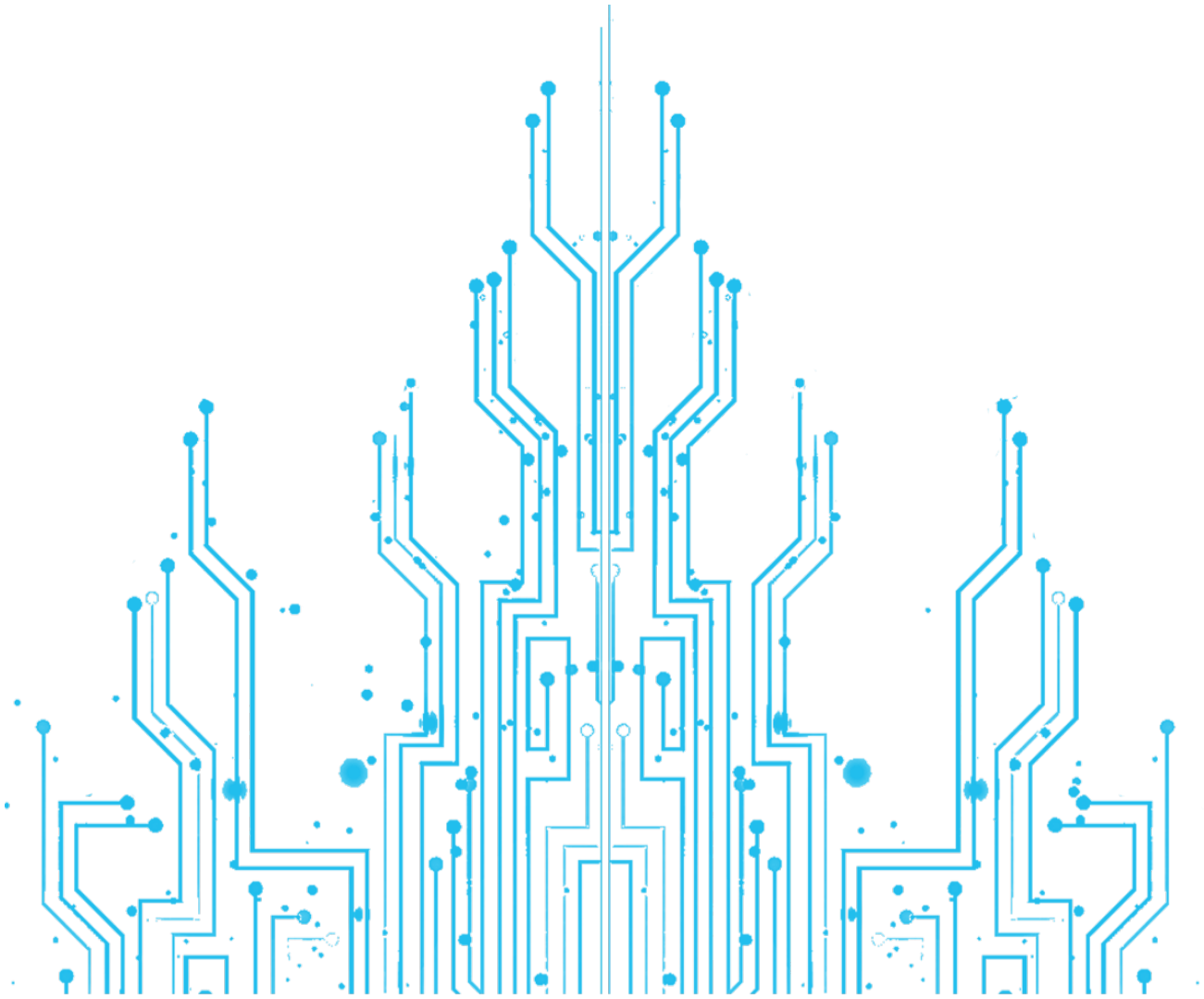
环境监测链(EMChain)

专注于区块链环境监测的公链



目录

摘要

EMC 旨在利用区块链技术完成自主性环境监测协同平台的建设，构建全球化协同共享平台，从而帮助全球解决“环境监测以及检测”的棘手难题。环境监测是了解、掌握、评估、预测环境质量状况的基本手段，是环境信息的主要来源。EMC 利用区块链的去中心化、去信任、集体维护、数据库可靠的技术特点，针对环境监测的样品不透明、难辨真假、中心化运营、监测信息的伪造、信任等行业痛点，将传统的中心化的信息孤岛打通，在信息安全以及保密的前提下，实现业务和数据共享。利用区块链的分布式账本体系，去中心化，信任机制，智能合约，共识机制，打造基于区块链技术的先进的环境监测服务系统，成为一个应用环境监测的商用区块链。在环境监测的每个环节布点、采样、样品运输与保存、分析监试、数据处理、分析评价及报告编写等方面每一个环节的信息实时上传存储让每一个动作都公开透明。EMC 作为环境监测行业价值传递的结算代币，利用区块链分布式、可信任、不可篡改性来记录所有环境监测的相关数据，包括物品从样品采集，样品取样到使用环境监测样品等各个环节的完整信息，进而对监测数据的价值有准确评判，以便进行交易。区块链加密算法打造安全交易，平台可以用于发送和接收数字资产，实现直接、快速转帐，确保交易安全。

一 项目背景

随着互联时代快速发展，区块链历经了 1.0、2.0、到现在的 3.0 时代，可谓是汲取了不少成功的经验，区块链具有可追踪溯源的功能还去中心化。

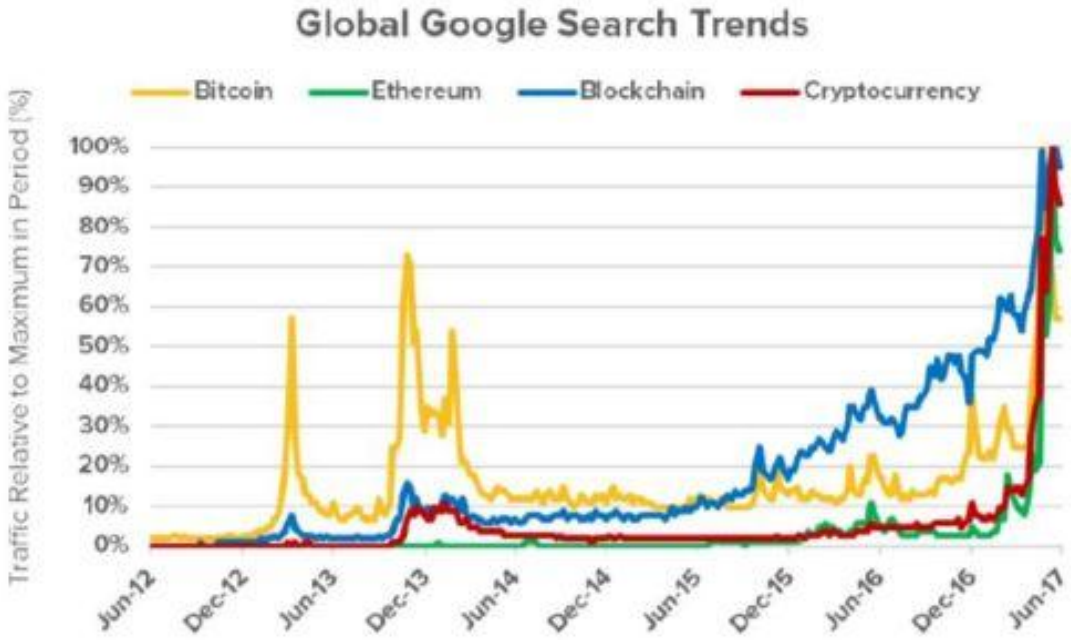
区块链是分布式数字存储、点对点传输、共识机制、加密算法等技术的集成应用。区块链是根据自身的机制和特征，将系统中的数据根据供应链的链接，形成一个新的完整的供应链，它的不可篡改性和信息公开性更好的维护了公平。

互联网挟持了传统实业，区块链将挟持传统互联网行业，中介、某行、甚至平台架构，未来都可能被颠覆，不复存在。区块链它独有的分布式数据库，使人和人之间有了真正的信任和公平。区块链采用 P2P 技术、密码学和共识算法等技术，具有数据不可篡改、系统集体维护、信息公开透明等特性。区块链提供一种在不可信环境中，进行信息与价值传递交换的机制，是构建未来价值互联网的基石。

区块链技术作为一种通用性术，从数字货币加速渗透至其他领域，和各行各业创新融合。未来区块链的应用将由两个阵营推动。一方面，IT 阵营，从信息共享

着手，以低成本建立信用为核心，逐步覆盖数字资产等领域。另一方面，加密货币阵营从货币出发，逐渐向资产端管理、存证领域推进，并向征信和一般信息共享类应用扩散。

区块链引发了世界性的关注，并成为一场全球参与竞逐的“军备”大赛，包括美国、英国、日本都认识到区块链技术巨大的应用前景，开始从国家层面设计区块链的发展道路。区块链及相关行业的加速发展，引领着全球正在跑步进入“区块链经济时代”，更多成熟的应用在加速落地。

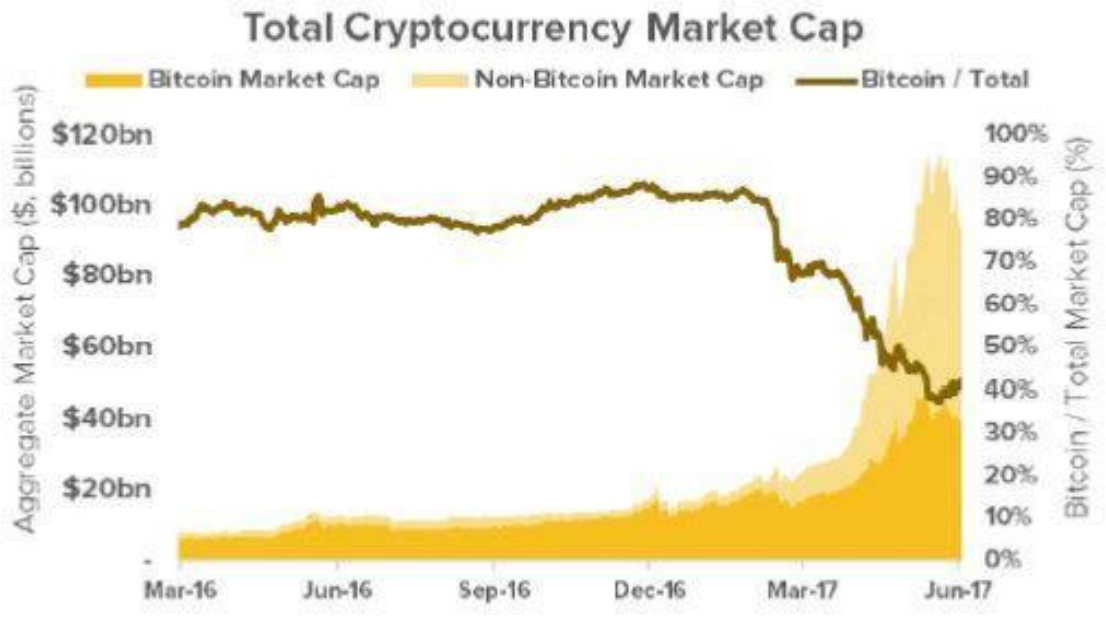


2017 年第二季度谷歌搜索量

此外，随着区块链代币总市值飙升，数字货币市场呈现出多元化的趋势。

2017 年年初，比特币几乎占据了加密货币总价值的 90%。而到第二季度末，这一数字下降至接近 41%。比特币对数字货币生态系统的全面主导地位大大降低，多种数字货币活跃发展。

总结而言，数字资产行业规模不断扩大，并呈现出市场多元化趋势。



2017 年第二季度数字资产行业市场多元

区块链成为互联网行业最火的一个名词，去中心化，分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链也是数字货币底层技术产物。比特币的火热，让全世界各国纷纷加入到区块链和数字资产领域中，其中不乏各大政府和企业的大力开发。随着社会的进步和发展，科学技术水平显著提高，越来越多前沿技术涌现，并广泛应用在社会各个行业中，极大地促进了全球经济的增长。区块链技术作为一项前沿技术，在环境监测中所起到的作用是十分突出的，尤其是在当前环境污染严峻的背景下，为人类社会长远发展带来了刻不容缓的挑战。区块链技术也成为当前环境保护的重要手段，可以实时监控环境质量变化，一旦出现严重污染情况，将及时有效地预警，采取合理手段加以控制。EMC 融合区块链技术以环境监测和检查为落地应用。对环境领域繁荣水环境、气环境、声环境、土壤等的技术检测服务，为社会各界提供公正、独立、准确的检测数据。凭借专业的环保技术、先进的检测实验室、稳健的质量体系和完善的服务流程，为社会各界提供独立、公正、准确的检测数据及分析报告，在环境检测服务领域内全球领先并具有一流公信力的检测数据。

二 项目介绍

2.1 公司介绍

伍德赛德集团(Woodside Petroleum Group)是在澳洲证券交易所上市的大型实业公司，和马耳他政府的鼎力合作下，践行将马耳他布莱克黄金项目做为依托，

架构全球生态环境检测与区块链技术结合，开拓新的领域环境监测，打造全球生态环境数据去中心化。

伍德赛德集团(Woodside Petroleum Group)在马耳他成立了 EMChain 技术有限公司，并取得了区块链牌照，现公司正着手全力加快开展 EMC 环境监测链（EMC）的发行。总计发行量为 1.88 亿。其中 70%用于交易回馈。而在互联网时代下，基于网络空间的虚拟市场无疑有着更多优势，掌握区块链技术，以及电子金融。其价值的界定很大程度上等同于项目的拥有的实际资产价值，因此，在欧盟和马耳他政府的支持和市场大环境的需要下，EMChain 技术有限公司推出了 EMC 环境监测链（EMC）。

建立在以太坊分布式智能合约 ETHerscan 上的广泛区块链加密应用技术，用户可查看在以太坊智能合约上所以信息。在世界各国推动区块链技术应用的今天，EMCain 技术有限公司并进军数字资产，将为市场带来更专业的革命性金融产品。

2.2 什么是 EMC

EMC 基于黄金托底虚拟货币落地应用环境监测等项目，旨在打造一个领先行业的去中心化环境监测平台。采集环境监测大数据，进行数据价值的挖掘，对环境监测者提供精准检测数据。利用区块链分布式数据存储技术和不可篡改特性，真实记录内容数据，服务数据，采集数据，样品分析数据等检测数据，并且对数据信息进行加密认证，保证数据的可信，并对数据进行溯源确权。通过授权，数据可对外分享和交易。平台采用智能合约就环境监测项目的各项交易进行合约支付，保证交易的公平与效率。EMC 旨在建立一个更加公平透明的环境监测项目支付体系，为共享环境监测生态提供了新的动力。EMC 是一款支付型货币，旗下产业有外汇，网上商城，数字货币交易平台。EMC 可以在旗下的一些平台作为消费。

2.3 EMC 的愿景

EMC 团队秉承进一步完善全球环境监测产业链检测数据，打造全球诚信透明高效的环境监测数据，是环境监测行业价值互联网顶级去中心化公有链，搭建环境监测产业链行业底层区块链设施，让全球智能环境监测系统产业能够在 EMC 链上快捷的开发自己的区块链应用，并根据智能合约自由交换数据，利用区块链的防伪、防篡改属性来记录每一笔交易和用户点击，让所有环境监测系统产业行业的上下游链条实现透明、高效，促进环境监测市场提高效率，降低成本。

2.4 EMC 的创新特点

EMC 平台借助区块链技术优势，基于环境监测的大数据应用和云计算技术，开发手机 APP 等服务端口，运用 LBS、物联网等核心技术，提供全球环境监测一体化解决方案。，平台具有具有如下显著特点：

高安全性　高完整性　高智能型　高便捷性

1）安全性：区块链加密算法打造安全交易，EMC 平台可以用于发送和接收数字资产，实现直接、快速转帐，确保交易安全。

2）完整性：区块链是一种能够永久记录交易的技术，它不能在之后被抹去，只能按照顺序不断更新，实质上保持了一条永不结束的历史轨迹。因此，EMC 能够完整记录物品的信息，便于追根溯源。

3）智能性：通过市场实践与数据分析后，开发手机 APP、INS 平台、微信平台、微博平台等信息系统，创建出独有的环境监测云计算平台，集合物联网、ERP、二维码、图像识别等先进技术，进过多种核心算法，精确计算出从地区到个人的监测产值、构成及利用率。

4）便捷性：EMC 让所有运营商参与其中，并能够获得相应金额。

2.5 环境监测与区块链的撮合

从中心化到去中心化，点与点完成结算。

环境监测与区块链结合的真正价值在于促进环境监测行业的结算中心化机构之间达成共识、构建联盟，形成多个中心组成的结算生态圈，这样的生态系统突出中心的职能，大大简化了中心化机构环境监测行业运营成本。

从不信任到信任，结算信任危机成为过去式。

环境监测与区块链的结合具有去信任化特性，基于互不信任的原则，整个环境监测系统的运作是公开透明的，通过“签名”机制和利用“少数服从多数”的朴素方式，却能够从环境监测交易机制上保障信用。

从不安全到安全，打消用户信息担忧。

环境监测与区块链的结合使数据存储从不安全到，不用担心用户信息泄露。首先，用户数据以块链结构存储，具有自校验性，篡改之后可以迅速发现。其次数据在多个节点都有相同的备份，即使某个节点上的数据被修改，也可以从其他节点上自动恢复过来，从机制上杜绝了黑客的数据篡改袭击。

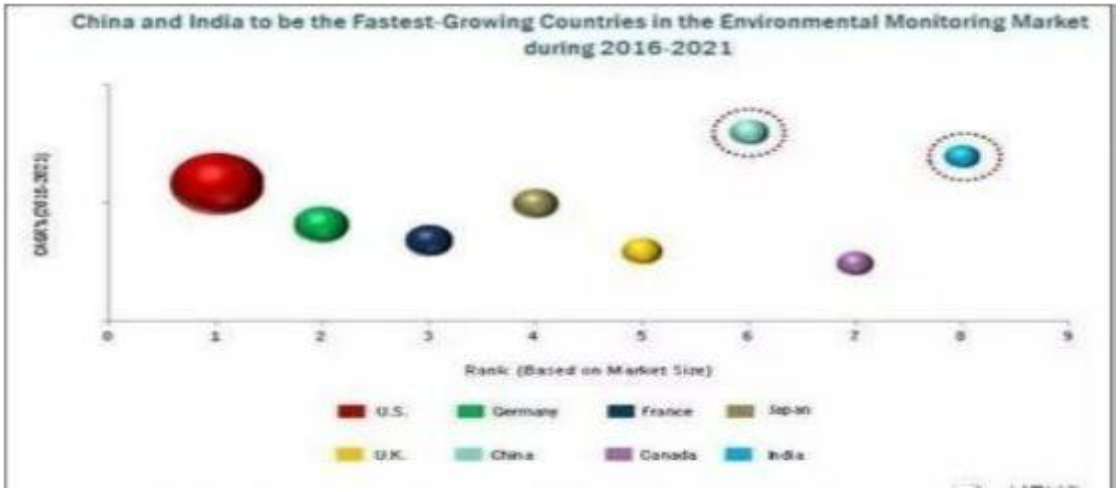
三 行业分析

3.1 行业现状

环境监测是环境管理和科学决策的重要基础，是评价考核全球改善环境质量、治理环境污染成效的重要依据。随着全球经济一体化和城市化进程的不断推进，环境问题成了公众最大的担忧，环境保护逐渐成为国家政策。随之而来的就是，最近几年环境监测仪器在环保基础上迎来了爆炸性的增长。

据麦姆斯咨询报道，至 2021 年，全球环境监测市场规模预计将达到 195.6 亿美元，2016~2021 年期间的复合年增长率为 7.70%。该全球市场增长的主要驱动力来自于政府为控制污染水平而日益增长的举措，政府对污染控制和监测、环境监测站建设的资金投入，以及对环保产业发展地不断推动。然而，环境监测解决方案相关产品的高昂成本、污染控制改革的缓慢实施，以及新兴国家环境技术的高出口壁垒是限制该市场增长的一些主要因素。此外，新兴国家不确定且反复无常的环境法规也是该市场增长面临的挑战。按照产品细分，全球环境监测市场可分为三大主要类别，即：环境监测器、环境传感器和环境监测软件。

环境监测器又进一步被细分为两个监测产品市场，即：固定式监测器和便携式监测器。环境传感器市场又进一步被细分为：基于产品架构的模拟传感器和数字传感器；基于应用的温度传感、湿度检测、化学检测、生物检测、颗粒物检测和噪声检测。归因于智能家居和现代建筑设计越来越多的采用以及创新环境监测技术的不断发展，便携式监测器细分市场预计在 2016~2021 内将以最高的年复合增长率增长。



图：2016~2021 年间环境监测市场规模排名以及年复合增长率预测（按国家细分）

按照地区细分，环境监测市场可分为北美、欧洲、亚太和世界其它地区。

在 2016 年，全球环境监测市场预计将被北美主导。政府对环境监测站维护和运营经费的不断增加，以及美国环境保护署（U.S. EPA）的严格规定正驱动北美地区市场的增长。归因于快速工业化、日益严格的环境管制政策的实施，以及日益严格的环境安全条例，亚太地区预计将在预测期内以最高的年复合增长率增长。

3.2 行业痛点

第一，环境监测行业众多运营商面临着无法协调的问题，环境监测的样品回收、样品处理、利用各运营商之间往往是独立运行、各自发展，达不到驱动协同的作用。

第二，众多环境监测企业对监测行业片面追求经济目标，过分强调其商业性而忽视了该行业的社会效益和环境效益。

第三，现有回收方式存在弊端。由于当前许多企业对垃圾的回收利用还仅停留在简单粗加工、切割、拆解、粉碎、分类打包后出售阶段，未形成一个集回收、分拣集散、利用为一体的网络体系，存在缺少统一规划乱设收购站点、管理无序、市场混乱现象严重，再生资源回收利用率低，资源浪费严重，企业规模小，加工技术落后，产业化程度低，回收不及时，处理不规范，环境污染严重，人们对再生资源行业缺乏进一步的认识，循环经济观念尚未形成。

第四，个体成立的回收点环境污染问题严重，许多都是以牺牲自然生态环境和人的身体健康为代价，如排放有害废水、废气、废酸危害环境。一些个体回收点进行假冒伪劣和有毒有害产品的加工，造成市场交易混乱，产生了不良的影响。以城市郊区或者城乡交界处为基础建立起的回收拆解加工点，给城市的环保工作带来了很大的困难。

第五，环境监测行业整体技术落后。对该行业急需引入的新技术、新设备，政府缺乏必要的关注和扶持，导致大量可再生的废弃物因此难以得到回收和利用。

四 平台构架

4.1 平台运行模式

EMC 的运行模式是基于区块链技术的新生态环境监测服务平台，是环境监测行业真实可落地的区块链的应用，通过 EMC 平台技术可以面向所有环境监测接口开放，有别于所有现实货币渠道及发行的运营平台；独立结算、独立运营、保护用户、兼顾公平、不改变原有环境监测体系，可以让传统环境监测与采用交易抽成模式环境监测接入环境生态圈。EMC 利用区块链技术实现去中心化运作。而去中心化本质就是减少中间链条。在环境监测产业应用中去掉渠道、发行、推广等运营各个环节，创造一种应用环境，让用户和用户之间、让用户和 CP 之间直接对接、直接结算；从而降低成本、提高体验、保护劳动进而形成用户自己的环境监测生态圈。EMC 建设了一个以 EMC 作为交易货币的环境监测服务生态圈。

EMC 是基于区块链技术上的应用，因此，具有加密的虚拟财产、去中心化支付、挖矿奖励等特点。

4.2 EMC-矿工机制模式

对任何数字货币系统来说，挖矿具有两重意义。首先，挖矿是产生货币供应的基本过程，而货币供应是矿工们的根本动机。其次，挖矿过程实际上是对交易数据的完整性进行加密处理，从而形成一个 checksum，因此也是保护货币信用、防止欺诈的核心手段。

4.2.1 挖矿计算机制

数字货币的加密计算包括两个方面的内容：1）公钥系统实现数字签名，2）单向加密实现交易记录的完整性计算。矿机主要负责后者的计算。交易数据的完整性计算通过特定数学函数实现，现有系统普遍采用以 SHA 及其变种的 Hash 函数，该函数需要满足以下三个要求：

（1）压缩性：把任意长度的交易记录计算为一个较短的、具有固定长度的字符串；

（2）隐藏性：计算具有单向性，即从计算结果很难推出原文，这里需要考虑当前正在高速发展的量子密码技术，基于数论的密码系统在量子计算面前是脆弱的；

（3）计算性：计算过程需要一定的、可以证明的工作量，其计算强度（体现为计算时间）相对可控。

除了上述条件以外，如果挖矿计算能够完成超越加密货币之外的应用（例如科学计算和机器学习），那么伴随矿机网络强大计算能力的硬件损耗和电力消耗就具有挖矿之外的价值，反过来也提升数字货币的价值。

4.2.2 EMC 矿机算法思想

区块链需要一定的工作量证明（Proof ofWork，PoW）机制，其目的在于防止所谓的『区块链分叉』或者 51%攻击，即矿工需要极大的运算能力才能成功篡改账本。目前最常见的 PoW 机制是哈希函数，矿工把交易记录整合到一个区块之后，需要对区块内容进行哈希运算，该运算结果首先是记录内容完整性的一种表征。其次，哈希计算结束后，矿工检查结果是否满足特定条件（例如小于某个阈值），如果不满足，则再次进行同样的哈希计算，直至满足阈值为止。这样，矿工必须完成一定计算量，才能提交区块。

PoW 机制对区块链的安全性具有重要意义，然而其计算结果对人类其它方面的生活全无意义，这也是以太坊和其它加密货币受到诟病的一大原因。EMC 的 PoW 模型构造方式如下：

EMC 的 PoW 实际包含两部分，（1）EMC 公益计算阶段；（2）传统 PoW 阶段。

在公益计算阶段，每个节点将根据共识获得的随机数，选择 EMC 公益计算问题之一进行解算，该问题包含了一系列候选 EMC 问题，必须通过长时间的拟合计算才能逼近某个结果，且问题属于初始条件敏感算法。当在规定的时间内，拟合目标不达标，则节点被取消进入下一步传统 PoW 计算的资格，将进入个体任务领取状态； 通过计算 EMC 发布的资源服务获得基本奖励。当拟合完成度达标的节点，则进入传统的 PoW 解算阶段。

在 PoW 解算阶段，每个合格的节点将对交易区块以及本次 EMC 参数的提交结果进行完整性校验，获得规定难度以内的随机值。当获得该随机值后，将迅速全网发布。而收到发布结果的节点将验证 EMC 的难度以及 HASH 校验值是否满足要求。如果满足则迅速转入下一区块计算，否则继续本地 PoW 计算。

上述实现方案的核心在于：

通过 EMC 计算，确定基础 PoW 候选者，没有在规定时间内的候选者，最佳选择是进行公益计算，获得个体服务收益。PoW 将 EMC 计算结果作为验证依据；但由于 EMC 与 HASH 运算通常属于独立的两类计算方式，因此二阶段的 EMC 计算能力，同样可以作为公益计算，获得个体服务收益。

EMC 通过参数配置，既可以选择仅支持二阶段运算，也可以选择支持全部阶段运算。

4.2.3 EMC 算法特点

EMC 是通过随机采样构造满足细致平稳条件的马尔可夫过程，使得样本分布任意逼近目标函数。贝叶斯后验概率的计算通常依靠 EMC，常见采样算法有 Metropolis-Hastings （MH）、Gibbs 和 Slicing 等。其中 MH 算法被认为是二十世纪十大算法之一，其基本思想是根据似然概率比值决定是否接受样本，EMC 算法具有这样一些特点：

（1）计算量大：复杂分布经常需要上百万次甚至更多次数的采样，计算时间极大；

（2）并行度低：经典的 EMC 算法采样过程中，先后产生的样本具有顺序依赖性，难以并行化；

（3）应用广泛：EMC 是贝叶斯计算的核心模式，在环境监测、矿产、环境检测数据、环境保护、金融、支付、广告传媒、网站点击等领域具有重要应用；

（4）易于评估：虽然 EMC 的计算过程复杂，但是相对容易评价计算结果的质量，例如可以通过似然函数进行评价。

4.3 EMC 加密钱包

EMC 融合区块链技术加密钱包是一种存储加密币的软件程序。利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据，创造加密钱包，实现安全支付。因此，用户在进行交易时，可以直接在平台上支付，而不需要有自己安全方面的顾虑。

EMC 加密钱包有两层含义：一是指存储以太坊地址和私钥的文件，还有一种是指以太坊客户端。账户拥有者有一个私人密钥通往他们的钱包，此密钥是访问区块链地址的唯一途径，因此，也是接收或发送信用的唯一方式。

在钱包中，用户保留他们的区块链数字资产，原则上，以太坊就是一个平常钱包里“普通”的钱。所以，用户不会把他们所有的钱放进一个钱包，同时也不会觉得它非常安全。在这种情况下，用户需要使用备份副本和安全密码。此外，用户可以将钱包视为一个存折，即纸钱包。这没有互联网接入，因此，它不更容易受到网络黑客的攻击。

4.4 物联体系

4.4.1 物联接口

物联接口是物联网中连接传感网络层和传输网络层，实现采集数据及向网络层发送数据的设备。它担负着数据采集、初步处理、加密、传输等多种功能。物联接口总体上可以分为情景感知层、网络接入层、网络控制层以及应用/业务层。每一层都与网络侧的控制设备有着对应关系。物联接口常常处于各种异构网络环境中，为了向用户提供最佳的使用体验，接口具有感知场景变化的能力，并以此为基础，通过优化判决，为用户选择最佳的服务通道。终端设备通过前端的 RF 模块或传感器模块等感知环境的变化，经过计算，决策需要采取的应对措施。

4.4.2 追溯系统

区块链提供了一个分布式的机制进行数据锁定，使数据可以被核查和独立审计。区块链是一种能够永久记录交易的技术，它不能在之后被抹去，只能按照顺序不

断更新，实质上保持了一条永不结束的历史轨迹。因此，在 EMC 中，所有物品的所有信息都能够被完整记录。

EMC 构建了一个追溯运行系统，平台上所有的环境检测的样品对接全球各大线上环境监测商城，以及各地的设备厂商、线下商场等，每一个检测样品都获得唯一的编号。获得编号后，检测样品就如同具有“身份证”，其每一次流通信息都会被记录起来，在 EMC 平台上形成轨迹。循着这个轨迹，地球资源的来龙去脉就有了可以查证的信息。

4.5 合约式分成模式

EMC 平台采用合约式分成模式。具体来说，从最初的环境监测将地球资源智能分类到后续的各种相关运营商，所涉及到的用户在完成平台规定的处理任务之后，平台会根据之前发包的价格合理分配给用户及运营商。这种合理的费用即代币。通过合约式分成模式，建立了完善的检测数据可信机制，形成环境监测收行业整体的良性运行。

4.6 反欺诈系统

我们拥有着自己的反欺诈运行系统。EMC 基于设备软硬件特征、上网环境、设备指纹等数万原始数据，结合聚类分析、连通图挖掘、频繁子图挖掘，PageRank 风险传播等相关算法，帮助识别欺诈风险，有效控制了欺诈成本。

EMC 项目选择符合国际标准的加密机制，对联众数据进行加密，用户间的数据和信息仅双方和拥有者有相应权限的用户可以查看。

（1）对称加密。对称加密是最快速、最简单的一种加密方式，加密（encryption）与解密（decryption）用的是同样的密钥（secret key）。对称加密通常使用的是相对较小的密钥，一般小于 256 bit。密钥的大小既要照顾到安全性，也要照顾到效率，是一个 trade-off。

（2）非对称加密。非对称加密为数据的加密与解密提供了一个非常安全的方法，它使用了一对密钥，公（public key）和私钥（private key）。私钥只能由一方安全保管， 不能外泄，而公钥则可以发给任何请求它的人。非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥。

（3）私钥（privatekey） 。非公开，是一个 256 位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。

（4）公钥（public key）。可公开，每一个私钥都有一个与之相匹配的公钥。ECC 公钥可以由私钥通过单向的、确定性的算法生成，目前常用的方案包括：secp256r1（国际通用标准）、 secp256k1（比特币标准）和 SM2（中国国标）。丝路链控制链与初始数据链选择 secp256r1 作为密钥方案。

（5）哈希算法：通常哈希算法是指安全散列算法 SHA，该算法是美国国家安全局设计，美国国家标准与技术研究院（NIST） 发布的一系列密码散列函数，包括 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512 等变体。目前比特币采用 SHA-256 算法。丝路链除 PoW 外，其余哈希算法均指 SHA-256。

五 创新/应用

5.1 核心创新

5.1.1 分布式伙伴模式

EMC 平台独具创新，利用区块链不可逆技术，建立环境监测处理链条，将全球众多环境检测数据利用分包的模式联合起来，形成一个可持续的协同平台，共同为世界资源环境问题作出贡献。

5.1.2 物联创新

EMC 平台利用分布式物联网（IoT）网络，采用标准化的点对点通信模型处理成千上万设备间的交易，这有效的削减了成本，包括部署和维护大型数据中心的费用，而且可以通过成千上万的物联网设备把计算需求和存储需求去中心化。这将避免由于一个节点的失败而导致整个网络的崩溃。

但是仅仅采用分布式物联网，会遇到的首要问题就是安全问题，为了解决安全问题，避免被欺诈或盗窃，EMC 平台将物联网与区块链进行结合。通过两者的结合，让环境监测行业循环利用的资源成为可能，以及让环境检测数据更加精准。EMC 平台所形成的资产可以被共享和再利用，而不是消费一次就处理掉。

5.2 应用落地

应用

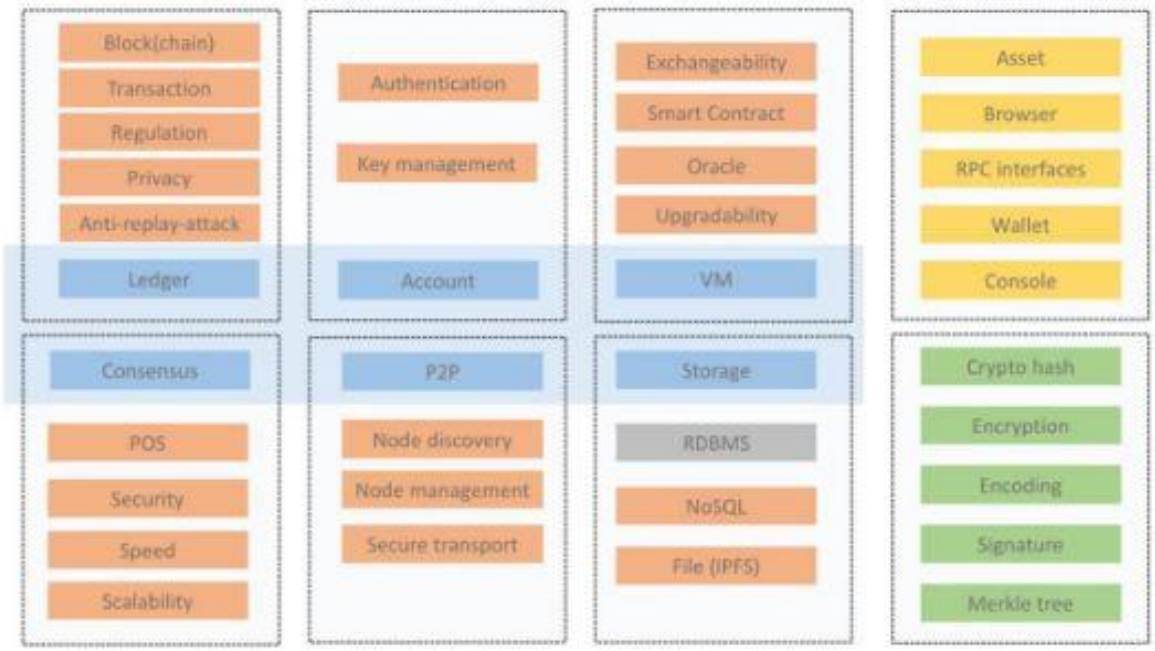
随着社会经济的快速发展，传统的中心化商业模式受到了多方制约，追求多方参与、对等合作的分布式商业模式由此逐渐显露实力，相对应的分布式技术也得以获得发展空间，而作为一种全新的分布式基础架构与计算方式，区块链技术也在近些年受到了广泛关注。EMC 作为区块链与环境监测探索的先行者，已逐渐实现了环境监测以及环境检测数据的应用和落地。EMC 平台大力推动底层区块链技术场景应用，充分发挥区块链技术的去中心化特征、不可篡改、互信共识、智能合约、可追溯与可审计等优势，不断推动环境监测和环境检测数据的落地应用。

价值

EMC 牵头多家成员机构，致力于打造世界级环境监测区块链公会，不断推动区块链环境监测生态圈的形成庞大精准的检测数据。EMC 作为全球第一、世界领先的高科技技术环境监测项目，有助于解决全球“环境监测”的问题，其也为区块链技术在环境处理行业的开源和应用落地做出了绝无仅有的贡献。EMC 平台根据环境监测行业领域的特殊业务需求、现有技术水平及法律法规等方面的要求或条件，从业务安全、性能、成本、政策、技术可行性、运维与治理等多个维度进行了综合优化，为行业未来的发展提供了契机。

六 EMC-区块链技术的应用

6.1 基础架构概述



6.2 开发服务层

6.2.1 智能合约生命周期管理

a） 允许开发者设计和创建包含商业逻辑的智能合约，环境监测业务服务系统通过接口等交互机制与区块链系统交互。

b） 提供智能合约的生命周期管理功能，如创建、调用、升级、销毁。

c） 提供对智能合约的升级与数据迁移能力，但是要满足原智能合约设定的升级规则。

6.2.2 智能合约组合服务

a） 通过组合已有的一个或多个智能合约来创建新的服务功能。

b） 为服务使用者设计集成的接口使其能访问多个区块链系统服务功能。

6.2.3 智能合约测试服务

a） 对区块链系统中实现的组件功能进行测试，以确保这些组件完整并正确地实现了服务功能。

b） 对区块链系统中实现的组件功能进行测试，以检测这些组件的系统安全性与健壮性。

c）确保服务功能接口的互操作性。

d） 测试宜覆盖区块链系统中的服务部署节点。

6.2.4 智能合约模板服务

a）环境监测系统在链上业务的支持方面采用目前主流的虚拟机机制，目前支持的是 EVM 虚拟机，可直接部署、运行 solidity 智能合约。并在积极研发更贴近金融级应用的其他虚拟机实现，以方便快速开发/ 定制链上业务逻辑

b）预定义合约模块：可以快速使用环境监测系统，针对一些常见的业务场景，环境监测系统预先开发了多个可直接使用的链上业务合约（比如积分链等），集团可根据实际需求直接选择部署/ 使用即可。

6.3 用户服务

6.3.1 钱包

用户能通过钱包创建自己的公私钥账户，并能通过钱包进行 EMC 交易智能合约调用等操作。

6.3.2 账户

对于 EMC 的用户通过交易和区块链互动来说，账户是必不可少的。账户代表着外部代理人（例如人物角色、挖矿节点 、自动代理人）的身份。账户运用公钥加密图像来签署交易以便可以安全地验证交易发送者身份。每个账户都由一对钥

匙定义，一个私钥和一个公钥。 账户以地址为索引，地址由公钥衍生而来，取公钥的最后 20 个字节。每对私钥 /地址都编码在一个钥匙文件里。钥匙文件是 JSON 文本文件，可以用任何文本编辑器打开和浏览。钥匙文件的关键部分，账户私钥，通常用你创建帐户时设置的密码进行加密。

6.3.3 存储

EMC 含有两方面的链外存储模块。IPFS 用来在链外存储大型文件，而结构化存储用来保存结构化记录，并且支持结构化查询语言。IPFS 模块：EMC 为支持大文件存储，引入了 IPFS 技术。文件通过 hash 存储，具有防篡改、永不丢失、防泄漏和访问安全等特性，避免意外事故对数据安全的冲击，确保相关信息能够永久保存，保证数据安全和用户隐私的不可泄露和丢失。结构化存储模块：结构化存储用来保存结构化记录，并且同区块链上的记录保持同步。

6.3.4 隐私保护

隐私模块提供加密合约相关服务以及各类隐私解决方案。加密合约：对有隐私需求的智能合约，提供了加密合约解决方案。在加密合约中，智能合约中的信息是经过加密的，调用合约的交易也是加密的。私密交易采用局部共识的方法，一笔私密交易的执行分为两步：第一步是预处理，将隐私交易转成一笔普通交易[S1=>S2]（S1 和 S2 分别为交易执行前后智能合约的密文状态）；第二步是将[S1=>S2]做为一笔普通交易打包进区块。私密交易 普通交易打包进区块

隐私解决方案：EMC 针对不同环境检测场景提供了不同的隐私解决方案，如多方计算和环境监测通信。通过安全多方计算，EMC 可以实现隐私的原始数据的完全隔离访问。环境监测系统上的安全通信解决方案为 EMC 带来了快速安全的数据分享服务。

6.3.5 EMC 区块链底层服务

安全机制

选择符合国际标准的加密机制，对链中数据进行加密，用户间的交易数据和交易者信息仅有交易双方和拥有者有相应权限的用户可以查看精准的环境检测数据。

共识机制

区块链的价值锚点在于链条自身的消耗与产出。当区块链选择 PoW（Power-of-Work, 工作量证明）作为共识机制时，每一次区块的生成消耗的算力都将成为其价值的基石。另外，在 EMC 上，每个节点都具备解决现实环境监测问题的能力，并能对外提供环境监测行业的环境检测数据、环境预测服务。如果 EMC 上的每个节点能够参与共享工作的结算，整个区块链条就具备了现实的产出价值。因此，为保证区块链自身价值最大化，SmartLink Token 将默认选择基于 PoW 的共识机制。PoW 的核心要义为：算力越大，挖到块的概率越大，维护区块链安全的权重越大。但由于 PoW 具备交易速度较慢等显性缺陷，因此在平台中后续的环境检测数据链，其共识机制将被设计成模块化的，可以通过控制链参数进行配置，能够动态适用公链和私链的不同应用场景。EMC 平台将针对环境检测数据链本身的应用场景和交易情况，选择合适的共识机制，确保各个分布式节点通过算法取得数据的一致性。

七 EMC 代币体系

7.1 物权属性

在数字交易平台中，拥有 EMC 代币的用户，就拥有了可以在规定平台、规定兑购点购买环境检测数据的权利。用户享有代币的所有权与处置权，即享有了代币的物权，可在法律规定的范围内任意处置代币。

7.2 货币属性

以自加密货币为中心的 API，可实现数据流转和代币的流通。在有 EMC 的平台上，用户行为数据、检测数据、电子货币、消费都可记录在链上，而有效行为又可进一步转化成代币。每个成员有独立节点，共享账本数据，有效增强了代币使用的透明性。也就是说，代币建立一个“价值交换”的桥梁。

7.3 股权属性

EMC 代币是以环境监测平台为其使用场景之一的虚拟数字货币，持有该代币的用户拥有环境监测平台的股权。但需要说明的是，代币并不是一种投资。

7.4 去中心治理模式

在去中心化治理系统中，任何决定都要在一个固定时间内完成投票，这个时间根据提议内容不同而发生改变。当且仅当收集到足够高权益的投票，提议才会执行，否则提议将会关闭。在去中心化自治系统中，并不是权益高者的一言堂，权益低者可以联合在一起制衡权益高者。去中心化自治内容包括但不限于用户注册、统计函数、抵押标记范围等，这些升级可以通过自治系统参与者共同投票参与决定。

八 EMC 实现发展规划

8.1 初期规划

本项目的核心在于区块链技术的应用与环境监测的融合，因此前期的工作重点在于平台的开发，在市场调研以及分析的基础上形成自己独特的商业模式。与此同时，发布白皮书、启动早期投资，实现 EMC 的搭建。同时，其他商盟、区块链、数字加密也将同步启动。

8.2 中期规划

平台搭建完成，资金募集到位，随后必须要充分利用公司资源，结合已有的商业模式开始试运营，同时面向目标客户进行推广，寻求更多更优秀环境监测的版权持有者加入平台，这样才能活跃整个平台氛围，为平台引入更多的流量。此外，开启分叉平台的搭建，确保主平台平稳运行。

8.3 未来规划

EMC 平台需要不断的完善用户信用体系，开发组织多语言平台，进行全球化环境监测产业协同运作，打造一个万亿级全球环境监测产业发展生态圈。与此同时，还将联系更多海外区块链交易所，积极推进海外 EMC 的上线计划，提升 EMC 项目的国际影响力。在交易所上线后，EMC 团队以及理事会会持之以恒的进行区块链技术的深度开发，同时维护区块版权行业生态的和谐发展。

九 EMC 理事会

9.1 理事机构

为确保 EMC 项目的公开和透明，EMC 通过设立最高决策机构——决策委员会进行管理。决策委员会下设业务委员会、技术委员会、综合事务委员会以及社区发展委员会，管理机构将由开发人员和职能委员会组成。决策委员会成员每届任期为两年，首届决策委员会成员由核心团队成员、区块链行业知名人士、法律专家和早期投资者组成，后续的决策委员会部分成员由社区选举产生。

9.2 理事监管

为了保证平台高效、透明、健康的运行，必须要对整个平台的活动进行监管。由于区块链技术的应用，平台所产生的各种数据都会被记录且无法篡改，因此一方面 EMC 平台可以自行内部监管，自主互信；另一方面，平台设置 EMC 自治委员会，对投资者社区大会负责，负责对其行使管理和监督的职能，两重监管保证平台以及平台利益相关者的利益。自治委员会每年根据所持代币的数量和币龄进行换届。

此外，理事会要设立审计、法律、财务等顾问，以报告、新闻的形式进行定期与不定期信息披露。理事会主要负责人的联系方式必须公开，接受各方的联络与监督。此外，理事会通过监督与报告双向通道，欢迎环境监测协同平台用户、使用者、投资者共同参与管理、监督运营，对平台运营过程中的问题、重大危机、欺诈、舞弊等问题进行举报，同时必须确保举报人的信息保护。

十 EMC 发行计划

10.1 发行方案

项目简称：EMC 环境监测链

英文简称：EMC

发行总量：发行总量恒定为 1.88 亿枚。

接收币种：ETH。EMC 是基于以太坊 ERC2.0 技术发行的去中心化区块链数字资产。

10.2 发行细则

EMC 发行细则如下：

交易回馈 70% 1.316 亿 所有用户在交易 EMC 的过程中即可开启交易挖矿机制，部分交易回馈以 EMC 的形式返还给用户，让用户真正受益于 EMC 项目，并且自发推动；

市场奖励 20% 3760 万 针对行业内的知名顾问专家，可以对 EMC 团队提供指导和帮助，有助于 EMC 平台健康发展的，以及 EMC 的运营，包括开发，市场，财务，推广基于 EMC 平台的场景落地；

基金会+技术持有 10% 1880 万 用于基金会持有和奖励开发团队等对 EMC 平台做出技术，业务贡献的人，维持 EMC 技术团队和社区持续研发；

汇总 100% 1.88 亿

十一 风险提示

数字货币投资作为一种新的投资模式，存在各种不同的风险，潜在项目参与者需谨慎评估投资风险及自身的风险承受能力：

数字货币销售市场风险

由于数字货币销售市场环境与整个数字货币市场形势密不可分，如市场行情整体低迷，或存在其他不可控因素的影响，则可能造成数字货币本身即使具备良好的前景，但价格依然长期处于被低估的状态。

监管风险

由于区块链的发展尚处早期，全球都没有有关数字货币分配与发放过程中的前置要求、交易要求、信息披露要求、锁定要求等相关的法规文件。并且目前政策会如何实施尚不明朗，这些因素均可能对项目的投资与流动性产生不确定影响。而

区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则 EMC 应用可能受到其影响，例如法令限制使用、销售数字货币有可能受到限制、阻碍甚至直接终止 EMC 应用的发展。

竞争风险

随着信息技术和移动互联网的发展，以比特币为代表的数字货币逐渐兴起，各类去中心化的应用持续涌现，行业内竞争日趋激烈。但随着其他应用平台的层出不穷和不断扩张，社区将面临持续的运营压力和一定的市场竞争风险。

人员流失风险

EMC 聚集了一批在各自专业领域具有领先优势和丰富经验的技术团队和顾问专家，其中不乏长期从事区块链行业的专业人员以及有丰富互联网产品开发和运营经验的核心团队。核心团队的稳定和顾问资源对 EMC 保持业内核心竞争力具有重要意义。核心人员或顾问团队的流失，可能会影响平台的稳定运营或对未来发展带来一定的不利影响。

资金匮乏导致无法开发的风险

由于创始团队筹集的数字货币价格大幅度下跌或者开发时间超出预计等原因，都有可能造成团队开发资金匮乏，并由此可能会导致团队极度缺乏资金，从而无法实现原定开发目标的风险。

私钥丢失风险

代币购买者在把代币提取到自己的数字钱包地址后，操作地址内所包含内容的唯一方式就是购买者相关密钥（即私钥或钱包密码）。用户个人负责保护相关密钥，用于签署证明资产所有权的交易。用户理解并接受，如果他的私钥文件或密码分别丢失或被盗，则获得的与用户帐户（地址）或密码相关的代币将不可恢复，并将永久丢失。最好的安全储存登录凭证的方式是购买者将密钥分开到一个或数个地方安全储存，且最好不要储存在公用电脑。

黑客或盗窃的风险

黑客或其他组织或国家均有以任何方法打断 EMC 应用或功能的可能性，包括但不限于拒绝服务攻击、女巫攻击、游袭、恶意软件攻击或一致性攻击等。

未保险损失的风险

不像银行账户或其他金融机构的账户，存储在 EMC 账户的资产通常没有保险保障，任何情况下的损失，将不会有任何公开的个体或组织为你的损失承保。

核心协议相关的风险

EMC 平台目前基于某个特定的链开发，尽管 EMC 团队会挑选目前最安全稳定的区块链作为基础设施，但该链发生的任何故障，不可预期的功能问题或遭受攻击都有可能导致代币或 EMC 平台以难以预料的方式停止工作或功能缺失。

系统性风险

软件中被忽视的致命缺陷或全球网络基础设施大规模故障造成的风险。虽然其中部分风险将随着时间的推移大幅度减轻，比如修复漏洞和突破计算瓶颈，但其他部分风险依然不可预测，比如可能导致部分或全球互联网中断的政治因素或自然灾害。

漏洞风险或密码学加速发展的风险

密码学的加速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给 EMC 平台，这可能导致代币的丢失。

不被认可或推广不力的风险

代币不应被当做一种投资，虽然代币在一定的时间后可能会有一定的价值，但如果 EMC 不被市场所认可从而缺乏使用者的话，这种价值会变得很小。有可能发生的是，由于任何可能的原因，包括但不限于商业关系或营销战略的失败，EMC 平台将不能取得成功。如果这种情况发生，则可能没有后续的跟进者或少有跟进者，显然，这对本项目而言是非常不利的。

无法预料的其他风险

基于密码学的数字货币是一种全新的技术，除了本白皮书内提及的风险外，还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其他风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。

十二 免责声明

本文档仅作为传达信息之用，文档内容仅供参考，不构成在 EMC 平台中出售股票或证券的任何买卖建议、教唆或邀约。本文档不组成也不理解为提供任何买卖行为，也不是任何形式上的合约或者承诺。

鉴于不可预知的情况，本白皮书列出的目标可能发生变化。虽然团队会尽力实现本白皮书的所有目标，所有购买 EMC 的个人和团体将自担风险。文档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。

本文档仅供主动要求了解项目信息的特定对象传达信息使用，并不构成未来任何投资指导意见，也不是任何形式上的合约或承诺。

EMC 明确表示不承担参与者造成的直接或间接的损失包括：

（1）参与者一旦参与 EMC 代币分发计划，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后果。项目团队明确表示不承诺任何回报，不承担任何项目造成的直接或间接损失。

（2）本项目涉及的代币是一个在交易环节中使用的虚拟数字编码，不代表项目股权、收益权或控制权。

（3）由于数字货币本身存在很多不确定性 (包括但不限于：各国对待数字货币监管的大环境、行业激励竞争 , 数字货币本身的技术漏洞)，我们无法保证项目一定能够成功，项目有一定的失败风险，本项目的代币也有归零的风险。

（4）虽然团队会努力解决项目推进过程中可能遇到的问题，但未来依然存在政策的不确定性，大家务必在支持之前了解区块链的方方面面，在充分了解风险的前提下理性参与。

团队将努力实现文档中所提及的目标，但基于不可抗力的存在，团队不能做出完全承诺。在适用的法律允许的最大范围内，对因参与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。