Blockchain privacy and security

方宇彤 罗景升 余道清 刘宸硕

北京大学

区块链：一个共享的、分布式的交易分类账，每一个事务通过一个节点网络进行验证。在一个节点网络中，每个节点都有区块链的副本信息，每个节点都能全部或部分维护大平台的功能。

Lazooz分布式拼车网络：网络中的参与者产生“Zooz”令牌，用于补偿司机，每笔交易都记录在区块链的节点网络中。

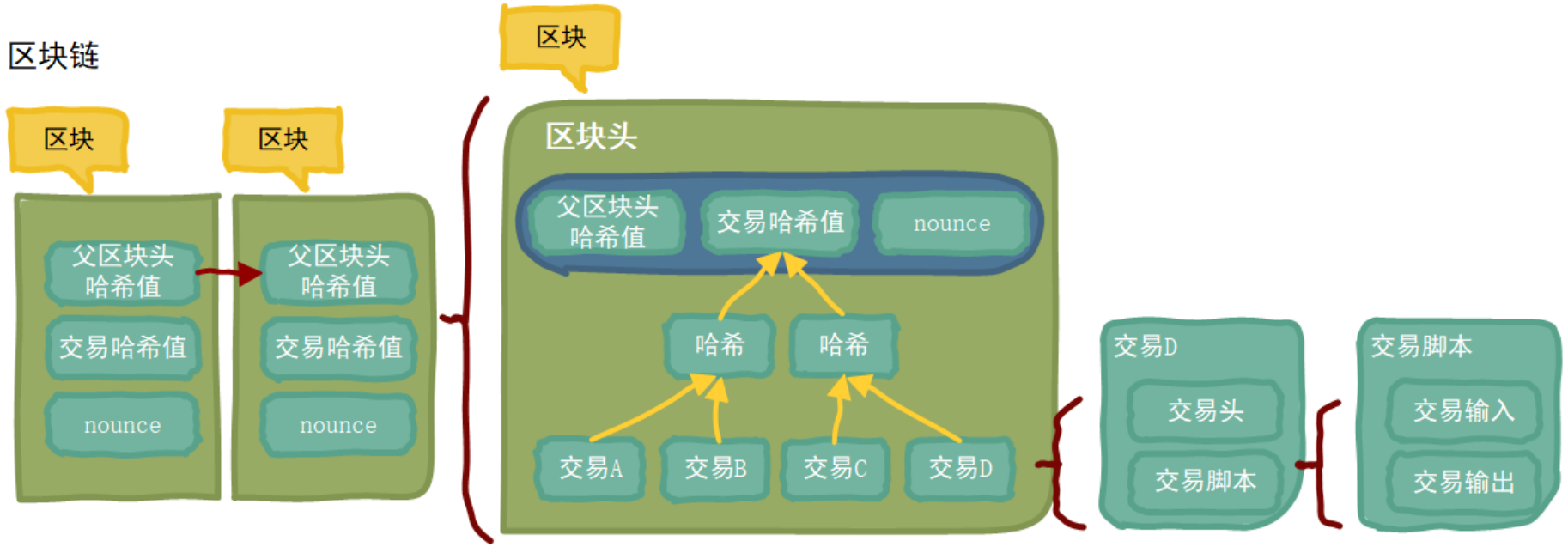
OpenBazaar通过比特币支付商品和服务，为参与者提供伪匿名交易，保证服务质量和安全

北京大学

去中心化的基于区块链的电子市场

市场特征	基于区块链的去中心化市场	传统电子市场
买卖双方	1、每个节点列出商品相关信息，个体销售者自己创建列表，冗余分布在网络中。 2、价格更改等算法不由单个卖家管理，错误降至最低。	1、有控制能力的公司以利益最大化为原则为类似产品实施差异化定价。 2、买卖双方的行为影响着市场地点的决策，某些控制公司决定停止接受某些支付方式。
交易情况	1、中介被排除在外，由加密货币直接交易，节约成本。 2、匿名和隐私功能减少了对个人账户信息的攻击。 3、买卖双方声誉独立于市场管理，公正、仲裁机制。	1、信贷、银行等部门的存在产生额外的交易成本。 2、真实身份和交易细节被盗用 3、买卖双方的声誉系统受到恶意攻击。
机构的基础设施	1、通过网络节点确定买卖双方遵守的合同和规范。 2、合同的全自动化、部分自动化和手工执行模式确保参与者的执行。	1、通过验证支付与商品的交换来履行合同。 2、外包劳务合同涉及大量交易成本。

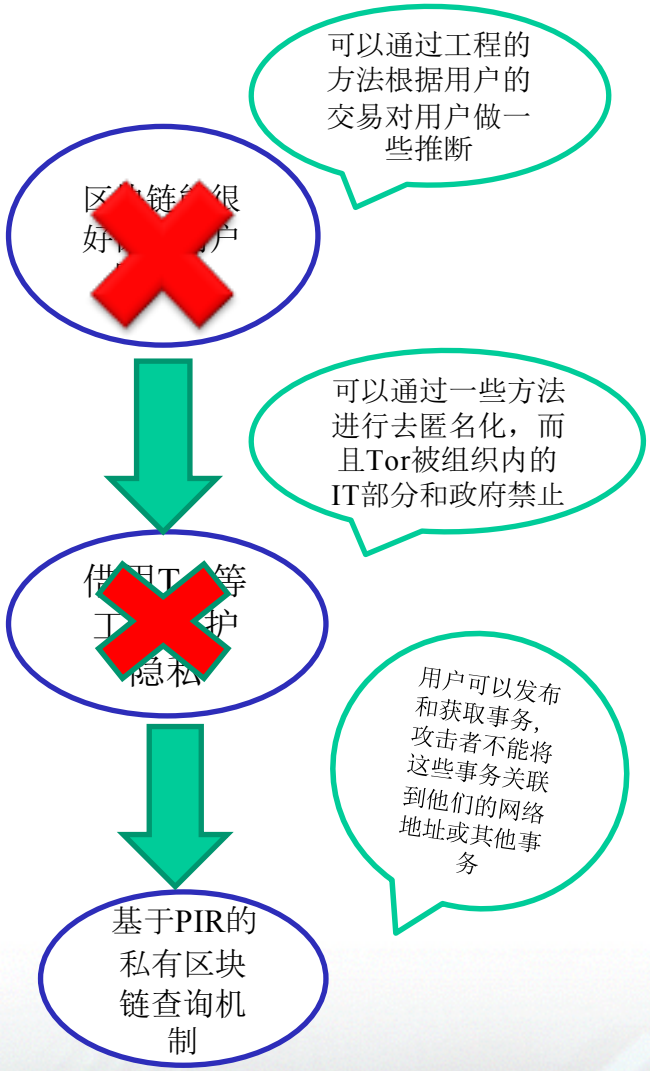
比特币世界的核心构成部分：区块链



当两大加密机制受到攻击：哈希、签名

- 主哈希
  - 冲突攻击：比特币失窃
  - 第二原像攻击：双重花费与比特币失窃
  - 原像攻击：区块链系统的全面崩溃
- 地址哈希
  - 冲突攻击：拒绝支付
  - 第二原像攻击：拒绝支付
  - 原像攻击：揭露地址
- 签名机制
  - 选择性篡改：比特币失窃
  - 完整性攻击：收到币后声称未收到
  - 拒绝攻击：改变现有交易

Blockchain Access privacy: Challenges and Directions



Blockchain Access privacy: Challenges and Directions

建议：

（1）推荐采用精心设计的比特币通信基础设施来改善用户公告的匿名性。P2P匿名通信网络可以结合一些现有的学术研究做为研究点,比如Pisces。

（2）对于许可的区块链系统主张通过将达成交易的共识流程与混合用户公告的过程相结合来提高效率并降低开销，建议开发量身定制的解决方案。

（3）SPV方法有缺点，可能向整个节点显示其公共地址的完整列表，缺乏匿名性,推荐通过PIR解决。

（4）PIR现在发展还不成熟，私有地将区块链交易纳入实践仍然需要一些基础研究和相当实质性的工程和实施努力。提出了一种方法来助于PIR进行查询。

背景：

1、量子计算快速发展，第一批量子计算机未来十年将投产

2、使用的哈希函数以及加密函数存在被攻破的可能

区块链使用的技术：

1、哈希函数：

单向性

碰撞避免

伪随机性

2、默克尔树

3、区块链协议

4、区块链公钥基础设施

PQChain：具体设计思想

1、将区块链协议与线下认证服务结合

具体步骤：

将一个有状态的签名架构转换为不需要维护用户状态的架构

使用区块链技术解决了签名数量有限制的问题

交易可追踪

2、如何保持长期稳定安全

具体想法：

最小安全假设：只依赖哈希函数的安全性

哈希结合

哈希函数代替

Thank you

北京大学