










































数据共享 文献调研

| Aa Name | Topic | Tool | Abstract | Where | Year |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|-----------------|
|  Blockchain-Based Privacy-Preserving Positioning Data Sharing for IoT-Enabled Maritime Transportation Systems | <div>位置共享</div> <div>船舶场景</div> <div>隐私保护</div> | <div>Merkle Commit</div> <div>ZK</div> | 解决利用区块链进行船舶位置共享时的隐私问题（身份、余额、请求关联信息） 四步： 1. A发布位置信息，通过Merkle Commit隐藏身份与数据之间的关联 2. B支付，通过ZK隐藏账户信息与具体金额 3. B获取，通过ZK证明B已经正确支付 4. A收款，通过ZK账户信息与转账记录 | <div>IEEE Transactions on Intelligent Transportation Systems - CCF B</div> | <div>2023</div> |
|  Privacy-preserving and efficient data sharing for blockchain-based intelligent transportation systems | <div>数据检索优化</div> | <div>布隆过滤器</div> | 解决利用区块链进行车辆数据共享时的「多关键字」搜索的性能问题 主要利用布隆过滤器选择「多关键字中的低频关键字」，过滤掉大多数结果，再匹配其他关键字。 没有进行其他安全考量，比如可搜索加密等 | <div>Information Sciences - CCF B</div> | <div>2023</div> |
|  EBSS: A secure blockchain-based sharing scheme for real estate financial credentials | <div>金融凭证</div> | <div>承诺方案</div> <div>群签名</div> | 提出了一个基于区块链的金融凭证安全共享方案，提供机密性、完整性、匿名认证，访问控制，跟踪和审计等 结合分层加密和访问控制设计了证书的机密性存储和不同的权限管理 采用了一个组合的基于群签名和基于承诺的方案来实现匿名认证 | <div>World Wide Web Journal - CCF B</div> | <div>2023</div> |
|  Secure and Distributed IoT Data Storage in Clouds Based on Secret Sharing and Collaborative Blockchain | <div>共识优化</div> <div>数据检索优化</div> <div>物联网场景</div> <div>秘密共享</div> | | 解决秘密共享中数据组织、存储和检索问题 数据组织：设计了一种秘密共享算法，消息份额长度较小 数据存储：设计了一种新的共识协议，将份额哈希和节点位置信息嵌入区块中 数据检索：节点存储数据利用平衡索引结构，并使用深度优先算法，提高检索效率 | <div>IEEE/ACM Transactions on Networking - CCF A</div> | <div>2023</div> |
|  Blockchain-Based Fair and Fine-Grained Data Trading With Privacy Preservation | <div>数据交易</div> <div>隐私保护</div> | <div>属性基匿名凭证</div> <div>零知识证明</div> | 提出了第一个基于区块链的公平和细粒度数据交易方案 利用基于属性的匿名凭证和零知识证明来设计数据交易过程，确保敏感数据的隐私性 设计制定了一个基于区块链的公平和细粒度数据交易的安全模型以评估方案性能 | <div>IEEE Transactions on Computers - CCF A</div> | <div>2023</div> |
|  Blockchain-based decentralized data dissemination scheme in smart transportation | <div>共识优化</div> <div>车联网场景</div> | <div>PoS</div> <div>群签名</div> | 基于区块链实现了一套车联网的数据传播方案 利用PoS（Ouroboros变体）共识算法为基础，可连接群签名技术保护隐私。 | <div>Journal of Systems Architecture - CCF B</div> | <div>2023</div> |
|  Blockchain Empowered Secure Video Sharing With Access Control for Vehicular Edge Computing | <div>访问控制</div> <div>边缘计算</div> | <div>属性基加密</div> | 设计了一个车联网环境下的视频数据安全、隐私共享方案 提出了一个VEC(车辆边缘计算)环境下的发布订阅系统解决数据分享 设计了一个结合动态静态属性的CP-ABE(Ciphertext Policy-ABE)方案（ABE-SD）实现细颗粒度访问 利用区块链来保存ABE-SD的组合策略树，并开发智能合约，将发布和订阅事件自动记录到区块链中，确保视频可追溯性和防篡改性。 | <div>IEEE Transactions on Intelligent Transportation Systems - CCF B</div> | <div>2023</div> |
|  Secure Crowdsensed Data Trading Based on Blockchain | <div>数据众包交易</div> | <div>可靠性评估</div> <div>同态加密</div> | 提出了一个基于区块链的Crowdsensed Data Trading（BCDT）系统 设计了一个智能合约BCDToken取代数据交易经纪人，以保证数据交易的可靠性。 实现了一个安全的真相发现和可靠性评级（STDTR）机制，配合同态加密，激励卖家上传真实的数据和消费者进行可靠评分，而不会泄露任何隐私的数据。 | <div>IEEE Transaction on Mobile Computing - CCF A</div> | <div>2023</div> |
|  ContractBox: Realizing accountable data sharing on the edge using a smallscale blockchain | <div>可信执行</div> <div>边缘计算</div> | | 解决区块链节点在边缘环境下数据和代码的机密性完整性问题。 利用可信计算，在一个物理节点中设立多个Enclave，Enclave中部署排序服务或使用Wasm沙盒技术部署智能合约，实现数据和代码的可信执行。 相比于Fabric，两个节点即可完成区块链功能，一个排序，一个包含多个智能合约 | <div>Computer Networks - CCF B</div> | <div>2023</div> |

| Aa Name | ≡ Topic | ≡ Tool | ≡ Abstract | 📍 Where | 📅 Year |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|-----------------|
|  TRUCON: Blockchain-Based Trusted Data Sharing With Congestion Control in Internet of Vehicles | <div>信任评估</div> <div>数据检索优化</div> <div>路由优化</div> <div>车联网场景</div> | <div>Kademlia</div> <div>布谷鸟过滤器</div> | 车辆与车辆之间需要传输大量信息（是否红灯等），本文解决信息路由、去重、信任评估问题。去重：利用布谷鸟过滤器防止冗余数据共享 路由：利用Kademlia算法与车辆之间的距离，实现信道的拥塞控制，限制转发的数量 信任评估：利用智能合约实现 | <div>IEEE Transactions on Intelligent Transportation Systems - CCF B</div> | <div>2023</div> |
|  Teegraph: A blockchain consensus algorithm based on TEE and DAG for data sharing in IoT | <div>共识优化</div> | | 基于TEE和TAG设计了一个共识算法，拜占庭错误容忍下限从3f+1减少到2f+1 | <div>Journal of Systems Architecture - CCF B</div> | <div>2022</div> |
|  LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue | <div>共识优化</div> <div>强化学习</div> | | | <div>IEEE Transactions on Dependable and Secure Computing - CCF A</div> | <div>2022</div> |
|  Blockchain-based data sharing with key update for future networks | <div>可更新加密</div> | <div>LESS</div> <div>ZK</div> | 可更新加密UE：数据所有者可以向区块链发送令牌，在链上进行新密钥生成与对应密文更新 设计了一种区块链的数据共享方案，该方案能够支持密钥和密文的链上更新（数据所有者无需链下生成），基于树的方案性能较高，基于DBDHE假设证明了前向与后向安全 | <div>IEEE Journal on Selected Areas in Communications - CCF A</div> | <div>2022</div> |
|  CrowdMed-II: A blockchain-based framework for efficient consent management in health data sharing | <div>医疗场景</div> <div>智能合约</div> | | 这篇文章比较水，讲的是医疗场景下智能合约整体架构的问题。例如，智能合约应该分多少类，一类智能合约应该包含哪些字段，实体与合约之间的调用关系等 还有一个基于组的访问控制，就是把RBAC更加简化了。 | <div>World Wide Web - CCF B</div> | <div>2022</div> |
|  A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things | <div>信任评估</div> <div>物联网场景</div> <div>零信任安全</div> | <div>共识算法</div> | 本文提出了一种基于区块链的去中心化信息共享协议，能够在零信任环境中运行。 方案可以通过智能合约检测和过滤构造的信息来保证公平性。 设计了一种内置共识和惩罚功能的投票机制。 | <div>IEEE Transactions on Computers - CCF A</div> | <div>2022</div> |
|  Comments on "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud" | <div>未授权访问</div> <div>机密性攻击</div> | <div>基于属性的签密</div> | 对Eltayieb et al.提出的一种基于区块链的基于属性的签密方案，以保护云中的数据共享。(doi: https://doi.org/10.1016/j.sysarc.2019.101653) 提出了质疑，指出该方案机密性可被打破，并且任何数据使用者都可以对外包数据进行未经授权的访问控制。 | <div>Journal of Systems Architecture - CCF B</div> | <div>2022</div> |
|  Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain | <div>信任评估</div> <div>共识优化</div> <div>医疗场景</div> | <div>PoS</div> | 本文在车联网环境下，目标是不利用RSU（路边单元）实现数据隐私共享 共识算法改进：设计了一种基于信任评分设计了一种DPoS算法 共享方案改进：基于共识算法，设计一套不依赖RSU（依赖5G基站）的共享流程 | <div>IEEE Transactions on Intelligent Transportation Systems - CCF B</div> | <div>2022</div> |
|  Privacy preserving in blockchain-based government data sharing: A service-on-chain (SOC) approach | | | 这篇文章也比较水，关注在政府数据共享领域。设计了一个基于区块链的数据共享过程，还弄了个数据共享中业务逻辑形式化描述 | <div>Information Processing & Management - CCF B</div> | <div>2022</div> |
|  TraceChain: A blockchain-based scheme to protect data confidentiality. | <div>云环境</div> | <div>密文策略属性基加密</div> | 基于密文策略属性加密CP-ABE，提出了一种加强版的E-CP-ABE，与CP-ABE相比，E-CP-ABE能够有效的降低算法的计算复杂度。本文提出的TraceChain与之前的仅支持用户追踪数据源的方案不同，还能够为数据所有者提供追踪数据的功能。 | <div>Software: Practice and Experience - CCF B</div> | <div>2022</div> |

| Aa Name | ≡ Topic | ≡ Tool | ≡ Abstract | 📍 Where | 📅 Year |
|-------------------------------------------------------------------------------------------------------------------|------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|--------|
| and traceability. | | | | | |
| Blockchain Based Non-repudiable IoT Data Trading: Simpler, Faster, and Cheaper | 激励机制 物联网场景 | | 本文提出了一个基于区块链的不可否认的IoT数据交易机制，通过区块链的智能合约以及分布式共识机制，并设计更加简单高效的证明验证机制，使得仲裁更加高效。同时设计激励机制使得仲裁次数降低。该机制支持近乎自动、实时、不可抵赖的数据交易。 | INFOCOM - CCF A | 2022 |
| Go-Sharing: A Blockchain-Based Privacy-Preserving Framework for Cross-Social Network Photo | 社交平台场景 访问控制 隐私保护 | 两阶段可分离深度学习TSDL 多所有者传播树 | 本文针对跨社交平台照片传播过程中导致的隐私泄露、归属权模糊的问题，设计了一个多所有者传播树来保证照片所有者在跨社交平台共享期间的有效管理，提出了一种动态隐私策略生成算法来解决多共享者之间的隐私冲突问题，并引入TSDL和随机噪声黑盒来识别照片所有权。 | IEEE Transactions on Dependable and Secure Computing - CCF A | 2022 |
| Blockchain-empowered efficient data sharing in internet of things settings | 扩容机制 路由优化 | MPR多路径路由 同态加密 支付通道 | 应用支付通道网络进行扩容 利用同态加密进行交易拆分 利用MPR进行路由 | IEEE Journal on Selected Areas in Communications - CCF A | 2022 |
| Trustworthy and Efficient Crowdsensed Data Trading on Sharding Blockchain | 数据众包交易 | 分层分片 | 本文关注数据众包感知交易，将众包交易系统与智能区块链结合（CDT-B），使用一个智能合约来作为可信第三方。在CDToken中设计了DUP机制、GTD算法、支付机制等机制，完成数据上传、数据预处理，数据真实性评估，支付等工作；由于区块链的效率较低，本文提出了LSMD，一种新型的分层分片区块链。通过节点的历史信息，根据节点的隶属度为不同的分片分配节点。 | IEEE Journal on Selected Areas in Communications - CCF A | 2022 |
| A high-concurrency blockchain model for large-scale medical cohort data storage and sharing | 共识优化 医疗场景 智能合约 | | 本文设计了一个MMA模型，该模型将用户(患者等)与医院资产(病例)分开，分为两类账户，实现资产操作逻辑与存储分离。第二是关注医疗信息在区块链上的高并发问题，设计了一种共识算法 | IEEE International Conference on Bioinformatics and Biomedicine - CCF B | 2022 |
| Blockchain-based Fair and Decentralized Data Trading Model | 数据交易 | 仲裁机制 | 提出了一个基于区块链的公平、去中心化的数据交易模型；其中提出了一个新的去中心化仲裁机制来解决数据交易中数据正确性的争议 | The Computer Journal CCF - B | 2022 |
| Sandbox Computing: A Data Privacy Trusted Sharing Paradigm Via Blockchain and Federated Learning | 联邦学习 | | | IEEE Transactions on Computers - CCF A | 2022 |
| A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks | SDN 医疗场景 | | 将 SDN 与基于物联网的医疗保健系统相结合可以显着改善医疗保健管理服务 WBAN无线体域网 通常是小型或微型无线网络，由附于身体或植入体内的微型智能设备组成。设备可提供持续健康监测和实时反馈信息，并长期记录和分析 本文将软件定义的WBAN与区块链结合，设计了一套数据共享架构。通过智能合约设计了访问控制机制（简单的ACL） | Computer Networks - CCF B | 2022 |
| Achieving privacy-preserving and verifiable data sharing in vehicular fog with blockchain | 数据聚合 车联网场景 隐私保护 | IBS 同态加密 | 在车联网背景下，路边单元RSU需要获取车辆的信息进一步处理。如何获取车辆的信息和保护车辆信息的隐私是本文重点。设计了一个基于车联网的数据共享框架。设计了一个基于同态加密和IBSC的隐私保护方案，实现RSU可以隐私聚合聚合车辆信息（如位置信息平均值），并且聚合后的结果是可验证的。 | IEEE Transactions on Intelligent Transportation Systems - CCF B | 2022 |
| ProvNet: Networked bi-directional blockchain for data sharing with verifiable provenance | 版权保护 | MinHash 变色龙哈希 可编辑区块 | 本文关注在区块链上的版权保护，例如未经授权的信息不允许再次分发，学术剽窃等。版权确认：利用MinHash计算数据集之间的Jaccard相似性，若不相似，则为数据所有者 数据共享：共享是一对多的，以有向图存储较好，设计了一种网状区块链 前向跟踪：先前共享的数据无效时，需要进行前向溯源，利用变色龙哈希和可编辑块 | Journal of Parallel and Distributed Computing - CCF B | 2022 |

| Aa Name | ≡ Topic | ≡ Tool | ≡ Abstract | ⌵ Where | ⌵ Year |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|--------|
|  Blockchain for health IoT: A privacy-preserving data sharing system | 共识优化 医疗场景 数据检索优化 隐私保护 | 可截取签名 | 在共享电子医疗病例场景下，设计了一种具有隐私保护的区块链系统。隐私保护：利用可截取签名生成一个内容提取访问结构，进行细粒度授权与保护隐私 检索优化：设计了一个智能合约，存储了电子病历id与区块id之间的关联 共识优化：认为电子病历共享应该处于拜占庭环境，改进Raft算法，设计了一种具有稳定机制的拜占庭容错算法（稳定度越高，成为主节点几率越高） | Software: Practice and Experience - CCF B | 2022 |
|  SloVChain: Time-Lock Contract Based Privacy-Preserving Data Sharing in SloV | 匿名共享 车联网场景 隐私保护 | 支付通道 时间锁 | 本文提出了一种基于支付通道的链下的匿名数据共享方案，利用时间锁合约来保证匿名性并设计了一个匿名惩罚程序来对恶意车辆进行处罚 | IEEE Transactions on Intelligent Transportation Systems - CCF B | 2022 |
|  A blockchain-based fine-grained data sharing scheme for e-healthcare system | 医疗场景 隐私保护 | 代理重加密 | 条件代理重加密 通过将条件与重加密密钥相关联来实现细粒度控制，但是条件是明文可能会泄露隐私 本文将条件嵌入到代理重加密密钥中，设计了基于区块链的电子病历共享方案。 | Journal of Systems Architecture - CCF B | 2022 |
|  Blockchain-based data sharing system for sensing-as-a-service in smart cities | | | 这篇文章感觉比较水，场景可能比较新（传感即服务），看了abstract、intro、conclusion，一直强调用了Σ 协议、Paillier 和 AES做了个系统，没说具体的东西，正文不想看了 | ACM Transactions on Internet Technology - CCF B | 2022 |
|  MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain (CCF A) | 医疗场景 数据检索优化 隐私保护 | 可搜索加密 属性基加密 | 解决数据「授权与搜索」时的隐私、效率问题 架构：链上存索引，链下存数据 数据加密：链下恒长ABE 数据搜索：链上布尔搜索 | IEEE Transactions on Services Computing - CCF A | 2021 |
|  A secure and efficient authentication and data sharing scheme for Internet ofThings based on blockchain | 物联网场景 | IBS | 本文主要是提出了一种基于身份签名的身份认证方案，然后设计了一个基于区块链的共享流程。创新点在于解决了前人工作中的的安全漏洞，提升了一点性能，主要在于密码学技巧 | Journal of Systems Architecture - CCF B | 2021 |
|  Cross-domain secure data sharing using blockchain for industrial IoT | 物联网场景 | IBS | 设计了一个物联网中数据跨域共享的方案 利用IBS和椭圆曲线进行访问控制和加密 利用多层签名，网关作为区块链与用户之间的中间件，对签名进行检查，增强数据完整性 | Journal of Parallel and Distributed Computing - CCF B | 2021 |
|  A blockchain-based trading system for big data | 数据交易 数据检索优化 智能合约 | 代理重加密 | 设计了一种双链和侧链组合的架构，记录数据摘要和评估信息，以便高效检索和验证。设计了智能合约来完成数据匹配和价格协商过程。使用代理重加密来对数据的传输过程进行隐私保护。 | Computer Networks - CCF B | 2021 |
|  A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing | 访问控制 跨域 | ABE | 本文基于多属性CP-ABE技术（多个域可以为用户分配属性），设计了一个基于区块链访问控制方案，属性可以进行跨域管理，解决只有单个属性权威时的单点故障问题。 | Journal of Systems Architecture - CCF B | 2021 |
|  A secure and trustworthy medical record sharing scheme based on searchable encryption and blockchain | 医疗场景 数据检索优化 访问控制 | 可搜索加密 | 提出了一种基于可搜索加密的数据共享方案。利用可搜索加密来保护索引和查询内容的隐私，并将索引存在链上，数据存在本地数据库中。提出了一种访问控制方案，保证数据更新满足前向安全要求。该方案还支持同时检索和细粒度检索多个医疗机构的数据，更符合实际应用。 | Computer Networks - CCF B | 2021 |
|  SPChain: Blockchain-based medical data | 医疗场景 数据检索优化 隐私保护 | 代理重加密 可靠性评估 变色龙哈希 | 利用变色龙哈希设计了新的块结构和链结构，从而达到优化数据检索的目的。使用代理重加密来保护存在医疗机构本地数据库中的病历，以达到隐私保护的的目的。 | Information Processing and Management - CCF B | 2021 |

| Aa Name | ≡ Topic | ≡ Tool | ≡ Abstract | 📍 Where | 📅 Year |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|----------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|--------|
| sharing and privacy-preserving eHealth system | | | | | |
|  Blockchain-based trusted data sharing among trusted stakeholders in IoT | SDN 物联网场景 | 共识算法 | 针对效率问题以及可信第三方存在的隐私和维护成本问题，本文提出了一种安全轻量级的三重信任架构（SLTA），包括一种新的软件定义区块链结构模型，一种更加轻量高效的共识算法（轻量级拜占庭容错算法）以及一种低开销的存储模型。 | Software: Practice and Experience - CCF B | 2021 |
|  A blockchain-based scheme for privacy-preserving and secure sharing of medical data | 医疗场景 隐私保护 | ZK 代理重加密 | 利用零知识证明来在不泄露隐私的情况下证明该数据满足医疗机构的需求。利用代理重加密保证多实体间数据共享的隐私问题。 | Computers & Security - CCF B | 2020 |
|  PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities | 智慧城市 物联网场景 | | 提出一个区块链数据共享框架，通过划分区块链来保护数据隐私网络进入各种通道，其中每个通道都包含有限数量的授权组织，并处理特定类型的数据。并且提供了一种名为PrivyCoin的数字代币形式的奖励系统，供用户与利益相关者/第三方共享数据。 | Computers & Security - CCF B | 2020 |
|  Blockchain-Based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds | 云环境 激励机制 | | 利用Shapley值设计了一种动态且公平的多云数据共享激励机制，开发了三种复杂的收入分配模型，并考虑矿工的参与协作。 | IEEE Journal on Selected Areas in Communications - CCF A | 2020 |
|  A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud | 云环境 访问控制 | 基于属性的签密 | 本文将属性基签名加密（ABSC）引入到区块链中，以在云环境中保证安全的数据共享。 | Journal of Systems Architecture - CCF B | 2020 |
|  SDTE: A Secure Blockchain-Based Data Trading Ecosystem | 数据交易 智能合约 | 可信计算 | 本文将数据处理即服务替换传统数据交易平台，提出一个提供数据处理分析的生态系统。使用intel SGX可行计算硬件构建可信执行环境，并通过以太坊智能合约处理共享的数据，以提供数据处理分析服务平台。 | IEEE Transactions on Information Forensics and Security - CCF A | 2019 |
|  Blockchain-based platforms for genomic data sharing: a decentralized approach in response to the governance problems? | 医疗场景 | | 本文发表在美国医学信息学协会杂志上，主要探讨医学邻域基因组数据共享所需要解决的问题以及相关思路，在技术邻域没有深入。 | Journal of the American Medical Informatics Association - CCF B | 2019 |
|  Truthful Crowdsensed Data Trading Based on Reverse Auction and Blockchain | 数据交易 智能合约 | | 提出了一种基于反向拍卖和区块链的众感数据交易系统，设计了基于逆向拍卖的智能合约来代替第三方，并利用对称和非对称加密对数据的传输过程进行隐私保护。 | Database Systems for Advanced Applications - CCF B | 2019 |
|  SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR | 医疗场景 | | 本文提出了一个共享框架SHAREChain，其以区块链存储元数据，并以注册表的形式进行数据的访问控制，由于偏向医疗期刊，在技术邻域没有深入。 | IEEE International Conference on Bioinformatics and Biomedicine - CCF B | 2019 |