山东大学计算机科学与技术学院

School of Computer Science and Technology, Shandong University

区块链技术与零信任计算

International Workshop on Edge Intelligence and Future Network, May 27, 2022, Hong Kong SAR, China

成 秀 珍

May 27, 2022

目 录
Content

学无止境

气有浩然

山东大学
SHANDONG UNIVERSITY

学无止境

气有浩然

Part 01

应用需求：零信任计算

1. 信任与零信任
2. 虚拟货币的发展
3. Web的发展
4. 计算范式的发展
5. 总结

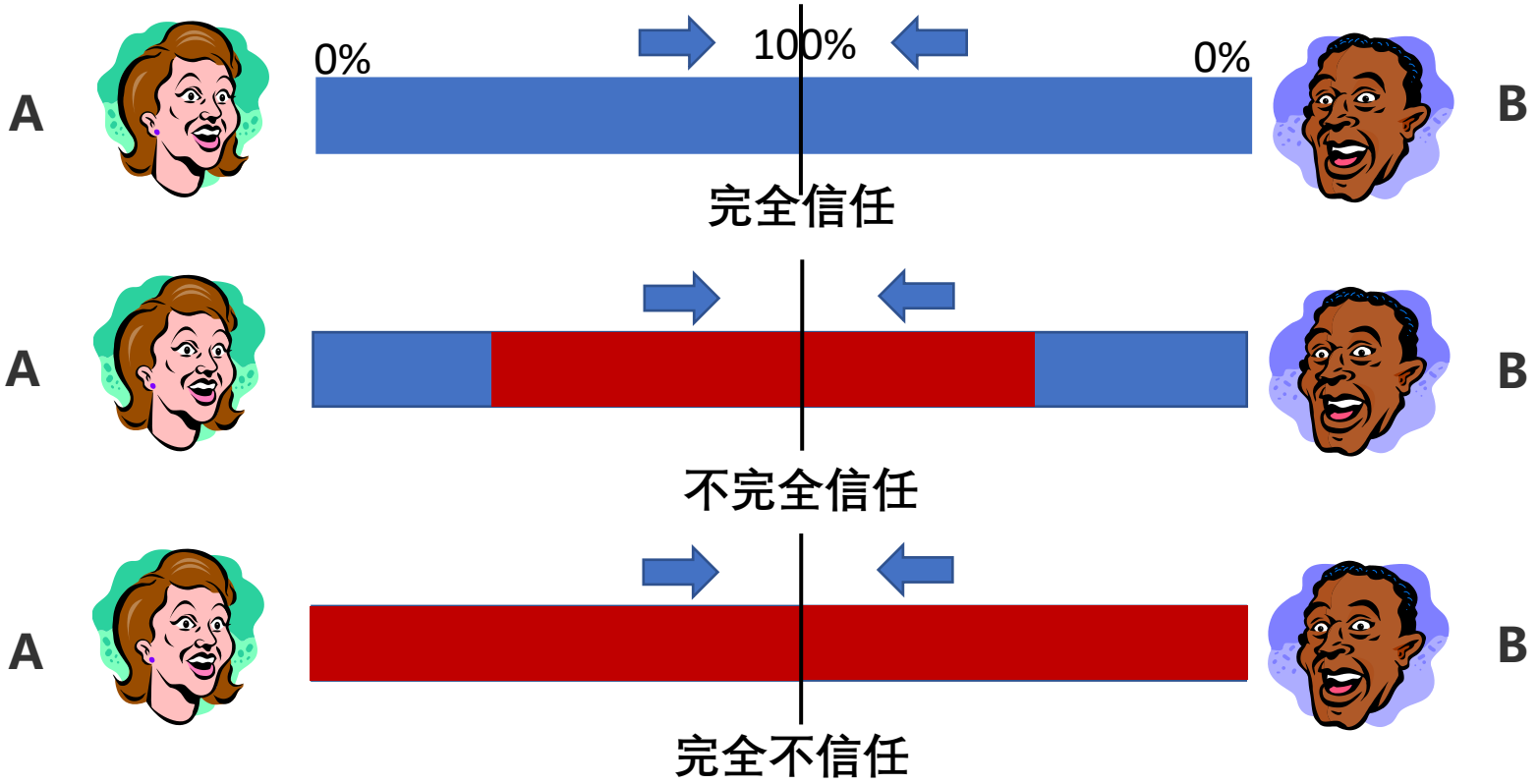
山东大学 SHANDONG UNIVERSITY

信任与零信任

Trust is the **subjective probability** by which an individual A expects that another individual B performs a given action on which its welfare depends.

信任是由个体所产生的**主观预测**，可以表示为某个体A期望另一个体B能够做到与A利益相关的事的概率。 [*D. Gambetta, Can We Trust Trust? 1988*]

[*D. Gambetta, Can We Trust Trust? 1988*]



零信任相当于不完全信任的**最坏**情况（完全不信任），现实中基于不完全信任的合作关系无处不在，常见于：虚拟货币、物联网、供应链、网络计算、元宇宙等领域。

从技术角度我们应该对信任程度不做任何假设，就是要考虑零信任。

虚拟货币——货币虚拟化过程就是去金属化的过程

最早的货币

贝币，是指先秦时期以海贝充当的原始货币

金属货币

周朝早期发明纯铜币

纸币电子化

20 世纪信用卡等交易工具兴起
货币脱离其价值实体以及价值载体而成为纯粹的价值符号

纸质货币

北宋时期”交子“、银票
货币逐渐脱离金属，转化为信用货币

加密货币

——未来

2008年**比特币**
区块链**提供了支撑技术**

虚拟货币——货币虚拟化过程也是信任转移的过程

实体货币 → 金属货币

对金属的信任

贝币，是指先秦时期以海贝充当的原始货币

信任从物体本身转移到实体货币

周朝早期发明纯铜币

人们建立对金属的信任

对政府的信任

信用货币 → 价值符号

对权威第三方的信任

零信任

20 世纪信用卡等交易工具兴起

货币脱离其价值实体以及价值载体而成为纯粹的价值符号

加密货币

北宋时期”交子“、银票

人们从对金属的信任转到对政府的信任

货币逐渐脱离金属，转化为信用货币

——未来

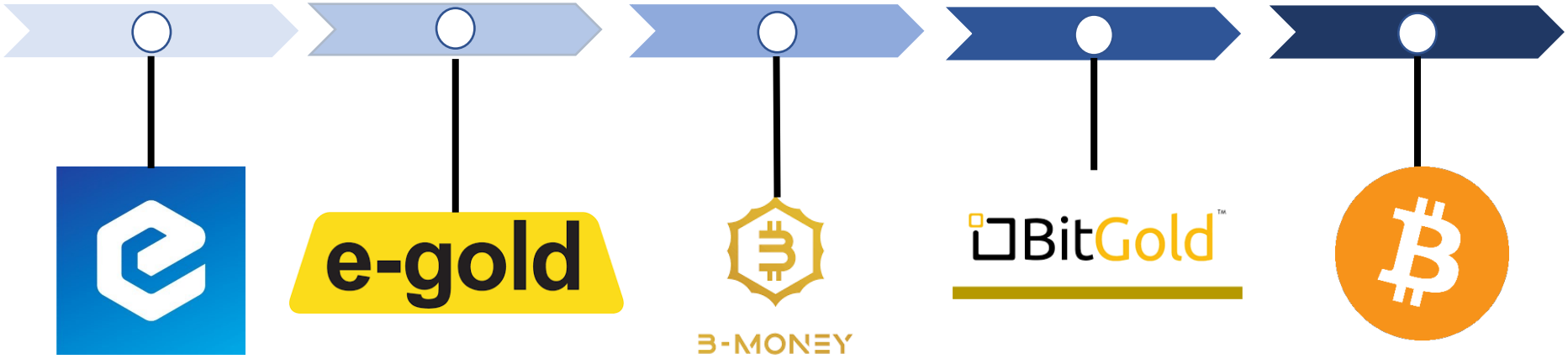
2008年**比特币**

区块链**提供了零信任之上的共识支撑技术**

货币的发展也是信任的发展

零信任在未来将会越来越普遍

虚拟货币——虚拟货币探索阶段



eCash　E-gold　B-money ＋ Bitgold ➡ Bitcoin

特点：使用盲签名技术支持匿名交易，避免双重支付问题。

特点：锚定黄金价格，将金本位时代交易模式电子化。

失败原因：需要一个**中心化机构**管理的服务器才可以运行。

特点：第一个有去中心化思想的数字货币，明确了分布式记账的概念。

失败原因：缺乏共识机制，无法解决双重支付和货币生成问题。

特点：引入PoW共识机制。

失败原因：没有找到合适的开发者导致设想没有成功落地。

特点：结合分布式账本和PoW共识，首次提出**区块链技术**并解决**零信任之上的共识**问题。

取得成功

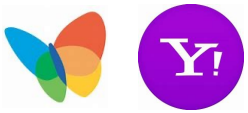
虚拟货币——虚拟货币探索阶段

[资料来源：国海证券研究所]

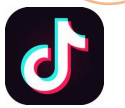
区块链技术成功解决了零信任之上的共识问题，开启了虚拟货币的新发展。除了虚拟货币，零信任之上的共识这一需求无处不在，比如网络计算、Web 3.0、元宇宙、供应链等。

Web的发展

Web 1.0 → **Web 2.0** → **Web 3.0**



1991-2004
- 门户网站与个人网站并存
- 用户只能被动接收网站所提供的信息
- 典型应用：新浪、搜狐、雅虎、MSN




2004-至今
- 用户参与网站内容的制造，但数据不在用户手中
- 大公司/平台垄断数据
- 典型应用：抖音、微博、博客、Facebook




探索阶段
- 用户完全拥有自己产生的内容数据
- 基于区块链技术的互联网
- 典型应用：NFT、DeFi、DAO、虚拟货币

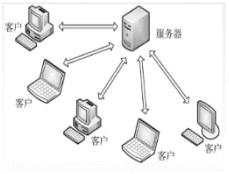
可读 → **可写** → **可拥有**

中心化（数据分散） → **中心化（数据集中）** → **去中心化（零信任）**

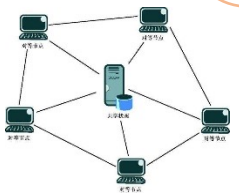
计算范式的发展

客户端-服务器模式 → 对等计算

终端算力发展



20世纪90年代-2008年
依赖特定的后端服务器来提供网络服务



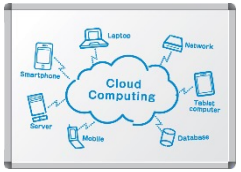
出现于1999年
互联网终端在应用层（overlay 层）按照特定规则互联为大规模对等网络

后端算力发展

网格计算 → 云计算

后端算力发展

本世纪初期-2006年
将政府和机构手中的平台纳入到互联网后端



2006年提出
将计算任务集中到某一高性能计算集群的云计算

未来：网络计算 ← 边缘计算

在零信任基础上，整合网络上所有的空闲资源，提供安全计算服务
– 成秀珍 (2022)

1998年提出，2016年被熟知应用
将计算任务分配到网络终端节点的边缘计算

郭得科，王怀民，国防科技大学. “网络计算典型形态的发展回顾和愿景展望”，2022

网络计算

定义

- **“网络计算”旨在零信任基础上，整合网络中所有的可用计算与存储资源，为各项任务提供高效、安全以及个性化的服务，确保用户数据的隐私性，保证任务结果的准确性与可靠性，实现“对任何一个人或者一项任务整个网络就是一台计算机”，即“Network-as-a-Computer (NaaC, 网络即计算机)” – 成秀珍 (2022)**

优势

- 基于区块链提供零信任下的可信计算环境，支持可容错的计算节点存在，拓展拜占庭容错算法的适用范围；
- 在零信任下整合各类互联网终端侧的计算能力，实现个性化资源调度与分配；
- 充分利用网络资源，实现高度置信的凡在计算，支撑工业互联网供应链元宇宙等应用；

总结 – 零信任计算

货币	Web	计算范式
• 金属 • 纸币 • 加密货币（较为成熟）	• Web 1.0 • Web 2.0 • Web 3.0（探索阶段）	• 云计算 • 边缘计算 • 网络计算（未来趋势）

技术支撑

零信任计算（Zero-trust Computing）

支撑

分布式组网：wChain

- 由山大团队提出；
- 用于多跳无线网络的快速容错区块链协议。

分布式计算：智能合约

- 由Nick Szabo 提出；
- 以数字形式存在；
- 支持无第三方交易；

支撑

分布式存储：IPFS

- 由Juan Benet 提出；
- 支持持久且分布式存储和文件共享；

零信任共识支持

区块链：为分布式系统提供零信任上的共识

新要求

① 改进存储模式，提高存储效率　② 降低计算开销，支持隐私计算的智能合约

学无止境

气有浩然

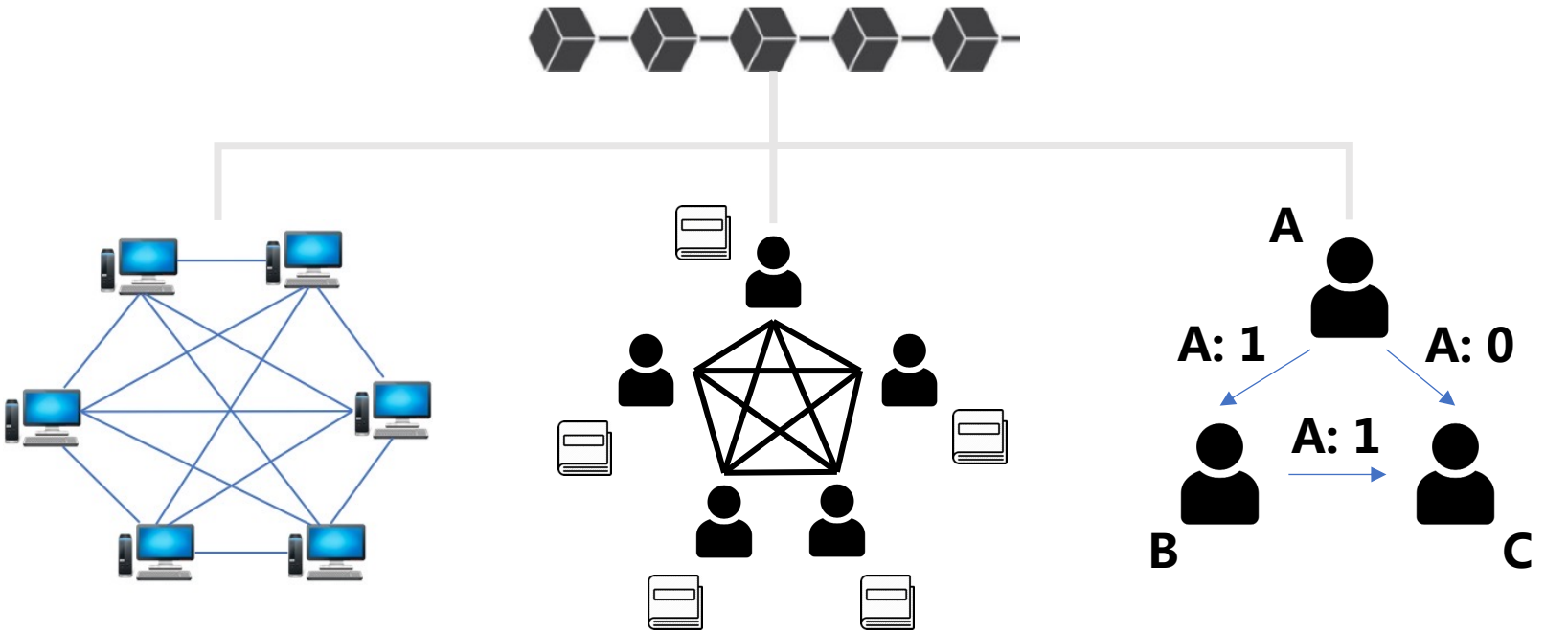
Part 02 零信任计算与挑战

1. 区块链的核心挑战
2. 零信任计算的挑战

山东大学
SHANDONG UNIVERSITY

区块链的核心挑战

设计新型区块链系统架构，提升区块链效率



区块链网络架构：动态自适应的、与共识和底层通信网络高效高度融合的网络架构

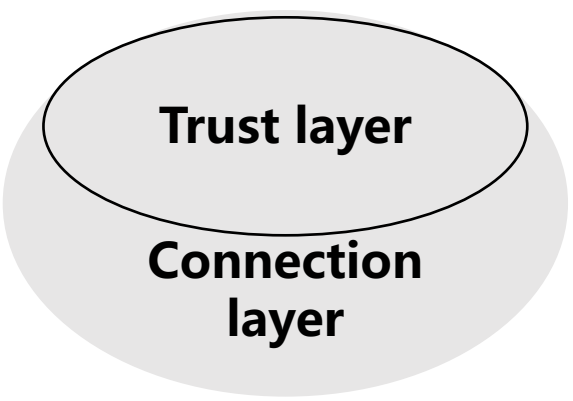
高度一致性和高可用性的分布式账本：全局存储一致、全排序、非歧义性

高吞吐低延迟低功耗共识算法：共识是网络的分布式公共驱动，需要研究高性能合作型共识算法

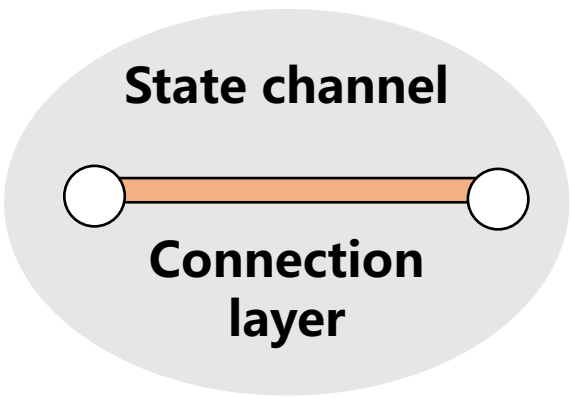
区块链的核心挑战

链内轻量级临时可信操作环境构建和安全解构

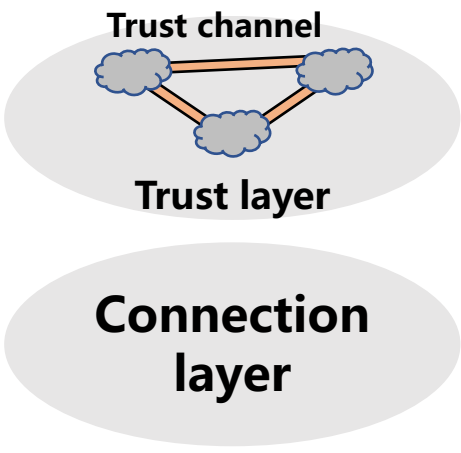
- 区块链中connection layer与trust layer重合，维持full trust layer极大限制了区块链的效率
- 目前Stefan等人提出了安全定义下的state channel [1]，通过创建点对点的临时可信操作环境，可以有效减少不相关节点的冗余性
- 但由于信任的量度可由用户定义，因此可在后果可接受的情况下降低安全等级，建立由用户定义信任程度的trust channel，增加方案的适用性



当前普遍结构



Stefan方案



需求

[1] Dziembowski S , Faust S , Kristina Hostáková. General State Channel Networks[C]// the 2018 ACM SIGSAC Conference. ACM, 2018.

区块链的核心挑战

模块化区块链系统设计

- 目前区块链系统采用单一一体化设计，每个区块链系统只支持一种共识算法，无法灵活应对多场景，难以构建统一的测试标准
- 模块化区块链系统设计
  - 支持多种共识协议，账本结构和组网方式，实现不同区块链系统性能对比，建立统一测试标准
  - 实现不同区块链系统间的简洁跨链协议，解决跨链难问题
  - 构建基于安全和隐私保护的模块接口和通信协议，解决跨链协同隐私计算难题
- SandyLab – 模块化区块链系统
  - 山东大学研发
  - 能够支持节点、共识算法模块
  - 网络拓扑以可拖拽（类似于思维导图）的方式构建

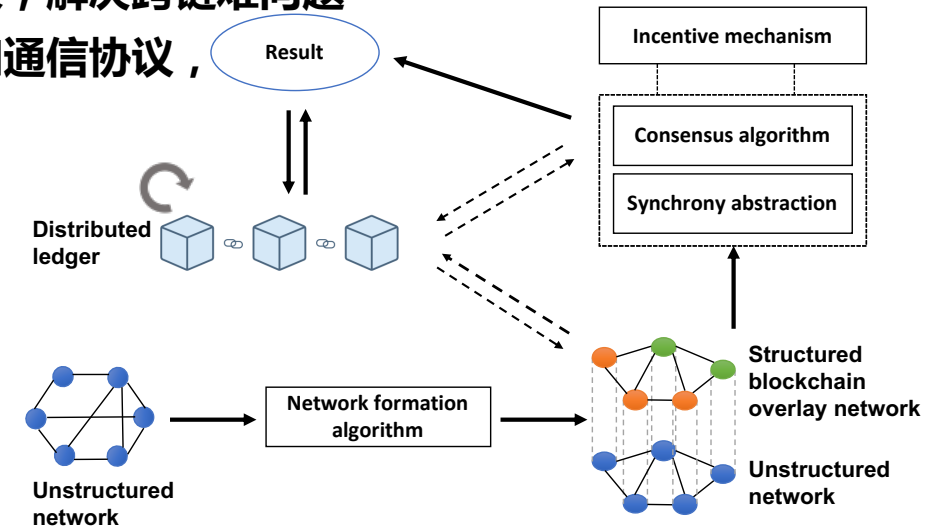


图 模块化区块链系统架构（来自 IIC）

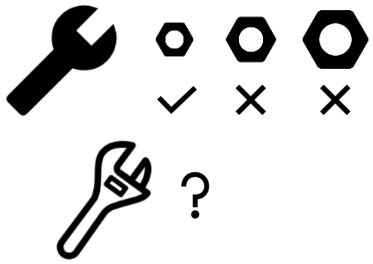
零信任计算的挑战

零信任可信组网

1. 零信任可信环境与底层融合不紧密
   - 底层资源受限设备因**数量庞大**难以管理，又因**计算能力差**易受攻击
   - 底层混合（有线+无线）网络**场景复杂**，技术**开发难度高**

海量资源受限设备
混合网络复杂场景

2. 零信任可信环境设计单一、不灵活
   - 现有零信任可信环境(区块链)难以与**多样、复杂的应用场景**做到紧密贴合
   - 现有零信任可信环境涉及大量无关节点，**计算资源消耗冗余严重**



零信任可信环境设计不灵活

3. 跨链可信环境发展缓慢、通用性差
   - 区块链**一体化设计严重**，跨链互操作难实现
   - 跨链安全、隐私与性能**存在短板**

零信任计算的挑战

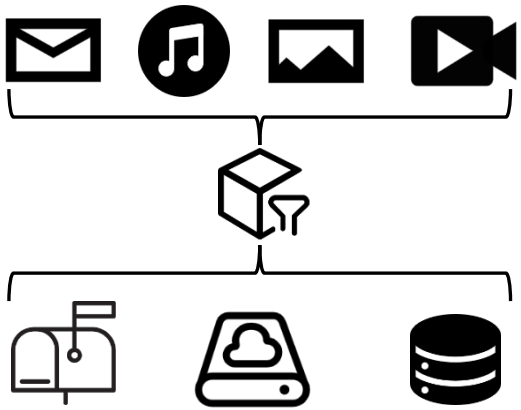
零信任数据流通

1. 零信任数据查找使用效率低
   - 非结构化数据存储缺失
   - 数据无序堆叠导致数据快速定位难

2. 数据共享步骤繁琐
   - 数据调度需要先读取内容，再进行转发
   - 数据调度延迟过高，不能支持高实时性应用

3. 数据边界不牢固，秘密数据易流出
   - 现有边界保护方案集中在数据流出后的追溯与追责
   - 亡羊补牢式的边界保护难以从源头防止数据边界被攻破

海量数据无序堆叠



中心化的“数据分拣”延迟过高

零信任下数据边界保护尤为必要

零信任计算的挑战

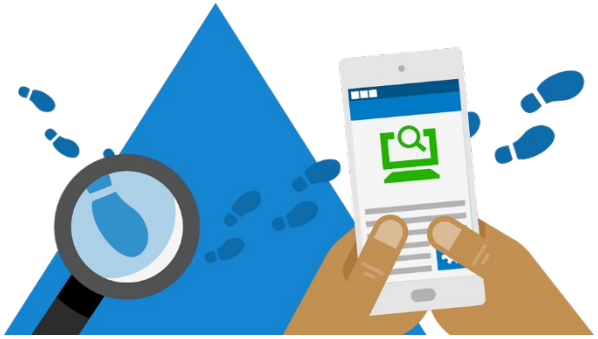
零信任计算

1. 链上合约执行效率低
   - 所有区块链节点需要针对同一合约**独立进行计算**
   - 针对合约执行的**协同计算缺失**
   - 区块链链上**计算能力扩展难**

2. 隐私保护特性缺失
   - 链上合约**公开执行**，隐私数据保护难

3. 链下计算应用场景受限
   - 现有链下计算应用**集中在支付场景**
   - 缺少更通用的链下合约执行机制

区块链上的计算主要体现为**智能合约**的形式。智能合约是一种能够被区块链节点解析的编程语言，发布在区块链上的一份智能合约会被**所有节点**解析并执行。



智能合约的公开执行提高了安全性，也降低了隐私性

链下计算应用集中在简单的支付场景

学无止境

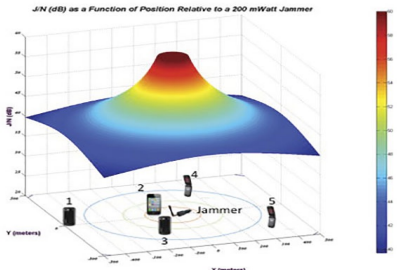
气有浩然

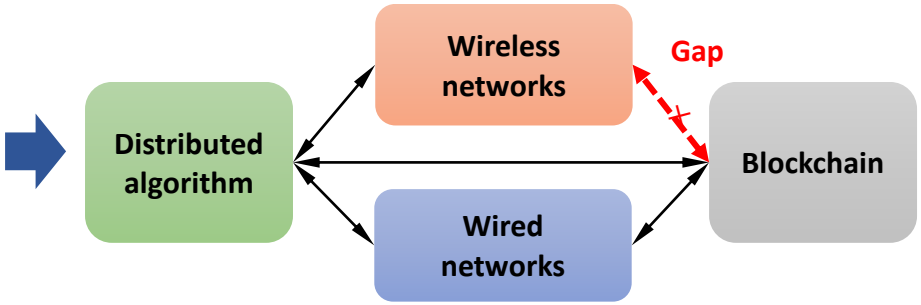
Part 03 山东大学相关研究

山东大学
SHANDONG UNIVERSITY

无线区块链协议

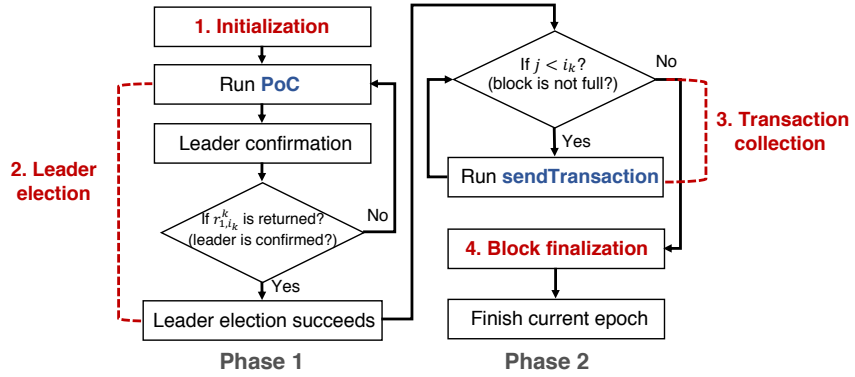
核心挑战:



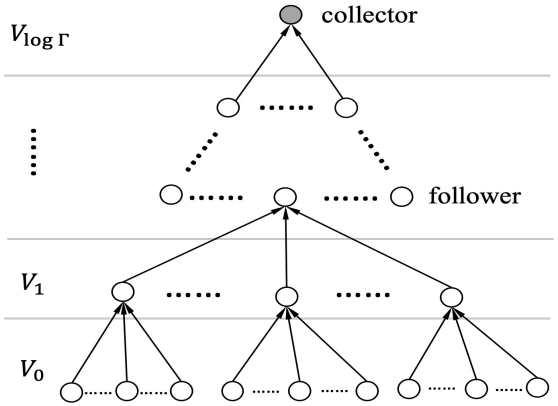


动态与不稳定的信道带宽　　**无线信道阻塞与干扰攻击**

提出单跳和多跳无线网络中的区块链协议:



BLOWN区块链协议（单跳）

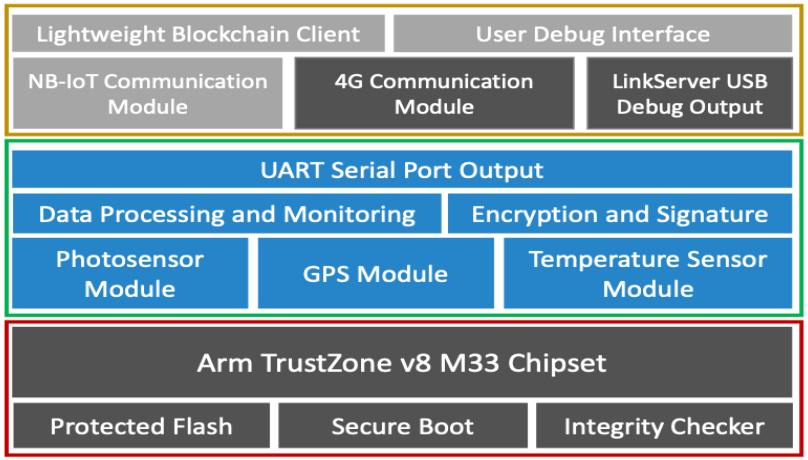


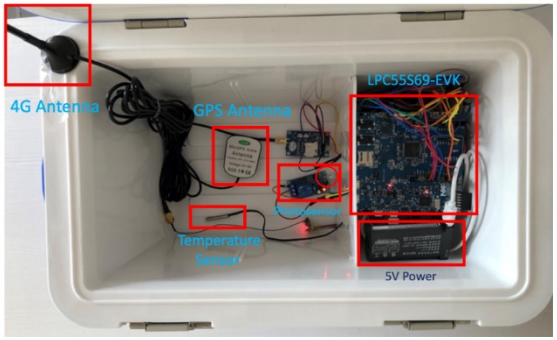
wChain区块链协议（多跳）

[1] Minghui Xu, Feng Zhao, Yifei Zou, Chunchi Liu, Xiuzhen Cheng, Falko Dressler. “BLOWN: A Blockchain Protocol for Single-Hop Wireless Networks under Adversarial SINR”. IEEE Transactions on Mobile Computing (2022).
[2] Minghui Xu, Chunchi Liu, Yifei Zou, Feng Zhao, Jiguo Yu, and Xiuzhen Cheng. "wChain: a fast fault-tolerant blockchain protocol for multihop wireless networks." IEEE Transactions on Wireless Communications 20, no. 10 (2021): 6915-6926.

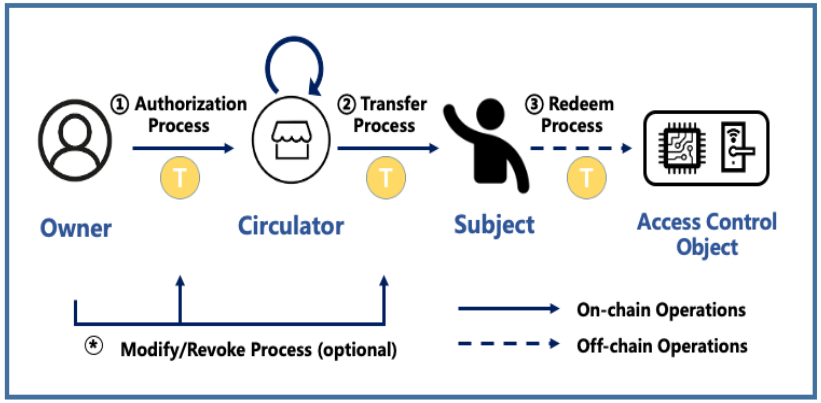
物联网访问控制机制与链上链下可信延伸技术

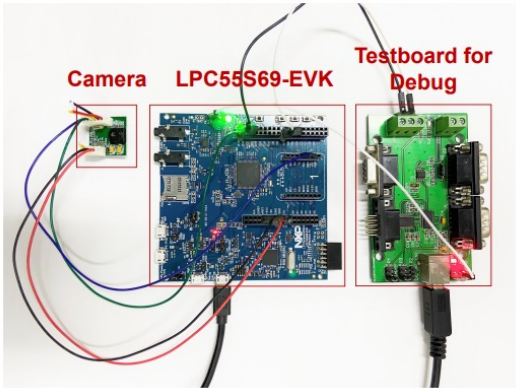
链上链下可信延伸：实现区块链对物理世界的可信控制和物理世界数据的可信采集与上链





通用精准访问控制：访问策略细粒度自定义，通过可信硬件实现访问策略可信验证





[1] Liu, Chunchi, Hechuan Guo, Minghui Xu, Shengling Wang, Dongxiao Yu, Jiguo Yu, and Xiuzhen Cheng. "Extending On-chain Trust to Off-chain--Trustworthy Blockchain Data Collection using Trusted Execution Environment (TEE)." IEEE Transactions on Computers (2022).

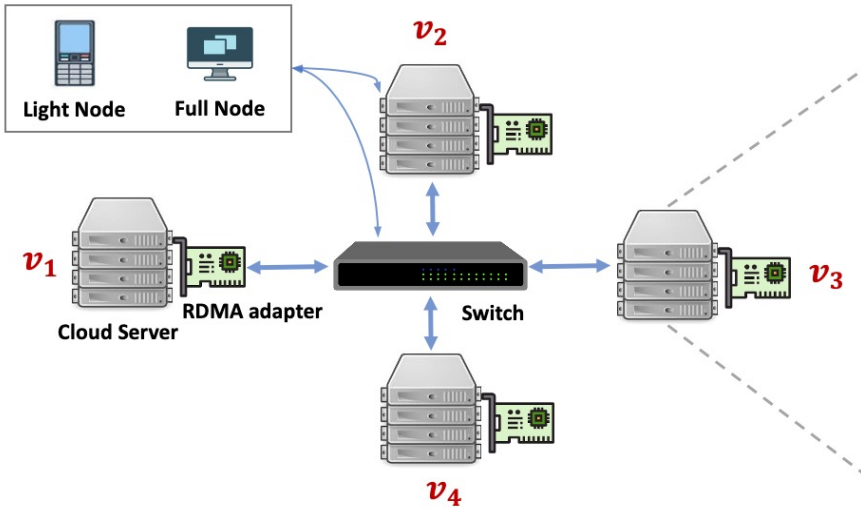
[2] C. Liu, et al. “TBAC: Tokoin-Based Fine-Grained and Accountable Access Control”, submitted to *IEEE Transactions on Mobile Computing*.

面向云计算的区块链系统

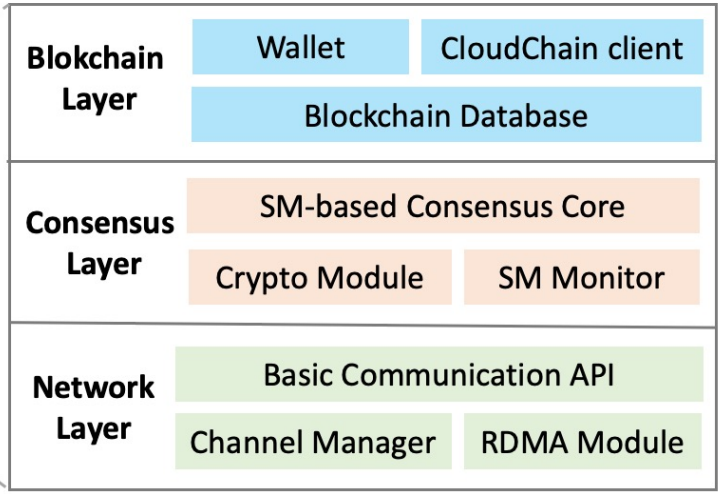
消息传递模型（目前区块链的通信模型）

- ❑ 通过消息交换实现通信
- ❑ 节点较为离散
- ❑ 需严格考虑异步问题

- ✓ 云计算环境节点紧密耦合、底层网络同步
- ✓ CloudChain支持基于共享内存的共识算法,利用RDMA可保证高性能



CloudChain Network

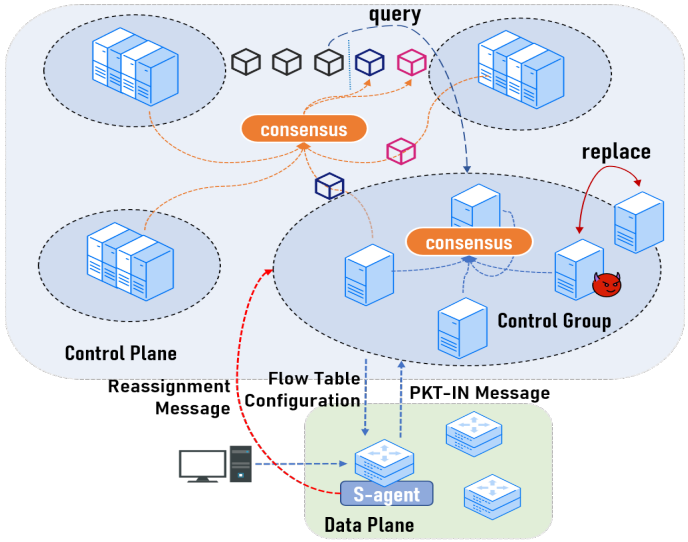


CloudChain System Architecture

[1] Xu, Minghui, Shuo Liu, Dongxiao Yu, Xiuzhen Cheng, Shaoyong Guo, and Jiguo Yu. "CloudChain: a cloud blockchain using shared memory consensus and RDMA." IEEE Transactions on Computers (2022).

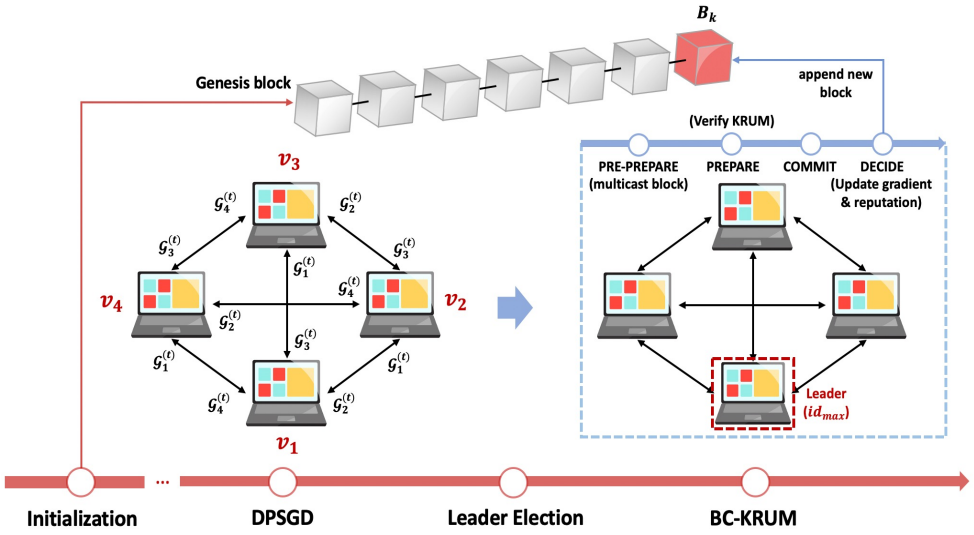
区块链+

区块链+软件定义网络



- ✓ 利用区块链，为软件定义网络控制平面提供最多容忍N/3拜占庭节点的可信计算环境
- ✓ 保证安全的流表更新操作，提供高效共识协议
- ✓ 检测拜占庭节点并支持可信的控制器重配置
- ✓ 支持网络拓扑可信控制，抗网络劫持攻击

区块链+去中心化学习



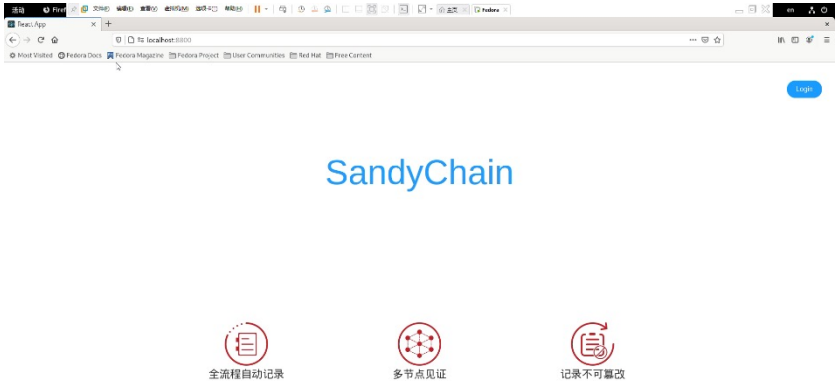
为去中心化学习提供安全与隐私保护：

- ✓ 安全：利用区块链、拜占庭容错共识算法保护分布式机器学习的安全性，使其(训练过程)具备拜占庭容错能力
- ✓ 隐私：在参数或梯度交换中引入差分隐私技术，保护数据隐私不泄漏

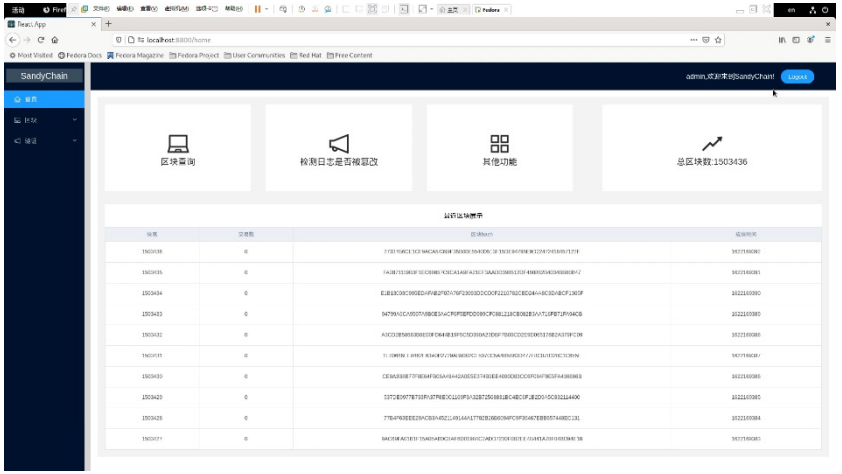
[1] Minghui Xu, Chenxu Wang, Dongxiao Yu, Xiuzhen Cheng, Weicheng Lv. “Curb: Trusted and Scalable Software-Defined Network Control Plane for Edge Computing”. 42nd IEEE International Conference on Distributed Computing Systems (ICDCS 2022).

[2] Minghui Xu, Zongrui Zou, Ye Cheng, Qin Hu, Dongxiao Yu, Xiuzhen Cheng. “SPDL: Blockchain-secured and Privacy-preserving Decentralized Learning”. IEEE Transactions on Computers (2022).

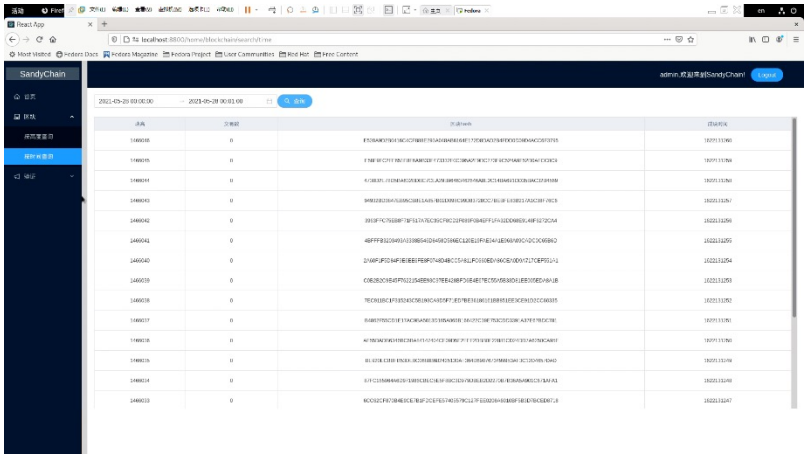
区块链平台



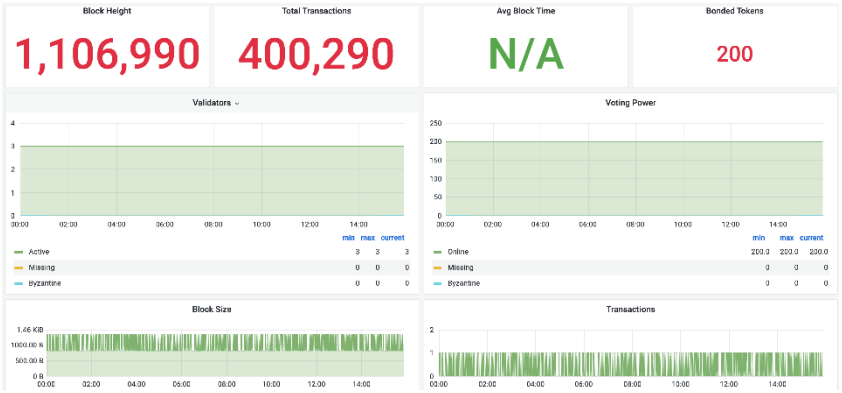
登录界面



功能面板



区块查询与检索



系统监控

山东大学计算机科学与技术学院

School of Computer Science and Technology, Shandong University

感谢各位专家  敬请批评指正

成秀珍