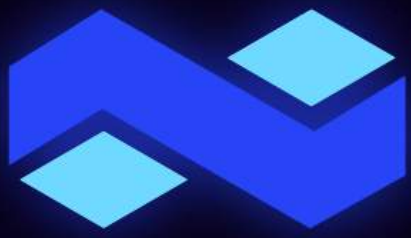


纳威

一个以隐私为中心，并在
区块链上聚合微型网络的协议

白皮书

目录

01

介绍

01 | 介绍

1.1 愿景

纳威是致力于建立全球分散通信网络的社会经济推动者。纳威的公共区块链协议为此生态系统中所有分散式社交应用程序（dApp）提供了极高的可扩展性、安全性和速度。

1.2 背景

继互联网诞生，社交网络就一直存在着。在1971年，“Qwertyuiop”就是通过电子邮件发送的第一条消息。在00年代推出的社交媒体平台、Friendster和MySpace之前，即时通讯IRC（Internal Relay Chat）于1988年首次被使用。如今，脸书、推特、Instagram、WhatsApp和Telegram是一些最受欢迎的社交平台。[1]

1.3 社交媒体的目的

根据《2019年全球数字报告》，全球社交媒体用户数为34.84亿，占全球人口的41%，同比增长9%。[2] 社交网络已经在世界各地的人群中占有一席之地，它允许用户：

- 建立全球性的网络
- 在其网络中共享更新
- 易于获取信息
- 创造商机

通过在一个单一的在线平台内连接大众，社交媒体彻底改变了人与人之间随时随地交流的方式。然而，当前的社交媒体平台面临着许多围绕着安全性以及由于集中治理体系而导致用户管理权不足的障碍。

[1] https://smallbiztrends.com/2013/05/the-complete-history-of-social-media-infographic.html
[2] https://datareportal.com/reports/digital-2019-global-digital-overview

02

问题

02 | 问题

2.1 数据隐私

2018年，脸书的剑桥分析公司丑闻揭露了现有集中式社交平台数据隐私保护的缺陷。在这起丑闻中，未经用户许可，多达8700万脸书用户的个人数据被泄露。泄露的数据使剑桥分析公司得以为政治性广告对用户进行分析和定位。[3] 这突显了当今社交网络领域的一个关键问题——用户无法控制其在线个人数据，现有的社交媒体平台能够在未经用户许可的情况下泄漏这些个人资料。

由于关键服务和平台的集中化，最终出现了数据隐私问题。这些集中化平台受益于网络效应，获得垄断市场份额，并优先考虑平台的使用和增长，以保持其底线。因此，他们越来越不可能以牺牲盈利能力为代价优而先考虑个人用户的隐私需求。对于目前没有可行的替代平台的用户来说，这是不公平和不道德的。

2.2 商业化

虽然数亿值的科技巨头已经从用户的背后赚取了巨大的利润，但用户却无法阻止他们的数据被商业化。
脸书和腾讯分别估值为55092亿美元和4290亿美元。（2019年1月7日）
脸书和腾讯的收入分别为5553亿美元和4562亿美元。（2018年）
比起脸书百分之92的广告收入，腾讯的广告收入只占了微薄的百分之20，然而，腾讯是一家科技集团，而不仅仅研发和管理社交媒体。这引起了人们对科技巨头利用社交媒体用户的担忧，因为他们正在以一种不道德的方式从用户身上获利。此外，现有的社交媒体应用程序缺乏奖励用户参与度的能力。没有一个可持续的应用内模型能够使用金钱利益激励用户参与他们的平台。鼓励用户提供优质内容可促进社交网络中的优秀参与者，并阻止诸如控制、网络欺凌和发布露骨内容等行为。

[3] https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

2.3 用户身份

当前的社交网络也面临着大量假账户使平台膨胀的问题。2018年脸书公布，其平台上有多达1.16亿个活跃的假账户。[4] 在社交媒体网站上注册只需验证电邮地址，但是用户可能不会仅限用于一个电子邮件地址，因此无法用电邮地址绑定用户。由于注册过程中不涉及身份验证，所以几乎无法在集中平台上识别合法用户。

网络犯罪活动也随着社交平台的发展而激增。据Statista报道，仅在美国，就有多达4.6万起网络诈骗案件和6600万美元的社交媒体诈骗损失。[5] 诈骗的受害者落入当前社会生态系统中流通的冒名顶替者之手。由于当前网络上有大量的假帐户，这给用户带来了不理想的体验。

2.4 社区服务

区块链技术自2009年中本聪（Satoshi Nakamoto）发布比特币白皮书以来一直是一项社区贡献。这产生了社区网络效应，加速了社区增长和区块链技术发展。随着社区和区块链的发展，越来越多的参与者将他们的时间、知识和资金投入到网络中，为新进入这个行业的用户创造价值。

从Reddit和Bitcoint Talk等互联网论坛起步的社区现在正转向WhatsApp、Telegram和微信等聊天应用程序。

品牌社区在任何公司的成长中都扮演着巨大的角色，但这对于区块链行业尤其重要。社区有助于当前与新用户的知识共享、内容创造、经验分享、产品创新、品牌忠诚度和保持力。强大的品牌社区使公司能够发展业务并留住忠诚的客户。

在区块链行业中，购买追随者、赏金和空投活动是初创企业拓展社区的一些流行策略。但是，由于虚假社区成员的增殖，上述策略可能代价高昂，而且效率低下。为虚假会员投入金钱和精力并不会形成一个活跃和忠诚的社区，但现有的解决方案却无法提供合法的社区黑客式增长服务。

[4] https://www.businessinsider.sg/fake-facebook-accounts-impersonate-tech-execs-tim-cook-elon-musk-sundar-pichai-2019-5/?r=US&IR=T
[5] https://www.statista.com/chart/15069/number-of-internet-scams-in-the-us/

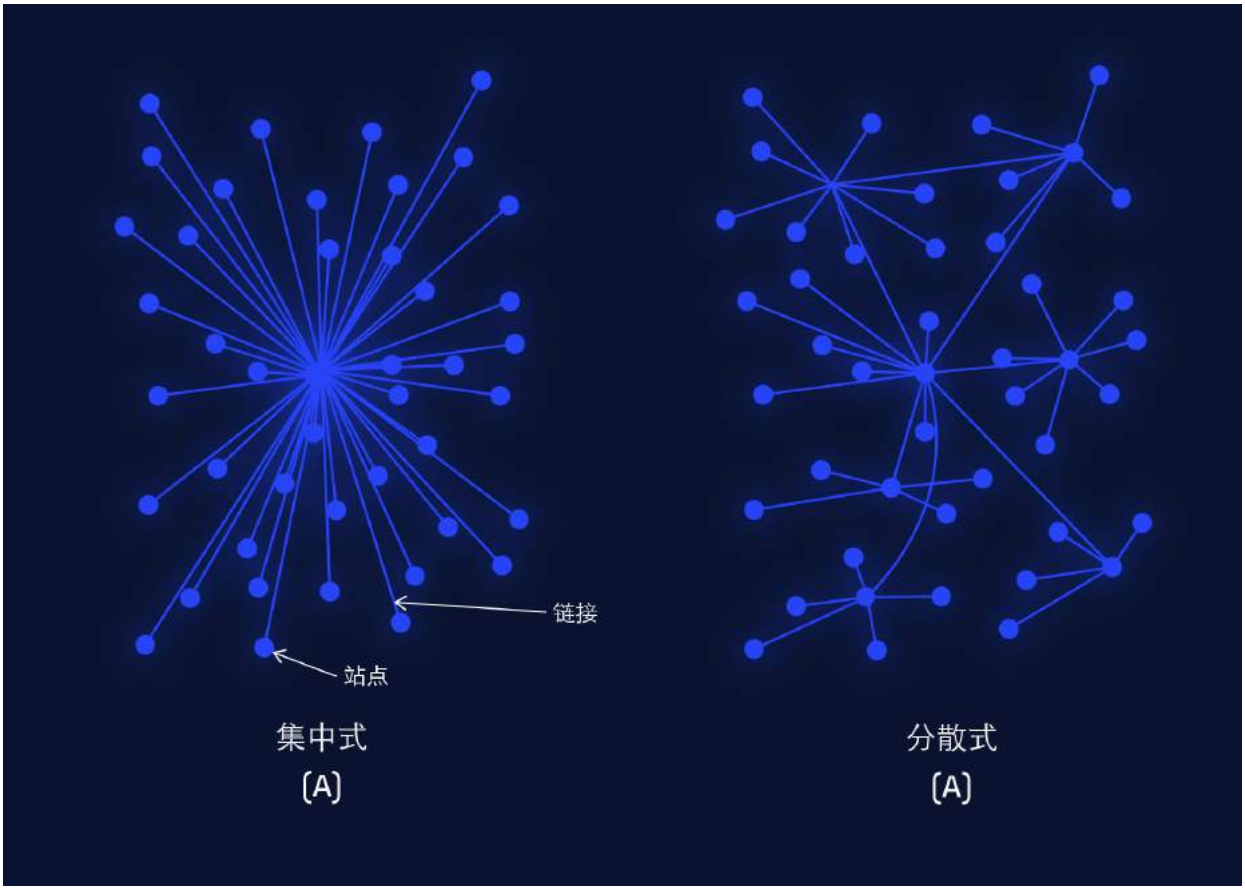
2.5 市场垄断

科技集团脸书和腾讯拥有22.3亿[6]和10亿 [7]活跃用户，分别占世界总人口的百分之28.9和百分之12.9。2019年全球网民有43.88亿，2019年全球社交媒体用户则高达34.84亿，2019年手机用户破51.12亿。[8] 将这些数据与脸书和腾讯用户的数量进行比较，很明显他们拥有巨大的互联网用户市场份额。目前科技巨头的市场份额，存在垄断的可能性。垄断有权控制价格，排除市场竞争。因为消费者没有替代品的选择，所以垄断市场能够膨胀其服务的价格，以高价提供服务给消费者。

2.6 安全性

社交媒体巨头的集中系统允许单一故障点，这些故障点易受数据泄露的影响。在2018年10月，Facebook披露，约有3000万用户受到黑客攻击。在数据泄露期间，攻击者设法劫取了属于1400万用户的所有个人资料。 [10] 在2016年，1.17亿LinkedIn用户的个人资料被攻击者入侵并出售。在集中式网络中，所有用户和用户数据都通过中央服务器连接。

[6] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
[7] https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/
[8] https://www.statista.com/statistics/617136/digital-population-worldwide/
[9] https://www.businessinsider.sg/facebook-30-million-users-affected-hack-fbi-asked-not-to- reveal-source-2018-10/?r=US&IR=T
[10] https://www.businessinsider.sg/facebook-30-million-users-affected-hack-fbi-asked-not-to- reveal-source-2018-10/?r=US&IR=T



当这个核心系统被黑客攻击时，依赖它的所有节点和涉众也跟着损失。这使得数据更容易受到黑客攻击和其他形式的数据盗窃。

2.7 可扩展性

随着分布式账本技术（如区块链）的出现，上述问题的解决方案已经存在，只是当前状态下的现有协议无法复制集中平台的可扩展性。WhatsApp用户每天发送大约650亿条信息，以及20亿分钟的语音和视频通话– 这大约是每秒740000条消息。[11] Visa则每秒处理超过2000笔交易。Twitter上每秒大约有6000条微博。

而当前分散的网络无法处理相同数量的事务。

理论上，ETH、NEO、EOS、Qtum和tron的交易速度分别为15 tps、1000 tps、1000 tps–1000000 tps、100 tps和2000 tps。

然而，到目前为止，这些网络还没有证明声称的每秒交易（TPS），而区块链的可伸缩三重模式是大规模采用的最大障碍之一。 因此，纳威的成立是为了解决这些问题。

[11] https://www.cnet.com/news/whatsapp-65-billion-messages-sent-each-day-and-more-than-2-billion-minutes-of-calls/

03

纳威解决方案

03 | 纳威解决方案

纳威旨在为用户在社交媒体和通信平台上面临的问题提供解决方案。区块链技术的实施使得一个透明的、可审计的账本，不只无法在没有用户的知识和同意下收集和发送数据，也消除了潜在数据泄露的单一故障点。社交平台用户将完全控制自己的通信经验与记录，而不受集中通信巨头的管制。如今，大众能够通过分散的平台重新获得该有的通信的安全和隐私，防止数据泄漏和利用。纳威致力于提供优质内容的自由，根据用户的喜好与习惯指导广告，鼓励用户在社交平台上积极地参与。包含用户内容、身份和在线行为的数据都将被加密并储存在分散的平台上。

在纳威协议里，中间商将被淘汰，以便公司能够直接与用户接触与交流。这样一来，公司就能够从潜在客户那里获得更精准的数据，客户也能选择向谁出售个人的数据。

此外，并非所有社交平台上的引领者都直接从每一个赞，好评或追随者得到激励。纳威通过允许生态系统中的用户奖励制作高质量内容的用户来简化这一过程。每个人都能够在生态系统中参与，这不仅从用户那里提升参与度，也能够提升内容的质量。

04

纳威协议

04 | 纳威协议

纳威协议将基于授权股权证明机制（DPOS）模型的衍生上运行，利用具有以下关键参数的可扩展、可持续生态系统区块链的速度和高级功能：

- 托管

加上授权股权证明机制，托管成为确保“去信任”、分权和民主化的关键功能。托管者也作为区块生产者，核实交易和建立此链。

- 权益证明管制

托管者与托管钱包具有投票功能，为确保民主性以及新提案的无缝通过和网络升级。作为嘉信原始产品的延伸，托管者与托管钱包将监督和审查分配池长时间的管理。

- 每秒传输的事物处理个数 （TPS）极高

区块链将基于固定数量的托管钱包，允许TPS和分权之间的良好平衡。根据设计，系统在任何时候的预期吞吐量都应超过500TPS。

- 动态令牌供应管理

纳威协议的标记学将考虑生态系统内的经济活动，以最高精度的几个关键触发因素为基础确定纳威标记最相关的经济需求。

- 微网络与微生态系统

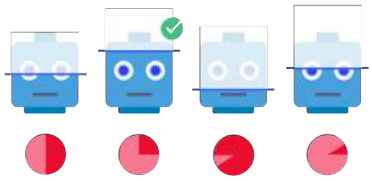
由于对隐私的需求，有些社区必须建立私人微网络，并使这些专用网络与协议同步。这些网络最终将成为建立社区服务产品的基础。

授权股权证明机制

在授权股权证明中，投票权的作用是确定谁将担任授权者的角色、维护网络和验证交易。

1 NVR币持有者都能投票决定验证者。

2 投票最多的验证者将成为授权者，验证交易并为此获得奖励。



纳威协议的共识模型基于行业中已验证的DPOS模型。该模型是一个安全、以其他传统模型，如工作证明（POW）或利益证明（POS）渐进的系统。这些传统模型在可伸缩性三重模式中有其自身的局限性，难以为可伸缩性、安全性和分散提供近乎完美的场景。一般来说，DPOS推动了区块链扩展（速度）的边界，同时保持网络内的安全和“去信任”的系统。

■ 共识

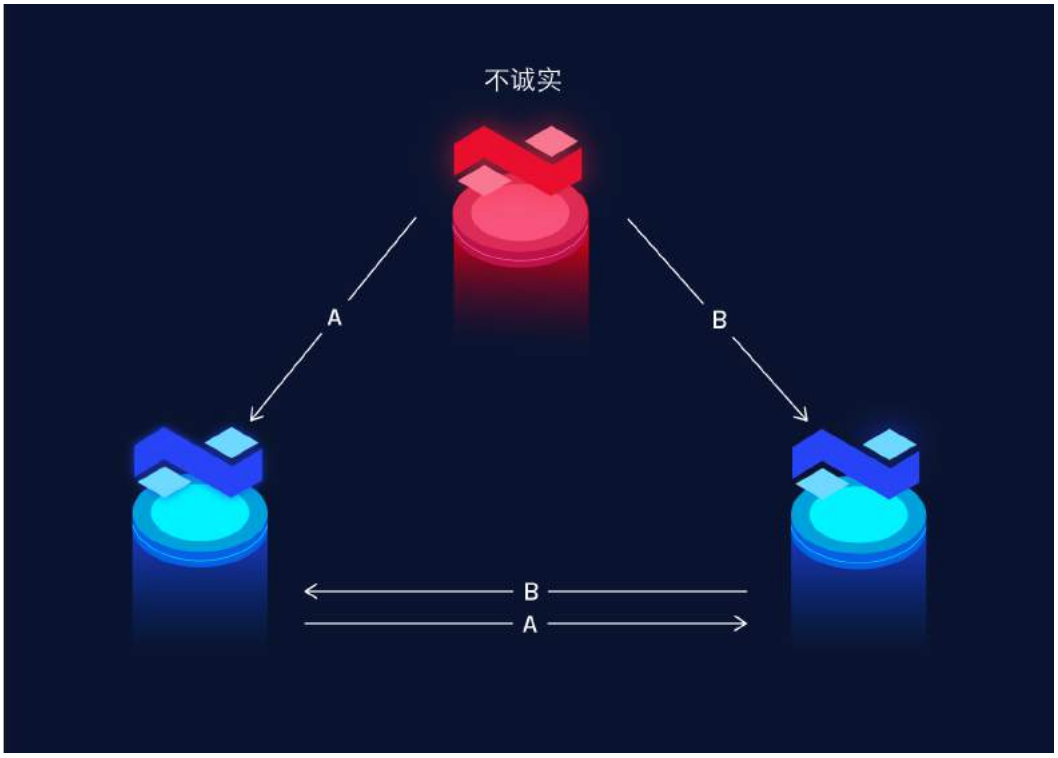
在纳威协议中，共识是经验证的拜占庭容错（DBFT）的衍生产品。为了更快地解决不诚实的节点/视图，并在大量不诚实的环境（例如20%<n<33%）中更快地签署块，纳威协议引入了实时调整的拜占庭容错（R–DBFT），这增加了授权者的数量。当不诚实的情况无效时，需要用rand（）因子来签署一个块。

共识节点– 共识安排的参与者。所有参与的节点都将随机地扮演双重角色，即广播者或实时代表。

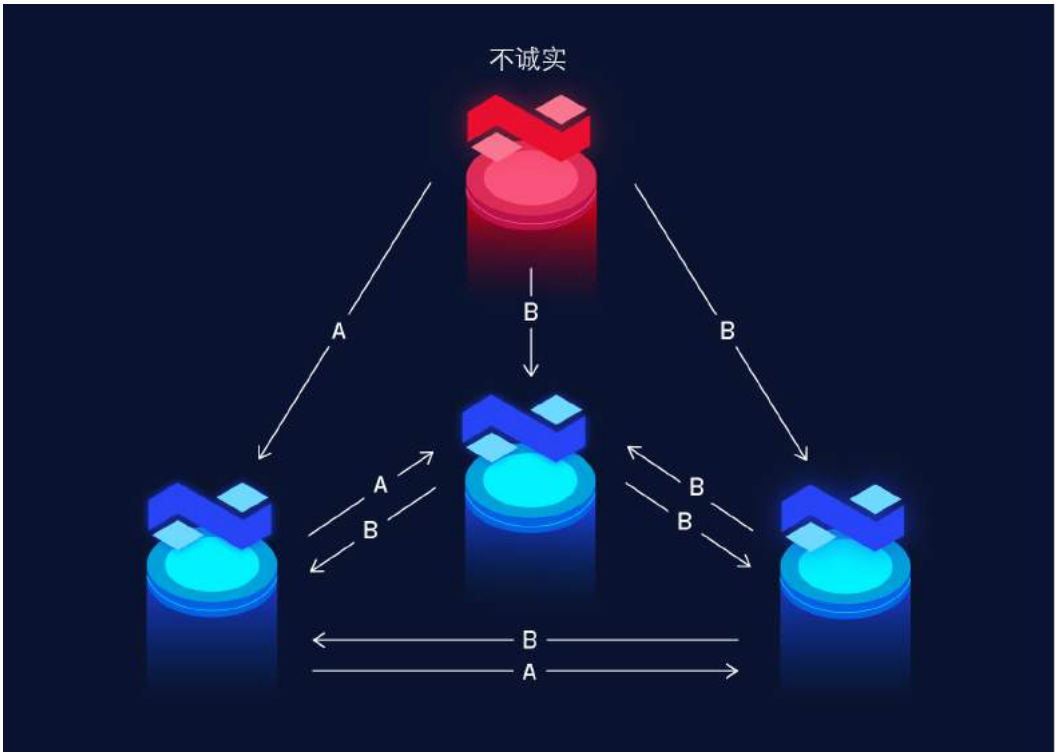
广播者– 选择一个随机节点作为负责提案传输的广播者。每个块确认实时只会选择一个广播者。

实时代表– 剩余不是广播者的选定节点将扮演实时代表的角色并签准以达成共识。

在标准DBFT场景中，每次检测到不诚实状况时都会更改视图。



在上面的示例中，对于不诚实的广播者，两个授权者都无法确定哪个节点不诚实，并且视图也发生了更改。



在上图中，因有四个授权者，中间节点和右节点接收到的块无法验证。这使得他们遵从一种新的观点，选择一个新的广播者，因为他们占了百分之66的多数。

对于RA–DBFT，该协议不同于这样一个事实– 即一个新的视图基于对以下因素的专有计算，带有rand（）因子所需的更多委托：

- 无效广播者和/或实时代表的数量
- 当前视图之前更改的视图数
- 实时计算不诚实节点的估计聚合百分比
- 不诚实节点的当前阈值限制

由于实时迭代和对这种情况的适应，不诚实的失效即使在非常有缺陷的（节点）环境中也会显著地增加签名块的概率。

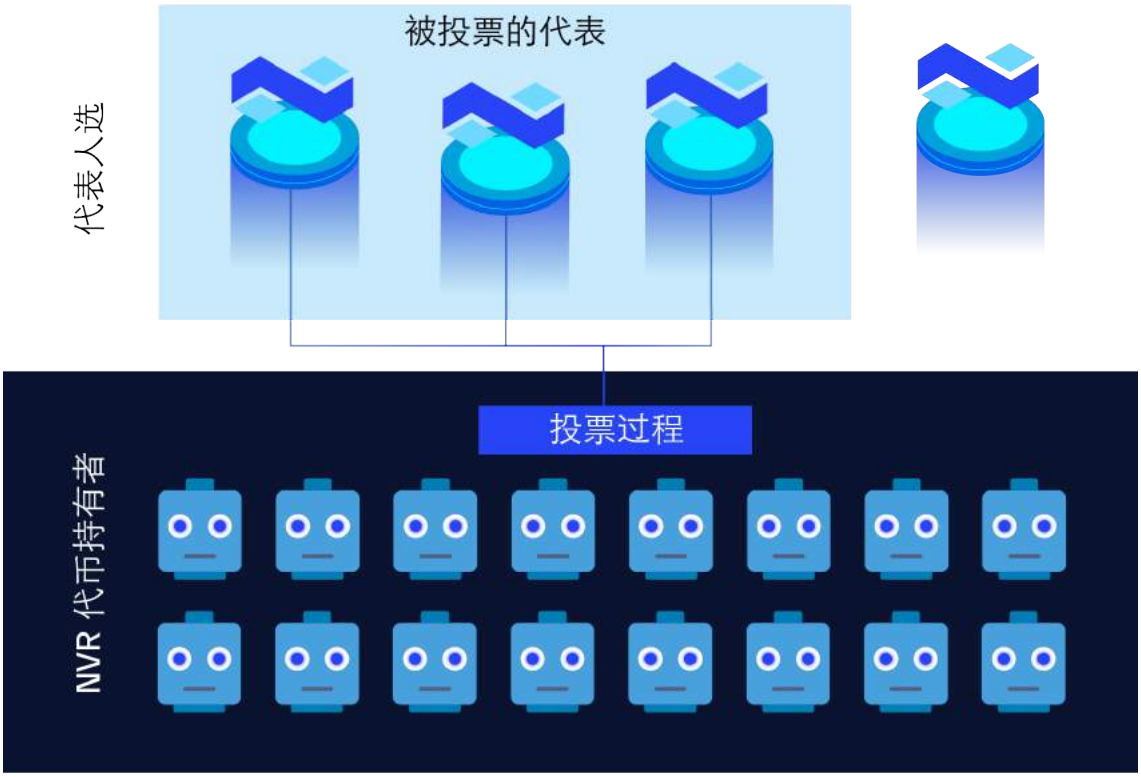
■ 隐私和匿名交易

为了保护个人隐私并在用户要求时保持匿名，纳威将采用zkSNARKs技术在有必要时“切换”和屏蔽区块链上的交易。zkSNARKs代表“零知识简洁的非交互知识论证”，指的是一种 证明结构。

在这种结构中，人们可以证明拥有某些信息，例如秘密密钥，而无需透露该信息，并且证明者和验证者之间没有任何交流。这是一种能在区块链上完全屏蔽加密交易的新方式。纳威协议中部署的zkSNARKs的性质将在未来的技术白皮书中详细说明。

■ 托管与管理

纳威代币持有者将能以投票指定代表他们达成协议共识的代表。在1000人的代表候选人库中，每一次将有100名成功投票的代表。



除了签署和验证链中的块外，代表还负责在链中的以下领域提出和签署提案：

- 纳威议定书的货币政策（通货膨胀/通货紧缩和）
- 提案的最低法定人数
- 代表人数（最小和最大）
- 托管钱包的数量和钱包的经济性
- 协议中的方向更改
- 管理变革
- 在代表中投进或投出票

代表们的投票是连锁进行的。为了提交提案，百分之51的代表需要批准提案。为了对提交的提案进行投票，百分之75的代表的法定人数需要通过提案，即作为软叉（或硬叉）写入链中。

05

纳威币

05 | 纳威币

纳威币是驱动整个纳威经济的燃料，在区块链上形成参与、奖励、激励和消费数字服务的效用。

NVR是一个关键的功能，没有它，协议就不能按照设计运行——一个用户、消费者、供应商、商家和利益相关者蓬勃发展的动态经济。

参与

为了参与纳威经济结构，用户必须先购买NVR作为纳威数字服务和网络的首个进入点。

服务消费

纳威生态系统内提供的所有服务，如SaaS Providence、节点运行和交易服务（Fin–Tech），都需要NVR代币作为支付和/或托管。

托管制

通过托管钱包（有资格成为选民）和代表来激励代币持有者是纳威的固有特征，因此奖励那些效力于分散治理的参与者。

投票权

链上的所有投票活动只能由NVR持有者和利益相关者进行。这确保了所有选民都以纳威的成功与繁荣保持一致，减少了敌对行动和破坏连锁经营的不良行为体。

5.1 纳威协议经济结构

该代币经济结构的概念化和设计是完全自主和动态的，独立于链上的任何外部或内部输入。经济的成功是代币持有者、利益相关者和生态系统的经济可行性三种要素之间的平衡——系统将根据宏观需求和供应根据特定的触发因素进行动态调整。

代币经济是用广义的加密经济博弈理论设计的。为了便于本次设计，提出了几个经济因素，这些因素将形成NVR的通货膨胀率。随着时间的推移，铸造的代币（通货膨胀）被分配给赌注钱包和代表。对于代币发行，这些功能每月进行汇总和展示：

在主链（NODapps）之上构建的dApps数量——随着每个附加的微生态系统（dApp），NVR经济结构每月进行校准，并发行1%以上的代币以应对附加需求。

代表数量（NOD)——上个月NOD的增量（增加）将以代币形式发行，形式为
((NOD (Month 2) – NOD (Month 1))/NOD(Month 1)*100%)/2

托管钱包数量（NOSW）——上个月NOSW的增量将以代币形式发行。
((NOSW (Month 2) – NOSW (Month 1))/NOSW(Month 1)*100%)/2

■ 托管钱包奖励

托管钱包将有资格以每月铸币总额的百分之30的形式发行代币，每月结算并需至少30天的托管。

■ 授权奖励

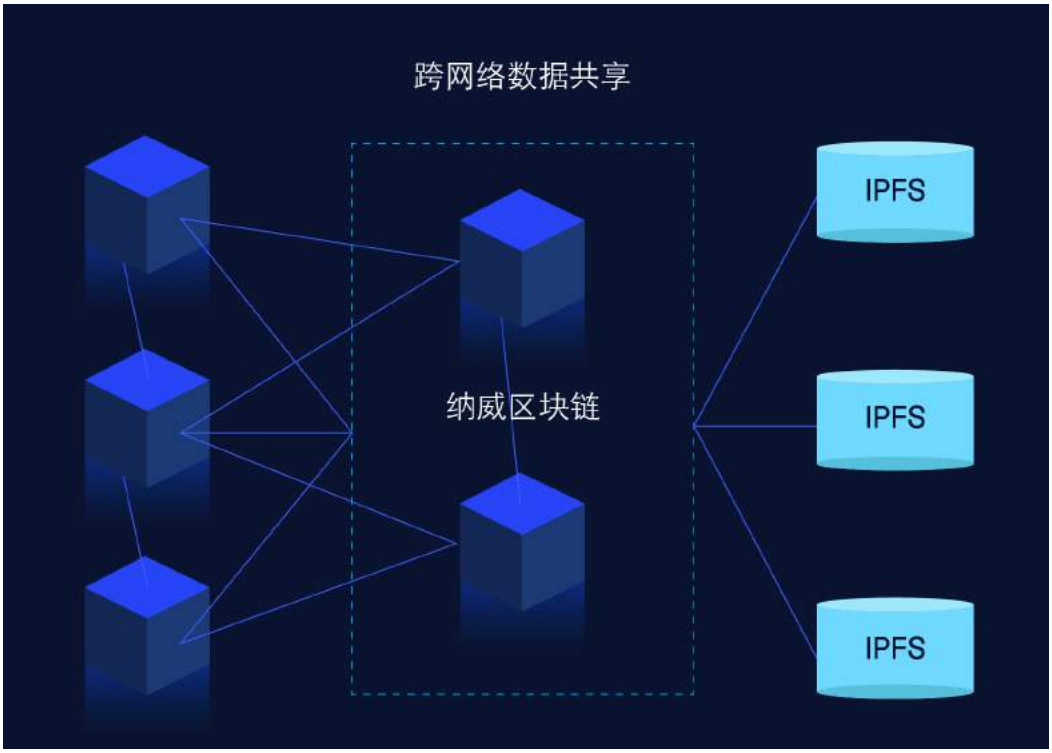
授权者将有资格以每月铸币总额百分之70的形式发行代币，每月结算并需至少30天的托管。

5.2 为何使用动态通货膨胀率

随着经济与连锁商业活动紧密相连，这将形成最健康的代币生态系统形式，其中经济利益与消费和激励相平衡，数字从广义的标记学政策中计算出来。

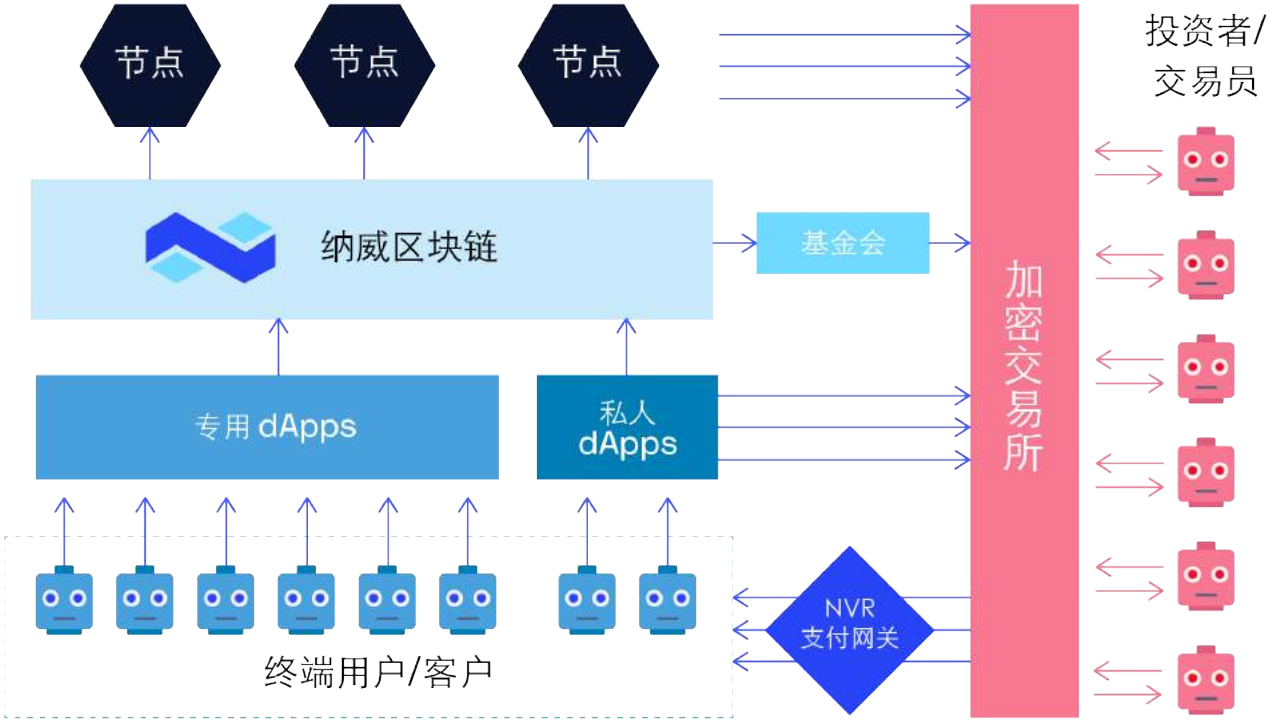
■ 如果因不可预见的经济事件，通货膨胀率需改变，怎么办？

只要达到所需的法定人数（百分之75的提案），就可以由授权者投票并修改动态。



通过在纳威协议基础上构建的专用dApp，企业网络能够在高级别上互连，同时在下链IPFS数据库中保持数据完整性。关键数据存储在纳威区块链，主链支持非隐私、非数据重操作（如ID哈希、用户操作、交易），这些操作大部分是匿名的。

5.3 NVR代币流动



■ 节点

每个月，节点（或授权者）将获得铸造的NVR为奖励，用于验证块和确保纳威区块链的安全。

■ DApps

建立在纳威区块链之上的本机dApp必须将NVR交易到链中。私人dApps将向区块链服务租赁支付NVR。

■ 终端用户/客户

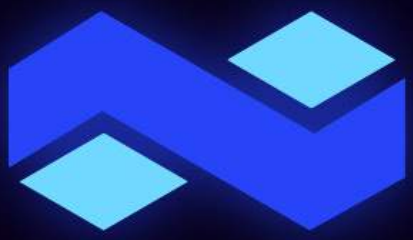
这些终端用户是纳威经济结构的基本组成部分，他们是dApps的客户，是代币经济结构直接的消费者，而他们的活动将使生态系统得以繁荣。

NVR支付网关

为了允许大规模采用并减少增长的抑制因素，关键是在某些消费者（后期采用者）和商家/供应商之间引入一个菲亚特网关作为中介。

基金会

每个月，有限数量的铸币令牌将被分发给纳威基金会，该基金会负责积极开发纳威协议，并与其他受欢迎的区块链建立互操作性桥梁。



纳威