We Media Chain

媒体区块网络白皮书 0.8

修订日期: 2018年5月18日

第一章、行业背景

1.1、自媒体流量交易

自媒体行业发展迅猛，越来越多的内容创作者通过自媒体实现了自己的社会价值，与之同时也为自己创造了收入，随之而来的，也有各种问题，内容抄袭，数据作弊，商业价值没有行业标准，收入不透明。

以微信公众号为例，目前微信有1000万个公众号，微信共有8.89亿月活跃用户，每人平均关注30个公众号，每天阅读10篇文章，仅公众号文章一项每天就会产生2.9亿阅读，而内容创作者通过微信公众号广告系统获得的收益却是微乎其微，而这些内容生产者的主要收入，必须依靠以营销性质软文投放，而价格不透明，中间商过多，没有可靠的费用担保平台这些问题，也不仅仅困扰着内容生产者，也是众多对微信公众号这一新媒体蠢蠢欲动的企业不敢大力投入的原因。

而区块链、智能合约技术，给了诸如为公众号流量变现的新思路，我们可以设计出一套去中心化的账单系统及智能合约系统，使用加密货币传递自媒体流量的价值，同时追溯媒体数据，使用智能合约促进各种各样的流量交易模式。

1.2、以销售线索为目的的媒体营销

而对于企业而言，销售线索的获取也变得更加重要，企业再诉求展示与点击效果的同时，更希望获得意向客户的信息，来帮助他们更好的营销和推广产品。因而构建一个消费者托管个人身份标识及隐私数据、自媒体提供推广渠道、企业直接从链上获取消费者授权的身份信息且通过推广渠道获得意向的分布式系统，变得十分有必要。

自媒体作为推广渠道，透过为企业带来有直接效益的营销服务，扩大了单位流量的价值，也能与那些不具备销售线索能力供给的媒体区分开来，获得更多的客户。

消费者通过向特定的机构开放信息获得更好，更精准的服务的同时，也能获取对应的收入，将本来应用在彼此不透明的信息猜忌模式里的费用，转移给真正提供信息和获得服务的消费者，最大化每个消费者的利益。

企业和机构也不再需要通过层层漏斗获得自己希望的客户，只需要在链上支付费用并设定筛选条件，就能得到想要的流量及用户。

第二章、技术细节

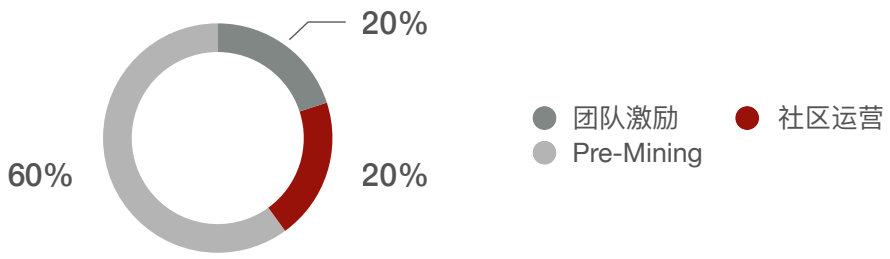
2.1、数字货币总量

WMC计划在主网上线前共发行15亿代币，这些代币将在主网上线时在创始块中做映射。

2.1.1、区块奖励策略

主网上线后，每年将会新产生1%的WMC，其中1/4奖励给20个超级节点，3/4分配给候选节点。

2.1.2、比例



20%代币用于团队激励，总计3亿，主网上线前不进入流通。

20%代币用于社区运营，总计3亿。

60%代币通过主网上线前的用户挖矿获得，总计9亿。

2.1.3、主网上线前的挖矿

主网上线前，为扩大用户规模，向授权我们使用数据的用户提供代币收入，借此吸引更多的DApp和消费线索购买机构加入。

9亿代币将在第一年释放50%，第二年释放25%，第三年12.5%，以此类推。

第一年每天共投放123.2877万，将分为两部分投放

1）数据交易，机构及开发者支付购买消费线索时支付的WMC，将占用当日产量。

2）挖矿奖励，除去数据交易部分的WMC，剩余的当日产量，将按照个人当日收入

$$I = (1232877 * (\frac{1}{2})^{c-1} - Y) * \frac{Xm}{\sum_{i=1}^{n} Xi}$$

计算收益，其中

Y代表机构及开发者数据交易使用的WMC的总量

c代表距创始日年份（1…n）

Xm代表用户个人的收益系数，n代表用户总量

Xi代表每个用户的收益系数。

如果总难度系数为1,000,000，个人难度系数为6，在空投开始第一年，当日机构购买消耗了1,000,000WMC，则该用户当日收入为

$$(1232877 * (\frac{1}{2})^{1-1} - 1000000) * \frac{6}{1000000} = 1.397262$$

2.1.4、机构及开发者使用WMC

初期机构在媒体及应用上发生数据交易时

媒体及应用可将流量转化为WMC，（产量减半）

限制媒体流量收益

$$I \leqslant N \times 5 \times (\frac{1}{2})^{c-1}$$

其中N为媒体产生的有效CPC，c为距创始日年份。

即第一年，每个有效CPC将获得5个WMC，第二年每个有效CPC将获得2.5个WMC，以此类推。

消费者可根据自己信息丰富程度来获得WMC，（动态价格）

由消费者设定维度基础价格，机构在设计评分算法时，会增加复杂程度，得到难度系数，其乘积将直接从机构扣除转移给消费者。

2.2、权益证明方式（DPOS）

2.2.1、背景描述

委托权益证明（DPOS）是目前所有共识协议中最快，最有效，最分散，最灵活的共识模式。 DPOS利用利益相关方批准投票的权力以公平和民主的方式解决共识问题。 所有网络参数，从费用估算到块间隔和交易规模，都可以通过选定的代表进行调整。 块生产者的确定性选择允许平均仅需要1秒就能确认交易。 也许对我们来说，最重要的在于共识协议旨在保护所有参与者免受不必要的逻辑检查。因为这一块对于大部分共识协议来说，是最大的瓶颈。

2.2.2、被选举的见证人区块生产过程描述

选举见证这个词是因为它是一个不受监管的法律上中立的词。 传统的合同通常有见证人（Witnesses）签名的地方。但是对于非常重要的合同，有时会使用公证人来进行公证。 见证人和公证人都不是合同的缔约方，但是他们在证明”整个合同是在指定时间由指定人签署而非其他人”起到非常重要的作用。 在DPoS中，见证人通过将其包含在链的区块中来起到类似的验证签名和时间戳事务的作用。

在DPOS的共识协议下，利益相关方（Stakeholders又名股东）可以选择任意数量的见证人来生成区块。在这里，区块是指一组更新数据库状态的事务。 每个账户允许每个见证人拥有一张选票，这个过程称为被批准投票。 如果说通过总审批的前N名证人被选中，那么见证人数目（N）的定义必须至少有50%的投票，利益相关方才能认为整个投票过程是足够的去中心化的。 当利益相关者提出他们所希望的见证人数量时，他们也必须投不低于该数量的投票。 同时也不能说为了实现去中心化而投出比见证人数量更多的票。

每当见证者们生产一个区块时，他们都会为他们付出的服务进行费用的收取。 他们的费用高低由利益相关者通过他们选出的代表制定（稍后讨论）。 如果见证人没有生产出一个区块，那么他们就没有收入，同时还有可能在未来被投票出局失去见证人身份。

每次经过一个维护间隔时间（目前为一天）活动证人的名单会更新一次，同时当选票会被记录。 然后将所有见证人轮换进行所谓的洗牌过程，并且每个见证人轮流在每2秒的一个固定时间内产生一个区块。 在所有见证人轮流直至洗牌结束，见证人再次进行洗牌过程。 如果在一次洗牌过程中，证人没有在他们的时间段中产生一个块，那么该时间段（2秒）后将见证人会被跳过，下一个证人产生下一个块。如此循环。

在整个过程中，任何人都可以通过观察见证人的参与率来监测网络健康状况。 如果在某个时候见证人的参与程度都低于一定水平，那么整个区块链交易网络用户可以被允许用更多时间进行交易确认，而且还会提醒用户需要对他们的网络状况保持高度警惕。 可以在出现问题后的1分钟内提醒用户区块链网络上可能存在潜在的问题。

2.2.3、选定的代表可以进行共识协议参数调整

这些能够进行参数修正的选定代表们（Elected Delegates）其选举方式的产生类似于证人的方式。 代表成为特权帐户的共同签名者，该特权帐户有权提出对网络参数的调整。 这个特权账户通常被称为创始账户。 这些参数包括交易费用，区块大小，见证人服务费用和区块生产的间隔时间等等。 在大多数代表批准了提议的变更后，利益相关方被授予2周的审查期，在此期间他们可以为代表投票是否同意或者取消提议的变更。
这种设计的选择是为了确保在技术上代表们没有直接的权力，并且网络参数的所有变更最终都需要得到利益相关方的批准。 这样做是为了保护代表不受可能适用于加密货币自身的管理员或者项目方的影响。 在DPoS下，我们可以确切地说，行政权力掌握在用户手中，而不是单方面的代表或见证人。
代表与见证人不同的是代表是一个公益身份，并不会有酬劳。 当然，一般来说，对整个区块链网络这些参数的调整是非常非常少的，毕竟涉及到整个网络。生成帐户可以在技术上执行任何其他帐户可以执行的任何操作，这意味着可以将资金发送到创建帐户或指定创建帐户作为托管代理。 起源账户也可以用来发行新资产。
当选代表可以帮助利益相关者执行需要高度信任和责任感的任务时，有大量的应用程序。

2.2.4、关于分叉

有时需要升级网络以添加新功能。在DPOS的共识机制下，所有变更必须由积极的利益相关方批准才能触发。 虽然技术上见证人可以单方面串通和改变他们的软件，但这样做并不符合他们的利益。 基于见证人自己在对区块链政策保持中立的承诺才能被选举上，因此见证人一般会通过保持重力来免受区块链网络管理员/经理/业主/经营者的指控，毕竟见证人也是他们的雇员。
只要利益相关方批准，开发人员可以实施他们认为合适的任何更改。这项政策不仅可以保护开发者，同时它还可以保护利益相关者，并确保没有任何人单方面控制区块链网络或让区块链网络失控。
硬分叉是如同替换了51%的见证者，因此利益相关者参与的越多，其对应的选举证人越多，那么整个系统的安全性就越高。
当然最终能够进行硬分叉，其实最终取决于网络上的每个愿意升级他们的系统的用户。并且不存在一个能够强制硬分叉的区块链协议。这意味着如果大部分用户愿意进行系统升级，那么就可以在没有需要利益相关方投票的情况下推出硬分叉来进行“错误修复”的操作。

实际上，很少通过直接大部分用户直接升级软件的方式进行硬分叉。一般来说，无论多小的内容升级，开发者和证人都应该遵循流程，等待利益相关者批准之后再进行分叉操作。

2.2.5、双花问题

在任何一个包含“前序交易”的区块链上都会发生双花问题，而使用DPoS共识机制下，该问题通过自身系统区块链重组来排除此类问题，因此这意味着即使见证人会因互联网基础设施的中断而导致通信故障，但通信故障导致双花的攻击行为可能性会非常低。同时该网络会在在发生故障导致见证人未能按计划生产区块的同时，能够监测自己的健康状况，并可以立即检测到通信中出现的任何损失。如果发生这种情况时，用户可能需要等到一半以上的证人确认交易后才能继续进行下一个交易，这个过程可能会长达一到两分钟。

2.2.6、交易权益证明机制

网络上的每个事务可以可选地（Optionally）包含最近块的散列哈希。 如果这样选择触发此项机制，那么交易的签署人可以在任何一个包含该交易的区块链中确信他们的交易。但这一过程的副作用是随着时间的推移，所有利益相关者需要验证整个历史的交易信息。

2.2.7、区块链重组

一般来说，由于所有见证人都是选举产生的，理因是高度负责任的，并且其自身是在专用时间段来生产区块，因此很少有可能存在两条竞争链的情况。虽然网络延迟会时不时阻碍到一名见证人及时收到前一个区块。 如果发生这种情况，下一个见证人将通过构建在他们首先收到的任何一个区块上来解决问题。 最后凭借整个区块链上99%的证人参与，来确认一个有99%的机会被验证的交易。

尽管该系统有强大的鲁棒性，能够通过对原链重组来对抗发生的区块错误。但该系统仍然存在一些潜在的软件错误、网络中断或无能/恶意的见证人会创造长于一个或两个块的多个竞争链的情况。 因为软件始终选择见证人参与率最高的区块链。但见证人自己每此只能产出一个区块，因此参与率总是比大多数人低。 所以，没有任何证人（或少数证人）能够做出更高参与率的区块链。 而参与率的计算是通过比较预期产生的区块量与实际产生的区块数量来进行的。

2.2.8、最大限度的去中心化

在DPoS共识机制下，每个利益相关者的影响力与其利益成正比，没有任何的利益相关者（用户）会被排除在行使这种影响力之外。 但是市场上的其他共识系统几乎都存在这种情况。 以下有很多种来排除了据大多数利益相关者（用户）影响力的方式。 其中一些方式是通过设计邀请制的机制来减少大多数利益相关者（用户）的系统控制参与度。 其他则是通过让参与费用高于他们的收入费用来排除其（用户）参与。 还有一种是通过技术上允许每个利益相关者（用户）参与，但是他们却可以被产生绝大多数块的一些大型玩家（庄）轻易地忽略其影响力。 而只有DPoS确保块生产的区块平均分配给整个系统的大多数人，并且每个人都有一种经济可行的方式来影响这些人。

2.3、角色

2.3.1、普通用户

普通用户持有一定量的WMC，可以自由交易并且参与投票；

2.3.2、见证人

由普通用户选举产生见证人代表投票的所有普通用户的WMC总量进行交易及合约见证，并获得交易手续费及区块奖励；

2.3.3、机构

机构通过购买媒体的流量及消费者的数据，消费自己拥有或者被许可的WMC。机构早期将直接或者间接向区块链投入资金

2.3.4、开发者

开发者为机构和媒体之间的价值交易建立桥梁，针对不同的领域，开发不同的DApp，帮助消费者更安全更便捷的获取服务，同时也让机构能够更直接的与消费者建立起联系。

2.4、技术规范

WeMediaChain使用智能合约保证透明，去中心化的，不可篡改的，高可靠性的基础。具有去中介化的信任，稳定性可靠性和持续性，强安全共识机制，交易的公开透明不可篡改基本特征。借助智能合约，媒体相关的所有数据都可以通过合约代码来描述，并且保留了区块链技术的优点。

为了实现所描绘的应用场景，我们将通过如下的实际技术解决方案来为链上的应用提供信用背书和技术保障。

2.4.1、ERC20代币，主网上线前的权益确认方案

在主网上线前采用符合 ERC20代币标准，可兼容以太坊钱包，方便用户进行存储、转账、交易等操作。通过ERC20代币实现去中心化的权益确认，WeMediaCoin的ERC20代币与主网的WeMediaCoin将具备相同的价值，这些代币将在主网上线时通过映射转移到对应的WeMediaCoin主网钱包中。

WeMediaCoin的ERC20代币在主网上线前会提供两种存储模式：

1、运营者可在合作机构官网查询到自己钱包中的余额，可进行站内转账、充值、提现等操作；提现操作会扣除WeMediaCoin的ERC20代币作为交易手续费，站内转账、充值不扣除手续费；

2、运营者可以下载桌面钱包、Chrome扩展MetaMask，在本地生成冷钱包，通过模式一中的体现动作将WeMediaCoin的ERC20代币提现到自己的钱包中，提现完成后，转账动作将扣除ETH作为矿工费，但是在以后我们将实现WeMediaCoin的ERC20代币支付矿工费的能力。

2.4.2、星际文件系统（INTERPLANETARY FILE SYSTEM，IPFS)，去中心的流量追踪及资源访问方案

IPFS的全称是InterPlanetary File System星际文件系统，是一个点对点的网络超媒体协议。它的目标是成为更快、更安全、更开放的下一代互联网。

IPFS将加密后的数据分块存储在由IPFS矿工组成的去中心存储网络上，可以随时随地高效安全的调取需要的数据，因为数据回源来自于最近的节点，所以能很好解决最后一公里传输性能的问题，而因为数据被分块且加密存储在分布式的节点上，数据被盗、遭受DDoS攻击的风险也大大下降。

WeMediaChain中的用户敏感数据、私钥、指纹等信息将隐匿存储在WeMediaChain中，资源提交较大、安全需求程度低、访问频繁的资源会通过私钥加密后储存在IPFS中，提供更为高效的访问、检索模式。

InterPlanetary文件系统（IPFS）是一个内容可寻址的分布式文件系统，它保证由其加密散列标识的文件内容的固定性。文件通过对等网络延迟解决。然而，内容寻址引用本质上是不可变的，因此在每个应用程序中都不实用。例如，如果HTML网页使用其引用嵌入图像，则每次更新图像时都需要更新引用，否则网页仍将引用旧版本的图像。如果许多网页中包含相同的图像，则所有这些图像都需要更新，因此它们自己的哈希值也会改变。这具有级联效应，并且通过引用而非价值来杀死包括对象的主要目的，以实现关注和重用的分离。

为了解决这个问题，IPFS使用InterPlanetary命名系统（IPNS），该系统提供从人类可读URI到其对应的当前IPFS哈希的映射。域名的所有者可以通过用他/她的私钥对请求进行签名来更新该域下所有URI的映射。IPNS可以以多种方式实现，但其当前的实现使用分布式哈希表（DHT）。因此，只有每个URI与其对应的散列的最近映射才可用于解析，而忽略任何历史映射。从档案的角度来看，这并不好，因为以前的文件版本可能仍然存在于IPFS存储中，但是其对应的URI映射却会丢失。

传统的网络档案可能仍然有一些历史观察，可以使用给定的URI来检索旧版本的文件，但这些记录将在IPFS系统之外，并且历史可能是稀疏的而不是事务性的。

我们可以通过对IPNS记录使用区块链来解决这些问题。通过这样做，IPFS可以像事务性存档引擎一样工作，同时将所有历史“URI - >哈希”映射保留在公共区块链中。使用IPNS Blockchain解析URI应该返回当前映射，而使用Datetime解析URI应该返回当时存在的映射。该备忘录框架可用于基于时间的脉冲中子源的分辨率。

WeMediaChain在为机构或者开发者提供流量追踪功能时，会将投放资源存储在IPFS并提供IPNS下更短更便于传输和记忆的资源域名，并同时提供访问追踪的能力，杜绝传统流量追踪方案中中心作假及数据不透明的问题，将会出现更多第三方清洗流量的应用，最大程度的规避流量作弊的灰色手段。

2.4.3、数据公证方案，数据公证人规则

对于WeMediaChain在执行智能合约时需要的真实数据问题，我们会采取数据公证人制度对数据提供者（见证人）进行群体智慧验证，由于这些真实数据是在现实世界已经发生的，此时投票的人通常已经从现实世界获取了真是的数据，大部分人会给出肯定或者否定的投票。我们使用80%（而非51%，因为这不仅仅是奖励及规则的竞争，而关系到数据的真实性）这个阈值来决定是否让结果生效。而数据提供者会缴纳押金，进而保证诚实节点及投票者能获得更多的利益。

2.4.4、数据脱敏及阻止二次贩卖方案，零知识证明&智能评分合约

零知识证明(Zero—Knowledge Proof)，是由S.Goldwasser、S.Micali及C.Rackoff在20世纪80年代初提出的。它指的是证明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。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。大量事实证明，零知识证明在密码学中非常有用。如果能够将零知识证明用于验证，将可以有效解决许多问题。

在有必要证明一个命题是否正确，又不需要提示与这个命题相关的任何信息时，零知识证明系统(也叫做最小泄露证明系统)是不可或缺的。零知识证明系统包括两部分：宣称某一命题为真的示证者(prover)和确认该命题确实为真的验证者(verifier)。证明是通过这两部分之间的交互来执行的。在零知识协议的结尾，验证者只有当命题为真时才会确认。但是，如果示证者宣称一个错误的命题，那么验证者完全可能发现这个错误。这种思想源自交互式证明系统。交互式系统在计算复杂度理论方面已经获得异常独立的地位。

零知识证明(Zero—Knowledge Proof)起源于最小泄露证明。设P表示掌握某些信息，并希望证实这一事实的实体，设V是证明这一事实的实体。假如某个协议向V证明P的确掌握某些信息，但V无法推断出这些信息是什么，我们称P实现了最小泄露证明。不仅如此，如果V除了知道P能够证明某一事实外，不能够得到其他任何知识，我们称P实现了零知识证明，相应的协议称作零知识协议。

在通常的大数据平台中，数据以结构化的格式存储，每个表有诸多行组成，每行数据有诸多列组成。根据列的数据属性，数据列通常可以分为以下几种类型：

1、可确切定位某个人的列，称为可识别列，如身份证号，地址以及姓名等。
2、单列并不能定位个人，但是多列信息可用来潜在的识别某个人，这些列被称为半识别列，如邮编号，生日及性别等。美国的一份研究论文称，仅使用邮编号，生日和性别信息即可识别87%的美国人。
3、包含用户敏感信息的列，如交易数额，疾病以及收入等。
4、其他不包含用户敏感信息的列。

所谓避免隐私数据泄露，是指避免使用数据的人员（机构、DApp开发者、数据分析师，BI工程师等）将某组数据识别为某个人的信息。数据脱敏技术通过对数据进行脱敏，如移除识别列，转换半识别列等方式，使得

数据使用人员在保证可对#2半识别列（转换后）、#3敏感信息列、#4其他列进行数据分析的基础上，在一定程度上保证其无法根据数据反识别用户，达到保证数据安全与最大化挖掘数据价值的平衡。

通常的数据脱敏算法包括以下几种，

名称	描述	示例
Hiding	将数据替换成一个常量，常用作不需要该敏感字段时。	500 —> 0 635 —> 0
Hashing	将数据映射为一个hash值（不一定是一一映射），常用作将不定长数据映射成定长的hash值。	Jim, Green —> 4563934453 Tom, Cluz —> 4334565433
Permutation	将数据映射为唯一值，允许根据映射值找回原始值，支持正确的聚合或连接操作。	Smith —> Clemetz Jones —> Spelde
Shift	为数量值增加一个固定的偏移量，隐藏数值部分特征。	253 —> 1253 254 —> 1254
Enumeration	将数据映射为新值，同时保持数据顺序。	500 —> 25000 400 —> 20000
Truncation	将数据尾部截断，只保留前半部分。	021-66666666 —> 021 010-88888888 —> 010
Prefix-preserving	保持IP前n位不变，混淆其余部分。	10.199.90.105 —> 10.199.32.12 10.199.90.106 —> 10.199.56.192
Mask	数据长度不变，仅只保留部分数据信息。	23454323 —> 234---23 14562334 —> 145---34
Floor	数据或是日期取整	28 —> 20 20130520 12:30:45 —> 20130520 12:00:00

除此之外，根据实际的业务场景我们还可以通过维度转换的方式，保证更大的数据安全级别同时满足企业数据挖掘的最大化收益，

假设一家金融机构评估目标用户的逾期可能性P

$$\mathscr{P} = f_s(f_1(Y_1), f_2(Y_2), f_3(X_1), f_4(X_2), f_5(X_3))$$

其中，
F1-F5为机构评估各个维度的标准化算法
Fs为机构为各个维度加权的算法
Yi为机构已知数据
Xi为用户敏感数据

而如果我们能找到函数Fx使得

$$X = f_x(fa(X_1), fb(X_2), fc(X_3))$$

$$\mathscr{P} = f_{s1}(f_1(Y_1), f_2(Y_2), f_n(X))$$

就可以使得机构在不知道Xi的情况下，得到诉求的结果P。

而因为Fx得到的结果X，与机构的算法Fsi及实际业务有着密切的关系，因此另外一家机构获得X的值对自身业务也是没有任何帮助的。

甚至进一步杜绝有相同需求的机构共享用户信息，我们可以使用用户的公钥加密Fx，用户本地使用私钥解密并运行算法Fx后，使用机构公钥加密X，返回给机构，机构不会向自己的竞争对手提供Fx的详情，因而机构贩卖X到市场中并不会有人为其买单。

2.4.5、阻止骚扰，私密通道

在传统中心化的营销体系中，通过电话及IM工具与消费者直接通信一直以来都存在这严重的问题，不仅机构可以肆意出售消费者的联系方式（此类问题已经通过私密专线等问题得以解决，但提供私密专线的中心仍旧保有用户的联系方式），且用户无法定向阻止机构的进一步骚扰电话。

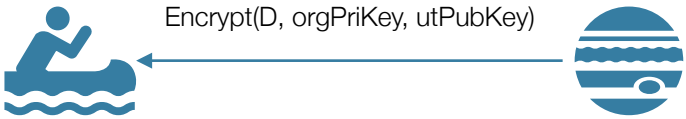
我们将通过基于时间种子的加密算法，为支付费用的机构建立起与消费者的私密通道，通过我们合作的各种DApp提供机构与消费者的通信通道，与此同时，一旦超过了通信的约定时间，机构向消费者的消息传输就会被中断。整个过程中不会有用户的私密联系方式流出，最大程度的保障了消费者的隐私。

我们认为在机构与消费者的通信过程中，消费者是处于相对弱势的地位，消费者使用通信产品的目的是为了与自己的朋友、家人通信，而非接收营销信息，这不仅仅指电话，也指那些中心化的IM软件，诸如QQ、微信、Facebook、Line等等，营销往往是这些中心化的通信产品的核心商业模式，在现代商业社会这无可厚非，但是随着越来越多的安全、私密、去中心的通信产品诞生，消费者将拥有更多在通信产品中的主动权，可以选择接受哪些或者不接受哪些信息；

基于这个即将发生变革，我们相信，搭建一条从机构到消费者，单向的，在一定时间内可以传输有效信息的通信通道，将是机构未来能与消费者取得联系的唯一通道。

而这一特性，将广泛应用到我们合作的去中心通信产品中，成为有效隔离骚扰同时又能为开发者和消费者带来收入的全新营销渠道。

机构消息传送时的加密过程可以简化描述为如下图示：



机构加密消息的过程如下：

$$utMessage = AES(encrypt(D, utPubKey), utPropSigned)$$

机构需要推送的数据D，会通过用户许可的一定时间有效的临时钥匙对utKey的公钥进行加密，得到仅用户能解密的隐匿消息体_utMessage，并使用utPropSigned进行对称加密，得到utMessage。

用户在公布utPubKey（用户许可的一定时间有效的临时钥匙对中的公钥）时，会使用utPriKey加密utProp（用户许可的一定时间有效的临时钥匙对中的时间信息）得到utPropSigned。

$$orgMessage = encrypt(orgMessage + utPropSigned, orgPriKey)$$

机构使用自己的私钥orgPriKey加密utMessage及utProp得到携带机构签名的orgMessage，

并将orgMessage，utPropSigned广播到区块网络中。

节点接收到消息后会经历以下的效验过程

1）节点使用机构广播的公钥解密orgMessage，得到utMessage及utPropSigned

2）节点使用用户广播的utPubKey解密utPropSigned得到utProp，

3）节点检查utProp生命的时间是否仍旧有效，如果已经超出utProp声名的时间，则拒绝该消息的传播

4）节点推送orgMessage到用户终端

用户接收到消息后会通过以下过程获取消息内容

1）通过自己已知的授权机构，确认消息来自自己授权的机构。

2）使用orgPubKey解密得到utMessage及utPropSigned

3）检查utPropSigned是否为自己签发，以及时间是否合法

4）解密得到消息体D

2.5、钱包

2.5.1、ERC20代币钱包

代币钱包提供冷钱包的基本能力，可以通过本地生成新的私钥及地址，来保存从合作机构提供的WMC；
代币钱包生成的钱包地址可接受WMC代币及ETH，由于ETH网络的限制，转移WMC需要支付ETH手续费，因而当WMC提现到冷钱包之后，转账需向冷钱包地址存入相应的ETH方可进行；
在ETH随后的升级过程中，我们会增加合约余额用户支付用户转移WMC的手续费，相应的会扣除一定的WMC；
因而现在本地钱包多用于余额汇集和长期存储的能力，如果需要进行转账可以通过合作机构提供的内部转账能力进行转账；

第三章、应用场景

3.1、追溯自媒体价值

成交价格及媒体数据将会写入区块链，无法篡改，新的交易会根据以往的交易信息进行评估；而媒体数据将会由见证人共同确认，避免作弊行为的发生；

3.2、合约交易

运用智能合约设定流量交易模式并经发布后不可修改

3.2.1、条件支付模式

媒体数据达到不同的级别，支付不同的WMC；

3.2.2、按量支付模式

媒体数据根据公式计算得到应支付的WMC；

3.2.3、收益转让

当媒体所有者发生变化时，能将价值及未来的收益过渡给新的所有者，变更一旦发生并且得到节点确认，就无法被撤回，原所有者也将得到相应的WMC；

3.3、数据交易

运用智能评分合约脱敏用户数据，并向机构提供有价值的维度评分数据。

3.3、消费线索交易

超级节点将提供用于追踪消费者点击行为基于IPFS的星际域名，当用户点击企业制作的广告同时，将会自动完成一次数据交易，将消费者的消费意向及维度评分提供给企业主并获得WMC。

第四章、WeMediaChain团队

4.1、开发机构

决策委员会，

主要负责制定重要决策、召开紧急会议，以及聘请解聘各职能委员会负责人。首届决策委员会成员将由团队成员以及早期投资人组成，任期为 3 年，期满后重新选出。决策委员会由5名成员构成；

代码审核委员会，

由开发团队中的核心开发人员组成，负责底层技术开发、开放端口开发和审核、各产品开发和审核等等；

财务及人事管理委员会，

主要负责项目募集资金的运用和审核、开发人员薪酬管理、日常运用费用审核等；

市场及公共关系委员会，

负责WeMediaChain技术推广、WeMediaChain产品推广和宣传、对外公告管理、公关维护等等；

第五章、合作机构

5.1、自媒体平台类型

预打包分配机制
公众号在自媒体平台的公众号图文、效果广告，可自主选择将部分流量以WMC形式结算，而不再继续参与流量变现服务；

参与主网上线前的挖矿
用户可以在合作机构及合作机构自媒体的平台上参与主网上线前的挖矿。

充值、转账、提现
运营者在合作机构获得的WMC将存储在运营者的合作机构账号中，在合作机构内的WMC内部转账可随时进行（无手续费），同时获得一个ETH地址，用户也可以从外部转入该ETH地址WMC进行充值（无手续费），用户希望将WMC提现到自己的冷钱包中时，可以支付一定的手续费（根据ETH矿工费动态调整）提现到自己的ETH地址；

5.2、合作机构规范

5.2.1、WMC兑换规则

合作机构在兑换比例不高于2.1.4规定的标准时，可自由约定兑换比例，且流量兑换WMC的兑换行为只能单向进行；
兑换请求将提交至WMC合作机构委员会进行审核，通过后方可完成兑换工作；

5.2.2、接入并接收WMC投放

合作机构应提供可以完全由WMC进行的CPC或图文交易，按照2.1.1规定的标准进行广告投放；

5.2.3、提供WMC充值、提现、内部转移、合作机构间转移的能力

合作机构应提供WMC向支持ERC20标准的冷钱包提现、从支出ERC20标准的冷钱包充值的功能，提现手续费由WMC支付（不超过转出WMC的5%或者100WMC，两者相较取较大值），可自由裁定，充值不应扣除手续费；

合作机构内部WMC转账应免除手续费；

合作机构机构间转账应按照转出机构的标准收取手续费（不超过转出WMC的5%或者100WMC，两者相较取较大值），接收机构不再收取手续费；

第六章、开发规划

6.1、第一阶段2018年4月 - 2018年6月

6.1.1、能够进行简单的信息打包，并以此为依据产生预分配的代币

6.1.2、完成钱包

6.1.3、支持合作机构进行主网上线前的挖矿

6.2、第二阶段2018年7月 - 2018年12月

6.2.1、完成DPoS机制，矿工可参与到挖矿工作中去

6.2.2、完成数据见证人规则，可由节点提交及确认真实数据

6.2.3、完成智能合约，能进行合约交易

6.3、第三阶段2019年

6.3.1、与自媒体平台建立合作，支持区块链回溯

6.3.2、与企业建立合作，使用WMC进行媒体广告投放

第七章、其他事务及法律风险

7.1 法律事务

自媒体链基金会会聘请专项法律顾问及常年法律顾问，主要目的用于建立法律纠纷预防机制、处理 已存在的相关法律问题，协助和配合相关部门。

7.2 免责条款

自媒体链基金会目标转变为非营利组织，链上用户获取的是WeMediaChain的使用权。购买者需明白在法律范围内，WeMediaChain 不做任何明示或暗示的保证，并且 WMC 是“按现状”购买的。此外，购买者应明白 WMC 不会在任何情况下提供退款。 本白皮书会根据项目进展升级版本，同样具备法律效应。

7.3 争议解决条款

当出现争议争议时，有关方面应依据协议通过协商解决，如协商无果，可通过法律解决。

第八章、风险提示

WeMediaChain 项目的所有权属于全体 WMC 代币持有人，并非权益投资项目。WMC 代币及用于换取 WMC 代币的比特币（BTC）、比特现金（BCC）等数字货币均非法定货币，本文档所提供信息不 构成任何投资建议，同时参与者应注意到（包括但不限于）以下风险：

8.1 运营性风险

指的是 WeMediaChain 在认筹资金以及开展业务的过程中违反了当地法律法规，造成无法继续经营的风险。

8.2 流通性风险

指的是在 WMC 没有被市场接纳或没有足够用户使用，业务开展停滞。

8.3 系统性风险

指的是底层技术出现重大问题，导致关键资料被才或丢失； 項目資金出現重大損失，例如：資金被盗，資金虧損，儲備金、大幅貶值等。

8.4 其他不可抗力风险

一切不可预料及不可抗力风险

免责说明

该文档只用于传达信息之途，并不构成本项目买卖的相关意见。以上信息或分析不构成投资 决策。本文档不构成任何投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任 何买卖证券的行为，也不是任何形式上的合约或者承诺。相关意向用户明确了解本项目的风 险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果 或后。运营团队不承担任何参与本项目项目造成的直接或间接的损失。