



# NEW POWER COIN

基于用户画像的  
去中心化互联网流量引擎

---

## 白皮书 (简体中文版)

V1.0

本文所载资料，仅作为技术说明提供，不涉及任何公开数字通证发行或募集，且不构成任何投资建议。

This Whitepaper represents general information about New Power Coin. Please ensure you first read the disclaimer and risk factors at the end of the document to fully understand the purpose, status, and limitations of this Whitepaper.

© 2018 New Power Coin Community. All Rights Reserved.



# 目 录

一、愿景	4
二、概要	5
2.1 背景介绍	5
2.2 自洽的闭环应用	6
2.3 超越传统平台	8
三、挑战	9
3.1 流量的来源	9
3.2 互联网流量环境	9
3.3 目前互联网流量的重大问题	10
3.3.1 流量被巨头把持	10
3.3.2 用户永远弱势	10
3.3.3 用户隐私难以被保护	10
3.3.4 流量集中导致科技创新低下	11
3.4 存量互联网广告业务的变革契机和新机遇	11
3.5 新力量币希望解决的问题	12
四、架构	14
4.1 技术需求	14
4.2 技术架构	15
4.2.1 去中心化价值传输网络	16
4.2.2 半中心化主节点网络	17
4.2.3 价值传输服务	17
4.2.4 流量交易服务	15
4.3 区块链设计	18



4.3.1 共识机制	18
4.3.2 主节点网络	20
4.3.3 匿名机制	24
<b>4.4 流量平台设计</b>	26
4.4.1 业务规划	26
4.4.2 业务逻辑	27
4.4.3 业务架构	34
4.4.4 业务扩展	36
<b>五、经济</b>	41
5.1 经济设计原理	41
5.2 基础经济数值	42
5.3 区块奖励	42
5.4 获取与消耗	43
<b>六、路线</b>	44
6.1 业务路线	44
6.1.1 广告流量业务分阶段发展的实现	44
6.1.2 业务各个阶段规划	44
6.2 研发路线	47
<b>七、总结</b>	49
<b>八、免责声明</b>	50



## 一、愿景

---

构建新一代的互联网流量来源：

**去中心化基于用户画像的全球在线流量引擎**

## 二、概要

---

### 2.1 背景介绍

2008年，中本聪先生提出的比特币和区块链打开了新一代互联网——Web3.0的大门。从比特币出现至今，区块链应用已经呈现出多种不同的形态。从分布式账本，到分布式计算平台，再到各类金融工具，区块链正在用一种去中心化的方式逐步解决越来越多的问题。

虽然当前的区块链应用普遍执行效率较低，因此只能在一定层面作为账本进行数据的保存，短时期内无法对外界提供计算能力。但是按我们的预期，随着区块链基础设施的逐步发展，运行在区块链上的计算能力将逐步增强。

---

**“Web3.0是一种我们为了某种目的而对互联网的重新架构，且在参与者之间采用一种完全不同的交互的模式。我们认为要公开的信息，我们就发布。我们认为要被认同的信息，我们就把它置于一个共识账本里。我们认为隐密的信息，我们就保密且永不公示。通信一直在加密渠道中进行，且从不使用任何可追溯的方式（例如IP地址）。”**

---

互联网正在开始向Web3.0过渡。Web3.0的目标就是在重塑互联网去中心化初心的同时，提供诸如价值转移、透明开放、高度信任、隐私保护以及互操作性等特性。

互联网上信息流动的过程中，用户兴趣点和注意力的迁移称为互联网流量。早期互联网和网络的倡导者都支持去中心化、互操作性和开放性。然而，随着时间的推移，互联网流量逐渐被集中以及控制在少数人的手中。在这种情况下，互联网流量生态环境不断恶化，中间成本不断增加、用户隐私数据被侵犯、恶意欺诈行为泛滥等，这导致参与方的利益都受到不同程度的损害。

互联网广告当前正在走向急速下降的趋势，核心原因有几个方面：

**1.**

互联网的发展趋势造成存量市场新增用户量降低，新增应用无论是互联网网站还是移动App都在争夺已存在市场，造成用户选择减少，需求降低；

**2.**

中间商对于广告的采购成本急剧增加，头部市场过于强势造成头部流量来源议价能力过强，长尾流量采购成本过高，资金占压严重；

**3.**

市场恶劣的情况造成劣币驱逐良币的恶性循环，流量数据造假扣量、内部回扣等黑幕在互联网广告行业时有发生；

**4.**

流量来源方为了拉低成本，不惜进行难以追踪的作弊造成流量质量逐年降低；

**5.**

为了实现精准匹配提高广告价格，用户隐私被严重侵袭；

**6.**

用户体验恶劣，广告平台提供的SDK使得多数应用强制用户看广告后才能继续使用实质功能，使得广告在用户层面口碑极差，极大拉低用户留存率。

面向互联网的发展趋势，我们计划实现一个在区块链上进行去中心化互联网流量交换的引擎，并以主网数字货币——新力量币(NEW POWER COIN, 代码 NPW) 作为经济支撑，实现其中的流量交易服务。

## 2.2 自洽的闭环应用

比特币及区块链非常伟大，但是对于比特币的经济模式我们只能部分认同，因为比特币的模式无可避免地产生一个问题：那就是不可能人人都参加挖矿，因为比特币从初创至今，经济链条并非自循环，而是单向的，如果人人都挖矿，生产出来的比特币不能流向下游，就会面临无人接盘的局面。比特币的价格主要是依靠后来者的购买而体现，只要一段时间内无人购买和认可，就会出现价值崩盘，使后来者经济上受到伤害。而这在比特币不长的历史上已经多次出现。这也是社会各界对比特币始终抱有怀疑，斥之为击鼓传花的根本原因之一。

这同样也是目前市面上所有加密货币的终极悖论，导致大部分加密货币只是昙花一现，还没来得及解决它们宣称要解决的问题，就已经被人们所放弃。

我们认为，加密货币不应如此，而应该有一个完善的、不完全依赖外力、经济自洽的闭环。用成熟产品向世人展示它的技术意义和实用价值，而不是单纯依赖“众人拾柴火焰高”，沦为炒作工具。

如果我们想想几乎每家每户都有的产品：电视机。它就有个典型而古老的经济闭环：

电视台给观众播放节目→观众收看节目→商家在节目中插播广告宣传商品→电视台收取商家广告费→电视台拿出部分收入准备节目→依此持续循环……

这是一个皆大欢喜的经济闭环，所有人都有付出，但得到的比付出更多，没有人成为单向经济链的末端，做最终受害者（抛开伪劣商品广告之类脱离正常轨道的特殊情况不谈）——商家虽然付出了广告费，但收获了将转化为购买力的关注度；电视台付出了准备节目的劳动和经费，收获了商家的广告费；观众收看电视节目得到娱乐，而且收看广告并购买商品，也不是单纯付出成为受害者，因为他们本身就需要这些商品。因此所有人都乐意、积极参与到经济闭环之中。

受此启迪，我们也给NPW网络设计了一个经济闭环，如下图：

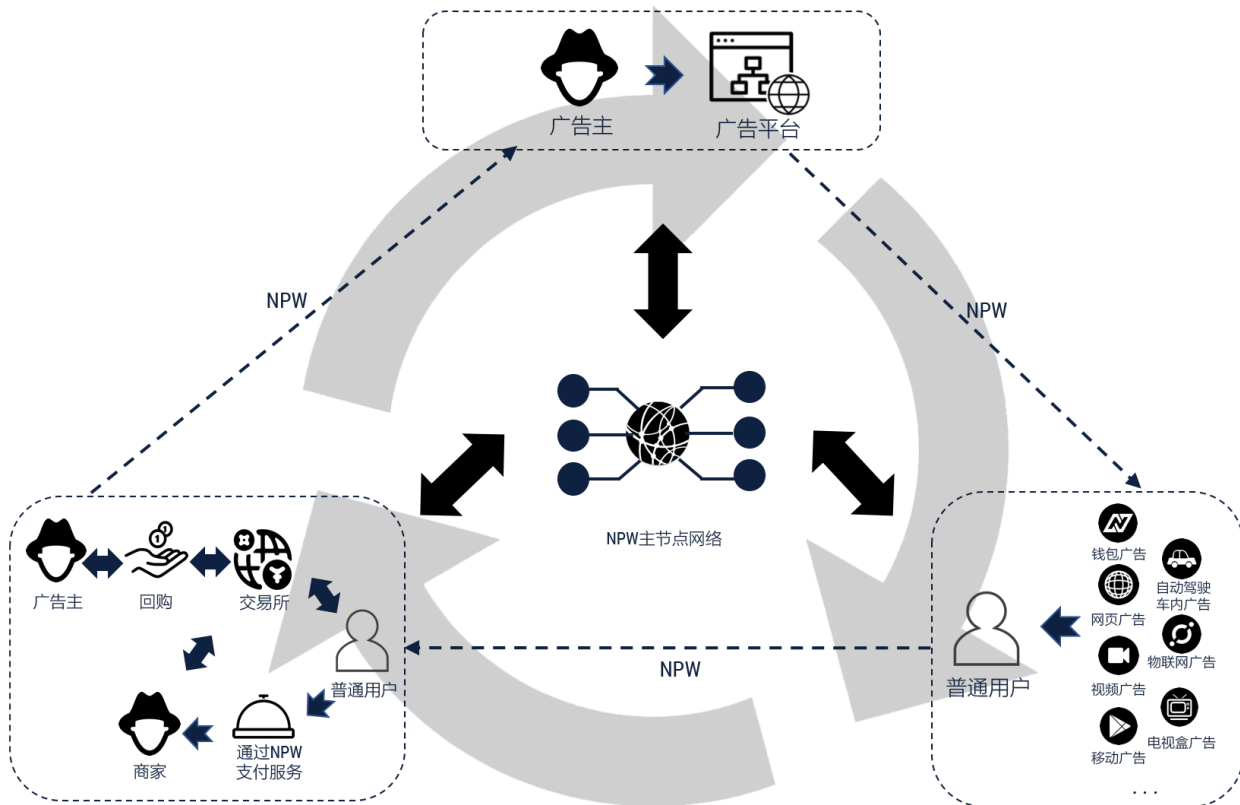


Fig. 1. 新力量币经济闭环模型

在我们的经济系统里：商家购买NPW，充值投放广告→用户在各种媒介中浏览或者静置播放广告信息得到NPW→用户把得到的NPW用于支付有偿服务和商品或者在平台套现→商家回购NPW用于投放广告→依此持续循环……

在电视台经济闭环，观众得到的是间接的精神娱乐得益，NPW终端用户得到的是直接的经济利益。

以上是对NPW网络的经济系统最简要，最核心的说明，详细的实现原理和机制请见后面章节。

## 2.3 超越传统平台

作为下一代的广告流量平台，我们利用区块链可以实现对传统宣传平台（电视台/电台/街头广告牌等）、传统互联网流量的超越，并有机会对接未来产生的任何广告流量来源：

- ✓ 广告主自助投放，流量方自动获利，来去自由；
- ✓ 完善的链上信任机制，各方都能确保流量作弊和扣量，统计完全透明，使得流量方利润提高，广告主成本降低；
- ✓ 统计分析计算在链上进行，在保障用户隐私不被第三方非法占有的同时还可以进行精准匹配，使得广告内容确实能真正帮助到最终用户；
- ✓ 彻底去除中间方，使得所有的广告投放、匹配、预算等工作自动执行，提高投放效率；
- ✓ 多个不同的流量来源进行真正的自动价格同步和实时竞拍，真正实现全网RTB（Real Time Bidding）；
- ✓ 由于信任机制的存在，最终用户也可以信任广告本身，广告形式从传统的推销变为最终用户通过广告真正主动获取广告信息来源作为消费参考。

目前，新力量币已经上线基础底层公链，具有**基于主节点提供互联网在线广告流量服务、快速便捷的主节点搭建能力、隐私交易能力、即时交易能力**等特性。



在此基础上，新力量币还将自主研发一整套独立的技术能力，逐步支持**去中心化流量交易、广告平台间流量对接、多平台及多广告形式展示、基于用户画像的精准匹配、流量来源用户隐私保护以及避免流量欺诈**等多种能力。



最终，新力量币将作为底层数据流转与网络交易交换的基准加密货币，建立一个庞大的**去中心化互联网流量交换、计费、投放、统计、用户画像、标签的底层引擎**，同时支持多种去中心化广告平台的运营。

互联网流量是互联网上最基础的价值服务，我们希望通过本文，介绍如何应用新力量币进行广告流量的应用，并描述新力量币的发展规划。



## 三、挑战

### 3.1 流量的来源

传统的互联网流量来源通常使用了数字广告交换网络的形态。传统的广告角色包括：



**广告主：** 进行推广的数字广告流量购买方；



**流量主：** 具备数字广告流量的软件/网站，可以向受众进行广告的展示；



**广告平台：** 聚合多个流量主和广告主，进行集中规划的广告交易。

广告的载体包括：互联网站、计算机软件、视频、应用App、游戏App、手机版页面等。同时，现代的互联网广告系统，通常都会为单一用户进行各类属性及操作的标记，以便理解用户的习惯操作行为。广告主通常可以通过这种标记方法进行用户的LTV（Life Time Value）管理。

例如：某独立游戏开发者Valerica Studios出于兴趣，开发出一款免费同人游戏，游戏经过测试，游戏的留存率和活跃率极高，由于传统上这类游戏难以获得利润，缺乏资金难以持续更新开发，因此该工作室登记成为了NPW的流量主，将游戏作为载体，使用NPW进行广告结算，获得了收入，为粉丝持续开发游戏。

### 3.2 互联网流量环境

互联网的存在基础是内容的获取，其次才是沟通和交流。在以上的过程中，用户兴趣点和注意力的迁移就转变为流量。研究表明，用户的注意力是很容易被引导和迁移的，因此拥有流量的控制权，等于拥有力量。

在过去的二三十年里，全球的互联网经历了巨大的发展。互联网的基础架构自出现至今，始终是基于“浏览器－服务器”和“客户端－服务器”的形态。在传统PC互联网时代，各类浏览器作为流量的基本入口，广告通过URL进行流量的跳转及统计分析。到了移动互联网时代，两大巨头Apple和Google占据了移动互联网唯一的两个操作系统入口：iOS和Android，形成了实质性的垄断。移动互联网的流量也从之前浏览器的URL跳转，变为只能通过激励的方式引导用户下载App。巨头们通过此种方式，迅速抢占流量入口，并迅速建立起基于广告流量的商业模式。

由于流量作为核心互联网资源，具备充分的稀缺性。过去的这二十年里，逐步有越来越多的公司进行互联网流量的引流和输出。正因为流量具备的稀缺性，第三方流量平台虽然不像巨头那样可以从更高维度进行流量的整合，但是也在一定层面对流量的价格和倾向性进行一定程度的控制，

可以通过拉高利润率，再通过洗流量的方式进行推广和销售。

随着互联网注意力的逐步迁移，市场上还将出现更多的全新产品和服务，也能够提供更多的流量来源。互联网的流量和注意力将作为永久的话题，无论技术形态和业务形态如何改变，都会始终以不同的形式存在。

### 3.3 目前互联网流量的重大问题

#### 3.3.1 流量被巨头把持

目前，多个互联网传统巨头的商业来源都是互联网广告。互联网广告是推动用户流量的一种形态，但不是唯一形态。

流量应当像流动的水，允许用户根据自己真正的兴趣进行随意流动，而不应当被限制在单一产品或者单一服务中。而互联网巨头将商业模式构建在互联网广告之上，实际对用户的潜在伤害是巨大的。互联网巨头拥有的海量数据能力，意味着用户是可以被分析的，用户的注意力是可以被操控的。这些利益都属于用户的基础利益，而巨头商业的目的是为股东负责，因此，对利益的把持和操纵造就了今天的互联网广告环境。

#### 3.3.2 用户永远弱势

基于中心化的广告模式一定会在一定程度上被操控，无法真正将数据的归属权返还给用户。

无论是基于用户搜索行为、购买行为还是社交行为的分析所产生的广告行为，都属于高效、高转化率的广告模式。这种方式的广告结果非常易于被操纵和控制，很难产生双赢的结果，用户永远会保持弱势。

用户产生的数据越多，对于广告平台来说就越属于正向循环。但是对于用户的权利来说，则会变为恶性循环，用户的使用行为始终受控于巨头的广告平台，用户的注意力将越发严重地始终被引导和操纵。

#### 3.3.3 用户隐私难以被保护

互联网上的流量模式，使得任何人包括中心化的广告平台都难以保护用户的隐私。用户的所有行为信息都会集中化地被储存、被分析。

虽然逐渐出现的各类监管，包括欧洲的GDPR的出现，使得巨头们对于用户数据的多数分析仍然属于定性分析，不涉及到具体用户，但是最终对于用户的控制，是单一的，独立的。同时，由于马太效应，越是头部的流量来源就越容易被操控，进而使得用户的行为数据更易被发掘，将会变成恶性循环，最终甚至形成恶性的政治事件。



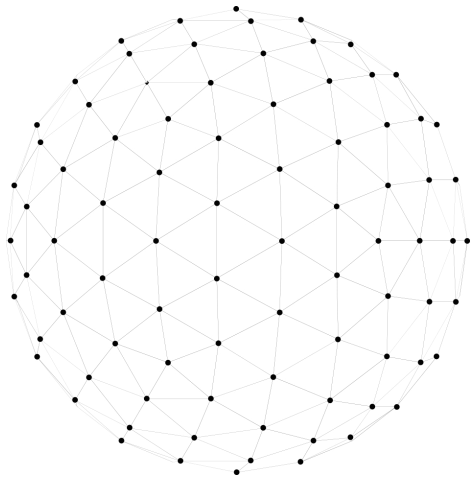
### 3.3.4 流量集中导致科技创新低下

由于流量易于操控，造成长尾不长，流行产品很容易受到人为操纵，头部内容和流量的过于集中爆发，将压抑科技创新和研发动力。因为仅仅通过资金推动，就可以快速获取人口红利，进而持续进行流量操控，在这一过程中，将无人有进行科技创新的动力。

## 3.4 存量互联网广告业务的变革契机和新机遇

区块链将传统的计算机形态从中心化计算转变为去中心化计算，正因为如此，人类第一次具备了可以不被人为操控并让计算机进行自动计算的能力。传统的线下业务利用计算机处理的效率不如纯信息流处理的效率高，因此多数的基于数字信息流的业务，都有机会向区块链的去中心化进行迁移。

互联网流量始终是一个巨大的市场，是互联网得以运行的底层基础。我们一直在探讨如何利用区块链技术找出痛点，解决流量服务的刚需。



**现存互联网广告市场已进入急速下降期，而今天的区块链所能够实现的功能还相当初级，主要体现在：**



用户认知存在局限，  
用户数量相当少；



底层技术相对简陋，  
开发深入度偏低；



用户体验较差，难以惠及普通用户；



应用过于初级，尚未具备行业特征。

在这样一个早期环境里，没有一个真正的标杆性的应用可以展示给人们，真正的区块链流量应用应该是什么样的。

对于巨头来说，对于区块链的进入很难对其核心业务造成真正意义的改变。无论是先期的巨额投入还是后期的庞大用户积累，都变为巨头的庞大负担，因为一旦开始利用区块链，就意味着商业模式的完全改变和颠覆。巨头没有动力，也没有能力用全新的这种技术和经济分配方式颠覆自己。

在这一从中心化模式向去中心化模式转换的过程中，对于多数巨头来说，打击有可能对其产生替代的竞争者才是其最重要的考虑点。因此我们也看到，现今的广告巨头，对于区块链和数字货币的广告是积极打压的，他们打着防止欺诈的旗号，禁止区块链的广告在其平台上出现。

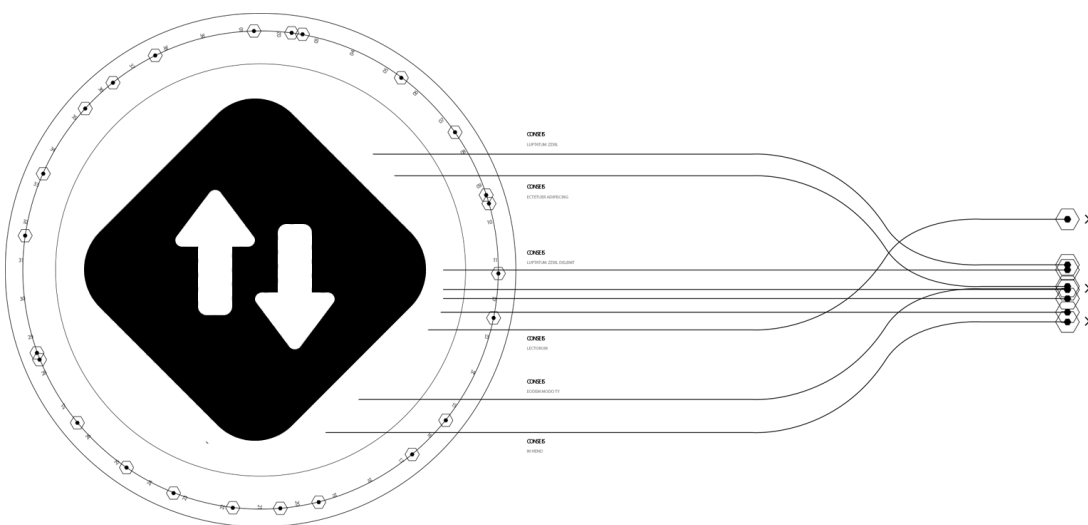
和所有商业服务一样，区块链流量业务也同样需要经济流转的刚需。先有刚需，就会产生服务的提供方，进而产生生态。有了生态，经济体系将会进行内部流转。

传统互联网数字广告行业另外的一个亟需解决的问题是它属于资金密集型行业，在广告投放过程中，资金占压严重，收款付款易于产生坏账。利用区块链进行经济流转能够起到高效安全，实时结算的效果，无需中介即可实现大规模的资金管理。

同时，现今的各类区块链项目，有着巨大的流量、社区维护、导入用户等刚需，项目方需要精准找到更多数字货币的使用者，共建社区。对于区块链这一新兴互联网形态，各方对于流量的需求巨大。

### 3.5 新力量币希望解决的问题

“流量”这一词，本身就是分散的。互联网上成千上万的用户，在不同服务、内容之间的跳转，本质是分散的，去中心化的，应当以用户真正的意志为转移，而不应被操控。传统互联网存在的种种限制让流量的控制权逐步汇聚到了巨头手中。



区块链的发展，必然和以往的行业发展一样，会经历递进的过程。流量作为互联网的基础，在区块链的去中心化时代应当首先被解决。发展的必然

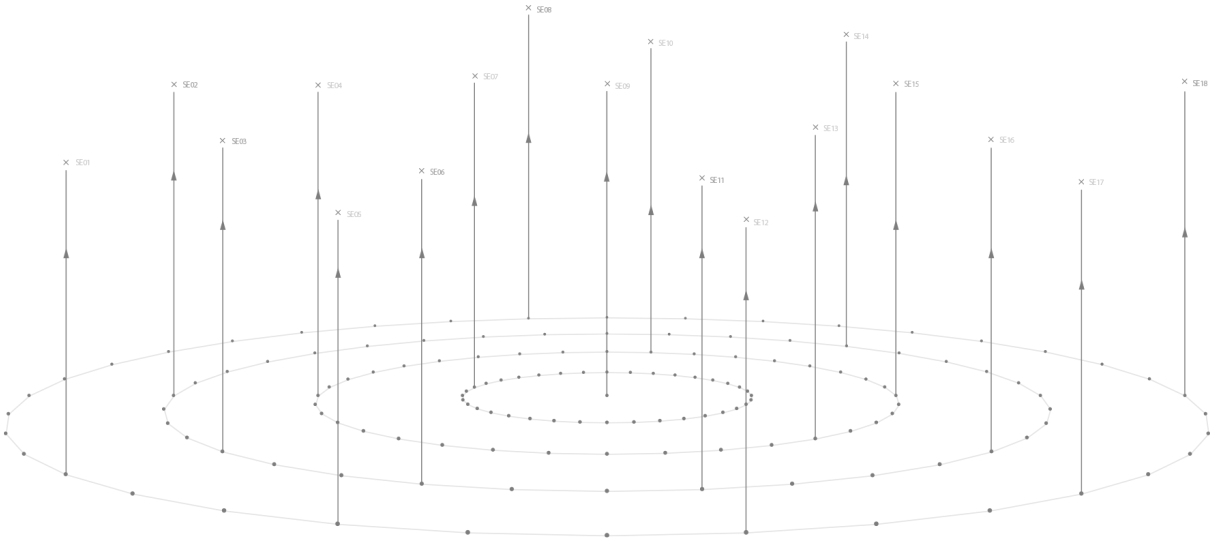
路径将从流量去中心化先行，逐步带动各类区块链基础设施，进而再带动基础应用。

未来5-10年，互联网的应用都将向去中心化转变，新力量币有机会搭建和传统互联网广告模式完全不同的全新流量推动模式，让用户也参与其中，不会被单一商业力量操纵，系统的整体设计并非为



中心化利益服务，而是使得参与在其中的各个角色共赢。

新力量币不仅仅能够作为一个基础的流量平台，除了作为最佳的应用示范，引擎基础链本身还将作为一个流量引擎，使得其他服务商也可以在其上构建自己的流量应用。



## 四、架构

我们的目标是构建去中心化在线流量引擎，新力量币是流量引擎运行的基础。我们将依据去中心化在线流量引擎的技术需求设计区块链网络及业务系统架构，下面我们将详细展开讨论。

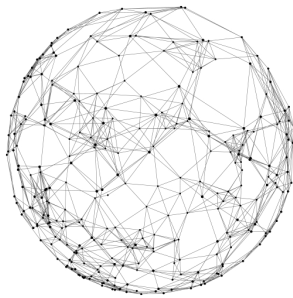
### 4.1 技术需求

在区块链流量的应用场景下，既需要网络上有足够多的节点在线，也需要有多台稳定保持在线的节点，才能够保障整体的流量服务持续和稳定。

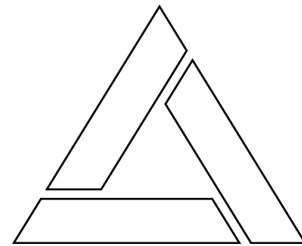
基于这个考虑，我们一方面可以通过PoS共识协议的权益积累回报，保障网络中有足够多的在线节点，因为用户只有打开钱包才能够以类似利息的方式获得回报，这就满足了我们第一个需求：网络上提供足够多的在线节点。

另一方面，由于主节点服务提供了高额回报，因此也将满足我们的第二个需求：网络上有人自发地提供固定IP地址，稳定可靠的全节点提供服务支持。通过主节点扩展服务，新力量币的流量系统将逐步利用主节点服务器提供在线广告素材验证、结算及统计、作弊分析以及分布式的用户画像能力。

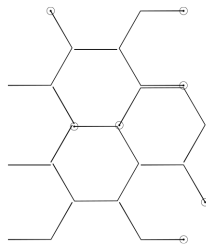
我们期望按照如下特性设计新力量币的基础目标特性：



去中心化：底层区块链网络将被设计为彻底消除对于中间人的依赖，完全独立运行的去中心化体系结构。



安全稳定：稳定运行包括两方面：(a) 区块链网络出块、交易稳定安全运行；(b) 经济体系稳定运行。



可扩展性：可根据服务需求对网络进行扩展，利用主节点服务器形成的第二层网络提供扩展服务。



隐私保护：在去中心化环境下保障特定用户和场景的匿名交易。





在此基础上，逐步丰富完善流量平台业务，使其支持：

- 1、主节点大规模扩展应用：通过主节点服务，逐步支持 (1) 广告素材资源、(2) 跨链、(3) 流量结算网关、(4) 作弊分析、(5) 作为未来基于AI的用户画像的半去中心化数据分析节点。
- 2、素材资源的去中心化存储：支持IPFS星际文件系统及其他CDN类去中心化文件系统的广告素材资源跨链存储。
- 3、开放流量引擎的中间层支持：作为基础公链的开放流量引擎的多平台、多广告形式的去中心化RTB（实时竞价广告枢纽）。
- 4、流量分析专属智能合约：单独为广告流量用户去中心化行为查询设计的智能合约脚本及虚拟机。
- 5、高性能低手续费：通过跨链/侧链的方式支持更快的交易速度，以便于对流量数据进行上链支持和统计。

流量业务将是一个逐步转变为去中心化的过程。在业务开展初期，将主要以中心化形态切入的数字广告流量平台，实现以下目标：

1. 分布式流量平台架构：设计目标支持承载充足流量
2. 自动扩展：根据实际需求进行统计分析跳转的容积扩展
3. 多广告形式支持：文字链、广告条、移动广告、视频广告等形式
4. 多平台客户端SDK支持：新力量币钱包专用接口、浏览器脚本、移动SDK、HTML5内嵌广告、视频广告前贴片及后贴片等。
5. 数字币充值兑付支持：支持新力量币数字货币充值及兑付提取。
6. 防作弊算法：大规模算法保障作弊数据清理。

## 4.2 技术架构

整体技术架构至下而上主要由三个层次组成：

- 1、**存储层**：支持IPFS星际文件系统及其他CDN类去中心化文件系统的广告素材资源跨链存储；
- 2、**网络层**：实现区块链网络，主要包括两层网络（去中心化价值传输网络和半中心化主节点网络）及跨链/侧链；
- 3、**服务层**：向用户提供流量服务，包括价值传输服务、流量交易服务、反欺诈服务、隐私保护服务、用户画像服务等。

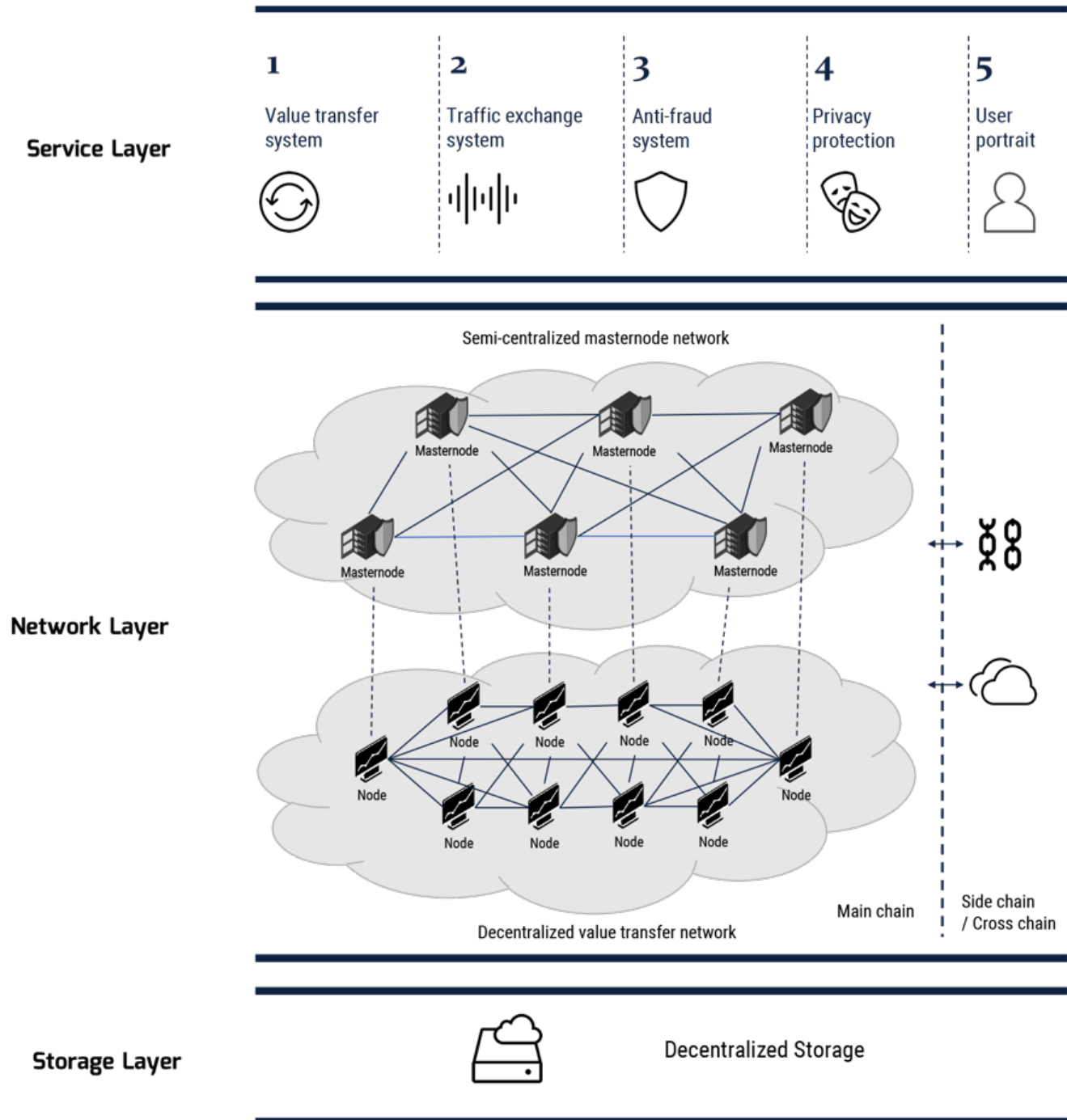


Fig. 2. 网络架构图示

### 4.2.1 去中心化价值传输网络

去中心化价值传输网络用于保障基础区块链的稳定，需要尽可能提高单一节点数量，保障网络的可用性、稳定性及安全性。

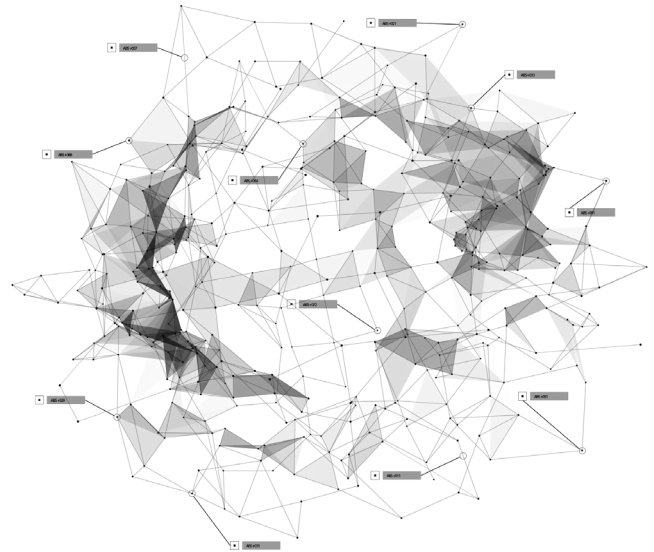
为了在早期维护主网的稳定性，基础主链在早期使用PoW共识，在0-3600个块阶段，设定为主节点70%，矿工30%的形态。为了在网络启动后鼓励更多人使用以便保障网络的稳定性及潜在业务需要，在23601个块后，主网自动切换为PoS共识，奖励为主节点80%，权益积累20%的形态。



### 4.2.2 半中心化主节点网络

主节点网络是相对稳定的，用户需要锁定一定的币量才可以建立主节点，并且可以通过获取主节点奖励。通过利用固定IP地址、提供持久稳定服务的主节点（主节点的持有人将通过提供比基础网络更有价值的服务而获得高额奖励），提供重要的基础服务支持。

主节点网络与底层去中心化价值传输网络相比，相当于一个小型网络，本身也具备达成共识的能力，与基础网络组成一个并行的双层网络结构。



这样做的优点是利用主节点组成的小型网络，可

以实现底层去中心网络难以实现的扩展功能，保障网络的运行效率。由于广告流量服务会进行密集的交易、作弊剔除以及统计分析，必须需要一个额外层的网络才能够保障服务的稳定运行。

### 4.2.3 价值传输服务

钱包作为用户与区块链网络交互的入口，它提供了最基础的价值传输服务。新力量币在早期提供一个功能完善的基于QT Framework的全功能钱包，钱包界面通过调用本地服务，实现了发送、接收、零币、交易记录、主节点设置等基础功能。

在QT钱包完成之后，为了实现更好的扩展性以便提供更高效率的扩展开发以满足业务需要，通过Vue.js前端框架及Electron对钱包进行彻底重构及改造。

改造后的钱包将极大地改善用户体验，通过使用Vue.js作为基本图形界面用于展示，特效部分使用自定义的CSS框架进行效果表现，最外层用Electron引擎构建成支持Mac、Windows及Linux的跨平台执行文件打包。

新钱包一方面作为本地节点，增加网络的稳定，另一方面在后台将直连广告平台的广告输出API接口，在本地进行广告的展示及统计。

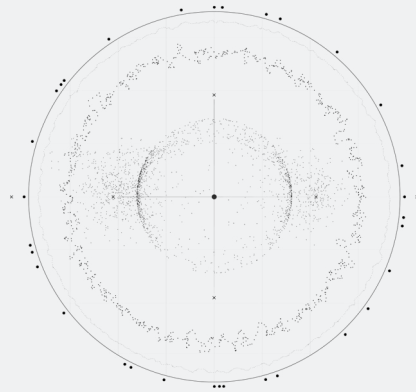
### 4.2.4 流量交易服务

早期流量交易服务将以中心化的方式运行，价值交换依赖新力量币的基础网络及新力量币基础货币作为经济支撑。后续整个平台也将逐步彻底去中心化，运行在链上，逐步进行迁移。同时，流量平台也需要挂接在线运行的主节点，进行作弊校验、统计分析，以及广告资源的存储及获取等工作。

流量平台的主要效用，在前期将被体现为一个集中化的DSP（Demand Side Provider，需方提供商）为广告主提供服务。另外，交易服务将对接新架构的新力量币钱包进行广告展示的处理、广告平台登录等操作。

## 4.3 区块链设计

我们设计基础链的核心目的，是为整体区块链网络的稳定运行，作为最底部的基础链条，用于保障网络真正去中心化运行。通过权益累积保障出块，同时通过主节点作为扩展，能够实现很多传统区块链网络难以实现的支持功能。



### 4.3.1 共识机制

底层的去中心化价值传输网络采用的是共识机制为权益证明（Proof-of-Stake, PoS）。PoS是最早起源2011年bitcointalk论坛QuantumMechanic的机制，核心想法是用“权益”来取代工作量证明的“算力”来达成共识。相比工作量证明（Proof-of-Work, PoW），PoS要更加环保、更加去中心化、激励措施更紧密一致。

权益证明主要分为基于区块链的权益证明以及基于拜占庭容错的权益证明。在基于区块链的PoS中，通过模拟工作量证明，持币者获取出块的权力，并追加到最长链的末端，比如Peercoin、Nxtcoin、Blackcoin等；在基于拜占庭容错的PoS中，伪随机的安排一个验证者在多轮投票的过程中提出一个区块，包括Tendermint、Casper、Ouroboros等。目前，基于拜占庭容错的PoS尚处于理论构建阶段，还未有成熟的实现。因此，本项目采用的是基于区块链的PoS作为底层去中心化价值传输网络的共识机制。

#### 4.3.1.1 工作原理

假设当前区块链的最长链末端区块为 $B_{prev}$ ，下一个需要寻找的新区块B将以 $B_{prev}$ 作为其前一个区块进行引用。节点将基于其具有的未花费交易（UTXO）争取出块的权力，如果UTXO所在的区块为 $B_{from}$ ，当满足以下条件时

$$\text{hash}(B_{from}, UTXO, T, M) < V / D$$

其中，T为当前时间戳，M为权重修正因子，V为当前UTXO的价值，D为当前的出块难度值，HASH为SHA-256函数。节点获得出块的权力，向全网广播新区块B，并获得相应的经济激励。

出块难度随着每一个新出的区块进行调整，调整方式采用区间滑动平均修正方式假设上一区块的难度为 $D_{old}$ ，区间范围大小为 $N$ ，理论出块间隔为 $TS$ ，实际出块间隔为 $AS$ ，则调整后的难度 $D_{new}$ 为

$$D_{new} = D_{old} * [(N+1)*TS] / [(N-1)*TS + 2*AS]$$

当实际出块间隔 $AS$ 大于理论出块间隔 $TS$ 时，调整后难度下降；反之，则难度上升。

权重修正因子（stake modifier）用于防止节点在UTXO被确认后立即开始提前构造新区块。在构造新区块时，节点必须选择该UTXO之后特定时间间隔的权重修正因子计算哈希值。权重修正因子以固定时间间隔进行重新计算。在计算时，依照一定规则选择区块组，并选取区块哈希的特定比特位来构造新的权重修正因子。

#### 4.3.1.2 初始分配方式

在区块链主网稳定后，采用的是单PoS共识机制。为了使PoS可以正常顺利地运行，前期需要在全网进行新力量币的初始分配。我们将采用以下几种方式进行新力量币的初始分配：

1. 主网上线后的第一个区块挖出后，按照主节点预售的比例向早期投资者分发；
2. 主网上线后的约一个月的时间内，通过POW挖矿的方式向矿工分发；
3. 主网上线后，上线全球多个交易所并开通场外交易，使用户可以通过多种渠道获得。

在区块高度1-23600阶段，新力量币使用PoW共识机制。挖矿算法使用NeoScript，将SHA-256替代为BLAKE2哈希算法，一个独立的NeoScript进程将占用大约 $s(N+3)*r*128$ 字节的内存空间。在区块高度23600之后，将仅采用PoS的共识机制进行区块生产。

#### 4.3.1.3 安全性考虑

##### 无利害关系（Nothing at Stake）

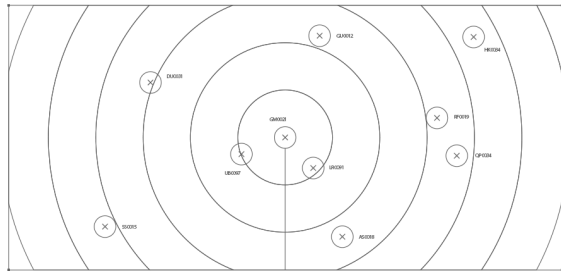
无利害关系指的是：由于缺乏惩罚措施，当区块链发生分叉竞争时，节点会在每个分叉上都创造新块，以保证获得奖励。如果节点想在多个分叉上同时出块，首先需要花费大量时间在代码层面进行修改。相比而言，对正确主链的验证仅仅需要很少的时间。而且，持币者所持有的新力量币是最稳定的激励。如果他在错误的分叉上持续出块，他面临的将是获取不到激励且币的价值降低。因此，无利害关系并不成立，维护网络稳定与每个持币者息息相关。

##### 长程攻击（Long Range Attacks）

长程攻击指的是：与51%攻击类似，通过制造更长的链，重写对攻击者有利的账本，长程攻击可以从很早之前的区块开始，甚至可以从创世块开始。在长程攻击中，如果需要从较早之前的高度开始，这要求攻击者获得足够多的旧私钥。目前，持币量前100的地址的币总和不超过总币量的30%。如果需要发动攻击，攻击者需要搜集到某个时间点获取总和超过总币量50%的地址的私钥。同时，他还需要足够的币用来做主节点的抵押。长程攻击只是理论上可行，在实际攻击过程中具有极大的难度。

### 4.3.2 主节点网络

新力量币很重要的一个能力是在基于PoS共识的去中心化价值传输网络上搭建了第二层主节点网络用来为流量业务提供服务。本质上，主节点也是网络中的全节点，但主节点需要保持长时间在线并提供额外服务来获取相应收益，从而支持网络高效稳定地运行。



#### 4.3.2.1 工作原理

主节点遵循的是服务量证明（Proof-of-Service）协议，主节点服务器通过提供扩展功能获得奖励。目前，实现主节点服务需要在钱包中锁定20000个新力量币，生成可以进行全网广播的主节点服务。主节点服务器上不存储币，而是通过使用二级私钥签名的方式，以保障提供服务的主节点中锁定币的安全性。主节点每隔5分钟，将通过ping消息证明节点在线。主节点在网络上发送所有已知节点的列表的消息，全网节点都将同步得到所有主节点，并且可以随时使用他们的服务。

在主节点网络中，主节点之间采用投票仲裁的方式达成共识。相比底层网络，主节点网络形成的决议优先级更高。由于主节点数量相对稳定，且长期保持在线，主节点网络通过投票仲裁方式可以高效地形成共识。

以即时交易为例，传统交易通常需要等待至少6个块以上的确认来保证交易的不可逆。但利用主节点网络可以加速这个过程。用户可以在全网进行交易锁定，使资金输出至特定的地址中。当交易锁定发送至主节点网络，主节点锁定该交易的输入并将该信息广播到全网，保证该交易被包含在随后挖出的区块中并且在等待确认的时间内不允许其被再次消费。

主节点收到交易请求后生成锁定事务，通过比较锁定事务的Hash与请求锁定输入的Hash，由Hash距离最远的十个主节点组成仲裁主节点组。这个主节点组中只要有六个节点对其有效性进行了投票，则可以成功的锁定交易输入。也就是说，只要选定的主节点组达成了共识，则该笔交易完成，且具有最高的优先级。交易的确认时间基本上等于交易广播至全网的时间。

与底层去中心化网络所使用的共识机制相比，通过主节点组的仲裁投票的方式，主节点网络提供了更加高效的服务，大大提升了底层网络的扩展性。

#### 4.3.2.2 奖励机制

新力量币希望通过主节点网络奖励的方式，给予提供了网络服务的主节点回报，同时利用这些主节点服务器提供流量服务。

主节点通过锁定一定数量币的形式，锁仓保障自己的主节点服务器的稳定运行，得到的回报是80%的区块奖励。相当于投资一台类似“矿机”的服务，获取持续的收益，保障了网络的健康稳定发展的同时，还能对业务进行服务。

运行一个主节点必须通过钱包锁定20000个新力量币，获取的奖励通过新区块下发。一个主节点当天的收益约为：

$$(n/t) * r * b * a$$

其中，n: 钱包控制的主节点数，t: 主节点的总数，r: 当前的区块奖励（当前区块奖励是100新力量币），b: 平均每天的区块数，当前网络每天区块通常是720个，a: 主节点的平均奖励（当前为每个区块奖励的80%）。

全网维护了一个主节点全局列表，当主节点在线时长超过一定时间（约20小时）时，它将被加入到主节点全局队列中。当主节点移动到全局列表的末尾时，剩余的主节点会缓慢地向列表顶部迁移。一旦主节点达到全局列表的前10%，它就有资格从选择池中进行选择。

候选池是全局队列的前10%。它的大小由总的主节点数决定。例如，如果有450个活动主节点，则全局列表中的前45个主节点可供选择。

一旦进入候选池，哪个主节点获得奖励将由Hash距离确定。将候选池中所有主节点的锁定交易的txid和n的哈希与当前高度前100的区块哈希比较，选择距离最大的主节点获取奖励。

在候选池中的主节点，其选择具有一定的随机性，因此无法预测何时获得奖励。假设当前候选池的大小50（即总共500个主节点），那么候选池中的节点被随机被选择的概率是1/50。

下表显示了在特定时间段内主节点获得奖励的概率。例如，在12小时内获得一次奖励的概率约为99.93%。但是，该表不能告诉我们在给定的一段时间后获得奖励的概率。例如：你有一个主节点，已经24小时没有获得奖励，那么你非常不走运，因为这种情况发生的可能性非常低。但是在下一个区块中获得奖励的机会并不会增大，依然是1/50。

时长（小时）	区块数	奖励概率
1/30	1	2%
1/10	3	5.88%
1/6	5	9.61%
1/3	10	18.29%
1/2	15	26.14%
1	30	45.45%
2	60	70.24%
3	90	83.76%
4	120	91.14%
8	240	99.21%
12	360	99.93%
24	720	99.9995%

Fig. 3. 主节点奖励

#### 4.3.2.3 部署方式

为了让主节点的部署更加容易，我们提供了一个简单易用的主节点一键部署脚本，只需在服务器中进行脚本的粘贴即可让多数人实现简单易行的主节点部署。早期的主节点部署脚本只支持单一的节点部署，随着脚本的更新，逐渐支持服务的自动启动、自动更新等功能。

每个主节点都将出现在全局列表中，他们在全局列表中的位置与其上次获得奖励的时间有关。加入网络的新主节点和已获得奖励的主节点放在列表的末尾。通过钱包界面或者使用RPC命令可以激活主节点：

```
masternode start
```

或

```
masternode start-alias
```

如果对已经在运行的主节点重新激活，该主节点将会放在全局列表的末尾，通过钱包界面或者RPC命令：

```
masternode start-missing
```

可以避免这种情况。



#### 4.3.2.4 安全性考虑

##### 女巫攻击

假设主节点网络共有N个主节点，在进行投票仲裁时，每个主节点被选入主节点组的概率为 $1/N$ 。当主节点组中的主节点被攻击者控制时，攻击者可以对主节点网络实施攻击。假设主节点网络中主节点的个数为500，在控制了不同主节点的情况下，攻击者成功实施攻击的概率为：

攻击主节点数	攻击成功概率	攻击所需NPW
10	4.07E-21	200,000
100	7.04E-08	2,000,000
200	9.13E-05	4,000,000
300	0.00569	6,000,000
400	0.105	8,000,000

Fig. 4. 攻击概率

每个主节点的成本为20000NPW，尝试主节点网络的成本很高。如果要获得约5.69%的攻击成功概率，需要控制主节点网络中的3/5的主节点，这也意味着需要购买600万个NPW。考虑到NPW的供应有限（本文发布时约为1300万）以及市场上流动性较低，因此实施此类攻击的难度将非常大。

##### 芬尼攻击

在芬尼攻击中，当攻击者成功找到一个区块时，该区块中包含一笔发送给自己的交易。他先不广播该区块，而是向商家发送交易以获取商品或服务。在产品或服务生成之后，在网络产生下一个区块之前，攻击者立即广播之前挖出的区块从而实现双花。

要阻止芬尼攻击，网络必须能够拒绝违反主节点共识的区块，必须能够通过主节点网络共识系统区分给定交易是否被成功锁定。只有当选定出来的主节点组将锁定成功的消息广播后，网络其他节点才会认为锁定成功，并且拒绝所有与其有冲突的区块。

##### 竞争攻击

攻击者向主节点网络同时提交两个相互冲突的请求，将一个请求提交给特定的主节点以欺骗接收方，同时将另一个请求向网络中广播以取回自己的币。在这样的攻击中，主节点网络将会暂时地发生分歧，但很快地会重新达成一致。主节点网络将只保留一个有效地事务，网络上的所有节点都将删除无效事务，并将有效事务转移到其内存池中。

另一种情况下，当主节点网络因为数据丢失或主节点下线而没有形成最终共识时，客户端的请求将通过底层网络达成共识。

### 4.3.3 匿名机制

我们认为未来的流量服务中，用户隐私是最需要被提及而且保障的。作为保障未来流量交易中用户隐私部分的基础，匿名机制是新力量币的底层能力中的重要一环。

#### 4.3.3.1 工作原理

对于传统的数字货币交易而言，每一笔交易的发送者、接收者及交易金额都将记录在区块链上。这对用户的隐私保护提出了很大地挑战，可以通过网络上各种信息以及与现实世界发生的交互记录等将地址与用户真实身份对应起来。在隐私交易中，发送者与接收者的关联关系应该被切断，使得交易具有匿名性。

新力量币采用的是**零币协议**（zerocoin），基于零知识证明来实现匿名交易。零知识证明指的是证明者（被验证者）能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。

在具体实现时，零币交易通过铸造和花费两个过程，从而隐藏交易的发送者和接收者的关系。通过铸造零币的过程，用户可以将NPW转换为零币zNPW放入零币池中，零币采用多种固定面额的方式存在；通过花费零币的过程，用户给出其在零币池中拥有相应数量零币的证明，就可以从零币池中取出零币进行发送，但该零币完全不附带任何用户地址信息。

下图给出了传统UTXO模型与零币协议的交易过程的示意图。子图(a)中，每笔交易都与之前的交易关联起来，且关联关系公开记录在区块链上；子图(b)中，铸造得到的币与花费的币之间没有一一对应的关系，从而切断了对零币来源追踪的可能。

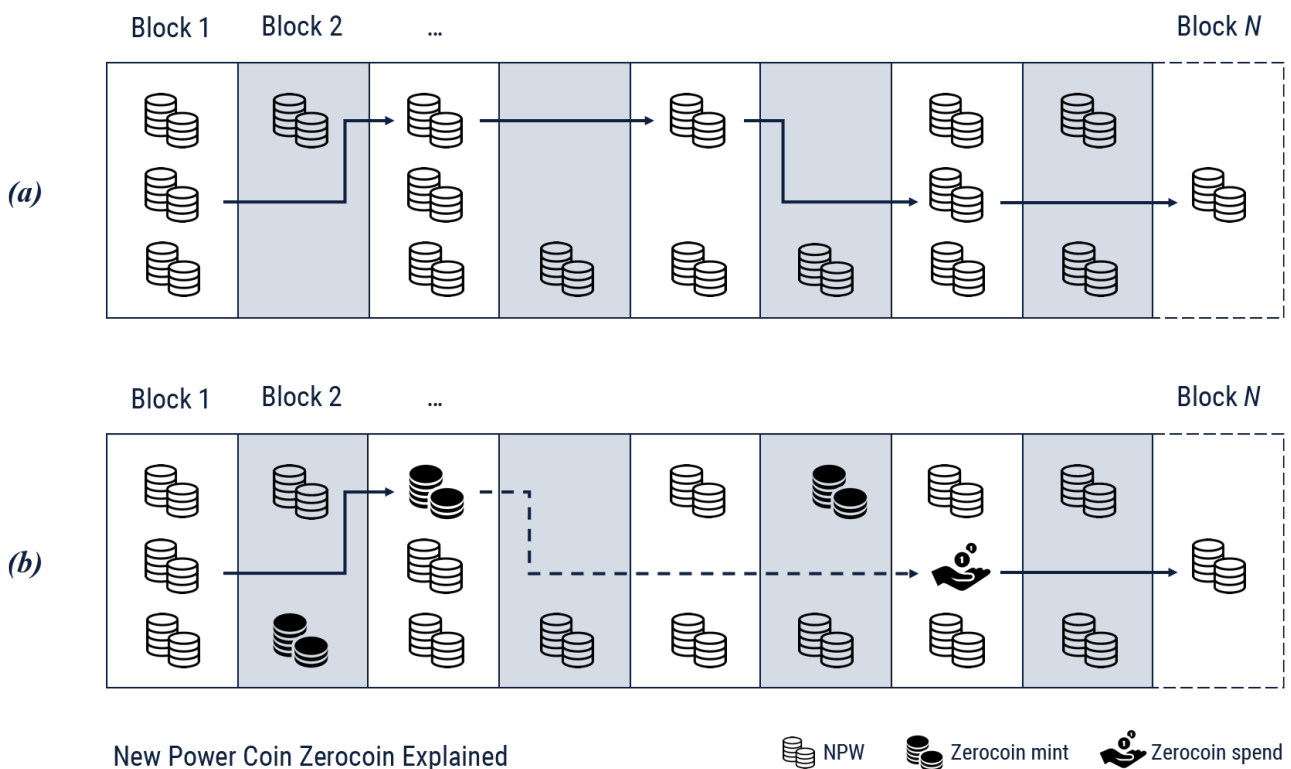


Fig. 5. 零币原理解析



在验证零币花费证明时，逻辑上需要保证相同的零币证明不被双花。节点在验证花费交易时运用零知识证明的方法，不需要知道具体花费的是哪个零币，只需要验证其花费证明是否在之前已被花费掉即可。

如果在零币铸造之后马上就进行零币花费，就会有一定几率将铸造和花费之间进行关联，从而进行时序攻击。为了防止时序攻击，在零币铸造和花费之间需要有一定的时间间隔。目前，新铸造出来的零币至少在相同面额的零币再铸造出3次后才可以进行花费。

#### 4.3.3.2 使用方式

用户在使用零币进行匿名交易时，按照自己的需求首先进行零币铸造，等待其成熟后，再发送给接收者。下图所示的例子中，用户1需要匿名发送125NPW给用户2，用户1通过零币铸造将普通的NPW转换为零币zNPW，分别获得面额100的零币1个、面额10的零币2个、面额5的零币1个；待铸造的零币成熟后，用户1将其发送给用户2，从而完成整个匿名交易的过程。

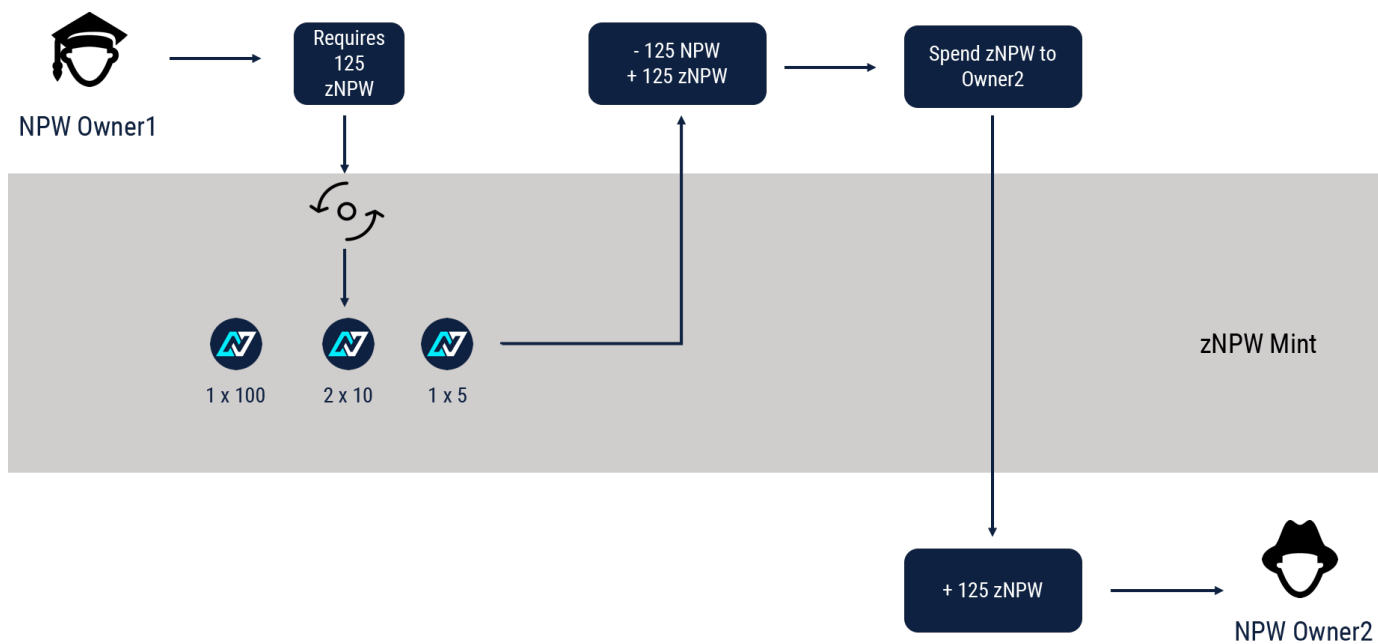


Fig. 6. 匿名转账图解

在新力量币的网络里，广告的交易可以通过匿名交易来保障用户真正的交易隐私，从而实现隐藏用户的交易记录及广告访问记录的效果。

在进行用户画像的过程中，我们还将利用同态加密算法双向确保用户的隐私数据可运算但不可见。通过匿名化的方式，我们可以对用户的任何广告操作行为做定性分析，而完全不会影响用户的隐私，用数学的方式实现隐私保护能力。

## 4.4 流量平台设计

由于具备了完善的价值传输网络的稳定性和二层主节点网络的便利性，新力量币不再局限于传统区块链的确认速度，并能够保障安全性。因此，我们在流量平台上可以实现多种创新业务，通过先建立中心化的业务平台，最终逐步过渡到去中心化的流量引擎。

### 4.4.1 业务规划

我们将分六个阶段逐步展开去中心化流量业务：

第一阶段将以“**新力量币兑付**”为切入点开展广告流量业务。新力量币作为有价值的数字货币，基础作用可以进行流量购买及交换，对比法币最大的优势是充值、流量采购都可以变得即时、自助，不通过任何充值平台或银行，从而更有效率。

第二阶段将会进行“**广告资源上链**”。主节点网络在保证服务稳定的同时，还可以作为广告资源（包括广告图片、音频、脚本、视频等资源）的分布式存储。因此，主节点将首先将替代一部分CDN的存储能力，在稳定后逐步迁移至IPFS或其他分布式去中心化存储资源中。

第三阶段将开展“**行为数据上链**”。用户与广告主、流量来源之间所有的对应，广告展示数据，广告点击及用户后续可跟踪到的行为数据都将上链存储作为后续的数据分析的基础。

第四阶段将实施“**用户画像计算**”。由于广告的精准确匹配需要进行用户画像，那么需要更充分的计算能力。由于流量平台是去中心化运转的，因此计算能力必须位于分布式节点上，因此这部分我们需要引入跨链/侧链的方式获取算力。

第五阶段将实现“**用户画像上链**”。用户画像将以智能合约的方式提供，这样广告主可以通过智能合约的自助查询方式，获取到精准配其需求的广大用户群体。

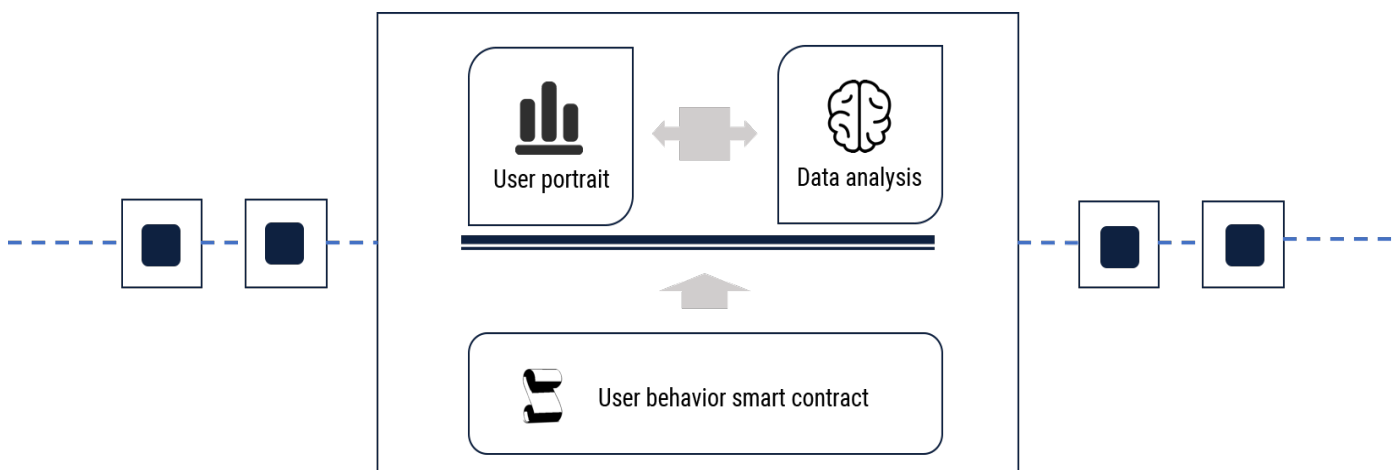


Fig.7. 用户画像上链

第六阶段将完成“**用户隐私服务**”。流量平台将支持隐私化的数据全区块链流量流转，在强有力的隐私保护的前提下，去中心化地为每个人进行定制化的全方位匹配服务。

## 4.4.2 业务逻辑

### 4.4.2.1 广告平台

基于新力量币的底层区块链，我们开发了初期的广告平台，作为应用的基础平台及未来作为基础流量引擎的示范，实现多种最基础的广告平台功能。

广告平台支持账户注册、广告主充值、广告投放、流量主广告代码及SDK获取、新力量币后台结算以及支持一个基于新改版的钱包的广告展示能力的后台投放系统。

广告后台的所有结算都完全基于区块链，广告投放后台的所有的区块链的功能、主节点的扩展功能以及交易功能都将基于新力量币的区块链进行开发。

用户注册广告平台后，账户将会自动在广告平台服务器本地建立新力量币钱包，钱包与账户冷热分离存储，用户的广告交易、储值都将存放在这个钱包内。同时，重要的点击行为也将上链存储，广告平台提供与区块链的操作接口，用于进行区块链的调用操作。提供的区块链操作接口实现广告投放模块、广告管理模块、防作弊模块、计费模块、结算模块对广告整个投放周期的维护和管理，通过节点对广告进行分发，网页、钱包、App等通过节点的接口获取广告进行展现。用户在广告投放过程中，交易快速、安全、稳定，杜绝作弊。

Order ID	Campaign Name	AD ID	Icon	App Package Name	Platform	Budget	Price	Amount	S	Creation	Operation
1020000015	Test Campaign	8363F878-05F1-431E-990E-8C828C224CC9		com.android.mediaplayer	Android		0.00003 N	0	<input checked="" type="checkbox"/>	Aug 8, 2018 11:15:06	
1020000014	Test Campaign	8363F878-05F1-431E-990E-8C828C224CC9			Web		0.00003 N	0	<input checked="" type="checkbox"/>	Aug 8, 2018 11:12:12	
1020000013	Test Campaign	8363F878-05F1-431E-990E-8C828C224CC9		com.android.mediaplayer	Android		0.00003 N	0	<input checked="" type="checkbox"/>	Aug 12, 2018 05:09:00	
1020000012	Test Campaign	8363F878-05F1-431E-990E-8C828C224CC9		com.android.mediaplayer	iOS+Android		0.00001 N	0	<input checked="" type="checkbox"/>	Aug 12, 2018 00:00:00	
1020000011	Test Campaign	8363F878-05F1-431E-990E-8C828C224CC9		com.android.mediaplayer	iOS+Android		N/A	0	<input checked="" type="checkbox"/>	Aug 12, 2018 00:00:00	
1020000010	Test Campaign	8363F878-05F1-431E-990E-8C828C224CC9		com.android.mediaplayer	iOS+Android		N/A	0	<input checked="" type="checkbox"/>	Aug 12, 2018 00:00:00	
1020000008	Test Campaign	8363F878-05F1-431E-990E-8C828C224CC9		com.android.mediaplayer	iOS+Android		N/A	0	<input checked="" type="checkbox"/>	Aug 12, 2018 00:00:00	

Fig.8. 广告平台预览

#### 4.4.2.2 充提兑付

根据不同角色，广告平台提供不同的充提兑付策略。

针对广告主，系统要求使用新力量币先充值后消耗，系统提供两种消耗方式：

- 1、固定限额消耗：设定广告Campaign时，指定每日消耗广告金额。
- 2、预算额度消耗：指定预算总额，系统将自动设定填充率和投放比，达到最优投放效果。

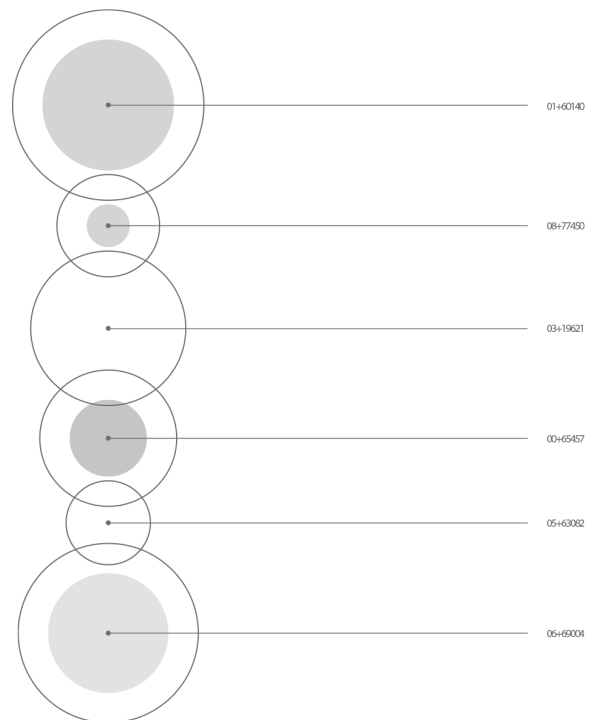
**广告主：**充值使用新力量币进行充值，类似数字货币交易所的形式，币直接打入流量交易平台的新力量币充值地址中，即可进行广告消耗。广告消耗直接使用用户在平台钱包内的余额，并在余额消耗结束后自动停止广告的投放并通知给广告主。

**流量主：**通过进入后台获取广告代码或SDK，流量主可以直接通过在自己网站/App上展示广告的方式赚取新力量币收入。广告平台支持每小时自动结算对账，结算的币将自动进入流量主的广告平台钱包，并可以随时提取。

**钱包用户：**我们设计了一种新型的广告形式，为使用钱包进行PoS权益积累的用户提供可选择的广告服务。用户打开钱包进行权益积累的过程中，可以自行选择是否展示由广告平台提供的广告，如果用户允许广告显示，则将按展示和点击数，通过广告矿池定期自动给用户钱包发送一定数额的广告回报收益，用户可以直接通过平台内钱包进行提取。

广告平台的整体结算使用新力量币的区块链网络进行处理，提供严格的安全处理措施。充提部分提供风控模块，绝对保障大额广告主及流量主的现金安全。

广告主及流量主的账户使用100%冷钱包，模块对接至广告平台的结算中心，杜绝私钥被盗风险。对接结算出口，冷热钱包隔离，通过多重证书签名的方式进行更安全的加密安全措施，保障最终结算的安全性和稳定性。





#### 4.4.2.3 用户钱包

前期，新力量币提供了一个基于Bitcoin QT的钱包客户端，用于实现发送、接收、零币以及主节点设置等功能。

基础钱包核心用于在早期提供新力量币基础区块链运行的基础能力，基础钱包的运行基于一个命令行客户端。主节点服务的设定也依赖于新力量币服务程序，在服务器上为主节点网络提供整体服务。基础钱包通过端口61472与其他客户端进行通讯。

PoS权益积累要求用户全程打开钱包软件才能够进行挖矿奖励，也是通过基础钱包的核心功能实现的。

#### 区块浏览器

钱包内部还内置有一个完整的区块浏览器可以查询所有区块链上的完整信息。区块浏览器的功能包括跳转、查询、查看交易详情。所有交易都将完全记录在链上供查询之用，不可篡改。

任何人也可以自己搭建自己的新力量币区块浏览器，当前作为例子，开发者提供了一个可以查询主节点网络的区块浏览器供用户使用。

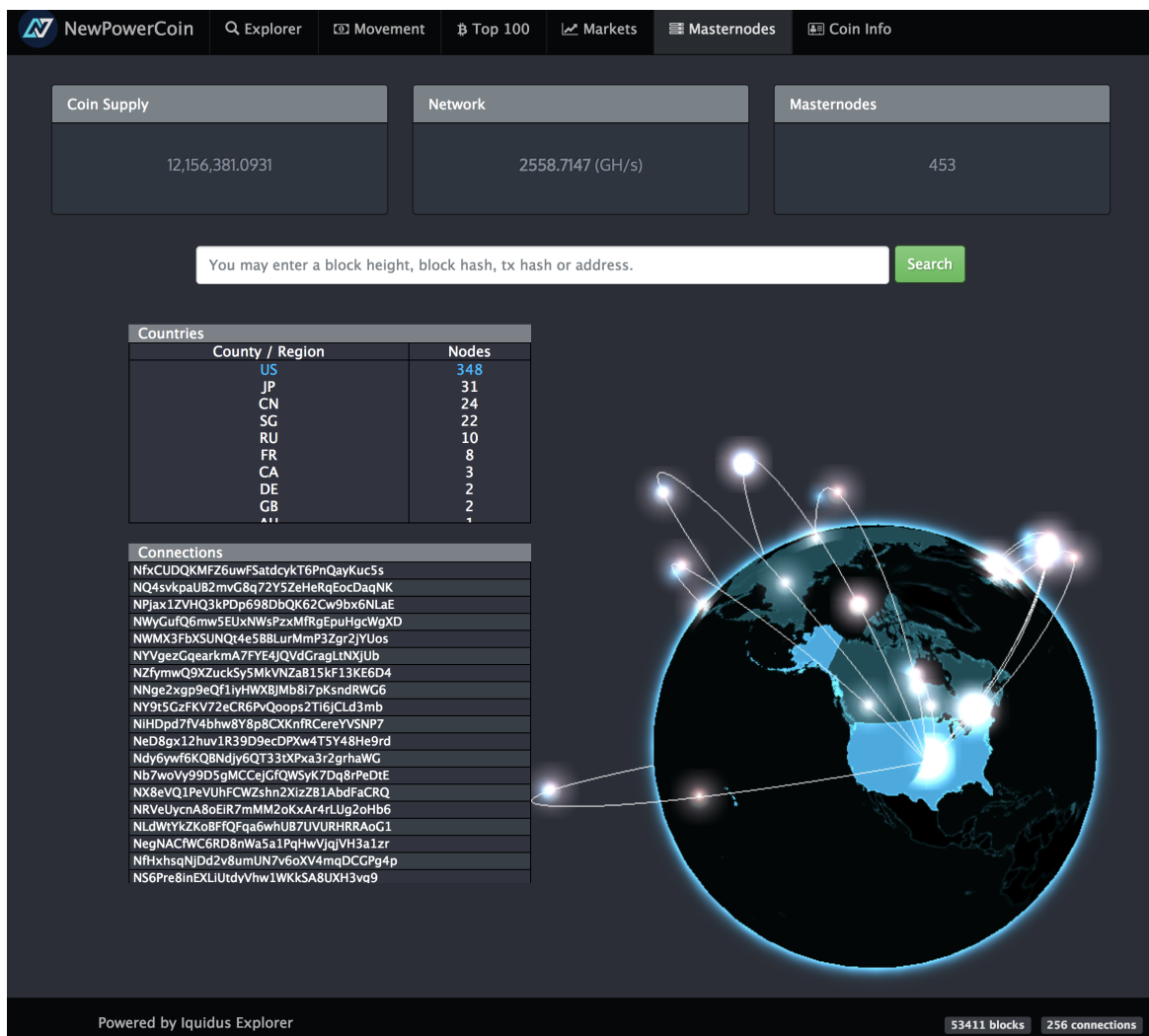


Fig.9. 区块浏览器



去中心化网络要实现广告投放最好的方式是拥有足够多的去中心化的节点，每个节点既可以作为区块链的服务提供者，也可以作为服务的接受者。这种终极模式是我们期望实现的最终流量引擎的形态。

要达到这一阶段的设计需要，现有的基于QT版本的钱包难以满足未来的拓展开发需求。因此我们重写了新力量币的钱包，用来作为未来的区块链流量引擎的底层。

## 易用性

我们观察到，目前的区块链使用者的绝大多数不具备初级的计算机使用能力。加密货币之所以流行受阻，很大原因也是传统的软件开发者并没有针对最终用户进行考虑，多数的软件都仅仅是个技术演示而非真正的软件产品形态。因此我们希望让所有的用户都能够用上我们的钱包，作为新力量币的节点通过PoS权益积累获取利息的同时，也可以变为广告服务的节点和广告服务的接受方，让全体网络共同受益。

基于这个原因，首先我们基于CSS3重新设计了一套全新界面，在这层界面的基础上进行钱包软件的设计工作。

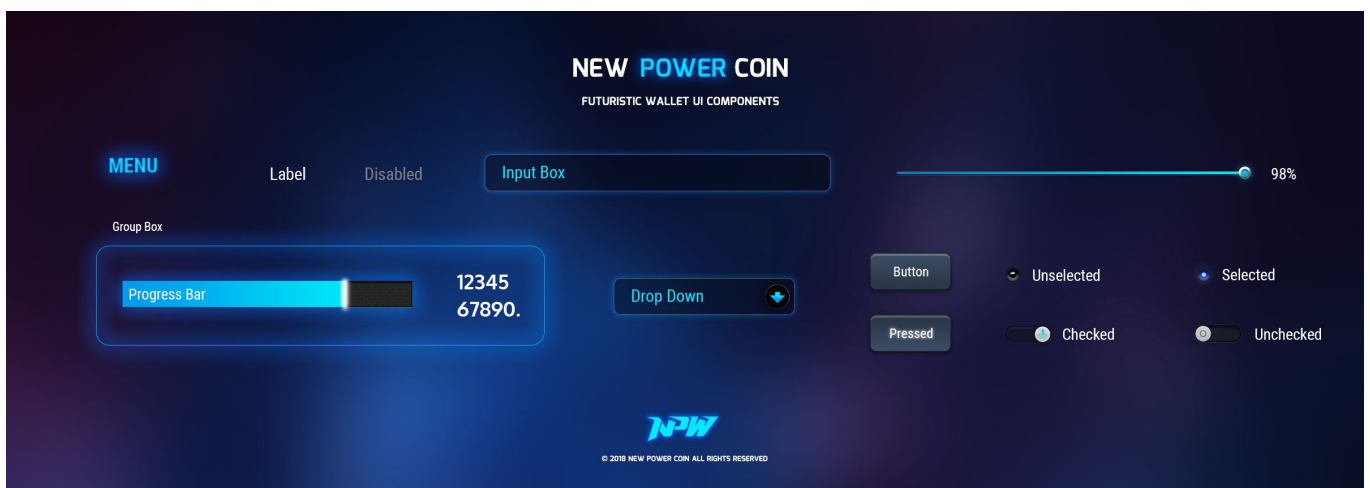


Fig.10. 钱包UI框架设计

钱包利用Vue.js作为基础框架，将除钱包节点服务之外的所有操作，都变为前端开发工作。随着新力量币网络的逐步升级，开发工作将越来越简单，便于维护。

与操作系统通讯调用部分，我们使用Electron框架，真正保障跨平台能力和扩展性。



Vue.js



Electron



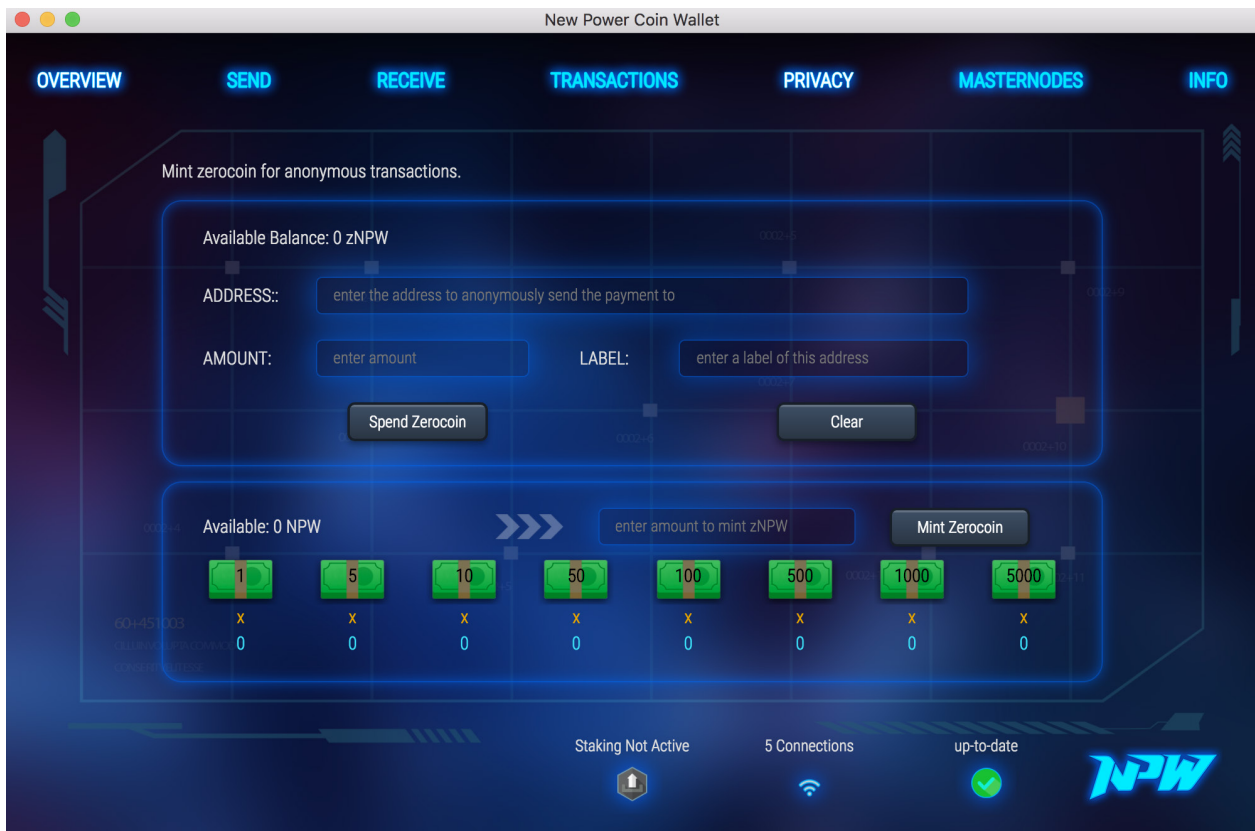


Fig.11. 钱包样式预览



## 扩展性

我们在钱包中实现的第一个扩展能力是一个广告展示框架，后端通过广告平台搭建的矿池提供区块链计费，前端用户只要打开钱包进行PoS即可看到广告并获得广告服务费，自动打入用户钱包账户地址。

广告平台后台登录也将被嵌入钱包内，广告主和流量主均可以直接在钱包利用私钥进行广告平台的单点登录，支付、转账等流量业务的基本功能。

广告流量引擎发展到终极形态的版本中，将不再有中心化平台，钱包即平台，平台即钱包。平台功能均置入钱包内进行管理和执行。在这一前提下，由于去中心化服务，区块链网络也无需过多考虑广告并发量及负载平衡等指标，只作为扩展的前端能力开发即可。

### 4.4.2.4 多平台广告支持

平台支持多个操作系统和多种类型的广告形态。

## 广告的形式

广告脚本代码支持：

文字广告：通过编写不同内容的文字链接，通过URL跳转形成的广告形式；

横幅广告：通常为不同尺寸的图片/动态图片组成的广告展示内容；

弹出广告：自动弹出的网页广告；

动态广告：使用HTML5或Flash技术设计的交互或动态广告；

视频贴片广告：在视频的前/后进行的广告插入。

未来将支持：

Alexa及其他语音助手的音频类广告；

跨链区块链形式的广告。

## 业务形式

广告的业务形式包括：

CPC：Cost Per Click 按点击计费；

CPM：Cost Per Impression 按展示量收费；

CPA：按用户行为计费（注册、观看等）；

积分消费：引导用户消费行为并给予积分奖励的广告；

社区群组广告：社区及讨论组推广；

口碑营销广告：通过推荐的方式带来新用户增长；

任务型广告：完成指定任务后即可获得现金收益的广告。



## 广告服务的行业及平台

数字广告不仅仅惠及传统的互联网，还能够惠及更多行业。服务的行业及平台包括：

传统互联网；

移动互联网;

移动HTML5及小游戏、即点即玩游戏等。

未来还将包括：

区块链社群;

AI、B2C产品;

物联网产品，可穿戴及智能家电；

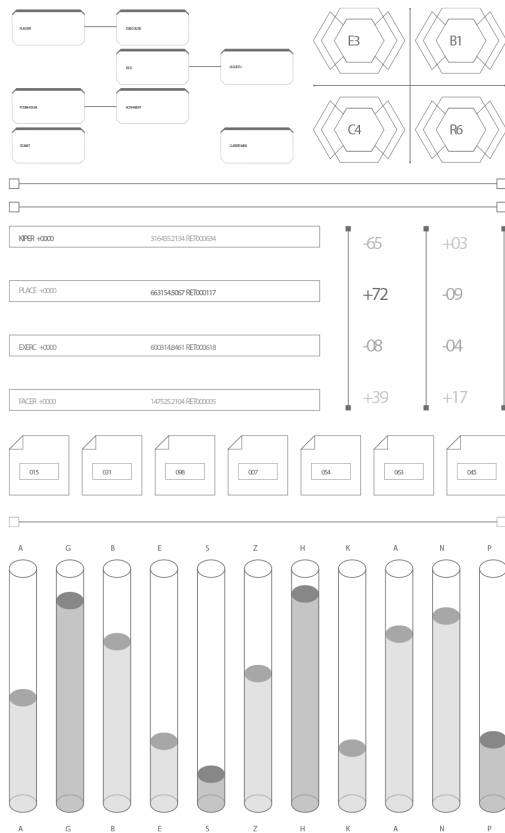
自动驾驶。

## 反作弊防护

互联网广告一个比较重要的痛点是非常易于作弊，传统大平台需要耗费极高的人力财力进行防作弊的管理。广告平台处理作弊管理分两部分，一部分是传统的防作弊处理，另一部分是基于区块链钱包的防作弊处理。

传统广告的防作弊：传统的流量防作弊的方式，通常使用限制来源的请求频次和请求量的方式，对于单一的来源，限制为一个固定的值。同时，将广告从展示、点击、行为等操作通过一个加密的指纹进行来源追踪。如果没有指纹或者指纹数据有误，或者广告的请求频次过大，通过来源ip、用户的行为标识，超出则判定为异常流量，最终通过日志结算时，异常流量将被剔除。此类的点击行为，还可以通过大数据机器学习进行标注，达到大规模降低作弊率的效果。

区块链钱包广告的防作弊：钱包通过加密的签名提供唯一性校验，广告回报和钱包自带的节点绑定，通过签名进行广告的展示和点击证明，验证是正在展示广告的钱包才可以被认为是合法交易。



### 4.4.3 业务架构

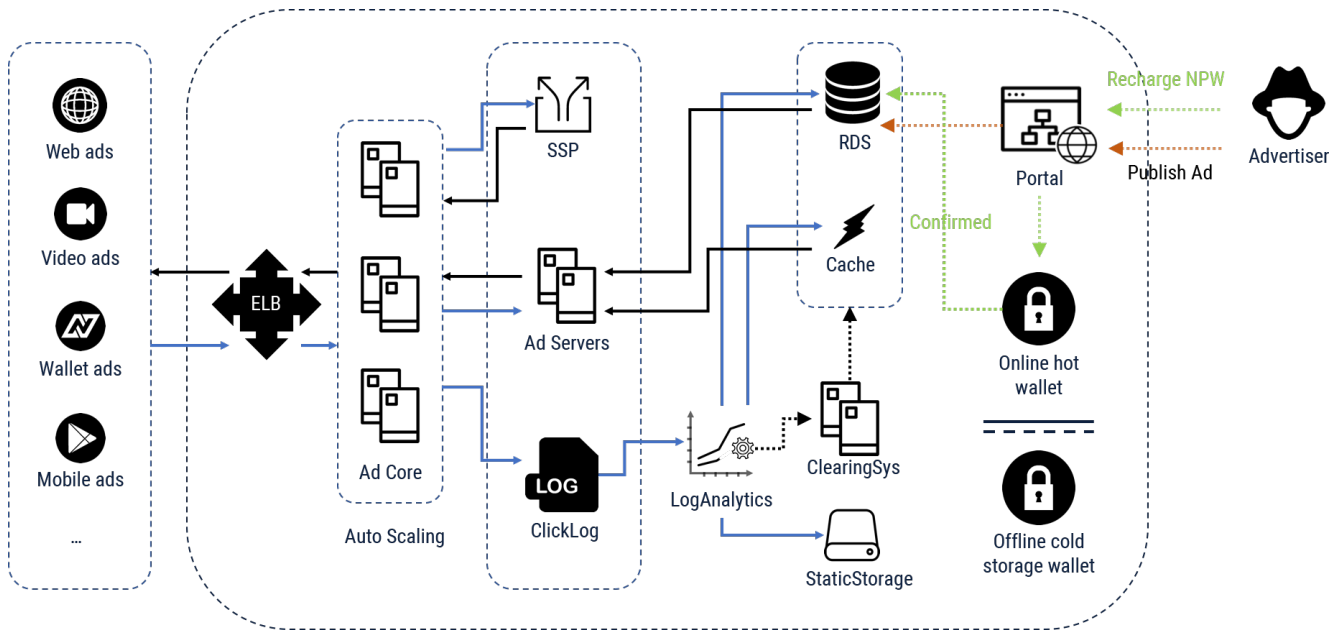


Fig.12. 广告平台业务架构

如图为广告平台的技术架构，下面将逐步解释其内容。

广告流量平台系统通过与底层基础链挂接以及架设单一主节点的方式，进行广告流量应用的服务支持。

我们通过架设一个安全完备的广告平台，同时支持多个广告主、流量主以及超大点击量支持的系统，后端对接新力量币的主链作为区块链的结算支持。广告平台支持区块链的部分包括：充值、结算、交易等方面。类似一个中心化的币币交易所，我们将在前期推出的广告流量服务也是一个基于中心化的广告流量基础服务。

#### 4.4.3.1 广告核心系统

作为广告平台的核心，通过底层区块链网络，保证了节点的可靠性和价值传输的安全性，并针对广告的投放实现了一套广告投放与展示的激励机制，对各个节点的广告请求、展示和点击等广告行为实现奖励。奖励通过结算模块直接发送到节点的默认钱包地址，由于结算的链上完成，可以保障广告平台的公开透明以及可追溯。

广告管理模块：通过节点提供接口来对钱包广告的发布进行管理，包括广告的预发布、广告发布上链等功能。任何人都可以通过下载钱包来实现广告的发布。

广告投放模块：主要是对钱包节点的广告投放请求进行鉴权、匹配、定向、优化等处理之后进行广告的投递。保证广告请求来源的合法性以及广告展现点击的验证。

防作弊模块：主要是针对钱包节点绕过或者欺骗投放模块进行广告投放行为的检测，对于验证不通过的广告请求行为进行相应惩罚的模块，以及对于异常流量进行限制投放频次或者降低收益。

计费模块：主要是对广告投放的CPM、CPC等方式进行投放计费，避免超量或者投放不足的情况产生，最终按照广告投放的策略进行计费。

结算模块：主要是针对流量主的流量消耗以及广告主广告消耗针对流量主进行奖励机制的模块，也就是系统对钱包节点进行奖励的模块。

对于流量平台，新力量币的区块链可作为一个去中心化的数据库，在这一个广告服务中起到的作用首先是数据存储功能，通过区块链的方式将最基础的结算数据存储上链。广告主和流量主均可以通过系统提供的接口进行一系列的数据查询，包括展示情况，点击情况、用户操作行为情况、统计分析、结算以及反作弊等数据，与区块链对接的接口包括Socket接口和HTTP接口两种，开发者也可以通过GraphQL进行定量分析。

先期阶段，所有的广告结算将通过新力量币的基础链交易方式写入区块链，保障广告收入结算公开透明不可篡改。后期将通过跨链/侧链的方式，逐步将所有展示及点击数据上链统计，通过去中心化的分布式存储进行数据分析。

#### 4.4.3.2 主节点系统

同时，针对主节点的改造将是逐步的，成系列的。当前的主节点能力仅仅提供了快速交易和隐私两个方面，广告平台本身也将逐步对于主节点进行一系列的扩展改造。

由于广告平台本身就是一个自我驱动，内部自成体系循环的流量交易所，流量通过新力量币进行承兑，从结构上广告平台本身与新力量币的区块链是紧密结合不可分割的。

通过在钱包节点实现与主节点通信的RPC API，供广告主进行广告投放，或流量主对广告进行展示得到的奖励。RPC的API包括广告管理模块（AdManagerMod）、广告请求（ImpMod）、广告点击（ClickMod）、防作弊（AntiCheatingMod）、RPC授权模块（RPCAuthMod）等组成。

广告管理模块：主要提供广告发布、广告获取、广告消耗等信息的查询RPC接口，广告主登录Dashboard平台通过调用RPC发布自己的广告，获取广告的消费数据，以及历史投放广告的信息。

广告请求模块：主要提供广告请求的RPC API，通过流量主获取广告核心模块的投放信息，并将返回广告数据展示在投放媒介来获取奖励。

广告点击模块：主要通过获取用户的广告点击行为和广告展示场景生成作弊校验算法，并将用户点击行为转发至主节点进行验证，并记录用户行为。

防作弊模块：主要是针对钱包节点广告展现和点击异常流量进行清洗以及限制的模块，针对钱包节点投递的广告进行跟踪和指纹验证，避免恶意流量流入广告内核。

#### 4.4.3.3 广告后台系统

广告后台系统主要提供广告主平台管理和流量主平台管理两部分，由于广告平台全部采用新力量币进行结算，因此广告主必须充值新力量币才能利用广告平台进行广告投放，新力量币索取方式可以通过OTC平台或者交易所进行购买，或者直接在广告平台的OTC区从流量主进行购买。

**广告主平台管理：**主要提供广告投放、广告投放历史查询、广告投放消耗等信息查询；

**流量主平台管理：**主要提供流量主流量消耗、流量收益、以及支付记录查询。

#### 4.4.4 业务扩展

##### 4.4.4.1 负载均衡处理

平台初始设计为日十亿次以上的交易处理，可以支持各类展示、点击、视频播放以及如安装应用等用户行为广告，以及未来扩展支持线下的视频、智能音箱、车载等广告形式。需要支撑的主要负载来源是通过日志记录广告请求并结算。

##### 中心化的高并发方案

接入层的解决方案：初期广告接入层通过 ELB（Elastic load balancing）对接桌面客户端及 SDK 进行广告投放，广告投放核心通过无状态设计支持水平和垂直可扩展能力来提升广告投放的容量和高并发访问量。能够轻松快速扩容增加广告平台接入能力。

广告投放核心的解决方案：广告投放核心采用高效规则匹配引擎，能够精准快速定位目标广告，增加广告转化率以及流量主收益。

数据处理层的解决方案：日志处理引擎采用分布式内存实时分析引擎结合多维分析数据模型，能够轻松处理亿级别的行为数据，通过机器学习能够快速识别异常日志，并还原用户真实流量和收益。

## 去中心化的高并发方案

由于去中心化的广告投放通过智能合约来完成，智能合约的运行常驻内存，天然保障了广告投放单节点的性能问题。然后通过扩展主节点数量可以水平无限扩展，来支撑广告平台的高并发接入。

### 4.4.4.2 主节点扩展

流量引擎的很多底层机制，都需要对于主节点进行各种类型的扩展。隐私交易和快速交易仅仅是针对主节点提供服务的一个基础案例，基于广告流量平台，对于主节点服务器功能的扩展规划包括：

1. 去中心化CDN存储及跨链IPFS数字广告素材文件索引支持
2. 统计分析及防作弊广告点击验证
3. 用户数据隐私保障
4. 用户标签及用户画像
5. 大规模广告统计数据压缩分析
6. SDK及广告脚本的远程随机校验

这些能力都将随着流量引擎平台的搭建，逐步拓展。目的是为了通过广告平台，逐步提供一个去中心化的流量支持引擎。

## 用户画像及隐私保护

为了对广告进行精准投放，对于用户行为需要有深度的画像能力和标签设置能力。

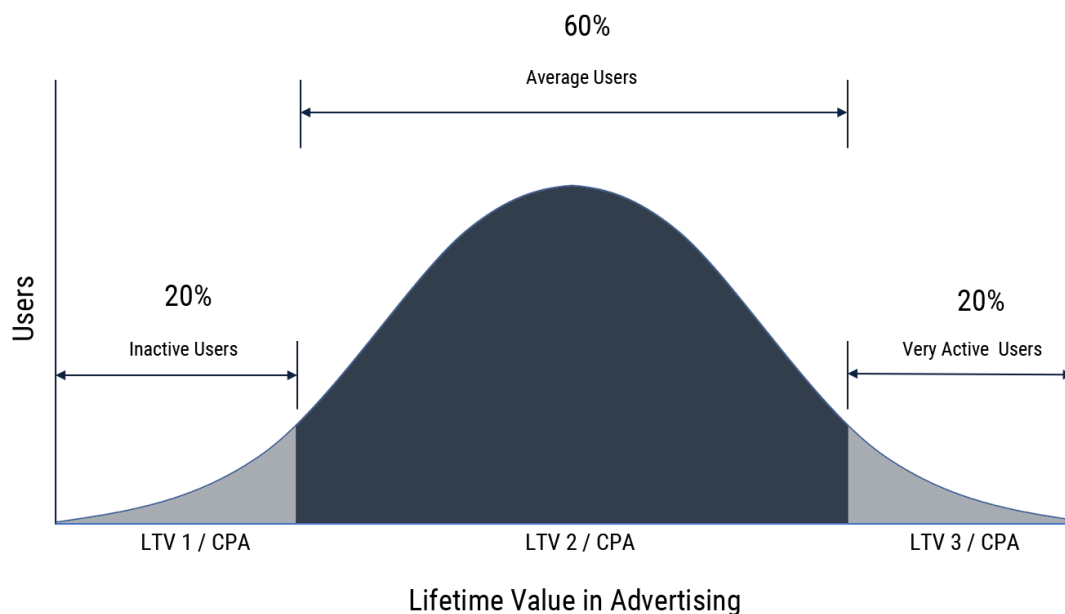


Fig.13. 广告中的用户生命周期

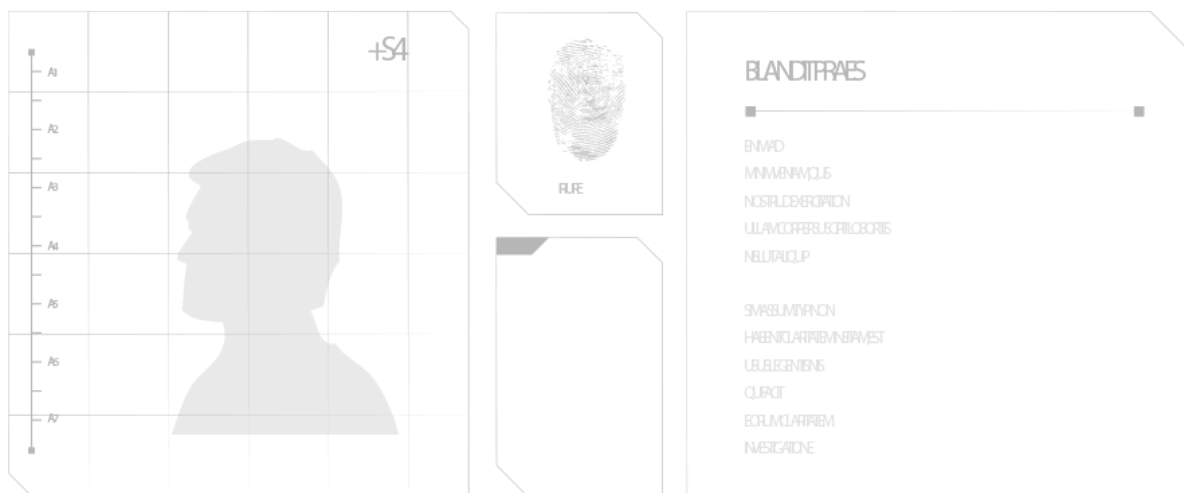
LTV (Lifetime Value) 在广告平台中, 通过标签的形式展示。广告主可以在投放的过程中, 自行选择用户的年龄、性别、位置、喜好等详细内容, 达到精准匹配的效果。

通过LTV可以了解用户真实的价值, 最大化有价值的用户。对于用户来说, 好处是可以精准获得自己所需的商品和服务。

传统的广告服务, 基于LTV的投放所得到最大的诟病是对于用户隐私保护, 用户在享受精准投放广告的过程中, 最担心的也是自己的私人信息被第三方中心化公司掌握过多。

得益于新力量币的主节点服务功能, 广告平台可以最大化地通过主节点的改造, 去中心化地对于用户的画像进行分析, 同时最大可能保障用户隐私数据不被任意第三方掌握。

举例说明: 利用混币的原理, 不同用户的相似浏览行为同时输入到主节点服务中, 通过主节点服务混合后返回不同输出, 以便达到正确效果的同时, 任何一方都无法获知用户的真正标示。通过零知识证明, 可以让用户享受到精准的服务, 而第三方广告主获得最大化收益的过程中, 用户的数据不被任何第三方公司拥有。





#### 4.4.4.4 基于流量引擎的智能合约

作为流量服务的基础引擎，不仅仅需要在广告流量支撑方面提供服务，还需要提供自动结算能力。为此，新力量币将提供一套基于广告流量统计、用户画像查询、大数据分析的智能合约脚本引擎。脚本机制类似R语言，用于在链上执行用户分析及精准匹配能力。

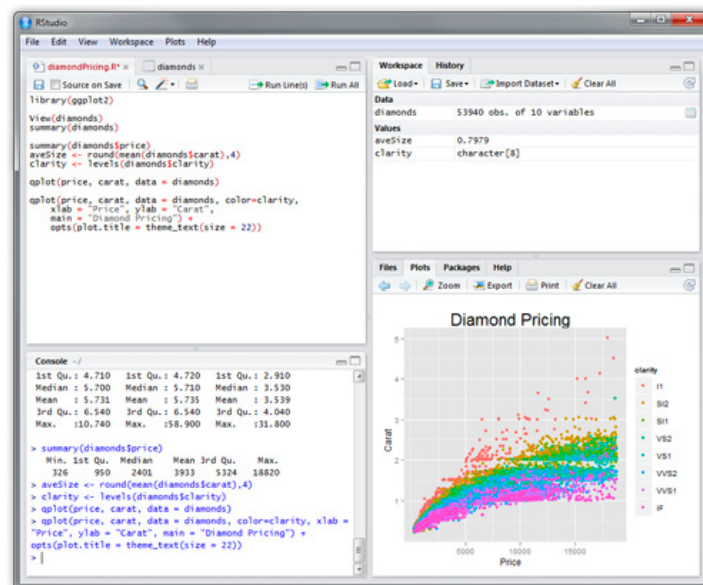
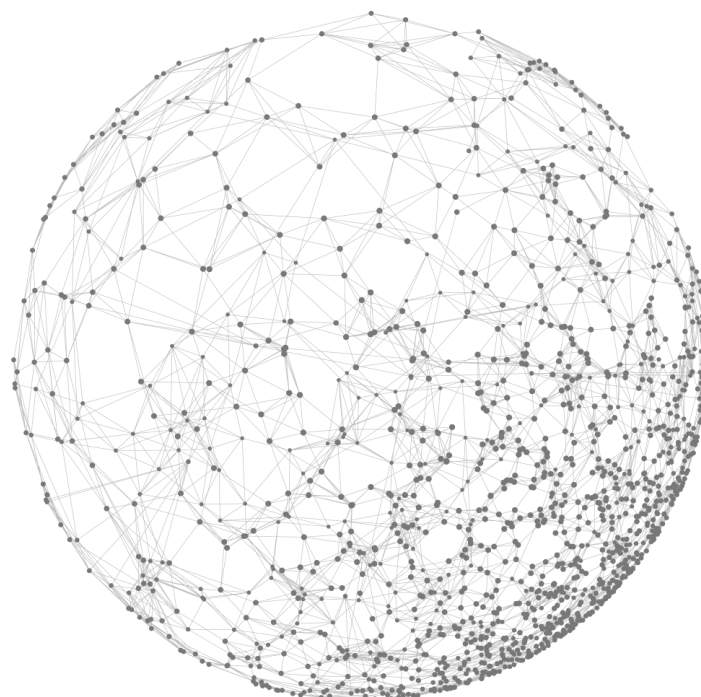


Fig.14. 将参考RStudio开发智能合约编辑器

#### 4.4.4.5 业务全球化

前期我们通过小规模市场试用，开始切入、完善广告业务，逐步切入全球每个角落。



## 五、经济

我们不认可如今权证（Token）的方式，它们并非去中心化的经济设定，而是所有的规则及权证的拥有权仍然归属于一个中心化的体系。因此，为了最终实现一个去中心化网络，我们通过一个上线的主链稳定运行作为整体实现路径基础。

### 5.1 经济设计原理

在发布本白皮书之前，这个新力量币的主网已经提前启动，稳定、安全地运行了一个阶段，并平稳地度过了PoW初始阶段，进入了PoS权益积累阶段。

为了实现流量归属用户，在不影响甚至提高用户体验的前提下进行去中心化广告的终极目标，经济的设计至关重要。

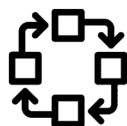
众所周知，数字货币的波动性有些时候可能相当严重，正因为主节点具备极强的锁仓能力，这对于维护新力量币价格的稳定拥有很重要的作用。

同时还需要考虑到，随着科技的发展，数字货币的总价值将极大提高。

我们希望在经济设计的过程中，考虑到互联网整体的经济发展以及流量发展，实现如下特性：



流量平台的自我增长能力



业务流动性的扩展能力



多方参与者自治和共识



与底层技术增强开发相辅相成，互相推进



经济闭环的整体价值提升



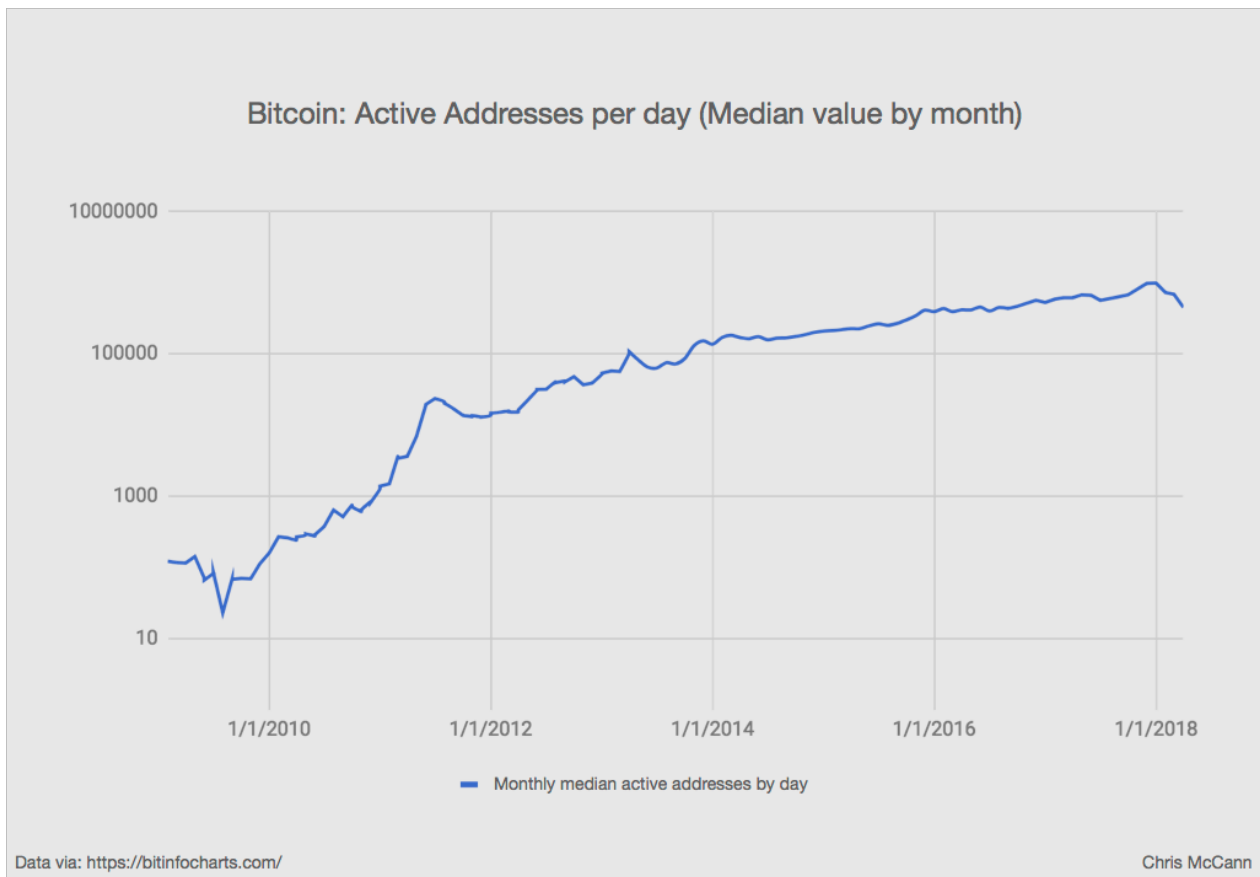


Fig.15. 比特币每日活跃用户地址数 © 2018 Chris McCann

以上是比特币活跃用户增长曲线，我们可以见到，在比特币主网上线后的一年多时间里，用户急剧增加，而第二到第四年仍处于快速增长期，随后增速放缓——大部分知名的区块链项目都有类似的现象，而比特币的产量却是固定的每四年减半，即其通胀设置与实际的用户增长并不同步。

如此设定会造成早期用户对收益期待过高而惜售，形成通缩，被资本利用进行过度炒作，继而一旦泡沫破灭，价格又陷入崩盘状态。即使是最被市场认可、价格最为稳定的比特币，牛市和熊市对比，价格亦相差数十倍，这样并不利于保持整体经济体系的良好运行，不能使加密货币真正得到有效的应用。

因此，我们对新力量币的产量作了如下文介绍的设置。

## 5.2 基础经济数值

所有的新力量币都通过挖矿挖出，新力量币在四年后的总供应量约为7300万，十年后的供应总量约为1亿。下图是新力量币产出量的预测图。

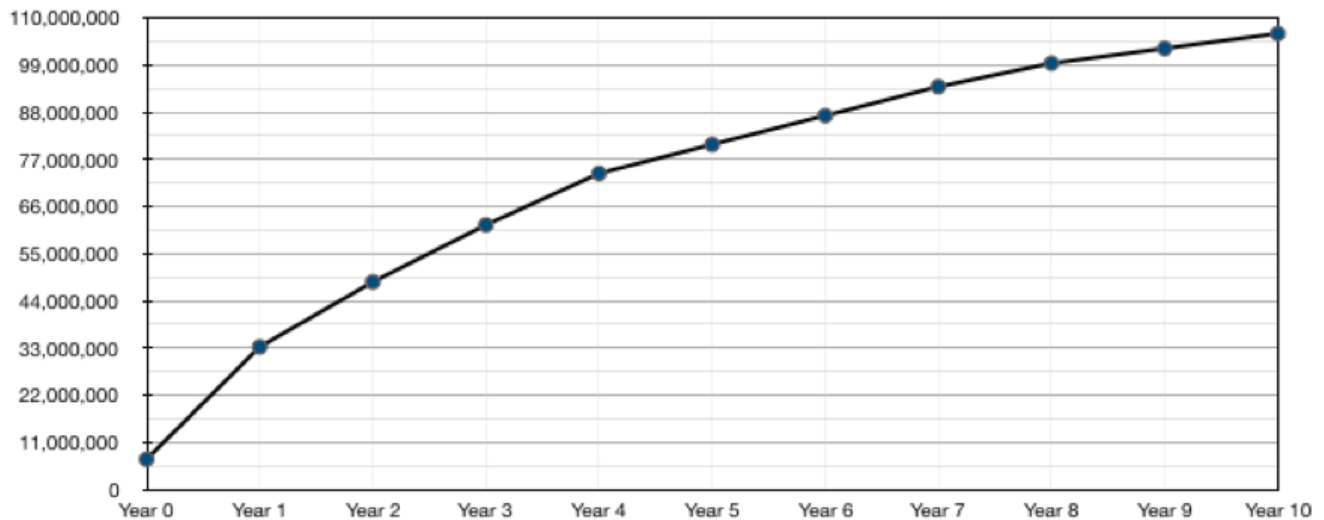


Fig.16. NPW 产出预测曲线

新力量币的产出分为两个阶段，PoW阶段为基础的挖矿阶段，初始的币都通过这个阶段挖出。

新力量币的区块产出时间定义为2分钟，区块大小为2M。

每个主节点需锁定20000个新力量币。

## 5.3 区块奖励

PoW 阶段	PoS 阶段
主节点: 70%, 矿工: 30%	主节点: 80%, PoS: 20%
[block# 1] 7,000,000 (Premined)	[block# 23601-300000] 100
[block# 2-2000] 1	[block# 300001-1000000] 50
[block# 2001-23600] 100	[block# 1000001-2000000] 25
	[block# 2000001-3000000] 12.5
	[block# 3000001-] 6.25

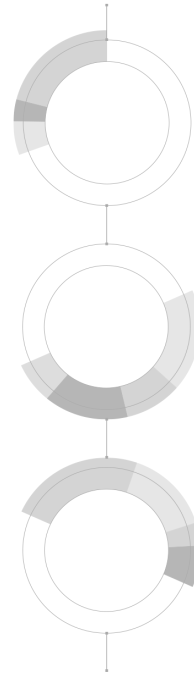
Fig.17. NPW 区块奖励说明

## 5.4 获取与消耗

与ERC20的Token不同，所有产出的新力量币都是真正的应用型数字币而非证券型代币，在新力量币广告平台的经济体系内，数字货币通过挖矿和权益积累获得，任何人都可以完全公平地获取新力量币进行广告的投放和提供。

在新力量币的广告流量平台中，通过充值及广告投放对新力量币进行消耗。消耗掉的币将作为投放流量主的奖励，重新进入经济循环。

当新力量币基础设施搭建完毕，作为基础流量引擎时，新力量币将作为底层基础加密货币，进入多个广告平台进行流转和消耗。



## 六、路线

### 6.1 业务路线

#### 6.1.1 广告流量业务分阶段发展的实现

对于新力量币整体发展的8年预期，虽然每个阶段都有挑战，但是最困难的部分是从零到一的部分。没有实际业务的数字货币，虽然在宣布的时候可以描绘一个漂亮的伟大前景，但是实际上没有核心业务就很难获取足够的价值。

自互联网发展之初至今，我们认为收入模型最明确的业务模式主要是在线游戏和数字广告，而广告流量的流转比游戏更加基础也更通用。

作为新力量币的业务支点，我们认为在战略上，去中心化广告业务是非常坚实且可靠，而且可实现的。

#### 6.1.2 业务各个阶段规划

##### 业务导入期规划

在业务发展阶段里，最初的业务导入期预期要经历约8-10个月时间，由少量参与者、话语领袖和爱好的加入开始。因此第一年的业务规划包括：

前三个月：从一些最基础的广告流量交换业务试水，商业模式上主要摸索币→流量，流量→币的互换模型。这一前提是新力量币已经具备一定的交换价值。因此我们最先从架设主节点开始，使得在最早期新力量币就有基础的实际需求。产生实际需求就产生了一定的价值，具有了交换能力。

导入期后续：核心广告业务尝试逐步启动的同时，同时需要不仅仅在广告业务本身下功夫，还要在数字货币的产品体验方面下功夫。由于发现了普遍数字货币存在着的体验差、普通用户接受困难，以及对于很多纯技术工作存在较大门槛等问题，因此在使业务大面积普及之前，我们通过钱包的改造，重新考虑新力量币的产品体验。所以通过以下改善来增强产品体验也是导入期一个比较重要的工作：

1. 钱包体验优化及重写
2. 跨平台钱包及轻钱包
3. 主节点简易架设能力输出

在白皮书发布之时，以上工作已经基本按预期规划完成。

一旦有了覆盖广泛的钱包及便于搭建的主节点服务器，新力量币网络就有了一个可以持续稳定发展的基础。

导入期的广告主客户不仅涵盖传统互联网客户（他们的广告投放不会与传统互联网广告投放有什么区别），更涵盖一部分从加密货币社区而来的区块链项目的广告主，因为这部分人群更活跃，因此区块链项目的广告主可以感受到比传统流量来源更高效的广告投放。

同时，由于巨头对于加密货币的强烈打压，Google、Facebook都出台了禁止加密货币广告的政策，也加大了区块链广告主的流量需求。

## 业务尝试期规划

业务尝试期主要任务是发展广告的基础业务及平台搭建。

在业务导入期，广告的投放尝试仅支持一个比较简单的轻量级的用户界面，我们将在业务尝试期将其发展为一个去中心化的平台。平台形式既支持通过网站中的页面访问，也将支持在钱包内直接进行广告投放，因此发展更多用户变得尤为关键。所以我们将在这一阶段开始逐步支持广告平台交易功能。由于已经登陆了一些小型化交易所，也更加便于发展更多对流量或收入有需求的用户。

在这一个阶段，最基础的流量交换广告平台将开发完成，同时各种广告形态、行业将越来越多地被支持。我们还将通过扩展钱包功能，增加尝试多种功能诸如：

- 钱包内的广告展现
- 钱包内收取佣金
- 钱包内广告自助投放
- 钱包内项目开发进展查询

等功能。

## 业务过渡期规划

经历了两到三年的业务夯实，平台实际交易流水已经逐渐达到一定规模。因为没有人真正“拥有”这个平台，也就意味着所有人都“拥有”这个平台，因此平台在这一阶段的竞争力将会非常强悍，已经可能达到或者超越普通的小规模广告公司。

同时，在这一期间因为全球广大新力量币社群对于开发及项目进展的参与，广告业务已经基本涵盖大部分主流市场。这一阶段的主要工作则需要根据现有的业务基础对于主链进行更高级别的优化，同时由于行业更加成熟，很多基础工作在那时也已经成为业界的标准，开发和改进起来将会更加容易，这个阶段的优化工作包括：

- 更高速度的共识
- 广告引擎专用的投放智能合约

尝试与第三方广告交换所进行RTB合作

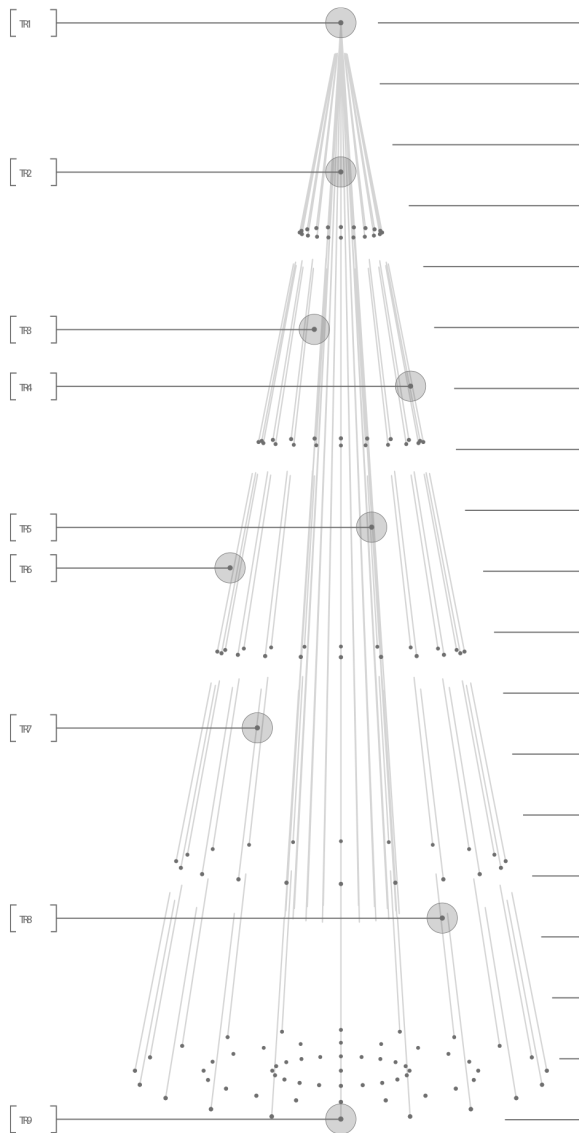
算法保障用户的点击行为及后续操作行为上链后的隐私性

## 业务放大期规划

在这一阶段，新力量币平台已经变成一个比较先进的去中心化广告平台，切入全球市场，并支持多种新的广告业务。

在这个阶段，互联网和科技技术将迎来一波新的爆发机遇，包括物联网AI、家用服务机器人、自动驾驶以及全新能源的使用等都将逐步进入人们的生活。新力量币平台在这一阶段的流量支撑能力足以横跨这些全新的业务形态，支持以更多媒体形态、更强交互性、更多场景进行流量输出。

由于在业务过渡期已经拥有了足量的用户流量数据储备，平台初步具备了用户精准匹配的用户画像能力，在这一阶段，我们将研发用户画像引擎并有选择地开放给第三方进行合作试用。用户画像的分析计算能力也将在这—时间上链进行分布式计算和分析。



这时的平台本身也已经像比特币和其他多种加密货币一样自然存在在互联网中，不被任何人“拥有”，所有的用户以自治的方式管理这一平台。

## 业务攀升期规划

在这一阶段，新力量币平台已经成为全球任何人都不能小瞧的流量平台，可以影响到的比肩如今的Google、Facebook、亚马逊等一线平台。在这一阶段新力量币将有机会不依赖任何交易所而是支持自身的交易能力，“流量即资产”。

这一阶段平台将在用户自治的过程中发展社会责任感，以保障每个人的隐私权及便于获取服务的权利共存为己任。同时支持以跨链的形式横向扩展，无论是基于IPFS或未来其他技术的跨链存储还是与其他主链进行交易能力的对接等。

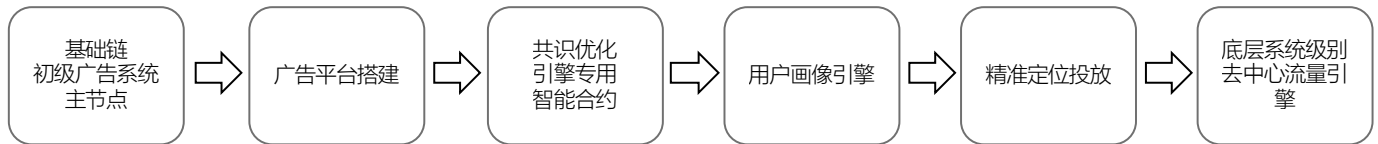
## 业务繁盛期规划

这时的新力量币发展经历了以上的阶段进入最繁荣时期，变成一个真正去中心化的全球流量基础引擎，支持流量通兑能力，服务于地球上

的每个人，让他们可以更快地获取任何信息的同时，隐私可以不受侵扰。对于需要进行推广的商家来说，可以在这个引擎上用自主编程的方式精准找到他所希望服务的用户群体。而整个平台都是广告发布者、广告接受者以及其他所有人全体自治的管理体系，不存在拥有者、管理者，全部体系通过一个自治、公平的规则持续运转。

## 6.2 研发路线

技术研发方面，开发路径将遵循以下步骤进行：



### 第一部分

**基础链部分：**新力量币区块链核心开发；

**初级广告投放系统：**流量积分系统、移动及PC互联网流量采买、钱包内置广告等功能；

**区块链网络：**包括本地钱包、主节点服务等；

后续进行功能扩展及用户体验优化，包括：

轻钱包、移动钱包等产品体验优化；

客户端本地一键部署主节点等功能。

同时广告开始支持多种广告形式。

### 第二部分

广告平台的产品整理和搭建，与新力量币的区块链整合能力，流量联盟，流量积分等工具，包括：

去中心化广告平台的基本版；

广告展示形式对接试验；

支持新力量币直通广告投放双方进行交易；

钱包内置支持广告形式展示；

钱包内可自助投放广告；

流量积分系统及用户任务功能。

广告形式满足多种行业需求。

### 第三部分

共识优化用于满足交易及数据流转速度；

基于类R语言的统计分析能力智能合约开发；图灵完备但包含更多流量引擎专用的API；



自助提交广告内容，设定广告价格；  
获取广告自助投放；  
实时上链结算；  
主动防作弊。

这一阶段的广告将支持各类平台。

#### 第四部分

用户画像的基本开发，基于大数据算法的用户标签设计。

对用户安全地实时分类；  
精准定位查询脚本；  
所有查询及数据上链保存；  
混币及零知识证明保障用户隐私不被破解侵扰。

#### 第五部分

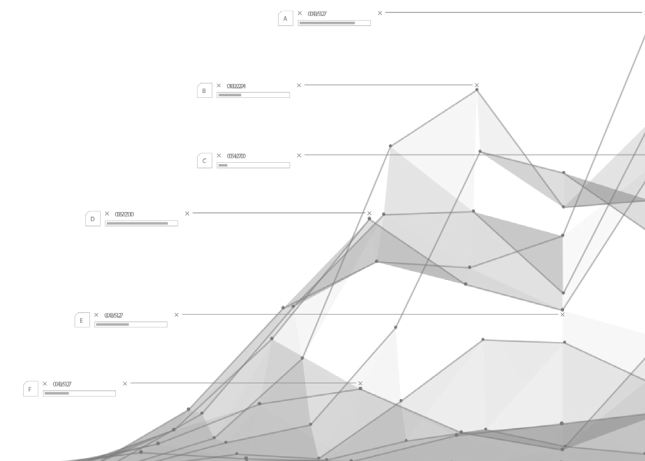
精准投放的智能合约化的对外开放，包括：

广告主自行创建智能合约；  
用户端任务自动执行和数据跟踪。

#### 第六部分

最终成为一个底层的操作系统级别的流量投放引擎，以开源、开放、去中心化的能力支持作为多种广告平台的底层服务操作系统，其他任何只要和流量相关的平台和应用都可以在其上构建。这部分主要包括：

对接各大广告平台实时竞价RTB（Real-time Bidding）；  
多广告平台对接，通过新力量币做实时承兑；  
多链智能合约及多种数字资产对接。



## 七、总结

---

互联网发展至今，流量能力是永恒的力量。Google、Facebook、Amazon等巨头都是以流量能力作为其业务基础，在互联网中展示其强大的用户掌控能力。任何一个巨头都无法将集中化的流量能力放弃，提供给第三方来支配。我们认为，今天的巨头越来越中心化地积累流量的同时，去中心化的，新的力量也同样在积累。

区块链的去中心化的机制提供了一种可能，数据不再被巨头掌握，而是真正归属于使用它的用户，为了帮助用户真正拥有数据，在享受精准服务的同时，无需担心隐私被其他人掌控。

**新力量币具备这样一个基础，可以用全新的力量，推动一个互联网流量新时代的发展。**



## 八、免责声明

---

**本白皮书中的所有内容仅供参考，不得依赖本文中的任何陈述作为任何决策的前提。**本白皮书描述的信息并非完全详尽，也不包含构成合同关系的内容。不得将本白皮书视为投资要约，它既不以任何方式也不应被解释为在任何司法管辖区提供证券。本白皮书不包含任何可被视为建议或可作为任何投资决策基础的信息或建议。

本白皮书中提出的“路线”部分可能会根据实际情况发生变化，将没有人对实际路线改变受到任何陈述的约束。

科技发展和密码学的进步无法保障任何时候绝对的安全性，NPW的源代码可能存在某些瑕疵、缺陷及漏洞，可能损害其可用性、稳定性及安全性并对其价值造成负面影响。同时开源的代码可能被任何成员进行升级、修改，任何人无法预料或保障某项升级、修改的准确结果，可能导致无法预料的结果。任何人士无义务从NPW持有者处进行兑换，也没有任何人士可以在任何时刻保障NPW的流动性或市场价格。

监管机构没有审查或批准本白皮书中提供的任何信息。因此，对于根据任何司法管辖区的法律、法规或规则的要求而产生的合规事宜，现在不会或将来也不会采取任何措施。本白皮书的发布或传播并不意味着适用的法律、法规要求或规定得到遵守。白皮书的条款和条件可能会有变动或需要修订。

本免责声明已经明确向本白皮书的读者传达了可能的风险，读者一旦参与使用NPW的任何软件或参与任何交易，代表其已确认理解并认可细则中的各项条款说明，接受其潜在风险，后果自行承担。