引用格式:樊凯,周自横,袁望淞,等. 基于区块链的安全多方计算研究现状与展望[J]. 信息对抗技术,2024, 3(3):41-62. [FAN Kai, ZHOU Ziheng, YUAN Wangsong, et al. Blockchain-based secure multi-party computation: its research status and prospects[J]. Information Countermeasure Technology, 2024, 3(3):41-62. (in Chinese)]

基于区块链的安全多方计算研究现状与展望

樊 凯[1,2],周自横[2*],袁望淞[2],纪世元[2]

(1. 西安电子科技大学网络与信息安全学院,陕西西安 710126; 2. 西安电子科技大学广州研究院,广东广州 510700)

摘 要 在分析区块链、安全多方计算的技术特点的基础上,探讨了它们技术融合的可行性。对近年来大量相关研究文献进行了多维度的梳理总结,并将其按照链上/链外安全多方计算进行分类,针对不同类别,分别提出了相应的构造模型。深入分析了基于区块链的安全多方计算的特点与优势,并从多维度对比了链上/链外安全多方计算,总结了它们的特征与应用场景,指出了未来的发展方向。

关键词 区块链;安全多方计算;隐私保护

中图分类号 TP 309.2 **文章编号** 2097-163X(2024)03-0041-22

文献标志码 A **DOI** 10.12399/j.issn.2097-163x.2024.03.003

Blockchain-based secure multi-party computation: its research status and prospects

FAN Kai[1,2], ZHOU Ziheng[2*], YUAN Wangsong[2], JI Shiyuan[2]

(1. School of Cyber Engineering, Xidian University, Xi'an 710126, China;
2. Guangzhou Institute of Technology, Xidian University, Guangzhou 510700, China)

Abstract Based on the analysis of the technical characteristics of blockchain and secure multi-party computation technology, the feasibility of their technical integration was discussed. A great deal of related research literatures in recent years were combed, summarized and classified according to on-chain and off-chain secure multi-party computation. Moreover, specific construction models were proposed for each category. Finally, an in-depth analysis of the characteristics and advantages of blockchain-based secure multi-party computation was conducted. By making a comparison between on-chain and off-chain secure multi-party computation in multiple dimensions, a conclusion of their features and application scenarios was drawn and the future research direction was prospected.

Keywords blockchain; secure multi-party computation; privacy protection

0 引言

隐私问题是互联网技术发展的核心问题之一。近年来,隐私泄漏事件层出不穷,越发凸显出隐私保护技术的重要性。然而,仅靠单一的密码学技术难以实现较强的隐私保护效果,技术融合是发展的必然趋势。隐私计算的核心技术之一是安全多方计算(secure multi-party computa-

收稿日期:2023-08-21 **修回日期**:2023-11-14
通信作者:周自横,E-mail:zhoupanda@stu.xidian.edu.cn
基金项目:国家自然科学基金资助项目(92067103)

tion，MPC)，但其在恶意敌手模型下却难以构造出满足公平性的实用、有效的协议。区块链技术的出现与发展为其带来了转机，目前，已有部分研究者使用基于区块链的安全多方计算，构造出恶意敌手模型下满足公平性的方案。

本文针对 MPC 与区块链相结合的研究工作进行系统、全面的梳理分析，旨在为该方向后续理论研究、实践提供一定参考。相比于前人的工作，本文的主要工作如下：

1）沿用了文献[1-2]的分类方法，根据方案构造不同，将区块链与 MPC 结合的工作分类为链上 MPC 与链外 MPC 2 类，提出了链上/链外 MPC 的框架模型。

2）总结了大量链上/链外 MPC 的相关研究工作，并按照时间和使用区块链不同进行排序，分析总结了它们的关键技术、参与方数量、安全模型等多维度特征。相较于以前的综述工作，本文涉及的样本数量更大，总结更深入、全面。

3）分析了区块链在链上/链外 MPC 中的作用，并将这类工作与传统的 MPC 协议模型进行对比，总结出基于区块链的 MPC 的特点与优势。

除此之外，本文从设计目标、设计重心、安全模型、可扩展性等多个维度分析对比了链上 MPC 与链外 MPC 的区别，总结了它们的优劣势以及应用场景，并指出了部分未来可能的发展方向。

1 MPC 的研究现状

MPC 技术随着姚期智院士提出并解决“百万富翁”问题[3]而诞生，它允许多个参与方在无可信第三方的情况下使用各方的私有输入来联合计算目标函数，并且每一方都无法获得除私有输入、输出外的信息。

MPC 的范式如图 1 所示。假设多个参与方 $P=\{P_1,P_2,\cdots,P_n\}$，想要通过函数 f 完成联合计算。每一个参与方输入私有数据 x_i，通过函数 $f(x_1,x_2,\cdots,x_n)\rightarrow(y_1,y_2,\cdots,y_n)$ 进行计算，最终每一参与方 P_i 只能获得自己的私有输出 y_i，并且无法知晓或推断出其他参与方的任何相关信息。

MPC 作为一种“可用不可见”的重要密码学原语，提供了较强的安全性保障，也因此被广泛地运用到隐私保护机器学习、隐私计算、区块链等前沿工作中，但其也有一定的局限性，具体表现为以下 3 点：

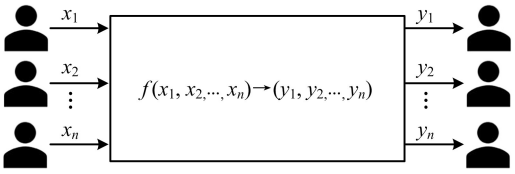

图 1 MPC 范式

Fig. 1 MPC paradigm

1）计算效率低。MPC 协议的计算非常依赖于网络的带宽、时延，同时构成协议的方案本身构成复杂，有较多基于密文的复杂计算任务，计算难度高。

2）可扩展性差。一方面，协议的计算通信开销[4]较高，在实际运用中，尤其是在大型的计算项目中很难达到理想的效果；另一方面，MPC 协议的构造非常复杂，缺乏应对需求变化而灵活变化的扩展能力。

3）公平性难以保障。在协议构造的过程中，保障 MPC 协议的公平性至关重要，然而早在 1986 年，CLEVE[5]就指出在不诚实大多数的情况下，MPC 不可能达成公平性。

区块链技术起源于对分布式系统的研究，随着 NAKAMOTO[6]提出比特币后变得更广为人知，引发了研究热潮。通俗来说，区块链就是一个分布式账本，其核心优势在于节点之间去信任化、去中心化的点对点交易、协调与协作，能够有效解决传统中心化系统中存在的高成本、低效率以及数据存储不安全等一系列问题[7]。区块链在经济、社会系统等领域有着广泛的应用场景，如数字存储、数据鉴证、选举投票等等。

通过 MPC 与区块链技术的结合来增强安全性是可行的手段。一方面，MPC 是一类更注重协议过程的安全性、隐私性的密码学原语，但是缺乏对数据正确性、完整性验证的手段。而区块链技术通过对数据全周期的可追溯，可以为 MPC 提供可行的数据验证手段，解决 MPC 这一大短板。另一方面，区块链和 MPC 均处理分布式环境中的安全和信任问题[8-10]，从实用场景方面考虑，两者相互契合匹配，能够有效进行技术融合。因此，本文以“基于区块链的 MPC”作为研究对象调研相关工作，其中的综述研究现状如下。

2019 年，ZHONG[11]等首先对区块链技术以

及 MPC 进行了简要的介绍，指出区块链具有提供安全性和激励的能力，能够为 MPC 协议提供公平性并提高其计算效率；接着分析了区块链如何为安全多方计算提供公平性，并建设性地给出了一个带简单奖惩机制的基本架构模型；最后，将该相关研究工作按照“使用比特币”和“使用区块链”分为 2 类，分别进行分析、总结，这是目前能找到最早的介绍 MPC 与区块链结合应用的综述文献，但是涉及的相关研究文献数量有限，所提出的架构模型也不具备普适性。

2021 年，WU 等[12]从区块链的隐私保护问题出发，认为 MPC 能够弥补区块链的安全缺陷问题，对 2 种技术的结合做了适用性分析，从秘密共享、零知识证明、同态加密 3 个技术层面做了分析比对，总结了不同技术在区块链中运用的优缺点，并分类介绍了最具有代表性的一批研究工作。文献[12]为区块链技术和隐私保护技术的结合提出了建设性意见，但是严格意义上来说，文章所介绍的内容并不是 MPC 与区块链的结合，而是隐私保护技术与区块链的结合。

2022 年，刘炜等[13]发表了隐私计算与区块链相结合的应用研究进展分析综述，分析了 MPC、联邦学习等隐私计算技术所面临的问题以及区块链如何赋能隐私计算，针对性地分析了各类隐私计算技术与区块链结合的特点、意义，并介绍、总结了部分相关研究工作，对隐私计算与区块链的技术融合做了分析与展望。文献[13]对于隐私计算和区块链技术的交叉融合来说意义非凡，但是关注点偏向于技术结合的广度，缺乏更深度的研究。

表 1 总结了基于区块链 MPC 分类的相关研究工作。

表 1　基于区块链的 MPC 分类总结

Tab. 1　Summary of blockchain-based MPC from different perspectives

分类	方案	时间/年份	关键技术	参与方	安全模型			区块链类型
					半诚实模型	恶意模型	其他	
链上 MPC	文献[1]	2019	Fabric	多方	—	—	Fabric 安全机制	Hyperledger Fabric
	文献[2]	2019	Fabric	多方	√	—		
	文献[14]	2021	SPDZ 协议 PVSS①	多方	√	带中止安全		
	文献[15]	2021	SPDZ 协议 加法同态加密 加法秘密共享	多方	√	带中止安全		
	文献[16]	2021	CP-ABE② Paillier 同态加密	多方	√	—		
链外 MPC	文献[17-21]	2013—2016	时间锁 哈希函数	两方/多方	√	公平性	财务公平③	比特币
	文献[22]	2015	全局 UC 模型	多方	√	公平性 鲁棒性	财务公平	
	文献[23]	2021	环签名	多方	√	—	满足拍卖场景需求	
	文献[24]	2015	智能合约 增量碰撞哈希	两方	√	—	隐蔽敌手模型下$(1-1/n)$威胁度	以太坊
	文献[25]	2018	智能合约 VSS④	多方	√	公平性	财务公平	
	文献[26]	2020	智能合约 加法秘密共享	多方	√	—	—	
	文献[27]	2021	Σ-协议 智能合约 Shamir 启发式	多方	√	带中止安全	—	

续表

分类	方案	时间/年份	关键技术	参与方	安全模型			区块链类型
					半诚实模型	恶意模型	其他	
链外 MPC	文献[28]	2015	分布式哈希表 PVSS	多方	√	带中止安全	—	区块链
	文献[29]	2019	PVSS 博弈论 智能合约 EOS 区块链	多方	√	公平性 鲁棒性	财务公平	
	文献[30]	2020	同态加密	多方	√	—	—	
	文献[31]	2020	智能合约 可验证同态加密	多方	√	公平性	财务公平	
	文献[32]	2021	智能合约 跨链交易	多方	√	公平性	财务公平	
	文献[33]	2021	环签名 智能合约 边缘计算	多方	√	—	—	
	文献[34]	2022	智能合约 零知识证明	多方	√	带中止安全	—	
	文献[35]	2022	NTRU 代理重加密 多密钥同态加密	多方	√	公平性	量子安全 财务公平	

注：① PVSS(public verifiable secret sharing，公开可验证秘密共享)。

② CP-ABE(ciphertext policy attribute-based encryption，基于密文策略属性基加密)。

③ “财务公平”指通过高额经济惩罚机制来遏制恶意敌手恶意行为所达成的公平性。

④ VSS(verifiable secret sharing，可验证秘密共享)。

2 相关知识

2.1 安全多方计算

MPC 协议的提出离不开严格的安全性假设，本节首先介绍目前协议中典型的安全需求、理想-现实范式模式以及敌手模型，并简要介绍 MPC 协议的安全模型。此外，MPC 协议的构造需要依赖各种不同的技术，在此介绍其中最主要的 3 大技术：秘密共享、不经意传输、混淆电路。

2.1.1 安全模型

安全需求 MPC 的研究目标是“在无第三方参与的情况下，各参与方之间的数据隐私性以及计算正确性”，这与传统密码学不尽相同，因此也带来了更为独特的技术要求。相关的综述工作[11-12,36-38]总结了 MPC 中最核心的 5 条安全需求：

1) 隐私性。任何一方都无法知晓或推断超出规定之外的任何信息。在执行协议期间，各计算方可能会获取到部分“中间值”，而隐私性要求这些“中间值”无价值，即各方无法使用该“中间值”推断出任何有用信息。

2) 正确性。协议各方都会获取到正确的输出。协议应该保证无论是否存在腐败方恶意篡改的情况，每一方都能够获取到正确的计算结果。

3) 输入独立性。腐败的参与方的输入与诚实的参与方的输入应该是相互独立的。例如在密封拍卖的场景下，各方的竞拍阶段出价或是修改出价都应独立于其他参与者完成。

4) 公平性。各方无论是否腐败，都应该能够得到自己的输出结果。

5) 输出保障性。也称为“鲁棒性”，即腐败方无法通过“拒绝服务”等攻击手段来中断协议。

2.1.1.1 带中止的安全

在 MPC 协议中，会出现腐败参与方提前获得输出结果，并拒绝发送最终结果给诚实参与方，阻止诚实参与方获取计算结果的情况。为了保证协议的效率与可行性，部分协议允许这种情况发生。这类协议的安全性通常不满足“公平性”与“输出保障性”，被称为“带中止的安全”。

2.1.1.2　理想-现实范式

在定义 MPC 协议安全性时，通常使用理想-现实范式，而不是基于属性的安全性定义。在“理想-现实范式”[39-40]中，构建了一个被明确定义、满足安全性需求的“理想世界”，在其中有一个可信第三方与完全安全的通信信道，通过“模拟器”来模拟“现实世界”中的敌手行为。理想-现实范式通过对比“现实世界”与“理想世界”的关系来定义安全，文献[38]给出了一种直观的定义：对于任何针对真实协议执行任何攻击的敌手，假设在理想世界中有同样的敌手与攻击，如果理想世界中的敌手和参与者的联合输入/输出与真实世界中的对应分布相同，则满足安全准则。

2.1.1.3　敌手模型

确定敌手的能力是 MPC 协议安全性定义中重要的一环，在本文中考虑以下 2 种敌手模型：

1）半诚实模型（semi-honest model）。在该模型中，所有参与者都会诚实地执行协议，但是他们是“好奇的”，会根据情况收集任何其他相关数据以推断其他参与方的私有输入、输出。半诚实模型是一种安全性较低的模型，但是具有这种级别安全性的协议能够保证不出现意外的数据泄漏[36]。

2）恶意模型（malicious model）。有恶意参与者的模型被称为恶意敌手模型。这类恶意的参与者会动用任何攻击方式以尝试破坏协议，获得他们想获取的信息。此类模型的安全性高，但是会严重影响协议效率。

2.1.2　秘密共享

秘密共享（secret sharing）技术于 1979 年被 SHAMIR[41]提出。自安全多方计算技术出现后，秘密共享被广泛应用于安全多方计算协议的构造中。秘密共享技术通过将秘密信息拆分为若干秘密份额，由多位参与者分别保存，通过参与者的合作，可以使用门限个数或者更多个数的秘密份额来重新构造出原始秘密消息。

Shamir-(k,n)门限秘密共享方案中，假设需要共享的秘密为一份数据 D，(k,n)门限机制的目标是将该数据分解为 $D_1,D_2,\cdots,D_n$ 这样的 n 个秘密份额，它们满足以下 2 个条件：

1）通过任意 k 个或者更多个秘密份额 D_i 可以轻松计算重构 D；

2）通过任意 $k-1$ 个或者更少个秘密份额 D_i 无法计算重构 D。

秘密共享技术的特点在于其计算量小、通信量较低，非常适合用于需要高频通信并进行复杂计算的安全多方计算协议之中。除了 Shamir 秘密共享外，现有的安全多方计算协议还常采用加法秘密共享、复制秘密共享[42]等方案。

2.1.3　不经意传输

不经意传输（oblivious transfer，OT）于 1981 年由 RABIN[43]提出。OT 的定义是：假设发送方有 n 个数据，数据接收方接受其选定的一个数据，且不能获取也无法知道其他数据，同时数据发送方无法知道接收方的选择。其形式化表达如下：

1）协议输入。假设 Alice 输入 2 个数据 $A=\{\alpha_1,\alpha_2\}$，Bob 需要输入 1 个选择位 $r\in\{0,1\}$。

2）协议输出。Bob 基于自己的选择位 r 获取到对应的数据 α_r，但他无法知晓另一个数据的任何内容，同时 Alice 也无法知晓 Bob 获得了哪一个数据。该 OT 协议可以记作$\binom{2}{1}$OT。

由 RABIN 提出的 OT 协议无法保障每次秘密交换都满足要求，不足以支撑实际的应用需求。在后续工作中，研究者们基于 RABIN 的协议进行了更加深入的研究，将 OT 分为 2 类：由 EVEN 等[44]提出的“1-out-of-2 OT”和由 BRASSARD 等[45]提出的“1-out-of-n OT”。

OT 对于 MPC 协议的构造来说是必要的，但使用公钥操作的 OT 协议代价非常高。为解决这个问题，BEAVER[46]引入了“不经意传输扩展”的概念，将少量的基本不经意传输扩展为大量不经意传输，虽然它能有效降低 OT 开销，但是并不实用。目前具体有效的 OT 协议分为 2 类[37]，分别是基于 IKNP 框架[47]的 OT 和基于 PCG 框架[48]的 OT。

2.1.4　混淆电路

最早的混淆电路（garbled circuit）协议由姚期智院士提出，LINDELL 等[49]为其方案提供了形式化表达与安全性证明。混淆电路基于布尔电路（逻辑运算）来构造安全函数计算，保证一方的输入不会泄漏给其他方。混淆电路的参与方称为混淆参与方（garbler）和求值参与方（evaluator）。

混淆表是混淆电路的核心，一个简单的与门电路的混淆表生成过程为：假设 Alice 是计算的

混淆参与方，设 X，Y 表示逻辑电路输入，Z 表示逻辑电路输出。X，Y，Z 的真实值分别是 α，β，$\gamma \in \{0,1\}$，在该电路中 $\gamma=\alpha \wedge \beta$。Alice 在生成真值表后，为输入值生成随机替换值 α_0，α_1（α_0，$\alpha_1 \in \{0,1\}^n$，n 为系统安全参数），它们分别对应 $\alpha=0$，$\alpha=1$ 的情况，对于 β，γ 同理。而后，Alice 使用每一行的前两位输入值替换值对最后的输出值替换值进行 AES 加密，并将得到的加密值顺序打乱，就得到了混淆表。表 2 展示了混淆表的生成过程。

表 2 混淆表生成过程

Tab. 2 The process of generating the garbled table

真值表			随机值替换后的真值表			混淆表
X	Y	Z	X	Y	Z	密文（打乱后）
0	0	0	α_0	β_0	γ_0	$\mathrm{Enc}_{\alpha_1}(\mathrm{Enc}_{\beta_0}(\gamma_0))$
0	1	0	α_0	β_1	γ_0	$\mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_0}(\gamma_0))$
1	0	0	α_1	β_0	γ_0	$\mathrm{Enc}_{\alpha_1}(\mathrm{Enc}_{\beta_1}(\gamma_1))$
1	1	1	α_1	β_1	γ_1	$\mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_1}(\gamma_0))$

2.2 区块链

2.2.1 区块链的基本结构

区块链有着开放共识、点对点通信、去中心化、去信任化、不可篡改、交易透明等优点，这让它在数字经济等领域内有着广泛的应用前景。这些特性很大程度上取决于区块链本身的结构组成，其中最为核心的 3 大要素是：基于时间戳的链式结构、基于 P2P 网络的分布式存储机制和基于去中心化节点的共识机制[50-51]。

图 2 展示了区块链的链式结构以及其中 1 个区块的具体内容。如图 2 所示，区块链的区块一般分为区块头和区块体 2 个部分，区块头中包含了版本号、时间戳、前一区块的哈希值、默克尔树根等字段，版本号字段用于标识交易规则的版本。在打包发布新的区块时，区块链要求记账的节点在新的区块上加盖打包发布的时间戳以标识区块数据的写入时间。区块中的父区块哈希值通过对父区块的区块头进行哈希计算（通常使用 SHA256）得到。区块链的区块体一般由一个默克尔树构成，该数据结构对数据块进行两两一组的递归哈希处理，直到只剩下一个根哈希。区块体基于此数据结构，对区块链中记录的交易进行分组哈希，得到最终的一个根哈希值，被称为默克尔树根记录在区块头之中。

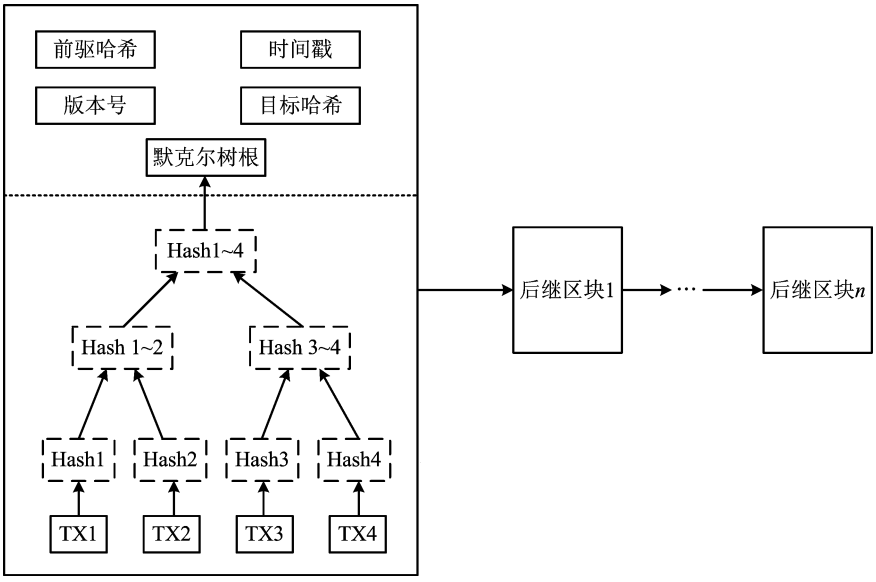

图 2 区块链结构

Fig. 2 Structure of the blockchain

时间戳与前驱哈希 2 个字段保证了区块链按照时间顺序记录区块发布。而默克尔树让区块链对于任何有关的改变都非常敏感,假设一区块中的数据被篡改,其区块头的哈希值就会随之变化。这样的结构组成保证了区块链不可篡改的特性。在特定的区块链下,区块头中的组件内容与功能也有所不同,如 Nonce 值在比特币中使用可以调整工作量证明(proof of working, PoW)挖矿的难度;在以太坊中使用则可以用来确认交易的顺序,防止双花攻击。

2.2.2　共识机制

共识机制是区块链系统组成中非常重要的一环,它解决了区块链的分布式账本中的数据一致性问题。区块链的共识算法起源于传统分布式共识算法,可以分为 2 类[52]:一是针对非拜占庭问题的崩溃容错(crash fault tolerance, CFT)共识算法,如 Paxos[53]、Raft[54]等;二是针对拜占庭问题的拜占庭容错(Byzantine fault tolerance, BFT)共识算法,如 PoW[6,55]、PoS[56]、DpoS[57]、PBFT[58]等。传统的分布式系统或许可链中通常使用 CFT 类共识,而以比特币为代表的一系列非许可链系统中,BFT 共识则是主流。

PoW 共识被中本聪设计为以“挖矿”的形式实现的共识机制,它通过算力竞争来保证数据一致性以及共识安全性,但该机制也导致了很大程度上的算力资源浪费。PoS 共识基于对自身“权益”的证明,即证明自身拥有一定的系统资产。PoS 能解决 PoW 的算力浪费问题,同时缩短达成共识所需要的时间。PBFT 是一个非常重要的共识机制,其目的是:在好节点不知道其他节点好坏的情况下,让好节点之间达成一致。PBFT 能够容忍小于节点总数 1/3 个数的恶意节点,同时它将算法复杂度从指数级别降低到了 $O(N^2)$。

2.2.3　智能合约

智能合约的概念最早被 SZABO[59]提出,最初,智能合约被定义为一种数字形式的承诺,它结合了协议、用户界面来规范和保护公共网络上的关系,是一种将现实世界的合约承诺数字化表达并可与用户交互的技术。而碍于计算方法的落后,智能合约起初并没有受到广泛的关注。区块链技术的出现与发展为智能合约带来了完美的应用场景,这也让智能合约成为了区块链的核心要素之一。以太坊[60]是首个内置图灵完备语言并且引入了智能合约的公有链[61],它的出现将智能合约的发展推进到一个新的阶段。

目前,对智能合约的定义不尽相同,有的认为智能合约是一种可以由软件执行的法律的合约,还有的单纯将其视为一类代码脚本,旨在满足某些定义的任务[62]。CLACK[63]给出了相对全面、广泛的定义:智能合约是一种自动化且可强制执行的协议;它可以由计算机自动化执行,虽然某些部分可能需要人工输入和操控;它的强制执行要么通过法律规定的权利与义务,要么基于不可篡改的计算机代码来实现。

与现实中合同订立流程类似,智能合约的生命周期可以分为 3 大阶段:合约生成、合约发布、合约执行[64]。在合约生成阶段,发布、签订合约的各方需要协商并制定合约的规范,明确各方在合约中的职责,验证合约的正确性后生成合约的执行代码;在合约发布阶段,智能合约以程序代码的形式附于区块链之上,部署上链的智能合约需要定期维护、升级;在合约执行阶段,智能合约基于触发条件、响应规则等预置条件等待外部事件的触发[7]并执行。

2.2.4　区块链分类

基于使用的场景、去中心化程度等目标需求不同,区块链可以被分为 3 类:公有链、联盟链、私有链。

1) 公有链。是任何人都可以参与使用、维护且参与者多为匿名的区块链。其核心特点在于完全去中心化,比特币是最有代表性的公有链应用。

2) 联盟链。多用于若干组织之间一起合作维护一条区块链,保持了受限的去中心化程度,其最有代表性的应用是超级账本 Fabric(Hyperledger Fabric)。

3) 私有链。与一般的中心化记账系统差别不大,有严格的权限管理,只有对应组织内部并通过了审核的成员才可以使用。

基于对权限的限制要求不同,公有链可被称为非许可链,联盟链和私有链可被称为许可链。在研究中私有链的应用场景非常少,所以一般来说许可链单指联盟链。3 种不同种类的区块链特性对比见表 3 所列。

表 3 3 种区块链特性对比

Tab. 3 Comparison of the three types of blockchain

	公有链	联盟链	私有链
参与者	任何人	获得授权的人员	仅所有者
共识机制	PoW、PoS	分布式一致性算法	分布式一致性算法
激励机制	需要	可选	无
特点	公开透明	平衡效率	安全快速
中心化程度	完全去中心化	部分去中心化	中心化
典型应用	比特币	Hyperledger Fabric	组织私有

2.2.5 Hyperledger Fabric

Fabric 是 Linux Foundation 旗下超级账本项目中的一个子项目，是目前最大的联盟链区块链系统之一。Fabric 提供背书策略、链码、通道等独特的机制，塑造了一个保障隐私的基于许可的平台，在隐私、许可方面的优势使得它被广泛用于链上 MPC 场景。Fabric 中的核心组件包括[65]：

1）组织与联盟。在 Fabric 中，一个组织也被称为“成员”，它们被区块链服务提供者邀请加入区块链网络。在一个区块链网络中，不同组织可以组成联盟，一个联盟不需要包含所有存在于网络中的组织。

2）账本。Fabric 中的账本由 2 部分组成“区块链”和“世界状态”。基于区块链的账本拥有不可篡改的特性，一旦区块上链，则无法被更改。“世界状态”是一个数据库，存储交易日志中包含所有键值。

3）智能合约和链码。在 Fabric 中智能合约管理交易逻辑，而链码管理智能合约的打包和部署。Fabric 会将智能合约打包进链码中，这个链码会被部署到一个区块链网络中。当智能合约被成功定义于区块链网络后，客户端应用可以通过发送交易提案的方式来调用合约。

4）Peer 节点。Peer 节点是区块链网络最基本的元素，可以维护多个账本、链码的实例。它们为组织所有，并由组织负责维护。应用程序需要连接到 peer 节点才可以访问账本和链码。

5）背书。背书是指一组被指定的节点来执行链码交易并返回一个提案响应给客户端应用的过程。背书策略指定了在该通道上需要响应背书的节点、通过交易背书的最小背书节点数等策略，提交的交易必须符合背书策略才可以被标记为有效。

6）排序服务。Fabric 专门设计了排序节点来保证交易有序，排序节点一起形成了排序服务。由于 Fabric 依赖于确定性的共识算法，因此保证了最终通过验证上链的区块是最终的、正确的，不会产生类似于比特币、以太坊中的分叉问题。具体来说，在交易流程中，排序服务负责将已背书的交易提案响应的交易进行打包，创建交易区块，随后交由 peer 节点验证并写入账本。Fabric v2.0 中推荐使用 Raft 共识来实现排序服务。

7）通道。通道连接其他组件，实现了一个基于数据隔离和保密的私有区块链。在一个通道内，特定的账本可以被所有 peer 节点共享，交易方也必须通过该通道的正确验证才能够与账本进行交互。

8）证书颁发机构（certificate authorities，CA）。CA 在区块链网络中分配 X.509 证书，用于识别组织中的组件。同时，由 CA 颁发的证书也可以为交易提供签名，用于背书环节。Fabric 的区块链网络中，各组件通过证书来标识自己来自于特定的组织，所以不同的组织一般使用不同的 CA。Fabric 也提供了一个内置的 CA，称为 Fabric-CA。

9）成员服务提供者（membership service provider，MSP）。Fabric 中，通过 MSP 来实现证书同成员组织间的匹配，被用于区块链网络的认证、授权和身份管理中。

图 3 为一个 Fabric 的区块链网络示例图，包含了组织 R_1、R_2，它们共同组建了一个联盟。通道 C 连接了 3 个 peer 节点 P_1、P_2、P_3 以及排序服务，peer 节点们共同维护着账本 L_1 并且安装并定义了链码 S_1。2 个组织中分别存在着各自的证书颁发机构 CA_1、CA_2，为 2 个组织分配证书，证书可以用来识别属于各组织的组件。2 个组织中还有 2 个应用程序 A_1 和 A_2，它们可能相同也可能不同，主要取决于组织想要如何处理 peer 节点上的账本副本。

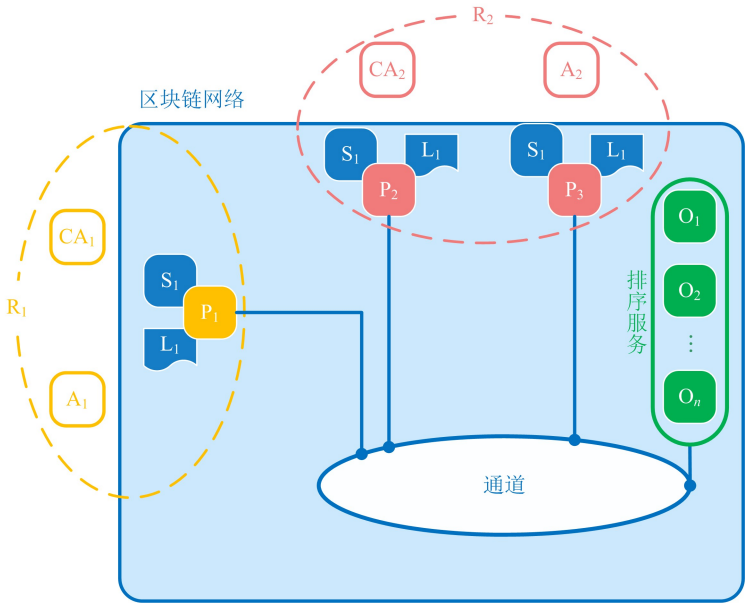

图 3　Fabric 网络示例图

Fig. 3　An example of Fabric network

3　链上 MPC

3.1　基本模型

链上 MPC 指将 MPC 协议集成到区块链网络上执行，计算节点作为区块链网络上的节点通过区块链进行通信，通过区块链的智能合约等机制来完成计算。区块链中背书策略（对于使用 Fabric 的链上 MPC）、共识机制的存在能够为链上 MPC 的构造提供更强的灵活性，也为协议的执行提供了安全性、可靠性的保障。

链上 MPC 通常基于 Fabric 构建，图 4 为存在 3 个组织的 Fabric 网络完成 MPC 的模型示意图。计算参与方可以通过一组应用程序 A_1、A_2、A_3 连接到 Fabric 网络，通过认证后以 peer 节点的形式存在于区块链网络中，它们可以存在于同一个组织也可以分散于不同的组织中。当需要完成 MPC 任务时，各方的组织构建起一个通道，每个参与节点都维护了一个通道账本的副本。各方协商后共同部署 MPC 协议链码，并通过链码、背书策略完成 MPC。通常由于 MPC 协议构造不同，链上 MPC 需要加入部分组件协助 MPC 的执行，如文献[1]使用“Helper 服务器”来协助不同 peer 节点之间的通信，文献[15]构造“解密器”来实现为背书阶段赋能加解密功能。

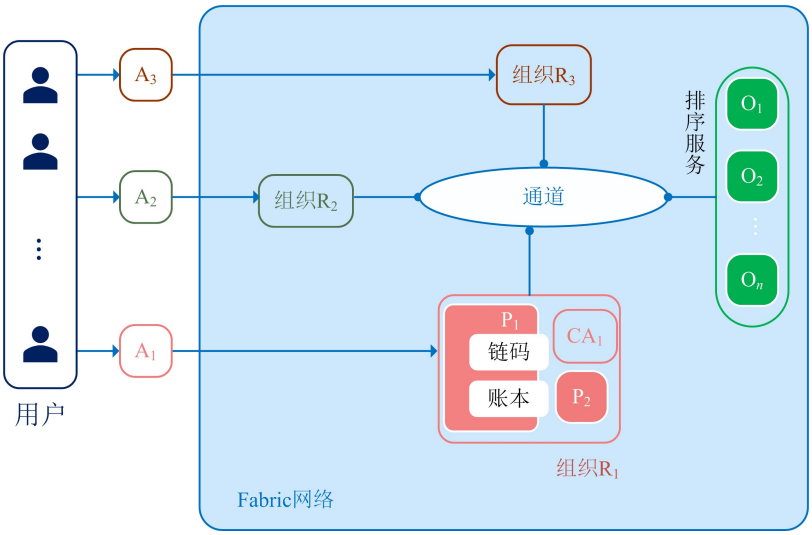

图 4　链上 MPC 模型

Fig. 4　On-chain MPC model

在构造 MPC 协议时，通常不考虑对参与方的身份、信道做安全性假设，而是直接认定为参与方之间有“安全直连的通信信道”。与普通 MPC 模型不同，链上 MPC 为 MPC 协议增添了一层“保护壳”，使用 Fabric 的组织、通道等组件为 MPC 的计算参与方提供了“身份”“通道”等隐私保护机制，能够解决 MPC 协议存在的这些隐私保护问题，提供了更实用的应用场景。

3.2 Hyperledger Fabric 的使用

2019 年，BENHAMOUDA 等[1]基于姚式电路设计了一个在 Hyperledger Fabric 上实现的支持私有数据的体系结构，并实现了一个简单的三方拍卖程序。为了在 Fabric 上支持私有数据，本文提出了 2 个关键的组件：一是本地配置，该组件需要支撑不同节点上实现背书逻辑的链码获得访问其他节点不可使用的本地参数的能力；二是节点内通信，该组件需要支撑运行在同一个 peer 节点上的链码能够与其他 peer 节点上的相同链码进行通信。在示例中，他们使用 Go 语言搭建了一个 Helper 服务器，在其中存储每个 peer 节点的本地参数，以便于在不同节点的链码实例之间建立通信通道。

同年，BENHAMOUDA 等[2]基于文献[1]的研究内容，在 Fabric 上实现了 MPC，并实现了一个首次公开募股(initial public offering，IPO)的价格清算方案。在一轮 IPO 中，每个投资者都可以通过经纪人的网络服务器(作为区块链的客户端)下单。下单完成后，经纪人将投资者的订单分解成若干份额，并将这些份额以加密的形式存储在区块链上。当确定结算价格的时候，各组织通过 MPC 协议来完成计算，这个计算在不清楚地显示顺序信息的情况下完成，甚至不向参与计算的组织透露，以保证协议的输入独立性、隐私性。

2021 年，GARG 等[14]面向企业的实际应用场景，提出了一个在 Fabric 上实现 SPDZ 协议[66]的系统架构。该系统由 Fabric 网络和与 Fabric 网络交互的后端组成，前者负责提供 Fabric 的功能以及支持 MPC 协议，后者负责与组织的实体进行交互，并且假设每个组织可以分别维护他们组织内 peer 节点的非对称密钥，保证其他组织无权访问这些密钥。SPDZ 协议的引入能够在一定程度上解决区块链的透明性带来的隐私问题，同时，区块链的存在也提高了 SPDZ 协议的构造、通信效率，使得该方案有着可观的安全性与效率。

2021 年，ZHOU 等[15]使用同态加密、零知识证明、秘密共享等技术构建了一个公开可验证的 MPC 协议，该协议构建于 Fabric 上，在链上进行计算，链外进行预处理。在链外预处理阶段，参与者使用“四元组生成协议”以获取足够数量的四元组，并使用一个“牺牲协议”来检查四元组是否有效。在链上计算阶段，所有参与方将私有输入分解并加密得到秘密份额，使用 Pedersen 承诺方案对秘密份额进行承诺，将它们都发布到区块链上。完成后，各方将“解密器”的地址存储到帐本中，由随机的参与方之一调用智能合约执行计算任务。最后，参与方通过“解密器”来解密输出并重构秘密，完成协议。不同于文献[1-2]的构造，方案不使用“辅助服务器”，而是添加了一个“解密器”组件，该组件本质上是一个 peer 节点，该节点中存放了参与方各自的私钥，作为解密者在背书阶段处理解密请求。在“解密器”中，还备有缓存机制，在收到相同请求的时候，会立即从缓存中获取到结果。作为一个可插拔的组件，“解密器”有着很好的便捷性，能够帮助完成整体协议执行并提高效率。

同年，QIAO 等[16]提出了一个基于 Fabric 的隐私保护信用评估系统，将 MPC 与同态加密技术作为安全组件实现了区块链上的隐私保护数据共享。该系统由数据、访问控制、数据加密、安全计算、模型存储 5 个模块组成。该系统使用区块链账本构建数据模块，去中心化的分布式存储能有效消除部分隐私泄漏隐患。在访问控制模块使用基于密文策略属性基加密[67]的数据访问控制策略，只有当该请求者的私钥、属性集、访问策略等内容完全匹配的时候才能够正常获取访问权限。数据加密模块使用线性转换加密技术，该技术使用一组公开参数与保密参数，保证转换后的数据隐私性。安全计算模块可以细分为加密部分和 MPC 部分。在加密部分，作者基于 Paillier 同态加密[68]构造了 Phillie 同态加密方案，在不解密密文的情况下完成线性回归计算。在 MPC 部分，计算节点负责加密数据的分解、分发与重构，使用这些数据联合计算得到回归系数，由一个可信预言机节点发送交易提案记录回归系数，上链存储。

3.3　链上 MPC 总结

表 4 给出了对链上 MPC 的部分工作总结。首先，从设计目标来说，目前的相关研究主要目标在于实用性，一类研究如何在区块链上实现 MPC 协议，另一类基于具体应用场景构造系统。其次，链上 MPC 主要依赖于许可区块链（尤其是 Fabric），原因有 2 点：一是许可区块链具有身份机制以及相对应的一套认证机制，其中的“组织”通常就是现实生活中的公司、政府部门等组织机构。这样基于许可的身份识别能够真实地对应现实社会中的利害关系[1]，这在本质上与 MPC 中的信任模型相同。二是链上 MPC 依赖于区块链的整体结构，能够更好地利用区块链提供的共识、背书策略、身份认证等机制工具，加之 Fabric 的可插拔组件，能够为链上 MPC 弥补可扩展性上的不足。

表 4　链上 MPC 总结

Tab. 4　Summary of the on-chain MPC

方案	安全性			设计目标	辅助组件	应用场景
	半诚实模型	恶意模型	其他			
文献[1]	—	—			Helper 服务器	在 Fabric 中支持 MPC
文献[2]	√	—			Helper 服务器	首次公开募股应用
文献[14]	√	带中止安全	Fabric 安全机制	实用性	Web 系统	面向企业
文献[15]	√	带中止安全			解密器	—
文献[16]	√	—			可信预言机计算节点	隐私保护信用评估系统

从安全性来看，链上 MPC 对 MPC 协议本身的安全性关注不高，本文研究范围内的相关协议安全性最高达到了“带中止的安全”。但由于链上 MPC 架构于区块链结构本身，对其安全性的考量还需要考虑到许可区块链（尤其是 Fabric）提供的身份认证、私有信道、背书策略、共识等机制。这些机制能够解决 MPC 节点之间身份管理、通信等方面的问题。

影响链上 MPC 使用最大的问题可能在于效率问题，它根植于多个方面，其中包括区块链内复杂的交易和出块机制对带宽的高需求，以及 MPC 协议本身的复杂性导致的效率低下问题等。当前的研究主要通过引入外部组件，在协议的执行流程上做预处理等改善操作以提高整体协议的效率，但效果不够理想。如何在不牺牲安全性的前提下增进链上 MPC 的执行效率，是未来一个重要的研究方向。

4　链外 MPC

4.1　基本模型

链外 MPC 的协议执行通过独立的 MPC 网络执行协议，如云服务器、私有网络或者本地计算机，而不依赖于区块链提供通信手段。在链外 MPC 构造中，通常会通过智能合约来完成 MPC 网络与区块链网络的交互。链外 MPC 的构造模型中通常包含以下组件：

1）MPC 网络。独立于区块链网络的 MPC 网络由 MPC 计算节点组成。这些计算节点可能是数据拥有者本身，也可能是具有一定算力的服务器，这些服务器通过提供算力的方式完成用户发布的 MPC 任务。

2）区块链。在链外 MPC 中，区块链作为可信的分布式存储、执行环境为 MPC 协议提供不同的业务功能。一方面，区块链提供了独特的交易、智能合约、时间戳等组件，可以在传统 MPC 的基础上集成强迫执行的奖惩机制、信誉机制等强大的功能机制，提高 MPC 的安全性。另一方面，区块链有着公开、透明、不可篡改的特性，在区块链上存储的信息可以被当作证明用于验证环节。

3）MPC 合约。在该模型下，MPC 合约指一组经用户协商后统一编码部署的智能合约。MPC 网络可以通过接口调用智能合约来实现不同的业务功能，如计算节点管理、协助计算、身份验证等。

4）用户。用户是 MPC 的结果请求者，他们可能是 MPC 计算节点本身，通过节点间的协商部署计算合约并在 MPC 网络中完成计算任务。

用户也有可能是单纯的数据拥有者，他们提供个人的私有数据并部署相应的节点管理合约、计算合约等不同类型的合约来完成所需的 MPC 任务，同时，他们需要提前向区块链支付一笔佣金，当协议顺利完成时会被支付给 MPC 的计算节点。

5）存储器。存储器不是一个必须的组件，部分链外 MPC 使用链外的数据存储系统来存储加密后的初始数据，在区块链上存储索引值和关键词来降低存储开销并加快访问效率。一个典型、常用的存储系统是星际文件系统[69]（inter-planet file system，IPFS）。

图 5 是链外 MPC 的一般构造模型，用户部署并发布 MPC 协议到区块链上，计算完成后他们可以通过智能合约接口与区块链交互，获得计算结果。数据拥有者的数据以加密的形式存放于存储器之中，数据索引将被发布到区块链账本上，在需要调用时可以通过索引完成查找。当用户共同协商并部署好 MPC 合约后，MPC 网络中的计算节点向区块链缴纳押金，并通过与区块链、存储器进行交互获得数据份额，完成计算。诚实完成计算的节点将结果提交，等待验证通过后可以赎回押金。

相较于普通的 MPC 模型，链外 MPC 活用了区块链交易机制、外部存储器等辅助设施，一方面帮助计算节点进行数据共享、完成计算，提供了实用的交互场景；另一方面为 MPC 协议提供了“奖惩机制”，提高了作恶成本，增强了安全性。

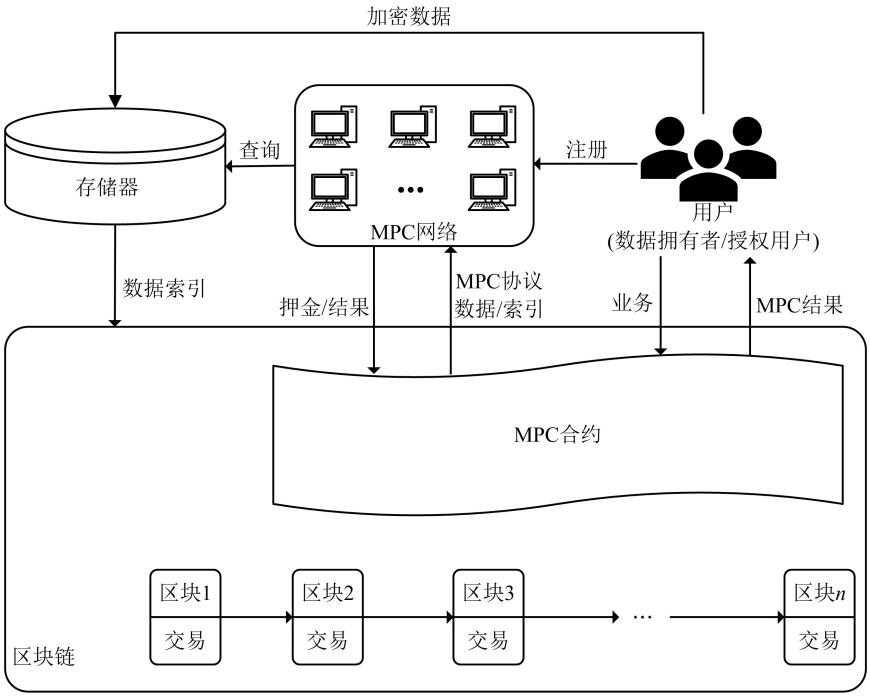

图 5 链外 MPC 模型

Fig. 5 Off-chain MPC model

4.2 比特币的使用

2013 年，ANDRYCHOWICZ 等[17]首次提出了基于比特币构建的 MPC 协议。他们基于比特币的交易以及时间锁机制，结合使用承诺、哈希等密码原语，构建了一种“定时承诺”。定时承诺分为 2 个阶段：一是交易的提交阶段，提交者在这个阶段必须进行承诺，并将承诺与押金绑定；二是打开阶段，提交者必须在限定的时间内透露出他的秘密，否则就将被罚款并将该金额用于补偿其他参与方。基于此定时承诺方案与 BLUM 的投币方案[70]，他们构造了一个在比特币上的安全多方抽奖协议。在抽奖协议中，各方需要在押金阶段内发布时间承诺，并缴纳 $N(N-1)$ 个比特币，其中，N 为参与人数。由于此协议对于押金的要求过于庞大，因此基本不适用于超过三方以上的情况。针对该情况，文献[71]基于安全私有信道假设前提下提出一个不需要押金的两方安全抽奖协议，但该方案使用场景还是受限严重。

同年，ANDRYCHOWICZ 等[18]提出了一个更为一般化的安全两方计算模型，该模型基于比

特币交易的“不可延展性”假设:区块链通过每一笔交易的简化版哈希(仅包含交易的主体)来对交易进行识别,而不是像原来一样通过交易的完整版哈希(主体和输入脚本)来识别。同时,他们将文献[17]中的“定时承诺”改进为“同步定时承诺”,保障只有在两方同时进行承诺的情况下,每一方的承诺才是有效的。基于假说与同步定时承诺方案,他们展示了如何在该两方协议中达成公平性,并介绍了几个可以适用本模型的应用场景。ANDRYCHOWICZ 等将文献[17-18]中的重要概念如定时承诺方案、同步定时承诺方案等内容在文献[71]中进行了总结分析,介绍如何解决比特币交易的延展性问题。

2014 年,BENTOV 等[19]基于文献[18]中的工作做了改进,在其基础上提供了更加正式的安全模型和安全定义。他们正式定义并实现了 3 个理想功能:索赔退款功能 F_{CR}^{*}、带奖惩机制的安全计算功能 F_{f}^{*} 以及带奖惩机制的抽奖协议功能 F_{lot}^{*}。在 2015 年,KUMARESAN 等[20]在文献[19]的基础上进一步改进,实现了一个称为安全现金分配的原语。他们将该原语设计为一个比普通安全评估函数更普适的多级反应函数,让它足以支撑各类涉及带状态的数据计算,比如,去中心化拍卖等。2016 年,KUMARESAN 等[21]再次对前面的一系列工作进行优化,将脚本复杂度从文献[17]的 $O(n^2|z|)$降低到了 $O(n\lambda)$,其中,n 为参与方的数量,$|z|$为计算函数 f 的输出大小,λ 为独立于 f 的安全参数。

2015 年,KIAYIAS 等[22]基于区块链使用了全局通用可组合(global universally composable,GUC)框架[72]提出了一种公平、鲁棒的 MPC 协议。他们首先提出 $\overline{G}_{\mathrm{CLOCK}}$ 和 $\overline{G}_{\mathrm{LEDGER}}$ 2 个理想功能以构造一个类比特币系统。$\overline{G}_{\mathrm{CLOCK}}$ 基于 KATZ 等[73]的想法改编,为系统提供全局时间戳服务,同步协议执行;$\overline{G}_{\mathrm{LEDGER}}$ 是对类比特币系统(比特币、以太坊等)的区块链公共账本的抽象,参与方以及执行的环境 Z 均可以全局访问该公共账本。本文基于以往的相关工作[72,74-75]引入了“Q-公平性”和“Q-鲁棒性”的概念,表达在全局理想功能下的协议公平性和鲁棒性。他们通过在一个包装器功能 W 中配备谓词 $Q_{\bar{G}}$ 作为过滤器来限制参与方的行为,具体来说谓词 $Q_{\bar{G}}$ 分为 3 个模式:$Q_{\bar{G}}^{\mathrm{Init}}$ 指定开始执行协议的条件;$Q_{\bar{G}}^{\mathrm{Dlv}}$ 指定参与方接收输出的条件;$Q_{\bar{G}}^{\mathrm{Abt}}$ 指定模拟器强制中止参与方行动的条件。相较于文献[17],文献[22]同样使用惩罚机制来保障安全性,但同时考虑了协议的鲁棒性,遏制了恶意参与方通过拒绝服务攻击等手段恶意中止协议而不受惩罚情况的出现。

2021 年,WANG 等[23]提出了一个基于区块链和 MPC 的密封拍卖方案,构建了一个无可信第三方的去中心化拍卖场景,并使用环签名和 MPC 技术来保障竞拍者的隐私并提供公开可验证性,相较于其他的相关工作在保证效率的同时达成了更高的安全性。该方案引入了文献[51]提出的基于比特币的押金机制,使用时间承诺等技术限制竞拍者的行为,不诚实的竞拍者将面临巨额的惩罚金,为协议提供了公平性,同时使用 RIVEST 等[76]提出的环签名技术,保证了竞标者身份的匿名性、不可伪造性。

4.3　以太坊的使用

2019 年,ZHU 等[24]提出了一个在隐蔽敌手模型下高效、可验证的安全两方计算协议 PVC-2PC,协议允许诚实方在不牺牲自身秘密的情况下用公开可验证的、不可否认的证据捕捉其他参与方的不诚实行为。考虑到攻击者的经济得失问题,他们提出了一种称为“财务安全”的新安全定义,财务安全的两方计算能保证作弊敌手的预期收益必定小于事先设定好的阈值(该值可以为负)。该财务安全的两方计算协议由一个基于“剪切和选择”混淆电路构造的公共可验证的隐蔽两方计算协议和一个通过以太坊智能合约实现的高效、去中心化的验证器组成。参与方在启动协议前都需要支付保证金,在协议执行过程中如果被发现有欺骗行为,那么诚实方只需要在协议执行过程中调用智能合约,一旦核实,则腐败方的保证金将转移给诚实方作为赔偿。

2020 年,黄建华等[25]基于以太坊智能合约构建惩罚机制实现了一个公平的 MPC 协议 BFSMPC。协议分为 2 个阶段:第 1 阶段将 Gennaro 基于可验证秘密共享的方案[77]与 Pedersen 承诺方案[78]结合,实现了一个不公平的通用 MPC 协议,完成了秘密份额的分发;第 2 阶段各参与方执行一个公平的秘密重建协议,为了避免恶意方提前终止协议,该协议也利用了押金机制。相较于文献[21]中的押金机制,BFSMPC 中的押金机制基于以太坊实现,通过由代码执行的

合约账户作为可信第三方来存储押金，将缴纳押金的总数从 $O(N^2)$ 降低至 $O(N)$。同时 BFSMPC 使用 ghost 共识机制，15 s 即可产生一个区块，相较于基于比特币的类似方案，仅出块效率方面就显著提高。

2020 年，LU 等[26]提出了一个基于以太坊的 MPC 系统，旨在实现隐私保护的数据共享与多方计算。该系统将 MPC 协议转移到链外执行，通过链上的智能合约来公平地选择计算节点，生成计算证书。用户能够使用应用层接口发布、参与、查询计算任务。具体来说，想要发布任务的用户需要制定计算合约在 IPFS 上发布，记录地址、时间戳、摘要信息等内容并将地址发送给以太坊区块链。系统使用“计算节点选择协议”和“通用链外计算协议”2 个智能合约组件协议层，赋能后续计算。

2021 年，WANG 等[27]提出了一个基于以太坊和 MPC 的隐私保护能量存储共享方案，旨在不揭露用户的隐私数据基础上完成储能调度服务以及成本分摊，方案使用 Σ 协议[79]以及 Fiat-Shamir 启发式[80]构造了非交互式的零知识证明，并使用 Pedersen 承诺方案[78]来隐藏区块链账本中的用户余额和交易值，并基于 SPDZ 协议构造了一个 MPC 协议 Π_{pess}。该协议首先使用 SPDZ 来对用户的需求总量进行聚合计算，在此过程中要求用户对个人需求量进行承诺以便于后续交易过程中的验证工作，并通过承诺创建零知识证明保证数据一致性，防范恶意行为。协议能够实现“带中止的安全”，同时在理想情况下能够为用户节省部分成本开销。但是由于方案本身计算开销较大，导致在以太坊上产生的 gas 费用较高，进而导致该方案难以投入实践运用。

4.4 其他区块链技术的使用

2015 年，ZYSKIND 等[28]提出了一个基于区块链的隐私保护分布式计算平台 Enigma。该平台链接到现有的区块链，将私有数据处理放于链下网络中进行，而区块链部分则负责管理访问控制、身份验证以及用作防篡改的账本。在存储方面，Enigma 链下网络使用了去中心化的链下分布式哈希表存储数据的引用，可以通过区块链访问。在计算方面，Enigma 对 MPC 做了 3 个方面的性能改进，分别是分级 MPC、网络缩减以及可适应电路。基于这些改进，Enigma 在大型的网络中也表现出较好的适用性。同时，Enigma 也使用了押金机制，任何节点有不诚实的行为或者过早地中止计算都会被罚款，保证了系统的公平性。

2019 年，GAO 等[29]结合使用公开可验证的秘密共享、博弈论、EOS 区块链等技术，提出了一个基于区块链的公平、鲁棒的 MPC 方案 BFR-MPC。BFR-MPC 使用区块链作为一个公开的账本维护了一个开放的信誉系统，以块高作为可信时间戳，通过智能合约支撑协议的执行。该系统将 MPC 协议视为不断重复的博弈，在每一轮博弈之中 MPC 节点的行为会影响其信誉值，对于诚实执行合约并提交结果的节点，将获得来自用户提供的佣金并提高其信誉值，否则降低其信誉值并扣留押金。经过博弈论的证明，该方案在恶意模型下也有着较好的公平性，同时公平可验证秘密共享、区块链可信时间戳等组件让 BFR-MPC 能够检测到参与方发送的错误信息，并在下一轮博弈开始前就将该参与方踢出计算，证明了协议的鲁棒性。此外，使用 EOS 区块链在出块速度上更有优势，基于比特币的平均处理时间在 10 min/块，而 EOS 区块链使用 BFTDPoS 共识，能够达到 0.5 s/块的速度，说明 BFR-MPC 的效率非常高。

2020 年，YANG 等[30]提出了一个用于隐私保护数据共享的基于区块链的 MPC 方案 Block-SMPC。在 Block-SMPC 中用户作为轻量级节点在区块链网络中存在，提供自己的私有输入并请求执行 MPC 协议。此外，还设计了一个动态聚合器联盟来进行可靠数据存储，并选择一个聚合器配合计算单元完成 MPC。Block-SMPC 使用 Elgamal 密码系统的变种加法同态加密方案构建了 MPC 协议，并引入了 PETER 等[81]提出的加密机制。Block-SMPC 克服了数据聚合中的单点故障问题，成功降低了用户和其他组件的交互频率，并通过权限分离机制保障了数据的保密性，实现了一个可伸缩的、分布式数据共享架构。

同年，BAUM 等[31]提出了一个高效的带罚款机制的 MPC 方案 Insured MPC，它可以使用任何一个具有特定属性的 MPC 协议，结合智能合约以及一个新的承诺方案，为 MPC 提供安全性保障，在使用全局随机预言机作为假设的 GUC 模型下被证明该方案是安全、公平的。他们将 CAMENISCH 等[82]的承诺方案，PEIKERT 等[83]

的 OT 协议以及 FREDERIKSEN 等[84]提出的投币协议相结合,提出了一个公开可验证的多方加法同态承诺功能 F_{HCom}。与文献[21]类似,Insured MPC 将 F_{HCom} 与一个具有特定属性的内部 MPC 协议相结合,在输出阶段对每个秘密份额承诺,参与方在区块链帐本上揭示承诺,智能合约负责进行验证并协调秘密重构,对于具有欺骗行为的参与方或是未揭示承诺的参与方将进行罚款。相较于同类方案,Insured MPC 的每个参与方计算并发布到区块链上的承诺输出大小是线性的,节省了许多计算开销。

2021 年,BAUM 等[32]对他们在文献[31]中的工作进行了扩展,提出了一个隐私保护的加密货币交换方案 P2DEX。P2DEX 支持多个用户跨链交换加密货币,只要所有的用户都能在一个链上使用一非私有的智能合约,那么该方案支持涉及任意数量的区块链,但该系统必须支持公开证明双花攻击的发生。系统的一组服务器负责以外包的方式进行跨链交易订单匹配,并对诚实的行为提供经济激励,而另一组服务器负责协议的执行。如果各方诚实执行协议,那么 P2DEX 的交换复杂度与一般集中式交易相当,而当在不诚实大多数的场景下,即使交易失败也能对不诚实的用户进行识别和惩罚,并保障诚实参与方的资金不会受损。

2021 年,GUAN 等[33]考虑到智能电网中边缘设备进行数据共享和协同计算时数据所有者和接收者双方的隐私保护问题,提出了一个基于区块链的边缘智能电网双端隐私保护的 MPC 方案 BPM4SG。BPM4SG 构建于联盟区块链上,各个角色之间有着权限等级的划分,由电力传输公司作为任务发起者,负责提供任务并准备数据、智能合约等相关参数;电力销售公司作为系统主节点,审批计算任务;矿工是电力系统中的服务器节点,计算参与方则是智能电网的边缘服务器。在 BPM4SG 的计算阶段,各参与方使用数字承诺与公钥生成一次性地址用于与其他参与方之间的数据传输。参与方收到数据的秘密份额后使用公钥加密,并生成环签名,以避免身份泄露。通过分组广播进行再一次数据混淆后,各方依次验证一次性地址与环签名。验证都通过时,参与方进行解密并处理数据,并再次加密后传输给任务的发起者,发起者将自行处理收到的各数据。该方案能保证半诚实敌手模型下的安全性,且相较于其他相关方案[85],有着更稳定的计算开销和更低的通信开销。

2022 年,YANG 等[34]设计了一种隐私感知、公开可审计的 MPC 方案 PaSMPC。具体来说,PaSMPC 使用区块链以承诺的形式来记录认证的参与方和数据用于跟踪审计,并基于改进的 Σ 协议构造的零知识证明来支持使用原始数据的计算任务在本地执行,可以通过智能合约来完成对数据的一致性和计算有效性的公开、自主检验。PaSMPC 架构由 1 台诚实的任务生成器 TG、1 组不诚实的数据提供者 DP 以及区块链组成。DP 首先通过 Pedersen 承诺以及私钥签名来保护私有数据传输上链,然后,TG 会根据计算任务部署合约、生成计算电路,并通过一可验证的不经意传输协议向 DP 发送相关密钥。DP 完成计算任务后,生成证明和签名上链,触发智能合约进行验证,只有对数据一致性以及计算正确性的 2 轮验证都通过时,该计算结果才会被认可并发送回 TG,否则计算终止。

2022 年,JIANG 等[35]提出了一个基于区块链和 NTRU 密码系统[86]的多密钥全同态代理重加密的 MPC 方案,该方案满足了可验证性、防共谋、可被查询方单独解密以及抗量子攻击等安全需求。该系统使用 IPFS 系统来辅助存储加密后的私有数据,在区块链账本上存储关键词、索引,为区块链节省了存储空间并提高了数据访问效率。此外,系统通过 NTRU 重加密进行密文转换,将同态计算的密文结果转换成由公钥加密的密文结果,便于获取结果。系统同样提供了押金机制,注册时要求计算节点缴纳押金,计算结束后,由区块链验证是否有不诚实的节点,对于不诚实方处以罚款并奖励给诚实方。为了提高节点达成共识的速度,本文的区块链系统使用了 XU 等[87]提出的 SGPBFT 算法,该算法改进了 PBFT 算法,通过引入积分制来完成视图轮换,并在每轮共识结束后都会对节点进行重新编号和调整,可以保证隐藏主节点的身份,抵御分布式拒绝服务(distributed denial of service, DDoS)的攻击。

4.5　链外 MPC 小结

从设计目标上来说,链外 MPC 大多研究协议的安全性问题,以文献[17]为代表,相关工作主

要通过区块链提供押金机制来为 MPC 协议提供公平性。但是，若敌手是“纯恶意的”，即这些敌手愿意支付高额经济惩罚来破坏协议的执行，则公平性不成立。因此，本文认为可以用“财务公平性”来描述这类研究工作的安全性。具体来说，“财务公平性”指通过高额经济惩罚机制来遏制恶意敌手恶意行为所达成的公平性。虽然财务公平性有一定的风险，但是绝大多数敌手都是利益驱动、理性的，纯粹恶意的行为是极少的。

表 5 是对链外 MPC 的总结。从使用的区块链不同来说，链外 MPC 的研究更倾向于使用以太坊或其他支持智能合约的非许可区块链。这是由于比特币本身不具备智能合约机制，难以实现复杂的交互功能，并且比特币本身出块慢，并不普适于高频率通信的 MPC 协议；而许可区块链往往需要添加相应组件才能够正常工作，构造与使用起来更加复杂，并且执行效率相对更低。

从安全性来说，链外 MPC 为 MPC 提供了一种新的解决方案，通过区块链引入奖惩、数据验证等功能机制，成功构造出一系列用于数据保护、数据共享等不同方向的满足财务公平性的协议。虽然链外 MPC 在假设的条件下能够达成财务公平性，在一定程度上有利于 MPC 的实际利用，但是多数链外 MPC 研究仍存在着单独的 MPC 网络，需要保障该单独的 MPC 网络的安全性，才能保证协议整体的安全性。

表 5 链外 MPC 总结

Tab. 5 Summary of off-chain MPC

方案	安全模型			设计目标	应用场景	区块链类型
	半诚实模型	恶意模型	其他			
文献[17-21]	√	公平性	财务公平	安全性	公平抽奖协议	比特币
文献[22]	√	公平性、鲁棒性	财务公平	安全性	提高安全性	
文献[23]	√	—	满足拍卖场景需求	安全性 实用性	密封拍卖	
文献[24]	√	—	隐蔽敌手模型下 $(1-1/n)$威胁度	安全性	隐蔽敌手模型下 的安全性	以太坊
文献[25]	√	公平性	财务公平	安全性	提高安全性	
文献[26]	√	—	—	实用性	隐私保护数据共享	
文献[27]	√	带中止安全	—	实用性	隐私保护储能共享	
文献[28]	√	带中止安全	—	实用性	隐私保护分布式计算平台	区块链
文献[29]	√	公平性、鲁棒性	财务公平	安全性 实用性	开放信誉系统	
文献[30]	√	—	—	实用性	隐私保护数据共享	
文献[31]	√	公平性	财务公平	安全性 实用性	提高安全性 降低系统开销	
文献[32]	√	公平性	财务公平	安全性 实用性	隐私保护加密 货币交换	
文献[33]	√	—	—	实用性	边缘智能电网双端 隐私保护 MPC	
文献[34]	√	带中止安全	—	—	隐私感知、可公开 验证 MPC	
文献[35]	√	公平性	量子安全 财务公平 抗 DDoS	安全性	提高安全性	

5　总结与展望

5.1　区块链的作用

区块链在链上/链外 MPC 中均扮演了不同的角色，提供了一些独特的特性和优势。

首先，区块链可以为 MPC 提供独特的通信手段。常规 MPC 协议模型依赖于传统的通信信道，因为对信道的假设过于复杂，所以一般情况下 MPC 协议默认参与方之间存在安全直连的通信信道。基于区块链的 MPC 不存在这方面的困扰，区块链去中心化的性质能够更容易建立起信任的通信渠道，通过交易机制等独特优势为 MPC 协议提供了新的通信方法。

其次，MPC 协议只考虑协议本身的计算安全、隐私保护，由于不考虑身份认证，因而很难被用于构建身份认证机制。相反，区块链中涉及到较多的身份认证机制，尤其是以 Fabric 为代表的许可链中，参与者需要有自己的“身份”“组织”。区块链可以为链上/链外 MPC 提供不同程度的身份认证机制，提高 MPC 协议整体的实用性。

最后，区块链与 MPC 协议的结合，提升了 MPC 协议的安全性。链外 MPC 的设计目标在于安全性，将区块链的交易机制与 MPC 协议流程相结合，成功在 MPC 协议基础上引入了交易机制、数据完整性验证等功能，成功实现了财务公平性等恶意敌手模型下的安全需求。链上 MPC 的计算参与方作为节点在 Fabric 上完成 MPC 协议，在协议本身安全性的基础上提供了多重身份认证、数据验证的功能保障，达到了更全面的安全性。

5.2　链上 MPC 与链外 MPC 对比总结

表 6 展示了链上 MPC 与链外 MPC 的对比总结。从使用的区块链类型上来看，链上 MPC 常使用许可链，尤其是 Fabric，而链外 MPC 常使用非许可链，这也造就了两者的设计目标的区别：链外 MPC 普适性强，能够相对灵活地结合使用外部系统的功能，结合区块链本身的特性特点，能够以相对安全、有效的方法来实现 MPC 协议，所以链外 MPC 的设计目标以安全性居多；链上 MPC 实用性强，将区块链本身的性能发挥到极致，通常会结合使用许可链的身份认证、私有通道等机制，有更全面、系统的隐私保护机制。

表 6　链上 MPC 与链外 MPC 的对比总结

Tab. 6　Comparison between on-chain MPC and off-chain MPC

内容	链上 MPC	链外 MPC
文献数量	少	多
使用的区块链类型	许可链	非许可链
设计目标	实用性居多	安全性居多
区块链使用程度	相对高	相对低
设计重心	将 MPC 与区块链结构融合，倾向于区块链	智能合约设计、MPC 设计，倾向于 MPC
安全模型	常见为半诚实敌手安全，但能通过区块链提供更强的安全性	常见为恶意敌手下的财务公平性，要达到更高的安全性需要依赖其他组件，如可信硬件
可扩展性	提供可插拔组件，但是不便于修改 MPC 协议与区块链结构本身	能添加其他的存储器、可信硬件等其他组件，MPC 协议本身也相对易修改
加密原语	MPC 与区块链本身	MPC 与区块链本身、零知识证明、属性基加密、代理重加密等
特点	基于许可、实用性强	安全性高、效率相对高
典型应用	首次公开募股、隐私保护信用评估	隐私保护数据共享、隐私保护能源存储共享

设计目标上的区别也导致了它们在设计重心上有所区分，链上 MPC 将 MPC 贯通于区块链结构中，而链外 MPC 多以智能合约接口访问为模式利用区块链提供部分功能，所以前者的设计重心偏向区块链，而后者偏向 MPC 协议本身。

总的来说，链上 MPC 与区块链本身联系更加紧密，基于许可链的隐私保护机制增强了系统

整体的安全性，并且能够通过增添自定义可插拔组件的方式在一定程度上提高可扩展性。也因此，链上 MPC 更适合被用于现实中企业、政府等存在身份机制的应用场景。链外 MPC 通过增强安全性的方式来提高 MPC 协议的实用性，它主要依赖于区块链的交易、智能合约等机制，加上由区块链强制执行的奖惩机制来提高 MPC 协议本身的安全性，以更加轻松的方式来达成公平性（相较于单独依赖于 MPC 本身）。同时，链外 MPC 可以与更多种加密原语进行技术结合，灵活性更强，适合用于隐私保护数据共享、能源存储共享等隐私计算的应用场景中。

5.3 研究展望

本文认为未来需要研究的内容有以下几方面：

1）构造方面。链外 MPC 已有一套相对成熟的构造体系，但是链上 MPC 还相对欠缺。目前的链上 MPC 高度依赖于 Fabric 以及其可插拔组件的特性，需要提供新的组件支持才能够成功实现链上 MPC。提出一种更加简单、高效的链上 MPC 构造方式是一大研究难点，但对于隐私计算的发展以及 MPC 的实践运用来说意义非凡。

2）效率方面。目前，无论是链外 MPC 还是链上 MPC 都缺乏效率评估体系，难以开展分析，但基于目前的研究可以得知链上 MPC 的效率相对更低。本文的后续工作将尝试从通信复杂度、交易复杂度、验证复杂度等多方面对相关方案进行分析，尝试得出一套可行的评价体系。如何系统评价并提高方案执行效率是当前的难点与痛点。

3）应用方面。链外 MPC 的构造模型已趋向成熟，下一步可以考虑技术融合并增强实用性，尤其是使用零知识证明、可信执行环境等隐私计算技术与之相结合，是当前发展的必然趋势。而链上 MPC 的实用性本身相对较强，亟需解决的还是效率方面的问题。

4）其他方面。本文的研究重心是“基于区块链的 MPC”，将区块链视作辅助技术来为 MPC 协议提供更强的安全性、实用性等。如何将 MPC 技术利用于区块链之中也是非常值得探索的研究方向，目前已经有部分相关研究成果，如私有智能合约框架 Hawk[88-89]、量子安全智能合约系统 SodsMPC[90]等。

6 结束语

隐私问题是科技进步发展的核心问题之一，技术融合指明了一条强化隐私保护技术的道路。基于区块链的 MPC 成功解决了长期以来 MPC 协议难以在恶意敌手模型下实现公平性的问题，大大提高了 MPC 的实用性，值得进行更加深入、全面的研究发展。希望本文的研究能对广大研究者的后续工作有所帮助。

参 考 文 献

[1] BENHAMOUDA F, HALEVI S, HALEVI T. Supporting private data on hyperledger fabric with secure multiparty computation[J]. IBM Journal of Research and Development, 2019, 63(2/3): 1-8.

[2] BENHAMOUDA F, DE CARO A, HALEVI S, et al. Initial public offering (IPO) on permissioned blockchain using secure multiparty computation[C]// Proceedings of 2019 IEEE International Conference on Blockchain. [S. l.]: IEEE, 2019: 91-98.

[3] YAO A C. Protocols for secure computations[C]// Proceedings of the 23rd Annual Symposium on Foundations of Computer Science. [S. l.]: IEEE, 1982: 160-164.

[4] 钱文君，沈晴霓，吴鹏飞，等. 大数据计算环境下的隐私保护技术研究进展[J]. 计算机学报，2022，45(4)：669-701.
QIAN Wenjun, SHEN Qingni, WU Pengfei, et al. Research progress on privacy-preserving techniques in big data computing environment[J]. Chinese Journal of Computers, 2022, 45(4): 669-701. (in Chinese)

[5] CLEVE R. Limits on the security of coin flips when half the processors are faulty[C]//Proceedings of the 18th Annual ACM Symposium on Theory of Computing. [S. l.: s. n.], 1986: 364-369.

[6] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J/OL]. Bitcoin, 2008, 4(2): 15[2023-09-06]. https://bitcoin.org/bitcoin.pdf.

[7] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016，42(4)：481-494.
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494. (in Chinese)

[8] 刘峰，杨杰，李志斌，等. 一种基于区块链的泛用型数据隐私保护的安全多方计算协议[J]. 计算机研究与发展，2021，58(2)：281-290.
LIU Feng, YANG Jie, LI Zhibin, et al. A secure multi-party computation protocol for universal data

privacy protection based on blockchain[J]. Computer Research and Development, 2021, 58(2): 281-290. (in Chinese)

[9] 王斌,张磊,张国印.基于多方安全计算的属性泛化mix-zone[J].通信学报,2019,40(4):83-94.
WANG Bin, ZHANG Lei, ZHANG Guoyin. Attribute generalization mix-zone based on multiple secure computation[J]. Journal of Communications, 2019,40(4):83-94. (in Chinese)

[10] CATHOMAS G, CACHIN C, ALPOS O. Multiparty computation on blockchain[D]. Bern: University of Bern, 2022.

[11] ZHONG H R, SANG Y P, ZHANG Y C, et al. Secure multi-party computation on blockchain: an overview[C]//Proceedings of International Symposium on Parallel Architectures, Algorithms and Programming. [S.l.]:Springer,2020: 452-460.

[12] WU S Q, LI J, DUAN F H, et al. The survey on the development of secure multi-party computing in the blockchain[C]//Proceedings of the 6th International Conference on Data Science in Cyberspace. [S.l.]: IEEE, 2021: 1-7.

[13] 刘炜,唐琮轲,马杰,等.区块链在隐私计算中的应用研究进展[J].郑州大学学报(理学版),2022,54(6):12-23.
LIU Wei, TANG Congke, MA Jie, et al. Application research and progress of blockchain in privacy computing[J]. Journal of Zhengzhou University (Natural Science Edition), 2022, 54(6): 12-23. (in Chinese)

[14] GARG S, VASHISHT R. A permissioned blockchain system for secure multiparty computation[J]. Journal of Physics: Conference Series, 2021, 1998: 012003.

[15] ZHOU J P, FENG Y X, WANG Z Y, et al. Using secure multi-party computation to protect privacy on a permissioned blockchain[J]. Sensors, 2021, 21(4): 1540.

[16] QIAO Y C, LAN Q J, ZHOU Z D, et al. Privacy-preserving credit evaluation system based on blockchain[J]. Expert Systems with Applications, 2022, 188: 115989.

[17] ANDRYCHOWICZ M, DZIEMBOWSKI S, MALINOWSKI D, et al. Secure multiparty computations on bitcoin[C]//Proceedings of IEEE Symposium on Security and Privacy. NJ:IEEE,2014:443-458.

[18] ANDRYCHOWICZ M, DZIEMBOWSKI S, MALINOWSKI D, et al. Fair two-party computations via bitcoin deposits[C]//Proceedings of the 18th International Conference on Financial Cryptography and Data Security. [S.l.:s.n.],2014: 105-121.

[19] BENTOV I, KUMARESAN R. How to use bitcoin to design fair protocols[C]//Proceedings of the 34th Annual International Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014: 421-439.

[20] KUMARESAN R, MORAN T, BENTOV I. How to use bitcoin to play decentralized poker[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. [S.l.:s.n.], 2015: 195-206.

[21] KUMARESAN R, VAIKUNTANATHAN V, VASUDEVAN P N. Improvements to secure computation with penalties[C]//Proceedings of 2016 ACM SIGSAC Conference on Computer and Communications Security. [S.l.:s.n.],2016: 406-417.

[22] KIAYIAS A, ZHOU H S, ZIKAS V. Fair and robust multi-party computation using a global transaction ledger[C]//Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques. [S.l.:s.n.],2016: 705-734.

[23] WANG J Z, SHEN Y, WANG B C. Sealed-bid auction scheme based on blockchain and secure multi-party computation[C]//Proceedings of the 5th Information Technology, Networking, Electronic and Automation Control Conference. [S.l:s.n.],IEEE, 2021: 407-412.

[24] ZHU R Y, DING C C, HUANG Y. Efficient publicly verifiable 2PC over a blockchain with applications to financially-secure computations[C]//Proceedings of 2019 ACM SIGSAC Conference on Computer and Communications Security. [S.l.]:ACM, 2019: 633-650.

[25] 黄建华,江亚慧,李忠诚.利用区块链构建公平的安全多方计算[J].计算机应用研究,2020,37(1):225-230.
HUANG Jianhua, JIANG Yahui, LI Zhongcheng. Constructing fair secure multi-party computation based on blockchain[J]. Application Research of Computers,2020,37(1):225-230. (in Chinese)

[26] LU K, ZHANG C Y. Blockchain-based multiparty computation system[C]//Proceedings of the 11th International Conference on Software Engineering and Service Science. [S.l.]: IEEE, 2020: 28-31.

[27] WANG N, CHAU S C K, ZHOU Y. Privacy-preserving energy storage sharing with blockchain and secure multi-party computation[J]. ACM SIGEnergy Energy Informatics Review, 2021, 1(1): 32-50.

[28] ZYSKIND G, NATHAN O, PENTLAND A. Enigma: decentralized computation platform with guaranteed privacy[EB/OL]. (2015-06-10)[2023-09-07]. https://arxiv.org/abs/1506.03471.

[29] GAO H M, MA Z F, LUO S S, et al. BFR-MPC: a blockchain-based fair and robust multi-party computation scheme[J]. IEEE Access, 2019, 7: 110439-110450.

[30] YANG Y H, WEI L J, WU J, et al. Block-SMPC: a blockchain-based secure multi-party computation for privacy-protected data sharing[C]//Proceedings of the 2nd International Conference on Blockchain Technology. [S. l.: s. n.], 2020: 46-51.

[31] BAUM C, DAVID B, DOWSLEY R. Insured MPC: efficient secure computation with financial penalties [C]//Proceedings of the 24th International Conference on Financial Cryptography and Data Security. [S. l.]: Springer, 2020: 404-420.

[32] BAUM C, DAVID B, FREDERIKSEN T K. P2DEX: privacy-preserving decentralized cryptocurrency exchange[C]//Proceedings of the 19th International Conference on Applied Cryptography and Network Security. [S. l.]: Springer, 2021: 163-194.

[33] GUAN Z T, ZHOU X, LIU P, et al. A blockchain-based dual-side privacy-preserving multiparty computation scheme for edge-enabled smart grid[J]. IEEE Internet of Things Journal, 2022, 9(16): 14287-14299.

[34] YANG Y H, WU J, LONG C N, et al. Blockchain-enabled multiparty computation for privacy preserving and public audit in industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2022, 18(12): 9259-9267.

[35] JIANG Y B, ZHOU Y, FENG T. A blockchain-based secure multi-party computation scheme with multi-key fully homomorphic proxy re-encryption[J]. Information, 2022, 13(10): 481.

[36] LINDELL Y. Secure multiparty computation[J]. Communications of the ACM, 2021, 64(1): 86-96.

[37] FENG D G, YANG K. Concretely efficient secure multi-party computation protocols: survey and more [J]. Security and Safety, 2022, 1: 2021001.

[38] ZHAO C, ZHAO S N, ZHAO M H, et al. Secure multi-party computation: theory, practice and applications[J]. Information Sciences, 2019, 476: 357-372.

[39] CANETTI R. Universally composable security: a new paradigm for cryptographic protocols[C]//Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science. [S. l.]: IEEE, 2001: 136-145.

[40] GOLDREICH O. Foundations of cryptography: volume 2, basic applications[M]. Cambridge: Cambridge University Press, 2009.

[41] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[42] CRAMER R, DAMGARD I, ISHAI Y. Share conversion, pseudorandom secret-sharing and applications to secure computation[C]//Proceedings of the 2nd Theory of Cryptography Conference. [S. l.: s. n.], 2005: 342-362.

[43] RABIN M O. How to exchange secrets with oblivious transfer[EB/OL]. [2023-09-08]. https://eprint.iacr.org/2005/187.

[44] EVEN S, GOLDREICH O, LEMPEL A. A randomized protocol for signing contracts[J]. Communications of the ACM, 1985, 28(6): 637-647.

[45] BRASSARD G, CRÉPEAU C, ROBERT J M. All-or-nothing disclosure of secrets[J]. Lecture Notes in Computer Science, 1987, 263: 234-238.

[46] BEAVER D. Correlated pseudorandomness and the complexity of private computations[C]//Proceedings of the 28th Annual ACM Symposium on Theory of Computing. [S. l.: s. n.], 1996: 479-488.

[47] ISHAI Y, KILIAN J, NISSIM K, et al. Extending oblivious transfers efficiently[J]. Lecture Notes in Computer Science, 2003, 2729: 145-161.

[48] BOYLE E, COUTEAU G, GILBOA N, et al. Efficient pseudorandom correlation generators: silent OT extension and more[C]//Proceedings of the 39th Annual International Cryptology Conference. [S. l.: s. n.], 2019: 489-518.

[49] LINDELL Y, PINKAS B. A proof of security of Yao's protocol for two-party computation[J]. Journal of Cryptology, 2009, 22(2): 161-188.

[50] LU Y. The blockchain: state-of-the-art and research challenges[J]. Journal of Industrial Information Integration, 2019, 15: 80-90.

[51] YUAN Y, WANG F Y. Blockchain and cryptocurrencies: model, techniques, and applications[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 48(9): 1421-1428.

[52] 袁勇,倪晓春,曾帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.
YUAN Yong, NI Xiaochun, ZENG Shuai, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022. (in Chinese)

[53] LAMPORT L. The part-time parliament[M]. New York: Association for Computing Machinery, 2019.

[54] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//Proceedings of 2014 USENIX Annual Technical Conference. [S. l.: s. n.], 2014: 305-319.

[55] JAKOBSSON M, JUELS A. Proofs of work and

bread pudding protocols[C]//Proceedings of the IFIP TC6/TC11 Joint Working Conference on Secure Information Networks: Communications and Multimedia Security. [S. l.]: Springer, 1999: 258-272.

[56] SALEH F. Blockchain without waste: proof-of-stake [J]. The Review of Financial Studies, 2021, 34(3): 1156-1190.

[57] SAMANI K, JAIN T. Delegated proof of stake: features and tradeoffs[EB/OL]. (2018-02-03)[2023-09-08]. https://multicoin. capital/2018/03/02/delegated-proof-stake-features-tradeoffs/.

[58] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[59] SZABO N. Formalizing and securing relationships on public networks[J]. First Monday, 1997, 2(9): 1-15.

[60] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151: 1-32.

[61] 欧阳丽炜，王帅，袁勇，等. 智能合约：架构及进展[J]. 自动化学报，2019，45(3)：445-457.
OUYANG Liwei, WANG Shuai, YUAN Yong, et al. Smart contract: architecture and research progresses [J]. Acta Automatica Sinica, 2019, 45(3): 445-457. (in Chinese)

[62] ZOU W Q, LO D, KOCHHAR P S, et al. Smart contract development: challenges and opportunities [J]. IEEE Transactions on Software Engineering, 2019, 47(10): 2084-2106.

[63] CLACK C D, BAKSHI V A, BRAINE L. Smart contract templates: foundations, design landscape and research directions[EB/OL]. (2017-05-15)[2023-09-08]. https://arxiv. org/abs/1608. 00771.

[64] 贺海武，延安，陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展，2018，55(11)：2452-2466.
HE Haiwu, YAN An, CHEN Zehua. Survey of smart contract technology and application based on blockchain[J]. Journal of Computer Research and Development, 2018, 55(11): 2452-2466. (in Chinese)

[65] Linux Foundation. Key concepts[EB/OL]. [2023-10-10]. https://hyperledger-fabric. readthedocs. io/en/latest/key_concepts. html.

[66] DAMGÅRD I, PASTRO V, SMART N, et al. Multiparty computation from somewhat homomorphic encryption[C]//Proceedings of Annual Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 643-662.

[67] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of 2007 IEEE Symposium on Security and Privacy. [S. l.]: IEEE, 2007: 321-334.

[68] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Proceedings of Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999: 223-238.

[69] BENET J. IPFS-content addressed, versioned, P2P file system[EB/OL]. (2014-07-14)[2023-09-08]. https://arxiv. org/abs/1407. 3561.

[70] BLUM M. Coin flipping by telephone a protocol for solving impossible problems [J]. ACM SIGACT News, 1983, 15(1): 23-27.

[71] ANDRYCHOWICZ M, DZIEMBOWSKI S, MALINOWSKI D, et al. How to deal with malleability of bitcoin transactions[EB/OL]. (2013-12-11)[2023-09-08]. https://arxiv. org/abs/1312. 3230.

[72] CANETTI R, DODIS Y, PASS R, et al. Universally composable security with global setup[C]//Proceedings of the 4th Theory of Cryptography Conference. [S. l. : s. n.], 2007: 61-85.

[73] KATZ J, MAURER U, TACKMANN B, et al. Universally composable synchronous computation[C]//Proceedings of the 10th Theory of Cryptography Conference. [S. l. : s. n.], 2013: 477-498.

[74] GARAY J A, MACKENZIE P, PRABHAKARAN M, et al. Resource fairness and composability of cryptographic protocols[J]. Journal of Cryptology, 2011, 24(4): 615-658.

[75] BONEH D, NAOR M. Timed commitments[C]//Proceedings of the 20th Annual International Cryptology Conference. [S. l. : s. n.], 2000: 236-254.

[76] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. [S. l.]: Springer, 2001: 552-565.

[77] GENNARO R, RABIN M O, RABIN T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography[C]//Proceedings of the 17th Annual ACM Symposium on Principles of Distributed Computing. [S. l: s. n.], 1998: 101-111.

[78] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]//Proceedings of Annual International Cryptology Conference. [S. l: s. n.], 1991: 129-140.

[79] DAMGÅRD I. On Σ-protocols[EB/OL]. [2023-10-08]. https://www. cs. au. dk/~ivan/Sigma. pdf.

[80] FIAT A, SHAMIR A. How to prove yourself: practical solutions to identification and signature problems [C]//Proceedings of Conference on the Theory and Application of Cryptographic Techniques. [S. l. : s. n.], 1986: 186-194.

[81] PETER A, TEWS E, KATZENBEISSER S. Efficiently outsourcing multiparty computation under multiple keys[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 2046-2058.

[82] CAMENISCH J, DRIJVERS M, GAGLIARDONI T, et al. The wonderful world of global random oracles [C]//Proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques. [S. l.]: Springer, 2018: 280-312.

[83] PEIKERT C, VAIKUNTANATHAN V, WATERS B. A framework for efficient and composable oblivious transfer[C]//Proceedings of the 28th Annual International Cryptology Conference. [S. l.]: Springer, 2008: 554-571.

[84] FREDERIKSEN T K, PINKAS B, YANAI A. Committed MPC: maliciously secure multiparty computation from homomorphic commitments[C]//Proceedings of the 21st International Conference on Practice and Theory in Public-Key Cryptography. [S. l.]: Springer, 2018: 587-619.

[85] LIU C H, LIN Q X, WEN S. Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning[J]. IEEE Transactions on Industrial Informatics, 2018, 15(6): 3516-3526.

[86] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[C]//Proceedings of International Algorithmic Number Theory Symposium. [S. l.]: Springer, 1998: 267-288.

[87] XU G Q, BAI H P, XING J, et al. SG-PBFT: a secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles [J]. Journal of Parallel and Distributed Computing, 2022, 164: 1-11.

[88] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//Proceedings of 2016 IEEE Symposium on Security and Privacy. [S. l.]: IEEE, 2016: 839-858.

[89] BANERJEE A, CLEAR M, TEWARI H. zkHawk: practical private smart contracts from MPC-based Hawk[C]//Proceedings of the 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services. [S. l.]: IEEE, 2021: 245-248.

[90] DOLEV S, WANG Z Y. SodsMPC: FSM based anonymous and private quantum-safe smart contracts [C]//Proceedings of the 19th International Symposium on Network Computing and Applications. [S. l.]: IEEE, 2020: 1-10.

作 者 简 介

樊 凯

男，1978 年生，博士，教授，博士研究生导师，研究方向为密码智能应用、人工智能安全、数据安全与隐私保护

E-mail: kfan@mail. xidian. edu. cn

周自横

男，2000 年生，硕士研究生，研究方向为区块链、隐私计算

E-mail: zhoupanda@stu. xidian. edu. cn

袁望淞

男，2000 年生，硕士研究生，研究方向为安全推理、联邦学习

E-mail: fyvoo@stu. xidian. edu. cn

纪世元

男，2000 年生，硕士研究生，研究方向为可搜索加密、应用密码学

E-mail: shiyuan. ji@outlook. com

责任编辑 董 莉