សាកលវិទ្យាល័យជាតិគ្រប់គ្រង

NATIONAL UNIVERSITY OF MANAGEMENT

THESIS

NFT-BASED IDENTITY CAN IMPROVE IDENTITY FRAUD PROTECTION IN CAMBODIA BANKING INDUSTRY

BY

HONG PHANNARATH

Phnom Penh
2023

FACULTY OF
DIGITAL ECONOMY

MINISTRY OF EDUCATION, YOUTH, AND SPORT

NATIONAL UNIVERSITY OF MANAGEMENT

FACULTY OF DIGITAL ECONOMY

NFT-Based Identity Can Improve Identity Fraud Protection in Cambodia Banking Industry

By

Hong Phannarath

**Project Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Bachelor of Digital Economy
(English-Based Program)**

**SPECIALIZATION IN
FINANCIAL TECHNOLOGY**

**Phnom Penh, Cambodia
October 2023**

MINISTRY OF EDUCATION, YOUTH, AND SPORT

NATIONAL UNIVERSITY OF MANAGEMENT

FACULTY OF DIGITAL ECONOMY

NFT-Based Identity Can Improve Identity Fraud Protection in Cambodia Banking Industry

By

Hong Phannarath

Project Thesis Submitted in Partial Fulfillment of the Requirements for the Bachelor Degree of Digital Economy

Supervised by:

Dr. Samreth Sovannroeun

Associate Professor at the Graduate School of Humanities and Social Science, Saitama University, Japan

Phnom Penh, Cambodia
October 2023

COMMITTEE APPROVAL

The members of the committee approved the thesis of **Mr. Hong Phannarath** defended on October 20, 2023.

Dr. KLEUNG Sinet (Chairman)

Assoc. Professor SAMRETH Sovannroeun (Committee Member)

Asst. Professor CHAY Sengtha (Committee Member)

DECLARATION

I declare that this thesis is my own work and has not been submitted for a degree at any university. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Hong Phannarath

National University of Management
Phnom Penh, Cambodia
October 2023

ACKNOWLEDGMENT

Firstly, I want to express my appreciation to Professor Hor Peng, NUM Rector. He not only supported students in my faculty with scholarships that was the foundation of me pursuing my academic goals, but his passion and love for the field and dream of developing the whole Digital Economy program has been outstanding. He is the icon of what motivates our commitment towards pushing to our very best. His dedication is unmatched, his sacrifice and his adoring nature are what open up opportunities for us like this.

I am very thankful to Dr. Samreth Sovannroeun, my external supervisor, and Mr. Kleung Sinet, my internal supervisor for supporting me throughout my time completing this paper. They were there throughout this roller coaster which I appreciate so much. Their experience and kindness were the key factors of how I managed to finish this paper with this result.

I want to express my appreciation to Dr. Phim Runsinarith, and Dr. Chay Sengtha for providing my comments and displaying my flaws during the process of conducting this study. They helped me rearrange my scope and gave important perspectives to sharpen up my thesis.

All the people I have mentioned are the core importance in my path of making this study. The understanding of what I needed to do and the scope and key points I had to make were coming from their precious ideas and comments.

I need to express my gratitude to the Ministry of Education, Youth and Sport for their support and commitment to develop such important fields to further promote the education capability in Cambodia.

Last but not least, I have to express my appreciation to my fellow classmates. Their support was amazing and incredible. Their encouragement was something special that made me believe and confident to finally finish this research.

ABSTRACT

Information is very important in the banking system. The struggles of managing personal data and avoiding frauds regarding it being used without consents are major problems for this world. Cambodia is nowhere new to this issue. Identity frauds can cause severe loss in properties and trusts, and the integrity of the modern banking system. The purpose of this research is to illustrate how there is a flaw in the banking industry in Cambodia in terms of identification. This research will later note down the problems that caused the researcher to conduct this specific paper, then evolve into the encouragement to answer the research question and follow the research objective that the researcher has come up with to lay a field and pattern to prove the topic of this study. This study proposes a solution of NFT-Based Identity or NID that will challenge the challenges that the current banking system faces in order to improve and push the potential of evolving technology further onto another step. This research's literature reviews will include existing studies that are relevant to gather general knowledge to shape up the foundation of this paper such as the understanding of Blockchain Technology, and what it means to secure identities in it regarding the pros and cons that this technology has to offer. The study will be conducted through the qualitative methodology surrounding ten interviewees that are qualified and very important to this study by offering originality and ideas relating to the topic. The result of the whole process of interviews will be converted into major codes and codes in order to describe the significant points using a data analysis methodology. This study is highly influenced by the connection between the findings from literature reviews and the findings from interviews to create a pattern of answering the research questions. This paper later discusses the relation between the results of the findings, then conducts a framework to further describe the flow of how NFT-Based Identity can improve the identity fraud in Cambodia banking system.

TABLE OF CONTENT

LIST OF ABBREVIATION

AFIS: Automated Fingerprint Identification System.

ATM: Automated Teller Machine.

CRM: Cash Recycler Machine.

DNA: Deoxyribonucleic acid.

eKYC*:* Electronic Know Your Customer.

ePAYMENT: Electronic Payment.

FTC: Federal Trade Commission.

ID: Identity (Card, Token).

KYC: Know Your Customer.

NBC*:* National Bank of Cambodia.

NFT: Non-Fungible Token.

NID: NFT-based Identity.

OTP*:* One Time Password.

CHAPTER I: INTRODUCTION

1.1. BACKGROUND

Throughout the decades of the common banking system, the development of a society has been getting stronger and stronger, and so has social security. However, the further the opportunity to experience new upgrades, the greater the risk can occur in the field. Identity has been one of the most important assets that the people of this modern civilization must have in this new era of banking. Hence, more identity criminals are never stopping from finding windows to operate their actions up upon this social expansion. Modern banking's security is still somewhat a dangerous way of doing banking. According to Holland (2023), personal data that is needed throughout the KYC process opens an opportunity for identity attacks. Nowhere that this new age of banking and customer data gathering are one hundred percent safe.

Faking and falsely representing someone else to illegally obtain benefits are a standout issue. The world is facing this issue all at the same time because it is very common and an open opportunity for thieves to get their hands on something that is not theirs and cause problems for innocent citizens (Forbes, 2023). Solutions are being discovered and implemented everyday including the reinforcement of laws and punishment. But, Identity Fraud is still a major problem that is in the wish-list of fully gotten rid of.

In recent years, Non-Fungible Token has been on a rocket building up its reputation in the economic world. Non-Fungible Token came with a short nickname of NFT, a special type of cryptocurrency that presents itself in the form of artwork, numbers, pictures, and many other things that the market finds valuable. A safe and secured design that stores tokens in a so-called "Blockchain", a newly introduced system of decentralization, that is strongly against the idea of the middle man. Bao and Roubaud (2022) argued that in this world of decentralization, no one has the exact control over the community of the market, every peer, node, has the same amount of engagement that plays a role of approving that one thing exists or belongs to someone.

1.2. PROBLEM STATEMENT

In today's environment, identity thieves are using their collected identities of someone else in many ways to achieve their goals, commonly in banking. Within the modern economy, identity fraud often occurs during the nature of payment systems because transaction of credit card payment systems has been characterized by the usage of anonymous data, which means more and more consumers are open to offer instant debit and personal information to succeed their shopping intentions (Anderson, Durbin, & Salinger, 2008). The United States, arguably the most developed country in the world, is still the most affected nation by this type of fraud. Matter of fact, one-in-four U.S. consumers encountered this type of fraud in 2021 (EQUIFAX, 2023). Showing that this issue remains pervasive. Over the last 10 years, this absolute predator of the technology era has tripled in cases in the U.S. in 2021 and 2022, about 1.2 million cases of identity fraud involving loans and leases occurred. The number grew up to 5.7 million cases in 2023 (National Council on Identity Theft Protection, 2023).

To further make this problem more related to Cambodia, cases around the region of Southeast Asia as developing countries are facing similar problems and issues are to be included. Radio Free Asia in 2022 reported that the police in Vietnam have arrested a fraudster group that conducted over 17 million pieces of illegal personal data to access bank accounts stealing over $1.6 million by taking control of victims' mobile phones. In Malaysia, it was reported by the Malaysian Deputy that around 250,000 suspicious cases of transactions were reported to the country's central bank in 2022, which was a 30 percent increase from the 2021 (Comply Advantage, 2023). Those transitions include frauds. Another case that was reported by the Coconuts Kuala Lumpur in 2023 involved the fraud in OTP used by a fraudster to steal 1 million ringgits. That OTP was used to access the man's account in order to operate the illegal act.

In Cambodia, identity fraud has not been seen as a major concern and no official report on identity fraud has been published yet. However, there are several cases that display the dangerous harm that identity can do such as in 2022 three foreign nationals were sentenced by the municipal court to several years in prison and ordered to pay about $30,000 each to the victim and $25,000 as compensation to the Canadia Bank.

Khmer Times (2022) showed that another similar case happened in 2022, where a Head Inspection Division at Hattha Bank was arrested and accused of stealing 6 customers' money by modifying their information to get access to their bank accounts where approximately $600,000 was lost. Another case reported by the Phnom Penh Post (2022) says that a woman took advantage of online banking technology as she successfully stole bank customer's OTP and stole their money by the access she got from this action. It was said that she was shortly arrested after she fraudulently took control over their bank account without their consent and recognition. And these cases keep on occurring in Cambodia which another one happened in June of 2022 where 2 men and a woman were arrested for faking public documents and faking identities to operate their money fraud obtaining about $35,000 from a bank. These 3 suspects forged identity cards pretending to be a landowner and an account owner and went to withdraw $35,000 on two separate occasions via Khmer Times (2022). Whereas in June, the three suspects activated their fake IDs and public documents to apply for a $90,000 loan from a Private Bank, but was fortunately denied.

Even though there has not been official data or statistics of this type of crime in Cambodia yet, it is indeed a great danger. Kongkea (2022) reported that such cases like this pushed the government and all involved ministries to take actions. As in March of 2023, NBC has appealed to the Cambodians to be more careful and pay close attention to potential identity frauds and thieves. Mobile applications such as Telegram, Messengers, WhatsApp and so on, are becoming a performing stage for thieves to take advantage of the public by faking identity, voices, and even pretending to be various institutions (Phnom Penh Post, 2023). The National Bank of Cambodia expressed concerns regarding this growing issue.

Considering the threats and problems that identity fraud can and has impacted, a new technology needs to be used in order to solve this issue. The researcher of this study would want to propose a solution involving the use of a newly invented platform called “NID” or “NTF-based Identity”. A platform that individuals can store their identity and personal information in the Blockchain technology ensuring safety and fraud-proof.

1.3. RESEARCH QUESTION

The study aims to answer the following research questions.

“What are the potential flaws of the current banking system in Cambodia in data management?”

“How can NFT-Based Identity improve the identity fraud protection in Cambodia banking system?”

1.4. RESEARCH OBJECTIVE

The objective of the study is to illustrate how NFT-Based Identity can improve the identity fraud protection in Cambodia banking system.

1.5. SIGNIFICANCE OF RESEARCH

This research wishes to offer an opinion in the banking industry as to influence the decisions and the proposal of using the Blockchain technology guarding customers' personal information from frauds. This study indicates a great view of how storing information in a safe environment like Blockchain technology can be a solution to prevent all sorts of identity fraud in the banking system, as it is a great reminder to the people, as well as banks, to take notice of this fast growing and developing technology era. In addition, implementing technology to get rid of frauds is a part of the UN' Sustainable Development Goal 11 where it displays a goal to make human resettlement inclusive, safe, resilient, and sustainable.

CHAPTER II: LITERATURE REVIEW

2.1. DIGITAL WORLD AND OPPORTUNITY FOR FRAUDS

Due to a study from facial recognition, expert forensic facial examiners and untrained super-recognizers provide better accuracy on face identification duties than the human members of the public (Phillips, 2018). Unfamiliar face-matching can be improved with the use of feature-by-feature comparison due to a learning, meaning that by using this methodology, the face-matching of unfamiliar faces can be significantly improved and reach its potential of flawless. Towler, White, and Kemp (2017) further claim that the rapid evolution of technology still keeps on increasing the ease creating sophisticated and compelling fakes. While these new technology advances encourage the excitement of the people and the society and become some of the best achievements in recent decades, there will always be fraudsters and individuals who are using these developments to deal damages. Therefore, it is essential to work and study to keep these threats aways (Nightingale, 2022). The power and complexity of frauds are escalating in this modern era, meaning that our understanding on these issues are growing bigger. Stephen Topliss, an expert and vice president of fraud and identity strategy company, describes that it is now the most crucial time than ever to learn and study to categorize frauds into type for the future ease (Devanesan, 2023).

This problem of digital fraud in terms of identity has continued to level up, cybercriminals are also a big threat connected to this issue, posing a huge challenge for many organizations, as they are ending up in an unprepared environment to solve and face this unfamiliar series of attacks. Mobile apps have been preferred as the channel for digital transactions. A report by LexisNexis Risk Solution Cybercrime Report analyzed about 80 billion digital payment transactions and found that more than three-quarters of them coming from mobile channels. This number shows exactly how extreme the issue is and its potential of occurring to the innocent people using their application making simple transactions and being frauded without them knowing.

2.2. EXISTING SOLUTIONS TO IDENTITY FRAUD

In the age of identity issues, more and more worries have always been pushed to the surface of concerns. Hence, throughout the years, there are solutions coming up to solve this problem including the creation of regularly updated IDs, law enforcements, and to shift the focus onto the process of identity verification where it relies on three means including knowledge-based, biometrics, and tokens to create a biometric system that read and detect facial features. Willox and Regan (2002) stated that signing up for identity fraud prevention service from private sectors is another solution. People sign up for services like this to prevent their information being used elsewhere without their consent while, still, identity prevention services are still not prone and enough to fully get rid of thieves. Alongside this there will be such solutions like changing the password of their accounts regularly, or using the two-factor authentication (Kinney, 2023).

In summary, people have been using to deal with identity fraud are subscriptions to identity fraud prevention service, law enforcement, biometric-focused process of verification, the creation of physical identity cards, and digital identity that describes our online lives in regard to online payment and purchases. LexisNexis (2023) describes further, other aspects of solving this issue can be seen as well such as fraud analysis and studies, and adding functions including freezing bank accounts or credit cards. However, these solutions are not enough to make a big impact in preventing identity fraud and theft. As people's personal information is still out there and is easily known by everyone, including cybercriminals, no one is completely safe because as far as your data is obtained, it is highly possible that it will be used illegally without you knowing. Security of personal information in today's world needs serious step-up and higher technology. All the data is still being kept and controlled by a higher authority that is open for cybercriminals to attack and get access to your information as the cases keep happening.

2.3. PROCESS FLOW OF TRANSACTION AND IDENTITY VERIFICATION MADE IN BANKS

According to EMB (2018), one of the biggest credit card companies in the world, the process of conducting a transaction can be listed down into steps for better understanding. Thus, in terms of transactions made between a customer and a third party such as a merchant, the first thing that happens right after the credit card being swiped or other payment mechanism being operated, the merchant's acquiring bank will request for an authorization from the customer's bank account to validate on available funds. The authorization will then pass back to the merchant point-of-sale after the verification on fund availability. Information including approval code and references for the transaction will be delivered to the merchant data. The credit card issuing bank will then send the fund to the end bank as a payment for the things bought by the customer. And the fund will later be deposited into the merchant's account including a possible charge of fee for the transaction. Customer's will be immediately debited the money cost of the purchase after it's being kept in a general ledger that awaited until the whole process is done. In relation to this case, other transaction and banking activities are conducted in a similar process that involves all of the parties and verification of funds.

However, the biggest question of this process is how do banks verify identities to approval. According to Chen from Investopedia (2023), in order for banks to verify one's identity for both the registration and completion of a transaction, KYC or eKYC has to be operated. A form of papers both physically and digitally will be needed for customers to fill out their important personal information. Information will be kept for the purpose of being used in the future. As reported by Emmanuel from YouVerify (2022) shows that before approving big transactions such as loans or huge cash withdrawal from the counter, banks verify those kept documents by conducting details along with a government-backed database to verify identities. To illustrate this even more, banks verify documents through steps. The first one is where they extract data from the identities from the customers using the customer due diligence procedure. Then, they run the key important information like ID numbers, facial features to compare with the established database. Finally, they will come to an end result whether there is a match that proves a customer is who they said to be.

It's no different from verifying identities in iBanking. Emmanuel continues, in iBanking, before requesting for transactions or other processes, the identity verification will be done in the same pattern but digitally. However, in some banks, customers will still have to be at the counter or the nearest bank branch to process big transactions.

2.4. IDENTITY STORED IN BLOCKCHAIN TECHNOLOGY

In this advanced society, the development of technology is getting stronger and stronger which makes financial institutions and businesses spark the courage to invest in digitalization to cope up with the world. Security has been the main goal and core of these investments. Thus, digitalization is mostly focused on the security aspect. Blockchain technology began its domination onto this play. When banking industries are transforming their services online and digital, e-KYC are getting common in this field of technology. Blockchain offers great features including the ability to be decentralized, staying away from any middle authorities, transparency, immutability, and anonymity (SANCTION SCANNER, 2023). Reusable digital identity is one of its names. Meaning that it can be verified and used both offline and online whenever they want to authenticate who they are. The data and personal information that is stored can be in a range of identity information, driver license, and even citizenship information. Governments from around the world have been pushing this investment and have a strong confidence about this solution. For example, India now has over 1.3 billion digital IDs for its citizens (99% of all adults) (Williams, 2023). Reusable digital identity has been launched and is seen as one of the future goals where it is predicted that this market will be seven times bigger in the next five years from a current of $32 billion to about $270 billion.

By what was mentioned above, Blockchain is a good source for keeping data in a secured place where it is under no control from any entity. On top of preventing fraud, even sharing personal data will have to be very consensual from the original owner. Every request for a data or personal information usage approval will be needed from the owner. The owner can share their information optionally In the Blockchain system, data owners will have complete data ownership without anyone faking it and using it in unwanted ways. All data will not only be seen on the device interface, but is stored securely in Blockchain decentralized storage that will require bad actors to do the impossible to hack or use the data without the recognition or consent from the owner. By storing personal data in Blockchain, digital decentralized identifiers enable the owner to cryptographically validate their proof of ownership over it and other connected data (DOCK, 2023). When personal data is being added into blockchain, every transaction or action made regarding the information, validity will be needed among all of the parties involved. Every computer, every node in the chain will be required to check for validity of the action and if the majority of the computers think it's valid, then the action may proceed.

2.5. PROS AND CONS OF APPLYING BLOCKCHAIN TECHNOLOGY INTO IDENTIFICATION

Digital identity will help service providers with a great way of verifying data and validating the information. Big countries are looking to digitize their citizens' information to make it easier to process day-to-day business, improving efficiency. Thus, there are various benefits that can be seen by using this method including the reduction of risk of identity fraud and thieves because storing identity and personal information in a form of NFT will automatically be checked from validation of the information and proof of ownership. Any possible unusual activity or a strange pattern that is not recognized by the owner of the information will be detected and flagged immediately which makes this almost fraud and theft proof. Uche (2023) added that in addition to being fraud-proof, storing identity information in Blockchain can have other benefits including convenience where you don't have to remember all of the names and numbers and you can also create profiles with a single set of credentials, regarding the authentication processes. It also offers other benefits as well including the safe and security aspect that it is hack-proof under full control of the owner.

However, whenever there is a good side, there is always another side that goes against the pros. In this case of digital identity, it is quite obvious that it still has a lot of flaws that can ruin the experience and the main focus for its creation. According to FM Contributors (2023), one of the most noticeable flaws that basing digital identity in Blockchain has is the single point failure. They added, "Because all of an individual's identity data is stored in one place, a data breach or cyber-attack could compromise an individual's entire identity. In this scenario, hackers could access sensitive information, such as financial data, medical records, and personal information, which could be used for identity theft or other nefarious purposes." Furthermore, in Blockchain, there is another challenge involving the consent of managing data where it is different from traditional identity verification methodology, the owner can consensually choose which part of the information to share with the third parties. "However, with Blockchain-based digital identity, this becomes more challenging, as all data is stored in one place, and revocation of access becomes more complicated.

Another consequence of digital identity is that it's actually easy to replicate, as the technology is continuing to grow more advanced, an artificial intelligence called Fakedeep has been on a rise of recreating people’s pictures and reaction that has become a big flaw and window for fraudsters to take advantage of, said Mitek (2022). Other than that, in digital identity, delegation is still an option where you still have to know whom to trust to share your data with. Digital identity is still hard to achieve and is a very big scope where the need of consumer and budget is even bigger to ignite up the adoption.

CHAPTER III: NID (NFT-Based Identity)

As raised in the problem statement section, a solution was proposed to solving identity fraud, NID. To further the understanding of this part, the researcher is proud to introduce the potential solution to improving identity fraud protection for banks.

3.1. OVERVIEW OF NID

NID or NFT-Based Identity is a platform where customers can restore their identity and personal information in a Web3 technology. All personal information and data including ID cards, phone numbers, bank numbers, passport numbers and so on. NID will enable users to store that information in a newly invented technology of Blockchain where everything is safe and untouched. NID distributes all your stored information in a form of NFT where nothing can be duplicated or copied and only you, the owner, can access and fully have control over it. Digitalizing all of it and securing it in Blockchain, that is a secure and decentralized environment to make it impossible to hack, steal or tamper.

3.2. NID FEATURES

NID wishes to serve their users with the most secure and comfortable environment possible. Assisting you to a very modern society where you are being represented as a token. It is a new way to manage your identity to make it easier to keep track of your IDs and other personal information to prove who you are and being put in a more secure way than the traditional methods of identity management. Storing all of the confidential information in one safe place and deploying it as a personal Avarta is one of the greatest features NID can offer. An Avarta will define proof of ownership of the data and will make it even easier for people and third parties to remember who you are. All of this is pretty much all about security that NID thrives to push forward. NID's digital nature, which is being lifted behind Blockchain technology, ensures that all of your important information will be protected from unauthorized access that can cause all sorts of danger. This will give users the relief about security breaches and enable them to enjoy and embrace the digital age.

3.3. NID'S TECHNOLOGY

NID foundation is built with Polygon technology of Polygon. Polygon is a growing system of Blockchain which was created to respond to the flaws of Etheruem's scalability providing a faster speed and lower cost. DeNicola (2023) describes Polygon as acting as the Layer 2 protocol for Ethereum, Polygon hopes to improve the cost and speed just like a smaller car that runs parallel to the main one but moving faster and takes fewer steps.

CHAPTER IV: METHODOLOGY

4.1. APPROACHES

A qualitative methodology will be used in this research through the lights of collecting Primary Data and Secondary Data. Where the approach of this research will target and collect opinions from individuals that have experience and a fair knowledge in the banking industry. Using the Semi-Structured methodology, this range of data will be collected through interviews with questions that are important to expand the understanding, perspectives and potential ideas on identity fraud. Interviews were conducted with the researcher always ready to note important key points down and transcript to transform in the themes and codes further in this research.

4.2. DATA COLLECTION

4.2.1. INTERVIEW PROCESS

The interviews were conducted in a time span of two weeks where the researcher asked and came to agreements with interviewees for the best times for the interview. The interviews are separated into three separate times by using the Phenomenological method to study potential experience and events regarding the issue as a part of this research. Interviews regarding this study were conducted through both face-to-face interviews and online via google meetings and telegram calls. Ten people were selected due to their very valid experience and understanding of banking and the process of requesting for transactions and other banking activities according to the selection from ten of the top banks in Cambodia (Open Development Cambodia, 2022).

The interviewees were asked 4 questions that are important and considered by the researcher that were believed to lead a pattern to answer research questions and create ideas to conduct research objectives for this research. The questions were:

Table 1: Interview Questions

Q. 1	Can you tell me about your background and experience in the banking industry?
Q. 2	Will you please guide me through a process of requesting transactions or loans or other activities involving the identity verification due to your knowledge?

Q. 3	What is your opinion on the current data management system in banks in Cambodia?
Q. 4	In your opinion, do you think current banks' data management system is perfect in terms of security, and what is the possible flaw?
Q. 5	What is the key potential of solving today's data management issue in banks, in your opinion?
Q. 6	Please provide me with your idea of what could be implemented to improve and make identification more efficient.

4.3. DATA ANALYSIS

Content analysis will be approached to imply on interviews conducted in this study to identify and analyze key concepts and key points expanding the view on identity fraud and banking system. The researcher will pursue gathering keywords and patterns that will turn out from the interviews that will help readers to understand and process the answers quite easily.

CHAPTER V: DISCUSSION

5.1. FINDINGS

The issue of identity fraud in this digital era is still a major concern for banks. To answer the research question, the researcher conducted, the uniqueness of this study was delivered through the interviews. As mentioned in the Introduction Chapter, the main purpose of this study is to learn how Digital Identity can improve the protection that current banks are having. Thus, in this Chapter, the researcher has included the profiles of respondents that will help improve the understanding of whom were asked and qualified for this research and the value of their offered information. After the profiles, the research followed the research methodology and formed up a table of themes and sub themes with a clear description of transcript, and later explained each theme in depth to expand the connection this finding has to the Literature Review Chapter.

5.1.1. PROFILES OF RESPONDENTS

After going through the process of asking questions, the researcher has come up with an understanding of profiles of the respondents and where do they come from. Ten bank staff were asked the first question and the result shows that all ten of them have had a career in this industry for at least 1 year, and an average of 3.4 years of working regarding security and data management per person. All ten of the respondents come from various departments they are working for including Customer Service Excellence, Branch Quality Assurance, Quality Assurance, Strategy, and Card Issuer from the mentioned top banks in Cambodia. All of them are from and working in the capital city of Cambodia, Phnom Penh. Therefore, the researcher can define the right audiences that can offer value information. By getting to know the profiles of the people we asked questions to, we get to understand the socioeconomic status of them that can provide valuable context of interpreting their answers, their behaviors and attitudes.

Table 2: Interviewee Profiles

No.	Interviewee's occupation	Position	Experience	Location
1.	Customer Service Excellence	Line Manager	+10 years in banking industry	Phnom Penh
2.	Quality Assurance	Senior Officer	+5 years in banking industry	Phnom Penh
3.	Quality Assurance	Senior Officer	+5 years in banking industry	Phnom Penh
4.	Branch Quality Assurance	Officer	+3 years in banking industry	Phnom Penh
5.	Branch Quality Assurance	Officer	+2 years in banking industry	Phnom Penh
6.	Strategy	Officer	+2 years in banking industry	Phnom Penh
7.	Strategy	Officer	+2 years in banking industry	Phnom Penh
8.	Customer Service Excellence	Assistant	3 years in banking industry	Phnom Penh
9.	Customer Service Excellence	Assistant	1 years in banking industry	Phnom Penh
10.	Card Issuer	Assistant	1 year in banking industry	Phnom Penh

5.1.2. THEMES

Transcripts from interviews are very important as to what essential concepts were noted down during the action. The researcher has provided a table involving Themes, Sub Themes, and Transcripts. The table concludes the final information that was suggested and displayed by the interviewees.

Table 3: Finding Themes

Themes	Sub Themes	Transcript
Customer Data Gathering	KYC	Gathering essential information from customers when registering to be included in CIF.
	eKYC	
Storing User's Personal Data	CIF (Customer Information File)	A unique electronic file containing digits that identifies each customer and its account type registered for the bank account.

Data Management Flaw	Core Banking System	All the data is kept and registered in the bank's core banking system, and is a place where all the banking activities occur.
Biometric Identification	Uniqueness in Natural Features	Collecting biometric information from individuals to identify the difference between each person to avoid serious identity fraud and false identity. Those features include fingerprints, facial features, perhaps DNA or genes.

Throughout the interviews, the researcher has transcripted the answers into 4 different key codes. Those happen to be what the interviewees' perspectives and experience that expressed to the questions being asked. Those codes contain a range from registering new customers to the understanding of where to store those data that is collected from the customers.

CUSTOMER DATA GATHERING

According to interviews with years of experience in the banking industry, both traditional and modern banking systems still have to gather information from customers through KYC in order to register them for a new user in the bank. However, as the technology evolves, smart phones have been on a rocket in usage worldwide, thus, there is a so-called "eKYC", where a lot of banks allow people to register to be a new user by themselves through bank's applications. Although it is being conducted differently from each other, the required information is still the same involving name, ID number, date of birth, phone number, a front-camera selfie including their face and their ID, and address. These are the data that common banks require in order to activate their new customers and register them in the banking system. The only difference that these two have is that when registering through eKYC, it requires the light on internet access and an application of the bank they want to sign up with. Whereas, signing up through KYC will need the customers to go physically to the counter of the bank's branch near by them, and fill out the paper physically as well, where there will also be an assist from customer service staff at the branch. Both are equally effective.

However, the more advanced the system and capability of the technology, the more consequences the bank has to deal with. The interviewee once quoted,

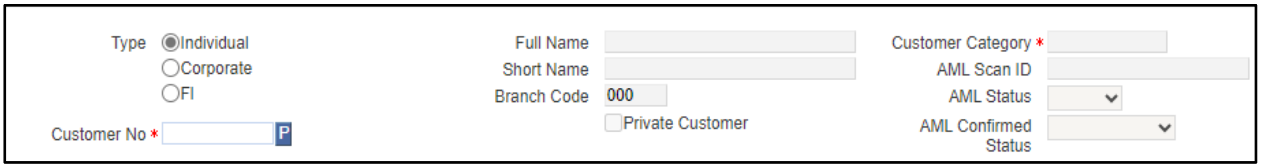
> *“ …since the implementation of eKYC, more error and conflict cases seem to occur more, and more work added to the Quality Assurance and the Teller team such as dead accounts, inactive accounts, and also people creating accounts using someone else’s phone number or ID card.”*

This shows the eKYC technology of enabling customers to register their account online does not always bring good things to the industry, creating new problems to deal with and exploit the flaws of information confidentiality of the customers.

STORING CUSTOMER’S PERSONAL DATA

When all the data required by the bank is complete and collected, customers will be successfully registered in the system in the form of CIF (Customer Information File). However, some banks consider calling it differently such as Account Number, Account ID, Bank ID, and so on. It still means the same. CIF is a file of digits sometimes can be 5, 6 or 7 digitals. Those digits are different from one another where one defines only one individual or one cooperation or one financial institution that was demanded at the beginning of the process.

Figure 1: Data Gathering for CIF



Type ● Individual ○ Corporate ○ FI

Customer No *

Full Name

Short Name

Branch Code 000

□ Private Customer

Customer Category *

AML Scan ID

AML Status

AML Confirmed Status

One CIF can effectively create plenty of accounts, although those accounts still belong to one person or entity. CIF can be used to identify a person or a cooperation when needed or when it is related to conflicts happening between an account. Picture and signature were also collected throughout the process where they are kept differently from any other general information of the customer, said one interviewee.

DATA MANAGEMENT FLAW

Each bank has its own banking environment. Core Banking System is a place where all of the data stored and all the activities being done regarding the bank. Most banks nowadays are being run by Oracle's Flexcube banking system. All of the banking activities are being conducted there including creating new customers, creating new customer accounts, depositing, withdrawal, and even transactions such as loans.

Hence, after receiving requests from customers about what they want to do about their bank accounts like the activities the researcher has mentioned above, identity verification needs to be done. Some activities and transactions take very little verification. For example, withdrawals through ATM and CRM, customers only need their smartphones with them or their credit or visa card in order to request for the withdrawal. In these types of processes, the banking system automatically performs without the interaction from the country except the record-keeping. The interviewee then added about decentralization,

> *" …the core banking system of current modern banks in Cambodia is nowhere near decentralization. Information and control are all under the banking's Core Banking team and counter."*

According to the interviewee, it supports the idea of this research where the researcher thrives to propose decentralization to revolute the data collection perspective of today's bank. Digitalized identity that is stored in the Blockchain technology is quite an opposite to what the data storing methodology we have nowadays, where again, it is more secure, centralized, and independent. However, it is important to notice that some banks allow their tellers to have the ability to store the information and access to the Core Banking System, while some banks do not and only their Data Department or Information Department do all that work after the information is all gathered.

Keeping all data and personal information in a centralized environment and with all human involvement in identity verification, it is in contrast from what a secure data management should be. Keeping such important and dangerous data in an environment as traditional as the Core Bank System can still lead to unwanted accessibilities and intersection by intruders. Whereas, information like this should be kept in a whole different place and more secure and in a surplus of technology.

BIOMETRIC IDENTIFICATION

To counter the issue of people with exact the same physical features that can cause severe frauds and problems to the banking identification, biometrics features including signatures, fingerprints, and official front-face picture are registered during the processing of creating an ID card, according to Dermalog (n/a). The "National Biometric Registration System" guarantees the identification of identities though DERMALOG AFIS. This push of the biometric identification system was also made in the Cambodia National Election according to Lee from BiometricUpdate.com (2015), where the National Election Committee pursued to sign up people from all across 24 provinces the 2018 National Election to ensure fraud proof and complete the first step of digital identity in Cambodia.

During the interviews, two of the interviewees emphasize the term biometric identity. Biometric identity includes the most important feature, fingerprints. One interview continues,

> *" …the final straw of why the number of identity fraud is as small as it is now, is because of the biometric barrier. Nearly 99% of human beings have unique fingerprints from one another, where when the case is serious enough to review all of the biometric information from the sources such as ID card and passport, fraudsters usually fail."*

Matter of fact, this is true, the biometric feature of fingerprint is the real barrier because due to studies all around the world, every fingerprint is unique. According to Ms. Biggers (2023), from healthline.com, a study done by the National Forensic Science Technology Center said that "no two people have ever been found to have the same fingerprints- including identical twins." There are more studies backing up this claim. For example, the one study from museum of science+industry Chicago, claims that "your fingerprints are unique. No two are the same, not even on the same person or on identical twins."

The emphasis from interviewees is really important in terms of what it means for this research. Biometric is a very underrated methodology that can be efficiently the solution to stopping identity fraud. However, the data that keeps this information is still in a not so safe hand, owners of fingerprints and other biometric data do not have access to them where it is quite a concern to where can we know and understand that our such important information is safe. Even though all of that data is kept in a different environment from banking, national databases, identity information that is kept with the government, all the fingerprint access and other features.

5.2. DISCUSSION

It is obvious that after all the studies have been done so far, identity fraud is an impacting issue for banking, and even the world in general. Having such a big issue in our hand, the research mentioned above at the Introduction Chapter about the overall purpose of this study. By trying to answer the research question of "How NFT-Based Identity Can Improve the Identity Fraud Protection in Cambodia Banking System" and following the research objective of "To illustrate how NFT-Based Identity can improve the identity fraud protection in Cambodia banking system", the research conducted a lot of Literature Reviews and Findings.

Hence, it is important to arrange all the findings and data and compare between the two to see the connection and what can we learn overall from those Chapters.

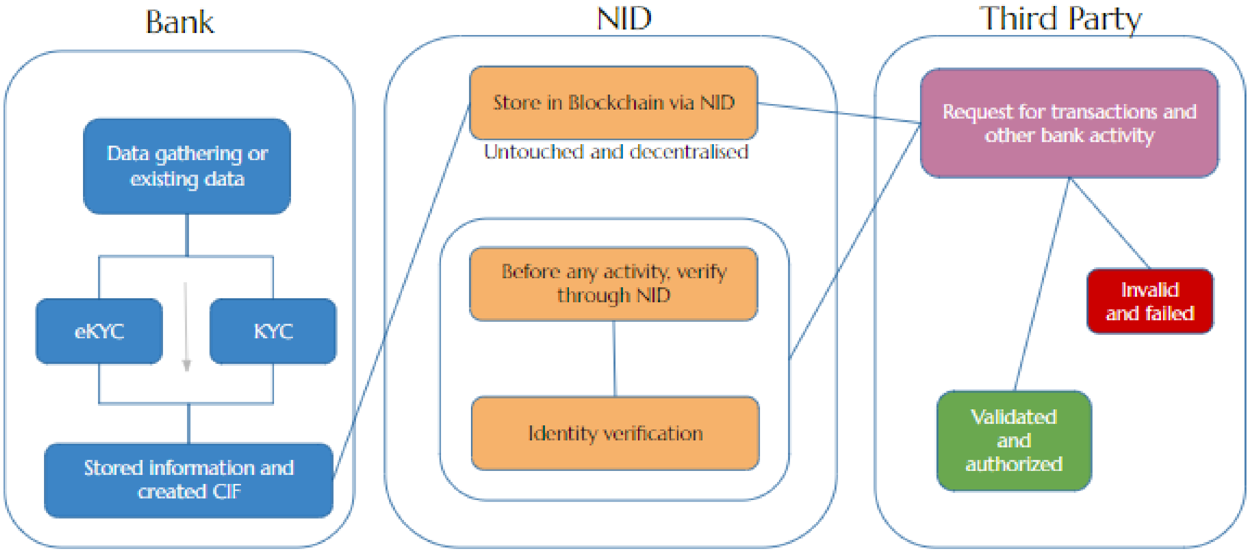
Due to the studies and research conducted in this paper, it recommends a strong point that digital identity has been a growing technology in recent years which is the problem that understandably leads to the cause of identity fraud. However, it is no joke to the authority or third parties or banks. They have been implementing and coming up with solutions throughout the years. According to the literature findings, traditional and modern solutions have been implemented to help protect customers' personal data, but those solutions are still displaying flaws. Flaws in terms of data settling. After all the solutions and modern ideas of how information should be transformed into, in this case, digital identity, it is still somewhat centralized that all the personal information of customers is still in the hand of a middle ledger that has control and power over those important assets. As stated above, these findings are great windows for this paper's research question to jump right in.

On the other hand, Blockchain has become one of the most common first thoughts and technologies that come to solve this identity information settling issue. Due to the proposal of using digital identity involving the technology of Blockchain, it is a great knowledge that Blockchain is indeed to where all the information should settle. But, there are some contrasts to this idea. Blockchain technology does not always provide advantages and benefits to answer the research question, but it also obtains unwanted cons. However, those consequences are nowhere from overtaking the positive impacts that Blockchain has in helping improve the protection of identity fraud. In summary, Blockchain technology shines a light to the research purpose of this study where keeping all the digital identities in a form of NFT stored securely in a chain.

In addition to this research, the findings according to interviews and codes transcribed from the answers given by the interviewees, it is important to learn every angle from the terms data in banking. The findings perfectly align with our literature findings creating a series of databases. Customer data gathering and storing before registering for a new individual must go through a process of KYC or eKYC, depending on the situation, both have the same effect. After collecting all the required data, according to the findings, a CIF will be formed which represents a person and their personal information. The findings suggest that a CIF is somewhat quite similar to NFT-Based Identity, where it serves a purpose of storing all the personal data. A CIF displays as digit numbers, where NFT-Based Identity can display both digits and Avatar. However, the contrasting facts about these two is that the environment they will be stored in. CIF is stored in a common banking environment and its flaw is that it's very centralized and having a ledger to be able to have access to controls on it. Whereas, NFT-Based Identity produces an Avatar that will be all stored in a very known secured Blockchain technology.

However, biometric identities such as fingerprints are the core proof of why storing digital identity in Blockchain matters. Given the significance that it has which leads to the ability to identify the difference between individuals, biometric identity is quite what makes NFT-Based Identity work. Through every identity fraud attempt, no way that can get past biometric information because it identifies the validation of the account and person. CIF which obtains information such as ID cards, that also leads to access of biometric information through that is stored in the government identity storage will give this research a good understanding as to what and how NFT-Based Identity improves this point because of the centralizing nature of the current data settlement. Framework below will give us a further understanding on this discussion:

Figure 2: Framework/Solution


Bank
NID
Third Party
Data gathering or existing data
eKYC
KYC
Stored information and created CIF
Store in Blockchain via NID
Untouched and decentralised
Before any activity, verify through NID
Identity verification
Request for transactions and other bank activity
Invalid and failed
Validated and authorized

The framework indicated how NFT-Based Identity would work in the real world while involving key sections including Bank, NID, and Third Party. To illustrate what is learned from all the findings in this research, the researcher has made a process of a case starting from the very beginning of creating a bank account.

Bank: In the beginning of the process of registering a new customer, the bank will do a series of data gathering via eKYC or KYC in order to include all the information needed to qualify the customer. CIF will be created for the customer that will represent that customer, that particular person.

NID: To include NFT-Based Identity into this play, the bank will need to cooperate and transfer or sign up the information of the CIF to NID in order to transform the CIF into a form of NFT. Then, all of the information gathered through eKYC or KYC by the bank will be kept in the NID system, or Blockchain to completely secure and make all of that data untouchable and give the customer full ownership. In NID, the duty is to verify and validate the transaction or banking activity requests to match the identification.

Third Party: Third Party in this case includes banks, financial institutions or any retail or business that enable ePayment. Before one of those third parties approve or execute an activity or transaction, a request will be sent to **NID** in order to verify the identity to further proceed the action. **NID** then sends out the result of the verification for the third party to decide whether to approve or disapprove the validation. However, **NID** can be used in a physical way where customers can install their **NID** information in their smartphone and display it to the third party once the identity verification is needed. This way it is faster to receive and validate the request sent from the third party.

In addition to the framework, biometric information can come to play in a very serious situation. For example, when a loan is requested and needs serious identity verification, fingerprints can be the key. This case is considered rare, for an illustration, when a twin sibling of someone with 100% physical features alike requesting for a loan or requesting for a rather huge withdrawal of their other twin's bank account, fingerprint can be the only key to separate these two from each other to cut down the fraud process. The biometric information is, again, kept in Blockchain technology.

5.3. RESEARCH LIMITATION

Although a proper study was wished to be conducted in this research, there is still a lot of potential that the researcher could explore. The lack of existing case studies and incidents related to identity fraud in Cambodia and the use of Blockchain in digital identity, created a hole in this research. As the researcher would consider case studies that support the idea of implementing such technology like Blockchain could be the core data to make this research a complete study. However, another hole that this research obtains is the non-relating nature to the quantitative methodology. Quantitative approach seemed to be irrelevant to this research, as it later affected the finding to which the actual data and numbers were missing causing quite an unfair circumstance in the study.

CHAPTER VI: CONCLUSION

Identity fraud has been a greater problem than what it seems to be. The advancement in technology that provides better living ease to the people, problems and consequences come with it. In this study, it was aimed at the particular problem of Identity Fraud in this technologized society in the banking industry. However, this paper proposed the solution of using the newly invented Blockchain Technology that offers a new idea and ideal environment to store all the information and personal data to avoid any sorts of those data being stolen or used without our consent.

Identity fraud is an issue that has been causing millions of dollars around the world. Hence, in this study, to even understand how it works and how can be protect it, the researcher gathered findings from experts and people with enough experience to quality to answer the depth of data gathering, how it is stored, baking environment, and the importance of biometric identity that later play such an important role in this paper. The results were significant because it helped indicate and illustrate how Blockchain can come and improve the system and route of storing data. The flaw in the current banking system is that it is kept in the centralized and common core banking system, so the proposal of storing them in Blockchain technology via NID suggested by the findings to be the ideal solution.

The framework was conducted to even illustrate it, proving a solid picture of the complete process of this study and the proposed solution.

Recommendation for future study: by the provided findings and result in this study, it should be important to take notice of the originality of it. The process of gathering and storing customer data and personal information is very crucial and begs for improvement. The information in the findings can be used to study how we should enhance it. The researcher recommends research questions for future studies taken from the originalities included in this paper as following:

“How can we improve the data gathering stage to a more secure and independent way?”

“How can we use biometric information more often in the banking industry?”

REFERENCES

Anderson, K. Durbin, E. & Salinger, M. A. (2008). Identity Theft. *The Journal of Economic Perspectives, 22*(2), 171–192. Retrieved from: http://www.jstor.org/stable/27648247

Biggers, A. (May 30,2023). Why Twins Don't Have Identical Fingerprints. Healthline.com. Retrieved from:

https://www.healthline.com/health/do-identical-twins-have-the-same-fingerprints

Bao, H., & Roubaud, D. (2022). Non-Fungible Token: A System Review and Research Agenda. *MDPI. 15(5), 215.* Retrieved from: *https://www.mdpi.com/1911-8074/15/5/215*

Coconuts Kuala Lumpur. (February 28, 2023). Malaysian man lost 1.4 million ringgit in 14-second scam call. *Coconuts.* Retrieved from:

https://malaysia.news.yahoo.com/malaysian-man-loses-1-million-033750378.html

Compy Advantage. (August 4, 2023). Malaysian Central Bank Records a Surge in Suspicious Transaction Reports and Scams. Retrieved from:

https://complyadvantage.com/insights/malaysian-central-bank-records-a-surge-in-suspicious-transaction-reports-and-scams/

DeNicola, L. (April 20, 2023). What is Polygon? How does it work? *Forbes Advisor.* Retrieved from: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-polygon/

DERMALOG, (N/A). Cambodia National ID Cards and ePassport. Retrieved from: https://www.dermalog.com/success-stories/cambodia

Devanesan, J, D. (July 20, 2023). Digital Identity is Key to Understanding (and Overcoming) Fraud Attacks. *FintechNews.sg.* Retrieved from:

https://fintechnews.sg/75320/sponsoredpost/digital-identity-is-key-to-understanding-and-overcoming-fraud-attacks/

Dock. (August 24, 2023). Blockchain Identity Management: Complete Guide 2023. Retrieved from: https://www.dock.io/post/blockchain-identity-management#:~:text=Blockchain%2Dbased%20identity%20verification%20provides,prevents%20identity%20fraud%20and%20theftg-thief-busted/

EMB. (November 12, 2018). Transaction Flow Explained: Step-by-step Process. Retrieved from: https://emerchantbroker.com/blog/transaction-flow-explained/#:~:text=Transaction%20flow%20is%20the%20process,processing%20networks%2C%20and%20card%20issuers.

Emmanuel, A. (March 29, 2022). How do banks verify identity? *YOUVERIFY*. Retrieved from: https://youverify.co/blog/how-do-banks-verify-identity

EQUIFAX. (2023). The Consequences of Identity Fraud. Retrieved from: https://www.equifax.co.uk/resources/articles/the_consequences_of_identity_fraud.html

FM Contributors. (March 28, 2023). Blockchain-Based Digital Identity: Benefits, Risks, and Implementation Challenges. *Finance Magnates.* Retrieved form: https://www.financemagnates.com/cryptocurrency/education-centre/blockchain-based-digital-identity-benefits-risks-and-implementation-challenges/

Forbes. (April 24, 2023). Fake Accounts And Fake Data: The Good, The Bad And The Preventable. Retrieved from:

https://www.forbes.com/sites/forbestechcouncil/2023/04/24/fake-accounts-and-fake-data-the-good-the-bad-and-the-preventable/

Holland, S. (August 19, 2023). Identity Theft in Neobanking: All You Need To Know. *SEON. Retrieved from: https://seon.io/resources/identity-theft-in-banking/*

James, C. (April 29, 2023). Know Your Client (KYC): What it means, compliance requirements. *Investopedia.* Retrieved from: https://www.investopedia.com/terms/k/knowyourclient.asp

Kinney, J. (August 21, 2023). 10 Ways To Prevent Identity Theft. *U.S. News And World Report.* Retrieved from:

https://www.usnews.com/360-reviews/privacy/identity-theft-protection/10-ways-to-prevent-identity-theft

KHMER TIMES (March 25, 2022). Court hears appeals by foreigners in bank fraud cases. Retrieved from:

https://www.khmertimeskh.com/501047202/court-hears-appeals-by-foreigners-in-bank-fraud-case/

KHMER TIMES. (September 23, 2022). Bank employee accused of stealing $600,000 to fuel online poker addiction. Retrieved from: https://www.khmertimeskh.com/501156853/bank-employee-accused-of-stealing-600000-to-fuel-online-poker-addiction/

KHMER TIMES. (October 6, 2022). Warning on bank security as mobile banking thief busted. Retrieved from:

https://www.khmertimeskh.com/501163763/warnings-on-bank-security-as-mobile-bankinUche, A. (Jul 16, 2023). 8 Pros and Cons of A Single Digital ID System. *Make Us Of*. Retrieved from: https://www.makeuseof.com/pros-cons-single-digital-id-system/

Lee, J. (November 13, 2015). Cambodia Testing Biometric Voter Registration System. Biometric Update.com. Retrieved from:

https://www.biometricupdate.com/201511/cambodia-testing-biometric-voter-registration-system

LexisNexis. (2023). Unify Physical and Digital Identity Intelligence for a Complete View of Your Customers. Retrieved from:

https://risk.lexisnexis.com/global/en/corporations-and-non-profits/fraud-and-identity-maagement

Mirfin, J. (Jul 11, 2022). What is the real impact of identity theft? *REFINITIV*. Retrieved from: https://www.refinitiv.com/perspectives/financial-crime/what-is-the-real-impact-of-identity-theft/

Mitek. (April 28, 2022). Advantages and disadvantages of reusable digital identity. Retrieved from: https://www.miteksystems.com/blog/advantages-and-disadvantages-of-reusable-digital-identity

Museum of Science + Industry Chicago (N/A). Science at Home. Retrieved from: https://www.msichicago.org/science-at-home/hands-on-science/fingerprints/#:~:text=Your%20fingerprints%20are%20unique.,to%20hold%20on%20to%20things.

National Council on Identity Theft Protection. (2023). *2023 Identity Theft Facts and Statistics.* Retrieved from: https://identitytheft.org/statistics/

Nightingale, S. (March 2, 2022). Identity Fraud in Digital Age. *Centre For Research And Evidence on Security Threats.* Retrieved from:

https://crestresearch.ac.uk/comment/identity-fraud-in-the-digital-age/

Open Development Cambodia. (February 9, 2022). Major Banks. Retrieved from: https://opendevelopmentcambodia.net/topics/major-banks/

PHNOM PENH POST. (March 23, 2023). NBC Warns Scammers in Disguise. Retrieved from: https://www.phnompenhpost.com/national/nbc-warns-scammers-disguise

RFA Vietnamese. (November 17, 2022). Vietnamese police dismantle fraud group that stole data and hack bank accounts. *Radio Free Asia*. Retrieved from:

https://www.rfa.org/english/news/vietnam/vietnam-bank-fraud-gang-11272022222721.html

SANCTION SCANNER. (2023). Features of Blockchain Technology. Retrieved from: https://sanctionscanner.com/blog/digitalization-and-blockchain-technology-372

Towler, A. David, W. & Kemp, R. (2017). Evaluating the feature comparison strategy for forensic face identification. PubMed. Retrieved from: https://pubmed.ncbi.nlm.nih.gov/28045276/

William, A. (2023). The Pros and Cons of Reusable Digital Identity: What You Need To Know. *Loginradius.* Retrieved from:

https://www.loginradius.com/blog/identity/pros-cons-reusable-digital-identity/

Willox, N., and Regan, T. (March, 2002). Identity Fraud: Providing Solutions. *LexisNexis.* Retrieved from: http://www.lexisnexis.com/about/whitepaper/identityfraud.pdf