Self-Sovereign Identity using Smart Contracts on the Ethereum Blockchain

Zachary Diebold, Master in Computer Science

University of Dublin, Trinity College, 2017

Supervisor: Dr. Donal O'Mahony

Centralised identity services that exist today fail to operate transparently and protect the rights of users. Single points of trust present constant operational risks for both companies and individuals. Self-sovereign identity is a solution to address this, which specifies a user-focused approach that gives full control of an identity back to the individual. This paper proposes the blockchain, a secure and decentralised trust-less system, as the platform to achieve this. A proof-of-concept identity system for the *Ethereum blockchain* is designed and developed in this paper. *Smart contracts* are used to facilitate the secure storage and open processing of user data. It also presents a novel approach to the secure recovery of encrypted private data. Emphasis is placed on the implementation security, information privacy and data recovery procedures of the system.