KPMG

加密资产洞察
第一期
去中心化金融简介

2021 年 10 月

序言：去中心化金融的重要性

虽然长期以来被斥为投机，但随着各类机构公开支持发展数字资产，加密经济在过去一年引发广泛关注。比特币价格频繁见诸新闻，但背后的真正原因是去中心化金融和创造者加密经济的兴起，主要体现在加密资产的交易和边玩边赚游戏（play-to-eam或P2E）的普及（“P2E”）。

本报告重点关注去中心化金融。以太坊（大多数去中心化金融生态系统的底层区块链）中“锁定的价值”在过去一年增长了 60 倍，达到900亿美元以上*。

去中心化金融由公共区块链以及智能合约（用于执行开发者和治理代币持有者设定的规则）所实现的金融服务组成，没有任何处于中心地位的个人或组织有能力干预或操纵用户的资产。

去中心化金融代表着一种全新的构建方式，以不断发展的新技术为基础，由充满热情和精通技术的市场参与者组成的大型社区推动。这种创新和竞争的组合吸引了两种潜在的对立力量——加速创新和监管关注。

创新速度非常快：似乎每天都有机构宣布新的去中心化金融借贷、交易所、保险、交易、聚合或稳定币项目。智能合约创新可能是改革传统金融服务中许多低效流程的关键。

监管机构正开始应对去中心化金融。合规风险以及与不受监管的开源代码合作的挑战，长期以来阻碍机构投资者直接投资去中心化金融（即，如果本金亏损，可能投诉无门）。投资去中心化金融应用程序对用户目前还不是很便利，这可能是许多人可能不太了解 Uniswap 或 dYdX 的原因——这两家交易所目前分别是最大的现货和期货去中心化交易所，每日处理的交易量与Coinbase不相上下**。

10年后，我们可能会回顾今天。届时，在我们的记忆中，去中心化金融的繁荣可能是加密行业整体成熟过程中一个有趣的插曲。目前仍是去中心化金融的早期，可能与互联网的早期相似——面临着成长的烦恼，但它预示着商业模式、社会交往方式和政治的根本变革。

本报告汇集了毕马威通过与监管机构、金融投资者和加密资产行业合作总结的市场洞察，阐述了去中心化金融的背景以及我们认为将影响其发展的关键因素。本系列后续报告将详细介绍去中心化金融协议的结构以及其他前沿加密资产应用案例。作为我们发布的关于去中心化金融的第一份报告，我们希望本报告为您提供有用的信息。

来源：*《去中心化金融脉搏》，2021 年 9 月 6 日访问；**Coinmarketcap.com，2021 年 10 月 19 日：Coinbase：49 亿美元；dYdX：41 亿美元；Uniswap：13 亿美元

目录

起源	4
原则与承诺	5
与传统金融和中心化金融的比较	6 - 7
技术堆栈	8 - 9
市场规模	10
监管	11
何去何从：去中心化金融的未来	12
毕马威联系方式与洞察	13 - 15
术语表	17 - 19

去中心化金融运动正以前几轮创新为基础，加速应用案例开发

去中心化金融是在区块链上进行的金融，无需中介，将参与方之间需要的信任降至最低

去中心化金融原则

- 透明 + 数据和代码不可改变
- 开源、开放访问、无需许可
- 治理分散
- 自行托管
- 应用程序可互操作
- 自动化程度高
- 价值转移

去中心化金融承诺

- 透明且可预测：
  没有处于中心的个人或组织干预的风险
- 安全性更高，用户完全掌控资产
- 创新速度更快
- 效率更高，交易成本更低

沃顿商学院与世界经济论坛提出的原则：传统金融、中心化金融和去中心化金融在原则上存在显著差异

	法定货币	加密货币	
原则	传统金融	中心化加密金融	去中心化金融
资产托管	由受监管的服务提供方或托管机构代表资产所有者持有。		由用户在非托管钱包中直接持有，或通过基于智能合约的托管账户持有。
记账单位	通常以法定货币计价。	以数字资产或稳定币（本身可能以法定货币计价）计价。	
执行	中介或机构对手方处理市场参与者之间的交易。		通过有关用户资产的智能合约执行。
清算及结算	通常在一段时间后由服务提供方、票据交换所或中心化交易所处理。		将交易写入底层区块链即可完成结算流程。
治理	由服务提供方、市场、监管机构和/或自律组织的规则规定。		由协议开发者管理，或由持有附带投票权的代币的用户决定。
可审计性	对专有代码由授权的第三方进行审计（开源代码可能进行公开验证）。		通过开源代码和公共分类账，审计师可以验证协议和交易活动。
抵押品要求	交易可能不涉及抵押品，或抵押品少于或等于所提供的资金。		由于数字资产存在波动，且缺乏信用评分，通常需要超额抵押。
跨服务交互	通过应用程序编程接口或专属中介实现有限的移动、互操作性。	交易场所通常与其他提供方（例如托管机构）集成，可以在区块链上将资产迁移到钱包。	任何服务都可以与同一区块链上的任何其他服务集成，并可能跨不同的区块链集成。
访问和隐私	由服务提供方进行身份检查。个人数据受国家隐私法律约束。		反洗钱监管机构讨论的身份验证要求。用户余额和交易活动通常是公开的。
安全	控制资产的软件系统易受黑客攻击和发生数据泄露。		易受黑客攻击以及智能合约或个人钱包的其他技术和操作风险影响。
投资者保护	政府强制规定的披露和消费者保护、反欺诈执法、风险敞口限额和保险计划。		默认用户承担所有风险，尽管诸如去中心化金融保险之类的私人安排可以提供一定程度上的保护。

资料来源：《去中心化金融超越炒作：去中心化金融的兴起》，由沃顿商学院区块链和数字资产项目与世界经济论坛联合编制。2021 年 5 月

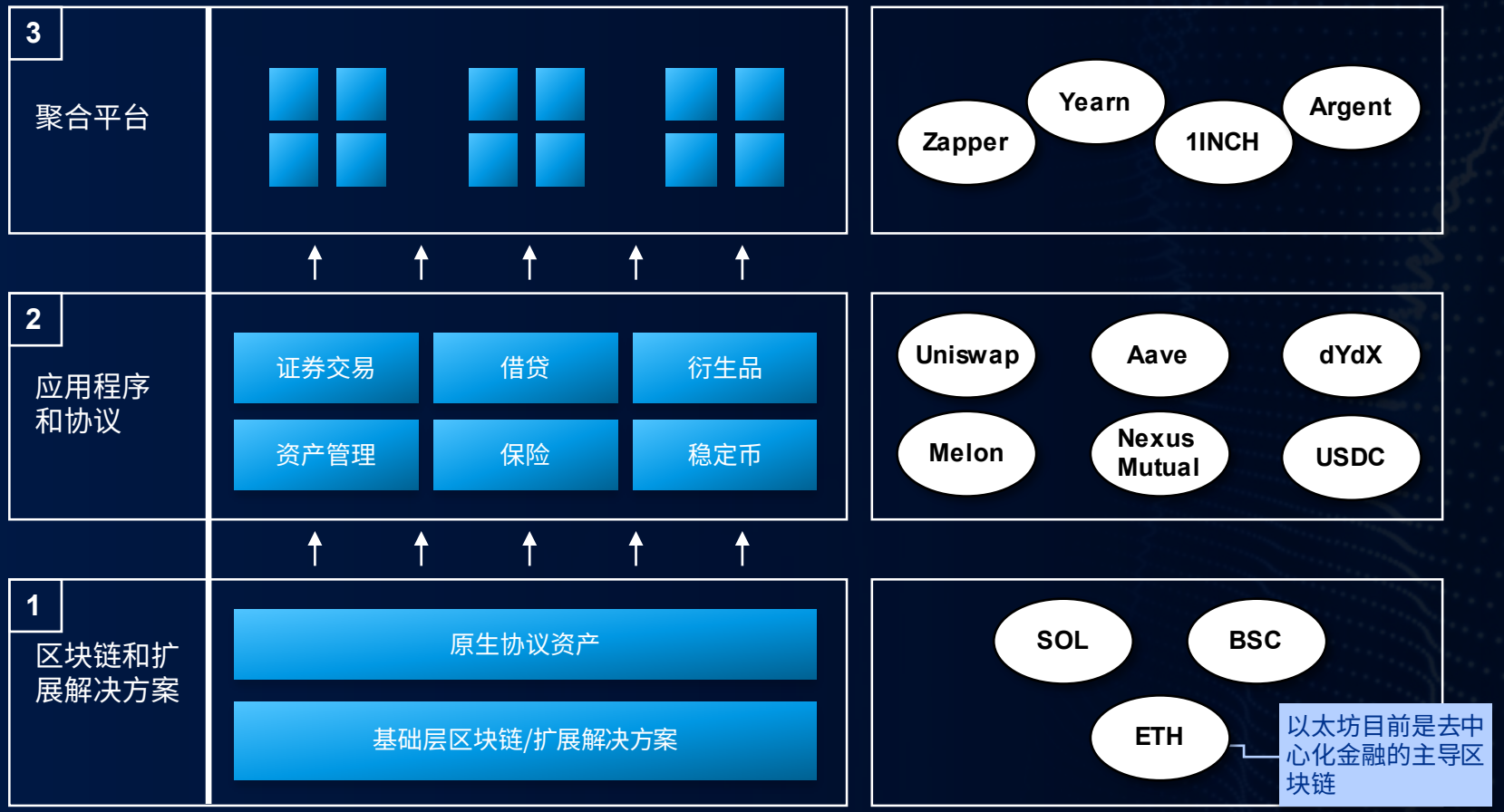
注：中心化金融一列是在原有的传统金融/去中心化金融模型中添加

去中心化金融通过去中心化应用程序提供金融服务，可能与传统金融和中心化金融服务形成竞争

	法定货币			加密货币					
	传统金融			中心化金融			去中心化金融		
货币	美元	人民币	欧元	USDT	USDC	BNB	DAI	BTC	ETH
商业银行/贷款	中国工商银行	美银美林	汇丰	BlockFi	Nexo	Celsius	Compound	Maker	AAVE
交易所	纽交所	港交所	纳斯达克	Binance	Coinbase	Kraken	dYdX	Uniswap	Curve
支付和钱包	Stripe	支付宝	Paypal	KuCoin	FTX	Huobi	Metamask	Phantom	Portis
保险	安盛	美国国际集团	平安	AON	Coincover	KASE	Opyn	Nexus Mutual	Etherisc
资产管理	黑石	东方汇理	先锋集团	Bitwise	Greyscale	Crescent	Melon	TokenSets	Zapper

去中心化金融堆栈依赖原生区块链、去中心化应用程序和协议以及建立在去中心化应用程序之上的协议

去中心化金融技术堆栈



第 3 层：聚合层：在去中心化应用程序层之上可以存在另一层应用程序，并与去中心化应用程序集成。例如，Yearn Finance聚合各种协议，跨应用程序提供有竞争力的流动性报价。

这之所成为可能，是由于共享互操作性标准实现的可组合性（就像砖块一样。去中心化金融拥有这种可组合性）。

第 2 层：应用程序和协议：协议是在底层区块链上运行的自治程序。用户以应用程序为接口，与此类协议交互。

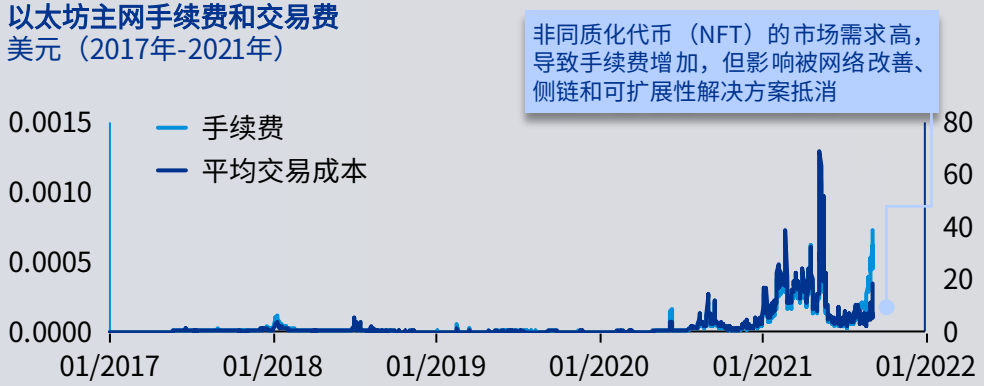
第 1 层：区块链和代币：每个网络的基础层。以太坊是去中心化金融中最常用的区块链。这一层中的替代区块链包括 Solana、Binance Smart Chain 和 Ethereum 扩展解决方案环境（例如 Polygon）。此类基础层具有原生代币，可用于支付在区块链上执行的操作，且通常能够创建和转移其他代币（同质化或非同质化）。

资料来源：基于 Schaer，2021 年，《去中心化金融：基于区块链和智能合约的金融市场》

以太坊是去中心化金融的主导区块链，但与其他第 1 层区块链相比，交易成本高，且吞吐量（每秒交易量）低

以太坊主网交易成本增速

以太坊主网手续费和交易费
美元（2017年-2021年）



为什么手续费这么高?

- 用户向矿工支付手续费，以推动以太坊区块链上交易的完成。手续费可能上涨，影响因素包括以太币的价格、交易的复杂程度以及网络流量。
- 以太币的价格以及市场的交易需求在过去一年呈爆炸式增长，部分原因是去中心化金融的兴起。

以太坊主网漏洞利用问题

抢先和逆转交易

- 在以太坊上，用户在公共“队列”（内存池）中广播交易，后续由矿工处理。每笔交易都附有手续费报价，矿工根据报价决定优先完成哪些交易。
- 恶意行为者（矿工或其他交易者）可以利用他们在决定区块打包方式中的仲裁员地位，使用此类信息“抢先”和“逆转”交易，从用户那里提取价值（“矿工可提取价值”），提高交易所代币价格和手续费。
- 据估计，矿工可提取价值总损失中，95%以上由交易所产生。

过去 30 天内因矿工提取的价值产生的总成本:**

2700 万美元

欺诈和漏洞利用

- 诸如“抽地毯”（即突然从流动性池中抽走流动性）之类的欺诈在去中心化金融中仍然很常见，但不限于以太币。
- 闪电贷漏洞利用在过去也很突出：闪电贷指的是基于智能合约的无担保贷款，可用于利用易受攻击的去中心化金融协议，以操纵价格“预言机（oracle）”，并从依赖价格预言机的去中心化应用程序中提取价值。

以太坊社区正在寻找**克服以太坊主网难题**的方法。
以太坊2.0（预计2022年发布）旨在降低手续费，通过“分片”增加交易处理能力，并从工作量证明（PoW）转向权益证明（PoS）验证机制。
与此同时，建立在**第 2 层以太坊**（例如 xDai、Optimism、Polygon）和**其他智能合约区块链**（Binance Smart Chain、Solana、Terra、Avalanche）上的去中心化金融生态系统正日益受到关注——不过仍需经历几轮创新，才能建立最佳实践和规模化流动性。

来源：*Etherscan.io **Flashbots 工具 (explore.flashbots.net)，2021 年 9 月访问

过去一年，去中心化金融中锁定的价值增长了 14 倍，超过1190亿美元。交易所是去中心化金融的重要组成部分，也是其创新能力的绝佳证明

2020 年 9 月至 2021 年期间，去中心化金融（包括 ETH、BSC 和 Polygon ）中锁定的总价值增长了 14 倍，达到 1193亿美*。

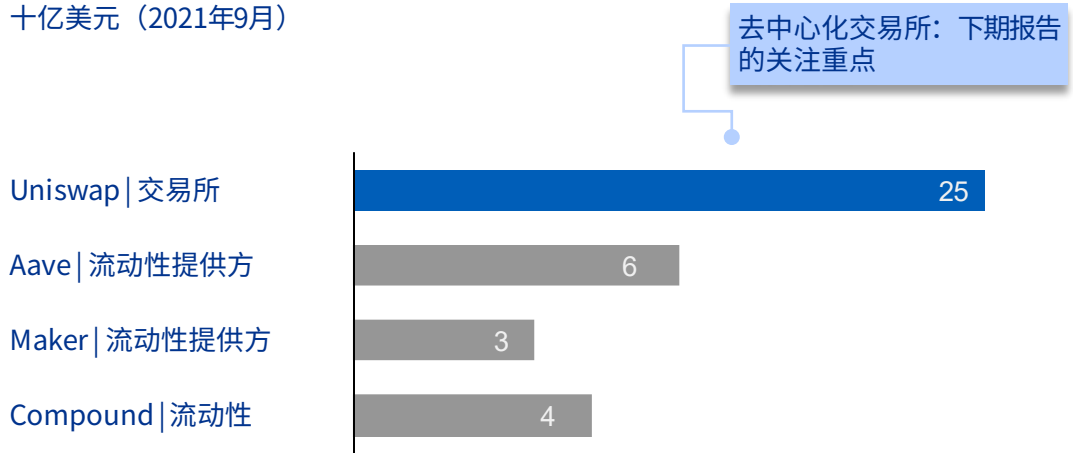
去中心化金融中锁定的总价值*
美元（2020年-2021年）

— 虽然在计算加入去中心化金融的包装代币的总价值时可能存在问题，但“锁定的总价值”（TVL）已成为衡量去中心化金融协议和市场参与度的流行指标。

— 根据平台的不同，该指标可能是指协议可以向市场参与者提供的以影响交易的代币总价值。

交易所是去中心化金融生态系统不可或缺的一部分

排名前四的DAO 代币（按完全稀释市值排名）**
十亿美元（2021年9月）



— 在中心化加密领域，最有价值的组织是 Coinbase、FTX、火币和 OkEX 等交易所。在去中心化金融中，最受欢迎的应用程序（按DAO 代币市值衡量）是一个去中心化交易所，与预期相符。

— 交易代币是去中心化金融的核心要素。通过代币的交易，流动性可以流入效益最高、需求最大的协议。去中心化自治组织 (DAO) 以代币为基础，为持有者提供奖励和/或治理权。

资料来源：*DappRadar，2021 年 7 月 9 日访问；**Coinmarketcap，2021 年 7 月 9 日

去中心化金融的快速发展让监管机构措手不及。我们认为监管终将出手

去中心化金融不适合现有监管框架

Uniswap等去中心化交易所属于无牌照经营，也未制定KYC/AML 规定。一些监管机构已就去中心化金融发表声明，但未一以贯之地执行

— EtherDelta 是一个CLOB式（封闭式限价订单簿）去中心化交易所，在 2018 年被罚款 388,000 美元，原因是为未具体说明的证券类代币的转移提供便利，且未在 SEC 注册。

— SEC 已阐明，没有协议功能的代币属于证券，但SEC执行政策缓慢且未一以贯之，导致开发者处于等待状态，因为已有其他开发者被罚，且正忙于筹集资金缴纳罚款。

事实确实如此，因为去中心化金融的监管很有挑战性

— 大多数资本市场监管机制依赖的是对中介机构问责。

— 但是，去中心化金融消除了中介机构，并导致治理和责任分散，因此成为问题。

KYC/AML是否适用?

— 在美国，KYC/AML 要求（BSA、FinCEN）取决于中介机构（即托管钱包），而在去中心化金融中不存在中介机构。

— 在没有隐私技术的情况下，在区块链上透明地标记钱包信息无疑会带来隐私问题。

这有碍于机构投资者直接投资去中心化金融

> “我认为，去中心化金融的前景确实令人激动 ……但我们不使用任何去中心化金融服务，因为我们没有能力审计自动化做市商（AMM）上的代码。我管理的是投资者的资金，我接收不了全部亏损的尾部风险。归根结底，我希望有可以追责的对象。”
>
> **— 家管理资产超过 1 亿美元的加密对冲基金董事总经理**

— 机构资金长期以来是数字资产增长的主要推动力。

— 缺乏监管可能导致欺诈/漏洞利用以及后续监管打击的风险增加。

— 这一点，再加上投资者在发生冲突时没有可以联系的中央中介机构，阻碍了机构资金流入去中心化金融。去中心化金融的增长主要依赖于零售和加密原生基金以及投资者的数量。

— 然而，机构资金通过投资相关服务（例如挖矿、对去中心化金融协议或团队的股权/代币投资）以及在受监管的交易所购买去中心化金融代币，从而推动了去中心化金融的发展，并面临相关风险敞口。

去中心化金融可能面临的监管方式

尽管目前监管形势不利，但监管资本市场的需要并未下降。由于潜在规模大，去中心化金融给监管机构带来了风险（金融犯罪、消费者保护、金融稳定）。

监管机构需要围绕替代合规等概念开发新的监管框架，使得去中心化金融的跨境性质与资本市场监管相匹配。此类新监管框架目前难以预测。

如何监管DAO?

虽然公司法可能适用于 DAO 中的参与者，但协议可以使用匿名钱包自主运行。强制关闭协议对监管机构来说可能具有挑战性（尤其是如果治理分散在许多匿名持有者之间，或者操作是自动化的）。

去中心化金融市场分化风险

如果加密资产社区认为立法不利，我们认为**流动性可能呈现分化之势**：

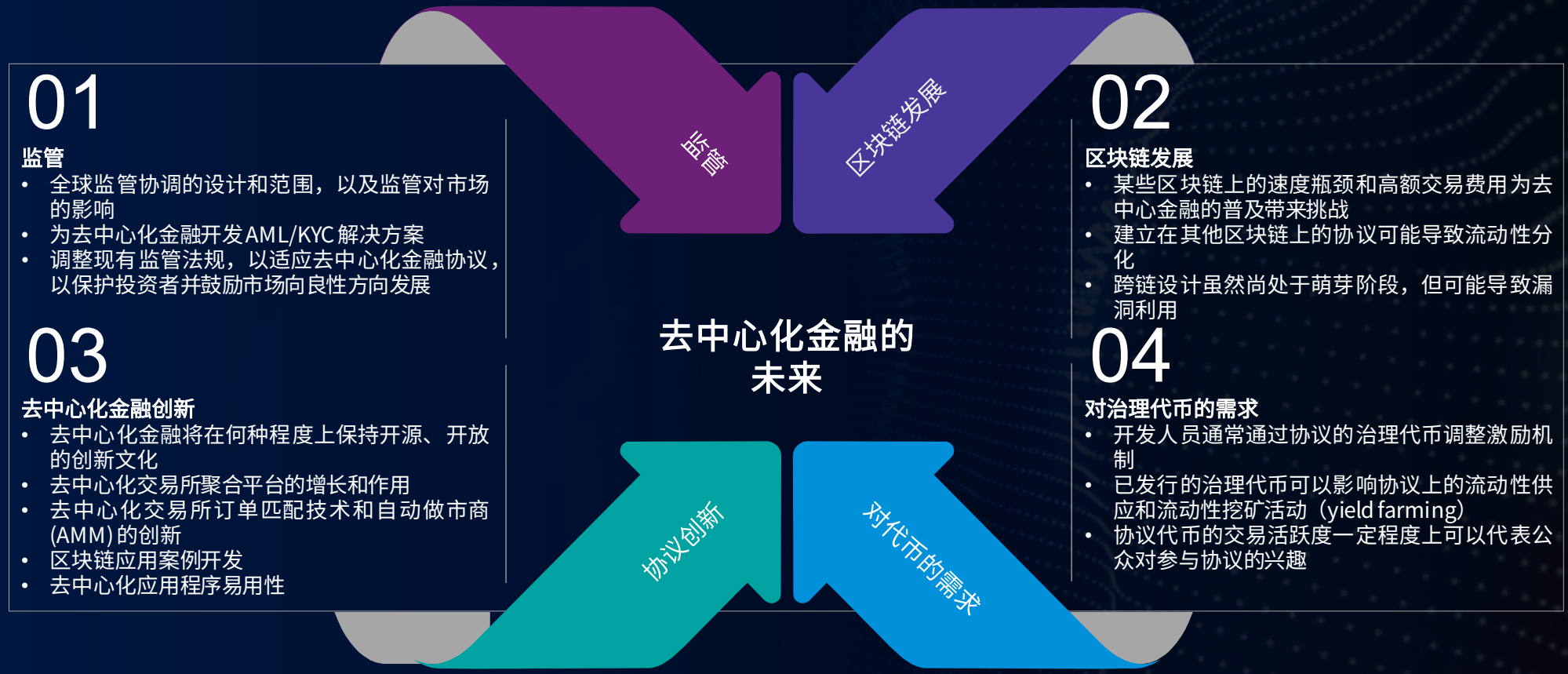
— 去中心化金融的某些部分符合监管规定，并可能更加中心化。此类交易场所可能提供机构流动性，但收益率较低。

— 收益更高、风险更高的非机构去中心化金融，主要服务零售投资者。

还可能出现区域分化，正如中心化交易所目前的情形。

资料来源：Massari、Catalini（2021 年），《去中心化金融、去中介化和未来的监管路径》，世界经济论坛和沃顿商学院区块链与数字资产项目（2021 年），《去中心化金融政策制定者工具包》

我们认为四大主题将塑造去中心化金融的未来



毕马威在加密资产的各个领域拥有丰富的经验

咨询

规划

- 战略与收入模式
- 产品管理与定价
- 领导力与治理

客户引导

- 客户引导、KYC 和投资者资格
- 资产来源
- 设立账户与资金支持
- 加密密钥配置和交易所集成
- 托管运营与物理安全
- 网络威胁防御
- 隐私
- 市场监察与欺诈监测
- 第三方风险管理
- 监管合规、集成和报告
- 储备证明

服务和交付

- 订单管理、簿记和结算
- 反洗钱、反恐怖主义融资和制裁
- Fork管理和网络治理
- 市场及网络数据
- 客户与账户维护
- 韧性与灾难恢复
- 区块链网络优化与风险管理
- 财务、损益和税务报告
- 内部审计、外部审计和鉴证

财务咨询

- 财务、技术、运营、人力资源、税务和商业尽职调查
- 估值与建模
- 筹资
- 目标公司识别及并购机会咨询
- 交易策略与股权价值故事讲述

毕马威联系方式及本报告撰稿人

中国香港

本报告作者

骆彬霖（Barnaby Robson）
财务咨询合伙人
电话：+852 6548 4923
电邮：
barnaby.robson@kpmg.com

Karl Koch
财务咨询经理

欧乐恒（James O'Callaghan）
技术支持与技术咨询主管合伙人
电话：+852 2143 8866
电邮：james.ocallaghan@kpmg.com

马绍辉（Paul McSheaffrey）
香港银行业与资本市场主管合伙人
电话：+852 2978 8236
电邮：paul.mcsheaffrey@kpmg.com

宋家宁
风险咨询合伙人
电话：+852 2978 8101
电邮：jianing.n.song@kpmg.com

Nigel Hobler
税务合伙人
电话：+852 2978 8266
电邮：nigel.hobler@kpmg.com

宋子睦
资产管理服务总监
电话：+852 3927 3008
电邮：matthew.sung@kpmg.com

庞伟祺 (Adam Bobrowski)
对本报告亦有贡献

美国（加密资产产品和服务）

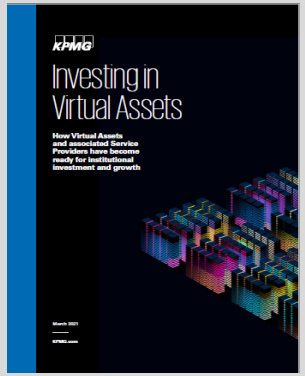
Arun Ghosh
咨询服务主管
电话：+1 617 988 1628
电邮：arunghosh@kpmg.com

Sam Wyner
咨询服务总监

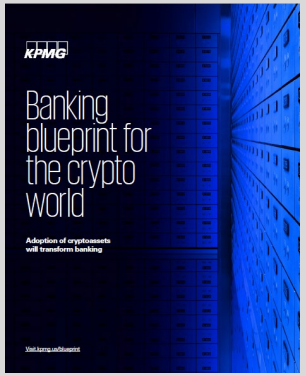
Patrick O'Kain
咨询服务经理

Okiki Famutimi
Jillian Johannes
对本报告亦有贡献

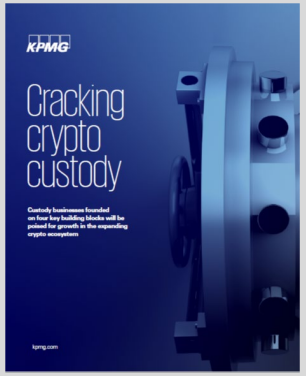
毕马威定期发布数字资产思想领导力刊物



投资虚拟资产
2021年

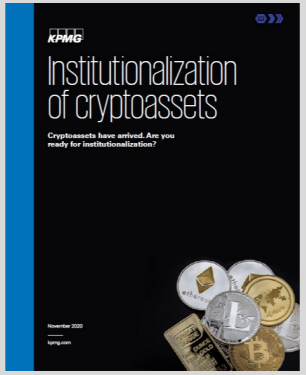


银行业加密资产蓝图
2021年



破解加密资产托管
2020年

六个关于区块链和加密资产的预测
2020年



加密资产的制度化
2020年

2019年下半年金融科技脉搏
2020年

毕马威思想领导力刊物

毕马威全球区块链和虚拟资产专业团队定期发布思想领导力和其他行业刊物，与客户和市场参与者分享我们的洞察。

此类刊物包括白皮书、调查报告、评论文章、监管分析等。

附录

术语表

术语	定义
反洗钱	为防止和/或监测洗钱制定的流程和政策
聚合平台	由网络应用程序/系统构成，用户通过单一的平台即可访问更为广泛的流动资金池
自动做市商	一种去中心化金融协议，通过流动资金池而不是传统的封闭式限价订单簿（CLOB）自动交易数字资产，无需许可
区块链	一种加密数字分类账，记录网络上发生的所有交易，并通过共识协议来确认拟加入区块链的新区块
中心化交易所	一种托管用户资金的加密货币交易所
中心化金融	通过托管用户资金的中心化公司组织提供的金融服务
加密货币	加密分类账上的代币，包括比特币和“山寨币”（在比特币之后发行的代币）。此类加密资产旨在充当交换媒介、价值存储手段，或为应用程序提供动力，通常不包括安全代币。“加密”这一术语通常用于任何基于加密技术的市场、系统、应用程序或去中心化网络
加密资产（或“代币”）	任何使用区块链技术构建的数字资产，包括加密货币、不可同质化代币（NFT）、稳定币和安全代币
去中心化交易所	一种无需处于中心地位的中介保管用户资金的加密货币交易所
去中心化金融	基于点对点软件的协议网络，可用于通过智能合约为借贷、衍生品交易、保险等传统金融服务提供便利
以太坊	一个支持智能合约交易和点对点应用程序的去中心化全球性计算平台。原生加密资产被称为“以太币”

术语表

术语	定义
法定货币	一种由政府发行的货币，无任何实物商品（例如黄金和白银）担保
Fork	对区块链的底层软件进行的根本性改变，导致产生两个不同的区块链
手续费（Gas）	以太坊区块链上使用的术语，指在区块链上进行交易时需要的成本
HODL	Hold On for Dear Life的略写，指在价格波动期间持有而不是出售加密资产
KYC	了解客户
流动资金池	持有两个或多个代币或加密资产的智能合约，目的是为市场参与者进行的交易提供便利
矿工/验证者	操作一台或一组计算机的个人或实体，将新交易添加到区块中，并验证其他矿工创建的区块。矿工收取交易费用，并因所提供的服务获得新代币作为奖励
挖矿	创建新区块以及将新交易添加到区块链中的过程。由“矿工”完成
预言机（Oracle）	在给定智能合约之外提供信息的服务、实体或智能合约。可以包括在区块链上找到的数据（价格馈送）和在区块链下找到的数据（天气、体育赛事）。通过受信任的 API 查询和验证外部数据源，然后将该信息转送到网络中的其他节点
协议	一种控制区块链运作方式的算法或软件
权益证明(POS)	区块链网络使用的共识机制/算法，根据持有代币的比例赋予验证者向区块添加交易的能力，以防止用户进行无效交易，提供分布式共识
工作量证明（POW）	区块链网络使用的共识机制/算法，根据计算能力赋予验证者向区块添加交易的能力，以防止用户进行无效交易，提供分布式共识

术语表

术语	定义
智能合约	以数字方式促进或执行交易方之间基于规则的协议或条款的软件
稳定币	旨在将价格波动降至最低的加密资产。稳定币的设计目的是跟踪标的资产的价格，例如法定货币或交易所交易商品（例如贵金属或工业金属）。稳定币可以由法定货币或其他加密资产提供担保
锁定的总价值(TVL)	在给定的去中心化协议中，锁定在智能合约中的资产金额，以美元计价
传统金融	传统的非加密货币金融，主要是指基于法定货币的金融
USD Coin（USDC）	通过 Center Consortium（由 Coinbase 和 Circle Internet Financial Limited（“Circle”）共同创立）发行的美元稳定币
USD Tether（USDT）	通过 Tether 组织发行的美元稳定币
流动性挖矿（Yield Farming）	一种提供流动性以换取奖励的策略，尤其指在短期内在去中心化应用程序之间转移资金的行为

kpmg.com/socialmedia