区块链安全与隐私

小组成员：徐一博 赖其才 周慧文 白恒瑞

区块链是什么

定义

- 是一个由多方参与共同维护的持续增长的分布式数据库，也称为分布式共享账本。
- 核心在于通过分布式网络、时序不可篡改的密码学账本及分布式共识机制建立彼此之间的信任关系
- 利用自动化脚本组成的智能合约来编程和操作数据，最终实现信息互联向价值互联的进化。

优势

- 分布式结构：

  相比现在中心化结构的信息管理形式，能够有效的减少数据泄露，外部攻击的风险

- 信任机制：

  不需要借助第三方权威机构信用背书达到共识，建立信任关系，能够减少大量成本

- 公开透明

  任何人都可以加入区块链，也能查询到区块链上的记录

- 时序不可篡改

  具有极强的可追溯性和可验证性，由密码学和共识机制保证了区块链的不可篡改性

引用论文

Top Ten Obstacles along Distributed Ledgers' Path to Adoption
Sarah Meiklejohn

Tyranny of the Majority: On the (Im)possibility ofCorrectness of Smart Contracts
Lin Chen, Lei Xu, Zhimin Gao, Yang Lu, and Weidong Shi

区块链技术存在的问题及潜在解决方式

问题

- 治理问题：谁制定规则？
  - Satoshi Oath
  - 智能合约
  - 博弈论
  - 奖惩机制
- 如何减少成本？
  - proof of stake
- 钥匙管理：如何防止丢失和偷窃？
  - 多重签名

治理问题：谁制定规则？

智能合约正确的可能性

- **智能合约的现有模型的局限性**
- 工作量证明（Proof of Work）
- 权益证明（Proof of Stake ）

  —拜占庭容错协议(BFT)

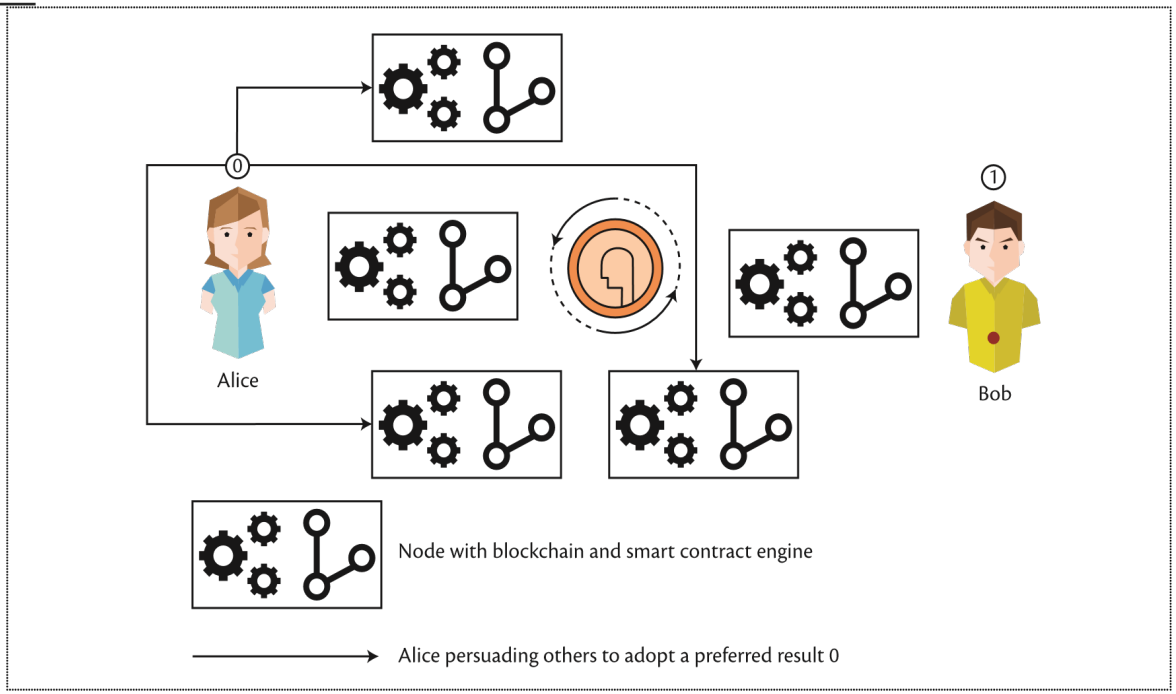


Figure 2. A smart contract involving flipping of a coin. The coin-flipping result determines the outcome of the smart contract; a participant can try his or her best to lead the system to accept his or her preferred result and maximize his or her profit.

治理问题：谁制定规则？

智能合约正确的可能性

- **博弈论**
- **设计合理的奖惩机制**
  - 纳什均衡行为模式
  - 超理性行为模式
  - 有限理性行为模式

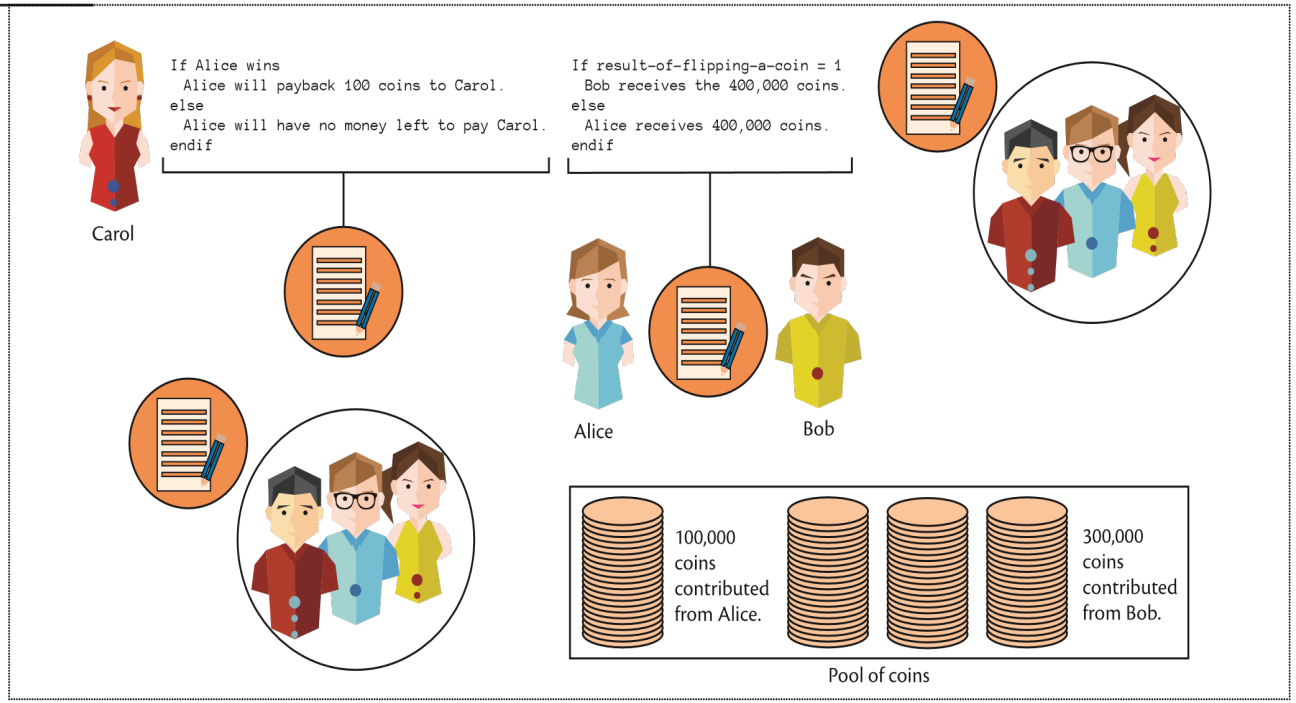


Figure 3. A smart contract involving a large number of indirect participants with economic interests tied to the current contract execution. Alice can have other contracts with participants other than Bob.

区块链技术存在的问题及潜在解决方式

问题

- 可扩展性：如何减少存储量？
  - SPV，闪电网络，账户分区
- 可扩展性：每个节点需要全部同意吗？
  - 分区，只接受和自己直接相关交易的共识
- 可用性问题：为什么要用分布式记账系统？
  - 提高产业链透明度
- 如何保护隐私？
  - 和信任的对手交易，信息可见性控制

引用论文

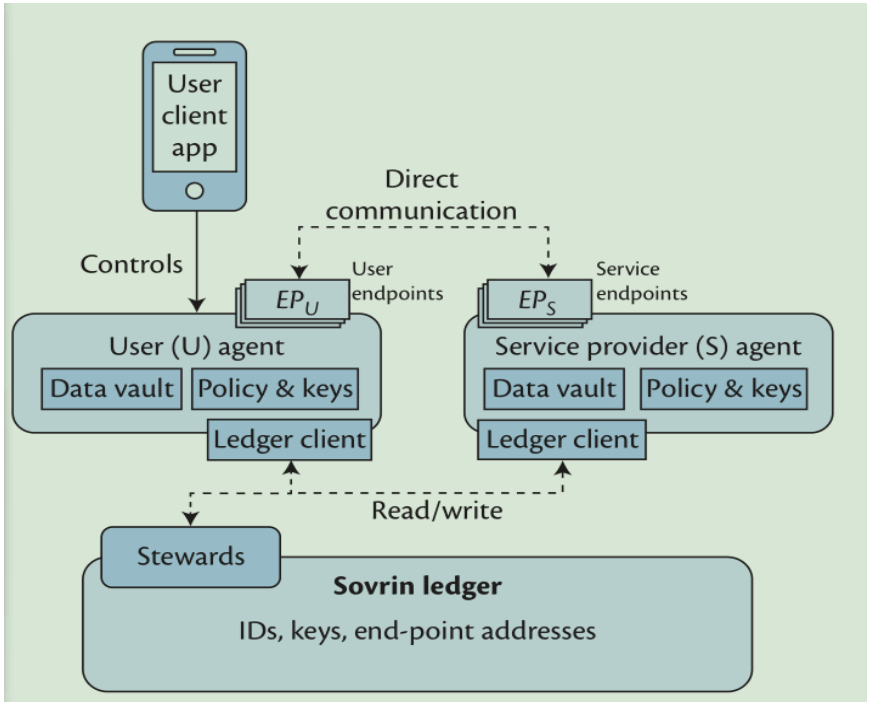
A First Look at Identity Management Schemes on the Blockchain

Paul Dunphy and Fabien A.P. Petitcolas

区块链解决隐私问题的具体应用Sovrin

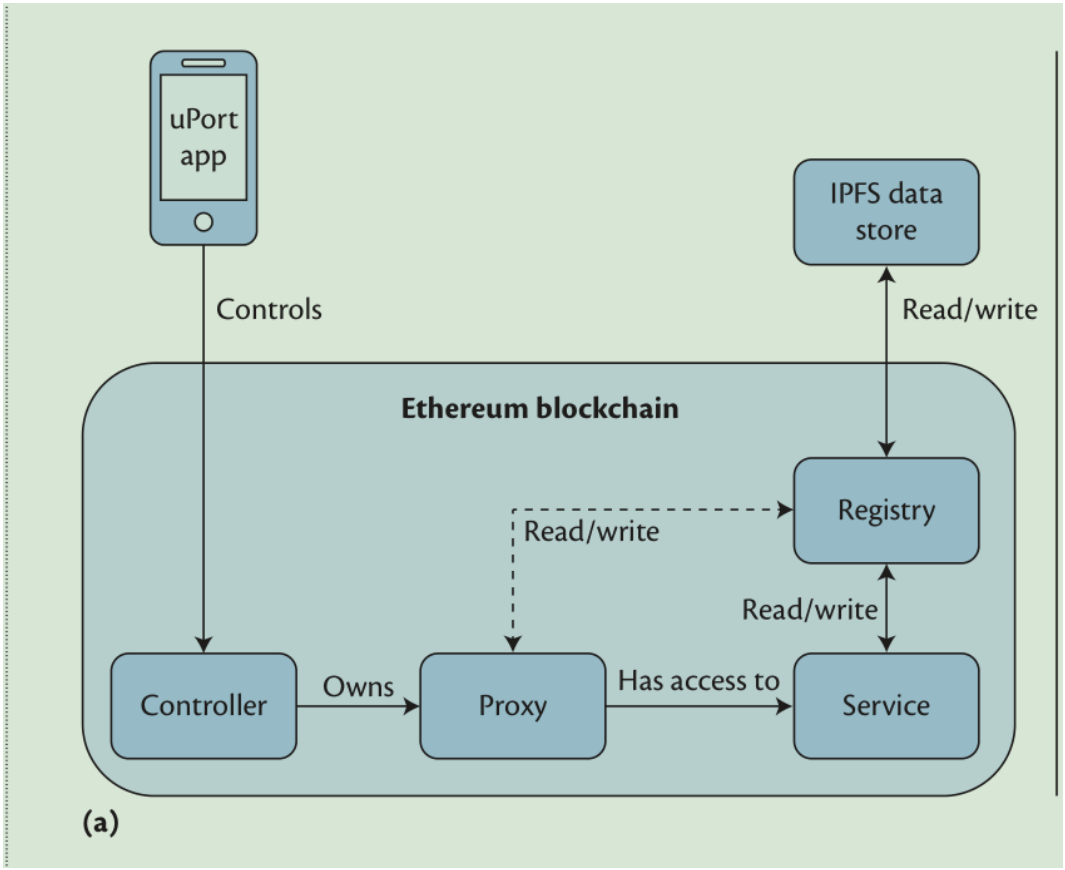
设计

- 分布式账本
- 可信机构（如政府、银行）
- 客户端应用与网络节点进行交互



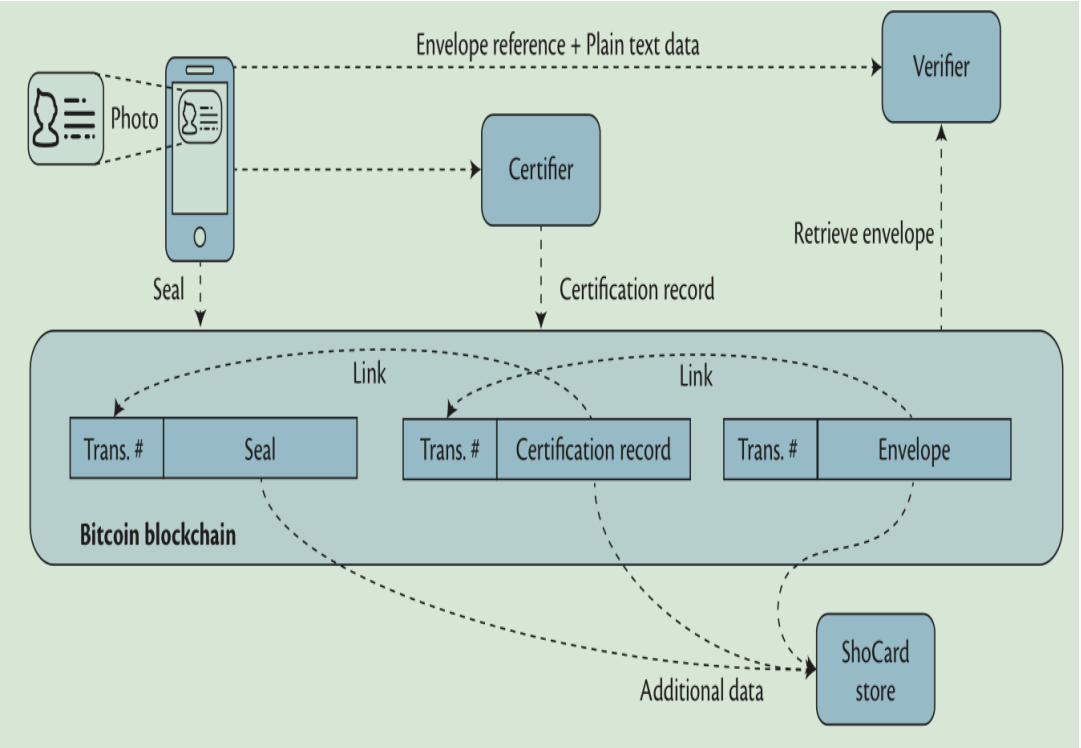
区块链解决身份验证问题的具体应用uPort

- 以太坊智能合约
- 以太坊虚拟机
- 控制方和代理方
- 非对称加密钥匙对
- 信息保留客户端



区块链解决身份验证问题的具体应用shoCard

- 比特币时间戳
- 用户相机
- 面对面环境
- 可选择透露性



隐私管理目前面临的障碍

- 可用性

虽然采用区块链技术能有效增强用户隐私管理的安全性，但是这其中的复杂操作给用户带来了一些麻烦，导致在用户里的推广会带来问题，所以如何增强用户体验是目前急需解决的问题。

- GDPR规则下的存储

采用区块链技术意味着信息的透明性，在GDPR出台之后，它对用户个人数据的存储有着严格的规定，而区块链的分布式账本的设计，使得信息必须得被多次大量的存储，这两者的矛盾，也是目前此技术推广所需要考虑的问题。

引用论文

BlockChain: A Distributed Solution to Automotive Security and Privacy

Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak

区块链技术与智能车辆产业的结合

智能车辆面临威胁

智能车辆越来越多地连接到路边基础设施（例如，交通管理系统），接近其他车辆，并且更一般地连接到因特网，从而将车辆结合到物联网（IoT）中。 这种高度连接性使得确保智能车辆的安全性的需要特别大。 恶意实体可能危及车辆，这不仅危及车辆的安全性，而且危及乘客的安全。 Miller和Valasek使用信息娱乐系统的无线接口对Jeep Cherokee进行了复杂的攻击，从而能够远程控制车辆的核心功能。 由车辆交换的数据包括敏感数据（例如，位置），因此可以开启新的隐私挑战。

区块链技术与智能车辆产业的结合

当前挑战

- 由于以下挑战，智能车辆中使用的传统安全和隐私方法往往是无效的。
- 集中化：当前的智能车辆架构依赖于集中式代理通信模型，其中所有车辆都通过中央云服务器进行识别，验证，授权和连接。 随着大量车辆的连接，这种模式不太可能扩展。 此外，云服务器仍将是一个瓶颈和单点故障，可能会破坏整个网络。
- 缺乏隐私：大多数当前的安全通信体系结构要么不考虑用户隐私-例如，他们在未经所有者许可的情况下交换车辆的所有数据，或向请求者显示噪声或汇总数据。 然而，在若干智能车辆应用中，请求者需要精确的车辆数据来提供个性化服务。
- 安全威胁：智能车辆具有越来越多的自动驾驶功能。 由于安全漏洞（例如，通过安装恶意软件）导致的故障可能导致严重事故，从而危及乘客以及邻近的其他道路使用者的安全。

区块链技术与智能车辆产业的结合

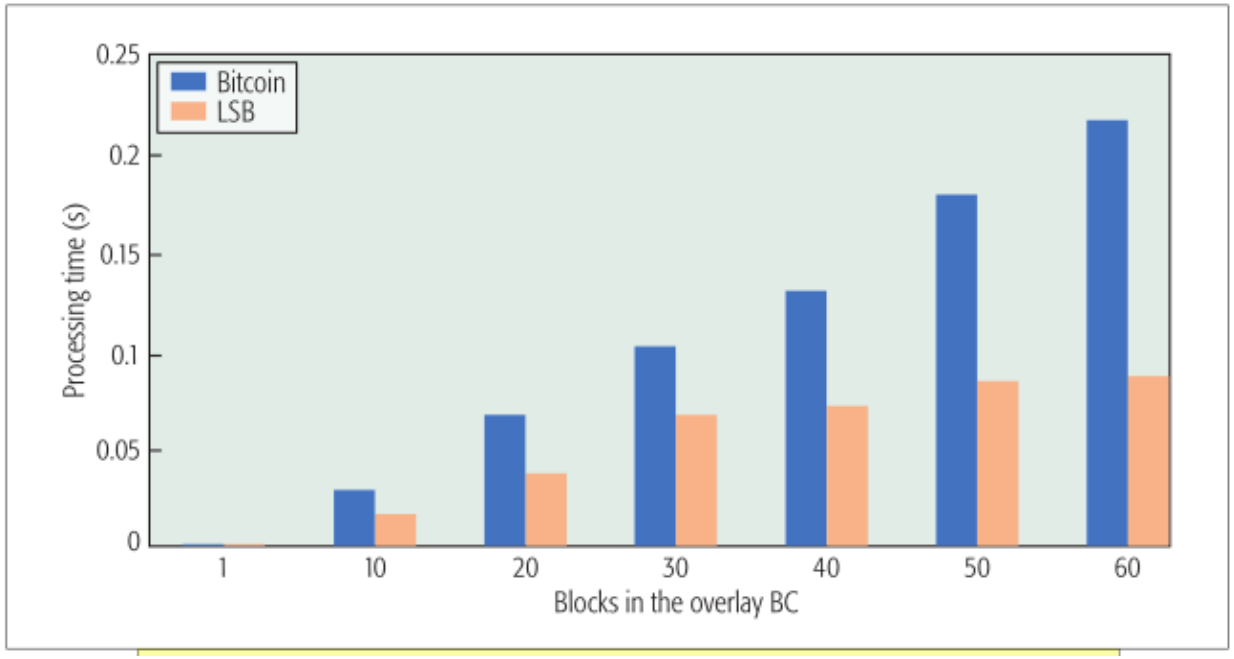
LSB实例

有计划的块生成过程消除了传统BC的显着处理开销。

分布式吞吐量管理方法（DTM）动态调整吞吐量

分布式验证算法减少与验证块相关的处理时间

为了解决可扩展性挑战，LSB对网络进行集群，并且只有CH（即OBM）管理BC。



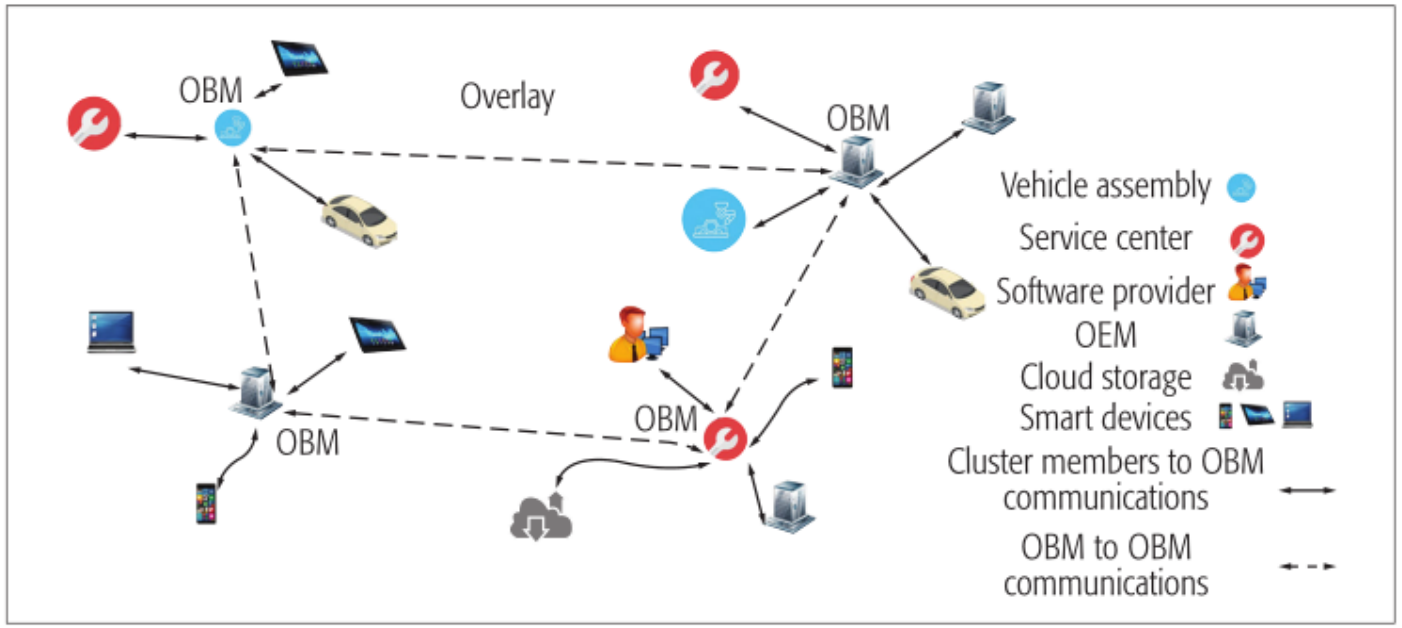
区块链技术与智能车辆产业的结合

区块链架构

OBM：所有交易都会广播到所有OBM。 OBM通过验证附加的签名来检查收到的交易的有效性。

密钥列表：每个OBM维护一个PK对列表（实质上是访问控制列表），该列表建立允许彼此通信的节点。

软切换：当车辆移动到新位置时，它会测量其附近的多个OBM的通信延迟。选择具有最低延迟的OBM作为新OBM。



THANK YOU