

# NewChat 技术白皮书

## 1.0 版

基于区块链技术的新一代跨国即时通讯系统

2018 年 5 月 7 日

# 目 录

目 录.....	1
○开篇摘要： .....	1
一、NewChat 解决的痛点及愿景.....	4
1.1 轻松解决跨国支付难题.....	4
1.2 严格保护用户信息隐私.....	4
1.3 解决跨国版权保护问题.....	4
1.4 从根本上解决激励问题.....	5
二、功能介绍.....	6
2.1 版本 1.0 功能介绍.....	6
2.2 版本 2.0 功能介绍.....	7
2.3 版本 3.0 功能介绍.....	8
2.4 版本 4.0 功能介绍.....	9
三、NewChat 产品架构.....	10
3.1 产品架构.....	10
3.2 NewChat 产品要素.....	11
3.3 关于 NC 的概述.....	12
3.4 广告系统.....	12
3.5 内容收益分成系统.....	12
四、激励机制.....	13
4.1 奖励池(REWARDPOOL ).....	14
4.2 社群奖励分配-PROOFOFACTIVITY （有效活跃度证明）.....	14
4.3 用户奖励分配-PROOFOFCONTRIBUTION （有效贡献度证明） .....	15
4.4 用户推广分配-PROOFOFNUMBER （有效推广证明） .....	16
五、 技术实现.....	17
5.1 客户端.....	17
5.2 核心功能升级模块一.....	17
5.3 核心功能升级模块二.....	18
六、技术总结.....	20

## ○开篇摘要:

NewChat 是一款专为全球不同国家、不同种族、不同语言的用户建立起来的跨国即时通讯系统平台。

NewChat 主要面向马来西亚、泰国、新加坡、中国、印尼、日本、韩国、美国等国家，已实现了中、英、日、泰国、越南、马来西亚等多国语言版本，并且实现了多国语言间的即时翻译，解决不同国家用户间的语言交流障碍问题。

NewChat 1.0 版本实现了数字货币钱包、数字货币转账、数字货币红包、即时翻译、即时聊天（包括文字、语音、表情、图片、视频、名片、地理位置信息）、群聊、视频通话、语音通话、阅后即焚、基于手机联系人交友、公众号、广场及朋友圈（发文、发视频、发图片、发链接、点赞、评论）、钱包充值等功能，测试版会屏蔽一些功能。

在 2.0 版本中，NewChat 的发展方向是基于区块链的去中心化即时通讯系统（将来会在全球布局 20 多个超级节点），不仅延续中心化聊天软件的免费、使用方便等特性，而且还会增加安全、保护隐私以及加密等其他功能，并同步推出一种让从未听说过数字货币的用户也能方便使用数字货币的解决方案，同时还能使用去中心化的共识机制为内容生产领域建立贡献定价和权益回报系统。

NewChat 具有去中心化特性，能做到实时加密和数据存储：中心化应用程序会引发诸多问题，如引发故障、安全漏洞、零匿名、零隐私等。现实世界中，我们的交易记录、对话信息、人际互动以及态度观点等个人隐私信息都保存在中心服务器上，这样会存在极大的泄漏风险，一旦信息泄露，相当于每个人都裸奔在阳光下的大街上。

现在我们处在一个信息快速发展的世界中，每个人每天都在互联网上留下自己无数的足迹，人们对隐私和安全有比以往更迫切的需求，2015 年 12 月巴西关闭 WhatsApp 以及社交媒体审查制度之后，巴西民众发现他们的言论遭到限制，他们迫切的需要一个去中心化的聊天系统。这个系统不会被关闭，不用考虑审查制度，也不会轻易被黑客攻击，隐私安全应该成为所有应用程序的默认设置。

当前世界上流行的 IM 应用程序都是中心化的：WhatsApp、Skype、Viber 等，这些应用程序都是使用公司服务器在网络中传输信息。这意味着每个应用程序都要受到中心化带来的低

效率的影响，例如：故障、安全漏洞、零匿名、零隐私等等诸多问题。基于目前的状况，一款基于区块链技术驱动的安全、高效的私密即时通讯系统成为大众的主流需求。

目前已经有一些去中心化的尝试，如 CoinSpark 和 Blockom。人们需求的趋势已经无法阻挡，甚至美国国防部高级研究计划局（DARPA）以及英联邦都在考虑搭建区块链即时通讯系统。但到目前为止，没有一个解决方案能在大型传统机构中流行起来，因为这些去中心化的解决方案并不是针对大众的。政府机构开发的项目是完全保密的，私人机构的解决方案大多数也只针对有经验的数字资产用户。

NewChat 将以区块链技术和应用为核心，针对大众推出去中心化即时通讯的功能，通过点对点的互动实现私密的交流。A 的信息可以到 B 的手机终端，B 的信息也可以到 A 的手机终端，这是两个节点的信息交流，而不是通过服务器派发（当前能够实现，未来可以完全实现去中心化）。这样直接点对点的方式，保证了信息的私密性。更不会在我们聊天的过程中，因为手机丢失或其它外在因素，导致信息的泄漏。

因此，NewChat 不仅延续中心化聊天软件的免费和使用方便等性能，同时还有安全、保护隐私以及加密的性能。通过区块链“备忘录”发送 IPFS 散列代码，只有接收人才能读取信息，而且将对所有的音频和视频流进行加密。避免了因使用公司服务器在网络中发送信息而受到中心化带来的信息泄露，系统故障、安全漏洞、零匿名、零隐私等风险。

在区块链上添加一个去中心化的 messenger，可以为用户接收解读消息，但会占用大量资源，对移动设备来说这几乎是一个难以解决的问题，这也是所有同类应用程序的通病。但在 NewChat 中，用户只需下载用户专用数据，而不用下载整个链。不仅可以节省电量，减少数据负担，还可以节省平台的时间。

另外，NewChat 不会有地域性差异，可以同时面向全球的用户。目前中国国内绝大部分的社交软件都是有地域性的，缺乏安全的信息保密机制。在国外，很多中国的聊天软件无法使用，在中国国内，很多国外的聊天软件也无法正常使用，例如推特和脸书。NewChat 的用户可以轻松的不同国家的人交流，无论你在世界任何地方，NewChat 通过区块链构建不同的节点，而通过节点传输是不受地域限制的。

## 数字货币转账：

除了传统的传输信息的功能，NewChat 还可以同时解决目前银行无法解决的转账问题。中国目前的社交聊天应用巨头——微信，其用户都必须忍受腾讯严格的审查制度，交易无法加密，以及中心化的金融系统微信支付问题。

但是 NewChat 可以保护用户的加密数据，通过区块链进行无缝转账，未来 NewChat 计划支持更多的数字资产转账。用户不必记住各种数字资产的接收人地址，或者其它专门的数据：只需要在聊天窗口就可以发送资金、资产和奖励给对方，或者可以将资金发送到用户名中或通过二维码进行转账。公司则可以通过 NewChat 建立企业账户并接受转账。

在 NewChat 中用户不需要花费任何手续费，NewChat 可以支持多种数字资产，并且安全指数极高，

同时 NewChat 有 更加先进的账户管理功能。让用户使用价格稳定的资产，如欧元、美元和人民币，同时支持数字资产如比特币、以太坊、莱特币等等，为兑换货币、资产、股票、债券和 ICO 代币等等提供了一个完美的全球化交易账本。

## 为内容生产领域建立贡献定价和权益回报系统：

在过去，活跃用户、优质内容的创造者和传播者们，为 Facebook、Twitter、Reddit、微博、知乎等社交网络和 UGC（UserGeneratedContent，用户生产内容）平台带来了海量流量和数百亿美元的利润。但是，这些生产内容的用户对于他们所创造的内容既不拥有完整的控制权，也不享受充分收益权。

相反，以营销为目的的文章，比如 软文，却可以轻松变现，但这些软文对社区优质原创内容存在着严重的挤兑。这一切，都使得优质原创内容生产者难以保持足够的创作动力。高质量的 UGC 正是知乎的价值所在。但是，UGC 并不直接创造价值，极难给碎片化的 UGC 以合理定价，这使得 UGC 的受益者——平台和读者都缺乏合理的途径回报内容生产者，整个 UGC 领域缺乏合理的激励体系来激励高质量内容的生产者。

NewChat 利用区块链技术完美解决了这个问题，NewChat 在以太坊 ERC20 标准的基础上，建立了一个利用区块链技术并使用去中心化的共识机制为内容生产领域进行贡献定价和权益回报的系统，使内容生产者、内容投资者、内容筛选者和生态建设者都能得到合理的激励与回报。

## 一、NewChat 解决的痛点及愿景

### 1.1 轻松解决跨国支付难题

国家之间货币无法高效流通，阻碍跨国用户的交流。除了传统的发送信息的功能，

NewChat 还可以同时解决目前银行无法解决的转账问题，通过区块链进行无缝转账，NewChat 支持利用虚拟货币进行转账、发红包。用户不必记住各种货币的接收人地址，或者其他专门的数据：他们可以将资金发送到用户名中或通过二维码进行转账。用户不需要忍受审查制度，实行交易加密，以及去中心化的金融系统支付问题。

### 1.2 严格保护用户信息隐私

大多数人都对安全、隐私和去中心化功能不敏感。现实世界中，我们的交易记录、对话信息、人际互动以及态度观点等个人隐私都会被中心化服务器记录下来。这是非常危险的，随时有可能发生系统或人为问题导致的个人隐私信息泄漏。

试想，如果我们能用手机上最常用的界面，只用信息窗口就可以发送资金、资产和激励，

那将会多么的方便，多么的高效。在 NewChat 中，用户可以在绝对安全的环境中，与家人、朋友分享其最私密的想法。

我们的愿景是把最安全的社交信息交流和数字资金转账结合到一个应用程序中，任何人只要能链接到互联网都可以免费使用。

### 1.3 解决跨国版权保护问题

近年来，版权的重要性已成为全球共识，各个领域的内容生产者都在其领域内为版权而努力，但现有的版权仅仅是国家内保护，并且保护方式仍有很多漏洞。

而在 NewChat 生态系统内，利用区块链技术，将用户产生的内容（包括用户信息、内容详情、时间等信息）打包，将这些要素构成了一个区块，在广播中公开，并且还设置有节点进行记账。因而在这个区块链系统中，所有用户都能明确内容的归属权，这也是目前全球性质的内容版权保护的一种最佳的形式。

## 1.4 从根本上解决激励问题

虽然内容创造者们为众多社交网络创造了巨大的流量与丰厚的利润，但是内容创造者们对于他们所创造的内容既不拥有完整的控制权，也不能享受到充分的收益权。

以中国问答平台知乎为例，知乎目前拥有注册用户超 6500 万，2016 年全年，知乎用户提出了超过 600 万个问题，撰写了超过 2300 万篇回答和 151 万篇文章，知乎 D 轮融资后估值超 10 亿美元。然而，知乎的价值创造者——优质内容生产者除了收获尊敬之外，并没有得到其它的回报，他们付出的劳动缺乏变现的途径。而另一方面，以营销为目的的文章，比如软文，反而可以轻松变现，但这些软文对社区优质原创内容存在着严重的干扰。这一切，都使得优质原创内容生产者难以保持足够的创作动力。基于以上情况，平台和读者都缺乏合理的途径回报优质内容生产者，激励创造出更多优质内容。整个 UGC 领域缺乏合理的激励体系来激励高质量的内容生产者。

而区块链技术能从根本上解决激励问题，让优质内容生产者获得合理的回报，通过正向激励，优质内容生产者会获得丰厚的回报，促使内容越来越优质。而低劣内容生产因为得不到激励，丧失创作的动力，自然淘汰。

NewChat 的愿景是通过区块链技术，打造一个新时代的跨国即时通讯系统，在数字资产全球化的趋势中，为整个区块链行业乃至全人类贡献一份力量，让参与通讯系统中内容生产，内容传播，内容筛选的用户获取每一个正向行为的激励。

NewChat 立志于服务全球亿量级用户进行区块链世界的无国界交流，非常方便的管理以及获取自己的数字资产。

## 二、功能介绍

### 2.1 版本 1.0 功能介绍

#### 2.1.1 即时通讯

#### 2.1.2 打破通信行业的地域性限制。

在 NewChat 生态系统中，不限制国家和地区，用户都可以在 NewChat 平台上进行注册和交流。用户可基于手机联系人、原有用户及好友关系进行通讯，满足用户间的即时沟通需求，包括文字、图片、表情、语音、文件、视频等，同时跨国用户间还可以进行免费的语音、视频通话。让使用者在网络上通过建立私人聊天室实现实时通讯服务，快捷方便的交流。

#### 2.1.3 阅后即焚

用户可以选择性将文字、照片或者视频设置阅后即焚，所发信息会有一个限定的生命周期，用户将消息发送给好友后，这些消息会根据系统所预先设定的时间按时自动销毁。此功能满足了那些想要发送商业机密或者敏感信息的用户，保护用户隐私不被泄露。

#### 2.1.4 数字资产红包

在 NewChat 生态系统内，不同国家的用户可使用其所在国家的法定货币兑换 NewChat 的数字资产，跨国用户之间可相互发送数字资产红包，对方不会有任何接收条件限制。

#### 2.1.5 数字货币

NewChat 生态系统内将发行加密数字货币，持有该数字货币的用户可在交易所将此兑换为法定货币。用户在使用系统过程中，会得到积分奖励，当积分积累到一定数量时，即可在系统内兑换为生态内数字货币。

#### 2.1.6 广场功能

NewChat 所有用户都能在广场中发表内容，包括文字、图片、视频、文章、链接等，系统将利用区块链技术，将用户产生的内容（包括用户、内容详情、时间等信息）打包，这些要素会构成了一个区块，在广播中公开，并且有节点将这些区块记录下来。在 NewChat 生态系统中，所有用户都会知晓内容的归属，因而可以很好的做到全球内容版权保护。



## 2.1.7 会话、文章及评论的即时翻译

NewChat 可实现跨国用户间的语言无障碍交流。当用户选择翻译功能后，向国外友人发出消息的同时，消息下方会立刻出现设置好的翻译语言。

在朋友圈、广场的场景中，翻译功能依然能够发挥作用。用户可选择将朋友圈、广场的内容翻译为自己想要的语言，增进内容的传播性，并且用户可看到其他用户对此条内容的看法，增进跨国用户之间文化的交流。

## 2.1.8 问答系统

问答功能可连接各行各业各国的用户，用户分享着彼此的知识、经验和见解，为整个生态源源不断地提供多种多样的信息。虽然网络百科几乎涵盖了概念性知识所有的疑问，但是问答模式则是对发散思维的整合。

## 2.1.9 钱包功能

国内绝大多数主流软件都不支持数字资产或者其他代币，或者一些主流数字资产的交易。而在 NewChat 中，以区块链作为核心技术，可以保证数字资产在 APP 平台的发布。

# 2.2 版本 2.0 功能介绍

## 2.2.1 万能钱包

- 支持多种钱包类型，轻松导入导出；
- 支持多种加密数字货币，包括以太坊、比特币等数字货币，后续版本会增加更多数字货币；
- 一键添加数字资产，实时跟踪交易动向，关注资产余额变化；
- 实时同步全球各大交易所行情；
- 价格变动预警，让你时刻把握投资机会；
- 内置交易兑换服务，方便快捷。

## 2.2.2 文章、图片、视频的跨国打赏

在 NewChat 生态系统中，用户可接受来自世界各地用户的新鲜趣闻以及独特见解，用户可利用虚拟货币对文章、图片、视频进行打赏，增加用户收入的同时还可以极大的促进用户

的发文积极性，营造更有价值、更有质量的开放式社区。

### 2.2.3 全球跨国广告

广告系统可以增强虚拟货币流动性，增加平台收入以及用户收入。NewChat 会引入“按时长、按广告位置付费”的计费模式。

BuySellAds.com 是一个全球领先的在线广告市场，其主要的业务是为网站主销售按时长计费的广告位。NewChat 将会采用类似的模式，在钱包内提供一个广告市场，将会展示各个平台能提供的广告位置选项以及费用，同时也会显示这些平台在区块链上的表现以及历史数据（如收入、内容数量等）供用户做参考，内容生产者可以在此承接广告获取收益。广告显示的时长和位置交给智能合约执行。

### 2.2.4 全球性付费社群

在 NewChat 生态系统中，用户可以创建属于自己的私有社群，可以设定其他用户加入该社群平台需要支付的虚拟货币数量。

### 2.2.5 付费文章、音视频、直播以及课程

内容生产者，包括但不限于文章、音视频、直播以及课程的生产者，可自行定价自己内容的价值，解决自媒体从业者长久以来内容变现的难题。

### 2.2.6 付费问答

问答功能可连接各行各业各国的用户，用户分享彼此的知识、经验和见解，为生态源源不断地提供多种多样的信息。同时，用户可付费给资深从业者解答问题，其他用户需要付费才能看到问题答案。这样极大的提高了社区内问答的质量，让用户更方便的得到专业的回答，同时给解答者增加收入，激励其回答参与更多的高质量问题。

## 2.3 版本 3.0 功能介绍

建立互动私密性，将完全采用区块链的技术改造通讯方式。现在微信等软件已经开始实

名制，在 NewChat 中，可以通过点对点实现互动私密的交流。

不设立独立服务器，所有用户的终端设备都是服务器，同时在全球 20 多个国家设立节点服务器，所有聊天记录都是加密后独立传输，安全、保护隐私以及加密的性能，在通讯后只保留在用户的手机上，不可找回，所有文件都将存放到区块链上。

---

## 2.4 版本 4.0 功能介绍

### 2.4.1 挖矿机制

用户可在 NewChat 内进行“挖矿”，“挖矿”所得为数字货币 NC（NewChat 平台内发行的加密数字货币）。

### 2.4.2 电商模块

增加电商模块，用户可使用平台发行的加密数字货币 NC 进行购买，种类可涵盖衣物、生活物品等多种类型产品，并且用户购买无地区与国籍的限制。

### 2.4.3 博彩游戏

用户下注即可成为玩家，使用货币为平台发行的加密数字货币 NC。游戏玩法多样简洁，并且游戏基于区块链技术进行开发，透明公正，每一条操作记录都会储存在区块链上，无法篡改。

### 三、NewChat 产品架构



#### 3.1 产品架构

NewChat 生态系统中，以区块链技术为底层框架，之上有聊天社区模块以及金融模块。

聊天社区模块包括即时聊天、社区内容、激励机制、用户中心。金融模块包括交易平台、钱包模块。

## 3.2 NewChat 产品要素

### 3.2.1 账户体系

NewChat 提供一套完整的账户体系，用户只需要通过手机号注册，即可加入 NewChat 生态系统。

NewChat 将会为每个用户分配唯一的数字身份(Digitalidentity)和 NewChat 的数字钱包，这些数据将会被写入 NewChat 的区块链网络。

用户使用唯一的数字身份，即可在 NewChat 生态中畅行无阻，享受 NewChat 提供的各项基于区块链的便利功能。

### 3.2.2 跨国通讯

在 NewChat 生态系统中，不限制用户的国家和地区，都可以在 NewChat 平台上进行注册和交流。用户可基于手机联系人、原有用户及好友关系进行在线通讯。

满足用户间的即时沟通，包括文字，图片，表情，语音，文件，视频等，同时跨国用户间还可以进行免费的语音、视频通话。

用户可以选择将文字、照片或视频设置阅后即焚，所发信息会有一个限定的生命期，用户将消息发送给好友后，这些消息会根据系统所预先设定的时间按时自动销毁。

跨国用户之间可相互发送虚拟货币红包，对方不会有任何接收条件限制。

NewChat 还可实现跨国用户间的无障碍交流。当用户选择翻译功能后，设定好和对方交流的翻译语种，当用户向国外友人发出消息的同时，消息下方会出现翻译语言。

### 3.2.3 内容发布

NewChat 支持用户发布多种不同媒介类型的内容：文字、图片、视频、链接以及问答。将来会继续支持更丰富的内容发布类型，包括签到、物品交易、直播等。

### 3.2.4 交互功能

交互模块包含：点赞、评论、打赏、分享等。

### 3.3 关于 NC 的概述

NC 是 NewChat 发行的加密数字货币，持有 NC 的用户可到数字货币交易所购买其它数字货币，也可以将其兑换为本国的法定货币。

NC 的获取方式：

- 用户在注册、使用 NewChat 的过程中可以得到 NC；
- 用户可以在数字货币交易所，用法币或其它数字货币兑换到一定比例的 NC。

### 3.4 广告系统

在 NewChat 钱包内会提供一个广告市场，商家可以在此上架广告内容，用户可以选择广告进行宣传，通过广告可赚取 NC。另外，广告系统可以增强 NC 流动性，增加平台收入。

在开发初期，NewChat 计划引入“按时长按广告位置付费”的计费模式，后续也会增加更多灵活的计费模式在广告市场中，将会展示各个商家提供的广告内容、类型以及报酬，同时用户也可以查询到自己得到的历史报酬数据。商家支付给用户的报酬用 NC 进行结算。

### 3.5 内容收益分成系统

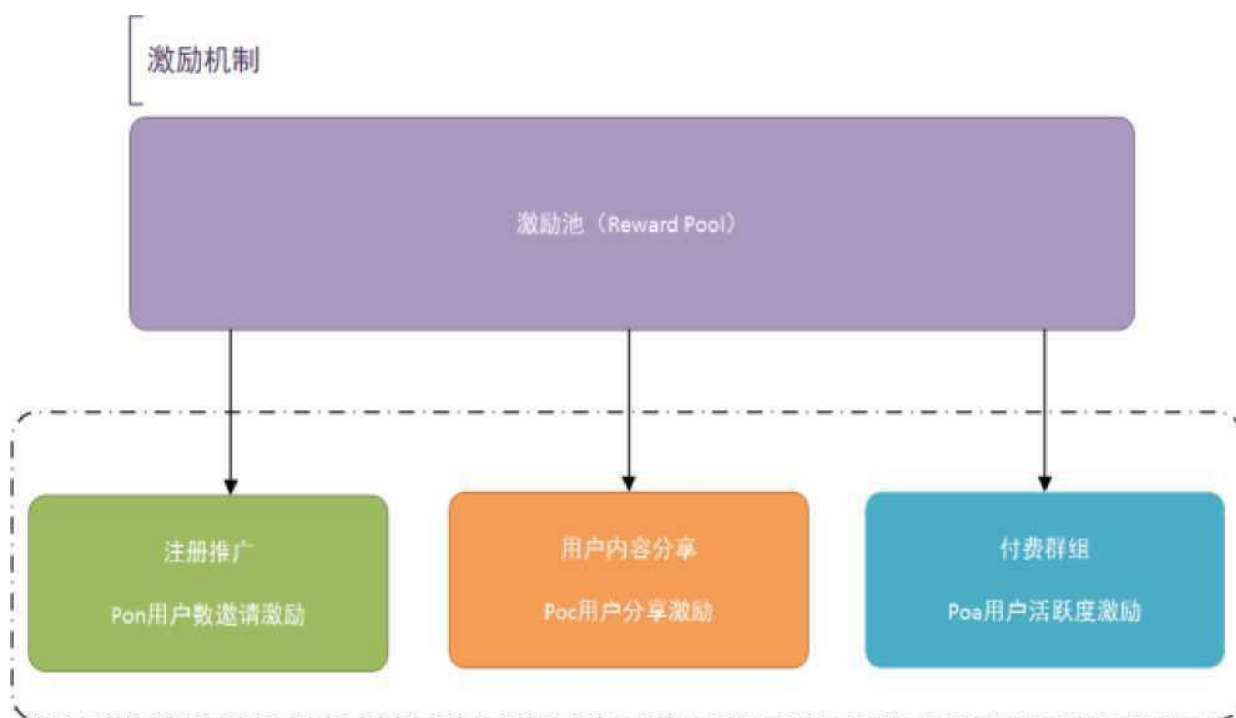
在 NewChat 生态系统中，允许用户投资由其他用户产生的优秀内容，并且投资者可获得其部分收益分成，而内容生产者（被投资者）也可以借此获得一次性收入以及后续的部分收益分成。

内容生产者在发布内容的时候可以设定为投资模式，并设定出让的收益分成份额以及投资截止期限。在期限内，内容投资者可以按份额投资该内容，内容生产者借此可以先获得一次性收入，而该内容在锁定期之后将会通过智能合约自动按份额分配给内容生产者和内容投资者。

## 四、激励机制

NewChat 设立专门的生态奖励基金，该基金采用 NewChat 内流通的虚拟货币 (NC) 作为唯一奖励方式。平台通过独有的 POA (Proof of Activity) + POC (Proof of Contribution) + PON (Proof of Number) 算法建立三重混合奖励机制，专门用于奖励对 NEWCHAT 生态系统建设及发展做出贡献的参与者。

奖励池系统每 24 小时进行一次激励分配计算，并根据计算结果，将奖励 token 自动分发到参与者的个人钱包中。



图中三种 NewChat 奖励机制示意图

## 4.1 奖励池(REWARDPOOL )

奖励池是一个专用于奖励 NewChat 生态系统建设及发展贡献者的奖励基金池。生态激励基金每天根据奖励弹性系数对奖励池进行自动补充。

## 4.2 社群奖励分配-PROOFOFACTIVITY (有效活跃度证明)

在社群功能中，采用 POA (Proof of Activity, 有效活跃度证明) 算法来进行奖励分配，即将奖励池中的虚拟货币按活跃度分配给每个社群群主。

POA 的计算方法如下：每 24 小时，奖励池将对每个社区的有效 DAU，有效聊天条数，有效聊天字数，有效参与聊天人数，有效在线人数，有效聊天时长，最高同时在线人数，新用户数量等数据进行计算，每个社群的活跃度值  $A_m$  为：

$$A_m = \sum_{i=1}^k a_i F_i$$

其中  $k$  为所有因子个数， $F_i$  代表社区活跃度证明的各个因子通过归一算法后的值， $A_i$  代表不同因子的权重。

每日分配数量为  $R$  的新增数字货币，将所有的已建设社群纳入分配范围，进行计算分配，每个社群管理员获得的奖励  $R_m$  为：

$$R_m = \frac{A_m}{\sum_{j=1}^n A_j} \times R$$

其中  $n$  是截止到分配时，整个生态内的社群个数。



### 4.3 用户奖励分配-PROOFOFCONTRIBUTION（有效贡献度证明）

NewChat 生态系统内，使用朋友圈及广场的用户每天也可获得相应的虚拟货币奖励。用户奖励将按照 POC（ProofofContribution，有效贡献度证明）算法，按照贡献度分配给朋友圈及广场的活跃用户。

NewChat 通过计算用户进行内容创作发布后，获得的浏览、点赞、评论、打赏、转发等行为；还有用户在朋友圈及广场内浏览内容，对其他用户发表的内容进行浏览、点赞、评论等这些行为，为每个用户计算等级  $L_n$

$$L_n = \sum_{i=1}^k a_i O_i$$

其中  $O_i$  为用户单个行为的次数通过归一算法后的值。同时包括了主动行为，如点赞、评论、发布内容等，也包括了被动行为如被关注、被点赞、帖子被浏览、帖子被评论等等。 $A_i$  是每种行为的权重。对于  $O_i$ ，在固定的时间周期内不同的行为有不同的阈值，超过阈值后进行该行为不会再影响用户的等级。

每 24 小时，NewChat 生态系统将通过 POC 机制放出奖励，奖励给当天所有为朋友圈和广场做过贡献的用户。

当天朋友圈和广场用户的贡献度  $C_n$ ，通过计算在当天范围内单个用户的主动行为  $S$  次数及被动行为：

其中  $S_i$  为单个主动行为次数通过归一算法后的值， $\alpha_i$  为该主动行为的权重， $\beta_i$  为单个被动行为的权重， $L$  为单个被动行为实施的人数。

$$C_n = \sum_{i=1}^k \alpha_i S_i + \sum_{i=1}^k \beta_i \sum_{j=1}^l L_j$$

## 4.4 用户推广分配-PROOFOFNUMBER（有效推广证明）

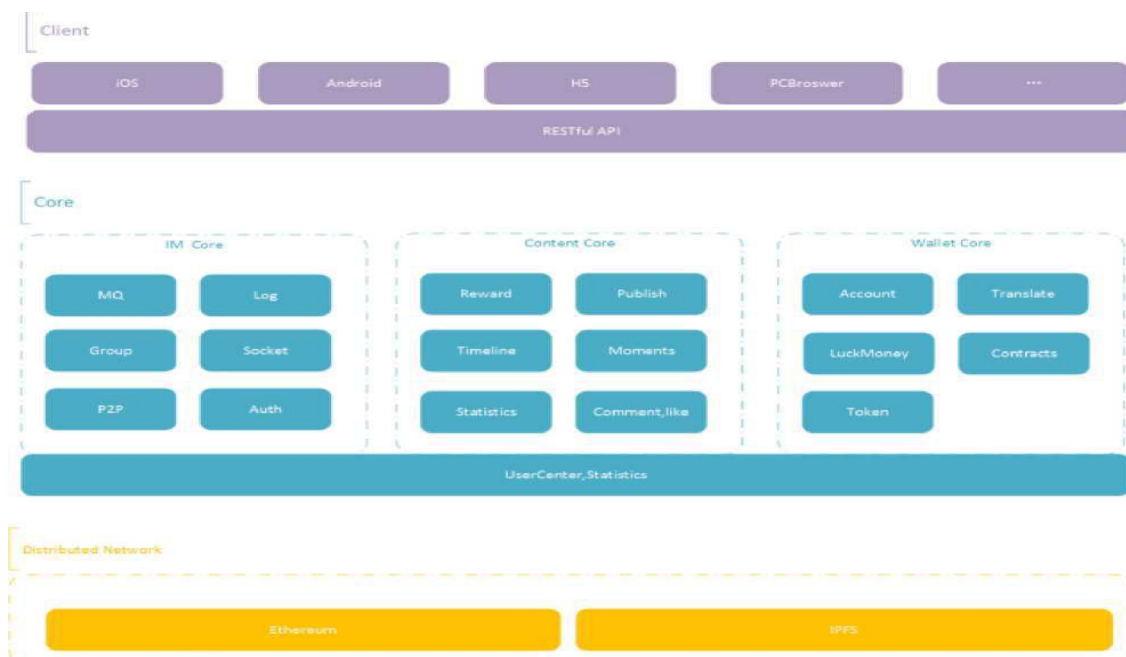
NewChat 生态系统内的用户通过分享推广 NewChat 可获得虚拟币 NC。奖励按照 PON（Proof of Number，有效推广证明）算法。按照推广后，实际贡献度分配给推广者。

NewChat 通过程序自动分配给每一位用户专属推广链接，根据该用户分享链接的次数，该链接获得的浏览数、通过该链接新注册的用户数等数据，为每个用户计算该获得的奖励  $N_m$  为：

$$N_m = \sum_{i=1}^k a_i O_i$$

## 五、技术实现

NewChat 的整体技术架构可分为三层：



客户端、核心功能层、底层架构。

### 5.1 客户端

客户端指 NewChat 为用户提供的各种终端产品，包括 iOS、Android、H5 等，以满足不同用户的需求。NewChat 还提供了一套功能完备的 RESTful API，其它公司的开发者，可以基于 NewChat 来开发自己的应用，也可以直接接入聊天核心库，快速在自己的产品中集成聊天模块。

### 5.2 核心功能升级模块一

客户端通过 RESTful API 访问 NewChat 提供的服务。为提供高可用、可并发、高性能的

RESTful API, 平台内部将搭建负载均衡、日志存储、服务监控、消息队列、授权验证、群组、钱包、智能合约、统一账户、数据统计等组件。

其中 UserCenter 模块为 NewChat 提供基础的账户服务, 账户将以最优的方式与以太坊账户相结合, 在保证用户资金绝对安全的情况下方便快捷的使用 NewChat 的各项服务。

Statistics 模块旨在记录保存 NewChat 系统内各项核心操作, 以便进行各项数据分析。数据分析包括群组活跃度计算、用户内容贡献度计算、用户注册和邀请分成计算等等。

IM 模块提供聊天通讯的各种基础服务, 包括消息队列, 群组, 点对点聊天, 推送, 长链接等各项基础服务。

钱包模块提供基于以太坊的帐户服务, 转帐, 智能合约, Token 等各类加密货币的服务 NewChat 同时将搭建开发者平台, 任何开发者都可以基于 NewChat 提供的接口开发第三方应用。

开发者平台上线时, NewChat 将提供完善的技术文档和示例程序以方便开发者快速上手。

## 5.3 核心功能升级模块二

NewChat 的部分核心服务是建立于区块链技术基础之上的。区块链部分目前基于以太坊公链开发。并计划在将来推出更适合社交场景的公有链。

### 5.3.1 Account

用户唯一的数字身份(Digitalidentity)标示;

### 5.3.2 Token

NewChat 的 Token (NC) 基于 ERC20 标准。用户可以通过 NewChat 基金会或者任何支持 ERC20 标准的应用来查看其 NC。在 NewChat 专属区块链公有链未上线之前, NewChat 将会基于以太坊发行原始 Token, 待公链完善后就会迁移, 迁移操作将不会对用户的使用和数字资产造成影响。

### 5.3.3 智能合约

以太坊的“智能合约”是图灵完备的，在 NewChat 底层中，众多约束都将写进智能合约中，以下介绍相关的部分合约实现。

在 NewChat，任何人都可以通过支付一定数额的 NC 创建一个自己的群组。为标示社区的唯一性和所有权，群组信息及其归属将会被写进智能合约。

NewChat 的智能合约中还将保存社区核心运营数据，例如用户规模、活跃留存、动态奖励等：群组的 POA 激励的分成算法；

内容生产者 POC 激励的分成算法； 用户注册邀请

时 PON 激励的分成算法；

以及随着 NewChat 发展的需要加入的其他动态规则。

### 5.3.4 IPFS

IPFS 网络是一个细粒度的、分布式的、易联合的内容分发网络，NewChat 动态中用户产生的图形、视频、文档等文件将存储 IPFS 之上。

NewChat 将对每个社区使用的资源情况进行统计，当发现有用户滥用资源时，将对该用户采取警告、封禁账户等措施。

## 六、技术总结

NewChat 将区块链技术更好的结合到社交通讯系统中来，解决了传统互联网技术无法解决的问题，创造了一个全新的生态，相信会给用户带来全新的体验，让普通用户无障碍对接全球的区块链数字资产世界，享受区块链技术带来的便捷。

本白皮书仅是对 NewChat 涉及的相关技术的部分概述，技术无止境，交流无国界，NewChat 的技术白皮书将随着更多生态的拓展而持续进行更新。同时，NewChat 将创造一个开放、共赢的技术生态，欢迎全球开发者共同参与和推进到 NewChat 生态体系技术的进步中来。

NewChat 团队

2018 年 5 月 7 日