Informatics Institute of Technology

In Collaboration with

University of Westminster, UK

Access Controlled Permissioned Blockchain

A dissertation by

Dewni Matheesha Weeraman

Supervised by

Mr. Sudharshana Welihindha

Submitted in partial fulfillment of the requirements for the

BEng (Hons) in Software Engineering

Department of Computing

May 2019

Abstract

Today, data privacy is being talked more than ever, and access controlling to improve this has become a high priority in business-centric enterprise applications. Many regulatory concerns are arising resulting of an increase in imposing laws to ensure the right amount of data is exposed to the relevant parties. In recent times, the blockchain technology has received much attention due to its tamper-proof property of record-keeping in a distributed ledger operating in a trustless environment. The original blockchain platform was of the intention of having a peer to peer network operating in a complete decentralized and anonymous manner. Later on, studies were conducted to research on the potential of blockchain, beyond its original application in bitcoin, to disrupt the traditional business practices. Many researches revealed that blockchain has the potential to reduce the required amount of trust expected in business interactions. However, it should be noted that businesses are concerned about having some control over the blockchain in being able to perform certain restrictions adhering to their business processes. The original platform architecture cannot decipher such concerns.

The aim of this thesis is to analyze how privacy related issues are being addressed in blockchains from the enterprise domain perspective. To answer this question, various existing blockchain models which have evolved in the spectrum of public vs. private and permissioned vs. permission-less aspects are compared in the level of privacy presented in terms of access control. Findings revealed that the enterprise domain is more focused towards private permissioned approach. However, there is a need to explore more on the granularity of the access control levels provided by these blockchains. In this research, a variation of private permissioned blockchain is introduced with hierarchies of access control to support the flexibility expected in enterprise level for transaction management.

Keywords: Blockchain, Distributed ledger, Access control, Transaction management, Privacy