CCF区块链安全与隐私前沿论坛（CCF-BSP 2022）

SPDL: A Blockchain-enabled Secure and Privacy-preserving Decentralized Learning System

汇报人：徐明辉

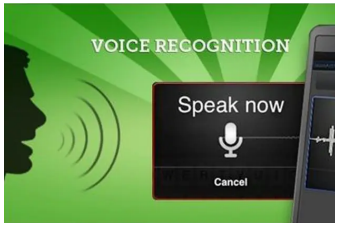
目录

什么是分布式学习

机器学习遇到的问题：样本数量不足，样本维度不丰富，模型规模太大，训练时间过长等

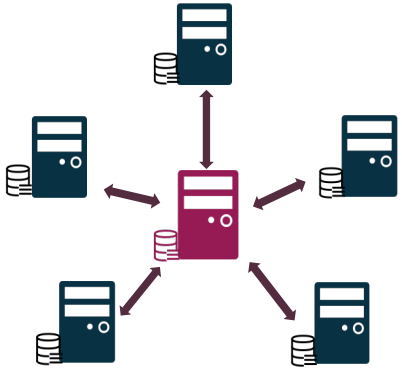
分布式机器学习：是指利用多个计算节点协同训练一个全局的机器学习/深度学习模型。

腾讯-微众银行联合多家医院构建“脑卒中发病风险预测模型”，脑卒中预测准确率达80%

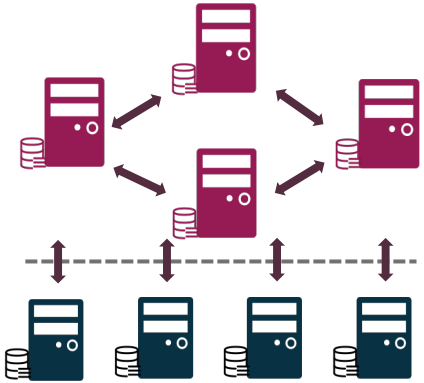


IBM通过分布式学习将自动语音识别训练时间由一周多压缩至11.5小时

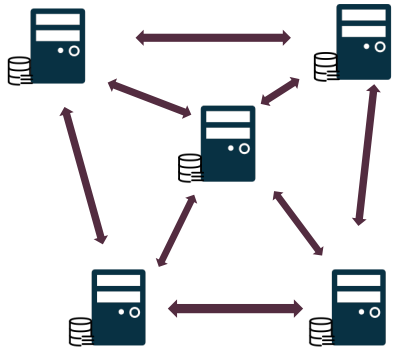
什么是分布式学习



(1) 联邦学习 [PMLR’17]

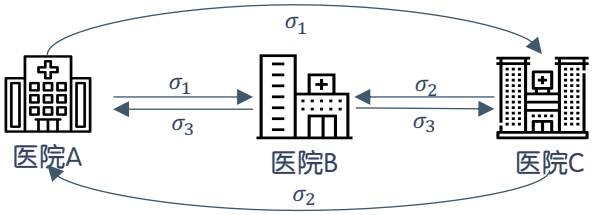


(2) 联邦学习 [PODC’20]

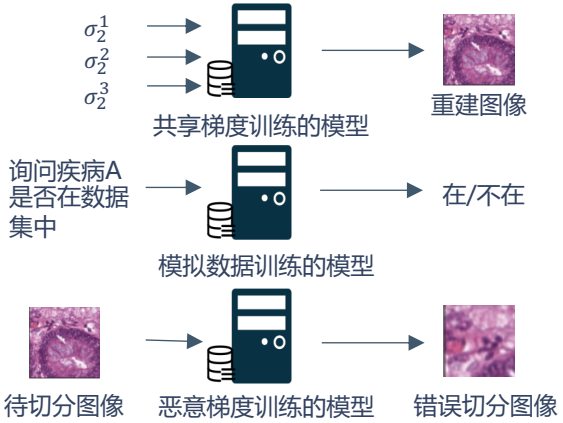


(3) 去中心化学习(Nature’21)

主要问题



三家医疗机构合作进行图像分割的模型训练

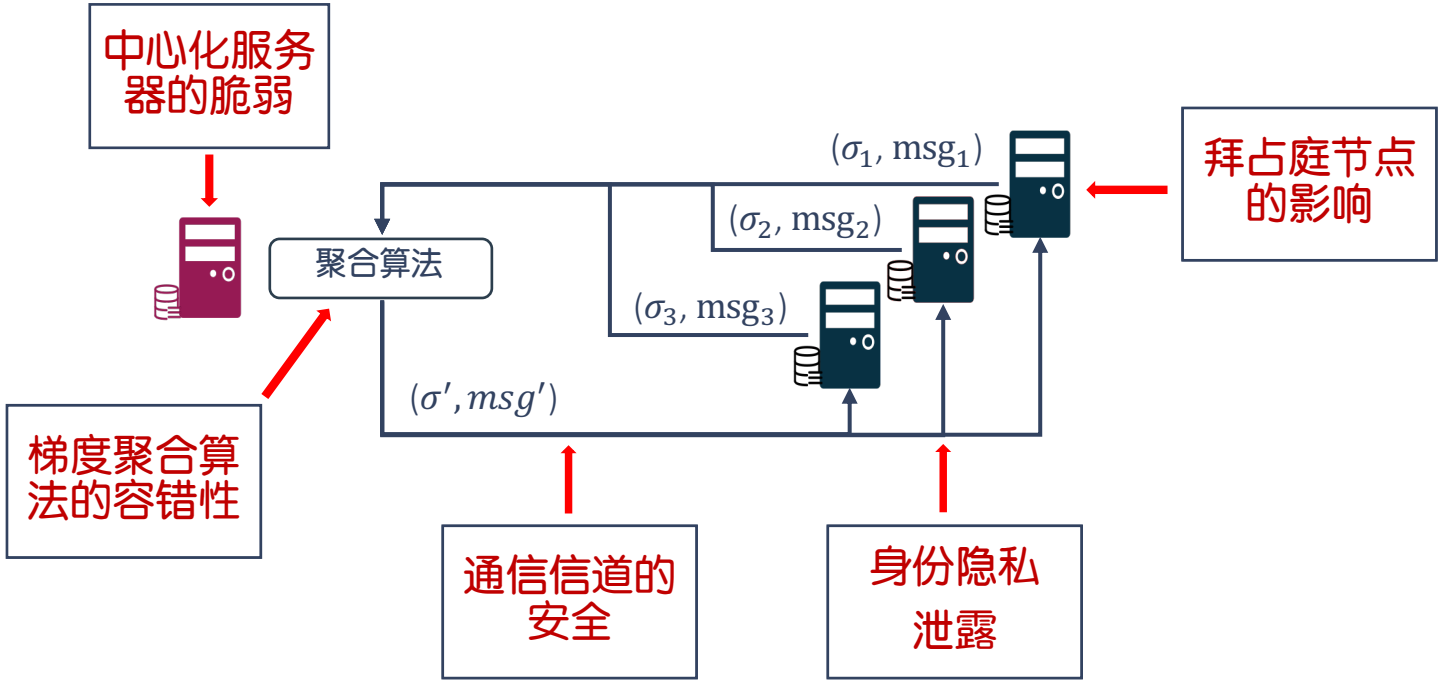


梯度泄露攻击　攻击者通过传递的梯度恢复病患的扫描图像。

模型逆向攻击　攻击者构造影子模型预测数据集中是否存在性别信息等病患的私人信息。

模型投毒攻击　攻击者可以生成恶意梯度，导致模型出现误判等问题，影响病患的诊断和治疗。

主要挑战


中心化服务器的脆弱
聚合算法
梯度聚合算法的容错性
$(\sigma_1, \mathrm{msg}_1)$
$(\sigma_2, \mathrm{msg}_2)$
$(\sigma_3, \mathrm{msg}_3)$
(σ', msg')
拜占庭节点的影响
通信信道的安全
身份隐私泄露

相关工作

	DP-FL	FL-Block	Y.Lu et al	LearningChain	Biscotti	SPDL
去中心化架构	√(带参数服务器)	√	√	√	√	√
可拓展性	×	√	√	√	√	√
拜占庭容错	×	×	√	√（POW）	√	√
抗女巫攻击	×	√	×	×	√	√
梯度隐私保护	√	√	√	√	√(承诺机制)	√
身份隐私保护	×	×	×	×	×	√

SPDL解决的主要问题

How can we efficiently coordinate the decentralized learning process while simultaneously maintaining learning security and data privacy for the entire system?

1 如何构建大范围的分布式训练网络？

需要解决节点之间的信任问题、激励问题、隐私问题等。

2 如何抵御拜占庭行为？

拜占庭节点会对共识过程、参数聚合过程、模型训练结果产生负面影响。

3 如何充分保护训练过程不泄露隐私？

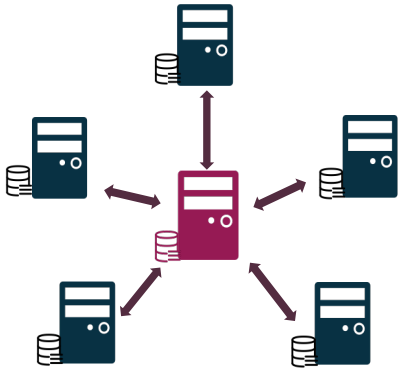
除数据隐私外，节点身份、设备信息等隐私也会带来安全问题。

02 SPDL设计

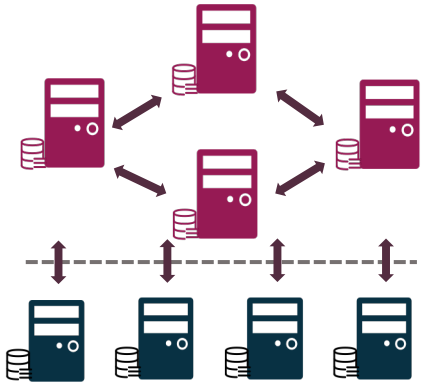
SPDL主要的技术方案

基于传统签名的分布式学习	基于公开网络的分布式学习	基于同态加密的分布式学习	使用同态加密的参数聚合
不能保护用户的身份隐私	不能保护设备信息隐私	时空开销大	不能应对拜占庭节点
↓	↓	↓	↓
可链接环签名	匿名网络	差分隐私	整合区块链协议、BFT共识与BFT GAR，提供容错性

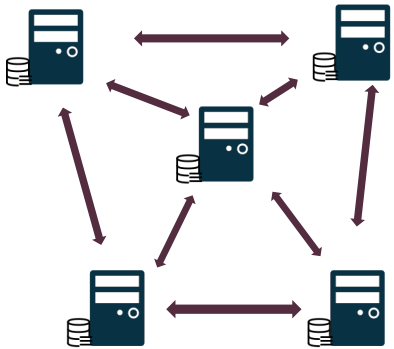
去中心化分布式学习



1）联邦学习A

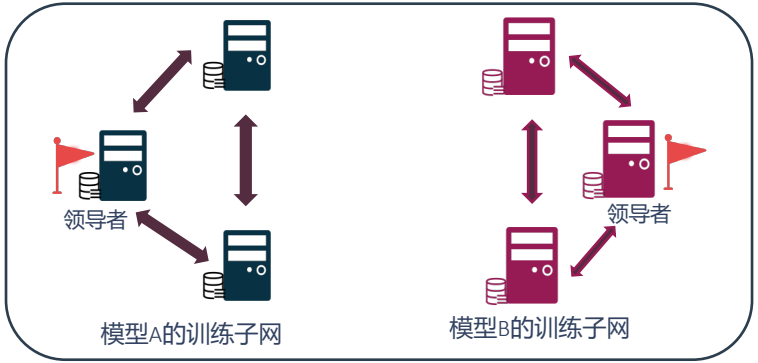


2）联邦学习B



3）去中心化学习(SPDL)

训练网络构成



模型A和模型B构成的训练网络

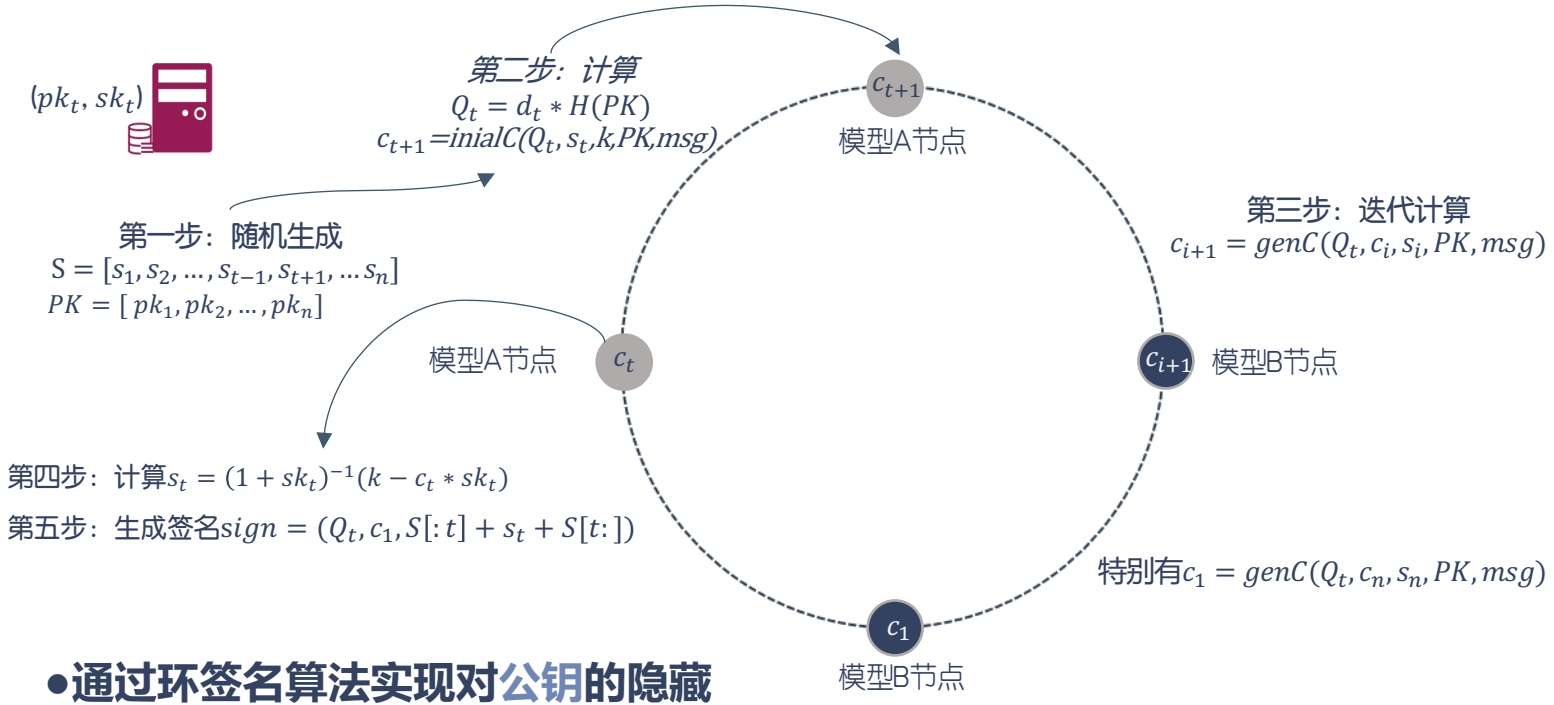
训练网络：我们把环签名的所有参与方称为一个训练网络。

训练子网：参与模型A训练的网络构成模型A的训练子网，一个训练网络可以有多个训练子网。

领导者节点：在一个训练子网中整合所有训练节点消息并发布确认消息的节点，由选举机制产生。

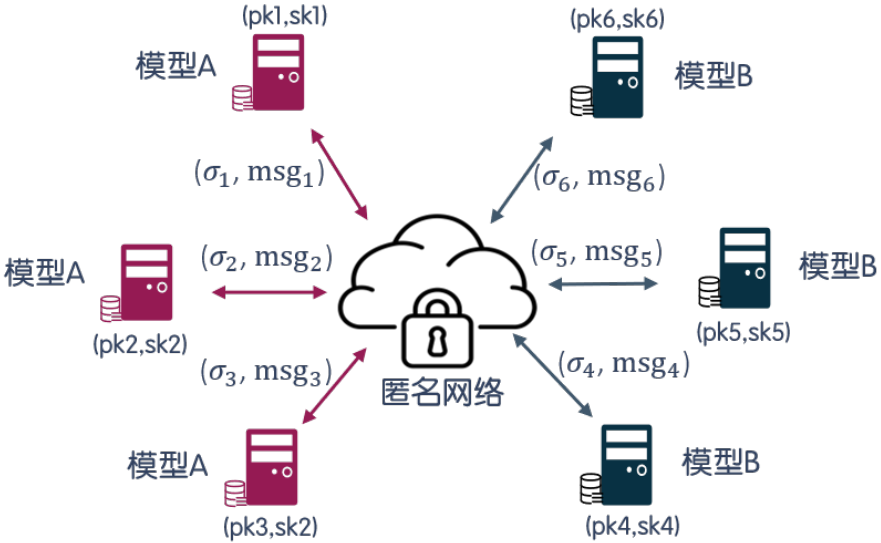
跟随者节点：接收所有训练节点消息并对领导者节点消息做出响应的节点。

可链接环签名

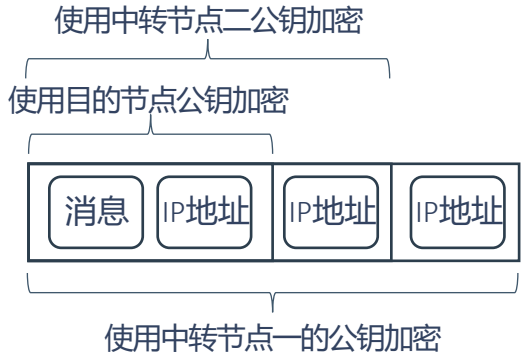


- 通过环签名算法实现对公钥的隐藏
- 通过多模型成环实现对参与模型的隐藏

匿名网络

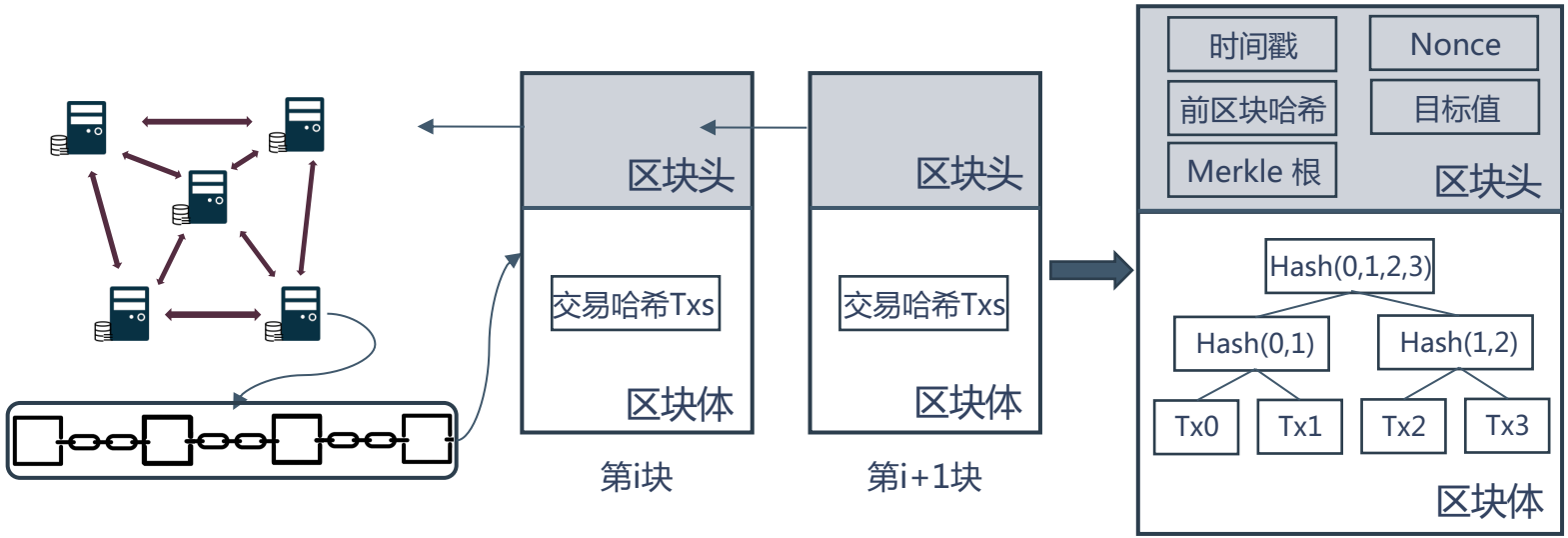


$$\boldsymbol{\sigma} = sign(sk, PK, msg)$$



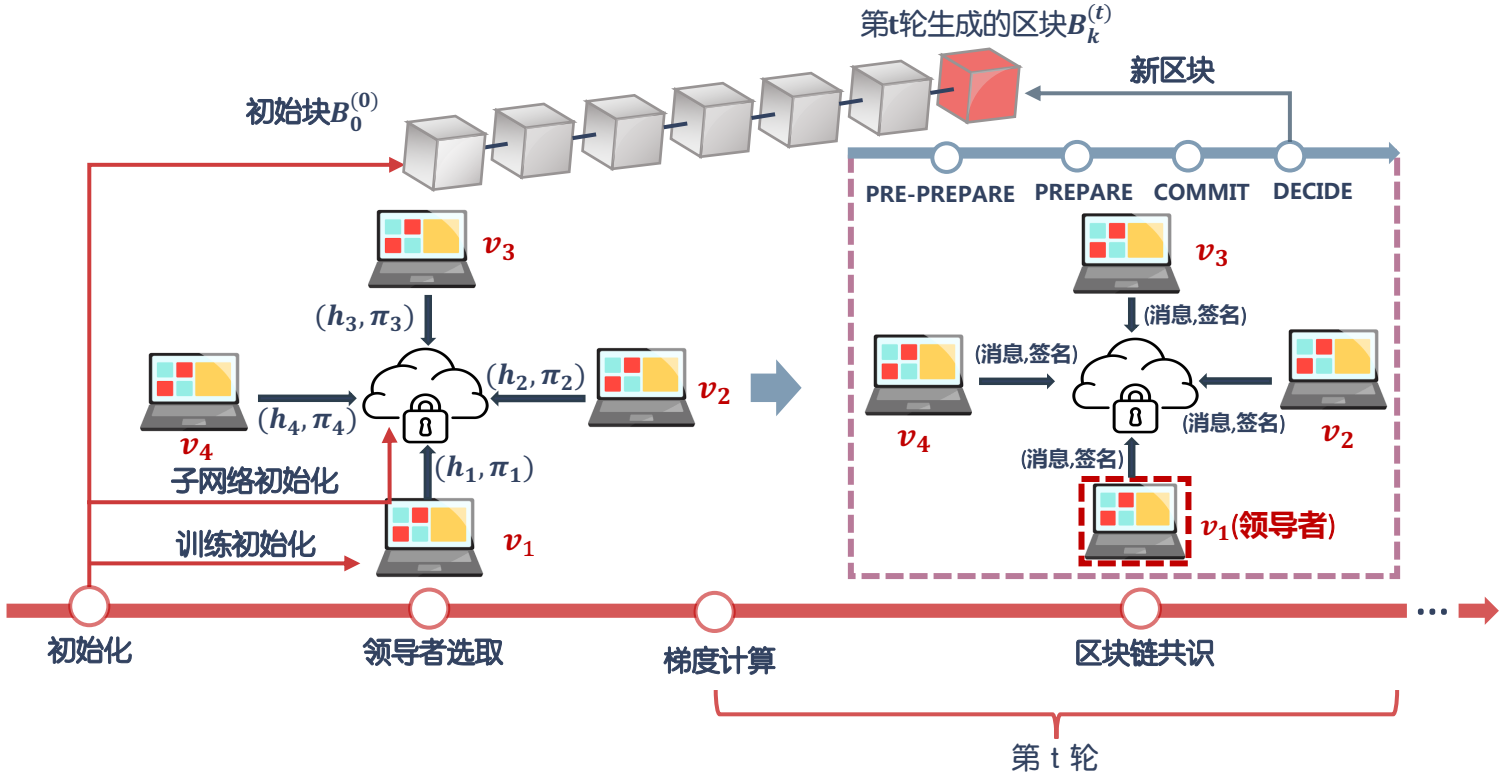
- **通过匿名网络算法实现了对IP等信息的隐藏**
- **公钥与IP的双重隐藏,保证信息的可验证性的同时隔离了数据和节点**

区块链

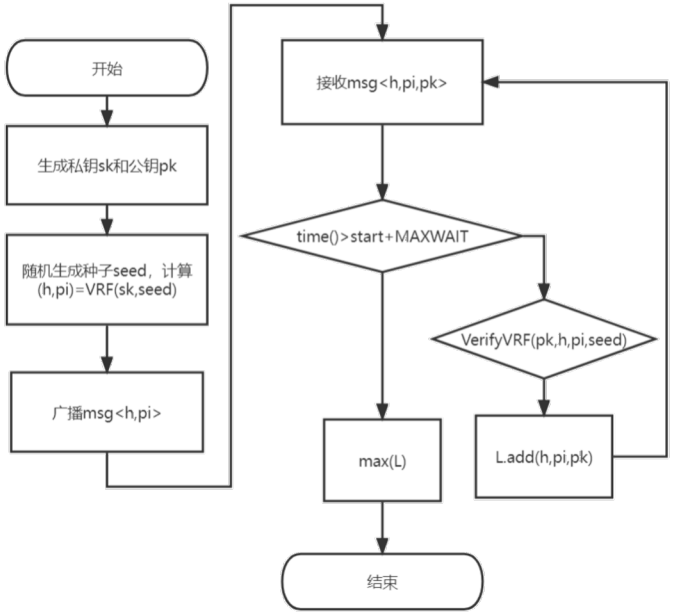


区块链可以在不互信多方之间保障数据（梯度聚合）的防篡改与真实性

协议流程



协议实现：选举领导者



1．每个节点生成自己的公私钥

2．通过可验证函数VRF生成一组(h, p_i)

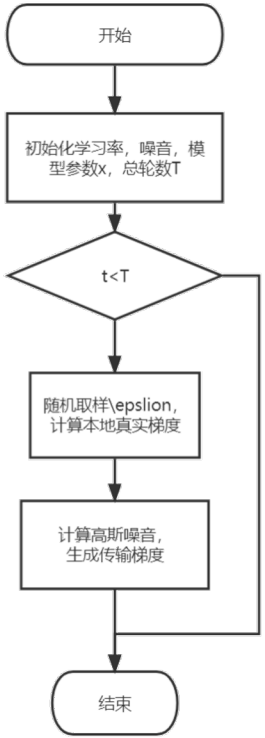
3．向所有节点广播(h, p_i)

4．每个节点等待接收(h, p_i)，通过验证则加入列表L

5．接收n个后L，从中选出最大值

6．等待超时则重新开始算法

协议实现：梯度计算



$$average = \sqrt{\sum_{i=1}^{n} grad[i]^2}$$

$$noise\_grad[i] = grad[i] + N(0, 10^{-6} * average * \sqrt{\frac{2 * \ln(1.25/\sigma)}{\epsilon}})$$

1．每个节点根据初始块设置自己的学习率，噪声，模型参数，轮数T

2．从训练集中随机取样，计算本地真实梯度

3．计算高斯噪音,生成传输梯度

协议实现：区块链共识

Algorithm 3: Blockchain Consensus

▷ To prevent deadlock, each node starts a view change if $\texttt{Time}() > start + \delta_2$
▷ PRE-PREPARE
if *role is leader* **then**
  $\Delta^{(t)} = \mathcal{K}(g_1^{(t)}, g_2^{(t)}, \cdots, g_n^{(t)})$
  $B_k^{(t)} \leftarrow \texttt{MSGB}(\Delta^{(t)})$
  broadcast $\langle \texttt{PRE-PREPARE}, id, B_k^{(t)}, h \rangle_{\hat{\sigma}}$
▷ PREPARE
if *role is follower* **then**
  compute $\tilde{\Delta}^{(t)} = \mathcal{K}(g_1^{(t)}, g_2^{(t)}, \cdots, g_n^{(t)})$
  while *receive* $\langle \texttt{PRE-PREPARE}, id, B_k^{(t)}, h \rangle_{\hat{\sigma}}$ **do**
    if σ *and* $B_k^{(t)}$ *are valid and* $\tilde{\Delta}^{(t)} \approx B_k^{(t)}.\Delta^{(t)}$ **then**
      broadcast $\langle \texttt{PREPARE}, id, h, vote \rangle_{\hat{\sigma}}$
▷ COMMIT
while *receive* $2f + 1$ $\langle \texttt{PREPARE}, id, h, vote \rangle_{\hat{\sigma}}$ **do**
  broadcast $\langle \texttt{COMMIT}, id, vote \rangle_{\hat{\sigma}}$
▷ DECIDE
while *receive* $2f + 1$ $\langle \texttt{COMMIT}, id, h, vote \rangle_{\hat{\sigma}}$ **do**
  $\texttt{Append}(BC_k^{(t)}, B_k^{(t)})$
  $x_i^{(t+1)} = x_i^{(t)} - \gamma \Delta^{(t)}$
  Update reputation

一轮共识过程如下：

PRE-PREPARE： 利用Byzantine Fault-Tolerant Gradient Aggregation Rule（BFT-GAR）算法计算聚合后的梯度，将梯度作为主要信息加入区块中发布

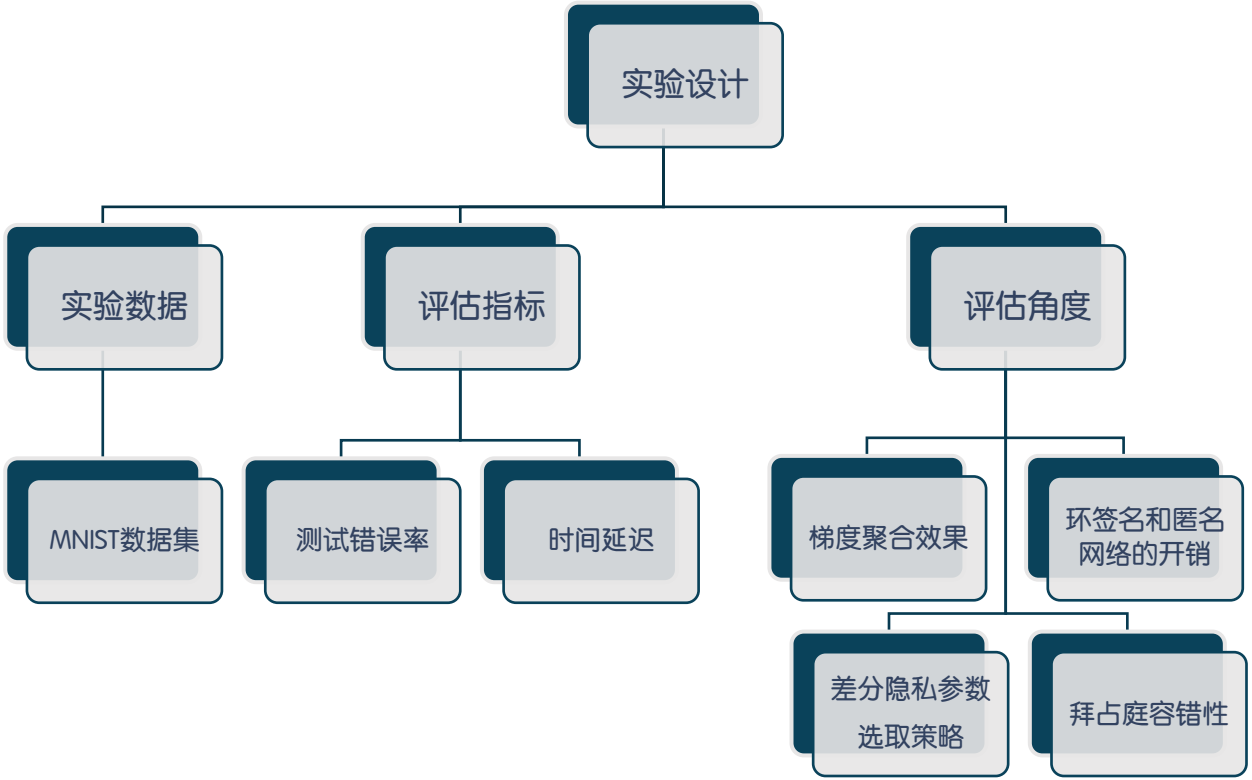
PREPARE： follower根据自己接收到的梯度重算聚合梯度，验证区块

COMMIT：当收到2f+1个投票时确认区块

DECIDE：更新区块与模型参数

03 实验分析

实验设计



实现方案

实验环境配置

- CPU（AMD R5-4600H）
- 16GB

网络通信

- gRPC框架
- P2P网络

机器学习

- Pytorch

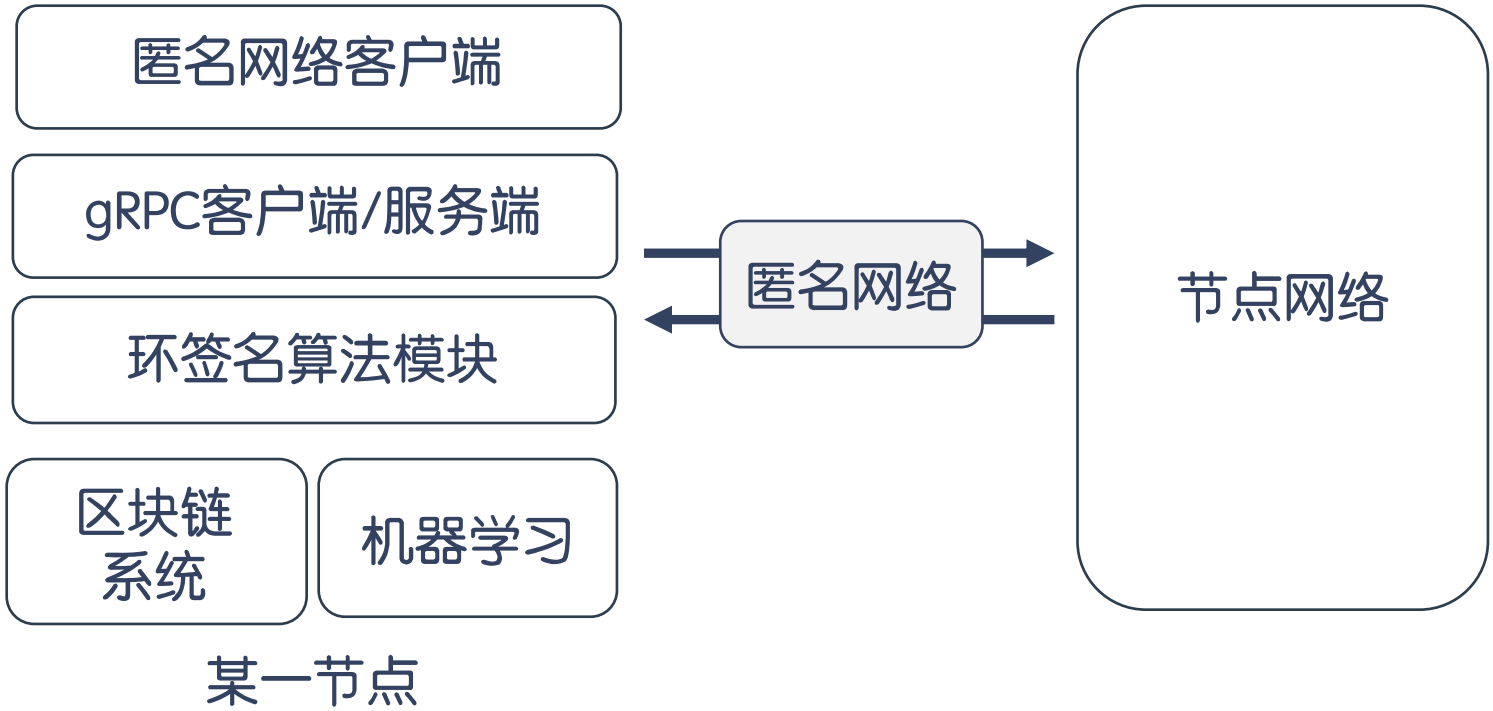
密码学

- SM2环签名算法模块

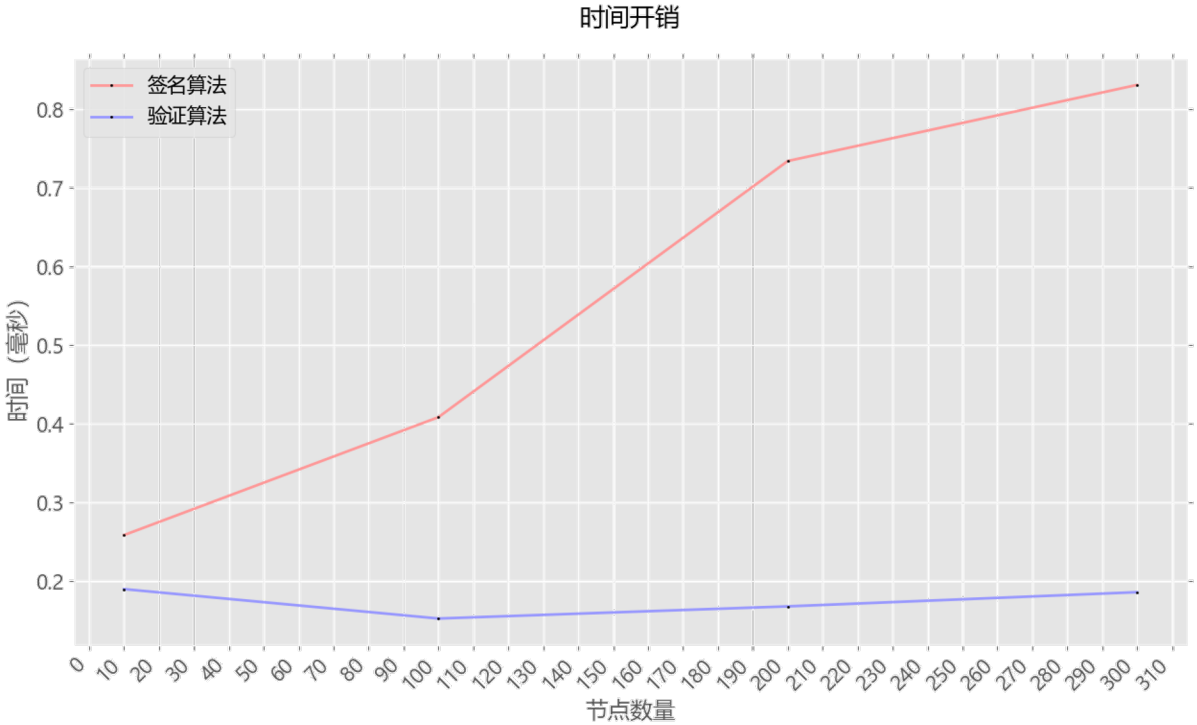
区块链

- 基于BFT共识算法的区块链系统

系统框架图

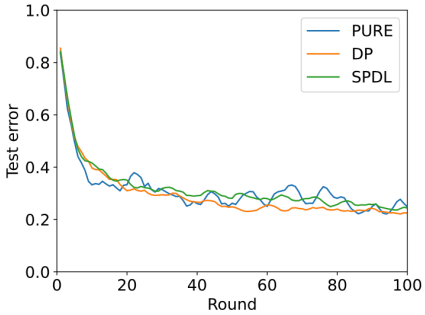


环签名算法的时间开销

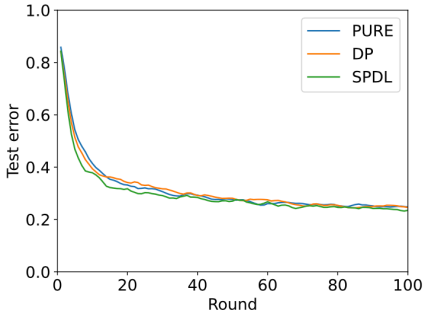


签名与验证理论复杂度均为O(n)
每增加一个节点签名时间增加不到3ms，验证时间变化较小

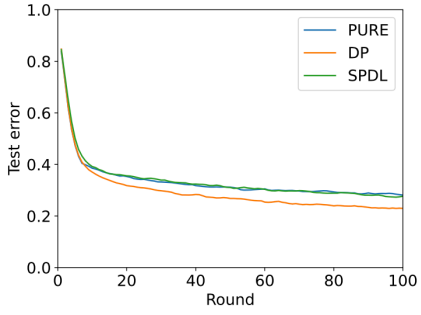
模型错误率（网络规模）



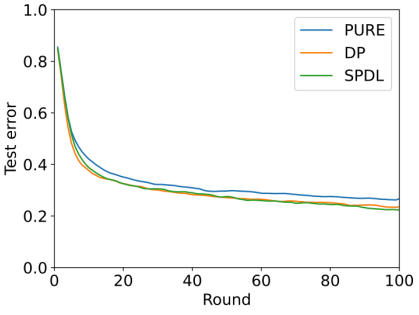
(a) $N = 4$



(b) $N = 10$



(c) $N = 20$

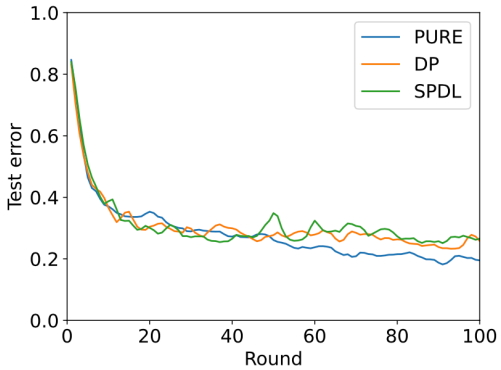


(d) $N = 30$

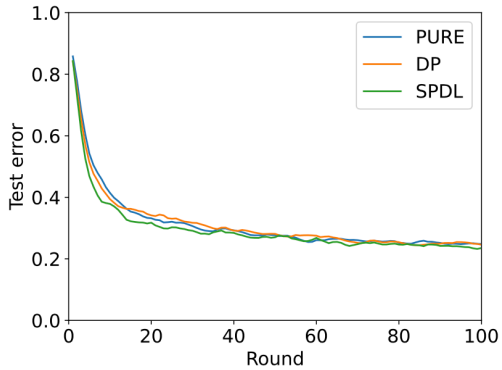
训练网络规模越大，模型收敛越稳定

目前研究表明：大模型训练会导致模型错误率升高

模型错误率（Batch Size）



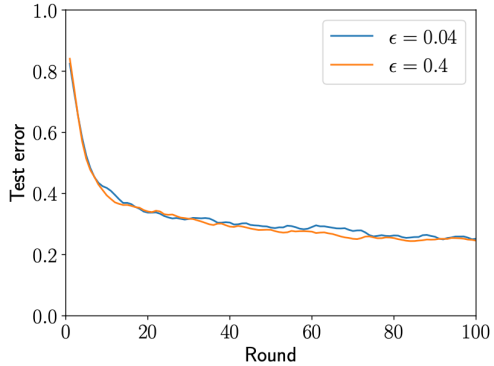
(a) $BS = 10$



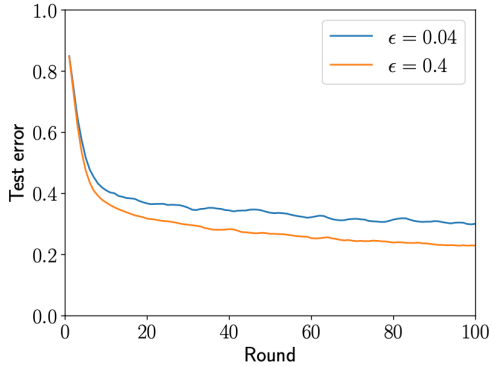
(b) $BS = 100$

增加批量大小，以确保稳定的收敛

差分隐私的参数策略：ϵ



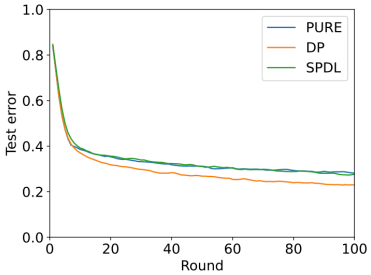
(a) $N = 10$



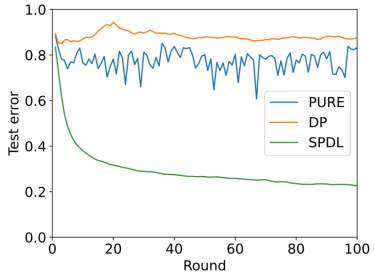
(b) $N = 20$

ϵ越大，隐私保护越强，但会造成模型错误率升高

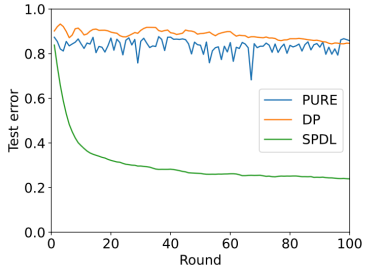
拜占庭容错性



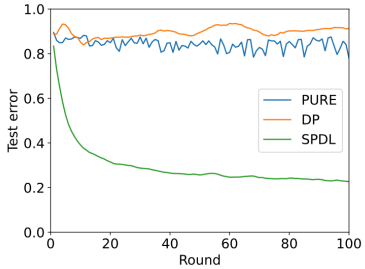
(a) $BR = 0\%$



(b) $BR = 10\%$



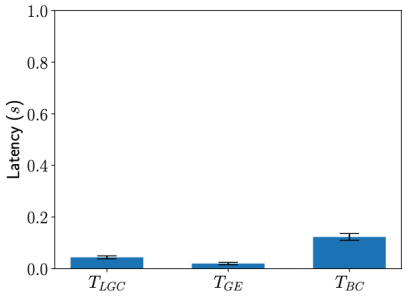
(c) $BR = 20\%$



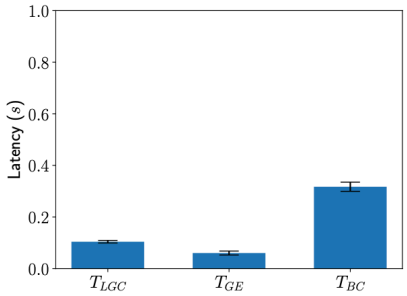
(d) $BR = 30\%$

对于不同程度的拜占庭式攻击，SPDL仍然可以提供相同的收敛性

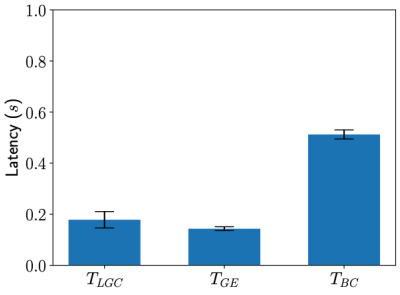
各阶段时间开销



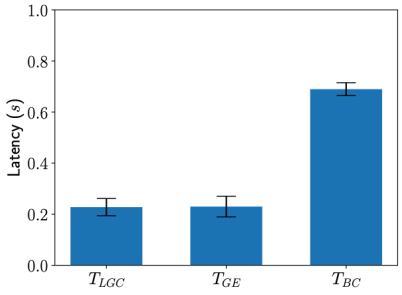
(a) $N = 4$



(b) $N = 10$



(c) $N = 20$



(d) $N = 30$

- local gradient computation plus adding noise whose overall time overhead is denoted by TLGC
- gradient exchange (TGE),
- blockchain consensus (TBC).

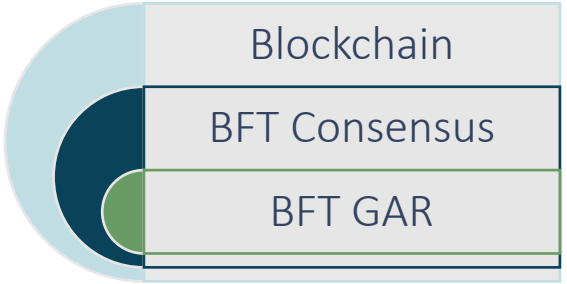
- 实验中区块链共识时间高于训练时间，但随着模型复杂度升高，区块链共识时间带来的延迟相对较小

04 总结展望

总结

1. SPDL引入区块链系统提供了信任与激励，以便构建**更大范围的去中心化学习网络**（小范围训练甚至无须使用区块链）

2. 为区块链、BFT共识，BFT GAR找到了一种**有机融合的切入点**，即统一的“拜占庭容错”特性。



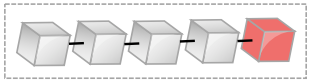
3. 更为全面的隐私保护，**不仅是数据隐私**（差分隐私），也包含身份隐私（环签名、匿名网络、区块链）

展望前景

适用于大型分布式学习场景

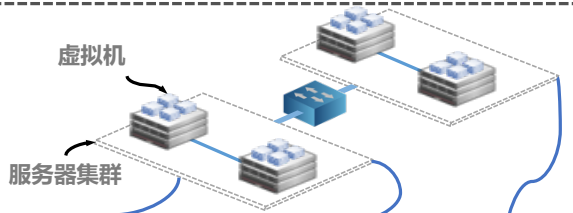
零信任假设下，需要强大的安全性和隐私保障

主要成果



区块链

云



CloudChain [TC’ 21] ✓ 云区块链

边

SandyChain [原型系统] ✓ 工业级区块链原型系统

SPDL [TC’ 21] ✓ 边缘可信智能
Curb [ICDCS’ 22] ✓ 边缘可信组网

TEMS [TC’ 20] ✓ 链下可信延伸

端

无线设备

wChain [TWC’ 21] ✓ 无线区块链（多跳）

BLOWN [TMC’ 22] ✓ 无线区块链（单跳）

Q & A

敬请批评指正

mhxu@sdu.edu.cn