DMOC WHITEPAPER

钻石公链白皮书 1.0

摘 要

21世纪人类由模拟电路时代，进入了数字电路时代。人类信息化系统也由原来单机系统进入了中心化的分布式系统，而到了今天人类将踏上一个历史的新征程：去中心化分布式信息系统。

众所周知在一个分布有众多节点的系统中，每个节点都具有高度自治的特征。节点之间彼此可以自由连接，形成新的连接单元。任何一个节点都可能成为阶段性的中心，但不具备强制性的中心 控制功能。节点与节点之间的影响，会通过网络而形成非线性因果关系。这种开放式、扁平化、平等性的系统现象或结构，我们称之为去中心化。

随着主体对客体的相互作用的深入和认知机能的不断平衡、认知结构的不断完善，个体能从自我中心状态中解除出来，称之为去中心化。

去中心化，不是不要中心，而是由节点来自由选择中心、自由决定中心。简单地说，中心化的意思，是中心决定节点。节点必须依赖中心，节点离开了中心就无法生存。在去中心化系统中，任何人都是一个节点，任何人也都可以成为一个中心。任何中心都不是永久的，而是阶段性的，任何中心对节点都不具有强制性。

当今社会已经存在了大量成熟的去中化心解决方案，但是他们都并还不够优秀。以至于他们的落地应用性非常弱，还不足以拿来商用，甚至是拿来解决传统应用的开发。DMOC (DIAMOND COIN) 基于当前的现状痛点，提出了全新的技术平台理念，成功地构建了一个可快速落地的IT信息化系统构建 的生态解决方案。（NetworkOmnipotenceApplication网络 全能应用）

在区块链行业不断发展的过程中，无序是导致欺骗最大的诱因，中心化、低水平的去中心化是阻碍区块链技术发展的关键性阻力。在无序的市场状态下行业需要一些先进力量进行结构性改变，回到瓦解时代，由一批敢于创新制造，敢于想象的浪人引领，打破原有的秩序，重塑新秩序，再由匠人肩负起一个重振时代，打造未来行业新方向。

我们希望在即将到来以及更远未来的项目中，不再有中心化集权的现象产生，广泛的DMOC社区成员共同引导项目发展方向，而不是单个核心团队来决定项目的未来，未来的DMOC将是也应该是多团队维护，多社群共识，100%属于所有DMOC持有者，真正使DMOC的社区共识成为鲁棒性基础，而不是某个精英集团的专属。

DMOC是为了应用而生，是可以解决全网络应用的基础设施，同时也将成就全新的区块链治理模式，为自身凝聚共识的同时将作为领导者为行业提供标杆案例，价值观与理念输出作为DMOC的突出优势随着治理框架逐步完善具备更优质的可借鉴性。

高质量的理论与数量众多且具备可拓展性的应用将共同成就DMOC的未来生态，也将成为引领行业的坚实力量。

不管你今天是否认可，我们正在悄悄地改变世界的未来！人类新的信息化征程再次到来！DMOC公链为应用而生，改变你、改变世界、改变未来！

参考资料:

Reid, Alex (1995). "IT Strategy Review, Distributed Computing – Rough Draft". Retrieved 2013-11-06.

目录 CONTENT

二、技术方案

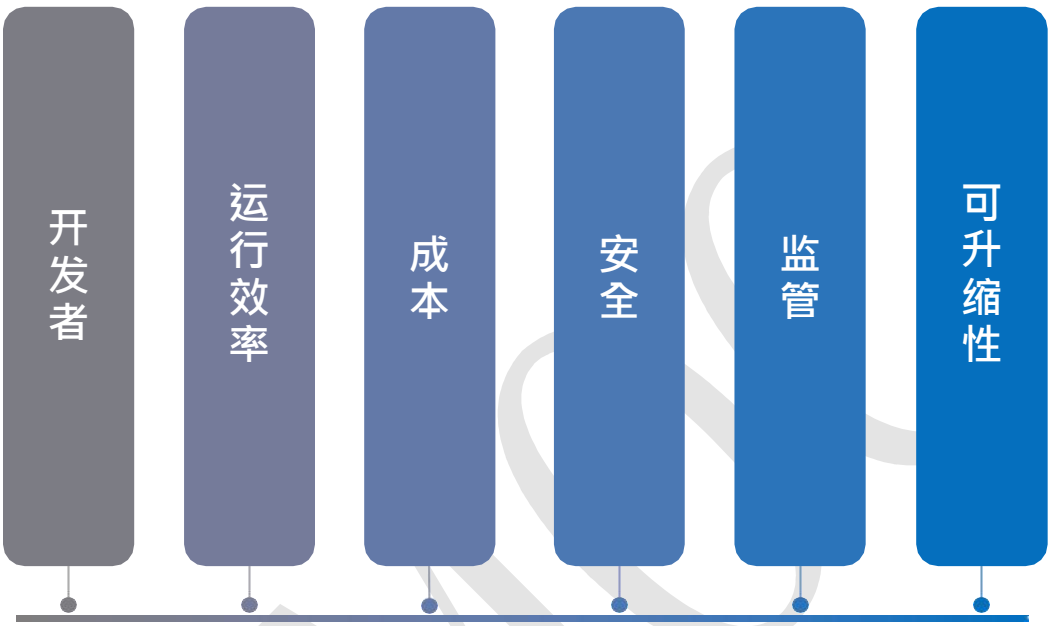
一、背景与愿景 Background and Vision

1.1 共有链是去中心化信息系统的基础设施

所有的去中心化应用都需要构建在相应的生态上，就好比网站需要运行在 Web 容器里面一样。过去统治了交互式 Web 时代的平台有：ASP/ASP.Net、PHP、JSP 等。这些开发语言使 Web 进入了一个高速发展的时代。而构建去中心化应用最好的方式就是在一个自身拥有去中心化特性的平台上进行应用开发，而 DMOC 公链就是针对应用开发做了大量优化和定制的去中心化基础平台。

1.2 传统公链的弊端

传统的共有链存在很多问题，下面我们来分析罗列一下，同时阐述一下我们是如何解决这些问题的。



1.3 开发者问题

1. 学习成本高

目前所有的公链应用开发学习的门槛都比较高，而很多传统的技术人员很难由原来的开发转到区块链应用开发上来。目前全世界最多的开发人员就是 Web 服务的技术员，这个群体人数是最

多的。这些技术员都需要重新学习一门新的编程语言， 比如： Solidity （ ETH）、基于 C/ C++ 的 WebAssembly（EOS）。我们做过测试如果一门技术需要技术员去重新学习新的语法的话，技术员多数会选择先观望看看。除非他现在手上的工作必须要用到这个技术，否则都会尽可能地用原有的技术知识体系去解决开发需求。DMOC 公链针对 Web 技术人员的技术低门槛上手特性，开发了一个划时代全新的编程语言：N++（N Plus Plus)，通过 N++程序员可以很容易就实现自己的交互式系统开发，特别是基于 Web 的应用系统。如果你本身就掌握 ASP/PHP/JSP 这类 Web 端的编程语言的话，我们可以非常地肯定您只需要 5 分钟就可以学会。

代码示例：

- 从表单中获取 userDMOCme 变量，并自动存入名变量 userDMOCme 中

  #request(“userDMOCme”);

- 从表单中获取 userDMOCme 变量，并自动存入变量 uDMOCme 中

  #request(“userDMOCme”,” uDMOCme”);

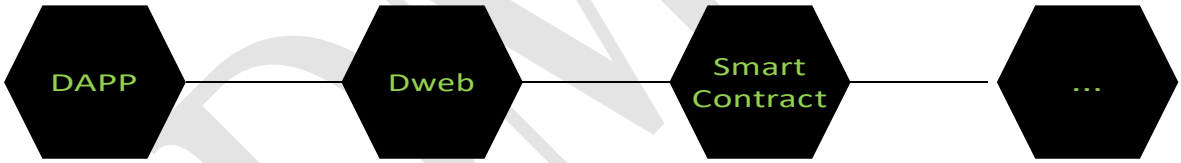
- 将变量输出到网页中

  <html><body>User:$uDMOCme</body></html>

- 保存数据到指定的 DAPP 区块链

  Blockchain.open(“dapp address”).insertDAG(“Hello world!“, “sign data”);

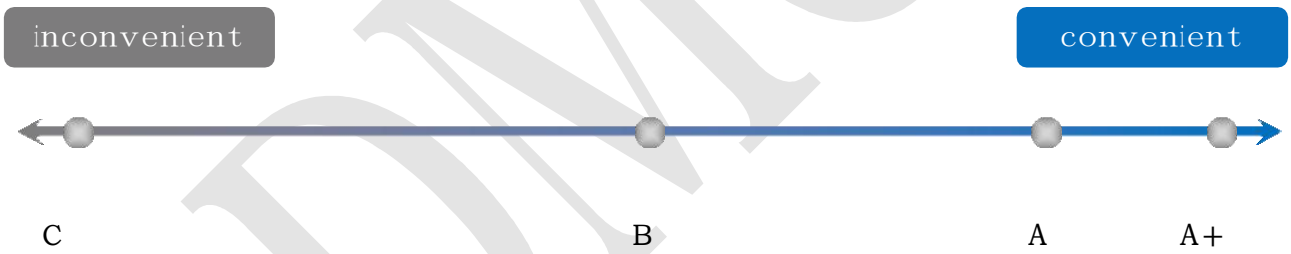
以上的代码语法是不是很熟悉？没错，所有的命令语法就是这么简单。再次强调如果你本身就是一名 Web 程序员，恭喜你，5 分钟内你就可以掌握如何使用 DMOC 开发一个属于你的去中心化应用/网站/合约……



2. 无良好的开发集成环境

作为一名高效的程序员，我们在用相应的编程语言做开发时，会有相应的开发工具：

编程语言	开发 IDE 工具	评价
C++	Microsoft Visual C++	A
C#	Microsoft Visual Studio	A
Java	IntelliJ IDEA/Eclipse	A
PHP	Zendstudio/phpStorm	A
Solidity (ETH)	Remix IDE(网页)/其他 IDE 插件模式集成，无法一键式发布应用	B
WebAssembly(EOS)	其他 IDE 集成，非官网，通过/C++/Rust 输出	C
N++	N++ IDE，一键式发布应用到公链，快速创建合约模板	A+



1.4 运行效率

公有链目前的性能问题主要集中在验证数据存盘的性能上。而这个问题所导至的性能低下原因主要是因为共识算法。所有的共识算法都有他的优点和缺点，而往往公链只硬性地提供了一种共识算法让你使用。以至于你在开发应用时会因共识特性而受限，如果这条公链他是基于

Pow做的共识，那么你所开发的dapp也只能是获得Pow共识的性能。如果公链使用的是Pos共识，那么你的应用性能只能是受限封顶于Pos的性能。为了解决这个问题，DMOC采用了异构复合链模式，将所有的应用独立发布在专用的实例链上，也就是每一个应用都有一条他专属的复合链。实例链由逻辑链和数据链组成，逻辑链主要负责共识的维护，数据链主要负责用于保存大量的数据。通过这样的构架，公链达到了分而治之的效果，同时获得了海量并发的高性能。由于N++提供了异步微服务的功能，因此一个大型的应用，我们还可以将它拆分为数十个小的实例链，从而实现百万级别的TPS。当前默认的实例链共识算法为：DPOS+DAG，未来我们还会继续升级更多的共识算法组合，让实例链具备热插拔式的无限扩展性。

1.4.1 成本

1、高额交易费

BTC的年度瓦斯费约为3000万美元，而ETH的年度瓦斯费约为2000万美元，而BTC每年需消耗20 亿美元的电力，ETH每年需消耗4.3亿美元的电力。不难看出瓦斯费只能负担一部分电费，根本无法覆盖投入产出成本。从各种主流公链的发展来看，区块链系统的交易成本一直在下降。但是分布式记账的硬件和软件成本高于集中式记账的成本，但必须远低于集中式记账的总成本。通过相对集中，链的交易成本已大大降低。为了支付高额的交易成本，区块链产业一直在寻找高利润的产业和更

大的商业合作。减少交易费，关键是降低机器的运营成本。DMOC通过混合共识模式，将数据的存储成本大大地降低。比如使用DAG存储的数据，我们可以将手续费下降到非常低。

2、运行维护成本高

以IPFS为例，目前IPFS的共识硬件投入成本是传统存储解决方案的好几倍。这种特性之下，存储的成本很难降低，除非互联网的数据大量重复，在大量的平台都接入IPFS之后，他的成本才有可能降低，然而这件事情传统的CDN缓存技术本身就已经在做。而且目前的所有互联网平台都做深耕细分的垂直领域，以至于他们平台上的数据都是唯一性的。全网根本不会出现重复的数据。就连视频网站他们的数据也都是打水印的，试想一下一个打了Youtube水印的视频，你希望出现在另外一个视频网站上吗？答案是肯定不希望，每一个平台都希望自己的视频的专有性，品牌的个性化。因此一份数据很难在多个平台中复用。而一些高复用的文件，最终可能会通过系统自带集成或者CDN缓存技术等给分化掉。利用现有可能的资源才是最省钱的，今天如果为了公链而公链去新采购一些最新的硬件服务器，那么你的成本永远都不会降下来。DMOC公链支持所有的传统Web服务器的接入，让所有的服务器都可以接入公链网络提供服务，从而降低运营成本。

1.4.2 安全问题

1. 某些数据会无限期暴露，缺乏隐私

数据隐私是个人权利，同时又是个人和组织以及涉及大量商业秘密和利益的某些行业的底线。建立一个健壮的信任的系统也是区块链吸引了众多拥护者的愿景和期望。从表面上看，区块链技术似乎是解决此问题的完美方法，因为区块链交易不需要绑定身份信息，世界上任何人都可以创建一个匿名钱包并进行交易。问题在于我们使用了一个通用的，易于追踪的分类帐。交易记录并公开存储在帐簿中，并且仅与由数字和字母组成的帐户地址相关联，因为没有绑定用户的真实信息， 因此产生误导性，无法为个人跟踪实体并确保隐私，而忽略了当前共有链的数据传输和存储是可公开观察的事实，例如智能化合同中的所有详细信息，包括发送方，接收方，交易数据，执行代码和存储条件。

实际上，这种保证隐私的“伪匿名”是阻碍隐私的最后也是唯一的保密层。一旦有人找到连接，所有隐私都将消失。这也打破了区块链交易完全匿名这一大前提。

2. 如果数据节点数太少，则容易受到粉尘的攻击。

公有链的第一个标准是节点数。国际技术标准是不能同时控制的一千个分散节点可以称为公有链。这是比特币和以太坊被业界接受的原因之一。权力下放的核心在于节点机制。一个真正分布的计

算节点必须有足够的节点参与，因为足够数量的节点代表了信誉，并且不能被篡改以实现足够的分散化来防止节点间的恶意攻击，例如粉尘攻击等。因此，节点的加入和退出应根据规则自由进入和退出，并且节点的阈值应足够低以允许更多数据节点参与。社区成员的积极参与也是区块链的核心精神。为了达到更多节点的加入，DMOC采用全节点可维护所有实例链的模式大大地增加了所有节点的数量。

3.更高的安全性

在传统的共有链设计中，计算层的计算和存储不是分开的。大多数共有链使用Gas机制来平衡主网络的计算能力。这种设计实际上存在两个问题。一是主网络的计算资源不分离。结果，计算能力的不均匀分布可能导致网络拥塞，甚至无法执行计算能力更小的DAPP。第二是合约行为和交易行为没有分开，从而造成了钱包被盗的可能性。

共有链的系统安全性需要一直得到改善，包括来自外部实体的攻击（拒绝服务攻击，DDoS等），来自内部参与者的攻击（模拟攻击，Sybil攻击，共谋攻击，Collusion攻击等）和组件。故障和计算能力攻击，双花攻击，交易和合同漏洞防御机制，身份和匿名性，数据库安全性等，甚至与量子计算作斗争，以解决各种隐私泄漏，欺诈和转移。数字经济时代的公链将面临更多的用户，它必须在安全审计，安全架构，编译器安全优化，虚拟机安全设计，合同安全模板等方面满足更高的标准，才能满

足用户的安全需求。

1.4.3 监管问题

1、任何人都可以匿名参加，缺乏相应的监督策略

区块链集中化的特征使许多共有链或项目不可避免地处于集中化的对立面，这实际上是当今社会主体的运作模式。每个人都可以匿名参与的模式在某种程度上也激发了不安全感的产生。区块链技术的最终用途必须是解决社会问题并提高生产效率。为了实现商业应用的普及和社会价值的提升，共有链的架构设计必须考虑如何解决与传统的中央监管机构的冲突和摩擦，以及如何与现实世界中的中央社会融合. 到目前为止，在传统的共有链研发领域，乃至整个区块链行业，还没有安全的升级方式，也缺乏制定办法并维持监管规定的法律规定和参考标准，仍然需要更多开发商，专业法律从业人员和其他相关人员的支持和参与。具体的实施情况尚不清楚，因为在标准中心没有环境授权是困难的，但是该法规已经开始积极地触及所有领域，并且将越来越严格，在这种情况下，将更加确保对于行业中的新问题和挑战。

2、奖励制度是混乱且可操纵的

3、激励机制被称为区块链的核心驱动力。

其目的是整合系统中所有利益相关者的价值，以作为鼓励参与节点参与区块验证工作的奖励。像比特币这样的健全的奖励机制应能迅速，连续地满足激励反馈，并且不会因任何原因而终止，并始终保持积极的激励，以便所有节点都能自发地维持整个系统的健康有序运行。公链网络系统的激励机制为许多开发商提供了新思路，并产生了许多不同的激励机制。为了使更多的节点参与进来，许多机制违反了激励的初衷，将奖励权掌握在自己手中，而不是将整个链的维护放在首位，这使市场充满了混乱。

1.4.4 可伸缩性问题

数字资产的体系结构在很多方面都不适合DAPP，主要有两个方面：

1.不够容易使用

区块链技术整合了计算机，网络，加密和其他领域的许多技术。这些技术对普通用户而言非常专业，例如私钥，公钥，地址，加密算法，共识机制，共有链和其他术语，足以使普通用户撤退。即使用户愿意学习，他也必须经过许多繁琐的步骤才能实际使用相关应用程序。例如，如果用户要使用基于智能合约的DAPP，则他首先必须做几件事：首先，他应该获得钱包地址和私钥，并且知道如何使

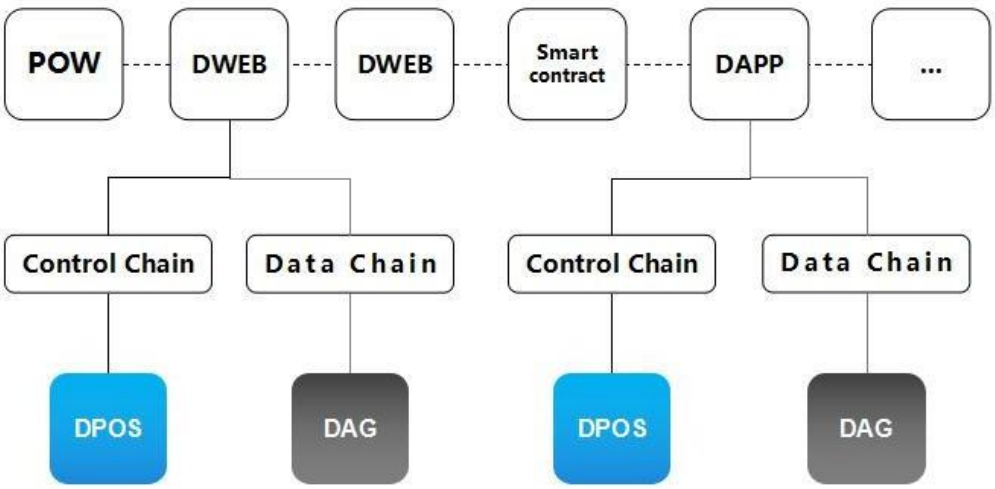
用钱包地址并正确保存私钥。其次，他必须以某种方式获取ETH，然后才能将ETH 转移到DAPP的钱包地址。对于区块链而言，此过程非常复杂，并且通常需要足够长的等待时间（超过一周），用户才能真正使用DAPP。基于区块链的DAPP的使用应与传统APP相同。而传统的应用只需要从App Store下载后，用户就可以免费或以非常低的价格使用该APP。可见由于不能做到数据的分而治之，传统的公链是不可能快速完成同步的，因此对于每个新用户而言钱包的 首次数据同步就已成为障碍。

2. 单一应用场景

数字资产上的所有Dapp应用程序只能共享一个主链。Dapps无法构建自己的子链，无法自定义自己的共识算法，也无法根据业务需求选择最佳配置。这导致当前正在发行数字资产。几乎没有 可以支持的业务应用程序场景，这不利于DAPP生态的构建。

DMOC可以针对不同的应用实例构建不同的共识算法。并且DAPP的数据会进行分而治之。

Running logic of DMOC



1.5 传统智能合约问题

除了传统链的固有缺点之外，传统智能合约还存在许多问题。智能合约是一种计算机协议，旨在以数字方式促进，验证或加强合同的谈判或履行，并允许无需第三方即可执行受信任的交易。

传统的智能合约存在以下问题：

合同问题：基于执行规则，数字货币交易的场景太简单，导致执行规则极其简单，这在我们的现实生活中仍然与合同相去甚远。在实际的商业和生活中，我们需要更多更好的合同规则和系统，尤其

是对于金融部门而言，复杂的一面代表安全性和灵活性。

输入可信度问题：不存在完全的图灵合同，并且参数输入是手动的。手动输入会带来输入错误 的风险。支持可靠的数据导入非常重要。即在发布应用时，同时进行默认数据的发布和数据的初 始化也很重要。通过首次应用发布数据初始化，可以减少大量数据录入交易产生的手续费，又可以实现精减的数据导入。

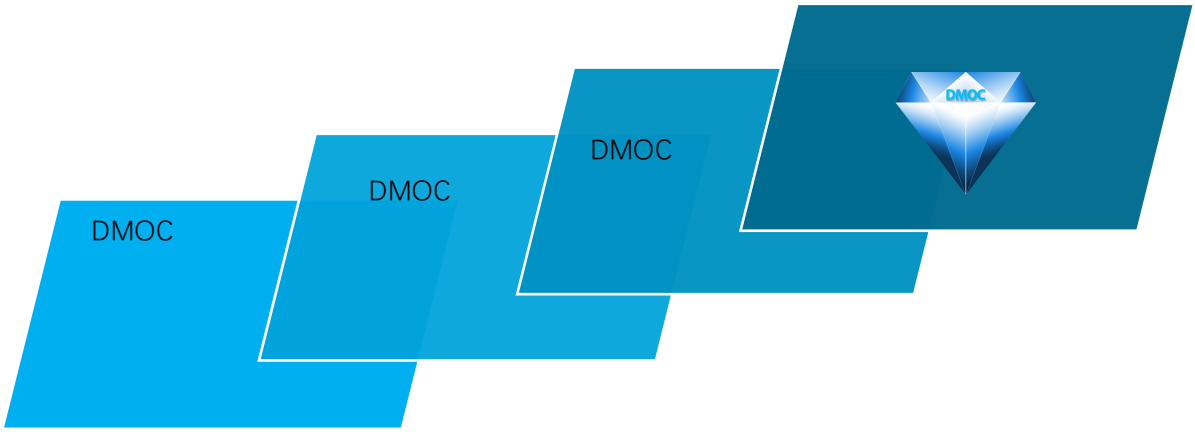
执行问题：由于不支持定时任务。因此所有的智能合约的触发都需要靠人为执行请求才可以执行。但是往往在做应用开发时，我们希望每隔多少个区块高度，就执行一次相应的任务。比如每天执行一次报表数据生成、K线分时线数据等业务，这些需求在当前的智能合约里面是无法实现的。但是DMOC引入了定时任务，用户可以给智能合约支付预存费用，让合约定时去执行相应的任务。

1.6 DMOC 愿景

DMOC公有链希望能通过自己的先进技术理念，改善公链生态。实现学习门槛低，易用的去中心化应用。完美地将传统技术生态的应用可链改落地。

二、技术方案 Technical Solution

2.1 基础设施



DMOC被设计为面向应用的主链，支持多样共识机制，分布式存储，动态定价，反量子计算，跨链运营和其他创新技术，如下所示：

节点层	共识层	实例层	应用层
DMOC 节点分为全节点和普通结点，成为全节点后会维护全网所有的数据。普通节点可以选择维护全网数据，也可以选择只维护指定的应用实例。	共识层是区块链协议的核心部分，定义共识算法和块数据范式。DMOC 采用了创新的异构复合链共识机制，用户可以选择最适合自己应用所需求的共识机制。	所有的应用都会实例化成复合链，由复合链为应用 提供业务支持。	基于 NVM 的虚拟机，应用由此虚拟机来执行逻辑计算。

2.2设计目标

DMOC被设计为面向应用的主链，支持多样共识机制，分布式存储，动态定价，反量子计算，跨链运营和其他创新技术，如下所示：

2.2.1 POW+DPOS+DAG 共识机制

应用主链	基于 POW 共识机制
应用实例	实例逻辑链(DPOS/自定义)+实例数据链(DAG)

应用主链（POW）：

所有的应用发布时，都需要将应用在主链中注册或卸载。每1000区块，调整一次计算难度。

2.2.2 应用全节点（21 * N）（DPOS+DAG）：

要获得记帐权，需要使用FNC进行投票，相关DMOC将进入一个为期3天的锁定期，锁定期结束后票可取消重新投。存入则为投票、提取则为取消，所以每个候选节点每轮的选票都会改变。每6秒会生成一个区块，每个节点可以获得10个区块出块权，合计：21结点*N*10区块=210个区块周期，相当于是1260秒完成一轮。投票后所对应的节点将会获得出块权，如果在出块的过程中，由于某个节点无法进行正常工作，此时只要有超过70%的节点投票检定某个节点当前不可正常工作， 则接下来他未出的区块全部由上一个节点来完成。投票时相应的节点设备需要在线，因为负责检票的设备将会尝试对此IP地址进行连接。如果无法连接，则会跳过此节点。投票系统会提前选举下一批名单，比如当前是正在第1区块高度，则会去选举从211区块高度后的选票，第211区块高度则会选出421区块高度的选票，以此类推。

2.2.3 收益分配方案：

1、持有DMOC的投票设备平均分配获得收益的80%，候选获得10%。

2、余下10%按投票数量进行加权平分，投票数量。每枚DMOC为1票，每设备封顶1000票。投票设备需要在线。

2.2.4 获得收益条件：

1、在Full Node Credentials应用中持有全节点凭证；获得凭证之后，可以下载随机试题进行性能测试。每一轮测试的分数都会自动上链。用于彰显此设备的计算性能。

2、拥有独立外网IP地址；

3、验票员会尝试连接投票人的地址检查网络检查，这样的话就可以迫使所有的矿工都必须要有设备，同时还要在线。如果发现不在线，则会自动跳过此节点。

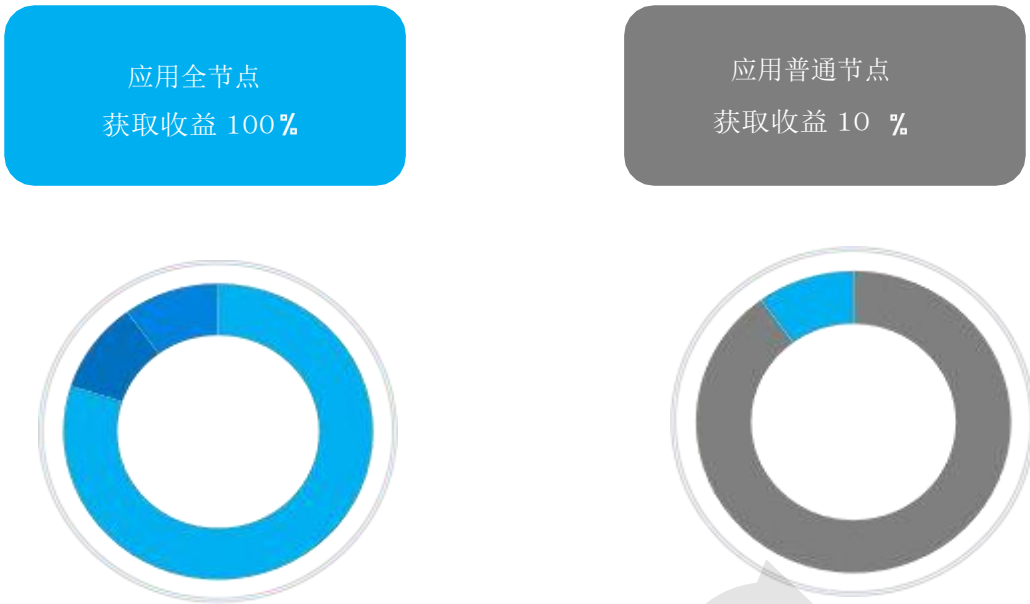
2.2.5应用普通节点（DPOS+DAG）

普通节点可以指定只维护某个或多个应用，赚取指定应用出块的奖励。要想维护指定的应用，同样需要在应用的投票系统中，进行投票选举，需要使用应用指定的Token来进行投票。默认全节点中的21个节点为所有应用的默认工作结点。如有新的投票节点的出现，则替代全节点。普通节点也可参于应用主链共识，但是出块只可以获得10%，另外的90%将会自动进入销毁池，直到销毁停止为

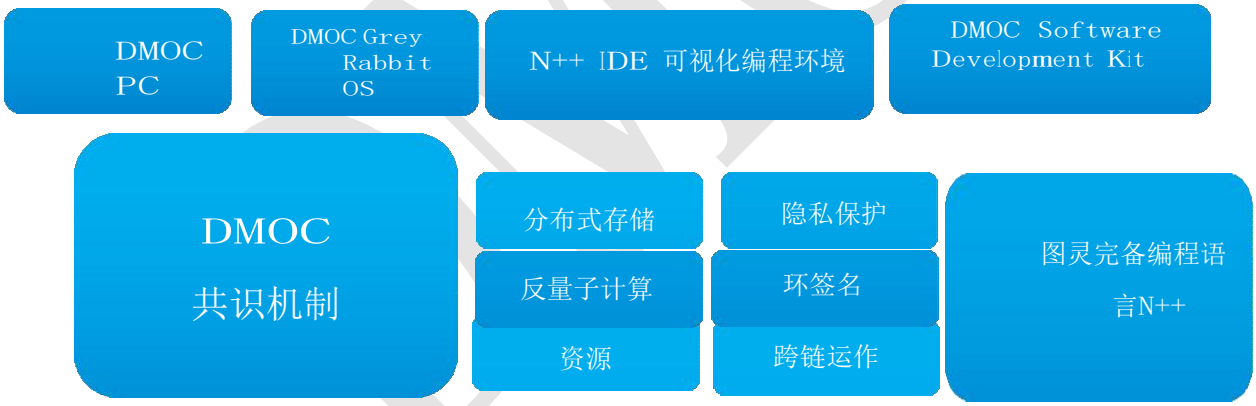
止。

2.2.6 获得收益条件：

1、普通节点可以投票DMOC全节点。获得10%加权分润收益，投票每设备封顶1000枚。



2、节点投票后需保持在线。否则将会被排除。并且数据应用也需要可用，因为检查员会随机请求节点进行访问请求，以确保发布的应用服务可用。



2.2.7 资源

2.2.7.1 运算Gas费（Execute Gas）

执行运算量，由NVM计算出运算量，并收取相应的Gas费。

2.2.7.2 存储Gas费（Store Gas）

全节点可在凭证中设定最低价格，凭证应用中每隔14400区块更新一次均价，应用打包时不可以低于此价。全节点矿工设定应用发布时每100K的价格=1DMOC,不够1M按1M计算，则应用低于此值不会被收录打包。

均价算法=所有全节点的投票价进行排序，取中间51%的数据进行平均值计算。即橄榄型的顶部和底部数据剔除后，进行均值计算。即顶部去除24.5%，底部去除24.5%的数据。

2.2.8 分布式存储

DMOC-Distributed File System是一组利用分布式哈希表技术的分布式存储协议。DFS通过文件内容（哈希）而不是文件路径（URI）为数据建立索引。大文件分为固定大小的数据块，这些数据分布在多个节点上。这种系统的主要问题是要在冗余和可靠性之间找到平衡。DFS计划通过令牌激励机制和建立骨干节点来解决这一矛盾。用户可以选择文件的可靠性要求，可靠性低的文件可以免费或几乎免费存储和访问，骨干节点(全节点)将为稳定可靠的文件提供高可靠性的文件。DFS 将通过合约为这些文件设置访问权限。此外，DFS可以与数字身份结合使用，从而可以发布，传输和撤销点对点记录数字身份的数字证书，而无需由集中式服务器进行管理。将来，可以将旧块数据存储在DFS中，以便大多数完整节点可以释放旧数据，获得更高的可伸缩性，并确保历史数据的完整性。存储价格由设备主自行进行设置，费用会按阶梯方式慢慢支付给设备主。

2.2.9 反量子计算

在以比特币为代表的当前区块链系统中，SHA-256哈希计算和ECDSA椭圆曲线密码构成了比特币系统的最基本的安全保证。但是随着量子计算机技术的不断突破，尤其是量子算法以Shaw算法为代表的相关运算理论上可以实现从指数级到多项式级的转换。经典计算机的这些“难题”问题必将在可预见的将来由实用的量子计算机解决。现有的大多数区块链系统都采用ECDSA，但是SHOR攻击算法对于量子计算机下的ECDSA签名算法非常有效，SHOR算法适合于解决大整数分解，离散对数反演等困难的数学问题，导致ECDSA签名算法非常不安全。在量子攻击下考虑到数字货币交易的高度安全性，DMOC采用了基于格理论的签名算法NTRUSign-251。

2.2.10 跨链运作

DMOC采用区块链异构跨链解决方案，将相应的目标公链数据结构在DMOC中重新实现实例链，并同步维护此链的数据。而数据源则由安全可靠的21个节点提供。比如我们如果需要与比特币进行互连， 那么就异构出一条比特币实例链来。所有数据同步比特币原有公链的数据。所有传输协议均采用原链的设计，以实现独立区块链之间的互连，并确保跨链交易的有效性和

用户隐私数据的安全性。通过这样的设计，可以确保原有目标链的功能均可在原有的公链中实现，不会有太多额外的技术障碍。

2.2.11 隐私保护（Zk-SDMOCRK 零知识证明算法）

DMOC提出了一种基于ZKSDMOCRK算法的跨链交易隐私保护方法。

ZK-SDMOCRK零知识证明算法是比较成熟和可行的隐私保护技术之一，具有更好的匿名性。它不需要信任中央节点或网络中其他用户的参与。用户可以通过与匿名货币进行交互来实现匿名交易，从而有效地保护了用户的隐私。跨链连接链作为转发和验证跨链匿名交易的载体，需要能够验证跨链匿名交易的有效性，跨链交易分为两类：跨链透明交易和跨链交易匿名交易。跨链透明交易提供交易本身的内容以及相关的Merkle分支证据。互联链网络中的验证节点可以根据并行区块链注册的验证规则来验证交易的有效性，匿名的跨链交易除了交易的有效性外不会透露任何信息。互联网网络中的验证节点需要了解在每个并行区块链网络启动阶段生成的公共参数，并使用这些公共参数来验证跨链匿名交易的有效性。区块链和零知识证明算法可确保互连网络中的验证节点除了跨链交易的有效性之外，不知道任何其他信息。

2.2.12 环签名

DMOC通过环签名技术实现了数字资产的匿名性。环签名技术描述如下：

下面显示了一个公共签名，只有一个参与者，可以进行一对一映射。环形签名模糊了身份，因为它只是属于某个组的某人，却不知道该组中的谁。这允许在虚拟货币交易中实现高度匿名，这可以被视为去中心化和不信任的组合。为了保持匿名，DMOC使用了一次性的环签名技术。环签名通过允许事务的发起者加入组，然后将事务作为一个单元加入，而不是从单个私钥签名中分配私密性。此技术允许发起者进行混合。验证者可以证明输出存在，并且组的成员之一是真正的签名者。但是，由于每个成员具有相等的概率权重，因此他们无法确定签名者是哪个组成员。随着组规模的增加，每个成

员成为真实签名者的可能性降低。环形签名，涉及合并用户的真实隐藏地址P，以及大量“虚拟”P散布在整个区块链上。签名由所有P验证，并且数学上任何相应的私钥都可以对交易进行签名，从而混淆了真实发送者的身份。为了防止重复支出（重复支出意味着同一笔钱同时出现在两个或多个交易中），每个DMOC交易都具有唯一的关键图像。通过获取隐藏地址P的哈希值并将其乘以私钥来创建密钥镜像，这对于每个事务而言都是不同的。这种机制确保每个P都能只能使用一次。DMOC网络维护着所有不完整密钥映像的数据库，因此，如果用户尝试重用密钥，则网络将拒绝交易。

2.2.13 虚拟机和智能合约

1. DMOC 虚拟机

DMOC Virtual Machine是为DMOC生态系统开发的轻量级图灵完备虚拟机。它是一种高性能的区块链网络分配器，旨在提供高效，便捷，稳定，安全和可扩展的自定义区块链系统。本白皮书中解释的虚拟机概念很狭窄。它不是通过操作系统对物理机的模拟。NVM支持微服务架构，同时具备动态解析功能，可实现Web动态渲染开发（类似ASP/PHP/JSP）。完整的操作过程如下:

将智能合约源代码编译为字节码。

将字节码和相关参数作为运行上下文推入执行堆。

每当执行引擎从当前上下文中检索指令时，它就会执行该指令并将数据存储在当前上下文的计算堆栈和临时堆栈中。

如果需要访问外部数据，它将使用可互操作的服务。

执行完所有脚本后，结果将保存在结果堆栈中。

2.DMOC 超级智能合约

DMOC所发布的程序，均为去中心化程序。文件名后缀为”.DMOC”，例如：用户登录userLogin.DMOC， 这个为源文件，编译后的文件为：useLogin.DMOC，如果需要发布动态网页，还可以编写为userInfo.nsp。

文件类型	后缀类型	类似于
N++程序源文件	.DMOC	.java、.cs
N++程序	.DMOC	.class、.ex

二进制文件		e
N++动态网页	.nsp	aspx、php、jsp

3.普通智能合约

合约模板：

1、DRC 代币合约

2、资产托管多签合约，转出币需多人同意

3、高级资产托管多签合约，转出币时如果全员同意立即成功；超过 67%投票率同意，3 天无人投反对成功；超过33%投票率同意，90 天无人投反对票则成功提币；超过10%投票率同意，180 天无人投反对票则成功提币。

4、信托合约：适合做信托理财，比如给儿子的生活费，每月自动释放 3000U。需儿子每月手工过来领取。

4.超级智能合约

1、可开发复杂运算系统，例如：OA、ERP、电商、数据分析、大数据、行业系统等等

2、可调度节点进行复杂运算，提高计算速度。每调用一个节点需要消耗Gas。

3、并行计算，通过调用GPU芯片，实现AI、图像识别、大规模复杂运算等。

4、专用组件：视频推拉流、图片存储。

2.2.14 图灵完备编程语言 N++

1. 语法介绍

命令	语法
注释	单行注释 ## This is a single line comment. 多行注释#* This is a one line comment. This is a two

	line comment. This is a three line comment. *#
变量	变量的设置： #var($age= "28") 变量的名称可以由以下字符构成： 字母 alphabetic (a .. z, A .. Z) 数字numeric (0 .. 9) 下划线underscore ("_") 变量的引用： 变量的引用需要使用前导符$，美元符号 $user $sex $age

获取数据	请求实例： https://domain.com/login?UserDMOCme=david&age=25 获取参数: 将获取到的值，存入名为uDMOCme的变量中 #request(“userDMOCme”,“uDMOCme”)获得的值,自动存入名为age的变量中 #request(“age”)
方法	$user.getAge() $page.getTotal() $page.setTitle("My Home Page")
命令	语法

条件指令	所有的指令前导符为#号，在指令前需要加上#号做为声明。 条件语句示例1： #if($user.getSex()==1)boy#{else}girl#e nd 示 例 2： #if($show) DMOC Server Page! #end 示例3： #if($age< 10) **School** #elseif($age== 18) **Liquor** #elseif($age== 28) **Married** #else **Nothing** #end
循环指令	 #foreach($product in $allProducts) $product #end

动态引用	引用本应用中其他的代码并合并执行 #import("tokenUtil.DMOC") 本合约引用另外一个合约中的代码: #import(“dapp address”, "tokenUtil.DMOC")
静态引用	载入指定文件的数据，并进行赋值 #include("kline-20190101.txt", $klineData)

命令	语法
保存到区块链	打开指定的dapp应用： #Blockchain.open(“dapp address”, $dapp1) 保存数据: # 使用我的私钥对数据进行签名，并且保存到数据链中。 # insertData和insertDAG是同样的效果 $dapp1.insertDAG(“Hello world!“,” sign data”); # insertLogic和insert DPOS是同样的效果 $dapp1.insertLogic(“Hello world!“,” sign data”); 也可以使用单行命令 #Blockchain.open(“dapp address”).insertDAG(“Hello world!“, “sign data”);

调用合约方法	打开指定的dapp应用： #Blockchain.open(“dapp address”, $dapp1) $dapp1.call("evenDMOCme", $callbackData)

以上的语法是不是看起来很熟悉，这就是你可以在5分钟内掌握N＋＋的原因。

2. 创建应用

1) 智能合约

在IDE中可以很方便地选择对应的合约模板来进行合约的创建，您也可以自己创建属于自己的模板。所有的合约模板可以自己使用，也可以发布给别人，成为合约标准，让更多的人使用。合约编写成功之后，可以将合约提交到测试链中进行测试。测试无误后可以提交到主链中。

2) 创建 DAPP

创建DAPP和创建合约一样，在IDE中创建自己的应用系统，然后编写相应的业务逻辑代码。然后同时也可以制作基于Web的UI界面进行数据交互，当然UI部份也可以使用桌面软件或者手机软件来进行显示。（取决于用户的需求）

3) 创建 DWeb

创建DWeb我们不光将代码逻辑部份打包上链，还会将界面部份也一同打开上链。这样的话，就可以轻松实现界面上链的好处。从而实现完全去中心化的应用。网站发布成功之后。您还需要将网站注册到DMOC DNS系统中，从而获得一个专用的访问域名。

4) 创建桌面软件

DMOC软件开发包含了Desktop的SDK套件，通过使用这个套件可以很容易就开发出具有可执行文件的桌面软件应用系统。具体说明将会后续在官网中公布。

3. 应用发布/卸载

1) 发布应用到公链

可以使用DMOC官方提供的工具进行应用的安装。当然也可以使用更加友好的线上应用进行安装发布。通过控制台命令将编写好的工程目录应用进行打包，打包命令如下：

打包

DMOC.exe -packaging

DMOC.exe -install -appDMOCme<软件名称> -version<版本号> - type<类型> -owner<作者钱包地址> -ownerSign<作者签

发布

参数

type:
standard 标准类型（默认）
immortality 永生应用（不可卸载）

发布应用到 DMOC AppStore

应用发布成功之后，用户可以在应用市场中提交自己的软件，为软件上传截图，icon图标，说明等信息。

2) 在应用链中卸载

卸载

DMOC.exe -uninstall -appaddress<软件地址> -owner<作者钱包地址> -ownerSign<作者签名>

可以使用DMOC官方提供的工具进行应用的卸载。当然也可以使用更加友好的线上应用进行卸载。

4.N++ IDE 可视化编程环境

通过开发工具，我们可以对写好的.DMOC程序文件进行编译，同时还可以在本地模拟浏览运行。

从而实现本地单机环境也可以进行软件的开发，测试，浏览。

1)将编译.DMOC 文件编译为.DMOC

通过GUI编程开发环境进行软件的开发，编译。

2)打包 dapp/dweb 包

通过GUI编程开发环境进行软件或网站的打包，发布等工作。从而降低用户的学习门槛。

2.2.15 DMOC SDK（DMOC Software Development Kit ）

DMOC SDK中包含了桌面开发套件，我们可以开发出基于Windows、Mac、Linux等桌面系统的应用软件。所有的数据会处于离线工作状态，当接入网络后。所有的数据会自动提交到线上。这个伟大的功能可以让用户很轻松地就开发出离线POS机，即使用户当时手机没有网络，POS机也没有网络，只要通过手机里的NFC数据签名，将来双方只要有一方上网后，数据将会广播到区块链网络中，从而进行数据确认离线支付的场境。同时也可以使用户在无网络的环境下进行工作或文档的录入，当进入到有网络环境时就可以自动将数据发布到线上。

2.2.16 DMOC Grey Rabbit OS (DMOC Grey Rabbit Operating System，简称 DGR，代号：灰兔)

1. 基于 Linux 内核开发的区块链操作系统

Grey Rabbit OS内核基于Debian，Debian是一个完全自由的操作系统。Debian GNU/Linux是一个操作系统及自由软件的发行版,它是由一群自愿付出时间和精力的用户来维护并更新的。我们在Debian的基础上重新定制开发了Grey Rabbit OS，将DMOC高度集成到了操作系统中。并完美的调用操作系统的资源为整个共有链生态提供应用支撑。

·稳定性

这里有许多运行多年的机器没有重启的案例。即便有的机器重启，也是由于电源故障或硬件升级。和其它那些一天要崩溃多次的系统比较一下。

·更快更容易的内存管理

其它操作系统也许在一两个领域内速度够快，但是基于 GNU/Linux 或 GNU/FreeBSD 的 Debian 对硬件要求很低且很平稳。在 GNU/Linux 下通过模拟器运行的 Windows 软件比在其原生环境中运行的速度更快。

• 更稳定的硬件驱动

大多数的硬件驱动程序是 GNU/Linux 或 GNU/FreeBSD 用户们所写的，而非厂商。

这可能意味着，对某些硬件的支持从无到有的过程之间会存在一些延迟。不过，在厂商停止生产或倒闭以后却仍可以对硬件提供长时间的支持。经验显示，开放源码的驱动程序通常比封闭式的好太多了。

• 良好的系统安全

Debian 以及自由软件社区非常注意在软件发布中快速地修复安全问题。通常没几天就会有修复过的软件被上传。因为开放源代码 ，所以 Debian 的安全性会在开放的情况下被评估。而且其它

自由软件项目也有相同级别的考核系统，用于防止潜在的安全问题被引入到基本系统的重要位置。

• 安全软件

许多人并不知道，任何机器都可以看到您在网络上发送 的任何信息。Debian 有著名的 GPG（和PGP）软件，允许邮件在用户之间秘密地被发送。另外，ssh 允许您和其它安装了 ssh 的机器创建安全的连接。

2.3 内置应用

- DMOC 浏览器
- DMOC 分布式磁盘管理
- DMOC 应用市场
- DMOC 钱包
- DMOC DNS
- DMOC N++ IDE

2.3.1 内置命令介绍

<最终命令以上线后为准>

2.3.1.1 DMOC PC （Hardware)

1. 基于 DOS 的个人电脑

<基于原创团队要求，此部份暂时保密，由项目推进程度来决定公布>

2. 功能介绍

<基于原创团队要求，此部份暂时保密，由项目推进程度来决定公布>

3. 内置应用

2.3.2 DMOC 核心代币

2.3.2.1 DGR凭证代币

a）DGR凭证代币

总量：35000，流通：15000，待解锁：20000。待解锁部份由自治社区投票决定是否开放。

b）全节点凭证

在DMOC公链中，矿机设备有两种工作模式：

全节点工作模式：维护全网所有的数据及共识。全节点模式开启的方式为，进行挖矿的矿工区块链地址持有全节点凭证即可。在FNC DApp（Full Node Credentials） 中可以进行全节点凭证的兑换。全节点可获得全额的区块打包收益。

注意：请使用矿工的地址来进行兑换。

普通工作模式：没有进入全节点工作模式的矿机默认会以普通工作模式进行共识维护。区块打包奖励仅为正常收益的10%。

2.3.2.2 DMOC公链代币

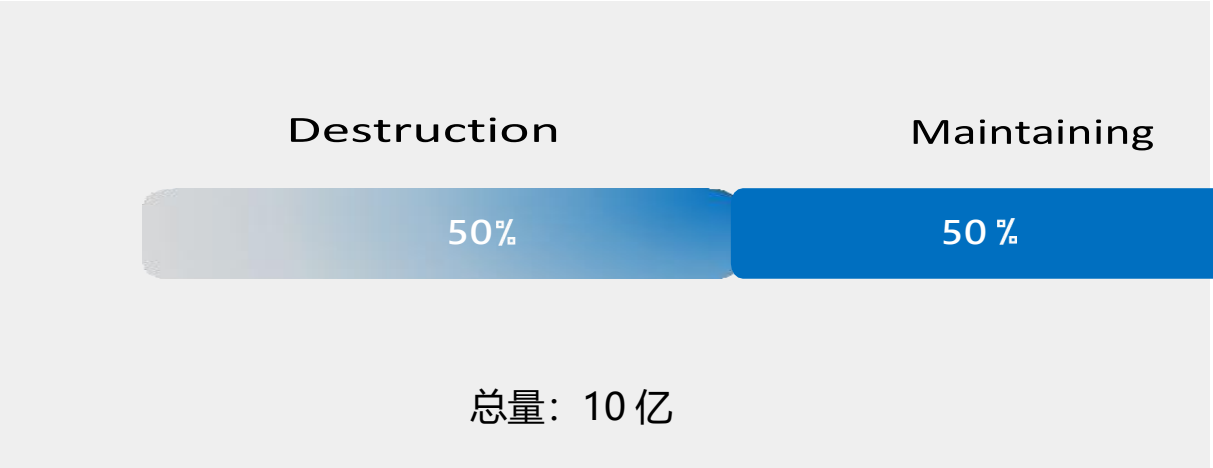
a）DMOC公链代币

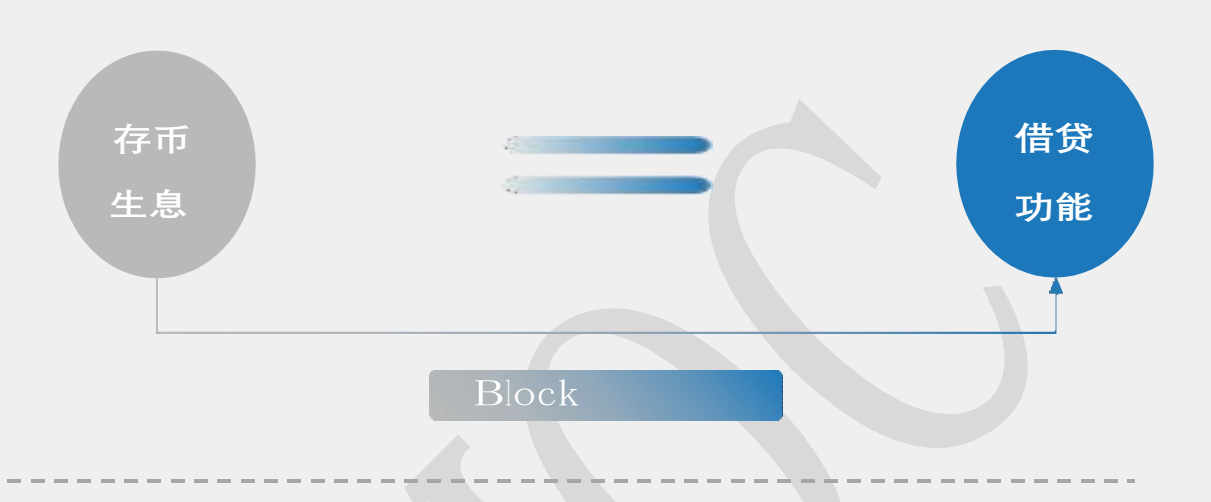
代币总量：10亿，销毁：公链手续费用中，50%销毁，50%用于维护费用

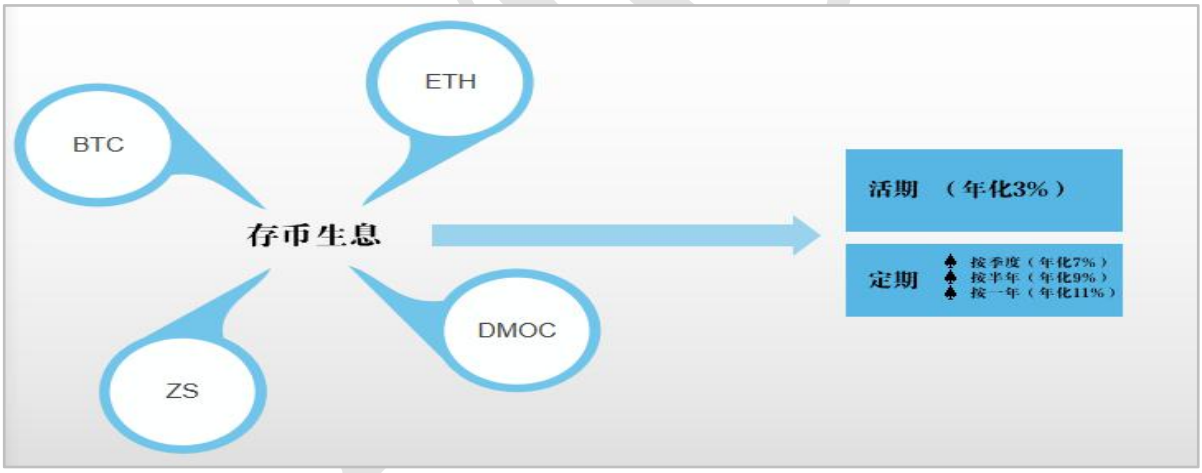
b）应用相关-DEFI板块

①.存币生息功能。具体是存BTC、ETH、ZS、DMOC这4种币，生息表现是增加相应存币的总量，按活期和定期两个方式进行结算，其中不满一季度，或者定期未到按活期（年化3%）按季度（年化7%）、半年（年化9%）按年11%。

②借贷功能，DMOC ZS，当天币价五折抵押借贷，借给usdt抵押者.


Destruction
Maintaining
50%
50 %
总量：10 亿


存币
生息
借贷
功能
Block


BTC
ETH
存币生息
DMOC
ZS
活期 （年化3%）
定期
按季度（年化7%）
按半年（年化9%）
按一年（年化11%）

c）应用主链（POW ）

2.4 应用主链定义

所有的应用都是一个实例，而每一个实例都会包含两条链。一条为逻辑链，一条为数据链。而实例的身份信息会写入到应用主链中。应用主链主要的工作就是存储应用实例的基本信息，用来标记应用的可用性。用户可以向应用链发布Install和Unstall指令，从而向公链系统申请实例化链资源。

2.4.1 应用发布费，应用卸载费发布应用

应用发布后，由POW打包的矿工进行应用实例链的创建，完成后广播所有的全节点进行同步。

a) 全节点接收到指令后进行数据和链的构建，并进行投票维护链上数据。

c) 应用创建成功之后，可在DNS中申请专属的域名。当此应用进入就绪状态之后，通知DNS系统， 以便DNS系统可以将流量引入到此节点上进行服务。

d) 应用被请求时，会检查缓存中是否有应用，如果没有的话从链上下载压缩包，并解压到磁盘中。并由NVM加载到内存中，进行业务的执行和渲染。

应用计价

计价策略	均价算法=所有全节点的投票价进行排序，取中间 51%的数据进行平均值计算。即橄榄型的顶部和底部数据剔除后，进行均值计算。即顶部去除 24.5%，底部去除 24.5%的数据。
发布应用计价	全节点可在凭证中设定最低价格，凭证应用中每隔 14400 区块更新一次均价，应用打包时不可以低于此价。全节点矿工设定应用发布时每 100K 的价格=1 Armc,不够 1M 按 1M 计算，则应用低于此值不会被收录打包。
交易手续费计价	全节点可在凭证中设定最低手续费价格，凭证应用中每隔 14400 区块更新一次均价，交易时不可以低于此价。
合约调用计价	读取数据免费,写入数据收费。执行运算量,由 NVM 计算出运算量,并 收取相应的 Gas 费。

2.4.2 卸载应用

卸载需要由作者的私钥来进行指令发送，卸载后可获得此应类累计交易手续费的5%奖励

应用手续费

矿工收益	50%的手续费为矿工的收入
销毁通缩	50%的手续费进入销毁通缩

2.4.3 铸币

出块时间：60s/Block，1小时60区块，1天1440区块，1年51.84万区块铸币生成DMOC，1枚/区块

每隔4年产量减半,连续减产第5次之后，保持每区块产出0.0625枚/区块

合计107年全挖完，Pow区块高度：55177296，第10年时累计产出49%的流通率。全节点收益：1枚/区块，普通节点收益：0.1枚/区块

区块高度	产币量
1至2073600	1
2073601至4147200	0.5
4147201至6220800	0.25
6220801至8294400	0.125
8294401至10368000	0.0625
10368001至55177296	0.0625

减产规则

e) 应用实例逻辑链（DPOS） 逻辑链定义

所有的应用实例在进行业务交互时，所需要的业务逻辑处理均由此链来完成工作。在发布应用时， 应用的代码文件会以ZIP压缩格式进行打包压缩。并保存在逻辑链的创世区块中，创世块的最大容量大小为64M，因此压缩后的程序包不可以超过64M。一但应用发布，不可修改。因此在发

区块类型	容量上限
创世块	64M
数据块	8M

矿工收益	50%的手续费为矿工的收入
销毁通缩	50%的手续费进入销毁通缩

f) 实例数据链（DAG ） 数据链定义

DPOS竞选出DWorker工作节点，所有的DPOS入选人均可接收外部提交过来的交易数据，但是只有DWorker工作节点进行数据的签名确认。其他DPOS节点只作为数据收集，工作集群中进行广播。通过DWorker模式隐藏真实的工作节点。每14400区块竞争一次新的DWorker节点，则1 天竞选一次。所有交易均为实时完成交易。因此理论上可以实现单机百万级别的并发。当然这个速度还要取决于网络环境和矿工的硬件性能。

矿工收益

被选中的工作节点，可以获得所有DAG交易数据的手续费。

2.5 DMOC DNS

功能定义：

I. 用户可将域名解析到指定的IP地址进行域名绑定。

II. 域名绑定时需要支付相应的出租绑定费 100DMOC，360天后可解绑回收，未到期解除绑定质押费用不退回。

2.5.1 域名需要开通泛解析功能才可以进行域名出租绑定

2.5.2 域名出租可以获得收益，租用者需要支付租凭费用

2.5.3 DMOC DFS分布式文件系统

I. Distributed File System 全球分布式文件系统说明

II. DFS应用

每份压缩文件需全网存储至少7份,每份副本存储在固定区块周期内观察节点会进行一次复查。

如果查到并没有存储或者无法打开， 则会进行投票处罚。

2.5.4 DMOC AppStore

I. 应用市场展示

II. 应用市场发布

III. 应用市场购买

IV. 热门应用排行榜

2.5.5 DMOC Full Node Credentials全节点凭证

所有的节点需获得全节点凭证才可以进入全节点工作模式，凭证兑换需要销毁DGR和DMOC，具体数据如下：

凭证数量	凭证数量	销毁 DGR	销毁 DMOC	销毁比重	销毁 DGR	销毁 DMOC
1-100	900	3	2851.2	.1	300	285120
101-1000	900	3	570.24	0.1	2700	513216
1001-2000	1000	2	285.12	0.1	2000	285120
2001-3000	1000	2	142.56	0.1	2000	142560
3001-5000	2000	1	142.56	0.15	2000	285120
5001-10000	5000	1	85.536	0.15	5000	427680
10001-20000	10000	0.5	42.768	0.15	5000	427680
20001-30000	10000	0.5	21.384	0.15	5000	213840
30001-50000	20000	0.1	19.008	0.2	2000	380160
50001-100000	50000	0.1	11.4048	0.2	5000	570240

2.4 海量存储与高并发支持

DMOC支持本地数据库存储、文件系统存储以及云存储多种方式。本地存储实现冷 热分离，数据库存储使用分库分表的模式，云存储支持按照云的集群规则扩展。

2.5 可靠一致的记录存储

DMOC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：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DMOC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

共识节点

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,DMOC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。

2.6 用户隐私和交易保密

DMOC中用户信息和区块链地址是隔离的。从各节点的记录存储中，无

法获取到相 关联的用户信息。 用户信息存储有权限控制，访问认证，加密存储等多层保护。 对交易保密程度较高的用户还可以选择交易不相关性

机制，同一个用户的每次交 易都映射到区块链上不同的地址上，从而保证了在交易账本上无法获取一个用户 的多笔交易的关联性。

2.7 安全的密钥管理体系

在DMOC的密钥管理解决方案中，提供了密钥保险箱和用户账户委托的功能来保 证密钥的安全。密 钥保险箱使用用户信息对密钥加密并分割存储在多个不同的节 点上，正常业务流程下不会访问密钥保险箱，当用户密钥丢失后，可以通过对用 户信息认证之后将密钥找回。DMOC所有委托账户操作会独立记录在区块链上，并 且对委托账户的操作有严格的频度限制和独立的风控策略，可以严格控制委托账 户的操作风险。

三、商业价值与生态

Commercial Value And Ecology

3.1 真正的100%史诗级匿名去中心化应用

过去所有的DAPP都并没有做到真正的去中心化，因为他们用的域名是实名支付的，如果应用的作者不去进行域名的续费又或者将域名解析走，那么都会导至应用无法再打开。另外DAPP的UI 部份多数是采用Web界面进行显示，这些Web界面都需要服务器进行存放，而服务器又是中心化的服务器，它存在可能被黑客修改的风险，同时作者如果不进行服务器的续费或者将服务器的文件删除，也都将会导至DAPP无法再正常工作。为了解决上述的问题，DMOC公链推出了划时代的全新理念“全托管模式”，DMOC公链将域名、Web界面、静态资源文件全部都改为了上链模式。所有人在DMOC公链上开发DAPP所有的域名都不再会是自己的域名，而是来自于全世界各地的域名提供商出租的域名，我们不需要去注册自己的专属域名，但是却可以在DMOC平台上租用无数的域名。通过这种匿名的去中心化租赁方式，DMOC为DAPP开发者提供了完全匿名去中心化的域名解决方案。同时也为DAPP的用户提供了一种可以永续使用DAPP的方式，当作者不再给域名续费时，作为应用的使用者，可以根据应用的地址，在DMOC DNS平台中自行自助续费，而不需要通过域名的作者同意就可以完成这样的动作。这样有效地解决了域名永续的概念。而且第一个DAPP平台至少都会提供5个域名，也就是说，只有还有一个域名可以访问，应用都可以打开。当出现了某一个域名不能正常工作时，系统会自动重新分配新的域名给到DAPP。确保DAPP永远都会有5个可用的域名。存放Web资源也是同理，在发布应用后，所有的Web资源将会同步到所有的矿工节点中，确保应用在所有的矿工中都有备份，从而实

现了应用的去中心化。而且当租期到了之后，普通用户也可以通过续费的方式，将网站再次激活打开。

3.2 新代币合约标准

DRC代币合约，此代币合约会细分为：稳定币合约，非稳定币合约。基中稳定币合约又会分为质押型稳定币合约，以及算法共识稳定币合约。用户可以通过DMOC公链提供的稳定

币合约模板，快速地开发出属于自己的代币。

3.3 基本应用方案

通过DMOC公链可以开发出传统的DAPP，解决去中心化应用的最后一个难点。实现以下应用的开发：

I. IOS/Android程序开发

II. DWeb应用开发

III. 智能合约/代币

IV. 桌面软件

3.4 高级应用方案

通过DMOC公链还可以开发复杂应用，比如目前所有公链都不支持的定时任务功能，当到达指定区块时智能合约自动触发相应的功能，而此自动触发所消耗的手续费来自于智能合约本身的余额。也就是开发者需要提前存一定量的GAS到应用中，又或者由用户在使用应用时多扣一些手续费作为应用未来的GAS定时任务费。通过此功能，我们就可以开发出非常复杂的定时周期任务进行复杂计算。

3.5 矿工节点全节点

I. 激活全节点凭证，支付3个ZS, 300个DMOC

IOS/Android 程序开发	DWeb应用开发	智能合约/代币	桌面软件

II. 成为全节点，维护全网所有数据，全额爆块

III. 每矿工周期为：10000区块

IV. 矿工每周期可投票下一期的全节点凭证，每一期到达50%区块时，为结束投票进行统计。每次投票可选择上调1%-10%成本，或下调1%-10%成本。

V. 参于投票人数不达21%时，作流票处理。系统自动降低5%全节点

凭证。

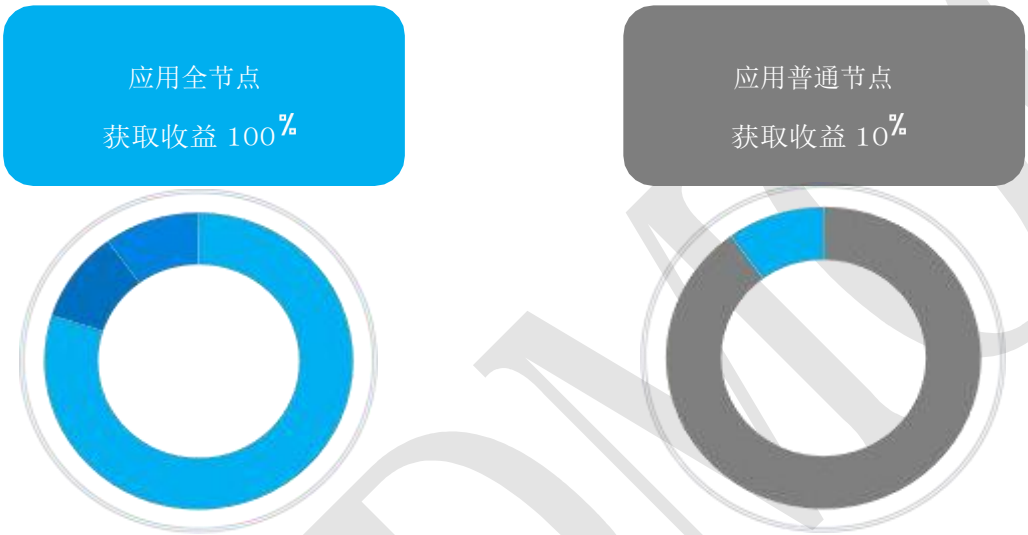
VI. 每矿工周期需有0.1%的矿工数量增长，低于此值不可以增加矿工费。

VII. 21*N节点

普通节点（默认）

I. 算力收益爆块10%

II. 轻节点，只维护内置应用和应用链，以及可自定义各别应用，或Top20，Top 100, Top 500应用。



3.6 生态应用

3.6.1 医疗电子处方

在技术上，DMOC依托区块链，利用DMOCNET底层技术支撑起了医疗数据交换网络，以分布式智能服务的方式将个人、医院、制药厂、保险公司链接到一起，包含了区块链加密储存的底层、链上服务的互联互通层和线下执行的业务逻辑层，实现了链上链下通联、数据隐私保护、授权访问和跨链资源调动。这样，身处共享平台的各方能够在不泄露患者隐私信息的前提下，根据授权交换必要的处方配药信息，保障电子处方的合规流转、安全访问，在全生命周期内可审计可追溯。

3.6.2 数字身份与应用

区块链使用的非对称加密算法是天然的用户认证系统，可构建去中心化的数字身份系统，DMOC-ID是系统命名空间中唯一的、 永久的身份标识。通过DMOC-Key，用户可以方便便管理自己的数字资产，比如：通证、数据、信用等， 以及对其进行访问控制， 比如：授权第三方访问自己的数字资产，获得收益等。于区块链的不可篡改等特性，也自然形成了信用体系。

信息访问：用户可以随时维护自己的数字资产，针对不不同类型数字资产设置相应的模式，分为私密、公开、收费等，以及为收 费模式的数字资产定价。

信息访问控制：第三方通过访问控制协议申请访问用户数字资产，用户可以选择授权通过、拒绝等。信息访问审计：查看自己的 访问控制记录，交易记录等。

信用访问：用户可以随时维护自己的个人信用，并设定自己的 信用模式。

信用访问控制：第三方通过访问控制协议申请访问用户信用， 用户可以选择授权通过、拒绝等。信用访问审计：查看自己的信用访问控制记录，交易记录等。

3.6.3 供应链

商品通常要经过物流、仓储、通关、销售等诸多环节，终交付到消费者手中。当出现售后服务的时候， 还会有对应的逆向流程。当前的供应链基本上是不不透明的，消费者很难确认商品产地、流转信息等，对于一些行业，比如：食品、药品、奢侈品，这是很大的问题。因此一个对所有利益相关方都公开透明的、可信的供应链体系非常重要。

商品数字身份：运用原子哈希等技术为商品建立数字身份，并 随时查阅其相关信息。

全流程溯源：通过运用DMOC-IOT、DMOC-Chain等技术， 在供应链全流程，针对商品的每次操作，比如：时间、地点、操作人、说明等，都将自动存储到区块链上，确保数据不不可篡改。供应链对利益相关方透明，可以随时跟踪商品状态。

商业合约智能处理：通过智能合约技术，可以根据预先设定的商业规则实

现自动保险理赔，物权转移等，减少交易摩擦，促进合 作。

3.6.4 IOT(物联网)

所谓物联网，即是嵌入了电子、软件、传感器、执行器以及连接硬件的物理设备网络，家用如路由器、摄像头、智能电视、手机、 平板电脑、智能音箱、甚至于扫地机器人、智能晾衣架、净水器等， 是科技化日常生活必不可少的一部分。这些设备的附件使他们能够在必要时连接和交换数据。DMOC物联网技术可用于通信，识别， 所有权和设备管理。为了避免重大崩溃和系统故障， IOT网络可以使用DMOC分布账本来同时存储和处理大量

数据以及各种请求。不间断运行，更好地安全性和隐私数据不以集中方式储存，由于服务器滞后等原因，不会存在停机或无响应设备的问题。物联网设备不需要通过第三方连接，DMOC可提供解决方案使其通过生成点对点连接以建立信任。成本更低，系统更稳定，当今的物联网基础设施中使用的服务器是专用的，由于其定制化需求导致生产及维护成本较高，DMOC提供分布式账本系统去除了中央服务器的使用，降低服务器成 本， 并且可避免由于系统不稳定导致的宕机。

解决方案:

1、物联网设备的部署通常很复杂。DMOC可以轻松提供物联网设备识别，身份验证和无缝衔接，安全的数据传输。这使部署 更加简单，安全。

2、无须第三方，物联网传感器可直接与目标交换数据，全网公证，这可以保护IOT设备的数据不被篡改。

3、DMOC支持各个设备的匿名和社区自治，保证了数据的完整性和独立性数据之间可以平等交换。

家用案例介绍:

路由器通常为家用IOT设备入口， 智能设备数据会通过路由器进行传输，形成完整的家庭IOT设备群画像； DMOC提供技术方案将家用路由器提供分布式存储节点，并提供物联网身份识别，成为点对点连接载体，确保输出数据在过程中不被篡改，更为快速安 全。

商用案例介绍:

以工业物联网为例，每家每户安装的智能电表为节点，使用电表以户为单位使用的能源数据进行分布式存储，形成数据闭环，不占用额外资源，不存在中央集群服务器宕机所导致的数据丢失问题，并且降低维护成本；数据可为能源企业提供业务理论支撑。未来农民也可以使用物联网设备来追踪他们的牲畜何时用尽了水和食物，制造商可以在重要的生成品即将耗尽时收到通知。当供应低于某个阈值时，他们甚至可以设置自动化机器来订购更多的产品。

3.6.5 资产管理

金融的核心之一是风险定价，风险的本质即不确定性，获取的有效信息越多，对风险的定价越准确。由该层面出发，金融是个吃数据的行业，强特征数据往往事 关企业和个人资金流水、健康等敏感数据。因而在资产管理行业，有大量的行业信息共享机制，包括金融行业的黑名单、多头借贷/投保风险、病例信息、车辆信 息等。DMOC利用区块链技术建立了数据分享和交易平台，机构不用将用户数据交 给第三方机构（有泄露风险），用户可以拿回资产数据自主权。

四、社区共识 Community Consensus

4.1 社区自治建立共识

高质量的社区治理机制可以聚集内部力量，促进自身发展并吸引外部支持。对全球区块链社区进行全面研究后，成功的区块链社区治理模型需要做到以下几点：

一、是建立健全社会激励机制。

只有给社区成员足够的激励措施，才能形成积极的反馈，以吸引更多的社区成员加入。在区块链社区中，共同的激励机制是“挖矿”活动。因此，为了提高社区成员的积极性，在设计社区治理时必须充分保证全节点的利益。

第二、充分的“社区自治”。“社区自治”的概念已成为区块链社区的“共识”。

但是，在实践过程中， 许多区块链社区在很大程度上是由项目方领导的。为了充分实现区块链社区自治，DMOC 将采用分布式社区模式，由社区成员通过投票独立建立。

第三、践行“法典化”。

DMOC会将社区治理的基本规则写入智能合约，由系统自动执行， 并通过合理分配治理权来确保社区规则的一致性和稳定性。 连锁生态中的重大事件和战略决策由DMOC连锁的所有所有者通过协商和投票决定。DMOC 的治理计划也将根据社区发展不同阶段的要求逐步完善。

4.2 链上自治

DMOC所有的重要参数、费率、计价区间等均由线上全节点投票决定。真正做

到平台由节点共识来维护。

4.3 链下治理

DMOC采用DPoS机制，全节点提供网络，存储和计算基础架构，并负责DMOC网络的交易验证，交易统计，区块打包和确认。全节点将获得成功打包的奖励，并且还将受到DMOC社区的监督。 全节点由社区的所有成员通过投票选举产生。每个凭证都被视为一票，所有凭证持有者都可以参与投票。代币持有人在参加投票时将需要在钱包中抵押代币。如果令牌在此期间被转出，将被视为提款。 为了确保有效执行节点选举，DMOC将为候选人制定一系列标准和规则。

五、生态路线图

Ecological Road Map

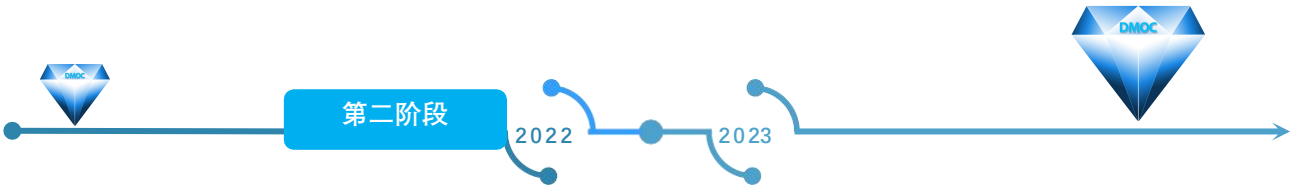
5.1 公链推进计划

先行生态

STEP 1	TRC20 代币启动，机构融资
STEP 2	DMOC 方案测试和技术团队建设。将项目推向世界。
STEP 3	DMOC 方案协议发布。DMOC 第一阶段的工作开始。

第一阶段

STEP 1	DMOC 第一阶段启动。招募节点合伙人。网体架构阶层管理形成公司化，推出 NVM 虚拟机测试资料及 测试网发布。将服务网点布局全球各城市。开始扩大技术团队并进行第二阶段的工作。
STEP 2	发布主网，并建立开源社区并在技术圈传播意识， 布道 DMOC 公链生态软件和硬件方案。



STEP 1

矿机算力预售。推出 DMOC USDT 算法稳定币。第一阶段，三万 T，抢完停止预售，提前三个月产币；第二阶段，三万 T，抢完停止预售，上线确定后提前一个半月产币；第三阶段，四万 T，抢完停止预售。

STEP 2

STEP 3

扩大了 DMOC 在 10 个国家/地区的地面营销和技术团 队，以了解推出 DMOC 教育服务，为全球技术员提供研发指导。DMOC 第三阶段的工作开始。DMOC 钱包编译上链，所有用户可发布自定义的内置 N A 钱包功能的 Android 应用 APP。

DMOC 薪酬并解决用户咨询。

STEP 4

DMOC 生态系统建立了并行的经济体系，允许廉价而 快速的汇款，使企业能够在全球进行交易，DMOC 钱 包正式接入支付网关商户功能。

上线全球百家顶级交易所。发布 DMOC Grey Rabbit OS。

第三阶段

- 2022 Q4-TRC20代币启动，机构融资

- 2022 Q4-DMOC方案测试和技术团队建设。将项目推向世界。
- 2022 Q1-DMOC方案协议发布。DMOC第一阶段的工作开始。
- 2022 Q2-DMOC第一阶段启动。推出NVM虚拟机测试资料及测试网发布。开始扩大技术团队并进行第二阶段的工作。
- 2023 Q3-发布主网，并建立开源社区并在技术圈传播意识，布道DMOC公链生态
- 软件和硬件方案。
- 2023 Q4-启动DMOC第2阶段，推出DMOC USD算法稳定币。为构建DMOC Pay
- 全球支付平台做好准备。
- 2023 Q1-扩大了DMOC在10个国家/地区的地面营销和技术团队，以了解DMOC
- 薪酬并解决用户咨询。
- 2023 Q2-推出DMOC教育服务，为全球技术员提供研发指导。DMOC第三阶段的工作开始。DMOC钱包编译上链，所有用户可发布自定义的内置DMOC钱包功能的Android应用APP。
- 2023 Q3-DMOC生态系统建立了并行的经济体系，允许廉价而快速的汇款，使企业能够在全球进行交易，DMOC钱包正式接入支付网关商户功能。
- 2023 Q4-DMOC第3阶段启动。上线全球百家顶级交易所。发布DMOC Grey Rabbit OS。

5.2 生态发展阶段准备期

从2018年10月到2020年9月，成立了一个团队来阐明业务发展需求，确定共有链设计思想，制定初步的开发和运营计划以及完整的白皮书，黄皮书和演示。

检验期

从2020年3月到2020年12月，团队按照计划推进该项目，包括开发基本组件，应用程序模块和智能合约标准，并逐步完善相关的社区治理体系。

发展时期

从2021年5月到2021年9月，团队根据计划进行了项目推广，包括开发基本组件，应用程序模块和智能合约标准，并逐步完善了相关的社区治理体系。发行TRC20令牌支持在线测试链来完成测试和升级。启动主网以启动DMOC实际货币之旅并建立新的生态系统。 节点构建：包括购买免费的节点服务器和扩展社区节点。开发者社区建设：开展宣传活动，设立奖励计划，吸引全球技术开发人才。

完善发展时期

2021年10月至2022年5月，改善社区，改善生态，促进跨链和跨国业务的扩展，大力发展生态社区，积极推动DMOC全球化。 应用程序构建：公链启动时，理想的状态是支持不少于10个杀手级应用程序和数百个DAPP，并通过黑客马拉松和其他大规模竞争吸引更多智能合约在链上部署。生态工具的构建：为了提高共有链的易用性，为开发人员提供了各种应用程序项目，例如钱包，浏览器和开发环境一键式部署解决方案，用户友好的移动链接（例如移动设备）移动开发和合约模板等。

成熟期

2022年6月至2023年12月，将继续迭代升级共有链功能，进一步深化节点

建设，开发者社区建设，应用程序建设等，并整合DMOC金融生态业务整体以及各种类型的合作伙伴资产。

六、免责声明 Disclaimer

除了本白皮书中所述的内容以外，DMOC团队对DMOC或项目许可证不作任何陈述或保证（尤其是关于其可销售性和特定功能）。项目应遵循自愿参与，承担风险，承担责任和自负盈亏的原则。DMOC的开发，维护和运营存在风险，这可能超出DMOC的控制范围。除了本白皮书的内容之外， 还要求用户注意以下所述的风险，并评估当事方承担以下所述的风险的能力。DMOC项目的开发可能存在以下风险：

信息不足

截至本白皮书发布时，DMOC仍在开发中。它的哲学，共识机制，算法，代码以及其他技术细节和参数可能会经常更新和更改。尽管本白皮书包含DMOC的最新关键信息，但它并不是绝对完整的，DMOC仍会不时为特定目的进行调整和更新。DMOC将尽可能为社区成员提供有关共有链发展的各种信息，但它不能确保将所有信息实时传输给每个令牌持有者。

与司法监督有关的风险

加密的数字资产正在或可能由不同国家/地区的当局监管。DMOC可能会不时收到一个或多个主管当局的查询，通知，警告，命令或裁定，甚至可能被勒令中止或终止任何与DMOC链有关的发展或行动。DMOC的开发，营销，推广或其他方面可能会受到严重影响，阻碍或终止。由于监管政策可能随时更改，因此DMOC在任何国家/地区的现有监管许可可能只是临时的。

密码学

加密技术的进步（例如密码破解）或技术进步（例如量子计算机的发明）可能会对基于密码的系统（包括DMOC）构成危险。DMOC不能始终保证DMOC的绝对安全。在合理的范围内，DMOC 将采取预防或补救措施，升级DMOC的基础协议以应对加密技术的任何进步，并在适当的地方采用新的合理安全措施。

开发失败或被放弃

DMOC仍在开发中，而不是随时准备发布的成品。由于DMOC系统的技术复杂性，DMOC可能会不时面临不可预测和/或无法克服的困难。因此，DMOC的开发可能会由于任何原因（例如由于不可抗力）随时失败或被放弃。

代码缺陷

没有人能够保证DMOC的源代码是完美无缺的。该代码可能具有某些缺陷，错误，缺陷和漏洞， 可能会阻止用户使用某些功能，暴露用户的信息或引起其他问题。如果存在此类缺陷，将会损害 DMOC的可用性，稳定性和安全性，从而对证书的价值造成负面影响。开源代码基于透明性， 以帮助社区识别和解决问题。DMOC将与DMOC社区紧密合作，以在将来不断改进，优化和改进DMOC源代码。

源代码升级

DMOC源代码是开源的，DMOC社区的任何成员都可以不时地对其进行更新，修改，修改或更改。没有人能预测或保证升级，纠正，修改或变更的确切结果。因此，任何升级，更正，修改或更改 都可能导致意料之外或意想不到的结果，这可能对DMOC的操作或通行证价值产生重大不利影响。

竞争

底层的DMOC协议基于开源计算机软件。在源代码中没有版权或其他知识产权的主张。因此， 任何人都可以合法地复制，复制，重制，设计，修改，升级和改进，重新编码，重新编程或以其他方式使用DMOC源代码和/或底层协议，以尝试开发具有竞争力的协议，软件，系统或虚拟机，虚拟平台与DMOC竞争，甚至超越或取代DMOC，DMOC无法控制。此外，将会有很多与DMOC竞争的基于区块链的竞争平台。在任何情况下，DMOC都无法消除，防止，限制或减少旨在与DMOC链进行竞争或替换的竞争努力。

市场风险

代币流动性和价格波动代币的交易仅基于相关市场参与者对其价值达成的共识。没有人能保证代 币的流动性或市场价格任何时间任何程度。如果令牌在公开市场上交易，其价格可能会急剧波动。这种价格波动可能是由市场力量（包括投机交易），监管政策变化，技术创新，交易所的可用性 以及其他客观因素引起的。这种波动也反映了供求平衡的变化。代币交易价格涉及的风险应由交 易者承担。

免责申明

本文档仅作为传达信息之用，文档内容仅供参考，不构成在DMOC 及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。

本文档内容不得被解释为强迫参与通证销售。任何与本白皮书相关的行为 均不得视为参与通证销售，包括要求获取本白皮书的副本或向他人分享本白皮书。

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， 与DMOC 签订的合同是真实有效的。所有参与者均为自愿签订合同，并在签订合同之前对DMOC 进行了清晰必要的了解。

DMOC 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、通证机制及通证分配情况。

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。DMOC 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。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。

DMOC作为 DMOC 链的官方通证，是平台发生效能的重要工具，并不是一种投资品。拥有DMOC不代表授予其拥有者对DMOC 平台的所有权、控制权、决策权。 DMOC 作为在DMOC 中使用的加密通证，均不属于以下类别：

①任何种类的货币；

②证券；

③法律实体的股权；

④股票、债券、票 据、认股权证、证书或其他授与任何权利的文书。

DMOC 的增值与否取决于市场规律以及应用落地后的需求，其可能不具备任何价值，团队不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。

在适用法律允许的最大范围内，对因参与众筹所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其它经济损失，本团队不承担责任。

DMOC 平台遵守任何有利于通证销售行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类检查

的所有信息必须完整准确。

DMOC 平台明确向参与者传达了可能的风险，参与者一旦参与通证销售众筹，代表其已确认理解并认可细则中的各项条款说明，接受本平台的潜在风险，后果自担。

禁止代币销售的国家公民不被允许参与。