國立交通大學

網路工程研究所

碩士論文

初稿

基於區塊鏈的身分管理及存取控制

Blockchain-based identity management and access control with LDAP

研 究 生：鄭人豪

指導教授：袁賢銘 博士

中 華 民 國 110 年 7 月

基於區塊鏈的身分管理及存取控制

Blockchain-based identity management and access control with LDAP

研 究 生：鄭人豪　　Student: Jen-Hao Cheng
指導教授：袁賢銘　　Advisor: Shyan-Ming Yuan

國 立 交 通 大 學
網 路 工 程 研 究 所
碩 士 論 文 初 稿

A Thesis Draft
Submitted to Institute of Network Engineering
College of Computer Science
National Chiao Tung University
in partial fulfilment of the requirements
for the Degree of
Master
in

Computer Science

Sep 2021

Hsinchu, Taiwan

中 華 民 國 110 年 7 月

基於區塊鏈的身分管理及存取控制

學生：鄭人豪　　指導教授：袁賢銘 博士

國立交通大學 網路工程研究所

摘　　要

隨著社群平臺愈來愈普及，多數網站提供第三方登入 (social login)，讓初次使用的用戶可以用第三方平臺現有的帳號完成註冊及登入，幫助用戶免於記下不同網站的帳號及密碼，亦不用填寫繁雜的註冊表單。對於用戶而言，可以達到更好的用戶使用體驗；對於應用程式開發人員而言，不必自行管理個資、建立會員系統，由第三方平臺負責管理，而當需要在提供多種不同的服務時，可以使這些服務支援同一種第三方平臺驗證方式，即可達到單一登入 (SSO) 功能。

在享受如此便利的服務的同時，用戶的網路身分仍是屬於第三方平臺的，而網路公司再將使用者與第三方公司進行比對，將這些資訊加以利用，可以提供符合需求之廣告，在使用服務同時也提供了自己的個資。

然而，以太坊區塊鏈擁有防偽造、防竄改及去中心化的特性，可以安全、有效存放紀錄於鏈上，達到透明性且安全性。透過以太坊虛擬機及以太坊智能合約可以建構去中心化的應用程式，提供更完整、多樣的功能。

本篇論文提出使用以太坊區塊鏈技術，使許多獨立的公司組織聯合，透過區塊鏈技術管理用戶身分並通行於這些公司組織之中，方便用戶管理及存取資料，提供第三方登入的優點，並使得去中心化平臺成為信任的第三方，負責管理對應用戶身分並且提供存取控制之功能，同時兼具區鏈特性，提升安全性。除了驗證用戶身分功能外，亦提供用戶授權功能，用戶可以自行決定授權範圍及對象，授權對象包含第三方服務 (TSP) 業者，第三方服務業者的加入不僅需要公司組織的許可，亦須要用戶授權方可存取該用戶資料。

關鍵字: 以太坊智能合約、第三方登入、第三方服務業者

Blockchain-based identity management and access control with LDAP

Student: Jen-Hao Cheng Advisor: Dr. Shyan-Ming Yuan

Institute of Network Engineering
National Chiao Tung University

Abstract

The humanity falls when people start to drink coffee and coke ...

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

1.2 Objective

Chapter 2

Background

Here is the background.

2.1 Ethereum Smart Contract

2.2 MetaMask

Metamask is a chrome extension for accessing Ethereum distributed application (DApp), this extension can enable web3 API in website so that users can interact with any Etehereum blockchain from Javascript, e.g., Mainnet, Testnet. It also creates identities by the user themself. The user of Metamask can create and manage their identities; moreover, Metamask provides an interface that user can perform a transaction to the connected blockchain.

Because the user manages owned Ethereum account through Metamask, the user can use the key to sign transactions or sign data to prove ownership of an account.

2.3 OAuth

2.4 Trust Service Provider (TSP)

2.5 Related work

Chapter 3

System Design

Here is the design.

3.1 Scenario

For user perspective, our proposed system provide a single digital ID with Ethereum blockchain.

3.2 Workflow

- Verify unique ID stage [**?**]
- Binding account stage Figure 3.1
- Third party login stage

Figure 3.1: Test figure

Chapter 4

Implementation

This chapter describes the implementation of Ethereum blockchain smart contracts, and defines relationshup between user and organization.

4.1 User Manager

manage identity

4.2 Organization Manager

manage mapping of user and orgs

4.3 Log Manager

record event

4.4 Access Manager

manage access of data

Chapter 5

Experimental Case Study

Here are the experimental case study

Chapter 6

Demonstration

Here is the demonstration.

Chapter 7

Experimental Evaluation

Here is the evaluation.

7.1 Gas consumption

7.2 Throughput

Chapter 8

Discussion

Chapter 9

Conclusion

Here is the conclusion.

Appendix A

附錄標題

A.1 Testing