The Summer Undergraduate Research Fellowship (SURF) Symposium
2 August 2018
Purdue University, West Lafayette, Indiana, USA

Exploring Confidentiality Issues in Hyperledger Fabric Business Applications

Shivam Bajpayi, Pedro Moreno-Sanchez, Donghang Lu, Sihao Yin
Department of Computer Science, Purdue University

ABSTRACT

The rise of Bitcoin and cryptocurrencies over the last decade have made its underlying technology (blockchain) come into the spotlight. Blockchain is a secure ledger of linked records called blocks. These records are cryptographically immutable and any tampering with the block is evident through a change in the cryptographic signature of the block. Among the blockchains deployed in practice today, Hyperledger Fabric is a platform that allows businesses to make use of blockchains in their applications. However, confidentiality issues arise with respects to the blocks in this blockchain network due to the fact that blocks might contain sensitive information accessible to all peers with a copy of the blockchain. In this work, we aim to address the confidentiality issue present in current Hyperledger Fabric. Our current approach consists of leveraging cryptographic techniques to ensure the confidentiality of the shared data in the blockchain along with crafted access control policies so that only authorized peers can access the otherwise concealed data. This becomes a crucial requirement especially with business models that require their transaction information to be concealed. Recent results show that the use encryption along with interesting access control policies allow obfuscation of data for desired outside entities, although more work is required.

KEYWORDS
Blockchain, Hyperledger, Confidentiality