融云链

D C A R

全球首个数字金融的通用超级银关

DESCARTES CHAIN

WHITEPAPER

CONCENT 目录

笛卡尔融云链的项目背景

1.1 金融——世界经济发展的核心

从公元前 2000 年的巴比伦开始，金融伴随着世界经济发展至今，到 2018 年为止，全球金融衍生品市场规模超过 600 万亿美金。 金融是现代经济的核心，为世界经济良性循环发挥不可忽视的作用。 货币资金作为一种重要的经济资源和财富，已成为整个社会经济生活传播的生命线和媒介。 几乎所有的现代经济活动都与货币和货币活动密不可分。

1.2 金融数字化发展的四大阶段

1.2.1 实体金融

实体金融的特征是，传统经济环境中经营金融产品的特殊行业。金融业起源于公元前 2000 年的巴比伦圣殿和公元前 6 世纪的希腊圣殿，以及用于支付利息的贷款业务。经过长期的历史演变，现代金融业逐渐由相对单一的古代社会形式演变为各种金融机构。在现代金融业中，各类银行占主导地位。商业银行是现代银行业最早也是最典型的形式。 除银行外，现代金融业还包括各种相互合作的金融机构，金融公司，贴现公司，保险公司和证券公司。 财务咨询公司，专业储蓄交易机构，典当行，黄金和白银行业，金融交易所和信用评级公司。

1.2.2 金融电子化

金融电子化的特点是利用现代通信技术，计算机技术和网络技术来提高传统金融服务的效率。降低运营成本，实现金融服务自动化处理，信息业务管理，科学决策财务，为客户提供更快，更便捷的服务。 达到提升市场竞争力的目的。在 20 世纪下半叶，金融电子商务随着电子技术的发展及其在金融业的广泛渗透而蓬勃发展。 它的出现不仅大大改变了金融业的面貌，扩大了服务业的种类，而且也在不断改变着人们的经济和社会生活方式。如今，所有社会组织和个人自觉或不自觉地直接或间接地意识到金融电子的存在，并享受他们提供的服务。

电子金融的出现导致了财务规则和效率的巨大变化。各个金融产品之间、金融产品与用户之间、金融与管理者之间仍旧未达成顺畅的沟通协作，互联网金融应运而生！

1.2.3 互联网金融

互联网金融融合了互联网技术和互联网精神与金融的核心功能，大大降低了成本。 减少信息不对称，使包括普通个人和企业在内的消费者享受到更好的普惠金融服务。

互联网技术包括大数据和云计算等新兴技术，这些技术将推动互联网充分利用“链接红利”。

互联网的精神在于平等，开放，透明和共享。根据诺贝尔经济学奖获得者罗伯特默顿的观点，核心金融职能包括资源分配，支付结算，风险管理，价格发现，资源和所有权划分以及创造激励措施。

另外，无论服务提供商是互联网公司还是传统金融机构或其他机构，只要符合上述互联网金融的描述，就可以将其归类为互联网金融类别。

互联网金融是跨界融合的产物，呈现出与传统金融不同的特征。

首先，物种蜕变，即打破了固有行业的形态或边界。 如果我们说金融是一个生态系统，互联网金融基因的植入将导致不同金融业务形式的界限变得越来越模糊。 “金融与非金融”与“金融与金融”之间的“行业跨界整合”已成为常态。 传统金融服务模式下不存在的许多“新物种”不断涌现。

其次，物种多样性，即商业模式，呈现出极其丰富的差异。 以众筹为例。以股权为基础的众筹项目将投资项目的股权作为回报，甚至是不提供回报的慈善众筹项目。

第三，物种的进化本质，即产品迭代速度大大加快。即使是一些已分类的互联网金融业务，内涵也会不断刷新。 以支付为例，二维码，声波支付，NFC，信标，生物识别支付等新型支付模式纷纷出现，线上与线下的界限也被打破。

简而言之，金融生态系统正在从一个相对分割的，静态的，模块化的工业时代迅速转变为融合， 动态和“分子化”（相对模块化，可以从一个更微小的维度划分）金融业务形式很难被分类， 即使被归类，他们也经常快速变化。

互联网金融本质上遵循的仍旧是传统金融承袭下来的规则与条例，仅仅从信息处理层面提高效率，但中心化的金融运行并非是最优的解决方案，大量第三方介入保障在提高效率的同时更加浪费了成本，从底层逻辑上改良金融的运行方式，区块链成为了新的选择。

1.2.4 数字（区块链）金融

互联网是为了解决信息快速传递的而发明的。但是，这种信息传输网络并没有保护有价值信息的内在机制。 我们不能点到点的传递包含所有权的信息。一些传统行业（如唱片行业和出版行业）因互联网的诞生而受到重创。 尽管各国政府越来越多地保护在线内容的版权，但从技术角度来看，仍然难以消除侵权问题。

从电子货币的诞生和发展的角度来看，尽管我们已经设法让货币以数字形式高效地流通，但这种数字化仍然是非常基础的。我们不得不依靠大量的第三方中介机构来确保电子货币的流通，这种方式提高了交易成本，比如手续费，还伴随着中心化的隐患。

区块链就是在这样的背景下诞生的。由于信息和价值是密不可分的，我们拥有一个全球高效和可靠的信息传输系统，这将不可避免地要求一个与之匹配的高效和可靠的价值传输系统。换句话说，区块链的诞生并不是偶然的，其背后有一个深刻的逻辑。 “区块链”这个名字可能是偶然的，但真正的区块链系统的诞生是不可避免的。

信用是制造货币的真正原材料。而区块链通过构造一个可以量化信用的经济系统，使得一个点对点的电子现金系统——比特币的出现成为可能。或者说，区块链创造了一个数字化的、可以点对点传输价值的信用系统。

1.3 数字货币兴起——数字金融萌芽的雏形

比特币早已经不是唯一的基于区块链技术的数字货币。据统计，截止到2018.3，发布的数字货币并且上较大平台的就有 1700 余种。

事实上，自比特币诞生以来，其模仿者或竞争对手纷纷涌现。 其中许多只是简单的复制和模仿比特币。 还有一些不是简单的模仿，有自己的创新和关注领域。就数字货币的市场价值而言，尽管比特币遥遥领先，但随后推出的以太坊和瑞波币的市场价值现在已超过 100 亿美元。

数字货币是目前区块链创造的使用最广泛也是受认可程度最高的一类应用。以比特币为代表的数字货币一度成为区块链的代名词。可以预期的是，即使在区块链广泛使用的未来，数字货币也仍然会是最为重要的区块链应用之一。

数字资产和区块链具有天然的亲和性。从一般意义上讲，数字资产包括任何以二进制格式存在并拥有所有权属性的资产。从狭义上讲，数字资产是指以电子数据形式存在的非货币资产，并在日常生活中出售。 比较典型是股票、债券等金融产品。

另外，由于区块链的公开，透明和难以篡改的特点，可以为任何现有数字资产或有价值的信息，作可靠的存在性证明，以及各种形式现实资产的登记或转移。这方面的应用可以包括产权，版权，公证和许多其他领域。

1.4 数字资产现阶段面临的重重困境

1.4.1 高居不下的交易成本

由于存在中心化的运营主体，中心化交易所会产生高昂的交易成本，而这些成本会加倍的从用户手中收取， 中心化交易所的交易成本主要由市场供给和监管政策决定。 它可以根据运营策略制定费率调整规则。 为鼓励用户进行高频交易，他们甚至可能不收取交易费，但他们通常会收提取资产的手续费。大多数交易所采用 IOU 会计方法。 交易所内部的挂单和成交，都是用平台的 IOU 来记录的，所以从技术上看交易成本是非常低的。（IOU： I OWE YOU 的简称，类似银行券的存在）

1.4.2 极低的应用效率

比特币和大多数区块链的设计只考虑交易，并不支持其他资产的定义或定义复杂的交易逻辑。如果你想添加新的功能，你必须升级系统，但困难在于完全分散的系统，比如比特币，任何变化都需要社区的一致同意，快速变化是非常困难的。

大部分变更本身是不必要或无法达成共识的，因为更多的灵活性往往意味着复杂性的增加和稳定性的降低。鉴于实际需求的多样性，甚至有些要求彼此冲突，区块链注定不会同时满足所有要求。

1.4.3 中心化的反规则控制

目前区块链领域火热，一批早期投资者积累到了第一桶金，财富效应带来了大批新的投资者， 这些投资者大部分并没有投资经验与良好的判断能力，再加上目前各个国家并没有相关的监管， 使得很多庄家可以恶意操纵币价，一个币种可在一天内有多达数倍的涨幅或者跌幅， 更有甚者在一天内 1500 倍跌幅的情况出现，在二级市场不断地完成收割，这种背后的高度波动，投机行为，洗钱和腐败问题引起了各国的高度关注。

1.4.4 与现实金融的隔绝

传统金融体系对数字金融崛起的抵制是源于“金融脱媒”的恐惧。 “金融脱媒的罪魁祸首”不是互联网和区块链，是原有金融体系的低效率，新技术只是“金融脱媒”的助力。任何经济体都存在效率问题，只有在市场化程度较高的环境中，引入充分竞争，市场参与者才会积极寻求改善; 在一个充满“金融抑制”的环境中，金融资源的配置并不完全符合市场机制 ——谁最需要它且能创造比别人多的价值，就会优先获得金融资源。 而是根据动力机制 ——按照分配者对资源的控制程度，以及分配对象与分配者关系远近来分配，这使得效率问题的改善自然遭到拒绝。“金融抑制”越严重，“金融脱媒”的欲望越强，创新的遭遇的抵制就越强; 这也意味着一旦实现“金融脱媒”，其规模和影响力也是前所未有的。虽然它们都是传统金融的替代品，互联网金融是一种渐进的改变，实现了“金融半脱媒”。 区块链技术是一种颠覆式的替代方案，它可能成为“有媒金融”的终结者。依赖垄断地位坐享收益的时代将成为历史。

1.5 数字金融崛起的趋势与时机

1.5.1 信用的可计算性

区块链是比特币的底层技术和基础设施。比特币是一种点对点电子现金系统，不依赖任何第三方。 通过密码学技术，中本聪构建了一个非常精巧的经济生态。 解决了在分布式结构下如何建立值得信赖的价值传输系统的难题。

香农是信息论的开创者，解决了 “如何用数学方法定义信息”这个关键问题允许以比特为单位对信息进行量化并且可以准确计算，从而奠定了数字通信的理论基础。 区块链技术的诞生解决了另一个巨大的问题 - 如何使用数学方法来定义信用。

在经济学领域，信用作为风险因素被定义为一个主体评估另一个主体采取特定行动的主观概率水平。对建立信用关系的前提假设，不同的学者看法不同，主要分歧是信用是否具有可计算性。

当有不同的选择时才可能出现信用问题。 当一个主体面对另一方具有大概率作弊的风险，就是信用出现的场合。从这个意义上讲，信用是一种行为策略，而行为策略的选择似乎可以从数学和游戏的角度来计算。最容易想到的是，只要潜在收益与信用活动概率的乘积大于潜在损失与不可信行为概率的乘积，信用就是占优势的行为策略。1990 年，科尔曼以代数方式提出了这种计算方法。

尽管有许多学者持有信用可计算的观点，他们也给出了信用计算的不同概念和方法，但他们都不能解决一个问题，即可操作性不强。另一诺贝尔获奖学者赫伯特·西蒙在他的文章中指出： 归根结底，人们是有限理性的社会动物。如果我们考虑到社会环境的多样性以及个人不是绝对理性的事实，那么我们会发现所谓的信用并不是一个单纯的计算概念，因此社会层面的信用行为也不能总是被单纯地简化为基于计算的主体间的相互影响。

或者我们可以说信用不是无法计算，只是我们还没有建立一个可以准确计算它的环境或系统。 区块链技术为这解决一问题带来了曙光。

1.5.2 区块链的信用表达式

所谓信用的定义不是计算某个人或参与者的信用，而是计算信用行为（如交易）的可信度。或者计算信用行为未来违约（欺诈）的可能性。违约概率越低，行为的可信度越高;相反，违约的可能性越高，行为的可信度就越低。

从经济学的角度来看，解决这个问题的障碍实际上源于这样一个事实，即在违规发生之前，违规的成本和收益不能准确计算。区块链是一个使用数学算法构建的经济系统，它本身就是一个对每个人都公开和透明的系统。在区块链中，可以准确计算违约（欺诈）行为所产生的成本以及可预期的收益。

信用行为的可信度可以定义为违约成本与违约收入的比率（信用行为置信度=违约成本/违约收入）。对于区块链上发生的任何交易，此公式可用于推导出精确的结果。

从出生到现在，比特币已经历了七年的争论。在没有任何可信的第三方担保的情况下，没有发生严重的欺诈行为。主要原因是欺诈成本往往远大于预期收益。 这也与 Satoshi Nakamoto 在创建区块链时所做的计算和预测一致。显然，当欺诈行为的成本远远高于收益时，而且成本和收益都可以提前准确计算出来，任何理性的参与者都不会有欺诈的动机。

1.5.3 价值互联网

信息不对称是指交易涉及的各方拥有的可指导交易决策的信息。一般来说，卖家比买家有更多关于交易项目的信息。随着互联网的出现，新一代的通信渠道和几乎瞬时的传输速度使得人们更容易获得他们想要的信息。今天，互联网对商业界产生深刻的影响，正是因为它打破了信息的不对称。

但是，互联网在打破信息不对称方面还远未完成。传统互联网只有统一的信息传输层，没有统一的价值传输层。在进行交易（价值传递）时，仍然需要依靠大量的中介来确保价值安全地储存和转移。这些中介机构的存在不仅降低了价值传递的效率，同时提高了价值流通的成本。

建立统一的价值传播互联网络，即价值互联网，是区块链发展演变的必然结果。价值互联网会完全消灭信息不对称，允许货币和数字资产的价值数字化，不再借助大量的中介机构。 数字资产能够在全球自由流通。市场效率会实现质的飞跃，甚至彻底改变当前的金融和经济格局。

1.5.4 基础协议与分层结构

本质上，互联网就像区块链一样是一个分散的网络，没有“绝对的中心”。不同之处在于互联网是一个高效的信息传输网络，它不关心信息的所有权，没有对有价值信息的内在保护机制。区块链是可以转让所有权的协议，将基于现有的互联网协议架构构建新的基础协议层。从这个角度来看，区块链（协议）将成为下一代互联网基础协议之一。

理应认识到，区块链是一个多层级的复杂系统。就像 TCP / IP 堆栈的分层结构一样，不同的层承载不同的功能。人们在统一的底层协议的基础上开发了各种应用层协议，最终构建了丰富多彩的互联网。

未来，不同层次和不同类型的区块链扮演不同的角色。我们相信未来区块链还将在统一的底层协议的基础上开发各种应用层协议，从而构建多元化的生态价值互联网。

1.5.5 颠覆性技术的发展曲线

变化常常促使人们放弃偏见并产生新的思考。

区块链的崛起将颠覆大部分人的固有认知，人们缺乏指数思维，对于新事物的发展，我们经常误判，高估其短期影响，低估其长期影响。 就像 2000 年互联网泡沫的崩溃一样，互联网被认为可以改变一切，无数资本追捧。突然间， 大家发现互联网并不是那么神奇，纷纷离去，互联网概念从云端跌进泥里。然而，有多少人能想到，仅仅十几年后，互联网摧枯拉朽般地改变了人类的商业模式，金融业态和生活方式。

笛卡尔融云链项目介绍

2.1 为什么要设计笛卡尔融云链?

1.项目技术的创新性

虽然跨链技术是众所周知的，但目前还没有项目被社区普遍认可和使用，因此被视为不成熟的技术。 就稳定性和安全性而言，它仍不能与传统的公链技术相媲美。有些项目提出用跨链或侧链作为解决方案，但推进落地者寥寥无几。

2.技术上实现的可能性

分析该项目的关键是看其技术实施的可行性。 跨链技术的实现需要复杂的机制设计和跨链智能合约编程能力， 投资的一个项目，关键要看项目在跨链技术下能否稳定运行。

3.与同类项目进行对比有明显的优势点

尽管只有有很少的项目落地，但可以看出，使用跨链侧链技术的项目通常是相似的机制。 使项目脱颖而出的关键是其技术稳定性和项目进度。

4.经济激励模型的设计

一个项目能否长远的发展，首先应仔细考察其经济激励模型，是否足以支撑初期社区冷启动，在发展中能否不断地激励旷工参与，不断地发展提升项目整体的价值，在后期形成正向反馈生态。

5.社群运营能力

从长远来看，项目的发展速度更多取决于团队是否具有社区运营能力，是否能够通过社区形成网络效应，并提高项目用户量。

6.服务质量是否能达到商业级别

存储可靠性，服务可用性，最终都需要由实际市场需求的验证。目前，大多数跨链项目和应用程序远没有商业可用性。 如何设计适合的智能合约。提出优秀解决方案的项目，势必成为这个行业的领袖项目。

2.2 什么是笛卡尔融云链?

笛卡尔要建立数字金融时代的超级公链，希望打破各个区块链独立封闭的价值孤岛困境， 解决传统金融与数字金融无法相容的难题。笛卡尔提供完善的金融功能，支持记录元数据，充分释放各类资产的流动性， 发掘资产潜在价值。笛卡尔正在成为链接整个数字货币世界与传统金融世界的关键基础设施，促进全球数字金融生态茂盛生长。

2.3 逻辑与方法

区块链技术在很多领域已被证明其巨大潜力，比如金融，信息管理，分布式网络和存储，资产管理，政务管理... 但目前为止，真实世界中的商业体系并没有

快速采用这个新技术。可能的原因有很多，以我们的观点，主要有三个问题：

1.可扩展性不足： 今天，世界上最大的互联网公司，也在为每天快速增加的数据和交易信息所困扰， 数据和交易量过大，会造成网络拥堵，拥堵使网络服务变得缓慢又昂贵，按照当前的区块生成速度，距离服务商业级应用还非常遥远。

2..连通性不够： 每个公链在上线之前必须设计出完整的经济系统，矿工生态，原生币，DApps 等。每一个已存在公链都是数字资产孤岛，彼此之间无法通信，即使理论上行得通，实际想要在各个公链之间转移和支付数字资产也非常困难。缺乏跨链互操作性正是阻碍区块链技术被广泛采用的大难题。

3..可用性不高：已有的互联网服务在计算，存储，网络带宽几个主要方面已经可以满足人类大部分信息处理需求，但是区块链互联网受限于计算和存储能力，同时在标准化协议，编程语言体系，开发框架，应用生态等几方面，都非常初级，暂时难以承载传统互联网的所有业务。

以上三个问题，最迫切是连通性，要实现多种数字资产的自由转移，交换，支付必须解决跨链通信的瓶颈；其次是可扩展性，最后是可用性，提高可用性是一个长期的基础建设工作，传统互联网也不是短时间达到今天的技术水平。 行业内的顶尖技术专家，以及笛卡尔的研发团队已经投身研究这三大难题。

2.3.1 技术发展路径

如果你不了解过去，就无法理解现在，把握未来。 在 2016 年 9 月，Vitalik Buterin 发布了《Chain Interoperability》研究报告，归纳了 3 种跨链技术：

早期的跨链技术以 Ripple，BTS，Cybex 和 为代表，他们关注的是资产转移；采用公证人技术。

第二种跨链技术分两个方向，一是侧链，以 RSK， Bytom, Lisk 等为代表，锚定主链 Coin，解决主链可扩展性；其二是中继，以 BTC Relay，Polkadot，Cosmos 为代表，关注的跨链基础设施；

第三种跨链技术是哈希锁定，以闪电网络为代表，目的是提升比特币网络的链外交易处理能力，是当前应用最广泛的一种技术。

跨链互通的类型

- 中心化或者多重公证人机制，当一组可信的参与者在 A 链上发生某个事件的同时，就在 B 链上执行相应的操作
- 侧链/中继： 一个区块链内置可以验证和读取其他区块链中的事件和/或状态系统
- 哈希锁定：链间设定相互操作的触发器,通常是个待披露明文的随机数的 hash 值。

公证人机制

促进跨链操作的最简单的技术方式就是使用公证人机制； 根据 Vitalik 的定义，公证人的机制是指：

一个可信的个体或者由多个可信的个体组成的组织向 X 链声明 Y 链上某个事件的确发生了，或者关于 Y 链上的某个声明是有效的.

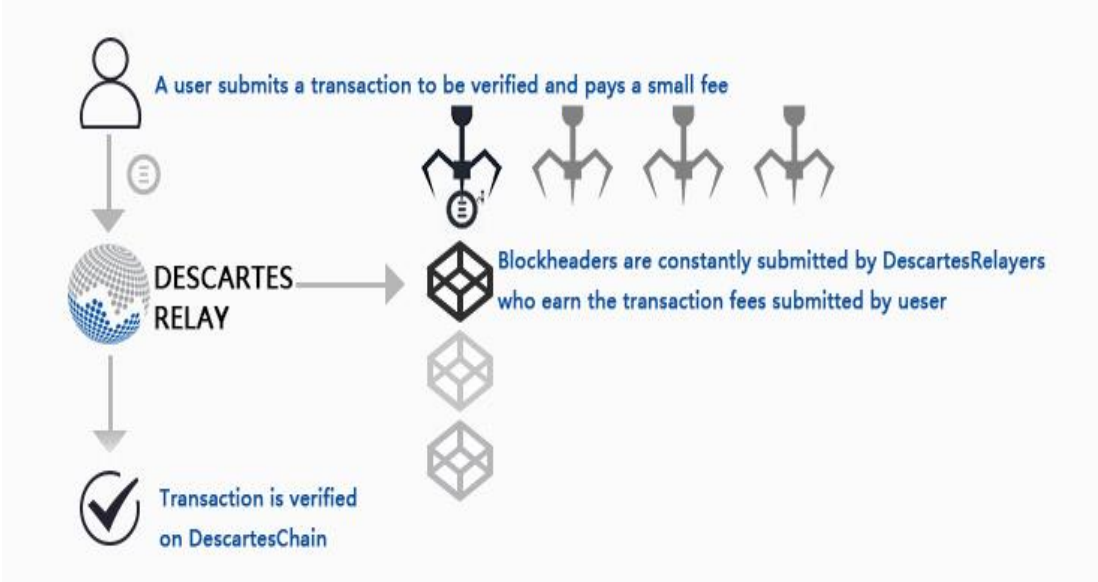
In a notary mechanism, a trusted entity or set of entities that is trusted as a group is used in order to claim to chain X that a given event on chain Y took place, or that a particular claim about chain Y is true.

这些可信的个体，可以主动监听并根据某些链中的事件自动触发相关操作，或者被动调用，发布签名消息。 简单的来说，就是通过第三方 “连接器” 或 “验证器” 互相自由地传输货币,来实现不同链上的资产转移。典型代表有:瑞波 Interledger 协议 执行的流程：

1. 公证人选举: 公证人由参与者选择；
2. 发起提案：发起者发起提案,所有参与者验证账本；
3. 制备: 通过托管机制实施账目移交。发起者首先授权,连接者依次托管；
4. 执行阶段: 参与者签名交易收据,并且提交给公证人,公证人通过拜占庭协议,确认交易

中继技术

相对于依赖可信的中介来传达链与链之间的信息，促进跨链互通更直接的方法是通过中继链。具体的实现流程：



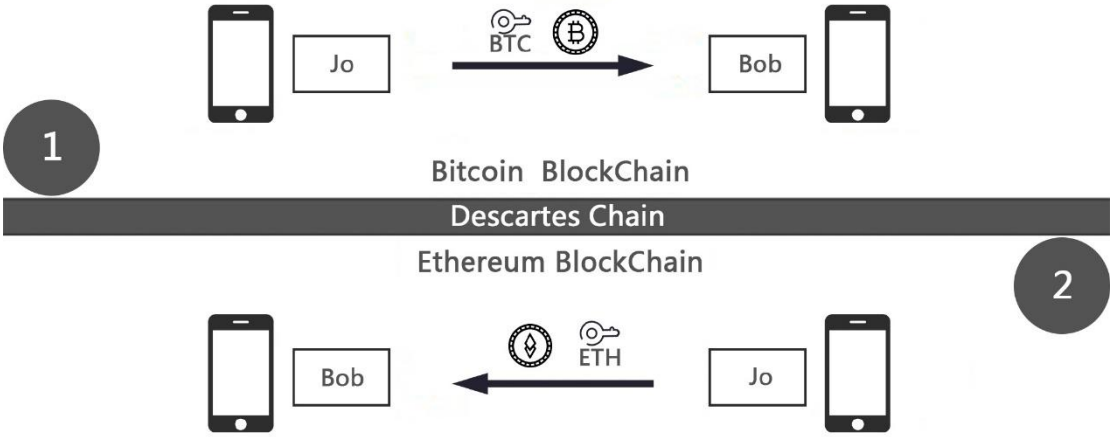
侧链/中继技术是基于新链条实现锚定主链上的令牌，从而实现资产转移，交易验证和信息交换功能。 典型代表有: BTC Relay、Polkadot、COSMOS 等

1. 主链交易：主链发起跨链交易,标明目标链,金额和接受方地址
2. 侧链监听,验证： 侧链收到事件,对该交易进行主链认证。通过轻客户协议,读取区块头,然后使用 Merkle 树进行密码认证交易
3. 在侧链生产相应的资产,用于流通
4. 反方向进行通过销毁资产,实现资产返回主链

哈希锁定

除上述的技术外，还有一种在区块链无须了解其他链太多的情况下实现跨链互通原子性操作的技术。 建立相互操作的链间触发器，通常是要公开的明文的随机数的散列值。 兑换赎回的机制是通过锁定原始散列值一段时间。 哈希锁定起源于比特币闪电网络 下面通过跨链数字资产交换的案例来阐述该机制实现方式:

1. A 生成随机数 S，并发送 hash(S) 给 B;
2. A 锁定资产，并设定条件：如果在 2X 时间内 A 收到 S,则转账给 B,否则退回给 A;
3. B 确认 A 的锁定和时间设定后，在 B 上锁定资产，并设定条件: 如果在 X 时间内 B 收到 S,则转账给 A,否则退回给 B;
4. A 在 X 秒内揭示 S，以便从 B 的合同中索取资产;
5. B 获知 S 允许 B 从 A 的合约中索取资产



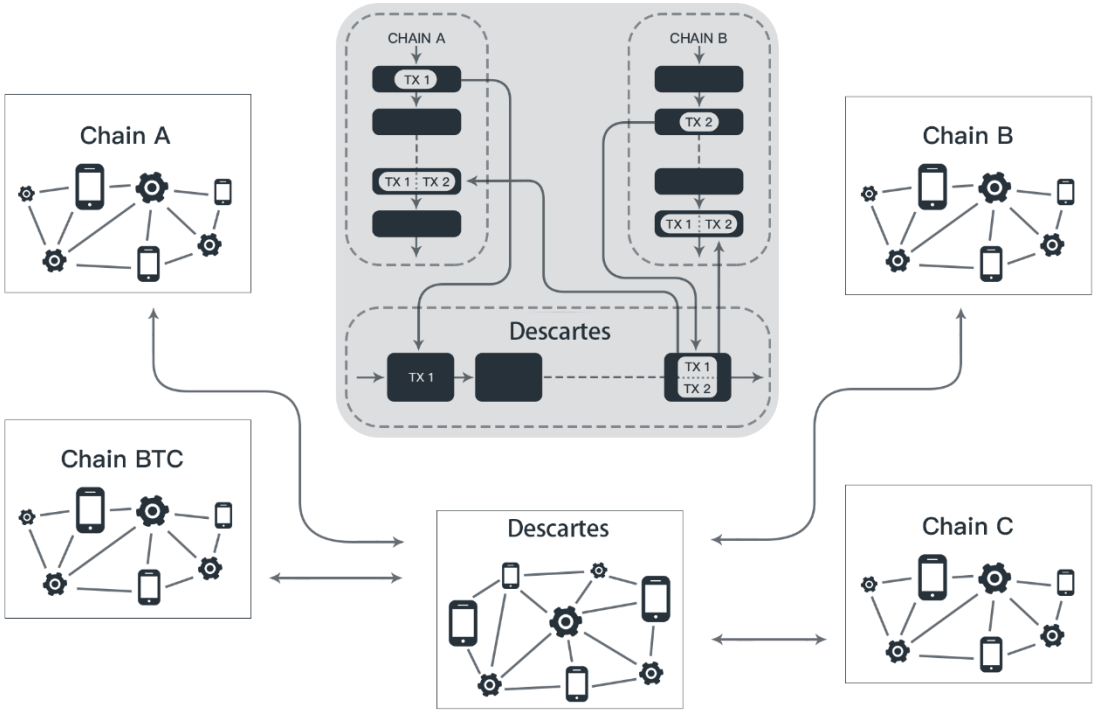
该机制的原子性是可证实的。如果 A 在 X 秒内揭示 S，则至少可以提供 X 秒的窗口可以让 B 来声明它们的的资产。 A 可能犯错导致延迟揭示 S，导致自己不能取回资产，然而这往往是 A 自己的错误，并且可以简单避免。如果 A 在 X 秒 到 2X 秒之间揭示了 S， 那么 A 无法获取他的资产，但 B 可以，这同样也是 A 的错； 如果 A 在 2X 秒之后，甚至不揭示 S，那么 A、B 两方各自取回自己的资产。 如果 A 不锁定自己的资产，那么 B 也不会锁定它的资产。如果 B 不锁定他的资产（或者在指定时间内锁定失败），A 可以选择不揭示 S，这样 A 可以取回自己的资产。

2.3.2 笛卡尔跨链解决方案

传统世界的资产转移到链上，跨链互通至关重要，但并不容易实现，因为每个链都有自己的网络协议， 通信标准和共识机制，而且这些模块尚在完善之中，想要在这些链之间移动资产，我们尝试了中继系统， 公证技术，原子交换，哈希锁定技术等，目的是寻找一个集中的解决方案，实现开发者， 用户，矿工和所有其他方达成了帕累托最优。 **所有的探索收敛于一个方向，即如何安全地授权多个无需信任的节点共同操作一个数字资产账户**，这也是笛卡尔融云链的技术核心。

- 保证数字资产的安全性
- 支持跨链智能合约编程
- 高鲁棒性
- 大规模金融应用的即时处理和响应
- 在满足系统自身规模扩张的情况下，不增加矿机节点的计算压力
- 跨链资产转移
- 跨链交易
- 所有权和使用权分离

针对上述需求，笛卡尔研发团队整合学术界前沿理论，开发出**分布式私钥生成和控制技术， 我们称之为 DKSC（分布式密钥安全分簇技术 Distributed Key Secure Cluster)，用 DKSC 生成原链的锁定账户， 不需要使用双向锚定方法，也不需要添加脚本扩展来识别和验证原始链上的 SPV 证据。 交易数据传回原区块链网络时，是符合其通讯标准和网络协议的合法格式，实现将跨链交易的核心流程和计算完全并入到笛卡尔链中完成。没有必要对原始链条的机制进行任何改变，因此无论现有的公有链或私有链，联盟链都能以较低的门槛接入笛卡尔链。降低跨链交易的成本，并自由映射每条链上的资产。



DKSC 分布式密钥安全分簇技术能够把个人或组织手中的数字资产控制权安全地转移到完全去中心化的区块链网络中。 密钥的产生和存储过程都是分布式的，没有任何一个节点可以获得完整的密钥，数字资产控制权的安全性得到保证，数字资产的安全就得到保证。 释放控制权的操作称为 Release，所有以密钥控制的数字资产都可以通过 Release 实现分布式控制和映射。 回收控制权的操作称为 Recycle， 它是 Release 的逆向操作，帮助用户回收控制权，解除资产映射。

DKSC 分布式密钥安全分簇技术能够把个人或组织手中的数字资产控制权安全地转移到完全去中心化的区块链网络中。 密钥的产生和存储过程都是分布式的，没有任何一个节点可以获得完整的密钥，数字资产控制权的安全性得到保证，数字资产的安全就得到保证。 释放控制权的操作称为 Release，所有以密钥控制的数字资产都可以通过 Release 实现分布式控制和映射。 回收控制权的操作称为 Recycle， 它是 Release 的逆向操作，帮助用户回收控制权，解除资产映射。

2.3.3 关键技术

高连接性网络分簇算法

区块链的底层是 P2P 分布式网络，通信特征是非周期性通信，任意单个节点都有全网广播权限，这带来 2 个问题：一是效率问题，耗时耗能低效；第二个是安全问题：如何判断节点诚实或恶意。

笛卡尔金融链不同于传统的网络通信方法，因为它使用了使用三角形的固有特性来确保连通性的分簇算法。 通过这种算法，网络中形成高度连接的骨干网络，减少了网络的路由表开销和整个网络的通信开销。

实施过程是这样的，在部署节点之前，节点由系统指定。网络消息通过广播进行初始化，整个网络被初始化，并由它启动分簇算法。当一个节点存在超过一

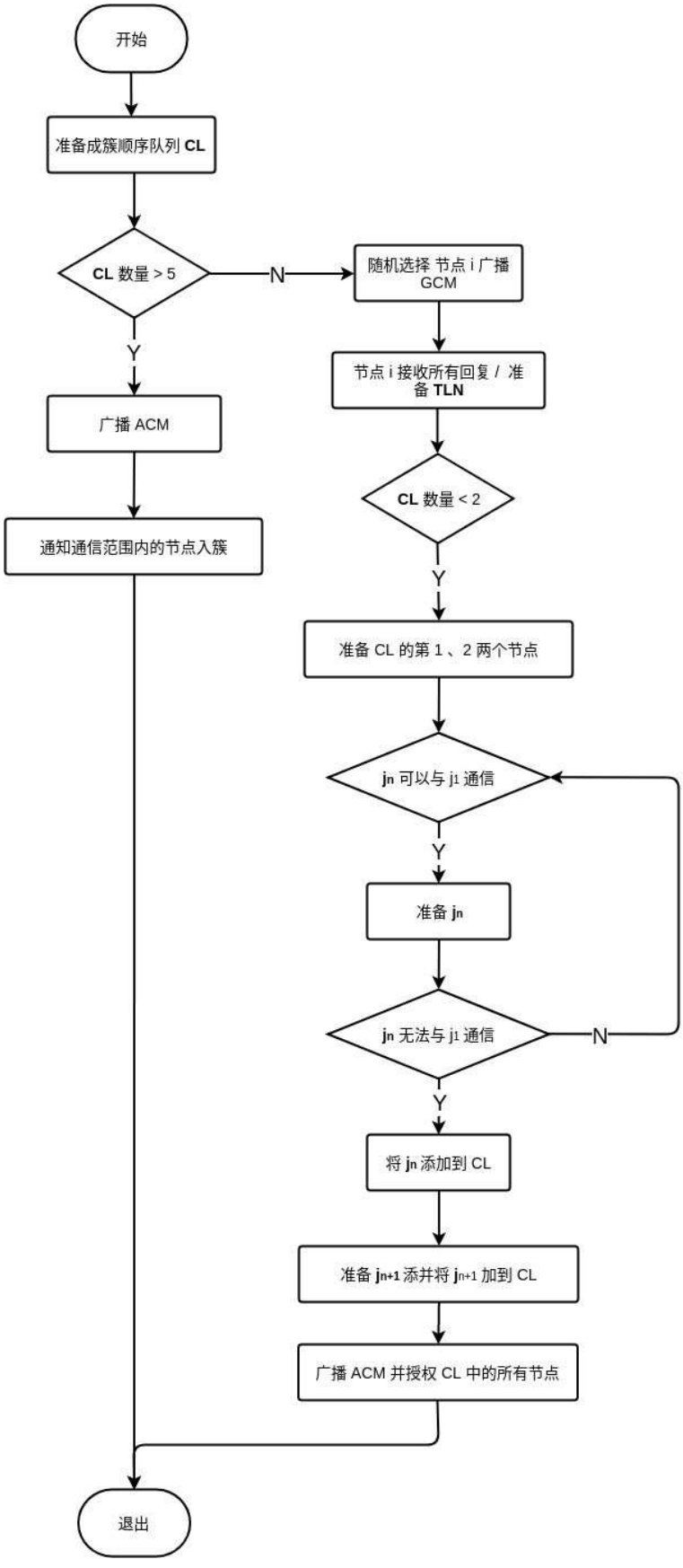
段时间，相邻簇头数量还未达到 3 个，节点进入补充节点并请求成簇，以确保整个网络中的任何非簇头节点都在 3 个簇头的通信范围内。 从而形成一种高连通的骨干网络。随着时间的变化，簇头节点消耗太多的能量，当该簇头节点能量低于一定数值时，进入簇头更新阶段，更换簇头节点，使网络保持正常工作水平。 该技术可以解决在满足系统自身规模扩张的情况下，不增加矿机节点的计算压力。

下面是核心算法，在算法描述过程中需要使用一些符号如表 1 所示:（ i 为当前广播 GCM 消息的节点)

符号	定义
LN(i)	i 的邻居节点列表
LN(i,j)	i 和 j 公共邻居节点
OM(i,j)=LN(i,j)	i 和 j 的重叠指数
GCM	成簇消息
ACM	通知入簇消息
CL	成簇顺序队列
TLN	临时邻居列表

分簇算法：

```
1) prepares CL and if CL' s size > 5 broadcast ACM  then exit
2) Node i broadcast the GCM
3) receives all replies or timeout then pre-
pares TLN
4) if CL' s size < 2 then prepares CL' s first and second node
5)     While(jn can communicate with j1)
6)          Prepares jn
7)          If jn cannot communicate with
8)                add jn into CL
9)          end if
10)    end while
11)    prepares jn+1 and add jn+1 into CL
12)    broadcasts ACM  and authorities permission to node in CL
13) end if
```


开始
准备成簇顺序队列 CL
CL 数量 > 5
N
随机选择 节点 i 广播 GCM
Y
节点 i 接收所有回复 / 准备 TLN
广播 ACM
CL 数量 < 2
通知通信范围内的节点入簇
Y
准备 CL 的第 1 、2 两个节点
jn 可以与 j1 通信
Y
准备 jn
jn 无法与 j1 通信
N
Y
将 jn 添加到 CL
准备 jn+1 添并将 jn+1 加到 CL
广播 ACM 并授权 CL 中的所有节点
退出

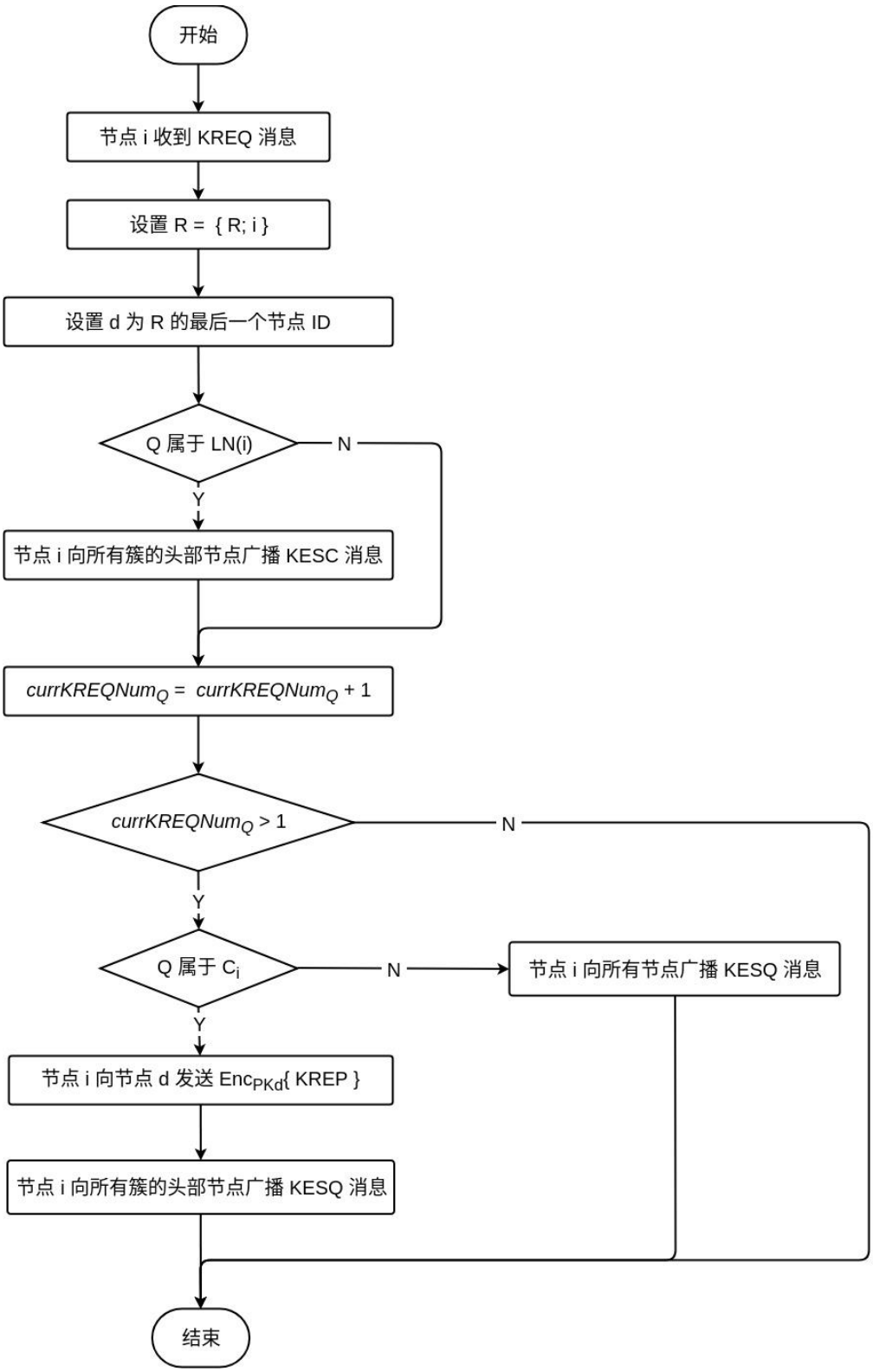
DKSCA （分布式密钥安全分簇算法）

由于公链是对开放的，不排除会有恶意节点加入网络。 笛卡尔采用一种安全的分簇算法，实现分布式密钥的生成和管理，加入网络各个节点都需要通过系统验证。 实现过程是这样的： 在所有簇头形成之后，广播的成簇消息包含它自己的公共密钥，接收到该消息的节点，保存其公钥，以确保整个网络中， 节点具有一跳内簇头节点的公钥。在部署系统之前，从密钥池中随机选择一些公钥存储。

节点的认证共分为 4 个阶段，并且对于广播消息均需要收到 2 条，节点才会对其处理并转发。 协议发起由簇头节点广播认证消息，使其 周边可互相通信的 3 个簇头节点发起协议，进入密钥搜索阶段。当网络中发现密钥，则根据来时路径返回密钥，此时进入应答阶段。当协议发起簇头节点验证签名并在数量上满足初始设定的门限值时， 广播密钥确认消息，协议进入确认阶段。而在整个认证协议执行过程中，如若发现异常情况，则立即进入协议终止阶段，防止恶意节点的攻击。

下面是核心算法，在算法的描述过程中使用到的符号如表 2 所示

符号	定义
Ski	节点 i 的私钥
PKi	节点 i 的公钥
Ci	节点中存储的公钥列表
R	消息传递的路由
{m}SK	对消息 m 使用 SK 的签名
EncPK{m}	对消息 m 用公钥 PK 加密
currKREQNumQ	关于 Q 的 KREQ 消息数量
SSN	协议发起簇头节点
S	请求节点
Q	请求公钥的 ID 号


开始
节点 i 收到 KREQ 消息
设置 R = { R; i }
设置 d 为 R 的最后一个节点 ID
Q 属于 LN(i)
N
Y
节点 i 向所有簇的头部节点广播 KESC 消息
currKREQNum_Q = currKREQNum_Q + 1
currKREQNum_Q > 1
N
Y
Q 属于 C_i
N
节点 i 向所有节点广播 KESQ 消息
Y
节点 i 向节点 d 发送 Enc_PKd{ KREP }
节点 i 向所有簇的头部节点广播 KESQ 消息
结束

```
DKSCA安全分簇算法：
1)  Node i receives a KREQ message
2)  d ← lastnodeIDinRandR←{R;i}
3)  if Q ∈ LN(i) then
4)        Node i radios KESC to all Cluster
Heads Nodes
5)        exit
6)   end if
7)   currKREQNumQ ← currKREQNumQ +1
8)   if currKREQNumQ > 1 then
9)        if Q ∈ Ci then
10)             Node i sends EncPKd{KREP} to node d
11)             Node i radios KREQ to all Cluster Heads Nodes
12)       else
13)          Node i radios KREQ to all nodes
14)       end if
15)   end if
```

网络安全性

网络安全威胁主要来自恶意节点攻击。不管攻击者是否知道密钥池信息，其想要通过簇头节点的认证，必须知道普通节点的 ID 并知道该 ID 对应的私钥信息。由于密钥对和 ID 之间没有直接关系，并且攻击者至多知道攻击中的公钥信息，所以不可能从公钥计算私钥。 因此，保证攻击者不能通过公钥获得私钥，从而保证攻击者不能伪造具有特定 ID 号的节点进行通信。

应用安全性

管理数字资产，实际就是管理私钥。以比特币为例，私钥的本质是一个随机数，比特币的私钥算法是对随机数运行 SHA256 运算生成长度为 256 位随机数。在前面加上版本号，后面添加压缩标志和附加校验码，然后再对其进行

Base58 编码，就可以得到 WIF(Wallet import Format) 格式的私钥。公钥由私钥经过椭圆曲线算法生成，比特币地址由公钥经过哈希函数(RPIEMD+SHA) 生成。
不论个人还是交易所，密钥都是完整储存在一个地方，可能是用户的电脑硬盘，它可能是提供钱包软件的第三方服务器，也可能是交易所服务器。 一旦发生黑客攻击，密钥泄露，丢失或者第三方监守自盗，都会造成用户的损失。

DKSC 技术不仅解决跨链通信难题，而且提高了数字资产的安全性，体现在两个方面：

- 密钥分片
  完整的钥匙被分成几个部分，每个部分被称为一个分片。 分片后的密钥从生成到存储、使用都不需要进行重组，从而使得在任何地方和任何时候都不会出现完整的私钥。
- 分布式存储
  分片后的密钥交给去中心化网络中的不同节点保管称为分布式存储。分布式存储的过程中，每个节点只会接触到密钥中的一个分片，任何单个节点或数个节点靠几个分片都无法重组出密钥，从而降低密钥泄露的风险。分布式存储密钥的方式，可以彻底避免发生被第三方恶意侵占的行为。

2.3.4 混合共识机制

以比特币为代表的 PoW 共识机制简单有效，但存在两大问题：

- 延迟高
  每笔交易的平均确认时间长达 10 分钟，最大支持每秒 2 位数的并发交易
- 浪费资源
  任何基于无需许可模型的共识机制，都要消耗额外的哈希算力来确保安全性，截止发稿时间，每个比特币交易的确认平均耗费 6 美元的电费。

笛卡尔融云链采用的是混合共识机制（Hybrid Consensus），因为混合共识机制解决了上述两大问题：

- 高速处理
  区块链上的交易速度上限取决于网络传输速率，不会有任何可见的限制
- 经济节约
  交易的确认由一组节点完成，能耗极低

笛卡尔融云链的混合共识机制将 PoW 和 PoS 融合在一起，分层运行。最底层是 PoW 矿工，负责确认交易信息，生成区块；顶层是 PoS 矿工，负责打包交易记录，并提交给 PoW 矿工处理。
每个节点通过运行一个随机的算法，判断自己属于 Pow 矿工或者 PoS 矿工，这个过程是自动完成，无需系统干预，确保选举机制公平可信，并且每 24 小时重选一次。 所有的 PoS 矿工 通过分簇技术，可实现全网交易信息的并行处理，每个簇处理的交易信息互不交叉，极大提高了笛卡尔链的交易处理能力，为部署大规模金融应用提供基础支撑。

2.3.5 反 ASIC 算法

区块链系统是依赖矿工运行的，他们查证交易记录，制造和储存所有的区块，并对写入区块链的区块达成共识。挖矿的本质是利用芯片进行「不完全哈希函数原像解谜」运算。这个算法的运算结果不是一个值，而是一个区间，芯片运算的结果落到这个区间内，就视为挖矿成功，当众多芯片参与运算的时候，成功就变成一个概率问题，大致上，在一个单位时间内，运算出符合条件谜底的概率，与芯片所贡献的算力成正比。 第一代矿工挖矿都是在普通的电脑上完成的，即利用 CPU 进行运算，CPU 用线性方式处理问题，所以矿工只能简单地按照线性的方式尝试所有的临时随机数，目前使用普通电脑的 CPU 进行挖矿已经无利可图了。 第二代矿工是意识到用 CPU 挖矿在做无用功，他们开始用显卡或者图形处理器（GPU）来挖。GPU 具有高吞吐量和高并行处理功能，这两点对挖矿都非常有利，哈希解谜存在大量的并行处理，因为你需要同时用不同的临时随机数计算多个哈希值。但是 GPU 挖矿有有许多缺点，缺乏冷却处理设备，同时 GPU 非常耗电，这些问题迫使用花大价钱购买可以搭载大量显卡的特定主板。 第三代矿机出现于 2011 年，称为现场可编辑逻辑门阵

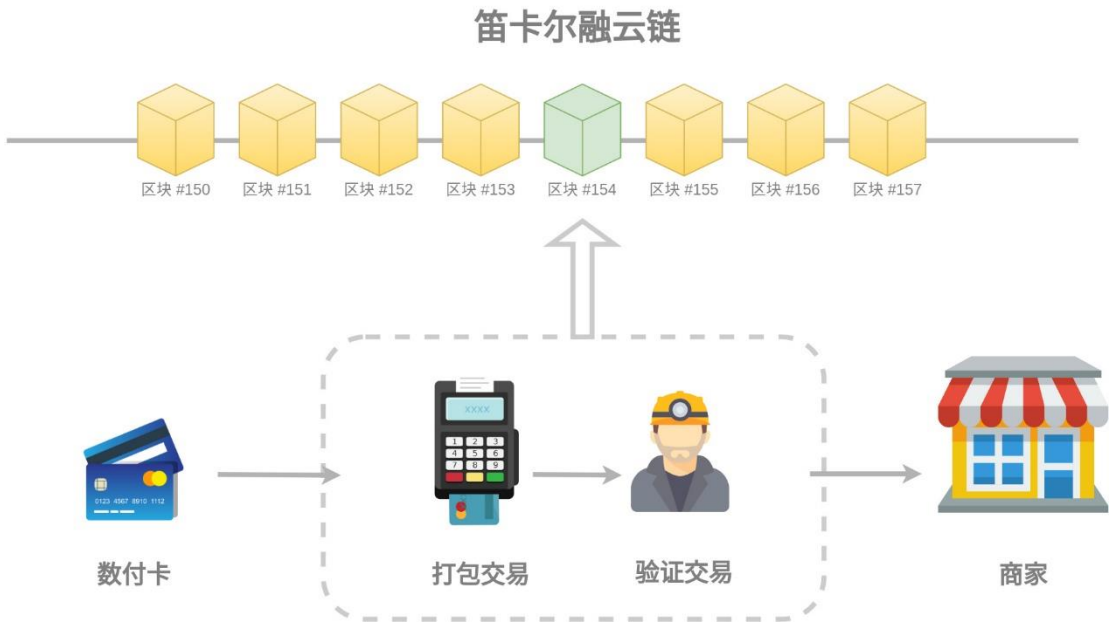
列（Field-Programmable Gate Array 简称 FPGA）。FPGA 的工作原理是在追求定制硬件的最佳性能的同时，用户可以现场调试或者修改硬件参数。相比之下，常用的硬件是出厂前就设计好的，出厂后无法更改定制，只能永远做同样的工作。FPGA 比 GPU 的性能好，更容易冷却，但因为 FPGA 操作门槛较高，不容易购买，在矿机历史上存在时间较短。 当今的挖矿市场主要被 ASIC（Application-specific integrated circuit 简称 ASIC)所主导，这些 IC 芯片被设计，制造，优化，只为了挖矿这一个目的。 ASIC 的出现使得挖矿从个人领域转移到大型专业挖矿中心，为了保持竞争优势，这些矿场公司大量采购更新的性能更高的 ASIC 矿机，而不是采购那些能直接出售给个人的矿机。现有的基于 POW 共识机制的加密货币，已经远离普通用户，只有购买专用的 ASIC 矿机才能参与挖矿，获得奖励。这产生了「后来者居上」,「资本主导」的局面，从长期看不利于数字货币普及和发展。笛卡尔链希望改变这种局面，我们设计一套反 ASIC 的算法。吸引普通用户参与挖矿，不需要太高的硬件投入，即可获得令人满意的奖励，同时避免形成硬件的军备竞赛，大量资金投入到算力升级的竞争中，对项目方和参与者都是毫无意义的。 现有的解谜算法（比如 SHA-256）在运算时只占用 256 位，可以很容易地放进 CPU 的注册机中，这为设计专用挖矿设备提供了基础。反之，我们将运算模块调大，使之不能轻易地放进 CPU 中，必须借助大量的内存来计算。这种方法我们称之为刚性内存解谜（Memory-Hard Puzzles）。 这种解谜算法只需要相对简单的算力但需要大量的内存，这就表示，解谜成本的上升速度将会跟内存速度的提升一样，维持在一个相对低的水平。不必担心有人会突然拥有超过 51%的算力对全网进行攻击。

2.4 应用场景

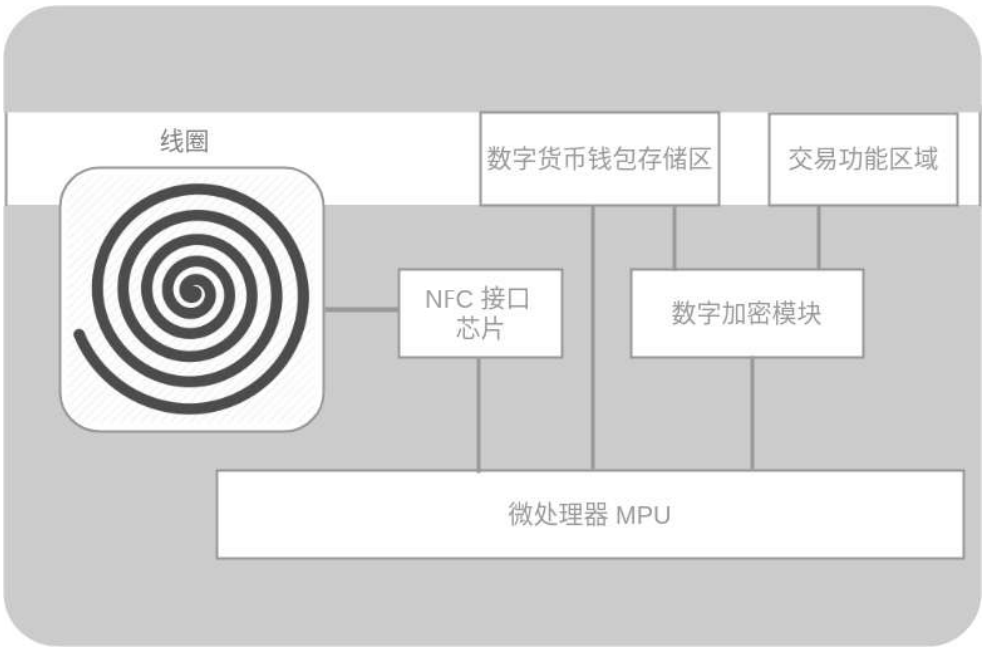
2.4.1 便捷支付

代表应用——数付卡

越来越多的商家正在接收比特币等数字资产作为支付方式。 对于用户来说，他们已经逐渐习惯和依赖电子货币。 银行卡已成为用户识别和参与交易过程的工具。 数字货币是电子货币的替代物，所以，笛卡尔链推出数字货币支付卡（简称数付卡），它是数字资产与银行卡完美融合的区块链金融服务。



笛卡尔融云链的用户只需持有数付卡，可在全球任何地方刷卡消费，商户的读卡器就是一个簇节点（即 PoS 矿工），能够即时处理该笔交易，将交易信息打包提交给距离最近的 PoW 矿工，矿工会在最新生成的区块信息中添加该笔交易信息，完成确认，整个过程在 1 秒内完成。



上图是笛卡尔数付卡内部结构，包括线圈，NFC 接口芯片，数字加密芯片，MPU 微处理器，数字货币存储模块。

用户的数字资产私钥存储在数付卡中，安全性至关重要，普通磁条银行卡的安全性极低，一个收银员就可以复制银行卡信息以创建复制卡。近年来，银行已经在借记卡和信用卡上加入了 EMV 芯片。 希望为刷卡交易提供额外的安全保护。 在最近的黑帽计算机安全大会上，来自 NCR 的安全研究人员已经证明，EMV 芯片卡可以像磁条卡一样轻松伪造。

数付卡使用 MPU 加密+ ASIC 加密，数据以密文形式存储在专用存储模块中。 即使入侵者从数据总线获取数据，也不可能知道密钥或其他敏感信息。这种保护措施可有效防范入侵和半入侵攻击。 每个卡总线加密密钥是不同的，所以即使入侵者完全破解，也不能生成具有相同密钥的芯片。 由于每个数付卡芯片都有一个唯一的 ID 号，因此不能购买具有相同 ID 号的数付卡。 在电路设计方面，数字支付卡将使用 ASIC 类逻辑设计标准模块结构，如解码器，寄存器文件。 这种设计方法称为混合逻辑设计。 混合逻辑使得不诚实的用户几乎不可能通过手动查找信号或节点来获取支付卡的信息而进行物理攻击。 大大提高了 MPU 内核的性能和安全性。 数付卡的读卡器采用 DKSCA 算法实现端到端加密，任何伪造的读卡器或被恶意篡改的读卡器所发出的交易信息，将不会被确认。 具体原理已在「2.3.3 关键技术」一节详细描述。

数付卡采用 NFC 近场识别技术，用户可以方便在支持 NFC 手机充值，设置双重验证（指纹，人脸识别），添加主流数字资产，不需要安装多个数字货币钱包，真正做到**一卡在手，走遍全球。** 支付转账，秒级确认，消费返现，每一笔支出都打折。

2.4.2 信贷借贷

代表应用——信链贷

随着数字货币成为更加广泛的交易媒介及更加重要的价值储藏载体，利用数字货币创造新的价值并获得相应收益是必然趋势，正如将比特币投资于“挖矿”，投资于其他区块链项目 ICO 类似。随着数字货币应用范围的不断增加，利用数字货币直接(不需要转换为法币，投资的收益也以数字货币计价)进行投

资的领域和机会逐渐增多。利用数字货币创造价值的人需要更多的数字货币，手中持有数字货币的人需要保值增值，数字货币的借贷业务需求会越来越多。笛卡尔融云链支持具有信用和资金能力的机构或者个人作为数字货币的供需中介，完成存贷业务。以以太币举例，实现方式是中介方在笛卡尔融云链上利用智能合约创建存款应用并设定利息，以太币存入方通过跨链机制将以太坊上的以太币转入笛卡尔融云链上的智能合约对应的地址，笛卡尔融云链上的存款智能合约发放对应该笔存款的凭证(笛卡尔融云链上的 token，类似银行的存单)到笛卡尔融云链上该用户的账户中，智能合约自动计算利息。当用户需要提取该笔以太坊存款时，将凭证转移回中介地址，合约执行跨链交易将凭证对应的以太币在原链上解锁转移回原有用户的账号中。该场景优于传统模式的重要一点总是，作为存贷中介方的存款准备金(该中介地址对应的被锁定的原链资产)是透明的，作为存款人能时刻知晓存款准备金情况。

2.4.3 交易通兑

代表应用——融云币

目前完成数字货币的兑换主要依赖于中心化的交易所和场外交易中间人。所有交易都基于对交易所和中间人的信任。多币接入笛卡尔融云链后，交易所或者中间人可以通过智能合约实现多币种的竞价交易和一对一的场外交易。笛卡尔融云链上提供隐私保护的交易机制，为有隐私保护需求的交易提供支持。将没有隐私保护的数字货币导入笛卡尔融云链链，并在笛卡尔融云链中发起隐私交易，最终再将数字货币转回原有链，一定程度上通过切断资金追踪路径实现了原有链的隐私保护。这一使用场景类似于较早出现过的混币模式。

2.4.4 人工智能

代表应用——智算蜂巢

人工智能就像是一个需要非常庞大数据喂养的怪兽，所以数据的来源、质量、隐私都是急需解决的问题。而区块链中的智能合约能将数据拥有方和使用方通过数据的物理隔离来实现隐私保护。在算力需求方面，一方面人工智能高性能

服务器很贵，另一方面就是服务器的更新迭代非常快，对于所有人工智能企业都是巨大的成本。所以，通过区块链技术手段可以帮助整个行业降低算力成本，提升计算效率，从而达到降低人工智能企业创业门槛的目标。

在人工智能方面，笛卡尔融云链旨在通过区块链及独特的技术方式，构建一个良性的生态圈，促进资源共享，激励更多人参与到智能化应用的开发与落地；推动人工智能在可信、可靠的环境中发展；让私人产生的数据，转化成给每个人的更精准化的服务。

智算蜂巢是由区块链技术驱动的人工智能计算平台，主要是帮助全球人工智能企业解决行业痛点：降低算力成本和保护数据隐私，旨在为更复杂的 AI 应用提供一个共有区块链平台，能够让数据资源方、应用开发方、运行平台资源方和用户在这个区块链上自由发布和使用各自的资源和应用

2.4.5 资产管理

代表应用——数恒升数资平台

我们已经看到传统的资产以联盟链的形式映射到区块链上的趋势，例如商业票据、商业积分、未来收益权、应收账款等。未来会有更多的金融资产以基于联盟链的分布式账本形式记录。当这些联盟链接入笛卡尔融云链后，联盟链成为金融资产的提供方，数字货币的持有者可以利用手中的数字货币购买这些资产进行投资。类比传统银行业务，这类似于在银行购买理财产品。区别在于更多的中介机构可以参与进来，或者资产持有人可以直接进行资产融资。

ICO 现已成为区块链领域众筹融资的重要手段，且这一趋势正向非区块链领域蔓延。越来越多的项目，尤其是基于以太坊的项目，直接使用智能合约进行 ICO，整个过程更加透明公平，但是只能使用以太币进行众筹，给持有其他数字货币的投资者造成了不便。基于笛卡尔融云链开发的 ICO 平台，或者单独的 ICO 项目，发行方以智能合约进行发行的同时，可以支持多币种进行投资。投资人能够更加方便的用以太坊、比特币或者其他任何与笛卡尔融云链连接的区块链代币进行投资，发起方可以更加便利的管理自己募集的资金更进一步，当项目上线时，新的区块链只要接入笛卡尔融云链，通过跨链机制就可以方便的

完成众筹份额与原生币的转换。利用笛卡尔融云链，我们将进入一个全流程基于区块链的数字权益发行时代。

数恒升是区块链突破性的金融生态系统，定义了基于加密货币的金融产品的协议。平台存在智能合约，无边界杠杆，理财产品（固定收益、市场指数、二元期权、期货、杠杆 ETF），数恒升生态系统为投资者提供了一个全面的金融市场，充满了满足其投资需求的金融产品，服务和应用。

2.4.6 保险合约

代表应用——合安保

传统保险行业巨头问题众多，用户保费超过 70%都没有用于赔付，而是成为了保险公司的利润，业务提成等一系列不必要的成本支出，如果能去除掉这个中心化的商业主体，用户将能够花费更少的钱或者更多的服务和赔付，同时，也避免了保险公司的霸王条款。而去中心化的相互保障保险合约平台，是基于区块链技术建立智能保障合约市场，用去中介化得互助保障模式替代中心化的传统保险模式。在平台上，世界范围内任何人可以用一个非常低的成本获得一个智能合约保障。让加入的用户之间实现互助保障，风险互抵，有效降低保险保障产品的运营成本，同时提供更高的保障资金安全性。让申请互助的用户大病有钱医，费用大家摊。加入平台的用户既是助人者，也是受益者。

2.4.7 去中心化交易所

代表应用——币融交易所

使用由 DPoS 保障安全的去中心化交易总账来创造可互换数字资产，拥有秒级确认速度，在交易过程中，币价波动瞬息万变，币币交易就像是在大海里游泳，一刻不能停息。这些资产可以市场化锚定美元、黄金、汽油等任何东西的价值。和所有的 DAC 一样，币融拥有可以像比特币那样在用户间转让的股权，实施了一个类似于银行或经纪公司的商业模式。同时又有别于传统的中心

化交易所，避免了中心化交易所譬如成本高，安全性差，交易所作恶等一系列问题。

项目历程与计划

2017. 3
融云链项目组及研发团队组建完毕
笛卡尔项目进入筹划阶段

2017. 10. 2
笛卡尔链基础模块测试
反ASIC技术融合测试

2018. 3. 21
智能合约组件测试
亚太地区项目运营开发团队成立，着手亚太市场

2018. 5. 3
乌克兰金融牌照正式审批通过
乌克兰金币交易有限公司成立

2018. 5. 18
笛卡尔与六道科技以及吉田资本签署亚太合作协议
笛卡尔链V1.0版本开始测试

2018. 5. 30
笛卡尔软硬件产品正式进入研发制作阶段
笛卡尔融云链官方网站内部测试

2018. 7. 2
笛卡尔融云链国际官网上线
项目智慧生态系统/白皮书进行公示
笛卡尔融云链部分开源、首期矿机全球预售开启

2018. 9
笛卡尔主链矿机首批量产完成并正式发售
笛卡尔搭配钱包同步上线

2018. 11
笛卡尔融云链Token登陆国际数字货币交易所
（火币、中币、比特儿等）

2019. 1
笛卡尔百家创世区块搭建完成
笛卡尔主链开源代码官网公示

2019. 3
笛卡尔区块链浏览器、区块链钱包、数字货币商城正式上线
笛卡尔线上应用矩阵初步完成

2019. 5
笛卡尔数字平台进入开发阶段
笛卡尔去中心化交易所正式上线

2019. 10
笛卡尔融云链首个线下应用"数付卡"完成开发
实现全球商户应用落地与全球无国家数字货币通

2019. 11
笛卡尔数字平台上线测试，开通BTC/ETH交易对
开通笛卡尔数字货币借贷业务

2019. 12
完成百条侧链接驳
完整智慧生态系统架构完成

项目已取得的资质

ВИПИСКА
з Єдиного державного реєстру юридичних осіб,
фізичних осіб-підприємців та громадських формувань

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
"ДЖІНБІ ДЕЙТЕ АССЕТС ТЕХНОЛОДЖІ ЛІМІТЕД"

Ідентифікаційний код юридичної особи:
42173455

Місцезнаходження юридичної особи:
03065, М.КИЇВ, БУЛЬВАР ВАЦЛАВА ГАВЕЛА/АКАДЕМІКА КАБЛУКОВА, БУДИНОК 51/16

Дата та номер запису в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань:
01.06.2018, 1 073 102 0005 037233

Прізвище, ім'я та по батькові осіб, які мають право вчиняти юридичні дії від імені юридичної особи без довіреності, у тому числі підписувати договори, та наявність обмежень щодо представництва від імені юридичної особи або фізичної особи-підприємця:
КУЗНЕЦОВ ІГОР МИКОЛАЙОВИЧ - керівник

Код: 314464085065

ОПИС
документів, що надаються юридичною особою
державному реєстратору
для проведення реєстраційної дії
"Державна реєстрація новоутвореної шляхом заснування юридичної особи"

Для проведення реєстраційної дії "Державна реєстрація новоутвореної шляхом заснування юридичної особи" юридична особа **ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ДЖІНБІ ДЕЙТЕ АССЕТС ТЕХНОЛОДЖІ ЛІМІТЕД"** надала наступні документи:

1. Реєстраційна картка на проведення державної реєстрації юридичної особи, утвореної шляхом заснування нової юридичної особи.
2. Рішення засновників або уповноваженого ним органу про створення юридичної особи (Примірник оригіналу).
3. Статут.
4. Документ, що засвідчує повноваження уповноваженої особи.

Особи, винні у внесенні до установчих документів або інших документів, які подаються державному реєстратору, завідомо неправдивих відомостей, які підлягають внесенню до Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, несуть відповідальність, встановлену законом (частини четверта статті 35 Закону України "Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань").

Отримати результат надання адміністративних послуг можливо за адресою: https://sor.minjust.gov.ua/ua/freesearch/

МЕЛЬНИК І.В.

Заявник: _____ _____ _____
(прізвище, ініціали заявника) (дата) (підпис)

Фактична дата формування опису: 31.05.2018

Стор. 1 з 1

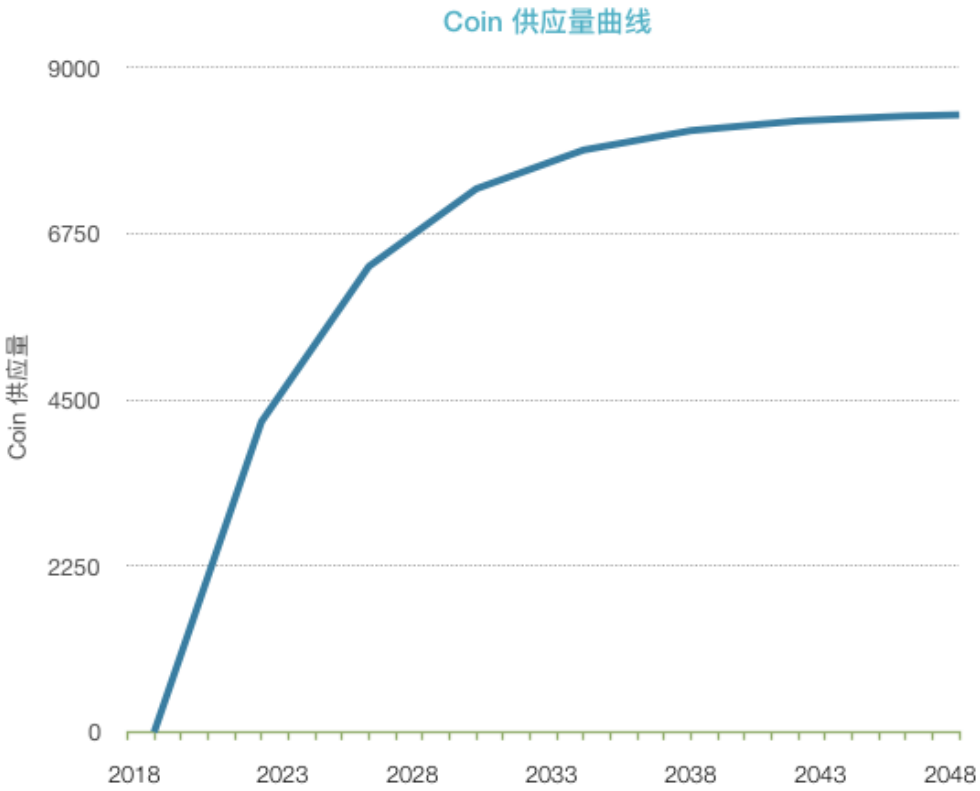
乌克兰

获得乌克兰财政部批准、司法部备案
全球首家获得乌克兰区块链金融牌照的区块链公司

2018 年乌克兰提出一项法案定义加密货币包括比特币为合法资产，能够用于兑换商品和服务。法案的第一部分对加密货币、交易所、交易、区块链、加密货币所有者以及矿工进行了定义。法案中提出加密货币所有者有权选择如何处理他们的加密货币，包括用于兑换其他加密货币，电子货币，法定货币或者商品和服务。乌克兰在 2018 年 1 月，乌克兰国家银行（NBU）表示，将“考虑”推出本国货币的数字版本。同年 5 月，乌克兰国家证券和股票市场委员会（SSMCS）宣布将把加密货币视为金融工具，并且随后出台了相关法律承认数字资产在支付领域的合法地位。乌克兰国家政权市场委员会主席 Timur Khromaev 表示，区块链、比特币、代币和其他技术解决方案已成为了该国金融市场的一部分。

目前整个乌克兰只颁发了八个数字货币牌照，仅有包括笛卡尔融云链在内的五个项目拿到了这个牌照。拥有这个牌照不仅仅是乌克兰政府对笛卡尔融云链项目过去几年努力的肯定，更是对笛卡尔融云链未来发展的鼓励与期望。

通证发行计划



发行总量 **1.26 亿** 枚 **全部由挖矿产生**

70% **矿工奖励** **10%** **笛卡尔基金会** **15%** **项目运营成本**

5% **项目研发成本**

风险提示

政策性风险:目前国家对于区块链项目以及互换方式融资的监管政策尚不明确，存在一定的因政策原因而造成参与者损失的可能性;市场风险中，若数字资产市场整体价值被高估，那么投资风险将加大，参与者可能会期望互换项目的增长过高，但这些高期望可能无法实现。

团队内风险: Descartes Chain 汇聚了一支活力与实力兼备的人才队伍，吸引到了区块链领域的资深从业者、具有丰富经验的技术开发人员等。在今后的发展中，不排除有核心人员离开、团队内 部发生冲突而导致 Descartes Chain 整体受到负面影响的可能性。

团队间风险:当前区块链技术领域团队、项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。Descartes Chain 项目是否能在诸多优秀项目中突围，受到广泛认可，既与自身团队能力、愿景规划等方面挂钩，也受到市场上诸多竞争者乃至寡头的影响，其间存在面临恶性竞争的可能。

项目技术风险:首先，本项目基于密码学算法所构建，密码学的迅速发 展也势必带来潜在的被破解风险;其次，区块链、分布式账本、去中心化、不同意篡改等技术支撑着核心业务发展，Descartes Chain 团队不能完全保证技术的落地;再次项目更新调整过程中，可能会发现有漏洞存在，可通过发布补丁的方式进行弥补，但不能保证漏洞所致影响的程度。

安全风险:在安全性方面，单个支持者的金额很小，但总人数众多，这也为项目的安全保障提出了高要求。电子代币具有匿名性、难以追溯性等特点，易被犯罪分子所利用， 或受到黑客攻击，或可能涉及到非法资产转移等犯罪行为。

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 Descartes Chain 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互换。任何与本白皮书相关的行为均不得视为参与互换，包括要求获取本白皮书的副本或向他人分享本白皮书。参与互换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 Descartes Chain 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 Descartes Chain 进行了清晰必要的了解。 Descartes Chain 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、代币及其机制、代币分配情况。 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。

参考文献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” [Online]. Available: https://bitcoin.org/bitcoin.pdf, 2008, accessed: 2018-01-22.

[2] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” [Online]. Available: http://gavwood.com/paper.pdf, 2014, ac-cessed: 2017-01-22.

[3] Jonathan Katz and Chiu-Yuen Koo. On expected constant-round protocols for byzantine agreement. J. Comput. Syst. Sci., 75(2):91{112, February 2009.

[4] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[5] Alysson Neves Bessani, Jo~ ao Sousa, and Eduardo Ad lio Pelinson Alchieri. State machine replication for the masses with BFT-SMART. In 44th Annual IEEE/IFIP International Con-ference on Dependable Systems and Networks, DSN 2014, Atlanta, GA, USA, June 23-26, 2014, pages 355{362, 2014.

[6] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive, Report 2014/765, 2014.

[7] Ran Canetti and Jonathan Herzog. Universally composable symbolic security analysis. J. Cryptology, 24(1):83{147, 2011.

[8] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[10] Ronald L Rivest, Adi Shamir, and David A Wagner. Time-lock puzzles and timed-release crypto. Tech-nical Report MIT/LCS/TR-684, 1996. Also available as http://theory.lcs.mit.edu/ ~rivest/ publications.html.

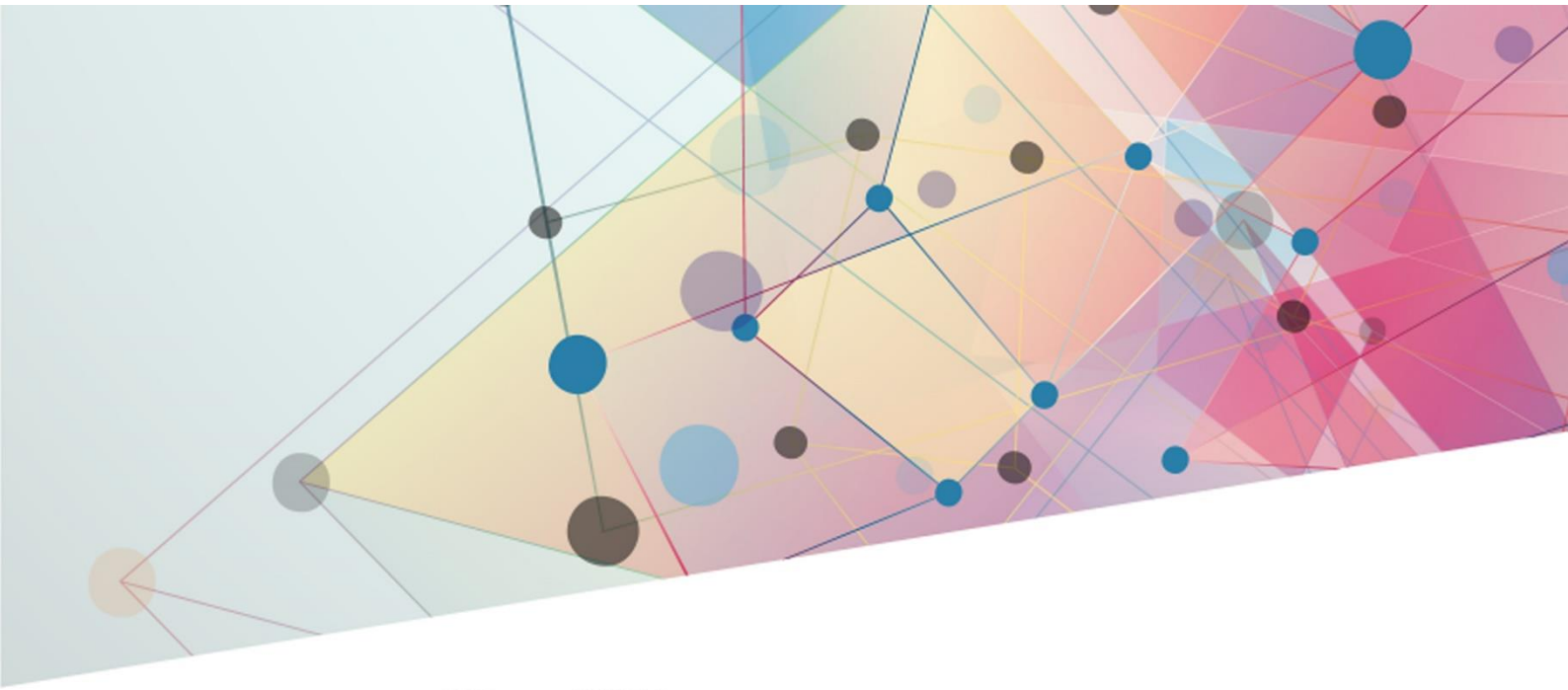
[11] Herman te Riele. Security of e-commerce threatened by 512-bit number factorization. Published at http: //www.cwi.nl/ ~kik/persb-UK.html, Aug 1999.

[12] Dennis Fisher. Experts debate risks to crypto, Mar 2002. Also available as http://www.eweek.com/ article/0,3658,s=720&a=24663,00.asp.

[13] Drew Dean and Adam Stubblefield. Using cleint puzzles to protect tls. In Proceedings of the 10th USENIX Security Symposium, Aug 2001. Also available as http://www.cs.rice.edu/ ~astubble/papers.

[14] Hal Finney. Personal communication, Mar 2002.

[15] Thomas Boschloo. Personal communication, Mar 2002.



DESCARTES CHAIN

开启一个全新的数字金融时代