

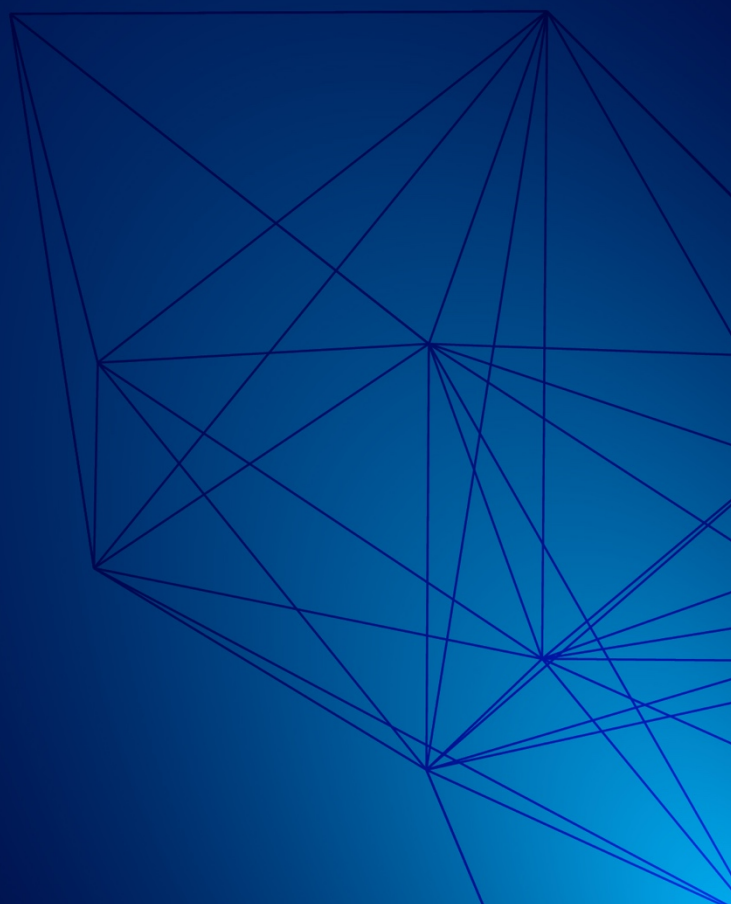


北大汇丰

PHBS FINANCIAL FRONTIER DIALOGUE

金融前沿对话

2021年第3期 总第89期



PHBS HFRI
北京大学汇丰金融研究院

主办单位：北京大学汇丰金融研究院

院长：海闻

执行院长：巴曙松

秘书长：本力

编辑：都闻心（执行） 曹明明 方垆豪 朱伟豪

北京大学汇丰金融研究院简介

北京大学汇丰金融研究院（The HSBC Financial Research Institute at Peking University，缩写HFRI）成立于2008年12月，研究院接受汇丰银行慈善基金会资助，致力于促进金融学术研究、金融市场运行、金融机构监管、金融政策决策之间的交流互动；立足粤港澳大湾区，以全球视野，构建开放的金融专业交流平台，使金融教学与金融研究相互带动，通过编辑出版专业刊物、发布专业研究报告、举办专业讲座、组织前沿学术会议等多种形式，为区域金融发展和国家金融决策提供积极的智力支持，努力将北京大学汇丰金融研究院打造成为聚焦市场前沿的金融专业智库。

北京大学汇丰金融研究院院长为北京大学校务委员会副主任、北京大学汇丰商学院院长海闻教授，执行院长为中国银行业协会首席经济学家、中国宏观经济学会副会长巴曙松教授。

2021 年值得关注的区块链十大应用领域—— 数字金融最新发展趋势

【对话主持】

巴曙松（北京大学汇丰金融研究院执行院长、中国银行业协会首席经济学家、中国宏观经济学会副会长）

【特邀嘉宾】

于佳宁（火币大学校长）

2020 年区块链行业取得了非常大的行业进展，不管是在市场、政策方面，还是在技术、应用方面都有了很大的突破。当然，其中最值得关注的还是一系列在金融领域的应用。我今天围绕以下十个主题，分享一下区块链应用和数字金融的最新动态。具体包括：加密信托、加密银行、STO、自动化做市商（AMM）与去中心化交易所（DEX）、新型稳定币、资产上链中间件（合成资产、预言机）、数字身份与数据隐私、加密收藏品、新公链基础设施、区块链分布式存储。

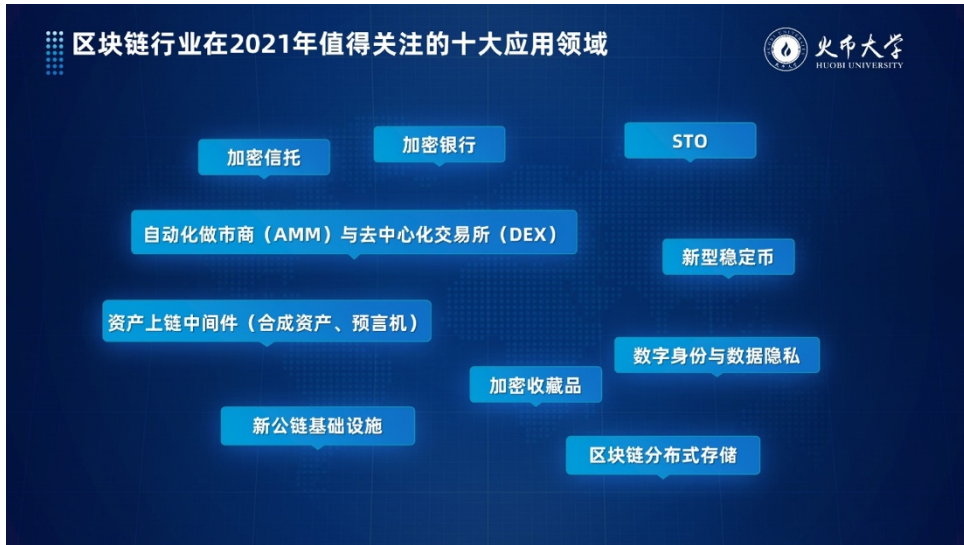


图 1

一、加密信托

加密信托，也就是最近华尔街基金配置比特币以及“灰度”的有关情况。最近，比特币的行情好，整个加密资产市场也进入了“牛市”。很多人把这轮牛市称为“机构牛”或“灰度牛”，原因是这轮牛市很大程度上源于欧美主流投资机构开始配置比特币等加密资产。2020 年 12 月 11 日，美国五大寿险公司之一美国万通人寿保险公司（MassMutual）通过纽约数字投资集团（NYDIG）为其普通保险帐户购买了价值 1 亿美元的比特币，这笔投资对于 MassMutual 而言仅仅只是其投资账户资金（约 2350 亿美元）的 0.04%。MassMutual 目前持有 NYDIG 500 万美元的少数股权。

2021 年 1 月 4 日，另类投资公司天桥资本（SkyBridge Capital）宣布推出比特币基金（SkyBridge Bitcoin Fund LP）。为了启动该基金，天桥资本及其关联公司已经投资 2530 万美元。于此同时，1 月 4 日，

天桥资本代表其旗舰基金（Flagship Funds）于 2020 年 11 月及 12 月投资的比特币基金仓位当时的市值已经达到 3.1 亿美元。Tudor Investment Corp 是一家由 Paul Tudor Jones 创建的资产管理公司。2020 年 5 月，Paul Tudor Jones 表示，其购买的比特币资产占其投资管理规模的 1%-2%。Tudor Investment 资产管理规模约 383 亿美元，其中 Tudor BVI 全球基金占 215 亿美元，Jones 通过 Tudor BVI 全球基金购买了比特币。此外，一些美股上市公司也开始配置比特币等加密资产。



图 2

这些资本和上市公司配置比特币等加密资产的背后，离不开一家神秘公司“灰度”（Grayscale）。2020 年，在全球蔓延的新冠肺炎疫情、股市崩盘以及不断加剧的地缘政治紧张局势的考验下，加之全球主要经济体前所未有的货币大放水刺激政策，传统资本渴望寻找具有明确

稀缺属性的另类资产进行投资。通过合法渠道入比特币等数字资产，成为传统投资人的需求。而“灰度”就抓住了这样的机会，搭建起了传统资本与加密世界之间的桥梁。

2021年1月14日晚，“灰度”发布了2020年第四季度数字资产报告。2020年初，该公司的资产管理规模为20亿美元。但是到了2021年1月14日，“灰度”已经拥有超过277亿美元的资产，增速颇为惊人。“灰度”成立于2013年，2020年进入快速增长期，并更加注重合规性：2020年1月21日，“灰度”比特币信托（GBTC）成功在美国SEC注册登记，成为首个符合美国证券交易委员会标准的数字资产工具；同年10月12日，“灰度”旗下的以太坊信托（ETHE）在SEC提交的注册申请也正式通过，它的资金流入与资产规模都实现翻倍增长，目前已是全球最大的加密资产管理机构。

当前，“灰度”共持有10只信托基金，9只单资产信托产品，分别对应比特币、以太坊等9种数字资产；另外还有一只数字大盘基金，包含4种数字资产，根据市值加权确定比例，分别是比特币BTC（81.63%）、以太坊ETH（15.86%）、比特现金BCH（1.08%）、莱特币LTC（1.43%），收取的年管理费为2%-3%。大型基金之所以倾向于通过“灰度”投资比特币等数字资产，是因为主要看重以下方面的优势：无需投资者亲自购买、转移和存储加密资产，也无需额外管理个人账户、钱包和私钥，因此，可以让投资者买得安心，买得省心；产品成交价格均严格跟踪市场走势，大单交易也不例外；其产品有产

权、可转让，并具备 IRA 投资资格。

二、加密银行

第二个方面的应用是“加密银行”。随着加密货币逐渐走进大众视野，加密资产的衍生金融服务需求量也越来越大。其中最直接的就是银行服务，目前已经在很多地方开展起来。2021年1月13日，发生了一件让行业热议的事情，就是美国货币监理署（OCC）对外宣布加密货币托管公司 **Anchorage** 通过了其银行牌照申请。**Anchorage** 也因此成为全美第一家获得设立“联邦级”银行许可的加密公司，美国第一家加密银行就此诞生。这对区块链行业甚至金融领域都具有里程碑意义：首先，对于 **Anchorage** 本身而言，获得这个银行牌照，使它无须再向各州政府逐个申请银行牌照，即可在全美范围内开展业务，原本加密银行想要在美国拓展业务需要的 49 张许可，现在浓缩为了 1 张；同时该公司拥有了“合格托管商”的背书，合规性使其能够吸引更多机构投资者。对于整个行业而言，该事件表明加密产业开始拥有开展相关业务的合法身份，并向正规军迈进；标志着加密银行日益成为被外界或者说权威领域认可的赛道；同时也预示着加密资产和金融不再有清晰的边界。这其实并非个例，现阶段不少具备敏锐洞察力的传统金融机构也已经开始纷纷探索布局加密银行产业。



图 3

目前，直接向加密资产公司提供服务的银行已超 30 家，其中有 90% 位于欧美地区。与此同时，近 20 家加密资产支付处理商正积极开拓类银行服务。加密银行逐渐成为金融机构加速布局的全新赛道，加密资产和金融正在实现创新融合。

三、STO（证券通证发行）

2020 年 12 月 10 日，星展银行官方公告显示，已获得新加坡金融管理局原则性获批被授予“认可市场营运商”（RMO）牌照，将正式推出全方位数字资产交易交易平台 DBS Digital Exchange。其所涉及的业务主要包括：证券化代币发行（STO）、数字资产交易和数字资产托管服务三大块。其中，星展银行此次公开要推出的 STO，对于非合规交易所来说是块难啃的骨头。而星展银行则明确表示，可支持有金融或房地产资产支撑的非上市公司股票、基金转化为代币进行交易。这

意味着，一些不具备上市条件的企业和机构，符合申请标准和监管要求后，可以将资产转化为数字资产登陆 DBS Digital Exchange，传统企业也由此接入了新型的融资通道。相比交易和托管业务，星展银行推出的 STO 被一些业内人士视作“颠覆性板块”。

三、STO（证券通证发行）

星展银行推出数字资产交易平台 DBS Digital Exchange

2020年12月10日，星展银行官方公告显示，已获得新加坡金融管理局原则性获批被授予“认可市场营运商”（RMO）牌照，将正式推出全方位数字资产交易平台DBS Digital Exchange

涉及的业务主要包括：证券化代币发行（STO）、数字资产交易和数字资产托管服务三大块

其中，星展银行此次公开要推出的STO，对于非合规交易所来说是块难啃的骨头。星展银行则明确表示，可支持有金融或房地产资产支撑的非上市公司股票、基金转化为代币进行交易。这意味着，一些不具备上市条件的企业和机构，符合申请标准和监管要求后，可以将资产转化为数字资产登陆DBS Digital Exchange，传统企业也由此接入了新型的融资通道。相比交易和托管业务，星展银行推出的证券化代币发行被一些分析人士视作“颠覆性板块”。

图 4

继星展银行后，2020年12月15日，香港上市公司BC科技集团旗下数字交易平台OSL获证监会第1类及第7类牌照，OSL也因此成为首家母公司上市、在港获牌、资产有保险覆盖、经四大会计师事务所审计的数字交易平台。OSL获牌后，既可以围绕STO展开业务，也可以上架BTC、ETH，这预示着香港有望成为全球首个完全规范的STO交易市场，意味着亚洲区的加密金融合规化已经启动，OSL也将受益于先发优势，抢占早期市场份额。这既为传统机构进场提供了有利通道，也增强了加密市场对于未来前景的信心。

STO 并不是 2021 年才出现的新产物，它早在 2017 年就已出现。当时，加密资产市场严重缺乏监管，乱象横生。特别是在 2018 年 10 月 15 日稳定币 USDT 发生信用危机事件后，人们愈发充分意识到了 ICO 无监管模式的危害。为解决 ICO 带来的乱象，美国证券交易委员会 (SEC) 就推出了 STO (Security Token Offering, 证券型通证发行)。SEC 希望在一个合法合规的监管框架下，进行 Token 的公开发行 STO 可以使持有者拥有某公司的某种所有权益，并且被美国证券交易委员会 (SEC) 合法监管，同时还要经过 KYC (客户调查)、AML (反洗钱)、合格投资者审查等监管环节。从本质上说，没有监管就没有 STO。这也让市场逐步意识到监管并不是灭顶之灾，而是给予合法身份，使其正大光明地发展壮大。图 5 为 IPO、ICO、STO 对比分析图，可以对照参考。

三、STO (证券通证发行)

>> IPO、首次通证发行、STO 比较分析 <<

项目/类型	IPO	首次通证发行	STO
证券类型	证券	Token/权益	证券
底层资产	实体有价资产	链上资产	实体有价资产
企业类型	依交易所规定不同 总体为大中型公司	几乎全部为概念型小公司 或去中心化组织	大部分为基于 实体公司的创业公司
上市成本	极高	最低	适中
企业风险	风险较小	风险极高	风险适中
融资规模	大	中小	大
监管	强	弱	尚不完善
中心化	是	否	是
运营透明	是	否	尚不完善
投资风险	中	高	较高
认证投资者	是	否	是
投资者保护	是	否	一般
24小时交易	否	7*24H	7*24H
指定交易所	是	否	有限牌照

图 5

STO 的诞生是希望将各类传统资产通证化,使得它们具有较高流动性。一方面,STO 最大优势就是主动接受监管,在有关部门的监督管理下合法合规运作,让更多的传统投资者能安全合法地参与通证的投资。另一方面,STO 能将现实世界的资产映射为数字资产,让所有权有更小颗粒的分割,在分割后就可以拥有更好的流动性,增加资产变现流通的渠道,STO 也因此被称为“数字时代的 IPO”或“IPO 的智能合约化”。

从某种意义上来说,STO 成为金融与加密资产世界的连接桥梁与融合加速器。我尝试总结了一下 STO 的优势,包括:合法合规性、快速结算、可编程性、高流动性、节约时间和成本、多重实用性。详见图 6。



图 6

当然 STO 市场在过去两年发展速度并不快,也反映其中存在一

些重要的弊端，包括：“旧瓶装新酒”、风险较大、体系不成熟、监管挑战。但是即使如此，也还有一批公司仍然坚持 STO 领域的探索与实践。总之，STO 是加密资产追求合规化、渴望主流化的一个体现，这个过程漫长而复杂，未来仍有很长的一段路要走。但 STO 在加速全球资产流动性方面带来的变革值得肯定，它或许会是未来金融发展的一种趋势。

四、自动做市商（AMM）与去中心化交易所（DEX）

基于以太坊等公链的 DeFi（去中心化金融，也就是金融类的去中心化应用 DApp）在 2020 年崛起，成为备受瞩目的明星赛道。从图 7 可以看到其增速确实颇为惊人。在该领域中兴起的了一批“去中心化交易所（DEX）”又尤为引人注目。而自动做市商（AMM）是去中心化交易所（DEX）最为关键的技术之一，这已被证明是最具影响力的 DeFi 创新之一，它能够为一系列不同通证创建和运行可公开获取的链上流动性。在自动做市商（AMM）的技术创新下，去中心化交易所 Uniswap 成交量曾一度超越老牌头部加密资产交易所 Coinbase，滑点水平达到 TOP3 交易所的现货最低水平，这就是技术革新的颠覆力量。甚至可以说，自动做市商（AMM）是最具影响力的 DeFi 创新之一，也代表了资产交易方式的变革方向。



图 7

AMM 的基本运作原理。“做市商”又称“流动性提供者 (LP)”，指的是需要在交易所上提供流动性的实体。他们为 DEX 中其他交易用户提供流动性，从而获得其他用户的交易手续费，在部分平台也可同时获得平台的激励通证。而自动做市商 (AMM) 不需要用户去挂单，而是直接通过算法去算出两个或几个资产之间交易的汇率，从而实现不用挂单等待的“即时交易”。但这样的交易池需要做市商预先存放一定数量的资产作为底仓，才能够有更好的流动性，以及更小的交易滑点在 DeFi 领域相对较火的 Uniswap 采用的是恒定乘积做市商 (CPMM) 的模式。根据 Uniswap 核心做市公式： $X*Y=K$ ， K 为常数，做市商工作时需按照实时市场价格充入等值的 A、B 两种资产，保证两个币种数量乘积不变。交易者需要交易时，可直接在交易池中按实时比例兑换，在保持乘积不变的情况下，一种资产的数量减少，

它所兑换的另一种资产数量自然会增加，这样就产生了价格的变化。自动做市商（AMM）很大程度地解决了去中心化交易所的流动性问题。但是也必须克服一些关键挑战，比如无偿损失、被迫多币种敞口、低资本效率的问题。但值得肯定的是，自动做市商（AMM）不仅仅只是实现了交易自动化、无人化，更重要的是它为金融市场引入了一种全新的交易模式和理念，或将为金融市场带来了一场范式革命。

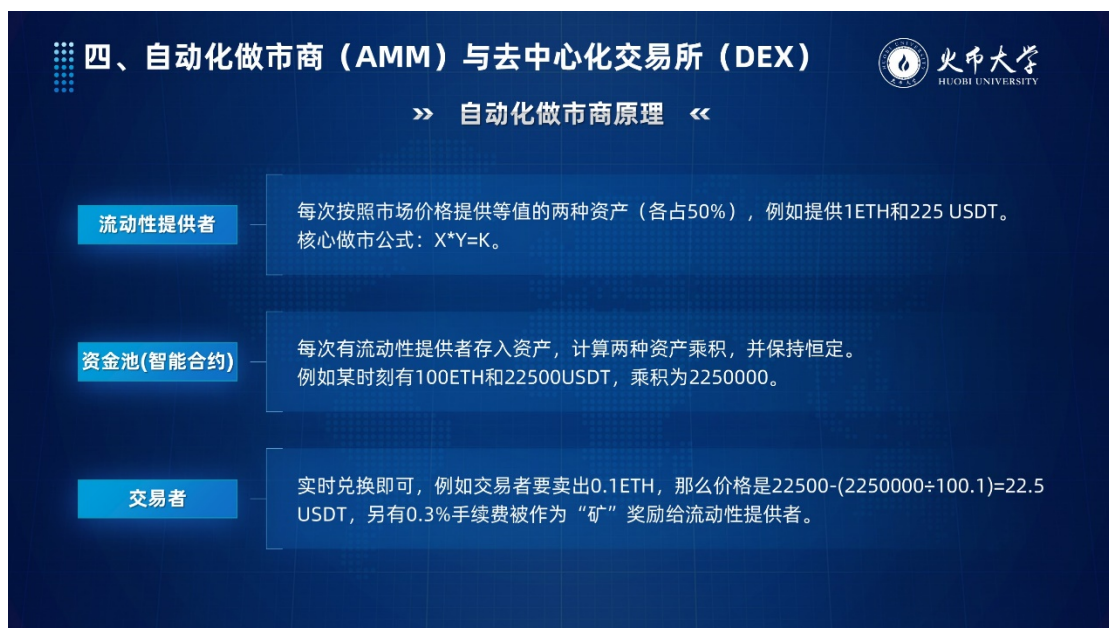


图 8

五、新型稳定币

当前，无论是比特币、以太坊，几乎所有加密资产都存在价格波动剧烈的情况，其价值属性难以被认可，无法成为通用支付工具，更多时候还是被视为一种投机/投资标的。所以，要想实现加密资产的支付属性，首先需要维持价格相对稳定，稳定币因此应运而生。2020年夏季的 DeFi 热潮，让越来越多人认清了加密资产巨大的波动性，由

此对一种价格更为平稳的通证的需求则水涨船高，稳定币也算是乘风而起了。但目前，稳定币龙头 USDT 的背后推手 Tether 多次增发 USDT，也让投资者们担忧不已，比如北京时间 2021 年 1 月 7 日 07:31，Tether 公司在波场网络又新增发 4.0 亿 USDT。Tether 的多次增发会促使人们渴望更加稳定的稳定币出现。



图 9

目前，稳定币大体分为三类模式：第一种是法币储备抵押模式：通过抵押法币，发行与法币价值锚定的稳定数字货币，即“中心化稳定币”。目前在稳定币市值中稳坐头两把交椅的 USDT、USDC，都属于中心化稳定币。这类中心化稳定币为法币与加密资产之间的流动搭建了重要桥梁，不过它们过于去中心化，所以也存在不少弊端。

第二种是数字资产抵押模式：通过在区块链的智能合约上质押数字资产，从而发行锚定法币价格的数字货币，即“去中心化稳定币”。

这个模式的代表案例是 MakerDAO 发行的 DAI，它初期专注于 ETH 质押，经历了一系列“黑天鹅”事件，就开放引入一系列中心化资产，如 wBTC、USDT、USDC 等一揽子加密资产作为质押。虽然获得了更强的稳定性，但也牺牲了部分去中心化特性。

第三种是算法模式：通过事先设定的算法机制，实现对稳定币供给数量的调节，从而使稳定币价格与法币锚定，即“算法稳定币”。像 AMPL 这类弹性稳定币就是通过算法调节货币供应量来调节价格稳定，可谓是 DeFi 世界的一种创新型稳定币。这些稳定币无须使用抵押品，试图通过市场供需来构建加密货币行业的原生通证。但没有抵押，也没有任何价值支撑，仅是通过弹性调节代币的供应量来维持币价锚定某个价值附近波动，对投机行为造成的价格波动的抵御能力弱。AMPL 上市至今，偏离锚定价格的时间高于 50%，不稳定才是它的常态。

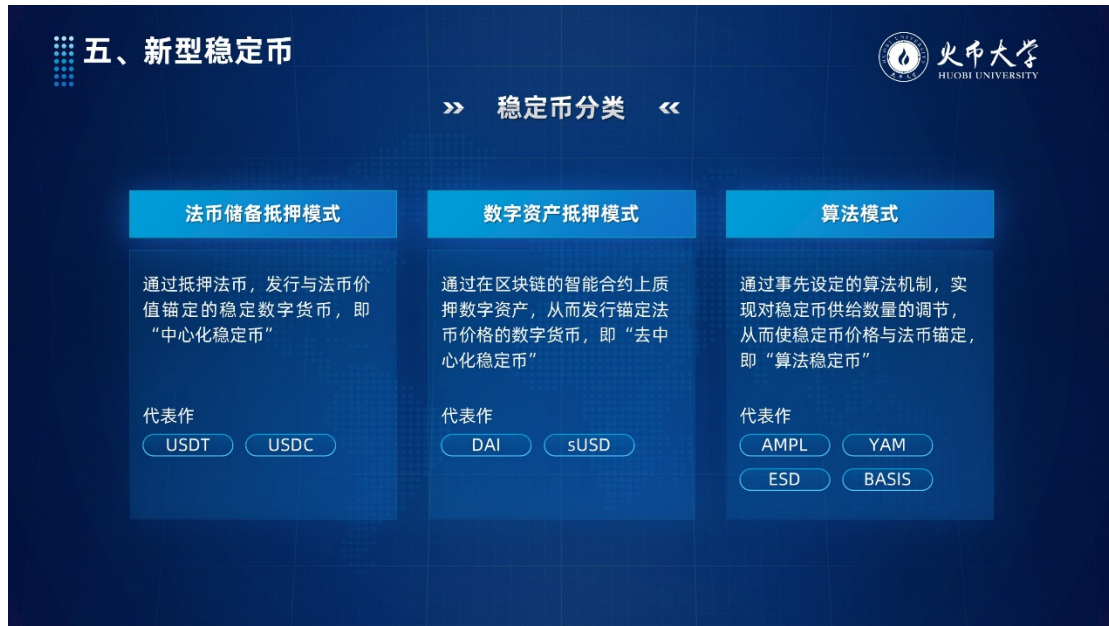


图 10

关于算法稳定币的未来，行业内有许多预测。有观点认为它的锚定点将会低于 1 美元，有观点认为将会出现锚定一揽子法币的算法稳定币，也有观点认为在 DeFi 和其他加密数字货币的加持下，一个完整的加密经济体即将出现。总之，放在历史长河中来看，仍处于混乱状态中的算法稳定币，虽然没有输出“稳定”，却为我们揭示了另一种秩序与规则。

六、资产上链中间件（合成资产、预言机）

从某种意义上来说，资产上链可能是区块链落地应用最好的方式之一。过去，我们讲“资产上链”，其实是指把现实世界的资产，比如房地产股权、债权，通过权力机构的授权或者确权来登记在区块链上。显然，这个路径是比较漫长的。现实世界的资产进入到数字世界，中间隔着一道栅栏，所以就需要用“中间件”来连接链上链下。DeFi

领域的“资产上链”其实是通过抵押数字资产来生成合成资产，并且合成资产的价格跟现实资产的价格形成一种锚定的关系来间接实现资产上链。这个过程其实有点儿像一种天平，天平的左边放着抵押资产，那么天平的右边就放着合成资产。

正如巴比特创始人长铗指出：“DeFi 就相当于给资产这个平面引入了一个虚坐标，我们用虚函数来实现了这样一个资产的映射过程。在映射过程里，其实也相当于资产的上链。就像第一个很成功的合成资产 MakerDAO 的 DAI，已经被广泛接受，它其实也可以充当美元使用。”我们可以将合成资产理解为模拟另一种资产价值的金融工具，可以为投资者提供更多样化的资本配置、对冲风险的机会，以及增加投资回报的工具，从而成为打开真实世界资产的价格敞口。

六、资产上链中间件（合成资产、预言机）

现实世界的资产进入到数字世界，中间是隔着一道栅栏的，所以就需要用“中间件”来连接链上链下。

DeFi领域的“资产上链”其实是通过抵押数字资产来生成合成资产，并且合成资产的价格跟现实资产的价格形成一种锚定的关系来间接的实现资产上链。

这个过程其实有点儿像一种天平，天平的左边就放着抵押资产，那么天平的右边就放着合成资产。

DeFi就相当于给资产这个平面引入了一个虚坐标，我们用虚函数来实现了这样一个资产的映射过程。在映射过程里，其实也相当于资产的上链。

图 11

预言机其实是一个将数据从系统外传输到系统内的工具。人们提

起区块链，总是说它所有交易记录链上可查、安全透明，但是要知道区块链是一个确定性的、封闭式的系统，运行在区块链上的智能合约是无法直接从外部获取数据的，只能在一个封闭、孤立的环境中执行任务。而预言机就可以作为智能合约和外部世界之间的双向桥梁，充当中间件，将链外数据真实输入到链内，从而保障链上数据真实性。

以预言机领域比较受到关注的 Chainlink 为例。Chainlink 是一个去中心化的 Oracle 网络，由数据的购买者和提供者组成。购买者请求数据，提供者以安全可信的方式返回数据。购买者选择他们想要的数
据，供应商竞标提供这些数据。供应商在出价时必须质押一部分 LINK 代币，如果行为不当，可将其扣除。同时，Chainlink 会使用 Oracle 信誉系统对提供的数据进行汇总和加权。Chainlink 共有 21 个信任节点，也就是 21 个现实信息的收集者。在信息传递中，Chainlink 要求必须有不少于 14 个节点提交信息才能计算可信答案。为防止信任节点团伙作恶，Chainlink 引入了节点声誉以及抵押代币的机制。

七、数字身份与数据隐私

随着人类社会的发展变迁，生产要素也随之改变。农业时代，土地和劳动力是主要生产要素；工业时代，资本和技术是主要生产要素；数字时代，数据成为最重要的生产要素之一。相较于传统生产要素，数据作为生产要素具有独特属性，比如易复制性；价值聚合性和多样性；价值认知多样性；交易关系将从买卖关系变为租赁关系。基于这些独特属性，我们在挖掘数据价值方面，往往面临一些挑战。



图 12

那如何找到高效利用数据资源与实现个人隐私保护的平衡点？实际上，实现数据隐私保护，核心是要建立起数据使用者和数据所有者之间的信任关系。当前，利用区块链+隐私计算，搭建基于区块链的分布式信任机制，可能会是比较好的解决方案。

一方面，利用区块链技术，可以把各自的数据上链，拥有自己的“数字身份”，从而多方建立一个联合参与共识的场景；同时使用密码学算法，实现链上数据难篡改、可追溯，从而实现数据的安全存储和转移；此外再基于智能合约等做一些数据治理和审计，由此支撑分布式的商业模式。另一方面，采用基于场景优化的隐私计算方案，其相较于传统的、通用的隐私计算解决方案，更高效实用。

总之，区块链和隐私计算相辅相成，可以更好地挖掘分布式场景下数据要素的价值。区块链技术注重多方参与，可以提高隐私保护的

安全性和透明度；隐私计算专注于多方参与过程中的用户数据保护，可以实现信息最小化披露，可以增强区块链的合规性，扩大其协作度。

未来，在区块链+隐私计算所搭建的生态里，我们每个个体都可以真正拥有自己的数据控制权，可以利用自己的“数字身份”安全存储数据，同时在使用某个业务时做“选择性披露”，从而进行可信安全的社会活动，并真正释放数据价值。



图 13

八、加密收藏品

2020 年在中国市场上看到更多的潮鞋文化、联名设计、盲盒经济的兴起，这些背后的核心逻辑就是 IP 的崛起，而 IP 则是未来所有产业的灵魂。在这样的一个 IP 时代，如何实现价值的流转，让产品的文化属性有更坚实的经济价值？可以看到，以区块链为基础的新型 IP 文化形态，以 NFT（非同质化的通证）开始崛起。NFT 全称为 Non-

fungible Token，中文名叫“非同质化通证”。常见的 Token（如 BTC、ETH 等）都是同质化的，每个 BTC 之间没有任何区别，可以互换和分割。而 NFT 的重要特征在于：每一个 NFT 拥有独特且唯一的标识，两两不可互换，最小单位是 1 且不可分割。我们可以把批量印刷的明信片理解为 FT，那么明星签名的明信片就是 NFT，因为这张明信片是明星在特别的时间、特别的地点、特别的场景签名的，这赋予了它特殊的意义，所以这张明信片就变得独一无二，具有了收藏价值。

2020 年 10 月 7 日，纽约佳士得拍卖行出现了一幅数字艺术品，没有实体承载的艺术品《心灵肖像》。这是一个以比特币为主题的系列艺术品中第 21 幅作品，以超过 13 万美金的价格成交，超出了很多人的想象。2020 年 1 月，欧洲足球锦标赛有超过两万张的门票以 NFT 形式发行。NFT 门票不需要原本发行机构参与验证，保障了门票的真实性，减少了交易市场摩擦，方便门票交易买卖。NFT 目前来看主要集中在加密艺术领域，但实际上文化价值在于版权。未来所有产业都与 IP 紧密结合，而 NFT 的价值不仅仅局限于艺术领域。在下一个文化艺术和产业相结合的爆发点，下一个盲盒经济中，NFT 将是关键性的桥梁。



图 14

九、新公链基础设施

公链赛道一直是区块链领域的热门赛道，提到公链不得不提的就是以太坊 ETH 和波卡 Polkadot。可扩展性一直是困扰以太坊发展的问题，尤其是 2020 年 DeFi 应用爆发，网络拥堵导致了高昂的手续费。性能不足让以太坊很难达到“世界计算机”的要求，也影响了用户体验。扩容是以太坊网络的当务之急，2020 年以太坊的进展主要集中在扩容方面。

那什么是以太坊 2.0？我们可以把 ETH 2.0 理解为一个处理各类货物的港口，信标链就是港口的灯塔，所有的货轮都要接受它的指挥和调度。分片链就是货轮，负责实际的货物运输工作。ETH2.0 的重要目标之一，就是对 ETH 1.0 进行扩容，大幅提高合约和交易的吞吐量，所以开发者设计 64 条分片链来并行处理链上事务，从而为以太坊提供高性能与可扩展性。

目前 ETH2.0 信标链已经上线，ETH2.0 整体上线预计要到 2022 年。面对日益增长的扩容需求，以太坊联合创始人 Vitalik Buterin 于 2020 年 10 月提出了一个新的以 rollup 为中心的以太坊路线图。面对此番战略转移，社区提问：在 Phase 0 上线后，以太坊 2.0 spec（计划）最大的变更会是什么？Vitalik 回应：有三个最重要的变化，具体参见图 15。之所有这些变更，都是为了一件事——让 ETH 2.0 更快上线，让人们更快用上。

九、新公链基础设施（以太坊2.0、波卡）

以太坊 2.0 路线图的变更

社区提问
在 Phase 0 上线后，以太坊 2.0 spec(计划)最大的变更会是什么？

Vitalik
有三个最重要的变化

- 路线图以 Rollup 为中心。将“Phase1”简化，仅用于承载分片数据(以便使用Rollup方案)的内容，实现起来更容易；
- 简化合并方案。在去年 10 月份，我发了一篇帖子，提到了以太坊 1.0 向以太坊 2.0 的过渡路线图。目前仍然是大致按照这个路线图的方案，但是有两点不同：
 - a. ETH 1 的交易将直接在信标链上，而不用放到分片之中；
 - b. 由于 Optimistic 方案的执行，可能大大缩短在 ETH1 和 ETH2 的合并期间的暂停时间。这使得合并实施起来更容易，并且我们也开始在创建 PoC（概念验证方案）阶段了；
- 各阶段并行。这是最新的考虑，也可能最容易被低估。本质上，轻客户端支持、数据分片(又名“阶段 1”)和合并方案，都会彼此独立，所以，无论其他的组件处于什么阶段，每个模块只要准备好了，就可以实施。

之所有这些变更，都是为了一件事：让 ETH 2.0 更快上线，让人们更快用上

图 15

另外一个重要的公链则是波卡，由 Parity 技术公司于 2017 年 11 月开始开发的，由以太坊前 CTO Gavin Wood（林嘉文）主导。波卡（Polkadot）的代币 DOT 上涨了近 70%，目前市值已经突破 161 亿美元，这也使其超越瑞波 XRP 成为市值第四的加密资产。根据 Gavin Wood 在白皮书中的描述，Polkadot 是一个区块链协议，旨在支持“不

同开发者创建的平行链”。简单来说，Polkadot 是一个由多条区块链异构组成的区块链集合，其在做的就是一套基于区块链技术的操作系统，类似于 Windows Android、iOS。可以利用波卡来开发各种各样的应用，也可以把现有的应用通过技术接入到波卡系统当中。波卡系统具有极高的跨链性能，这给其生态上的各种应用提供了极强的交互性，被业内人称为“跨链之王”。

近期，波卡的“平行链插槽拍卖”成为业内热点。如果说波卡是一条旺盛的商业街，插槽就是街边的旺铺。要想在商业街中售卖自己的商品，就必须参与到插槽拍卖中。北京时间 2021 年 1 月 13 日凌晨 3:00 左右，万众瞩目的波卡平行链开发工作再次迎来一大里程碑，平行链测试网 Rococo V1 正式开放注册申请，这意味着 Kusama 和 Polkadot 平行链插槽拍卖和上线将逐渐拉开帷幕。

十、区块链分布式存储

存储并不是一个新领域，目前存储行业主要有四类：桌面级存储、企业级存储、云存储和区块链存储。伴随区块链技术的发展与成熟，区块链存储开始愈加受到关注，它旨在解决此前存储市场存在的四个关键问题包括：1. 数据存储成本太高；2. 数据中心化管理风险较大；3. 大规模数据传输和维护较难；4. 容易受到攻击。区块链存储，也称为“分布式存储”，是指用区块链激励构建的去中心化存储系统，是区块链和存储系统的有效结合。区块链本身是一个分布式的账本，是一个分散数据库，使得区块链技术在存储方面具有先天的应用场景

和优势。



图 16

分布式存储（IPFS）（InterPlanetary File System，星际文件系统）是一种内容可寻址的点对点超媒体协议，旨在取代传统互联网协议 HTTP，创建开放的分布式存储和共享文件的网络传输协议。在 IPFS 网络中的节点构成了一个分布式文件系统，任何人可以在全世界任何一个地方快速获取存储在 IPFS 系统上的文件。具有下载速度快、全球存储、安全、数据永存等优势，能可以很好解决 HTTP 现阶段所存在的问题。

其中，“内容寻址”是 IPFS 当中极为关键的一环。那什么是“内容寻址”呢？假设你想从网上下载一张照片，你需要告诉电脑去哪里找这张照片，也就是照片所在的 IP 地址或域名——这就叫“地址寻址”。而 IPFS 则是把“地址寻址”改为“内容寻址”，即每个文件都

有其独特的哈希值,我们也可以理解为指纹,当你想下载某个文件时,只需问网络“谁有含有这个哈希值的文件”,然后 IPFS 网络上的某个节点就会将文件提供给你。而 Filecoin 正是由 IPFS 同一团队 Protocol Labs (协议实验室)开发的项目,属于 IPFS 之上的一个激励层,激励机制则是 FIL 通证。在 Filecoin 网络中的矿工可以通过为客户提供存储和检索服务来获取 FIL;相反,客户可以通过花费 FIL 雇佣矿工来存储或分发数据。

简单来说,Filecoin 项目的目标是整个云存储市场,把所有闲置的存储资源利用起来,形成一个算法市场。随着 5G、大数据的发展,云存储市场体量不断增长,在 Filecoin 的炒作热度之下,存储领域吸引了不少流量和资金,迎来了更多关注和机会。

十一、 问答环节

Q1: 区块链在我国金融领域的应用和发展面临的最大障碍是什么呢?趋势如何?

A1: 大公司比较倾向于建设联盟链系统,大部分区块链项目仍处于“金融科技”的层面,距离资产数字化仍然差了“临门一脚”,主要原因一方面是技术的瓶颈,另一方面是全球监管对于加密资产的模糊性,随着越来越多的国家将加密资产与数字金融纳入立法,合规态势愈发清晰,我个人预计在 2021 年就会有更多突破性的案例。

本文根据北京大学汇丰金融研究院执行院长巴曙松教授发起并主持的“全球市场与中国连线”第三百四十三期（2021年1月18日）内容整理而成，特邀嘉宾为火币大学校长于佳宁博士。

于佳宁，经济学博士，毕业于中国人民大学，副研究员职称，权威区块链专家，区块链教育专家，“产业区块链”理念提出者，被《中国周刊》誉为“培育‘区块链思维’的领路人”。于佳宁博士曾任工业和信息化部信息中心工业经济研究所所长等职务，曾参与多项国家政策起草研究工作。于佳宁博士现任火币大学校长、中国通信工业协会区块链专委会轮值主席、中国技术经济学会区块链分会副理事长、中国民营科技实业家协会区块链技术应用专业委员会副理事长兼数字经济智库院长、全国高校人工智能与大数据创新联盟区块链专委会副主任委员、中国计算机学会区块链专委会委员、中国工业与应用数学学会区块链专委会会员、海南自贸港区块链试验区特聘专家、亚洲区块链产业研究院（新加坡）产业咨询委员会委员、中国国际商会区块链创新服务产业委员会特聘专家等职务。

【免责声明】

“全球市场与中国连线”为中国与全球市场间内部专业高端金融交流平台。本期报告由巴曙松教授和熊婉芳博士共同整理，未经嘉宾本人审阅，文中观点仅代表嘉宾个人观点，不代表任何机构的意见，也不构成投资建议。

本文版权为“全球市场与中国连线”会议秘书处所有，未经事先书面许可，任何机构和个人不得以任何形式翻版、复印、发表或引用本文的任何部分。



PHBS HFRI
北京大学汇丰金融研究院

