DIGITAL RINGGIT USING DIGITAL SIGNATURE FOR AUTHENTICITY

FATIN ZULAIKHA BINTI SHAMSUL RIZAL

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: [**DIGITAL RINGGIT USING DIGITAL SIGNATURE FOR AUTHENTICITY**]

SESI PENGAJIAN: [2023 / 2024]

Saya: ____FATIN ZULAIKHA BINTI SHAMSUL RIZAL_____

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)

_____ TIDAK TERHAD

Fatin

(TANDATANGAN PELAJAR)

Alamat tetap: No 314 Kg Ketari 28700 Bentong Pahang .DM

(TANDATANGAN PENYELIA)

(NUR AZMAN BIN ABU)

Tarikh: 20/9/2023

Tarikh: 22/09/2023

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak

DIGITAL RINGGIT USING DIGITAL SIGNATURE FOR AUTHENTICITY

FATIN ZULAIKHA BINTI SHAMSUL RIZAL

This report is submitted in partial fulfilment of the requirements for the Bachelor of [Computer Science (Computer Security)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

DIGITAL RINGGIT USING DIGITAL SIGNATURE FOR AUTHENTICITY

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : _____ Date : 20/9/2023

FATIN ZULAIKHA BINTI SHAMSUL RIZAL

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of [Computer Science (Computer Security)] with Honours.

SUPERVISOR : _____ Date : 22/09/2023

PROFESSOR MADYA DR NUR AZMAN BIN ABU

DEDICATION

The basis of my journey has been my devoted parents, whose undying love, support, and encouragement I would want to dedicate this FYP report to. I will always be grateful for your support and efforts since they have inspired me to continually aim for the stars.

Additionally, I want to extend my sincere gratitude to my supervisor, who had a crucial role in the development of this project. Your tremendous guidance has helped me navigate the complexity of this research thanks to your knowledge, experience, and mentorship. You have genuinely inspired me with your perseverance, passion, and unshakable dedication to my academic development.

Thank you to my parents and boss for being my pillars of support and for having faith in me. Without your constant support, this accomplishment would not have been possible. I've dedicated this piece to you as a sign of my gratitude and respect.

ACKNOWLEDGEMENTS

I would like to thanked my supervisor, Professor Madya DR. Nur Azman bin Abu for who have provided me with a fantastic opportunity to get involved in the development of the field of Central Bank Digital Currency (CBDC).

The advice he gave me constantly helped me to overcome the issues I was having with this assignment. Thank you very much to my supervisor once more. I would also like to thank my beloved parents who have been giving me support and motivation throughout my project.

The journey in completing this project was a quite interesting ride. The journey taught me a lot of knowledge and amazing input. Therefore, I hope the project will be go smooth and clear.

ABSTRACT

The creation CBDC (Central Bank Digital Currency) are ongoing worldwide. CBDCs are needed to modernize a national network of finance, and central banks have taken different approaches to design and research. A digital currency that the central bank created would need to support quicker and less expensive payments while maintaining customer privacy. Despite Malaysia's lack of a privacy laws, it is crucial to preserve consumer privacy. The privacy rights of customers would need to be protected, but a digital ringgit would also need to provide the openness required to discourage illegal behaviour. A large growth of BNM's function in the financial system and the economy shouldn't be aided by a digital ringgit. The private sector would provide accounts or digital wallets under a bank intermediation to simplify the administration of a digital ringgit payment system. These already established potential middlemen will provide services on a free market for digital ringgit.

ABSTRAK

Penciptaan CBDC (Central Bank Digital Currency) sedang berjalan di seluruh dunia. CBDC diperlukan untuk memodenkan rangkaian kewangan nasional, dan bank pusat telah mengambil pendekatan yang berbeza untuk mereka bentuk dan penyelidikan. Mata wang digital yang dibuat oleh bank pusat perlu menyokong pembayaran yang lebih cepat dan lebih murah sambil mengekalkan privasi pelanggan. Walaupun Malaysia kekurangan undang-undang privasi, adalah penting untuk mengekalkan privasi pengguna. Hak privasi pelanggan perlu dilindungi, tetapi ringgit digital juga perlu menyediakan keterbukaan yang diperlukan untuk menghalang tingkah laku yang menyalahi undang-undang. Pertumbuhan besar fungsi BNM dalam sistem kewangan dan ekonomi tidak seharusnya dibantu oleh ringgit digital. Sektor swasta akan menyediakan akaun atau dompet digital di bawah pengantaraan bank untuk memudahkan pentadbiran sistem pembayaran ringgit digital. Orang tengah berpotensi yang sedia ada ini akan menyediakan perkhidmatan di pasaran bebas untuk ringgit digital.

TABLE OF CONTENTS

PAGE

Contents

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

LIST OF ABBREVIATIONS

FYP	**-**	**Final Year Project**
VS		**Visual Studio**
RM		**Ringgit Malaysia**
ECDSA		**Elliptic Curve Digital Signature Algorithm**
ECC		**Elliptical Curve Point**
RSA		**Rivest, Shamir, Adleman algorithm**
DRM		**Digital Ringgit Malaysia**
MOD		**Modulo**

LIST OF ATTACHMENTS

.

CHAPTER 1: INTRODUCTION

1.1 Project Background

A memo of understanding (MoU) on collaboration in the domain of CBDCs was reportedly signed by the five BRICS countries—Brazil, Russia, India, China, and South Africa—in July 2021. The BRICS countries agreed, per the MoU, to "explore the possibility of establishing an independent CBDC network" that would enable trade between the signatory countries. But neither a timeline nor an explanation of how such a network would function were given.

More recently, the head of the Russian central bank claimed that the BRICS countries were discussing the possibility of creating a unified platform for CBDCs in March 2022. According to the governor, the platform would permit cross-border transactions between BRICS member countries and would let BRICS countries to test their CBDCs in a collaborative setting.

It's crucial to remember that plans and advancements in the field of CBDCs are subject to frequent and rapid modification, therefore it's feasible that there have been new upgrades since my knowledge cutoff date.

From the latest news on CBDC of BRICS countries until September 2021, there had been discussions and announcements about the possibility of a BRICS Central Bank Digital Currency (CBDC), but no concrete plans or actions had been taken yet.

1.2 Problem statement

Table 1.2-1 Summary table of problem statements

PS	Problem Statement
1	Can CBDC be connected with current mechanism for confirming authenticity the currency of digital ringgit notes.
2	Time consuming in verifying the authenticity of digital ringgit.
3	The mechanism of verifying physical currency be applied to enhances user authentication and security in CBDC wallets.

1.3 Project research question

Table 1.3-1Summary table of problem of project research question

PS	PSQ	Project research Question
1	1	Which type of curve in ECDSA that is suitable to be apply in this project?
2	2	Which hash algorithm that is going to support in this project to produce the right length of hash message value?
3	3	What type of data presentation after successfully generate digital signature value?

1.4 Project Objective

Table 1.4-1 Summary of table project objective

PS	PSQ	PO	Project Objective
1	1	1	To study on digital signature algorithm ECDSA SECP256K1
2	2	2	To generate a digital signature that can be present as barcode
3	3	3	To verify a digital ringgit offline

1.5 Project Scope

The primary functions of the code are to generate an ECDSA-based digital signature, SECP256K1 system parameter, hash the message using SHA-256 because it is practical to generate a QR code that stores the public key and digital signature. The goal is to use cryptographic techniques to build a reliable and a fast anti-counterfeit method.

1.5.1 Modules

1.5.1.1 Hash library

For this project it will used Secure Hash Algorithm 256-bit (SHA-256). SHA is used to get the hash value to generate the message from random numbers.

1.5.1.2 ECDSA

This module, is using elliptic curve cryptography operations. Elliptic Curve Digital Signature Algorithm (ECDSA) will be used in order to generate the digital signature.

1.5.1.3 QR Code

For this module it will assign the value of the digital signature is in Hex. The output will represent in barcode format. The barcode type is 2-dimenesion which is the QR Code.

1.6 Project Contribution

Project contribution is the referring to the output of project. The table below is presenting the project contribution
Summary of Project Contribution

Table 1.6-1 Summary table of Project Contribution

PS	PSQ	PO	PC	Project Contribution
1	1	1	1	improve method of anti-counterfeiting among digital ringgit user's wallet
2	2	2	2	Strengthen the CBDC economy by preventing counterfeiting and protecting the value of the currency of digital ringgit.
3	3	3	3	Improve operational efficiency by utilizing QR codes on currency notes to represent digital signatures for easy verification.

1.7 Report Organization

This section will highlight an overview of each chapter in this project report.
Chapter 1: This chapter is about the beginning and introduction of this project. It will summarize the background of this development project, the problem and the objectives of the project.

Chapter 2: This chapter is about the project's literature review. It will describes the past research that is related to this project. This chapter presents a critical evaluation of the problem, its supporting data, and a potential solution based on related research.

Chapter 3: This chapter is about chosen methodology that will used in the implementation of this project. The methodology describes the steps that occur during each stage of the selected technology. The project milestones will also include a step-by-step description for each activity.

Chapter 4: In this chapter, it will examine the thorough analysis, strategic design, and precise implementation phases of the project in this crucial chapter. These stages are crucial to not just bringing the project's concept to life but also ensuring that it integrates seamlessly with the target user base and other systems.

Chapter 5: This chapter is about testing. Specifics on how to evaluate the outcomes of each segmentation strategy and decide which is best for segmenting land use are provided via testing and analysis.

Chapter 6: This chapter is about project conclusion. The conclusion includes the project summary, project contribution, project constraints, and expected future work.

1.8 Conclusion

As a conclusion this chapter shows the project's objectives and how will advance the field of security in the future have been explained and made apparent. The following chapter will concentrate on the literature review of the development Digital Ringgit.

.

.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This section will cover literature review. It will outline the critical review by past authors that had been joined in area electronic cash implementation. The project required fact gathering with some researches in order to gain a better view of idea to imply in the projects.

This chapter will analyze the data, draw conclusions, and provide a summary of the literature on related projects and system-related research. The main goal of a literature review is to compile and evaluate all pertinent references for a research paper. For this project, since it is using RM notes currency the closest object that can relate is electronic cash. Additionally, to assists this project to find the best way to produce digital signature on Digital ringgit Malaysia (DRM). This chapter gives information about the existing system's functionality and the project's domain. This chapter will also cover the methodology used to design the project, the software requirements, imported libraries and comparisons of the project's parameters and attributes.