

区块链与秘密分享融合技术综述

张亮^{1,2,3,4}, 刘百祥^{1,3,4}

(1.复旦大学 计算机科学技术学院 上海市智能信息处理重点实验室, 上海 200433;

2.海南大学 网络空间安全学院(密码学院), 海口 570228; 3.上海区块链工程技术研究中心, 上海 200433;

4.复旦大学义乌研究院, 浙江 义乌 322000)

摘要:近年来,区块链的持续发展使得应用密码学受到广泛关注,同时引起更多国内外学者对信息安全的重点研究。秘密分享技术作为构建安全多方计算协议的基础原语,具备门限特性且在应用中具有拜占庭容错性特点。由于在信息安全三要素,即机密性、完整性和可用性上的契合,区块链和秘密分享存在关联性和互补性。现有研究通过融合区块链和秘密分享技术提升了系统稳定性和效率,取得对分布式系统研究的突破。阐述区块链共识算法与拜占庭容错协议之间的关系,分析秘密分享对于实现权益证明共识算法的重要性。总结基于智能合约实现的不同种类的秘密分享体制,以及运用智能合约和秘密分享技术构建的密码协议和具体应用。说明公共通告栏与区块链、秘密分享技术之间的联系,综述使用秘密分享技术优化区块链数据存储的研究,并列举融合区块链存储和秘密分享技术可解决的实际应用。在此基础上,介绍区块链与秘密分享的功能特性和性能指标,展望两者融合的未来发展方向。

关键词:秘密分享;区块链;信息安全;门限;拜占庭容错;应用密码学

开放科学(资源服务)标志码(OSID):



中文引用格式:张亮,刘百祥.区块链与秘密分享融合技术综述[J].计算机工程,2022,48(8):1-11.

英文引用格式:ZHANG L, LIU B X. Survey on integrated technology of blockchain and secret sharing[J]. Computer Engineering, 2022, 48(8): 1-11.

Survey on Integrated Technology of Blockchain and Secret Sharing

ZHANG Liang^{1,2,3,4}, LIU Baixiang^{1,3,4}

(1.Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China; 2.School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, China;

3.Shanghai Engineering Research Center of Blockchain, Shanghai 200433, China;

4.Yiwu Research Institute of Fudan University, Yiwu, Zhejiang 322000, China)

[Abstract] In recent years, the continuous development of blockchain have attracted widespread attention in the field of applied cryptography, and an increasing number of researchers worldwide are focusing on information security. As a basic primitive for constructing Secure Multi-Party Computation (SMPC) protocols, Secret Sharing (SS) technology has threshold characteristics and it is Byzantine Fault Tolerant (BFT) in applications. Due to similarities in terms of three elements of information security (confidentiality, integrity, and availability), blockchain and SS technology are related and complementary. Existing studies have made breakthroughs on distributed systems by integrating these two techniques. Firstly, this paper elaborates on the relationship between blockchain consensus algorithms and BFT protocols and analyses the importance of SS technology in implementing Proof of Stake (PoS) consensus algorithms. Secondly, it summarizes several types of SS systems based on smart contracts and cryptographic protocols or applications leveraging both smart contract and secret sharing technologies. Thirdly, it demonstrates the connection between the public bulletin board and blockchain, summarizes current research on incorporating SS technology for reducing blockchain storage, and introduces practical applications combining blockchain storage and SS technology. Finally, this paper presents the functional characteristics and performance indicators of blockchain and SS technology, and points out potential development directions when integrating these two techniques.

[Key words] Secret Sharing (SS); blockchain; information security; threshold; Byzantine Fault Tolerance (BFT); applied cryptography

DOI:10.19678/j.issn.1000-3428.0064102

基金项目:国家重点研发计划(2019YFB2101703);国家自然科学基金(U19A2066);上海市科技创新行动计划(20222420800, 20511102200);广东省重点领域研发计划(2020B0101090001);复旦大学义乌研究院项目(2019YFB2101703)。

作者简介:张亮(1989—),男,博士研究生,主研方向为区块链、应用密码学;刘百祥,讲师、博士。

收稿日期:2022-03-04 **修回日期:**2022-06-20 **E-mail:** briliasm@gmail.com

0 概述

区块链以经济金融学、密码学、博弈论和计算机科学为支撑^[1],近年来受到科技界和金融界的广泛关注,我国也将区块链列为一项互联网新型基础设施建设设施。早期的区块链系统仅采用密码学中的签名验签技术、哈希算法和一定的经济激励实现去中心化的数字货币功能。本质上,区块链是一个分布式的账本,即由多人共同对数据进行维护,保证数据在分布式场景下的一致性和正确性。早在1982年,LAMPOR等^[2]就提出了分布式系统的共识问题,即拜占庭容错(Byzantine Fault Tolerance, BFT)协议。与最早的区块链(比特币^[3])不同,从技术角度,拜占庭容错协议没有考虑经济刺激因素;从功能角度,拜占庭容错协议没有考虑交易的往来,因此没有形成一套类似比特币的数字货币系统;从规模角度,公有区块链允许参与者自由进出,而拜占庭容错协议具有准入门槛限制;从系统参与者角度,区块链和拜占庭容错协议均是多方协同合作,在无第三方权威和允许一定量恶意节点的前提下实现诚实参与者间的共识。

区块链的发展使得更多学者发现了区块链与拜占庭容错系统的相同点,使得两者的相关研究井喷式发展。秘密分享(Secret Sharing, SS)技术^[4]在拜占庭容错系统的发展史上占据重要地位。秘密分享是指分发者将秘密拆分成多个份额并分别发送给分布式场景下的多个份额接收者(即份额持有者),当且仅当超过一定数量的份额持有者合作才能恢复出发发者的秘密。此后,可验证秘密分享(Verifiable SS, VSS)^[5]和公开可验证秘密分享(Publicly VSS, PVSS)^[6]技术相继被提出。

秘密分享技术的分布式和容错性特点使其在数据可用性和数据隐私领域得到广泛引用,而可验证性进一步使得数据能够不被篡改,从而保证了数据完整性。因此,可验证秘密分享技术的研究是数据安全领域的核心之一。通过合理的设计和应用,秘密分享技术可以实现无中心的多方协作与多方计算。秘密分享技术涵盖了信息安全的三要素——数据机密性、数据完整性和数据可用性,即C.I.A.。

区块链也是一种安全多方计算(Secure Multi-Party Computation, SMPC)系统。区块链与秘密分享技术的结合,使得许多基于密码学的应用能够快速得以实施。区块链在共识的达成、数据的存储和智能合约中均可以与秘密分享技术相结合,从而在提升区块链稳定性和效率的同时,丰富区块链的功能,使得更多基于密码学的产品落地。这两者的结合能使一些经典的应用场景得到更高效和便利的实现,如电子投票^[7]、密钥管理^[8]、数据恢复^[9]等。

本文介绍秘密分享与区块链的融合研究,从共识层、合约层和存储层角度,结合秘密分享技术进行综述。虽然区块链近年来得到了迅速发展,但其在扩容性、共识速度、应用范围和存储冗余度等性能指标上仍存在不足。本文通过介绍秘密分享技术在区

块链领域中的应用和融合,为区块链的优化和发展提供新的视角和思路。

1 背景知识

1.1 (公开)(可验证)秘密分享

在秘密分享协议中, n 表示参与者个数, t 表示门限值, $0 < t \leq n$ 。在秘密分发阶段,分发者将秘密分为 n 个份额,并安全地发送给对应的份额持有者;在秘密恢复阶段,任意 t 个份额持有者可以恢复出秘密。秘密分享协议的安全性要求任意少于 t 个份额持有者不能得到秘密的任何信息。

秘密分享(SS)协议要求分发者诚实可信。可验证秘密分享协议在份额分发算法中添加承诺值,使得份额持有者可以根据份额和承诺值判定分发者的诚实性。相对于秘密分享,可验证秘密分享使得份额持有者可以发现秘密分发者是否向其发送了伪造的份额值。

在可验证秘密分享(VSS)协议中,份额是高度隐私信息,因此需要使用安全信道传输份额。为了能够在公开信道上传输份额,并且同时能被任何第三方验证,公开可验证秘密分享(Public VSS, PVSS)协议被提出和实现。在PVSS协议中,份额使用份额持有者的公钥加密保护得到。通过添加非交互的零知识(Non-Interactive Zero-Knowledge, NIZK)证明,加密后的份额能在公开环境中被任何人验证其正确性。

图1概括了秘密分享和可验证秘密分享在数据安全领域所具备的功能特性^[10]。这些功能特性使得秘密分享技术成为构建安全多方计算协议的重要基础原语,也使得秘密分享与区块链的结合成为可能。

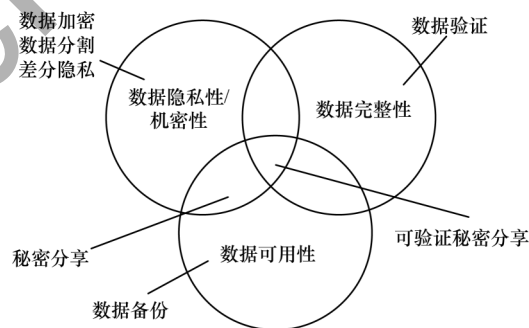


图1 (可验证)秘密分享在数据安全领域的功能特性

Fig.1 Function characteristics of (verifiable) secret sharing in the field of data security

1.2 区块链系统

从技术栈角度,区块链系统的构建可以划分为存储层、网络层、共识层、智能合约层、应用层等5个层级^[1]:存储层采用合适的数据结构或数据库对交易、事务和区块进行高效的存储管理;网络层采用点对点网络通信协议实现节点间的数据传输,其中允许出现拜占庭节点的恶意行为;共识层采用分布式共识算法和激励机制,实现拜占庭容错能力并解决分布式一致性问题;智能合约层基于分布式共识下的合约运行环境,提供高级语言编译和运行接口以

及相关的程序编译、执行环境;应用层提供用户可编程接口,使得技术人员能够简便自主地实现智能合约代码。

1.3 拜占庭容错

拜占庭容错(BFT)是指分布式系统具有容错性的特点,其起源于分布式系统中一个著名难题——拜占庭将军问题。构建拜占庭容错系统的难点在于,在存在恶意参与者的情况下,形成正确的共识困难度较高,并且需要同时满足安全性和活性:安全性是指所有诚实的参与者在所有决策中总是得到一致的共识结果;活性是指共识最终总是能达成,不会被恶意参与者中断。

1.4 安全多方计算

安全多方计算(SMPC)^[11]是指在无可信第三方的情况下,如何安全地将不同参与者手中的数值作为输入,计算一个函数值的问题。区块链常被看作

是一种安全多方计算协议或系统,而秘密分享通常作为安全多方计算的一种密码原语。秘密分享协议可以归纳为一组密码原语算法,协议中的秘密持有者通过网络分发份额,最后份额持有者通过网络协商达成份额是否分发成功的共识。区块链是一种遵循特定协议,具备存储、计算和可编程能力并且还在持续发展的系统。区块链系统中等节点通过构建并广播消息,然后对历史数据在全网达成一致性的共识。

秘密分享协议和区块链系统都具有多方性、容错性、分布式存储,以及借助网络协商达成共识的特性。结合文献[12]对安全多方计算和区块链技术的对比,本文进一步对比了(公开)(可验证)秘密分享((P)(V)SS)协议、安全多方计算和区块链技术,如表1所示,从中可以看出,秘密分享技术在安全多方计算和区块链中均具有重要作用。

表1 秘密分享、安全多方计算与区块链的对比

Table 1 Comparison among (P)(V)SS, SMPC and blockchain

对比内容	(P)(V)SS	SMPC	区块链
原理	秘密分发者向多个份额持有者发送其秘密份额,当且仅当超过额定秘密份额时,分发者的秘密可以被恢复	在分布式网络中,多个参与者各自持有秘密输入,共同完成某个函数的计算,除了计算结果外,任何人没有得到其他任何有效的信息	通过构建点对点网络,区块链中的参与者根据协议对合法交易进行验证、确认,并根据激励机制维护历史账本
技术特点	多方参与、容错性、分布式存储、(公开)可验证性、单一分发者	输入隐私性、计算正确性、去中心化	去中心化、基于激励机制的自信任、防篡改
关键技术	拉格朗日插值、零知识证明、拜占庭容错	加密电路、不经意传输、同态加密、秘密分享	签名认证、零知识证明、秘密分享、拜占庭容错
指令虚拟机	否	否	是
通信网络	是	是	是
应用场景	区块链系统、安全多方计算	联合数据分析、隐私计算、数据可信交换	数据共享、去中心化计算平台、数字货币
优势	可提高分布式场景中参与者的可信度	可保护参与者的数据隐私	可提升参与者的可信度,降低数据流转成本

2 秘密分享与区块链共识的融合研究

2.1 共识算法的拜占庭容错性特点

比特币^[3]使用工作量证明(Proof of Power, PoW)共识算法,一次性解决了区块链的多个问题:1)PoW算法解决了矿工节点和奖励对象的问题,只有一个成功完成工作量证明的节点才能具备合法打包权和接受系统的奖励;2)矿工的唯一性能够有效地解决“双花”问题,使金融系统无差错运行;3)根据最长链原则,要想对区块链系统进行控制,需要对历史上所有的交易进行重新打包和重新挖矿,而这被认为在经济上是不可行的;4)PoW系统中的任意节点可以任意加入和退出,并且对系统中的其他节点不产生影响。

文献[13-14]通过将PoW共识算法提供的无争议性和安全性与拜占庭容错协议相关联,从而证明区块链也是一种具备拜占庭容错性的状态机副本模型系统。在PoW共识算法中,当矿工节点宣布对最新区块 $a_k \leftarrow b$ 的打包权时,其不仅是对最新区块 b 的声明,也是对历史区块 $\{a_1, a_2, \dots, a_{k-1}\}$ 的再次确认。由于多个矿工在某一段时间内可能都成功地找到了PoW要求的工作量证明,根据最长链原则,唯一的矿

工的工作在全网形成共识,从而体现安全性。由于所有的矿工都是独立工作的,根据PoW算法的要求和复杂度系数调整,诚实参与者完成工作量证明并公之于众,同时得到所有诚实节点的确认和认可,即保证活性。

区块链中的PoW算法与经典拜占庭容错(BFT)协议有紧密联系。表2总结了PoW算法和BFT协议在实现区块链共识算法时的差异。

表2 PoW算法与BFT协议的对比

Table 2 Comparison between PoW algorithm and BFT protocol

对比内容	PoW算法	BFT协议
共识前提	少量节点基于前序证明实现共识即可	超过系统额定数量的节点共同决策
耗能	高	低
节点数	几乎无限	有限(通常在几千以内)
节点自由进出	是	否
激励机制	是	否
节点身份管理	否	是
共识特点	概率确定性	即时确定性

文献[15]指出,对拜占庭容错共识算法的扩容研究方案包含并行处理事务、使用可信硬件、设置代理委员会、选取密码学原语和优化通信网络拓扑结构。近年来,越来越多的研究使用秘密分享技术优化具备拜占庭容错性的共识算法。随着区块链的持续发展,研究者提出了非对称拜占庭容错共识算法^[16]。非对称拜占庭容错共识算法起源于非对称信任,即在分布式系统中,每个参与者根据自己已获得的信息判断其他参与者是否诚实可信。可信随机数是解决拜占庭容错共识算法中公平问题的基础,在此方面,文献[16-17]使用秘密分享技术构建可信随机源,保证了随机数的可获得性。

2.2 秘密分享与拜占庭容错协议

秘密分享协议和拜占庭容错协议均具有容错性。通常,一次秘密分享协议的运行只有单一的分发者,而拜占庭容错协议往往要求所有节点对等。因此,秘密分享协议常作为构建拜占庭容错协议的子步骤或子环节。许多具备拜占庭容错特性的协议,如可验证随机数信标(Beacon)协议^[18-19]和分布式密钥生成DKG协议^[20],通过让每个参与者在每个轮次中分别调用一次秘密分享协议,从而达到去中心化的目的。不同的通信信道和敌手模型对拜占庭容错协议的效率 and 安全性有巨大影响,拜占庭容错协议通常使用VSS或PVSS协议来验证消息发送者的诚实性,并提升消息在协议中的恢复能力。

拜占庭容错协议通常直接达成对某一明文的共识,而明文不能有效地保护数据的隐私。鉴于此,文献[21]提出VSSR(VSS Recovery)协议应用到拜占庭容错协议中,从而构建了一个私有的基于键值对的PBFT协议^[22]。

不仅秘密分享技术可以改善具有拜占庭容错能力的协议,具备拜占庭容错能力的协议也可以促进秘密分享协议的研究。在秘密的份额被分享之后,随着时间推移,多个份额被恶意节点持有的概率将增大。在恶意节点结合超过门限值的份额前,秘密持有者需要定时更新份额,只要攻击者访问少于设定的阈值,系统就会保持安全,使得攻击者只有较少的时间来破坏秘密分享体制。

主动式秘密分享(Proactive Secret Sharing, PSS)^[23]是对秘密分享的一种扩展,被用于加强秘密分享者秘密的安全性。在PSS协议中,秘密份额的更新过程由份额持有者发起,每个份额持有者各自构造一个随机的多项式,并执行秘密分享的分发过程,最后每个份额持有者更新手中的份额值。用此方法可避免攻击者通过收集足够的旧的份额值来恢复秘密。相对于同步情况下的PSS协议,APSS(Asynchronous PSS)协议^[24]更能抵抗DoS攻击和动态敌手攻击,异步情况下的PSS更实用和贴近真实网络情况。虽然

网络模型更切实,但是APSS协议^[24]借助互联网实现通信并达到网络节点中的共识,其通信量复杂度达到了指数级别。

2.3 秘密分享对PoS共识的贡献

PoW共识需要消耗大量电力,在此背景下,引申出了权益证明(Proof of Stake, PoS)共识算法^[25]。PoS设计思想不是通过做工作量证明,而是通过抵押权益体现对区块链系统的忠诚,最后从共识算法中分得红利。由于区块链的所有规则都是公开透明的,因此如何有效地制定激励机制显得尤为重要。其中,为了体现公平原则,可信赖的随机数至关重要。因为在透明机制下不能按照已知的信息来分配挖出的矿,否则所有参与者都将对系统发起攻击,最大化自己从系统中获取的利润。比特币系统通过PoW算法和最长链原则解决了该问题。PoS共识算法则是为解决耗能耗电的PoW算法而被提出。

区块链中的PoS共识算法与Beacon协议是一对孪生问题^[25-26]。事实上,PoW共识算法根据哈希值的随机性来选取最终的矿工,拥有算力高的节点成为矿工的概率更高。文献[25]指出PoS共识算法的一个重大挑战是设计好的方法在分布式系统中实现领导节点的公平和随机选取。Beacon的研究是为了防范恶意节点通过概率分析和协议模拟影响协议的公平性和随机性,甚至破坏系统的可用性。为了实现区块链系统中PoS相关的共识,PVSS技术得到广泛研究和应用。

由于PVSS技术的多方协同性和公开可验证性,因此其经常被用于构建Beacon协议,进而实现PoS共识算法的核心思想。Ouroboros^[25]、SCRAPE^[27]、RandShare^[28]、Hydrand^[26]等系统均依托点对点网络模型,使用PVSS作为底层密码原语技术实现Beacon协议,这些协议均可进一步用于实现权益证明共识算法。图2描述了基于PVSS协议生成Beacon协议的一般流程,其中,每个轮次后 n 个参与者都会得到一个共同的公开可验证随机数。

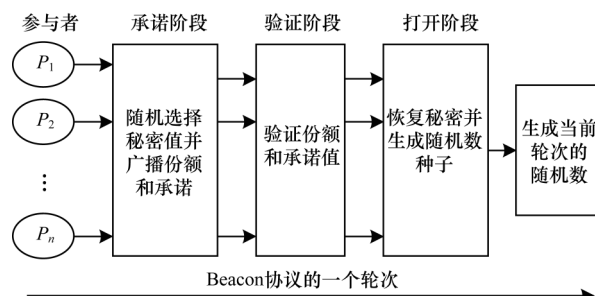


图2 基于PVSS实现Beacon协议的一般流程

Fig.2 General procedure of Beacon protocol implementation based on PVSS

通过使用不同的(P)VSS协议和假设不同的网络通信模型,Ouroboros^[25]、SCRAPE^[27]、RandShare^[28]、Hydrand^[26]和Dfinity^[9]实现的Beacon协议也具有不同

的性质和复杂度。对上述方法实现的 Beacon 协议进行对比,如表3所示。其中: n 是系统中的节点个数; c 是对系统分组后的组成员节点个数;Hydrand^[26]通过在每一个轮次中选取一个领导节点,模仿同步条件下的

拜占庭容错协议过程实现 Beacon 协议。通过对比可知,Hydrand^[26]通信、计算和验证复杂度较高,并且具备良好的活性/随机性,但是,该系统假设的是同步的网络通信模型。

表3 不同 Beacon 协议的对比
Table 3 Comparison among different Beacon protocols

协议	(P)VSS	活性/随机性	是否实现 PoS	通信模型	通信复杂度	计算复杂度	验证复杂度
Ouroboros ^[25]	PVSS	高	是	同步	$O(n^3)$	$O(n^3)$	$O(n^3)$
SCRAPE ^[27]	PVSS	高	否	同步	$O(n^3)$	$O(n^2)$	$O(n^2)$
RandShare ^[28]	PVSS	低	否	异步	$O(n^3)$	$O(n^3)$	$O(n^3)$
Hydrand ^[26]	PVSS	高	否	同步	$O(n^2)$	$O(n)$	$O(n)$
Dfinity ^[9]	VSS	中	是	同步	$O(cn)$	$O(c)$	$O(1)$

3 秘密分享与智能合约的融合研究

智能合约是一段代码,与传统的程序代码不同,为了体现区块链的不可篡改、可追溯以及公开透明性,智能合约的代码和数据通常是公开的。智能合约代码运行和数据沉淀(即写入区块链)都是在区块链共识之上的。从比特币的脚本到图灵完备执行环境,智能合约使得任意可以计算的问题都能够得以解决。总体而言,在无须可信第三方存在的情况下,区块链的智能合约提供了两大功能,即公开透明的存储和计算。本节将从区块链合约层和秘密分享体制中找到结合点:一方面,分析区块链智能合约如何为秘密分享体制的实现带来便捷;另一方面,发掘基于区块链智能合约和秘密分享技术的应用场景。

3.1 基于智能合约的秘密分享体制

区块链的智能合约由一组代码组成,这段代码具有公开透明性。采用零知识证明方法可以保护合约参与者的身份信息和敏感隐私数据。

原始的秘密分享技术需要借助隐蔽安全的信道将秘密持有者生成的份额传递给其他人。PVSS 等技术通过对份额进行加密处理,使其可以在公开的信道上传递和存储,同时保证份额在传递过程中的机密性。PVSS 使用了非交互的零知识证明技术用于证明被加密份额的正确性。在零知识证明中,验证者可以将加密后的份额上传到区块链,从而使得区块链能自动判断加密后份额的正确性。智能合约提供了公开透明的存储和计算能力,将其与 PVSS 相结合,可以有效提高系统性能。

区块链智能合约除了能实现 PVSS 协议之外,还可以为支持公开验证的秘密分享协议提供服务。文献[29]使用智能合约技术实现了一种无中心的分层秘密分享(Hierarchical Secret Sharing, HSS)体制。通常份额持有者具有层级的关系,因此通过多次运行秘密分享体制,可以使秘密能够实现多层级的管理。在 HSS 体制中:一方面,智能合约承担着可信验证者的角色;另一方面,通过智能合约,协议能够使用抵押来要求参与者正确地遵守协议。文献[29]基于以太坊测试网络验证了其方案的可行性,并给出

了以太坊 Gas 消耗和算法执行时间消耗。相较于非基于区块链智能合约的 HSS 协议,该协议仅需 1 轮通信,同时具备可验证性和公平性且无须可信第三方。

图3显示了基于智能合约构造秘密分享协议的流程。其中:分发者在分发过程中通过智能合约实现份额的分发和验证;份额持有者在秘密恢复过程中通过智能合约实现秘密的重建;智能合约可以提供公开验证计算、可信存储、激励机制等服务。

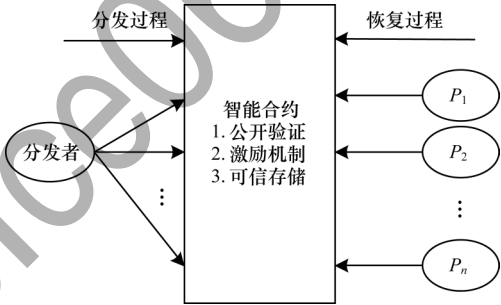


图3 基于智能合约实现秘密分享协议的过程

Fig.3 Procedure of secret sharing protocol implementation based on smart contract

3.2 智能合约和秘密分享结合的应用

目前,区块链技术已经从加密货币发展成为一项可编程的分布式基础设施,区块链上的程序也被称为智能合约。秘密分享协议可以结合一些应用场景,在智能合约之中实现并应用。

传统的电子投票系统需要依赖中心化的服务器来保证系统的完整性和安全性,然而中心化的服务器本身容易带来很多其他的问题,如单节点故障、信息泄露、贿选问题等。文献[30-31]均结合应用了秘密分享、同态加密和区块链智能合约实现电子投票系统。HSIAO 通过初始化 5 台计票服务器,每一个投票者将投票信息分成 5 份,其中任意 3 份可以恢复出对应的原始值,从而避免了单节点故障问题。区块链智能合约提供了公开透明的存储和计算,使得参与者能够对计票过程进行审计,提升了投票过程的公平性。

区块链智能合约在数据保护方面存在不足,为提升智能合约的安全性和隐私性,文献[32]开发了基于安全多方计算的智能合约平台。该平台包括3个层级:合约层,计算层和群组通信层。在合约层,提供了智能合约的框架描述,包含实现流程、语言结构和语法;在计算层,通用的线性秘密分享技术被用来保护参与者的输入和保证计算的正确性;在群组通信层,非阻塞的广播协议基于非阻塞的消息传递接口和拜占庭容错协议实现,具备异步的具有节点故障容错的网络通信服务。在该文研究中,秘密分享技术被用于构建安全多方计算协议,实现了群组合作中的信息隐私保护。

在医疗领域,结合使用区块链智能合约和秘密分享协议的研究也广泛流行。文献[33]提出一种使用区块链存储和智能合约验证计算的医疗数据共享解决方案。由于医疗数据具有极高的隐私性要求,而区块链提供的是公开透明的存储,为克服数据被窃取和监听的困难,该方案在系统中增加了用户和群组进行秘密分享的软件层。

一项具体的分布式应用的实施,可以证明基于区块链的智能合约技术具有可行性。然而,智能合约还可以进一步抽象成为一种无中心、可交互、可执行程序的对象。将智能合约和秘密分享相结合,对网络安全或密码学领域将有进一步的贡献。

文献[34]基于区块链的智能合约提出CHURP协议,并实现了主动式的秘密分享技术,其使用非对称二元多项式得到份额更新过程中的门限值,并使用高效的多项式承诺协议防止初始化失败,同时表明链上通信、计算的高成本性,引入基于点对点网络的链下通信,从而降低协议成本,提高可用性。该文附录指出,所提协议可用于智能合约认证,即通过构建共享密钥,使得基于智能合约即可生成门限签名,从而提供授权服务。

文献[35]使用基于区块链智能合约的秘密分享技术实现具备“时间意识”的秘密管理方案。由于门限秘密分享和区块链都具有去中心化的特性,因此该方案中“时间”不会被某一个或几个操控而导致秘密提前泄露。区块链智能合约一方面提供了高效的计算能力和公共的数据存放平台,另一方面基于以太坊区块链的代币奖励诚实行为和惩罚恶意行为,从而提高了系统的安全性。

文献[36]使用区块链实现公共通告栏和公开验证者,基于DH交换加密和VSS协议实现分布式密钥生成ETHDKG协议。在ETHDKG中,份额密文信息、争议信息、密钥恢复信息均通过智能合约传递,并且这些信息的正确性要经过智能合约的验证。值得注意的是,ETHDKG采用的DH交换加密和VSS协议并没有构成非交互的PVSS协议,因为该方案中加密后的份额并不能由任何第三方来检验,

而需要等份额持有者解密后来判断。如果份额持有者解密后发现份额有误,可构造非交互的零知识证明来“抱怨”秘密分发者,而不泄露自己的份额值。

4 秘密分享与区块链存储的融合研究

4.1 公共通告栏

由于共识效率低下,对于分布式节点,获得具备一致性、可用性的数据是困难的,因此研究者提出公共通告栏^[37]的概念。公共通告栏具有活性和持久性的特点:活性是指任意恶意的用户无法阻止诚实的用户获取通告栏上的信息;持久性是指公共通告栏上的信息和数据不能被恶意篡改。许多基于秘密分享的多方协议^[27,38]和分布式应用^[39]基于公共通告栏进行实现。通过假设公共通告栏,分布式协议可以规避共识协议的讨论,并获得较低的通信复杂度。

文献[40]指出,在现实世界中,由于人为因素,可能出现计算不公开透明的问题,从而导致不公平现象。该文基于可信硬件和公共通告栏的技术实现安全的多方计算解决方案,其在可信硬件内执行秘密分享协议,实现了见证者解密。

在区块链技术落地之前,公共通告栏通常作为一种假设。随着近来区块链的持续发展,尤其是支持通用数据存储的区块链系统,如比特币、以太坊、IPFS(Interplanetary File System)等,使得公共通告栏技术得以实现。以比特币为例,该区块链系统即是基于点对点通信、多数节点诚实性、数字签名技术、随机预言机等假设实现公共通告栏。

4.2 区块链系统存储优化

区块链又称为分布式记账技术。分布式存储系统的显著特征是将所有的数据以副本的形式分布式地存储在不同的服务器中。因此,分布式存储是分布式记账的应有之意,也是共识的必要条件,更是区块链数据公开透明的基石。区块链中保存所有数据的节点称为全节点。比特币的发明者考虑到普通的个人电脑、手持设备计算能力和存储能力有限,为这些轻量级设备设计了可以使用的客户端,又称为轻节点,提出了简易支付验证(Simple Payment Verification, SPV)技术。由于区块链系统采用Merkle树的数据结构对交易进行管理,因此降低了交易正确性的验证成本并提升了查询速度,使得轻节点虽不能参与共识(即不能进行挖矿),但能够参与交易的发起和查询,以及交易准确性的验证。

随着越来越多区块链事务和交易的生成,区块链系统数据存储量与日俱增。为减少区块链数据的存储量,除SPV技术外,基于编码技术^[41-42]、分布式文件存储系统^[43]和多项式承诺技术^[44]等许多相关研究被提出。本节介绍采用秘密分享技术的门限特性来降低存储数据冗余度的研究。

文献[45]提出了分布式存储区块链(Distributed Storage Blockchain, DSB)技术。在DSB中,每个节点

仅存储所有数据的一部分,显著降低了区块链单节点的数据存储量。在该方案中,区块链的节点被划分为不同的区域,每一个区域有一组对应的公私钥对(PK,SK)。每个区域的区块数据均用PK加密保护,SK在区域内用秘密分享协议,由区域内的每个节点保管其中的一个份额。加密后的区块数据使用信息分发算法(Information Dispersal Algorithm, IDA)同样分布式地存储在区域内的节点中。在之后的工作中,文献[46]进一步提高了数据的完整性,同时分析了存储消耗和数据丢失率的关系,以及数据恢复消耗和安全性的关系。为解决DSB技术中当节点发起DoS攻击时会引起巨大网络通信开销的问题,文献[47]提出了局部秘密分享(Local Secret Sharing, LSS)的概念。LSS是一种层次化的秘密分享技术,图4体现了其中的层级关系。LSS包含一个全局秘密和多个局部子秘密,并且由部分子秘密能够恢复出全局秘密。LSS与HSS类似,但HSS强调的是全局秘密的分层管理,而LSS中局部秘密需要用于恢复子秘密。

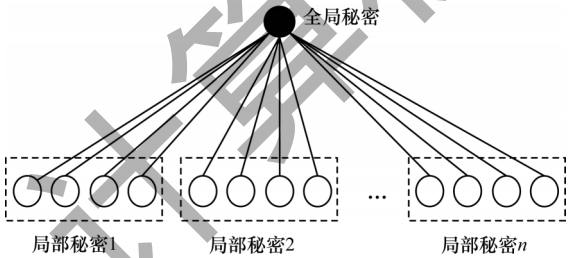


图4 LSS协议的层级关系

Fig.4 Hierarchical relationship in LSS protocol

在文献[45]提出的DSB协议中,全局秘密和局部子秘密采用不同的秘密分享多项式,存储开销较

大,而文献[47]提出的LSS协议仅需维护一套多项式,能够使得密钥存储开销减半,同时也优化了密钥恢复的网络通信开销。LSS是基于局部可修复码(Locally Recoverable Code, LRC)技术实现的。在编码理论中,通常通过添加修复码位来校正错误位。在全局秘密管理中,文献[47]使用Shamir秘密分享协议,将份额分发给所有的参与者节点。在局部子秘密的管理中,LSS协议对每一个区域利用LRC技术的编码多项式应对一个节点故障的情况。

虽然文献[46-47]均使用秘密分享技术降低了区块链存储冗余度,但是区块链中的区块可能由数千笔交易构成,从而导致区块也非常大,往往远大于一个大整数。当一个区块被切分成多个切片再进行秘密分享时,会导致需要存储大量的中间信息。鉴于此,文献[37]提出了使用多值秘密分享(Multi-Secret Sharing, MSS)的区块链存储优化方案。该方案先将原始的区块链切片,然后采用递归调用Shamir秘密分享协议的方式,重复利用秘密分享产生的中间结果,从而减少了所需的中间辅助变量,最终优化了存储效率。

表4对比了传统区块链^[3]以及文献[46-47]方案的单节点存储消耗、恢复区块时通信量和系统容错能力。假设区块占用空间大小不超过 η ,区块头占用空间大小不超过 q (η 和 q 均用整数表示), p 是访问其他子区域的额外开销, n 是总节点数, t 是分区的节点数或门限值。虽然通过文献[46-47]方案能够对区块链系统存储带来优化,但往往只适用于节点相对固定的区块链系统,即联盟链。

表4 存储开销、恢复区块时通信量和容错性的对比

Table 4 Comparison of storage cost, communication traffic in block recovery and fault tolerance

协议	是否区块加密	存储开销	通信量	容错性
Bitcoin ^[3]	否	$\text{lb } \eta + \text{lb } q$	$\text{lb } \eta + \text{lb } q$	$n-1$
文献[46]协议	是	$\text{lb}(\eta/t)+1+2\text{lb } q$	$\text{lb } \eta+2(t+1)\text{lb } q+p$	$n/t-1$
文献[47]协议	是	$\text{lb}(\eta/t)+\text{lb } q$	$\text{lb } \eta+t\text{lb } q$	$2n/t-1$

4.3 基于区块链存储和秘密分享的服务

将区块链的分布式容错存储和秘密分享技术相结合,能够提供许多信息安全所需的服务。这些服务对密码体制的功能、云计算、物联网等应用的效率和可用性均具有重要作用。

除了在区块链本身的存储解决方案上进行优化,区块链本身也是一个分布式的存储数据库。一些其他区块链项目,如StoreJ^[48],使用区块链来存放加密后的隐私数据信息,用于防止个人信息丢失,从而保护个人隐私。由于区块链的透明性,StoreJ中的

节点可能通过收集和整合数据对加密的隐私数据发起密文攻击,从而降低隐私数据的安全性。文献[49]提出一种使用秘密分享和区块链的点对点网络在线存储的方案,而不使用区块链直接存放加密数据。该方案使用秘密分享技术,通过将秘密拆分成份额,利用点对点网络分布式地储存在网络内存中,而利用区块链保存那些拥有份额的节点列表。由于点对点网络本身的异构性和变动性,区块链中的列表数据会通过共识算法使得每个人的隐私数据保留在网络中。在这样的点对点网络中,个人通过其ID和密

码授权获得个人私有数据的权限,通过区块链中的节点列表得知应该向点对点网络中的哪些节点获取数据。

IPFS 是另一个存储类的区块链项目,主要提供解决大文件大数据的存储方案。IPFS 同样仅提供透明的存储。为了保护数据的机密性和用户的隐私,文献[10]使用秘密分享技术、IPFS 存储和以太坊实现了一种透明传输、可确权、可访问控制的文件共享方案。在该方案中,文件所有者首先将文件上传至 IPFS 中,然后得到 IPFS 返回的文件哈希值。文件所有者用智能合约记录 IPFS 中对其文件存储的所有节点,并使用秘密分享技术将哈希值分散到上述节点中,最后将加密后的秘密份额上传至区块链中。

在云数据管理方面,文献[50]借助区块链去中心化存储和计算的特性,将云数据的访问控制能力部署在智能合约中,从而构建了无中心的云数据管理模式。同时,为了从云服务器上将加密云数据的密钥和云数据分离开来,该文使用了秘密分享技术分布式地管理密钥。但是,该方案需要加入一种新的区块链节点——“主节点”来进行存储秘密分享的密钥。在物联网领域,文献[51]为了解决智慧城市

中个人管理海量隐私数据的问题,提出通过区块链存储和管理云服务商的访问权限,并使用秘密分享技术分布式地管理用户个人隐私信息。

5 未来展望

中心化系统由于单点共识,因而具备高吞吐率和高响应率,而去中心化系统能够解决对等协作方之间的不信任问题并提高容错能力。在计算机硬件条件和网络环境均不断优化的背景下,中心化系统的性能和效率快速增长,而去中心化系统的吞吐率由于低效的共识却提升甚微。秘密分享协议通常是为了构建具有容错性或者去中心化的系统,秘密分享和区块链两者独立或关联的研究还有诸多可以推进的探索方向。一方面,随着秘密分享技术及其对应安全多方计算应用的介入,区块链有了新的探索方向,包括基于拜占庭容错协议的区块链、基于权益证明的区块链、区块链存储优化、基于区块链的安全多方计算等;另一方面,由于对区块链的理论支撑或应用场景的需要,秘密分享协议相关的技术有着更为细分的发展方向,包括 VSS、PVSS、PSS、APSS、VSSR、LSS、MSS 等。表 5 对比了秘密分享相关协议的特点和用途。

表 5 秘密分享相关协议对比
Table 5 Comparison of related secret sharing protocols

协议	含义	特点或用途
SS	秘密分享	构建安全多方计算的核心密码原语,常用于构建 VSS ^[5] 、PVSS ^[6] 等协议
VSS	份额可私有验证的秘密分享	份额持有者可验证分发者是否诚实,常用于构建 BFT ^[17,21] 、PVSS ^[6,27] 等协议
PVSS	份额可公开验证的秘密分享	任何人都可验证分发者是否诚实,常用于构建 DKG ^[9,36] 、Beacon ^[25-28] 等协议
PSS	支持份额更新的秘密分享	降低份额被泄露的风险,常用于构建 APSS ^[24] 等协议
APSS	异步环境下份额可更新的秘密分享	更安全、更贴合互联网环境下节点可变的拜占庭容错系统,包括公有区块链
VSSR	份额可恢复且可验证的秘密分享	可构建通信复杂度更优的拜占庭容错系统或具备无中心化第三方服务等
LSS	局部秘密分享	分层级的秘密管理等
MSS	可分发多值的秘密分享	公开可验证的多值秘密分享、位置信息隐私保护 ^[52] 、电子投票系统等

制约分布式或去中心化系统共识的重要原因在于协议的高复杂度,尤其在分布式节点数量快速增长的情况下。未来可从以下方面入手进行更深入的研究:

1) 在分布式场景下,为了达成共识,需要考量每个节点或所有节点需要执行的计算量,即计算复杂度。由于在分布式场景中,通常还考虑了可能存在未知的恶意节点或损坏节点,因此协议的设计还包括了必要的验证计算,验证所花费的计算量也属于计算复杂度。基于拜占庭容错或 PoS 的协议和共识算法通常会在每一轮共识中选取一个“领导”(leader)推进协议,leader 对各参与者传输值的计算

复杂度及其网络传输时延最终决定了平均的共识速度。此外,当传输值还需要进行隐私保护时,通常需结合 SS 协议,尤其是 PVSS 协议。此时,由于 PVSS 协议采用了 NIZK 证明,因此参与者节点还需对证明进行验证,从而可能增加计算复杂度。

2) 在分布式场景中为了达成共识,需要考量整个网络的通信量,即通信复杂度。网络通信内容既可以是正常的协议所需的数据,也可以是恶意节点为破坏信息系统而伪造的数据。在区块链系统中,数据和块通常是经过签名认证过的,从而避免了 DDoS 攻击。在基于拜占庭容错或 PoS 共识的系统中,通常每个参与者节点都需要发出各自的信息以

对最后的共识做出贡献,从而使得网络通信复杂度至少达到 $O(n^2)$,并且不诚实的节点可能故意偏离协议规定,从而引起较高的网络通信复杂度。上文讨论的公共通告栏能够在一定程度上降低协议的通信复杂度,但是高效构建公共通告栏也是一项值得继续探究的问题。

3)为了达成某种协议的共识,节点间需要进行足够的通信协商轮次。由于网络有延时性,因此低轮次的网络通信对于达成共识更具备现实价值。相对于VSS协议,PVSS协议数据可以采取公共通信信道并可以接受任何人的验证,因此,PVSS往往只需要一次性分发份额,而不需要参与解决份额相关的争议。在基于(P)VSS实现的DKG协议和Beacon协议中,通信轮次都是重要指标,而不同的DKG协议和Beacon协议的设计可以产生不同的区块链模型和共识算法。通过对比不同的拜占庭容错共识协议,可以看出通信轮次和网络通信量之间通常存在权衡和折中。

4)网络模型包括同步模型、半同步模型和异步模型,不同的通信模型假设会决定协议可能存在不同的漏洞和受到不同类型的攻击,因此,协议也需要有相对应的处理方式。同步模型是一种较强的假设,优点是协议设计者可以借助一些其他工具(如公共通告栏),缺点是可能受到一些由于攻击者利用网络时延差而发起的网络攻击。异步或者半同步通信模型能够更好地模拟真实的互联网环境,但通常对应的协议需要更高的网络通信复杂度或更多的通信轮次,甚至牺牲一部分活性或安全性。

5)可重配置性是指分布式系统中节点是否可以自由进出。比特币系统的工作量证明不需要依赖其他节点的信息和数据,可以由节点根据历史区块链数据独立完成,因此节点自由度高,可以自由进出。基于拜占庭容错或PoS共识的协议通常假设固定节点数量和一定比例之内的恶意节点数量,节点间需要通过协作确定最终的共识,恶意节点加入或诚实节点离开可能使得诚实和恶意节点比例失衡,最终使得系统为恶意节点所控制,并且节点的进出本身就需要达成共识,即何种节点可以进出,何时可以进出,因此,基于拜占庭容错或PoS共识的协议往往缺乏可重配置性。基于主动式秘密分享的协议致力于解决份额变化或参与节点变化,具有解决可重配置性问题的潜力。此外,Dfinity团队提出的公开可验证可重新分发的秘密分享协议(Public Verifiable Resharing Scheme,PVRS)^[53]也使解决可重配置性问题获得了突破性进展。因此,PVRS的研究也有待进

一步深入,同时PSS和PVRS的联系及区别也有待发掘。

6)容错能力是指分布式系统中可以容忍的损坏和恶意节点比例以及发掘恶意行为的能力。容错比例越高、发掘恶意行为能力越强说明容错能力越强。由于通常会假设恶意节点具有共谋性,因此为了避免恶意节点占据压倒性优势,需要假定诚实节点数多于恶意节点数,可推断出恶意节点比例通常小于 $1/2$ 。SS协议中分发者可以是恶意的,因此VSS被提出用于解决分发者的信任问题,提升容错能力。PVSS协议更是允许任何人都可以验证分发者的诚实性,使得分布式系统具备更好的公开性和透明性。

7)区块链存储优化,即基于区块链信息存储冗余度高的客观现实,在保证安全的情况下,降低区块链全网的存储能力。本文第4节介绍了研究人员在相关领域做出的贡献,然而这些研究成果还没有被应用到主流的区块链系统中。存储优化(单节点的存储量减少)可能影响节点校验区块的能力和用户访问区块链数据的便捷性。因此,如何设计兼顾存储优化和功能完整性的区块链,也是具有研究价值的课题。

8)区块链共识算法^[54]决定了区块链应用的公信力、吞吐率、扩容能力等,而优良的共识算法应着重考虑协议复杂度、可重配置性、容错能力、存储优化等指标。为了获得更优的区块链共识算法,应继续深入研究秘密分享相关协议。此外,通过使用秘密分享实现分片技术^[55],对节点进行分组管理也可以提升共识效率。

6 结束语

区块链是一种基于经济学和密码学的去中心化系统。区块链的透明计算和存储特性降低了信任成本,去中心化特点提升了容错能力。而秘密分享是构建分布式系统和去中心化协议的基础技术,融合应用秘密分享技术可使区块链得到进一步发展。本文从信息安全三要素角度,指出区块链系统和秘密分享技术存在高度契合,分别阐述区块链、秘密分享及安全多方计算等基础理论知识,并进一步介绍秘密分享技术与区块链共识层、合约层和存储层相结合的研究成果。在未来,许多基于秘密分享的多方协作协议均能通过区块链以较低成本实现。同样,秘密分享也能为区块链技术发展带来重要的探索方向——更多基于秘密分享的区块链共识、智能合约及存储的研究将被提出和实现。

参考文献

- [1] 张亮,刘百祥,张如意,等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1-12.
ZHANG L, LIU B X, ZHANG R Y, et al. Overview of blockchain technology[J]. Computer Engineering, 2019, 45(5): 1-12. (in Chinese)
- [2] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.
- [3] SATOSHI N. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2022-02-10]. <https://bitcoin.org/bitcoin.pdf>.
- [4] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.
- [5] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C]//Proceedings of the 28th Annual Symposium on Foundations of Computer Science. Washington D. C. , USA: IEEE Press, 1987: 427-438.
- [6] STADLER M. Publicly verifiable secret sharing [C]//Proceedings of EUROCRYPT'96. Berlin, Germany: 1996: 190-199.
- [7] LI J, WANG X M, HUANG Z G, et al. Multi-level multi-secret sharing scheme for decentralized E-voting in cloud computing[J]. Journal of Parallel and Distributed Computing, 2019, 130: 91-97.
- [8] HANKE, MOVAHEDI M, WILLIAMS D. DFINITY technology overview series, consensus system[EB/OL]. [2022-02-10]. <https://arxiv.org/abs/1805.04548>.
- [9] NAZ M, AL-ZAHRANI F A, KHALID R, et al. A secure data sharing platform using blockchain and interplanetary file system[J]. Sustainability, 2019, 11(24): 1-24.
- [10] ATTASENA V, DARMONT J, HARBI N. Secret sharing for cloud data security: a survey[J]. The VLDB Journal, 2017, 26(5): 657-681.
- [11] YAO A. Protocols for secure computations[C]//Proceedings of FOCS'82. Washington D. C. , USA: IEEE Press, 1982: 160-164.
- [12] 中国信通院. 数据流通关键技术白皮书[EB/OL]. [2022-02-10]. <https://www.docin.com/p-2107226644.html>. CAICT. White paper on key technologies of data circulation [EB/OL]. [2022-02-10]. <https://www.docin.com/p-2107226644.html>. (in Chinese)
- [13] ABRAHAM I, MALKHI D. The blockchain consensus layer and BFT[EB/OL]. [2022-02-10]. <http://eatcs.org/beatcs/index.php/beatcs/article/view/506/495>.
- [14] GRAMOLI V. From blockchain consensus back to Byzantine consensus[J]. Future Generation Computer Systems, 2020, 107: 760-769.
- [15] BERGER C, REISER H P. Scaling Byzantine consensus: a broad analysis[C]//Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. Washington D. C. , USA: IEEE Press, 2018: 13-18.
- [16] CACHIN C, ZANOLINI L. Asymmetric asynchronous Byzantine consensus[EB/OL]. [2022-02-10]. <https://arxiv.org/abs/2005.08795>.
- [17] DU M X, CHEN Q J, MA X F. MBFT: a new consensus algorithm for consortium blockchain[J]. IEEE Access, 2020, 8: 87665-87675.
- [18] BHAT A, SHRESTHA N, LUO Z T, et al. RandPiper: reconfiguration-friendly random Beacons with quadratic communication[C]//Proceedings of 2021 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, 2021: 3502-3524.
- [19] CASCUDO I, DAVID B, SHLOMOVITS O, et al. Mt. random: multi-tiered randomness Beacons[EB/OL]. [2022-02-10]. <https://eprint.iacr.org/2021/1096.pdf>.
- [20] ZHANG L, QIU F Y, HAO F, et al. 1-round distributed key generation with efficient reconstruction using decentralized CP-ABE[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 894-907.
- [21] BASU S, TOMESCU A, ABRAHAM I, et al. Efficient verifiable secret sharing with share recovery in BFT protocols[C]//Proceedings of 2019 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, 2019: 2387-2402.
- [22] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.
- [23] HERZBERG A, JARECKI S, KRAWCZYK H, et al. Proactive secret sharing or: how to cope with perpetual leakage [C]//Proceedings of CRYPTO'95. Berlin, Germany: Springer, 1995: 339-352.
- [24] ZHOU L D, SCHNEIDER F B, VAN RENESSE R. APSS: proactive secret sharing in asynchronous systems[J]. ACM Transactions on Information and System Security, 2005, 8(3): 259-286.
- [25] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//Proceedings of CRYPTO'17. Berlin, Germany: Springer, 2017: 357-388.
- [26] SCHINDLER P, JUDMAYER A, STIFTER N, et al. HydRand: efficient continuous distributed randomness[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C. , USA: IEEE Press, 2020: 73-89.
- [27] CASCUDO I, DAVID B. SCRAPE: scalable randomness attested by public entities[C]//Proceedings of International Conference on Applied Cryptography and Network Security. Berlin, Germany: Springer, 2017: 537-556.
- [28] SYTA E, JOVANOVIĆ P, KOGIAS E K, et al. Scalable Bias-resistant distributed randomness[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C. , USA: IEEE Press, 2017: 444-460.
- [29] ZHANG E, LI M, YIU S M, et al. Fair hierarchical secret sharing scheme based on smart contract[J]. Information Sciences, 2021, 546: 166-176.

- [30] TSO R, LIU Z Y, HSIAO J H. Distributed E-voting and E-bidding systems based on smart contract[J]. Electronics, 2019, 8(4): 422.
- [31] HSIAO J H, TSO R, CHEN C M, et al. Decentralized E-voting systems based on the blockchain technology[C]// Proceedings of CSA/CUTE 2017. Berlin, Germany: Springer, 2018: 305-309.
- [32] ZHU Y, SONG X X, YANG S, et al. Secure smart contract system built on SMPC over blockchain[C]// Proceedings of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data. Washington D. C., USA: IEEE Press, 2018: 1539-1544.
- [33] CYRAN M A. Blockchain as a foundation for sharing healthcare data [EB/OL]. [2022-02-10]. https://www.researchgate.net/publication/323973053_Blockchain_as_a_Foundation_for_Sharing_Healthcare_Data.
- [34] MARAM D K S, ZHANG F, WANG L, et al. CHURP: dynamic-committee proactive secret sharing[C]// Proceedings of ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2019: 2369-2386.
- [35] NING J, DANG H, HOU R, et al. Keepin time-release secrets through smart-contracts[EB/OL]. [2022-02-10]. <https://eprint.iacr.org/2018/718.pdf>.
- [36] SCHINDLER P, JUDMAYER A, STIFTER N, et al. ETHDKG: distributed key generation with Ethereum smart contracts [EB/OL]. [2022-02-10]. <https://eprint.iacr.org/2019/985>.
- [37] BAUM C, DAMGÅRD I, ORLANDI C. Publicly auditable secure multi-party computation[C]// Proceedings of International Conference on Security and Cryptography for Networks. Berlin, Germany: Springer, 2014: 175-196.
- [38] YUAN J T, LI L X. A fully dynamic secret sharing scheme[J]. Information Sciences, 2019, 496: 42-52.
- [39] LIU Y N, ZHAO Q Y. E-voting scheme using secret sharing and k-anonymity[J]. World Wide Web, 2019, 22(4): 1657-1667.
- [40] ADIDA B, MARNEFFE O, PEREIRA O, et al. Election a university president using open-audit voting[C]// Proceedings of 2009 Conference on Electronic Voting Technology/ Workshop on Trustworthy Elections. New York, USA: ACM Press, 2009: 1-10.
- [41] DAI M J, ZHANG S L, WANG H, et al. A low storage room requirement framework for distributed ledger in blockchain[J]. IEEE Access, 2018, 6: 22970-22975.
- [42] WU H H, ASHIKHMIN A, WANG X D, et al. Distributed error correction coding scheme for low storage blockchain systems[J]. IEEE Internet of Things Journal, 2020, 7(8): 7054-7071.
- [43] ZHENG Q H, LI Y, CHEN P, et al. An innovative IPFS-based storage model for blockchain[C]// Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence. Washington D. C., USA: IEEE Press, 2018: 704-708.
- [44] TOMESCU A, ABRAHAM I, BUTERIN V, et al. Aggregatable subvector commitments for stateless cryptocurrencies[EB/OL]. [2022-02-10]. <https://eprint.iacr.org/2020/527.pdf>.
- [45] RAMAN R K, VARSHNEY L R. Dynamic distributed storage for blockchains[C]// Proceedings of IEEE International Symposium on Information Theory. Washington D. C., USA: IEEE Press, 2018: 2619-2623.
- [46] RAMAN R K, VARSHNEY L R. Distributed storage meets secret sharing on the blockchain[C]// Proceedings of Information Theory and Applications Workshop. Washington D. C., USA: IEEE Press, 2018: 1-6.
- [47] KIM Y, RAMAN R K, KIM Y S, et al. Efficient local secret sharing for distributed blockchain systems[J]. IEEE Communications Letters, 2019, 23(2): 282-285.
- [48] StoreJ[EB/OL]. [2022-02-10]. <https://www.storj.io/>.
- [49] FUKUMITSU M, HASEGAWA S, IWAZAKI J Y, et al. A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain[C]// Proceedings of the 31st International Conference on Advanced Information Networking and Applications. Washington D. C., USA: IEEE Press, 2017: 803-810.
- [50] SOHRABI N, YI X, TARI Z, et al. BACC: blockchain-based access control for cloud data[C]// Proceedings of the Australasian Computer Science Week Multiconference. New York, USA: ACM Press, 2020: 1-10.
- [51] CHA J, SINGH S K, KIM T W, et al. Blockchain-empowered cloud architecture based on secret sharing for smart city[J]. Journal of Information Security and Applications, 2021(57): 2214-2126.
- [52] WERNKE M, DÜRR F, ROTHERMEL K. PShare: position sharing for location privacy based on multi-secret sharing[C]// Proceedings of IEEE International Conference on Pervasive Computing and Communications. Washington D. C., USA: IEEE Press, 2012: 153-161.
- [53] GROTH J. Non-interactive distributed key generation and key resharing[EB/OL]. [2022-02-10]. <https://www.docin.com/p-1650395684.html>.
- [54] 薛立德. 区块链共识算法及其应用研究[D]. 合肥: 中国科学技术大学, 2021.
- XUE L D. Research on blockchain consensus algorithm and its application [D]. Hefei: University of Science and Technology of China, 2021. (in Chinese)
- [55] 黄华威, 孔伟, 彭肖文, 等. 区块链分片技术综述[J]. 计算机工程, 2022, 48(6): 1-10.
- HUANG H W, KONG W, PENG X W, et al. Survey on blockchain sharding technology[J]. Computer Engineering, 2022, 48(6): 1-10. (in Chinese)