就在不久前刚刚结束的博鳌亚洲论坛2022年年会上，中国金融学会会长周小川表示，隐私计算等多项技术的发展，为应对数据跨境流动和自由交易中面临的安全、隐私和定价等问题提供了有力支撑。

IDC中国日前发布的《隐私计算全景研究》报告，对隐私计算的发展潜力给出了量化数据。报告称，2021年中国隐私计算市场规模突破8.6亿元。隐私计算发展迅速，但商业环境尚未成熟，整体市场还有很大的发展空间。

满足开放和保护的双重要求

近年来，随着数字经济的发展，数据安全、数字经济治理等议题成为社会关注的焦点。今年的政府工作报告首度将“数字经济治理”写入其中，为数据要素市场的良性发展及数据健康流通打下了基础。

自2015年全国首个大数据交易中心在贵阳成立以来，各地顺应人工智能、大数据的发展潮流，纷纷筹建数据交易中心。据统计，截至目前，北京、上海、深圳、重庆、合肥等地均启动了数据交易所或数据交易中心建设，全国各地的数据交易中心已超过30所。

但数据交易的市场并没有顺利打开。现实情况是，各方出于对安全性、隐私性等问题的考虑，致使“数据高墙”林立、数据流通受阻。

数据只有在使用、加工和流通的过程中才会产生价值，如何让数据真正高效流通起来是国内数据交易市场亟待解决的难题。

那么，怎样在保证数据高效流通的基础上，兼顾数据的开放与保护？香港科技大学智能网络与系统实验室主任、深圳致星科技有限公司创始人陈凯认为，隐私计算技术以“数据可用不可见”的特性，平衡了数据开放共享和隐私安全保护的矛盾，可在保证原始数据安全的同时，实现对数据的计算和分析，为数据要素在跨域流通环节中的安全隐私问题提供了技术解决方案。

隐私计算是由两个或多个参与方在不泄露各自数据的前提下通过协作对数据进行联合处理。在隐私计算技术的加持下，数据的处理与分析过程可保持不透明、不泄露、无法被恶意攻击及被其他非授权方获取，满足开放和保护的双重要求。

隐私计算促进数据要素市场化

国家工业信息安全发展研究中心发布的《中国隐私计算产业发展报告(2020—2021)》显示，结合我国大数据产业规模来看，2020年至2021年间，隐私计算产品市场规模约为10亿元，未来基于隐私计算的数据交易应用模式市场或将达到千亿级，隐私计算开辟了数字时代下的新蓝海。

2020年被认为是隐私计算元年，除了垂直的初创企业外，不少互联网企业、综合IT服务商、人工智能、大数据等相关企业纷纷试水隐私计算赛道。据不完全统计，仅2021年上半年，国内隐私计算领域新增融资金额已超过6亿元，在所有获得融资的企业里，融资金额过亿的企业更是超过了

半数。

投资持续走热的同时，隐私计算落地应用情况如何？根据艾瑞咨询发布的《2022年中国隐私计算行业研究报告》显示，隐私计算目前正处于落地初期阶段，金融、政务、通信运营商领域的商用实践相对领先。其中，金融行业对数据安全性、隐私性要求严格，成为隐私计算落地应用的重要领域。

Aleo将实现区块链领域标志性突破，加速Web3.0的到来

区块链技术的进步，打开了Web3.0的大门，
Web3.0的构想，则是一个相对去中心化的，以用户个人数字身份、数字资产和数据完全回归个人为前提的的自动化、智能化的全新互联网世界。

区块链技术奠定了Web3.0发展的基础，解决信息孤岛和数据垄断的问题，完全公开透明。虽然匿名但是
当前经过大数据分
析依旧可以获得用户信息，更加重了
用户隐私安全的问题。
Web3.0中非常重要的一点是：用户真正掌握自己的身份和数据所有权，实现Web3.0愿景必须拥有自己的链上/网络上的隐私。

“区块链领域的两个最大挑战是隐私和可扩展性，”
KoraManagementLP创始人DanielJacobs说。

“随着区块链行业的不断发展，它正在证明其支持由可访问性、效率和互操作性定义的数字生态系统的潜力，” 软银投资顾问公司的投资者AaronWong说。

各大公链争端的焦点是高扩展性、隐私性，并未有很大的差异化竞争，在以太坊完成POS以及分片转型后，我们应该关注哪些？

Aleo是第一个提供完全去中心化隐私保护应用程序的平台，换言之就是去中心化应用程序的未来

将建立在ALeo支持的零知识密码学至上。Aleo通过区块链的去中心化系统融合零知识加密（ZEXE）技术保护网络上的数据来实现这一目标：
为用户和应用程序开发人员提供绝对隐私的计算和数据保护。

正如Aleo的COO在以太坊开发者大会上说：“Aleo有点像以太坊和Zcash应运而生的产物”。

高性能：

使用零知识密码学，Aleo将智能合约执行至链下，已实现各种去中心化应用程序，它们即完全私有又可以扩展到每秒数千笔交易。

易用性：

Aleo平台提供端到端工具，支持隐私保护应用程序的开发、部署和可持续性。

可扩展性：

建立在开放的公共区块链上，Aleo带来了以太坊的所有灵活性，同时具有更佳的可拓展性构架，无需重新运营每笔交易，只需验证其正确性即可。

可编辑性：

Aleo为零知识提供了全栈解决方案，使ZK在应用程序队栈的每个级别都可编程，一提供实际使用，从而实现大规模的分散式计算。

这样我们更加容易了解Aleo做的一些事情，即是基于Zcash和以太坊的产物，改善了以太坊隐私保护的不足，也弥补了Zcash单一性。

相对于其他区块链隐私项目，Aleo不仅具备隐私性和高扩展性，同时Aleo作为一个应用程序的开发平台，从Leo编程语言、Aleo
Studio开发环境、工具端、RPC、隐私保护应用程序的开发、部署和可持续性等，具备完善的开发环境。也完全具备了WEB3.0所需的基础设施：区块链与跨链技术、去中心化身份、分布式存储、隐私计算的所有属性。
Aleo将成为去中心化应用程序发展的优质沃土，实现区块链领域标志性的突破，也将加速Web.3的到来。

参与Aleo的本质？

安全与效率的平衡，是数据要素产业发展的一大难题。陈凯认为，无论是多方安全计算、联邦学习、同态加密，还是秘密共享等隐私计算技术，在实际应用场景中都对算力提出了巨大的需求与挑战。倘若算力性能无法提升，那么隐私计算将难以处理越来越多的海量数据，也就无法实现自身的规模化发展。

值得期待的是，目前算力的提升得到了社会各层面的普遍重视。在国家层面，京津冀、长三角、粤港澳大湾区、成渝、内蒙古、贵州、甘肃、宁夏等8地已启动建设国家算力枢纽节点，标志着“东数西算”工程已进入到规划建设阶段。隐私计算消除了数据壁垒，为数据要素市场化、全国数据资源流通“一盘棋”提供了有效技术支持，因而也将成为“东数西算”工程实施“软”建设的关注重点。在企业层面，构建一个良好的发展生态，是隐私计算发展与规模化应用的关键所在。因此需促进各方互通互联，实现技术开放与迭代，充分释放算力市场的巨大发展空间。

对于ALEO作为全球性的开源的隐私应用开发平台，未来众多的去中心化隐私应用程序都将建立在Aleo主网至上，在实际应用场景中，不仅仅需要底层技术的支持，更需要庞大的算力支撑整个网络生态的发展。

官方通过aleo积分或者代币的奖励，让更多的人贡献出自己闲置的服务器算力资源，共同打造一个具备全球性的隐私计算网络。根据官方主网的要求配置硬件，为主网提供隐私算力获得Aleo奖励的过程即是挖矿。隐私应用程序开发人员，在ALeo网络上开发隐私应用程序，消耗Aleo积分或者代币，从而实现生态的良性发展。类似于滴滴打车，滴滴搭建整个打车平台，司机为平台提供运力获得订单人民币的奖励，乘客支付人民币获得出行服务。不同之处aleo具备完善的经济模型和通缩机制，每三年减半，最终维持在每个区块12.5的产出奖励。随着主网上线以及整个生态的发展加上通缩机制，Aleo的价值也将呈现几何倍数的增长。

主网预计第三季度上线，6月中旬测试网即将开始，依旧属于项目的早期阶段。也就是整个区块链领域所说的头矿阶段，对于挖矿而言，测试阶段官方每天的奖励数量（Aleo积分或代币爆块）是主网上线后每天的奖励数量的几倍，也是对早期参与者的认可。同时测试阶段参与人数较少，同样100个积分的爆块，100个人参与和10000个人参与哪个收益更大，不言而喻。

俗话说“买在无人问津处，卖在人声鼎沸时”对所有的传统的，非传统的项目而言都是正确的。判断趋势，把握趋势，很重要选择合适的时机进场同样重要。