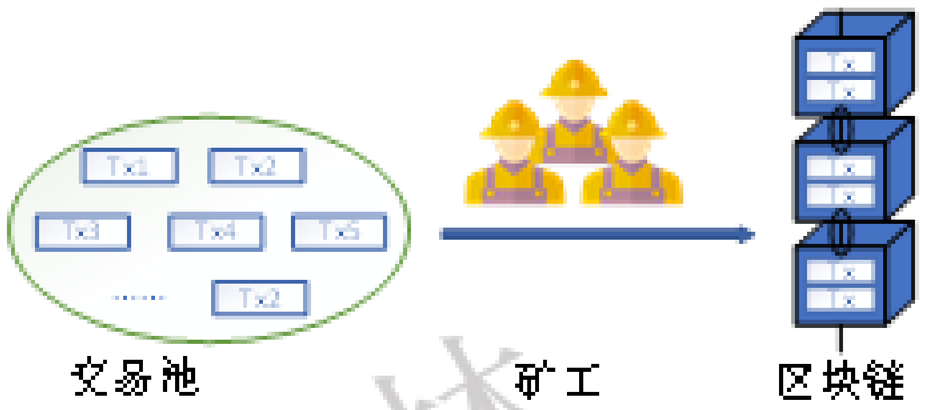
北京交通大学
BEIJING JIAOTONG UNIVERSITY

构建韧性安全的区块链系统

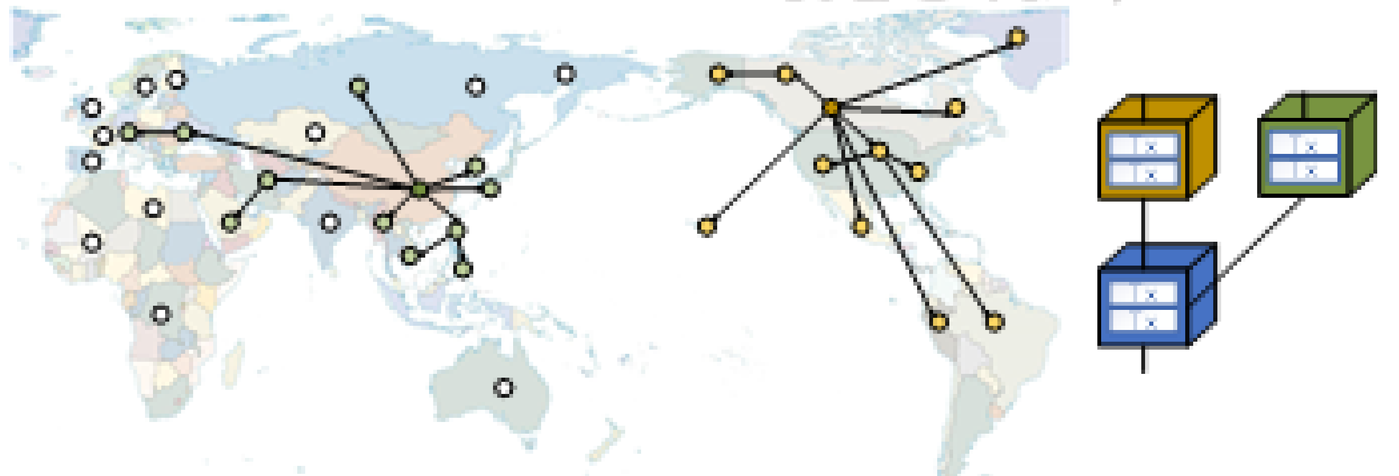
分析区块链网络的可用性，并研究区块链中主要的攻击。

◆区块链网络可用性分析

➢研究以比特币为代表的区块链网络可靠性。分析网络中节点连接数目、网络传输延迟、区块大小等因素，对区块链网络可靠性的影响，可靠性分析包括对分叉概率、分叉持续时间、交易和区块的处理速度等指标的评估。



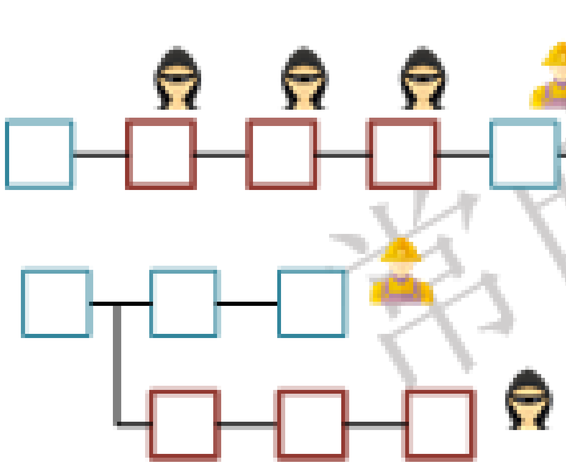
矿工将交易池中的交易打包记录到区块链



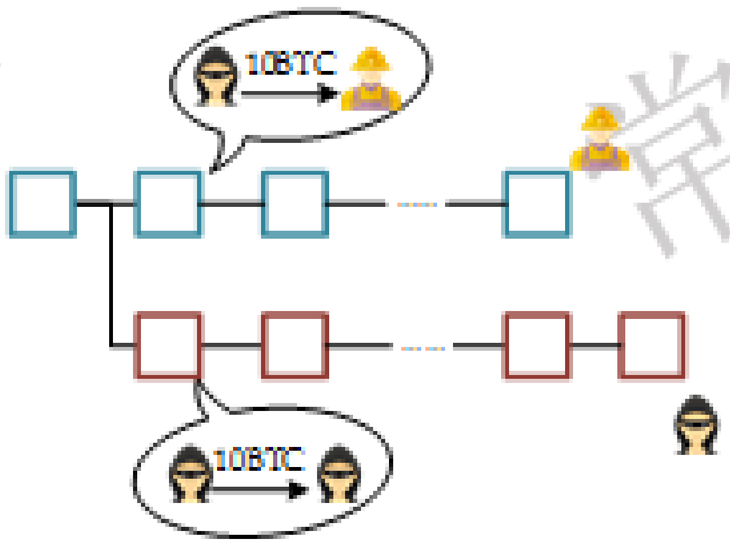
同时产生区块时，区块链产生分叉

◆区块链攻击分析

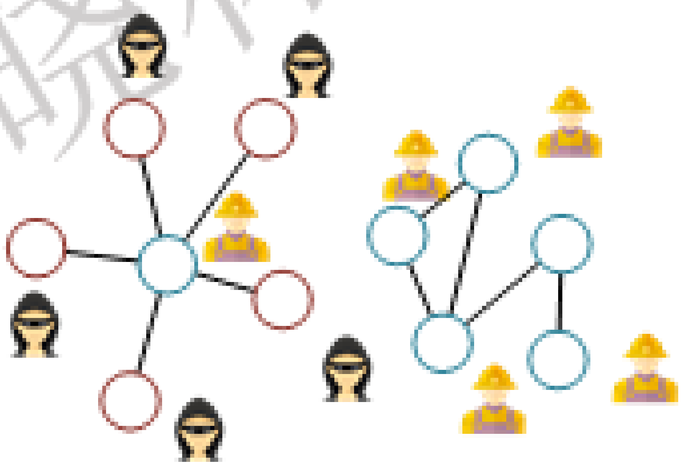
➢研究了在区块链系统中，常见的攻击（包括双花攻击、自私挖矿、日蚀攻击、平衡攻击和块扣留攻击等）对系统公平性（如矿工收益）、性能（如吞吐量）以及安全性（如抵抗其他攻击能力）的危害，并考虑网络延迟和区块链协议对攻击的影响。



自私挖矿：有策略地公布区块创建更长的链使诚实矿工损失



双花攻击：通过创建一条更长的链将已转出的币转给自己



日蚀攻击： 攻击者将某些矿工与其他矿工隔离

部分研究成果发表于IEEE TNSE (SCI 1区), IEEE TNSM (SCI 2区)， COSE(SCI 3区, CCF B类)等期刊。