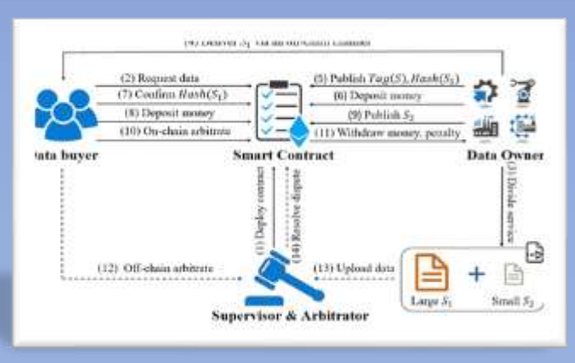
Emnets
2023-2024年终总结会

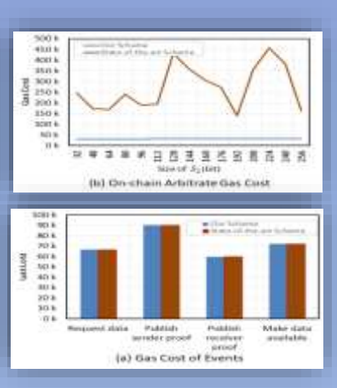
区块链组-王子平 @Emnets, ZJU

Paper Reading & Thinking

[INFOCOM'22] Blockchain Based Non-repudiable IoT Data Trading: Simpler, Faster, and Cheaper

随着物联网快速发展，据统计，截至2021年，已有285亿物联网设备，在2021年产生了875ZB的数据，至2030年，物联网设备上产生的数据的市场价值预估为3.9万亿，为了提取这些分布式数据的价值，在物联网设备间进行数据交易成为必要。此前存在两种传统的交易方法，第一种是基于存在可信第三方的假设，第二种是基于概率的方法，随着区块链技术的传播，随后出现了基于区块链的方法，我们提出了一种新的基于区块链的数据交易模式。
本文提出的方法在交易双方的公平性与解决纠纷的成本上相比此前的方法有了显著提升。

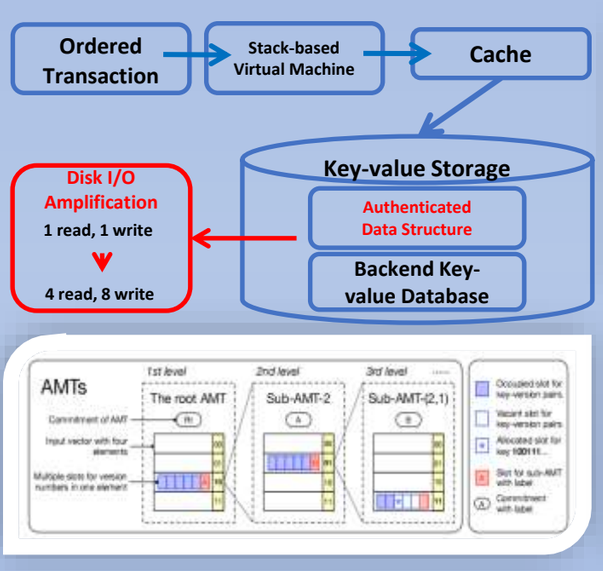


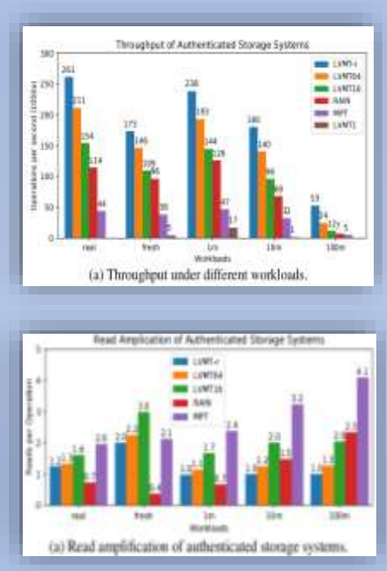


思考：在进行链下仲裁时，数据拥有者必须付出暴露数据的代价，或许可以引入零知识证明技术解决该问题以保证数据拥有着的数据隐私。

[OSDI'23] : An Efficient Authenticated Storage for Blockchain

从区块链性能的发展历程看，最初的比特币和以太坊只能达到低于每秒30条交易的吞吐量，而用于转账交易的Visa可以做到每秒处理20000条交易。其主要的瓶颈在于账本达成共识阶段的时间开销，近年来通过共识协议上的创新，区块链已经可以达到与visa同一量级的吞吐量，为进一步提高吞吐量，目前的瓶颈在于执行交易时在存储层的读写操作，交易执行时间中的80%都消耗在了存储层。
本文基于AMT提出了一种新的ADS（Authenticated Data Structure）以替换区块链系统中通常使用的Merkle Tree、MPT等结构，以此来减少存储交易时对于磁盘的读写次数。





思考：本文提出的方法借助于已有的ADS结构就，通过对其进行改造以适配于区块链系统，得以优化存储开销，但是在提供验证功能上该方法仍然存在额外存储开销。但这种通过已有结构的变体运用于不同场景以产生奇妙反应的方法提供了一种可借鉴创新方式。

Learning & Doing

学习项目一：分布式存储系统IPFS

IPFS，全称 InterPlanetary File System， 译为星际文件存储系统，是一个无需中央服务器管理数据的开放系统。该系统包含以下几个主要模块：Multiformats 模块用于加密和描述数据，libp2p 模块时系统数据传输的核心，IPLD 模块使用Merkle DAG结构来定义和组织数据。其设计目标旨在创建持久且分布式存储和共享文件的网络传输协议。

学习目的：为了搭建一个提供数据存储服务的平台，通过在多节点上部署IPFS系统组建成一个私有的IPFS网络，以提供数据存储与数据检索功能。在IPFS私有网络的基础上，可以进一步搭建区块链网络并通过实现智能合约来实现各类应用。将物联网设备接入存储网络与区块链网络，可以实现物联网数据的安全存储与数据交易等功能。其与区块链系统的结合旨在降低区块链系统的存储开销

学习项目二：区块链Hyperledger Fabric

Hyperledger Fabric 是来自 Linux Foundation 的开源项目，这是一个模块化区块链框架，也是企业区块链平台实际采用的标准。作为开发企业级应用程序和行业解决方案的基础，开放式模块化架构使用即插即用组件来满足各种用例的要求。
Hyperledger Fabric作为学术界认可度比较高的联盟链，非常适合作为搭建区块链应用的基础区块链平台。

学习目的：Fabric作为联盟链属于 Permissioned Chain，其在设计上与公链(Permissionless)存在差别，在学习过程中先对区块链的系统结构及其设计目的进行学习与分析，在有了一定的认知后，基于fabric的测试网络学习智能合约的编写，并通过剖析 sdk 源代码以开发区块链客户端实现应用。

TimeChain

TImeChain是我目前参与的主要工作，该工作目标为实现物联网时序数据的高效存储并基于区块链提供数据安全性与数据可靠性。我在其中负责实验部分，基于Hyperledger Fabric测试网络实现相关应用功能，并对设计结构的性能指标进行测试。

经验总结

在该学年的学习过程中，我从对区块链技术的一无所知出发，通过学习区块链课程、阅读区块链论文、了解区块链项目等方式，对区块链应用及其底层技术都有了一些初步的认知。同时通过接触区块链开源项目，对于如何认知大型项目有了一定的经验，也提高了阅读开源项目代码的能力，并在此过程中深入的到区块链系统的具体实现中，加深了我对目前先进区块链系统架构的理解。在实际部署 IPFS 私有网络与区块链网络的过程中，我在学习新的开发工具的同时也提高了解决问题的能力。

年终致谢

本学年是我进入实验室的第一学年，非常荣幸能够加入Emnets这个大家庭。在每周的组会上，听着师兄师姐的汇报与董老师高老师的教诲，我对于科研应该做什么、应该怎么做渐渐清晰、逐渐揭开了它的神秘面纱。在区块链组中，我往往难以完成既定的任务，非常感谢吕博和滕师姐的耐心指导与关怀以及工作能力上的包容。期待明年的科研生活能够取得进步 ！

EmNets Group