When Intrusion Detection Meets Blockchain Technology: A Review

With the purpose of identifying cyber threats and possible incidents, intrusion detection systems (IDSs) are widely deployed in various computer networks. In order to enhance the detection capability of a single IDS, collaborative intrusion detection networks (or collaborative IDSs) have been developed, which allow IDS nodes to exchange data with each other. However, data and trust management still remain two challenges for current detection architectures, which may degrade the effectiveness of such detection systems. In recent years, blockchain technology has shown its adaptability in many fields such as supply chain management, international payment, interbanking and so on. As blockchain can protect the integrity of data storage and ensure process transparency, it has a potential to be applied to intrusion detection domain. Motivated by this, this work provides a review regarding the intersection of IDSs and blockchains. In particular, we introduce the background of intrusion detection and blockchain, discuss the applicability of blockchain to intrusion detection, and identify open challenges in this direction.