



# 数字资产基础设施如何推动 城市成为Web 3.0中心

2023年6月

因我不同  
成就不凡  
始于1845



## 目录

序言	04
#1 数字资产托管的必然未来及香港的机遇与挑战	07
#2 数字资产领域的DeFi和CeFi基础设施	11
#3 Web3：下一代数字经济的信任基石	15
#4 在香港建立区块链技术生态系统	18
#5 风险投资应关注的区块链基础设施项目	21
#6 实现数字资产与传统金融基础设施的融合	24
#7 适用于Web 3.0中心的法律框架	27
#8 为Web3.0风险投资和私募股权投资赋能的独立专业服务机构	30
参考文献	34
联系人	36

# 序言



**欧振兴**

德勤中国华南区主管合伙人

随着我们的世界变得越来越数字化，城市必须紧跟创新步伐以保持竞争力。香港长期以来一直在金融和贸易方面处于领先地位，如今香港正致力将自己打造成全球数字资产中心。随着数字基础设施在智慧城市发展中的重要性与日俱增，采用区块链和分布式账本技术等新科技的需求变得至关重要。

在数字化转型时代，投资于稳健数字基础设施的城市可为Web 3.0的蓬勃创新奠定坚实的基础。为此，必须了解数字资产兴起所带来的挑战与机遇，如对安全便捷的托管解决方案的需求。通过采用由Web 3.0赋能的去中心化系统，城市可以创建更安全、更透明的网络，从而推动更大程度的协作和价值创造。

Web 3.0的好处显而易见，包括增加隐私保护、减少审查，以及加强对个人数据的控制。然而，欲实现这些好处并支持这一新范式，城市需要投资于必要的数字基础设施。此外，城市可以利用现有资源为Web 3.0初创公司和企业家创建一个支持性的生态系统，如提供融资、指导和交流机会，以及联合办公空间和创新中心。

随着Web 3.0的出现，城市必须认识到数字基础设施在塑造我们社区未来的关键作用。通过投资于这些基础设施，并培育支持创新的生态系统，诸如香港这样的城市可在这一激动人心的互联网新篇章中发挥引领作用。

“Web 3.0指去中心化互联网，是基于分布式账本技术的新一代互联网。我相信未来Web 3.0将广泛而有效地应用于全球经济的许多方面。目前，还仅处于革新之初。

香港欲发展成为Web 3.0创新浪潮的引领者，必须具备完善的数字基础设施。香港政府已在这方面做了大量工作。举例而言，最新的《施政报告》指明香港将继续加强5G基础设施建设。同时，根据财政预算案安排，香港将就建立人工智能超算中心进行可行性研究。

下一步，我们应该制定具有前瞻性和实用性的Web 3.0发展战略和监管框架。”

**邱达根先生**

香港立法会议员（科技创新界）



“预测未来既充满想象力，又令人着迷，尤其是当未来与我们每个人密切相关时。Web 3.0代表数字经济发展的一种新范式，其不仅是由新技术驱动的一场商业变革，更是实现可持续社会价值创造的一种创新途径。Web 3.0的技术及商业价值为增长和创新提供了巨大机遇，可广泛应用于各行各业。随着全世界迈向Web 3.0时代，城市转型成为数字资产创建和交易中心将愈发依赖数字基础设施。从实践来看，采用政府主导的Web 3.0发展模式，以强有力的计划和政策鼓励Web 3.0创新和应用，辅以监管措施和规范指引Web 3.0的健康发展，已经成为全球主要国家的共识。

香港拥有强大的数字基础设施、友好的营商环境以及蓬勃发展的金融科技和区块链产业，能够充分利用Web 3.0创新带来的机遇。随着去中心化技术和区块链应用的兴起，香港有潜力成为数字资产创建和交易中心，以及开发Web 3.0新应用和平台的领导者。此外，凭借其在亚太地区所处的战略位置，以及其成熟的金融市场和国际交易联系，香港可成为企业进军不断发展的数字经济领域的理想门户。”

**黎瑞刚先生**

推广香港新优势专责小组成员



# 致谢

## Web 3合作伙伴



## 撰稿人



#1

# 数字资产托管的必然未来及 香港的机遇与挑战



**Lily Z. King**  
Cobo首席运营官



要将香港建设成为全球Web3中心，发展、支持和加强香港的区块链基础设施至关重要。这包括建立安全可靠的区块链网络、发展充满活力的开发者社区、制定有利的监管架构、提供安全便捷的资产托管解决方案，以及推出培训计划。其中，作为即将到来的机构采用数字资产的入口，数字资产托管发挥着至关重要的作用。

### 1. 作为入口的资产托管

数字资产托管是保障客户数字资产安全的关键。其为数字资产的创建、管理和交换奠定了基础，让交易、银行服务和大宗经纪业务等服务成为可能。

托管解决了机构在数字资产保管和增值方面面临的两大最大问题：安全性和可访问性。

通过采用基于多方计算（MPC）的私钥管理、访问CeFi和DeFi的混合解决方案、交易所场外结算服务、实时交易储备监控等新技术和创新，托管机构不断创新，以满足投资者和用户的需求。

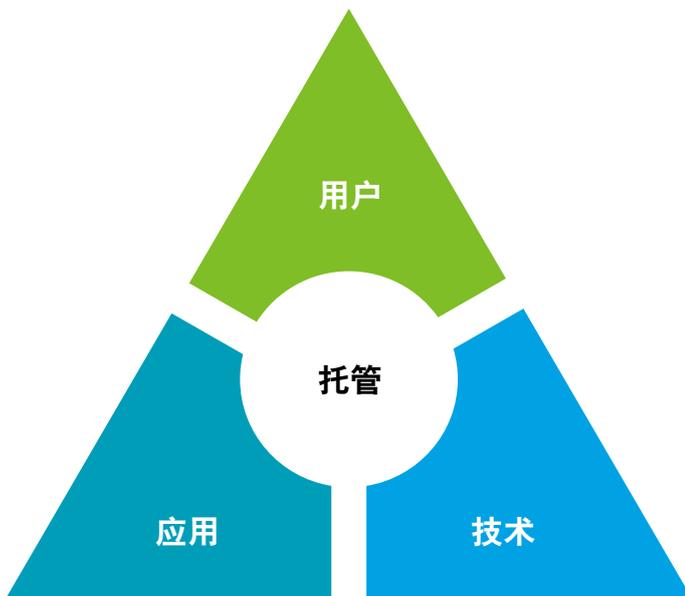
自2019年初以来，托管资产（AUC）总额增长达到了惊人的600%，超过2,000亿美元【1】。这引起了全球投资者的关注，这些投资者在2021年向该领域投入了45亿美元的资金，而前一年仅为8.5亿美元【1】。



## II. 三位一体模型

要了解区块链生态系统中托管角色的不断演变，需引入三位一体模型，其中托管处于用户、应用和技术三位一体的中心。过去几年，这三个因素逐渐成为数字资产行业发展的主要驱动力。

### 数字资产托管的三位一体



#### a. 用户增长：数量与多样性

目前，拥有数字资产的用户估计已超过4.2亿人【2】。随着用户数量增加，其构成也发生了重大变化，早期用户主要是赛博朋克和极客程序员，但现在有了DAO组织、加密基金，以及越来越多的大公司和金融机构。与个人用户相比，这些机构玩家在访问区块链应用并与之交互时有着截然不同的需求。

#### b. 快速演进的区块链技术

从2009年的比特币到2015年以太坊上的智能合约引入，再到Avalanche、Cosmos等一层区块链，以及Arbitrum、Optimism等正在崛起的二层区块链，区块链生态系统不断发展，新技术迅速涌现。展望未来，我们将看到越来越多的一层、特定应用链，甚至是Rollups模块化区块链。这种多链、多层的环境将不可避免地导致资产、用户和应用的分裂。

#### c. 区块链应用大爆发

2020年之前，主流的区块链应用主要是加密货币交易所、钱包以及一些支付服务。在那之后，智能合约推动了新区块链应用程序的爆炸式增长。在短短一到三年的时间里，DeFi、NFT

和DAO组织已经成为价值数十亿美元的庞大行业。除此以外，还有GameFi、SocialFi等应用生态。现在有超过4,000个去中心化应用（DApp）【3】，Web3.0的概念无疑正在成为主流。

## III. 数字资产托管的必然未来

鉴于用户、应用和技术的快速变化，托管方必须超越简单的保险箱功能。我们对数字资产托管的必然未来有4个关键预测。

### a. 安全密钥存储 → 全栈解决方案

区块链应用是建立在一个四层堆栈上，由区块链、智能合约、协议和应用层组成。托管方应了解每一层的工作原理并将各层无缝集成。托管方需开发全栈解决方案，赋能用户安全高效地连接到底层区块链、访问智能合约和协议，并与各种应用程序进行交互。

### b. 碎片化的用户体验 → 统一的用户体验

很明显，未来的区块链世界将涉及多链和多层。这意味着用户将不得不通过不同的入口/访问点访问各个区块链及其应用，从而导致用户体验欠佳和效率低下。托管方应找到一种促进数据和资产转移的方法，同时在目前孤立的区块链之间实现互操作和可组合的操作。最重要的是，所有这些都必须由统一且简单的用户体验来实现。

### c. 面向个人用户 → 企业级可编程性

随着越来越多的专业团队进入加密领域，对可定制托管解决方案的需求将持续上升。他们参与不同的协议和应用将产生更专业的需求。

### d. 中心化基础设施 → 分布式私钥管理

中心化私钥管理有几个优点：首先，更容易实现合规；此外，由于其很容易与传统系统和工作流程整合，其被视为对机构更友好的解决方案。然而，其致命缺点是单点故障。在整个加密货币历史中，许多针对中心化托管方和交易所的成功攻击均证明了这一点。此外，如果没有持续的审计，它就缺乏透明度。

我们相信，分布式私钥管理是更强大区块链应用的基础，例如通用无私钱包、社交恢复型钱包、链上信任、职权分离，甚至是以前从未考虑过的新型区块链应用。这一领域已经有许多尝试，包括但不限于基于MPC的托管解决方案，以及结合账户抽象和智能合约托管的混合私钥管理。

#### IV. 香港的机遇与挑战

香港作为国际金融中心，有潜力成为全球数字资产中心，但挑战与机遇并存。香港拥有强大的传统金融业和深厚的资本市场，可以提供流动性、专门知识和基础设施，为数字资产的发展提供了坚实的基础。此外，香港拥有大量对数字资产感兴趣的投资者和客户，尤其是来自亚洲市场的投资者和客户。

因此，香港的数字资产发展自成立以来就与金融业紧密相关。这种环境使得香港能够相对轻松地生成连接区块链技术和实体经济的用例，为香港在追求Web 3.0愿景方面提供了相当大的优势。举例而言，2023年2月，香港发行了全球首支由政府发行的代币化绿色债券，根据政府绿色债券计划（GGBP）发行了8亿港元的代币化绿色债券【4】。

托管是机构采用数字资产并最终在现实世界经济中采用加密货币的关键。对于香港来说，为了保持竞争优势，必须站在不断发展的托管行业前沿并与时俱进。

##### a. 监管框架

香港拥有世界上最完善的金融市场监管框架之一。该框架可用于数字资产监管。目前，香港对区块链的监管方式与传统金融遵循相同的高标准。这体现在“相同业务、相同风险、相同规则”这一香港加密货币政策原则中。

香港的监管框架目前是通过自上而下的方式实施，这样更有利于既有机构。虽然这种方式有效地促进了政府、金融机构、大型Web2互联网公司 and 区块链原生企业之间的合作，但也制约了草根开发者和企业家的机会。为确保区块链技术继续依靠自下而上的创造力和活力蓬勃发展，必须在自上而下的监管和自下而上的创新之间取得平衡。

传统的金融监管框架可能无法完全容纳区块链行业的独特变化。数字资产生态系统在不断快速发展。因此，监管机构可能需要努力跟上技术进步的步伐，避免过度监管或监管不足，从而扼杀增长或造成风险。

香港在为数字资产业务提供清晰一致的指导和监管方面可充当全球引领者，并确保初创企业、机构和投资者有信心在其所在管辖区内安全运营。

##### b. 科技生态系统

香港要建立创新创业生态系统，就必须吸引和支持世界一流的基建企业和技术。只有纳入云计算、区块链、数字资产托管、网络安全甚至人工智能的强大且可扩展的基础设施，才能实现数字资产的安全性、互操作性和演进。

托管是该基础设施的核心组成部分。强大的托管行业有助于减少与数字资产所有权相关的风险，提升投资者对数字资产的信心，从而推动数字资产的主流采用。对于香港而言，拥有稳健且值得信赖的托管行业，可以成为其在全球数字资产领域的竞争优势。

由于数字资产托管是一个新兴的发展领域，香港拥有独特的机会来塑造和建立行业的最佳实践和标准。这可通过在安全性和透明度方面设定高标准并采用最新的技术解决方案来实现。

2023年是香港重新恢复其作为全球数字资产领导者和Web3.0中心地位的绝佳机会。目前对于区块链行业的信任处于最低点，有足够的重塑空间。香港可以利用其在传统金融领域的优势，拥抱创新和多元化人才，并制定健全合理的监管框架，以重振信心并塑造行业叙事和发展轨迹。



#2

# 数字资产领域的DeFi和CeFi基础设施



**任煜男**  
欧科云链执行董事、  
董事局主席兼行政总裁



自2008年比特币系统诞生以来的10多年间，加密货币行业经历了指数级增长。自2021年起，加密货币总市值已经超过1万亿美元，在2021年底的牛市期间甚至达到3万亿美元【5】。

本部分讨论的中心主题是CeFi和DeFi基础设施现状，该等基础设施将支持用户更好地探索加密世界。同时，我们还将就该等基础设施的后续发展进行展望。

### 1. CeFi基础设施

管理加密货币风险的主要方法之一是通过中心化金融（CeFi）进行管理。CeFi实际上是对传统金融市场的一种模仿。企业充当用户资产的托管机构、交易平台和贷款人。由于用户可借由CeFi系统使用加密货币进行存储、交易、赚取利息、借贷和支付，因此，CeFi已经成为零售商和机构进入加密世界的一种简单而有效的方式。

中心化交易所是CeFi行业的重要组成部分。据称全球排名前15大交易所拥有的用户数字资产总额达2,180亿美元【6】。Binance、OKX和Coinbase为其中三家代表。此外，还有其他几家公司也致力于为零售商和机构提供与加密货币相关的一体化金融服务。正如Amber和Matrixport，客户可通过这两家公司获得贷款、结构性产品、场外交易和投资服务，据称这两家公司已经处理数十亿资产，为数百家机构客户提供服务。随着对中介机构有更高要求的机构客户的需求不断涌现，而中心化交易所又成为黑客攻击的目标，对托管服务的需求稳步增加。Fireblocks和Copper是托管服务行业的佼佼者。通过使用MPC技术，这两家公司成功地吸纳了许多机构成为他们的客户。

#### 1.1 基础设施平台



图1：CeFi基础设施平台

与证券交易所和商业银行等金融机构类似，CeFi基础设施平台通常归一家机构所有并由其管理，而用户必须信任该等机构。CeFi技术主要遵循传统金融机构的系统逻辑，核心涉及以下三个方面：

- 网关、支付和结算。法币与数字货币的兑换（Fiat on/off-ramp）服务提供商可以帮助用户使用信用卡/借记卡或银行账户，直接向Web3世界的现有用户购买/出售加密货币。正如Moonpay，其声称目前已服务超过500万用户。
- 托管、帐户和资金管理系统。CeFi公司如何通过确保安全妥善存放用户资金，成功赢得用户的信任，这是一个优先考虑的问题。这些公司进行了一些探索，如发布存款证明（PoR）报告，整合第三方托管机构，或与第三方合作以监控账户。CeFi 实体需要谨慎考虑确保其平台上用户资产安全的最佳方式。
- 交易撮合引擎。为确保交易富有流动性，交易基本上是根据订单簿而设计，而流动性是订单簿上买入和卖出订单数量的函数。此外，还有与此相关的做市商。Tower和Jump Trading等做市商通过提供报价，为市场提供流动性和深度。

#### 1.2 监管

随着加密市场的指数级增长，监管也在不断发展。美国、日本、德国等发达国家及地区已经就加密货币建立了相关的监管框架。相关公司需要在监管部门进行登记，并遵守反洗钱/反恐融资（AML/CFT）等相关法律。然而，一些其他国家（如中国大陆）已正式禁止加密货币挖矿和交易等活动。

#### 1.3 当前挑战

对手方风险和透明度不足是CeFi实体受到质疑的主要原因。在目前的CeFi 背景下，通常由充当中介机构的中心化交易所来撮合执行交易、存储用户所持有的代币和处理交割清算交易流程。与所有活动均由智能合约管理并可通过链上数据追踪的去中心化协议不同，用户需要信任CeFi实体（即用户相信其可以随时从这些实体提取资金），并相信这些实体可保护他们的资金免受黑客攻击。

FTX 之所以会倒闭，是因为其在未经用户同意和未向用户披露的情况下挪用了用户资产，这不仅使用户对于存放在CeFi实体的资产安全产生了深刻的担忧，也严重摧毁了用户对于行业的信任。

即使许多监管部门已经公布了监管框架，但仍需要细化加密货币监管规定。几家监管有序的实体因挪用或不当管理客户资产而倒闭，这表明监管部门不但需要提供指引，还需要深入调查这些实体的实际运营情况。此外，这些监管框架高度重视反洗钱（AML）相关法规，但可能还需要关注消费者保护。幸运的是，一些监管机构已开始关注这一领域，并计划加强对风险管理方法、产品标准的要求，进一步保护消费者的权利。

## 2. DeFi基础设施

### 2.1 DeFi基础设施组件

DeFi的核心基础是比特币、以太坊以及其他区块链协议。这些区块链的总锁定价值（TVL）在2021年11月左右达到峰值至1,750亿美元，之后缓慢下降，稳定在300亿~500亿美元左右。其中，以太坊的锁定价值遥遥领先，占据区块链总锁定价值的60%，紧随其后的是BSC、Tron、Arbitrum和Polygon等。这些区块链之间的竞争尚未结束。

在此基础上构建的DeFi应用程序本质上是智能合约，旨在提供与传统金融系统类似的服务，而无需依赖中介机构。目前，主要的应用程序集中在去中心化交易所、借贷市场、预言机（Oracles）、流动性挖矿（yield farming）等方面。相比中心化交易所，去中心化交易所的一大主要优势是用户能够控制自己的私钥；贷款协议是DeFi的另一快速增长领域。此外，对赚取巨额收益的需求导致了智能合约的激增，这类合约旨在最大限度地提高持有加密代币的收益。

### 2.2 DeFi 技术堆栈



图2：DeFi技术堆栈【7】

上述堆栈模式显示了如何以分层的方式构建DeFi应用程序和协议。

- 结算层为已使用的区块链，包含区块链生态系统的基本运行规则。交易实际上是在这一层执行。为了提高区块链的性能和可扩展性，还在该层中融入了Sharding、ZK等技术。
- 资产层建基于结算层，包含在其上创建的加密资产，如BTC、ETH等。各协议或项目均可根据业务需要定义自己的代币，以满足经济模式的运行需要。

- 协议层体现了去中心化金融的主要功能，包括交易、借贷、衍生品、保险等。该层为整个生态系统提供了核心业务逻辑，也为应用层提供底层服务。
- 应用层包含面向用户的应用，这些应用连接到协议层的协议和标准。由于智能合约交互是基于web浏览器的网页前端界面进行，因此该协议易于使用，可提供良好的用户体验。
- 聚合层本质上是应用层的扩展。聚合器创建以用户为中心的平台，连接多个不同的应用程序和协议，从而简化了复杂的事务。用户可使用在该层运行的应用程序作出明智的决策，并将通过使用DeFi应用程序获得的优势发挥到极致。

显然，DeFi技术堆栈有关各层的相互建构体现在以下两个方面。一方面，DeFi各项功能的实现是DeFi技术堆栈各层之间的互联互通的结果。另一方面，DeFi技术堆栈某一层的可扩展性、去中心化或脆弱性程度取决于底层区块链（尤其是共识机制）的特性。

### 2.3 当前挑战

#### 监管挑战

监管金融活动通常有三大目标。第一、防止资金用于非法活动、洗钱或避税；第二、保护金融市场各方免遭欺诈和滥用；最后、确保市场和支付系统健全，整体金融稳定。

目前，DeFi解决方案尚未达到上述目标。从各个角度来看，构建明确的DeFi监管框架可能会对此有所助益。然而，目前的问题在于，由于DeFi应用和底层区块链协议具有匿名性和无需许可性，监管机构难以沿用中心化中介机构所适用的框架，如银行账户由谁开立、哪些文件必须提供，抑或相关信息如何收集和存储。

#### 技术挑战

分布式账本去中心化程度对网络的可扩展性提出了更高的挑战。直观地说，随着账本变得更加去中心化，为了达成协议共识，确保区块链安全，需分发更多的副本，消耗更多资源。在去中心化、安全性和可扩展性这三个属性之间进行权衡的这一理论，由Vitalik Buterin提出。这一区块链三难困境引起了广泛关注。为了同时实现这三个目标，已经引入大量新的区块链解决方案。

### 3. 前景展望

如上所述，CeFi和DeFi领域均已拥有相对完善的基础设施平台，可为用户提供各种服务。然而，问题与挑战也随之而来。2022年，FTX的破产、Luna崩盘事件和黑客攻击等一系列黑天鹅事件造成了巨大损失。区块链行业需要引进更多技术和基础设施来确保资产安全。同时，还有必要提升基础设施的性能和效率，实现更大的可扩展性。那么，区块链行业的未来将如何？

#### 3.1 ZK-Rollup 技术持续落地实践

以太坊的合并对性能提升有限，而基于Rollup的扩展可能会提供新的解决方案。Rollup升级的重点是在降低成本的同时，提升性能和兼容性。ZK Rollup受到DeFi社区的青睐，但由于其难以与EVM兼容，在很大程度上受到限制。此外，引进EIP4844将大大降低Rollup的gas费用。在Rollup领域，相较Optimistic Rollup，ZK Rollup具有的一个明显优势是几乎能做到上传主链上数据的实时确认，而无需等待7天挑战期。随着zkEVM的发展，困扰ZK Rollup的最大问题将得到解决。虽然ZK Rollup相比其他机制而言拥有更多用例，但开发ZK Rollup时面临的主要矛盾是ZKP的生成速度慢，同时成本较高。

#### 3.2 多链网络将促进整个生态系统蓬勃发展

Cosmos设想构建一个由多链组成的生态系统，这可以推动区块链行业的进一步发展。应用链借助主链开发工具独立构建，在由主链构建的生态系统内具有跨链、安全共享的优势。在技术实现方面，Dapp应用程序构建自己的区块链已经不再是问题。然而，Dapp链却受到其他条件的限制：(1)维护自身网络安全需要更大的成本；(2)主链本身的特性是否与Dapp的需求相匹配，如性能、用户习惯、EVM兼容性等。

#### 3.3 去中心化存储展现极大潜力

虽然去中心化存储在本年度并未获得太多的关注，但其表现出持续进步的迹象。存储领域已经或即将出现更多的真实需求、更多的访问渠道和更高级的功能。首先，存储协议可存储更多真实数据。Filecoin在2022年底实施了Filecoin plus计划，真实数据存储量持续增加。与加密市场的波动相比，这些存储需求更加稳定，且有望持续增加，可为存储协议提供生存环境。其次是可访问性。通过提供更多的网络访问权限，存储协议将渗透到Web 3的更多方面，并加强其主渠道作用。第三是将会出现更多功能。存储方面最重要的升级是其可叠加在计算层上，从而实现超出硬盘范围的更多功能。

#### 3.4 全球监管将进一步趋严

2022年，一些协议引起了监管机构的关注。加密货币公司Tornado Cash被美国财政部制裁，去中心化自治组织Ooki DAO成员被美国商品期货交易委员会（CFTC）起诉，同时对于以太坊是否属于一种证券也颇有争议。在未来一两年，随着加密货币资产监管框架的引入，以及各国监管政策的实施，可能会出台专门针对链上协议的相关立法，如欧盟正在试点DeFi“嵌入式监管”方案。链上协议可能须遵循KYC、AML等反洗钱措施。当监督、起诉和执法成本有效降低时，对链上协议的相关监督将进一步加强。



#3

# Web3: 下一代数字经济的信任基石



**徐思彦**  
腾讯研究院高级研究员



**秦青**  
腾讯光子区块链技术预研负责人



**孙畅**  
腾讯云国际战略总监



自19世纪40年代计算机出现以来，每10~15年就会出现一个新的技术周期。我们目前所处的Web 2.0互联网时代，主要建立在用户到服务端的BS/CS架构之上，用户可自由参与内容的创建和共享。在Web3时代，我们不但可以在互联网上阅读和交互信息，还可传输资产。每个人都可以享受计算、存储和资产等各个领域的去中心化服务，成为各自信息数据的所有者和管理者。

Web3将开辟一个全新的数字时代。我们认为，区块链技术将赋能下一个互联网时代。根据a16z的一份报告显示，预计到2031年，全球Web3用户数将达到10亿。作为下一代互联网基础设施网络，Web3尚处于起步阶段，但其需求正在迅速膨胀。举例而言，去中心化身份（DID）为可信数字身份和跨机构数据交互提供了重要基础。用户可以信任互联网上具有加密安全和数据隐私保护的真正身份凭证。商品领域的数字创新（如NFT）通过将真实商品虚拟化，有助于品牌的永久保存和创意传播。同时，Web3还在金融、组织形式和数字空间等多个领域带来了创新应用。

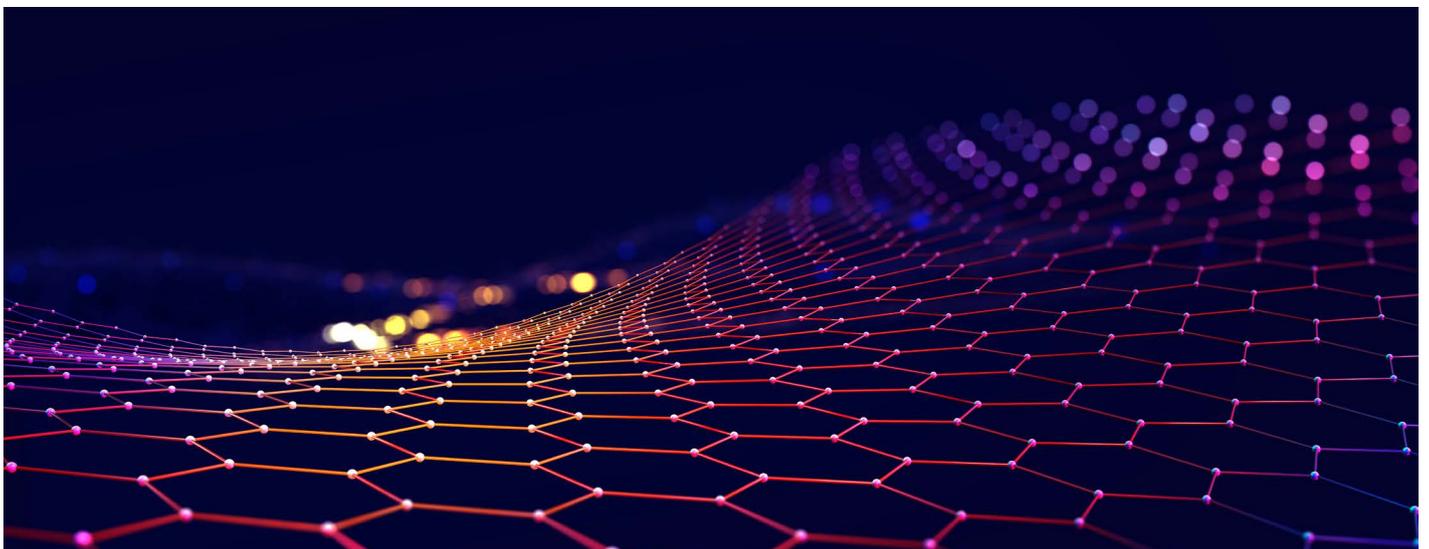
随着Web3生态系统的逐步部署，数据和身份管理从以平台为中心向以个人为中心转型，适应此需求的新技术和商业模式亦将应运而生。在此背景下，Web3将为当前的数据垄断、隐私风险和算法歧视等问题提供解决方案，并推动网络向平等、治理和开放价值式互联网的代际转型。

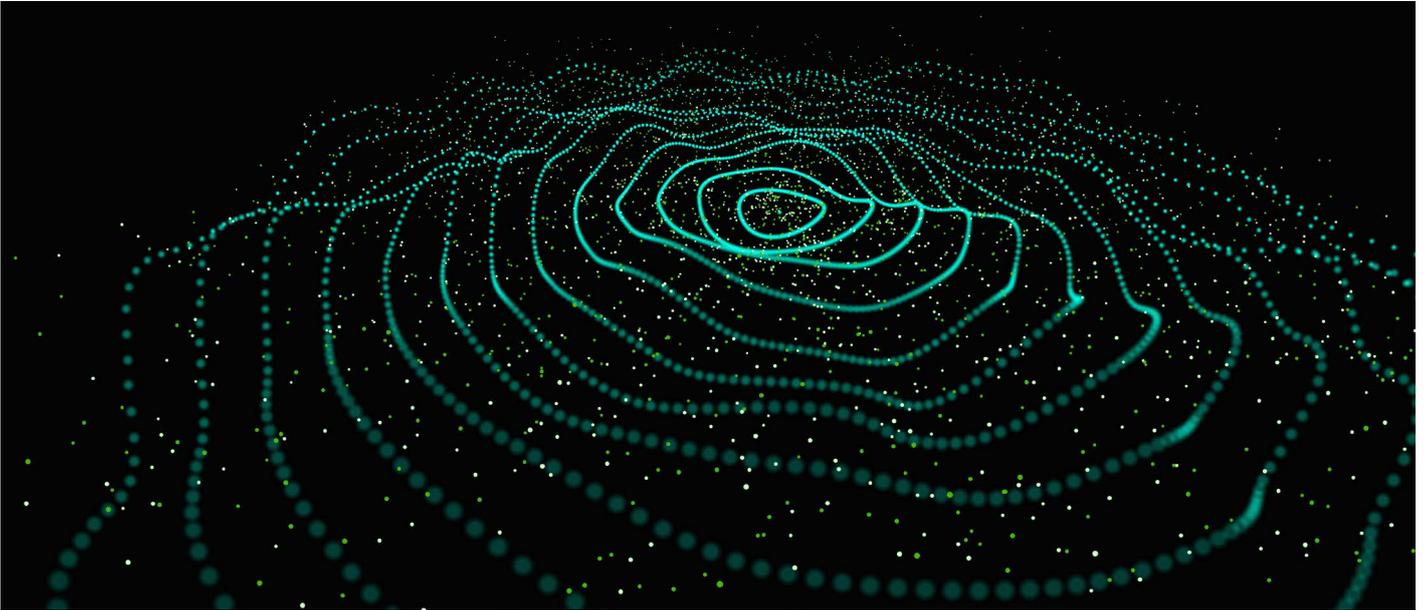
在Web3时代，腾讯云致力于通过支持全球Web3生态系统发展，并提供全套基于云的产品和基础设施，帮助构建者加速采用去中心化技术。

区块链是Web3生态系统嵌入去中心化基础设施的基本要素，该基础设施用于验证区块和交易数据。以最流行的区块链平台以太坊为例，以太坊由大约12,000个以太坊节点构建而成，尽管这些节点分布在100多个国家，但有超过50%的节点是托管在美国【8】。简而言之，以太坊节点是运行连接以太坊网络所需软件的计算机，其可以在本地实体机器上自行构建，也可以托管在云服务器上【9】。迄今为止，出于设置成本低、弹性伸缩、服务器正常运行时间较长及现收现付订阅模式等原因，有超过60%的以太网节点由第三方（其大多为云服务提供商【10】）托管。

除以太坊外，BNB Chain、Polygon和Avalanche等其他热门区块链也支持推广云环境，让公众建立各自的区块链节点，以提高资源去中心化程度和网络稳定性。Web3生态系统的其他重要元素还包括不同类型的去中心化协议，如跨链桥、数据存储、网络路由和数据仓库。这些协议通常建立在云环境中，以奠定初步基础，并确保快速上市。从长远来看，这些协议对云环境上的机器规格进行分类，供大众市场运行节点，以便展开去中心化网络，实现公平共识机制。

鉴于Web3应用的架构不同于常规Web2应用的架构（原因在于Web3应用需要实时调用链上数据），因此，开发者构建Web3应用的进入壁垒更高，进而各类面向Web3的开发者工具应运而生。最值得注意的解决方案是远程过程调用（RPC）节点提供商，其减轻了开发者建立和管理自身区块链节点的负担，并为主要区块链生态系统提供可靠而全面的连接。如前所述，不同区块链的RPC节点可以建立于云端，以确保能覆盖全球并优化网络连接。





由于Web3社区十分重视数字所有权和公平治理的重要性，因此，去中心化身份（DID）和去中心化自治组织（DAO）是Web3生态系统中的两个热门创新领域。云环境中有专门的工具包提供商负责开发服务，并基于不同区块链基础设施提供轻松访问DID和DAD的途径。中介性Web3服务提供商可以凭借云技术实现快速上市，并为全球的Web3开发者群体和用户群体提供灵活可靠的服务。

因此，利用底层区块链和中间件工具，构建者能够开发Web3去中心化应用，确保真正的数据所有权，并开启用户新体验。一个典型的用例是去中心化金融（DeFi），即建立在区块链网络之上的金融产品（如交易平台和借贷平台）。这类DeFi项目可编写智能合约以自动执行订单，并可利用RPC节点调用和写入区块链数据。项目还可以使用云服务器来构建用户界面，并提供额外的数据分析功能，为用户体验增加价值。

随着以太坊的发展进入了第十个年头，且距离比特币发生第四次减半还有不到一年的时间，Web3社区瞄准了游戏，以吸纳更多用户并实现大规模采用。整个行业都在推动全链游戏，但考虑到现有产业化游戏发展流程的成熟度和玩家对高质量游戏显示的需求，大多数Web3原生游戏工作室和Web2传统游戏工作室均利用云端在链下环境中开发游戏，并利用区块链使数字所有权合法化。基于云的产品可供选择范围很广，比如云渲染软件和低代码软件开发工具包（如数字化身），这些产品可用于减轻工作室从零开始开发的负担，并赋能工作室专注于游戏逻辑设计和代币经济模型设计。

我们旨在就自区块链的基础设施构建到大规模采用的各环节，与全球开发人员合作，更好地理解Web3的本质，共同塑造下一代数字经济。

#4

# 在香港建立区块链技术生态系统



杜宇  
万向区块链实验室总监

WANXIANG BLOCKCHAIN LABS  
万向区块链实验室

### 香港Web3行业迎来新机遇

2022年10月31日，香港财经事务及库务局正式发表《有关虚拟资产在港发展的政策宣言》，阐明政府为在香港发展具活力的虚拟资产行业和生态系统而制定的政策立场和方针。政策宣言发表后，香港建立了一个监管框架，涉及香港证券及期货事务监察委员会（SFC）、香港财经事务及库务局（FSTB）和香港金融管理局（HKMA）等机构。香港作为全球金融中心，拥有完善的传统金融体系和强劲的资本市场，并在融资和吸引人才方面出台了多项扶持性政策，致力发展成为国际创新科技中心。所有这些因素都为将香港打造成全球Web3中心奠定了坚实基础。全球Web3行业的发展本质上是一场技术较量。欲发展成为发达的国际Web3中心，需拥有基于数字资产的技术性基础设施、全球认可的Web3应用产品以及配套的技术和服务体系，以维持全球Web3产业链的稳定、高效运行。因此，建立成熟、繁荣和多层级的区块链技术生态系统，将有助于香港Web3行业的发展。

### 香港得天独厚的优势

香港在发展Web3行业方面拥有得天独厚的人才资源。香港作为国际化大都市，移民政策相对开放，在语言、交通、文化、货币政策等方面的国际化程度较高，从而在吸引全球杰出人才方面具有优势。另外，香港有五所大学跻身世界前100名，拥有实力雄厚的国际专家和学者队伍，以及世界一流的科研和产业平台，为培养顶尖的创新技术人才提供了坚实的基础和成熟的机制。此外，香港政府也积极制定短期和长期人才培训和引进策略，加大对人才体系的资金投入，推动国际合作，建立可持续且不断优化的顶尖创新技术人才储备。香港作为中国的特别行政区，依托《粤港澳大湾区发展规划纲要》等一系列国家政策的有力支持，在迅速成为国际创新技术中心方面具有战略优势。中国拥有世界上规模最大的高等教育体系，接受高等教育的人口达2.4亿，众多大型科技公司和科研机构在全球创新领域发挥着愈发重要的作用，为香港创新科技行业的发展提供了重要的智力支持。同时，中国内地是全球最大的区块链人才聚集地之一，在Web3行业拥有宝贵经验和基础，是香港Web3人才的重要来源地。

### 香港区块链技术生态系统的发展

过去十年来，区块链技术已取得重大进展，不再局限于早期的比特币点对点支付系统，或智能合约出现后的代币投机混乱时代。相反，区块链技术已经朝着注重应用的实用性、可扩展性和成熟度的方向发展。

近年来，区块链技术应用从支付发展到去中心化金融（DeFi）。非同质化代币（NFT）的日益普及点燃了金融游戏化（GameFi）和元宇宙的热潮，从而吸引大量Web2构建者进军Web3行业。然而，高进入壁垒仍阻碍web3获得更广阔的行业认可，并遏阻用户涉足此领域。另外，DeFi应用方面的合规性问题也可能引发用户对资产安全的顾虑。因此，让用户更好地了解相关内容，并鼓励开发人员参与推动生态和技术进步至关重要。

目前，第一层公有链已经非常成熟，形成了由以太坊和多个与以太坊虚拟机（EVM）兼容的替代链为主导的行业格局。为了应对“不可能三角”带来的挑战，第二层公有链已成为确保公有链安全同时提升可扩展性的最优解决方案。因此，第二层已成为公有链竞争后半程最关键的课题。

公有链技术仍处于优化阶段，同时还需对若干技术挑战进行进一步研究。这些挑战包括隐私与效率的兼容性，其中零知识证明（ZKP）可提供可行的解决方案，但开发难度较高。此外，行业核心开发人员正聚焦验证器中心化和抢先交易（最大可提取价值，MEV）等问题，提出了许多性能和体验优化解决方案，如数据分片、区块提议者和构建者分离（提议者/构建者分离，PBS），和账户抽象（AA）。

香港应密切关注行业的最新技术趋势，并鼓励生态开发商围绕第二层、ZKP和去中心化身份（DID）等创新技术和生态系统进行研发。将香港的科技金融行业优势与DeFi算法和机械创新方面的研究相结合，可探索出更合规、更安全的DeFi应用程序。推广NFT和元宇宙概念，加大力度突破Web3界限，将吸引更多用户加入此生态系统。



### 推动香港区块链技术生态系统蓬勃发展

在香港构建区块链技术生态系统的核心是以开发人员和卓越项目为中心。我们旨在建立全面的项目发现和培育机制，提供全方位的行业指引、资源和资金支持。我们的目标是培育顶级Web3项目，引领行业走向繁荣。



我们的方法首先是创建一个活跃的开发者社区，并通过组织线上线下峰会和沙龙等行业交流活动促进社区发展。此类举措将吸引用户和开发者加入社区。另外，与香港的大学、行业协会等组织合作，能进一步连接创新人才，打造极具潜力的开发者社区。

在开发者社区，我们将定期举办黑客马拉松，发掘真正具有创新潜力的初创公司，并筛选出具有实用性、独特优势或创新理念的商业计划和产品。这些初创公司团队将在最初阶段获得社区关注，形成第一批用户，获得资助，并成为未来杰出公司的雏形。

下一步是建立孵化器，并组织新手训练营。孵化器将为从黑客马拉松中选定的项目提供早期资源和指引，包括共享办公空间、后端服务、技术指引和战略支持。凭借上述支持，初创公司可以成功应对创业初期的挑战，补齐短板，将想法和计划转化为有形产品。

新手训练营主要针对更为成熟的项目，通过为期三个月的密集培训为项目团队提供全面的资源支持，培训内容涉及融资指引、上市和品牌建设战略。我们旨在帮助项目团队打造一个流量丰富且充满活力的社区生态圈。

最后，通过多轮融资和项目宣传，优秀项目将会脱颖而出，有效助力技术应用，形成品牌效应。这将加强香港产业生态系统的影响力，吸引更多开发者进入本地生态系统，推动Web3的大规模采用。

### 区块链技术生态系统将推动Web3行业发展

借助开发者社区、黑客马拉松、孵化器、新手训练营、资源和财务支持，我们预计将大量颇具品牌影响力和竞争力的杰出项目将脱颖而出，从而推动香港整体Web3生态系统的发展。

首先，这些顶级项目可以吸引更多人才来港就业和合作，鼓励更多企业家加入Web3生态系统。创新人士汇聚香港，形成更大、更活跃的开发者社区，从而激发更多的创新和灵感。此外，领先项目的知名度可以改善孵化器和投资公司的品牌形象，吸引更多资金流向香港，从而加强对本地创业者的支持力度，生成更多成功项目。最后，一批具有前瞻性的影响力人物和投资公司将脱颖而出，在顶级项目的创建和投资方面表现卓越，并将引领整个行业的观点，赋能香港项目赢得更多用户和资本的关注，增强品牌影响力。

凭借人才、项目、基金和品牌的不断融合，香港的Web3行业生态系统将形成积极的飞轮效应，不断繁荣并发展成为极具竞争力的全球生态系统。



#5

# 风险资本应关注的区块链基础设施项目



**郑嘉梁**  
HashKey Capital 研究总监

**HASHKEY**  
▶ Capital

加密货币和区块链飞速发展，成为充满机遇和潜力的领域。网络、协议、数据存储和安全性皆是区块链领域基础设施项目的重要组成部分。HashKey Capital作为以太坊最早期的投资者之一，区块链基础设施项目是其重中之重。因此，我们的投资组合中有很大比例的基础设施项目，例如公有链、去中心化云服务、节点基础设施、模块化区块链等。以下是我们对基础设施垂直机遇的看法。

### 去中心化云服务

区块链去中心化云服务提供了高度可靠且安全的存储、计算和检索。使用集中存储方式时，用户数据和隐私极易泄露，而集中存储在数据库也极易受到攻击。就长期存储而言，相比亚马逊云科技（AWS），目前的去中心化存储项目 Arweave 更为便宜。去中心化生态系统甚至还有专门用于查询数据的社区，如 MetricsDAO（其会对数据任务提供奖励）。

- 去中心化存储：可将数据分散存储在不同节点上，以提高数据的可靠性和安全性。部分服务可能会使用分布式文件存储系统，如 IPFS 或 Swarm。
- 去中心化计算：将计算性任务分布在不同节点上进行，以实现高容错性（即使一个节点发生故障，其他节点仍然可继续运行）。
- 去中心化索引：搜索和查询区块链中存储的数据。由于区块链上的数据呈分布式，因此，查询数据变得更为复杂。索引协议（如 The Graph）使区块链数据更为标准化且易于查询。

### 节点基础设施

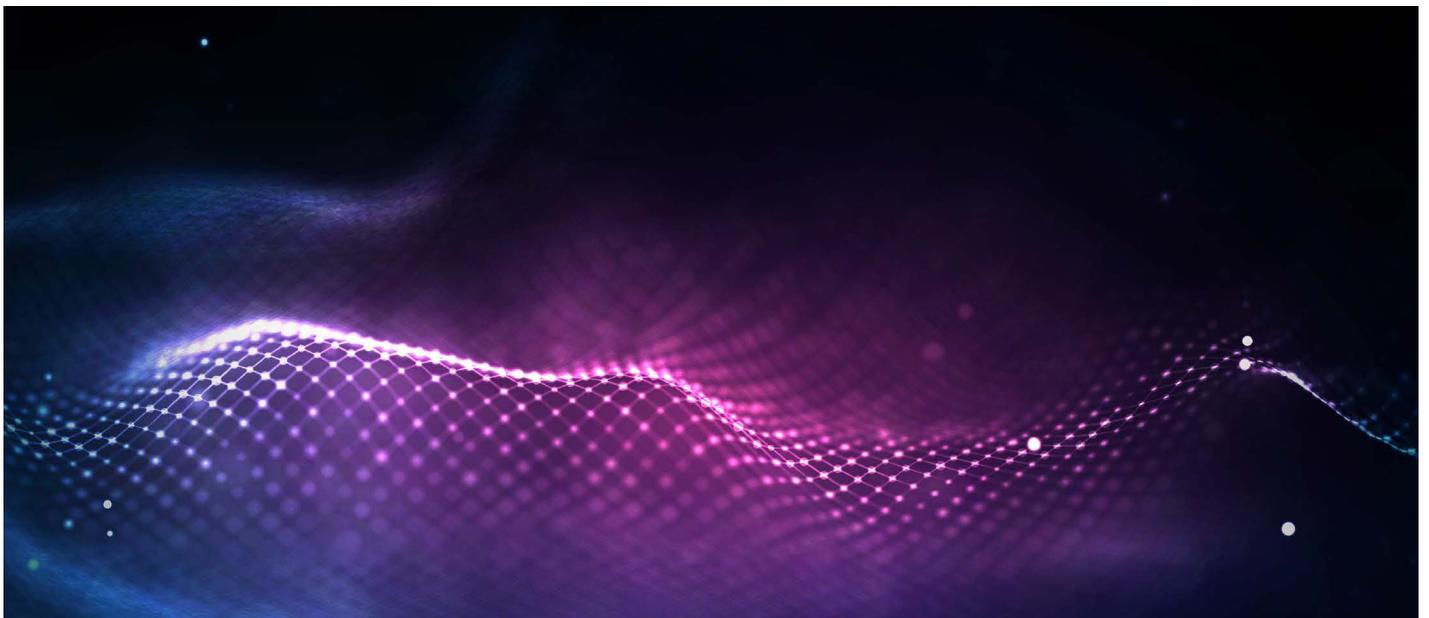
区块链网络通过其节点记录所有交易信息。因此，与区块链交互或执行新交易的任何应用皆须与节点通信并更新数据。节点间通信通常会使用远程过程调用（RPC）。

远程过程调用是一种基于客户端/服务器模型的通信协议，允许客户（如其他应用程序）通过网络调用远程服务器（即节点）上的功能。例如，如下表所示，若某应用程序（如 OpenSea 或 AAVE）发起任何交易，则相关交易信息需通过 RPC 协议（比如 Alchemy，其目前支持以太坊、Solana、Polygon、Arbitrum 和 Optimism）发送到区块链上的某个节点上。

### 链上链下数据的互操作性

区块链数据类型包括交易、区块、元数据、状态和合约。由于这些链上数据无法与现实世界的链下数据交互，因此，预言机（oracle）的作用至关重要。其中一个经典示例是 DeFi 协议，其要求获取交易双方的实时价格。

对于由预言机提供的数据而言，数据源、数据的准确性和速度，以及数据聚合方法均尤其重要。下页对不同项目中的一些设计进行了详细对比。自 NFT 引起公众关注以来，已出现了若干 NFT 预言机。



节点操作	 Chainlink	 Band Protocol	 PYTH	 API3
谁负责运行预言机节点?	第三方	第三方	数据提供方	数据提供方
他们是否运行不同的链?	否, 但理论上可以	是, BandChain	否	否
他们是否运行链下网络?	是, 模块化点对点网络	否	否	否
<b>汇总方法</b>				
价格在哪儿汇总?	链上 (目的地为第一层) 和链下	链上 (BandChain)	链上 (Solana)	链上 (目的地为第一层)
价格如何汇总/报告?	中位数	可自定义	置信区间	待定

图2: 预言机经济对比, 来源: Delphi Digital

相关项目: Pyth 网络、Chainlink

### 公有链和数据可用性

公有链有几个不同的维度: 无需许可/需要许可, 公开交易/私人交易, 以及去中心化区块生产/中心化区块生产。比特币和以太坊2.0等区块链无需许可, 且以去中心化方式生产区块。另一方面, 最近由香港政府发行的代币化绿色债券是由高盛的Canton区块链开发。该企业区块链需要中心化区块生产系统。

尽管计算和验证已转移到第二层, 第一层存储仍然面临严峻的可扩展性挑战。模块化区块链是目前的一种新趋势, 将执行层、结算层、共识层和数据可用性层分解为不同的模块, 并选择合适的模块组合起来, 以创建适用于不同应用场景的区块链网络。

凭借模块化设计, 区块链可更灵活、更高效且更具成本效益地应用于各种领域。Celestia 和 Polygon Avail为数据可用性项目方面的示例。HashKey Capital认为模块化区块链拥有巨大潜力, 且非常看好这类区块链。我们在上年发表了一篇关于模块化区块链前景的文章, 本年度将更加关注Cosmos生态系统。

总体而言, 区块链基础设施项目为区块链技术的应用和发展提供了关键支持和基础架构。因此, 机构应关注此类项目的趋势和创新方向, 以发现有潜力、有发展前景的项目, 并为其提供支持和资金, 进而推动区块链产业的发展。

#6

# 实现数字资产与传统金融基础设施的融合



**任骏菲**  
潘渡投资  
行政总裁兼董事



**PANDOFINANCE**

### 加密货币金融服务基础设施和趋势

区块链作为一项新技术，近年来在应用领域引领了创新飞跃。这种与技术相关的代币经济学（即加密货币），已经（尤其是在投资界）获得很多关注。作为一种新兴资产类别，加密货币已逐渐为越来越多的投资者所接受，其成为重要资产类别的趋势也非常明显。

然而，无论是在客户背景调查、服务提供商生态系统还是用以确定相关风险的服务方面，目前的金融服务基础设施尚不足以在加密货币领域为投资者提供传统金融服务体验。

很明显公众对加密货币相关金融服务的兴趣和需求呈与日俱增的趋势，但是，为使这一趋势更为健康地发展，还需付出更多努力。确实需要构建广泛包含加密货币的金融服务基础设施，因此可建立一个网关，以无缝利用客户在传统金融服务方面的经验。越来越多的传统金融机构将涉足加密货币业务，同时，越来越多的加密货币原生玩家也将从传统金融机构学习经验教训和专业知

### 助力配置人设定流动性加密原生风险

香港证监会（SFC）将授予越来越多的虚拟资产（VA）业务升级牌照，从而为配置人（即专业投资人或受信投资人）提供更广泛的选择，将其法定资本直接配置到加密资产，设定预期的加密原生风险，以实现资本增值或投资多元化。理论上讲，根据该等业务升级牌照提供的产品，可为专业投资人或受信投资人提供与传统对冲基金策略或产品几乎相同的资产配置体验。

由于只有声誉良好且获批准的服务提供商，才能参与从资产托管人、交易所到基金管理和会计等业务链，因此，在此业务升级牌照下，整个运作流程也与传统对冲基金几乎相同。

就所提供的基金战略而言，行业将有意从简单、低风险、以配置为导向的战略入手，如BTC和ETH的业绩跟踪器，仅对大市值加密货币进行主动管理等。这样既能确保配置人的原始意图和需求得到满足，同时，还能保护配置人免于承受极端风险，因为此资产类别过多的信息流和快速的创新步伐，可能会以不可预测的方式突然发生许多变化。

随着香港加密货币资产管理行业日趋成熟，其本地的监管框架亦变得更加健全，行业参与机构将进一步加速丰富战略服务，增加产品多样性，以便能更好地为配置人服务。

### 公众需求不可忽视

整个行业的繁荣需要更广泛的包容性。在这个区块链创新飞跃的时代，普通个人和家庭的作用举足轻重，他们对于生态系统的发展尤为重要。

为了促进大众对于区块链演进的了解，将发行越来越多面向零售的投资产品。举例而言，我们将看到越来越多专门针对区块链主题或区块链延伸主题的低成本交易型开放式指数基金（ETF）。这些产品有效赋能大众获得区块链相关增长的机会，也有助于公众了解区块链技术和应用程序的相关情况和取得的进展。



### 亟需弥合加密货币资产和“传统”金融市场之间的理解鸿沟

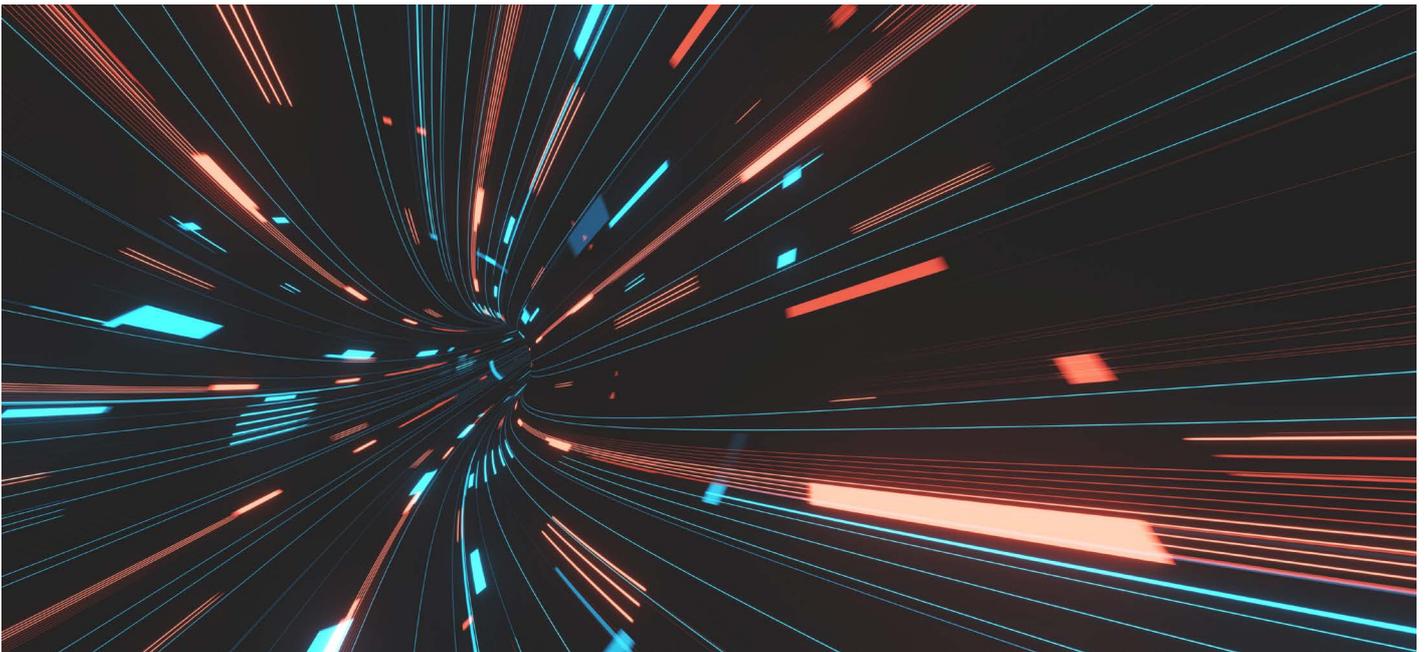
我们很高兴看到，香港证监会（SFC）正在从“资产”的角度规范加密货币相关金融活动，将加密货币视为合法的资产类别，并就其建立全面的监管框架。

无论是提供给受信配置人的两款100%虚拟资产投资产品，还是现有的两款面向大众的ETF产品，潘渡均根据SFC的指引，以一种非常谨慎的方式，尽最大努力在加密货币资产和传统金融市场之间无缝衔接投资者体验。尽管值得为之付出努力，但这项工作本身并不轻松。例如，潘渡虚拟资产产品的推出引起了不同交易对手的关注，成为一个行业性事件。为推动该衔接流程变得更加精简和友好，需要监管机构、银行和其他专业服务提供商等所有利益相关方携手合作。

从潘渡的经验和角度来看，第一条建议将是寻求生态系统利益相关者之间的理解统一。例如，尽管加密货币是一种相对较新的资产类别，但说到底，其是获得香港证监会等监管机构认可的资产类别。最好是不加区别地对待这一资产类别与其他“传统”资产类型（至少要在战略拥护和监管行动层面上无差别），才能更有效地构建涵盖加密货币、股票、固定收益、大宗商品等的整体监管和业务处理框架。

根据潘渡的理解，行业应尽快实施的另一项重要举措将是利用该领域的现有创新技术。例如，尽管中心化加密货币交易所存在许多问题（大多数问题可能是“道德”问题），但不可否认的是，在7天24小时全年不间断交易、流动性、保证金追踪和头寸清算、订单匹配、集中式订单簿管理等方面，其交易技术和基础设施远远领先传统交易所。若不以相对更快的步伐引进更先进的技术，无论是对普通大众还是受信机构而言，从事加密货币相关业务的成本都相对较高，这反过来导致在受监管的交易框架下市场流动性相对薄弱的问题。若缺乏流动性，市场风险管理实际上就更为困难。

因而监管机构和整个行业应该考虑市场风险管理/运营/流程/道德风险管理之间的平衡。这将会面临权衡取舍。



#7

# 适用于Web3中心 的法律框架



**林惠贞**

贝克·麦坚时律师事务所  
合伙人（注册外国律师）

**Baker  
McKenzie.**

清晰有力的法律框架对于Web3中心的发展至关重要，可推动合作，吸引投资，而这对于Web3生态系统的发展和可持续性不可或缺。

为了促进Web3技术的发展和采用，法律框架须同时考虑Web3的经济和技术方面。该等法律框架须足够敏捷，能够快速响应新兴技术趋势和不断发展的行业惯例，且须得到为推动创新以及认可和了解区块链技术潜在优势而专门制定的法律和政策的支持。

Web3中心的法律框架须解决下述几个关键问题，这些问题对于确保基于区块链技术的去中心化应用程序、协议和服务生态系统的安全、透明和合规至关重要。

### 技术与法律

便利性监管框架的一个关键要素是法律的明确性，这有助于公司和用户了解各自的权利、义务和潜在责任。通过提供明确法律依据、清楚的规则和稳定的运营环境，监管框架有助于降低风险，从将有力激励公司和用户进入Web3领域，刺激对Web3生态系统的投资增加，并促进其发展和演进。

具体而言，使用区块链技术作为执行交易、存储数据和保存记录有效的媒介应得到法律认可。法律对区块链技术的认可和接受可以确保该等技术得到妥当、安全地使用，赋能Web3生态系统的参与者充分利用其潜力，并向潜在投资者保证其投资所依赖技术的合法性。

应就智能合约的使用和强制执行制定准则。目前，尽管一些地区已采取措施来认可和监管智能合约，但对于智能合约尚无全球统一的法律认可。现有的监管框架可能无法处理某些与智能合约的认可和监管相关的一些更为细微、更加复杂的问题，尤其是有关法律责任、执法、争议解决和合同解释的问题，而这些问题对机构投资者和组织而言十分关键。

### 融合数字资产领域与传统金融领域

还应就数字资产的法律定性制定明确的准则。这对于确定管理数字资产的法律地位、税务影响以及其他发行和使用规则的适用至关重要。同样，也应明确规定数字资产交易和Web3中心内的挖矿和质押等活动的税务影响，并对数字资产领域独有的活动制定具体指引。

对于处于Web3领域的许多公司、用户和开发者而言，一大关键挑战在于如何融合传统金融系统与数字资产领域。具体而言，获取银行服务和法定货币与加密货币的兑换通道一直是一大难题。为了发展Web3中心，监管框架必须促进数字资产和传统资产这两个不同网络间可预测、无缝、有效的金融融合。

### 消费者保护

消费者保护是数字资产和dApp领域的另一关键问题。法规对于让消费者安心参与Web3中心内的活动方面发挥着重要作用。监管框架必须为用户提供保障，保护用户免受欺诈、欺骗或恶意行为的侵害，同时还要根据这些产品和服务所处的独特技术环境进行适当调整，以创建一个安全可靠的生态系统，让消费者放心访问创新应用程序。创建可让消费者作出明智决策并加强消费者保护的框架，将增强消费者的信心，从而提高消费者对去中心化应用程序、数字资产和分布式账本技术的采用率和使用率。

此外，监管框架还须解决数据隐私和安全等消费者问题；并应包括去中心化数据存储、身份管理解决方案、隐私保护协议和透明政策执行方面的明确措施，以确保充分披露数据的处理方式。

### 许可和监管

数字资产交易所、钱包和Web3中心涉及的其他中介实施反洗钱法规和打击恐怖主义融资的法规，是帮助遏制非法金融活动的重要措施。这些中介机构须设定适当流程和控制措施来管理客户风险，并监控和报告可疑活动。

在Web3中心内运营的数字资产服务提供商和其他公司，应遵循明确的许可和注册要求。应明确界定触发许可或注册要求的活动和服务范围，并须对适用的许可和注册要求予以调整，以反映Web3和数字资产的特质。此外，还须定期更新许可和注册管理机制，以反映新出现的趋势、技术的变化和不断演变的风险。

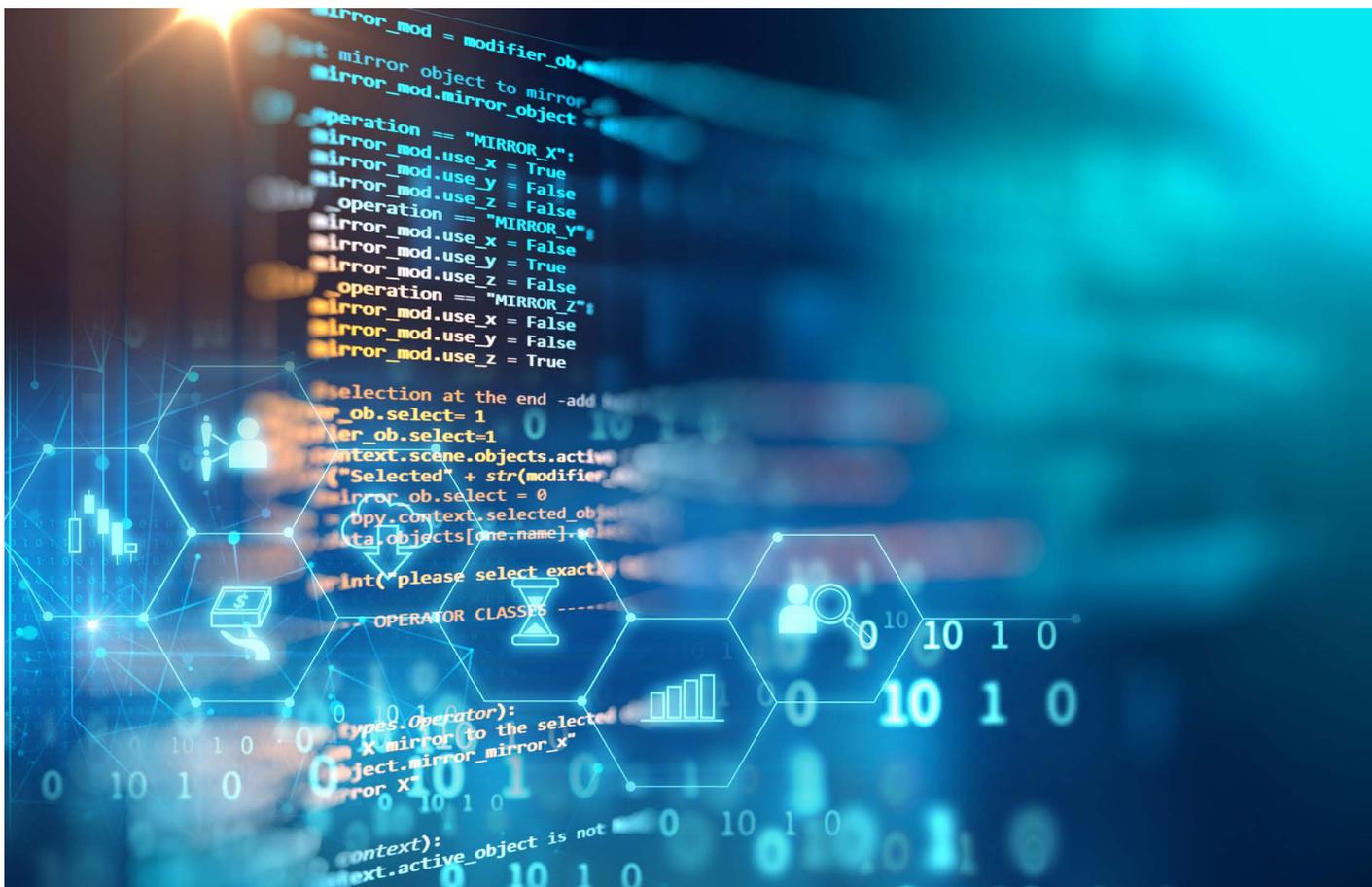
具体而言，有效的监管框架必须就如何监管DeFi协议及服务（包括借贷、质押、衍生品、保险和稳定币）提供明确指引。鉴于近年来DeFi快速发展（预计还将加速），随着行业的发展，为提高行业透明度，建立公平的市场惯例，保护投资者并防止市场操纵行为，就必须制定明确而具体的法规来处理DeFi协议及服务的关键问题。

以Web3为中心的法律框架还应为去中心化自治组织（DAO）及类似治理机制提供结构并认可其运作，此类机制已成为Web3生态系统的共同特征。DAO提供的框架有助于确保网络内的全体利益相关者均按照既定规则 and 标准运作，同时仍保留适当灵活性和创新性。通过就纠纷处理方式和可行补救措施提供明确一致的指引，DAO还可为其成员提供额外法律保护。为DAO的成立和运作创建定义明确的环境，将有助于确保这类组织能够在Web3新兴数字经济中继续蓬勃发展。

## 监管方法

鉴于新兴技术和行业惯例的快速发展，Web3中心监管框架必须具备灵活性和敏捷性。提高该监管框架适用性的一种方式是利用监管沙盒。在此类沙盒中，创新者可在监管机构监督下的受控环境中测试新产品及服务，但不受该监管制度全部要求的约束。监管沙盒旨在促进创新和维护监管之间保持谨慎的平衡。监管沙盒是监管机构紧跟金融科技领域新兴趋势和评估潜在风险的重要手段。

政策制定者可为Web3制定有效的法律及监管框架，通过采取积极举措并与行业利益相关者和开发者合作，处理可能造成风险或问题的基本因素。实施细致入微且量身定制的监管框架解决Web3的上述关键问题，将有助于为企业、用户和开发者营造安全可靠的发展环境。此举将鼓励创新，同时为用户提供必要保护，赋能监管机构紧跟新兴技术和趋势。



#8

# 为Web3.0创投及私募 股权投资赋能的独立 专业服务机构



**罗远江**  
德勤中国  
创投及私募项目  
华南区主管合伙人

**Deloitte.**

## 构建值得信赖的去中心化架构和生态系统

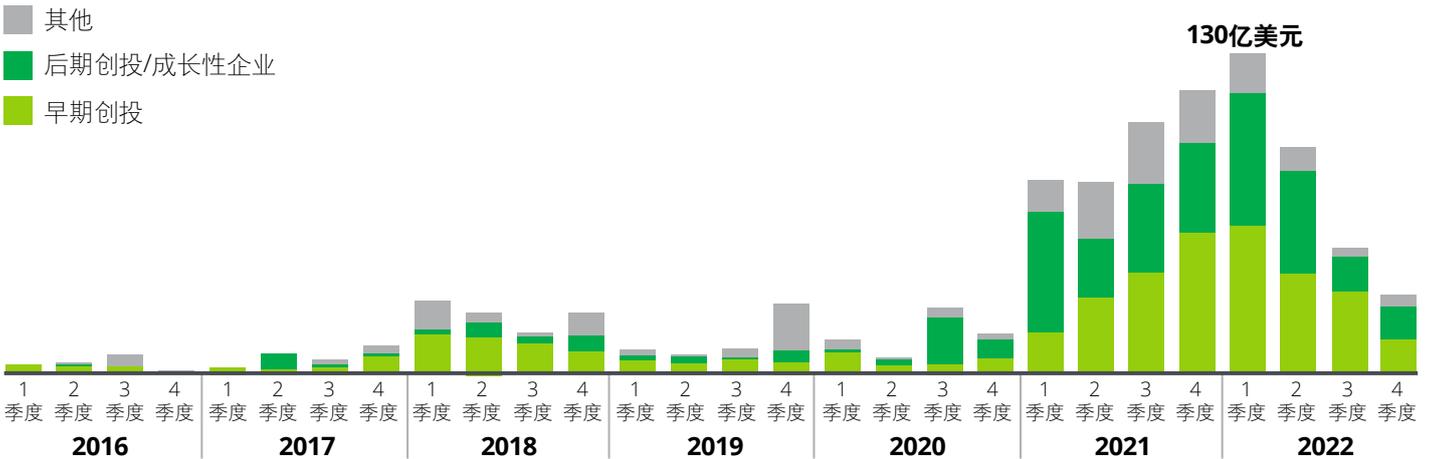
### Web 3.0旨在吸引创投及私募股权投资者

从一开始，建立利益相关者的信任就是区块链技术的主要优势之一。区块链赋能的“无信任”系统被视为应对政府、媒体、货币、企业和其他公共和私人机构信任度不断下降的良方。之所以称其为“无信任”系统，是因为其信任并非建基于单个人或企业之上，而是建基于用户社区之上。然而，加密货币交易所FTX和Silvergate银行的倒闭动摇了投资者对数字资产的信心。市场参与者正试图评估这类倒闭造成的损害程度，以及这将如何塑造未来几年的Web3.0行业。

近期的加密货币暴跌和21世纪初的互联网泡沫崩盘有一些明显的相似之处，包括非理性繁荣、缺乏投资纪律等。但是正如过去二十年以来互联网技术已成为人们生活和工作中不可或缺的技术一样，Web 3.0的巨大转型潜力也将继续吸引创投和私募股权（VC/PE）投资者。

图：近年来，投资者已向Web 3.0公司投入约940亿美元资金，其中大部分在2021年之后投入

### 全球对web3相关公司的投资情况（单位：十亿美元）



2016~2022年投资总额：940亿美元

注：仅包括股权投资，不包括加密货币投资；包括PitchBook上归入加密货币/区块链垂直分类领域的所有交易；Coinbase 2021年的直接上市除外  
资料来源：PitchBook, Crunchbase, The Block, CoinDesk, Bain analysis [13]

在丧失信任的大环境中，独立的专业审计及咨询公司可赋能“无信任”区块链和Web 3.0系统重建信任。一些研究报告表示，区块链技术或能完全消除审计师审计财务报表的需求。如果所有交易均记录于不可篡改的区块链中，审计师还有什么可审计呢？但这种主张过分简化了信任问题。

审计师根据严格的法规、职业操守和审计准则执业，独立于被审计单位。他们运用客观性和职业怀疑态度，对被审计单位的财务报表是否存在重大错报，并根据业务约定对被审计单位财务报告的内部控制是否有效运行提供合理保证。公众普遍认为，审计师通常会提高被审计单位所发布信息的可信度，并可增强对资本市场的信心。

德勤的观点更为务实。除Web 3.0行业参与者外，我们还发现成熟企业、机构、监管部门、政府和专业审计及咨询公司在Web 3.0的采用、发展和信任建设方面发挥着重要作用。审计及咨询公司将继续发挥重要作用，并助力在Web 3.0创投及私募股权投资生态系统中建立信任。

## 法规

从FTX的破产倒闭中汲取经验，密钥管理方面的内部控制不足或缺失以及治理结构不善，是导致数家交易所崩盘的共性因素。法规对于确保投资者信任、提供透明性和法律确定性，以及保护Web 3.0生态系统的完整性至关重要。这些年来，政府开始愈发关注Web 3.0行业参与者，并已就分布式账本技术及其应用出台全新监管框架和规则。制定标准和规则的首要目标是确保上述平台及应用的治理、内部控制、运营和配套功能符合监管机构为保护投资者利益而制定的要求。

根据香港证券及期货事务监察委员会（“证监会”）所发布适用于虚拟资产服务提供者（VASP）的建议指引，正在或打算在香港运营虚拟资产交易平台的申请人，均须向证监会提交一份外部评估报告，内容包含其业务模式、治理、内部控制、网络安全、客户背景调查（KYC）及反洗钱（AML）机制；程序是在提交其牌照申请时向证监会提交第一阶段评估报告，并在获证监会原则上批准之后提交第二阶段评估报告。

从投资者角度来看，当决定使用Web 3.0交易所平台交易其加密货币或托管其数字资产时，其提出的最常见问题是“我的资产安全吗？”。随之而来的通常会是一个更难回答的问题，“你们怎么得出此结论？”据此，已成为行业基准的安全运营中心（SOC）认证开始发挥作用。

SOC 1及SOC 2认证分别侧重于平台或托管机构的不同方面，提供一种全球公认的有效方式，以有别于其他服务提供商。SOC 1主要关注与企业财务报告相关的内部控制活动，而SOC 2则关注与安全性、可用性、进程完整性、机密性和隐私性相关的内部控制活动。国际注册职业会计师协会根据其信任原则就有效控制设计制定了通用标准。独立评估师负责认定一家公司所做的工作是否符合该等标准。因此，第三方鉴证报告有助于建立投资者对Web 3.0公司的服务交付流程和控制内部的信心。

## 网络安全

Web 3.0行业参与者快速增长，所处理的资金和数字资产数额巨大，对黑客极具吸引力。过去数年内，黑客攻击事件导致投资者资金损失，这极大地影响了投资者对Web 3.0的进一步采用和信任。此外，因分散式阻断服务攻击造成系统不可用或执行缓慢，也会损害投资者对交易所的信任。

采用有效的网络安全程序对于防止和检测外部恶意黑客攻击至关重要。拥有充足的网络安全预算固然重要，但如何组织和治理网络安全程序比计划就此花费多少金额更加重要。

在施行全面有效的网络安全计划的同时，专业服务公司还采用了不同的方法。举例而言，一种辅助性“交易监控”检测技术可就记录于用户钱包中的交易与交易所余额以及由第三方节点记录于公有链分类账上的交易进行核对。理论上，交易所记录的交易必须与相关钱包和第三方节点所记录的交易相等。若有差异，则可能表明有人未经授权访问了交易所，并可能进行了恶意交易。【11】

## 密钥管理

许多博主和记者错误地宣称区块链存在大量安全漏洞。迄今为止，所有造成利益相关者数字资产损失的已知事件均与区块链技术的缺陷无关，而更有可能是由于用于管理或存储数字资产的软件（即交易所软钱包）存在漏洞，或是源自未经授权访问私钥导致的欺诈行为。

上述事实表明信任有赖于适当的私钥管理和访问管理权限把控。作为投资者资产的托管机构，数字资产平台须确保操作私钥的机密性、完整性和可用性。

大多数利益相关方均已发现这些风险，但尚未找到有效且具成本效益的适当解决方案。有些方案既可满足这两项要求，又以专业服务公司在支付行业私钥管理方面的丰富经验为基础。某些独立专业服务公司在这一领域提供的服务包括安全密钥存储及托管、完全托管服务以及在下一代平台推出之前提供第二种意见的加密咨询服务等。【11】

## 尽职调查

尽管许多Web 3.0行业参与者开展了不同程度的客户背景调查（KYC）和反洗钱（AML）调查，在入行期间，还应就财富或资金来源进行更多的尽职调查。

上述尽职调查可通过约定的“来源证明”程序实现。对于每个给定的钱包地址，该程序将检查与使用法定货币收购数字资产相关的所有交易，确保与股东、银行、交易所、经纪人、托管机构及其他利益相关者的现金转账、银行电汇确认书、账户信息、贷款协议或类似文件等证明文件一致。

如果某数字资产平台因被用于洗钱而受到“点名批评”，其后果将影响深远，日后该平台几乎没机会恢复声誉。因此，开展充分的尽职调查对管理和减轻相关声誉风险至关重要。

【11】

### 审计师在Web 3.0生态系统中的未来角色

区块链系统将规范跨行业的交易处理，审计及咨询公司能为Web 3.0技术的投资者及用户提供鉴证服务。审计师的技能、独立性、客观性及专业知识将有助于其胜任未来工作。以下所列审计师的潜在贡献仅供参考；审计及咨询公司在承担这些角色前，可能须要通过大量监管和专业程序。【12】

#### 智能合约审计师

如上所述，可将智能合约嵌入区块链，以实现业务流程自动化。缔约方可能希望聘请鉴证服务提供商来验证智能合约是否按照正确的业务逻辑实现。此外，审计师还可验证智能合约和触发业务事件的外部数据源之间的接口。若没有独立评估，区块链技术用户可能面临无法识别错误或漏洞的风险。为承担这一新角色，审计师需要备有一套新技能，包括理解技术编程语言和区块链的功能。

在财务报表审计中，管理层负责建立内部控制制度，以验证智能合约源代码是否与预期业务逻辑一致。如果某实体在区块链上拥有智能合约，其独立审计师很可能会考量管理层对底层代码的控制权。然而，许多公司可能选择重复使用已经活跃在区块链上的其他实体所构建的智能合约。未来的审计准则和指引将需要考虑这项技术，以明确审计师在有关情形下的职责。

#### 联盟链服务审计师

在现有区块链平台上推出新应用程序或利用或订阅现有区块链产品前，用户可能希望就其平台架构的可靠性和稳健性获得独立鉴证。与各参与者自行开展尽职调查相比，聘请审计师来实现上述目标更为高效。此外，关键的区块链元素（如加密密钥管理）的设计应包括复杂的通用信息技术控制（GITC），为敏感信息提供持续保护，并提供对安全性、可用性、进程完整性、隐私性及机密性的处理控制。参与者可能将需要一个值得信赖的独立第三方，确保私有链控制措施的有效性。

#### 管理

获许可的区块链解决方案将得益于由值得信赖、独立且公正的第三方担任中央访问授权管理员。该职能负责身份验证或参与者获准访问区块链前需完成的进一步审查程序。同时，中央管理员还可验证区块链协议的执行和监控。若该职能由区块链用户或节点执行，则其可能会获得不正当的优势，从而削弱了联盟链成员间的信任。由于该角色旨在整个区块链中建立信任，因此，在确立其职能和法律责任时需适当谨慎。

独立的审计及咨询公司作为值得信赖的专业机构可履行这一职责。

#### 仲裁

业务安排也许会错综复杂，甚至会导致善意的当事方之间发生纠纷。对于获许可的区块链，可能需要仲裁来解决联盟链参与者之间的纠纷。该职能类似于遗嘱执行人，通常由包括审计师在内的合资格专业人士担任。当智能合约的精神与法律文件、合同协议或正式文书不一致时，区块链上的参与者将需要这类职能来执行合同条款。应进一步考量以确定是否有必要设立仲裁职能。

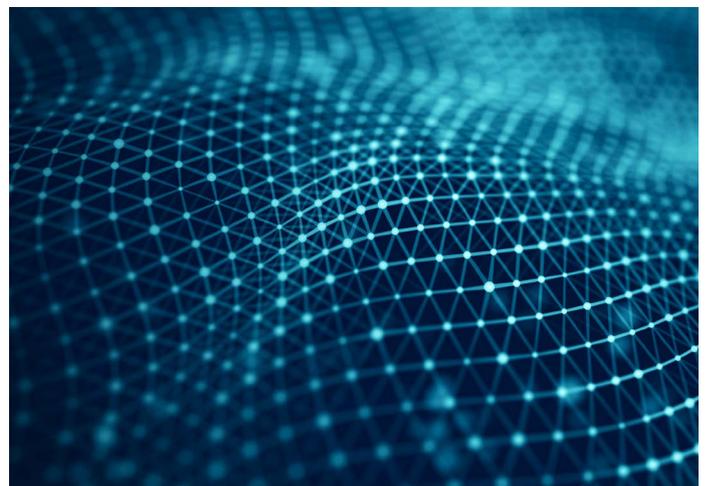
#### 结论

尽管加密货币领域存在炒作和动荡，Web 3.0技术仍将继续发展，这一投资主题仍与创投和私募股权高度相关。

无论是为下一代互联网提供资金的创投或私募股权机构，或是为Web 3.0公司或涉足Web 3.0的传统公司开展尽职调查的投资经理，还是评估新型基金和分销渠道的策略师而言，Web 3.0将是未来十年的重要主题。

尽管区块链被描述为“信任机器”，其链下组件和流程（如钱包、尽职调查和网络安全）控制措施的成熟度尚不符合这一定义。人们普遍认为，信任对于推翻人们对数字资产和交易所的悲观看法至关重要。我们往往缺乏必要的资源来确定在健全的内部控制框架内，相关风险是否得到充分管理。独立的第三方专业审计及咨询公司有能力弥合这一差距，并提供必要鉴证服务。

现在可能还不是贸然行动的时候。然而，为就投资机会做好准备，创投或私募股权机构应致力于与知识渊博、经验丰富的专业服务公司建立深厚的Web 3.0合作伙伴关系，以将这一技术趋势转化为优势和机遇。



# 参考文献



**参考文献：**

**数字资产托管的必然未来及香港的机遇与挑战**

1. Blockdata, Crypto Custody: The gateway to institutional adoption, January 27, 2022
2. Triple-a, Cryptocurrency Ownership Data
3. 10 Clouds, Embarrassed by the Speed of Your DApp? Use DApp Scaling, April 7, 2022
4. HKSAR Government's Inaugural Tokenised Green Bond Offering, February 16, 2023

**数字资产领域的DeFi和CeFi基础设施**

5. Coingecko, Global Chart, accessed March 12 2023
6. Coingecko, Top Crypto Exchanges Ranked by Trust Score, accessed March 12 2023
7. Schär, F., Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets, accessed March 13 2023

**Web3：下一代数字经济的信任基石**

8. Etherscan, Ethereum Node Tracker
9. Ethereum, SPIN UP YOUR OWN ETHEREUM NODE
10. Ethernodes, Ethereum Mainnet Statistics

**为香港Web3.0赋能的独立专业服务机构**

11. Sandro Psalia, "Building trust in crypto exchanges, 2018
12. Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession, 2017
13. Thomas Olsen, Gene Rapoport, Alexander Mitscherlich, Kelly Pu, and Parker DeRensis, 2023 Global Private Equity Report, 2023

# 联系人



**欧振兴**  
德勤中国  
华南区主管合伙人  
电话: +852 2852 1266  
电子邮件: edwau@deloitte.com.hk



**陈耀邦**  
德勤中国  
科技、传媒及电信行业  
华南区领导合伙人  
电话: +852 2531 1388  
电子邮件: ybchan@deloitte.com.hk



**罗远江**  
德勤中国  
创投及私募项目  
华南区主管合伙人  
电话: +852 2852 5658  
电子邮件: phlaw@deloitte.com.hk



**吕志宏**  
德勤中国  
数字资产香港领导合伙人  
电话: +852 2852 6324  
电子邮件: rolui@deloitte.com.hk



**何颂佳**  
德勤中国  
全球金融服务行业  
审计及鉴证合伙人  
电话: +852 2852 6489  
电子邮件: teho@deloitte.com.hk



**刘晞彤**  
德勤中国  
创投及私募项目经理  
电话: +852 2109 5135  
电子邮件: prlau@deloitte.com.hk



# 办事处地址

## 北京

北京市朝阳区针织路23号楼  
国寿金融中心12层  
邮政编码: 100026  
电话: +86 10 8520 7788  
传真: +86 10 6508 8781

## 长沙

长沙市开福区芙蓉北路一段109号  
华创国际广场3号栋20楼  
邮政编码: 410008  
电话: +86 731 8522 8790  
传真: +86 731 8522 8230

## 成都

成都市高新区交子大道365号  
中海国际中心F座17层  
邮政编码: 610041  
电话: +86 28 6789 8188  
传真: +86 28 6317 3500

## 重庆

重庆市渝中区民族路188号  
环球金融中心43层  
邮政编码: 400010  
电话: +86 23 8823 1888  
传真: +86 23 8857 0978

## 大连

大连市中山路147号  
申贸大厦15楼  
邮政编码: 116011  
电话: +86 411 8371 2888  
传真: +86 411 8360 3297

## 广州

广州市珠江东路28号  
越秀金融大厦26楼  
邮政编码: 510623  
电话: +86 20 8396 9228  
传真: +86 20 3888 0121

## 杭州

杭州市上城区飞云江路9号  
赞成中心东楼1206室  
邮政编码: 310008  
电话: +86 571 8972 7688  
传真: +86 571 8779 7915

## 哈尔滨

哈尔滨市南岗区长江路368号  
开发区管理大厦1618室  
邮政编码: 150090  
电话: +86 451 8586 0060  
传真: +86 451 8586 0056

## 合肥

安徽省合肥市蜀山区潜山路111号  
华润大厦A座1506单元  
邮政编码: 230022  
电话: +86 551 6585 5927  
传真: +86 551 6585 5687

## 香港

香港金钟道88号  
太古广场一座35楼  
电话: +852 2852 1600  
传真: +852 2541 1911

## 济南

济南市市中区二环南路6636号  
中海广场28层2802-2804单元  
邮政编码: 250000  
电话: +86 531 8973 5800  
传真: +86 531 8973 5811

## 澳门

澳门殷皇子大马路43-53A号  
澳门广场19楼H-L座  
电话: +853 2871 2998  
传真: +853 2871 3033

## 南昌

南昌市红谷滩区绿茵路129号  
联发广场写字楼41层08-09室  
邮政编码: 330038  
电话: +86 791 8387 1177  
传真: +86 791 8381 8800

## 南京

南京市建邺区江东中路347号  
国金中心办公楼一期40层  
邮政编码: 210019  
电话: +86 25 5790 8880  
传真: +86 25 8691 8776

## 宁波

宁波市海曙区和义路168号  
万豪中心1702室  
邮政编码: 315000  
电话: +86 574 8768 3928  
传真: +86 574 8707 4131

## 三亚

海南省三亚市吉阳区新风街279号  
蓝海华庭(三亚华夏保险中心)16层  
邮政编码: 572099  
电话: +86 898 8861 5558  
传真: +86 898 8861 0723

## 上海

上海市延安东路222号  
外滩中心30楼  
邮政编码: 200002  
电话: +86 21 6141 8888  
传真: +86 21 6335 0003

## 沈阳

沈阳市沈河区青年大街1-1号  
沈阳市府恒隆广场办公楼1座  
3605-3606单元  
邮政编码: 110063  
电话: +86 24 6785 4068  
传真: +86 24 6785 4067

## 深圳

深圳市深南东路5001号  
华润大厦9楼  
邮政编码: 518010  
电话: +86 755 8246 3255  
传真: +86 755 8246 3186

## 苏州

苏州市工业园区苏绣路58号  
苏州中心广场58幢A座24层  
邮政编码: 215021  
电话: +86 512 6289 1238  
传真: +86 512 6762 3338 / 3318

## 天津

天津市和平区南京路183号  
天津世纪都会商厦45层  
邮政编码: 300051  
电话: +86 22 2320 6688  
传真: +86 22 8312 6099

## 武汉

武汉市江汉区建设大道568号  
新世界国贸大厦49层01室  
邮政编码: 430000  
电话: +86 27 8538 2222  
传真: +86 27 8526 7032

## 厦门

厦门市思明区鹭江道8号  
国际银行大厦26楼E单元  
邮政编码: 361001  
电话: +86 592 2107 298  
传真: +86 592 2107 259

## 西安

西安市高新区唐延路11号  
西安国寿金融中心3003单元  
邮政编码: 710075  
电话: +86 29 8114 0201  
传真: +86 29 8114 0205

## 郑州

郑州市金水东路51号  
楷林中心8座5A10  
邮政编码: 450018  
电话: +86 371 8897 3700  
传真: +86 371 8897 3710



因我不同  
成就不凡

始于1845

#### 关于德勤

德勤中国是一家立足本土、连接全球的综合性专业服务机构，由德勤中国的合伙人共同拥有，始终服务于中国改革开放和经济建设的前沿。我们的办公室遍布中国30个城市，现有超过2万名专业人才，向客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务与商务咨询等全球领先的一站式专业服务。

我们诚信为本，坚守质量，勇于创新，以卓越的专业能力、丰富的行业洞察和智慧的技术解决方案，助力各行各业的客户与合作伙伴把握机遇，应对挑战，实现世界一流的高质量发展目标。

德勤品牌始于1845年，其中文名称“德勤”于1978年起用，寓意“敬德修业，业精于勤”。德勤专业网络的成员机构遍布150多个国家或地区，以“因我不同，成就不凡”为宗旨，为资本市场增强公众信任，为客户转型升级赋能，为人才激活迎接未来的能力，为更繁荣的经济、更公平的社会和可持续的世界而开拓前行。

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构（统称为“德勤组织”）。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为承担责任，而对相互的行为不承担任何法律责任。德勤有限公司并不向客户提供服务。请参阅[www.deloitte.com/cn/about](http://www.deloitte.com/cn/about)了解更多信息。

德勤亚太有限公司（即一家担保有限公司）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100个城市提供专业服务，包括奥克兰、曼谷、北京、班加罗尔、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、孟买、新德里、大阪、首尔、上海、新加坡、悉尼、台北和东京。

本通讯中所含内容乃一般性信息，任何德勤有限公司、其全球成员所网络或它们的关联机构并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合格的专业顾问。

我们并未对本通讯所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。

© 2023。欲了解更多信息，请联系德勤中国。

Designed by CoRe Creative Services. RITM1503440



这是环保纸印刷品