GEEKCHAIN

White paper

基于区块链共享人力协作网络
解决商业技术链上服务

工作草案，2018 年 5 月，修订版 V1.1

官网 http://www.geekchain.org

目录

摘要 Abstract 4

1 Geekchain 的背景及意义 5

1.1 信息网络的发展历程 5
1.2 区块链是价值所趋 6
1.3 仍需解决的问题 7
1.4 为什么需要 Geekchain 7

2 Geekchain 的设计理念 8

2.1 稳定性 8
2.2 安全性 8
2.3 可扩展性 9
2.4 易用性 9

3 Geekchain 的产品方案 9

3.1 极客创作者版权库的保障 10
3.2 分布式节点共享协助平台 11
3.3 Geek 多方撮合众包平台 11
3.4 发展区块链极客爱好者自治社群 11

4 产品结构和流程 12

4.1 业务流程 12
4.2 撮合交易流程 13
4.3 版权、授权追踪 14
4.4 社群建设 14
4.5 博弈测价策略 15
4.6 价值稳定感知策略 15
4.7 反盗版反盗用机制 15

5 技术与实现 16

5.1 合约和 GVM 的实现 16
5.2 共识机制 18
5.3 账户模型 19
5.4 分叉网络 20
5.5 价值互换协议（Value Exchange Protocol） 21
5.6 事件驱动 23

6 发行计划与用途 23

7 核心团队 24

7.1 成员介绍 25

7.2 极客世界介绍 28
8 发展路线图 28
8.1 Geekchain 阶段性规划安排 28
9 风险说明和免责声明 29
9.1 政策风险 29
9.2 技术风险 29
9.4 统筹风险 30
9.5 竞争风险 30
9.6 交易风险 30
9.7 黑客风险 30
9.8 未保险损失风险 31
9.9 免责声明 31
参考文献： 31

摘要 Abstract

Geek Blockchain 极客链（以下简称 GeekChain 或 Geek）致力于打造一个无边界的区块链世界。区块链自 21 世纪初期发展起来，是目前全世界认为最有潜力、最具想象力的一种技术革新。在人类的发展史上共经历过三次工业革命，第一次以蒸汽机的发明为标志，让机器代替了手工劳动；第二次以电能的突破、应用和内燃机的发明为标志，直接推动人类进入电气化时代；第三次以电子计算机、核能、空间技术、生物工程的发明和应用为标志，不仅推动人类社会的巨大变革，更深刻地影响了人类的生活和思维方式。每一次工业革命都带来生产力的巨大提升，而作为生产要素之一的生产关系，改变并没有那么巨大，依旧是自上而下、金字塔层级的中心化组织。组织的业务越复杂，层级越多，效率提升就越困难。区块链是去中心化、去信任化的网络，可以实现点对点价值交换，被人们称之为价值互联网。Geek 认为区块链技术最有可能改进当前的生产关系。在 Geek 的帮助下，我们可以创造这样一个世界一个人和人直接相连，去信任化的，在社区或者社会共识下，相互协作、点对点相互交换、价值驱动的世界。GEEK 是一个旨在通过区块链去中心化、分布式账本链接全球极客来重构商业服务。链上多方的协作、DIY 的开放共享平台提供发烧级协作共享应用，通过 Geektoken 的价值传递创造激励体制的分布式网络和庞大的 Geek 社区。通俗的说，GEEK 是一个基于区块链由民间极客共同协作的网络生态体系，也称商业技术孵化器。服务商业，以人为本，共享价值。

Geek 将分三阶段来实现上述目标。首先，我们利用模块化的设计方法构建安全稳定的区块链网络，这一阶段即可实现智能合约及数字资产，同时我们将引入智能魔盒——一个可以智能化测试和监测合约运行的环境，魔盒可确保即将正式运行在链上的合约足够安全，避免类似 DAO 事件的发生。接下来，我们利用区块链分叉来满足不同的商业诉求，如保险、电子文档、数字货币、溯源追踪、用户信用记录等。这一阶段将实现一个不断进化、容易使

用、低成本的、适度定制化的区块链网络。最后，通过价值互换协议将已经分叉的、仍然活跃的网络连接在一起，甚至与其他网络（可能是非区块链的）打通数据交互，构建出一个相互连接、多维度数据关联的网络世界。利用多维度数据，如个人资产、信用、生产和消费数据，可以更好地将社区共识、个体行为、价值交换有机地整合在一起。Token 承载生态中的价值，Geek Blockchain 将它命名为 Geek，持有 Geek 将获得合约发布、网络分叉等区块链基础服务。为构建上述生态，GeekChain 在设计上把安全性、稳定性、可扩展性放在首位。GeekChain 作为一个公有链，我们选取了更实用、占用资源更少的委托权益证明（Delegated Proof ofStake，以下简称 DPOS）共识机制，并在其基础上创新出基于结果的委托权益证明（Result-Delegated Proof of Stake，以下简称 RDPOS）共识机制，在同样安全的情况下，RDPOS 更有利于提升整个网络的合约性能，结合对网络其他参数的整体优化，理论上的交易处理速度可达到甚至超过 1000TPS（transGeekion per second）。

我们以为大智若愚而富有科学精神的极客文化打造区块链协作时代，构建于互联网之上，经历上网，协作，去网，重生将超越云时代成为真正去中心化大数据集散中心，由 GEEK 成员协作共治探索并创造全面释放民间 GEEK Power。形成开放共享的新型极客社区，提供商业支持服务，共享技术创新、应用创新的价值激励网络，引领时代发展，加速构建明日世界。

1 Geekchain 的背景及意义

1.1 信息网络的发展历程

1969 年 10 月 29 日，阿帕网加州大学洛杉矶分校（UCLA）第一节点与斯坦福研究

院（SRI）第二节点连通，标志着人类开启了互联网时代。以互联网为代表的信息技术，在其蓬勃发展的近 50 年时间里，不仅主导了第三次工业革命，更成就了如 Amazon、

Google、Facebook、Alibaba 等伟大的互联网企业，让人们又一次看到技术改变世界的力量。

Geek 的原意本是指代一群行为反常、怪异的人一样，当极客这一群体最初出现时，他们很难被当时社会的主流所接受。随着计算机文化的兴起，黑客一度被媒体妖魔化为破坏脆弱的计算机系统的洪水猛兽。只有深入了解当前的技术，极客们才能够构建下一代技术，知识产权的拥有者也许会说这些他们自己就能做到，但是纵观计算机工业的历史，推动变革的新技术往往是由那些不安分的外部人员所开发的。伴随着电脑和互联网技术的发展，呈现出与科技高度结合的特征，这些 Geek 一般是受过教育的、知识丰富的小群体。因为这种技术 Geek 的风行，在上个世纪的最后二、三十年中，许多与电脑和互联网相关的技术或商业传奇都刻下了 Geek 的烙印，比如微软的 Bill Gates、比如 Linux 之父 Linus Torvalds 等等。

2008 年 10 月 31 日，发烧级极客中本聪发布了比特币白皮书——《一种点对点的电子现金系统》，宣告了价值传输网络的到来。比特币有许多值得称赞的设计，如：防篡改，数据备份，参与者相对匿名，无其他信任方等。但其本身的交易性能和工作量证明（Proof ofWork，简称 POW）共识机制也逐渐暴露出问题。区块链技术从比特币衍生而来，近些年，人们主要围绕区块链的交易性能、共识算法、安全匿名进行创新，如：石墨烯、闪电网络对交易性能的提升；权益证明（Proof of Stake，简称 POS）、委托权益证明（DPOS）、实用拜占庭容错（PrGeekical Byzantine Fault Tolerance，简称 PBFT）对共识算法的丰富和改进；零知识证明（Zero-knowledge Proof，简称 ZKP）、混币提升交易安全等。

1.2 区块链是价值所趋

为什么会出现区块链，我们真的需要吗？GeekChain 作为区块链早期的参与者和见证者，认为这一创新不可逆转更不会昙花一现，原因有两个。其一，人们需要真实、有价值的信息、够降低信任成本。计算机和互联网让信息分享更加便宜、更加便捷，利用信息透明，优化价值链，提升协作效率。但是，无法杜绝的虚假信息、违约行为也让人头疼不已，基于互联网的传播和复制也极为容易，人们为信任所投入的成本已经越来越大，必然阻碍效率的进一步提升。其二，人们需要一个将共识、行为和价值激励相互连接的生产关系网。相比工业革命带来生产力巨大飞跃，生产关系的改变就不那么巨大。人类的生产活动以组织为中心

开展，依旧是自上而下、金字塔层级的中心化结构。组织业务越复杂，层级越多，要实现客观公正的利益分配就越难，因此，效率提升也就难上加难。区块链将分布式存储、加密技术、P2P 网络等技术融为一体，有去中心化、去信任化的技术优势，被人们称之为价值互联网。区块链最有可能解决人与人之间的信任问题，并缔造出新的生产关系网络——点对点价值交换。

1.3 仍需解决的问题

比特币自 2008 年诞生以来，以此为原型衍生出区块链技术，无数技术爱好者参与贡至献，发展方向百花齐放。有专注于去中心化平台的以太坊（Ethereum）、发展数字货币为主的比特币（Bitcoin）、莱特币（Lite Coin），以信息存档为方向的公证通（FGeekom），为保护用户隐私目的的 Zcash 和 Dash，专注于去中心交易所的比特股（Bitshare），甚是 R3CEV 力推的分布式账本平台 Corda。尽管行业发展生机勃勃，但区块链无论从技术创新还是商业应用，还面临很多挑战。

（1） 智能合约仍存在安全隐患，黑客可利用漏洞盗取用户的数字资产；

（2） 以不同应用目标而建立的区块链平台，彼此之间存在兼容性问题。尽管人们已经发现并尝试特定链之间的信息交互，但这种局部的解决方案还不足以支撑整个区块链生态发展；

（3） 区块链缺少和现实物理世界的交互，让许多应用创新不得不流于形式，如商品溯源；

（4） 目前，区块链应用仍有较高的技术门槛，导致大规模商用的成本太高；

（5） 存在性能瓶颈，目前分布式系统的性能还难以赶超中心式系统，或者说，分布式系统还难以实现大规模商用。

1.4 为什么需要 GeekChain

GeekChain 在设计上把安全性、稳定性、可扩展性放在第一位。通过引入模块化的虚拟机、智能魔盒、价值交换和分叉机制，从而创造出一个不断进化、容易使用、低成本的、适度定制化的区块链网络。此外，GeekChain 通过对出块间隔、区块容量、共识算法的优化，理论上可达到 1000TPS 的可用性能。GeekChain 相信，通过技术创新将能够解决人与人之间的信任、也能缔造一个新的生产关系网络，更好地将社区共识、个体行为、价值交换有机地融为一体。发挥极客价值与创意。

2 Geekchain 的设计理念

2.1 稳定性

稳定性是确保 GeekChain 可用的必要条件。区块链自带去中心化特征，去中心化网络通常较复杂并充满不确定性。因此，我们借助模块化设计工具对区块链进行抽象和简化，通过单独构建模块化虚拟机——Geek-Geek-Lua Virtual Machine（以下简称 GVM）运行智能合约，这样的设计可带来两个好处。一是优化 GVM 性能直接提升合约执行效率，减少系统耦合带来的干扰因素；二是弱化区块链网络与智能合约运行状态的相关性，即便合约执行出现问题，或虚拟机运行异常，区块链网络的稳定性依然能够保证。

2.2 安全性

PoW 曾对比特币网络的安全贡献功不可没，但由于日益增长的挖矿需求和算力难度提升，几乎所有权利都集中到矿工和矿池手中。通过专业合作，他们事实上已经成了高度中心化的“中央服务器”。如果联合超过 51%的算力，理论上就能够控制大多数比特币交易，如我们熟知的 DOS（Denial of Service）攻击。此外，高昂的电力消耗也同样让人诟病。相对于 PoW 模式来说，PoS 模式仍在发展，这些发展方向主要立足于安全和应用。PoS 模式比 PoW 模式在安全上有很大优势，但前提是吸引到足够的持有者来进行 PoS 挖矿，

才能充分的发挥出安全的优势。DPoS 是 PoS 的改进，而 GeekChain 创新出更具商业普适意义的 RDPoS 共识机制。与 DPoS 同等安全的情况下，理论上可提高出块响应，增加网络的稳定和安全。除此之外，GeekChain 创新性地提出智能魔盒机制。任何人发布的合约，首先要在智能魔盒中试运行，GeekChain 会对其进行全路径自动化测试，并持续监控其运行状态，若健康程度恶化，或发现漏洞。网络自行判断将其终止，避免问题合约对区块链生态造成破坏。

2.3 可扩展性

可扩展性的提出，为了解决区块链彼此不兼容的信息孤岛问题。首先，我们认为升级、分叉是网络进化的有效途径之一，分叉后形成一个主链和若干子链。主链和子链从技术角度看完全对等，只是基于社区共识给它们设置不同的标识。每一条子链可根据不同的商业应用做适度化定制，通过在子链之间构建 VEP，其工作方式类似于网关，子链之间通过 VEP 可交互信息和交换价值。通过这样的协作可形成多应用的区块链生态。不仅如此，非区块链的线上数据也将纳入 GeekChain 生态，辅以智能合约，可对现实世界中的事件做出响应。

2.4 易用性

GeekChain 通过两方面来实现易用性。一是提供区块链即服务平台（Blockchain as a Service，简称 BaaS）来降低企业及个人的使用门槛。通过网络分叉、数据定制、智能合约

发布和升级、资产交易监控等并辅以可视化功能，让区块链应用变得简单易用。二是 GeekChain 提供多种语言支持，从 Lua、C++到 Java，让不同平台的开发者都可以便捷地开发。

3 Geekchain 的产品方案

3.1 极客创作者版权库的保障

Wikipedia（维基百科）堪称一部网络时代的超级知识宝典，它对 Geek 的定义已经逐渐从早期痴迷技术发展到痴迷于与技术、想象力、创造力相关的一切活动，这也许和它的创始人也自称为 Geek 有关。Geek 不再特指某种技术天才或技术鬼才，他们不再自我封闭、游离于主流人群之外，而是用技术手段、创新能力和源源不断的想象力不断地将更新更好的生活方式、娱乐方式推向高潮、推向顶点。

网络极客这一大群体里，在今日的互联网环境提供了大量有助于社会发展和推动生产力发展的碎片化技术价值、理念价值。我们基于保障极客的创作并给予广泛的激励。更好的延续这文化打造价值互联、互信、传递、激励的网络平台。搭建创作者版权库价值激励的同时保障创作权。

互联网之上的作品由于数字化的特征，在计算机和互联网之间可以方便的传输，也造成了作品极易被人下载、拷贝，从而造成了无意识的侵权，互联网发展的越来越好，数字内容也将越来越多，技术文献、有价值的笔记作品、图文音视频、应用程序等逐渐成为了主流。知识经济的兴起使得知识产权成为市场竞争的核心要素。但当下互联网生态里 知识产权侵权现象严重，数字资产的版权保护成为了行业痛点。区块链去中介化、共识机制、不可篡改的特点，利用区块链技术，能将数字内容产业的各个环节进行有效整合、加速流通，缩短价值创造周期；同时，可实现数字内容的价值转移，并保证转移过程的可信、可审计和透明，有效预防盗版等行为。我们将搭建一个面向所有人开放的全球极客版权库，通过区块链来搭建版权库，收录创作者的作品信息，准确记录创作者的创作历史，利用区块链技术进行版权交易追溯，保障作品交易有据可查，有法可依。对极客创作者来说，是保护他们的创作热情和作品收益；对商家来说，是为他们购买合法作品提供的保证，不再被无版权的人诓骗。产品提供的功能包括作品登记，版权查询，交易查询，授权查询等。

3.2 分布式节点共享协助平台

传统的节点文件共享环境具有针对性强,限制多,传输不稳定,使用不方便等限制。通信技术的发展、节点的普及,对移动计算的文件共享环境提出了新的挑战。我们以分布式账本为基础构建了节点共享协作的公链网络 ,针对移动网络资源分散的特点和智能设备文件共享数据互操作的需求,提出了基于智能代理的对等分布式文件共享平台—JFS/M(JTang Filesystem for MobileComputing),通过智能代理屏蔽智能设备不同的计算能力,将其纳入 P2P 对等网络文件共享流程之下;通过对等架构将众多处于网络边缘的资源文件纳入分布式文件共享体系,并利用其容错,高可靠性的特点提供稳定的负载均衡服务。

公链集合了文件系统、数据互操作的网络环境以实现用户的共享协作。通过网络算力实现加密存储、可溯源，私钥保障创作权利，基于同网络公链的公钥传输协作操做等技术的实现。不论是技术极客还是内容极客都能顺利的出入公链网络共享文件信息进行可信、可靠的协作操作。

3.3 Geek 多方撮合众包平台

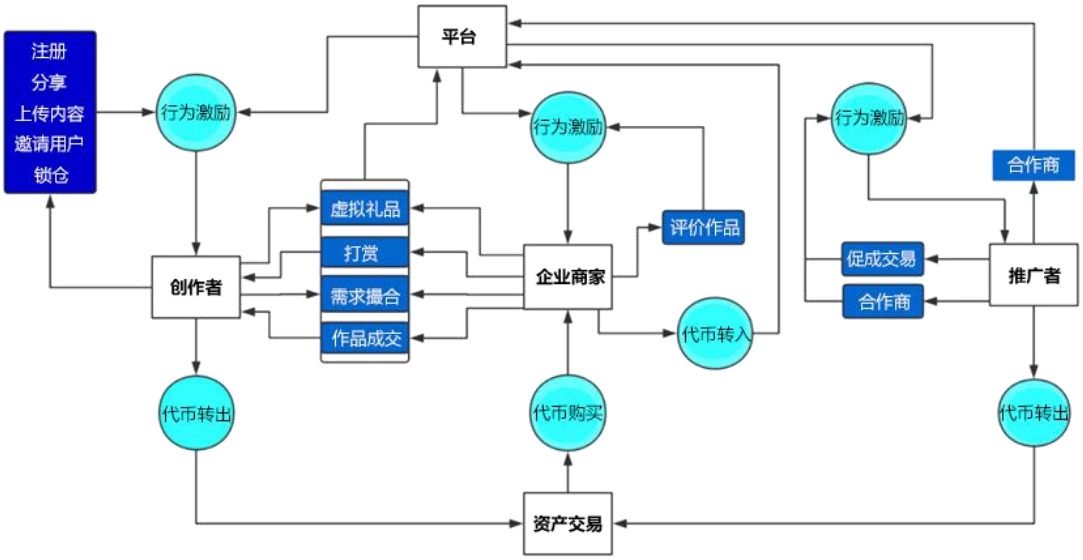
为什么要做这个？商业机构有技术与创意的需求 ,市场需要个性化、欣赏性的优质材料；创作者因为没有这些市场信息，缺少产生；众多企业客户，包括技术公司、传统商业个体、私人甚至创业者们等需要大量的定制化、个性化的技术亮点、创意 Idear，这些价值内容需要创作者来产生。为了满足市场对人才、创意、技术等软硬性需求，商家可以提出自己的需求，创作者可以提交自己的作品集，两者进行匹配，我们提供这种撮合交易平台，促进价值版权的形成与流转产生效益，从而更好的繁荣商业市场发展。

3.4 发展区块链极客爱好者自治社群

区块链技术的发展离不开社群的支持，从区块链诞生的那一刻起，就与社群发展模式相伴而生。平台会内化社群自治机制，通过代币的流通和成员的贡献，共同发展 Geek 社群并且从中获益。应用区块链技术建立社区虚拟币产生与流通机制，创作者可通过上传作品、点赞、评论、回复等行为的发生自动赚取 GeekChain Token，并可利用 GeekChain Token 购买社区产品与服务，从而激发社区成员的参与度，形成以 GeekChain Token 作为核心激励机制与衡量社区贡献度重要指标的自治社群组织模式。生态平台设置有激励池，用于激励社群的互动。不同角色有不同的激励获取和消费途径。互联网的价值取向是一个动态变化的过程，最早是生产者输出什么，用户就消费什么。随着全民互联网时代的到 来，用户参与感价值的增强，用户的角色已经从价值的被动消费者变成了共同创建者。创作者和商家之间的互动交流、联动激励，会演变出更加富有价值的优质内容的诞生，形成良性的互动循环。通过代币激励可以鼓励用户对违规内容和违规行为进行监督，社群人人都可以监督举报得到代币奖励，从而净化平台内容，共同维护平台的健康发展。

4 产品结构和流程

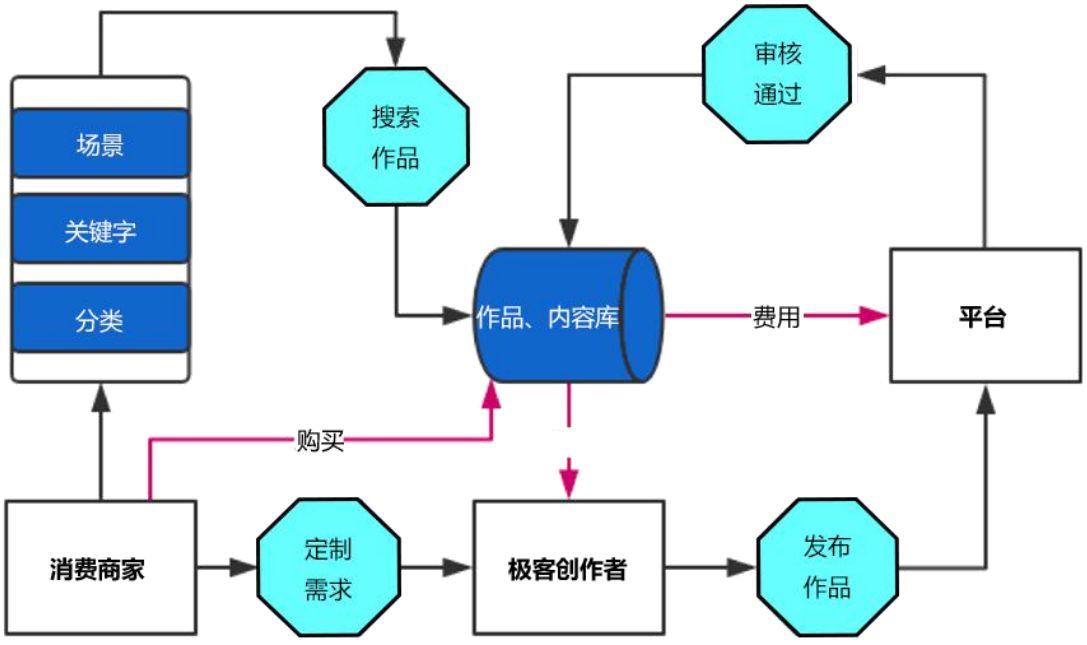
4.1 业务流程



GEEK流通生态图

本系统中的应用生态存在 5 种角色，系统内角色：平台、创作者、消费者、推广者，外部流转角色：资产交易。通过他们之间的资产流通，实现了 Geek 生态系统里的资产流通。

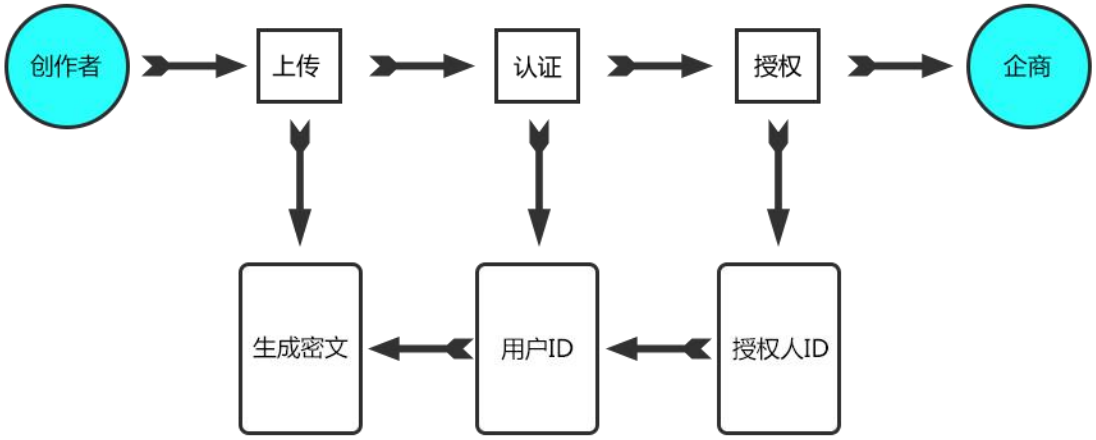
4.2 撮合交易流程



撮合交易流程图

平台连接创作者和商家，创作者提供图片资源，商家提供需求，商家支付费用给创作者和平台，各取所需，完成交易，交易会被记录在区块链系统中，开放查询。

4.3 版权、授权追踪



版权授权流程图

作品登记： 作品登记：创作者上传作品后会生成唯一指纹 hash，作品经过公示期获得认证后将与创作者 ID 一起记录在区块链上。作品授权：在交易平台可以进行作品授权给商家，供商家在不同场景下使用，商家 ID 与作品指纹 hash 一同记录在区块链上。授权查询： 授权查询：输入作品指纹 hash 可以查询到所有的授权商家和授权场景，可以依此判断商家是否合法使用作品。

4.4 社群建设

本着区块链社群“人人为我，我为人人”的精神，规范化运作区块链自治社群，鼓励有贡献的人持续进行社群维护，制定以下激励条款：

1、促进交易奖励：通过推广人的产品链接达成的交易，推广人可以获得交易额的 5%作为奖励。

2、用户增长奖励：通过推广人的邀请链接吸引新用户成功注册，推广人可以瓜分当天的邀请奖励。

3、内容贡献奖励：创作者的内容的赞越多，奖励越多，会按照分级奖励。

4、活动参与奖励：平台会定期举办数字艺术活动，参与活动的自愿服务者将得到活动预算的奖励。

4.5 博弈测价策略

为创作者提供测试定价的功能，创作者可以通过奖励 GeekChain Token 来为他的作品定价，比如他有一副精美卡通图案，目前作者定价 100 元，平台会提供三种选项给定价参与人：价格过高，价格合适，价格过低。参与人需要采取押注的形式进行投票，票数最高的选项将会成为“大众的选择”，其余选项的投票人的抵押和创作者的奖励一起被“大众的选择”的投票人平均分配。这个公式可以表达为

f(x) = max(low,fit,high)

f(x)是大众认为的定价，x 是输入作品，low 代表定价低了，high 代表定价高了，

fit 代表价格合适。这种策略只为创作者的定价提供参考，并不具有强制性。

4.6 价值稳定感知策略

为了防范代币波动给创作收入带来不利影响，平台提供了稳定价值的结算服务，用户可以按照法币作为定价依据，购买方在交易过程中需要支付相同价值的代币，由平台来提供稳定担保，可以直接在交易所兑换为法币，也可以持有代币。

4.7 反盗版反盗用机制

创作者在发表作品前，需同意平台的保证原创条款，假如违反该条款将需要退回非法所得，且失信行为永久记录，并且额外支出 1 万 GeekChain Token 违约金。作品发表后，

将会进入公示期，任何社群成员都可以监督举报违规作品，举报需要标明引用原作地址，为了防止滥用举报机制，举报行为将会消耗 GeekChain Token，超过 30 人举报，将会启动审查机制，如果确定为盗用作品，被列为失信人员记录在区块链上，举报人将会获得返还 GeekChain Token，同时平台启动侵权追诉，所有举报者将会平分违约金。

5 技术与实现

5.1 合约和 GVM 的实现

传统智能合约，仅限链上数据的输入和输出，这样只能支持一些简单的应用场景。正因如此，GeekChain 重新定义了智能合约，除链上数据外，还允许链上和链下的数据进行交互，并支持对链上、链下数据状态的变化做出事件响应。现实世界中的商业应用大多非常复杂，这种复杂体现在数据结构和逻辑规则上。为了实现上述目标，GeekChain 在顶层设计上做了两方面准备。一是将潜在的应用抽象，提取通用需求，提前设计好 API 接口和数据结构。二是选取一种图灵完备语言，尽可能去逼近真实物理世界中的规则。Lua 是一种图灵完备的编程语言，编译器和字节码虚拟机为在区块链中做了针对性设计和优化。因此，GeekChain 使用 Lua 作为 GeekChain 区块链上智能合约编程的首选语言，它支持静态编译成字节码并在区块链网络中按需执行。合约在区块链网络中的生命周期可分为五个阶段。

（1） 创建 Lua 源码；

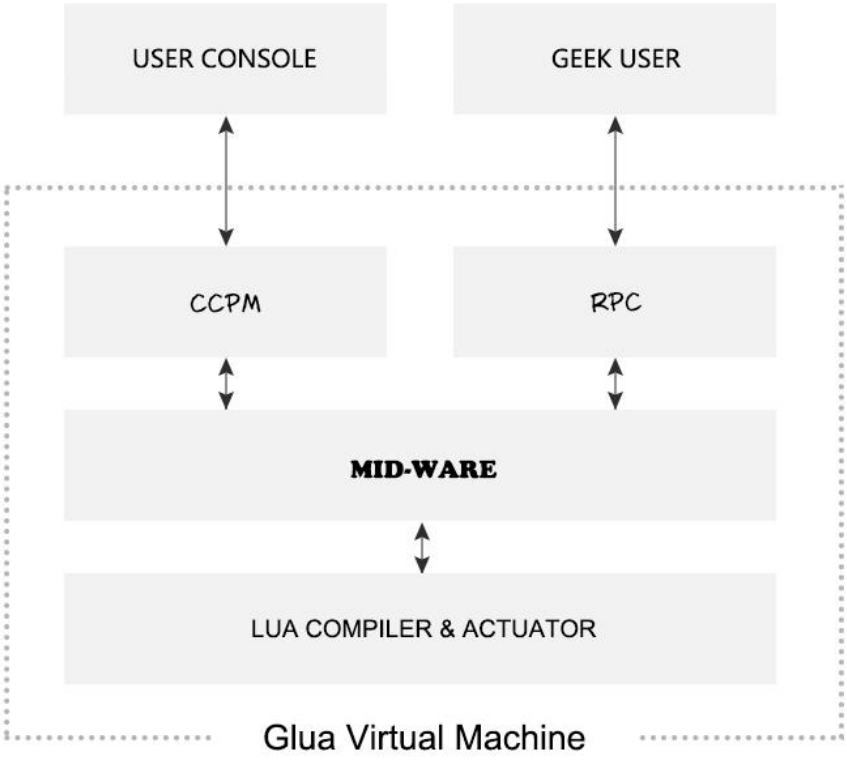
（2） 编译器将源码编译为 gpc 字节码；

（3） 用 gpc 字节码注册临时合约并向合约充值；

（4） 调用合约 API；

（5） 升级或销毁合约；

上述生命周期中，合约的注册、调用、升级需要消耗 Token。一方面执行合约必须占用计算机资源、区块链容量和网络流量，需要对资源提供者做出奖励；另一方面也是利用经济学手段提高网络攻击的门槛从而降低风险。为了更加稳定地执行合约，我们构建独立 GVM 模块，其结构如下：



GVM虚拟机架构图

GVM 包含四个模块。合约通过用户控制台（Console-User），以命令行的形式进行编写。CCPM（Contract command processing module）是合约命令行的处理模块，负责接收，并将输入传递到中间层，还负责将底层处理完的结果反馈给控制台。RPC（Remote Procedure Call）模块负责接收来自区块链网络的 Lua 执行请求，并将请求发送到中间层，待合约执行完成之后将结果返回给区块链网络。中间层（Mid-Ware）负责将 CCPM 和 RPC 传来的命令和请求同步传递给底层的 Lua 编译器和执行器进行编译，执行。并将编译执行结果返回给 CCPM 或 RPC。Lua 编译执行器（Lua Compiler & Geekuat

or）负责编译，运行 Lua 执行环境，接收和执行 Lua 脚本，并将执行结果反馈给中间层。一个活跃的区块链网络，合约调用非常频繁，为确保合约能够稳定而高效地运行。GVM 有两个设计原则：一是尽可能缩短进程启动和关闭时间；二是任何操作在不同节点不同时间每次调用的结果必须一致。除 Lua 外，GVM 还将支持 C#，Java，solidity（以太坊的合约编辑语言）等高级语言的编写，使不同平台的开发者都能够参与进来。

5.2 共识机制

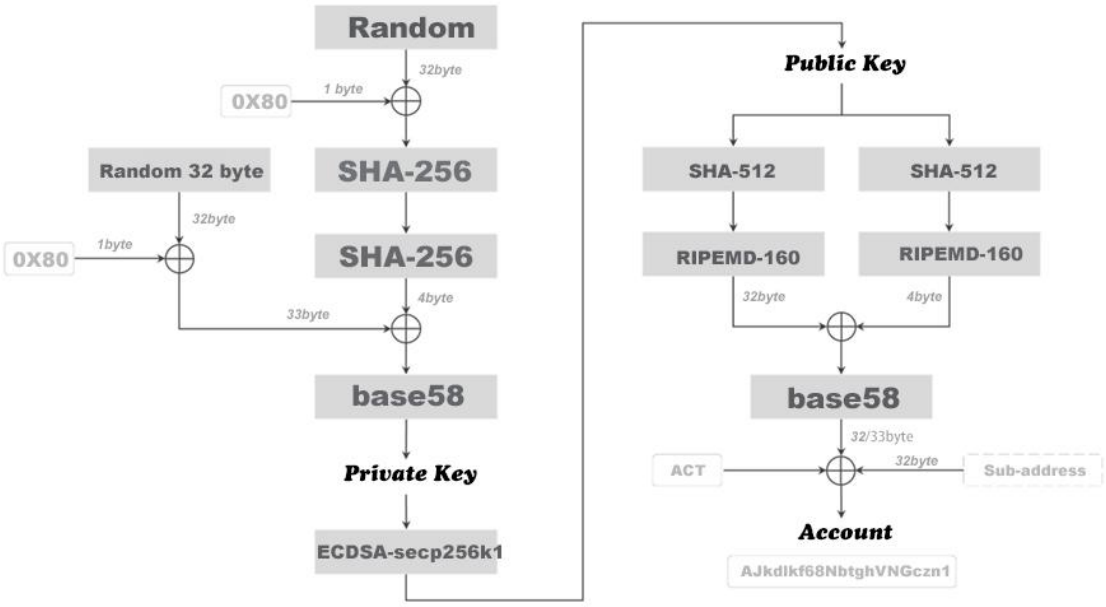
由于分布式的特点，区块链需要共识机制才能正常运转。目前广泛应用的共识算法主要有：工作量证明（PoW：Proof of Work），股权证明(PoS：Proof of Stake)，实用拜占庭容错算法（PBFT：PrGeekical Byzantine Fault Tolerance），委任权益证明（DPoS：Delegated Proof of Stake）。从安全实用考虑，GeekChain 选取 DPoS，并在其基础上改进得到 RDPoS 共识机制。

RDPoS 不仅继承了 DPoS 的优点——不需要消耗额外算力即可实现产块后的权益分配，它还能会根据网络的交易状态动态决定由代理或全体节点验证智能合约的执行结果。GeekChain 作为公有链，形成社区共识离不开经济手段——Token 的支持。持有 Token 不仅可获得合约发布、网络分叉等区块链基础服务，还能参与投票，成为代理节点提供服务获得 Token 奖励。GeekChain 把这种 Token 命名为 Geek，每一个 Geek 持有者称之为权益人，根据 Geek 持有数量分配相应的投票权重。代理节点由权益人投票选出。票数最多的前 99 个代理依次轮流验证交易，顺序由所有代理节点共同决定，并保证无法被篡改。代理正常工作可以获收益，反之工作异常或不工作，则会受到惩罚。从理论上看，RDPoS 相比 DPoS 可进一步提升网络交易能力。比如：对于某些执行时间较长、或内部状态空间占用较大的智能合约。代理仅打包结果交易的 Hash 值，而由所有节点自行验证该 Has

h 值 。在满足智能合约被快速验证的同时，也减少了整个网络的拥塞。此外，我们在共识算法上做了一些优化，避免代理节点固定不变，避免逐渐衍变为中心化的网络。

5.3 账户模型

在区块链网络中，账户地址是为了安全交换而设计出来的方案，其中的账户、公钥、私钥生成过程存在如下关系：私钥—>公钥—>账户地址，这三者都使用了安全散列算法（Secure Hash Algorithm，简称 SHA），可确保足够的安全。散列是信息的提炼，通常其输出要比输入小得多，且为一个固定长度。以目前的技术手段，加密性强的散列一定是不可逆的。即通过用户的账户地址，无法推导出用户的私钥信息。私钥、公钥、账户的具体的生成过程见如下流程：



私钥、公钥、Accont账户的生成

按照账户地址的字节长度，可分为两类账户，主账户和子账户。

主账户长度为 35~36 个字符，子账户长度为 67~68 个字符。子账户是在主账户后加上 32 个随机字符生成的，只要子账户前 35~36 个字符完全一致，可认为它们都从属

于同一个主账户。这样的账户结构，可扩展其交易性能。即从属同一个主账户的子账户可以在同一时段内并行交易，而不用担心“双花”问题。另外，子账户的设计可以节省账户开销和管理，这一设计主要用于交易所的账户设立和分配。GeekChain 使用了 Account 模型而非比特币的 UTXO 模型（Unspent TransGeekionOutput）。尽管 UTXO 设计非常巧妙，支持多笔交易并行，且账户隐私保护相对较好。但是，比特币的账户设计是面向交易的特定设计，要基于 UTXO 实现智能合约是非常困难的。而 GeekChain 生态中的智能合约，往往需要条件、状态来触发资产交易，因此 GeekChain 最终选择了 Account 模型。

5.4 分叉网络

引用以太坊基金会董事会成员——Taylor Gerring 的话，区块链硬分叉可以让网络更有韧性。GeekChain 提出适宜分叉的网络，基于两点考虑。一是保持健壮的生命力，二是满足不同的应用场景。首先，区块链网络是众多参与者按照某些共识组建起来的一个社区，共识上的分裂使得硬分叉发生，而这种分叉有时好有时差。通过人们的筛选、淘汰，最终将留下一批有价值的区块链网络，这一点非常符合自组织世界中物种和环境不断自我进化的规律。其次，区块链目前还处于发展初期，相比数字货币而言，其他应用还需要进一步探索。围绕区块链，目前已有许多创新，如闪电网络、零知识验证、侧链技术、隔离见证等等。从这些创新上可以总结一个规律——即不同交易性能、不同共识方式、不同智能合约、不同技术特点，组合起来就是为满足某一类特定需求。因此，通过分叉实现不同的网络，满足多样化需求是可行的。但多样化会带来其他问题，下一节我们将描述如何解决。

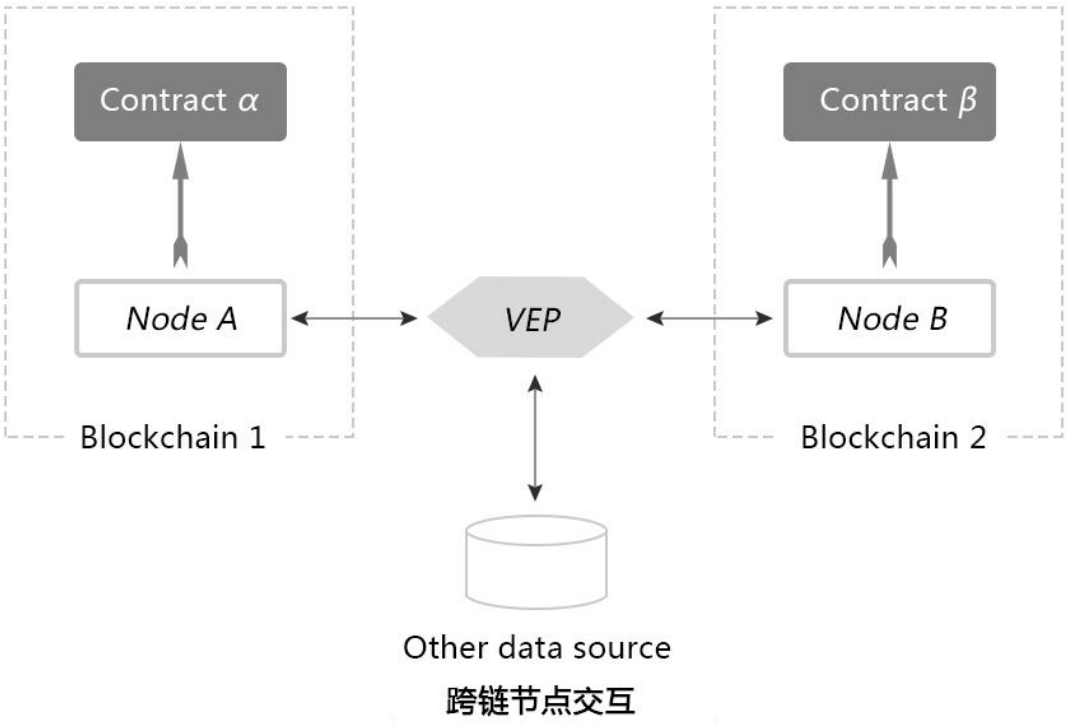
GeekChain 将作为整个分叉网络的起点，也可称其为主链。主链可以分叉出与之平行的子链，子链也可继续分叉，所有链地位平等。分叉发生时，VEP 将记录并广播这一子链的注册信息，如创世块信息、子链 ID、种子节点、数字资产、服务识别号等。如果分叉继续发生，这些注册信息将再次被 VEP 更新并同步到整个网络中。当链与链之间需要交互时，

通过注册信息即可以服务发现的方式建立连接，并在 VEP 框架下实现信息交互和价值交换。VEP 类似于互联网的 DNS 服务，负责注册信息、更新信息、提供访问服务。为了让上述目标成为可能，GeekChain 搭建了 BaaS 平台，利用可视界面和多语言支持，大幅降低开发者门槛任何人都可通过分叉建立自己的应用，从而更好地激励社区开发者的创新动力。社区活跃度提升，Geek 价值增长，社区吸引力增加，更多的开发者和使用者参与。正反馈效应将让 GeekChain 生态越来越好。

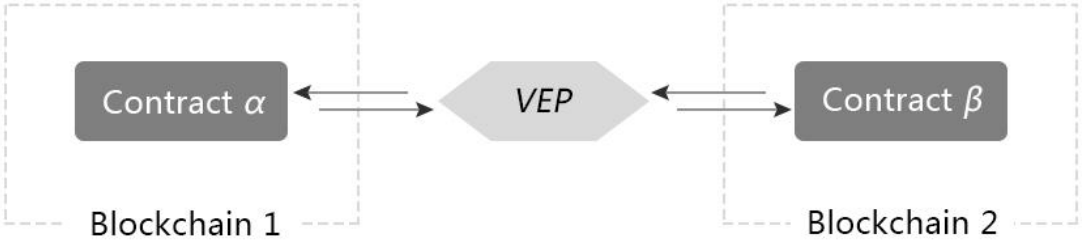
5.5 价值互换协议（Value Exchange Protocol）

VEP 是不同区块链网络之间连接的标准协议。如前所属，一个网络能够承载的应用有限，彼此连接起来形成更大的网络，可产生的价值叠加就越大。我们先了解单个网络节点是如何相互信任的。区块链网络最大的优点在于能够提供可靠的信息查询，这种可靠性体现在分布式账本和分布式共识。区块链网络是众多参与者按照某些共识组建起来的一个社区，节点在共识和激励的作用下形成了相互信任关系。推而广之，把一个区块链网络当作节点，多个区块链网络之间形成连接，也需要这样一个共识机制。因为不同网络的平等性、可信度、利益诉求让网络协作变得困难，再加上网络中总有坏节点。因此，协作前预先设定的规则尤为重要。这就如同人类社会中跨组织协作需要有法律，契约和道德的约束。

VEP 为如何协作制定了准则。它登记每个链的注册信息，并提供服务给受信列表中的链进行查询和连接请求。VEP 支持跨链节点交互和跨链合约调用两大应用场景。前者利用存储在节点的数据或外部数据的状态变化，间接地让合约之间产生交互，并可能产生新的信息。例如：按照合同约定到期未偿还贷款，将会影响到个人信用。贷款记录可以存储在区块链 A，而信用数据则可以存储在区块链 B，个人身份信息可能来自外部的公用数据库。后者则是合约之间相互调用，一个最简单的例子就是两个链的 Token 互换，并让总价值保持不变。



跨链节点交互



跨链合约调用

VEP 中包含以下内容：

（1） 链的注册信息，网络身份、服务识别号、种子节点信息等，类似于 DNS Domain Name Server）中记录的信息；

（2） 跨链验证协议；

（3） 数据通信协议；

（4） 资产交换协议；

（5） 奖罚机制；

5.6 事件驱动

依托于 VEP，GeekChain 可实现链与链之间的信息交互和价值交换，甚至将现实物理世界中的 IOT（Internet of Things）、AI（Artificial Intelligence）、企业或公共服务数据库等非区块链数据源也纳入到生态中，做到实时的事件驱动（Event-Driven）。实现事件响应的 5 个步骤：

（1） 场景识别、分类并设定响应标准；

（2） 开启监听服务，获取数据；

（3） 计算和响应判定；

（4） 执行，通过 VEP 调取数据，执行合约；

（5） 反馈执行结果；

6 发行计划与用途

GeekChain Token 是基于 Geek Blockchain 公链生成的代币。发行总量为 100 亿枚，其总量上限已设定，不可更改，不可增发。

Geek 是极客链（GeekChain）上的数字资产，Geek 是个人用户使用的数字资产。它不仅具有流通价值，同时还是基于极客链应用的必备加密数字资产。它的应用价值主要体现在以下几个方面：

1、在极客链上开发、认证应用、使用链上服务（例如链上转账的矿工费）需要支付或燃烧 Geek，Geek 是作为链上应用运行唯一使用到的 Token。

2、随着 GeekChain 合作的客户和数据源越来越多，数据交易的交易量越来越大，基于公链网络就可以收到更多的佣金，团队会定期拿出佣金收入的 10%按照当时二级市场的价格回购 Geek 并销毁。

3、在内容创作产生版权时见证人可作为选票使用，同时创作者技能认证程度，获得 token 奖励。

4、在客户端产品，基于公链网络的网页应用和 Dapp 中，Geek 将作为重要支付手段。具体体现为：

1）用户与用户、用户与商家、商家与商家之间互相使用 Geek 进行结算；

2）使用公链网络公共服务需要用 Geek 结算；

3）当完成商户的任务，或是参与一些活动时如共享协作，将会收到 Geek 作为激励。

初期发售所筹得的资金将用于以下用途: 开发公链生态网络，Web 客户端和 Dapp 应用与交易平台国际版，整合区块链技术使平台具备数字货币与内容作品进行交易的能力；包含此过程中所需的技术执行、营运、推广费用。基金会的编制将确保公平。基金会将会对项目方和团队持有的代币实施 3 年逐步释放的方案。

比例	**分配对象**	**分配规则**
35%	基金会	用于研发和运营
15%	创始团队	3 年逐步释放
15%	知名网络极客	3 年逐步释放
15%	渠道商	12 个月的锁仓期
20%	社群成员	贡献奖励即时生效

代币分配表

7 核心团队

我们是一家以用户为中心的区块链创业团队，由新加坡世界网络极客基金会(World Network Geek Foundation Ltd.)发起；创始团队成员曾在顶级 IT 机构全球活动策划公司

担任高级管理工作，曾负责过世界 500 强企业的 IT 技术难题攻克和网络创意的策划及执行，如：星巴克、雀巢、 惠普、LG、 三星 、奔驰、路虎、大众 、Apple、飞利浦、NIKE、IBM、阿里等，部分成员参与过著名国际极客大赛和信息版权管理的工作，研究极客文化并激发世界每个极客的成果得到应用，致力于挖掘网络极客的潜在商业价值，在版权交易，教育，人才管理领域中有着丰富的经验及资源。2016 年在新加坡成立世界网络极客基金会，基金会致力于研究与探索区块链在人才、版权、众包协作、商业服务领域的应用，同时建立基金会智库具有典范意义的是按和标志性技术产品与素材库，开源共享。我们的团队汇集行业内和技术领域的思想领军人物与充满激情的创造者 ,为全球用户带来最直接的无缝互联的区块链落地投资价值。

7.1 成员介绍

Justin Wang

联合创始人| 核心研究
商业策略和技术专家

曾担任财富 500 强医疗保健公司的首席企业架构师，160 亿美元对冲基金的架构和开发负责人以及一家基金的首席技术官，该基金在他的技术平台上三年内回报超过 40%。

Shawn Wei

联合创始人| 核心开发
曾任北京众链科技区块链项目总监

加州大学伯克利分校的计算机科学硕士。在 LinkedIn 和 Opentable 高级软件工程师。负责区块链系统“DNA”的核心设计和开发。

杨文传

联合创始人| 技术顾问
区块链架构师

某上市公司 C++项目负责人

区块链架构师、Cellular Automata、Ising Model、分布式信息处理系统领域专家。全栈工程师

Bob Murray

联合创始人| 核心研究

在技术，安全，数字内容以及国际和移动支付行业拥有丰富经验的连续创业家。他是雷曼兄弟的前投资银行家，在那里他帮助政府、金融赞助商和他们的投资组合公司筹集国际私募股权和高收益资本。

Allen Dixon

联合创始人| 首席运营官
Blockasset 创始合伙人

擅长将技术与市场紧密对接， 创造新的商业模式。在电信行业拥有 20 年以上的丰富经验，曾领导多个与 Apple、Amazon 和初创企业合作的项目。

Andrew Pipolo

战略顾问
Paypal 日本和澳大利亚前任常务董事

Andrew Pipolo 在亚太和欧洲的支付和技术行业拥有超过 20 年的经验。他曾担任 PayPal 澳大利亚和和 PayPal 日本的常务董事。

Chris Wu

商务拓展和运营
资深商务拓展和技术项目经理

在 Qualcomm 和 Amazon 的网络部门工作近 10 年，曾担任资深商务拓展和技术项目经理，具有丰富的行业经验。

Mr.Wang 市场总监

前阿里巴巴市场部总监

曾负责阿里巴巴跨境电商海外市场的拓展

互联网从业 10 年，三节课联合创始人，曾任阿里巴巴运营经理，第八课堂 COO，八哥招聘运营合伙人。

Mateusz Spychaj

特约顾问
世界著名网络极客

A.B. 哈佛大学，计算机科学，Boltzmann.io 首席技术官

第二名—哈佛—麻省理工学院联合编程比赛

Ash Shilkin

特约顾问
自由网络职业者

毕业于伦敦大学计算机学院，曾受雇于 IBM、Google 等技术公司破解技术难题

自由软件和开源运动倡导者

7.2 极客世界介绍

全美人气最高的业余互联网极客交流平台，在业内拥有良好的口碑与权威，以众多优质技术超前的原创作品而闻名全球，吸引众多知名网络极客、IT 爱好者在此聚集!平台致力于为经验丰富的极客和积极努力的 IT 从业人员提供一个良好的展示自我的平台。

2018 年 1 月，Geek 基金会与极客世界达成战略整合，使用极客世界优质的用户及丰富的作品资源，打造全新的作品版权交易平台(ART STORE)，平台会使用 GeekChain Token 作为流通数字货币，未来会将交易平台的全部数据建立在区块链上，建立商业上链 Geek 全球多国平台内容运营团队，推动 GeekChain Token 的全球化运作。

8 发展路线图

8.1 Geekchain 阶段性规划安排

对于极客链的整体发展，是个短期建设与长期发展相结合的发展过程，并随着区块链和智能合约技术的成熟与普及，逐步完善下述战略举措。

第一阶段，孵化（2016~2018）。利用模块化的设计方法构建安全稳定的区块链网络，试和监测合约运行的环境，魔盒可确保即将正式运行在链上的合约足够安全。

第二阶段，应用（2018~2019）。通过分叉来满足不同的商业诉求，如数字版权、电子文档、数字货币、溯源追踪、个人信用记录等。这一阶段将实现一个不断进化、容易使用、低成本的、适度定制化的区块链网络。

第三阶段，生态（2019~2020）。通过价值互换协议（VEP），将诸多分叉连接，甚至与其他网络（可能是非区块链的）打通数据交互，构建出一个相互连接、多维数据相互关联的网络世界。

Geekchain发展计划

9 风险说明和免责声明

9.1 政策风险

区块链目前尚处于早期，国家对于区块链项目的监管政策上不明确， 这有可能对项目的发展和流动性产生不确定影响。目前数字资产价值波动巨大，存在暴涨暴跌、庄家操控的风险。投资风险相对较大，参与者可能缺乏市场经验，无法把握市场的不确定性。这有可能会带来资产的冲击和心理压力，投资者需要有较强的承受能力，请各位参与者谨慎参与。

9.2 技术风险

基于 GeekChain 区块链技术的 Geek 代币发行标准目前是兼容比较强，但并不排除以后公链升级有可能引起的新问题。项目的更新过程中，有可能出现漏洞，漏洞发现后会及时修复，但不保证不造成任何影响。

Geek 目前拥有一支在线插画社区和区块链领域从业经验资深的小伙伴组成。团队内部当前稳定，凝聚力强，在今后的发展过程中，不排除有核心人员离开，团队内部发生冲突而导致 Geek 受到负面影响的可能性。

9.4 统筹风险

团队将不遗余力地实现白皮书中所提出的所有发展目标。目前团队已有完善的技术和商业团队，然而技术开发等事项发展存在不可预 因素和不确定性，现有的商业模型与统筹思路存在与市场需求不能良好吻合的可能，从而导致盈利难以实现或未达到投资者预期。同时，由于本白皮书后续可能随著项目进展进行调整，如果项目后续进展细节未被投资者及时获知，投资者因信息不对称而对项目认知不足，有可能会造成投资损失或影响项目后续发展。

9.5 竞争风险

当前区块链行业项目众多，竞争十分激烈，Geek 借助其目前的核心团队成员快速成长，运营推广。强大的市场竞争，会给项目带来压力，项目是否能在诸多优秀项目中得到广大市场认可，这和团队本身有关，也受到市场上诸多竞争对手的影响，不排除会面临恶性竞争的可能。

9.6 交易风险

GeekChain Token 作为一种数字货币资产，其交易具有极高不确定性，由于数字资产交易领域母前尚缺乏强有力的监管，故而数字货币存在暴涨暴跌、全天候交易、庄家操盘等险，个人参与者若无投资经验，可能会对个人资产造成损失。投资者应根据自身情况及经验妥善选择投资方式。

9.7 黑客风险

在安全性方面，我们一直以最高标准要求自己，也收到过来自黑客的威胁，我们都已应对。但黑客的攻击依然无法避免，随着 Geek 数字资产的增值，更容易成为犯罪分子的攻击目标，存在一些不可预知的风险。

9.8 未保险损失风险

Geek 是基于区块链去中心化技术开发的，用于存储 Geek 的钱包密码如果丢失，将不会有任何组织为你找回，请妥善保管，平台不会为个人 钱包密钥丢失行为承担任何结果。

9.9 免责声明

本白皮书，仅作为产品介绍，传达信息之用，不作为投资参考。本文档不构成也不理解为提供任何互换行为指导，所有互换都是自愿原则。相关意向用户请明确了解 Geek 的风险，投资者一旦参与投资即表示接受了该项目风险，并愿意维持承担一切相应后果。本基金不承担任何参与 Geek 项目造成的直接或间接资产损失。

区块链作为新兴产业，具有极高的投资风险和技术风险，属于高风险投资行业。白皮书作为技术和产品描述 ,阐释了技术和产业的布局和前景 ,不建议没有风险承受能力的人投资。

参考文献：

[1] 祝凯. 基于 P2P 的分布式存储系统研究[J]. 中国传媒大学学报（自然科学版）,2008,(3).doi:10.3969/j.issn.1673-4793.2008.03.005.

[2] 董健全,武雪丽,李智昕. P2P 网络中应用移动 Agent 进行资源搜索的研究[J]. 计算机工程与设计,2005,(1).doi:10.3969/j.issn.1000-7024.2005.01.009.

[4] 高伟,韩华,代亚非. 一种 P2P 环境下分布式文件存储系统的缓存策略[J]. 计算机工程与应用,2004,(30).doi:10.3321/j.issn:1002-8331.2004.30.015.

[5] 周邺飞. 区块链核心技术演进之路——共识机制演进(1)[J]. 计算机教育,2017,(4).doi:10.3969/j.issn.1672-5913.2017.04.040.

[6] 朱建明,付永贵. 基于区块链的供应链动态多中心协同认证模型[J]. 网络与信息安全学报,2016,(1).doi:10.11959/j.issn.2096-109x.2016.00019.

[7] 郭彬,于飞,陈劲. 区块链技术与信任世界的构建[J]. 企业管理,2016,(11).doi:10.3969/j.issn.1003-2320.2016.11.043.

[8] 董耀祖,周正伟. 基于X86架构的系统虚拟机技术与应用[J]. 计算机工程,2006,(13).doi:10.3969/j.issn.1000-3428.2006.13.026.

[9] ROSENBLUMM., GARFINKELT.. Virtualmachinemonitors:currenttechnologyandfuturetrends[J]. 2005,5(5).

电子科技的演变，由连接信息-到链化信息，信息传递-到价值传递，折射网络-到映射网络 逐渐趋于虚拟到真实的过程。我们在享受到科技带来的福利同时，正是电脑背后的一只只 GEEK 夜以继日的贡献而成……