សាកលវិទ្យាល័យជាតិគ្រប់គ្រង

NATIONAL UNIVERSITY OF MANAGEMENT

THESIS

THE INTEGRATION OF SINGLE DIGITAL IDENTITY THROUGH NID IN CAMBODIA

BY

RATANA DANETH

Phnom Penh
2023

FACULTY OF
DIGITAL ECONOMY

MINISTRY OF EDUCATION, YOUTH, AND SPORT

NATIONAL UNIVERSITY OF MANAGEMENT

FACULTY OF DIGITAL ECONOMY

The integration of Single Digital Identity through NID in Cambodia

By

Ratana Daneth

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

(English-Based Program)

SPECIALIZATION IN

SMART CITY PLANNING AND MANAGEMENT

Phnom Penh, Cambodia

October 2023

MINISTRY OF EDUCATION, YOUTH, AND SPORT

NATIONAL UNIVERSITY OF MANAGEMENT

FACULTY OF DIGITAL ECONOMY

The integration of Single Digital Identity through NID in Cambodia

By

Ratana Daneth

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

(English-Based Program)

Supervised by:

Dr. Samreth Sovannroeun
Associate Professor
Graduate School of Humanities and Social Sciences
Saitama University, Japan

Phnom Penh, Cambodia
October 2023

COMMITTEE APPROVAL

The members of the committee approved the thesis of **Ms. Ratana Daneth** defended on October 6th, 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 Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Ratana Daneth

National University of Management

Phnom Penh, Cambodia

October 2023

ACKNOWLEDGEMENT

First and foremost, I would like to express my utmost gratitude to the people who supported and helped me during the process of completing the thesis. Their words of encouragement have by far pushed and motivated me throughout this amazing yet sometimes tiresome academic journey.

I would like to start by conveying my profound gratitude to Dr. Hor Peng, Rector of NUM for providing me with this scholarship and always encouraging all of the students to try our best throughout our academic journey. He has always been a motivating icon for me whose determination and support never fail to provide my classmates and me with many opportunities ensuring a brighter and better path for our academic journey.

I sincerely would like to express my heartfelt appreciation for Dr. Samreth Sovannroeun for being such a supportive and encouraging external supervisor for me and the NID team as a whole. His support and guidance have been one of the most important factors that motivated and encouraged me along this journey.

I would like to also express my warmest thanks to all of my internal supervisors for their immense support with my thesis journey. Their deliberate feedback has significantly helped with the progress as well as the nature of this research paper.

Lastly, my deepest appreciation goes to my loved ones, family, and friends, especially my parents for giving me this opportunity and supporting me to be who I am today. I am forever in debt with their love and kindness.

ABSTRACT

The concept of identification can be traced back to the Babylonian Empire which only gathered information on the number of people and the resources available. As time progressed, the way data was collected improved and As a result, a variety of documents were introduced. As time passes, Identification cards don't only center on the concept of an individual's identity. It also focuses on other aspects such as cards for other sectors such as driver's licenses, cards for educational purposes and work purposes, cards for digital payment, etc. Different cards were made for different purposes. For daily necessities, people have to carry around more than 3 cards maximum everyday. With the use of too many cards, people have faced a lot of problems such as confusion, technical issues, exclusion, bugs, and privacy and security risks. This research begin with a deeper understanding toward the concept of 'Digital ID' and 'Single ID'. It aims to understand positive impacts as well as limitation of both concept. It will then look into how NFT-based Identification (NID) will be able to integrate these 2 concepts together under one application in Cambodia as well.

Keyword: Digital Identity, Single Identity, Non-Tungible Token (NFT), Blockchain, Polygon SDK, Cybersecurity.

Table of Contents

CHAPTER ONE: INTRODUCTION

1.1 Background of the Research

The term “ID” stands for identity document. This is a document that is used to confirm a person's identity. It's typically a formal card that includes your name, picture, and other identifying details. Identity documents have been commonly used for centuries to establish a person's identity and citizenship. The concept of identification can be traced back to the Babylonian Empire which only gathered information on the number of people and the resources available. As time progressed, the way data was collected improved and as a result, a variety of documents were introduced. Birth certificates, land title documents, and citizenship papers were among them. A lot of these records are still in use today, although the earliest instance of what might be called "modern ID" dates back to 1414. King Henry V of England received the initial passport at this period. These credentials, known as "safe conduct" documents, were issued so that residents could establish their identification when traveling. Following this, the use of photographic identification became widespread in the early 20th century when photographs were added to passports and other ID documents. The requirement for a photographic passport was introduced in Australia and Great Britain in 1915 while France has had a national ID card for all citizens since the beginning of World War II. Those types of cards will contain personal details, including the person's complete name, picture, gender, date of birth, and identification number.

Further into that, Identification cards don’t only center on the concept of an individual’s identity. It also focuses on other aspects such as cards for other sectors such as driver’s licenses, cards for educational purposes and work purposes, cards for digital payment, etc.

1.2 Research Problem

As time passed, the number of IDs that people had to carry around started to increase tremendously. There can be several reasons why people have too many IDs.

First, different IDs were created for different purposes. Hence, going through their daily life, people have to carry around different IDs for different purposes. For instance, one for educational purposes, one for work, one driver's license, one national identification card, and one passport, in which all of the mentioned IDs are required to be carried in a physical form. Hence, the average IDs that people carry around every day are up to more than 5. With the use of too many cards, people have faced a lot of problems such as confusion, technical issues, exclusion, bugs, and privacy and security risks.

With the incoming trend, people are trying to adapt to the cashless way of living Those types of cashless society resulted in the creation of digital ID. People frequently struggle with practical issues, such as carrying and managing several cards and gaining access to services that demand special identification, which might cause problems for the cardholder while using them (Smith, Brown, Johnson, 2020). With Digital ID, it offers a more convenient way to access services and verify one's identity online. They eliminate the need for physical documents and can be easily accessed and used on various devices. However, there are still some limitation to the use of digital ID such as the confusion due to the usage of many accounts as well as the security issue.

Comes the invention of "Single ID". The concept of a single ID refers to the use of a unique digital identity that can be used across multiple platforms and services. Single ID offers users the 'Single ID' of having to use one ID to access to all of their accounts such as accounts for payment purposes, educational purposes, work purposes or government official IDs. The only drawback is that, this ID sometimes comes in a physical form which frustrates the users because of the need to carry around card.

1.3 Research Objective

The key objective of this research is to understand:

- To examine the positive impacts of the concept of "Digital ID" as well as its limitations.

- To examine the positive impacts of the concept of “Single ID” as well as its limitations.
- To explore how NFT-based identification, or NID, could be the solution integrated to achieve the concept of Single Digital ID inside Cambodia.

1.4 Research Question

This research aims to address two main research questions which include:

- Digital ID: What is the concept of “Digital ID” and what are the positive impact of this concept as well as its limitation?
- Single ID: What is the concept of “Single ID” and what are the positive impact of this concept as well as its limitation?
- The Integration of NID: How can NID integrate the Single ID concept in Cambodia in order to improve the current system used by the government?

1.5 Research Significant

The purpose of this study is to provide a comprehensive understanding of the concept of “Single ID” and “Digital ID” which has been deemed as the solution to the mentioned problems above. This allows the reader to understand the underlying issues people faced when they had their own and had to carry around many cards and how this concept utilizes this problem into a non-problem instead. Beside, we’ll also take a look at the limitation of both concept especially in the context of Cambodia as well.

This study also indicate how Cambodia could integrate the use of this concept in order to lessen the hassle caused by the problem of having too many cards and their need to carry all of the cards physically with the use of NID. Readers will be equipped with a comprehensive understanding of the concept of NID supported by its framework. NID will come as an alternative solution for the readers and its users in terms of

improving the process of having to remember all the card details as well as getting confused amongst all of the different cards they have to carry around.

CHAPTER TWO: LITERATURE REVIEW

2.1 The Positive Impacts of Digital ID and Its Limitations

Before understanding comprehensively the concept of “Single ID”, it’s best to grasp the meaning of the term “Digital Identity” beforehand. The term digital identity refers to a one-of-a-kind depiction of a subject involved in an online transaction. In the context of a digital service, a digital identity is always unique. In another term, Digital identity refers to the information utilized by computer systems to represent external entities, including a person, organization, application, or device. It includes all of an individual's accumulated data and is essential for automating access to computer-based services, confirming identification online, and allowing computers to manage interactions between entities (Techtarget, 2017). Furthermore, Mahajan, et al. (2019) also found that the opportunity for value creation through digital ID is growing as technology improves, implementation costs decline, and access to smartphones and the internet increases daily. The foundational digital infrastructure that supports digital ID grows in reach and drops in cost every day. More than four billion people currently have access to the internet, and nearly a quarter-billion new users came online for the first time in. Hence, the creation of digital ID offers people a varieties of advantages which include:

The Use of Mobile-Solution Only

The usage of mobile phones as smart applications was key to the Digital ID notion. In today's society, there is a growing demand for mobile-first solutions. Digital identity enables this approach by allowing users to carry their credentials with them wherever they go, share them whenever they want, and be authenticated by any private or public entity in order to quickly access services.

Better Access to Service Online

Digital identity helps with the process of establishing easier access to services online. It ensures democratized access to services, unlocking a range of essential services now available online, such as accessing government benefits, education, bank

accounts, and booking medical appointments. In fact, every service provider commonly has a user database that stores the user's information in their system. These providers also have their identification verification methods, which may be the same or vary completely from other service providers. For instance, Identity verification is an important process that helps to identify the identity of the users. There are several methods to identify the users all of which have their own drawbacks as well (Schulman, n.d.). Those methods include:

1. Knowledge-based authentication: Refers to a system that utilizes something the person knows, like their PIN number or password. However, the downside to this ID verification method is the risk of identity theft if someone learns the user's information and can impersonate the user.

2. Two-Factor Authentication: Just like the name, this method requires two steps before access will be granted; one step is the knowledge of the user such as the password or login information then the second step is something only they possess for instance, a swipe card. The downside is that it requires more time when logging in or signing up for an account which may turn people away from using this identity verification method.

3. Database Methods: For this method, access to information is granted when it matches what was submitted by the individual and stored in the database. This ID verification method is very easy to use and because it has such a high success rate, it's used in many organizations including banks. However, the downside of this method is that if an individual knows what information was submitted by them for storage then they can impersonate themselves without any problems.

4. Online Verification: This method refers to when access is granted as long as they are able to get through a security question and answer or the ID verification is done on an external site. However, its drawback lies in the fact that there's no way for companies to ensure that someone isn't pretending to be you in order to

gain access with the ID verification which could lead to a serious case of frauding or misleading information.

5. Biometric Verification: This is the most commonly used system that require the user to use their personal identities as the ID verification itself which could be something like the user’s fingerprint or retina scan to ensure someone isn't pretending to be the user and trying to gain access. This method can be deemed as the safest method but the downside of this ID verification method is that it can take time for organizations in order to collect these physical pieces of ID information. In conclusion, identity verification is an important part of any organization's security.

Better Access to Public Services

The political world and corporations continue to push for various digital ID initiatives to support transformation by ensuring secure online access to public services. Trade and economic expansion are made easier with improved access to public services through electronic identification. A good example is the European Union, which adopted the eIDAS regulation that facilitates trust services, electronic ID, and the easy exchange of administrative documents throughout the region. The European digital identity enables users to rapidly access public services in any of the Union's member states and is accessible to all European enterprises and residents.

Enhanced Portability

Driver's licenses, passports, ID cards, and other conventional forms of identity can be carried around and are portable. But in other nations, or even in different states within the same nation, some of these kinds of identification might not be officially recognized. Academic credentials also have a problem. In both situations, the person is dependent on outside parties to change, distribute, or validate parts of these documents. Different rules apply to the concept of portability in the context of digital identity. A digital ID is portable because it can easily be transferred and used in other places, and since it is entirely up to the user to decide how his personal data is utilized.

This perfectly indicates that users could have several ordinary accounts on different platforms with different credentials. Despite all of the benefits, as stated, digital ID still has its downside as well. Those limitation includes:

- Difficulty in managing multiple IDs: Keeping track of multiple digital IDs can be cumbersome and lead to risky practices, such as duplicating passwords. This can compromise the security of personal information and increase the risk of data breaches. Users usually face the problem of identity confusion due to the similarity of card designations and the numerous credentials that they have to remember and differentiate. Having to carry and present several identification cards can be ponderous for users which in fact, leads to misunderstandings during administrative procedures and possible delays in receiving services.
- Increased risk of identity theft: With multiple digital IDs, there is a higher risk of identity theft and fraud. Hackers can use stolen information to access multiple accounts and services, causing significant harm to individuals and organizations.

Hence, comes the concept of 'Single ID' to eliminate these problems, streamlining the identity verification process.

2.2 The Positive Impacts of Single ID and Its Limitation

The concept of a Single ID refers to the use of a unique digital identity that can be used across multiple platforms and services. In simpler words, it refers to a digital identity system that allows users to access multiple websites, shops, apps, and services from partner companies with one single login. The idea of a single ID system centers on a lean communications protocol for managing registration, authentication, and authorization processes on a SaaS basis in a zero-knowledge modus. A SaaS-basis in a zero-knowledge modus refers to a cloud-based Software as a Service (SaaS) product that is built on a foundation of zero-knowledge, meaning that the service provider maintains no knowledge of the customer's data or information (Xiippy, 2021). The system offers enhanced security and improved privacy which ensures that the

customer's data is secure and private, as the service provider has no knowledge of the data or information being stored. This approach helps to protect against unauthorized access and maintain privacy. Besides, it also increased control and compliance as the system allows the customer to retain key ownership and full ownership of their data, without relying on the service provider. This approach gives the customer more control over their data and ensures that they are the only ones who can access it which reduces risk caused by credential confusion and data fraud. These advantages make it an attractive option for companies that want to help reduce the risk of data breaches and cyber attacks, as the service provider has no knowledge of the customer's data or information (Chisholm, 2021).

The concept of single ID offers many benefits covering all aspects of lives including security as well as the economic aspect. The contents and requirements for different IDs vary widely.

- The use of one ID for everything: Single IDs offer an opportunity to standardize requirements, simplify information sharing, and allow any organization, from national governments to small businesses, to work with a single identity. Due to the fact that one user could have several ordinary accounts on different platforms with different credentials. A single digital ID system aims to eliminate this problem, streamlining the identity verification process and reducing the need for people to constantly transfer their personal data to service providers, thereby exposing that data to hackers. Having a single, trusted ID would offer individuals a much simpler, more streamlined experience while at the same time making the process of owning several digital IDs much more convenient.
- Enhanced users' privacy: another driving force behind the positive impact of Single ID is the enhancement of the user's privacy protection. Information security and data privacy have been a constant concern in today's increasingly digital world. Privacy and security are converging, thanks to the rise of big data and machine learning as well as the growing market of AI. This convergence means that privacy and security are now becoming more critical and on par with

the threat of adversaries accessing our data without authorization. Besides, many security analysts claim that human error is the biggest challenge in data privacy and security. Ill-informed and unaware employees can use weak passwords, mistakenly delete data, fall prey to phishing scams, and more (Burt, 2019). This is why, a single verified ID decreases the need for people to constantly transfer their personal data to service providers, thereby exposing that data to hackers.

However, despite all of the benefits, this concept still has some drawbacks that user should be mindful off. Those include:

- ID that comes in traditional form: Despite having only one ID, Single ID can occasionally be seen in physical form. One of the main disadvantages of physical ID cards is the need to carry them everywhere, which can be inconvenient and burdensome for individuals. Additionally, there are concerns about the security of physical ID cards, as they can be lost, stolen, or damaged. There are also privacy concerns associated with physical ID cards, as they can be used to track individuals' movements and activities. For instance, in some countries, carrying an ID card is compulsory, and failure to do so can result in fines or other penalties. Besides, implementing a physical ID card system can be expensive, and ongoing costs are associated with maintaining and updating the system

2.3 Case Study

2.3.1 Aadhaar of India

Aadhaar is a biometric identity system in India that centers around a 12-digit identity number linked to fingerprints and iris scans and was officially launched in January 2009 supported by India's Ministry of Electronics and Information Technology. Through Aadhaar, each user receives a card with that number on it, which can be cross-referenced with the biometric data held in a database. Aadhaar is a unique number, and no resident can have a duplicate number since it is linked to their individual biometrics, thereby identifying fake and ghost identities which result in leakages today. The idea

behind Aadhaar was to create a centralized system for the whole of India reliant on one form of recognizable ID, rather than the old, decentralized system of birth certificates and ration cards which were vulnerable to loss and damage and left marginalized people, particularly the rural poor people that are struggling to obtain state services (Perrigo, 2018). The Aadhaar system has been increasingly linked to bank accounts, income tax accounts, mobile phone numbers, and social welfare programs, such as disability and elderly pension schemes. The National Health Mission established the health management information system across various states of the country, where everyone is also provided with a unique health identification number. Linking this unique health identification number with the Aadhaar system has been proposed (Ganeshkumar et al., 2019). The Aadhaar system provides targeted interventions, such as subsidies, cash benefits, and incentives provided by the state, which can reach the intended beneficiaries without pilferage or loss. Aadhaar has been considered a strategic policy tool for social and financial inclusion, public sector delivery reforms, managing fiscal budgets, increasing convenience, and promoting hassle-free people-centric governance.

2.3.2 Singpass of Singapore

Singpass is Singapore's national digital identity system that provides Singapore citizens and residents with easy and secure access to over 2,000 government and private sector services online and in person. Singpass is managed by the Government Technology Agency (GovTech) and is one of eight strategic national projects that drive Singapore's Smart Nation vision. Singpass employs Two-Factor Authentication (2FA) methods such as the Singpass app, Singpass Face Verification, and SMS One-Time Passwords (OTP) to provide an additional layer of security to better protect users' personal data. The Singpass system has created endless possibilities for the government and businesses to provide innovative and user-centric digital services, based on APIs made available by NDI (OPSI, 2020). What started off as an identity and access management system for government services has grown into an ecosystem of products

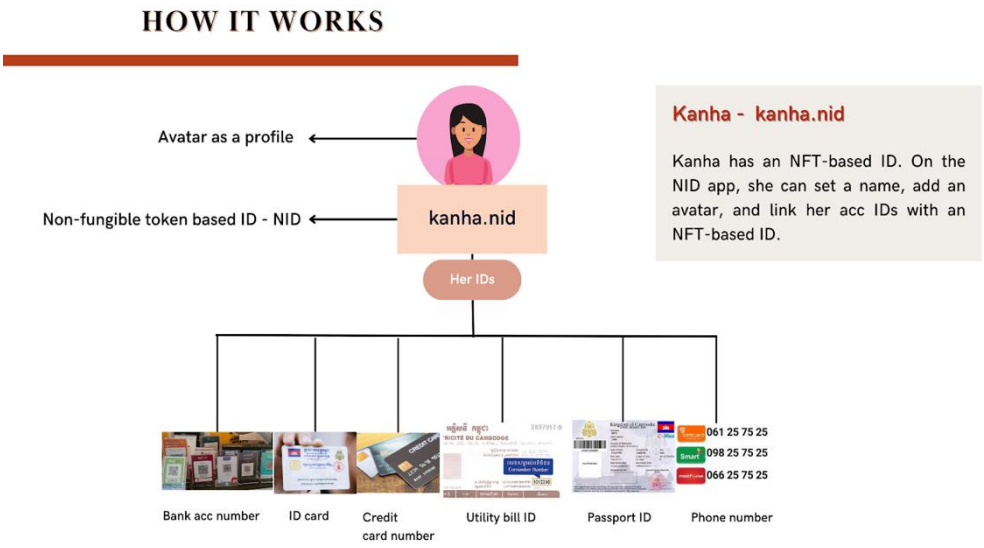
and services adopted by 97% of the population who are eligible age to use Singpass. Singpass provides a convenient and secure platform for users to transact with government agencies and private sector organizations. To date, this includes 700 organizations offering more than 2,000 services (Smartnation, 2022). Today, Singpass has a user base of more than 4.5 million users, covering 97% of Singapore Citizens and Permanent Residents aged 15 and above. More than 350 million personal and corporate transactions are facilitated via Singpass every year.

CHAPTER THREE: NFT-Based Identity (NID)

3.1 Introduction to NID

In today's living, people are creating many identity numbers from a workspace, daily living, and payment, to personal documents. Those types of IDs include bank account IDs, national ID cards, driver's license IDs, utility bill IDs, credit/debit cards, phone numbers, email addresses, website domain names, and to name a few. When people make transactions and seek to use those IDs, of course, they cannot remember all digits of IDs. Hence, some problems are possibly arising at the same time such as the possibility of transferring it to the wrong account ID, time-consuming, high cost to dispute, cross-institutional, or how disorganized the IDs are.

Figure 3: How the system of NID works



Source: NID Whitepaper, (2023)

NID is a Web3 platform that allows users to create a digital ID that stores varieties of identical numbers including national ID cards, bank accounts, utility bill

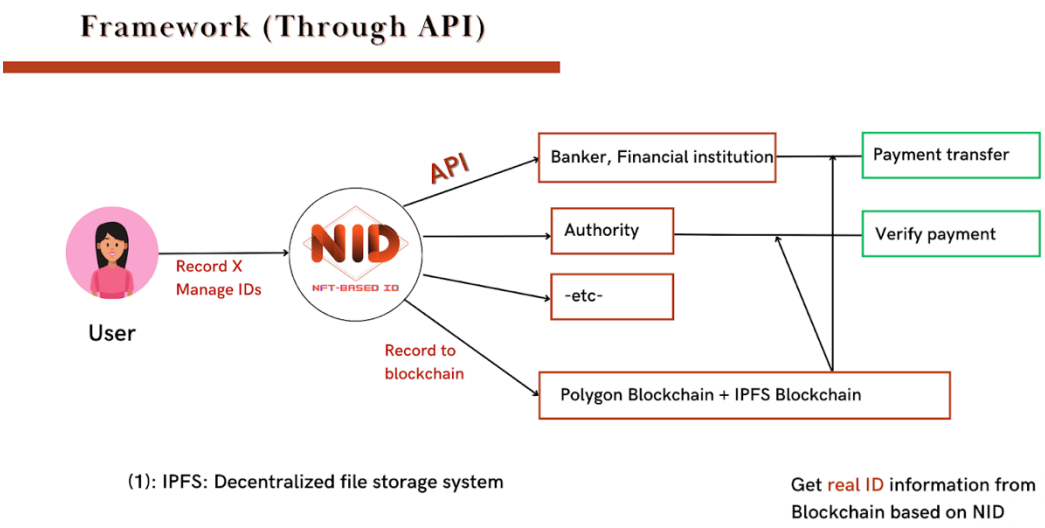
IDs, phone numbers, email addresses, and many more all together in one place. NID enables users to create a digital ID that can be used to connect all of the important information mentioned above in one place. Being able to create unique digital IDs based on users' preferences and store all the important identity information secured in a newly digitalized ID software, users are no longer required to care about security, losing and forgetting them, or even confronting any inconveniences of holding many IDs anymore. NID employs a non-fungible token, which is a unique digital identity that cannot be duplicated or swapped, is stored in a blockchain, and is used to verify ownership and validity. To assure ownership that cannot be duplicated and ownership that cannot overlap, NID is issued as NFT, which is unique, evidence of ownership, tradable, and may contain digital files as well as ID information, in accordance with ERC-721.

3.2 NID Framework

The Figure below illustrates the framework of NID. Once user creates an account through NID and input their card information which includes bank account IDs, national ID cards, driver's license IDs, utility bill IDs, credit/debit cards, phone numbers, email addresses, or website domain names, all of this information will be stored through blockchain with the help of Application Programming Interface, which also known as API. The use of API allows our developer team to sync data between multiple platforms into our blockchain and can facilitate communication among the various microservices in web applications as this term refers to all of the functions offered through NID. Furthermore, NID enables users to store their data inside the blockchain through the help of IPFS. “IPFS " in simple terms refers to a hard drive of blockchain. IPFS assures us that the data included in this network are unique (they are uniquely identified by an identifier) and are protected against modifications, making this data immutable. In the event that this data is changed, a new “hash” identifier is generated, which would not coincide with the one stored in the blockchain for the recorded data or the old information that the user stored in NID. IPFS and blockchains can work well together because IPFS would connect all these different blockchains in a

similar way to how the internet connects all websites. Hence, all of the information stored by the user inside NID will be protected through blockchain working closely with IPFS and the help of API as well.

Figure 4: How the system of NID works



Source: NID Whitepaper, (2023)

3.3 Features and Functionality

With the goal to enhance users 'capability, NID system introduces several key features that aim to boost user experiences through functions like easy customization, conveniences, and better engagement within the platform such as:

- Avatar and Name Customization: Users can now select their own distinctive avatars and names, giving their NID profile a more personalized feel. This feature not only encourages individualism but also improves the quality of platform interactions.

- Seamless Account Number Integration: The procedure of managing many accounts is made easier by NID. Users no longer need to keep track of many account data because they can easily link their various account numbers to their NID. Account administration and transactions are simplified by this integration.

- NFTs Trading: By enabling users to trade NFTs, the NID system embraces the NFTs' rising popularity. The platform's ability for users to buy, sell, and exchange NFTs creates intriguing new possibilities in the field of digital collectibles and assets.

- Customized ID Purchase: Users have the option to purchase distinctive, personalized IDs from NID based on their interests. Their digital identity is further personalized by this function.

- Connection to Multiple Services: Users can link their NID to a variety of services, including those offered by the application, not just bank accounts. As a result, a flexible and integrated digital ecology is created.

- Simplified Transactions: In terms of payment system, NID makes transaction processing easier for users. Users can access all of their linked bank accounts by just entering their NID. This simplifies financial transactions and reduces the possibility of choosing the incorrect account while transferring money.

- User-Centric Experience: By making it easier to manage various accounts and improving the overall user experience, NID strives to deliver a more unified and user-centric single digital ID experience for everyone accessed to the application.

3.4 Technology

What is more, NID's foundation is built on the Polygon Blockchain, a decision impacted by a number of essential factors such as usability, utility, stability, and security. Polygon is a Layer 2 scaling solution that aims to address the scalability issues of the Ethereum blockchain, while other blockchain platforms like Ethereum and Solana are Layer 1 solutions. Polygon offers faster and cheaper transactions compared to Ethereum, which can be slow and expensive. Polygon SDK is a modular, flexible framework for Ethereum scaling and infrastructure development. It is designed to become the go-to framework for developers to quickly and easily build and launch multiple scaling and infrastructure solutions. Polygon SDK also aims to support building and connecting two major types of solutionssuch as adaptors for external blockchain networks and enterprise modules and products. Another thing is that, Polygon SDK is secured through its use of the Ethereum blockchain which is considered one of the most secure and battle-tested programmable blockchains in the world, followed by the use of zero-knowledge technology for compliance use cases .hich enables users to prove their identity without necessarily disclosing personal information to third parties. Polygon SDK also enables developers to create standalone chains that are fully responsible for their own security, making it a secure and flexible framework for Ethereum scaling and infrastructure development.

CHAPTER FOUR: RESEARCH METHODOLOGY

This section aims to discuss the techniques utilized in the research which includes the research strategy, data collection and how it can be measure.

4.1 Research Strategy

This research paper will integrate the use of 'literature review' method to abstract and analyze data in order to support the paper and to answer the first 2 question while integrating the method of 'Theory of Change/TOC' to answer the last question.

4.2 Literature Review

A literature review is a way to obtain an overview of published documents on a given topic, with a view to synthesizing, summarizing or writing up existing material. Literature review can be used to find out how much material is available on a specific topic before further research (such as interviews, surveys, etc.) is undertaken. Because it involves reviewing existing material, literature reviews can be useful in determining whether a programme has already been implemented in a given area, or with a certain group. Literature reviews are flexible and rely on a range of data sources, including academic literature, online material, discussions with individuals, publicly available statistics, the press, or directories or databases. Literature can be used before a project to find out information about the issues that the project or intervention is seeking to address, the main needs of the target group or the key issues to consider when implementing a programme in a given area (Hague and Wilcock, 2014).

4.2.1. Data Collection Methods

The steps required to conduct a literature review vary depending on the type of review. Typically the standard steps for conducting a literature review include defining

a research question; identifying, selecting and reviewing relevant literature; and lastly, synthesizing the evidence (production of the output).

- Defining a research question: this step includes defining an appropriate issue to be examined and formulating research questions that will guide a literature review process. The resources available to complete the job, the research question to be addressed, the planned next steps, and where evidence is likely to be available all have a role in determining the type of review that is required, such as how thorough and methodical it should be.
- Identifying, selecting and reviewing relevant literature: In order to identify, select, and review relevant studies, it is necessary to agree on inclusion and exclusion criteria, and to determine search terms. When the research question has been finalized and the sources have been selected, sources should be assessed for reliability. This involves examining the publication venue and author of the study results (such as a peer-reviewed academic article, a blog post, or a study sponsor's marketing bulletin), any bias in the document, the sort of evaluation results displayed, and, if appropriate, the funding source for the study. The sources that will be most helpful in addressing the research questions should be the ones that are reviewed.
- Extracting Data: The following step involves gathering or extracting applicable information from each primary study included in the sample and deciding what is relevant to the problem of interest. The kind of information that needs to be gathered does, in fact, mostly depend on the initial research questions. However, crucial data may also be acquired regarding the original study's procedures, design, and participants, as well as its qualitative and quantitative findings (Cooper & Hedges, 2009).
- Synthesizing the evidence: Synthesizing findings helps bring together relevant evidence into a cohesive whole, providing a basis from which to make suggestions for future evaluations, research studies and policy formulation or

implementation. Collecting findings through this process allows attention to be given to the quality and relevance of the evidence.

4.3 Theory of Change (TOC)

Theory of Change is essentially a comprehensive description and illustration of how and why a desired change is expected to happen in a particular context. It is focused in particular on mapping out or "filling in" what has been described as the "missing middle" between what a program or change initiative does and how these lead to desired goals being achieved. This is accomplished by first determining the desired long-term goals, then working backwards from these to determine all the prerequisites (outcomes) that must be met for the goals to materialize. The outcomes plan then serves as the foundation for determining the kind of activity or intervention that will produce the results noted as necessary before the long-term goal can be achieved. Through this approach, the precise link between activities and the achievement of the long-term goals are more fully understood.

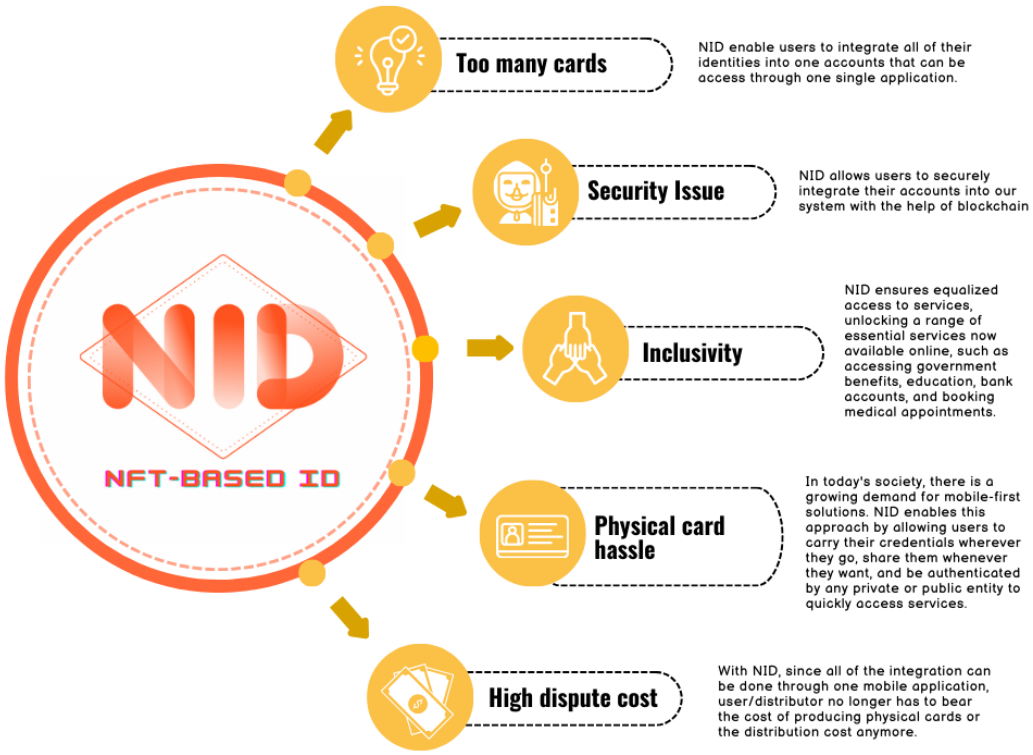
4.3.1 Data Analysis Methods

In developing the logic model it is important to identify key components of the programme and relationships between them(Hofman & Anke, n.d.). In order to analyse the data with the proposed framework, the study must go through all these steps in order to achieve the desirable outcome:

- Problem statement: articulate the problem that programme is trying to solve or the needs that it is trying to address. In this case, how NID try to integrate the concept of both Single ID and Digital ID together.
- Set specific goals: define what the programme is trying to accomplish.
- Resources and activities: identify available resources and how these will be used to implement the programme and achieve its goals.

- Outcomes: determine how outputs make a lasting change and contribute to programme goals. For instance, how NID can bring the positive impacts of Single Digital ID to Cambodia just like either Singpass or Aadhaar.

4.3.2 NID's TOC Diagram



The Diagram above illustrates how NID will be able to tackle the existing problem through the Theory of Change model. Further elaboration will be discussed through finding parts.

CHAPTER FIVE: RESEARCH FINDING

5.1 The Positive Impacts and Limitations of 'Digital ID'

Digital identity refers to the information utilized by computer systems to represent external entities, including a person, organization, application, or device. It includes all of an individual's accumulated data and is essential for automating access to computer-based services, confirming identification online, and allowing computers to manage interactions between entities (Techtarget, 2017). Every day, the basic digital infrastructure that underpins digital ID expands in scope and becomes more affordable. Nearly a quarter of a billion additional users went online in 2016, adding to the more than four billion individuals who already have access to the internet. Therefore, the development of digital ID provides people with a number of benefits, such as:

- The use of mobile solution only: the idea of a single ID was fundamentally based on the use of smart applications on mobile devices. There is a rising need for mobile-first solutions in today's culture. This strategy is made possible by digital identity, which gives users the freedom to take their login information with them wherever they go, share it with anybody they choose, and be verified by any private or public entity to swiftly access services.
- Better Online Service Access: establishing simpler access to services online is made easier with the use of digital identity. By guaranteeing democratized access to services, it opens up a variety of crucial internet services that are now accessible, including obtaining government benefits, schooling, bank accounts, and scheduling appointments for medical care.
- Better Access to Public Services: A variety of digital ID projects are still being pushed by business and politics to support change by enabling safe online access

to government services. Improved access to public services through electronic identification facilitates trade and economic growth.

- Enhanced Portability: A digital ID is portable because it can easily be transferred and used in other places, and since it is entirely up to the user to decide how his personal data is utilized. Passports, ID cards, driver's licenses, and other traditional forms of identification are transportable and portable. But some of these forms of identification might not be officially accepted in other countries or even in different states within the same country. Parts of these papers are typically changed, distributed, or validated by outside parties. A digital ID is portable because it can easily be transferred and used in other places, and it is entirely up to the user to decide how his data is utilized.

Despite all of the benefits, as stated, digital ID still has its downside as well. Those limitation includes:

- Difficulty in managing multiple IDs: Managing numerous digital IDs can be difficult and result in dangerous behaviors, including using the same passwords multiple times. Due to the similarity of card designations and the multiple credentials that users must remember and distinguish, users frequently experience identity uncertainty. Users may find it burdensome to carry around and provide multiple forms of identification, which can cause confusion during administrative processes and delay in receiving services.
- Increased risk of identity theft: The risk of fraud and identity theft is heightened when using numerous digital IDs. Hackers have the ability to access several accounts and services using stolen information, which is extremely harmful to both people and businesses.

5.2 The Positive Impacts and Limitation of ‘Single ID’

A single identification that can be used on several platforms and services is referred to as a single ID. In plainer terms, it alludes to a digital identification system

that enables users to sign in only once to access a variety of websites, stores, apps, and services from affiliated businesses.

The concept of single ID offers many benefits covering all aspects of lives including security as well as the economic aspects such as:

- The use of one ID for everything: Single IDs give organizations of all sizes—from national governments to small businesses—the ability to collaborate using a single identity while standardizing standards and making information sharing easier. Individuals would benefit from a more simpler, more streamlined experience and would find it much more easy to possess many digital IDs if they had a single, trustworthy ID.
- Enhanced users' privacy: The increased user privacy protection is a further force behind Single ID's beneficial effects. In today's increasingly digital environment, information security and data privacy have been a continual issue. The largest problem with data privacy and security is human mistake. Employees who lack knowledge or awareness may use weak passwords, accidentally destroy data, be fooled by phishing scams, and more (Burt, 2019). This is why having a single verified ID reduces the need for consumers to continually provide their personal information to service providers, increasing the risk of hackers gaining access to that information.

However, despite all of the benefits, this concept still has some drawbacks that user should be mindful off. Those include:

- ID that come in physical form: Single ID sometimes come in a physical form in which frustrate the users because of the need to carry around card. Physical ID cards have a number of drawbacks, including the requirement to carry them at all times, which can be bothersome and burdensome for people. Physical ID cards raise additional security issues because they are vulnerable to loss, theft, and damage. Physical ID cards raise privacy issues as well because they can be used to monitor people's movements and activities. For instance, it may be

illegal to travel without an ID card in some nations, and doing so may result in fines or other consequences. A physical ID card system can also be expensive to implement, and continuing expenses for maintaining and updating the system are involved.

5.3 The Integration of NID as Solution

NID is a Web3 platform that allows users to create a digital ID that stores a variety of identical numbers including national ID cards, bank accounts, utility bill IDs, phone numbers, email addresses, and many more all together in one place. NID enables users to create a digital ID that can be used to connect all of the important information mentioned above in one place. Just like what the concept of Single Digital ID proposes, NID enables users to link more than one account ID due to the NFT feature that allows NID to securely and easily attach all of the user's important information into one system or location. Users no longer need to input different account information or numbers when processing transactions, paying utility bills, transferring money, or accessing any official accounts in the government system. With NID as the replacement, users may now link more than one identity number, allowing NID to safely and conveniently attach all of the user's critical information in one area only which is through their mobile application.

CHAPTER SIX: DISCUSSION

As stated in the problem statement part, this research paper aims to gain a deeper understanding in terms of the positive impact as well as the limitation of the concept of ‘Single ID’ and ‘Digital ID’. As such, both of the concepts have their own benefits as well as their own limitation as well. Integrating both concept together will result in greater benefits in terms of aspects such as user’s experience, security and economic as well. For instance, A single digital ID can simplify and streamline the user experience

by providing a single point of access to multiple services and applications. This can save time and effort for users, making it easier for them to access and use services. Users will no longer needed to remember or note down many credentials or carryinga around many cards anymore. One application with a single log in will enable them to gain access to everything with just their smart phone. This can also improve the user experience and reduce the risk of exclusion for those who cannot access or use certain digital ID systems.

In fact, as a developing country, Cambodia is currently in the process of digitizing its identity system. So far, the government has plans to collect biometrics and issue digital ID documents. In addition, Cambodia also has a Digital Government Policy in place that aims to improve public service delivery through establishing a governance system. However, the usage of digital technology in Cambodia is still basic, and public understanding of digital transformation is underdeveloped which become the biggest problem the country continues to face despite its efforts. Cambodia's potential to improve social protection programs through digital technology is large, but it currently lacks a universal and easily verifiable system. So far, despite the growing market toward digital identity, Cambodia’s knowledge regarding the integration of both concept is still deemed to be non-existed. How Could the Integration of NID Offer the Concept of a Single Digital ID to Cambodia?

6.1 NID Integration as Cambodia’s Digital Single ID

Single Digital Identity for everything

Just like what the concept of Single digital ID proposes, NID enables users to link more than one account ID due to the NFT feature that allows NID to securely and easily attach all of the user's important information into one system or location. Users no longer need to input different account information or number when processing transactions, paying utility bills, and transferring money or accessing into any official accounts in the government system. With NID as the replacement, users may now link

more than one identity number, allowing NID to safely and conveniently attach all of the user's critical information in one area only. In the case of Cambodia, citizens would now be able to connected all of their cards and other personal information into one identity which could reduce the amount of cards they have to carry around physically and also the problem of having a difficult time accessing their information in government system such as the welfare system, the public health card system or information for daily purposes (driver's license, nation identification card, etc).

Enhanced Security and Improved User's Privacy

Information security and data privacy have been a constant concern in today's increasingly digital world. Privacy and security are converging, thanks to the rise of big data and machine learning as well as the growing market of AI. This convergence means that privacy and security are now becoming more critical and on par with the threat of adversaries accessing our data without authorization. Besides, many security analysts claim that human error is the biggest challenge in data privacy and security.

As for Cambodia, the country byfar has a limited pool of cybersecurity experts, which is a challenge especially in term of information security as well as data privacy. Despite increasing internet use in Cambodia, knowledge of digital safety practices remains limited, leaving internet users vulnerable to threats. What the government could do is to, first, adopt a "privacy-and-security-by-design" approach to ensure that privacy and security are built into the enabling technology from the start such as the implementation of Single Digital ID system. This approach highly involves incorporating an assessment of risks to privacy and security into the planning process. Moreover, government should ensure that the digital ID system is inclusive and accessible to all, regardless of socioeconomic status, gender, or other factors. This can be achieved by designing the system with the needs of marginalized communities in mind. As for NID, any user could create an account as long as they download our mobile application.

CHAPTER SEVEN: CONCLUSION

At last, this research paper has comprehensively looked into the positive impacts of both Single and Digital ID concepts as well as their limitation. As such, Single Digital ID refers to a digital identity system that allows users to access multiple websites, shops, apps, and services from partner companies with one single login. It offers an opportunity to standardize requirements, simplify information sharing, and allow any organization, from national governments to small businesses, to work with a single identity. Having a single, trusted digital ID would offer individuals a much simpler, more streamlined experience while at the same time making the process of owning several digital IDs much more convenient.

With the case of NID, this mobile application will enables users to link more than one account ID due to the NFT feature that allows NID to securely and easily attach all of the user's important information into one system or location. Users no longer need to input different account information or number anymore. With NID as the replacement, users may now link more than one identity number, allowing NID to safely and conveniently attach all of the user's critical information in one area only. In the case of Cambodia, citizens would now be able to connected all of their cards and other personal information into one identity which could reduce the amount of cards they have to carry around physically and also the problem of having a difficult time accessing their information in government system such as the welfare system, the public health card system or information for daily purposes (driver’s license, nation identification card, etc).

Despite this, this research paper still has limitation due to the scope of the research itself. Further study shall discover even more impactful aspects of NID and how this mobile application will be able to unleash its full potential toward Cambodia’s society once it released.

REFERENCES

Antone, E. (2022, June 1). Extending zero trust to your saas applications. Obsidian Security. https://www.obsidiansecurity.com/blog/extending-zero-trust-to-your-saas-applications

Biometrics: Definition, use cases, latest news. Thales Group. (2023, May 20). https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

Burt, A. (2019, August 23). Privacy and cybersecurity are converging. here's why that matters for people and for companies. Harvard Business Review. https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies

Cointelegraph. (n.d.). Cointelegraph Bitcoin & Ethereum Blockchain News. Cointelegraph. https://cointelegraph.com/learn/polygon-blockchain-explained-a-beginners-guide-to-matic

Contributor, T. (2017, August 30). What is digital identity?: Definition from TechTarget. WhatIs.com. https://www.techtarget.com/whatis/definition/digital-identity

Fleetwood, D. (2023a, August 9). Non-probability sampling: Types, examples, & advantages. QuestionPro. https://www.questionpro.com/blog/non-probability-sampling/

Fleetwood, D. (2023b, September 4). Quantitative research: What it is, Tips & Examples. QuestionPro. https://www.questionpro.com/blog/quantitative-research/

Gopichandran, V., Ganeshkumar, P., Dash, S., & Ramasamy, A. (2020, April 1). Ethical challenges of Digital Health Technologies: aadhaar, India. Bulletin of the World Health Organization. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7133485/

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

OPSI. (2022, November 16). Singapore's National Digital Identity - singpass. Observatory of Public Sector Innovation. https://oecd-opsi.org/innovations/singpass/

Perrigo, B. (2018, September 28). What to know about Aadhaar, India's biometric identity system. Time. https://time.com/5409604/india-aadhaar-supreme-court/

Person. (2022, May 10). The history of Id. Veriff. https://www.veriff.com/blog/the-history-of-id

Polygon Lab. (n.d.). Announcing polygon SDK: The gateway to multi-chain ethereum!. The Value Layer of the Internet. https://polygon.technology/blog/announcing-polygon-sdk-the-gateway-to-multi-chain-ethereum

Schulman, H. (2021, August 16). 6 identity verification methods. Lightico. https://www.lightico.com/blog/6-identity-verification-methods/

Singpass Singapore's National Digital Identity (factsheet). Smart Nation Singapore. (2022, March 2). https://www.smartnation.gov.sg/media-hub/press-releases/singpass-factsheet-02032022/

Solana vs. Polygon vs. ethereum – the ultimate comparison - blockchain council. Blockchain, AI & Web3 Certifications. (2023, March 12). https://www.blockchain-council.org/blockchain/solana-vs-polygon-vs-ethereum/

Uche, A. (2023, July 16). 8 pros and cons of a single digital ID system. MUO. https://www.makeuseof.com/pros-cons-single-digital-id-system/

Wikimedia Foundation. (2023, September 4). Identity document. Wikipedia. https://en.wikipedia.org/wiki/Identity_document

William, A. (n.d.). The Pros and cons of Reusable Digital Identity: Loginradius blog. loginradius. https://www.loginradius.com/blog/identity/pros-cons-reusable-digital-identity/

Xiippy.ai. (2021, April 8). Zero-knowledge SAAS; the only way SAAS must and will be. Xiippy. https://xiippy.ai/Blog-and-News-Articles/zero-knowledge-saas-the-only-way-saas-must-and-will-be-2d7afdada00b