

**DEVELOPMENT OF DECENTRALIZED APPS USING BLOCKCHAIN  
TECHNOLOGY TO IMPROVE MALAYSIAN GOVERNMENT SERVICES IN  
MINISTRIES OF HOME AFFAIRS – DIGITAL IDENTITY MANAGEMENT**

**BY  
PANG YI WERN**

**A REPORT  
SUBMITTED TO  
Universiti Tunku Abdul Rahman  
in partial fulfillment of the requirements  
for the degree of  
BACHELOR OF INFORMATION SYSTEMS (HONOURS) BUSINESS  
INFORMATION SYSTEMS  
Faculty of Information and Communication Technology  
(Kampar Campus)**

**JAN 2022**

## REPORT STATUS DECLARATION FORM

**Title:** Development Of Decentralized Apps Using Blockchain Technology To Improve Malaysian Government Services In Ministries Of Home Affairs – Digital Identity Management


**Academic Session:** Jan 2022


I **PANG YI WERN**

declare that I allow this Final Year Project Report to be kept in  
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

  
\_\_\_\_\_  
(Author's signature)

  
\_\_\_\_\_  
(Supervisor's signature)

**Address:**

Sungai Long Residence,  
Jalan Sungai Long, Bandar Sungai Long,  
43000, Kajang, Selangor.

\_\_\_\_\_

Mr. Su Lee Seng  
\_\_\_\_\_  
Supervisor's name

**Date:** 22/04/2022

**Date:** 22/04/2022

Universiti Tunku Abdul Rahman			
Form Title : <b>Sample of Submission Sheet for FYP/Dissertation/Thesis</b>			
Form Number: <b>FM-IAD-004</b>	Rev No.: <b>0</b>	Effective Date: <b>21 JUNE 2011</b>	Page No.: <b>1 of 1</b>

**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY**  
**UNIVERSITI TUNKU ABDUL RAHMAN**

Date: 21/04/2022

**SUBMISSION OF FINAL YEAR PROJECT /DISSERTATION/THESIS**

It is hereby certified that **Pang Yi Wern** (ID No: 1801768) has completed this final year project/ dissertation/ thesis\* entitled “**Development Of Decentralized Apps Using Blockchain Technology To Improve Malaysian Government Services In Ministries Of Home Affairs – Digital Identity Management**” under the supervision of Mr. Su Lee Seng from the Department of Digital Economy Technology, Faculty of Information and Communication Technology.

I understand that University will upload softcopy of my final year project / dissertation/ thesis\* in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.


Yours truly,



(Pang Yi Wern)

## DECLARATION OF ORIGINALITY

I declare that this report entitled “**DEVELOPMENT OF DECENTRALIZED APPS USING BLOCKCHAIN TECHNOLOGY TO IMPROVE MALAYSIAN GOVERNMENT SERVICES IN MINISTRIES OF HOME AFFAIRS – DIGITAL IDENTITY MANAGEMENT**” is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature :  \_\_\_\_\_

Name : Pang Yi Wern

Date : 22/04/2022

## **ACKNOWLEDGEMENTS**

I would like to express my sincere gratitude and appreciation to my supervisor, Mr. Su Lee Seng, who has given me this bright opportunity and endless support to engage in a Blockchain-based project. His advice and guidance have assisted me throughout the stages of my project. I really gained a wholesome experience while learning and exploring something new and unfamiliar. A million thanks to you for trusting me.

Furthermore, my proposed project may not be accomplished successfully without the support from my Blockchain project teammates including Gunn Wei Teong, Laan Wei Yi, Lim Jason and Chew Jia Lun – thank you for the help during the hard times of the development process! Glad to be part of the Blockchain team with you guys.

Finally, to my parents and family, I really am grateful and appreciated for their support, unconditional love, and continuous encouragement throughout the project journey.

## **ABSTRACT**

In this project, it proposes the development of decentralized identity management system using Blockchain technology. This proposed project focuses on improving Malaysia government services in Ministries of Home Affairs in terms of better safeguarding and managing user's identity claims or documents. Nowadays, whether the way of identification is through physical or digital, there are still some challenges during the management process that exist both physically and electronically. Problems faced by existing identity management system including risks of data breaches, abuse of trust issues and over-relying on middleperson. This shows that security, trust, and convenience are important factors to make the identification process tamper resistant, trustable and cost and time effective.

The emergence of blockchain distributed ledger technology is having the potential to enhance transparency, trust in record keeping, user control in transactions that involve identity information and decentralization in identity management. It is having a bright future in the upcoming years and has been increasingly used and improved up till now. The characteristics like transparency, trust and tamper resistant has revolutionized different aspects including business, government and political interactions, social and any other value exchanging mechanisms. Blockchain ensures that governmental procedures and business transactions are highly secured, trustable, effective, and efficient. Therefore, Blockchain technology is selected to improve Malaysia government services in terms of identity management. The scope of the project will be log-in interface to control access of different roles, verification procedure to ensure validity of user's registered claims, user and government are connected in one system, and user having self-sovereign identity.

This project has also reviewed other existing blockchain identity management system in order to evaluate the strengths and weakness of other systems and apply those strengths and improve the weakness through my proposed project. The methodology used in this project is prototyping-based methodology, which is under the rapid application development (RAD) methodology category. The tools or technologies involved in the project are visual studio code for the web application development, Metamask extension on web browser for the Ethereum tesnet

connection and Infura service public API that offers the ability to get access to a node that is hosted on the Rinkeby network.

There are three main roles in the proposed blockchain identity management system which are user, issuing authority and service provider. All three roles are connected in one system. Users can register and manage their identity claims by having self-sovereign identity. Issuing authority will be responsible in verifying user's registered identity claims to prove the validity of the claims. While for service provider, before accessing user's identity claims, they are required to send access request to users for their approval to access their claims. Metamask accounts are required to logged-in to allow all process of the system work effectively.

In conclusion, at the end of the project, the proposed system will be able to solve all problems stated in existing identity management system which are risks of data breaches and identity thefts, abuse of trust issues that results in lack of trust in business parties and over-relying on middle person issue.

## **TABLE OF CONTENTS**

<b>TITLE PAGE</b>	<b>i</b>
<b>REPORT STATUS DECLARATION FORM</b>	<b>ii</b>
<b>FYP THESIS SUBMISSION FORM</b>	<b>iii</b>
<b>DECLARATION OF ORIGINALITY</b>	<b>iv</b>
<b>ACKNOWLEDGEMENTS</b>	<b>v</b>
<b>ABSTRACT</b>	<b>vi</b>
<b>TABLE OF CONTENTS</b>	<b>viii</b>
<b>LIST OF FIGURES</b>	<b>x</b>
<b>LIST OF TABLES</b>	<b>xiv</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xv</b>
<b>CHAPTER 1 INTRODUCTION</b>	<b>1</b>
1.1 Problem Statement and Motivation	1
1.2 Objectives	3
1.3 Project Scope and Direction	6
1.4 Contributions	9
1.5 Report Organization	11
<b>CHAPTER 2 LITERATURE REVIEW</b>	<b>12</b>
2.1 Review of the Technologies	12
2.2 Review of the Existing Systems/ Applications	16
2.2.1 Interoperable Blockchain Solution For Digital Identity Management	16
2.2.2 uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain	18
2.2.3 ShoCard Blockchain-Based Identity Management System	21
2.2.4 A Comprehensive Integration of National Identity with Blockchain Technology	24
2.2.5 Summary	26



<b>CHAPTER 3 SYSTEM METHODOLOGY/APPROACH (FOR DEVELOPMENT-BASED PROJECT)</b>	<b>29</b>
3.1 System Design Diagram/Equation	29
3.1.1 Use-Case Diagram for Proposed Blockchain Identity Management System	29
<b>CHAPTER 4 SYSTEM DESIGN</b>	<b>34</b>
4.1 System Flowchart Design	34
4.2 System Flowchart Design Description	37
4.3 Graphical User Interface of Blockchain Identity Management System	40
<b>CHAPTER 5 SYSTEM IMPLEMENTATION (FOR DEVELOPMENT-BASED PROJECT)</b>	<b>71</b>
5.1 System Methodology	71
5.2 Project Timeline	74
5.3 Technologies and Tools Involved	75
5.4 Implementation Issues and Challenges	76
5.5 System Testing	77
5.6.1 Use Case Testing	77
<b>CHAPTER 6 SYSTEM EVALUATION AND DISCUSSION</b>	<b>81</b>
6.1 System Testing and Performance Metrics	81
<b>CHAPTER 7 CONCLUSION AND RECOMMENDATION</b>	<b>98</b>
7.1 Conclusion	98
7.2 Recommendation	99
<b>REFERENCES</b>	<b>154</b>
<b>WEEKLY LOG</b>	
<b>POSTER</b>	
<b>PLAGIARISM CHECK RESULT</b>	
<b>FYP2 CHECKLIST</b>	

## LIST OF FIGURES

<b>Figure Number</b>	<b>Title</b>	<b>Page</b>
Figure 2-1	Architecture of Proposed Solution	17
Figure 2-2	uPort Component	20
Figure 2-3	Working of uPort	20
Figure 2-4	An overview of key elements of ShoCard	22
Figure 2-5	Data flow in blockchain application	25
Figure 4-1	System Flowchart Diagram	29
Figure 4-2	Prototype Development Example	37
Figure 4-3	Log-In Page	39
Figure 4-4	Log-In Page (Metamask Web Extension)	40
Figure 4-5	Log-In Page (Metamask Account)	41
Figure 4-6	Account Registration Form	42
Figure 4-7	Account Registration Form (Memtamask Transaction Confirmaton - User)	42
Figure 4-8	User Log-In	43
Figure 4-9	User Homepage	44
Figure 4-10	Digital Wallet Section	44
Figure 4-11	Digital Wallet Creation	45
Figure 4-12	Digital Wallet Creation (Metamask Transaction Confirmation)	46
Figure 4-13	Digital Wallet Details	46
Figure 4-14	Identity Claims Section	47
Figure 4-15	Identity Claim Registration Form	47
Figure 4-16	Identity Claim Registration Form (Metamask Transaction Confirmation)	48
Figure 4-17	List of Registered Identity Claims	49
Figure 4-18	Confirmed Transaction Notification	49
Figure 4-19	List of Registered Identity Claims(ii)	50
Figure 4-20	List of Registered Identity Claims(iii)	51

Figure 4-21	Identity Card Image View	51
Figure 4-22	Driving License Image View	52
Figure 4-23	Account Registration Form (Issuing Authority – Government)	52
Figure 4-24	Account Registration Form (Metamask Transaction Confirmation – Issuing Authority)	53
Figure 4-25	Log-In Page (Confirmed Transaction)	53
Figure 4-26	Issuing Authority Log-In	54
Figure 4-27	Issuing Authority Homepage	54
Figure 4-28	List of Registered Pending Claims	55
Figure 4-29	View Details Button	56
Figure 4-30	Verification Procedure	56
Figure 4-31	Verification Procedure (Metamask Transaction Confirmation)	57
Figure 4-32	Confirmed Transaction Notification	58
Figure 4-33	Registered Pending Claims	58
Figure 4-34	User Log-In	59
Figure 4-35	Status Check	59
Figure 4-36	Account Registration Form (Service Provider)	60
Figure 4-37	Account Registration Form (Metamask Transaction Confirmation - Service Provider)	61
Figure 4-38	Metamask Confirmed Transaction Notification	62
Figure 4-39	Service Provider Log-In	62
Figure 4-40	Service Provider Homepage	63
Figure 4-41	Request Access Form	63
Figure 4-42	Request Access Form (Metamask Transaction Confirmation)	64
Figure 4-43	Metamask Confirmed Transaction Notification	65
Figure 4-44	Access Request Section	65
Figure 4-45	Access Request Approval	66
Figure 4-46	Metamask Transaction Confirmation	66
Figure 4-47	Metamask Confirmed Transaction Notification	67

Figure 4-48	User-side Approved Access Request	67
Figure 4-49	View Claim of Approved Request	68
Figure 4-50	Identity Claim Details of Approved Request	68
Figure 4-51	View Identity Claim Image.	69
Figure 4-52	Identity Card Image View	69
Figure 5-1	Prototype Methodology Model	70
Figure 5-2	Prototype Methodology Model – Second Phase	71
Figure 5-3	Final Year Project 2 (FYP2) Estimated Timeline	71
Figure 6-1	Case(b)	74
Figure 6-2	Case (a)	82
Figure 6-3	Case (c) – (i)	82
Figure 6-4	Case (c) – (ii)	83
Figure 6-5	Case (d)	83
Figure 6-6	Case (e) – (i)	84
Figure 6-7	Case (e) – (ii)	84
Figure 6-8	Case (e) – (iii)	85
Figure 6-9	Case (f) – (i)	85
Figure 6-10	Case (f) – (ii)	86
Figure 6-11	Case (g) – (i)	86
Figure 6-12	Case (g) – (ii)	87
Figure 6-13	Case (h) – (i)	87
Figure 6-14	Case (h) – (ii)	88
Figure 6-15	Case (h) – (iii)	89
Figure 6-16	Case (h) – (iv)	90
Figure 6-17	Case (i) – (i)	90
Figure 6-18	Case (i) – (ii)	91
Figure 6-19	Case (j) – (i)	91
Figure 6-20	Case (k)	92
Figure 6-21	Case (l) – (i)	92
Figure 6-22	Case (l) – (ii)	93
Figure 6-23	Case (l) – (ii) & Case (o)	93

Figure 6-24	Case (m) & Case (n)	94
Figure 6-25	Case (p) – (i)	94
Figure 6-26	Case (p) – (ii)	95
Figure 6-27	Case (q) – (i)	95
Figure 6-28	Case (q) – (ii)	96
Figure 6-28	Case (q) – (iii)	96

## LIST OF TABLES

Table Number	Title	Page
Table 2.1	Comparison Table	27
Table 2.2	Comparison between the existing applications and proposed application	30
Table 3.1	Use Case Description of Register Account	31
Table 3-1	Log-in to web portal	31
Table 3-2	Create Digital Wallet	31
Table 3-3	View Digital Wallet Details	32
Table 3-4	Register Identity Claims	32
Table 3-5	View Registered Identity Claims	33
Table 3-6	Approve or Reject View Request	33
Table 3-7	Approve or Reject User Identity Claims Registration	33
Table 3-8	Send request to Access User Identity Claim Details	75
Table 3-9	View Approved Identity Claim Details	77
Table 5-1	Tools to use	27
Table 5-2	System Verification Plan	30

## LIST OF ABBREVIATIONS

<i>DApps</i>	Decentralized applications
<i>ID</i>	Identity
<i>SIM</i>	Subscriber Identity Module
<i>RFID</i>	Radio-frequency identification
<i>SP</i>	Service provider
<i>OTP</i>	One-time password
<i>eID</i>	Electronic Identity

## **Chapter 1: Introduction**

### **1.1 Problem Statement and Motivation**

- **Risk of data breaches and identity thefts**

Whether the way of identification is through the age-old paper or digital, the thefts and misuse of personal identity information are still a challenging issue that exist both physically and electronically. According to [24], identities and personal information have become essential elements of the information age. Therefore, they become a target to be used by criminals to gain unlawful benefits or commit crimes under the names of others [24]. Users will be disclosing and sharing own personal information to other parties such as on online platform to transact or exchange values. However, there is a high risk of data breach and identity theft during the process, where hackers may perform unauthorised access on user's personal data without getting noticed or even hack through centralized database of authorised authority. This is where user's identity got stolen and hackers may use those stolen identities on behalf of their identity to commit crime or to gain personal benefit.

One of the top complaints received by the Cybersecurity Malaysia (CSM) was the threat of identity theft [7]. [2] stated that in terms of citizen personal data protection, Malaysia have been ranked as 5th worst country in the world, listed in the category of some safeguards in data but are weakened in protection. Identity theft cases in Malaysia are growing in number and it is said that there are even more cases which are not reported [7]. Most of the personal data which is used in identity theft was most likely retrieved from many data breaches over the past year as least amount of data only was encrypted [7]. A recent survey conducted by Fair, Isaac and Company (FICO,) 7% have indicated that about 1.5 million Malaysians say their identity has been stolen and used by fraudster to open accounts for illegal purposes such as money laundering, bribes and other illegal activities. These issues shows that the problem of data breach and identity theft is still active and on-going since the past few years till now, which is a serious matter for the citizens of Malaysia.



- **Abuse of trust resulting in lack of trust among parties in business.**

According to [25], trust has become a significant factor in business transactions since the starting of the handshake. In the past, most of the business transactions are performed face-to-face, therefore, the concern was just to make sure that the person to transact with was who they said they were. Even if they were not, if the service is delivered and paid on time and correctly, the business process will not be affected. However, looking at today's business transactions, most of them are increasingly performing online. No face-to-face interactions are involved in transacting and the verification process of a person are highly relied on digital methods [25]. However, unauthorized access and hacks may happen during the process. Besides that, documents that are stored in a digital form can be copied and modified without anyone realizing it [25]. This makes the documents hard to be trust. There are existing solutions that offers verified and secured document management, but they can be very expensive and often involves the control of a third-party [25]. In some cases, if the transaction process turns out to be something fraudulent, we are unable to track where that transaction come from, who's behind this, where they are in the world or even where to begin recuperating the losses [25]. This way, it can lead to increase in potential frauds and corruptions in business transaction processes. These issues have result in lack of trust among parties in businesses.

Based on [23], good track record of transparency is absent in Malaysia, which can lead to poor governance and corruption. According to [8], transparency international have stated that when institutions or official authorities are weak, it thrives corruption and also result in low public trust. It is important having government transparency in order to ensure the management of contracts have strong internal accountability arrangements. One of the critical cases relating to abuse of trust is where three men, including a father and son are arrested to facilitate investigations into a criminal breach of trust case involving over RM300 million related to an investment company, which is a big issue to the public [14].

- **Over-relying on middle person for transaction process.**

Relying on middle person in manual process in the delivery of government services may be an issue. This will result in high cost in transaction processing

including the complex procedure in processing such as registration, verification and issuance of identity documents, and labour cost to carry out transaction processes. Other than that, relying on trusted middleperson or third-party in transaction processing can be very unnecessarily expensive as each middleperson make some money along the process and unnecessarily time consuming as the more processes are created and some executed manually. This may reduce effectiveness and satisfaction of the citizens in public service delivery. Nevertheless, giving third-party or middle person to have full control over sensitive data may lead to critical risks. There are chances that user's personal data may be leaked or even manipulated by others to commit fraud, perform unethical transaction or personal gain.

Based on [9], it stated that completion of government transaction may take an average of 5.4 hours and also up to 11 hours in some countries. Other than that, in-person transaction delivery will cost up to 40 times more compared to delivery transaction through online [9]. Besides that, big corporation like Malaysia Airline Bhd have experienced a personal data security incident as well [3]. Enrich members were notified that their personal data such as name, date of birth, contact details and various frequent flyer data including status, tier level and number might have been compromised. The lack of visibility, control, and security insight have led to a critical blind spot for Malaysia Airlines as their critical data and system were taken care by third-party IT service vendors [3].

### 1.2 Objectives

- **To develop a tamper-resistant identity management system with strong data protection mechanism to mitigate risks of identity thefts and data breaches in Malaysia.**

In my proposed project using blockchain technology, it is able to mitigate the problem of trust issues, identity thefts and data breaches by being tamper-proof and having strong data protection. With Blockchain, records stored in the database are immutable and tamper resistant due to its strong data protection mechanism. Blockchain is a distributed ledger that only allows append-only operation; therefore, this results an immutable transaction data in the blocks and fully irreversible where data can't be easily exploited, manipulated or destroyed. Cryptography concept with encryption and hash functions will be applied on the storage of user's identity claims

in Blockchain to have better security in data protection. This helps to achieve data integrity as all participating nodes are able to know whether identity details have been altered by referring to the hash generated towards the identity claims, which make the national identification system to be more secured. Having strong data protection, trust of security is imposed therefore the citizens can feel more secured in providing their personal details without worrying much about data leakage and breaches. Other than that, having the characteristic of strong data protection makes government service provider to be more reliable and offers government sector a good reputation in terms of trusted service provider.

- **To integrate a distributed ledger in the identity management system for good identity record management that imposes trust to business parties.**

In my proposed project, trust issues, identity thefts and data breaches, over-relying on middle person issue can be solved. Abuse of trust issue can be solved where participating parties in the network do not need to trust each other but trust can still be imposed in the system. In blockchain, trust is enforced and applied in the system, regardless of the parties in the chain. This is because parties are all forced to behave and act in trustful ways via consensus mechanism, distributed databases, cryptography hash functions and Merkle tree. Before each block of transactions can be added to the blockchain database, participating nodes are required to perform the consensus mechanism, where they are forced to check and agree that transactions are valid. The block being added is then timestamped and secured with cryptography hash functions to ensure data integrity and appended to the previous block in the chain. In this way, Blockchain can keep track of changes towards the records within the chain to prevent fraud and modifications. Only participating nodes in a network can store, view and distribute digital information in a security-rich environment that is able to foster trust, transparency and accountability in business relationships within different parties. This automated distribution process has eliminated the need of middleperson. Besides that, it is very rare and hard for fraudsters to hack and exploit a decentralized Blockchain. It consists of different technological mechanisms working together towards a common goal. For example, proof of work (PoW) and proof of stake (PoS) from the consensus mechanism are used to protect the network by mitigating cyber-

attacks from hackers. Being decentralized also prevents single point of failure and mitigates data breaches.

- **To eliminate middle person in identity management transaction process to cut identity management cost and time.**

In my proposed project, middle person or government intermediaries to carry out the identity management process is eliminated that solves the over-relying on middleperson issue by saving time and cost in transaction processing. Blockchain acts as the distributed ledger where any contracts, business transactions and values (record of ownership of asset like money, identity claims, land titles etc.) are shared, managed, and maintained in a decentralized form across different people at different locations instead of storing data in a centralized form and coordinated by middleperson. This is where middleperson has been eliminated. My system that is built on a decentralized network such as Ethereum Blockchain, uses smart contract for any verification processes that replaces the job for middleperson to control the identity claims/documents of the users. Any registration and updates regarding user's identity claims are distributed to all participating nodes and updated at their own copy blockchain database at their respective nodes in consensus. This automated distribution process is able to save time and cost in transaction processing and updating from unnecessary expensive labor cost and complex procedures.

- **To allow users to have control over their identity claims and apply effective reviewing process to ensure controlled sharing of identity claims.**

From my proposed project, it can mitigate the problem of identity theft and data breaches, trust issues as well as over-relying on others issue. Users can have self-sovereign identity from my project by being able to own and control the sharing of their identity claim details. A digital wallet will be integrated to my system for user's side to act as a reference place for user to store and manage their identity claims at the Blockchain network. Before any legal institutions or service providers intend to access user's details, they are required send access request to users for approval. Users then able to review which access request of their particulars they want to approve. In this way, user's identity claims are controlled by their own and they are safe from identity thefts and data breaches, eliminates the need of middleperson for

transaction process and prevent abuse of trust issues from third-party and legal authorities in identity management. Besides that, giving users control helps to mitigate the burden of the government authority. Business authorities or legal institutions who require user's identity assets will only need to deal with the user himself instead of accessing with the government, which prevents backlogs to happen at the government side.

### **1.3 Project Scope and Direction**

For my proposed project, it focuses on developing an identity management system using Blockchain technology that can solve problems faced by current identity management solutions in Malaysia. The system is built on a Ethereum Blockchain that combines a smart contract and a frontend user interface.

In this proposed system, the concept of the identity management will be the combination of blockchain technology and web application. The web application will be acting as the frontend user interface for users to interact with the blockchain network while registering and managing their identity claims. There are three main roles in this blockchain identity management system including user, issuing authority (government) and service provider (registered/ legal institutions).

- **Log-in procedure to control access of different roles.**

Through the system, users can register and manage their identity claims. The registered claims are then required to be verified by the issuing authority. Besides that, service providers who wants to access user's identity claims are required to make a request from the users. Each role is only allowed to access functionalities intend to be performed by them. Therefore, a verification procedure such as a log-in page that leads to the specific interface for each role will be integrated to the system. This helps to ensure effective authorization process and controlled access are present to prevent unauthorized access of each specific roles functionalities which enhances high security. Metamask software will be used as the log-in procedure. Users are required to log-in to their Metamask account which requires password or secret recovery phrase to connect to the Blockchain Rinkeby Test Network for all functionalities of the system to work.

- **Verification procedure to ensure validity of user's registered claims.**

Risk of data breaches and identity thefts in Malaysia is one of the problems stated earlier. This is where user's identities are stolen and used by fraudster to create fake identity registrations with other's particulars for illegal purposes. However, through my proposed system users can upload their identity claims or documents to the Blockchain network but is required to be verified by trusted issuing authority (government) for the validity of claims. User's fingerprint will act as the base of verification (source of proof) in order for the government to approve the validity of the identity claims provided by the user. The government side will compare the fingerprint provided by the users with the one stored at the old database to see whether they match using its AI system. Only when the matching percentage of the two fingerprints reaches a certain range (e.g.: 95% – 100%), the government will then approve the validity of the identity claim. Once claims are verified, the validity status will be updated on the Blockchain network. Blockchain only allows append-only operation. Two of the main characteristics of Blockchain are immutable and fully irreversible, where identity claims and details stored are all cryptographically recorded and cannot be modified and deleted. In this way, it can track the authenticity of the claims to see whether they are valid. This prevents fraud and imposes trust towards user's identity claims. In this way, it helps to solve the trust issues as well. Timestamping in Blockchain can also verify whether that claim existed at a certain date and time, therefore, it is really hard for fraudsters to forge fake identities of other users or modify user's details as the original identity claim can be traced.

- **Users side, government side, and legal institutions are connected in one system.**

Moreover, the problem of over-relying on middleperson for transaction has also been eliminated. Through my system, both registration and verification of identity claims can be performed at the same system. Users do not need to go through

different middleperson (government intermediaries) physically or online for the registration and verification process of their identity claims as both users and the government are connected through my proposed system. My proposed system that is built on a Ethereum Blockchain utilizes smart contract for the claim registration and verification process. Smart contract is a type of program constructed that is used to store conditions and perform transactions based on conditions set. This is where the identity claims registration and verification process are automated. Other than that, connecting the user side and service provider side helps to eliminate the need of a middle person or notary person as well in transacting processing. This eliminates middleperson or notary person by saving time and cost from expensive labors and manual or complex procedures involved in existing identification solutions. Besides that, users can also view their stored claims on the blockchain network with the use of smart contracts and prove their identity. In this way, users do not need to carry around their physical identity assets and able to access their claims at the system anytime.

- **Users having self-sovereign identity.**

Lastly, users can have self-sovereign identity through my proposed project. This is where they can have full ownership towards their identity claims and control them. Service providers who intend to access user's particulars are required to request access from the user. Users can then review which identity assets they allow others to access to. Only user approved identity claims can be viewed by the service provider. This process is also triggered using the smart contract where only approved access of details by the user can be shown to the service provider. User having self-sovereign identity helps to solve the trust issues between the users and third-party who store and manage user's identity claims as well as eliminate government intermediaries in controlling user's identity claims for sharing. From here, users do not need to share all identity claim details to other parties which can mitigate risks of data breaches and identity thefts.

### **1.4 Contributions**

My proposed project, which is Identity Management decentralized application using Blockchain technology, it benefits both government (Ministry of Home Affairs) and citizens of Malaysia in terms of secured digital identity management. In a government context, my proposed project offers an identity management approach

where central authority like Malaysia government will be dealing less on the sharing of personal data of the citizens. This leads to fewer personal data management and less governmental bureaucracy. Less governmental bureaucracy means eliminating some complex multi-layered governmental systems and processes while managing the identities of the citizens, which is much cost effective and efficient. This approach reduces the time and cost of data management, eliminate the need for intermediaries, and increases the efficiency of identification process while putting citizen's security and privacy first.

The proposed system will not store any user's information. Data of the users will be stored on blockchain database in a decentralized manner rather than hackable centralized servers. Thus, it is not possible for data manipulation on the blockchain as all participating nodes will store the same data, any modifications in one node will be easily realized and notified to other nodes. Once users' identity claims are stored on blockchain, claims will be then encrypted securely through cryptography and cannot be manipulated and destroyed. Massive data breaches of users' identity claims and documents can be very difficult as well. This have delivered a tamper-proof, high data transparency in governance and secured system to the government sector of Malaysia to manage citizens' identity claims and data. Furthermore, data are stored in a decentralized manner using Blockchain technology. Whenever natural disaster or loss of data has occurred, data can be still recovered or retrieved from other nodes of the network as it does not store at only one centralized database.

Besides that, through my proposed project citizens of Malaysia (users) will have full ownership and control over their identity claims and documents. This is where users are owning self-sovereign identity without any interference and control from any central authority, middleperson, or third-party vendor, which eliminates the need of intermediaries and middleperson to store and own users' identity data. An identity management system that is linked with blockchain is highly secure for identity owners. Smart contracts of Ethereum Blockchain are used by the system to enable controlled data disclosure from the user. Without the explicit consent by the user, no transaction of the user's identity details can be carried out. This has eliminated the need for intermediaries for transaction processing and control over users' sensitive identity claims and documents.

Moreover, my proposed project can also bring convenience to the citizens of Malaysia while being highly secured. After users have stored their identity claims and



documents digitally on blockchain, users can then access their identities anytime through the decentralized application without the need to carry out physical identity claims and documents. With my proposed project, users will not need to give their sensitive personal claims and details to any third-party vendor or legal organizations for storage and control as their digital identities are cryptographically stored directly on Blockchain within the internet browser. From the proposed project, personal details that are encoded to the Blockchain can be accessed by third parties only with the consent by the users. This way, it has eliminated the need for intermediaries to store sensitive personal identity claims instead of eliminating the entire access of the intermediaries. This allows portability and efficiency for users and helps reduce data breaches and identity thefts issues in Malaysia as well.

Other than that, giving the users control in the process of sharing their personal data not only maintains user's privacy, but it also mitigates backlogs occurring at the government side. Connecting the user and service provider in one system can also eliminate the need of notary person for registrations or transactions that involves user's identity claims. Users can directly share those required identity claims to service provider through the system, which avoids transaction payment and the need of notary person in performing complex multi-layered procedures. Besides that, users do not need to go that specific location physically to carry out the transaction process as well. Therefore, this approach is both cost effective and efficient. Other than that, it is also quite useful for businesses or legal institutions as they are able to directly request and acquire user's identity assets or documents through the system. Businesses or legal institutions who requires user's identity claims including banks (opening a new account requires identity card/ residence permits/visa), vehicle companies (buying a vehicle requires driver's license & identity card), school or universities (registering for an education requires identity card & birth certificate), government services (registering or replacing an identity card requires our birth certificate) etc.

### **1.5 Report and Organization**

This report is organised into 7 chapters: Chapter 1 Introduction, Chapter 2 Literature Review, Chapter 3 System Methodology/ Approach, Chapter 4 System Design, Chapter 5 System Implementation, Chapter 6 System Evaluation and Discussion and Chapter 7 Conclusion and Recommendation.

The first chapter is the introduction of this project. There are sections of problem statement, project background and motivation, project scope, project objectives, project contribution, and report organization. The second chapter is regarding the literature review performed on several existing identity management systems or frameworks in the market in order to evaluate the strengths and weaknesses of each of the system. After the evaluation, we will then refer to the existing system's strengths and weaknesses as a milestone to improve our proposed project. The third chapter will be discussing about the overall system design of the proposed project. The fourth chapter will be talking about the details on how to implement the design of the system including the flowchart design and graphical user interface design. Moreover, the fifth chapter reports the system implementation including sections like System methodology, Project Timeline, Technologies and Tools Involved, Implementation Issues and Challenges and also the System Testing Verification Plan. While for Chapter 7, it reports the conclusion of the whole project development process and recommendations.

## **Chapter 2: Literature Review**

### **2.1 Review of the Technologies**

Blockchain Technology is the new wave of disruption that has revolutionized different aspects such as business, political interaction and social, and any other way of value exchange mechanisms. Another way of saying is it is a rapid phenomenon that is already in motion [6]. Blockchain serves as a peer-to-peer network which is run by large number of participating nodes where no trusted central authority is needed to serve as intermediary in verifying, securing, and executing the transactions [21]. This is where zero trust network is imposed, and all structural information are stored within the network [21]. Zero-trust network is a security concept where all users or entities are required to be verified before they are allowed to access data or application, therefore security of the system can be maintained [27].

According to [17], the word ‘Blockchain’ is composed with two words, ‘block’ and ‘chain’. A block refers to a collection of data records. While for chain, it refers to a public database of these blocks that are stored as a list [17]. These lists are connected using cryptography concept. Since blockchain operates as a peer-to-peer network model, there is no single node, and nodes don’t have to trust one another [11]. Therefore, it is important that appropriate safeguards for transaction information on unsecured channels are in placed while maintaining transaction integrity in Blockchain [11]. Hence, cryptography has become the most essential and fundamental requirement for blockchain to safeguard user’s privacy and transaction information as well as maintaining data consistency [11].

Based on [11], cryptography primary applications mainly focus on protecting the security of participants and transactions, against double-spending, and lack of influence of middleperson on operations. There are wide range of purposes served by cryptography to applications. In some situations, it helps to secure different transactions running on a network. Besides that, it also finds applications in verifying the transfer of digital assets. Blockchain applications have leverage the real-world signatures concept by leveraging cryptography techniques along with encryption keys. Cryptography techniques uses advanced mathematical codes for storing and transmitting data values in secure manners. Hence, it ensures that only individuals for whom the transaction or data is intended able to receive, read and process the transaction and verify both the authenticity of participants and the transaction [11].

Cryptographic hashing method is one of the critical highlights in blockchain cryptography [11]. It acts as a basic component of blockchain technology. With the use of hashing, it enhances immutability in blockchain, the most important feature in the blockchain [11]. Keys are not involved in the encryption process through cryptographic hashing. Cipher or an algorithm is leveraged to get a hash value of a particular length from the input [11]. Hashing takes a string of any length as input and produces an output with a fixed length [11]. SHA-256 cryptographic hash function is used as the most common applications of hashing in blockchain [11].

Merkle tree is a binary tree of cryptographic hash pointers, which referred as “binary hash trees” [6]. Hashing paired data (refers to transactions placed at the leaf level) are used to construct the Merkle tree, then hashed outputs are hashed up till the root node (Merkle root) [6]. According to [26], it is defined by the way of data structuring where large body of information can be verified extremely quick and efficient for accuracy. It is a crucial component of blockchain technology and cryptocurrency, and basically transformed the world of cryptography such as the way of encrypted computer protocol’s function. It has gained and grown in popularity over the years especially in cryptocurrency. Satoshi Nakamoto has mentioned Merkle trees several times while introducing the concept of Bitcoin and they are used as Bitcoin’s foundational code. Cryptocurrencies like Ethereum has adopted Merkle Trees as well [26].

Besides that, Blockchain is fundamentally a distributed ledger technology where the transactions are replicated across large number of nodes in a shared and decentralized way [6]. Each transaction that exists in the public ledger are all validated in consensus before entering and added to the database of all nodes [6]. All permanent entries that are broadcasted and reflected on all copies of the database hosted by different nodes imposes transparency [6]. Other than that, the distributed ledger only allows append-only operation; therefore, this results an immutable transaction data in the blocks and fully irreversible. These characteristics have ensured data integrity in the database [6]. Due to the beauty of blockchain, many firms and top financial institutions across different industries has adopted the use of blockchain in order to speed up the time of transactions, reduce fraud or risk factors, and lower the cost of transactions by obsolete the need of intermediary services [6].

Blockchain aims to enable decentralization. With the use of this technology, decentralized systems can be used to replace the centralized systems. According to

[6], distributing process can be carried out either in a centralized or decentralized way. In a centralized way of distribution, it is controlled by a central repository, also represented as master node, where it is responsible in distributing the data or task across all participating nodes [6]. While for the decentralized distributed systems, there is no such master node for the distribution process. No one has to know or trust anyone else in the network and any computation of data will be replicated across all participating nodes in a consensus [6]. To make it simple, it is where each participating node will have a copy of the exact same data in the form of a distributed ledger. If a participating node's ledger is modified or corrupted in any way, it will be rejected by most of the participating nodes in the network.

Blockchain which acts as a decentralized system of distributed ledger technology, does not suffer from the conventional centralized systems limitations as well [6]. There is no central point of failure result in being fault tolerant and attack resistant, hence it is more secured. It also acts as a symmetric system where all participating nodes will have equal rights and authority, therefore it is democratic in nature and unethical operations can be reduced [6]. This has imposed characteristics such as immutability of data, transparency among participants and resilience against adversarial attacks [6].

Blockchain technology popularity is mostly caused by the fact of where real-world problems can be solved as it delivers tamper proof security and more transparency compared to other common technologies [6]. The blockchain use cases have gone beyond the banking and finance sector, as has cover other industries including the government sector, retail, supply chain, healthcare, e-commerce, and energy [6]. This is due to different problems are being addressed by different flavours of the blockchain technology [6]. In order to allow the use cases being implemented, applications that interacts with the blockchain is being introduced, which is called decentralized applications (DApps) [6]. The decentralized apps can be built on the blockchain platform called as Ethereum, where it is capable in empowering the various blockchain use cases [6]. Due to the beauty of blockchain technology, it can be integrated into my project as it solves the problems in my research.

One of the most successful cryptocurrencies use case is Bitcoin, the blockchain-based cryptocurrency, which has inspired the potential of Blockchain to be used for other use cases [10]. This cryptocurrency is known for its usage and understanding of the Blockchain technology having an essentially decentralized design of software

architecture and as a model of data persistence [10]. When blockchain started being popular, only cryptocurrency bitcoin is being used to handle payments, but few years later people start to realise the potential of blockchain technology beyond just cryptocurrency and various studies have suggested blockchain can be used in different areas as well other than transacting payments [6].

In the year 2008, Satoshi Nakamoto have written the “Bitcoin: A Peer-to-Peer Electronic Cash System” that described a purely per-to-peer version of electronic cash, this is where the cryptocurrency Bitcoin was established and at the same time, greater efforts in technological aspect is being created in order to trace and verify transactions [10]. After the release of white paper by Nakamoto, in the year 2009, Bitcoin was offered up to the open-source community [5]. Blockchain have gave the answer in terms of digital trust as important information is recorded in a public space where anyone is not allowed to remove the records [5]. It gives the characteristic of transparent, decentralized and time stamped [5].

Highly complex algorithm is used by Bitcoin to avoid unauthorized creation and duplication of the Bitcoin units [4]. The code uses the underlying principle which is cryptography, which is based on advanced computer engineering and mathematical principles [4]. Therefore, it is highly impossible to break through the source and manipulate the content or information underlying the currency [4]. For each of the Bitcoin, it is a computer file that is stored inside a digital wallet app on a computer or smart phone [13]. The users are able to send Bitcoins to other parties while other parties are also able to send bitcoin to the users, which is in the peer-to-peer basis [13].

Around the year 2014, people start to realize blockchain can be used beyond cryptocurrency and have started their investment and exploration in blockchain how blockchain is able to improve many kinds of operations [5]. At the core of blockchain, it is an open decentralized ledger where it records the transactions between two parties without the need of third-party authentication in permanent way and the records cannot be eliminated [5]. This has contributed a much efficient process and is able to reduce the cost and time of transactions [5]. After the entrepreneurs have understand about the potential of blockchain, there was an increase of discovery and investment to see the ability of blockchain that could impact sectors like healthcare, supply chain, government, insurance, transportation and more [5].

For my proposed project, it focuses on developing an identity management decentralized web application (DApp) using Blockchain technology. This proposed project helps to solve the problems faced in existing identity management solutions that could improve Malaysian Government Services in Ministries of Home Affairs in terms of managing Malaysian citizen's identity claims such as identity cards, birth certificates, land asset claim etc. The national identification system can be improved by digitizing the system using blockchain technology. The DApp is built on a Ethereum Blockchain that combines a smart contract and a frontend user interface.

### **2.2 Review of the Existing Systems/ Applications**

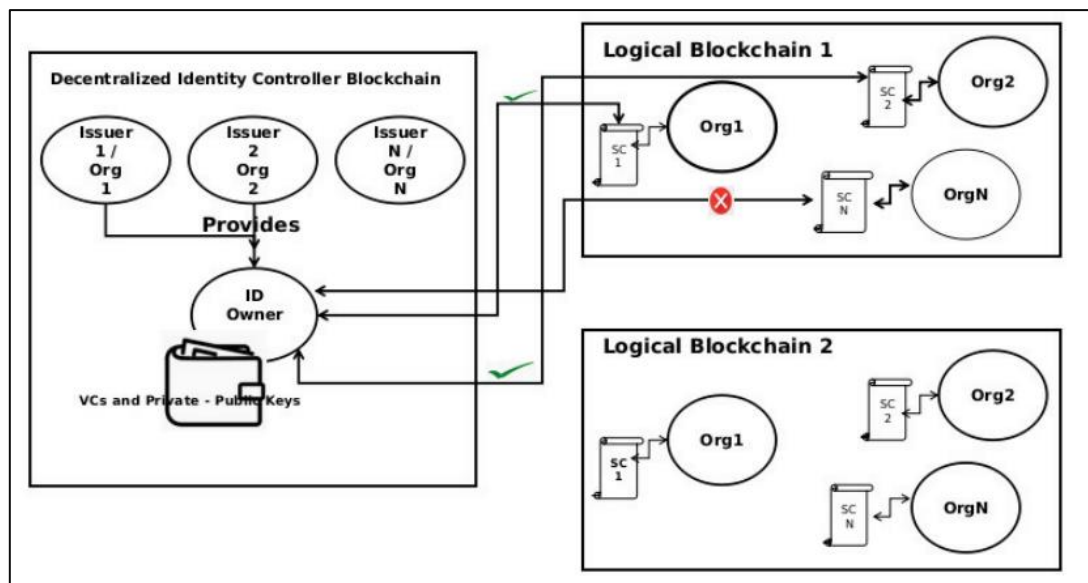
#### ***Previous works on Identity Management Solutions Using Blockchain Technology:***

##### **2.2.1 Interoperable Blockchain Solution For Digital Identity Management [22]**

[22] have offer a solution for the digital identity management, in order to solve problems in existing identity management including lose, theft, vulnerable manipulation, data being breached and exploited by governments and private entities. Besides that, most of the users' data are private, however, the data owners do not own the data. Through the Blockchain platform, it fills the gaps of those issues by implementing the concepts of cryptography, Zero-Knowledge-Proofs and decentralization.

The proposed blockchain identity management system consists of an identity owner entity that stores identity claims or documents that are valid and verifiable issued by trusted issuing authority. Verifier can use digital keys and cryptography to authenticate the claims. While for Zero-knowledge Proof, it ensures the verification process to be carried out successfully without the need to disclose full information of the user. This is where only necessary information will be shared to the verifier; therefore, the verifying entity will have "zero-knowledge" regarding the user's private claims but is certain about its authenticity. This concept is really useful to solve trust issues where identity owners don't have trust on verifying entity but are still required to provide their private details.

For the proposed digital identity management to be completely decentralized, registration of identity holders can integrate a dedicated blockchain platform. Once the user has logged-in this platform, users are required to submit their claims to issuing authority to check for validity. Issuing authority will be responsible for the verification process. Once verified, user's data will then be encrypted and stored in his digital wallet on the blockchain platform. From here, identity claims will be completed owned by the user where they are able to control the sharing of their particulars to requestor party or legal institutions. Hence, users are having self-sovereign identity. This self-sovereign identity can be linked to the user's personal details with the holder's digital keys. Authorized authorities will be responsible in verifying the claims on the blockchain network. After the identities are verified, the trusted identities are used to control the access of the identity holders and to verify whether that person has the right to interact with the smart contract stored on the blockchain network.



**Figure 2-1 Architecture of Proposed Solution**

The identity owner interacts with the issuing authority over the blockchain. Once valid digital identities verified by the issuer, the owner will then store identity claim in his digital wallet. Issuer will then use their private keys to sign user's identities and stored on the blockchain network (Hyperledger Indy). Based on Figure 1, Issuer 1 and Issuer 2 issues the digital identities to the identity owner. The owner is now the authorized members of these two organizations. The owner then can use those verifiable credentials stored in his wallet corresponding to organization 1 and 2, to



identify himself as the members of these two organizations on the blockchain platform. The connector developed by the authors forms a mechanism where the identity owner presents his identity stored in his digital wallet to the organizations. The organization will then verify the identity and grant the owner the right to invoke the smart contract on the blockchain as only members will have the access to invoke them. Now the owner can interact with the smart contract deployed by organization 1 or organization 2. The connector will make sure public-private keys that is used on the blockchain are connected to the user's digital identity claims that is verified by issuing authority on identity controller blockchain network.

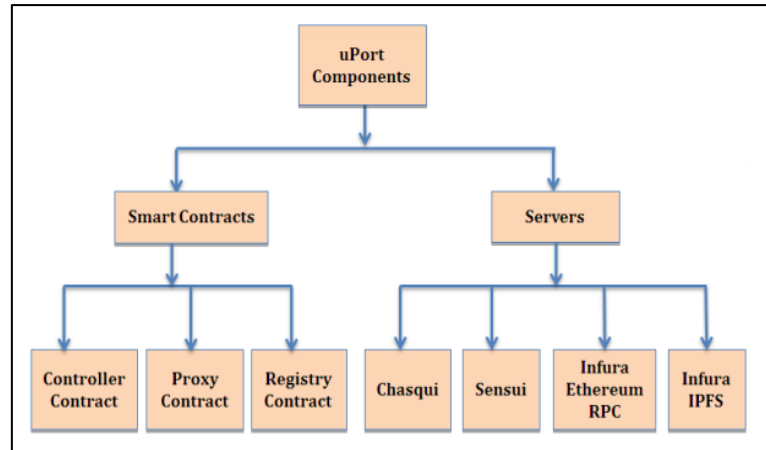
The strength of the proposed solution is having a decentralized system. This is where the digital identity management is performed on the blockchain network, where any process regarding the identity such as registration, issuance and verification are shared and will be known across different participating nodes (parties) on the same blockchain network. Besides that, cryptography concept is applied on user's verifiable identities or credentials and stored on the blockchain network. This ensures the security and privacy of user's data, where the data cannot be easily manipulated, exploit, or breach. The hash of the data is hard to be calculated and solved without the user's private key, which makes it harder for people to access without the right or permission. Other than that, the identity stored in this system is self-sovereign. This is where the user will have ownership and complete control towards their own data. The user is able to select which data to be shared and which verifier can have that specific information. This helps to prevent the threat of identity theft and illegal impersonation of an identity. Nevertheless, the verification process with the use of smart contracts are useful as smart contracts can set conditions and determine who have the right to access to a certain service or even validate the validity of the identity by making assertions. However, this proposed solution does not have a log-in section to restrict the access to user's digital wallet that stores identities. This can be insecure and dangerous as anyone can easily gain access to the user's digital wallet. Anyone can have control towards the user's personal data and can send them to whatever party they want.

### **2.2.2 uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain [19]**

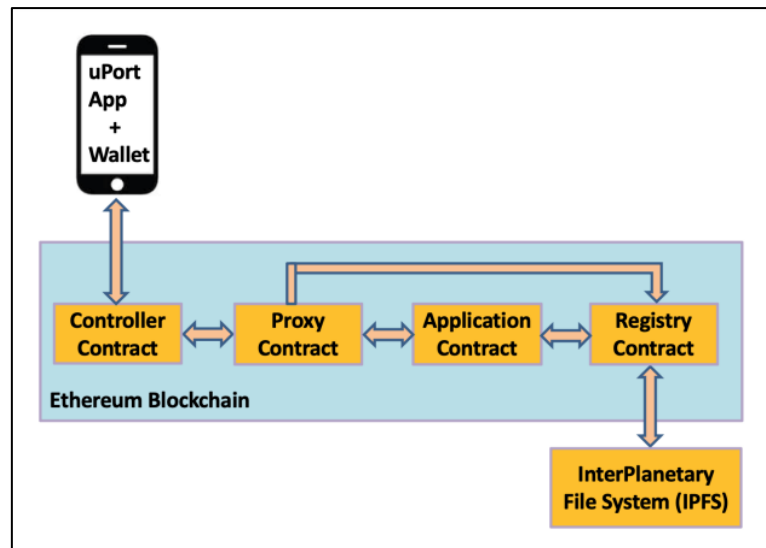
Through the open-source identity management system (uPort), users, entities and organizations are able to have self-sovereign identities. A uPort identity is a digital representation of a certain user or organization that is developed through a smart contract. The identity will then be stored on the Blockchain (Ethereum) in order to create assertions relating to their identity and interact with other smart contracts on-chain or off-chain. This characteristic has met the biggest requirement of having a self-sovereign identity where users are able to make claims regarding themselves. A smart contract is developed through coding and is then stored in a unique address on the Ethereum Blockchain. The contract is then run to control and manage valuable items like digital asset (identities and credentials) or Ethereum currency (ETH).

In existing cryptography-based identity management using public key mechanism, identities are represented by public keys while the ownership of them are determined by possession of the private key that is used to control the public key. One main concern against this principle is losing a private key leads to losing an identity. The cryptographic key management issue can be resolved by uPort system as Blockchain acts as the identity certification authority where user's digital identity will be represented by the smart contract stored in the network. Other smart contracts can also control these smart contracts in the network. The contracts can then be used to recover user's keys.

uPort identity management system acts as an open-source framework to deliver a decentralized identity and offer self-sovereign identity to a user. This framework uses public permissionless blockchain Ethereum and its smart contracts. Smart contract is defined as a program written to detect, achieve and perform a transaction agreement automatically. By employing this open-source framework, Users are able to register and display their identity in a much secure manner, such as transfer their claims, sign transactions and manage their data and cryptographic keys. A uPort identity can be generated for users, entity, organizations, and other resources. Users can then fully own and govern their own identity without the need of third-parties or intermediaries. In addition, all identity that consists of private details are stored in identity owner's digital wallet. This is where personal information exposure is kept to a minimum.



*Figure 2-2 uPort Component*



*Figure 2-3 Working of uPort*

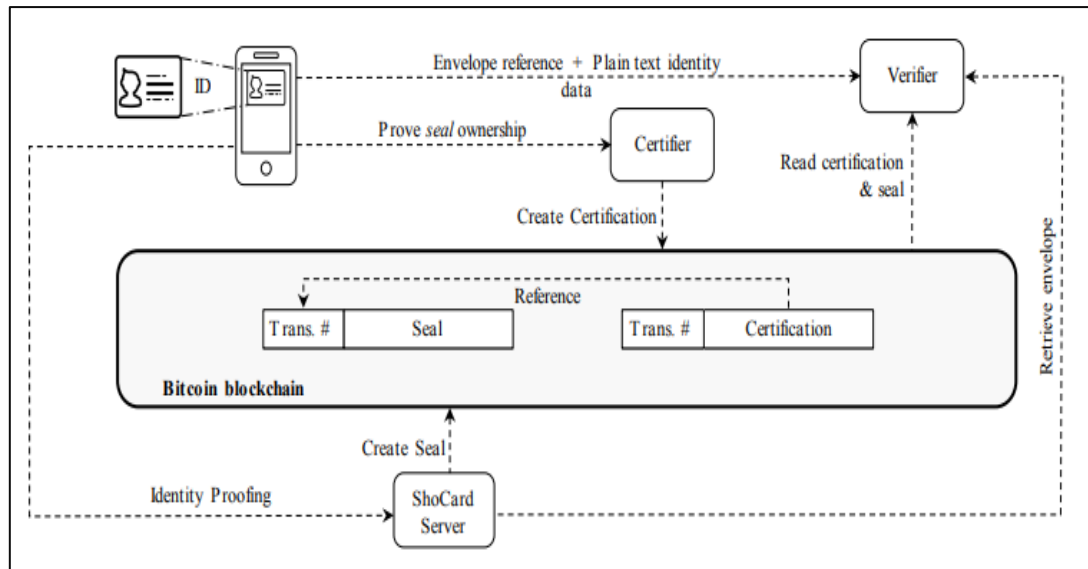
Based on **Figure 2-3**, any user of application can interact with any application contract in the uPort identity management system for identity related information. However, two main contracts are involved in the interaction including proxy contract, a user's permanent and universal identifier, and the main controlling program (controller contract). The user or application uses the controller contract to interact with the proxy contract, by sending a request to the smart contract. The proxy contract will then interact with the application contracts and forms a layer in between the private key of the user. It is then stored in the digital wallet and application contracts. A standard RPC interface offered by Infura is required by uPort to interact with the Blockchain Ethereum network. When a transaction is sent to the Sensui server, they do not need to have any Ether in their sending account as it offers sufficient Ether for

the transaction fee payment. The uPort identity that consists of user's identity details can be stored off-ledger as well including OneDrive, Drop Box, Google Drive etc. This action can be done by the establishment of cryptographic link to an external data structure using a registry contract. However, only proxy contract can update the registry contract. Infura IPFS interface is required for uPort to interact with the IPFS network.

One of the strengths of the uPort Open-Source Identity Management System is self-sovereign identity can be created. This is where the user will have full control and ownership of their personal data instead of other third party. Releases of personal and private data stored in the owner's digital wallet are kept to a minimum. User friendly data management and control functionality are offered by the system, where user can store, control, and share identity details to any party they want. The uPort identity management system also offers a user-friendly application interface to interact with the blockchain network. Besides that, personal data and credentials are stored in the identity are encrypted using cryptographic keys and are stored in the blockchain, which is tamper-proof. This helps safeguard the security and privacy of user's identity. However, user's mobile device's authentication procedure is not completely secure, as there is no log-in section to access the user's digital wallet account. Anyone who have the user's mobile phone or digital device can easily gain access to user's personal data.

### **2.2.3 ShoCard Blockchain-Based Identity Management System**

ShoCard is a blockchain-based identity management system which falls under the category of decentralised trusted identity. According to [28], centralised service (issuing authority) will provide an identity claim, which is used for the process of identity authentication of user based on records identity evidence on a distributed ledger. Further validations can be performed by trusted third parties to see the validity of identity asset such as trusted documents or credentials like passports. To make it simple, it normally exists as an identity provider platform to offer identity proofing service which maintains legitimacy.



**Figure 2-4: An overview of key elements of ShoCard [20].**

According to [20], bitcoin is used by ShoCard as a timestamping service for user identity information's signed cryptographic hashes, which will be mined to the Bitcoin blockchain. ShoCard uses a central server as an important part for the scheme. This is where the server intermediates the interaction between a user and relying party for the exchange of encrypted identity information. Three phases are being relied on this scheme which are bootstrapping, certification and validation. **Figure 2-4** shows the overview of ShoCard architecture.

[20] have also stated that bootstrapping phase will be implemented during the creation of a new ShoCard. A new symmetric key pair for the user will be created by the ShoCard mobile application and then scans their identity documents or credentials by using the camera of user's mobile device. After that, the encryption process will be done on the scanned data, and then being stored on the user's mobile device. The signed hash of the data will be then integrated into the Bitcoin transactions, so the data validation process can be carried out later. The resulting number of Bitcoin transactions will build the user's ShoCardID and then is saved in the mobile application which acts as a pointer to the ShoCard seal.

Based on [20], after the bootstrapping phase of a ShoCard, the user is able to gather additional attributes by interacting with identity providers in the certification process. In order for the certification to be associated into a ShoCard, identity providers are required to verify whether the user acknowledge both the data hashed to create it, and also cryptographic keys that signed the seal. In the way of face-to-face,

this can be achieved where users are needed to provide the original identity data forming the seal from the user's mobile device and present the credentials. The signed hash of new attributes and the associated ShoCardID is taken by the certificate in a Bitcoin transaction initiated by the identity provider. Bitcoin transaction number must be shared by the provider along with a signed cleartext of the new attributes directly with the user. This is because the attributes must be provided by the user to the relying parties and does not want to lose them in case the user lost their mobile device. The ShoCard server provide a storage place for the certificates which are encrypted, which can be known as envelope. User is able to share the certificates only to the relying parties they selected as ShoCard will never learn the encryption key.

Lastly, will be the validation phase. [20] have also emphasized that the validation process will be carried out when a specific relying party are required to carry out verification of a certification to decide whether the users is permissioned to access a service. The user is required to provide the envelope reference and its encryption to key to the relying parting for validation. The relying party will then perform the checking after the envelope is retrieved. Aspects that will be validated including whether envelope signature was created match with the same private key that is used to sign the seal. To also check whether is it a trusted entity who created the certification signature and the plain-text certification signature match with the one hashed and signed in the certificate. Moreover, to check whether user have presented the identity data in the pending transaction, is the same as those in the seal being hashed and signed.

ShoCard provides an identity that can be trusted which leverages distributed ledger technology to bind a user identifier, an existing trusted credential such as identity card, passport, driver's license, and additional identity attributes, together through the cryptographic hashes kept in Bitcoin transactions [20]. The main use case of ShoCard is the verification of identity which can prevent fraud and ensures only the user themselves are able to use their personal information to make exchanges [20]. There are some strengths exist in the blockchain-based identity management systems, where users are able to store and secure their own digital identities. The identity information and key of the user will be used together to ensure privacy. The need of third-party database is eliminated using the ShoCard system. The authentication code of the user is stored on the blockchain by ShoCard. This results in the legitimacy of personal identity can be guaranteed and third-party verification can be facilitated.

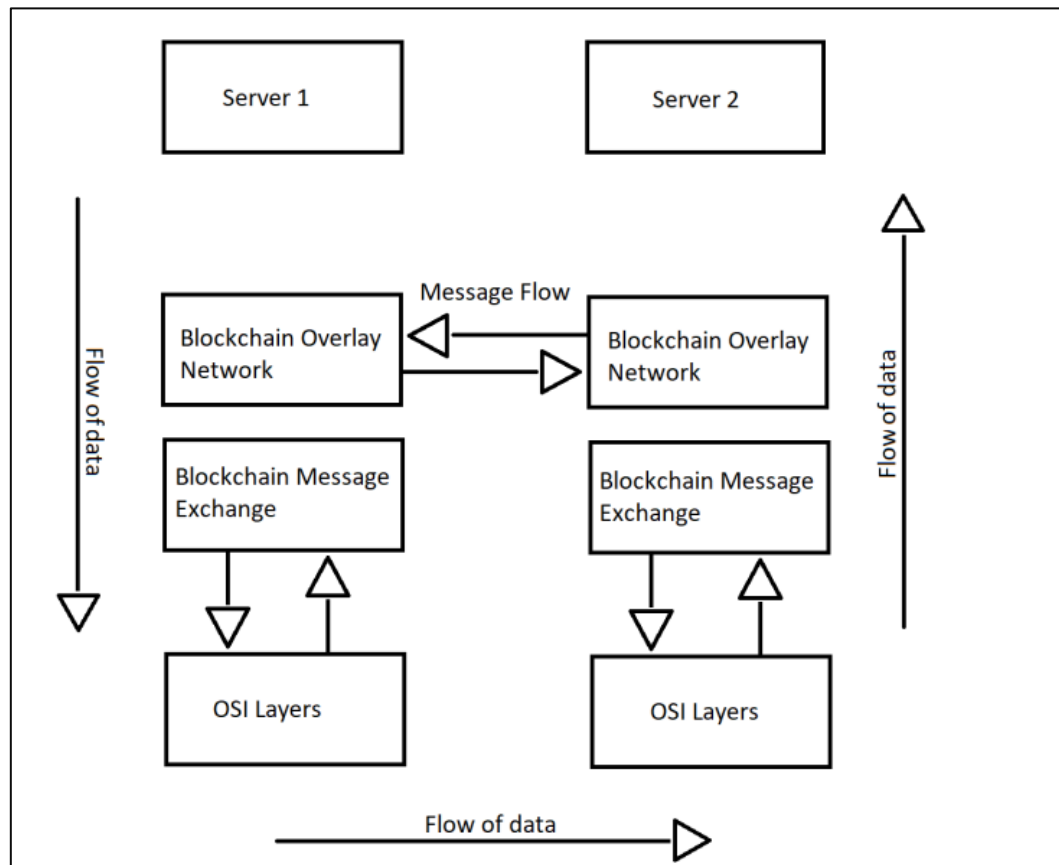
Other than that, ShoCard also having the strength bearing less risk of data breach as ShoCard central server will act as intermediary between ShoCard users and relying parties in the distribution of encrypted certificate [20]. The ShoCard will never learn the encrypted public key which is not risky [20]. It is able to speed up the transaction and verification process as there is no middle person needed to perform so. The storage place for identity information is secured and the sharing of identity information to relying parties can be controlled by the end-user [20]. Moreover, it is consistent and simple as QR codes are being used for the scanning process of identity documents, which is brings better user experience [20]. However, ShoCard unidirectional identifiers only is supported and do not have the concept of a public registry of ShoCardIDs [20].

### **2.2.4      A Comprehensive Integration of National Identity with Blockchain Technology [16]**

This paper has proposed a model where utilization of blockchain technology in national identity system. This entire national identity system will be digitized to allow every user to hold their national identity system on their own mobile device. Regime officials are able to check the user' identity by scanning the QR code or the barcode. The strength of the system is transparency can be achieved between the citizens and government. The entities present in the blockchain will be the citizens of the country and the government where it is a hierarchical system.

A hierarchy will be engendered by the proposed module where only authorised officials are able to access legitimate or personal information of a specific user. The application consists of a feature where the application is able to grant officials to access the particular information only for period of time set. Any entity who view or access the information will be updated and recorded in the ledger. It is a public ledger where all activities being performed in the national identity portal are being tracked therefore the system is able to guarantee there will be no illegal or unethical operations can be carried out by an individual. The government officials will be placed on top of the system in the hierarchy of the system. This is because supplemental feature is allowed so that funds can be transferred, and important identity documents can be uploaded to the system therefore all nodes in the network will be notified of any updates.

Different entities will have different contracts therefore the function of different entities varies. More features will be given to the government and the user will have features such as send, receive, revoke, grant, and transfer. After any variations in information all involved entity will be notified, and the system will have triggers. A unique blockchain address will exist in each entity, and the use of multichain will be developed in this model.



*Figure 2-5 Data flow in blockchain application*

Based on **Figure 2-5**, generic flow of data in blockchain applications is illustrated. Higher level semantics are provided by the blockchain overlay network where multiple types of blockchain including vertical specific blockchain, private blockchain and public blockchain are allowed to provide management abstraction and co-exist. Handshake logic which is carried out between the nodes is specified by the blockchain message exchange and also the serialization format of the message to be exchanged across the wire.

In the terms of digital identity, the strength of the proposed model is where blockchain technology have made digital identities to be tracked and monitored in a



much-secured manner which results in reduce in fraud commitment in industries such as citizenship documentation, national security, healthcare, banking and many more. Identity authentication can be carried out to be proof the identity of a specific citizen. The proposed model is able to authenticate identity uniquely in an immutable, secure and irrefutable manner. Digital signatures are all also utilized for authentication which is through public key cryptography. For the blockchain authentication of identity, the right private key must be used to sign the transactions and only the owner will be having the private key. Endless applications associated with the government sector can be used with blockchain technology including the birth certificates, citizen identity and passports. But one weakness is that, although users are able to hold the national identity system at their own mobile device, they still will not have control over their identity claim details. The system will be the one able to grant officials to access the particular information of the users.

### 2.2.5 Summary

**Comparison Table:**

	2.1	2.2	2.3	2.4	Proposed Project
Users able to submit identity claims regarding his personal details	✓	✓	✓	✓	✓
View Identity Claim Records	✓	✓	✓	✓	✓
Smart contracts are used for verification process.	✓	✓	✗	✓	✓
Users able to have full ownership and control over identity claims. (Self-sovereign identity)	✓	✓	✓	✗	✓
User's registered identity claims can be verified by trusted issuing authority.	✓	✗	✓	✓	✓

Digital wallet that acts as reference place to store and manage identity claims.	✓	✓	✗	✗	✓
Legal institution can select and send access request towards user's identity claim details.	✗	✗	✗	✗	✓
Log-in page to control access of different functionalities for different roles	✓	✓	✗	✗	✓
User friendly interface to allow users to interact with the blockchain network easily.	✗	✓	✗	✗	✓

*Table 2-1 Comparison Table*

Based on the comparison table, my proposed system will consist most of the functions and features that other identity management solutions using Blockchain technology have. However, something different from my proposed project compared to other solutions is my system can support three different roles for the identity management process, which are user, issuing authority and service provider (Legal Institution). This is where three roles are connected in one system. Before being able to access to the identity management web portal (my proposed system), users are required to register or log-in themselves according to their specific roles in order to access their functionalities they intend to perform in my proposed system. This characteristic can be an advantage for the government sector or legal institutions as it brings convenience as well as saves time and cost in terms of identity processing and management, without the need to separate these three roles into three different systems or different intermediaries. Most of the compared identity management solutions using blockchain does not have this characteristic.

Besides that, although most of the systems compared earlier are in mobile application based, my proposed identity management decentralized application will be developed as web based. I choose to develop my system as web based as Blockchain technology is one of the latest trends in the web development industry. Most important fact, my proposed system does not need to be downloaded or installed as it can be used at web browser directly, which is much more convenient for users. This fact is where my system does not need to have any application store approval so it can

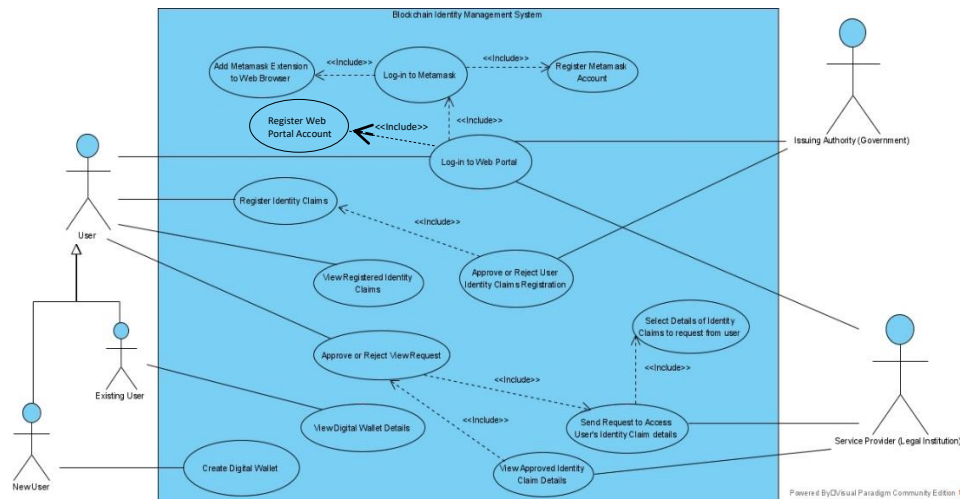
be launched directly. The web application is also easy to maintain as they have a common codebase regardless of mobile platform. The web portal is also user friendly that allow users to interact with the system and blockchain network easily with simple steps.

Moreover, something different regarding the sharing of user's identity claim details is service provider or legal institution can select which user identity claim details to view and send that access request to the users. This way users will not need to share all details to others, only with the one required by the legal institution. And also, only users' approved access request details can only be viewed by legal institution. In this way, users still have control over their identity claims. Other compared identity management solutions require users themselves to send their identity claim details to others.

## Chapter 3: System Methodology/ Approach

### 3.1 System Design Diagram/ Equation

#### 3.1.1 Use-Case Diagram for Proposed Blockchain Identity Management System



**Figure 3-1 Use Case Diagram for Blockchain Management System**

<b>Use case</b>	Log-in to web portal
<b>Purpose</b>	<p>Allow users to access the Blockchain Identity Management System.</p> <p>User who does not own any web portal account is unable to have access to the system. He is required to register himself a web account.</p> <p>Before user register or log-in to the web portal, user is required to log-in to their Metamask account. For user who does not own a Metamask account is required to install the Metamask extension on the web browser. After the installation, user is then required to register an Metamask account. After user has registered or logged-in to web portal account, user is then able to access the system.</p>
<b>Actor</b>	User, Issuing Authority (Government), Service Provider (Legal Institution)
<b>Trigger</b>	When user starts the web portal.
<b>Main flow</b>	<ol style="list-style-type: none"> <li>1.Go to log-in page of the web portal.</li> <li>2.User/ Issuing Authority/ Service Provider log-in to their Metamask account.</li> <li>3.User/ Issuing Authority/ Service Provider install Metamask extension on web browser and register a Metamask account. (If don't have any)</li> </ol>

	<p>4. User/ Issuing Authority/ Service Provider log-in to their account.</p> <p>5. User/ Issuing Authority/ Service Provider register a web portal account. (If don't have any)</p> <p>6. System allow User/ Issuing Authority/ Service Provider to access the web portal.</p>
<b>Alternate flow</b>	4a. System does not allow User/ Issuing Authority/ Service Provider to access web portal if account is invalid.

**Table 3-1 Log-in to web portal**

<b>Use case</b>	Create Digital Wallet
<b>Purpose</b>	Allow new user to create a digital wallet that is used to store the identity claims. Single user account can only create a single digital wallet.
<b>Actor</b>	New User
<b>Trigger</b>	When user access the web portal for the first time after fresh registration.
<b>Main flow</b>	<ol style="list-style-type: none"> <li>1. After registration of web portal account and access to the web portal, user will be brought to the create digital wallet page.</li> <li>2. New user is required to create a digital wallet by keying in details like full name, email address and mobile number.</li> <li>3. New user is required to accept the transaction from Metamask account in order to store digital wallet on Ethereum Blockchain.</li> <li>4. New user can view their digital wallet details at the wallet section once has successfully created a digital wallet.</li> </ol>
<b>Alternate flow</b>	3a. System fails to create user digital wallet if user reject transaction from Metamask.

**Table 3-2 Create Digital Wallet**

<b>Use case</b>	View Digital Wallet Details
<b>Purpose</b>	Allow users to view the details of the digital wallet they have

	created as reference.
<b>Actor</b>	Existing User
<b>Trigger</b>	When user go to the wallet section by clicking the option on the menu header bar.
<b>Main flow</b>	1. Go to wallet section in the web portal to view digital wallet details user has created previously.
<b>Alternate flow</b>	1a. System unable to display any digital wallet details if user has not created a digital wallet.

*Table 3-3 View Digital Wallet Details*

<b>Use case</b>	Register Identity Claims
<b>Purpose</b>	Allow user to create claims of his different identity asset such as identity card, driving license, birth certs etc.
<b>Actor</b>	User
<b>Trigger</b>	When user click on the create identity button at the identities section option.
<b>Main flow</b>	<ol style="list-style-type: none"> <li>1. Go to identities section in the web portal.</li> <li>2. Click on create identity button.</li> <li>3. Register an identity claim by filling in details like identity description, identity number, full name, date of birth and address.</li> <li>4. User is required to accept the transaction from Metamask account in order to store identity claims on Ethereum Blockchain.</li> </ol>
<b>Alternate flow</b>	4a. System fails to help user register their identity claim if user rejects transaction from Metamask.

*Table 3-4 Register Identity Claims*

<b>Use case</b>	View Registered Identity Claims
<b>Purpose</b>	Allow user to view claims of his different identity asset.
<b>Actor</b>	User
<b>Trigger</b>	When user click on identities section on the menu header bar.

<b>Main flow</b>	<ol style="list-style-type: none"> <li>1. Go to identities section in the web portal.</li> <li>2. View list of registered identity claims.</li> </ol>
<b>Alternate flow</b>	2a. System will not display any identity claims if user has not registered an identity claim before.

*Table 3-5 View Registered Identity Claims*

<b>Use case</b>	Approve or Reject View Request
<b>Purpose</b>	Allow user to have control over their identity claim details whether to allow outsiders to access them.
<b>Actor</b>	User
<b>Trigger</b>	When user click on view access request section on the menu header bar.
<b>Main flow</b>	<ol style="list-style-type: none"> <li>1. Go to view access request section in the web portal.</li> <li>2. View list of requested identity claim details.</li> <li>3. Approve or reject the access.</li> </ol>
<b>Alternate flow</b>	<p>2a. System will not display any request if there are no outsiders request for the identity claim details.</p> <p>3a. User unable to approve or reject access if service provider does not send request.</p>

*Table 3-6 Approve or Reject View Request*

<b>Use case</b>	Approve or Reject User Identity Claims Registration
<b>Purpose</b>	Allow trusted issuing authority such as the government to verify whether user's registered identity claims are valid and trustable.
<b>Actor</b>	Issuing Authority (Government)
<b>Trigger</b>	When issuing authority click on approve or reject button at registered identity claims list.
<b>Main flow</b>	<ol style="list-style-type: none"> <li>1. View registered identity claims list once access to account on web portal.</li> <li>2. Verify validity of user's registered identity claims by clicking either approve or reject button.</li> </ol>
<b>Alternate flow</b>	1a. System will not display any registered identity claims if user

	does not register any.
--	------------------------

**Table 3-7 Approve or Reject User Identity Claims Registration**

<b>Use case</b>	Send request to Access User Identity Claim Details
<b>Purpose</b>	Get permission from user to access user's private and personal identity claim details
<b>Actor</b>	Service Provider (Legal Institution)
<b>Trigger</b>	When service provider clicks on the send request button after selecting the details they want.
<b>Main flow</b>	<ol style="list-style-type: none"> <li>1. Select details of user's identity claim to request to from user for approval.</li> <li>2. Send request once finish selection of details by clicking the send request button.</li> </ol>
<b>Alternate flow</b>	None

**Table 3-8 Send request to Access User Identity Claim Details**

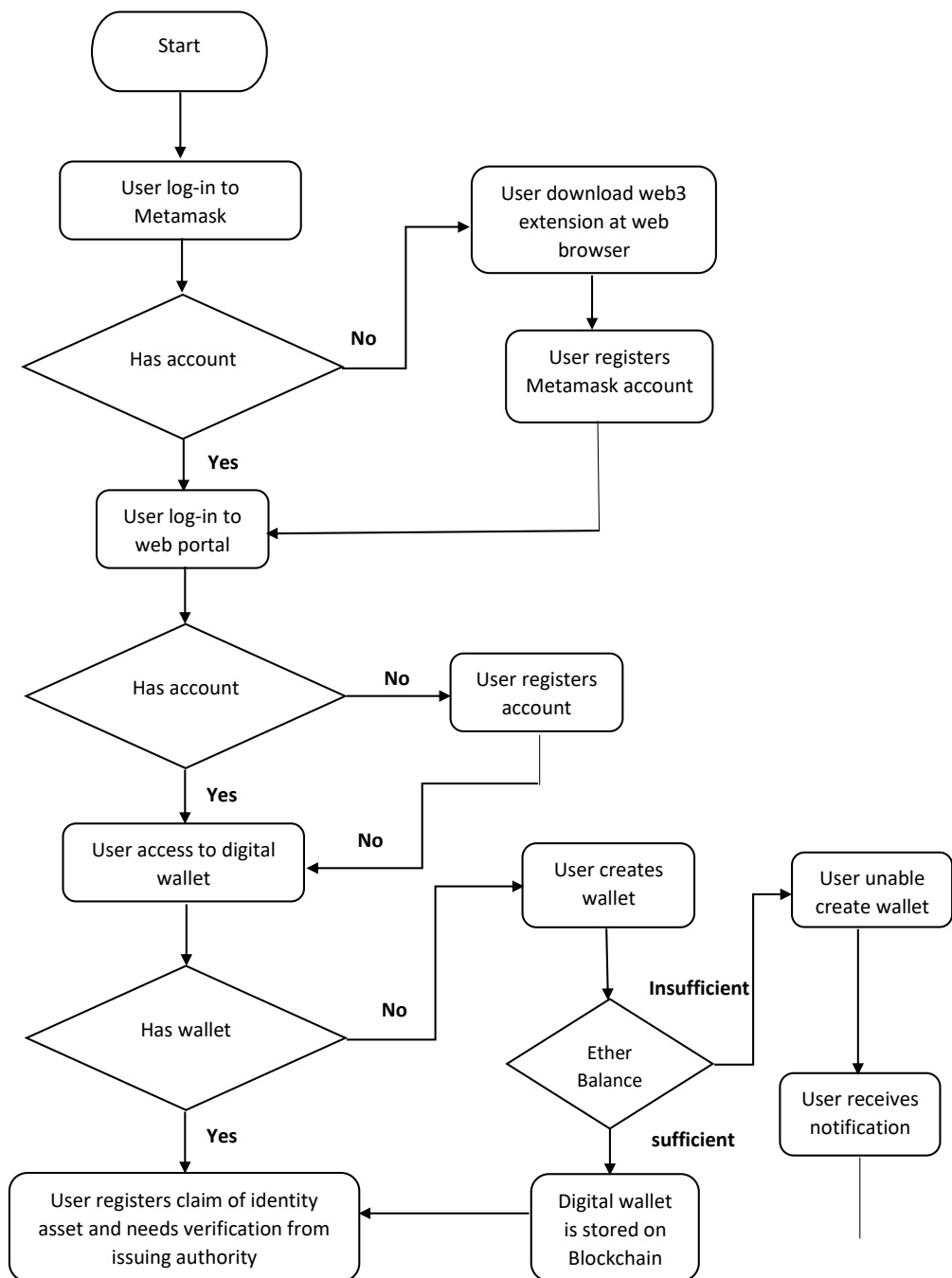
<b>Use case</b>	View Approved Identity Claim Details
<b>Purpose</b>	Allow service provider only access user approved identity claim details only.
<b>Actor</b>	Service Provider (Legal Institution)
<b>Trigger</b>	After service provider access to their account on the web portal.
<b>Main flow</b>	<ol style="list-style-type: none"> <li>1. Log-in to their web portal account.</li> <li>2. View details approved by the user.</li> </ol>
<b>Alternate flow</b>	2a. System will not display any user's identity claim details if user does not approve access of the service provider towards the details.

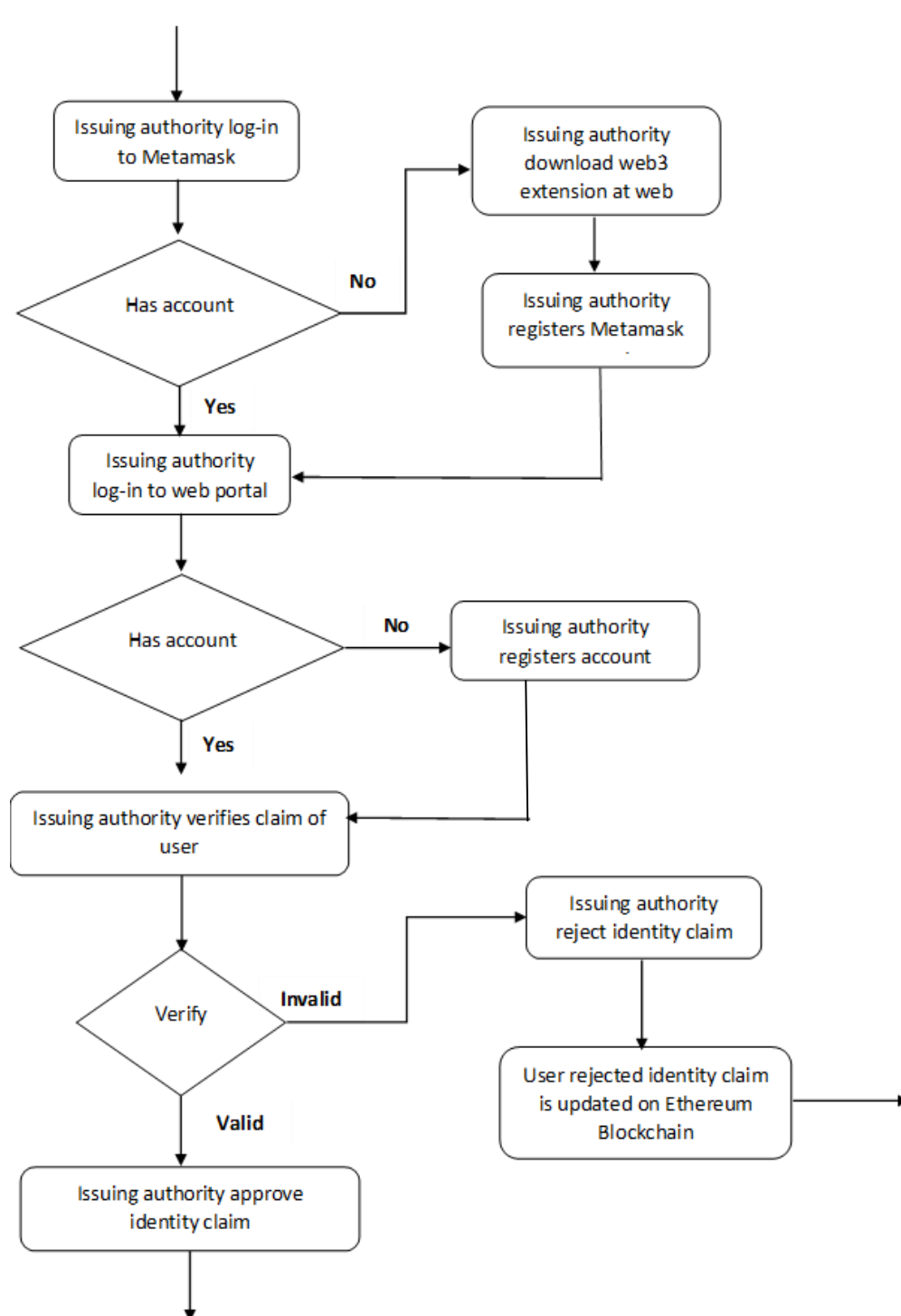
**Table 3-9 View Approved Identity Claim Details**

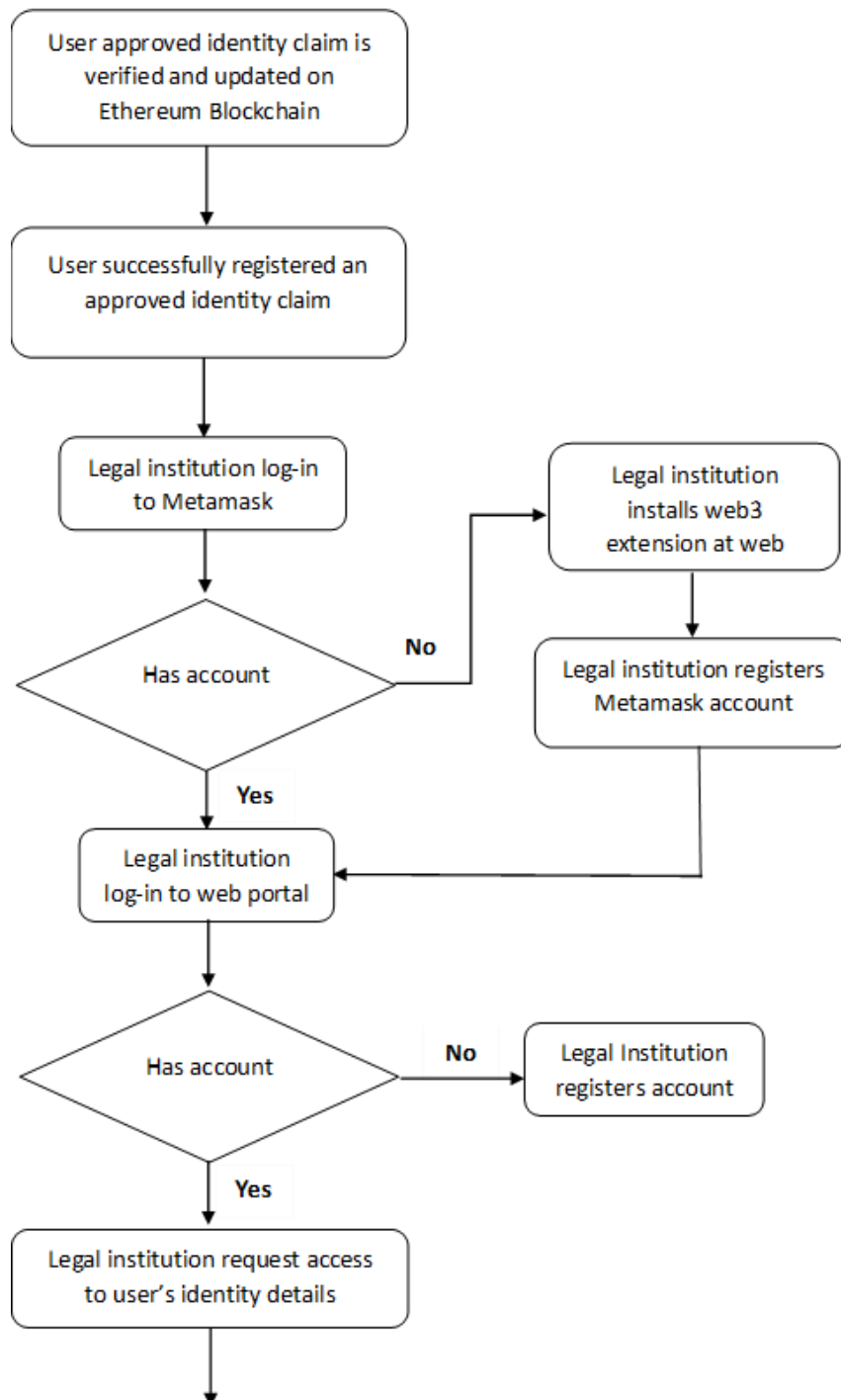
## Chapter 4: System Design

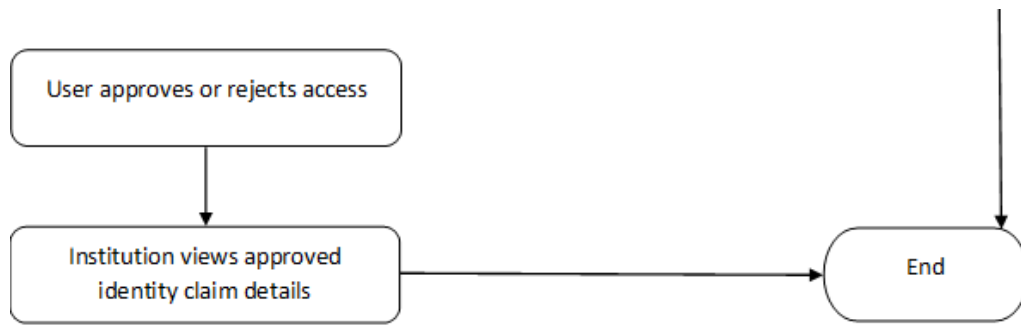
### 4.1 System Flowchart Design











*Figure 4-1 System Flowchart Diagram*

## **4.2 System Flowchart Design Description**

Firstly, users are required to log-in to their Metamask account. For users who do not own a Metamask account are required to install the Metamask extension on the web browser. After the installation, they can then register their Metamask account. After users logged-in to the Metamask account, users are required to log-in to the blockchain identity management web portal. However, for new users who do not own a web portal account are required to register one before accessing the portal.

After users have successfully logged-in, users will then access their digital wallet. For new users, they are required to create a digital wallet which is used to store their identity claims/documents. Users need to ensure that their Metamask wallet has enough balance of ether to make the payment for digital wallet creation. After the users have accept the transaction from Metamask, the digital wallet is then created and stored on the Ethereum Blockchain. A single user can only have a single digital wallet.

When there is a digital wallet exists on the users' account, user is then able to register claims of their different identity assets. Users are required to key in the necessary information for a claim such as identity card claim (E.g.: identity description, identity number, name, date of birth, address etc.). After user has completed the registration, user's registered identity claims are needed to be verified by issuing authority (Government).

Issuing authority are required to log-in to their Metamask account. For users who do not own a Metamask account are required to install the Metamask extension on the web browser. After the installation, they can register their Metamask account. After log-in to the Metamask account, issuing authority can view and verify the user's claim

registration at the web portal by logging-in to their web portal accounts. For new users of the issuing authority, they are required to register an account before having access to the portal. After they have successfully accessed the web portal, they are able to view the claims from the user and verify the details of the user by either approving or rejecting the claim. User's fingerprint will act as the base of verification (source of proof) in order for the government to approve the validity of the identity claims provided by the user. The government side will compare the fingerprint provided by the users with the one stored at the old database to see whether they match using its AI system. Only when the matching percentage of the two fingerprints reaches a certain range (e.g.: 95% – 100%) , the government will then approve the validity of the identity claim.

Back to the user side, user can check their identity claim status at their registered identity claims list to see whether it is approved or rejected. When user's claim has been approved by issuing authority, user's identity claim is then updated as approved on the Ethereum Blockchain. User has then successfully registered an approved identity asset claim. Now user will have full control over the details of his identity claim.

Legal institution can request for user's identity claim details by logging-in to their accounts of the web portal. Before logging-in to the web portal, they are required to log-in to their Metamask account. For legal institution who do not own a Metamask account are required to install the Metamask extension on the web browser. After the installation, they can register their Metamask account. For new users of the institution, they are required to register a web portal account to access the portal. Now, legal institution can request access for user's identity claim details.

Back to user side, users can view and approve access of the institution after legal institution have sent their request access. User can choose to approve when he is willing to share his assets to the institution. This shows that users are now having a self-sovereign identity. Legal institution can then access and view approved identity claim of the user.

### **Comment and highlight the feasibility of the proposed method**

The proposed method used in this project is the prototyping-based methodology under the Rapid Application Development (RAD) methodology category. The prototype shown below is the system design of my proposed system (Blockchain Identity Management System) which is designed and developed according to the prototyping-based methodology. After undergoing the first phase of the methodology which is planning and requirement gathering, I have identified that the main values of system that is able to deliver to the audience which are high security, trust, and timesaving and cost effective. Values delivered complies to the problem statements to be solved stated earlier. The proposed project is also achievable in terms of money, technical, time, and results after carrying out the feasibility analysis.

The image shows a wireframe prototype of a system interface. It consists of a rectangular frame containing the following elements:

- Title Bar:** A horizontal bar at the top labeled "Title (System Logo)".
- Menu Bar:** A row of five buttons, each labeled "Function".
- Right Button:** A button with a plus sign icon and the label "+ Button" located to the right of the menu bar.
- Content Area:** A large rectangular area below the menu bar, divided into two horizontal sections by a single line.

***Figure 4-2 Prototype Development Example***

While for the second phase, analysis, design and implementation (prototype development), a simple and quick prototype design is developed and evaluated by the user based on user requirement. Some refinement will be carried out by incorporating user's suggestion. Figure 4(a) shows the final simple system prototype design that is accepted by the user after some refinement.

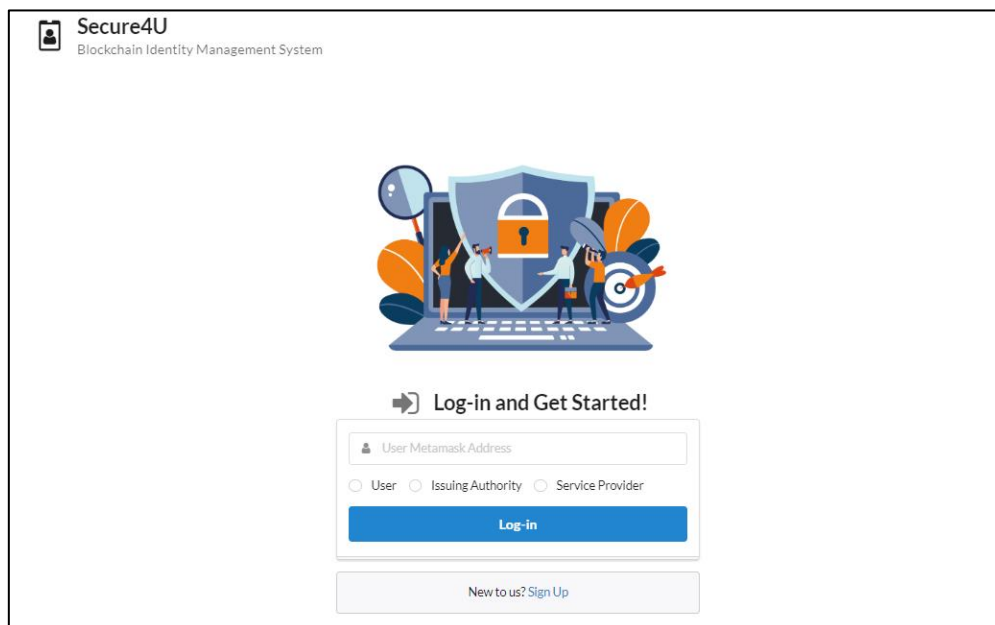
Next, proceed to the last phase, which is design, implementation, testing, maintenance (Iterative Development). A proper and potential system design is then developed after alternative design exploring at the design phase. After that, the development and testing process in building elements of the system are carried out concurrently based on the final system design. Results of the preliminary work obtained is shown at the system prototype section (below). In conclusion, the proposed

method is highly feasible towards my proposed project. The results obtained shows that the method used is effective and efficient in terms of project development cost and procedures, which makes the system development to be performed successfully.

### **4.3 Graphical User Interface of Blockchain Identity Management System**

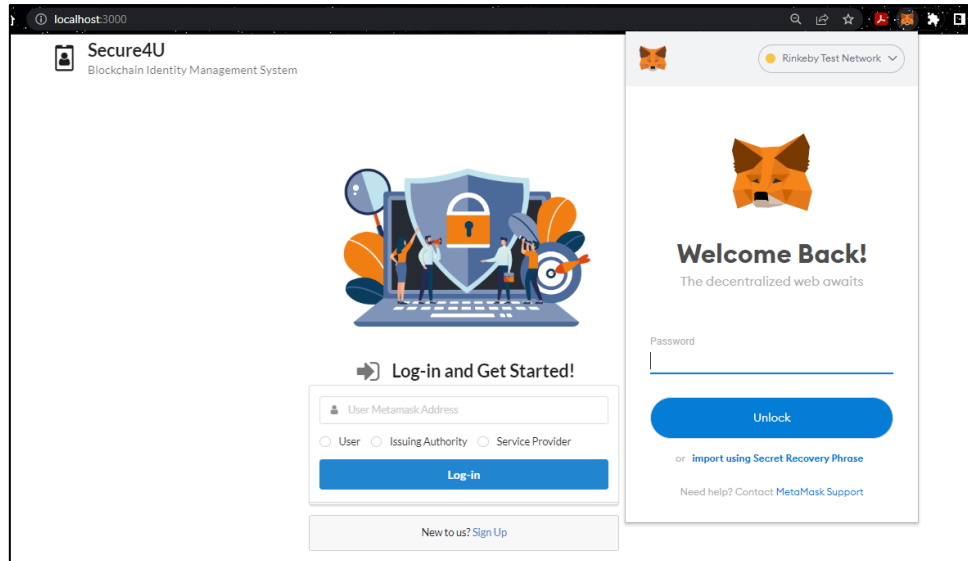
This part will be displaying the system design as well as demonstrating the work flow of my proposed system.

#### **User Role:**



***Figure 4-3 Log-In Page***

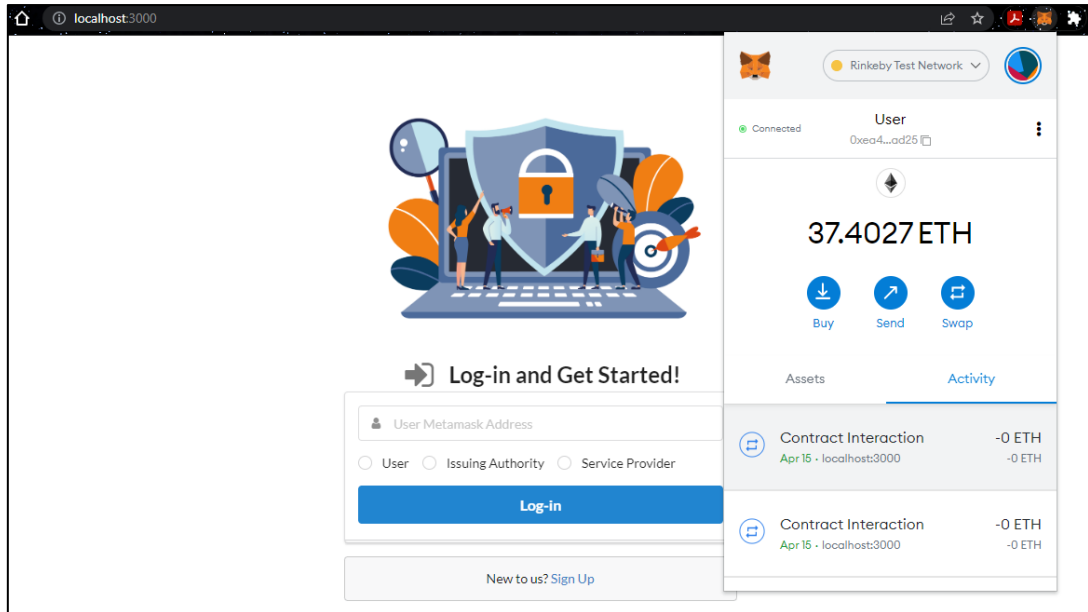
Firstly, a log-in page will be displayed as the starting of the system. Different roles of users are required to log-in to the system by entering their meta mask account address as well as selecting their respective roles in order to access their respective functionalities through the system. There is no password required to log-in as the log-in feature of the system is linked to the metamask account from the metamask web extension.



**Figure 4-4 Log-In Page (Metamask Web Extension)**

All types of users of the system are required to log-in to their metamask account through the web extension as displayed in **Figure 4-4**, before users are able to access the system by entering their own metamask account address. They are either required to log-in through their passwords or import using their secret recovery phase. Secret recovery phase is an alternative that are used only when users have forgotten their passwords. For new users who do not own a metamask account are required to install the metamask web extension through chrome. Metamask is quite important not only to access the system, but it is also a software cryptocurrency wallet that is used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.





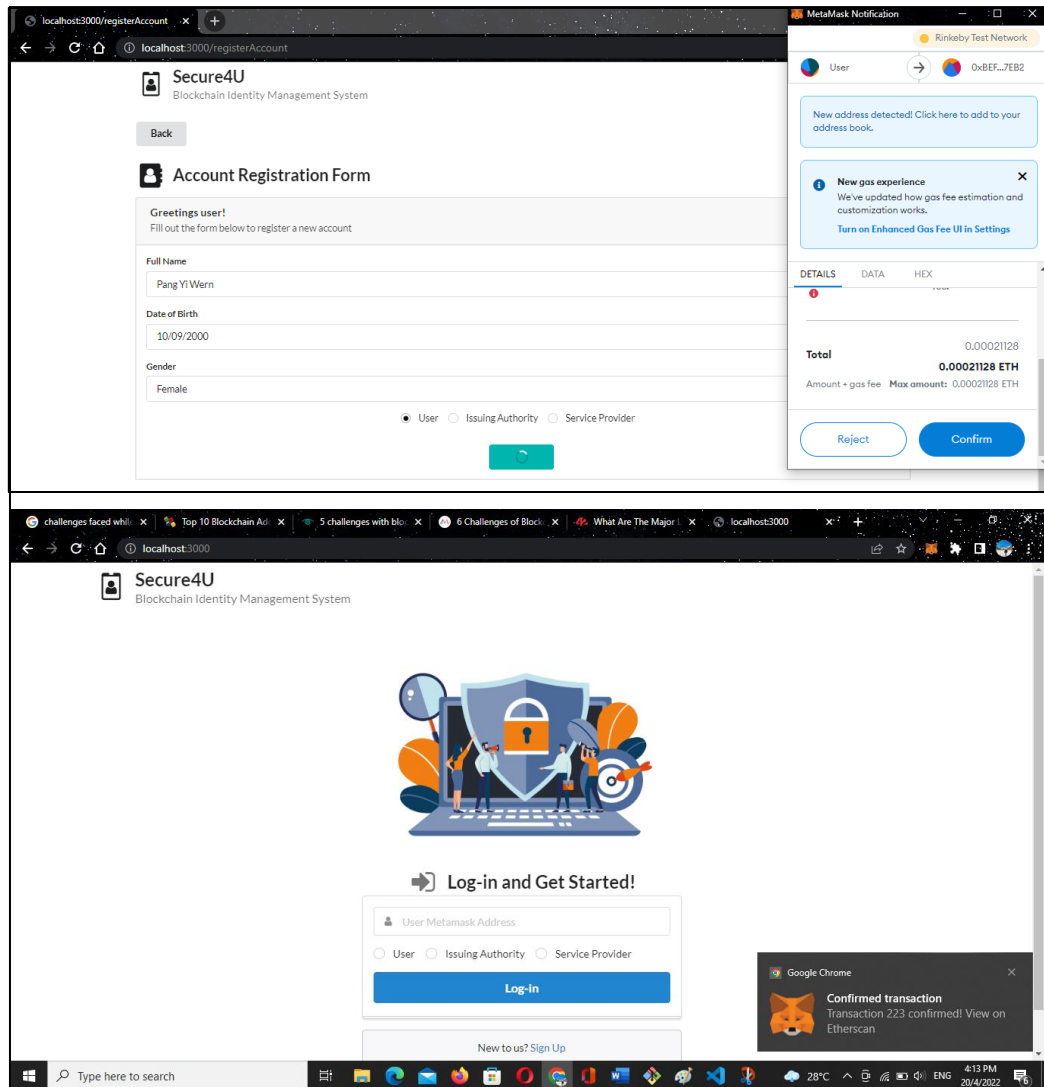
**Figure 4-5 Log-In Page (Metamask Account)**

Based on **Figure 4-5**, after users have logged-in to their metamask account, they will then be brought to their account that is used to access the rinkeby test network (blockchain test network) and to store ether for blockchain transactions. For existing system users, they are now able to log-in to the system by entering their account address and selecting their roles after accessing their metamask account. For new users, they are required to sign up by clicking the sign-up link tag as shown.

 The image shows a web form titled "Secure4U Blockchain Identity Management System". It has a "Back" button and a "Account Registration Form" header. Below the header is a message "Greetings user! Fill out the form below to register a new account". The form contains three input fields: "Full Name" (with the text "Lily Tan"), "Date of Birth" (with a placeholder "DD/MM/YYYY"), and "Gender" (with a placeholder "Male/ Female"). Below these fields are three radio buttons: "User", "Issuing Authority", and "Service Provider". A green "Register" button is at the bottom of the form.

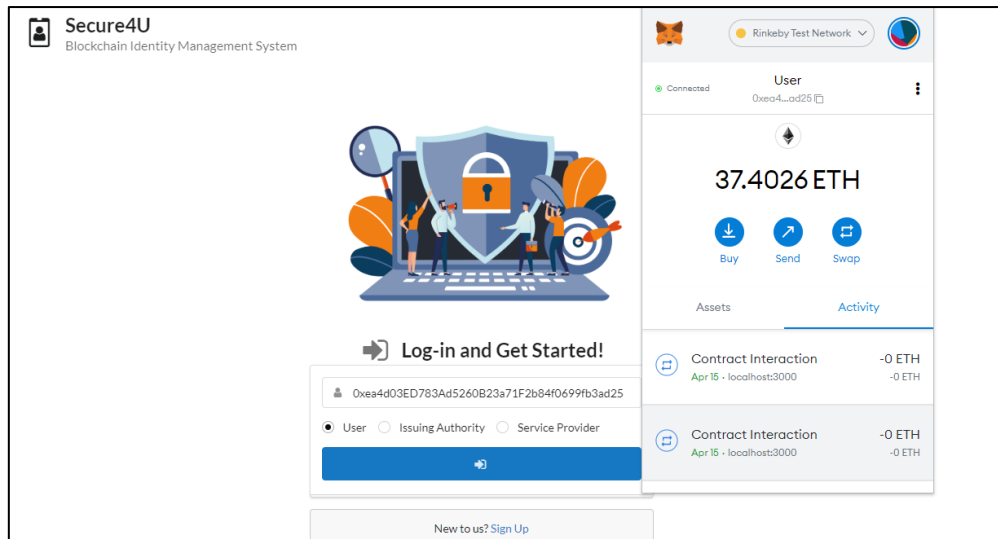
**Figure 4-6 Account Registration Form**

After clicking the sign-up link tag, users will then be brought to the account registration page. Users are required to fill in the account registration form as displayed in **Figure 4-6**.



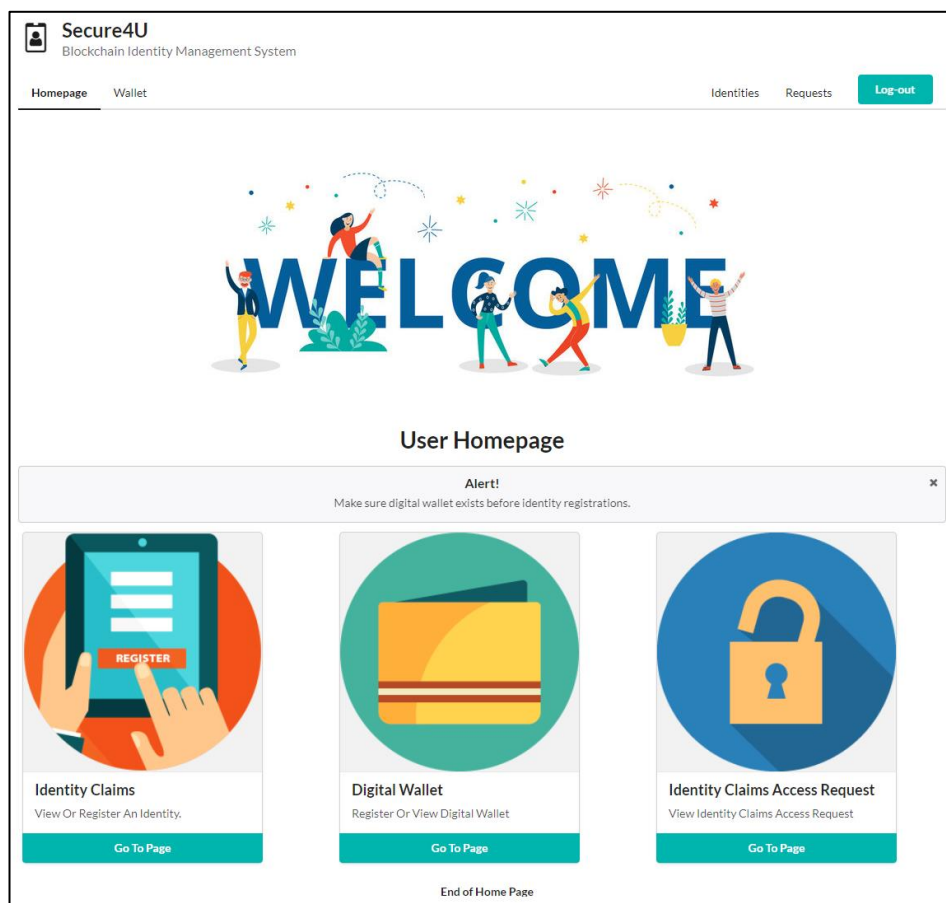
**Figure 4-7 Account Registration Form (Metamask Transaction Confirmation - User)**

When users are done filling up their form, they may then click the register button. A notification from metamask will pop up asking users for transaction confirmation as well as showing the amount required for the transaction (refer to **Figure 4-7**).



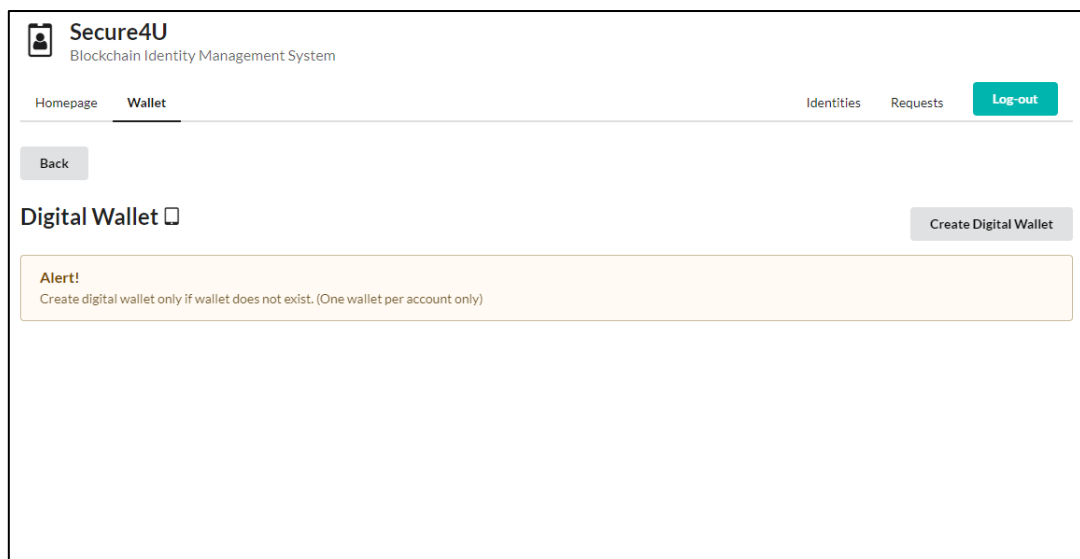
*Figure 4-8 User Log-In*

After the transaction has been confirmed and processed, users will be brought back to the log-in page (refer to **Figure 4-8**). User's account registration details has also been stored in the Blockchain database. Users can now log-in to the system.



*Figure 4-9 User Homepage*

**Figure 4-9** shows the homepage for the role *user*. There are three functionalities can be performed for the role *user*. The identity claims function allows user to register their identity asset to the system and view their registered identity assets. Before the users can register their identity claims/ identity asset, they are first required to register their own digital wallet using the Digital Wallet function. The digital wallet will be used to store the identity assets of the users and to store the profile of the user, which contains general details of the user. While for the third function, it is used to view the requests made by legal institutions (service provider) in order to for them to access the user's identity assets.



**Figure 4-10 Digital Wallet Section**

After users have clicked the digital wallet functionality at the user homepage, they will be brought to the digital wallet page (refer to **Figure 4-10**). Users who do not owned a digital wallet can click the create digital wallet to create one.

**Secure4U**  
Blockchain Identity Management System

Homepage Wallet Identities Requests **Log-out**

**Back**

**Create your wallet here:**

Greetings user!  
Fill out the form below to create a new wallet

First Name: Lily Last Name: Tan

Email Address: xxx@gmail.com

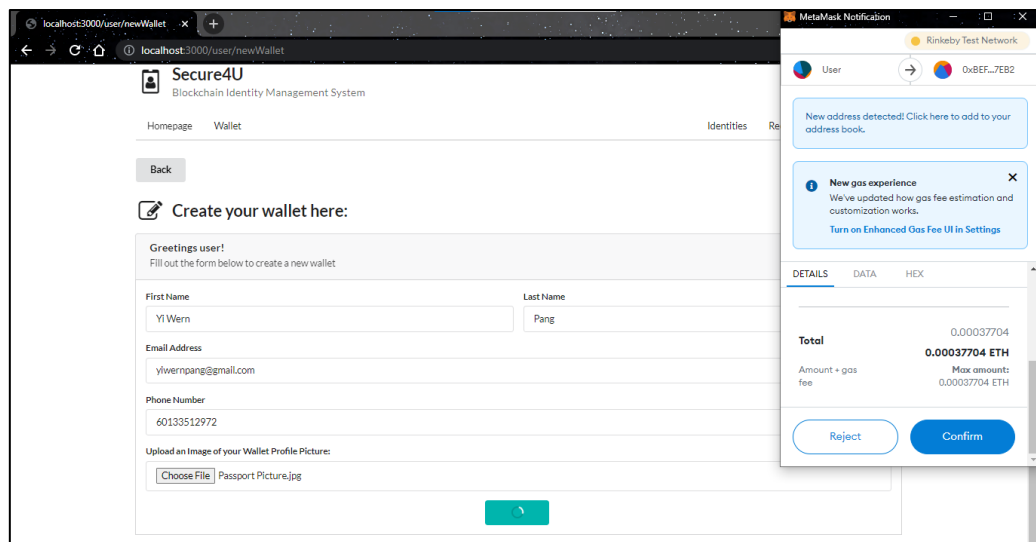
Phone Number: 601000000000

Upload an Image of your Wallet Profile Picture:  
Choose File No file chosen

**Register**

*Figure 4-11 Digital Wallet Creation*

Users will then be brought to the create wallet form after clicking the create digital wallet button (refer to **Figure 4-11**). Users are required to fill in the listed details to create the wallet.



*Figure 4-12 Digital Wallet Creation (Metamask Transaction Confirmation)*

After users have clicked the register button, a metamask transaction notification will then pop up along with the amount of ether required for the transaction (refer to **Figure 4.12**).

The screenshot displays the 'Secure4U Blockchain Identity Management System' interface. The top navigation bar includes 'Homepage', 'Wallet', 'Identities', 'Requests', and a 'Log-out' button. A 'Back' button is located on the left. The main heading is 'Digital Wallet' with a 'Create Digital Wallet' button on the right. An alert box states: 'Alert! Create digital wallet only if wallet does not exist. (One wallet per account only)'. The central section is titled 'Yi Wern Pang's Digital Wallet Details' and features a circular profile picture of a woman. To the right of the photo are four input fields containing the following information:

- Blockchain Account Address: 0xea4d03ED783Ad5260B23a71F2b84f0699fb3ad25
- Full Name: Yi Wern Pang
- Email Address: yiwernpang@gmail.com
- Phone Number: 60133512972

*Figure 4-13 Digital Wallet Details*

After the transaction has been confirmed and processed, users' digital wallet is then stored in the Blockchain database. Users will then be brought back to the digital wallet page and their registered digital wallet details will be displayed (refer to **Figure 4-13**).

The screenshot displays the 'Secure4U Blockchain Identity Management System' interface. The top navigation bar includes 'Homepage', 'Wallet', 'Identities', 'Requests', and a 'Log-out' button. A 'Back' button is located on the left. The main heading is 'List of Identity Claims' with a 'Register Identity Claim' button on the right. Below the heading is a large empty rectangular box for displaying the list of identity claims.

*Figure 4-14 Identity Claims Section*

Now users can register their identity asset by clicking the identity claims function at the user homepage (refer to **Figure 4-9**). The list of identity claims page will be displayed to the users. User can register their new identity by clicking the register identity claim button (refer to **Figure 4.14**).

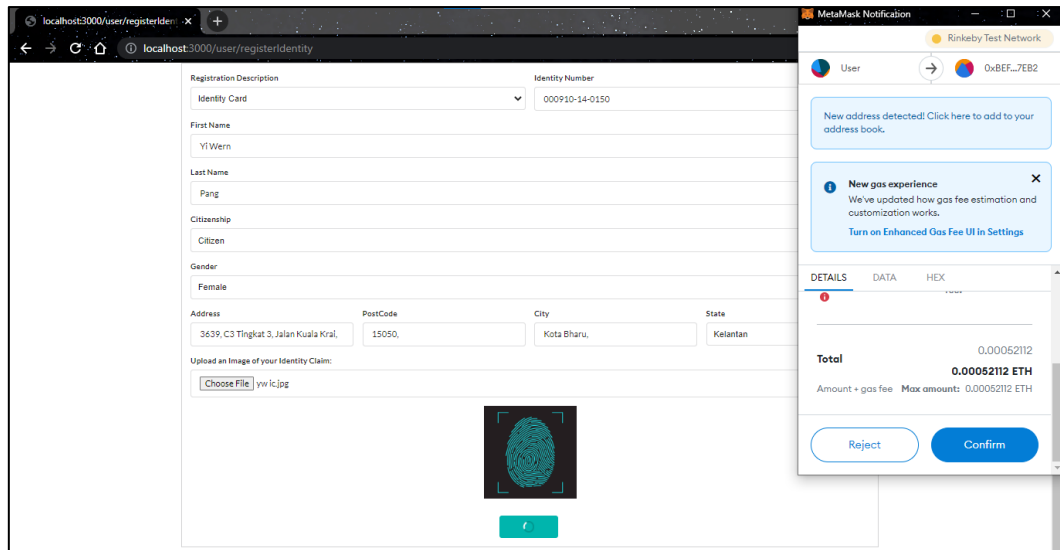
The screenshot shows the 'Identity Claim Registration Form' within the 'Secure4U Blockchain Identity Management System' interface. The form includes a 'Back' button, a 'Greetings user!' message, and instructions to fill out the form. The registration details are as follows:

Field	Value
Registration Description	.....
Identity Number	000000-00-0000
First Name	Lily
Last Name	Tan
Citizenship	.....
Gender	.....
Upload an Image of your Identity Claim:	Choose File No file chosen

Below the form fields is a fingerprint image placeholder and a 'Register' button.

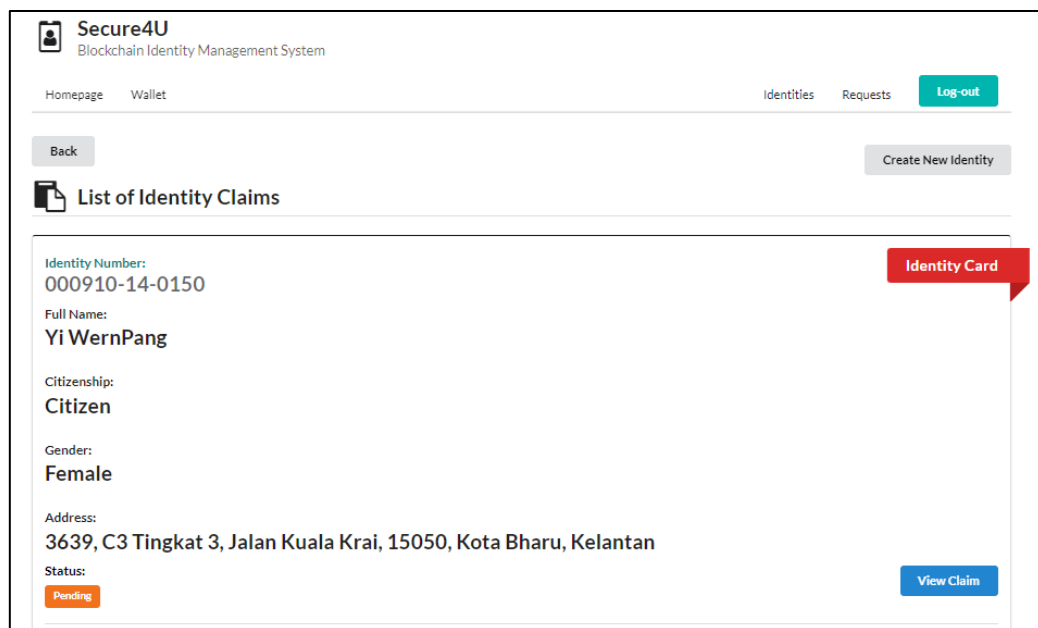
**Figure 4-15 Identity Claim Registration Form**

Based on **Figure 4-15**, after clicking the register identity claim button, an identity claim registration form will be shown to the users. Users are required to fill in the particulars required in the form such as registration description, identity number, first name, last name, citizenship, gender and uploading the image of their identity asset. The fingerprint image shown in the system is the fingerprint uploaded or scanned by the user. The usage of the fingerprint is not under the scope of my project, but it will be used while performing one of the functionalities of my system, which will be explained after.



**Figure 4-16 Identity Claim Registration Form (Metamask Transaction Confirmation)**

After users have clicked the register button, a metamask transaction confirmation will pop up along with the amount of ether required for the transaction (refer to **Figure 4-16**).

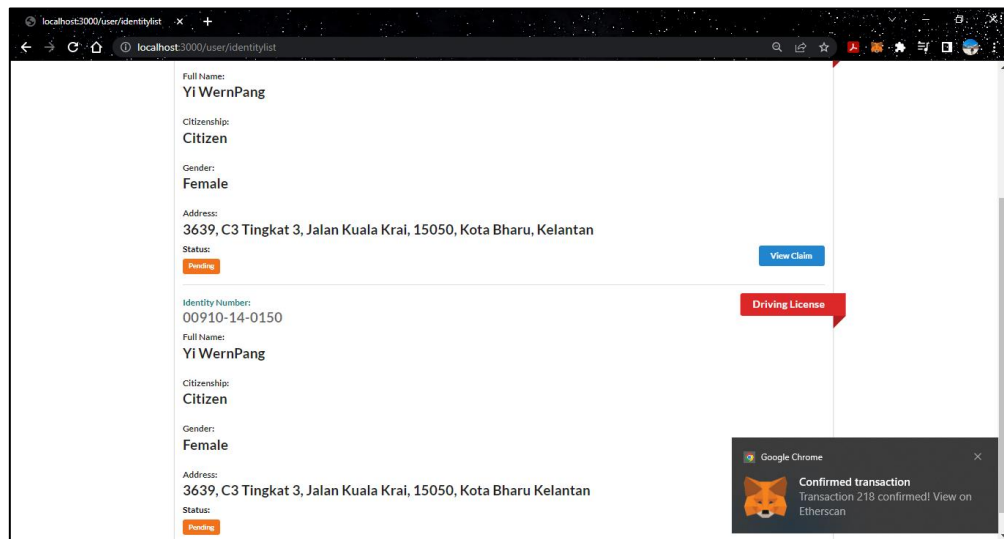


**Figure 4-17 List of Registered Identity Claims**

Based on **Figure 4-17**, after the transaction has been confirmed by the user and processed by the system, the registered identity claim will then be stored in the Blockchain database. Users will then be diverted back to the list of identity claims page. Users' registered claim will be displayed at the page with the status of pending.

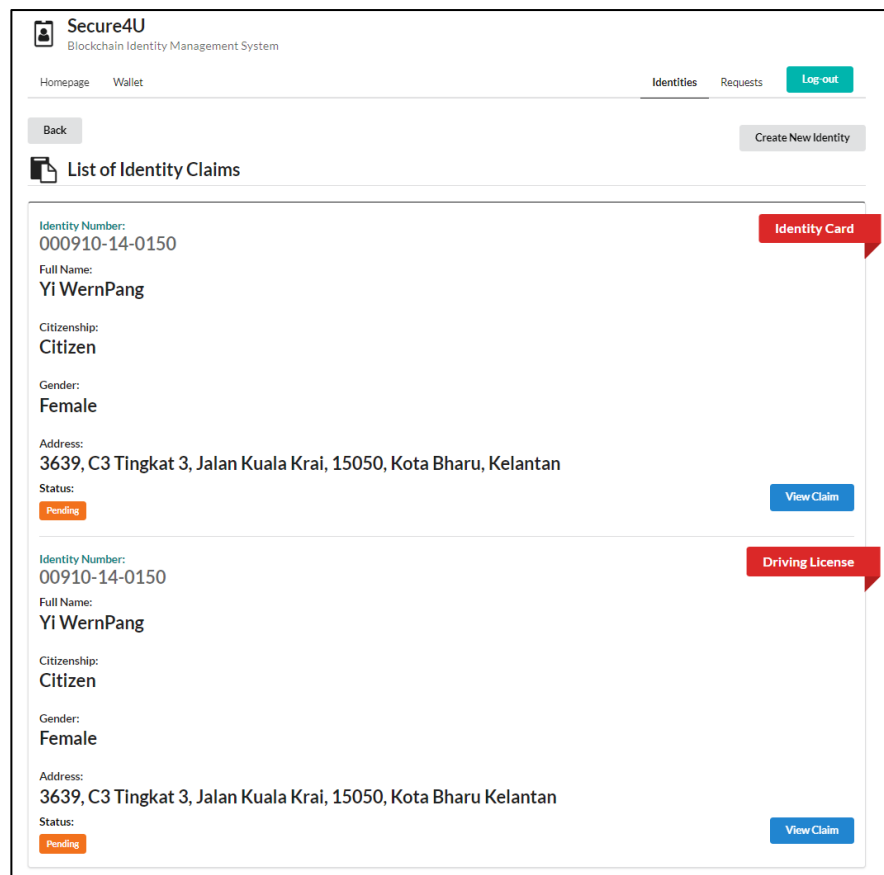


The pending status shows that the registered claim has yet to be verified by the issuing authority, which is the government.



**Figure 4-18** *Confirmed Transaction Notification*

The right bottom corner of **Figure 4-18** shows the pop-up notification from metamask that indicates that the transaction made has been confirmed. This shows up for every transaction after they are being confirmed.



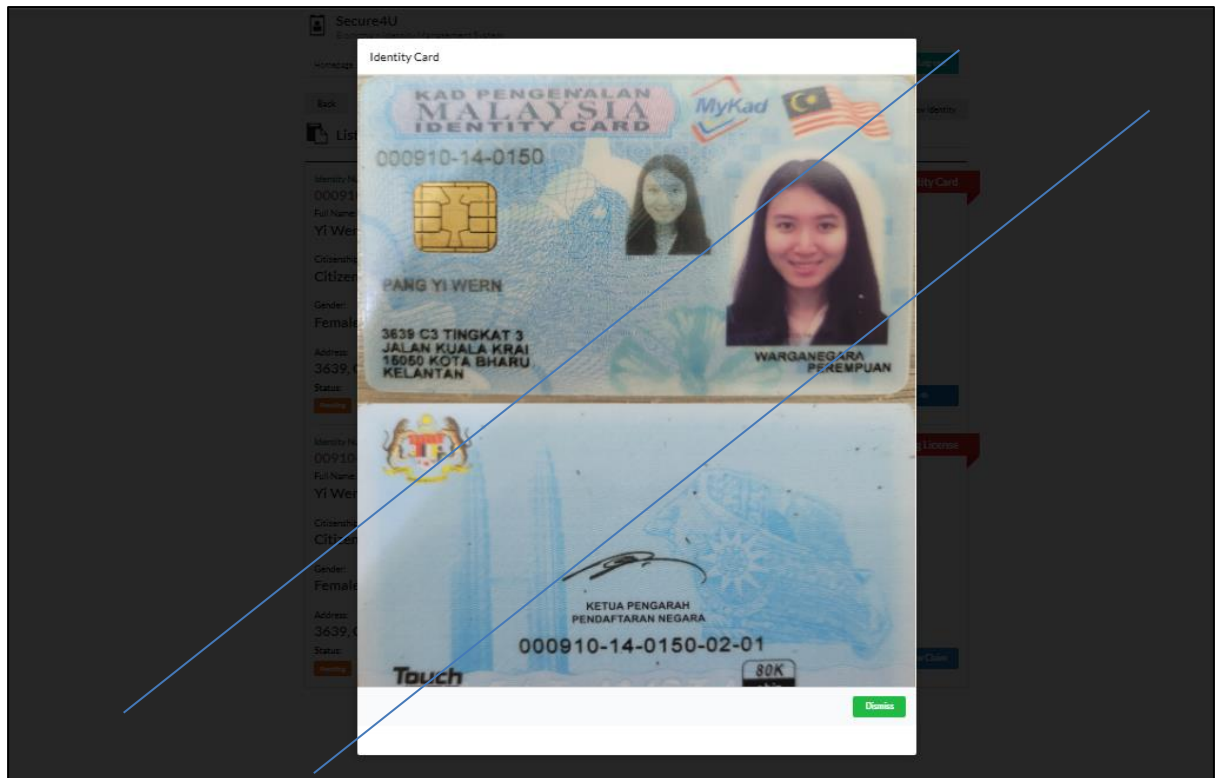
*Figure 4-19 List of Registered Identity Claims(ii)*

**Figure 4-19** shows the list of identity claims registered including the second registered identity claim (driving license).



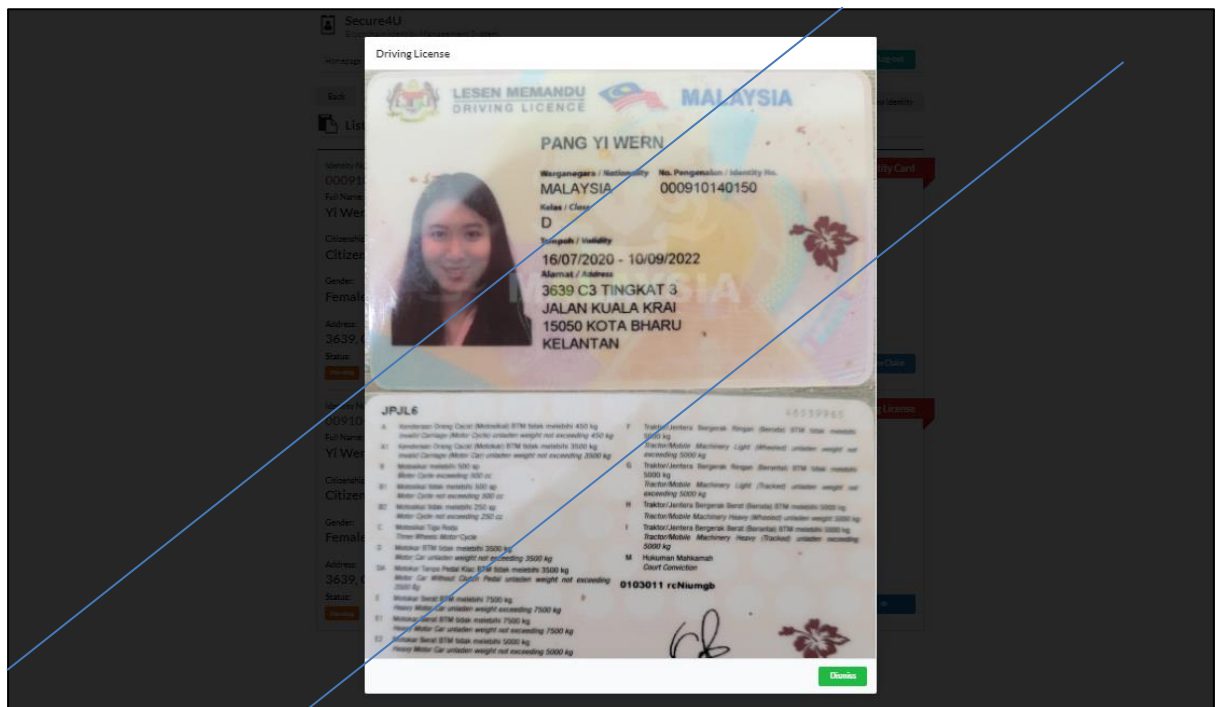
*Figure 4-20 List of Registered Identity Claims(iii)*

After users have clicked the view claim button on one of the registered identity claims, the picture of that specific claim will be displayed (refer to **Figure 4.20**).



*Figure 4-21 Identity Card Image View*

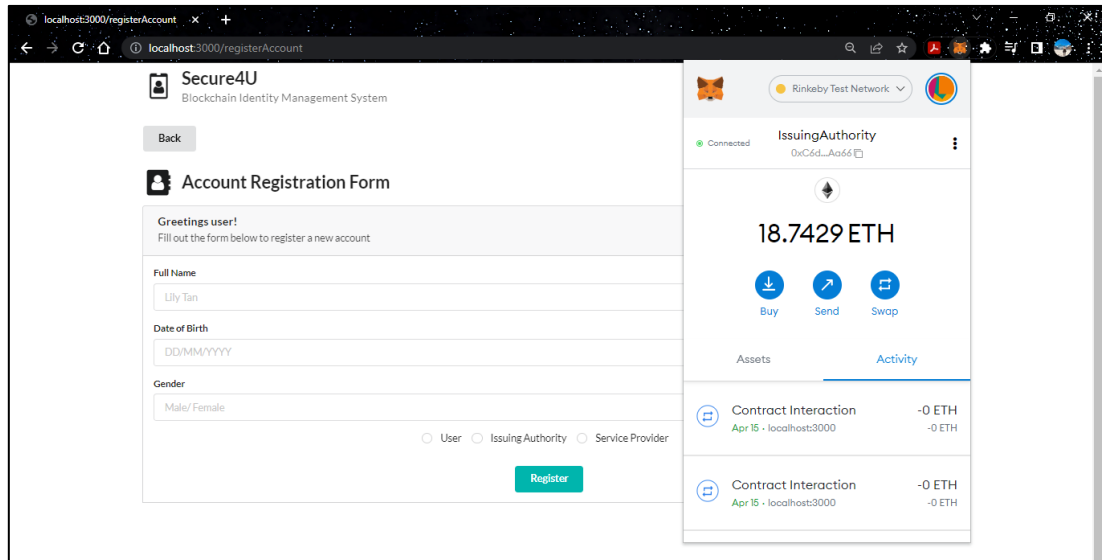
**Figure 4-21** shows the pop-up image of the identity card claim.



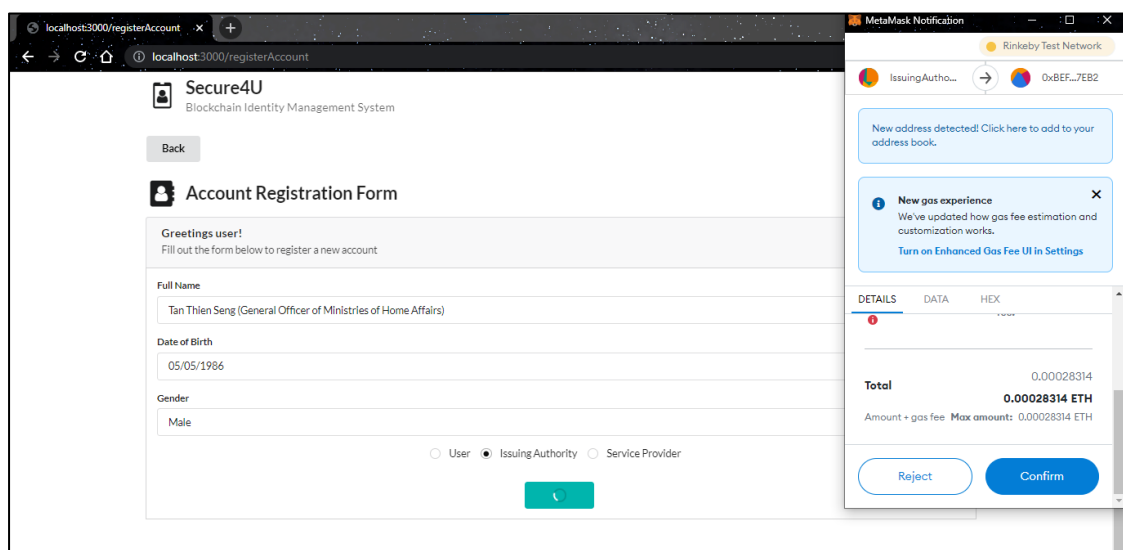
*Figure 4-22 Driving License Image View*

**Figure 4-22** shows the pop-up image of the driving license claim.

### Issuing Authority (Government) Role:



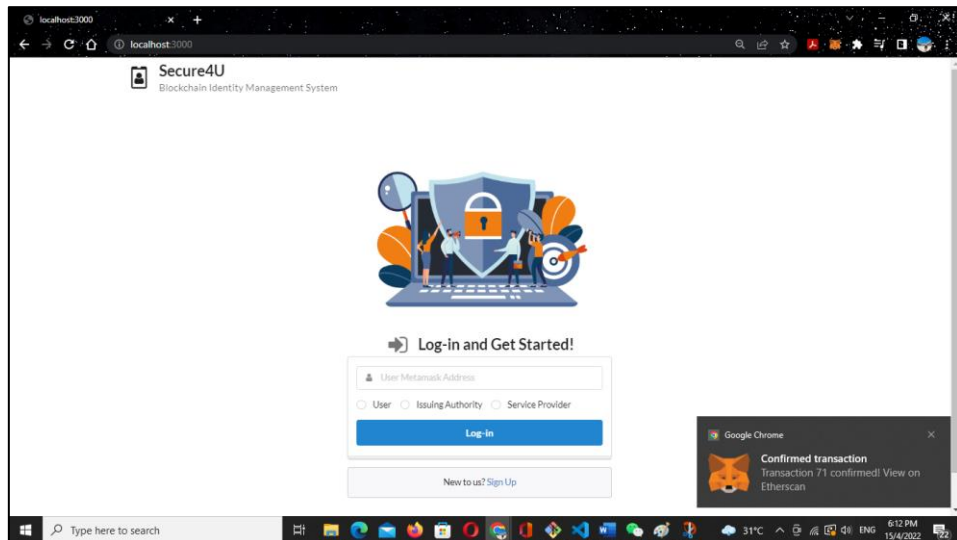
**Figure 4-23 Account Registration Form (Issuing Authority – Government)**



**Figure 4-24 Account Registration Form (Metamask Transaction Confirmation – Issuing Authority)**

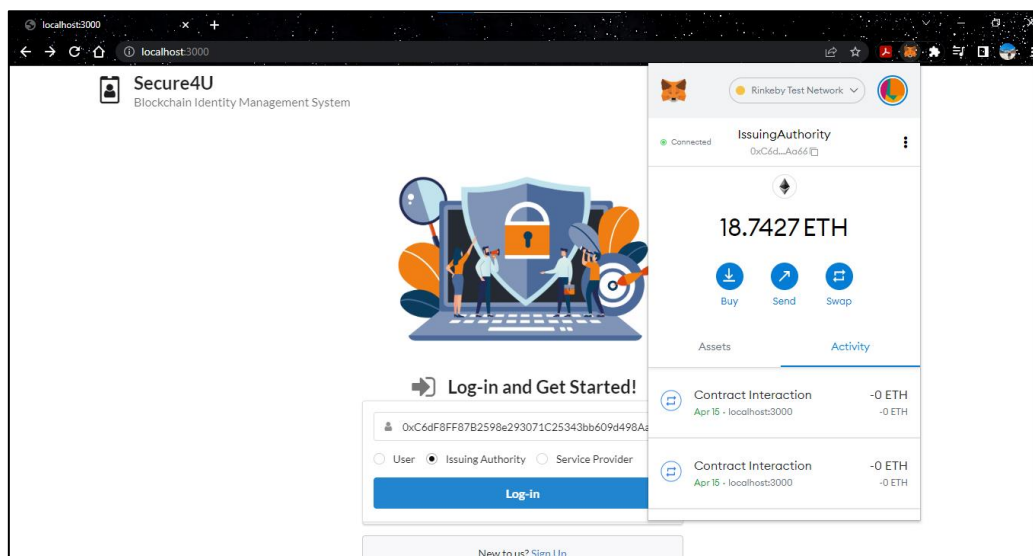
Same as the *user* role, after issuing authority have logged-in to their metamask account, they will then be brought to their account that is used to access the rinkeby test network (blockchain test network) and to store ether for blockchain transactions. For existing system users, they are able to log-in to the system by entering their account address and selecting their roles after accessing their metamask account.

While for new user of the issuing authority, they are required to sign up by clicking the sign-up link tag at the log in page. Account registration form will then be displayed. New user of the issuing authority needs to fill in the details and click register after completing the form. A metamask transaction confirmation will then pop up (refer to **Figure 4-23** & **Figure 4-24**).



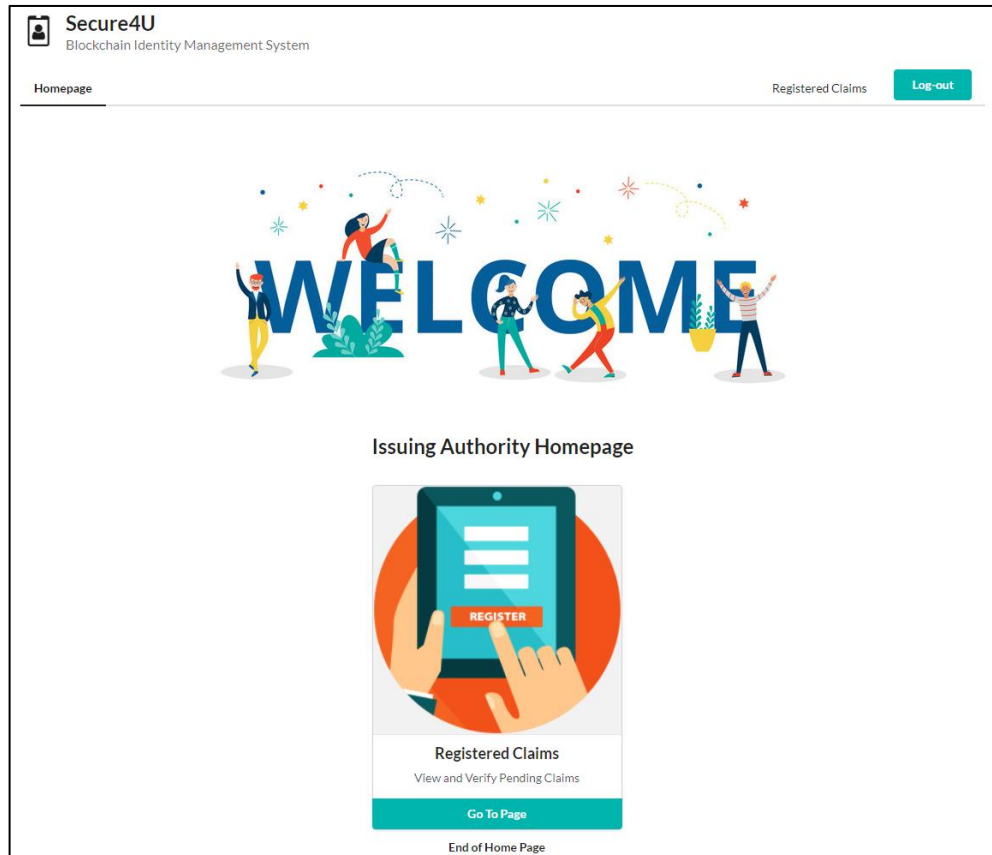
**Figure 4-25 Log-In Page (Confirmed Transaction)**

After the transaction has been confirmed and processed, a confirmed transaction notification from metamask will pop out (refer to **Figure 4-25**). User account details are also stored at the Blockchain database. Users are then diverted from the account registration page to the log-in page.



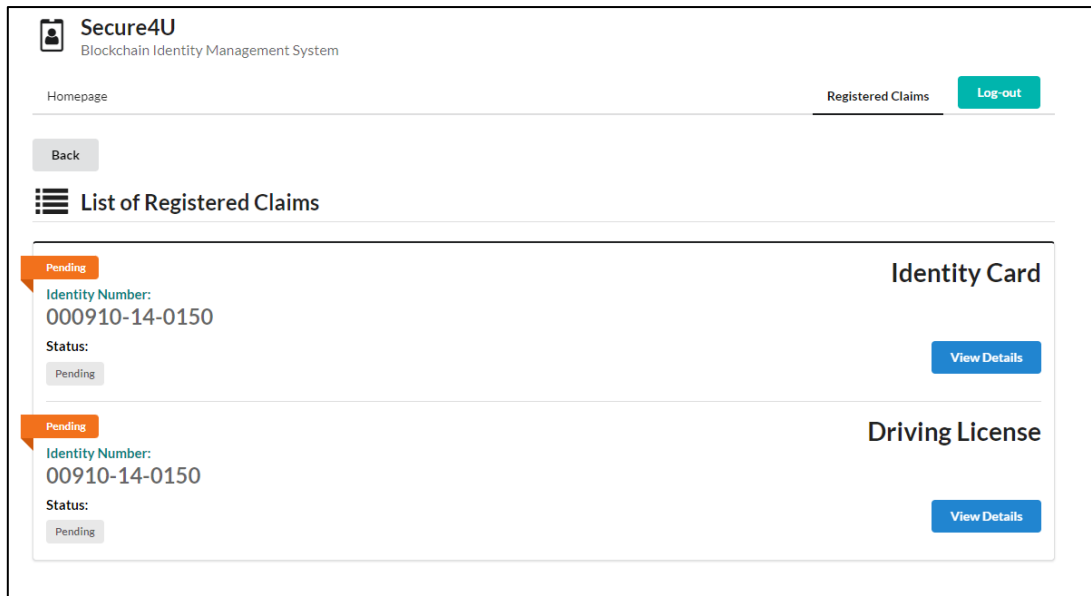
**Figure 4-26 Issuing Authority Log-In**

Issuing authority can now log in to the system by entering the metamask account and select the issuing authority role (refer to **Figure 4-26**).



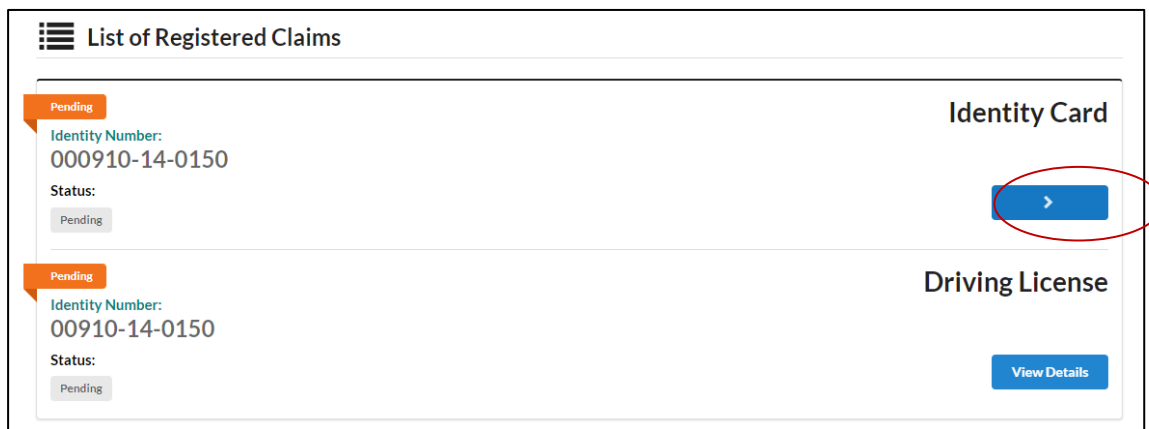
**Figure 4-27 Issuing Authority Homepage**

Based on **Figure 4-27**, after the issuing authority has logged in to the system, a homepage with a registered claims function will be displayed. This function allows user to view and verify pending identity claims that are registered by the users.



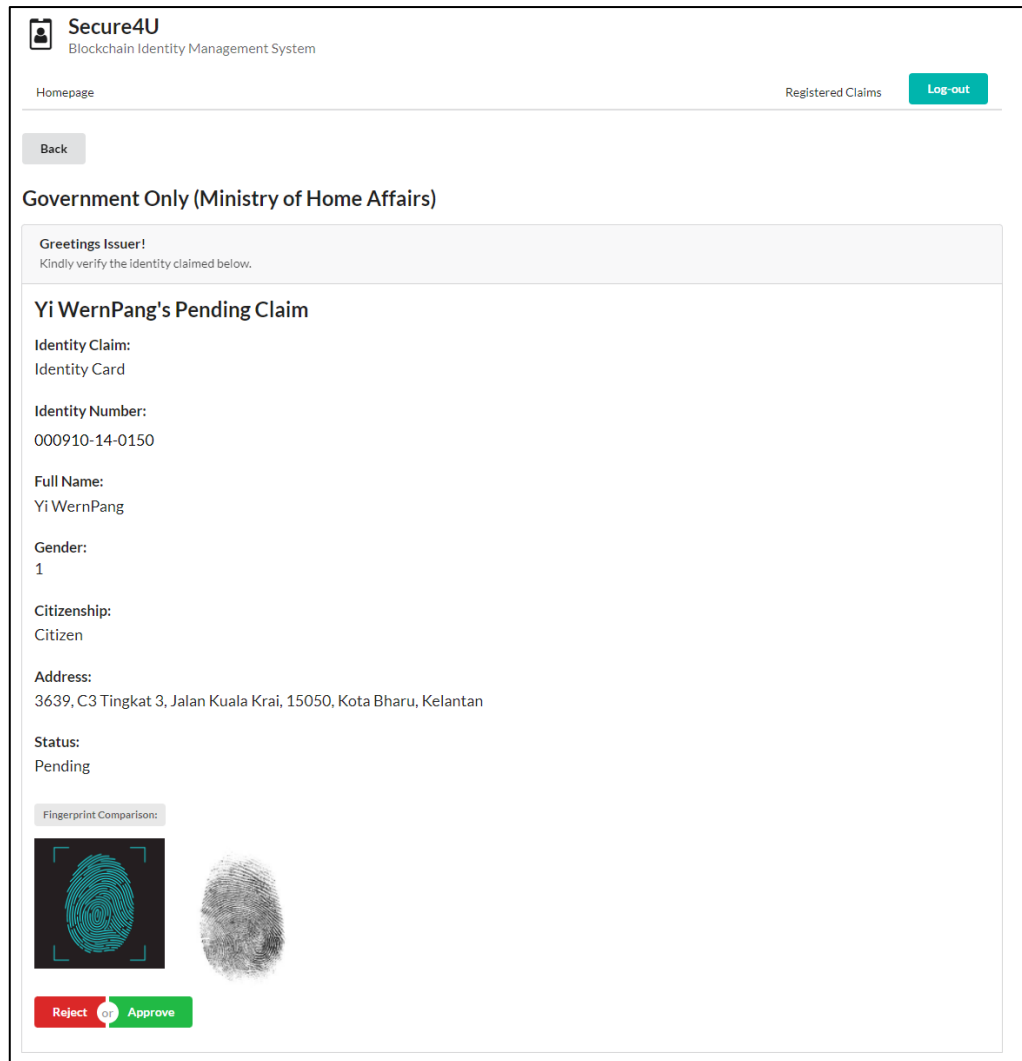
*Figure 4-28 List of Registered Pending Claims*

When users clicked the go to page button, list of pending registered claims will be displayed (refer to **Figure 4.-28**).



*Figure 4-29 View Details Button*

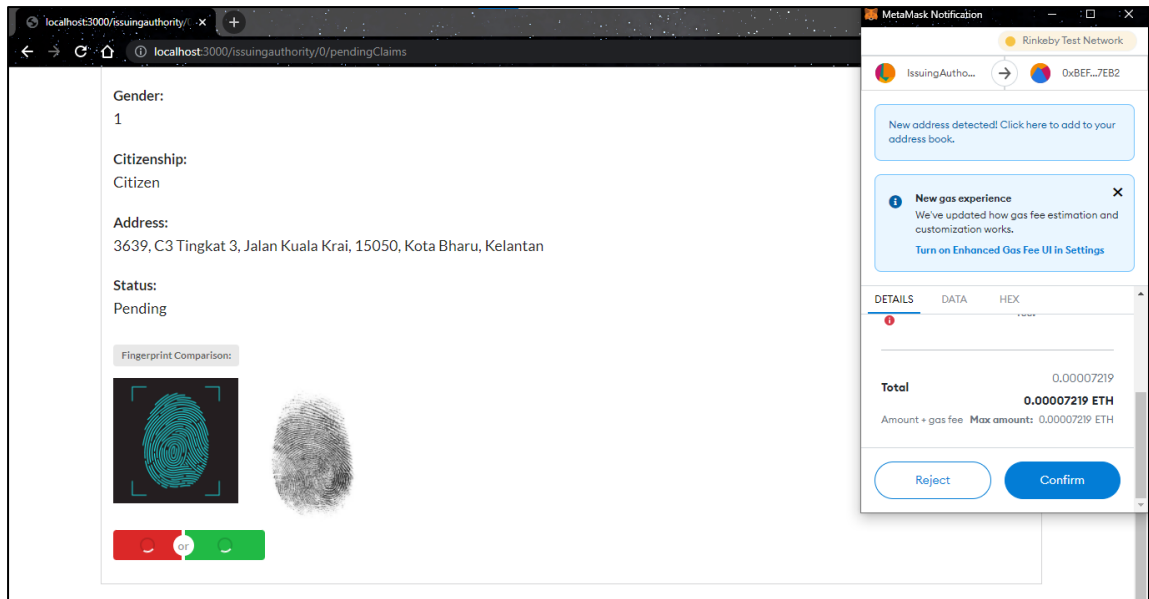
Issuing authority can click the view details button to see the details of that specific registered claim (refer to **Figure 4-29**).



**Figure 4-30 Verification Procedure**

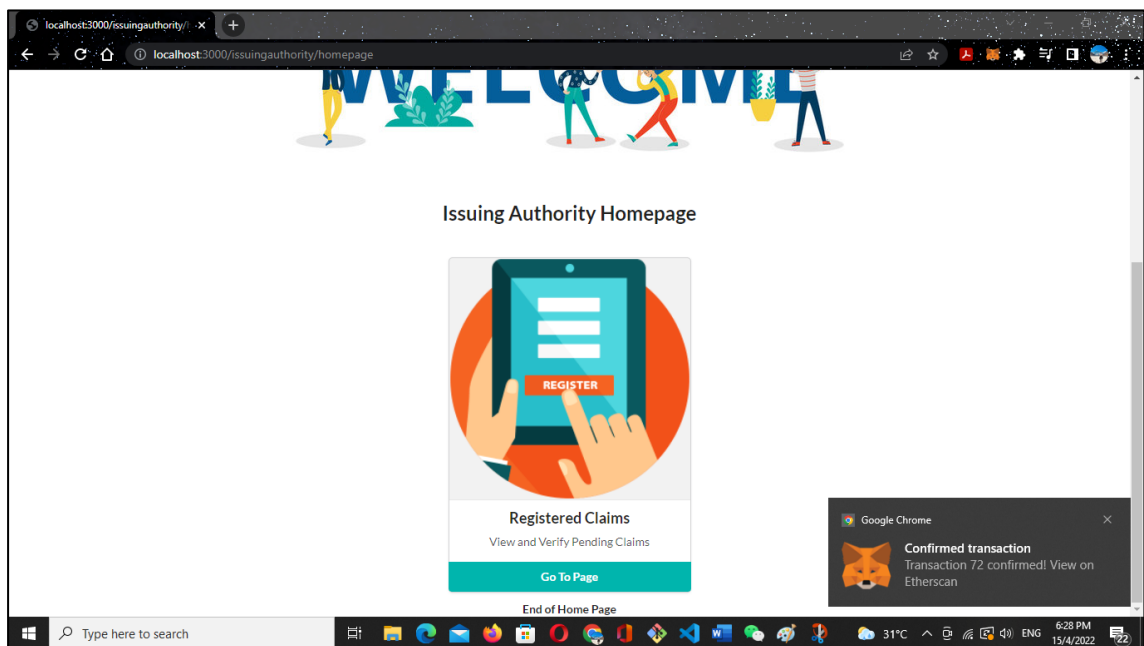
Based on **Figure 4-30**, the issuing authority will then be brought to the claim verification page. Issuing authority will be responsible in verifying the validity of users' registered claims by either approving or rejecting them. However, the issuing authority is required to verify the claims based on some sort of source of proof. Previously while users are registering their identity claims, an image of a fingerprint is also displayed. The fingerprint image that is scanned or uploaded by the user will be compared to the one that is stored at the existing database of the Ministries of Home Affairs using an AI system. If the similarity of the two fingerprints has met the percentage range set (e.g.: 98 – 100%), the issuing authority will then approve that specific claim. Although the similarity check using AI software is not under my project development scope, but it is the way how issuing authority will verify the validity of the claim.





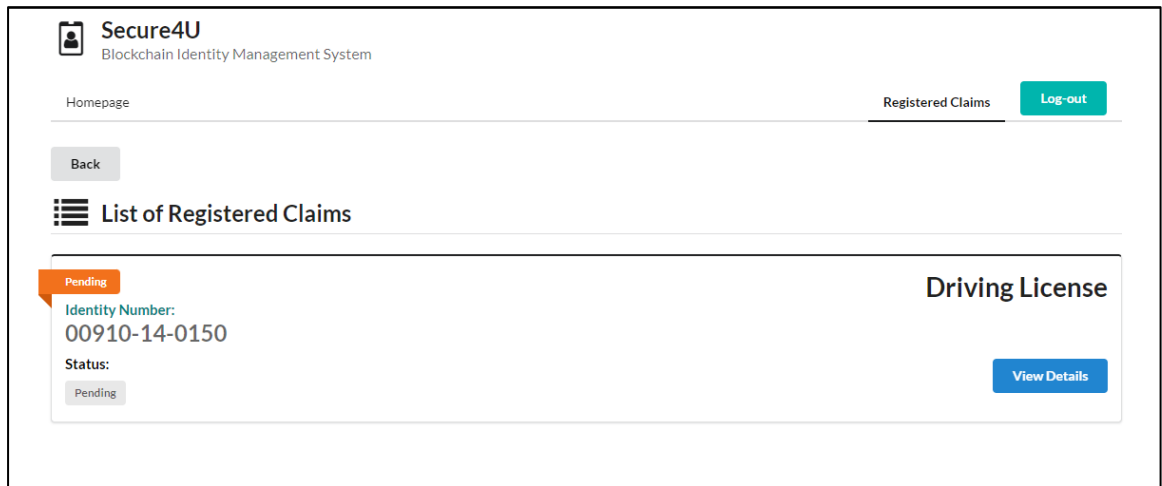
**Figure 4-31 Verification Procedure (Metamask Transaction Confirmation)**

After issuing authority has clicked the reject or approve button, a transaction confirmation notification by metamask will pop up (refer to **Figure 4.31**). If issuing authority has approved the claim, user's identity claim status will be switched from pending to valid. If the issuing authority has rejected the claim, the status will be changed from pending to not valid.



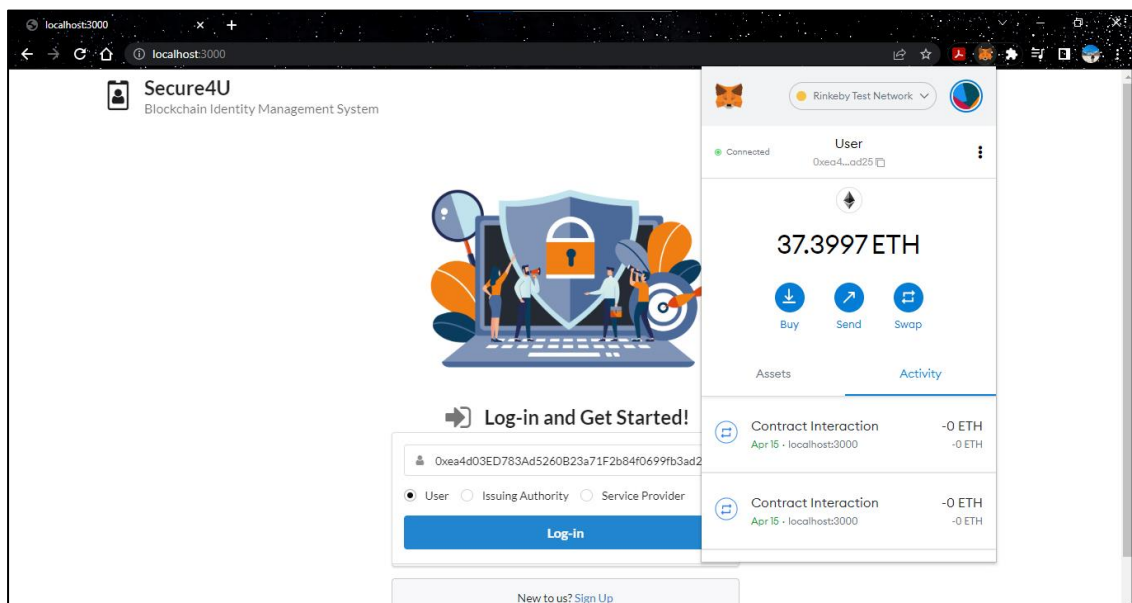
**Figure 4-32 Confirmed Transaction Notification**

A confirmed transaction notification will pop up after the verification transaction made by the issuing authority has been confirmed and processed. The updated status of user's registered claims will then be stored to the Blockchain database (refer to **Figure 4-32**).



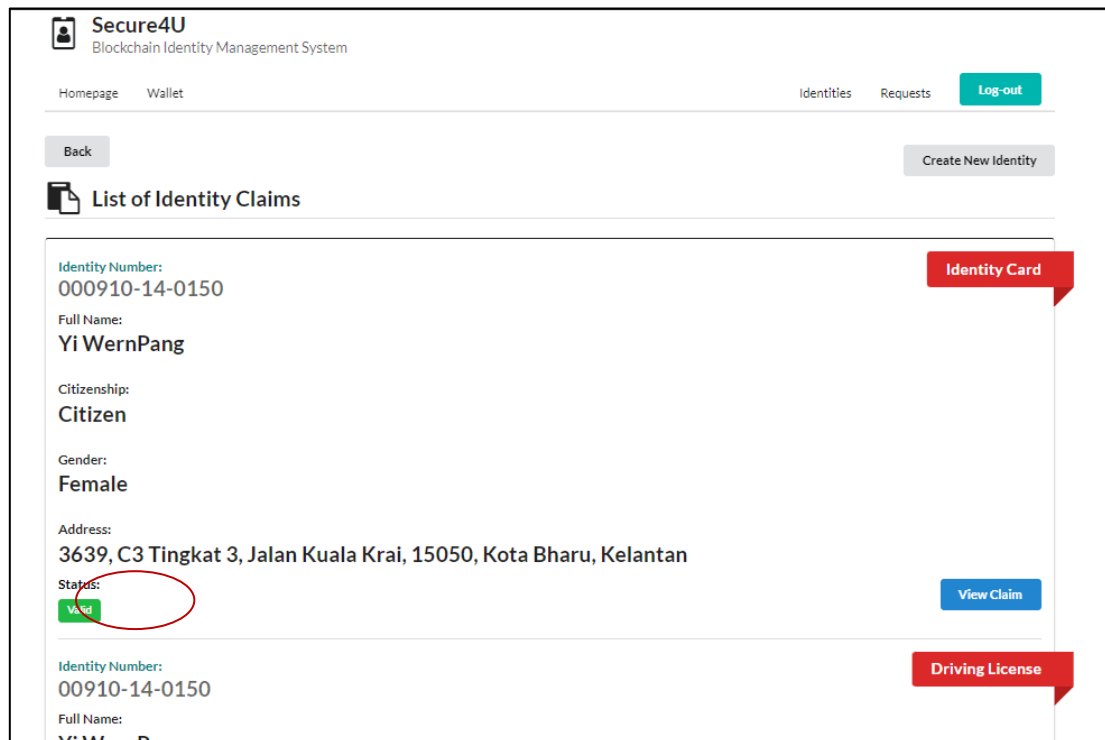
**Figure 4-33 Registered Pending Claims**

Previously, there are two registered claims displayed. Now there is only one registered pending driving license is shown. This shows that the verification process for the identity card claim is performed successfully (refer to **Figure 4-33**).



**Figure 4-34 User Log-In**

To make sure that the user's side status is updated, we will now log in to the user's side.



*Figure 4-35 Status Check*

After clicking into the identity claims functionality from the user's homepage, we can see that from the list of identity claims, the status for identity card claim has switched from pending to valid (refer to **Figure 4-35**).

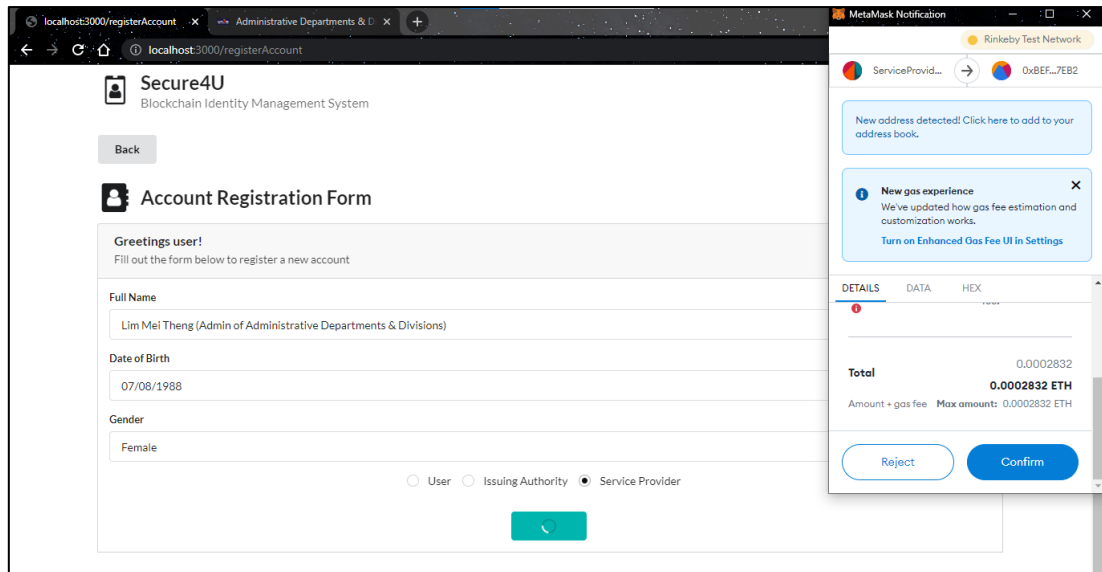
**Service Provider (Legal Institutions) Role:**

The screenshot displays the 'Secure4U Blockchain Identity Management System' interface. The main content area shows the 'Account Registration Form' for a 'Service Provider'. The form includes a 'Greetings user!' message, a prompt to 'Fill out the form below to register a new account', and three input fields: 'Full Name' (containing 'Lim Mei Theng (Admin of Administrative Departments & Divisions)'), 'Date of Birth' (containing '07/08/1988'), and 'Gender' (set to 'Female'). Below these fields are radio buttons for 'User', 'Issuing Authority', and 'Service Provider' (which is selected). A green 'Register' button is at the bottom right of the form. On the right side, a Metamask wallet overlay is open, showing a balance of '18.7435 ETH' and transaction history under the 'Activity' tab.

Assets	Activity
	Contract Interaction Apr 13 - localhost:3000 -0 ETH
	Contract Interaction Apr 13 - localhost:3000 -0 ETH

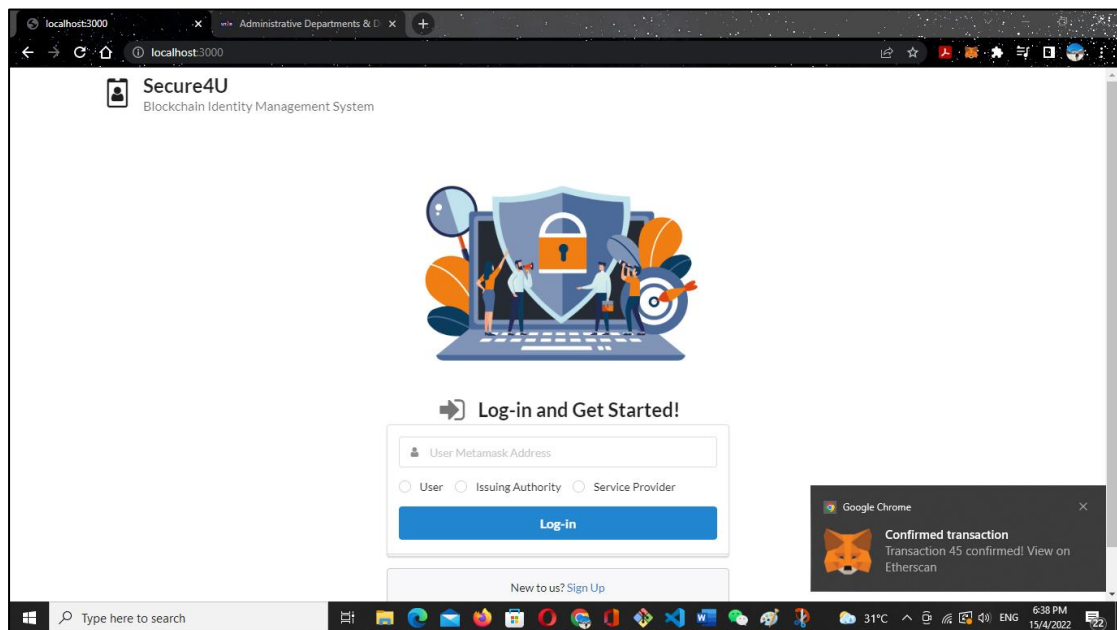
**Figure 4-36 Account Registration Form (Service Provider)**

Same as both the *user* role and *issuing authority* role, after the service provider have logged-in to their metamask account, they will then be brought to their account that is used to access the rinkeby test network (blockchain test network) and to store ether for blockchain transactions. For existing system users, they are able to log-in to the system by entering their account address and selecting the service provider role after accessing their metamask account. While for new user of the issuing authority, they are required to sign up by clicking the sign-up link tag at the log in page. Account registration form will then be displayed. New user of the issuing authority needs to fill in the details listed at the form (refer to **Figure 4-36**).



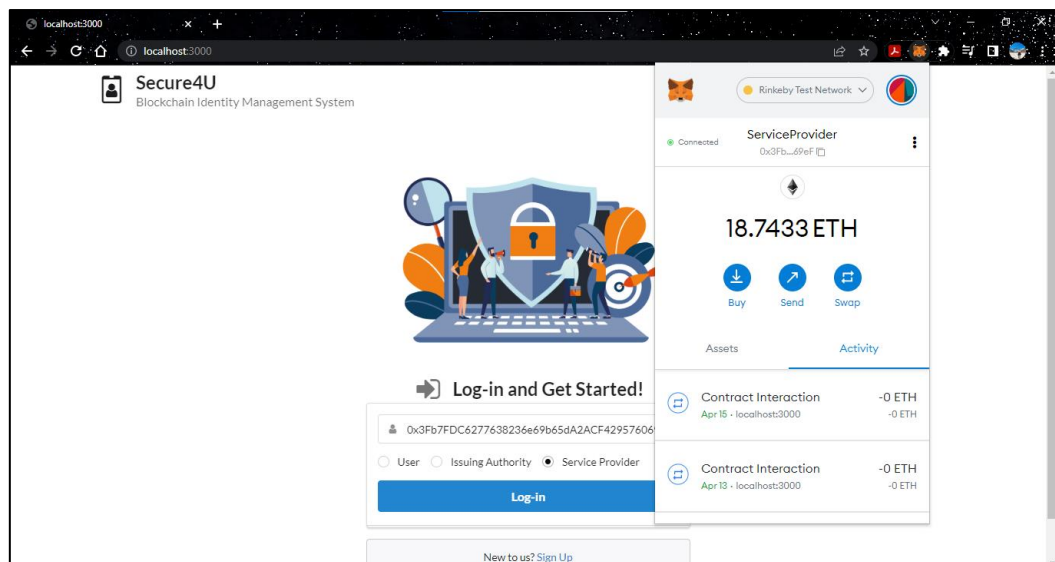
**Figure 4-37 Account Registration Form (Metamask Transaction Confirmation - Service Provider)**

A metamask transaction confirmation will then pop up after new users of service provider have clicked register (refer to **Figure 4.34**).



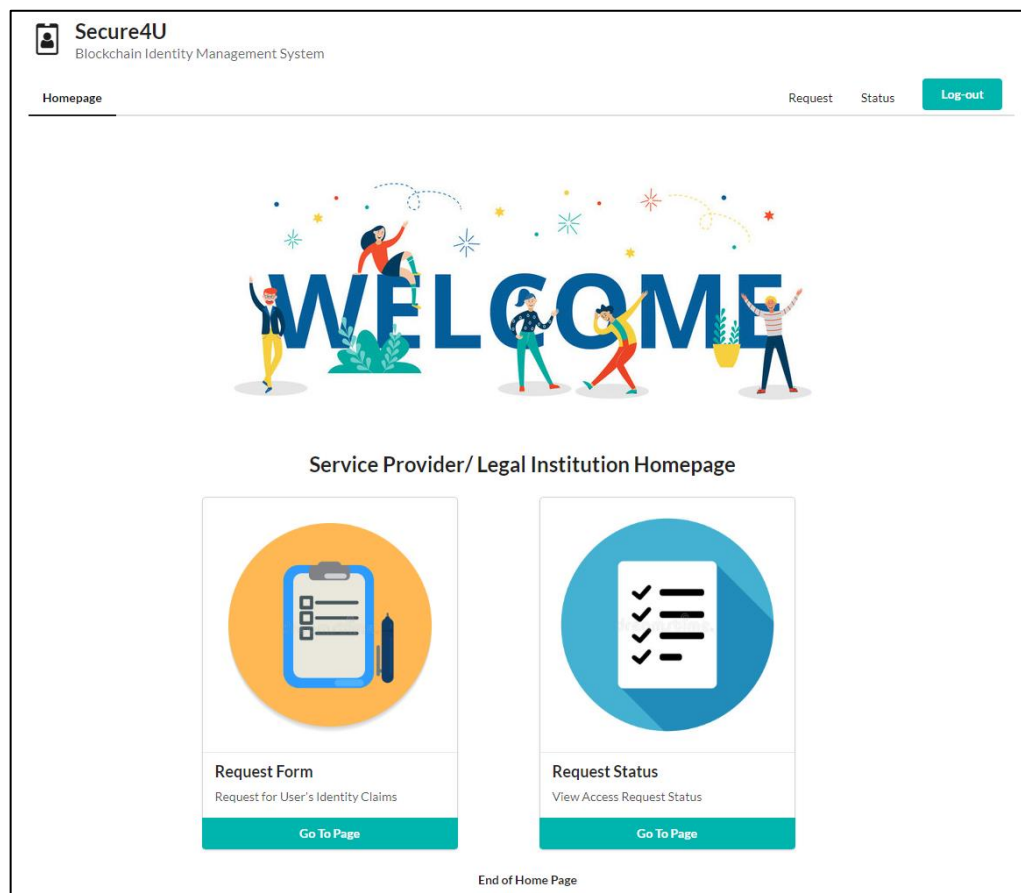
**Figure 4-38 Metamask Confirmed Transaction Notification**

A confirmed transaction notification will then pop up after the transaction has been confirmed and process. The new account of the service provider has been stored in the Blockchain database as well (refer to **Figure 4-38**).



**Figure 4-39 Service Provider Log-In**

The service provider can now logged-in to their account by entering their Metamask account address and selecting the service provider role (refer to **Figure 4-39**).



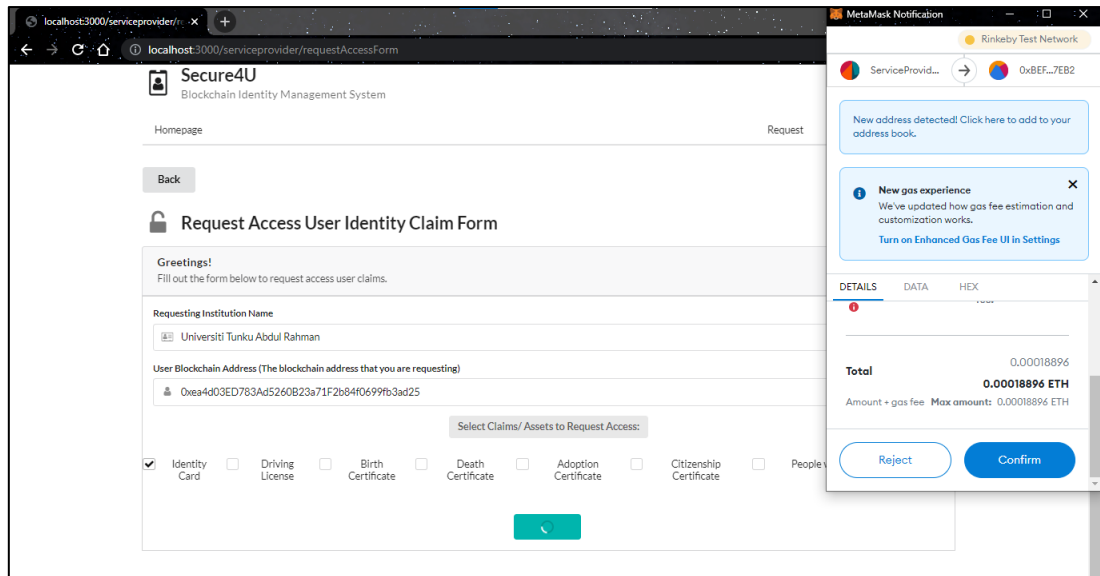
**Figure 4-40- Service Provider Homepage**

After the service provider has logged in to the system, the service provider's homepage will be displayed. There are two functionalities for the role *service provider*, which are request form and request status. For the request form function, the service provider or legal institutions can request for identity claims from the user they want. Service provider can then view the status of the requests made through the request status function (refer to **Figure 4-40**).

The screenshot shows the 'Request Access User Identity Claim Form' interface. At the top, the header includes the 'Secure4U' logo, the text 'Blockchain Identity Management System', and navigation links for 'Homepage', 'Request', 'Status', and a 'Log-out' button. Below the header is a 'Back' button. The main title is 'Request Access User Identity Claim Form'. A 'Greetings!' section instructs the user to 'Fill out the form below to request access user claims.' The form contains two input fields: 'Requesting Institution Name' with a placeholder 'Institution Name' and 'User Blockchain Address (The blockchain address that you are requesting)' with a placeholder 'User Address'. Below these fields is a section titled 'Select Claims/ Assets to Request Access:' which lists seven categories with checkboxes: 'Identity Card', 'Driving License', 'Birth Certificate', 'Death Certificate', 'Adoption Certificate', 'Citizenship Certificate', and 'People with Disabilities (OKU) Certificate'. A 'Request' button is located at the bottom right of the form.

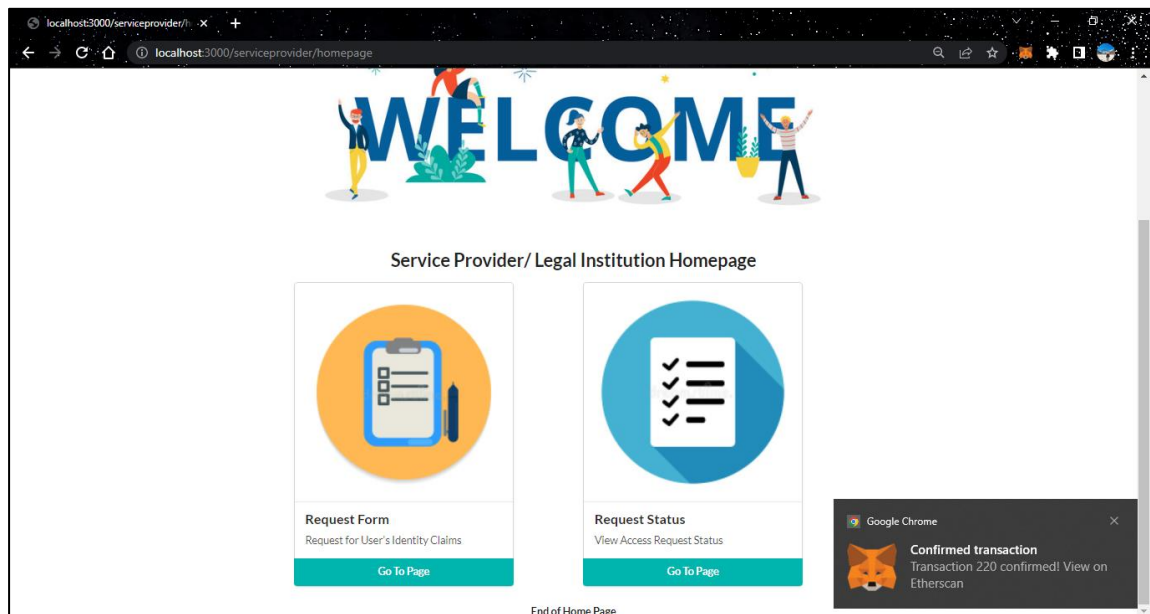
**Figure 4-41 Request Access Form**

The service provider will be led to the request access user identity claim form after clicking into the request form functionality (refer to **Figure 4-41**).



**Figure 4-42 Request Access Form (Metamask Transaction Confirmation)**

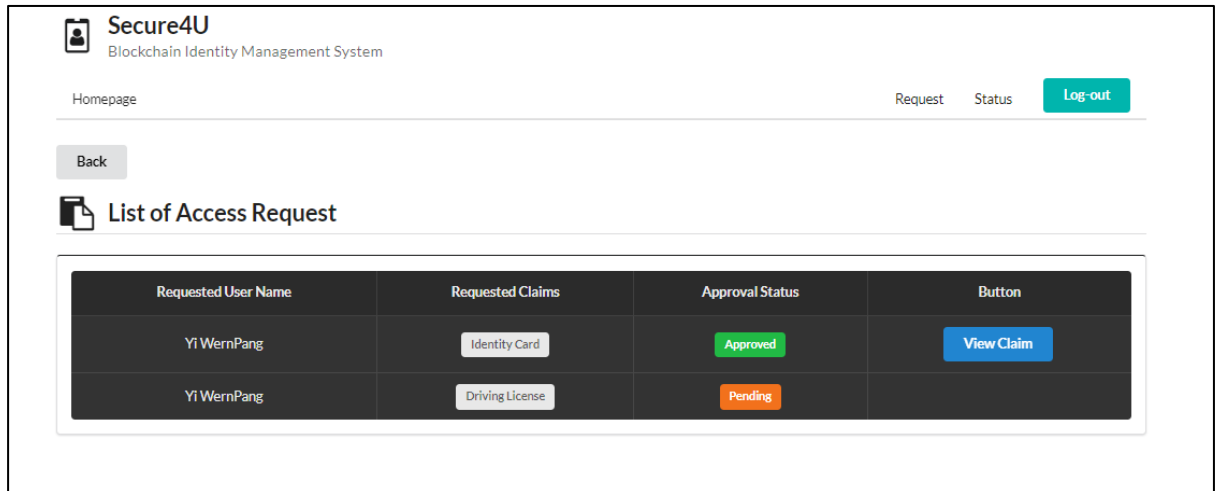
Service providers are required to provide its institution name and the blockchain address of the user they intend to request and select the claims they intend to access. After the service provider has hit the request button, the transaction confirmation notification will be displayed (refer to **Figure 4-42**).



**Figure 4-43 Metamask Confirmed Transaction Notification**

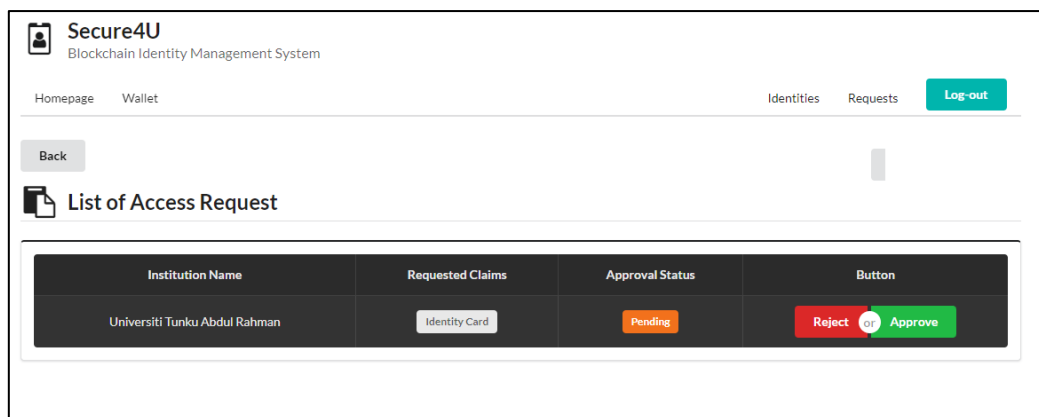


After the transaction has been confirmed and processed, a confirm transaction notification will be shown (refer to **Figure 4-43**). Service provider is also diverted back to the homepage.



**Figure 4-44 Access Request Section**

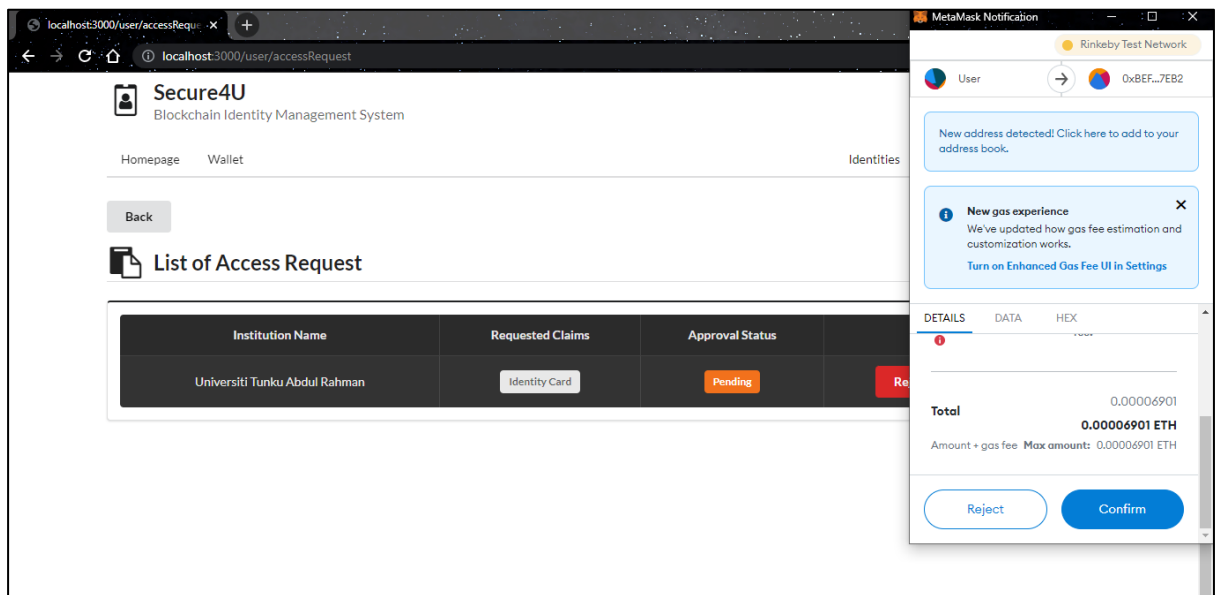
The request status functionality is where service provider can see the status of their requests. If the status of the request is being approved, a view claim button will be shown in order to let the service provider to access the user's claim.



**Figure 4-45 Access Request Approval**

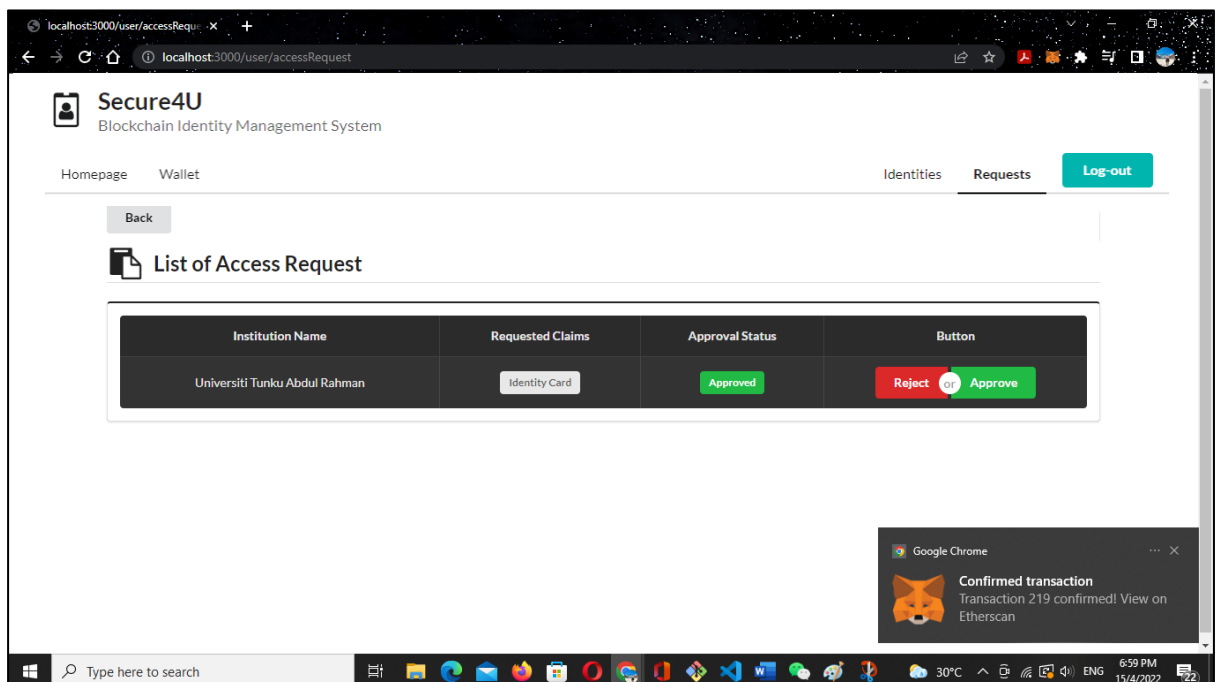
Back to the user side, user can see those request made by the service provider through the third functionality at the user homepage (refer to **Figure 4-9**). User can

either choose to approve or to reject the request access made by that specific institution (refer to **Figure 4-45**).



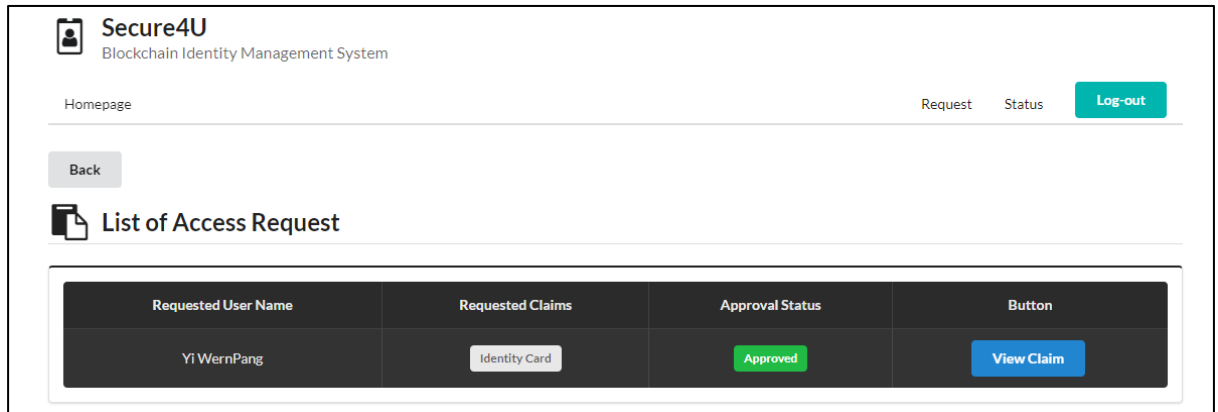
**Figure 4-46 Metamask Transaction Confirmation**

A confirmation notification from metamask will pop up after user's have choosed to approve or reject the request (refer to **Figure 4-46**).



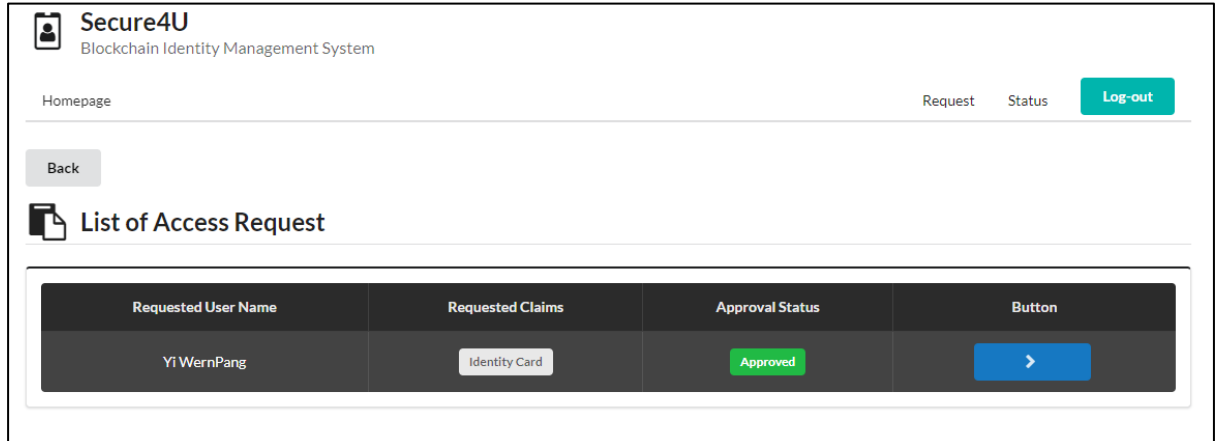
**Figure 4-47 Metamask Confirmed Transaction Notification**

After the transaction has been confirmed and processed, a confirmed transaction notification will pop up. The request access status will then be updated to the Blockchain database (refer to **Figure 4-47**).



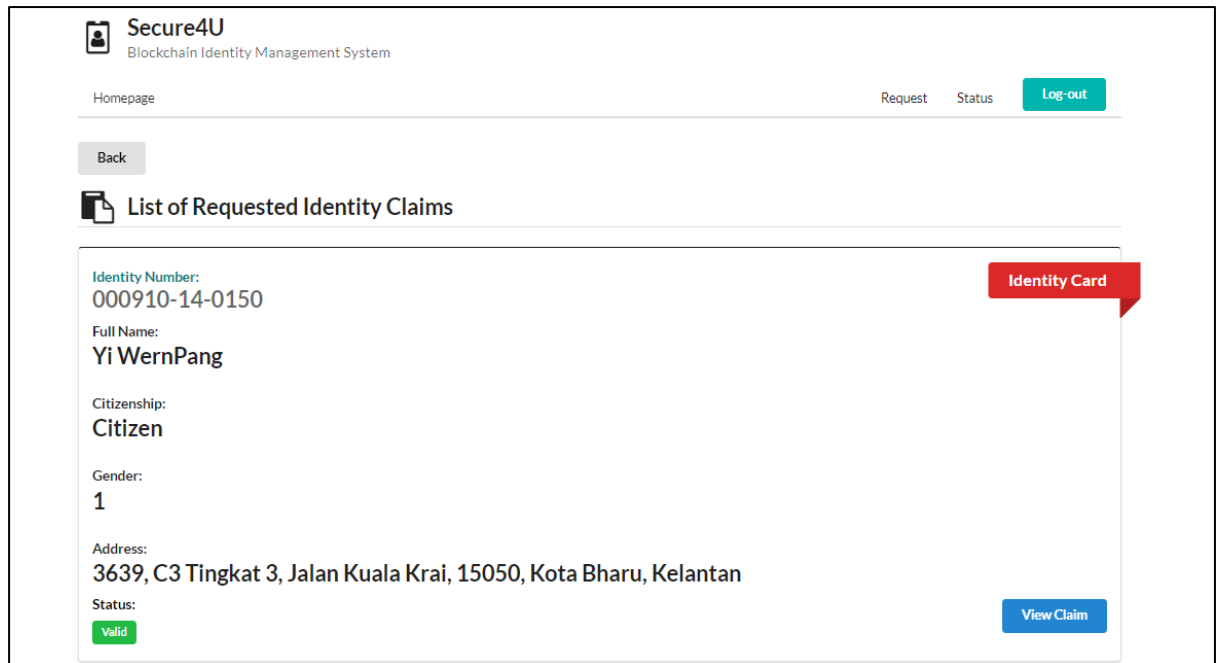
**Figure 4-48 User-side Approved Access Request**

Back to the service provider side, we can see that the approval status has switched from pending to approved (refer to **Figure 4-48**).



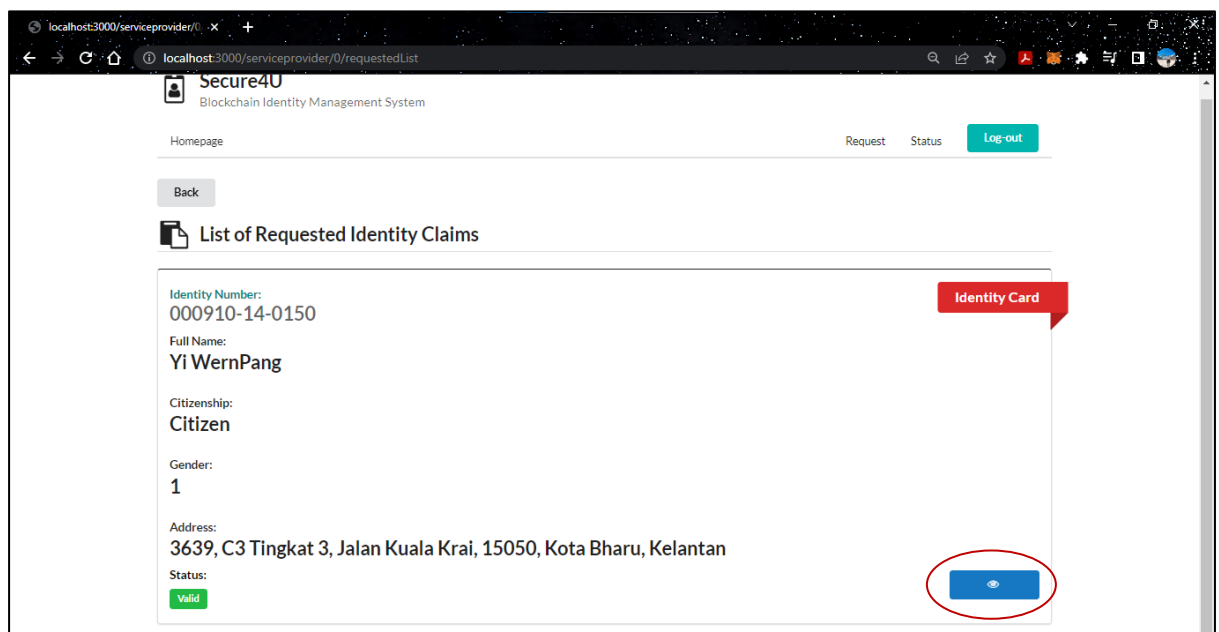
**Figure 4-49 View Claim of Approved Request**

The service provider can now view the claim they have requested from the user by clicking the view claim button (refer to **Figure 4-49**).



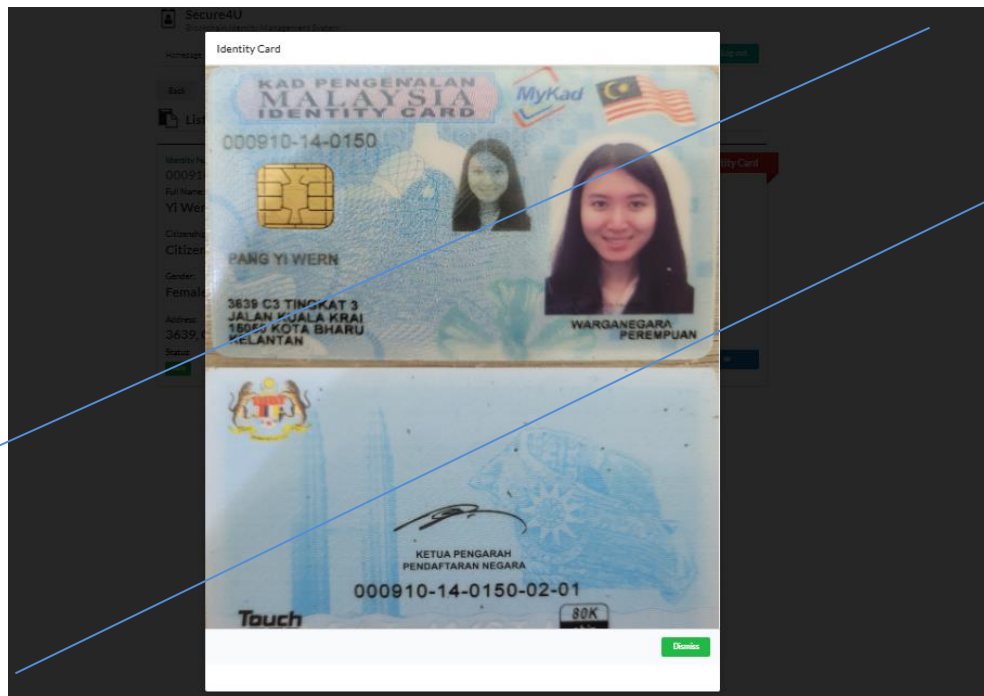
*Figure 4-50 Identity Claim Details of Approved Request*

**Figure 4.50** shows the identity card details requested by the service provider.



*Figure 4-51 View Identity Claim Image*

Service provider can view the requested document image by clicking the view claim button (refer to **Figure 4-51**).

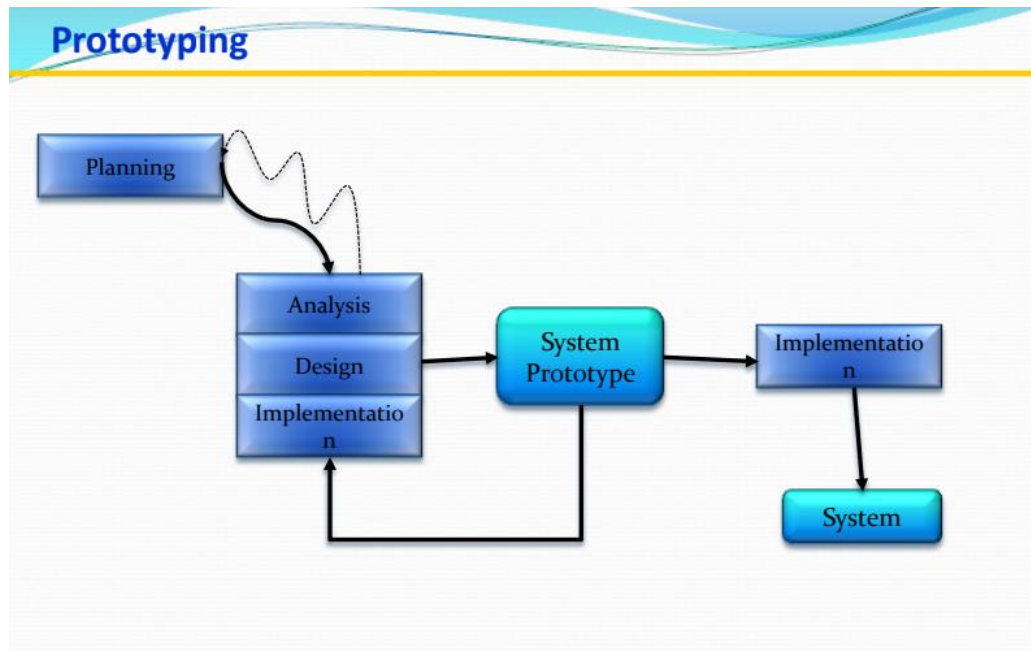


**Figure 4-52 Identity Card Image View**

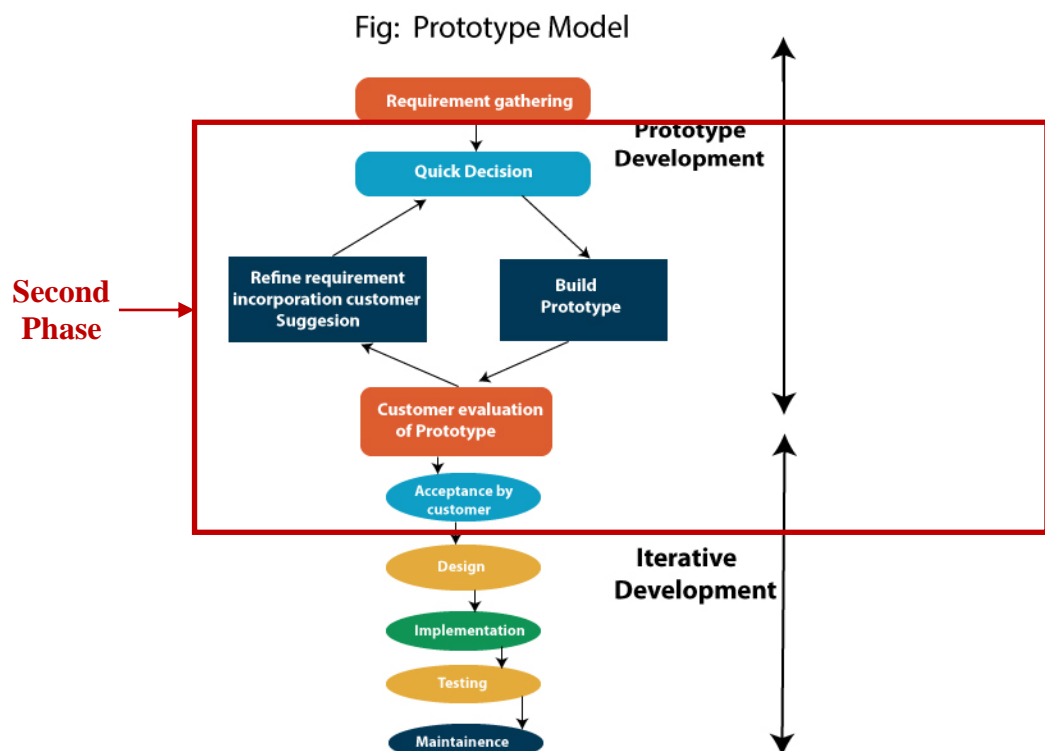
**Figure 4-52** shows the image of the identity card of the user after clicking the view claim button.

## Chapter 5: System Implementation

### 5.1 System Methodology



*Figure 5-1 Prototype Methodology Model*



*Figure 5-2 Prototype Methodology Model – Second Phase*

The proposed methodology involved in this proposed project will be prototyping, which falls under Rapid Application Development (RAD) methodology category (Refer Figure 3). A prototyping-based methodology is where the analysis, design and implementation phases are performed concurrently. These three phases will be performed repeatedly in a cycle until the system is completed. This method emphasizes on creating prototypes, for example, incomplete versions of the application to allow users to test and evaluate the proposals, instead of having them to interpret and evaluate the design based on descriptions.

This is the main reason why I have selected this methodology as I am able to get the users' evaluation and feedback throughout the prototyping process as involving users in the process helps reassures user working on system and quickly refine real requirement. Besides that, with the help of users' evaluation and feedback, I am able to detect any issues regarding the system faster and deliver a useful system to users quickly. When a problem is detected, the stage of process will then return to the analysing phase, designing solution phase, and implementing phase. With users' feedback, repeat these three phases a cycle until a complete system that will meet users' requirement and expectation is done.

### **First Phase: Planning / Requirement Gathering**

During the planning phase, it involves identifying what value does the system bring to which target audience. After determining the values that the system is able to deliver and who will benefit from the values, requirement gathering process will then be performed. User requirements will be collected as much as possible in order to understand the target audience better and identify what are the real problems they are facing. This helps to determine what functionality should be included in the proposed project. Besides that, feasibility analysis will be then performed in terms of technical, economic and organizational. This analysis helps to identify whether the proposed project is an achievable and realistic goal in terms of money, time and final output result.

### **Second Phase: Analysis, Design and Implementation (Prototype Development)**

During the second phase of the methodology, the analysis phase involves building a simple and quick prototype design that will be evaluated by the user based on user requirement. If user is not satisfied with the prototype, some refinement will

be carried out by incorporating user's suggestion. Once system prototype is accepted by the user, the methodology will then proceed to the next phase, or else this phase will be repeated until the system is complete and meet user's expectation (Refer to Figure 4).

### **Third Phase: Design, Implementation, Testing, Maintenance (Iterative Development)**

During the third phase of the methodology, which is also the last phase, a proper system design will be then created through extensive data discovering and alternative design exploring at the design phase. The system design phase describes necessary specifications, features and operations that is able to meet the functional requirements of the proposed system. After choosing the final potential system design, will then proceed to the implementation phase. The implementation phase involves building the elements specified in the design phase through coding. Since the system design and requirements are gathered accurately and completely through repetitive evaluation and refinement that match user's needs on the previous phase, the coding process will be much efficient and streamlined. Next, for the testing phase, it involves testing out the program and procedure to see whether the system meets the initial goal and work according to user requirement. Any errors detected must be solved immediately with new solutions. When the system has been completed and delivered to users, maintenance phase is required to be performed where end users are able to fine-tune the system in order to support operational effectiveness, boost system performance and add new capabilities.



**5.2 Final Year Project 2 (FYP2) Timeline**

Activity	Period (Week)													
	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14
<b>Chapter 1: Introduction</b>														
Problem Statement and Motivation														
Project Scope														
Project Objectives														
Impact, Significance and Contribution														
Background Information														
<b>Chapter 2: Literature Review</b>														
Fact Finding														
Critical Remarks of Previous Works														
<b>Chapter 3: System Design</b>														
Use-Case Diagram														
Flow Diagram														
<b>Chapter 4: System Implementation</b>														
System Methodology														
Technologies and Tools Involved														
Project Timeline														
Verification Plan														
System Development														
Implementation Issues and Challenges														
System Testing														
System Documentation														
<b>Chapter 5: Conclusion</b>														
Project Review and Discussion														
Novelties and Contributions														
Future Work														
Check and Finalize FYP2 Report														
FYP2 Report Submission														
FYP2 Presentation														

**Figure 5-3 Final Year Project 2 (FYP2) Estimated Timeline**

**5.3 Tools or Technologies Involved**

<b>Tools</b>	<b>Type</b>	<b>Description</b>
Metamask	Cryptocurrency wallet	A web browser extension that offers the simplest yet secure way to connect to the Blockchain Identity Management System. It allows users to interact with the Blockchain identity management system, store cryptocurrency, pay transaction fees and transfer cryptocurrency to others.
Remix	IDE	An open-source tool where developers code smart contract with solidity language directly from the web browser. Remix is also used for the initial development and testing of smart contract.
Visual Studio Code	IDE	To develop the front-end and back-end of Blockchain Identity management System.
Rinkeby Test Network	Ethereum Blockchain	An Ethereum test network that is used to deploy and interact with smart contract.
Infura	Ethereum API	This API connects the Blockchain Identity Management System to the Ethereum network for smart contract deployment purpose.
Semantic UI	Front-end framework	To develop the user interface of the Blockchain Identity Management System.
Web3.js	Ethereum JavaScript API	To allow users to interact with the existing smart contract at the front-end of the Blockchain Identity Management System.
Node.js	JavaScript runtime	To install the packages or dependencies needed in the development process of the Blockchain Identity Management System. It also provides the runtime environment for the system to run.
Solidity	Programming language	To create smart contracts on Ethereum.
JavaScript	Programming language	To develop the front-end and back-end of the Blockchain Identity Management System.

React	JavaScript library	To construct the front-end and back-end of the Blockchain Identity Management System.
Next.js	React framework	To assist in front-end development by providing navigation to the Blockchain Identity Management System.

*Table 5-1 Tools to use*

#### **5.4 Implementation Issue and Challenges**

There are some issues and challenges faced during the implementation of the proposed project, Blockchain Identity Management System. The development of identity management system using Blockchain Technology is quite challenging as the technology involved is an area that I am highly unfamiliar with. More time and efforts are required for me to be familiarized with this new technology. Since it is something new and not many people are implementing this technology in Malaysia, the learning resources and references regarding the Blockchain technology are very limited as well. However, I have managed to find an online course and references from other countries which it is really useful for beginners of Blockchain development. It has guide me the concepts and ways to develop and implement a Blockchain project.

Previously I was facing the challenge in allowing the service provider to send access request for users by selecting the user's identity claim details that they intend to access. I planned to allow service provider to be able to select the identity assets from the user they want and send that request to that respective user by entering that user's blockchain account address. However, I have managed to solve the errors faced during Final Year Project 1 at my Final Year Project 2. I have managed to search a solution from the internet as a reference for me to solve the issue faced. Now this functionality is working well after the system testing and evaluation process (Chapter 6). Service provider can now send a request to access user's identity assets.

Besides that, as my proposed system involves managing different identities that users owned, it will be better those users are able to upload softcopies of the

identity asset and store in the blockchain system to act as stronger evidence and references. Previously I was facing the challenge where allowing user to store their in image in Blockchain directly can be very expensive. I am required to find another alternative way for me to store the image in Blockchain without paying a high transaction fee.

The alternative way I have found out to prevent a high transaction fee while storing an image is by storing it into the Interplanetary File System (IPFS) first, then only use the one store at IPFS to store at the Blockchain system. Previously due to the lack of knowledge in IPFS, I am not able to allow users to upload softcopies of their documents while registering their identity claims during Final Year Project 1. However, during Final Year Project 2, I have explored and learned the required knowledge, which is Interplanetary File System (IPFS) in order to upload an image on the Blockchain network with a lower transaction fee. Now, I am able to implement IPFS in my Blockchain identity management system. Therefore, users are now able to upload their identity document image to the Blockchain database while registering their identity asset details to the Blockchain database.

## 5.5 System Tesing

### 5.5.1 System Testing

Case No.	Test Case	Expected Result
(a)	User, issuing authority and legal institution log-in to Metamask account before using blockchain identity management web portal.	All functionalities present at the blockchain identity management system will work.
(b)	User, issuing authority and legal institution who do not log-in to Metamask account before using identity management web portal.	All functionalities present at the blockchain identity management system will not work.
(c)	User, issuing authority and legal institution register an account on blockchain identity management web portal.	One Metamask account of the users can only have one blockchain identity

		management web portal account.
(d)	User, issuing authority and legal institution log in to blockchain identity management web portal.	User, issuing authority and legal institution who do not own a web portal account is unable to log in to blockchain identity management web portal.
(e)	User creates digital wallet after access to blockchain identity management web portal.	<ul style="list-style-type: none"> <li>- Digital wallet is stored at the Blockchain database.</li> <li>- User can view digital wallet details at the wallet section of the web portal.</li> <li>- User can register their identity assets/ documents.</li> </ul>
(f)	User does not create digital wallet after access to blockchain identity management web portal.	<ul style="list-style-type: none"> <li>- User unable to view digital wallet details at the wallet section of the web portal.</li> <li>- User cannot register their identity assets/ documents.</li> </ul>
(g)	User intends to create many digital wallets.	User unable to create more than one digital wallet at one account of the web portal.
(h)	User registers identity claims on the blockchain identity management web portal.	After user has registered an identity claim on portal, the registration status will be set as pending. This is where users are required to wait for the verification by the issuing authority. Upon approval, user's identity claim is stored on Blockchain. When issuing

		authority has approved the identity claim, status will be updated as approved, if reject status will be updated as rejected. Upon any registrations of identities or updates including pending, approved, or rejected, it will be stored or updated at the Blockchain database.
(i)	User views registered identity claims on the blockchain identity management web portal.	No identity claims will be displayed by the system if there are no identity claims registered by the user. Once user registered an identity claim, it will then be displayed to the user.
(j)	Issuing authority view user's registered claims	At the issuing authority side, only registered claims that are pending for verification will be displayed as a list
(k)	Issuing authority approve or reject user's identity claim registration	<ul style="list-style-type: none"> <li>- After the issuing authority has approved or reject the claim that is pending for verification, that specific claim will not be shown at the issuing authority side anymore.</li> <li>- User side will be updated from pending to either valid or not valid.</li> </ul>
(l)	Service provider sends request to user to access user's identity claim details.	- Service provider's selected identity claim details are

		<p>sent to user.</p> <ul style="list-style-type: none"> <li>- User side can view and either to approve or to reject the request made by the service provider.</li> <li>- Service provider side can view the status of their request from their side.</li> </ul>
(m)	Service provider requested user's identity claim details and rejected by user.	Service provider unable to view rejected request of user's identity claim details.
(n)	Service provider requested user's identity claim details and approved by user.	Service provider can view approved request of user's identity claim details.
(o)	Service provider requested user's identity claim details and pending approval from the user.	Service provider unable to view a pending request of user's identity claim details.
(p)	User uploads their digital wallet profile picture during digital wallet creation.	Uploaded picture will be displayed at the digital wallet section.
(q)	User uploads their identity claim/ identity asset image during identity registration process.	Image of the identity claim can be viewed by clicking the view claim button at the list of registered claims section.

**Table 5-2 System Verification Plan**

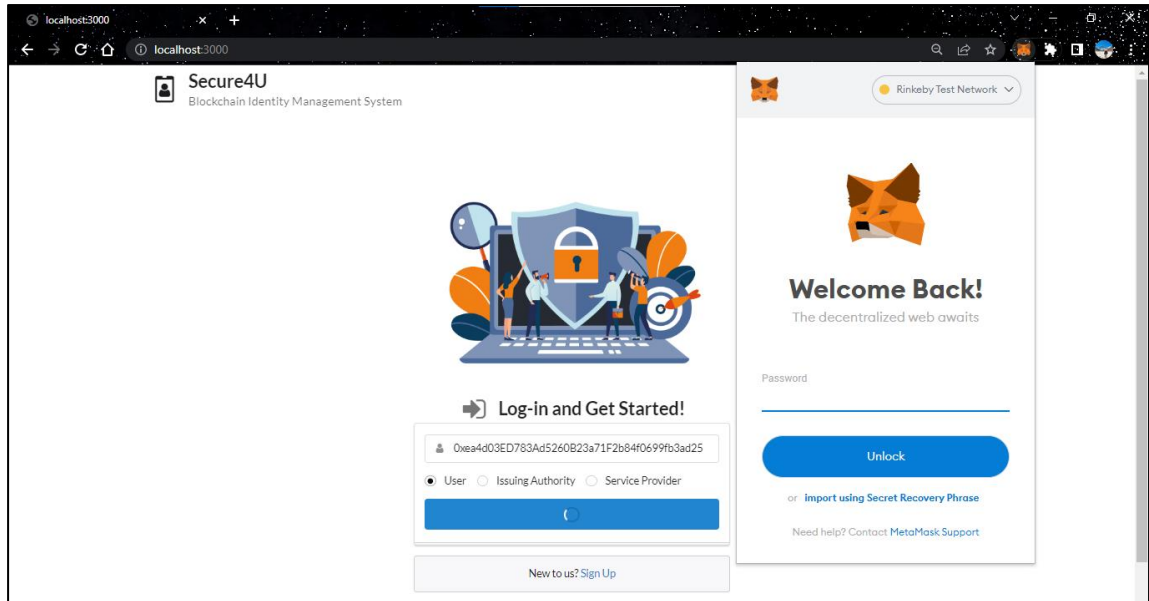
## **Chapter 6: System Evaluation and Discussion**

### **6.1 System Testing and Performance Metrics**

Testing is part of a more general verification process where it is intended to show that a program works in the way that it is intended to work and to discover program defects before it is put into real use. These are the functionalities of the Blockchain Identity Management System that is required to be tested for its performance whether they have met the expected output results. This system consists of three roles which are user, issuing authority and service provider/ legal institution. For the system user part, it can be divided into new user and existing user. Now I will perform the system evaluation and performance testing based on the verification plan stated at *Chapter 5, Section 5.5*.

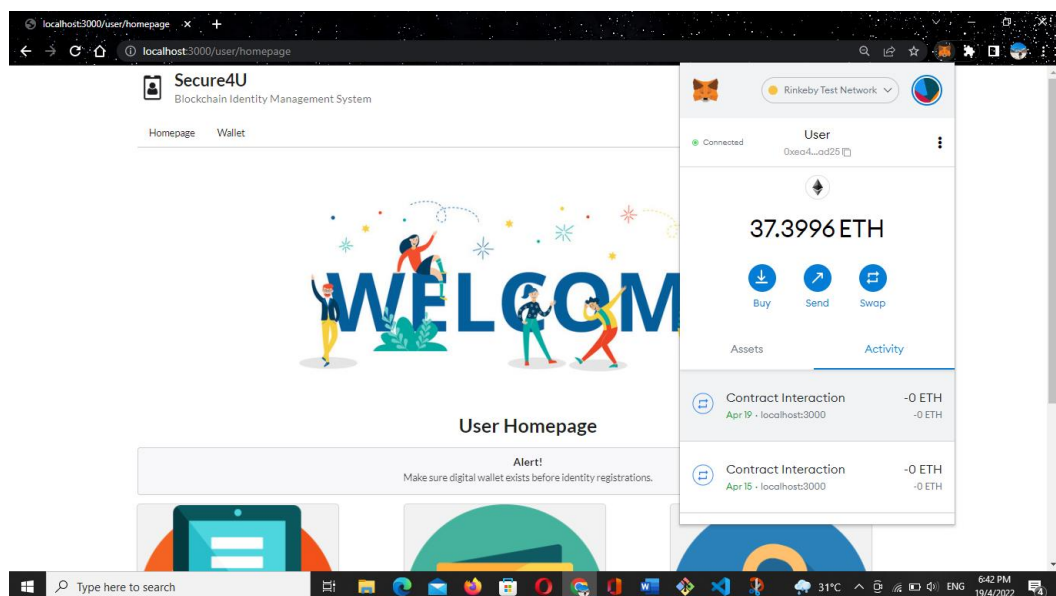
All roles including user, issuing authority and service provider can use the Blockchain identity management web portal only when the metamask web extension is present. This is because the Metamask is linked to the Blockchain Identity Management system. System users can only log-in, make transaction and interact with the Ethereum blockchain with the Metamask software cryptocurrency wallet. All functionalities present at the blockchain identity management system will not work if system users do not log-in to Metamask. Therefore, all system users are required to log-in to their metamask account in order for them to access the web portal and for the blockchain identity management system to work.





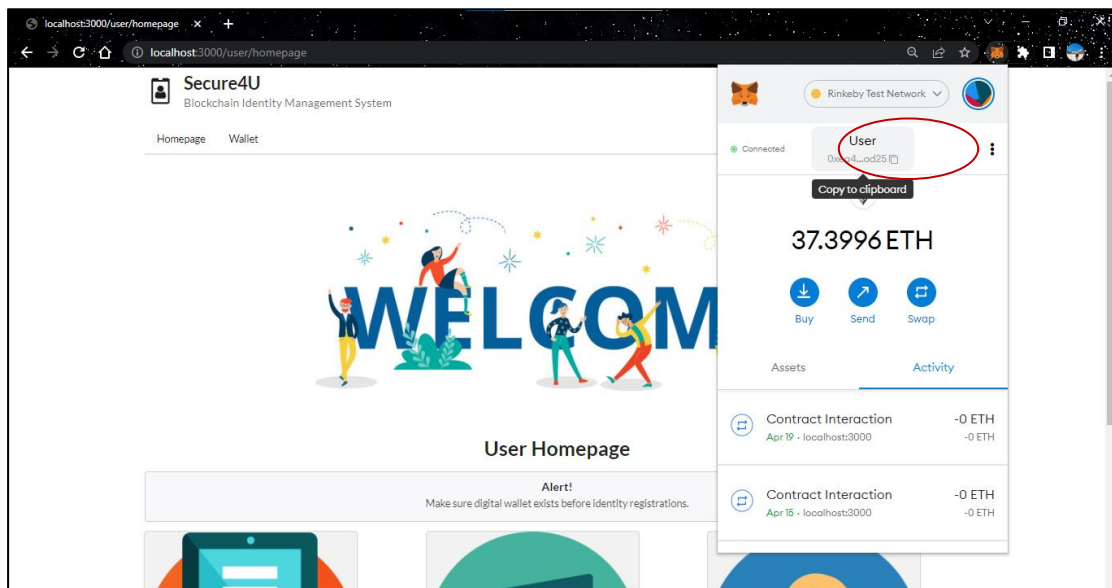
**Figure 6-1 Case(b)**

Based on Figure 6-1, it shows the case where user is not able to log in to the blockchain web portal when the user did not log-in to Metamask. The log-in button will only keep loading instead of accessing the web portal. This shows that the system performance for the log-in part is working as expected.



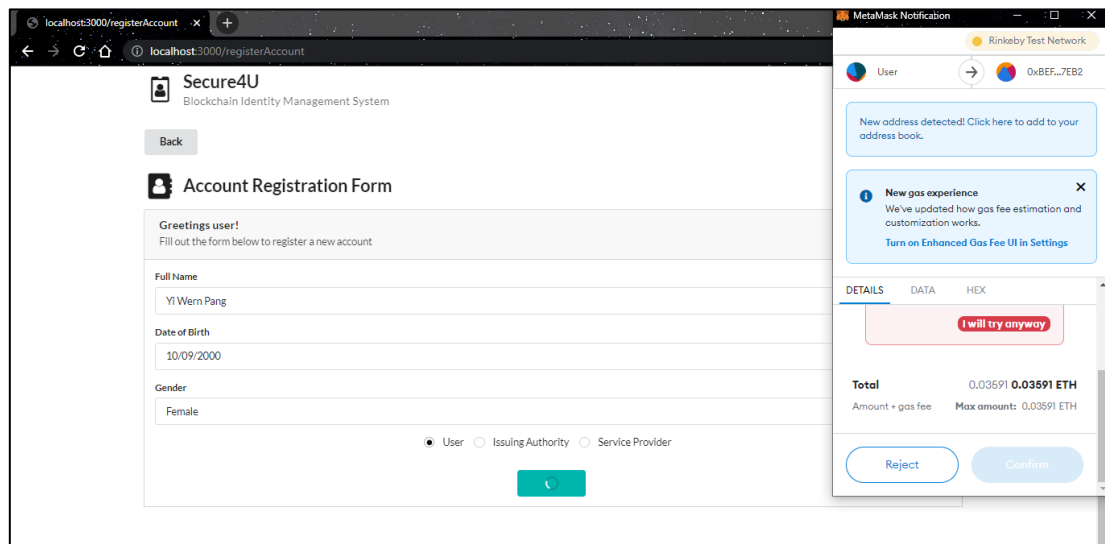
**Figure 6-2 Case (a)**

Based on Figure 6-2, user is able to access into the blockchain identity management system web portal after the user has logged-in to his Metamask account.



**Figure 6-3 Case (c) – (i)**

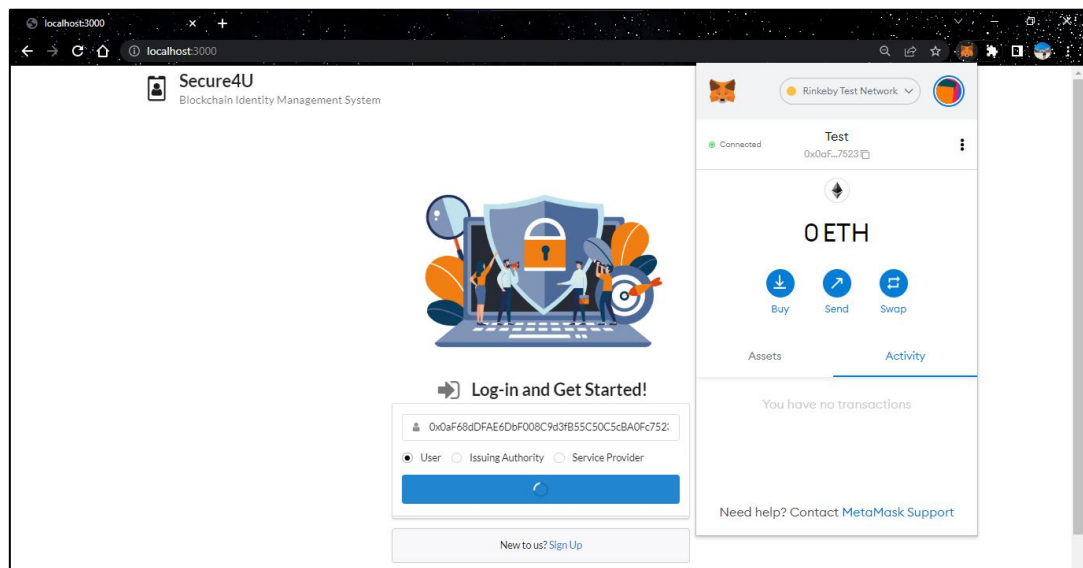
Besides that, to avoid duplicate account registrations, only one Metamask account of the users can only have one blockchain identity management web portal account. According to **Figure 6-3**, it has showed that the account address of the user has been registered in the system as the user is able to access to the blockchain identity management web portal.



**Figure 6-4 Case (c) – (ii)**

Meanwhile, based on Figure 6-4, I have tried to use the same account address to register another account of the system. The Metamask notification has indicated

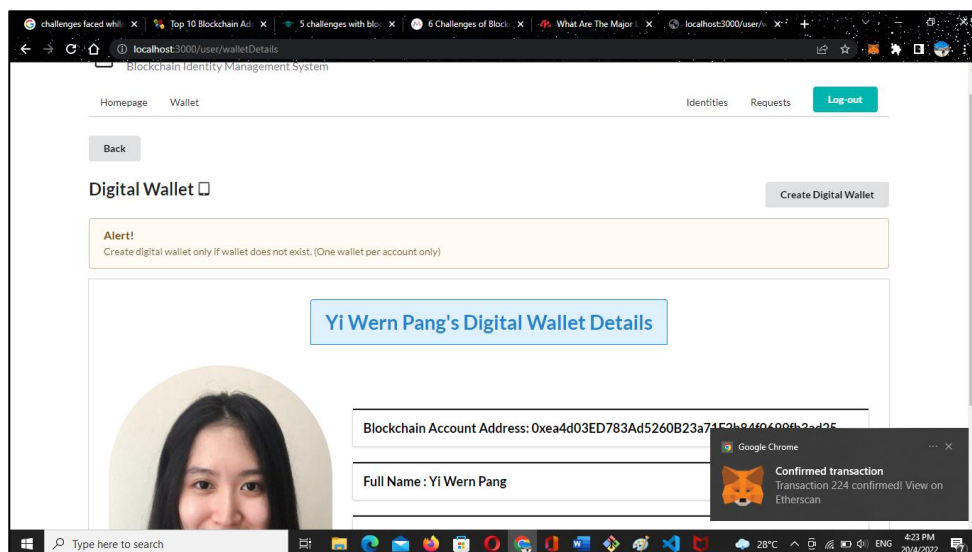
that the registration will be failed, and I am not allowed to make the transaction. This shows that the system performance for the registration part is working as expected.



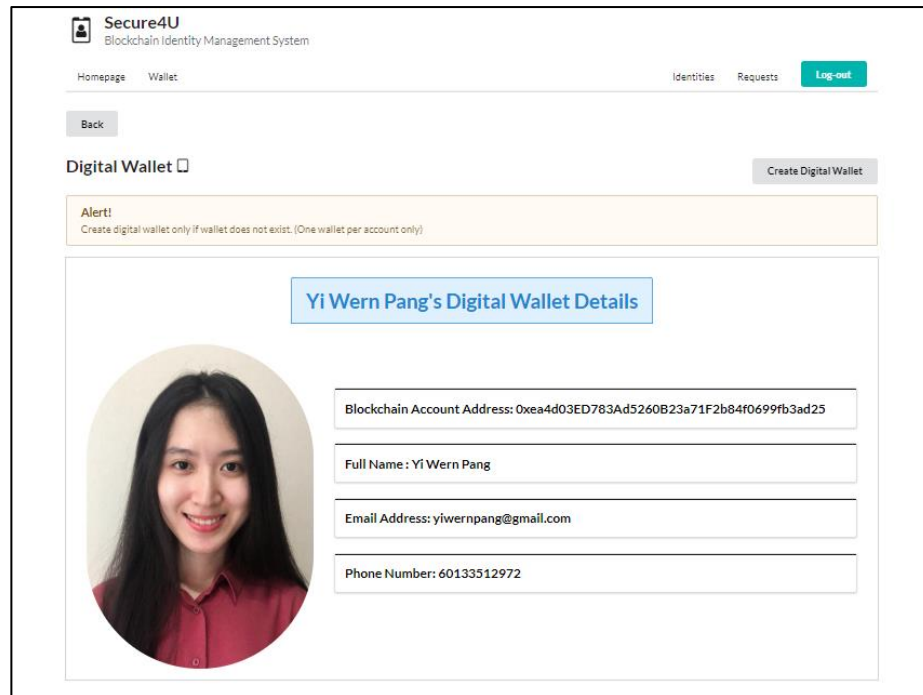
**Figure 6-5 Case (d)**

Now I will try logging in the Blockchain identity management web portal using an account address I have yet registered into the system. Based on Figure 6-5, although I have logged-in to the Test Metamask account. However, the Test account address that was used to log-in is not registered with the system. The system user has failed to log-in to the system having the button in loading process.

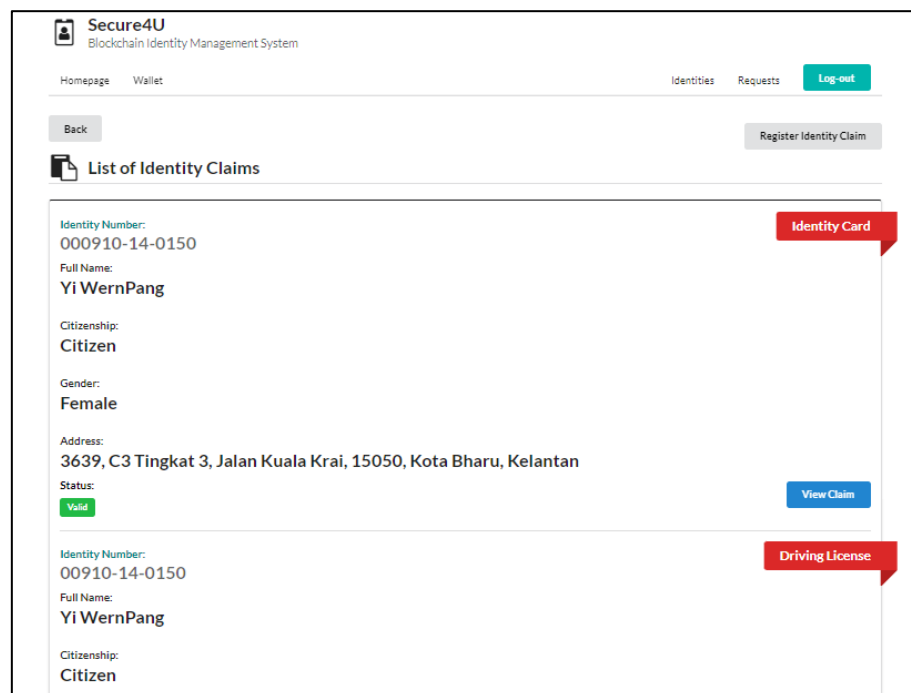
After user has registered and logged-in to the Blockchain identity management system, they are required to create their digital wallet in order for them to register and store identity claims to the system, as well as creating their digital profile.



**Figure 6-6 Case (e) – (i)**



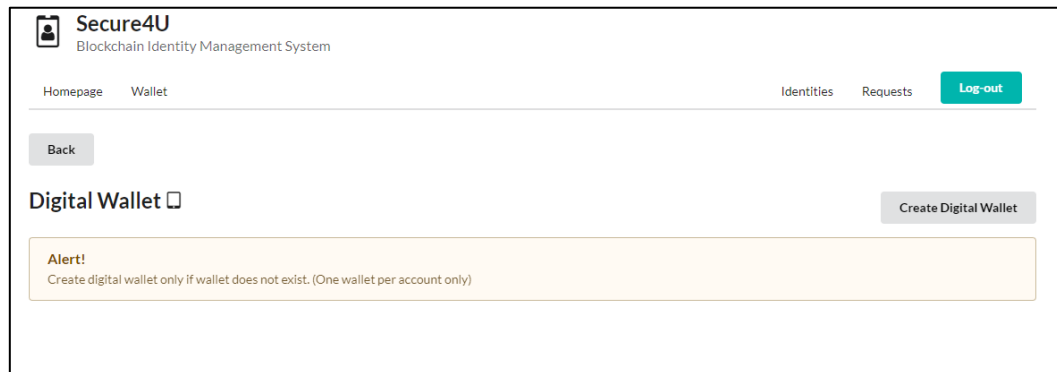
*Figure 6-7 Case (e) – (ii)*



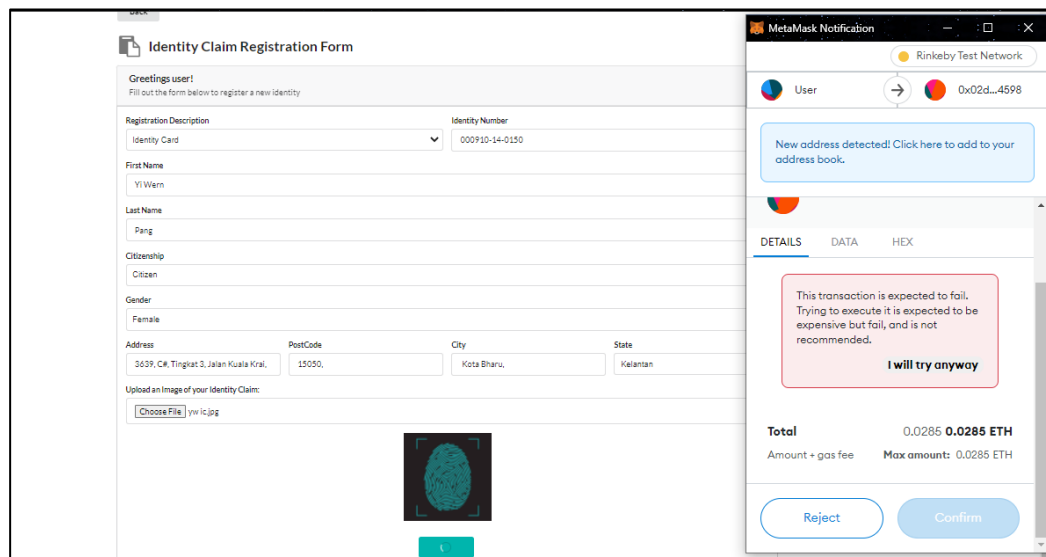
*Figure 6-8 Case (e) – (iii)*

Users who have created their digital wallet after they have accessed to the Blockchain identity management web portal, the digital wallet details will be stored at the Blockchain database. Besides that, a digital profile card will be displayed

consisting of the users' general details. Besides that, users are also able to register their identity assets to the system (refer to **Figure 6-6**, **Figure 6-7** & **Figure 6-8**).



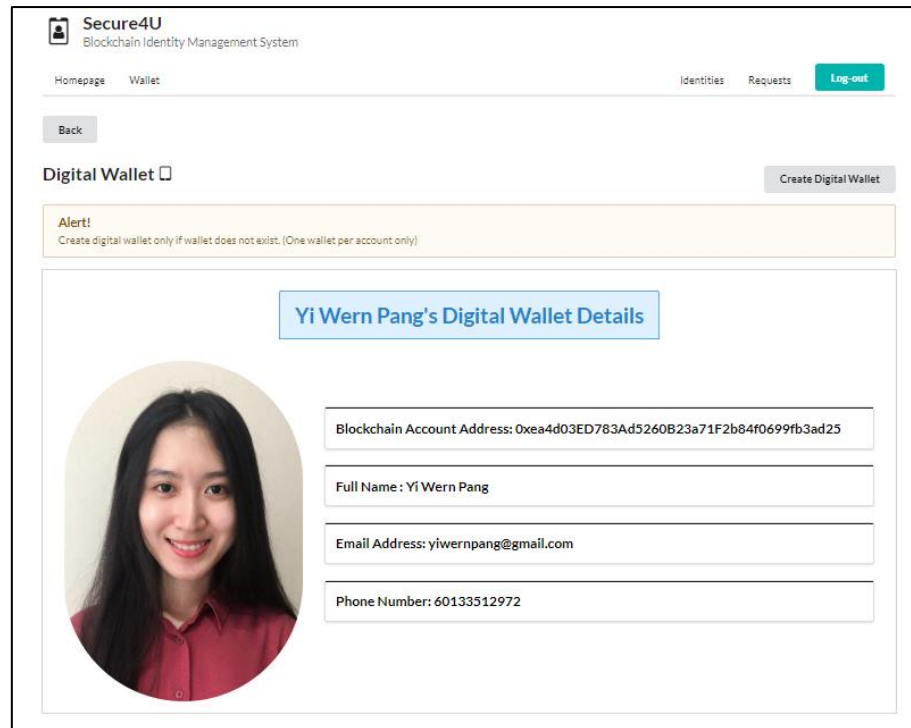
**Figure 6-9 Case (f) – (i)**



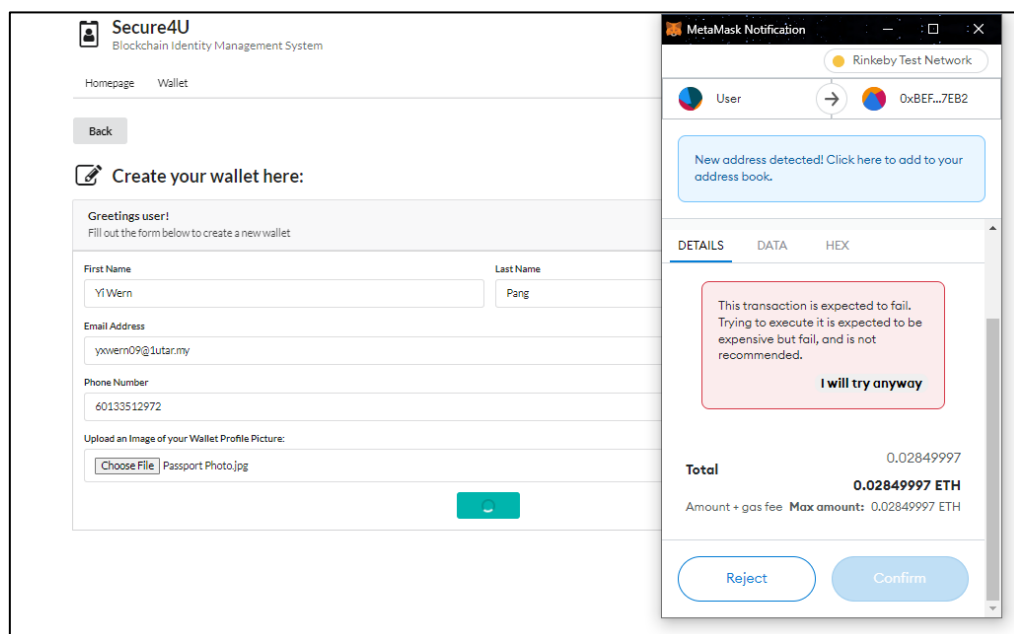
**Figure 6-10 Case (f) – (ii)**

However, based on **Figure 6-9** & **Figure 6-10**, it shows the case when users did not create digital wallet after access to blockchain identity management web portal. These users are unable to view their digital profile and also unable to register any identity assets.

Users who intend to create many digital wallets will fail to do so. In order to prevent duplicate digital profiles created, each user can only have one digital wallet for each account.



*Figure 6-11 Case (g) – (i)*

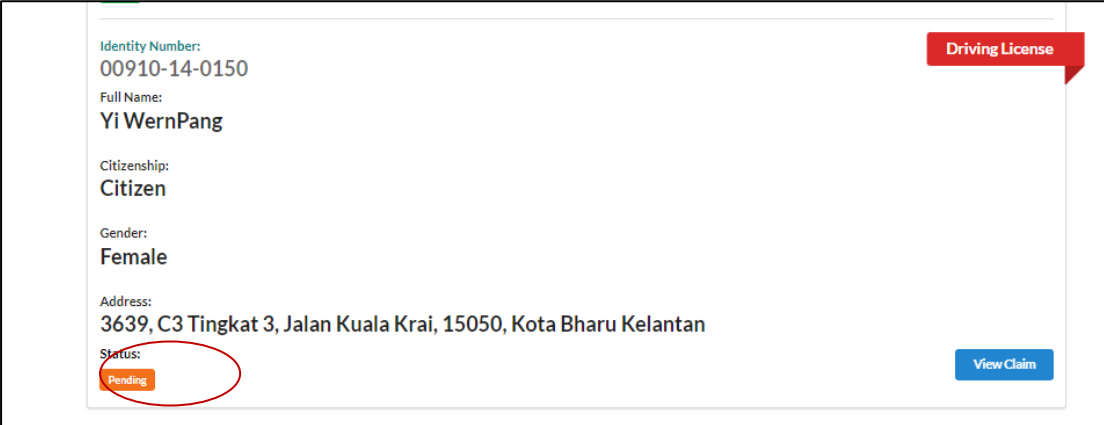


*Figure 6-12 Case (g) – (ii)*

**Figure 6-11 & Figure 6-12** shows the case where the user intends to create another digital wallet although an existing one has been displayed. However, the

user's action was unsuccessful. Metamask transaction confirmation has indicate that the transaction will be failed and banned the user from confirming that transaction.

For the next test case, after user has registered an identity claim on portal, the registration status will be set as pending and labeled in yellow. This is where users are required to wait for the verification of the identity claim's validity by the issuing authority. When issuing authority has approved the identity claim, status will be updated as approved and labeled in green, if rejected the status will be updated as rejected and labeled in red.



Identity Number:	00910-14-0150	Driving License
Full Name:	Yi WernPang	
Citizenship:	Citizen	
Gender:	Female	
Address:	3639, C3 Tingkat 3, Jalan Kuala Krai, 15050, Kota Bharu Kelantan	
Status:	Pending	View Claim

*Figure 6-13 Case (h) – (i)*

**Figure 6-13** shows the case where the user has just uploaded his identity claim to the system, and the validity of the claim is currently pending for verification and labeled in yellow.

**List of Identity Claims**

Identity Number: 000910-14-0150  
Full Name: Yi WernPang  
Citizenship: Citizen  
Gender: Female  
Address: 3639, C3 Tingkat 3, Jalan Kuala Krai, 15050, Kota Bharu, Kelantan  
Status: Pending

Identity Card

View Claim

Identity Number: 000910-14-0150  
Full Name: Yi WernPang  
Citizenship: Citizen  
Gender: Female  
Address: 3639, C3 Tingkat 3, Jalan Kuala Krai, 15050, Kota Bharu, Kelantan  
Status: Valid

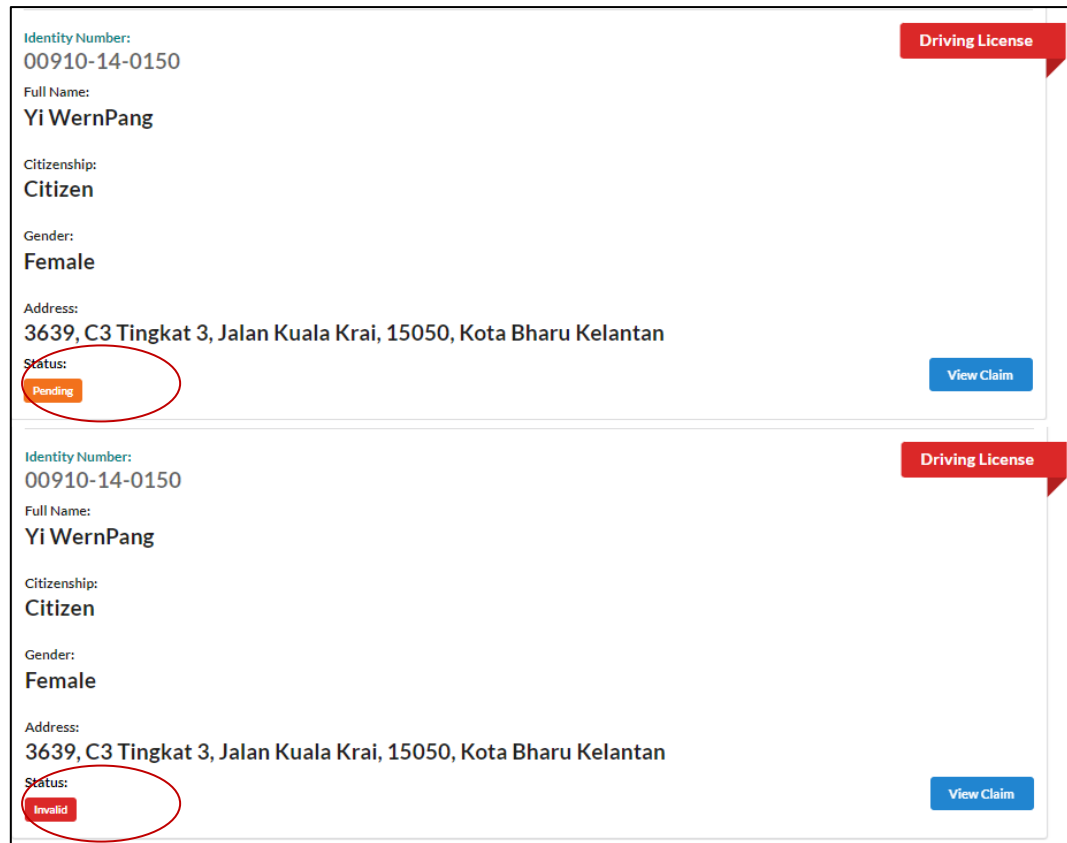
Identity Card

View Claim

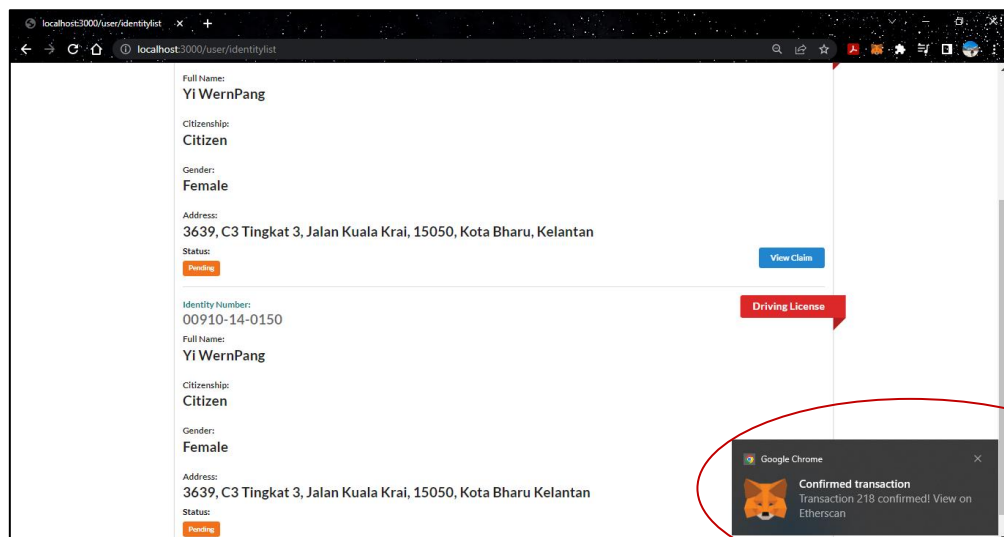
*Figure 6-14 Case (h) – (ii)*

**Figure 6-14** shows the case where the user identity claim has been verified and approved by the issuing authority. The status has switched from pending to valid, and the color from yellow to green.





*Figure 6-15 Case (h) – (iii)*



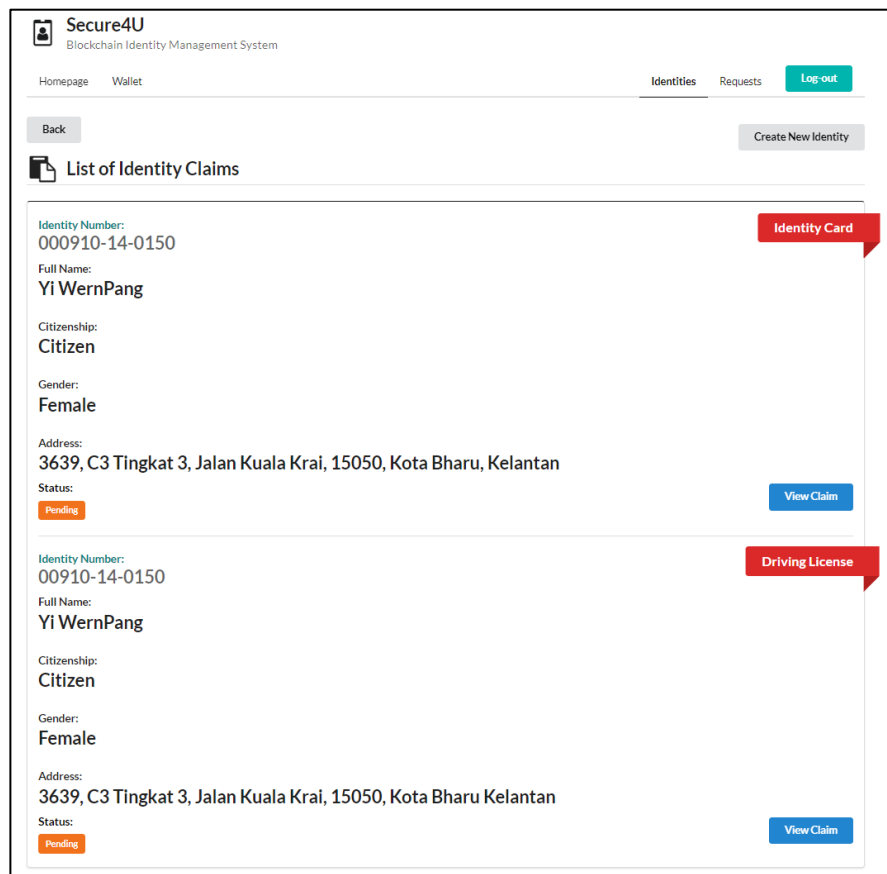
*Figure 6-16 Case (h) – (iv)*

**Figure 6-15** shows the case where the user identity claim has been verified and rejected by the issuing authority. The status has switched from pending to not valid, and the color from yellow to red. Upon any updates including pending, approved or

rejected, that specific will be updated and store at the Blockchain database (refer to **Figure 6-16**).



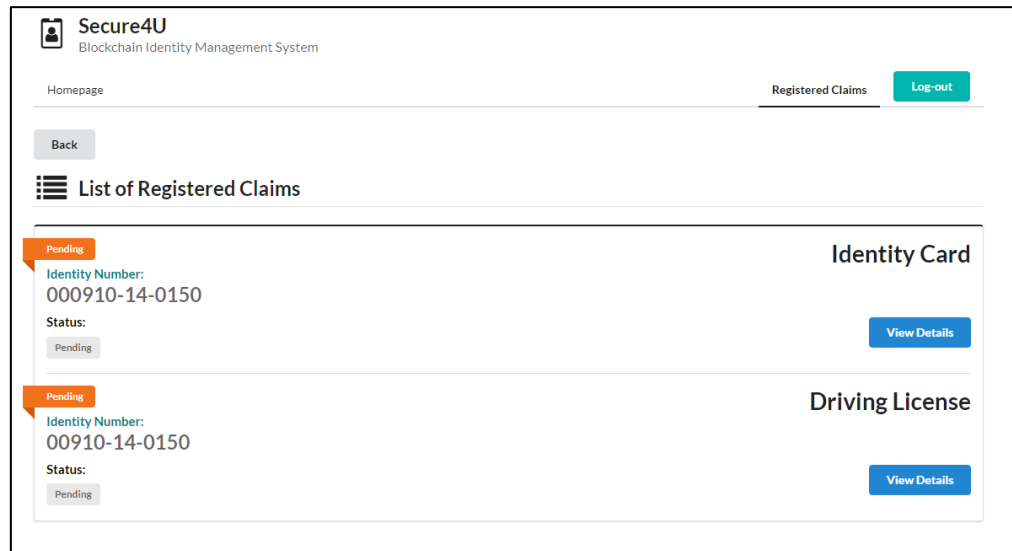
**Figure 6-17 Case (i) – (i)**



**Figure 6-18 Case (i) – (ii)**

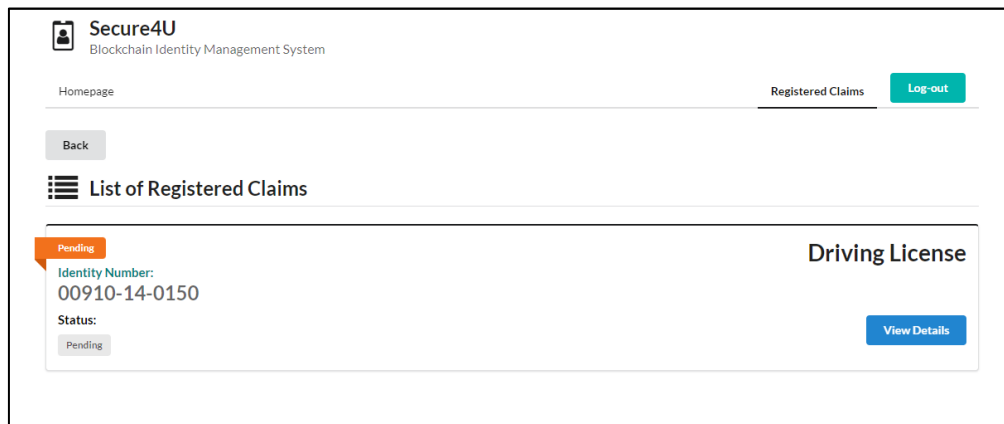
When the user tries to view the registered identity claims on the Blockchain identity management system, no identity claims will be displayed by the system if there are no identity claims registered by the user. Once user registered an identity claim, it will then be displayed to the user. The results are achieved as expected after performing the test case (refer to **Figure 6-17** & **Figure 6-18**).

For the case when issuing authority views user's registered claims, only the ones that are pending for verification will be displayed to the issuing authority side. This is to prevent unnecessary information to be displayed and viewed multiple times by the government which is more effective in terms of cost and time.



*Figure 6-19 Case (j) – (i)*

**Figure 6-19** have showed that the list of registered claims that are displayed at the issuing authority side are the ones with the status labeled as pending only.



*Figure 6-20 Case (k)*

For the case when the issuing authority has approved or rejected the registered claims that are pending for verification, that specific claim will not be displayed at the issuing authority side anymore. Based on **Figure 6-19**, previously there are two claims that are pending for verification. After the issuing authority has approved one

of the registered claims, which is the identity card claim, only one registered claim is displayed on the list, which is the driving license that is still pending for verification (refer to **Figure 6-20**). Besides that, the registered claims from the user’s side will be updated as well, which is from pending to either valid or not valid. Based on **Figure 6-14**, it has switched from pending to valid.

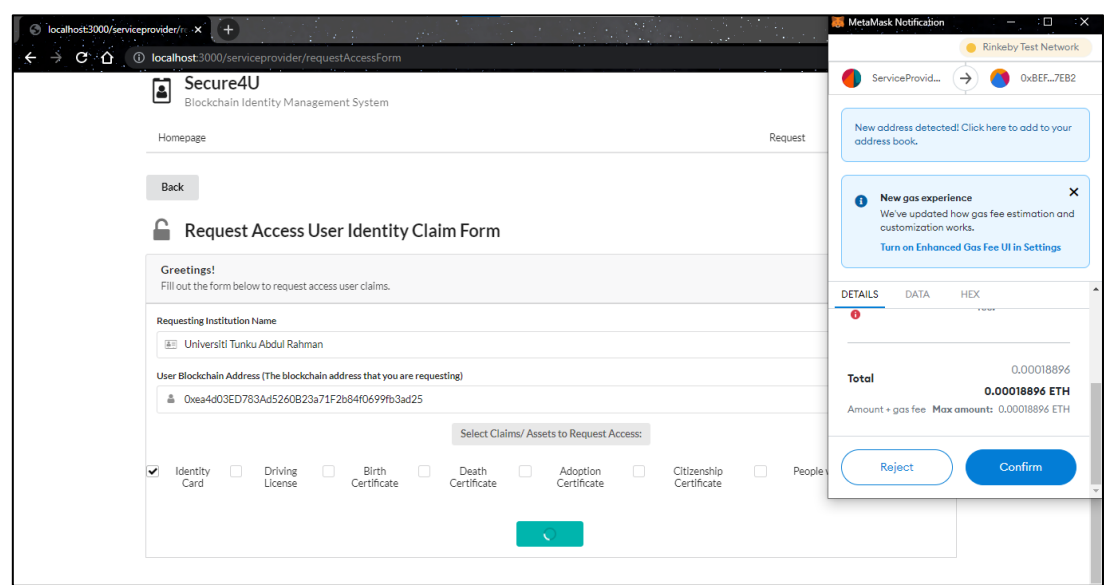


Figure 6-21 Case (I) – (i)

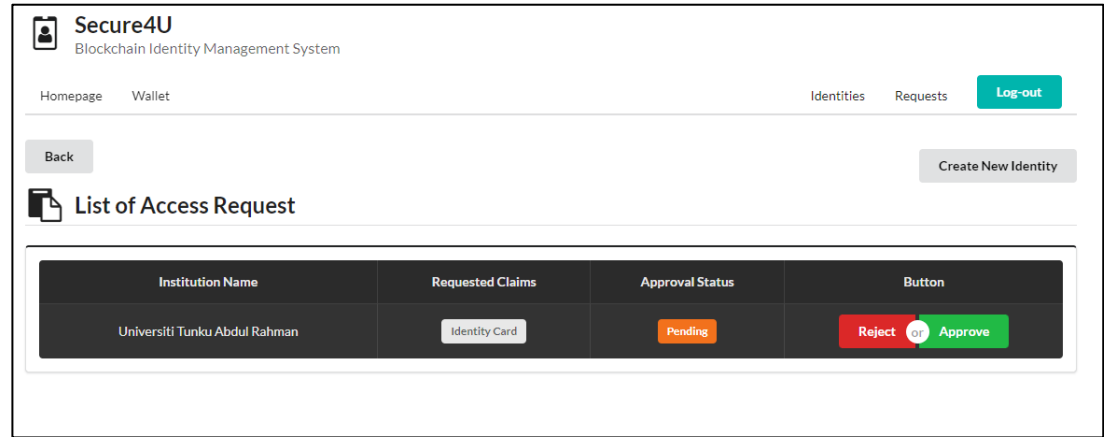
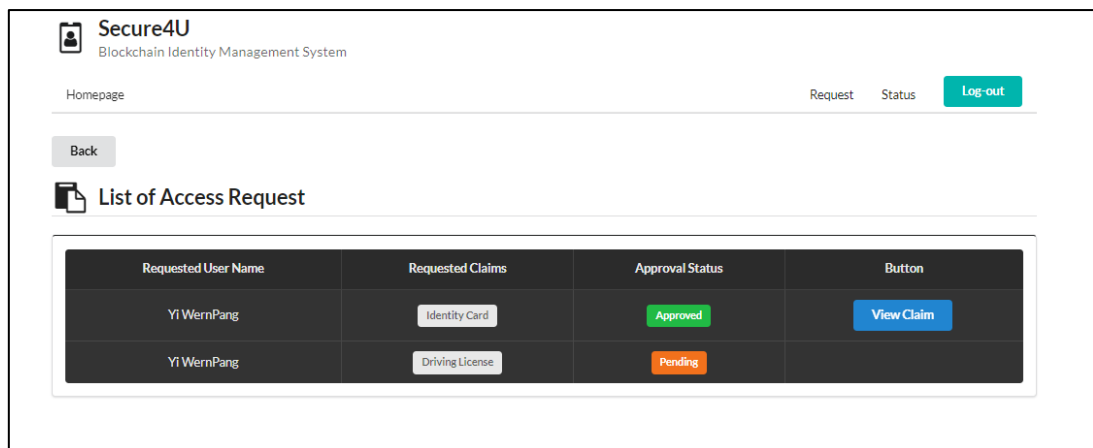
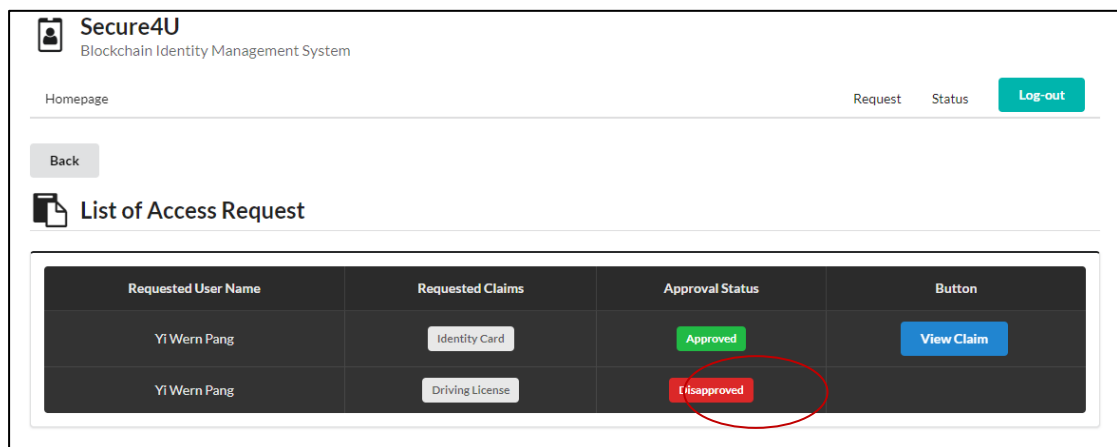


Figure 6-22 Case (I) – (ii)



**Figure 6-23 Case (l) – (ii) & Case (o)**

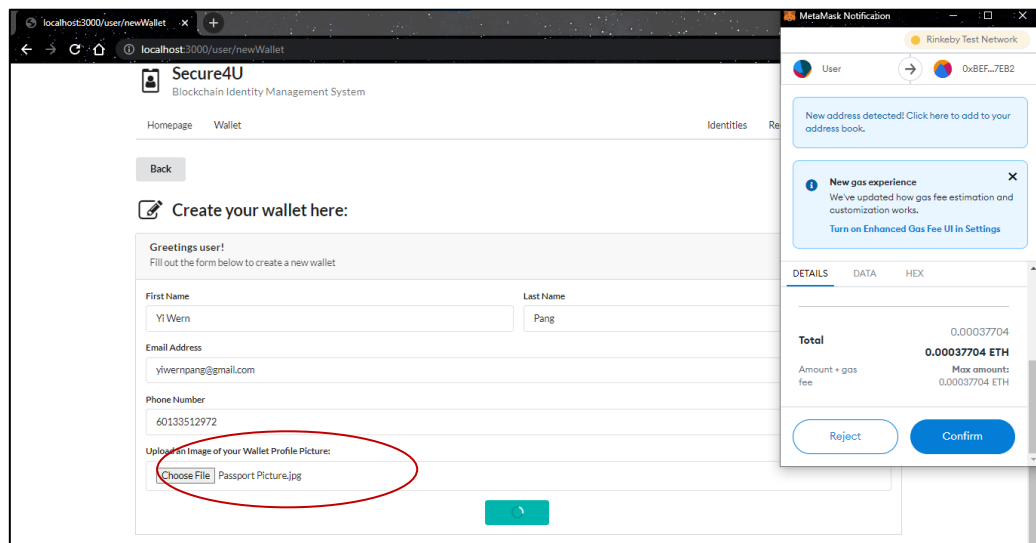
When the service provider/ legal institution sends a request to a specific user to access user's identity claim details, the user side is able to see that specific request. Based on **Figure 6-21** & **Figure 6-22**, after the service provider has sent a request to the user to access its identity card claim, that specific request can be seen through the identity access request function at the user side. User can decide whether to approve or reject the request. Other than that, the service provider can also view the status of his request through the request status at his side (refer to **Figure 6-23**).



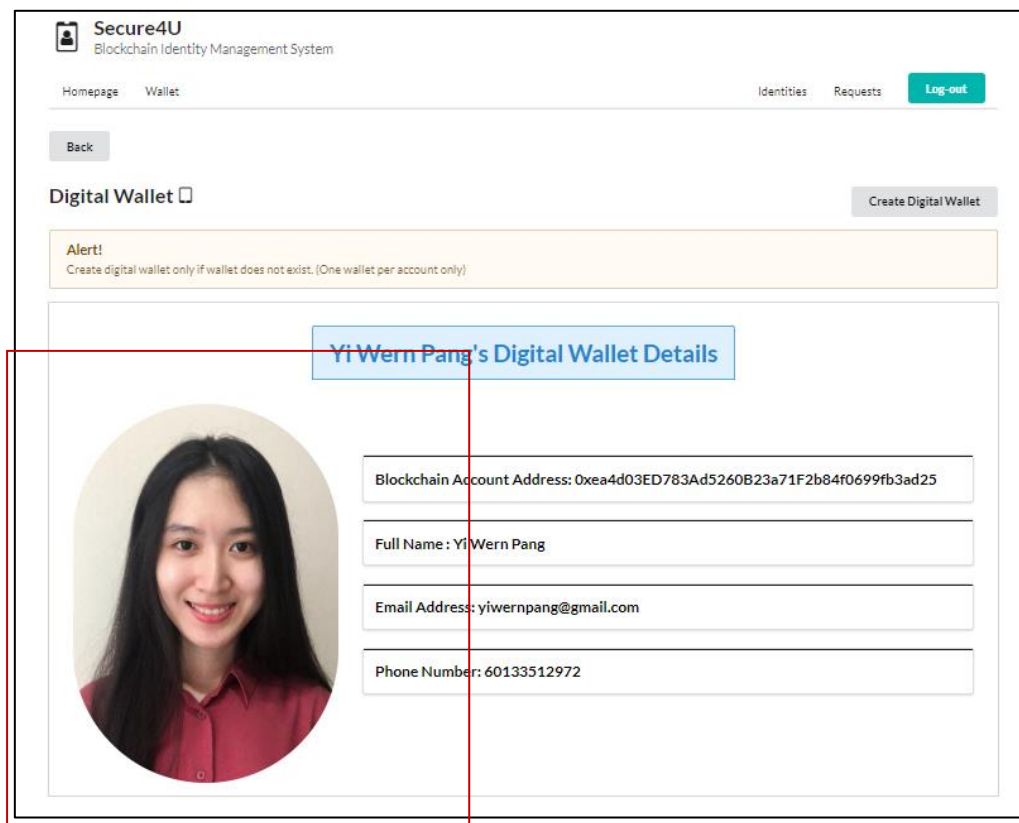
**Figure 6-24 Case (m) & Case (n)**

In the case where the service provider requested user's identity claim details and has been rejected by the user (refer to **Figure 6-24**). The service provider is unable to view the requested claim. While for pending approval claims, the service provider is not able to view the requested claims as well (refer to **Figure 6-23**). If the service provider has requested user's identity claim details and has been approved by the user,

the service provider is able to view the approved claims by clicking the view claim button (refer to **Figure 6-24**).

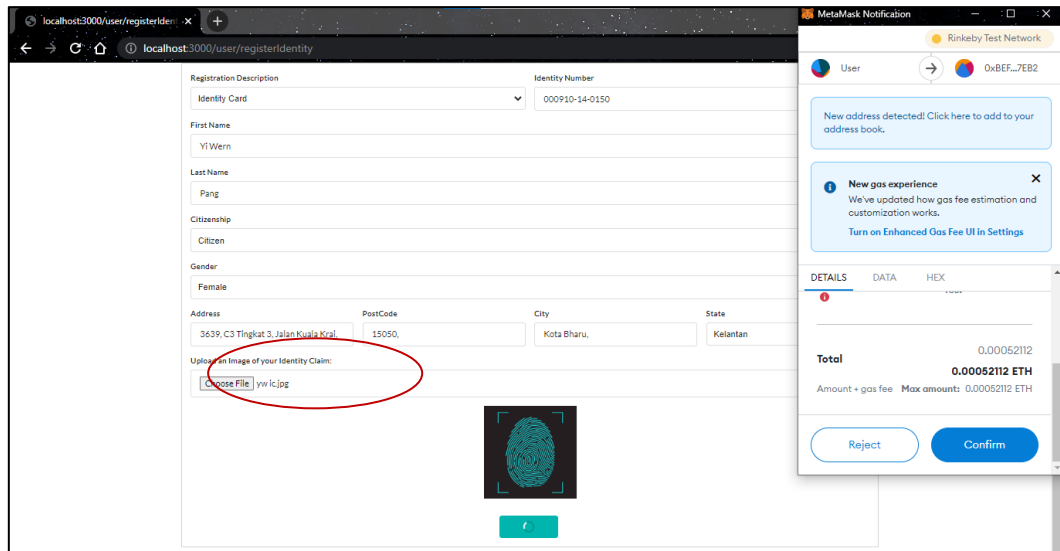


**Figure 6-25 Case (p) – (i)**



**Figure 6-26 Case (p) – (ii)**

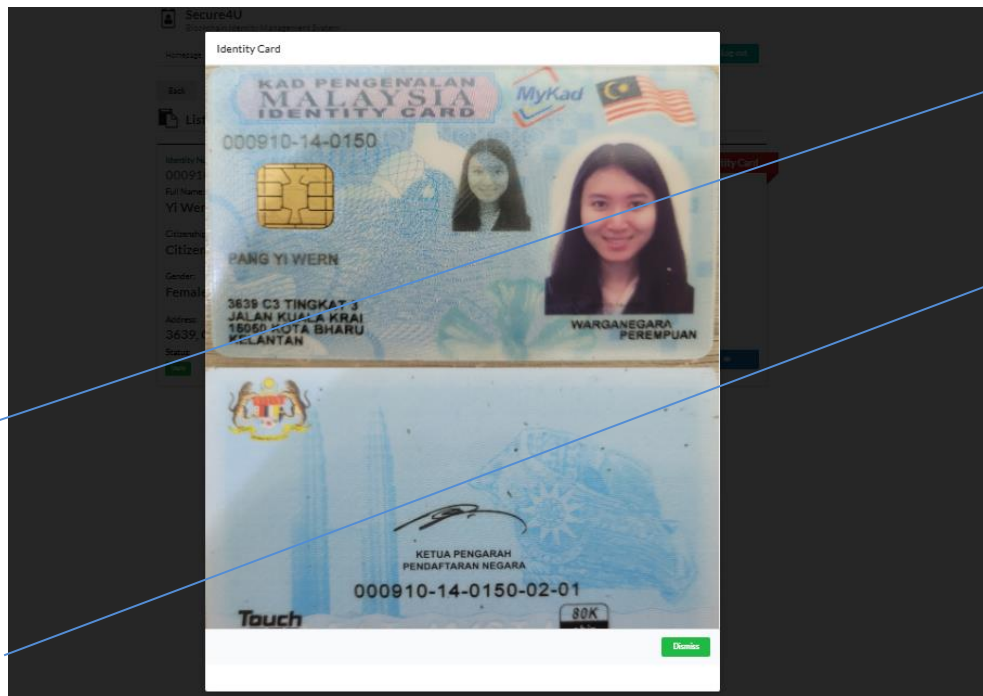
For this case, if the user has uploaded a picture for his digital profile at the digital wallet part (refer to **Figure 2-25**), the picture uploaded by the user will be displayed by the system at the digital wallet part (refer to **Figure 2-26**).



*Figure 6-27 Case (q) – (i)*



*Figure 6-28 Case (q) – (ii)*



*Figure 6-28 Case (q) – (iii)*

Besides that, if user have uploaded a picture during his registration of identity claims, the image of the identity claim can be viewed at the list of registered identity claims part by clicking the view claim button. This case has been tested and the results are as expected (refer to **Figure 2-27**, **Figure 2-28** & **Figure 2-29**).

After performing all the system testing and evaluation according to the verification plan set at Chapter 5, Section 5.5, the performance of all test cases is working as planned.



## Chapter 7: Conclusion and Recommendation

### 7.1 Conclusion

The proposed project focuses on developing a blockchain identity management system to solve the problems faced by existing identity management solutions in order to improve Malaysia government services in Ministry of Home Affairs in terms of identity management.

There are three main *problems* stated including risk of data breaches and identity thefts, abuse of trust resulting in lack of trust in business parties and over-relying on middle person for transaction processing. There is a huge *motive* for these problems to be solved as it can lead to a great lost for both citizens and government of Malaysia. Data breaches and identity thefts due to lack of data protection can be a serious issue as citizen's details may be used or forged by fraudsters to perform illegal activities under user's identity. Citizens' data privacy has also been violated which cause them to be reluctant to offer their personal details or claims to others including trusted authority. This is where abuse of trust issue is aroused as well. Most of the business transactions are performed online, which makes trust even harder to be foster as citizen's or government may not know who they are transacting with, and the validity of claims made by others. While for over-relying on middle person for transaction process, it can be very unnecessarily expensive as each middleperson make some money along the process and unnecessarily time consuming as the more processes are created and some executed manually.

*Solutions* offered by my proposed system can solve the problems stated. Using Blockchain technology, my proposed system can mitigate the risks of identity thefts and data breaches as well as trust issues by being tamper-proof and having strong data protection. This is where data stored are immutable and tamper resistant due to its strong data protection mechanism. Blockchain also acts as a distributed ledger that allows append-only operation; therefore, this results an immutable transaction data in the blocks and fully irreversible. This is where data cannot be easily exploited, forged, changed, or destroyed. The verification procedure by issuing authority will be ensuring the validity of user's registered claims

While being decentralized, business transactions and values are shared, managed, and maintained in a decentralized form across different people at different locations which eliminates the need for middleperson. Both citizens (users) side and government side are connected in my proposed system. This security-rich

environment is able to foster trust, transparency, and accountability in business relationships within different parties. Besides that, users are also having self-sovereign identity using my proposed system. This is where they can own and control the sharing of their identity claims to service providers or legal institutions.

Other than that, to successfully develop a good identity management system using blockchain technology, I have **reviewed** other existing blockchain identity management systems as well. The proposed project will be including most of the features that exist in the existing systems. However, something different from my proposed project is that my proposed system is a web-based system that supports three different roles for the identity management process (three roles are connected in one system). Besides that, users can own and control the sharing of their identity claims through the system.

Moreover, the **methodology** I have used is the prototyping method under Rapid Application Development (RAD) methodology category, which is highly feasible for my proposed system development. While for the main **challenges** faced, most of the resources and language used to complete this proposed project is unfamiliar for me, where I am required to spend more effort in learning the fundamentals of Blockchain as well as developing a system using Blockchain. After performing the testing and evaluation regarding the performance of my system based on different test cases, the performance of the system is working as planned.

In conclusion, the idea of digitizing our national identification system using Blockchain technology has not yet been implemented in Malaysia. Therefore, my proposed system may offer a wholesome experience to both citizens and government of Malaysia in terms of better safeguarding and managing user identity claims and transactions.

### **7.2 Recommendation**

After the development of my proposed project, there are some recommendations could be used in order to further improve my proposed project. The identity claims verification procedure that will be done by the issuing authority can be improved by integrating an AI software for the fingerprint comparison in order to prove the identity claims are registered by the original owner of the claims. Besides that, a face recognition algorithm can be integrated into the system as well. The facial recognition can be used by the user during the system log-in, registration of the identity asset to

prove its identity and also can be used while approving the identity access request made by the service providers. Both fingerprint or facial recognition will act as the base of proof or base of verification to show that the original owner itself is dealing with the system process. Most of the identity management system in the market are currently having this feature in order to act as the base of verification of a person's identity. However, due to the timeframe and area of expertise required, I am not able to develop this feature into my proposed system.

Despite of the difficulties and challenges that will be faced during development of a Blockchain project, the reason why I have chosen to implement Blockchain technology in my Identity Management System is because I really wanted to learn this technology as it is currently a valuable skillset needed in the market. Blockchain technology is now viewed as the future database which is now highly popular in advanced countries like Japan, China, Singapore, South Korea etc. Therefore, I highly recommend that learning this skillset can be really useful for our future career.

Other than that, using the case of the Russia-Ukraine War, we could never have imagined that someday they could be caught up in a war. Most of the centralized database that are used to store valuable data will surely been destroyed during the war. As the database is centralized, it acts as the only source of storage where all data could not be traced and retrieved anymore after the damage. The citizens of Russia and Ukraine will not be able to define which identity documents do they own neither identify whether that person is the person he has claimed. This is where Blockchain will come in handy. Blockchain acts as a distributed ledger technology where the database is in a decentralized manner. The database of all different nodes is connected, and each node are having the same copy of data. In this way, the citizens of Russia and Ukraine can retrieve and trace back their data from other nodes of the network. Therefore, this is the main reason why I highly recommend that the Blockchain technology should be implemented in Malaysia government services for its traceability and tamper resistant storage.

## **REFERENCES**

- [1] A.C. Benjamin, A.C. Emmanuel, and E. Franklin, “*National identification issues and the solution using smart card technology*,” in International Journal of Engineering Research & Technology (IJERT), 3(8), pp.314-320. Jun. 2020.
- [2] A. Tang, “Study: Malaysia the fifth-worst country for personal data protection.” TheStar.  
<https://www.thestar.com.my/news/nation/2019/10/16/studymalaysiathe-fifth-worst-country-for-personal-data-protection>. (accessed Jul.4, 2021).
- [3] A. Yusof, “Malaysia Airlines in data security "incident".” New Straits Times.<https://www.nst.com.my/business/2021/03/670856/malaysia-airlines-data-security-incident>. (accessed Jul.28, 2021).
- [4] B. Martucci, “What is Bitcoin – History, How It Works, Pros & Cons.” Money Crashers. <https://www.moneycrashers.com/bitcoin-history-how-it-works-pros-cons/>. (accessed Jul.11, 2021).
- [5] B. Marr, “*A Very Brief History of Blockchain Technology Everyone Should Read*.” Forbes. <https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchaintechnologyeveryoneshouldread/?sh=5a61f82d7bc4>. (accessed Jul.3, 2021).
- [6] B. Singhal, G. Dhameja, & P.P. Sekhar, “*A beginner’s guide to building blockchain solutions, Beginning Blockchain*.” SpringerLink.  
<https://doi.org/10.1007/978-1-4842-3444-0> . Accessed: Jul 1, 2021.
- [7] C. Fam, “CSM: Identity theft increasing in Malaysia mainly due to numerous data breaches.” The Star. <https://www.thestar.com.my/tech/tech-news/2019/04/16/ram-credit-information-to-work-with-cybersecurity-malaysia-to-prevent-identity-theft/>. (accessed Jul.4, 2021).

## REFERENCES

- [8] D.A. Sattar, "Cultivate accountability transparency during Covid-19 pandemic." New Straits Time.  
<https://www.nst.com.my/opinion/columnists/2020/07/606726/cultivateaccountability-transparency-during-covid-19-pandemic>. (accessed Jul.11, 2021).
- [9] "Digitization of transactional public services would reduce red tape and corruption, save money in Latin America and the Caribbean." IDB.  
<https://www.iadb.org/en/news/digitization-transactional-public-services-would-reduce-red-tape-and-corruption-save-money> (accessed Jul.11, 2021).
- [10] E. A. Franciscon, M. P. Nascimento, J. Granatyr, M. R. Weffort, O. R. Lessing and E. E. Scalabrin, "A Systematic Literature Review of Blockchain Architectures Applied to Public Services," *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2019, pp. 33-38, doi: 10.1109/CSCWD.2019.8791888. Accessed: Jul.1, 2021. Accessed: Jul 1, 2021.
- [11] G. Iredale, "Blockchain Cryptography: Everything You Need To Know." <https://101blockchains.com/blockchain-cryptography/> (accessed Aug. 2, 2021).
- [12] G. Menegazzo Verzeletti, E. Ribeiro de Mello and M. Silva Wangham, "A National Mobile Identity Management Strategy for Electronic Government Services," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 668-673, doi: 10.1109/TrustCom/BigDataSE.2018.00098. Accessed: Jul 11, 2021.
- [13] "Guideline: What is Bitcoin and how does Bitcoin work?."

## REFERENCES

- BBC.  
<https://www.bbc.co.uk/newsround/25622442#:~:text=How%20does%20Bitcoin%20work%3F,Getty%20Images&text=Each%20Bitcoin%20is%20basically%20a,send%200Bitcoins%20to%20other%20people.&text.> (accessed Jul.3, 2021).
- [14] "Identity theft alert." The Star. <https://www.thestar.com.my/business/business-news/2021/05/01/identity-theft-alert> (accessed Jul.28, 2021).
- [15] J.A. Torres, G. Verzeletti, R. Távera, R.T. de Sousa Júnior, and E. de Mello, "A national identity management strategy to enhance the Brazilian electronic government," *in CLEI Electronic Journal*, 20(3), pp.8-1. Dec. 2017.
- [16] K. Mudliar, H. Parekh and P. Bhavathankar, "A comprehensive integration of national identity with blockchain technology," 2018 International Conference on Communication information and Computing Technology (ICCICT), 2018, pp. 1-6, doi: 10.1109/ICCICT.2018.8325891. Accessed: Jul 16, 2021.
- [17] M. Sahu, "Cryptography in Blockchain: Types & Applications." upGrad <https://www.upgrad.com/blog/cryptography-in-blockchain/> (accessed Jul. 28, 2021).
- [18] S. E. Haddouti and M. D. Ech-Cherif El Kettani, "Analysis of Identity Management Systems Using Blockchain Technology," **2019 International Conference on Advanced Communication Technologies and Networking (CommNet)**, 2019, pp. 1-7, doi:10.1109/COMMNET.2019.8742375. Accessed: Jul 15, 2021.
- [19] N. Naik and P. Jenkins, "uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain," 2020 IEEE International Symposium on Systems Engineering

## REFERENCES

- (ISSE), 2020, pp. 1-7, doi: 10.1109/ISSE49799.2020.9272223. Accessed: Jul 11, 2021.
- [20] P. Dunphy and F. A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," in *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20-29, July/August 2018, doi: 10.1109/MSP.2018.3111247. Accessed: Jul 15, 2021.
- [21] R. A. Canessane, N. Srinivasan, A. Beuria, A. Singh and B. M. Kumar, "Decentralised Applications Using Ethereum Blockchain," *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, 2019, pp. 75-79, doi: 10.1109/ICONSTEM.2019.8918887. Accessed: Jul 1, 2021.
- [22] S. Choudhari, S. K. Das and S. Parasher, "Interoperable Blockchain Solution For Digital Identity Management," 2021 6th International Conference for Convergence in Technology (I2CT), 2021, pp. 1-6, doi: 10.1109/I2CT51068.2021.9418220. Accessed: Jul 13, 2021.
- [23] S.K. Khor, "Malaysia does not have a good record of transparency." The Star.  
<https://www.thestar.com.my/opinion/columnists/vitalsigns/2020/01/15/malaysia-does-not-have-a-good-record-of-transparency>. (accessed Jul. 4, 2021).
- [24] S. Mohamed, "Identity Crime in the Digital Age: Malaysian and Mauritanian Legal Frameworks," in *International Journal of Law, Government, and Communication*, 4(15), pp.154-165. July. 2019.
- [25] "The Importance of Trust in Online Business Transactions."ManagedLEI.  
<https://managedlei.com/blog/importance-of-trust-in-online-business-transactions/#:~:text=A%20sense%20of%20trust%20in,trade%20safely%20across%20borders%20increases>. (accessed Jul.11, 2021)

## REFERENCES

- [26] “What is a Merkle Tree and How Does it Affect Blockchain Technology?.” Selfkey. <https://selfkey.org/what-is-a-merkle-tree-and-how-does-it-affect-blockchain-technology/> (accessed Aug. 2, 2021).
- [27] “What is Zero Trust?” CROWDSTRIKE. <https://www.crowdstrike.com/epp-101/zero-trust-security/>. (accessed Jul.2, 2021).
- [28] W. L. Sim, H. N. Chua and M. Tahir, "Blockchain for Identity Management: The Implications to Personal Data Protection," **2019 IEEE Conference on Application, Information and Network Security (AINS)**, 2019, pp. 30-35, doi: 10.1109/AINS47559.2019.8968708. Accessed: Jul 15, 2021.



**WEEKLY LOG****FINAL YEAR PROJECT WEEKLY REPORT***(Project II)*

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 1
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

**1. WORK DONE**

[Please write the details of the work done in the last fortnight.]

- Supervisor brief guidelines regarding FYP2 and give comments to improve our report better. (FYP1 as reference).

**2. WORK TO BE DONE**

- Review background information, problem statement, project objectives, project scope, literature reviews etc. from fyp1 report to improve it better and place the improved ones into FYP2 report.

**3. PROBLEMS ENCOUNTERED**

- No problems encountered yet.

**4. SELF EVALUATION OF THE PROGRESS**

- Refer back to FYP1 system to see which module pending to complete and modify ui design of the system.
- Learn the fundamentals and resources to develop other module of the system through online learning sources.
- Not yet start the reporting part.



Supervisor's signature



Student's signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 2
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

## 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Supervisor brief additional guidelines regarding FYP2.
- Supervisor check on progress of the report and development.

## 2. WORK TO BE DONE

- Make some improvements for the adjustments made at Chapter 1 FYP2.
- .

## 3. PROBLEMS ENCOUNTERED

- No problems encountered yet for system development part.

## 4. SELF EVALUATION OF THE PROGRESS

- Learning the fundamentals and resources to develop the system through online learning sources.
- Completed the Chapter 1 part to be improved for FYP2 report and reviewed by supervisor.



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 3
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Supervisor briefs additional guidelines regarding FYP2
- Supervisor check on progress of the development and report

### 2. WORK TO BE DONE

- Minor adjustment on the design part.
- Review back the overall flow of the system and its functionalities (Constructing Flowchart, Use Case Diagrams)
- Complete Chapter 3 of the report by next week.

### 3. PROBLEMS ENCOUNTERED

- Minor problem at the coding part.

### 4. SELF EVALUATION OF THE PROGRESS

- Project still in development process. (Working on a function of the proposed system).
- Completed FYP2 report up to Chapter 2.



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 4
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Completed Chapter 1, Chapter 2, Chapter 3 for the report.
- Supervisor brief other requirements regarding FYP2.
- Supervisor check on progress of the development and report.

### 2. WORK TO BE DONE

- Make some adjustment on Chapter 3 diagrams.
- Continue completing the function development of the proposed system.

### 3. PROBLEMS ENCOUNTERED

- No problems encountered so far.

### 4. SELF EVALUATION OF THE PROGRESS

- Completed Chapter 1, Chapter 2 & Chapter 3 for the report.
- Project still in development process. (Working on a function of the proposed system).



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 5
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Completed Chapter 1, Chapter 2, Chapter 3 for the report.
- Supervisor brief other requirements regarding FYP2.
- Supervisor check on progress of the development and report.
- Continue completing the function development of the proposed system.

### 2. WORK TO BE DONE

- Complete rest of the parts of Chapter 5 of the report by next week (week 6).

### 3. PROBLEMS ENCOUNTERED

- No problems encountered so far.
- Minor problems at the coding part for constructing the system needs to be investigated.

### 4. SELF EVALUATION OF THE PROGRESS

- Starting on the system ui design improvement.
- Completing the main functions of the proposed system.



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 6
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Supervisor checks on progress of the development and report
- Completed Chapter 1, 2 and 3 of the report.

### 2. WORK TO BE DONE

- Complete Chapter 5.
- Work on ui design of proposed system.

### 3. PROBLEMS ENCOUNTERED

- No problems encountered so far.

### 4. SELF EVALUATION OF THE PROGRESS

- Overall system main function is completed.
- Working on additional function of the system.
- Half-way completing Chapter 5.



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 7
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Supervisor checks on progress of the development and report
- Completed Chapter 1, 2, 3 and 5 of the report.

### 2. WORK TO BE DONE

- Continue improving user interface design of proposed system.
- Continue developing the additional function of the proposed system.

### 3. PROBLEMS ENCOUNTERED

- No problems encountered so far.

### 4. SELF EVALUATION OF THE PROGRESS

- Overall system main function is completed.
- Working on additional function of the system.
- Working on user interface design of the proposed system.
- Completed Chapter 5 of report.



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 8
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Supervisor checks on progress of the development and report
- Completed Chapter 1, 2, 3 and 5 of the report.

### 2. WORK TO BE DONE

- Continue improving user interface design of proposed system.
- Continue developing the additional function of the proposed system.

### 3. PROBLEMS ENCOUNTERED

- No problems encountered so far at the development process.

### 4. SELF EVALUATION OF THE PROGRESS

- Overall system main function is completed.
- Working on additional function of the system.
- Working on user interface design of the proposed system.
- Completed Chapter 1, 2, 3, 5 of report.
- Doing Chapter 4 and 6 of the report.



Supervisor's signature



Student's signature



## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 9
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Supervisor checks on progress of the development and report
- Completed Chapter 1, 2, 3 and 5 of the report.

### 2. WORK TO BE DONE

- Show proposed system to Supervisor by next week.

### 3. PROBLEMS ENCOUNTERED

- No problems encountered so far at the development process and reporting part.

### 4. SELF EVALUATION OF THE PROGRESS

- Overall system main function is completed.
- Working on additional function of the system.
- Working on user interface design of the proposed system.
- Completed Chapter 1, 2, 3, 5 of report.
- Completing Chapter 4 and 6 of the report.



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 10
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Showed Supervisor overall system development.
- Supervisor gave suggestions and comment
- Supervisor checks on report progress.

### 2. WORK TO BE DONE

- Amendments of the proposed system needed to be done.
- Show supervisor the amendments of proposed by this week.

### 3. PROBLEMS ENCOUNTERED

- No problems encountered.

### 4. SELF EVALUATION OF THE PROGRESS

- Overall user interface and functionalities of the system works smoothly.
- Completing Chapter 4 and 6 of the report.



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 11
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Completed system development.

### 2. WORK TO BE DONE

- Complete Chapter 7 of the report.
- Complete the formatting of the report.

### 3. PROBLEMS ENCOUNTERED

- No problems encountered.

### 4. SELF EVALUATION OF THE PROGRESS

- Overall user interface and functionalities of the system works smoothly.
- Completing the report.



Supervisor's signature



Student's signature

## FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> 3,3	<b>Study week no.:</b> 12
<b>Student Name &amp; ID:</b> Pang Yi Wern 18ACB01768	
<b>Supervisor:</b> Mr. Su Lee Seng	
<b>Project Title:</b> Development of Decentralized Apps Using Blockchain Technology to Improve Malaysian Government Services in Ministries of Home Affairs – Digital Identity Management	

### 1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Completed system development.
- Completed report.

### 2. WORK TO BE DONE

- Submit report by Week 13.
- Complete presentation and send video to supervisor and moderator.

### 3. PROBLEMS ENCOUNTERED

- No problems encountered.

### 4. SELF EVALUATION OF THE PROGRESS

- Completed system development.
- Completed report.
- Preparing for FYP2 presentation.



Supervisor's signature



Student's signature

**POSTER**

**Final  
Year  
Project**

# BLOCKCHAIN IDENTITY MANAGEMENT SYSTEM

**Project Overview**

The project aims to improve Malaysian government services in Ministries of Home Affairs by better safeguarding and managing Malaysia citizens' identity claims using Blockchain Technology that enhances security, trust and transparency.

**Project Statement**

- Risks of data breaches and identity thefts
- Abuse of trust resulting in lack of trust among parties in business
- Over-relying on middle person for transaction process

**Project Objectives**

- To develop a tamper-resistant identity management system with strong data protection mechanism to mitigate risks of identity thefts and data breaches in Malaysia
- To integrate a distributed ledger in the identity management system for good identity record management that imposes trust to business parties
- To eliminate middle person in identity management transaction process to cut identity management cost and time
- To allow users to have control over their identity claims and apply effective reviewing process to ensure controlled sharing of identity claims

**Project Scope**

Decentralized web application:

- Log-in page to control access of different roles of the system
- Verification procedure to ensure validity of user's registered claims
- Users and government are connected in one system
- Self-sovereign identity

**Methodology**

- Developed using prototyping methodology
- Visual Studio Code for website development
- Remix Editor for smart contract coding

**UTAR**  
UNIVERSITI TUNKU ABDUL RAHMAN

**Bachelor of Business Information Systems (Honours)**

**By: Pang Yi Wern**

**Supervisor: Mr. Su Lee Seng**

## PLAGIARISM CHECK RESULT

## PLAGIARISM CHECK RESULT

Document Viewer

### Turnitin Originality Report

Processed on: 21-Apr-2022 00:09 +08  
ID: 1815528029  
Word Count: 18978  
Submitted: 1

YiWern FYP2 Check By Yi Wern Pang

Similarity Index	Similarity by Source
6%	Internet Sources: 3% Publications: 2% Student Papers: 2%

<a href="#">include quoted</a> <a href="#">include bibliography</a> <a href="#">excluding matches &lt; 7 words</a> mode: <a href="#">quickview (classic) report</a> <a href="#">Change mode</a>
<a href="#">print</a> <a href="#">download</a>
1% match (Internet from 04-Sep-2021) <a href="https://101blockchains.com/blockchain-cryptography/">https://101blockchains.com/blockchain-cryptography/</a>
1% match (publications) <a href="#">Paul Dunphy, Fabien A.P. Petitcolas. "A First Look at Identity Management Schemes on the Blockchain", IEEE Security &amp; Privacy, 2018</a>
<1% match (Internet from 27-Jul-2021) <a href="http://eprints.utar.edu.my">http://eprints.utar.edu.my</a>
<1% match (Internet from 20-Mar-2022) <a href="http://eprints.utar.edu.my">http://eprints.utar.edu.my</a>
<1% match (publications) <a href="#">Jennifer Harder. "Accurate Layer Selections Using Photoshop's Selection Tools", Springer Science and Business Media LLC, 2022</a>
<1% match (publications) <a href="#">Monica Gahlawat. "Survey of Online Identity Management Techniques on Blockchain", International Journal of Security and Privacy in Pervasive Computing, 2020</a>
<1% match (Internet from 09-Dec-2020) <a href="https://www.leewayhertz.com/blockchain-identity-management/">https://www.leewayhertz.com/blockchain-identity-management/</a>
<1% match (Internet from 06-Mar-2022) <a href="https://wikimili.com/en/Sorare">https://wikimili.com/en/Sorare</a>
<1% match (Internet from 12-Jun-2018) <a href="https://www.iadb.org/en/news?created=&amp;created_1=&amp;created_2=All&amp;f%5B0%5D=filter%3A1126&amp;f%5B1%5D=filter_news_by_country%3A1008&amp;f%5B4%5D=fi">https://www.iadb.org/en/news?created=&amp;created_1=&amp;created_2=All&amp;f%5B0%5D=filter%3A1126&amp;f%5B1%5D=filter_news_by_country%3A1008&amp;f%5B4%5D=fi</a>
<1% match (publications) <a href="#">Yang Liu, Deblao He, Mohammad S. Obaidat, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo. "Blockchain-based identity management systems: A review", Journal of Network and Computer Applications, 2020</a>
<1% match (Internet from 04-Jun-2021) <a href="https://sit124-assignment3-group24-2021.azurewebsites.net/blockchain-historical-information/">https://sit124-assignment3-group24-2021.azurewebsites.net/blockchain-historical-information/</a>
<1% match (Internet from 16-Dec-2021) <a href="https://archives.astroawani.com/2021/07">https://archives.astroawani.com/2021/07</a>
<1% match (student papers from 15-Mar-2015) <a href="#">Submitted to Laureate Higher Education Group on 2015-03-15</a>

## PLAGIARISM CHECK RESULT

<1% match (publications) <a href="#">Nitin Naik, Paul Jenkins. "Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems", 2020 IEEE International Symposium on Systems Engineering (ISSE), 2020</a>
<1% match (student papers from 06-Aug-2021) <a href="#">Submitted to Purdue University on 2021-08-06</a>
<1% match (student papers from 11-May-2021) <a href="#">Submitted to Barcelona School of Management on 2021-05-11</a>
<1% match (student papers from 29-Nov-2018) <a href="#">Submitted to Universite Saint Joseph on 2018-11-29</a>
<1% match (student papers from 03-Oct-2019) <a href="#">Submitted to University of Limerick on 2019-10-03</a>
<1% match (Internet from 01-Jan-2022) <a href="https://digitalassets.lib.berkeley.edu/techreports/ucb/text/ERI-92-59.pdf">https://digitalassets.lib.berkeley.edu/techreports/ucb/text/ERI-92-59.pdf</a>
<1% match (Internet from 10-Apr-2022) <a href="https://ir.unimas.my/id/eprint/33936/1/Nursyuhada%20Binti%20Amir%20Shariffuddin%20-%202024%20pgs.pdf">https://ir.unimas.my/id/eprint/33936/1/Nursyuhada%20Binti%20Amir%20Shariffuddin%20-%202024%20pgs.pdf</a>
<1% match (student papers from 13-Mar-2019) <a href="#">Submitted to International Islamic University Malaysia on 2019-03-13</a>
<1% match (student papers from 08-Sep-2019) <a href="#">Submitted to University Of Tasmania on 2019-09-08</a>
<1% match (Internet from 13-Dec-2018) <a href="https://pdf.usaid.gov/pdf_docs/PA00KC7M.pdf">https://pdf.usaid.gov/pdf_docs/PA00KC7M.pdf</a>
<1% match (student papers from 23-Nov-2020) <a href="#">Submitted to Solihull College, West Midlands on 2020-11-23</a>
<1% match (publications) <a href="#">Kumaresan Mudliar, Harshal Parekh, Prasenjit Bhavathankar. "A comprehensive integration of national identity with blockchain technology", 2018 International Conference on Communication Information and Computing Technology (ICCICT), 2018</a>
<1% match (Internet from 23-Mar-2022) <a href="https://www.w3.fund">https://www.w3.fund</a>
<1% match (Internet from 30-Mar-2020) <a href="https://www.toptal.com/insights/innovation/blockchain-identity-management">https://www.toptal.com/insights/innovation/blockchain-identity-management</a>
<1% match (publications) <a href="#">Sridhar Alla, Suman Kalyan Adari. "Beginning MLOps with MLFlow", Springer Science and Business Media LLC, 2021</a>
<1% match (Internet from 02-Aug-2021) <a href="http://docplayer.net">http://docplayer.net</a>
<1% match (Internet from 03-Mar-2022) <a href="https://ebin.pub/sensors-and-measurement-systems-2nbsped-8770226075-9788770226073.html">https://ebin.pub/sensors-and-measurement-systems-2nbsped-8770226075-9788770226073.html</a>
<1% match (publications) <a href="#">"New Approaches for Security, Privacy and Trust in Complex Environments", Springer Science and Business Media LLC, 2007</a>
<1% match (publications) <a href="#">Christoph Buck, Christian Olenberger, André Schweizer, Fabiane Völter, Torsten Eymann. "Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-trust", Computers &amp; Security, 2021</a>
<1% match (publications) <a href="#">K. Pubudu Nuwanthika Jayasena, Poddivila Marage Nimasha Ruwandi Madhunamali. "chapter 15 Blockchain and IoT-Based Diary Supply Chain Management System for Sri Lanka", IGI Global, 2021</a>
<1% match (publications) <a href="#">Ramani Selvanambi, Bhavya Taneja, Priyal Agrawal, Henil Jayesh Thakor, Marimuthu Karuppiah. "Blockchain-Based Identity Management Systems", Wiley, 2022</a>
<1% match (publications) <a href="#">Suyel Namasudra, Ganesh Chandra Deka, Prashant Johri, Mohammad Hosseinpour, Amir H. Gandomi. "The Revolution of Blockchain: State-of-the-Art and Research Challenges", Archives of Computational Methods in Engineering, 2020</a>
<1% match (Internet from 12-Jan-2022) <a href="https://inechain.com/search?q=icloud+activation+bypass+tool">https://inechain.com/search?q=icloud+activation+bypass+tool</a>
<1% match (Internet from 30-Oct-2020) <a href="http://static.garmin.com">http://static.garmin.com</a>



Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1 of 1



## FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

<b>Full Name(s) of Candidate(s)</b>	PANG YI WERN
<b>ID Number(s)</b>	18ACB01768
<b>Programme / Course</b>	Bachelor Of Information Systems (Honours) Business Information Systems/ Faculty of Information and Communication Technology (Kampar Campus)
<b>Title of Final Year Project</b>	Development Of Decentralized Apps Using Blockchain Technology To Improve Malaysian Government Services In Ministries Of Home Affairs – Digital Identity Management

Similarity	Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)
<b>Overall similarity index: <u>6</u> %</b>  <b>Similarity by source</b> Internet Sources: <u>3</u> % Publications: <u>2</u> % Student Papers: <u>2</u> %	
<b>Number of individual sources listed of more than 3% similarity: <u>0</u></b>	
<b>Parameters of originality required and limits approved by UTAR are as Follows:</b> (i) Overall similarity index is 20% and below, and (ii) Matching of individual sources listed must be less than 3% each, and (iii) Matching texts in continuous block must not exceed 8 words <i>Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.</i>	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

***Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.***

*Su Lee*

\_\_\_\_\_  
Signature of Supervisor

Name: Mr. Su Lee Seng

Date: 21/04/2022

\_\_\_\_\_  
Signature of Co-Supervisor

Name:

Date:





# UNIVERSITI TUNKU ABDUL RAHMAN

## FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (KAMPAR CAMPUS) CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	18ACB01768
Student Name	Pang Yi Wern
Supervisor Name	Mr. Su Lee Seng

TICK (✓)	DOCUMENT ITEMS
	Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
✓	Front Plastic Cover (for hardcopy)
✓	Title Page
✓	Signed Report Status Declaration Form
✓	Signed FYP Thesis Submission Form
✓	Signed form of the Declaration of Originality
✓	Acknowledgement
✓	Abstract
✓	Table of Contents
✓	List of Figures (if applicable)
✓	List of Tables (if applicable)
✓	List of Symbols (if applicable)
✓	List of Abbreviations (if applicable)
✓	Chapters / Content
✓	Bibliography (or References)
✓	All references in bibliography are cited in the thesis, especially in the chapter of literature review
✓	Appendices (if applicable)
✓	Weekly Log
✓	Poster
✓	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)
✓	I agree 5 marks will be deducted due to incorrect format, declare wrongly the ticked of these items, and/or any dispute happening for these items in this report.

\*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report.

(Signature of Student)

Date: 21/04/2022