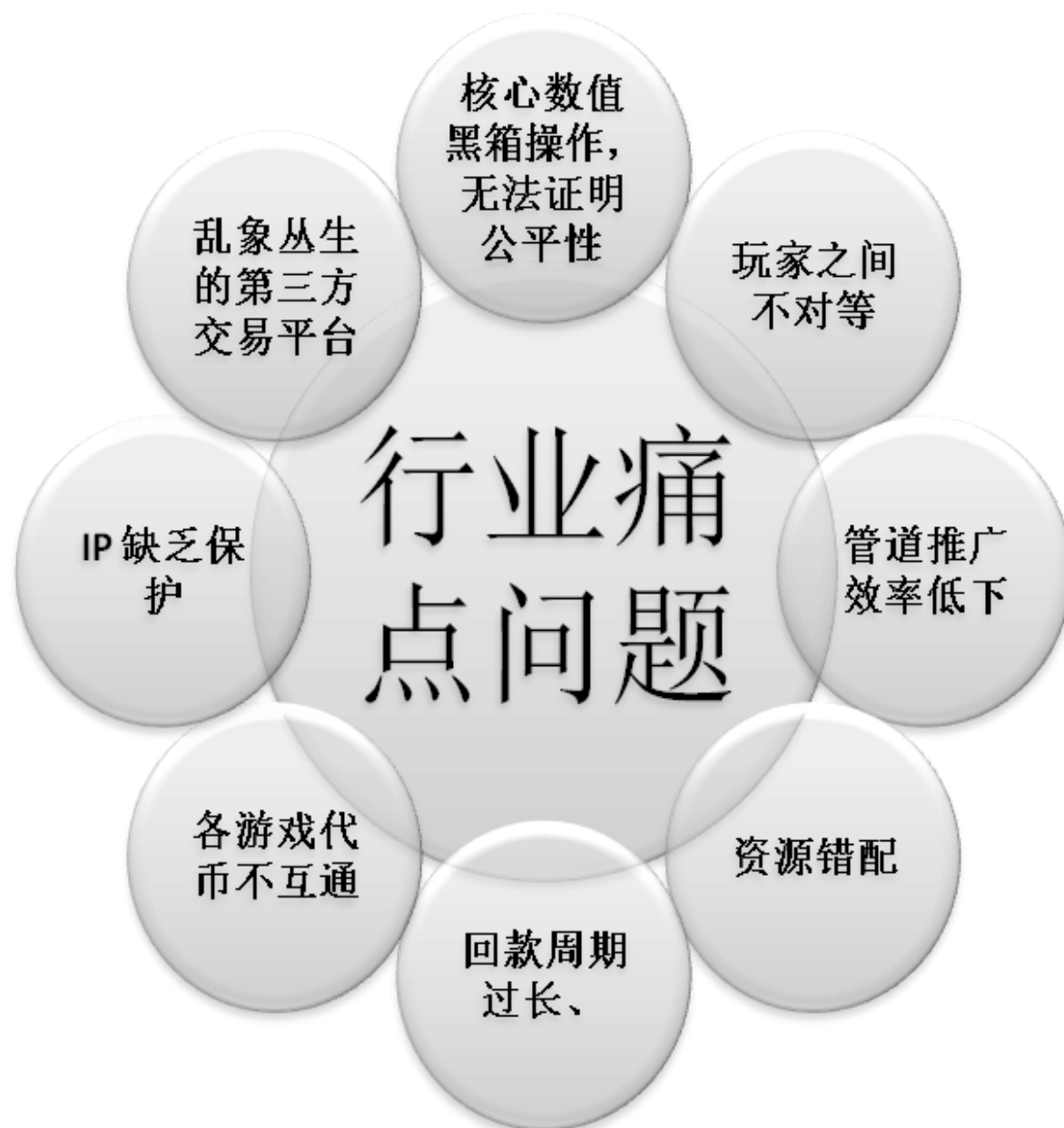
1.3.2 游戏产业的前景与现状

据统计，2016 年全球游戏产业产值已首次突破 1000 亿美元，超过了电影与音乐产业的总和。预计到 2020 年，全球游戏产业产值 将达到 1290 亿美元。移动游戏将会占据产业 51% 的份额，超越 PC 游戏和视频游戏机等传统游戏平台的产值。2016 年中国游戏玩家达到 6 亿人，市场规模达到 246 亿美元，超过了第二名美国的 241 亿美元。亚太地区占全球游戏市场规模的 46%、北美和欧洲地区各占 24%，其中，中国游戏玩家 93% 的支出 流向中国游戏开发公司开发的游戏，美国游戏玩家 56% 的支出投向美国游戏，36% 的欧洲游戏玩家支出投向欧洲游戏。另外，自 2015 年以来，全球游戏产业 70% 的收购交易都由中国买家完成。作为手游产业大国，中国企业将无可避免地要承担起主导产业未来发展的角色，而结合区块链技术的 NUBC 应运而生。

根据投资银行 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 1500 亿美元，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 2000 亿美元。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、网页游戏以及移动游戏成为最主要的用户聚集领域，而得益于智慧移动设备的大规模普及，手机游戏已经成为游戏产业中最重要的市场。

1.3.3 现有游戏产业存在的问题

在线娱乐，无论是在中国游戏市场，还是在全球游戏市场，多多少少存在一些局限性，主要表现在以下几个方面的痛点：



图：游戏行业的痛点问题

1) 游戏核心数值黑箱操作，无法证明公平性

几乎所有线上游戏中都会存在使用者获取游戏道具、游戏奖励、以及各类开奖类活动，然而在现有游戏开发和运营体系中，这些核心数值的算法，都是不公开、不透明、甚至不公正的，游戏开发商和运营商通过在服务器上采用黑箱操作。

2) 玩家之间不对等

游戏用户会尝试各类不同类型的游戏，其中常见的会有：棋牌、MMO、MOBA、竞技、博彩等等，各类游戏内的数值平衡以及玩家之间的公平性，是游戏使用者非常在意的内容。玩家之间有时处于一个不公平、不对等的环境中，用户无从查询和考证，带来游戏性和竞争性的损失，造成用户流失。

3) 管道推广效率低下

游戏推广管道一方面连接游戏运营商，一方面将游戏推荐给游戏用户，并从中获取收益，然而因为使用者充值数据只存储在游戏运营商服务端处，因此游戏推广管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”，游戏推广管道无法也无从获取真实的推广效率回馈，从而导致游戏管道推广效率下降，无法进一步优化及转化。

4) 资源错配

在游戏研发领域，一方面是中小型 CP 因为资金压力无法实现对游戏品质的提高和 IP 的追求，

空有好的创意却很难实现，或者在实现之前就被迫放弃；另一方面却是众多中小型发行商为找好游戏四处奔波却求之不得。

5) 回款周期过长

游戏发行后，回款周期过长，从用户充值到发行商收到款项，一般最少为 4 个月，一般为 5-6 个月，甚至一年。发行商、CP 资金占用周期过长。好的游戏开发时间长达 1-2 年，而游戏上线后的资金回收却达到 5-6 个月。

6) 各游戏代币不互通

由于各游戏的代币之间的不互通，且游戏公司众多，导致一方面是在游戏中的充值不能通用，常常造成浪费；另一方面是游戏用户二次转换较难，一个游戏的用户转到另一个游戏用户中存在很大的壁垒。

7) IP 缺乏保护

游戏的同质化、抄袭泛滥，一款好的游戏出台后，无数换皮版本出现，拉低整个游戏产业的发展水平。同类游戏的品质亦过度参差，在 IP 缺乏保护的情况下，出现大量抄袭 IP，粗制滥造的情况。

8) 乱象丛生的第三方交易平台

随着游戏行业的发展，游戏装备、帐号、代币等交易需求炽热，第三方的虚拟游戏内容交易市场逐渐形成规模。不过，由于缺乏成熟的第三方交易平台，这类交易往往完全独立于游戏系统，存在交易成本高、难以执行、易生纠纷等问题。

中国游戏用户规模达 5.66 亿人，而我们相信上述游戏行业的问题的经济价值高达整个产业产值的 45%。这些行业所关心的问题，在某种意义上制约了行业的进一步完善与进化，而近年来区块链技术的飞跃发展，为游戏行业带来了变革的契机。

1.3.4 解决方式

随着游戏行业及区块链的深入了解，我们发现这样的设计并不合理，理由是当中所涉交易成本 (gas fee) 会非常高昂，同时执行时间亦不能满足一般游戏的需求，而以太坊网络的稳定性亦令人忧虑。有见及此，真正能服务游戏产业的 NUBC 应运而生。为兼顾合作者权益和项目的可行性，NUBC 同时采用了两种最成熟的主流技术，以太坊 Ethereum 和 HyperledgerFabric。

NUBC 是一个立足于游戏产业的去中心化的共享社区，主要针对中小型发行商、中小型 CP、所有游戏玩家、IP 生产者、渠道商、合作者等所共同打造的一个生态系统。其核心是一套基于区块链技术的去中心化的账号和结算系统，使用 NUBC 币作为结算代币，打造一个在各个游戏中通用的数字代币-NUBC。

第二章、Number Chain 简介

2.1 什么是 Number Chain?

Number Chain, 中文为数链, 简称 NUBC, 是在全球在线娱乐上, 一个基于以太坊、分布式的、采用智慧合约方式来保证游戏公平性的游戏平台。内存块链上数据全网共识、不可篡改的特点, 使得 NUBC 区别于传统游戏平台, 完全杜绝了传统游戏中存在的数值黑箱操作、用户之间不平等以及游戏产业链数据不透明。

2.2 平台描述及愿景

在 Number Chain 的区块链技术的全球在线娱乐平台上, 由于此平台具有公开、公正、公平的特性, 用户与平台之间能进行无障碍的沟通, 不存在数据删除, 或者交易记录不能删除的特性, 建立一个公平、公正、平等的游戏生态圈。

对于平台的愿景: 对于游戏运营商而言, 帮助游戏运营商在游戏人气凋零的情况下完整保留用户的人脉数据, 在下一个游戏出来后立刻传导到新游戏中。对于游戏用户而言, 游戏玩家可以把游戏中的人脉关系传输到任意一个游戏之中, 不会流失。

2.3 NUBC 的平台优势

2.3.1 公开、公平、公正

NUBC 将公开平台上所有运行游戏中用于保证公平性的核心随机数数值, 包括游戏道具奖励概率、游戏中随机数获取、玩家匹配平衡数值等, 完全做到核心数据的公开透明。相较于传统游戏中的服务端数据操控, NUBC 创新的引进 Qaclize (外部信息中介) 形式来产生随机数, 数据通过加密信道传输, 从而做到真正意义上的公平、公正。

2.3.2 安全稳定

私钥安全性

NUBC 只需要使用者输入以太坊钱包地址, 就可以通过转账来进行游戏充值或投注等行为。整个投注过程不需要使用者提供任何私钥和密码, 没有任何使用者帐号敏感信息会残留在您的电脑上或者浏览器中, 更不会在网络上传播, 达到最佳的安全防护状态。

终端安全性

NUBC 全站采用 HTTPS 协议, 即安全超文字传输协定, 使用秘密频道对资讯进行加密传输, 具有身份验证、信息加密和完整性校验的功能, 可以有效防范信息窃听、信息篡改和信息劫持的风险。

团队经验丰富

NUBC 开发及运营团队由具备多年网络安全经验、数千万用户量级别游戏平台运营经验的专业人士组成, 确保平台运行安全稳定。

2.3.3 流畅的游戏体验

NUBC 是基于以太坊进行开发，但单纯的以太坊 Dapp 仍然存在交易速度过慢的情况，无法满足和完成大规模的、图形化的、多人在线的游戏要求。因此 NUBC 团队充分发挥自身在平台建设领域内的丰富经验，采用“深度耦合”的方式，将不影响公平性的信息通过传统方式构建，将核心数据通过内存块链上的智能合约处理，两者无缝的进行调用与结合，从而实现了既保证公平性、又保证流畅游戏体验的完美效果。

2.3.4 多终端、多语言支持

NUBC 目前主要以英文语言版本为主，我们将很快上线俄语、韩语、日语等其他语言版本，以满足不同地区使用者的体验需要。同时，我们还会陆续推出多终端版本支持，包括：WEB、移动 APP（IOS、ANDROID）、PC。

2.3.5 多种虚拟货币支持

NUBC 将以 ETH 作为基础平台流通货币，在 ICO 完成后，会支持平台本身的代币(NUBC Token)，并在后续陆续支持其他主流虚拟货币，预计包括：BTC、BCH、LTC、ETC、EOS、XRP 等。

同时，考虑到 NUBC 全球化平台的属性，以及不同国家地区的合规性要求，故 NUBC 不支持任何国家的法币充值与流通。

NUBC 还将建立新代币准入机制，对提出申请流通的新代币评价其内存块链资产在平台使用者中的使用情况并充分考虑其安全性后进行判断是否准入。



图：NUBC 平台的优势

2.4 应用场景

2.4.1 游戏数字代币结算平台

是以 NUBC 币为结算币，可直接充值于各个游戏来进行结算，成为各游戏使用的统一代币。使用 NUBC 的目的在于服务于手游行业的中小发行商、渠道商和开发商，同时辐射到游戏用户，提供全新的数字代币进行交易结算，打通各个角色之间的壁垒。

1) 通用账号 — 各使用 NUBC 代币的玩家，可在使用时自动获得平台唯一身份，成为平台用户，享受各种服务，且无需再各个游戏间重复注册，采用平台账号，即可一键登录，直接进入各游戏，方便快捷。

2) 实时收益 — 在各游戏中增加 NUBC 币结算接口，采用 NUBC 数字代币进行结算，游戏收益各方均可在结算平台中以代币形式直接获取游戏收益分成，避免原有 N+数月的回款周期，平台可以做到 N+1 甚至更快，获得快速的现金流支持。结算时可选择兑换成 NUBC 代币期待升值。并可实时核算分成数据。

3) 新的分发平台 — 汇集中小型渠道方，以 NUBC 币支付方式结算，方便促销、账期控制，将成为各游戏的一个重要分发平台。

4) 推广、用户聚集 — 针对发行商来说，可充分利用共享社区的用户群体进行促销、市场、玩家推广、分发平台、主播联盟、用户分享等众多模式对游戏进行推广。

5) 开创游戏共享新模式 — 游戏共享模式，玩家可使用“一键分享”模式将该游戏直接分享给其他玩家，并获得分享奖励。各个游戏中均有 NUBC 币 SDK 接口，玩家一经使用，自动成为平台会员，对游戏的分享打下良好的基础。同时平台也会根据用户的推广数量，设置阶梯返还机制。这样用户在游戏内会首选 NUBC 作为结算方式，也会形成在用户间互相传播的效益。

随着加入数字代币结算体系的游戏、发行商、渠道商和用户越来越多，数字代币可应用到各个游戏中，打破了游戏之间、发行之间和渠道之间的壁垒。通过运营，用户的不断激增也将带来更多的收益，最后形成一个游戏共享、交流的大社区。

2.4.2 游戏众筹

在社区内，专门设立游戏众筹平台。众多的中小型游戏开发商、发行商可通过平台的协助以 NUBC 进行众筹。玩家可参与众筹，提前参与到游戏开发中来，更早的体验游戏并可获得游戏代币。众筹游戏将必须接入 NUBC 代币结算方式。中小开发商通过该方式不仅可以获得更宽松的研发环境，并且可以实时的和用户进行互动，做出真正符合用户需求的游戏产品。

对于平台而言，通过这种方式可极快速的扩展含有数字代币结算技术的产品，以便后续更快的进行结算方式的改变。

2.4.3 游戏分发平台

汇集众多中小型渠道形成一个新的游戏分发平台。以 NUBC 结算方式进行结算，前期以赠

送加补贴的方式获取众多渠道平台的支持，快速的让渠道商去推广数字代币的结算方式，让更多的产品、用户使用数字代币，扩大应用范围。NUBC 作为平台之间的通用代币，而 NUBC 的帐户系统则作为所有游戏的通用帐号，贯穿整个平台。

随着玩家对于 NUBC 和帐户系统使用的倚重，会有越来越多的渠道加入联盟，成为社区游戏发行的一个重要分发平台。

2.4.4 IP 共创计划

透过 IP 共创平台，建立 IP 创造者与使用者的桥梁。平台将与众多拥有 IP 的企业和团队合作，包括影视作品、小说、漫画等各类 IP，向游戏发行公司、研发公司提供 IP 合作，以达到游戏的 IP 增值。IP 共创平台将向双方提供磋商机制，设定该 IP 的游戏增值价值，并采用区块链技术的协议方式对该价值进行约定，约定可采用虚拟币直接分批有条件结算，或按游戏收益进行分成。

NUBC 共享社区已经与国内某知名版权方达成战略合作，将拿出数百个 IP，向众多游戏厂商和发行者提供 IP 合作。IP 共创的模式，不但可以在游戏的开发上，同时也在游戏的衍生品的打造上。如在开发 IP 时需要支持，社区可提供众筹的支援。

2.4.5 影游互动

电影和游戏已经成为了当下最热门的两种娱乐形态，彼此间的跨界合作展现出巨大的市场潜力。文化产业高度发达的欧美国家不乏影游成功联动的案例。涵盖电影、游戏、动漫等诸多商业模式的 IP 逐渐成为成为互联网时代文化产业的核心因素，中国网络游戏的千亿市值与电影产业三百亿规模的联合将带动周边产业在未来爆发增长至万亿规模。

NUBC 共享社区会采用影游同时上线的方式，使电视剧的画风和游戏的闯关相辅相成，而这种新式组合也改变了影视产业的布局模式。影视与游戏同步打造，虽然展示内容各有侧重，但对于粉丝而言，娱乐体验却可叠加，甚至升级。



图：NUBC 应用场景

2.5 NUBC 社区与用户的关系

NUBC 社区由开发商、运营商、渠道商、玩家和合作者共同组成。通过众筹平台和结算系统，贯穿整个社区，建立一个闭环的游戏娱乐共享社区。而 NUBC 作为社区中的权益代币，用作游戏众筹和 NUBC 权益分享。

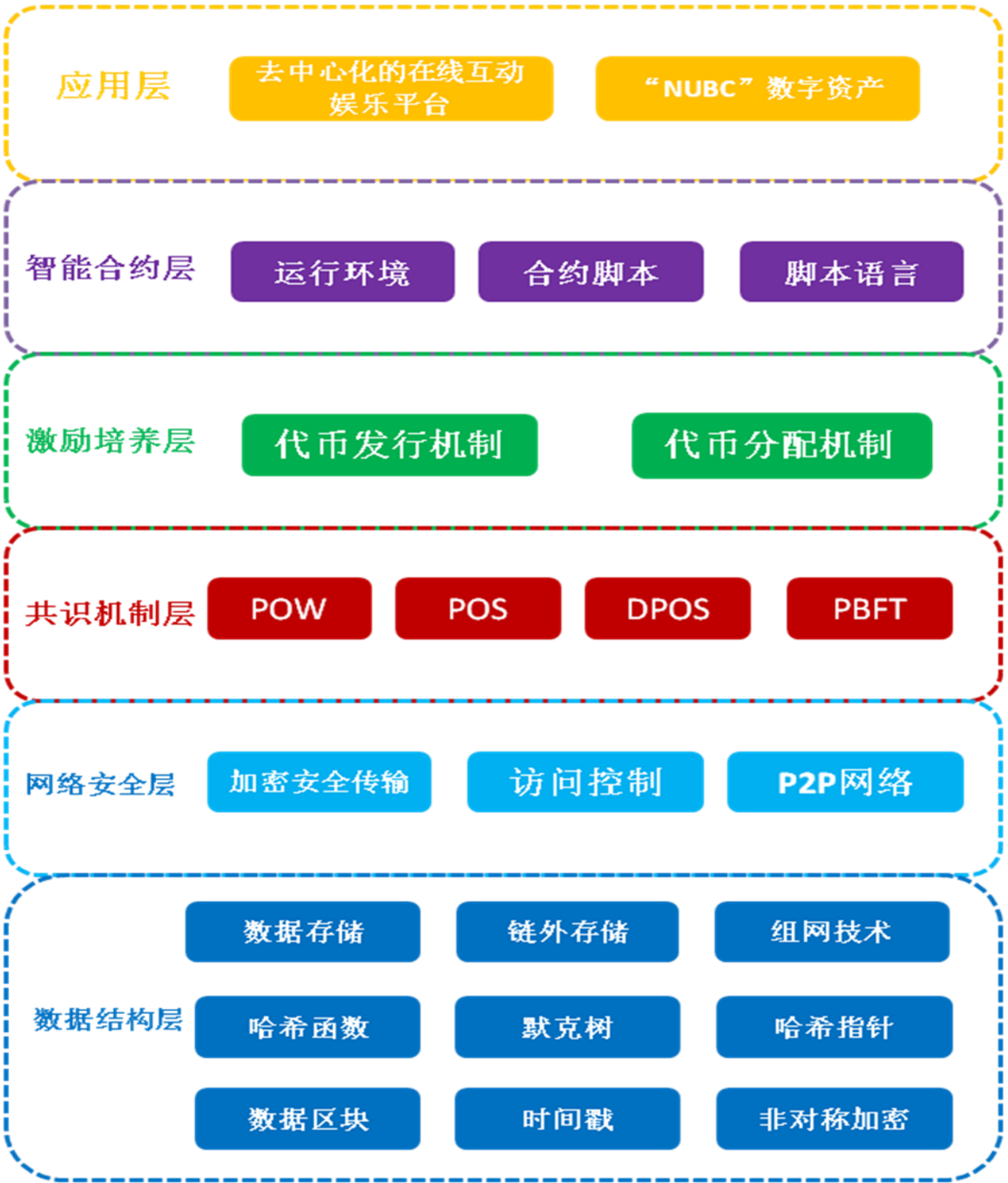
开发商可通过 NUBC 社区进行众筹，从而获得数字资产进行游戏开发，并和运营商、渠道商建立完全去信任化的分成机制。

而玩家在成为社区用户后，亦可以享受众多的服务：

拥有统一账号，可一键进入任何游戏、交易，无需多个账户；统一虚拟代币，并通用于多种关联服务，可直接在游戏、直播、衍生品中使用等。同时，玩家可以享受“分享游戏”的收益；用户在游戏中使用数字代币进行结算，除了获得等值的代币外，还可以获得额外的数字代币奖励，该奖励同样具备流通性和升值空间。

第三章、技术架构

3.1 平台框架



NUBC 设计的目的是基于脚本和链上原协议概念进行整合和提高，使得第三方服务商开发者、商家、使用者、用户能够创建任意的基于共识的、可扩展的、标准化的、特性完备的、易于开发的和协调的应用。

NUBC 通过使用以太坊底层技术，建立终极且抽象的基础层——内置有图灵完备编程语言的区块链，使得任何人都能够创建合约和去中心化应用，并在其中设立他们自由定义的所有权规则、交易方式和状态转换函数。在 NUBC 系统中，状态是由被称为“账户”（每个账户由一个 20 字节的地址）的

-----Number chain -----

对象和在两个账户之间转移价值和信息的状态转换组构成的。类似于以太坊，NUBC 中的账户包含四个部分：随机数，用于确定每笔交易只能被处理一次的计数器；账户余额；账户的合约代码（如果有的话）；账户的存储（默认为空）。

NUBC 将有两种类型的账户：外部所有的账户（由私钥控制的）和 合约账户（由合约代码控制）。外部所有的账户没有代码，人们可以通过创建和签名一笔交易从一个外部账户发送消息。每当合约账户收到一条消息，合约内部的代码就会被激活，允许它对内部存储进行读取和写入，以及发送其它消息或者创建合约。

NUBC 采用 P2P 分布式签名系统保障安全。P2P 网络具有自组织性，负载均衡性，容错性，低成本，高可用性等特性。由大量 peer 节点组成的 P2P 网络可以提供巨大的计算能力，同时成本很低。本项目的分布式安全 CA 方案将本来由高性能服务器完成的数字签名计算分散到 P2P 网络中，具体有以下特点：

- 1) 检查区块引用的上一个区块是否存在和有效。
- 2) 检查区块的时间戳是否比引用的上一个区块大，而且小于 15 分钟。
- 3) 检查区块序号、难度值、交易根，叔根和燃料限额（许多以太坊特有的底层概念）是否有效。
- 4) 检查区块的工作量证明是否有效。
- 5) 将 $S[0]$ 赋值为上一个区块的 CBCTE_ROOT。
- 6) 将 TX 赋值为区块的交易列表，一共有 n 笔交易。对于属于 $0 \cdots n-1$ 的 i ，进行状态转换 $S[i+1] = \text{APPLY}(S[i], \text{TX}[i])$ 。如果任何一个转换 发生错误，或者程序执行到此处所花费的燃料（gas）超过了 GASLIMIT， 返回错误。
- 7) 用 $S[n]$ 给 S_FINAL 赋值， 向矿工支付区块奖励。
- 8) 检查 S_FINAL 是否与 CBCTE_ROOT 相同。如果相同，区块是有效的。否则，区块是无效的。

3.2 区块链的功能说明

3.2.1 共识机制

共识机制是区块链技术的一个核心问题，它决定了区块链中区块的生成法则，保证了各节点的诚实性、账本的容错性和系统的稳健性。常用的共识机制主要有 PoW、PoS、DPoS、Paxos、PBFT 等。基于区块链技术的不同应用场景，以及各种共识机制的特性，主要可以从性能效率、资源消耗、容错性、监管水平等几个方面进行评价和比较。

共识机制功能组件具备以下功能：

- a) 支持多个节点参与共识和确认；

- b) 支持独立节点对区块链网络提交的相关信息有效性验证；
- c) 防止任何独立的共识节点未经其他共识节点确认而在区块链系统中进行信息记录或修改；
- d) 应具备一定的容错性，包括节点物理或网络故障的非恶意错误，以及节点遭受非法控制的恶意错误，以及节点产生不确定行为的不可控错误。

3.2.2 智能合约 (Smart Contract)

由尼克·萨博 (Nick Szabo) 于 1995 年提出，他给出的定义是：“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。”承诺定义了智能合约的本质和目的。数字的形式意味着合约以计算机可执行的代码的形式运行，只要参与者达成协议，智能合约建立的权利和义务，就由计算机或计算机网络执行。

基于区块链的智能合约不仅能发挥智能合约低成本高效率的优势，而且可以避免恶意行为对合约的正常执行的干扰。将智能合约以代码化的形式写入区块链中，利用区块链技术实现数据存储、读取及执行过程可追踪透明化且不可篡改。此外利用区块链的共识算法构造的状态机系统能使智能合约高效的运行。

智能合约的功能组件包括：

A 开发运行环境，包括：

- 1) 提供编程语言支持，必要时可提供配套的集成开发环境；
- 2) 支持合约内容静态和动态检查；
- 3) 提供运行载体支持，如虚拟机等；
- 4) 对于与区块链系统外部数据进行交互的智能合约，外部数据源的影响范围应仅限于智能合约范围内，不应影响区块链系统的整体运行。

B 存储环境，包括：

- 1) 防止对合约内容进行篡改；
- 2) 支持多方共识下的合约内容升级；
- 3) 支持向账本中写入合约内容。

3.2.3 加密安全技术

区块链中使用非对称加密的公钥对来构建节点间信任。非对称加密算法由对应的一对唯一的密钥（即公开密钥和私有密钥）组成，任何获悉用户公钥的人都可用用户的公钥对信息进行加密与用户实现安全信息交互。由于公钥与私钥之间存在依存关系，只有持有私钥的用户本身才能解密该信息，任何未经授权的用户甚至信息的发送者都无法将此信息解密。

加密功能组件具备以下功能：

- a) 支持国际主流加密算法，如 AES256 等对称加密算法和 RSA、ECC 等非对称加密算法；
- b) 支持我国商密算法，如 SM4、SM7 等对称加密算法和 SM2、SM9 等非对称加密算法；
- c) 应具备明确的密钥管理方案，确保区块链底层安全机制正常运行；

d) 加密算法应具备抵御破解的能力，宜定期审核加密算法的安全性，必要时采用更高破解计算复杂性的加密算法。

3.2.4 数据存储

区块数据结构在区块链中，数据以区块的方式永久储存。区块链的时间戳解决了区块的排序问题，新区块生成时便记录着上一个区块通过哈希计算得到的哈希值，实现了区块密码学链接。每一个区块记录了其创建期间发生的所有交易信息。在区块链中，如果待存储的是一些字符串、Json 对象，可以使用扩展账本结构链存储；如果是图片、视频等较大的多媒体文件，可以将文件的哈希值存储在链上，而原文件可使用云存储存储到云端。

数据存储功能组件包括以下功能：

- a) 支持持久化存储账本记录；
- b) 支持多节点拥有完整的数据记录；
- c) 支持向获得授权者提供真实的数据记录；
- d) 确保有相同账本记录的各节点的数据一致性。

3.2.5 链外存储

在该系统中有大量的文档、图片、视频数据，不适于存储在区块链上，但是为了保证数据的完整性，我们使用现金的 hash 加密算法，将大型文件输入哈希函数中，输出一个固定长度的哈希值，并将哈希值存储在区块链上，这样既保证了系统的运行速度，又保证了大型文件的安全性。

3.2.6 组网技术

组网技术是区块链的核心技术之一，在去中心化的组网架构中区块链才能实现不依赖中心网络的特性。区块链网络协议一般采用 P2P 协议，确保同一网络中的每台计算机彼此对等，各个节点共同提供网络服务，不存在任何“特殊”节点。不同的区块链系统会根据需要制定独自の P2P 网络协议，比如比特币有比特币网络协议，以太坊也有自己的网络协议。

3.3 技术特点

NUBC 技术总体特征是公开、透明、可验证，或者至少在一定范围的具有这些特征。而从效果上看，则是不可篡改与可追溯。项目应该会选擇开放程度较高的类似于公有链的架构，因为项目对各方隐私的要求高，反而对于流程透明性有极强的需求。

当然，项目以太坊 2.0 区块链技术，但从目前技术能力和全球在线娱乐市场的需求上来看，不排除项目中会搭建新的链和共识机制，就好如 NUBC 的共识机制。

这样做的优势在于既不会像当前比特币区块链那样依赖大量算力消耗能源的工作量证明，又能将数据公开程度及影响面设定在可控范围内。通过大数据能够对支付用户节点的行为作为有效判断的依据，而不至于像 The DAO 那样出错之后，却由于节点行为不可控而造成的解决方案难以统一的问题。当然，自有区块链在相关延展性也更适合项目根据自身发展需要量体裁衣。

3.4 技术说明

NUBC 技术团队都有多年的互联网和区块链开发经历，简单来说，相比于传统的跨国交易，NUBC 具有以下特点：

安全

NUBC 依赖加密验证交易，会验证涉及交易的各方身份。这确保如果没有涉及各方的同意，一个“错误的”交易不能被加到区块链上。每次要向区块链加入一笔新的交易就需要进行一次复杂的数学计算：哈希计算，这取决于交易数据、涉及交易的各方身份和之前交易的结果。现有区块链依赖先前的区块链这一特性确保了恶意参与者不能篡改交易历史记录。这是因为如果改变之前的交易数据，现有的哈希值将会受到影响，不能与账本的其它备份相匹配。

透明

NUBC 本质上是一种分布式的数据库，被多个节点维护和同步——比如，多个频繁互相交易的对手方。此外，交易数据必须在各方间保持一致，才有可能被加入区块链。这就是说从设计上多方能访问同样的数据（某些情况下机构内部的本地数据）——因此极大增加了交易的透明性，而传统系统依赖于多个躲在防火墙后面的“私藏”数据库，从外部是不可见的。

效率从概念上讲，维护区块链数据库的多份备份不会比一个单一、中心化的数据库更有效率。但现实世界中，多方已经在维护包含同样交易信息的数据库备份了。许多区块中，关于同一交易的数据互相矛盾——导致成本高昂、耗时冗长的对账程序。跨组织使用区块链这样的分布式数据库可以极大地减少人工对账需求，因此大量节约成本。此外，某些情况下，NUBC 可以让各个组织获得共同能力，免除重复劳动。

联盟链采取多个 VP 节点的模式，NVP 节点分担 VP 节点的工作压力，承担处理 API 请求和 events 的工作，VP 节点需要验证交易、运行代码、记录账簿、达成共识。

第四章、Number Chain 的生态圈

4.1 网络节点

支撑 NUBC 公链的网络节点，通过共享主机云服务获得服务交换；

各个企业客户的服务器主机资源或租用的云主机资源进行共享，实现分布式的分发；

企业客户的相关大数据内容会分布在上千台的共享主机上，自己的主机也会负责其他企业客户的内容，这些数据内容都通过加密，保障数据的安全性。

4.2 NUBC 的云平台

NUBC 核心的平台，为开发者提供便捷的开发环境和底层接口支持，包括手机 APP 查验端、微信小程序落地

子链管理系统：子链的生成，运维开发者信息及开发项目进度管理系统，商品唯一身份信息管理系统，消费者信息管理系统 企业信息管理系统

标签管理系统：条形码、二维码、三维码、RFID 移动营销公共平台接口组 移动电商公共平台接口组

手机查验 APP 接口组 微信小程序二次开发中间件

4.3 DAPP 的开发者

DAPP 开发者是过去曾从事商业服务管理开发或有志于拓展区块链上商业生态开发和技术的企业或个人，通过 NUBC，开发者可以很便捷的进行商业个性化定制应用的区块链化，使用最新的技术服务品牌企业，抢占市场的先机。

汇集商业 NUBC 的应用开发企业和个人，建立 NUBC 学院和开发者俱乐部，全球巡回的培训和路演。

4.4 Number Chain 的生态联盟

NUBC 生态联盟的成立，希望可以实现两方面的作用：

首先，利用区块链技术和物联网技术，打通 NUBC、商户、监督机构间的用户与商户的交易信息，了解用户享受服务，到奖励来源、最终用途都有明细的记录，公开透明，不可篡改，同时连接微信、支付宝、贝宝等支付平台，还有微信小程序等等平台，极大提升用户的体验度和真实感以及信任感。

其次，NUBC 联合政府、优质商户，打造 NUBC 生态联盟，积极符合各国家标准的制定。借助区块链技术，可以确保信息的绝对安全，为 NUBC 全流程信息管理提供有力的安全保障。通俗的讲，通过搭建区块链联盟网络，构建一个公平、公正的娱乐环境，同时能够盈利的平台，实现开发商、运营商与用户共赢的局面。

第五章、Number Chain 发展历程与规划

2017.5 项目立项及团队组建，完成法人运营主体及团队

-----Number chain -----

- 2017.8 完成全球在线娱乐行业调研，大数据分析
- 2017.9 确定 NUBC 基础模型
- 2017.10 提出 Number Chain 平台概念
- 2017.11 顶级技术团队组建完成，并已完成区块链原理的底层架构及玩法第一部分的设计工作。
- 2017.12 Number Chain 白皮书准备
- 2018.2 官网上线
- 2018.3 准备众筹事宜
- 2018.8 上线 Number Chain 平台测试版
- 2018.9 完成服务器存储数据中心的升级和技术测试
- 2018.10 Number Chain 平台正式版正式推出

第六章、代币简介

6.1 NUBC 代币说明

数链，其英文名是 Number Chain，NUBC 是 Number Chain 的简称，也是去中心化 NUBC 的结算代币。

NUBC 是一种基于 NUBC 平台实现的结算代币，用于在全球在线娱乐 Number Chain 平台上娱乐、投资、交易所平台等的交易的结算。NUBC 在 NUBC 系统中为用户交易提供的交易媒介。

NUBC 是整个 NUBC 生态系统的母链唯一代币，任何跨子链的数据交互及资产交换都需要消耗母链代币，当生态系统形成后，跨链数据交互变成高频事件，此时各方面对 NUBC 的需求量不断提升。NUBC 代币持有者拥有 NUBC 母链发展方向的股权分配权。

6.2 NUBC 获取途径

1. 他人转赠获取，通过他人或者交易所交换获得 NUBC 代币。
2. 在应用场景中，通过在线互动娱乐等多种活动获得 NUBC 代币。
3. 融资获得，通过 ICO 或者购买原始币获得 NUBC 代币。

6.3 NUBC 发行方式

总计发行 10,000,000,000NUBC，NUBC 代币机制通过一个设置上限的首次代币发行，占所产生的代币总量的 20%NUBC，20%的代币将会用于公开 Pre-sale。

1ETH=8 万枚 NUBC。

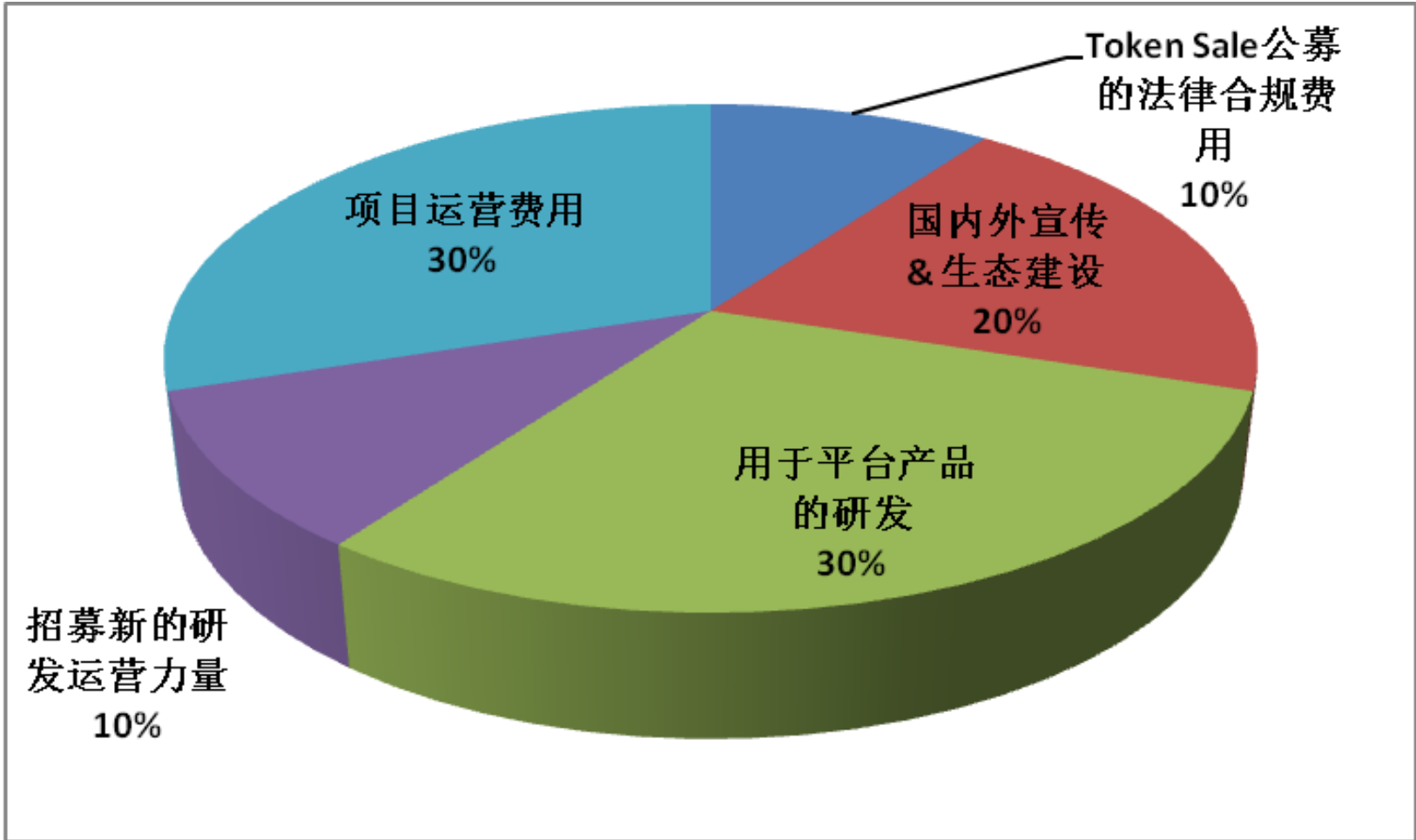
NUBC Token 公开 Pre-sale •

预计 20 亿枚

锁仓:上线前解锁 50%，其它 50%锁定 3 个月

个人最低购买限额：1ETH

6.4 募集资金使用说明



图：资金使用说明

- 10% Token Sale 公募的法律合规费用
- 20% 国内外宣传 & 生态建设
- 30% 用于平台产品的研发
- 10% 招募新的研发运营力量
- 30% 项目运营费用

6.5 分配方案

发行的代币将会如下分布：

- 20%通过公开售卖投入流通
- 10%通过私募投入流通
- 50%储备代币为基金会代持

主要用于建设平台生态系统，全部用于免费赠送给用户

- 10%为基金会所有

- 10%为基金会员工所有
- 基金会持有的 10%代币锁定 24 个月。
- 基金会员工持有 10%代币锁定 12 个月。

第七章、NUBC 基金会及组织架构

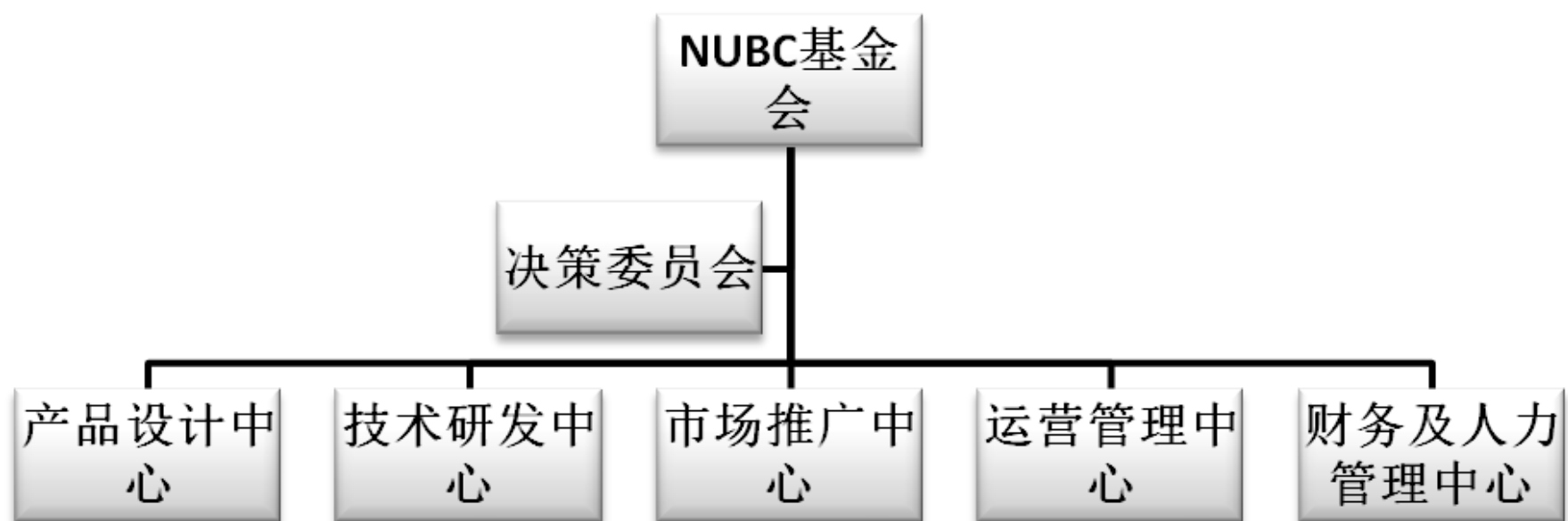
7.1 基金会

为了 Number Chain (NUBC) 的开发建设和治理透明机制、倡导和推进 Number Chain 的工作顺利进行和开展、促进开源生态社会的安全、和谐发展， Number Chain 在境外建立了 NUBC 基金会 (Number Chain Foundation) (以下简称“基金会”)。

基金会通过区块链数据结构，实现商户、用户、平台上交易的区块链化，实现用户、商户、合作伙伴、第三方、政府等相关方的共赢利益，保证项目管理的有效性、可持续性和安全性，推进 NUBC 区块链技术的发展推广，将 NUBC 区块链技术与更多场景结合，通过通用推广奖励、营销激励、电子商务、活跃奖励等一系列措施，实现 NUBC 币的生成、赠送、交易等功能，建立 NUBC 区块链的生态系统。

7.2 组织架构

为了在公开和透明的原则下，合理高效地利用基金会的资金和资源，为了推动 NUBC 的快速发展，为了更多结合了 NUBC 的行业、场景、应用的落地，基金会由产品人员、开发人员、市场人员、运营人员和职能部门组成，组织架构包含决策委员会、产品设计中心、技术研发中心、市场推广中心、运营管理中心、财务与人力管理中心，具体组织架构图如下：



图：NUBC 基金会构架图

决策委员会是 NUBC 的最高决策机构，承担最终决策职能，决策委员会委员无职位高低之分，负责对基金会战略规划、年度计划、预算等重大事项进行审议和审批，并代表基金会对 NUBC 的生态重大议题做出表决。首届决策委员会成员由 NUBC 创始团队及投资人选举产生。

决策委员会设立首席执行官，由决策委员会票选产生，对决策委员会负责。

首席执行官的具体工作职责：负责实施决策委员会的有关决议和规定，管理日常运营，完成其下达的各项指标，并定期将实施情况向决策委员会汇报。首席执行官组建产品设计、技术研发、市场推广、运营营销、财务人力等部门，负责溯源连的相关产品的建立、研发、运营、维护等事宜。

产品设计中心

产品设计中心分为产品部和设计部，产品人员负责探索 Number Chain 与相关行业、领域及场景应用结合的可能性，建立可持续性具体发展策略，进行市场调研，制定产品原型，掌握项目开发进度，保证方案落地与实施；设计人员进行 UI 设计及其他图像设计等工作。

技术研发中心

技术研发中心由 NUBC 的核心开发人员组成，负责底层技术开发、开放端口开发和审核、管理开源代码、修改源代码、相关及衍生产品的开发、测试、上线、审核及系统维护等工作。

产品人员和研发人员将持续关注行业动态，了解社区热点，在社区中与参与者进行交流，不定期举办技术交流会，了解技术发展趋势，促进双方共同发展。

市场推广中心

市场推广中心负责 NUBC 的技术推广，核心产品及衍生产品推广，拓展合作伙伴，提供服务，联系媒体合作，进行广告宣传，设计用户互动，调研、确定及签约新增推广渠道等工作，根据合作伙伴及用户的要求，定制宣传方案等。

运营管理中心

运营管理中心在产品人员及研发人员设计开发的产品基础上，为社区及项目服务，对 NUBC 项目及产品进行运营、宣传和推广。运营人员负责产品的运营，积极拓展用户，将 NUBC、终端用户、合作伙伴紧密地联系在一起，从而打造落地最快最广泛的 NUBC 商业区块链。

产品人员、研发人员、市场人员、运营人员等将紧密合作，根据实际情况，召集相关部门人员召开立项及项目追踪会议，沟通项目进展及需求，为合作伙伴及用户提供更好地服务。

财务及人力管理中心

负责处理基金会内的财务、人力、法务、行政管理等相关事宜，财务人员主要负责项目募集资金的运用和审核，日常运营费用支付及审核，成本控制，风险管控等；人力负责相关人员考勤及薪酬管理；法务负责拟定及审核各类文件，规避可能存在的各类法律风险；行政负责相关日常行政事宜。

第八章、团队与顾问

8.1 团队成员与顾问

(1) Jack Li

创始人兼首席执行官，

连续成功创业者，早期比特币投资人。负责 NUBC 的日常运作，拥有多伦多 ROTMAN 商学院 MBA，热衷于研究提高微观经济的市场效率。

(2) Qaunain Haeems

CTO

拥有九年技术解决方案的工作经验，曾任职百度，腾讯，奇虎 360，等一线互联网企业。在大数据，广告算法，BT 系统和 CTR 平台等有丰富的经验，具有亿级系统架构的开发能力，对高并发系统框架设计有丰富经验，在团队管理、战略规划和业务统筹方面都有丰富的实战经验，同时，在密码学方面也有着极深的造诣，也是比特币 Bitcoin 早期投资者。

(3) Beck Chu

资深区块链产品经理

加拿大麦吉尔大学计算机信息学硕士, 具有丰富的区块链产品研发及项目管理经验, 曾任华为区域项目总监, 负责中美洲 3 国（危地马拉、萨尔瓦多、洪都拉斯）的交付与服务业务。

(4) Alan Lee

资深区块链专家 伦敦大学学院区块链技术中心研究员

Alan 目前就职于伦敦大学学院区块链技术中心, 从事于加密数字货币交易和代币发行监管的研究。Alan 创办了中英区块链协会, 它致力于给中英两国间区块链领域研究铺路搭桥。他是伦敦大学学院的金融数学博士生, 专注于算法和高频交易。 他还曾在一些投资银行负责过量化投资和大数据项目, 其中包括瑞士信贷银行等。

(5) Sunny Wang

首席营销官

10 年营销领域经验。曾任盛大游戏高级营销总监, 高级媒体总监, 具有丰富的处理媒体工作经验。

(6) 张星沛

首席法律顾问

张律师是林张律师事务所的创始合伙人之一。他在英格兰获得法律学士学位, 在英格兰和威尔斯以及香港都获得律师资格。张律师在处理与商业法, 企业和商业交易以及 IPO, 私募股权投资, 兼并收购和融资等外商投资有关的法律事务方面有丰富的经验。

8.2 联系方式

Telegram: https://t.me/nubchain_cn

Email: nubchain@gmail.com

Twitter: <https://twitter.com/NubChain>

Website: <http://www.nubchain.io>

第九章、投资机构



第十章、法律事务与风险提示

10.1 法律事务

NUBC 项目会成立一家设立在海外的 BVI 公司，即 NUBC 基金会。该基金会将作为独立的法律主体，全权负责组织团队来开发、推广和运营 NUBC 项目，并承担所有相关责任。

NUBC 基金会将严格按照 BVI 所在地法律法规，以恰当方式面向特定人群进行互换，并给与数字货币 NUBC。出于有法律限制的国家公民或群体限制，数字货币 NUBC 将不在某些国家地区进行公开众筹或公开募集等行为。数字货币 NUBC 作为一种具有实际用途的虚拟商品和使用，不是证券，也不是投机性的投资工具。

NUBC 基金会在数字货币 NUBC 互换中所获的收入，将由 NUBC 基金会主要将用于技术开发、市场营销、社区建设、财务审计、商务合作等用途。

NUBC 平台依然很有可能会在全世界不同国家受到主管机构的质询和监管。为了满足和遵守当地的

法律法规 NUBC 平台可能会在有些区域无法提供正常的服务。

10.2 风险提示

本项目在售卖之前，不会在任何媒体组织任何公开的宣传及广告推介活动，平台团队也没有组织任何微信群，QQ 群，邮件列表进行推介，请大家参与前谨慎判别。

本文档只用于传达信息之用途，并不构成未来买卖原生数字资产的相关意见或投资意见，也不是任何形式上的合约或者承诺。

投资者一旦参与私募与售卖即表示了解并接受该项目风险，并愿意个人为此承担一切相应的结果或后果，平台明确表示不承担任何参与平台项目造成的直接或间接的损失。

本项目所涉及的原生数字资产是一个在平台上使用的加密数字编码，并不代表平台项目股权、债权、收益权或控制权。

同时 NUBC 基金会在此明确不予承认和拒绝承担下述责任：

- (1) 任何人在互换数字货币 NUBC 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；
- (2) 任何人在购买数字货币 NUBC 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使用或无法提取数字货币 NUBC；
- (3) 由于任何原因，数字货币 NUBC 的互换计划被放弃；
- (4) NUBC 的开发失败或被放弃，以及因此导致的无法交付或无法使用数字货币 NUBC；
- (5) NUBC 公有链开发的推迟或延期，以及因此导致的无法达成事先披露的日程；
- (6) NUBC 源代码的错误、瑕疵、缺陷或其他问题；
- (7) NUBC 的故障、崩溃、瘫痪、回滚或硬分叉；
- (8) NUBC 未能实现任何特定功能或不适合任何特定用途；
- (9) 对数字货币 NUBC 计划所募集的资金的使用；
- (10) 未能及时且完整的披露关于 NUBC 公有链开发的信息；
- (11) 任何参与者泄露、丢失或损毁了数字货币 NUBC 的钱包私钥；
- (12) 第三方分销平台的违约、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、解散或歇业；
- (13) 任何人与第三方分销平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；
- (14) 任何人对数字货币 NUBC 的交易或投机行为；
- (15) 数字货币 NUBC 在任何交易平台的上市、停牌或退市；
- (16) 数字货币 NUBC 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制；
- (17) 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、

-----Number chain -----

损失、 索赔、 责任、 惩罚、 成本或其他负面影响。