去中心化金融的交易机制综述

邓钇敏[1,2]，司世景[1]，王健宗[1]，李泽远[1]，肖京[1]
1. 平安科技（深圳）有限公司，广东 深圳 518063；
2. 中国科学技术大学先进技术研究院，安徽 合肥 230026

摘要
去中心化金融（DeFi）是一种基于区块链和智能合约提供金融服务的新范式，现已涉及包括借贷及其衍生品在内的众多领域。因此，作为DeFi基础的交易机制成为重要的关注点，其直接影响着上层应用的稳定性。主要讨论DeFi领域的交易机制，首先介绍与交易机制相关的概念和协议；然后通过实现方式对交易机制进行分类，分别详细讨论了基于交易委托账本、自动做市商和聚合器方法的交易机制实现，并比较归纳实现方案之间的区别与联系；最后分析并总结了去中心化交易面临的公平性、安全性、匿名性问题，提出了相关的未来研究方向。

关键词
区块链；去中心化金融；去中心化交易所；交易机制；自动做市商

中图分类号：TP399 文献标志码：A doi: 10.11959/j.issn.2096-0271.2022064

Exchange mechanism for decentralized finance: a survey

DENG Yimin[1,2], SI Shijing[1], WANG Jianzong[1], LI Zeyuan[1], XIAO Jing[1]
1. Ping An Technology (Shenzhen) Co., Ltd., Shenzhen 518063, China
2. Institute for Advanced Technology, University of Science and Technology of China, Hefei 230026, China

Abstract
Decentralized finance (DeFi) is a new paradigm for providing financial services based on blockchain and smart contract, which support many applications including loans and derivatives. Therefore, the exchange mechanism of DeFi has attracted large amount of attention, as it directly affects the stability of upper-level applications. The exchange mechanism of DeFi was reviewed. Firstly, the concept and the protocols related to exchange mechanism were introduced. Secondly, the transaction mechanism was classified through their approaches of realization, and the methods based on order book, automated market maker and aggregator were discussed respectively. The differences and connections among the implementation of those methods were introduced. Finally, the fairness, security and anonymity problems faced by the decentralized exchange were analyzed and summarized, and potential future research directions were proposed.

Key words
blockchain, decentralized finance, decentralized exchange, exchange mechanism, automated market maker

0 引言

区块链技术和数字资产行业的发展提供了一种解决传统金融问题的全新方案。去中心化金融（decentralized finance，DeFi）[1]是一种基于区块链技术的应用，通过开源协议和分布式网络提供无中介要求的金融服务。特别是DeFi具备解决传统金融行业中存在的信息流通速度慢、中介机构的额外成本高等问题的独特潜力，现有的DeFi应用涉及包括交易、借贷[2]、加密货币衍生品[3]在内的众多金融领域，市场表现活跃。面对社会动荡等不安因素，市场缺乏可靠的中心化托管时，DeFi模式更能促进资产的流通。

DeFi的技术基础是区块链和智能合约（smart contract）技术，其中区块链提供了一种分布式交易记录账本的实现方式，DeFi的诸多协议均可被视作账本的上层应用。此外，智能合约同样是DeFi能够被广泛应用的重要基础。智能合约本质上是一组被预先定义的处理事务规则的程序编码，智能合约语言支持原语和条件执行操作，极大地拓展了DeFi协议的表达能力。

DeFi的应用经济生态涉及不同层面的多种协议，其中最重要的是链上资产交换（asset exchange）协议，交易机制的设计关系到复杂应用的稳定性。常见的资产交易表现形式可以被分为中心化交易所与去中心化交易所（decentralized exchange，DEX）两类。中心化交易所本质上是基于中央机构的数字化实现，去中心化交易所则由于分散式运作，提升了交易的公平性和透明性，得到了广泛研究和关注。

在现有的文献中，已有研究者对区块链[4]、DeFi[5]以及DEX[6-7]进行了综述。然而就DeFi的交易机制而言，现有的研究成果[6]局限于特定的交易机制实现方式，目前还缺乏系统性的综述工作。为此，本文从去中心化交易所的交易协议设计出发，概述了相关研究成果，提出了统一的表述形式，分析了各类交易机制的优缺点，最终总结出去中心化交易所交易机制的应用优势和发展方向。本文对DeFi交易机制进行了系统性梳理，希望进一步丰富交易机制的研究内涵和充实现有金融理论体系，助力完善市场激励和监管制度，为后续的深入研究和技术应用提供系统性的参考意见。

1 基础概念

1.1 区块链

2008年中本聪提出了比特币（Bitcoin，BTC）[8]的构想，在其设计中，交易记录通过一种以区块相互链接的方式来维护，由此产生了区块链的概念。作为比特币的技术基础，区块链是一种基于密码学方法链接的不断增长的分布式记录账本。与传统的账本实现方式相比，区块链的分布式账本信息由参与者基于共识算法来维护，具有透明可追溯和难以篡改的特性。

区块链结构如**图1**所示，一个区块通常由区块头和区块体组成，并且区块头中保存了前一区块的哈希值，以此形成链式结构。区块头中的数据结构主要包括版本、时间戳、随机数、树哈希等内容。其中，随机数主要用于基于工作量证明[8]的共识机制的建立，而树哈希则用于简易支付验证的改进，降低了数据结构的规模，提升了网络传输性能[9]。区块体包含了事务信息，以便参与者进行验证。

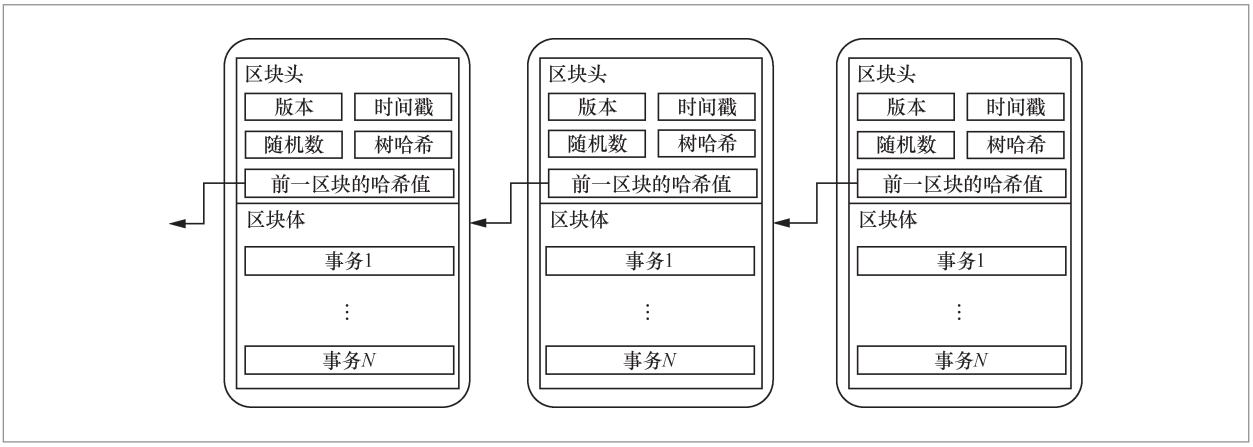

图1 区块链结构

区块链目前已经逐步发展为涉及多层次的体系结构[10]，如图2所示，DeFi领域的研究与实现主要集中于应用层。

此外，DeFi的成功应用还依赖于作为技术基础的智能合约。智能合约最早于1995年被提出，其是一种以数字形式定义并基于程序化方式执行的交易承诺[11]。2013年，以太坊（Ethereum）白皮书[12]提出比特币是一种弱化的智能合约的观点，基于此观点提出了以太坊的设计，其中包括图灵完备语言以及以太坊虚拟机的构想，以此实现了基于区块链的智能合约技术。

智能合约的本质是一组处理事务规则的程序编码，且处理规则由区块链的共识机制确认。智能合约依赖于具备状态机机制的区块链，且参与方能够以一定方式与区块链进行交互。当事务信息被确认后，合约代码就会在区块链网络中的所有节点上执行。执行过程需要消耗算力成本，因此需要向合约的参与方收取费用。以太坊将燃料（gas）定义为衡量算力资源消耗的量化指标[13]，当执行交易时，燃料将按照特定的规则逐渐减少。智能合约的执行语言允许条件执行和迭代操作，能够与具备相同上下文环境的事务进行交互以及支持原子性操作，这些特点使得其具备足够的描述协议具体内容的表达能力，因此能够创造具备复杂功能的DeFi应用。

图2 区块链层次体系结构

1.2 去中心化金融

近年来，DeFi已经从区块链基础[14]发

展成复杂层次体系[15]，如图3所示，DeFi的基础架构可以分为基础设施层、资产层、协议层。

● 基础设施层：该层次的功能为提供应用基础设施。该层次主要由区块链及其原生协议组成。区块链原生协议主要指底层区块链原生资产协议，如比特币[8]、以太币（ETH）[12]，该协议联系了部分基础设施层与资产层的功能。基础设施层提供了可信存储事务的方式，确保能够基于共识机制确认事务状态的转变。

● 资产层：该层次的功能为确定资产协议。该层次主要由区块链原生协议以及能够被基础设施层区块链接受的其他资产协议组成，这些资产协议通常被称作通证（token）。

● 协议层：该层次的功能为设定用例标准，例如为交易、借贷、加密货币衍生品和投资管理等提供标准定义，这些标准通常以一组智能合约的形式实现。为了便于向用户提供基于协议的服务，开发者基于协议层开发了不同种类的用户应用接口，通常以基于Web浏览器的方式与智能合约交互。

鉴于DeFi领域的复杂性，接下来主要对与交易机制相关的协议进行介绍，以便说明其内涵。相关协议包括通证、稳定币（Stablecoin）以及链上资产交换协议，通证主要提供交易的货币基础；稳定币确立了通证的价值关系；链上资产交换协议则由一类协议组成，其中最重要的是去中心化交易所协议，其保障了交易的实现。

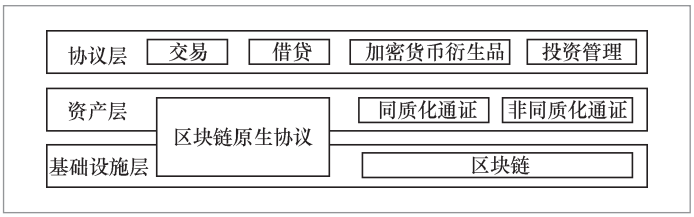

图 3 DeFi 架构

● 通证：通证的定义为以数字形式存在的权益凭证[16]。通证目前主要有两种形式：一种是以ERC-20标准[17]为代表的同质化通证，另一种是以ERC-721标准[18]为代表的非同质化通证[19]。两者的主要区别在于通证中的不同个体间是否能直接互换，同质化通证的不同个体间能够直接互换，类似于货币的价值系统；非同质化通证的不同个体间不能直接互换且存在本质性差异，类似于权益的价值系统。DeFi中的交易行为主要面向同质化通证，非同质化通证的交易更类似于拍卖行为。

● 稳定币：稳定币[20]本质是一种以锚定法定货币（通常为美元）为单位，通过嵌入稳定机制保持价格稳定的数字货币，其中比较引人注目的是MarkerDAO的Dai[21]币，其通过超额抵押资产并在抵押资产价值低于抵押线时触发清算的方式维持价格的稳定。另外，泰达币（Tether USD，USDT）[22]虽然不属于DeFi领域中的稳定币概念，但由于其依赖于可信第三方的维护，经常被用于其他DeFi协议并起到相似的作用。除了基于抵押机制实现，还有单纯依赖算法实现在锚定价格附近波动的稳定币，如AMPL（Ampleforth）[23]。总而言之，稳定币的使用为交易行为提供了价值参考，数字货币以及其他权益通证的价值能够通过稳定币与法定货币建立联系，保障了交易的价值属性。

● 链上资产交换协议：链上资产交换协议主要由与交易相关的协议组成，其中去中心化交易所协议是一类满足去中心化特点的交易协议[24]。所谓的去中心化特点主要指在任何时刻中心机构都不会拥有用户的任何资产，去中心化交易所会在链上处理所有交易，以便参与者验证每笔交易的真实性。

2014年，比特股（Bitshares，BTS）

诞生，其旨在建立一个点对点的去中心化支付系统，发行代币BTS[25]，去中心化概念兴起。2017年，基于以太坊公链运行的抵押借贷项目MakerDAO以发行稳定通证和抵押融资的特点，在全世界范围推广DeFi。自此之后，DeFi的应用领域逐渐扩大，融入更多传统金融产品。2019年，去中心化交易所出现。2020年，Compound掀起了流动性挖矿的热潮，DeFi再次迎来爆发性增长[26]。截至2022年4月，DeFi总协议锁仓量达到2 219.1亿美元。未来DeFi将朝着分叉式发展，一部分为迎合特定领域的合规性要求接受监管，出现“许可型DeFi”概念，同时为用户保持一定的透明度；另一部分仍保持无须许可和匿名的特点加快完全去中心化进程。

2 交易机制

目前，基于价格发现机制的不同，去中心化交易所协议拥有几种实现方式，包括交易委托账本（order book）、自动做市商（automated marker maker，AMM）、聚合器（aggregator）等协议，其中自动做市商是目前广泛采用的方法。本节根据交易实现方式将现有主流DeFi交易机制分为3类：交易委托账本、自动做市商和聚合器，并对交易机制的设计实现和相应的交易所进行分析介绍。

2.1 交易委托账本

2.1.1 实现原理

交易委托账本是传统金融中最常见的交易实现方式，如证券、期货交易所等金融机构采取该方式撮合买卖双方的交易意图。具体而言，首先，做市商提供交易资产意图，包括交易方向（买入或卖出）、成交价格以及交易数量。如**图4**所示，做市商1提出以99元的价格购买1单位资产的意图。之后，交易所创建账本，并将所有接收到的意图收集聚合。然后，交易所将聚合后的账本公开发布至所有用户。最后，为了完成交易，需要进行订单匹配的过程，交易所将提出购买意愿的交易单与账本中的订单进行匹配，以当前可用的最佳价格处理购买者的订单。

2.1.2 具体工作

基于交易委托账本的交易所根据其处理账本的方式以及订单匹配的方式进行分类。自数字货币交易市场出现以来，交易委托账本经历了从中心化到去中心化的转变。早期的Coinbase[27]、Binance[28]等平台基于中心化方式实现。其中，Coinbase是首家在纳斯达克上市的中心化交易所[29]。以Coinbase为例，其订单匹配方式基于先进先出（first-in-first-out，FIFO）原则，具体的含义是做市商提交的订单按照价格/时间优先级进行匹配。优先处理价格位于买卖填充区域的交易订单，当订单的价格相同时，按照时间顺序进行处理，较早提交的订单将被优先处理。当订单无法在填充区域内完成交易时，聚合剩余的交易信息，并在链下发布账本，Coinbase提供包括BTC、ETH等在内的遵守ERC-20协议的数字货币资产的交易。Binance则是国内比较知名的中心化交易所，其订单匹配方式类似于Coinbase，主要区别在于其底层采用了自行设计的币安智能链（Binance smart chain，BSC），主要交易会基于BSC进行，以解决交易中的拥塞问题。

然而，中心化交易所的固有特点导致其具有内在缺陷。中心化交易所因为由中

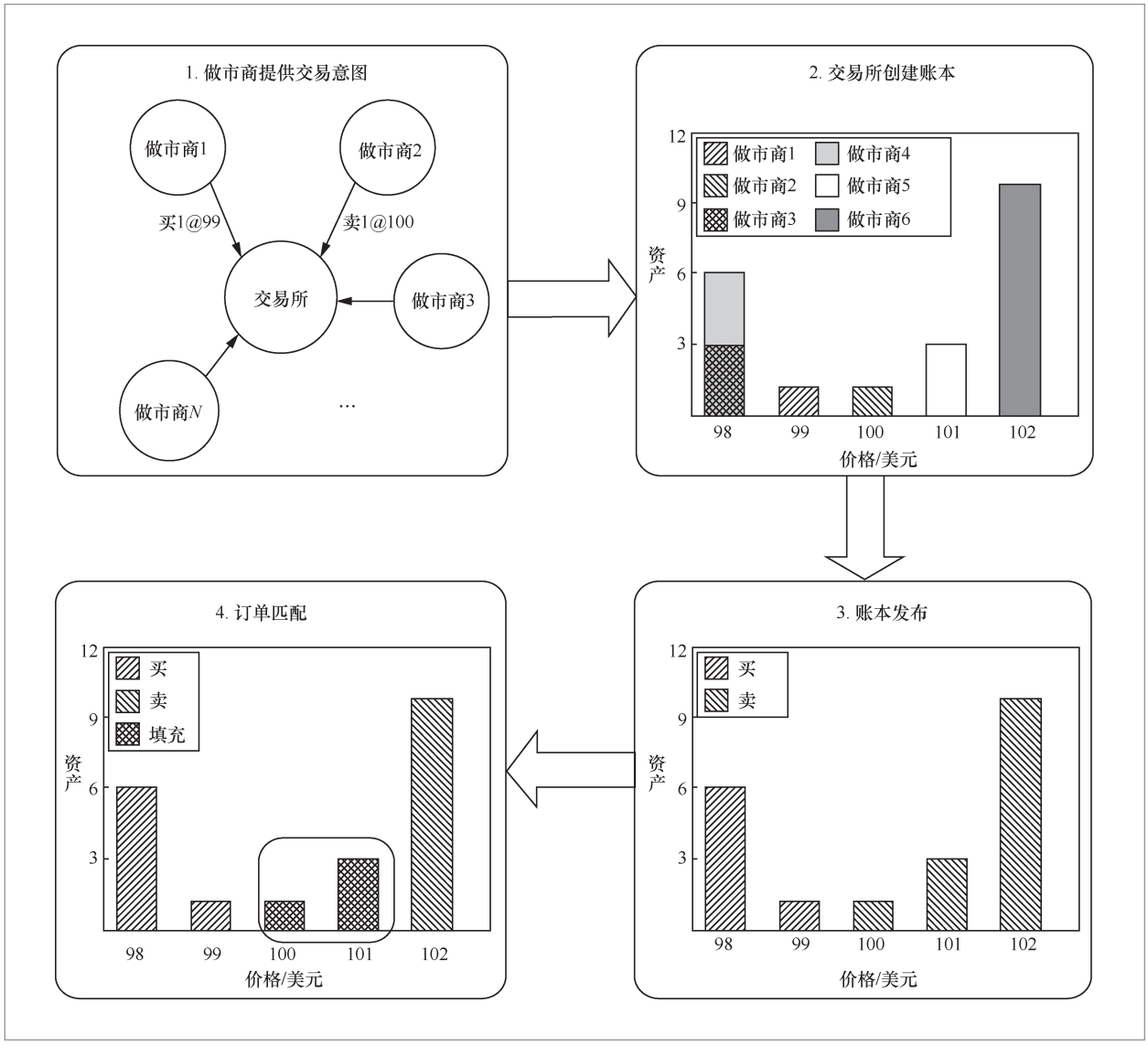

图 4 交易委托账本流程

央机构维护交易账本信息，因而可以控制信息以及访问状态[30]。控制信息主要指在收集参与者的交易意图时，中心化交易所具有披露订单内容以及时间的能力，这可能会导致交易所可以从撮合交易中获取不正当利益。另外，中心化交易所为了促进资产的流通，通常倾向于保管用户的资产，例如Binance会保管参与者的资产，这也带来了由黑客攻击造成的资产丢失风险[31]。

目前，基于去中心化的实现方式逐渐受到关注，去中心化的属性主要体现在此类交易所削弱了对交易过程的控制权[32]，实现了一定程度的权利下放。dYdX[33]是一个经典的去中心化交易所，其与Coinbase类似，订单匹配方法按照价格和时间优先级的顺序进行。然而，dYdX的去中心化体现在其匹配合约时通过开源的智能合约自动执行匹配和交易过程。另外，受

限于以太坊区块的燃料限制，dYdX每次最多仅能匹配10份订单，当买方需求足够大导致前10份做市商订单难以满足时，将会执行更新账本信息的操作以满足交易需要。近年来创新性地出现了各种去中心化交易所，下面将介绍具有代表性的4个去中心化交易所。

- Serum[34]是一个比较特殊的去中心化交易所，其特点在于实现了比较少见的链上账本的公布方式。由于dYdX提出的交易意图众多以及部分方法的底层实现主要基于以太坊及其变体，其难以具备即时的链上收集与处理信息能力。而Serum得益于底层Solana[35]区块链的高吞吐量和高性能特点，实现了高流动性的链上账本。除此之外，Serum的交易方法也有所改进，订单匹配过程仍然采用FIFO机制。但在交易过程中，不同于其他常见的直接向合约发送待交易资产的方式[34]，其考虑了合约执行依赖诚实的验证节点的问题。因此，其提出双方在交易前首先进行资产抵押，等智能合约执行完成后再对抵押资产进行处理。此方法被认为是基于FIFO机制的抵押改进版本（collateral-FIFO），有效减少了交易双方的违约风险。当然，此方法需要交易双方提前准备等值的同种数字货币资产作为抵押，因此不允许参与未持有的货币种类的交易，这在一定程度上降低了可用性。

- 0x Relayer[36]采用了开放订单簿（open order book）的订单匹配方法，其本质上通过设置中继器（relayer）不断接收并广播地址全为0的订单。任何参与者都可以充当中继器角色，实现0x协议并提供资产托管服务[37]。当其他参与者看到相关的订单信息时，其可以通过本地调用特定函数构造交易。0x Relayer采取链下托管账本、链上交易的形式，参与者都能创建交易所托管订单，在一定程度上降低了交易费用，使交易更自由，但可能会对流动性有影响。

- Waves Exchange[38]则是稳定币交换的交易所，提供了Waves代币与锚定各国法定货币的稳定币的交换方式。其中，数字货币与稳定币之间的交换通过FIFO机制进行，而稳定币基于Neutrino[39]协议维持与法定货币一致的稳定性。不同于基于超额资产抵押方式实现的稳定币[21]，Neutrino通过预言机以及Waves代币间的发行与销毁机制实现稳定币功能。

- Injective[40]提出了基于频繁批量拍卖（frequent batch auctions，FBA）的订单匹配机制。其在交易间隔内收集订单，并在间隔结束时按照优先级顺序进行排序。之后进行统一清算价格的流程，直到交易间隔结束并且批量拍卖成交后，订单才会被聚合成账本并发布。相比传统的FIFO订单匹配机制，FBA在保持交易效率和靠近市场价方面具有优势。

本节主要对基于委托交易账本的交易所进行综述，根据订单匹配机制、账本收集方式和依托的底层区块链进行分类，具体见**表1**。在创新性方面，Serum体现出链上账本的创新，0x Relayer和Injective提出了新型订单匹配机制，Serum和Waves Exchange提出新的区块链以应对特殊的交易需求。

表1 不同交易委托账本的方法

交易所	订单匹配机制	账本收集方式	底层区块链
Coinbase[27]	FIFO	中心化链下	Ethereum
Binance[28]	FIFO	中心化链下	BSC
dYdX[33]	FIFO	去中心化链下	Ethereum
Serum[34]	collateral-FIFO	去中心化链上	Solana[35]
0x Relayer[36]	open order book	去中心化链下	Ethereum
Waves Exchange[38]	FIFO	去中心化链上	Waves Blockchain
Injective[40]	FBA	去中心化链下	Ethereum

2.2 自动做市商

2.2.1 实现原理

交易委托账本的去中心化主要体现在交易所实现了一定程度的权利下放，而基于自动做市商机制的去中心化交易所是目前业界比较热门的选择，交易流程完全实现去中心化。自动做市商采取交易者与流动性池（liquidity pool）交易的方式，无须特定的交易对手即可获得流动性。其中，流动性池由锁定在智能合约中至少两种类别的资产通证（通常是不同种类的数字货币，如BTC与ETH）组成[41]，因此可以通过部署包含各类数字货币作为资产储备的智能合约创建流动性池，并由流动性池创建者（liquidity pool creator）第一个向流动性池提供流动性。

当交易发生时，一种资产将会被添加到流动性池中的资产储备中，并从其他类别的资产储备中提取资产（以BTC-ETH流动性池为例，当BTC资产被添加时，ETH资产会被同时提取），添加和提取的交换比例不同于上述交易委托账本的订单匹配方式，而是利用恒定函数，通过允许资产数量沿着函数定义的曲线移动的方式确定。下面首先对自动做市商涉及的参与方和经济系统进行介绍，然后综述具体恒定函数的设计。

自动做市商的参与方主要涉及3种角色，分别是流动性提供者（liquidity provider, LP）、交易者（trader）以及套利者（arbitrageur）[42]。其中，流动性提供者主要为流动性池提供资产储备以提高流动性，交易者主要参与与流动性池的交易，套利者具有确保流动性池内的资产与公开市场价格持平的作用。

自动做市商的经济系统主要涉及三方面的内容：奖励、显式花费和隐式花费[42]。其中，奖励主要是指一种激励机制，显式花费指的是每次交易需要付出的成本，隐式花费则指交易机制伴随的隐式损失，包括滑点和无常损失[43-47]。接下来描述自动做市商机制常见的执行行为。

交易所发布原生代币后，鼓励流动性提供者通过质押资产[48]长期持有代币，以获得投资奖励。在创建初期，还会根据代币持有份额分享治理收益，以吸引参与者和提高社群治理水平。为了维护流动性，交易所还要求流动性提供者赎回资产储备时缴纳罚款。

作为参与方，流动性提供者通过增加一种或多种资产储备的方式向池内提供流动性，从而换取相应贡献比例的池内股权，参与分红奖励。当流动性提供者赎回提交的资产储备时，需放弃池内股权并缴纳罚款，且需要承担潜在的无常损失。而交易者向流动性池提交指定输入资产交易请求时，需缴纳手续费和验证费用。手续费以分红形式补贴流动性提供者，验证费用作为底层区块链验证交易的算力成本。当交易规模较大，而池内流动性较低时，交易价格明显偏离实际价格，便产生了滑点，这意味着交易者需承受滑点带来的隐式损失。当池内流动性较低时，单笔交易可能导致池内资产相对公开市场产生较大的价格波动，从而产生套利空间。套利者会在不同市场中买卖相同资产，并从价格差异中获利。

无常损失是自动做市商机制的主要风险之一，体现在池内锁定资产在公开市场价格波动时造成的损失。传统的自动做市商机制依靠套利者的套利行为进行池内资产的调节，以在价格波动后达到新的稳态，而套利者获取的利润是流动性提供者的潜在损失。这种损失是不定的，价格的波动

仅会造成浮动盈亏。无常损失真正发生在流动性提供者赎回资产储备时，例如当资产价格出现暴跌时，部分流动性提供者选择赎回资产储备，其赎回的资产价值已然下跌，而池内资产价格受此影响继续下跌，出现“死亡螺旋”现象；或者池内资产价格跌幅过大，难以恢复[47]。

由此可见，自动做市商机制可以被描述为涉及多类参与方和执行行为的经济系统。自动做市商机制的状态转移方式如**图5**所示，其中池内状态会根据不同参与方的不同行为而变化。

尽管自动做市商机制涉及的概念复杂，但其核心原理能够用形式化的方式进行描述[5,49]。具体而言，本节将通过定义一组基本机制及其状态转移的方式描述其核心过程，并说明常见的恒定函数设计，以及隐式损失的形式化定义。符号与定义见**表2**。

流动性池是自动做市商中重要的概念之一，其状态会受到执行行为的影响，因此可以通过状态空间表示建模的方式进行描述。X表示流动性池的状态，参与方执行行为对其产生影响的过程表示如式（1）所示，流动性池的具体表示如式（2）所示。

$$X \xrightarrow{\text{行为}} X' \tag{1}$$

$$X = \left[\{t_i\}_{i=1,\cdots,n}, C\right] \tag{2}$$

自动做市商的核心在于流动性池中每种资产的数量，恒定函数描述的是各类资产之间的组合关系，包括但不限于恒定和、恒定积等方式[50]。值得注意的是，恒定函数的不变性的前提在于池内流动性的稳定，当提供或赎回资产储备时，恒定函数会发生变化。

恒定状态值可以被认为是池内通证数量的某种组合关系所产生的结果，无论通证数量关系如何变化，在其他条件不变的前提下，恒定函数的状态定值保持不变。恒定函数用于在多类通证之间建立守恒关

表2 符号与定义

符号	定义
C	恒定状态值
t_i	通证i的数量
x_i	池内通证C的数量变动情况，$x_i<0$表示从池内提取通证i，$x_i>0$表示向池内添加通证i
$C(t)$	恒定函数
$E_{i,j}$	以通证j表示的通证i的价格
S	滑点

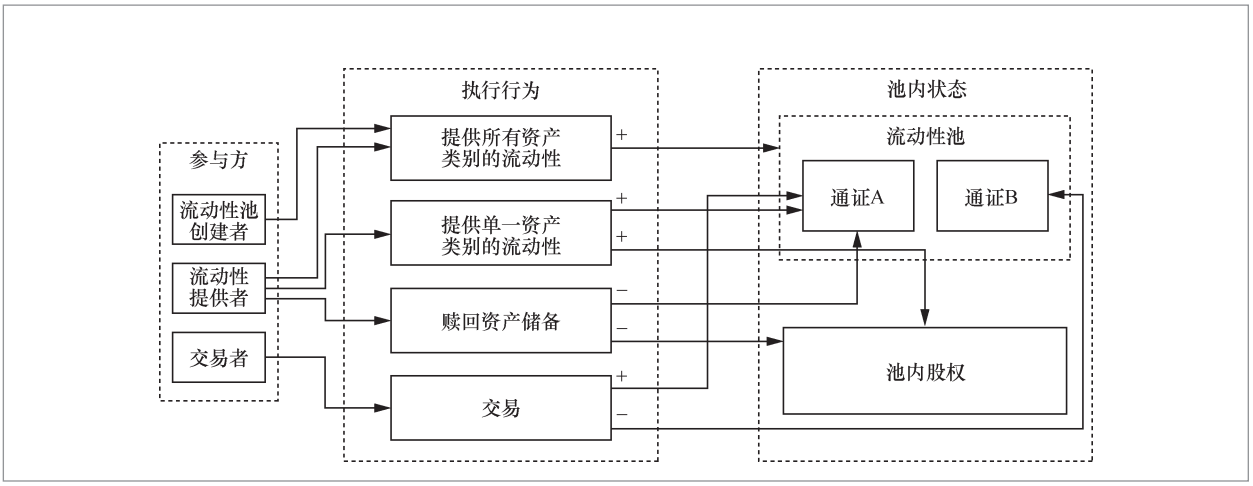

图 5 自动做市商机制的状态转移方式

系。建立好守恒关系后，即可描述通证间的交换关系，具体的描述如式（3）所示。

$$E_{i,j}=\frac{\partial C\left(\{t_i\}_{i=1,\cdots,n}\right)-\frac{C}{\partial t_i}}{\partial C\left(\{t_i\}_{i=1,\cdots,n}\right)-\frac{C}{\partial t_j}} \quad (3)$$

执行交易的一般过程可以被描述为向池内加入x_i个通证i，由于需要维持恒定状态值不变，因此将得到x_j个的通证j，在交易过程中其他通证将保持不变。由于恒定函数的设计，交易过程中的预设价格不等于真实价格，因此滑点的计算方式即衡量预设价格和真实价格之间的偏差，具体如式（4）所示。

$$S\left(x_i,\{t_i\}_{i=1,\cdots,n},C\right)=\frac{\frac{x_i}{x_j}}{E_{i,j}}-1 \quad (4)$$

对自动做市商涉及的概念进行定义以及形式化描述的过程如前文所述。下面将利用上述定义对经典的自动做市商协议进行综述。

2.2.2 具体工作

本节着重对UNISWAP[51]、mStable[52]、Balancer[53]等经典自动做市商机制进行分析。其中，UNISWAP是在两类通证之间进行直接交易的方法，其核心思想在于交易过程中始终不改变两类通证的数量乘积，因而被称作恒定积做市商；mStable同样针对两类通证关系，但其保持不变的是两类通证的数量之和，因而被称作恒定和做市商；Balancer提供了一种在多类通证之间进行交易的方式，其中每类通证i都设置了对应的权重w_i，且所有权重之和为1。值得注意的是，权重是流动性池的超参数，流动性池一旦建立，权重也就确定了，无论是流动性变化还是交易行为均会对其造成影响。UNISWAP可被看作Balancer的特例，当w_1=w_2=0.5时，Balancer退化为UNISWAP协议，具体见**表3**。

不同做市商机制的恒定函数对比如**图6**所示，值得注意的是，交易过程会被约束在恒定函数的曲线中。**图6（a）**和**图6（c）**说明了恒定积做市商机制具备稳定市场的功能，而**图6（b）**所示的恒定和做市商在价格波动产生套利空间时，池内价值较高的资产将被清空，退化为账本交易机制。

第一代自动做市商机制局限性较高，如无常损失带来的暂时性亏损、低流动性伴随的低资本效率等。根据UNISWAP的中心思想，当资产价格变动时，需要依靠套利者的活动使自动做市商提供的价格与外部市场相匹配的方法，会导致自动做市商内的暂时性亏损，而这种亏损只能等待通证的相对价格恢复到原来价值才会消失。

针对暂时性亏损情况，可以采取预言机[54]动态调整自动做市商内的通证相对价格，使内部汇率与外部市场价格相匹配。自动做市商的改进还体现在提高资本利用率上，主要方案有控制低滑点、实现稳定币交易以及增强流动性。

除了上述经典自动做市商机制，还有其他被广泛应用的自动做市商机制。其中多数协议[53-55]可被看作经典机制的改进变体。目前，UNISWAP发展到了v3版本[55]，通过控制滑点增强流动性；Balancer也推出了v2版本[42]，提出了资产管理器设计，将自动做市商逻辑从资产管理中分离。下面将对其中影响力较高的方法进行综述。

- UNISWAP v3[55]对经典UNISWAP[51]协议进行了改进，两者最主要的区别在于恒定积函数。UNISWAP v3提出了滑点控制的概念，在恒定函数的设计中加入了滑点控制参数，因此实现了流动性创建者精确控制资产价格变化曲线的方式。此外，UNISWAP v3还允许用户通

过承担不同的风险等级获得补偿。改进的主要目的是将流动性集中供应在交易意图活跃的区间，因此扩大了恒定函数值，并减少了滑点对交易产生的损失影响。

● 与交易委托账本中的Waves Exchange 类似，自动做市商也具有支持稳定币交易的机制。StableSwap[56]提供了一种稳定币交易的机制。由于稳定币的价值锚定法定货币，可以认为在特定时间内各种稳定币之间的价格比例固定。StableSwap的恒定函数设计采纳了恒定和函数与恒定积函数的优点，交易曲线介于二者之间。当稳定币的交换比例接近真实价格比例时，恒定函数形式接近恒定和函数，因此交易滑点较低；而当交换比例远离真实价格比例时，恒定函数形式接近恒定积函数，提供了一种市场均衡的能力。

● SushiSwap[57]是与UNISWAP极其相似的协议，仅仅在社群治理结构中有所区别。2020年8月，SushiSwap通过“吸血鬼攻击”（vampire attack）[58]的方式掠夺了UNISWAP的流动性。“吸血鬼攻击”产生的主要原因在于SushiSwap早期兼容UNISWAP的流动性池，通过增加通证激励的方式，流动性提供者获取了更高的收益。随着流动性的转移，SushiSwap侵蚀了竞争对手的市场份额，提高了自己的知名度和流动性，实现了快速发展。截至2021年8月，SushiSwap仍然占据大部分自动做市商市场的份额。

● Raydium[59]是一种结合自动做市商和交易委托账本的机制，与其他常见的基于恒定函数的方式不同，其采用常数函数定义交易方程，而且能够通过Serum[34]的交易委托账本提供流动性，这意味着

表 3 恒定函数

对比项	UNISWAP	mStable	Balancer
恒定函数状态值C	$t_1 \cdot t_2$	$t_1 + t_2$	$\prod_i t_i^{w_i}$
预设价格$E_{i,j}$	$\frac{t_1}{t_2}$	$C - t_2$	$\frac{t_1 \cdot w_2}{t_2 \cdot w_1}$
交易后通证数量t_2'	$\frac{C}{t_1 + x_1}$	$C - (t_1 + x_1)$	$t_2 \cdot \left(\frac{t_1}{t_1 + x_1}\right)^{\frac{w_1}{w_2}}$
交换数量x_2	$-\frac{t_2 \cdot x_1}{t_1 + x_1}$	$-x_1$	$t_2 \cdot \left[\left(\frac{t_1}{t_1 + x_1}\right)^{\frac{w_1}{w_2}} - 1\right]$
滑点 $S\left(x_i, \{t_i\}_{i=1,\cdots,n}, C\right)$	$\frac{x_1}{t_1}$	0	$\frac{\frac{x_1 \cdot w_1}{t_1 \cdot w_2}}{1 - \left(\frac{t_1}{t_1 + x_1}\right)^{\frac{w_1}{w_2}}} - 1$

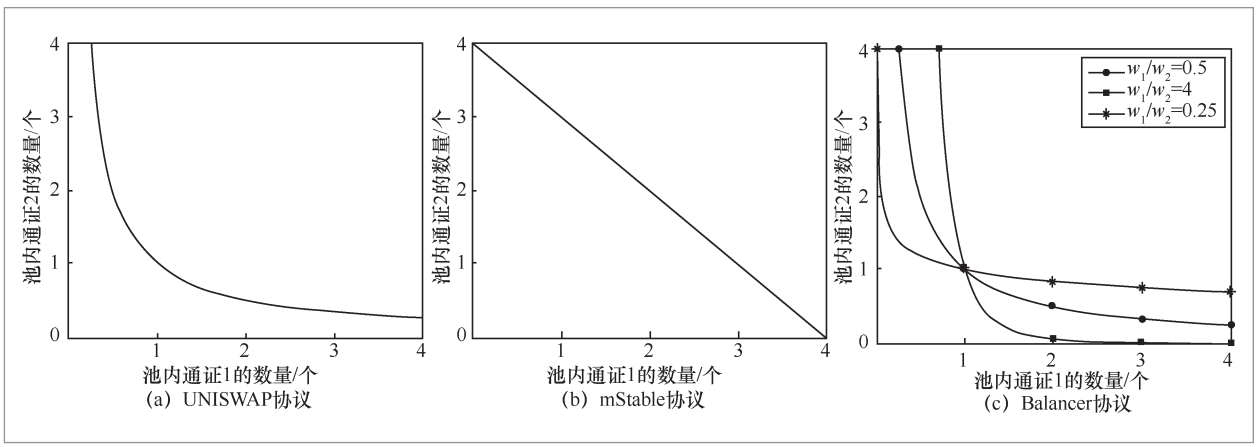

图 6 不同做市商机制的恒定函数对比

其流动性来源不仅包括自身的流动性池，还包括Serum的所有订单信息。目前，Raydium根据基于常数函数的特定方式对账本上的订单进行定价，预计还将采用预言机方法进一步提高流动性。

总体而言，自动做市商机制的活力主要来源于流动性，上述4种变体的改进方向普遍在于提高流动性，降低无常损失对流动性提供者的负面影响，进一步保障DeFi参与者的权益，加快资产的流通，提高交易效率。

本节主要对基于自动做市商的交易机制进行综述，并根据恒定函数、池内资产交易形式和底层区块链进行分类，具体见**表4**。

2.3 聚合器

2.3.1 实现原理

准确而言，聚合器协议并非一种独立的交易机制，其交易功能的实现依赖于其他DeFi协议。聚合器本质上是对多种交易协议的聚合，并为交易者提供统一的服务[60]。目前由于自动做市商机制的广泛应用，不可避免地产生流动性割裂的现象。因为各类自动做市商机制遵守不同协议，甚至储备不同资产的流动性池并不能相互交易，所以各个流动性池的流动性释放相对于公开市场存在时延，这种时延就是产生套利空间的根本原因。聚合器协议能够收集市场上各处的流动性并寻找最优交易路径，以此实现降低交易成本的目的。简而言之，聚合器本质上是一种路由搜索算法，基本流程如下。

算法1：聚合器搜索算法

1.流动性收集。聚合器首先收集具备流动性的提供方，记作Set。

2.交易信息处理。根据交易者提出的$A \rightarrow B$请求，在所有流动性提供方中寻找所需的流动性提供方，记作Set'。

3.算法执行。对Set'中的所有流动性提供方进行遍历与协议计算，寻找其中代价最小的交易路径。

4.结果返回。将路径结果返回给交易者。

总体而言，不同的聚合器协议之间的主要区别在于算法执行过程的不同。聚合器通常并非聚合单一协议，本文主要对具备聚合交易协议能力的聚合器协议进行分析。

表 4 不同自动做市商协议

协议名称	恒定函数	池内资产交易形式	底层区块链
UNISWAP[51]	恒定积	两类	Ethereum
mStable[52]	恒定和	两类	Ethereum
Balancer[53]	恒定积	多类	Ethereum
UNISWAP v3[55]	恒定积	两类	Ethereum
StableSwap[56]	改良恒定和与恒定积	多类	Solana[27]
SushiSwap[57]	同UNISWAP	同UNISWAP	同UNISWAP
Raydium[59]	特殊	两类	Solana

2.3.2 具体工作

1inch 聚合协议（1inch aggregation protocol）[61]是目前比较流行的聚合器协议。其主要通过组件路径发现器实现对交易路径的搜索。组件路径发现器能够在多个流动性池中拆分交易，实现了更广泛的交易状态空间搜索。另外，组件路径发现器还支持利用市场深度分析交易源请求和目的请求路径的深度关系；特别地，还能够针对同一份协议的不同市场深度拆分交易请求并部分交换，以降低燃料费用。

Matcha[62]是基于0x[63]协议的聚合器实现。0x协议除了提供路径搜索方案，还特别提出了一种激励做市商的机制。通过发送通证奖励补贴做市成本的方式，激励

做市商快速按照市场价格的比例提供流动性，因此降低了搜寻交易路径以及进行交易拆分所需要的成本。0x协议利用流动性提供者和去中心化交易所的竞争性特点，通过特有的通证经济学激励具备了相较于两者的竞争优势。

总体而言，目前聚合器协议受到越来越广泛的关注，其能够连接不同交易协议之间的流动性，完善交易机制，减少市场达到均衡状态前的波动。**表5**给出了交易委托账本、自动做市商、聚合器3类去中心化交易机制的多维度对比。除交易委托账本外，自动做市商、聚合器两类交易机制都依赖智能合约进行价格发现和交易撮合，采用区块链技术进行清算，三者的治理方法都基于去中心化的自治组织，自动做市商和聚合器还在合约开发过程中加入了治理内容。在具体的交易行为中，交易委托账本的流动性依赖于交易量和订单匹配方式的实现，缺乏机动性；自动做市商的流动性依赖外部提供，具有巨大的潜力和活力；而聚合器结合多种流动性池，进一步提高了交易的机动性。

3 总结与展望

本文总结了目前DeFi领域的交易机制，首先概述了与DeFi领域相关的研究工作，包括区块链、DeFi的基本概念，以及两者之间的联系；接着对基于交易委托账本、自动做市商以及聚合器的交易机制进行了介绍，分别对比了交易委托账本和自动做市商机制中多种实现方法的区别与联系；针对目前广泛应用的自动做市商机制进行了形式化的定义与描述，总结了作为其核心思想的恒定函数设计。基于DeFi的实现特点和本质，后文将从公平性、安全性与匿名性3个方面对去中心化金融交易体制的未来发展方向展开讨论。

3.1 公平性问题

由于DeFi具有透明性和不被第三方监管的特点，交易公平性问题普遍存在于交易委托账本机制和自动做市商机制中，其中抢先交易现象[64]尤为严重，不同形式的抢先交易需要落实不同对策。

对于基于交易委托账本的去中心化交易所而言，链下账本的维护和交易上链的过程中存在时间间隔，攻击者通过设置高手续费提前进行交易，从而获取不当利益。可以从智能合约的编写来解决这方面问题，例如通过设置交易时延提高抢先交易成本。

自动做市商的公平性主要面临三明治攻击[65]和闪电贷（flash loan）攻击[66]

表 5 3 类 DeFi 交易机制

交易机制	交易委托账本	自动做市商	聚合器
价格发现机制	账本收集公开	智能合约	智能合约
交易撮合方式	账本收集公开	智能合约	智能合约
清算系统	区块链	区块链	区块链
治理方式	去中心化自治组织	去中心化自治组织+智能合约	去中心化自治组织+智能合约
流动性依赖	交易量	流动性提供者	流动性提供者
交易对象	最优报价者	同种流动性池	多种流动性池
交易实现	订单匹配	同个恒定函数	多个恒定函数

的威胁。三明治攻击体现在攻击者通过交易行为操纵真实价格，以抢先交易低价买入被攻击交易所需资产，令其以较高价格提取所需资产，攻击者紧随其后高价卖出同种资产。闪电贷攻击是指在同一笔链上交易中实现无须抵押的借款和还款，攻击者可以在短时间内获得大量资本来操纵多个市场的不同资产价格，并从中获利。

为了避免三明治攻击，可以设法保证普通用户的交易在区块中的优先权与部分信息的隐藏。闪电贷攻击瞄准的是某些对外部市场价格不敏感的预言机的漏洞，因此可以利用去中心化预言机，通过多个来源确定资产价格，提高交易所对资产价格的敏感性和精确定价能力。未来解决方案可以往交易保护和精准定价方向进一步发展，以便更有效地维护交易公平性。

3.2 安全性问题

DeFi领域关系到众多数字资产的安全，因此其安全性问题尤为重要。DeFi应用的安全性取决于底层实现的安全性，底层实现所依赖的区块链和智能合约技术的安全性值得研究。

目前智能合约的安全隐患包含合约漏洞和逻辑错误两方面，重入漏洞[67]是其中一种严重的安全隐患。合约开发过程中的逻辑错误等无法从根本上避免，特定情况下的代码执行错误同样可能带来严重的损失[68]。为了减少智能合约代码的漏洞以及逻辑错误，合约审计[69]的方法被提出，自动化的审计执行方法也是能够提高系统安全性边界的重要研究内容。针对智能合约的安全问题，未来解决方案可以继续朝着完善代码开发方向发展，进一步加强代码的逻辑和重视代码维护工作。

3.3 匿名性问题

在DeFi领域中，需要关注参与交易行为的用户的隐私信息管理。基于区块链的DeFi交易环境具有透明开放性，方便用户观察交易。而匿名是为了合法保护用户隐私资料，但是产生恶意交易行为的用户逃脱责任的情况难以避免，影响了交易生态的治理和管理。如何平衡隐私保护和恶意交易行为打击是未来监管的一大挑战。

基于以太坊的交易行为是有可能实现用户身份追踪和行为推理的，其通过利用代理的伪匿名性将代理的真实身份绑定到链上地址。目前用于加密货币的交易可靠性验证的技术有零知识证明[70-72]和多方计算[73-74]。这些技术涉及底层区块链的计算，其使用和部署都需要付出相当大的算力成本，降低这一成本也是DeFi协议的改进方向。其他底层区块链也可以借鉴以太坊的案例来开展交易隐私管理的改进工作，以便进一步维护DeFi的经济生态。

参考文献:

[1] ZETZSCHE D A, ARNER D W, BUCKLEY R P. Decentralized finance[J]. Journal of Financial Regulation, 2020, 6(2): 172-203.

[2] GUDGEON L, WERNER S, PEREZ D, et al. DeFi protocols for loanable funds: interest rates, liquidity and market efficiency[C]//Proceedings of the 2nd ACM Conference on Advances in Financial Technologies. New York: ACM Press, 2020: 92-112.

[3] WU Y. A quantitative analysis on BitMEX perpetual inverse futures XBTUSD contract[J]. Undergraduate Economic Review, 2021, 17(1): 12.

[4] ZHENG Z B, XIE S A, DAI H N, et al.

Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352.

[5] SCHUEFFEL P. DeFi: decentralized finance – an introduction and overview[J]. Journal of Innovation Management, 2021, 9(3): 1–11.

[6] MOHAN V. Automated market makers and decentralized exchanges: a DeFi primer[J]. Financial Innovation, 2022, 8: 20.

[7] LEHAR A, PARLOUR C A, BERKELEY C. Decentralized exchanges[R]. 2021.

[8] NAKAMOTO S. Bitcoin: a peer–to–peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.

[9] ZHOU Q H, HUANG H W, ZHENG Z B, et al. Solutions to scalability of blockchain: a survey[J]. IEEE Access, 2020, 8: 16440–16455.

[10] GUDGEON L, MORENO–SANCHEZ P, ROOS S, et al. SoK: layer–two blockchain protocols[M]//Financial cryptography and data security. Cham: Springer International Publishing, 2020: 201–226.

[11] SZABO N. Smart contracts: building blocks for digital markets[J]. The Journal of Transhumanist Thought, 1996, 18(2).

[12] BUTERIN V. Ethereum white paper[Z]. 2014.

[13] CHEN H S, PENDLETON M, NJILLA L, et al. A survey on ethereum systems security[J]. ACM Computing Surveys, 2021, 53(3): 1–43.

[14] CHEN Y. Decentralized finance: blockchain technology and the quest for an open financial system[J]. SSRN Electronic Journal, 2019.

[15] SCHÄR F. Decentralized finance: on blockchain– and smart contract–based financial markets[J]. Review, 2021, 103(2): 153–174.

[16] NADLER M, SCHÄR F. Decentralized finance, centralized ownership? An iterative mapping process to measure protocol token distribution[J]. arXiv preprint, 2020, arXiv:2012.09306.

[17] VOGELSTELLER F, BUTERIN V. ERC–20 token standard (EIP 20)[Z]. 2015.

[18] ENTRIKEN W, SHIRLEY D, EVANS J, et al. EIP–721: non–fungible token standard[Z]. 2018.

[19] WANG Q, LI R J, WANG Q, et al. Non–fungible token (NFT): overview, evaluation, opportunities and challenges[J]. arXiv preprint, 2021, arXiv:2105.07447.

[20] BERENTSEN A, SCHÄR F. Stablecoins: the quest for a low– volatility cryptocurrency[M]//The economics of fintech and digital currencies, [S.l.:s.n.], 2019.

[21] BRENNECKE M, GUGGENBERGER T, SCHELLINGER B, et al. The de–central bank in decentralized finance: a case study of MakerDAO[C]//Proceedings of the 55th Hawaii International Conference on System Sciences. [S.l.:s.n.], 2022.

[22] SAENGCHOTE K. Where do DeFi stablecoins go? A closer look at what DeFi composability really means[J]. SSRN Electronic Journal, 2021.

[23] COLLIBUS F M, PARTIDA A, PIŠKOREC M. The role of smart contracts in the transaction networks of four key DeFi–collateral ethereum–based tokens[C]//Proceedings of 2021 International Conference on Complex Networks and Their Applications. Heidelberg: Springer, 2022: 792–804.

[24] TSAI W T, HE J, WANG R, et al. Decentralized digital–asset exchanges: issues and evaluation[C]//Proceedings of 2020 3rd International Conference on Smart BlockChain. Piscataway: IEEE Press, 2020: 1–6.

[25] 翟冉, 陈学斌. 区块链的共识机制研究[J]. 数据与计算发展前沿, 2021, 3(3): 86–94.
ZHAI R, CHEN X B. Research on blockchain consensus mechanism[J]. Frontiers of Data and Computing, 2021, 3(3): 86–94.

[26] 郑磊. 去中心化金融和数字金融的创新与监管[J]. 财经问题研究, 2022(4): 65–74.
ZHENG L. Innovation and regulation

of decentralized finance and digital finance[J]. Research on Financial and Economic Issues, 2022(4): 65–74.

[27] BODZIONY N, JEMIOŁO P, KLUZA K, et al. Blockchain-based address alias system[J]. Journal of Theoretical and Applied Electronic Commerce Research, 2021, 16(5): 1280–1296.

[28] BUSAYATANANPHON C, BOONCHIENG E. Financial technology DeFi protocol: a review[C]//Proceedings of 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering. Piscataway: IEEE Press, 2022: 267–272.

[29] Oxford Analytica. Coinbase listing will pave way for other exchanges[J]. Emerald Expert Briefings, 2021.

[30] QIN K, ZHOU L, AFONIN Y, et al. CeFi vs. DeFi–comparing centralized to decentralized finance[J]. arXiv preprint, 2021, arXiv:2106.08157.

[31] MARELLA V, ROSHAN M, MERIKIVI J, et al. Rebuilding trust in cryptocurrency exchanges after cyber-attacks[C]// Proceedings of the 54th Hawaii International Conference on System Sciences. [S.l.:s.n.], 2021.

[32] WERNER S M, PEREZ D, GUDGEON L, et al. SoK: decentralized finance (DeFi)[J]. arXiv preprint, 2021, arXiv:2101.08778.

[33] JULIANO A. dYdX: a standard for decentralized margin trading and derivatives[Z]. 2018.

[34] Serum. Serum white paper[Z]. 2021.

[35] LI X Y, WANG X Y, KONG T L, et al. From Bitcoin to Solana-innovating blockchain towards enterprise applications[C]// Proceedings of 2021 International Conference on Blockchain. Heidelberg: Springer, 2021: 74–100.

[36] WOOTEN J, MCGUIRE H. Decentralized order books for global financial markets[Z]. 2020.

[37] WANG R, TSAI W T, HE J, et al. A distributed digital asset-trading platform based on permissioned blockchains[C]// Proceedings of 2018 International Conference on Smart Blockchain. Heidelberg: Springer, 2018: 55–65.

[38] Waves. Waves exchange[Z]. 2021.

[39] IVANOV S, PUPYSHEV A. Neutrino protocol white paper[Z]. 2020.

[40] CHEN E, CHON A. Injective protocol: a collision resistant decentralized exchange protocol[Z]. 2018.

[41] AOYAGI J, ITO Y. Liquidity implication of constant product market makers[J]. SSRN Electronic Journal, 2021.

[42] XU J H, VAVRYK N, PARUCH K, et al. SoK: decentralized exchanges (DEX) with automated market maker (AMM) protocols[J]. arXiv preprint, 2021, arXiv:2103.12732.

[43] BOUERI N. G3M impermanent loss dynamics[J]. arXiv preprint, 2021, arXiv:2108.06593.

[44] JUN A. Liquidity provision by automated market makers[J]. SSRN Electronic Journal, 2020.

[45] ANGERIS G, EVANS A, CHITRA T. When does the tail wag the dog? Curvature and market making[J]. arXiv preprint, 2020, arXiv:2012.08040.

[46] EVANS A. Liquidity provider returns in geometric mean markets[J]. arXiv preprint, 2020, arXiv:2006.08806.

[47] LABADIE M. Impermanent loss and slippage in automated market makers (AMMs) with constant-product formula[J]. SSRN Electronic Journal, 2022.

[48] GERSBACH H, MAMAGEISHVILI A, SCHNEIDER M. Staking pools on blockchains[J]. arXiv preprint, 2022, arXiv:2203.05838.

[49] TOLMACH P, LI Y, LIN S W, et al. Formal analysis of composable DeFi protocols[M]// Lecture notes in computer science. Heidelberg: Springer, 2021: 149–161.

[50] WANG Y G. Automated market makers

for decentralized finance (DeFi)[J]. arXiv preprint, 2020, arXiv:2009.01676.
[51] AIGNER A, DHALIWAL G. UNISWAP: impermanent loss and risk profile of a liquidity provider[J]. arXiv preprint, 2021, arXiv:2106.14404.
[52] mStable. mStable document[Z]. 2021.
[53] MARTINELLI F, MUSHEGIAN N. Balancer: a non-custodial portfolio manager, liquidity provider, and price sensor[Z]. 2021.
[54] KRISHNAMACHARI B, FENG Q, GRIPPO E. Dynamic curves for decentralized autonomous cryptocurrency exchanges[J]. arXiv preprint, 2021, arXiv:2101.02778.
[55] ADAMS H, ZINSMEISTER N, SALEM M, et al. UNISWAP v3 core[R]. 2021.
[56] MICHAEL E. StableSwap – efficient mechanism for Stablecoin liquidity[Z]. 2019.
[57] Sushi. The SushiSwap project[Z]. 2020.
[58] STONE D. Trustless, privacy-preserving blockchain bridges[J]. arXiv preprint, 2021, arXiv:2102.04660.
[59] Raydium Team. Raydium protocol litepaper[Z]. 2021.
[60] COUSAERT S, XU J H, MATSUI T. SoK: yield aggregators in DeFi[J]. arXiv preprint, 2021, arXiv:2105.13891.
[61] 1inch Network. Introducing 1inch v2 – DeFi's fastest and most advanced aggregation protocol[Z]. 2020.
[62] Matcha. Matcha – simple crypto for everyone[Z]. 2021.
[63] 0x. 0x Docs[Z]. 2021.
[64] ESKANDARI S, MOOSAVI S, CLARK J. SoK: transparent dishonesty: front-running attacks on blockchain[C]// Proceedings of 2019 International Conference on Financial Cryptography and Data Security. Heidelberg: Springer, 2020: 170-189.
[65] ZHOU L Y, QIN K H, TORRES C F, et al. High-frequency trading on decentralized on-chain exchanges[J]. arXiv preprint, 2020, arXiv:2009.14021.
[66] CAO Y X, ZOU C W, CHENG X F. Flashot: a snapshot of flash loan attack on DeFi ecosystem[J]. arXiv preprint, 2021, arXiv:2102.00626.
[67] LIU C, LIU H, CAO Z, et al. ReGuard: finding reentrancy bugs in smart contracts[C]//Proceedings of 2018 IEEE/ACM 40th International Conference on Software Engineering: Companion. Piscataway: IEEE Press, 2018: 65-68.
[68] PeckShield. bZx hack full disclosure (with detailed profit analysis)[Z] .2020.
[69] HE D J, DENG Z, ZHANG Y X, et al. Smart contract vulnerability analysis and security audit[J]. IEEE Network, 2020, 34(5): 276-282.
[70] PANJA S, ROY B. A secure end-to-end verifiable e-voting system using zero-knowledge proof and blockchain[M]// A tribute to the legend of professor C. R. Rao. Heidelberg: Springer, 2021: 45-48.
[71] WANG Y S, KOGAN A. Designing confidentiality-preserving blockchain-based transaction processing systems[J]. International Journal of Accounting Information Systems, 2018, 30: 1-18.
[72] BÜNZ B, BOOTLE J, BONEH D, et al. Bulletproofs: short proofs for confidential transactions and more[C]//Proceedings of 2018 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2018: 315-334.
[73] RAMAN R K, VACULIN R, HIND M, et al. Trusted multi-party computation and verifiable simulations: a scalable blockchain approach[J]. arXiv preprint, 2018, arXiv:1809.08438.
[74] BENHAMOUDA F, HALEVI S, HALEVI T. Supporting private data on hyperledger fabric with secure multiparty computation[C]//Proceedings of 2018 IEEE International Conference on Cloud Engineering. Piscataway: IEEE Press, 2018.

作者简介

邓钇敏(1999-),女,中国科学技术大学先进技术研究院硕士生,中国计算机学会(CCF)会员,主要研究方向为深度学习、计算机视觉和元宇宙等。

司世景(1988-),男,博士,平安科技(深圳)有限公司资深算法研究员,中国科学技术大学硕士生企业导师,CCF会员。发表机器学习、大数据和人工智能领域国际核心论文20余篇。

王健宗(1983-),男,博士,平安科技(深圳)有限公司副总工程师、资深人工智能总监。CCF理事、杰出会员,CCF大数据专家委员会委员,主要研究方向为联邦学习、深度学习、云计算、物联网和元宇宙。

李泽远(1993-),男,平安科技(深圳)有限公司高级产品经理,中国计算机学会青年计算机科技论坛深圳分论坛领域主席委员,主要研究方向为联邦学习、多方安全计算等。

肖京(1972-),男,博士,平安科技(深圳)有限公司首席科学家,深圳市政协委员,中国计算机学会深圳会员活动中心副主席,清华大学、上海交通大学、同济大学、香港中文大学、深圳大学、上海纽约大学客座教授,长期从事人工智能与大数据分析挖掘相关领域研究工作,发表计算机图形学、自动驾驶、3D显示、医疗诊断、联邦学习等领域国际核心论文230余篇,授权专利220余项。

收稿日期: 2022-04-24
通信作者: 王健宗, jzwang@188.com
基金项目: 广东省重点领域研发计划“新一代人工智能”重大专项(No.2021B0101400003)
Foundation Item: The Key Research and Development Program of Guangdong Province (No.2021B0101400003)