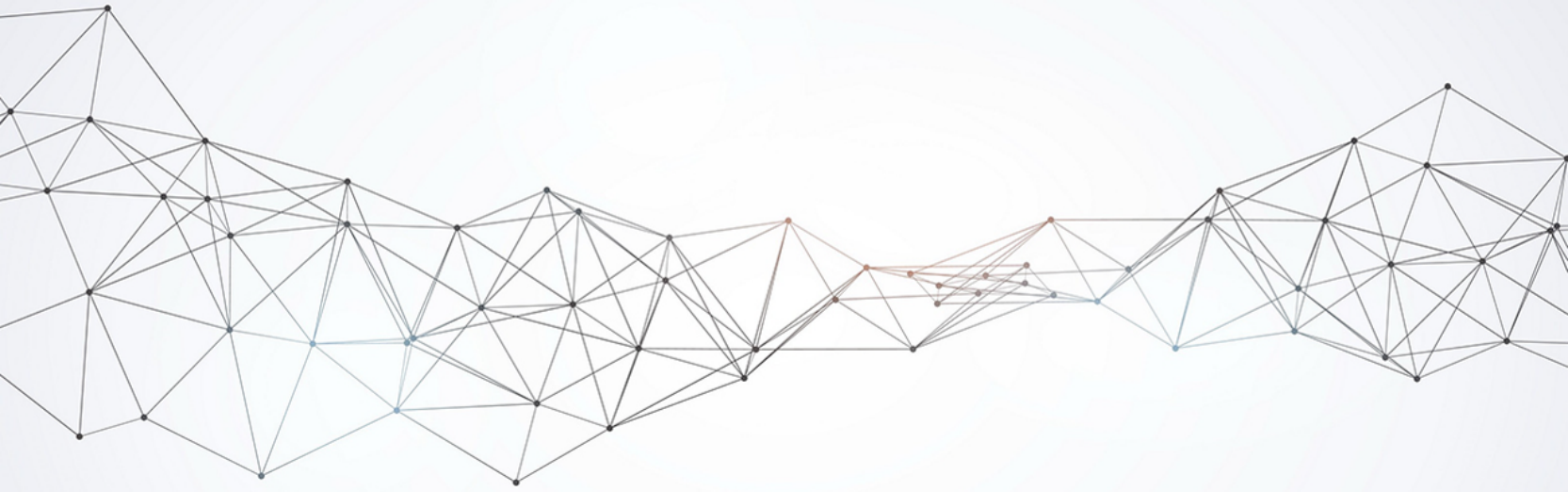
NGK

WHITE PAPER

SHAPE YOUR BRIGHT FUTURE WITH NGK INVESTMENT



APPLICATION VALUE OF NGK AND USDN

DRIVE INNOVATION, LINK THE FUTURE

NGK BLOCKCHAIN IS A COMMERCIAL FINANCIAL BLOCKCHAIN OPERATING SYSTEM BASED ON DISTRIBUTED APPLICATION DESIGN, THROUGH THE MOTIVATION OF DIGITAL MONEY TO PROMOTE PARTICIPANTS IN THE NETWORK, NGK MAIN NETWORK HAS TWO TOKEN SMART CONTRACTS DEPLOYED, THE APPLICATION IN DIFFERENT FIELDS IS REALIZED BY DECENTRALIZED MECHANISM, A GLOBAL TOKEN NETWORK BUILT WITH A BLOCKCHAIN BUSINESS AND FINANCIAL ECOSYSTEMTHE OWNERSHIP OF THIS WHITE PAPER BELONGS TO THE OFFICIAL WEBSITE OF NGK.IO.

NGK SPIRIT STONE

摘 要
Abstract

数字货币的历史从2009年比特币的诞生开始至今已经发展了十余年，全球共计出现了上万个区块链项目，经历了区块链1.0与2.0时代，区块链即将步入3.0时代，即通证经济时代，商用平台的出现，使“通证经济”成为可能，并带来了生产力发展与生产关系的变革。

从金融领域走向了通证经济，未来区块链的价值核心之一通证（Token），通证作为一种价值的凭证，将成为区块链网络的应用载体，通证不仅仅适用于去中心化的激励，更多体现在数字经济权益上，让经济权益通过区块链实现经济增长，让整个生态圈的每一个人、每一个角色自发参与协作，自发参与维护。在具有现实经济的理念上，通过区块链实现商业变革，让价值权益上链发行，全球任何的商家和企业都可以共同参与进来，形成区块链数字化的用户共享、经济共生、产业互通的商业生态，Token作为大规模群体协作的激励媒介，极大地调动社区参与者的积极性和创造性，充分激发出经济体的活力，极大地促进区块链商业经济的增长。相信在未来数字经济终将实现传播流通以及落地的商用价值。

基于此背景下NGK通证应运而生，NGK.IO平台联合了美国哥伦比亚大学，美国硅谷 Silicon Valley Interconnected Finance Group（SVIF），瑞士区块链金融研究所SBC,以及全球知名的数字资产管理公司FBG共同研发，平台拥有众多技术领先的研发精英，和众多实力投资公司鼎力支持，在美国受SEC证券交易委员会监管。

NGK.IO团队从 2018 年开始潜心研究推出NGK区块链数字货币基金和产业生态相结合的盈利方式，全面打造更加完善的商业生态圈，必将再次引领区块链市场。NGK通证作为NGK.IO平台上无障碍使用的通证，从而连接线上线下各行各业的商家，实现商业落地应用，不仅助力传统产业转型升级，更撬动了互联网经济的杠杆，推动了实体经济的发展。

NGK.IO通过跨链可以为不同的消费场景形成价值的互通，为全球“通证经济“商业化进程做出一定的技术力量，相信在未来NGK.IO将对价值交换的速度必然会有飞跃的提升，从而实现真正联合互通的价值网络！NGK.IO作为区块链平台，帮助数字资产的管理和流通，为提升生态效率和促进市场繁荣贡献一份力量！

在技术层面上NGK.IO致力于打造一个通用的智能合约编程平台与区块链操作系统，NGK.IO有自己的图灵完备的编程语言以及运行环境，专为数字资产提供安全的金融服务，避免了智能合约带来的巨大安全风险；NGK.IO力图实现安全可靠、快捷便利的跨链资产转移、跨链智能合约调用，更高的TPS能力为后续区块链实现商用平台的实现提供技术支撑。NGK.IO公链延续了EOS软件堆栈的WebAssembly机制，可以非常轻松地开发DAPP，任何人都可以在NGK.IO并行链上开发或使用跨链DAPP。

与EOS不同的是，NGK.IO将在钱包易用性上采用更先进的技术实现，从而彻底解决EOS所面临的CPU资源不足导致的用户交易体验差的问题。在生态治理上，NGK.IO沿用EOS的21个超级节点机制，同时采用

更加民主，去中心化的治理结构，并有效地解决了传统区块链系统面临的低吞吐量，交易确认延时，区块膨胀等区块链式结构先天的悖论问题。技术实现上NGK.IO大大提高了系统效率，交易处理能力，实现了商业级的提高。

基于AI智能、大数据算法分析、机器学习等技术研发的数字金融衍生品投资策略管理系统，旨在成为第四代区块链金融投资领域的代表。通过区块链科技，持续进行共识机制优化、交易处理速度提升、智慧合约多样化、资产杠杆化、扩展性提升，帮助投资者社区、社群做出安全、有效、精准的投资与资产管理决策，在全球范围内配置与优化数字资产管理效能，推动全球数字资产金融投资产业的创新与进化，成为区块链金融行生品全维度指数大数据中心。随著频密指数波动交易，NGK在未来区块链金融和数字资产创投领域将会创造无限价值。

NGK数字通证将是NGK.IO公链技术内生结算桥梁，用于激励的生态系统内的建设者、参与者、开发者、使用者以及各种商业应用、数字资产、积分汇兑等！NGK.IO将以落地通证为基本发展战略，引领全球支付新模式！

目 录
Content

摘要 1

一 NGK.IO 背景与意义 9

1.1 信息网络的发展历程 9
1.2 区块链是大势所趋 11
1.3 技术瓶颈仍需解决的问题 12
1.4 区块链商业化落地进程的困境 14
1.5 用户和市场痛点 15
1.6 为什么需要 NGK.IO 18

二 什么是 NGK.IO 19

2.1 系统设计原则 22
2.2 哲学思想 23

三 NGK.IO 使命与愿景 25

四 NGK.IO 架构设计 27

五　NGK.IO 公链　31

5.1　NGK.IO Token 钱包　31
5.2　智能合约运行　32
5.3　黑洞销毁机制　33

六　令牌发行机制　35

6.1　Token 种类　35
6.2　发行计划　36
6.3　算法性稳定币 USDN　37

七　NGK.IO 的技术特点　41

八　NGK.IO 改进分布式储存系统　51

九　NGK.IO 核心技术优势　53

9.1　抗量子攻击密码算法　53
9.2　独创的匿名 P2P 通信网络　54
9.3　虚拟机独立架构　54
9.4　简化应用构建技术　55
9.5　石墨烯技术　55
9.6　跨链技术　56

十 NGK.IO 共识算法 58

10.1 BFT–DPoSS 共识机制 58
10.2 PBFT 检查点协议 61
10.3 一致性算法 63
10.4 投票激励机制 65
10.5 超级节点 67
10.6 分布式超级节点选举算法 DSNE 71
10.7 超级节点的重新选择 71
10.8 节点四大状态 72
10.9 惩罚机制 72

十一 跨链交互机制 74

11.1 体系内的跨链通讯 74
11.2 NGK.IO Core 采用的跨链方案优势 75
11.3 更安全随机数方案 76

十二 NGK.IO 企业级侧链应用 78

十三 NGK.IO 通证支付系统 84

13.1 传统支付构架的技术弊端问题 84
13.2 NGK.IO 引领通证支付创新未来 85

十四　NGK.IO 公链实现步骤 88

十五　NGK.IO 去中心化预言机 91

十六　NGK.IO 治理结构 95

16.1　超级节点机制 95
16.2　超级节点收益来源 96
16.3　超级节点挖矿机制 97
16.4　超级节点权利与职责 97

十七　NGK.IO 未来生态建设 99

17.1　NGK.IO 国际市场新模式建设 99
17.2　全球金融支付国际化 100
17.3　NGK Wallet 多链钱包 100
17.4　NGK.IO 金融衍生品交易所 101
17.5　NGK.IO 社区文化推广 102
17.6　NGK.IO 金融孵化项目 102

十八　NGK.IO 未来技术框架与路线 103

18.1　NGK.IO 未来技术框架 103
18.2　NGK.IO 未来技术路线 105

十九　结语 108

二十　风险提示与免责申明 109

一

NGK.IO
背景与意义

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。

2008年10月31日，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 of Work，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（Practical 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。

截止 2019 年 12 月，全球虚拟数字货币交易所资讯数据超过千家， 而实际数据甚至超过万家。

他们犹如天上的繁星，为以区块链技术为核心的通证经济点亮了明灯。

同时，我们也注意到，随着通证经济的来临。目前的绝大部分交易所，功能性和指向性仍然为交易。而对于通证经济的方向上，准备很少，甚至没有准备。

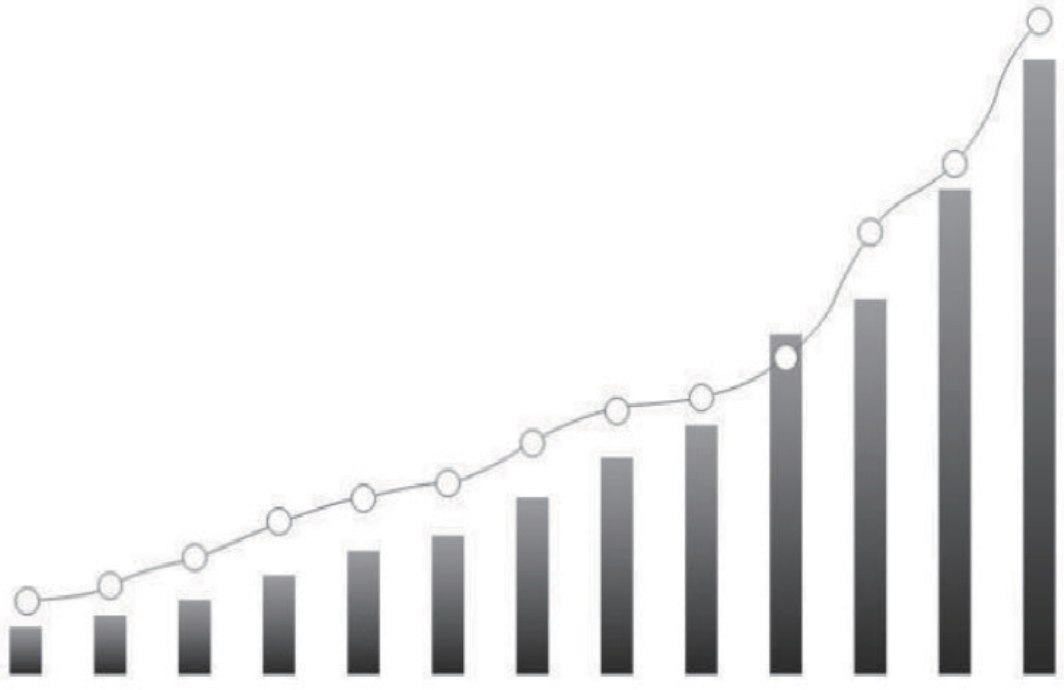
扎克伯格和他的 Facebook 在 6月18日发布了 Libra 白皮书。随后 2019年7月16日，美国参议院银行、住房和城市事务委员会就Facebook的新加密货币Libra举办听证会。

本次事件得到了全球关注，许多国家高度重视，并召开金融会议， 探讨

数字加密货币与通证经济。

我们可以看到，通证经济脚步的一点点临近，而这将会是如同上世纪末互联网革命一样。世界现有经济模式将被改写，亿万财富将重新分配。

1.2 区块链是大势所趋



全球区块链项目生态图谱

为什么会出现区块链，我们真的需要吗？NGK.IO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 技术瓶颈仍需解决的问题

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（Factom），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），甚至

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 区块链商业化落地进程的困境

区块链经过了数年的发展，毫无疑问，技术的改进使得现有的区块链拥

有了更多的落地场景的可能，其技术本身带来的不可篡改性、分布式等特性使得其在一些实际应用领域有很好的落地场景，但由于发展时间比较短，一些方面（诸 如信息隐匿性）仍未成熟，这些很大程度上限制了区块链技术在一些应用场景的落地。发展至今，区块链商业化进程道路上依旧面临的痛点仍是完善基础设施，规范产品标准，简化人为因素等多原因：

- 基础设施的搭建欠缺；
- 区块链应用缺乏产品化和评测标准，解决方案提供商在服务同行业的多个用户时，由于没有统一标准，产品仍没有获得大范围的应用；
- 传统思维限制区块链商业化推进，由于市场对于区块链应用的落地太过急切，但现状又是底层去中心化的公有链对于各行业不能通用，智能合约太过简单不能支撑复杂的商业场景；
- 项目多停留在POC阶段，没有生产系统以及大规模推广应用的验证机会，并未形成真正意义上的E2E行业解决方案；
- 跨主体多方协助时仍需要设计巧妙合理的分配机制！

1.5 用户和市场痛点

数字货币管理不便

尽管数字货币市场在快速发展，但对于数字货币的存储和管理，仍然没有很好的解决方案，如何安全备份一种数字货币的钱包密钥或地址私钥，就已经是拦在用户面前的一大门槛。现在面对越来越多的数字货币类别，用户进行不同资产配置或分散投资时，管理门槛进一步提升，而应对的策略——要么是针对不同类型的数字货币，安装不同的去中心化钱包分别管理；要么是索性放在中心化钱包或者交易所里，让中心机构代为管理。前者给用户使用和管理带来了极大不便，后者又存在一定的安全隐患（中心机构被攻击，或经营不善倒闭等情况将带来资产损失）。如何更好的兼顾安全性和便利性，是该领域服务商一直努力的方向。

交易和兑换门槛高

目前数字货币的交易和兑换，主要通过交易所完成，这对非专业用户是很高的门槛 —— 注册交易所需要严格的实名身份认证；交易数字货币需要学习相关流程和操作步骤，充值和提现通常还会有一定限制；数字货币之间的兑换，需要先用数字货币换为法币，再用法币买入另一种数字货币。

另一种方式是提供场外的数字货币交易，有买卖需求的用户各自报价，大家只需像使用C2C商城一样，看到合适价格，一对一交易。但不足的地方是，为了保证交易双方不违约，交易过程中数字货币通常需要托管在平台方，这又衍生出平台方可能违约的风险，主观盗币或客观因黑客

攻击等原因造成损失。

区块链性能不足及设计不合理

2017年8月比特币发生了第一次大型的分叉，产生了BCH，随后几个月，不断的有人对比特币网络进行分叉。以太坊网络因为发生DAO事件，硬分叉为ETC 和ETH。这里原因是什么呢?

1 比特币性能严重不足，BCH打着为比特币扩容的旗号对比特币进行了硬分叉；

2 算力越来越集中，本来应该去中心化的系统沦为一家控制，随意操纵区块链网络，违背了区块链去中心化的初衷；

3 以太坊的智能合约，是区块链非常大的进步，但是这种设计理念却有一个巨大的问题，即把金融逻辑和业务逻辑耦合在了一圈；

4 在EOS主网逐渐发展的过程中，我们发现了一些偏离期望的地方。作为最有竞争力的第三代公链，大家希望看到的是能够有更多、更丰富的应用能够在 EOS 上面运行，开发者会将 EOS 作为自己应用开发的首选平台，但是由于目前EOS的资源模型的限制，导致了很高的使用成本，包括为用户创建更多的账户，以及部署运营DApp需要的较高成本。针对白皮书中要实现的上百万TPS需要的关键技术IBC，一直没有进行推进，主网多次出。

现CPU计算资源不足的情况，更是加剧了对跨链通讯需求的迫切性。此外，由于EOS采用的BFT–DPOS共识机制，一个交易需要近三分钟才能保证不可更改，虽然相较比特币、以太坊是有很大的进步，但是这也给EOS的应用场景带来很大限制，快速支付只能聚焦于小额转账，大额转账必须要等待足够长的时间才能保证不可更改，这就限制了链上、链下用户支付体验。

区块链开发成本高、算力浪费大、连接现实世界难

区块链技术的大力发展，未来将有各行各业的企业使用区块链技术，而区块链开发成本高将使创业者望而却步；POW的挖矿模式，由于算力竞争激烈，被淘汰的矿机被当做垃圾扔掉，极为浪费，多种工作机制又无法具备POW的去中心化优势；区块链技术本身很难知道现实社会的数据，比如温度多少、股价多少、天气如何等等数据，虽然一些矿工可以提供一些常用的数据，但是由于现实世界数据种类复杂繁多，矿工无法提供创业者想要的数据，而创业者如果完全自己提供这些数据，又做不到去中心化的特性，很难让人信服，导致区块链连接现实世界难。

“DAPP+”应用场景缺失

数字货币要有更长久的发展，就必须有更广泛的应用场景支持。目前随着区块链领域研究的深入，特别是针对智能合约方向的探索，逐渐有一些产品方案和实体经济生活相结合，在需求端谋求合作共赢。但真正落地并规模使用的还很稀缺，同时针对用户端的服务更是屈指可数。无论是比特币、以太坊，还是基于智能合约平台新发行的各种代币，只有和实体世界有了更多的交互，才能增 加 DAPP 自身的价值，进而促进数字

货币的市场繁荣和实体世界的效率提升。

1.6 为什么需要 NGK.IO

目前区块链的系统主要矛盾在于DAPP的运行效率和现实商业需求严重背离，数字交易与性能方面严重不足以及链接现实世界的成本居高不下。

NGK.IO在诞生之初，技术实现上就摈弃了广泛节点的验证方式，而采用DPOSS 机制，由 21 个主要节点出块，并采用制度去降低主要节点作弊的可能性。这是目前提高性能最具备可行性的方式，换句话说，NGK.IO在理想和现实中选择了现实，NGK.IO的模式设计更贴近商业用户的需求。

NGK.IO交易速率上通过并行处理可高达数百万TPS，并且可供普通用户免费使用、采用快速出块机制来确保低延迟和高度优化的串行性能。并设计了一系列机制以保证商业用户的易用性。

在商业应用场景中NGK.IO通过虚拟机、智能沙盒、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，NGK.IO通过对出块间隔、区块容量、共识算法的优化， 使得TPS 超过 100 万，未来 NGK.IO 将通过技术创新，解决人与人之间的信任问题，缔造一个全新的生产关系网络，更好地将社区共识、个体行为、价值交换有机地融为一体，以实现NGK.IO服务平台商用价值!

二

什么是 NGK.IO

NGK.IO是一个基于C++为主要编程语言，底层采用WebAssemblyJIT虚拟机并支持STL开发库技术的通用的区块链编程平台，采用 IPFS 顶级分布式存储的一个去中心化分布式区块链操作系统。NGK.IO必将引领区块链行业未来的基础设施，NGK.IO内置图灵完备的编程语言，用户可以用之来建构和定义他自己的各种特性，可以开发自己的应用与区块链系统，可以发行自己的货币。NGK.IO同时拥有可一键定制的侧链，NGK.IO提供专有的跨链和跨合约技术，将主链和侧链链接在一起。无论

是NGK.IO上的合约资产，还是非NGK.IO上的资产，都能通过NGK.IO具有的跨链及跨智能合约的技术自由的完成价值传递和兑换。

NGK.IO底层是基于一种名为石墨烯的区块链技术开发的，NGK.IO采用DPOSS共识机制，由21个投票选出来的节点生产区块，而且NGK.IO在运行智能合约时无需像以太坊那样每一步都要消耗GAS，这使得用户免费使用Dapps成为可能，更符合互联网产品使用免费、依靠增值服务和广告等业务盈利的商业模式，所以我们可以认为基于NGK.IO开发的Dapps才是真正Dapp。 NGK.IO 的设计目标是 TPS 超过 100万，更是提出 NGK.IO 区块确认时间将达到的 3 秒，因此 NGK.IO 将具有非常卓越的性能，有希望改变当前区块链技术无法落地的局面。由此我们可以预见，未来会有众多区块链创业项目选择基于 NGK.IO 发行 Token，开发出大量可以落地的Dapps，吸引数亿用户来使用，NGK.IO有望形成丰富和完整的商业生态，同时衍生出大量交易 Token 的需求。 NGK.IO 基于NGK.IO主链和NGK.IO智能合约为底层运行环境，充分利用区块链和NGK.IO的生态系统，建立一个安全、可验证公平性、去中心化、去信任化、无国界的商业与金融一体的区块链系统，为创新型企业团队提供产业基金、互联网基金、区块链基金以及物联网与人工智能等金融服务和产业孵化服务，打造世界级生态商业闭环。

包括比特币、以太坊在内的传统的区块链，底层采用的是区块+链式结构。这种结构设计会带来区块数据膨胀，交易延时，吞吐量低等先天性缺陷。比如著名的比特币扩容之争，双方的争议点在于是否进行区块扩容。支持扩容的一方认为，在交易越来越多的情况下，很多交易无法及

时打包进区块，会造成大量交易长时间延时，为解决该问题需要进行扩容。而不支持扩容的一方则认为，扩容之后区块变大，将会使区块数据迅速膨胀，以至于普通的个人电脑难以储存。这就是传统区块链先天性缺陷的体现，而且还是悖论式的。

我们希望在前人的基础上，为NGK.IO带来的优秀的共识机制并设计一套异构多链体系，实现更好的商用生态。

性价比高的链上资源：
开发者可以根据自身需求自由选择运行的侧链，允许多个侧链接入整个生态，会使得资源的供给可以充分满足市场的需求，这样可以稳定链上资源的成本，另一方面，很多应用会希望链上可以提供稳定的资源和TPS，通过部署专门的侧链，可以充分保证DApp运行不会被其他应用干扰。

允许扩展链功能：
某些时候开发者和用户需要扩展链功能以实现其特殊的需求，进而部署专门的联盟链或者私链以侧链加入NGK.IO。

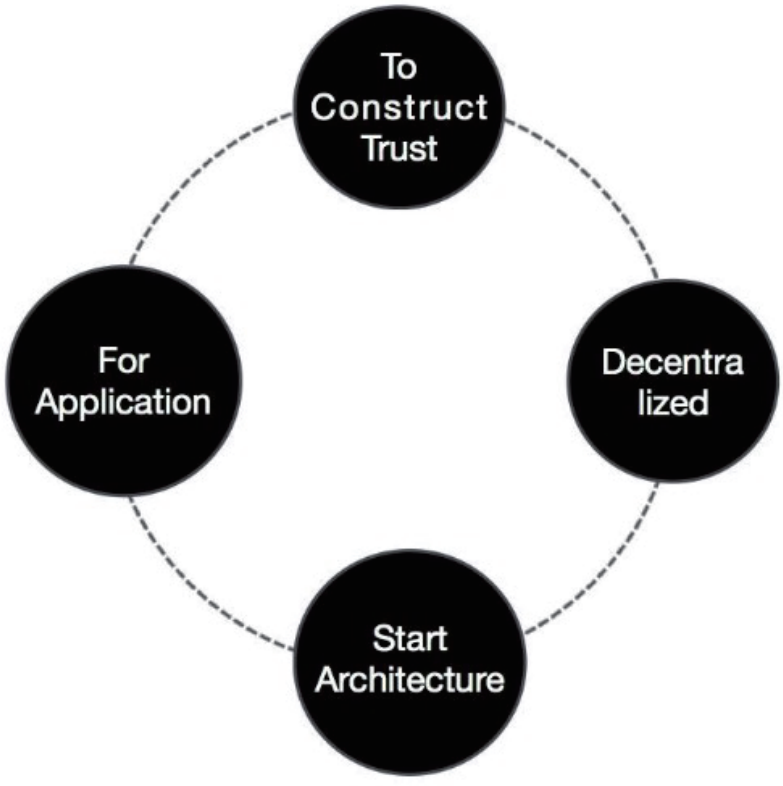
多链间价值：
交换多链系统中通过中继层，可以很方便的交换多个链上的资产，进一步，可以在中继层上部署去中心化的交易所。

支持无缝迁移基于其他链的应用：

我们可以引入其他底层链技术和智能合约技术，以侧链的形式提供给开发者和用户，这样开发者可以很方便的移植已有的应用到NGK.IO生态中。

2.1 系统设计原则

NGK.IO严密的设计逻辑是建立在严格的设计原则与哲学基础上的，区块链系统的鲜明特性与应用需求相冲突，技术方法与现实条件相矛盾，难以调和，系统设计需要遵循完整的因果循环原则，这是建立在一套哲学思想基础上的。



- 构造信任 — 这是区块链的核心使命，系统设计的目的就是为应用构建一个可信任的系统。

- 去中心化 — 是区块链的核心特征，是构造信任的根本手段。

- 开放架构 — 开放是去中心化的必要条件，开放意味人人平等、代码开源、 设施平民化。

- 面向应用 — 开放架构导致平等参与、平等使用，互不信任的参与者需要信任机制保证。

2.2 哲学思想

根据上述设计原则构建系统，面临一个无法调和的矛盾：去中心化、可扩展性、可靠性三者不可兼得，去中心化而又可扩展，则系统不可靠；可扩展而又可靠则无法去中心化；去中心化而又可靠则不可扩展。

要解决这一矛盾，需要一套可行的哲学理论，我们归纳出四项哲学原则：

- 信任源于非信任—区块链系统值得信任，但参与节点互不信任；

- 可扩展的不可扩展性—可信任的去中心化系统不可扩展，但局部节点可扩展；

- 无裁决权的中心化非中心化 — 扩展局部节点形成中心化，若将裁决权上交变成去中心化；

- 可靠的不可靠性 — 非中心化的局部中心节点不可靠，但去中心化的裁决机制是可靠的。

三

NGK.IO
使命与愿景

NGK.IO的使命是搭建数字商业最坚固、强大的基础设施，为商用数字社会提供完备的去中心化解决方案，普及区块链技术在各行各业的应用，打通区块链金融领域，引领新时代的变革。

NGK.IO将打造强大的P2P生态体系，构建一个去中心化的商业生态圈。现行的数字资产并没有实现真正的商用落地，NGK.IO希望通过打通数字资产与商业的价值对接，连接各行各业，以平台通证NGK.IO作为平台上

无障碍使用的通证，具备金融支付功能，公开、透明、去中心化。

NGK.IO通证将强大的线下商业应用场景与高效的区块链互联网金融完美结合，将搭建起数字货币和法定货币之间的桥梁，未来将实现NGK.IO智能合约模拟中央银行增加或者缩紧货币供应以保持币价的相对稳定产生的算法型稳定币USDN以打造全球数字通证结算网络体系。为广大用户、商户提供更具效率、更富有价值的智慧服务，助力通证经济撬动实体产业转型升级，最终使数字经济服务于各行各业，加速数字经济循环和产业流通。

四

NGK.IO
架构设计

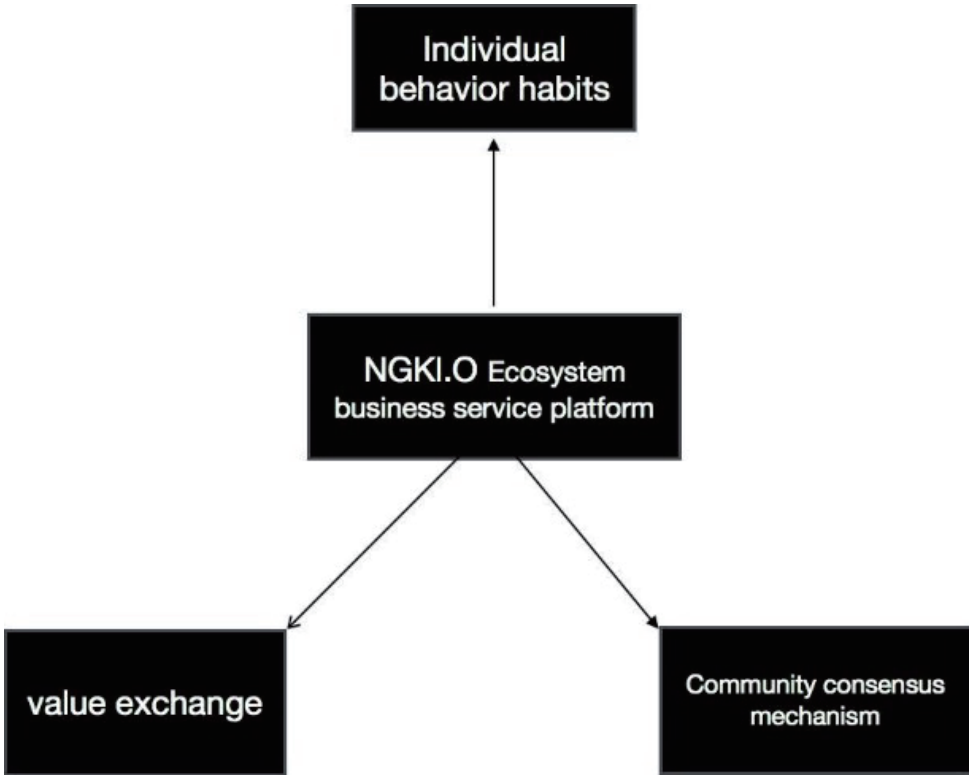
经过市场调研和分析，我们发现区块链发展过程中存在一些问题，区块链技术人才稀缺、研发成本高昂的状况，在短时间内都不可能缓解；越来越多的应用场景需要区块链技术的支撑；现有区块链性能受限，不同链之间无法通信；机构会倾向使用联盟链、私有链，而二者去信任不完全。NGK.IO可为此提供一个可靠的架构解决方案。

灵活易用的区块链基础设施

NGK.IO为开发者和用户提供完整的基于图灵完备的模块化开发。开发者和用户无需研究密码学、共识机制、存储方式等底层技术细节，使用简单快捷的可编程环境直接对接商业应用，从而降低区块链商用成本。

适配海量的区块链应用场景

在应用层面，可以预期区块链将作为机构甚至个人在工作、生活多方面的底层基础支持，NGK.IO通过模块化、多链并行、智能合约等运行机制，为应对未来各种各样的应用场景和区块链底层的不同需求提供支撑。



高性能驱动区块链商用落地

商业应用对性能的要求极高，NGK.IO致力于解决现有区块链的性能受限问题，采用平行扩展技术，通过“主链+子链”多链并行的运行机制，分离主链和子链的业务，以满足百万级TPS需求。

数据透明与商业保密的平衡

对于机构而言，数据保密性和安全性极其重要，而区块链的公开透明特性却让机构有所顾虑。NGK.IO通过数据隔离和跨链审计的方式，让子链的业务数据保密性和安全性得到保障，解决数据透明与商业保密的平衡问题。

NGK.IO集商业与金融于一体的区块链系统，其底层架构是一个完全分布式的网络。NGK.IO团队经过不断反复辨证探讨，最终设计当前最为先进的DPOSS模式的激励机制和权益价值保障–黑洞机制。

NGK.IO以“区块链技术+”的形式改变传统产业格局的一项去中心化理念，打造更加公平，公正的商业体系，重构商业生态场景。NGK.IO以区块链不可篡改，去中心化，高度自治等特性，运用在构建传统商业及金融体系的数字虚拟星球之中，以NGK.IO数字钱包为入口，以创新的DAPP 生态为导流方向，采用开放的 SDK 接口，完全去中心化，将传统领域商业线上转型，更多的方便快捷的实现无缝对接接入，构建同全新数字金融生态，实现金融科技的跨越式发展。

五大分层结构：

1 P2P 网络层：这个层定义了基础的p2p协议。

2 区块链层：该层处理与区块链操作相关的所有操作，如共识，数据访问等。

3 交易（TX）层：该层处理TX请求和回复。它还处理控制类TX请求，并在必要时调用与智能合约相关的操作。

4 智能合约层：该层执行虚拟机内的智能合约执行，并保持临时合同状态。

5 API 层：API 用于处理终端用户输入并获取下层的输出及返回。

五

NGK.IO 公链

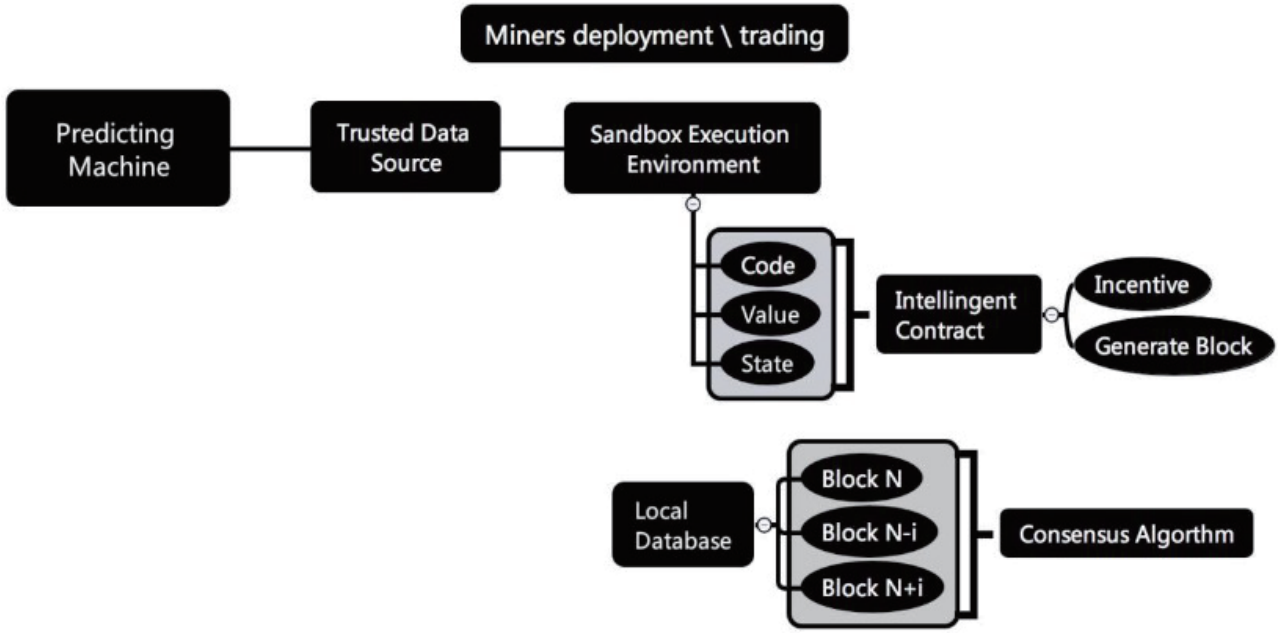
5.1 NGK.IO Token 钱包

NGK.IO技术团队在NGK.IO基础系统正式上线时同步为用户提供基于NGK.IO主网钱包，包括转账、资源质押赎回、资产、私钥管理等基础功能。NGK.IO主网钱包是一个具有完整区块链生态的链上钱包，去中心化链上点对点、去中心化点对点通讯、跨链储存和交易，包括NGK、USDN等数字货币平台的所有数字货币。

投资者转账时可以将交易的所有数字资产完全控制在自己的钱包中，将资产和资金储存于任何第三方，体现真正的区块链去中心化和匿名性，更加贴近区块链定义的原始形态，具有匿名性，不可篡改，不可逆的特性。从安全角度而言，只要用户保存好私钥，就可以确保自己的钱包安全。同时NGK.IO主网钱包可以降低普通用户接触了解区块链的门槛， 作为区块链世界的窗口。

5.2 智能合约运行

本项目的权益通证NGK将会在基于NGK.IO主链上通过智能合约发行，NGK所有的交易数据皆可在NGK.IO网络上查询到，从而保证NGK.IO所有数据做到公开透明。平台内的所有核心功能，包括挖矿、支付、质押、解锁等交易行为全部基于NGK智能合约执行，所以会消耗NGK.IO账户 CPU、NET以及RAM。



智能合约的运行机制

智能合约的运行机制

NGK.IO模型一方面囊括智能合约全生命周期中的关键技术，另一方面对智能合约技术体系中的关键要素进行划分，体现智能合约核心的研究方向和发展趋势，为智能合约研究体系的建立与完善提供参考，奠定基础。

智能合约的生命周期根据其运行机制可概括为学习、协商、开发、部署、运维和自毁六个阶段，其中开发阶段包括合约上链前的合约测试，学习阶段包括智能合约的运行反馈与合约更新等。模型自底向上由基础设施层、合约层、运维层、智能层、表现层和应用层组成。

NGK.IO在智能合约的治理上增加了黑名单和白名单，开发者的智能合约可以通过官网进行提交专业评测，通过专业评测可获得技术合约认证，而存在问题的智能合约也将可能被投票至黑名单，以此来保障主网不受合约漏洞的困扰。

5.3 黑洞销毁机制

NGK Token 所有的销毁都将通过系统独特设计的黑洞机制来执行。

NGK黑洞公钥为 ：

NGK1111111111111111111111111111111114T1Anm

原始NGK.IO主网络创建块的生产者使用的公钥。世界上没有人有与这个

公钥对应的私钥。黑洞意味着只有可以进入而不能离开，这是目前最安全的解决方案。与以太网相比，在合约中有一些可以留下“后门”的功能，它可以被开发来控制合约数据和其他行为。NGK.IO在系统中真正实现了公平、安全和透明。

六

令牌
发行机制

6.1 Token 种类

NGK.IO中TOKEN分为3个大类即NGK原生代币、算法型稳定币USDN、开发者创建的 Token；

1 **NGK 原生代币**
NGK.IO平台上主要的原生代币，用于超级节点出块奖励与候选节点投票奖励、交易手续费，侧链索引费、质押投票等；

2 **算法型稳定币**

USDN智能合约模拟中央银行增加或者缩紧货币供应以保持币价的相对稳定产生的算法型稳定币USDN；

3 **开发者创建的 Token**

在 NGK.IO 平台上，开发者可以创建 Token，构建 自己的 Token 模型及激励机制同状态。

6.2 发行计划

NGK.IO 系统原生代币

发行总量：10 亿枚

预挖量：0.6 亿 （0.1 亿用于分配初始资源）

挖矿量：9.4 亿

每年释放量：1.5 亿

黑洞燃烧 / 利润回购

算法型稳定币：USDN

发行总量：无限制

算法实现：债券凭证机制，增发/销毁

认筹奖励：认筹 1USDN 可获得 1 股权指数（1：1）

奖励限定：前 1–5000 万认筹 USDN

6.3 算法性稳定币 USDN

USDN 智能合约稳定算法有三种机制；

USDN 流通货币：可以进行自由交易的数字货币

USDN 债券凭证：用于增发和销毁USDN 的凭证

USDN 股权指数：用于增发 USDN，奖励股权指数持有人算法稳定币的诉求同样是遵循规则胜于自由裁量。相比于 Grin 和比特币，USDN 算法型稳定币的改进之处在于采用了核心算法的响应式，而非单一固定的规则。比如根据货币的市价调整货币的供给，反过来影响货币的预期价格。智能合约算法型稳定币将 USDN 锚定美元价值，1USDN = 1美元，当稳定币的价格高于一美元时，系统会给债券的持有者发放 USDN，来增加稳定币的供给，以平复价格到一美元左右。当稳定的价格低于一美元时，系统会发行新的债券，从市场上回购 USDN，减少 USDN 的流通总量，将价格推动回一美元附近。

如果兑付完市场所有的债券凭证，仍然需要进行增发，系统会按照智能合约将需要增发的 USDN 流通货币全部奖励给 USDN 股权指数的持有者，将按照持有 USDN 股权指数的比例来进行分配。

6.3.1 算法货币政策

为了维持价格平价，算法支持的稳定币试图通过货币政策控制其货币供应量。通过扩大和收缩市场上可用的稳定币供应来做到这一点。例如，

如果稳定币的价格过高，则稳定币协议的算法将铸造新币并将其引入市场 – 增加供应直至价格平价。如果价格太低，该算法将通过以折扣价出售债券来买入市场上的稳定币。这些债券使其持有人有权在未来日期获得一个 USDN 的单位 – 激励稳定币持有者出售其稳定币获得债券凭证，并减少总供应量直至价格平价。

6.3.2 费雪方程式

被人们奉为金科玉律的费雪方程式为传统金融货币市场提供很大的价值意义，NGK.IO基于算法稳定的数字货币政策将采用费雪方程式的理论作为其支撑基础。

方程式的主体公式：MV = PQ（1）
式中，M为货币需求量，为货币流通速度，P为总体商品价格，Q为商品交易量。

对公式（1）两边取对数并微分可得：
M/=Y/+P/–V/（2）其中，“/”代表增长率。
货币流通速度V是一个制度变量，在短期内变化很小，可以假定V/ =0。

由于在现实生活中，交易量Q不易被及时、准确地统计到，因此后人就用国民收入Y来代替Q，这就可得到M/=Y/+P/。也就是说，在假定货币流通速度稳定的条件下，货币供应量的增长率应等于经济增长率与通货膨胀率之和。当货币供应量增长率不等于经济增长率与通货膨胀率之和时，其差额即为超额货币，即超额货币EM= M/–Y/–P/。

BANCOR 算法计算公式如下：

CW = Balance / TotalValue = Connector Balance / Smart Token's Value;

TotalValue = Price * Supply = Smart Token's Price * Smart Token's Supply ;

Price = Balance / (Supply * CW) = Connector Balance / (Smart Token's Supply * Connector Weight)

计算公式涉及多个参数，名词说明：

Token的供应量【Smart Token's Supply】，简称Supply；

Token的价格【Smart Token's Price 】，简称Price；

Token的总市值【Smart Token's Total Value】，简称TotalValue；

储备金余额【Connector Balance】，简称Balance；

储备金固定比率【Connector Weight】，简称CW。

6.3.3 实现规则

NGK.IO 推出算法型USDN稳定代币，USDN 持有者充当做市商，当它的价格跌到1美元以下时，买入更多的代币；当它的价格超过1美元时卖出。当做市商无法弥补价差时，一个算法缓冲区就会启动，自动买卖储备资产，使USDN更接近1美元的价值。通过在需要时自动购买和出售代币，USDN的供应量理论上可以扩大并缩小来实现目标。这些自动转换

6.3.4 增发与销毁机制

USDN 会通过协议算法，根据代币汇率变化（如USDN 兑美元汇率的变化）来计算并调整 USDN 的代币供应量。如果 USDN 的交易价格高于 1 美元，那么区块链就会创造并分发新的USDN。

稳定币USDN抛弃了抵押模型，而是把现实生活中的央行的货币调控机制移植过来通过算法来实现。

当稳定币需求上升导致其价格大于锚定的法币（E>1），就增发稳定币；

当稳定币需求下降导致其价格小于锚定的法币（E<1），就销毁稳定币；

七

NGK.IO 的技术特点

在企业级区块链解决方案中，单个区块链的并发处理的能力主要受制于共识算法。实际的联盟链应用中，绝大部分时间里，各节点间网络状况是良好的，节点故障或者是拜占庭节点的概率小，这样在绝大部分时间里，只需要解决多个节点数据一致性，高效完成交易即可。只要在发现有节点故障或者欺诈的时候，能够自动切换到具有拜占庭容错的算法就可以保证业务顺利进行。NGK.IO区块链提供的自适应的区块链共识算法，在网络状况良好、无节点故障或者欺诈的情况下处理效率很高，并

且可以准确检测节点故障或者节点欺诈；当检测到 节点故障或者欺诈，系统自动启用拜占庭容错的算法特性，保证容错节点在小于 1/3 总节点数的情况下，系统正常运转；当所有坏节点修复或者拜占庭容错节点解决之后，所有节点数据能全一致的时候，自动切回到高效的算法上。自适应算法很好保证联盟链绝大部分时间内高效的并发处理，并且精准处理了节点错误的问题。

在“自主创新、安全高效、开放分享”的设计原则下，NGK.IO区块链打造的企业级基础设施服务，具有如下特点：高性能、高安全性、高速接入、高效运营：高性能：5000+TPS，3 秒出块

NGK.IO区块链采用高效自适应的共识算法，保证了共识完成即交易确认，并且对交易确认过程中的其他环节，如签名算法、账本存储方式等进行了优化，实现了秒级确认交易。通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，NGK.IO将以实现秒级的快速交易验证。满足绝大部分区块链商业应用场景的用户体验。

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，NGK.IO的处理性会进一步大幅提高交易吞吐量，目前NGK.IO支付海量并发，交易支持秒级确认；提供海量数据存储，具备每秒万级的处理能力；闪电交易速度，在发起交易请求后，通过广播1.5秒

即可完成交易确认股权证明的交易。NGK.IO系统需要每一个交易包含最近一个区块头的哈希值。这个哈希值有两个目的：

A　防止不包含内存块引用的交易在分叉时重放发生；

B　通知网络对应的用户和他们的股分当前在某个具体的分叉上；

低门坎：0 成本创建，资源可使用

为保证NGK.IO系统的快速发展，降低用户使用门坎，系统采用账户初始资源机制，用户可以低成本甚至0成本创建账户，同时为每个账户分配免费的初始资源，来满足用户日常的转账操作，用户将无需再担心由于资源不足造成的糟糕用户的体验。

低消耗：交易成本低

NGK.IO区块链实现了可视化的服务交付和可视化的服务度量。在服务交付方面，从代码编译、测试、灰度环境验收到正式环境部署，整个服务交付流程实现可视化管理。在服务度量方面，对数据进行了标准化的分层归类，从基础设施、上层组件、应用服务、到用户侧，基于应用的拓扑架构，收集各类指标，统一到一个分析平台中展现。NGK.IO区块链提供通用高效的信息采集组件，部署在业务层、共识节点层以及账本存储层，信息采集组件把机器的系统信息（如CPU，内存、硬盘、网络等状态）、节点使用状态（如节点访问量、访问时耗、节点健康状态等）以及业务使用情况（业务访问量、成功率、耗时分布等）实时展示到监控界面上，便于整个系统的管理。

不同于BTC和ETH，NGK.IO转账几乎“免费”。转账过程中会消耗一定网络带宽资源（NET）、CPU计算资源(CPU)。但NET和CPU都是可再生资源，用户可以通过抵押NGK的方式获得，账号信息、智能合约执行信息存储需要消耗运行内存资源（RAM）,RAM是稀缺资源，需要购买，所以说NGK.IO转账是免费的，但是还是需要消耗NGK购买的RAM。

智能合约

基于NGK.IO系统块链使用的是 WebAssembly（http://webassembly–.org/）（WASM）来执行用户编写的智能合约，只支持C/C++语言。WASM是一种新兴的Web标准，广泛应用于Google、Microsoft、Apple 等。同时NGK.IO 提供专用的API 函数，提供了更强大的类型安全并降低了智能合约开发难度。智能合约定于了NGK.IO系统与外部进行交互的相关界面并实现界面功能，用户通过智能合约提供的界面与合约进行交互。开发者可以决定用户可执行的操作以及可以调用相应程序来处理用户的请求。

数据存储

区块链复式的记账模式，在系统不断的运用，积累了大量的数据，造成运行速度下降，NGK.IO将会实现分离存储、分表存储机制，实现数据海量存储。每一个智能合约都拥有独立的数据库，同时支持新建数据库表以及对数据的增删改查。多索引API:Multi_index为NGK.IO系统数据库提供C++界面。多索引反复运算器：多索引表中对象数据的查询。同时所有DAPP开发团队需要承担数据存储的运行成本，用户将不用支付程序

支付程序运行费用。

基于分布式数据的建设及沉淀，链上数据将是NGK.IO上最珍贵的资产，分布式数据的应用将打破传统的数据应用机制，链上数据将是最真实，最可靠的数据，同时数据的隐私级别更高，更强，调用分布式数据应用，将经过用户直接授权后方可使用，NGK.IO未来将不断的创新，以算法产品为重点，更好的服务于NGK.IO用户，实现分布式数据的高效应用。

未来数据将不再是垄断寡头的专属，数据将回归用户自身，这也是NGK.IO构建高度自治，公平，公开，公正的信仰，NGK.IO的信仰也是全世界每一个人的信仰，繁荣的生态离不开每一个支持NGK.IO的用户，相信这一天一定不会很久。

节点API

丰富的应用开发框架和灵活的部署方式，方便不同类型的用户快速接入，构建应用；侧链超级节点将会为开发者、钱包提供全球范围内的节点服务，包括 API Node、History Node、Peer Node。

- API Node：支持发送交易，查询帐户，查询合约数据库等操作。
- History Node：支持查询帐户交易记录，合约历史记录等操作。
- Peer Node：用于节点之间的数据同步。

跨链通信

所有跨链交易完全在去中心化环境中完成，初始化初始内存块信息后，通过NGK.IO智能合约可以完全自主验证后续所有内存块的有效性，无需依赖对中继或者合约外部信息的信任。急速确认，跨链交易从发起到对应链上产生交易 对仅需要 3 分钟即可。交易并行，不同的跨链交易完全独立执行，互不干扰。安全，由于采用了生产者签名校验和严格的逻辑检查保证交易不会被恶意攻击，安全的验证交易的真实性。

高安全性

安全第一，去中心化是灵魂。比特币部分解决了双重支付问题，但仍然面临51%攻击（实现双重支付）的风险，政府或大财团要实施攻击并不难。NGK.IO的透明锻造机制和超级节点可以抵御90%攻击，可以认为杜绝了双重支付的可能，收购 90%的币在现实中不可行，即使政府在收购之后也会失去攻击的动机。

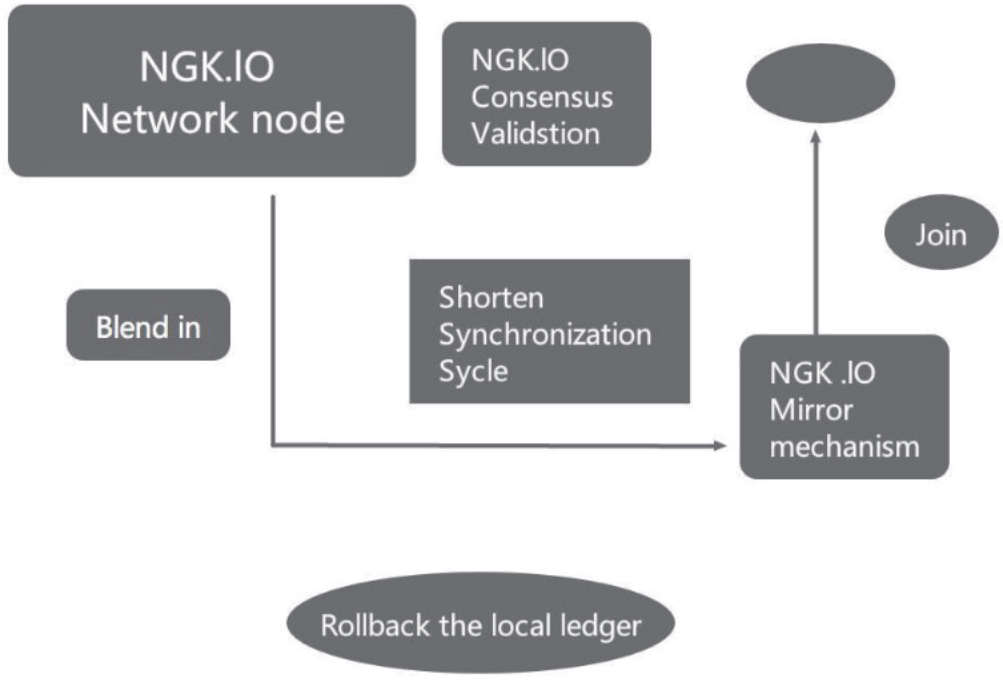
NGK.IO为此提供丰富的权限策略、安全的密钥管理体系和用户隐私保密方案，保障数据安全。NGK.IO区块链通过非对称加密的数字签名保证业务请求在传输过程中不能被篡改，通过共识机制保证各节点的数据一致的存储。对于已经存储的数据记录通过节点内的自校验性和准实时多节点数据校验来保证已经存储的数据记录不能被修改。

节点的自校验性：NGK.IO区块链采用块链结构存储数据记录，其中部分记录的修改会破坏块链结构的完整性，可以快速校验出来并从其他节点

将数据恢复。另外NGK.IO区块链每个记账节点都有自己的私钥，每个区块头中包含了本节点私钥的签名，区块内数据的修改都可以通过签名校验出来。 多节点准实时的数据校验：当节点的私钥被盗取，恶意用户是存在修改账本链上所有数据的可能性的，NGK.IO区块链提供了多节点间准实时的数据对比机制，可以及时发现某个节点账本数据被篡改的情况。

节点数据快速同步

NGK.IO将会研发镜像机制，可以定期对本地账本制作镜像，实现便利的回滚机制（特指本地账本），在统一共识下，可以指定镜像标签进行回滚;同时，缩短新加节点加入运转的周期，仅需同步最新镜像及少量近期交易集合，即可融入网络并参与共识验证。



高拓展性

NGK.IO的区块链结构，能够满足不同业务领域的需求，提高系统的可扩展能力和维护效率。即可用于标记资产和资产转移，也可提供不可篡改的多维事件记录，NGK.IO公链期望通过跨链可以为不同的消费场景形成价值的互通，为全球区块链商业化进程做出一定的技术力量。

未来随着用户交易数的增多，不可避免的会带来区块链数据膨胀的问题。科扩展性解决的是如何尽可能高效的存储不可篡改的区块链数据，NGK.IO的解决方案是：

1　从交易层把部分交易迁移到子区块链上运行。比如说侧链、闪电网络等等。

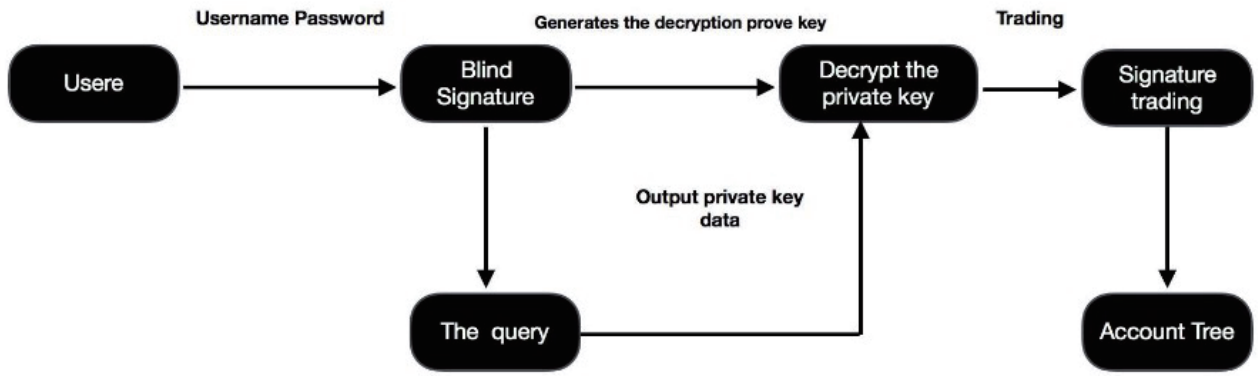
2　从减少存储上着手解决。将原始数据进行裁剪分片，研究更安全的客户端，只存储非全量验证数据就可以正常工作。

最终性

比特币与以太坊，有一个最大的问题就是没有一个确定的不可更改的最终状态。理论是，如果有足够的算力，足够的出块速度，产生一条更长的隐藏链，就可以把之前的区块推翻。NGK.IO内置图灵完备的编程语言平台经过见证人发布见证区块后，就已是最终确定的状态，无法推翻。

安全私钥存取方案

为了方便用户使用NGK.IO服务，除了传统的客户端生成和保存的机制，NGK.IO还提供网络托管存取和私钥硬件存取(U-key)两种方案。网络托管存取，即把用户名和密码通过特定算法映射成私钥并在服务端进行存储。服务器端存储的私钥均为加密数据，私钥仅能在用户端解密；硬件私钥是为了满足金融行业及物联网行业的使用需求。



多重隐私保护方案

提供多重隐私保护功能。首先，NGK.IO底层提供同态加密方式，用户所有数据均加密存储，仅用户本身可见。并提供加密中间件服务，用户可根据业务需要进行选择。最后，上层应用可以在录入时对数据进行加密处理，NGK.IO平台负责对用户生成的加密数据进行写入和读取。

联盟链低成本接入方式

面向商用用户可自主搭建联盟链形态提供多种业务场景的 API 接口，如:资产、 溯源、存证等，供这些场景相关的业务直接使用。在新的业务场

景下，NGK.IO可以基于现有的框架为用户快速定制接口，满足业务功能需求。同时提供已封装的支持多种主流开发语言(JAVA、C++、node-js、PHP)的 SDK 软件开发包。

目前NGK.IO技术服务主要有两种:一种是搭建一套NGK.IO底层，提供一套标准化的API并开放，然后由开发者自己对接应用；另外一种是配合上层应用解决一些行业痛点，将分布式账本内嵌到已有的应用系统中。

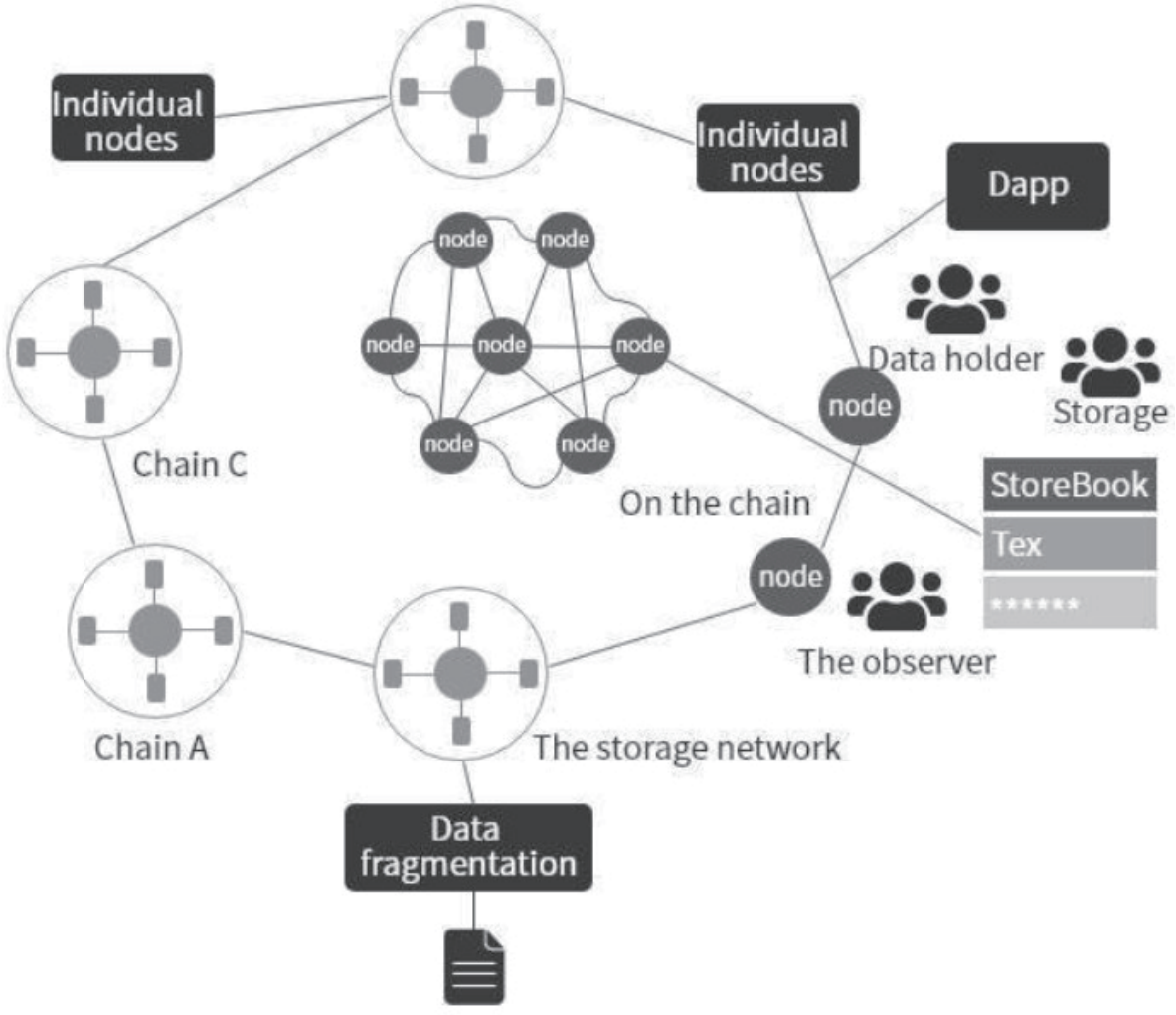
NGK.IO作为商业应用公链技术形态可以不断的满足业务需求，逐步迈向成熟，所以我们通过对底层分布式账本的封装，降低上层应用使用的门槛，在对接和使用的过程中，不断地优化和完善底层分布式账本和共识算法，使之更加贴近商用诉求。

八

NGK.IO
改进分布式储存系统

作为一个可以任意运行智能合约的平台，NGK.IO改进分布式储存系统为支持商业环境高并发和网络存储需求，选用IPFS为其存储基础架构。IPFS的网络提供了动态的、细粒度的、分布式的网络存储支撑，可以更好地适应商 业高频分发网络（CDN）的要求。NGK.IO 大文件会被切分成小的加密分块，下载的时候可以从多个服务器同时获取。在对象层和文件层，大部分数据对象都是以MerkleDAG的结构存在，并具备双重哈

希去重，能够灵活支持内容寻址和去重存储。



在此基础上，NGK.IO提供了一系列应用框架，包括分布式数据交换协议、分布式流程管理协议等，使用通用的API、SDK以及各种应用功能组件，实现开发部署的便捷化，支持DAPP产品敏捷开发。

NGK.IO这种高度封装化的分布式账本架构、快速地支持大量并发进程的存储结构，使得NGK.IO具备了应对商业复杂应用场景需求的能力。

九

NGK.IO
核心技术优势

9.1 抗量子攻击密码算法

随着量子计算机技术的发展和量子霸权的实现，通用量子计算机不再是理论上可望而不可及的圣杯，并将在可预见的未来带来一系列深刻的变化。基于大数分解和离散对数问题的非对称密码体制的崩塌是这一转换中最突出的特征之一。NGK.IO目前使用的ECDSA签名算法也难以逃脱。因此，我们将引入一种新的反量子加密系统来应对上述挑战。

在众多的抗量子密码系统中，NGK.IO 引入 NTRU(包括加密和签名)作为主要的加密系统。FrodoKEM系统和Sphincs作为备份密码。考虑到加密系统在理论上还不完善，并且处于国际后量子密码标准定制阶段，NGK.IO将保持各种密码方案的可扩展性。同时，基于加密签名系统还可以方便地构造量子安全的匿名硬币，保持了NGK.IO最大的可扩展性，同时在早期阶段保持对多密码系统的支持，也最大限度地减少了某个密码系统崩溃带来的不可逆结果。

9.2 独创的匿名P2P通信网络

在匿名交易层面，NGK.IO系统结合传统加密虚拟货币的特性，通过零知识证明和环签名，设计了效率更高和安全性极好的交易匿名和隐私保护方法，满足不同应用场景隐私保护需求！NGK.IO系统设计实现了节点匿名接入实现的方法，并采用私有加密的通信协议，极大地增强了底层通信网络中节点的匿名性， 确保子节点间通信难以被追踪和破解。

9.3 虚拟机独立架构

在合约层 NGK.IO 通过开放 RPC（Remote Procedure Call 远程过程调用）接口来使虚拟机与NGK.IO进行集成，并且脚本语言和虚拟机的实现将独立于NGK.IO操作系统技术，任何开发语言或虚拟机只要有适当的、性能足够的沙箱都可以通过RPC与NGK.IO集成在一起。并且NGK.IO目前已经可以支持Wren、WASM、EVM三种虚拟机，因此以太坊上的应用可以通过简单的修改就能直接移植到NGK.IO系统中，实现多链之间的

互通，对于应用开发可以实 现更简单的系统嫁接与转化。

9.4 简化应用构建技术

NGK.IO针对技术开发者支持动态加载相关组件，实现了应用层的业务逻辑和区块链底层实现的解耦，同时为应用开发者提供友好的API接口，比较重要的有以下几个插件： chain_plugin 、 http_plugin net_plugin 、 producer_plugin。这样的工具组件又极大的降低了开发人员的技术门槛，使得在NGK.IO上开发自己的去中心化应用成为一项比较简单的工程。

9.5 石墨烯技术

NGK.IO引入石墨烯技术Graphene（石墨烯）使用区块链来记录参与者的转账信息及市场行为。由于每个区块总是指向前一个区块，因此一个区块链条包含了所有在网络上发生的交易信息。区块链是一个公开的、可审计的账簿，每个人都能够查看详细数据，并验证交易、市场订单和买卖盘数据。Graphene（石墨烯）旨在实现一种区块链技术或协议。当其与具体的区块链整合后，其本身逐渐进化为一种生态系统。

转账速度特别快。现在的平均确认时间是 1.5 秒，出块时间是3秒，在石墨烯进一步进化的NGK.IO上可能到了零点几秒，所有的延迟仅仅只是来源于网络，而不是处理本身，所以它的性能是非常强大的。我们对比一下：比特币是10分钟出块，以太坊大约是1分钟；确认时间上比特币是

1小时，以太坊是十几分钟，基于石墨烯技术的NGK.IO只需要秒级的时间。

吞吐量比较高。石墨烯的吞吐量现在实测大约是3300笔每秒，理论上可以到 10 万次，甚至可以扩展到百万次，比如按照 NGK.IO 的规划就可以达到百万次。对比一下：比特币大约每秒七笔，以太坊每秒三四十笔，这完全不是一个数量级。在真正解决实际问题时，很明显每秒几笔是不符合要求的，那每秒3000多笔基本上已经超过了VISA的处理能力，已经算一个工业级的区块链产品。

- 石墨烯极其稳定。石墨烯技术开发运行已久，从来没有出过明显的BUG，也没有资产被盗的情况。

- 功能非常强大、完备、容易操作。NGK.IO引入石墨烯上的多重签名功能是可以用作公司治理的，它可以设定两个参数：首先它可以设置百分比，每个人占多少百分比，无论多少人都可以随便设。第二个是阈值，就是超过多少个签名就可以生效。

9.6 跨链技术

NGK.IO跨链技术应用于跨链资产转移、跨链原子交易、跨链数据共享、跨链 合约执行以及去中心化交易所等广泛场景，NGK.IO引入侧链/ 中继（Sidechains / Relays）技术，侧链是一种锚定原链的链结构，但并不是原链的分叉，而是从原链的数据流上提取特定的信息，组成一种新的链结构，而中继则是跨链信息交互和传递的渠道。不论是侧链还是中

继，作用都是从原链采集数据，扮演着listener的角色。侧链和原链不能直接验证对方块的状态，因为这样会形成循环，但相互只包含轻节点是可行的，相应的验证逻辑可由链协议本身或应用合约实现。一般来说，主链不知道侧链的存在，而侧链必须要知道主链的存在。

十

NGK.IO 共识算法

10.1 BFT-DPoSS 共识机制

NGK.IO采用了BFT-DPoSS(Delegated proof of stake&service)共识算法，基于原有DPOS算法的基础上进行提升，在传统DPOS算法中超级节点并没有赋予更多应有的职责和义务，很大程度的阻碍了生态的发展，而在DPOSS算法将超级节点权力进行下放，让DAPP开发者来担当，一方面可以激发开发者的积极性，另一方面推动了DAPP生态发展，更符

合内存区块链共享、共治的去中心化管理理念。

DPOSS共识机制的目标是让只有提供实际“服务”的DAPP才能成为生产节点（BPS）。DPOSS结合了公链的共享治理特点，又结合了联盟链信任特点，加上DAPP生态服务者为主链生态赋能，三大特征完美结合。

DPOSS从而达到了500毫秒的出块间隔。该机制的具体过程是：NGK.IO的持有者通过投票系统对各个超级节点竞选者进行投票，选出21个节点为超级节点。然后这21个超级节点以自身的网络资源状况商议出一个出块权拥有顺序，在每个超级节点拥有出块权时，以间隔为500毫秒（500毫秒是NGK.IO团队通过大量实验测试得出的当前网络状态下可达到的最小的稳定状态下的出块间隔）连续产生12个新区块，然后切换到下一个超级节点连续产生之后的 12 个区块。

该方式可以保证一个超级节点可以连续以 500 毫秒的间隔产生区块，因为在同一超级节点产生新区块时不受当前网络状况的影响，但由于网络的延迟很难使得其他节点对已经产生的区块进行确认，使其成为不可逆区块。

同时NGK.IO引入了BFT协议，当超级节点A产生第一个新区块后，A将该区块进行签名并广播给其他超级节点，其他超级节点对该区块进行验证后对其进行签名并返回给A节点，当A节点收到来自14个不同节点签名的区块后，该区块就成为不可逆区块串联到之前的区块链中（以500毫秒产生新区块的过程和对区块进行BFT协议共识的过程在超级节点中是

同时进行的，即确认过程不影响超级节点产生新的区块）。

NGK.IO团队通过大量实验测试，在当前的网络状况下，一个超级节点广播一个新区块并确认的过程可在1秒的时间内完成。因此，每个新区块的产生到成为不可逆区块最多需要1.5秒的时间，这就使得跨链通信的时延大大缩小。上述过程虽然可以保证同一超级节点产生新区块时可以达到500毫秒的间隔，但当切换超级节点产生区块时，由于网络延迟使得上一节点产生的最后几个新区块有可能被该超级节点忽略。

为解决此问题，NGK.IO选用了确定顺序的超级节点轮流出块，比如以纽约（美国东海岸）、悉尼（澳大利亚）、渥太华（加拿大）、日本东京、中国北京这样的顺序，该顺序使得上一节点产生的最后区块传播到下一节点时有最小的延迟，从而避免下一个超级节点忽略上一节点产生的区块。如果是随机定义出块权的超级节点，那么在现有的网络条件下，出块间隔只有控制在3秒时才可保证下一节点较大概率上不会忽略上一节点产 生的区块。

使用上述BFT–DPOSS协议就可以使得NGK.IO的出块间隔降低到500毫秒，这也使得跨链通信的时延大大缩短，单位时间内可确认的交易数量大大提升。未来技术层面上支持百万级别用户的量级已不是难题。

DPOSS共识算法具有极强的抗分叉能力，因为区块添加到一条区块链分叉的速率与拥有该共识的超级节点比例是相关的，也就是说，具有较多超级节点的分叉会比拥有较少的那一条分叉增长速率快。任何时候一个

诚实的超级节点看到一条有效的更长链时，都会从当前的分叉切换过来，又由于超级节点数量为奇数个，所以在任何时刻一定会有一条较长的链。当一个超级节点设法在两条分叉上同时生产区块时，NGK.IO的持有者会在下一轮投票中将该超级节点删掉，并且NGK.IO社区会给予相关恶意节点一定的惩罚。

NGK.IO在技术层面上对DPoS中存在的问题进行优化改进，提出投票激励机制配合节点互评两种核心方案来提升社区活跃度，以及及时对恶意节点进行剔除和惩罚，促进系统始终保持高安全和高效率。

10.2 PBFT 检查点协议

NGK.IO引入投票激励机制以及PBFT的检查点协议，针对DPOS共识机制投票的积极性不高和对恶意节点的不能及时有效地处理等问题，提出投票激励机制和检查点协议两种核心方案。通过投票激励机制可以鼓励代币持有者积极投票，选出相对公正的21个超级节点，配合检查点协议，通过 21 个节点间互相检查，做到及时删除恶意节点。

当系统中出现记账节点状态为Exception或Error时，对恶意节点处理效率明显要更高效。

PRE-PREPARE

出块节点出块以后，广播给网络里的所有其他中继节点。

PREPARE

指中继节点收到请求后向全网广播将要对此请求进行执行。

COMMIT

中继节点收到足够多的对同一请求的prepare消息，向全网广播执行此请求。

COMMITTED-LOCAL

中继节点收到足够多对同一请求的commit消息，完成了验证工作。

VIEW CHANGE

出块节点因为各种原因失去其他节点的信任，整个系统更改出块节点的过程。

由于NGK.IO采用了BFT的算法，所有超级节点是通过投票的方式提前确定的，在一轮出块中整个系统的出块顺序是完全不变的。当网络情况良好并且出块节点没有发生改变的时候可以认为不存在view change状态。当引入PBFT后，为了避免分叉导致共识不前进的情况，加入view change机制，抛弃所有未达成共识的块进行replay，不断重试直到继续共识。

Checkpoint

在某一个块高度记录共识证据，以此来提供安全性证明。当足够多的中继节点的 checkpoint 相同时，这个 checkpoint 被认为是 stable 的。

其中生成包括两大类：

1 固定 k 个块生成

2 另一类是特殊的需要提供安全性证明的点，例如出块超级节点排名发生变更的块。

10.3 一致性算法

NGK.IO软件利用唯一已知的分散式一致性算法，该算法被证明能够满足区块链上应用程序的性能要求关于DOPSS。在这种算法下，那些在采用NGK.IO软件的区块链上持有令牌的人可以通过持续的批准投票系统选择区块生产者。任何人都可以选择参与块生产，并有机会生产块，只要他们可以说服代币持有人投票给他们。

NGK.IO软件能够精确的每3秒生成一个块，并且只有一个生产者有权在任何给定的时间点生成一个块。如果在预定时间没有生成块，则跳过该时间段的块。当跳过一个或多个块时，区块链中会出现3秒或更多秒的间隔。

使用NGK.IO 软件，块以126个/轮次（每个生产者6个，21个生产者）生产。在每轮的开始，21个独特的区块生产者优先选择由代币持有者投票。选定的生产者按照15个或更多生产者约定的顺序安排。

如果生产者错过了一个区块，并且在过去24小时内没有产生任何区块，

则他们将被移除，直到他们通知区块链他们打算再次开始生产区块为止。这可以确保网络平稳运行，最大限度地减少由于未被证明不可靠的块生产者而造成的错误数量。

在正常情况下，DPOSS区块链不会遇到任何分叉，因为区块生产者不会竞争，而是合作生产区块。如果有分叉，共识将自动切换到最长的链条。这种方法是有效的，因为块添加到区块链分叉的速率与共享相同共识的区块生产者的百分 比直接相关。换句话说，拥有更多生产者的区块链分支的生长速度要比拥有更少生产者的区块链更快，因为拥有更多生产者的分叉会遇到更少的缺失区块。 此外，没有块生产者能够在两个分叉上同时生产块。这样做的块生产者可能会被投票出局。这种双重制作的密码证据也可用于自动删除滥用者。

通过允许所有生产者签署所有块，拜占庭容错被添加到传统DPOSS中，只要没有生产者签署具有相同时间戳或相同块高度的两个块。一旦15个生产者签署了一个区块，该区块被认为是不可逆转的。任何拜占庭式的生产者都必须通过以相同的时间戳或签名签署两个块来产生他们背叛的密码证据。在这种模式下，不可逆转的共识应该在 1 秒内达成。

NGK.IO系统对于每笔交易都包括最近的区块头的哈希值。

- 防止分叉区块链上出现大量交易记录;
- 使得系统能感知到用户是否在分叉出来的区块链上;

随着时间的推移，所有用户最终直接确认块链，这使得难以伪造假冒链，因为假冒将无法从合法链路迁移交易。

10.4 投票激励机制

由于NGK.IO是DPOSS共识机制，每个NGK.IO持有人都有投票权。作为一个货币持有者，投票是一项非常重要的权利，需要每个投票员珍惜和正确行使。投票不是直接的收益，而是在超级节点选举中，当NGK.IO持有者选择一个足够好和可靠的超级节点来保证NGK.IO网络的稳定运行时；在公投中，对该提案的投票将使社区对特定的NGK.IO生态问题发表意见，甚至改变NGK.IO的主体网络设置和构成，这有利于NGK.IO生态的繁荣和稳定。只有当以上两者都实现了，那么随着NGK.IO的发展，NGK.IO 持有者手中也会升值，这也是间接投票收益。

另外DPoSS共识机制需要从竞选节点中选出21个超级节点来轮流执行区块链的记账和上链等职责，但由于缺乏对投票的激励机制，致使广大代币持有者投票积极性不高，最终导致票选出 21 个节点耗费了大量的时间效率不高。故NGK.IO提出了投票激励机制，以奖励投票的代币持有者，减少票选 21 个节点以及其他去要投票的场景所耗时间，提高效率。

社区发起投票活动时，代币持有者从投票到获得收益需要两个阶段。具体步骤如下：

1　代币持有者进行投票，至投票活动结束时，对投票者是否有资格后

的收益及获得多少收益进行清算。

2 当计算完收益后，投票者并不能立刻收到奖励，需要经过锁定期才能获得奖励。

奖励公式：

以投票选出 21 个节点为例，其中 VOTES 为投票数，与投票者所持代币数量一比一的关系。N为常数，表示此次奖励总数。I只有1和0两个值，表示投票者是否有权获得奖励，例如：投票者所投的竞选节点是否成为最终节点。T与投票者投票的日期相关，投票者投票的日期与社区发起投票的日期相差越大，则T越小。

在PBFT共识算法中存在主节点（primary）和从节点（replica）两种角色。 一次共识中只有一个主节点，其他都为从节点。主节点负责对一段时间内的交易进行验证，通过验证的交易被打包进区块，最后上链。这一概念与NGK.IO的DPOSS 节点的概念类似。在NGK.IO中21个节点轮流获得记账权，获得记账权的节点与PBFT主节点的职责大致相同，其余100个节点也与PBFT从节点的职责类似。在PBFT中，一旦主节点出现问题或为恶，可以立即进行试图切换，但在DPOSS中，却无法及时删除有问题的节点。

故 NGK.IO引入 PBFT 的检查点协议。在 PBFT的检查点协议中，由于拜占庭服务器的存在，一致性协议并不能保证每一台服务器都执行了相同的请求，所以，不同服务器状态可能不一致。因此，设置周期性的检查点协

议，将服务器同步到某一个相同状态。

10.5 超级节点

在分布式数据中心，目前有 300 个候选节点。这些候选节点的参与者通常包括矿池、加密货币兑换、区块链咨询公司和NGK.IO爱好者团队。投票选出的超级节点将根据区块生成顺序(字母顺序)(65139)进行交易，以获得区块生产奖励。除了21个超级节点外，NGK.IO生态中还有49个备选节点。这些备选节点的存在是为了取代一些面临问题或受到干扰的超级节点，以维持系统的稳定性。此外，设置备选节点的另一个用途是权利平衡。首先，如果一个超级节点作恶，其他超级节点可以通过投票取消邪恶节点的状态，而备选节点将始终监控超级节点的行为。如果出现非法行为，备选节点将通过民主手段吸引选票，取代邪恶节点，从而实现民主与监督的作用。

NGK.IO的备选节点随时准备替换现有的超级节点。它们需要确保与超级节点相同的硬件设施，以便节点的替换不会影响NGK.I 网络。

10.6 分布式超级节点选举算法 DSNE

DSNE是分布式算法，选举过程通过节点间的消息传递进行。节点之间的边有可能在选举过程中发生故障而不能通信，所以算法应该考虑到边的容错问题。DSNE是三阶段选举算法，下面分别分析在不同阶段发生边故障的情况。

边在第一阶段发生故障有四种情况：

1 故障边属于生成树，则父节点把这 条边对应的子节点信息删除；子节点从其余邻边中选择最小权重的边，向该边的另一节点发送“Father”消息，请求建立父子关系。

2 故障边属于最小生成树，则该边一定是其中一个节点的最小权重边，这个节点要删除故障树边信息，同时向其余相邻边的最小权重边连接节点发送带有标记<Branch>的空消息，收到此消息的节点记录该树边信息。故障边的另一节点只需要删除故障树边信息。

3 故障边既属于生成树，也属于最小生成树，同时完成以上两种操作。

4 故障边既不属于生成树，也不属于最小生成树，则两个节点只需要把该边信息删除，就不会对后边的选举过程产生影响。

边在第一阶段发生故障有四种情况：

1 故障边属于生成树，它连接着一对父子节点，子节点重新整理自己的消息内容，然后向其余邻边中的最小权重边发送消息，父节点删除该子节点信息，不再等待来自故障边的消息；

2　故障边属于最小生成树，连接边的两个节点分别重新整理自己消息内容，向各自父节点发送消息；

3　故障边既属于生成树，也属于最小生成树，同时完成以上两种操作；

4　故障边既不属于生成树，也不属于最小生成树，连接边的两个节点分别重新整理自己消息内容，向各自父节点发送消息。

边在第一阶段发生故障有两种情况：

1　故障边不属于最小生成树，则不影 响选举结果的广播；

2　故障边属于最小生成树，若父节点没有其他子节点，则沿着它的父节点方向传递故障边对端节点的消息，通知其他节点若和故障节点相邻，可以通过非树边告知选举结果；若故障边的父节点还有其他子节点，则沿着其余子节点方向和其父节点的方向同时传递故障边对端节点的消息，通知其他节点若和故障节点相邻，可以通过非树边告知选举结果。

从通信复杂度和时间复杂度分析选举DSNE算法的性能。算法的第一阶段是一个洪泛的过程，首先假设每个节点向所有邻节点发送选举消息，则每条边传递2个选举消息，因此消息的数量是2m；考虑到节点不会向其父节点发送选举消息，但是要发送“Father”消息，所以加上并减去

（m－1）条消息，因此第一阶段发送的消息数量为2m。第二阶段是从叶子节点沿着生成树逐步向根节点返回消息的过程，消息数量为（n－1）； 第三阶段是根节点沿着最小 生成树发送选举结果，消息数量为（n－1）。因此算法需要的总的消息数量为2m+2（n－1）。假设无向图的网络直径为d，算法的运行需要三个阶段，每个阶段都遍历所有节点，因此算法的时间复杂度上界是 3d。超级节点选举过程也可以看成是求解最小生成树的过程！

假设一个节点聚集可以用连通无向图 G=（V，E，W）表示，V是节点集合，|V|=n，每个节点有唯一的标识，如 IP 地址；E 是边集合，|E|=m；W 是边 的权重集合，权重在这里表示延时，并假设每条边的权重不同。这是一个较强的假设，但是可以通过简单的方法实现，比如GSH[6]中的方法。

除此以外，还假设每个节点知道自己相邻边的权重和相邻节点标识。消息可以独立地在一条边的两个方向上传递，按发送的顺序到达接收方。选举通过节点间的消息传递来实现。

选举过程用到了生成树的概念，因此还涉及到根、父节点、子节点、叶子节点的概念。连通无向图中的边如果属于最小生成树，则称为树边branch，否则称为非树边。最小生成树的子树称为片段。

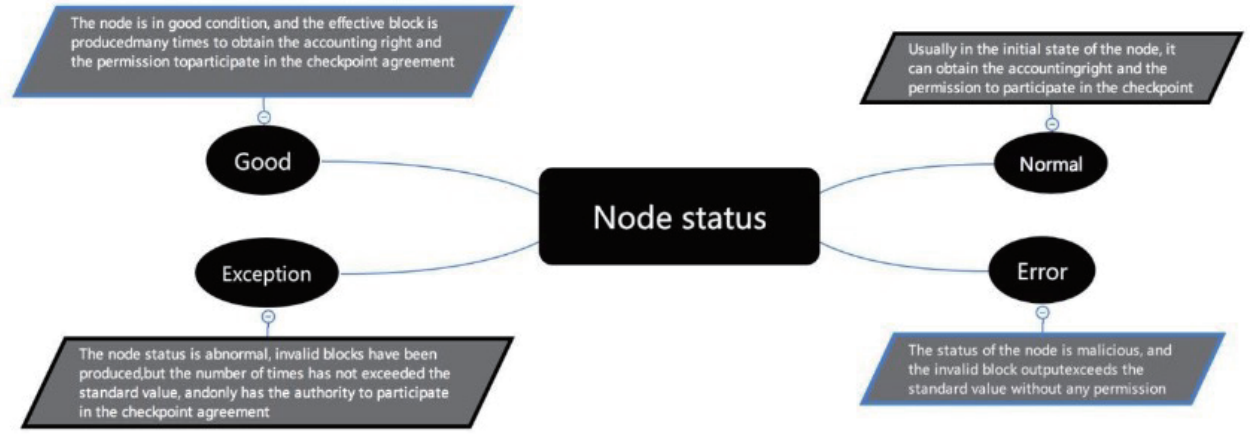
- 定理1MST是连同无向图的最小生成树，则每个节点的最小权重边一定属于MST。

- 证明假设连通无向图共有n个节点，除节点i之外的所有其他节点已经构成片段（MST的子树），那么要构成MST的话，节点i必然要通过其最小权重的邻边连接片段，才得到最小生成树。因此一个节点的最小权重邻边必然属于MST。

10.7 超级节点的重新选择

经过一次完整的选举过程，根节点可以获得所有节点的能力信息，通过排序可以将前N位的节点及其能力排序进行广播，其他节点收到选举结果后，默认能力最强的节点为当前的超级节点。若该节点失效，则默认排序第二的节点作为新的超级节点，依次类推。只有排序前N位的节点同时失效才有必要启动一轮新的选举过程。

10.8 节点四大状态



为了有效防止恶意节点持续地产生无效区块或其他恶意行为，给 21 个节

点都添加一个节点状态，将节点状态定义为4种；成为代理节点后，初始状态为Normal，多次产出有效区块，则状态转换为Good。当代理节点产出无效区块时，不管当前状态是Good或Normal，直接转换为Exception。代理节点若产出无效区块的次数超过标准定值，则节点状态转化为 Error。

10.9 惩罚机制

当代理节点状态转换为Exception时，会限制其权限，此时节点仅有参与检查点协议权限，轮空记账权。下一轮，其状态自动恢复为Normal，产出无效区块的次数累计不清空。

当代理节点的状态转换为Error时，首先节点不具备任何权限，其次会将其作为代理节点时间段内的收益锁定，并将其从代理节点中删除，此后不再具备选代理节点资格。

惩罚机制主要针对的是状态为Error的代理节点，因为其产出无效区块的累计次数超过了标准定值，故可认定其为恶意节点，需对其采取一定的惩罚措施。

十一

NGK.IO
跨链交互机制

11.1 体系内的跨链通讯

NGK.IO把链间通讯作为实现高并发的解决方案，以链间通讯技术构建多条链间的流转通道，通过水平拓展的方式来增加NGK.IO整个生态的承载能力。跨链通讯的本质问题是解决对各个链之间交易可信度的证明。异构的区块链系统（例如EOS、ETH）因为区块生成速度、内部数据结构、共识机制等都有很大差异，因此异构去中心化跨链的实现难度相对

去中心化跨链通信的基础是轻客户端（Light Weight Client）和交易验证技术（SPV/Simple Payment Verification）。轻客户端是由区块头构成的一条链，不包括区块体，所以轻客户端只占用很小的空间；SPV 技术使用 merkle 路径来证明一个交易是否存在于某个区块中。

11.2 NGK.IO Core 采用的跨链方案优势

- **完全去中心**

  轻客户端在智能合约中实现，当初始化了正确的起始区块信息，合约就可以完全自主验证后续所有区块的有效性，无需依赖对中继或合约外部信息的信任。

- **轻量**

  轻客户端无需连续同步原链所有区块头，只根据需要同步区块链的一部分片段即可获得可信区块用于验证交易。

- **快速的跨链交易**

  一个跨链交易从产生到在目标链上产生对应交易只需要不到3分钟时间。

- **跨链交易并行**

  不同的跨链交易之间互不影响，可以并行执行，因此支持很大的并发量。

- **安全**

  由于采用了生产者签名效验和严格的逻辑检查，可以保证轻客户端自身的正确性，无法被恶意攻击，因此可以安全的验证交易的真实性。

- NGK.IO主链的兑换通道，将实现NGK.IO可以十分方便的在“NGK.IO”侧链和 NGK.IO 主链之间流通，包括 NGK.IO上面的其他优质数字通证；与此类似，“NGK.IO”将会推进与其他基于 NGK.IO 技术的侧链建立流通通道，让整个NGK.IO生态开始迈进生态网络的建设，“NGK.IO”将会作为一个核心流通纽带，加速整个NGK.IO生态的发展与进化。

11.3 更安全随机数方案

目前NGK.IO上面已知的随机数方案基本上都是结合可预知的多个字段，比如blockid、timestamp等作为随机种子的一部分，然后再结合用户端、DApp项目方或者直接由DApp方线下生成。该类方案存在一定的安全风险，无法降低对 DApp 项目方可信度的依赖， 以及无法避免一些重放攻击(比如INLINE_ACTION形式)。针对以上问题，“NGK.IO”启用了block_extension特性，提供了bpsig_action_time_seed方案，bpsig_action_time_seed不仅可以防止重放攻击，而且还需要BP节点的签名私钥进行签名，并把生成的seed存入block_extension，便于其 他节点进行验证，结合bpsig_action_time_seed就可以构造出用户、节

点、DApp项目方三方参与的更安全的随机数方案。bpsig_action_time_seed的生成方式如下：bpsig_action_time_seed=sign(BP_Sign_Key, F(block_timestamp, 0.5) + global_action_sequence)

注:

BP_Sign_Key

使用BP私钥签名的目的就是避免他人进行投机计算F：将 block_timestamp按照0.5向下取整的函数，降低BP调整时间戳来进行投机概率

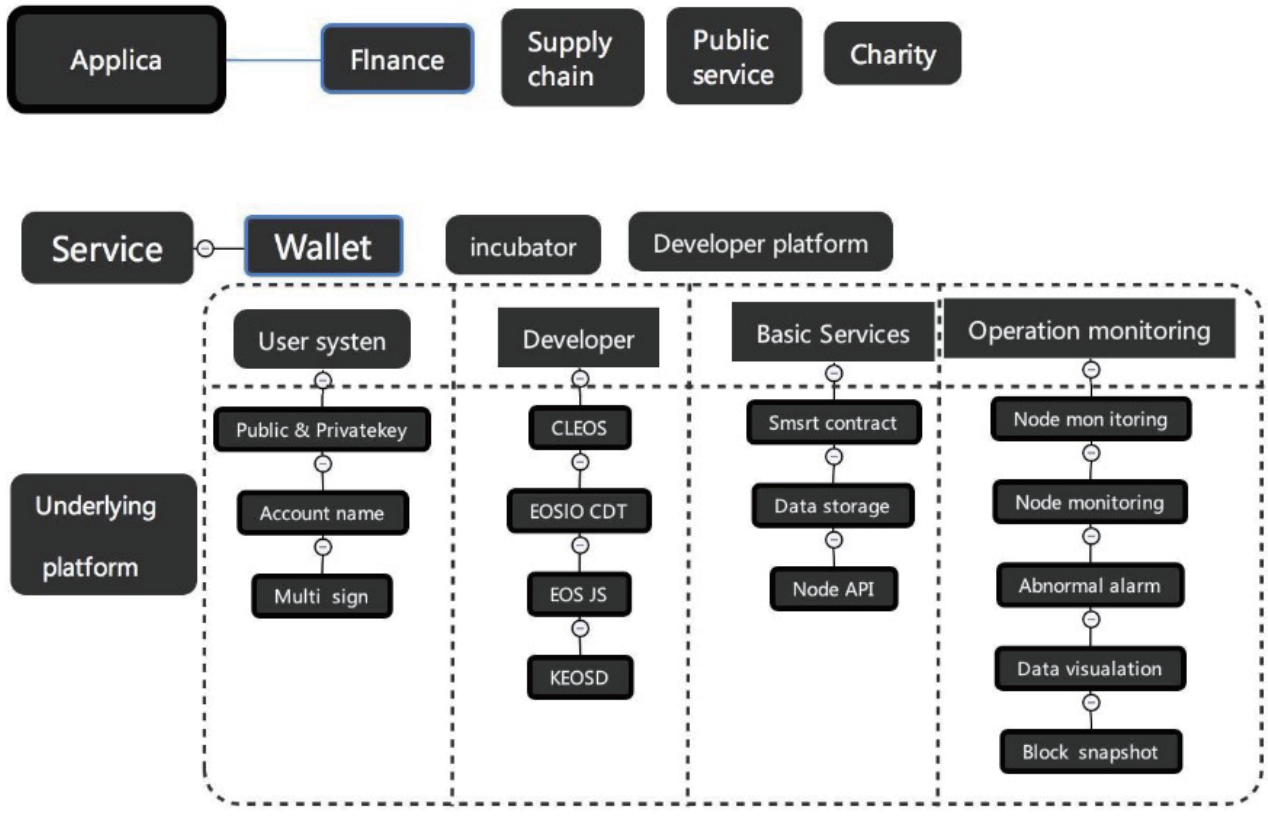
global_action_sequence:全局action自增标识，可以用于防止INLINE_ACTION 攻击。

十二

NGK.IO
企业级侧链应用

NGK.IO 公链重要设计模型是主链+多侧链，“一链一场景”，这个设计的目的是保证资源的有效隔离，同时让平台具备横向扩展能力。

NGK.IO侧链专注于数字资产的金融功能，以实现商业级的应用。从各项指标来看，NGK.IO通过并行链的方式，最高可达到百万级TPS，在并行本地链时可以达到毫秒级的确认速度，可以说NGK.IO在吞吐能力方面的优越性无人能及。



未来“NGK.IO”将会为侧链上的DApp开发者提供英文版本的开发文档、开发者工具、Javascript SDK、丰富的示例代码，让开发者能专注于产品功能开发，高效完成在NGK.IO侧链上的产品应用部署。

侧链创建

当开发者开发了DApp，DApp需要独立的计算资源以确保运行效率的时候，需要考虑为它单独创建一条侧链。

当用户需要提升或降低侧链性能的时候可以向系统提出申请，这个过程就好比云服务商升降机服务器一样方便，避免了不必要的资源浪费。

- 创建账号；
- 在账号中充值一定量的NGK.IO；（具体抵押的数量由生产节点协定）
- 调用合约发起创建侧链申请；
- 生产节点投票（需满足 2/3 以上生产节点投赞成票）；
- 如果生产节点同意了创建侧链的请求，将在 3 天以内完成侧链节点的创建。

未来“NGK.IO”将会为侧链上的DApp开发者提供中英文版本的开发文档、 开发者工具、Javascript SDK、丰富的示例代码，让开发者能专注于产品功能开发，高效完成在NGK.IO侧链上的产品应用部署。

侧链退出

侧链开发者由于DApp的运营问题或其他原因需要关闭侧链的时候，需向系统提出申请，由生产节点审核，生产节点通过审核后可完成退出。

在侧链的索引费账户余额不足时，由议会组织通过提案的形式共同决定是否继续对这条侧链做索引，生产节点有权停止这条侧链的服务。

侧链开发者费用模型

独享侧链的收费模型如下：

- 按时间付费模型，根据实际的区块生产时间支付独享资源的使用费（CPU 资源/RAM 资源/DISK 资源/NET 资源），这就好比一个开发者要将应用程序部署到云服务器一样，需要按照云服务器的配置情况支付费用（CPU/RAM/DISK 以及固定的带宽）；

- 跨链索引费模型，为确保跨链转账/验证能力，在创建侧链时需要抵押一定量的NGK.IO用于支付索引费。索引费按照区块的数量收取，单价由议会组织及开发者共同协商决定。主链生产节点为侧链节点索引区块， 让侧链具备跨链转账及验证能力，延伸了侧链的功能，维护侧链网络的安全，主链生产节点为此获取索引费。

参加扶持计划侧链开发者费用模型

设置 4 条侧链用于支持独享侧链的开发者创新，采用如下费用模型：
开发者分成模型，开发者承诺将一定收入比例平均分给生产节点；
跨链索引费模型（同独享侧链的收费模型）

- 申请“扶持计划”的开发者，需提交项目计划书及分成方案，由生产节点评审，评审通过后可在三个月内享受“侧链开发者扶持计划”；

- 三个月后由生产节点投票选择继续扶持或停止扶持；

- 停止扶持后，生产节点有权停止这条侧链的服务。

共享侧链开发者费用模型

共享侧链提案：

设置1条共享侧链任何开发者均可部署合约，共享侧链可选择采用开发者付交易费模型或者开发者收入分成+用户付交易费模型。

开发者付交易费模型：

开发者的合约在运行的时候需要持续的消耗资源，开发者要按照消耗的资源支付费用，这样能促使开发者对程序作出优化，尽可能的减少对资源的消耗。当资源Token耗尽时，这个合约的交易执行失败，开发者需保持足量的资源Token以保证合约的持续运行。开发者交易费将进入共享侧链共识合约平均分配给生产节点。

开发者收入分成模型+用户付交易费模型：

为了共享侧链的安全，如果开发者选择了收入分成模型需同时选择用户付交易费模型。开发者承诺的收入分成按照预定的比例分配给生产节点。用户交易费进入共享侧链创建者指定地址。共享侧链的创建者要支付跨链索引费以确保能跨链转账及验证功能。

在侧链中生产节点的责任

- 构建及维护侧链节点，让开发者的合约得以正常的运行；
- 维护侧链的安全。

- 停止扶持后，生产节点有权停止这条侧链的服务。

在侧链生态中对生产节点的奖励

- 独享侧链开发者按时间支付侧链的使用费，使用费按分钟打入共识合约，在侧链索引主链数据时分配给生产节点；

- 开发者以区块为单位向生产节点支付区块索引费，索引费按侧链选择的资源类型不同而单价不同，具体价格由生产节点协定，费用在生产节点完成索引时分配给对应的生产节点；

- 如果开发者使用了侧链支持计划，那么开发者产生的收益将被锁定在其盈利的合约账户上，开发者在收取盈利的时候，会自动将此前承诺的部分打入共识合约，在下一次侧链索引主链数据时，承诺的盈利会被平均分配给生产节点；

- 开发者付交易费模型，交易费会直接打给共识合约，在侧链索引主链数据时分配给生产节点；

十三

NGK.IO
通证支付系统

13.1 传统支付构架的技术弊端问题

目前市场上，区块链系统在支付架构采用两种技术流程：

- 支付层采用三层架构，交易数据经过Endorser节点进行预执行状态，得到状态读写集，RW-SET返回客户端，客户端再次打包交易发送至Orderer，Orderer打包排序后交给Commiter节点进行存储。

- 采用在客户端完成签名后发送到区块链节点，节点将交易打包成区块，并且交给EVM 执行，状态数据以MPT树状组织存储。

以上两种方式基于传统的底层构架所，使得不同的平台在架构上存在巨大差别，不仅交易处理时序不同，计算与存储结构也不同，无法做到产生交易并实现跨平台互通。如果要实现金融和溯源监管有关备案信息的跨链互通，那么就必须要打通各个场景的互访，这将面临比传统数字资产实现跨链更为复杂的业务逻辑。

基于此NGK.IO业务逻辑进行了改良并与常规区块链平台有很大不同，在技术手段上NGK.IO在不同业务场景已经实现不同的合约逻辑，每个场景都获得底层模块的系统支持。目前NGK.IO区块链技术已经在众多应用领域初露头角，未来相信NGK.IO应用层面将覆盖金融、溯源、文化、游戏等众多行业。

13.2NGK.IO 引领通证支付创新未来

我们如何突破这些生态之间的技术壁垒，实现区块链支付时代？NGK.IO整合技术创新，给出了答案！

NGK.IO旨在全球促进区块链不同地区与不同产业带之间的互动。技术团队为这些异构区块链，设计了一种统一的语言，即统一的架构抽象。NGK.IO从核心数据结构、区域块链交互模式和交易管理等方面提取行业

主流块链产品的核心和必要的公共子集，从多个层面抽象出区域块链平台。这使得NGK.IO不仅能够支持异构区块链之间的互联，还能够支持同构区块链平台的扩展。

另外，NGK.IO为常见的多通道、多组和多链扩展方案打开了跨链组件。实现渠道、群体和链之间的相互作用形成了一个重要的“六位一体”：

- 跨链适配器：是指连接一个区块链的接口，可以通过跨链路由加载，可以配置多个区块链适配器，达到连接多个区块链的效果。跨链路由构间将自动同步区块链适配器的配置信息，以帮助用户处理位于其他区块链的资源。

- 跨链资源是指用户可访问的数据对象，如智能合约和数字数据中心上的数字资产。类似于区块链适配器的配置信息，跨链资源的元信息在跨链路由器之间同步。用户通过统一的接口在跨链分区中寻址和调用资源。

- 为了满足未来多样化的业务互联需求，NGK.IO根据海量数据跨链的典型业 务特点，建立了跨区域互联的网络交互和部署架构。作为一个多方参与的区块链应用程序，NGK.IO涉及多个服务组织，业务部署在多个跨区域数据中心。

- NGK.IO为跨区域场景设计了一个安全、可靠和高效的网络架构。基于TCP长连接、心跳、自动重连和加密通信技术的网络机制保证了大规模跨区域互联的稳定性、及时性和安全性。

- 部署了灵活的体系结构。由于跨链需求通常源自成熟的区块链应用

- 用项目，跨链部署架构需要能够与现有的区块链实例兼容。NGK.IO是以非侵入性的方式设计的。在一个独立的过程中，跨链路与区块链节点是分开部署的。在不改变现有区块链网络架构的情况下，可以实现灵活的架构部署。跨链路利用部门间网络传输跨链信息和区块链信息。结合网络自动路由功能，只要跨链路有直接或间接可访问的网络链接，就可以完成跨链交互。

- 它可以自由定制，也可以被多方访问。由于实际业务场景中的跨链需求差异很大，并且所访问的区块链平台也各不相同，因此定制和定制的跨链能力是必不可少的。NGK.IO的区块链适配器和交叉链接资源支持免费定制。根据区块链的类型、系统资源和所访问的网络条件，选择不同的区块链适适配器和交叉链接资源。

十四

NGK.IO
公链实现步骤

NGK.IO主导研发的区块链底层公链系统，它专门为支撑商业去中心化应用（Decentralized Application）而设计，其代码开源。NGK.IO公链期望通过跨链可以为不同的消费场景形成价值的互通，为全球区块链商业化进程做出一定的技术力量，相信在未来NGK.IO将对价值交换的速度必然会有飞跃的提升，从而实现真正联合互通的价值网络！

区块浏览器

NGK.IO浏览器提供多种语言和多种测试网络。网站新增12种语言版本，并增加了Kylin 测试网，并提供即时在线反馈窗口，Alfred插件功能，使NGK.IO区块信息查询更加高效，实现了智能合约在线验证功能，用户可以直观的查看NGK.IO的合约源代码！

NGK.IO 钱包

NGK.IO官方钱包，是链上的钱包应用，绑定用户账号后，能够实现系统内交易效率更高，延续NGK.IO团队一贯的优势，在收发代币，管理交易和转账过程中，采用更简单的设计隐藏区块链复杂逻辑，打造普通用户都可以快速上手的数字货币应用产品，增速NGK.IO币的使用与普及。

SDK

为了快速增加NGK.IO系统中的其它生态厂商，NGK.IO系统将打造一套SDK，把代币消费，奖励机制都封装在一起，并且，NGK.IO系统团队将提供一系列技术支持服务，以便于各个生态商的顺利接入。

API

NGK.IO团队针对不同的NGK.IO币应用场景，设计了通用API接口，使得商家和用户可以使用最简单的方式在自己的产品或页面里嵌入代币的消费应用，每一个用户都可以通过复制代码的形式，嵌入第三方应用，使得NGK.IO币的流通变得更为简单。

其它生态厂商的接入

为了快速发展，NGK.IO系统将引入各种主流互联网应用。NGK.IO计划系统在设计中有部分代币将通过生态厂商进行分发。这样有利于代币的迅速扩张，加速生态系统的成熟和繁荣。

十五

NGK.IO
去中心化预言机

NGK.IO会将加密生态应用下的诸多功能全部采用智能合约的方式执行。将智能合约以数字化的形式写入区块链中，有区块链技术的特性保障存储、读取、 执行整个过程透明可追踪、不可篡改。

预言机是NGK.IO智能合约获取外部信息的唯一途径，智能合约系统要求不可信任的代码用一种特殊的语言重写，不幸的是基于性能的安全沙盒将强迫所有的合同作者使用一种类似大洋国的大量词汇及文法被简化、

取代或取消的语言，造成智能合约的实用性大打折扣；例如，按照农产品价格情况来支付投保人赔款的农产品价格险保单，传统IT人员一般认为是如下的流程：智能合约会在预定的时间，从期货交易场所获取农产品价格，然后按照获取的数据采取预设的行动，听起来很简单，但却不可能实现，为什么呢？因为这里衍生出了两个问题，一是共识问题，二是受信方问题。

预言机（oracle）在NGK.IO 网络上部署了一个Oracles 的智能合约，如果需要其数据访问服务，只需要在自己的智能合约中引用该智能合约，然后根据API文档中描述的方法进行相关的调用即可；如果某些组织利用以太坊技术搭建了自己的私有链或者联盟链，预言机（oracle）在Github上提供数据服务的开源智能合约代码，通过自己部署后，一样可以像公有链一样调用；预言机（oracle）提供了多种数据源服务器，包括Url访问、数据搜索引擎、区块链内容数据、IPFS文件访问等等，其中Url访问和区块链内容数据提供了基于TLSNotary的可信证明技术，也是常见的数据访问需求。

智能合约能被应用于塑造具有明确的条件和结果的任何类型的协议或者关系；智能预言机使得智能合约的实施变得简单、灵活和强大；下面是NGK.IO智能预言机现在可以期许的一些应用，从最简单应用的开始，难度依次递增：

- **桥接价值网络**
  像比特币和瑞波这样的分布式网络的记录账户和余额的账本或者区

块链是分开的；传统的金融系统也有它们自己的账本，建立在的账本，建立在智能预言机上的合同能够在分开的系统之间创建自动的、完全可信的桥接；这样的桥接能够接收来自于其中一个系统的支付，然后立即在另一个系统发起支付。

- **代理**

  智能合约能够很容易地建立起来，充当代理账户，监控两人之间的交易；商品、财产或者服务的买家把货款打到合同账户中，这个合同将监控外部服务信息，例如对于域名交易，它会监控域名注册者，对于房产交易，它会监控公开房屋所有权记录；当所有权由卖家转到买家时，合同会自动将货款发给卖家。

- **密码学货币钱包控制**

  目前比特币和瑞波没有好的机制使得“拉回支付”（pull payment）可行；“拉回支付”即如同信用卡支付模式，卖家代表买家发起支付；合同控制的钱包包括许多不同类型的复杂控制，从每日取款限额到允许特定实体收款；这将使得认购、条件支付和不用公开私钥的精细化钱包控制成为可能。

- **数字资产拍卖**

  如果智能合约被给与了数字资产的所有权，它就能执行拍卖规则；它可以被设计为在比特币或者瑞波网络上接受投标资金，拍卖结束后，向投标失败者返还资金。

- **金融衍生品**

  监控数字或非数字资产的合同也能够应用于期货合约、远期合约、互换合约、期权合约。

- **债务和权益**
  其它基于根据事先制定的规则实现支付和权益变动的证券也能够写成智能合约。

- **智能财产**
  智能财产的经典例子是智能汽车，它能通过可转让的，但不可伪造的数字标记（digital　token）知晓谁是它的主人；合同可以管理所有权的转移和附带规则，这包括临时性授权和其它协议中担保财产的潜在使用。

- **投票**
  未来智能合约可以用来执行民主、官僚和其它类型的对资产或者组织的控制结构；像其它所有应用一样，合同执行事先定义的规则，甚至包括更改合同自身代码的规则；许多非金融应用要求更复杂的基础设施和更加成熟的生态系统，所以我们预期这样的应用建成需要一段时间。

十六

NGK.IO 治理结构

16.1 超级节点机制

NGK.IO提出分布式超级节点选举算法DSNE，保证了能在更短的时间内完成选举。基于信任模式的P2P超级节点选取机制,参照人类社会的交际模式,通过计算节点的总体信任度作为评选超级节点的一项重要指标,在计算节点信任度的过程中引入奖励惩罚因子和时间衰减因子,同时为了减轻在拥有大量节点的网络中进行超级节点的评选所带来的网络负载，我们

采用阈值过滤算法对普通节点进行阈值过滤,筛选得到备选超级节点集合,然后再从备选超级节点集合中 选取最优的超级节点。

超级节点选举算法适应动态变化的网络条件，应用进程可以随时加入或离开网络，并可能发生随机的故障与恢复，进程之间还存在消息丢失和消息延迟；领导人选举服务包括组维护、故障检测和选举算法三个模块，使用速度（选举服务占用的时间）、平均错误率和领导人可用性三个QOS指标来衡量选举服务的性能。但由于应用进程在加入网络时需要向一个集中式的共享库进行注册，从而使算法在这方面失去分布式特征。

超级节点的选举需要遍历节点集合中的所有节点，通过分布式的最小生成树算法可以实现遍历的目的，因此可以很容易地将最小生成树算法改造为选举算法。分布式最小生成树（MST）算法，具有最优的通信复杂度和较好的时间复杂度，并在此基础上MST 算法引入一些非常基本的思想和概念。一个节点作为根节点启动算法，发送“follow-me”消息。收到“follow-me”消息的节点，如果消息传递边是它邻近边中的最小权重边，则勾到MST树上。如果有的节点没有把它们自己勾到MST树上，就选择一个新的根，旧根“迁移”到新的根上，继续上述过程。最坏情况下，算法需要（n/2－1）次根迁移时间复杂度是（dn），消息复杂度是（2m+dn/2－1）。这里的参数n、m和d分别是网络中的节点数量、边数量和网络直径。

16.2 超级节点收益来源

NGK.IO 超级节点收益为：
全网 95%的资源消耗（交易费用）奖励给超级节点， 剩余 5%累积存放至Worker Proposal 奖励给公链DAPP 技术开发者与应用开发贡献者主要用途：奖励 NGK.IO 生态社区、生态贡献者、生态建设之，保障整个 NGK.IO 生态能够良好的发展壮大。

16.3 超级节点挖矿机制

在没有社区竞选超级节点的情况下，NGK.IO官方基金会管理21个超级节点，每一轮（X秒待定），前10个节点有6/10的几率出块，后11个节点有3/11的几率出块。

出块率计算公式为：
一段周期的实际出块数目/一段周期的实际出块数目。

当有社区超级节点进入后，官方超级节点会逐渐退出（退出机制参照超级节点竞选段落内容），但至少保留3个官方超级节点，继续对投票给官方超级节点的用户和跑全节点的用户进行奖励。

16.4 超级节点权利与职责

超级节点的权利与职责相辅相成，在主网上线后，可积极配合开发者共同建设NGK.IO生态联盟，同时保障系统整体的安全性，共同抵制个别生产节点的作恶以及中心化集权等问题。

权利

超级节点作为区块生产者，最直接的权利出块权与记账权，其中奖励层面上最直接的权利是能获得全网交易手续费的95%奖励（NGK.IO全网交易手续费95%=超级节点收益）。

职责

作为NGK.IO生态中的超级节点，负责BFT–DPoSS工作证明（挖矿），记账以及新合约的审核工作。

十七

NGK.IO
未来生态建设

17.1 NGK.IO 国际市场新模式建设

NGK.IO将通过区块链技术的应用，打造世界级，无需兑换，可全球自由买卖，涵盖生产企业、国际贸易、物联网、医疗领域、融资投资、证券交易所等领域的数字支付系统，实现更加高效便捷的跨业态、跨境支付机制，大幅度地降低支付成本，显著提升交易效率，进而成为数字货币时代的支付基础设施，甚至彻底改变当今世界支付系统的面貌。

建立NGK.IO社区内部自己独有的级别标准化体系，最终借助NGK.IO市场化运作手段促进建立行业级别标准化体系（行业规则）。随着NGK.IO落地场景应用的增加，NGK.IO通证的价值将进一步显现。

17.2 全球金融支付国际化

NGK.IO将连接全球消费者和线上线下商家，还原用户行为价值打造未来千万亿市场规模的平台。推动行业资产实现数字化转换过程，加速行业资产的流动性，实现行业资本化运转。

NGK.IO将发行算法型稳定币USDN，应用于区块链各支付场景的支付工具，提供给商家和企业，并快速推广到个人用户，培养用户习惯，最终构建基于区块链金融的开放式支付系统。解决全球支付效率不高的问题，NGK.IO通过构建NGK.IO的VPN子网技术实现闪电支付网络转账秒级确认，保证实时消费不受区域限制的影响。打造区块链支付3.0新时代！

17.3 NGK Wallet 多链钱包

NGK Wallet多链钱包支持多平台通证，不同平台通常采用的技术方案都各不相同，NGK Wallet对其他平台钱包逐一进行接口开发，支持内置交易所和跨链互兑。

NGK Wallet多链钱包生成用户多钱包的统一密钥，通过助记词即可登

入。在未来用户可以同时使用NGK Wallet多链钱包上的NGK/USD-N/BTC/USDT/ETH等数字资产开始金融服务，NGK Wallet多链钱包，可作为个人冷温钱包存储数字资产工具，同时将支持NGK/USDN/BTC/USDT/ETH 智能合约属性，安全稳定，公开透明。

17.4 NGK.IO 金融衍生品交易所

NGK.IO金融衍生品交易所流通NGK/USDN代币，通过独创的兑换网络，以及对接交易所API，为用户提供简单、便捷、安全的兑换和交易服务。

NGK/USDN通过智能合约和跨链网关和跨智能合约技术，实现无风险的金融衍生品兑换服务。用户通过NGK/USDN代币享受金融增值衍生品兑换，由平台方或其他第三方创建兑换的智能合约，由合约机制监控和执行兑换过程，规避了参与各方在交易过程中的违约风险。相比于中心化的平台服务，智能合约避免了平台方主观的违约风险或客观遭受攻击给用户带来损失。金融衍生品推陈出新，简单方便的交易通过交易所来买卖金融衍生品。NGK.IO还推出一系列衍生激励机制，通过用户个人或者组团集体行为，为金融生态做出持续贡献来获得一定比例的NGK代币。

NGK.IO 通过对接交易所 API，为用户提供最优的市场价格和简单的操作体验——NGK.IO通过优化筛选机制，给用户呈现简单的买入价和卖出价，用户只需输入数量，就能像在电商平台一样方便的完成金融衍生品的交易。

17.5 NGK.IO 社区文化推广

在全球以每个地区为单位成立行业文化推广NGK.IO社区，每个社区发起人基金会给予相应的NGK通证做为奖励。

17.6 NGK.IO 金融孵化项目

NGK.IO不仅仅提供金融内的项目孵化并提供种子基金，为指定项目扩大研发团队助力。NGK.IO金融生态内孵化项目将在未来呈现欣欣向荣的态势。

十八

NGK.IO
未来技术框架与路线

18.1 NGK.IO 未来技术框架

NGK.IO 技术全景

平台通证NGK.IO技术全景包括基础网络层、中间协定层及应用服务层。NGK.IO技术全景基础网络层由数据层、网络层组成，其中数据层包括了底层数据区块以及相关的数据加密和时间戳记等技术；网络层则包括分散式组网机制、资料传播机制和资料验证机制等。

中间协议层由共识层、激励层、合约层组成，其中共识层主要包括网络节点的各类共识演算法；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；合约层主要包括各类脚本、演算法和智能合约，是区块链可程式设计特性的基础。

平台通证NGK.IO应用服务层作为区块链产业链中最重要的环节，包括区块链的各种应用场景和案例，包括可程式设计货币、可程式设计金融和可程式设计社会。应用层是平台通证NGK.IO应用生态的底层技术架构，开源的可程式设计的应用层为建立全球数字货币应用生态提供了技术保障。

NGK.IO 开源协议

平台通证NGK采用的创世块是在EOS开源协定的区块链基础上新创立的公有链， 使用者能够进行点对点的货币交易与即时结算，轻松便捷地转换交易资产（传统货币、电子货币以及其他各种形式的资产），大幅降低了跨行转账尤其是国际转账过程中的风险与手续费。

不同于中心化网络模式，P2P网络中各节点的电脑地位平等，每个节点有相同的网络权力，不存在中心化的服务器。所有节点间通过特定的软体协定共享部分计算资源、软体或者资讯内容。钱包兼具P2P独特的开源网络技术是构成平台通证NGK技术架构的核心技术之一。

NGK.IO P2P 网络模式

NGK.IO协定与传统的银行SWIFT电汇协议对比：通过传统的银行SWIFT转账要被收取高额的手续费并耗时3到5天，使用NGK.IO跨境转账则能即时到达。NGK.IO与比特币的对比：基于NGK.IO拥有兑换和交易的功能，让全网所有处于分散式网路的使用者都能够进行点对点的货币交易与即时结算；而比特币区块链本身不具备交易功能，其交易需依赖交易平台。

NGK.IO 通证非对称加密演算法

非对称加密算法是指使用公私密金钥对资料存储和传输进行加密和解密。公开金钥可公开发布，用于发送方加密要发送的资讯，私密金钥用于接收方解密接收到的加密内容。公私密金钥对计算时间较长，主要用于加密较少的资料。常用的非对称加密算法有RSA和ECC。

NGK.IO正是使用非对称加密的公私密钥对来构建节点间信任的。

NGK.IO 一致共识

NGK.IO遵循开源协议，因此，在分散式节点之间，有相似的协商一致性的重要步骤。“一致共识(Consensus)”是整个网络就同一总账达成一致的过程。如果每个人选择了一套完全不相干的验证者，网络将不会达成一致共识，总账的特殊版本就是唯一正确的总账。但实际上，人们的UNL列表会重复，这种重复导致可靠的验证者达成同样的协商。

18.2 NGK.IO 未来技术路线

（一）未来 1–2 年

为支持NGK.IO智能合约，我们将在此阶段快速构建一个功能大致完整的原型项目，用以测试和验证功能。

- 构建NGK.IO测试用原型，开启公链生态开发工作
- 超级节点竞选
- 支持NGK.IO智能合约，引入侧链机制

技术

完善技术设计文档，完成基础模块代码开发，并上线主链，持续完善智能合约，多链并行，跨链共识等早期功能。完善主链周边生态，包括区块链浏览器，轻钱包，移动端钱包，智能合约虚拟机，编译器，开发工具，多语言适配等。

生态

建立并发展和完善开源社区，启动和推进更多应用接入。

（二）未来 3–5 年

完善NGK.IO功能，并开放跨链资产转移、跨链智能合约调用功能。

技术

主链中实现更多共识模块的植入，并对网络、存储等模块自我进化，并

完成对接各行业应用的标准技术方案体系；探索与大数据、人工智能等其他领域结合的新生态系统。

生态

形成一个成熟的开源社区，大规模建立应用子链。

（三）未来 5 年以后

完善核心的多链功能，商业化进程迈进：

- 商业化DEFI 应用程序
- 完成第三方侧链功能
- 完成异构侧链接入

技术

建立一个区块链、大数据和人工智能融合发展的技术平台，为工业、农业和商业的生产和经营需求提供全方位解决方案。

生态

形成一个区块链、大数据和人工智能融合发展的开源社区，提供全面的价值对接和协作平台。

十九

结语

相信通过NGK.IO的不断的应用打造和生态完善，基于NGK.IO系统将形成一个全球多元化的数字商业网络，我们可以在这个网络中实现经济共享、价值互换、商业共生、高速流通的生态发展，而NGK.IO可以协助保护市场的权益、自由和财产，将区块链技术不断的推行，将应用不断的扩展，打造属于NGK.IO所有用户的数字经济商业帝国。

二十

风险提示与免责申明

本白皮书仅作为一份概念性文件，用于描述NGK.IO提出的数字资产生态系统和NGK.IO的数字资产，并不构成买卖NGK.IO的相关意见。文中描述和分析不可视为投资建议，也不构成投资意向或教唆。参与通证销售则代表参与者已达到年龄标准，具备完整的民事行为能力，NGK.IO团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、通证及其机制、通证分配情况。

文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。NGK.IO明确表示，概不承担参与者因依赖本文档内容、本文信息不准确之处，以及本文导致的任何行为而造成的损失。

另外团队将不遗余力实现文档中所提及的目标，然而基于不可抗力的存在，团队不能完全做出完成承诺。

NGK.IO无意构成任何司法管辖区内的证券或者其他任何受管制产品，本白皮书不构成招股说明书或任何形式的要约文件，也无意构成任何司法管辖区内的证券或者其他任何受管制产品的要约或招揽。

NGK.IO的数字货币发行没有任何形式保证或承诺。在贡献之前，您应确自己完全理解贡献行为的意义，并仔细审查贡献协议的规定与有关风险。

获取NGK.IO的数字货币为自愿行为，不可退款，不能取消且无法获得赔偿。本白皮书并未经过任何司法管辖区的监管机构审查，不构成任何投资建议，也不应作为任何合约或购买决定的依据。

对于本文中描述的讯息、声明、意见及其他事项的准确性或完整性，或以其他方式传达的相关信息，我们不提供任何声明或者保证。本文中的任何内容，均不可作为对未来的承诺或陈述依据。

在适用法律所允许的最大范围内，任何因本白皮书的任何相关人员或任何方面而产生或与之有关的任何损失（无论是否可以预见），其所有责任均免除。可能受限但无法完全免除的责任范围，仅限于使用法律所允许的最大限度。 本白皮书对任何特定机构或组织的引用仅供说明之用。

随着区块链技术与行业整体态势的不断发展，NGK.IO可能会面临一些尚未预料到的风险。请参与者在做出参与决策之前，充分了解团队背景，知晓项目整体框架与思路，合理调整自己的愿景，理性参与通证投资。

您必须听取一切必要的专业建议，包括税务和会计处理相关事务。我们希望NGK.IO计划能够取得成功，但我们无法保证成功，且数字资产投资风险系数较高，请务必评估风险及承受能力。