区块链网络中抗多样化矿工行为攻击的安全多链共识方案

张文波[1]，汪涛[1,2]，张朝阳[1]，冯景瑜[1]
[1]西安邮电大学网络空间安全学院，中国西安市，710121
[2]中国邮政储蓄银行，中国西安市，710000

摘要：跨链技术的发展使得不同区块链间的互操作成为可能，多链共识在区块链网络中变得日益重要。然而，目前对单链共识方案的研究较多，涉及可信矿工的多链共识方案的探讨相对较少，这为恶意用户在不同链上发起多样化矿工行为（diverse miner behavior, DMB）攻击提供了机会。DMB攻击者可以在某些链（称为mask链）上表现友好并参与共识过程，以提升其信任值，而在其他链（称为kill链）上从事对网络具有破坏性的行为。本文提出一种名为Proof-of-DiscTrust（PoDT）的多链共识方案，旨在防范DMB攻击。该方案引入DiscTrust信任理念，用于评估每个用户在不同链上的信任值。用户的信任值被分为本地信任值和全局信任值。针对DMB攻击者通过在kill链上交替创建真实或虚假区块来维持其信任度的问题，设计了一种实施DiscTrust机制的动态行为预测方法。此外，针对多链环境，提出3个可信矿工选择算法，分别用于选择网络矿工、链矿工和链矿工领导者。实验结果表明，PoDT方案能够抵抗DMB攻击，并且在多链环境中比传统共识方案更为有效。

关键词：区块链；跨链；信任机制；多链共识
https://doi.org/10.1631/FITEE.2200505