Managing Blockchain Based Digital Identity for Payment System

Master Thesis

Krisna Setioaji
Msc Management of Technology

TUDelft

Managing Blockchain Based Digital Identity for Payment System

by

Krisna Setioaji - 5046068

in partial fulfilment of the requirements for the degree of

Master of Science
in Management of Technology

at the Delft University of Technology,
to be defended publicly on August 27, 2021

Chairperson	: Prof.dr.ir. M.F.W.H.A. (Marijn) Janssen
First Supervisor	: Prof.dr.ir. M.F.W.H.A. (Marijn) Janssen
Second Supervisor	: Dr.ir. Z. (Zenlin) Roosenboom-Kwee

Acknowledgements

Undoubtedly, writing a thesis is an activity that is not only very challenging but also rewarding at the same time. At first, you may feel confused, even excited at times, but other times also feel so overwhelmed and stressed. Personally, my interest and curiosity in the socio-technological aspect of Blockchain technology are one of my main drivers and source of energy that keeps me moving forward to finish the master thesis.Being able to finish the master thesis and the MOT program was no easy feat. This would not be possible without the support of many parties and individuals. Therefore, I'd like to take this opportunity to thank the remarkable parties and people behind this marvellous journey. Firstly, I would like to thank Bank Indonesia (BI), the Central Bank of Indonesia, for providing me with the scholarships and the opportunity to pursue the master degree at the TU Delft.

I would like to thank Prof. Marijn Janssen as my first supervisor for his expertise on the subject and his enthusiasm in providing valuable feedback towards the research work. He has patiently shared his knowledge, literature and thoughts that guided me through finishing the thesis. Without those insights, I would not have finished my thesis in this direction. I would also like to thank Dr Zenlin Roosenboom-Kwee as my second supervisor for her knowledge, critical comments, eyes for details, and constructive feedback that helped me write a qualified report.

I would like to thank all of the interviewees for their unique insights and comments and their support with the discussion, knowledge and experience that greatly help me to finish the master thesis. Every detail during our discussion is a valuable insight for this research.

Also, I would like to thank the Delft Indonesian Student Organization (PPI Delft) friends that I cannot mention one by one- you have been my surrogate family and a home away from home, my big Indonesian family in the Netherlands where we can share our ups and downs. I also want to thank my MOT friends, especially my fellow MOT adventurer, mas Tofan, Rere and Bisma. Thank you for being a great teammate and keeping me sane during the pandemic and MOT hectic period. It is always a pleasure to discuss this with you guys and know that we are in this together.

I am also deeply indebted to my family in Indonesia, Mama, Papa, Pak De, Bu De, mbak, mas and everyone for their unique way of support. I am forever grateful to have you supporting me in every way possible. I believe the journey in TU Delft would not have happened without your blessings and prayers.

Finally, thank you, my dear wife, Rizka who fully supported me during my study. Thank you for spending most of your time taking care our beautiful daughter, Ayana, since her birth in Delft. I am sorry for not being there to help you all the time, because I keep myself busy with exams and thesis. Thank you for always supporting me in everything I do. Without you, this journey would not be as challenging and rewarding at the same time. Thank you for always being there, pushing me to do my best and to be the better person I am.

Krisna Setioaji
Delft

Summary

Online technology has transformed how people pay and utilise various services; payment methods that are mobile, fast, efficient, and secure have become basic needs. Digital identity is crucial to ensure the trust of doing business; however, its current implementation in payment services faces a data vulnerability, low data control for the user, and redundancy during the onboarding processes. Furthermore, the current Know-Your-Customer (KYC) process cannot fully verify the genuine identity, experience a loss of users' privacy, have data monopolisation, and risk abuse due to market power. Therefore, a revolution in digital identity is needed, such as blockchain technology. Blockchain is a data structure used in a distributed ledger, stored and distributed in a package called a block, and connected in a digital chain. Blockchain uses cryptographic methods and algorithms to record and sync data across the network with parties validating using a consensus protocol, rendering it impossible to tamper or modify the information without authorisation. By using blockchain technology, public institutions can ensure the security of personal data, both for the public and for industries. Industries can use the user's information as long as it obtains consent from the public following the applicable regulations, while users can control their data based on their needs and consent. Industry players can do KYC efficiently and safely without violating the data owner's privacy and consent. With these possibilities, blockchain technology is expected to enhance digital identity in the payment system significantly.

However, literature in blockchain-based digital identity specifically used for the government's payment ecosystem is still limited. Most blockchain research in the financial field focuses on the transactional part. Additionally, the study of digital identity mostly focuses on researching the technology on how it can enable the self-sovereign identity. None have discussed how blockchain-based digital identity can impact the payment system and examine its socio-technical changes within the ecosystem. Therefore, this study aims to fill the gap before governments can implement the technology by identifying the suitable type of blockchain architecture for the payment ecosystem, its impact on the current payment ecosystem and stakeholders, and finally, how the system will be governed. The main research question will be formulated as **"How can blockchain-based digital identity be managed for the Payment System in Indonesia?".**

Indonesia is chosen as the case study due to the rapid development of the payment ecosystem in Indonesia. Bank Indonesia formulated The Indonesia Payment System Blueprint 2025 (2019), which has the Payment ID development as one of its initiative to answer the financial challenges. This research will aim to answer the gap in blockchain-based digital identity concerning Payment ID development in Bank Indonesia.

This explorative study aims to find a suitable approach to implement and manage the blockchain-based digital identity for payment systems in Indonesia from the organisational and governance perspective to help stimulate the implementation of this technology. This study aims to find a suitable blockchain type to fulfil the payment system's digital identity requirement, discuss the implication of blockchain technology to the payment ecosystem- especially its opportunity and risk, and find a suitable data governance approach to manage the data within the blockchain-based digital identity.

The data was collected through literature reviews and semi-structured interviews with actors in Indonesia's payment ecosystem and blockchain technology. The initial literature study and interviews form the design concept of a blockchain-based digital identity in the payment system. It will be displayed to users and market players in the payment ecosystem to see its relevance to current business processes. The results of the two interviews were then used as the starting material to analyse the impact of blockchain technology on the payment system. There were 12 interviews session with various respondents from different stakeholder perspectives and technical levels and elaborated with data triangulation and the carefully selected respondents.

The findings identified several issues in the current digital identity. The regulators view that there is a lack of digital identity data availability required for data analysis. The market views that the current self-maintained digital identity still has a security risk and data integrity problem, and a new form of Payment System digital identity is needed to resolve issues like identity fraud, cumbersome KYC processes and data mismatch. The users view data control as an issue as they do not know which institutions records and use their data. Operational redundancy is another concern as various financial institutions asked them for the same data during onboardings. By implementing blockchain-based digital identity for payment systems, these stakeholders expected

several benefits such as data availability, data integrity, better digital identity security, operational efficiency and user data control.

Based on the current situation of the Indonesian payment ecosystem, requirements were identified and developed to determine the suitable blockchain architecture for implementing the blockchain-based PaymentID. Consortium Blockchain (Private Permissioned) with the Proof of Authority Consensus was chosen as the blockchain type as payment system regulators have to control and supervise the data, ensuring compliance within the digital identity. However, this decision also sparked a dilemma: centralising digital identity may give the regulators more control over the data, but it might lose data transparency in the public's eye. On the other hand, if blockchain-based digital identity is stored decentrally, the regulators may lose control over the data.

The government also face technological and technical challenges when implementing this technology as regulators and market players lack knowledge about blockchain. The complexity of the regulation and governance among government institutions are also major challenges that require inter-institutional collaboration. Lastly, the market players will face the technological and business process transition challenge because it can cause changes in their strategy to gather and utilise the users' digital identities.

Subsequently, to facilitate the needs of the regulators, market players and the users, we need to identify the area of responsibility on several governance processes in the blockchain-based PaymentID. The four main governance processes that are recommended are governance on block creation, governance on Payment ID Registration, governance on the trusted list, and finally, governance on user keys and credentials.

This research contributes in identifying high-level requirements to develop a blockchain-based digital identity based on the needs of the relevant actors and the scope of the payment ecosystem. Furthermore, this study reflects that implementing a blockchain-based identity in an established ecosystem is a complex task, not merely an IT project but also a change in the whole ecosystem. This study is expected to assist policymakers, regulators and the public regarding the potential advantages and challenges of using a blockchain-based digital identity.

This study is limited as it only investigates one country, Indonesia. Additionally, similar technologies in developing countries such as Indonesia are rare, so it is difficult to find a suitable implementation case as a benchmark. Secondly, the quality of the case studies is closely related to the quality of the researchers, which may lead to bias from the researcher's side, affecting the formation of conclusions from this study. This is mitigated by having a structured research methodology and carefully selecting the participants and interviewees to represent the existing condition in the payment ecosystem.

Several recommendations for further research are as follows. 1. Research to develop a blockchain-based digital identity platform that is suitable for the payment ecosystem. We recommend a prototyping and experimenting approach to observe the socio-technical complexity of the system. 2. Research related to the performance of blockchain-based digital identity for implementing a payment system environment that aims to find out the scalability of the technology. 3. Research on how change management is implemented in transition to blockchain-based digital identity, which aims to find a more concrete action plan for the technology and business transition processes.

Table of Contents

List of Figures

List of Tables

Terminology

Term	Definition
Blockchain	A distributed database of records or public ledger of all transactions or digital events that have been executed and shared among actors within a network of participants. Blockchain can also be represented as a database form that has decentralised security and synchronisation.
Cryptocurrency	A digital currency used to digitally buy products and services that utilise blockchain or distributed ledger with strong cryptography to secure its online activities, including transaction, coin/token creation, and ownership verification.
Digital Identity	A set of digital records that represent a user or an individual. It contains characteristics that can make an individual or a person unique and different from the other entities.
Know Your Customer (KYC)	Guidelines or processes of verifying customers' identity by organisations or financial institutions before starting business with new clients or customers. This process is necessary for financial institutions to reduce the risk of financial fraud, identity theft, money laundering or other illegal financial activities.
Self-Sovereign Identity (SSI)	A digital identity approach that gives data ownership to the users and enables them to control their personal data. External parties will require consent from the users if they want to access their personal data
Identity Provider (IdP)	An entity or organisation that provides services to store and manage identities. This entity can also provide authentication services to service providers that rely on its services.
SP	An entity or organisation that provide services or digital resources for users authenticated to use their services.
PJSP	PJSP in Indonesian means "Penyedia Jasa Sistem Pembayaran" or Payment Service Provider. It is an entity that provides a variety of electronic payments ranging from bank-based payments such as bank transfers and credit cards to electronic money and electronic wallet provider.

1 Introduction

1.1. Identity Challenge in Financial Technology

The digital revolution in the last decade has drastically changed people's economic behaviour. Consumption patterns that are now shifting towards digital platforms require payment methods that are mobile, fast, efficient, and secure. The new form of collaboration between economic actors through economic sharing in developing countries has begun to reduce the role of financial institutions as *middlemen*. However, without proper regulations, the digitalisation of the economy and finance also carries risks that need to be monitored. These risks include, among other things, increased shadow banking activity, unfair business competition, and misuse of consumer data (Bank Indonesia, 2019). The latest research results from Experian (2019) showed that Indonesia's business today is expected to offer more than just personalised products; consumers also need companies to provide security and convenience in every interaction. The annual Global Identity and Fraud report (Experian, 2019) also revealed that more than three-quarters (or 78%) of Indonesian consumers say safety is their top priority, followed by convenience - an increase compared to the previous annual report where 77% of Indonesian consumers rated safety as their most important element when conducting online activities. In addition, when companies have confidence in their ability to identify consumers, as many as 48% of Indonesian companies experience increased losses from year to year due to fraud, often caused by the inability to identify consumers. The same report noted that 100% of companies in Indonesia believe in their ability to identify and re-identify their customers - the highest number in the APAC region apart from India.

However, while this should reduce the incidence of fraud, fraud continues to increase every year. There is a real concern when as many as 36% of consumers in Indonesia (lowest in APAC) state that they do not feel identified or known when doing online activities. The report found that the key factor for better consumer engagement is the identification and recognition of each consumer. The data collected from each interaction strengthens the identity authentication process and builds familiarisation. Other findings from this report

- this is the fourth annual report published - related to the Indonesian market include: 1) 93% of consumers cite protecting their data from theft or misuse - which may lead to fraud, as very important in providing the customer experience, (2) 82% of consumers said it was crucial to have a safety demonstration when interacting and doing online activities, 3) 66% of consumers want more control over their data usage, 4) 85% of consumers understand the importance of their personal information to the company, 5) Nearly all consumers (97%) like adjustments made to the customer experience - a result of using their data, 6) Only 23% of companies prioritise specifically targeted products and offerings.

In this case, the robustness of digital identity is considered necessary for the financial technology environment, as digital identity functions to protect against cybercrime and fraud, enabling the Know Your Customer (KYC) standards and ensuring the market's integrity (Arner, 2019). However, the study also mentioned that there are currently main concerns on the digital financial identity: Inability to verify the genuine identity, the loss of users' privacy, and data monopolisation and risk of abuse due to market power.

1.2. Payment System Digital Identity

Bank Indonesia formulated The Indonesia Payment System Blueprint 2025 (2019), which is oriented towards developing a digital financial ecosystem in Indonesia to answer those challenges. Following the payment system blueprint, based on the 4th initiative (Bank Indonesia, 2019), Bank Indonesia will build a Data Hub as a public infrastructure to enable data openness and optimise its use for the public interest. Bank Indonesia will establish a secure payment System ID (Payment ID) as an anchor for the payment system data. This Payment ID will later function as a component of the national retail payment ecosystem. The development of this Payment ID will impact several stakeholders currently involved in the Indonesian payment system, such as regulators, banks, payment system financial technology (fintech) and payment system users. With an integrated payment interface, everyone with a bank account can create a Virtual Payment Address (VPA) and immediately transact via mobile devices. The use of VPA represents a bank account and a customer's Payment ID, thereby increasing convenience and security when making transactions. Furthermore, Payment ID will also be an enabler for the user in the digital financial services ecosystem. By linking the unique parameter to the Payment ID, it is expected that the government can efficiently channel social funds directly to the recipient's bank accounts. Subsidy recipients will be authenticated based on KYC data from their Payment ID. Therefore, to realise this Payment ID, Bank Indonesia requires technology and/or a platform that is governable, auditable, and secure at the same time. In finding this solution, one technology that offers various features and capabilities to accommodate secure and auditable data is blockchain technology.

1.3. Blockchain Technology as an Enabler

Crosby et al. (2015) defined blockchain as distributed publicly shared records between actors within a network. Blockchain is a data structure used in a distributed ledger, stored and distributed in a package called a block and connected in a digital chain, thus the name Blockchain. Blockchain is a type of data structure in a chain, not a ledger nor technology. Blockchain uses cryptographic methods and algorithms to record and sync data across the network. Blockchain can also be represented as a database form with decentralised security and synchronisation (Peters & Panayi, 2016). The data inside a blockchain is validated by the parties inside the network using a consensus protocol (Yli-Huumo et al., 2016), then combined into a 'block' of information which forms a chain of preceding validated blocks of information (Nofer et al., 2017), therefore called 'blockchain'. This process renders it impossible to tamper or modify the information entered into the records, which has the potential to be adapted into systems with a high degree of privacy and security.

Blockchain technology possesses various novel characteristics that make it an enabler of the next generation of Information and Communications Technology (ICT) (Kogure et al., 2017), promising innovation at every level, starting from strategic, organisational, economic, informational, and technological (Ølnes et al., 2017). Organisations from various fields and levels have tried to experiment and implement this technology with the hope of optimising the ICT structure. These fields range from data management, finance, Internet of Things, Cyber

Security and many others (Zile and Strazdina, 2018 and Rawat, Chaudhary and Doku, 2019). In government, many organisations have done research and pilot projects related to blockchain technology to build effective, efficient and trustworthy government through transparency and synergistic networks.

1.4. How blockchain can enable the Payment ID

Blockchain technology's potential in enabling existing business processes can be used as the basis for making Payment ID. By using blockchain technology, Bank Indonesia as a public institution can provide services that can ensure the security of personal data, both for the public and for industries in need. Industries can use public information as long as it obtains consent from the public following the applicable regulations.

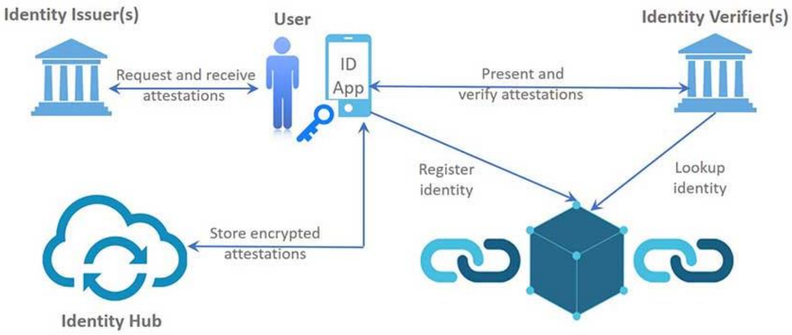


Figure 1.1 . Blockchain based digital identity illustration,

by Businessworld.in, 2018, http://www.businessworld.in/article/The-Future-Of-Identity-Is-Self-Sovereign-And-Enabled-By-Blockchain/29-10-2018-163096/.

On the other hand, the public can also easily control their personal data according to their needs and consent. On the public side, they can easily register themselves on the payment system platform and fintech without filling the KYC data as it has been accommodated by Payment ID. In comparison, industry players can do KYC efficiently and safely without violating the data owner's privacy and consent. The use of blockchain technology is expected to reduce the risk of unauthorised access through strong encryption and auditable temper-proof data.

1.5. Problem Statement

Blockchain technology is an innovation that can improve various industries through its main characteristics: Decentralised, Secure, Programmability, Auditability, Transparency, Immutability. These characteristics are also why the government of various countries is interested in conducting research and piloting projects to improve their business process, as Calvin and Duan (2020) stated. Following that research, the study on the domain of blockchain-based digital identity specifically used for the government's payment ecosystem is still prevalent. Most blockchain research related to the financial field focuses on the transactional part, such as the P2P payment (Xu et al., 2016; Zheng et al., 2016; Lindman et al., 2017) and cryptocurrencies and online payments (Holub and Johnson, 2018; Iansiti and Lakhani, 2017; Tang et al., 2019). On the other side, the study of digital identity mostly focuses on researching the technology design and how it can enable the self-sovereign identity (Maesa and Mori, 2020; Alen, 2016; Tobin and Reed, 2016; Lee, 2017). None of the research above discusses how blockchain-based digital identity can impact the payment system and examine its socio-technical changes within the ecosystem.

Although it seems promising how blockchain can enable digital identity management for the government, especially in administering the payment system, challenges still lie, untouched by any studies. Several issues need to be addressed before the government can further implement such technology: the suitable type of blockchain architecture, its impact on the current payment ecosystem and stakeholders, how the system will be governed, etc. This study aims to fill the gap of those questions to find the suitable governance framework of blockchain-based PaymentID.

1.6. Research Objective

Given that blockchain technology is a rapidly evolving technology, organisations need to devise a governance framework to manage the implementation of this system to take advantage of its development and mitigate the impending risks that may arise with this development. Following that idea, this study is an explorative study that aims to find a suitable approach to implement and manage the blockchain-based digital identity for payment systems in Indonesia from the organisational and governance perspective to help stimulate the implementation of this technology. Firstly, this study aims to find a suitable blockchain type to fulfil the requirement of the payment system digital identity. This study will also discuss the implication of blockchain technology to the payment ecosystem, especially for the opportunity and risk of implementing the technology and finding the suitable data governance approach to manage the data within the blockchain-based digital identity.

1.7. Research Question

Further studies will be carried out with the following research questions (RQ):

“How can blockchain-based digital identity be managed for the Payment System in Indonesia?”

This main question will be answered by addressing the following sub-research questions (SQ):

1. What are the Payment ID’s core requirements as the primary digital identity in the Indonesian payment system?

   -The Payment ID’s core requirements need to be captured as the primary goal of implementing this system. This data will be the baseline on the technology’s minimum functionality and serves as a reference for answering the following SQ.
2. What type of blockchain architecture is suitable for the PaymentID?

   -The SQ will be answered by comparing several blockchain-based digital identity components and determine the most suitable architecture solution for the PaymentID based on the answer from SQ1 and SQ2
3. How will the actors and stakeholders in the payment ecosystem be impacted by implementing the blockchain-enabled PaymentID?

   -This SQ will discuss how the new blockchain-based digital identity will impact the payment ecosystem, the benefits, and the risks in adopting this new technology.
4. What are the required governance process that needs to be formulated for PaymentID?

   -This SQ will discuss the required governance process governance process that needs to be formulated by the stakeholders to ensure that PaymentID can can fulfill the needs of its stakeholder as blockchain-based digital identity

2 Research Methodology

2.1 Research Flow & Methodology

This research will be conducted in a case study. Based on Yin (2014), a case study is carried out to investigate a contemporary phenomenon in real life where the boundaries between the phenomenon and the context are still unclear; hence, various sources and evidence are needed to study it. This study will explore the role of digital identity in the payment system and blockchain's applicability in the payment ecosystem.

Data collection is carried out through literature reviews and interviews with actors in Indonesia's payment ecosystem and blockchain technology. The literature study results and initial interviews will form the design concept of a blockchain-based digital identity in the payment system. This design concept will then be displayed to users and market players in the payment ecosystem to see its relevance to current business processes. After that, the results of the two interviews will be collected and used as the starting material for discussions about the impact of blockchain technology analysis on the payment system. The proposed research will follow the logical process flow depicted in figure 2.1.

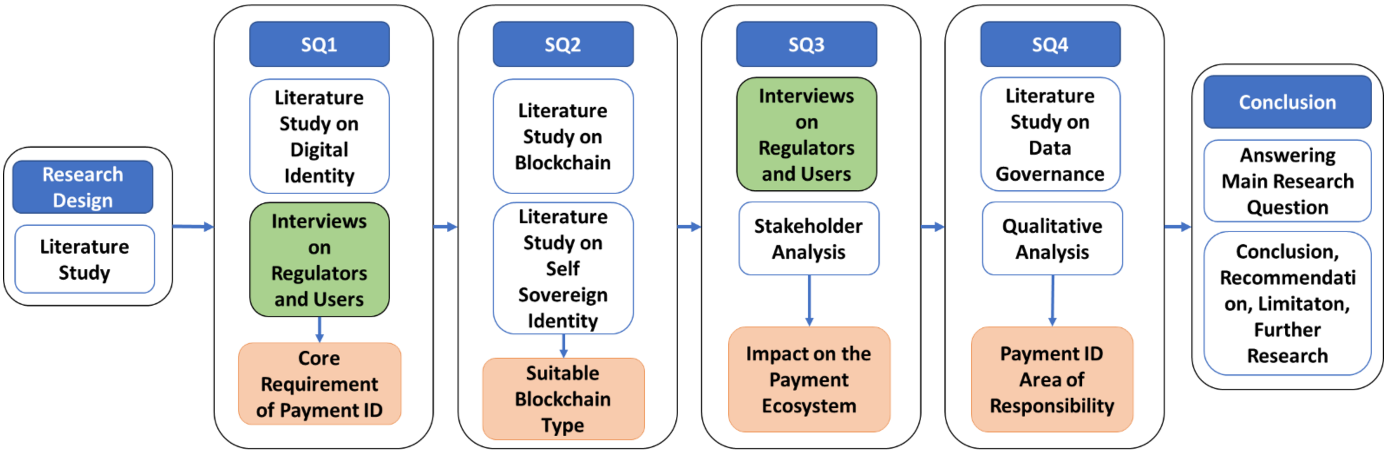

Research Design
Literature Study
SQ1
Literature Study on Digital Identity
Interviews on Regulators and Users
Core Requirement of Payment ID
SQ2
Literature Study on Blockchain
Literature Study on Self Sovereign Identity
Suitable Blockchain Type
SQ3
Interviews on Regulators and Users
Stakeholder Analysis
Impact on the Payment Ecosystem
SQ4
Literature Study on Data Governance
Qualitative Analysis
Payment ID Area of Responsibility
Conclusion
Answering Main Research Question
Conclusion, Recommendati on, Limitaton, Further Research

Figure 2.1 Research Flow Diagram

1. To answer SQ1 and SQ3, semi-structured interviews will be conducted early to capture the current state of Indonesia's payment system and the future state that Bank Indonesia wants to achieve through the implementation of Payment ID. The key concepts and core characteristics of the future payment system state will be analysed through literature study on

ecosystem theory and other related research such as stakeholder theory to provide the required theoretical background.

2. SQ2 will be answered by conducting a systematic literature study to find the empirical evidence and theory that can help construct a suitable approach based on the requirements of SQ1. The literature will be derived from the related domains: blockchain, and self-sovereign identity.
3. Stakeholder analysis will be used to answer SQ3 based on the initial interview result. Stakeholders will be categorised based on their role within the payment ecosystem and mapped using the interest-influence matrix. Following that, the impact analysis will be conducted by analysing how the stakeholders will be impacted based on the four aspects: cost, benefits, risks and opportunities. SQ3 will result in the impact analysis of implementing blockchain technology for payment ID.
4. Lastly, a Literature study on data governance and qualitative analysis will form the data governance framework based on the stakeholder analysis on SQ3. The data governance framework will be in a data stewardship diagram and use case model example.

2.2 Data Collection

The required data for this study derived was from the **literature study** and **semi-structured interviews**. Semi-structured interviews will be conducted in structured questions and supported with in-depth follow-up questions related to the initial questions (Given, 2008). To ensure the same perception of the research approach, an informal preliminary discussion and interviews will be conducted with Bank Indonesia involved in developing the Payment ID through email and online interviews. Other participants include users of the payment system in Indonesia, such as banks and payment system fintech.

Table 2-1 Sub-research question and required data

No.	Sub Question	Required Data	Chapter
1.	What are the Payment ID's core requirements as the primary digital identity in the Indonesian payment system?	• Interviews with Bank Indonesia	Chapter 5

No.	Sub Question	Required Data	Chapter
		• Payment System Regulations documents • Literature studies on digital identity • Literature studies on the payment system	
2.	What type of blockchain architecture is suitable for the Payment ID?	• Literature studies on blockchain • Literature studies on blockchain-based digital identity	Chapter 5
3.	How will the actors and stakeholders in the payment ecosystem be impacted by the implementation of the blockchain-enabled Payment ID?	• Answer from SQ4 • Literature studies on blockchain-based digital identity • Interviews with Bank Indonesia • Interviews with payment system fintech	Chapter 6
4.	What are the required governance process that needs to be formulated for PaymentID?	• Literature studies on blockchain governance • Literature studies on blockchain-based digital identity • Interviews with blockchain experts • Interviews with Bank Indonesia	Chapter 6

2.3 Literature Study

The initial method used in this research is SLR or systematic literature review to analyse the problems that occur and formulate solutions. Keele (2007) mentioned some advantages of the SLR method, namely: (1) summarising evidence concerning a particular phenomenon or technology; (2) identify existing research and look for gaps as a basis for further research; (3) to form the basis of a framework for conducting new research.

SLR can also check empirical evidence that can support or refute a hypothesis and create new hypotheses. In this research, the literature is taken from three main topics: digital identity, blockchain and finance. Technology implementations related to digital identity and blockchain will be collected and compared to find their strengths and weaknesses to propose technology implementation solutions. This literature review will be combined with digital identity requirements in the payment ecosystem in Indonesia to determine solutions that can be implemented for digital identities in the Indonesian payment ecosystem and how they are managed.

A literature study will be conducted to understand the grounded theory related to the topic and the implementation approach of blockchain technology. The approach can be described as follows:

1. **Utilising scholarly search engines** such as google scholar, Scopus, and ResearchGate to obtain the related research data.
2. **Utilising general search engine and Bank Indonesia website** to gather the industry overview and regulation related to Indonesia’s payment system and digital identity.
3. **Identifying the main keywords** and the related keywords that correspond with the topic, for example: “Payment System”, “Blockchain”, “Governance”, “Digital Identity”, “Security”, “Privacy”, “Self-Sovereign Identity”. The keyword will be used combined with other relevant keywords on the google scholar search engine.

4. **Filtering articles** by using the exclusion criteria on the scholarly search engine and reading the overview of the article (abstract, introduction and conclusion).
5. **Finalising the selected articles** by reading through the filtered article and putting the most relevant articles as the reference.

2.4 Semi-structured interview

The Semi-structured interview will act as the primary data collection based on Indonesia's payment ecosystem and capture insights from related stakeholders about the possibility of the blockchain-based digital identity for Indonesia's payment system. The interview participants comprise several actors and stakeholders related to the payment system in Indonesia and blockchain practitioners. There will be 5-10 respondents representing five different parties: regulator, bank, payment system fintech, blockchain consultant, and payment system users. This participant selection enabled the data triangulation to obtain a holistic view of the blockchain-based digital identity technology. The respondent will be asked for their consent before the interview, and the data collected from the interview will be anonymised to ensure the respondent's privacy. The respondent selection will be made by following these criteria:

1. **Affiliation**: The affiliated party that is actively engaged with either payment system activity and blockchain implementation in Indonesia will be considered as the target respondent:
    1. Bank Indonesia (as the payment system regulator),
    2. Payment System fintech.
    3. Organisation that has already implemented blockchain technology, especially for digital identity and;
    4. Blockchain consultant
    5. Payment system users
2. **Respondent Experience**: The targeted interviewees are preferably people with high experience in either payment system, digital identity, and blockchain implementation in their respective organisation. Furthermore, we expect 2-3 minimum years of experience for the blockchain part since this technology is still in the early diffusion phase in Indonesia.

Table 2-2 Interviewee List

Interviewee	Type	Institution	Role
R1	Regulator	Bank Indonesia	Data development and management Division - Payment System Policy Department
R2	Regulator	Bank Indonesia	Digital data development and big data analytics Division – Department of Statistics
R3	Regulator	Undisclosed Organization	Security Analyst
B1	Commercial Bank	Multinational Investment Bank	Client Lifecycle Management Analyst
B2	Commercial Bank	Indonesian State -Owned Bank	Security Engineer
F1	Fintech	Major Ride Hailing Fintech Company	Director
F2	Fintech	E-Wallet Fintech Company	Head of Fraud Management
F3	Fintech	E-Wallet Fintech Company	Product Manager
C1	Blockchain Consultant	Blockchain Consultant Company	CEO
C2	Blockchain Consultant	Blockchain Consultant Company	Senior Partner
U1	User	Payment System User	Payment System User

E1	Digital Identity Expert	TU Delft	Professor of GovTech & Innovation in Digital Government Ecosystems

3. **Interview Protocol:**

   The protocol in this interview uses the framework developed by Castillo-Montoya (2016). This framework focuses on four main aspects, namely:

   a. Determine the alignment between interview questions and research objectives

   b. Create inquiry-based conversations

   c. Receive and refine interviews based on feedback

   d. Become a protocol line interview

   The procedures carried out in the interview process include:

1. Inviting the respondent to be a participant in the interview through formal and informal messages. It contains a brief explanation of the research and why the background and experience of the respondent plays an important role in the interview process.
2. Planning the interview by preparing the date and video call link either using Zoom or the Microsoft team. Next, conduct brief research related to the respondent's institution background to gain a more specific understanding of the insights provided by the participants.
3. Asking permission to record the conduct of the interview. Respondents will be asked for their consent before conducting the interview, and the data collected during the interview will be anonymised to ensure respondent privacy.
4. Detailing the background and the expected goals of the research to the participants. The explanation will also cover the basic concepts of Blockchain technology, such as its main characteristics and approaches to its implementation in various industries. The interview questions will initially be developed in English; however, to ensure that respondents understand the questions and avoid miscommunication, the interview questions will be translated into Indonesian during the interview. Furthermore, the interview will be recorded, transcribed, and translated into English.

5. Recording important information and insights from participants. Followed by follow-up questions to clarify or dig deeper into the key aspects explained by participants.

2.5 Coding and Data Analysis

The results of each interview are stored in a separate document, then transcribed one by one. Documents in Indonesian are also translated into English. This translation is not translated literally, but according to the context being discussed, this is done to avoid syntax errors and redundant information. The transcription and translation results were then reviewed again for final validation of the raw data interviews. After that, all the transcribed documents are loaded into the ATLAS.ti application for the coding needs. In the ATLAS.ti application, the transcribed documents are divided based on the interviewee categories, namely: regulators, banks, PJSP, users and experts. The coding process is carried out in two phases. In the first phase, to extract the content from the interview, open coding was carried out. According to Friese (2014), open coding is the initial stage to refine raw data into concepts. This makes open coding suitable for explorative research such as this research. When conducting the open coding, every sentence or statement related to digital identity and blockchain is highlighted and assigned a code that describes the statement. This activity was carried out on all text in the raw data interviews. The results of the coding at this stage are still explorative and unstructured. So that more coding process is still needed in the second phase.

In the second round of coding, similar codes are combined and renamed. Some codes deemed redundant are also deleted, and their quote will be assigned to the closest related code. With the tools provided by ATLAS.ti, the number of occurrences or the significance of a code can be easily seen, thus simplifying the process of code combining. After that, the categorisation was carried out. This categorisation is done hierarchically in the sense that grouping is done multiple times with different levels of detail, with the top of the hierarchy being the main topic of this research. Following that, the main categories on the top hierarchy are The Driver of PaymentID Development, Challenges in PaymentID Development and Potential Impact of Blockchain-based Digital Identity. The results of the second stage of the coding process are also visualised into a network diagram to facilitate the coding and analysis process.

2.6 The Goodness of Measures

2.6.1 Triangulation

Triangulation is needed to ensure that the research conducted is valid. Based on Yin (2009), four aspects of triangulation can be used to provide research validity: data triangulation, methods triangulation, researcher triangulation, and theory triangulation. In this regard, the theory triangulation was not carried out in this research because of the nature of the study. The research is conducted as exploratory research to explore the nature and impact of a phenomenon by performing a semi-structured interview to better understand the existing problem within the payment ecosystem. In contrast with theory triangulation, this research did not combine different theory angles to explain a specific phenomenon. On the other hand, researcher triangulation cannot be carried out because of the limited number of researchers, which is only the writer. In this regard, two of the triangulations were carried out in this study to ensure that the research still has the validity:

1. Data Triangulation: The data collected comes from several different sources; the primary data source used the results of several interviews, while the primary data in this study was collected from diverse literature studies, regulatory documents, and guidelines.
2. Respondent Triangulation: Based on Maimbo & Pervan (2005), triangulation can be carried out on respondents based on their provided perspectives. Several respondents from both the same and different backgrounds were given the same questions to obtain a more holistic perspective and increase the reliability and validity of the research. Furthermore, this triangulation also used to minimize the bias given the limited number of the researchers.

2.6.2 Reliability

Reliability can indicate whether the methods and instruments used are stable and consistent (Sekaran & Bougie, 2016). One method used to improve data stability is to perform a multiple-translation method in data processing. The interview questions will initially be developed in English; however, to ensure that respondents understand the questions and avoid miscommunication, the interview questions will be translated into Indonesian during the interview. The interview will be recorded, transcribed and translated into English. In the coding process, some of the transcribed results will be checked for relevance to the intended context; if there is a difference in meaning, the script will be translated back into Indonesian and find the equivalent sentence according to the English language. Some of these processes are also reconfirmed by respondents to obtain reliable and relevant quote results with the context they convey. The method is quite time consuming and is expected to increase the reliability of the data collected in this study.

3 Digital Identity

Identity, in general, refers to the verifiability of a person to answer the question on ‘Who am I?’. It contains characteristics that make an individual or a person unique and different from the other entities (Olsen and Eric, 2016). In the digital environment, identity can be seen as a set of properties that can define an entity. Windley (2005) stated that one primary purpose of a digital identity system is to authorise a subject for particular actions. For example, when a person or a subject wants to access resources such as data, they should present credentials or proof that they have the right to assert that a particular identity belongs to them.

The rise of digitalisation has changed the way people do business. The need for high availability and reliability of individual records have caused Digital Identity to become a primary need for almost every business. Digital identity is a crucial element of doing business, especially for compliance and customer due diligence (CDD). Digital Identity, in short, is a set of digital records that represent a user or an individual. The data in these records are managed in a structured format by the entity providing the information and ensuring its validity (Ayed, 2014).

3.1 Properties of Digital Identities

The following are four properties commonly found in the current development of digital identity based on several studies:

1. **Entities** : By definition, entities are objects that exist independently. It is a set of digital records representing a user or an individual: In short, a person’s digital identity is a digital representation of that person with various kinds of notes and evidence to prove that he is who he is. Entities in a system can also be represented as the smallest unit of an object that can be identified and distinguished from other objects. This entity can represent an individual, an organisation or a component of the system itself. Sharman (2011) divided entities in a digital identity management system into three categories, namely: “Locally Installed Identity Agents” (Local IdA): identity agents that are installed on devices owned by users, which can be on personal computers, laptops or

smartphones. (2) “Remote Identity Agents” (Remote IdA): an identity agent on the network that has its own public key and private key. This entity is managed by parties that store user credentials such as financial institutions, universities, etc. (3) “Relying Parties” (RP): or parties that depend on digital identity services. This RP could be an online service provider used by users in their daily activities. In the real use case, a user with a device that has a Local IdA will make a service request to the RP. Furthermore, RP will communicate with Remote IdA to perform user verification. Remote IdA will send a confirmation message to the RP. When the verification process is successful, the user will receive authorisation to be able to use the services of RP.

2. **Attribute** : Attributes are types of data used to identify entities. This usually consists of two aspects (Zhang et al., 2008); who you are and profile:

A. Who You Are: A unique identity that is owned only by the individual. This aspect can be anything such as physical form, unique items including information and knowledge that only belongs to the entity.

B. Profile: A description of an entity that can describe who the entity is after this entity is verified. It also includes the entity’s rights and accesses. Some facilities exist in digital service providers.

3. **Lifecycle** : Clark et al. (2015) noted three general stages passed by digital identity, namely: registration, where there is a creation of a digital identity and a validation process for that identity; issuance of credentials or documents stating that the identity is the property of a certain person and the last is authentication for the use of services on the system.

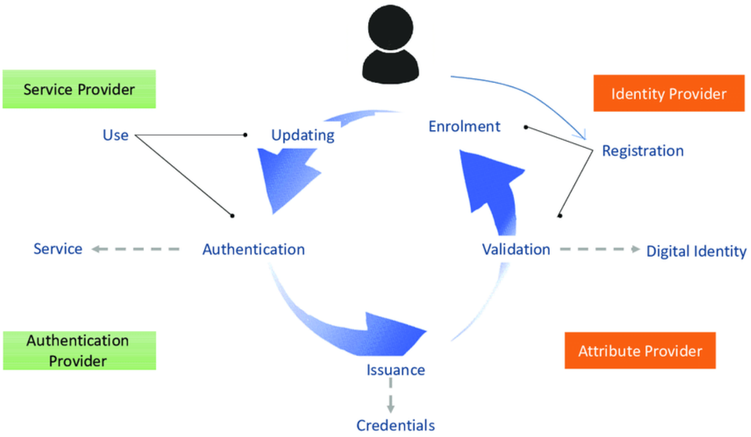


Figure 3.1 Digital Identity Life Cycle.
Adapted from: DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network by Kassem et al.

A. **Registration**: The registration process has two processes at this stage: registration and validation. In the registration process, creating a digital identity is carried out simultaneously with the recording of the main attributes of the user who has registered himself. The main attributes recorded by the system can range from biometric data such as fingerprints to textual and numeric data such as name, place of birth date, email home address, and others. After the user claims the data he submitted, the identity will be validated to ensure its validity. These data will be checked based on evidence in the real world, such as checking data at the civil registration office and other supporting documents such as passports.

B. **Publishing**: After the registration process, the issuance process will be carried out so that later this digital identity can be used by users. This published digital identity is electronic and stored in the issuer database. To use it, users access it electronically under the settings of each digital identity service provider. Depending on the issuer, it can be embedded into a device the user can physically carry, such as a smartcard or token. In addition, users can also access digital identities by installing certain software on their gadgets.

C. **Authentication**: Once a user is registered and has credentials, the user will be authorised to access the facilities provided by the service provider. To ensure that specific users have access to specific services, they must go through the authentication process. At its most basic, this authentication process confirms the identity - that the user is the person they claim to be. A familiar example is providing a username and password. Another case is the multi-factor authentication method; thus, apart from using a username and password combination, users are also asked to input the code from their token or gadget when logging into a system. After that, users can use services provided by service providers, such as transferring funds to mobile banking users.

4. Policies: A set of rules used by system owners to regulate and manage the use of digital identities. It also determines the requirements for digital identity to access and use the information resources available in the system. This requirement is made by considering business needs, information security needs and applicable laws or regulations.

3.2 Authentication Types

Garfinkel and Spafford (2003) stated that the existing computer systems are all secured by two main activities: identification and authentication. The relationship between these two processes is unique; on the one hand, identification is an activity that involves providing non-personal information from the user to the system administrator whose function is to determine whether this user is a registered user on the service provider's system. On the other hand, authentication generally contains sensitive and confidential information because it relates to the verification and validation process on whether this user is a user as he claims. When viewed from a broader scope, in the access control section, three main activities play an important role; the first is identification, followed by authentication and authorisation. In the context of security, these three things need to be operated independently because if an error occurs, it can cause fatal problems (Auernheimer and Tasi, 2005). Of the three aspects, authentication is the component that causes the most problems because it has a high-security risk compared to the other two aspects (Pernul, 1995).

According to Menkus (1998), the authentication process can be divided into three main types of processes:

a. **What the user knows**: An authentication method based on the user's knowledge; this could be confidential information known only to the user himself. This form of authentication is also commonly known as knowledge-based authentication. The most common form of authentication for this type, for example, is the personal identification number (PIN) at banking ATMs and passwords on internet accounts. PIN is an authentication method containing numerical digits commonly found in banking users, especially if they want to make transactions through bank ATMs. Users are required to memorise their secret PIN and enter it on an ATM or credit card EDC when they want to make a transaction. The bank will authenticate and provide authorisation if the pin entered by the user is the same as the pin registered by them.

Besides PIN, using a username and password combination is an authentication method widely used in various services, especially on the internet. Even so, usernames and passwords have a high risk of being stolen. This method is increasingly being abandoned, especially for high-risk application services such as financial application services. A more sophisticated password method is the OTP or one-time password, which requires users to request a new password when they are about to access a service. Usually, the OTP method is made possible by using other tools such as smartphones or physical tokens as a medium for receiving OTP responses at user requests to the server.

b. **What the user has**: A form of authentication that relies on objects or systems owned by the user which function as an irreplaceable tool in the authentication process. Some examples include:

   i. Smart Cards: Smart cards, often called ICC (Integrated Circuit Cards), are made of plastic cards the same size as credit cards in which there is a silicon chip called a microcontroller (Li et al., 2013). This card usually has various functions, not only as an identity card but also as a payment card or an agency membership card. This smart card has an encrypted storage capacity capable of storing passwords.

   ii. Tokens: Physical tokens can contain chips with functions that vary from very simple to very complex, including several methods of authentication. The simplest token does not require a connection to a computer. Some tokens have a physical appearance; in this case, the user only needs to authenticate by inputting based on the number displayed to gain access to the digital identity; the number that appears on this token can also be referred to as an OTP. Another form of token that has become widely available over the years is two-factor authentication (2FA) using a mobile device or smartphone that allows issuance of OTP via voice call, SMS, or Unstructured Supplementary Service Data (USSD) (Panjwani, 2010).

iii. Public Key Cryptography: In cryptography, the public key infrastructure (PKI) is a means of authentication, data security and anti-denial tools. Technically, PKI is an implementation of various cryptographic techniques that aim to secure data, ensure the authenticity of data and senders and prevent denial. In PKI implementation, the system will generate a key pair, namely the Private Key and Public Key. The private key is used when the user signs a digital signature or open a document addressed to the user. Other users use the public key to encrypt documents to ensure only the user who owns the private key of the public key pair can open the document (Al-Riyami and Paterson, 2003).

c. **What the user is**: A method that takes advantage of the uniqueness of the physical form and the characteristics and psychology of humans that differ from one another. Sometimes this method is also called biometric authentication. Biometric authentication systems offer programmable methods to identify measurable physiology, such as voice samples, iris recognition or fingerprint authentication. This method is widely used because each individual has a unique physiological character (Bhattacharyya et al., 2009). Compared to token-based and knowledge-based authentication methods, the physicality of biometric authentication is very difficult to imitate, which is why biometric authentication is mostly used to protect highly sensitive data.

3.3 Categories of Digital Identity Management

Identity is a representation of an entity in a particular application domain (Jøsang and Pope, 2005). Digital identity is a partial identity in digital format. For each entity, there may be one or more unique or non-unique digital identities (Modinis, 2005). The growth of the internet and online services has triggered the search for a practical, secure, and privacy-proof architecture by safeguarding digital identity and access management (IdM) (Dabrowski and Pacyna, 2008). This led to the development of a series of identity management models. In this section, the comparison between models will be made based on the following entities definition:

- User: a person or organisation who utilises the digital identity to facilitate their activities such as accessing social media, accessing particular services such as banking service, etc.
- Identity Provider (IdP): is an entity that manages the digital identity and is responsible for the digital identity lifecycle starting from the registration, authentication and authorisation. This entity records the attribute and the user's identity and may also be responsible for verifying the identity provided by the user.
- Service Provider (SP): This entity can provide services for its user as long as the user is authenticated and authorised to use the services. IdP is critical to ensure that the correct user has access to the correct services provided by the SP

1. Isolated Identity Model

This most basic model has SP and IdP components incorporated in a single system. In this case, the service provider (SP) also acts as an Identity Provider, which functioned as organising the digital identity lifecycle of the user. Until now, this model is the most common model on the internet and web services. As an illustration in figure 3.2., each pair of SP and ID stands alone and records their own digital identity data.

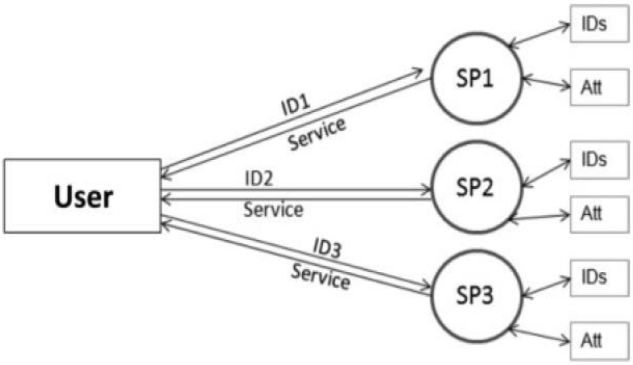


Figure 3.2. Isolated Identity Model Illustration

The drawback with this model is that users will be forced to have too many usernames, and the authentication method may be different. If users use the same username and login on each system, it will reduce their security level; if cyber-attackers can hack the system with the lowest security level, the user's username & password can be used to access other service provider systems. On the other hand, because the control of the data is not in the user's hands, the data stored by SP is also vulnerable to being misused without the user's knowledge.

2. Centralized Identity Model

Jøsang and Pope (2005) defined IdP as it becomes the central body responsible for organising digital identities that several service providers can use. Users can access multiple SPs using the same digital identity without authenticating multiple times when they have authenticated one of the SPs connected to the main IdP. This system is also known as SSO or Single Sign-On. In this model, the user is quite facilitated because he is not required to memorise many username & password combinations to access several SPs.

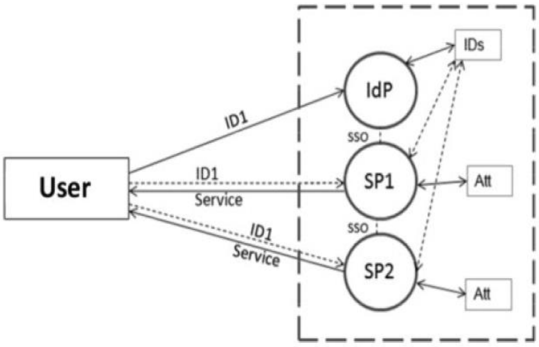


Figure 3.3 Centralized Identity Model Illustration

On the other hand, the vulnerabilities are centralised in the central IdP so that if the IdP is compromised, cyber-attackers can access the SP connected to this IdP.

3. The Federated Identity Model

Based on Chadwick (2009), the Federated Identity model is a combination of 2 or more SPs that form a federation. With this federation, users can take advantage of their credentials to authenticate and access SPs members of this federation. Authentication and authorisation between systems in one federation usually requires an agreement related to data ownership so that each SP has clear governance over their own data(Balasubramaniam et al., 2009). This agreement can also be called the Circle of Trust.

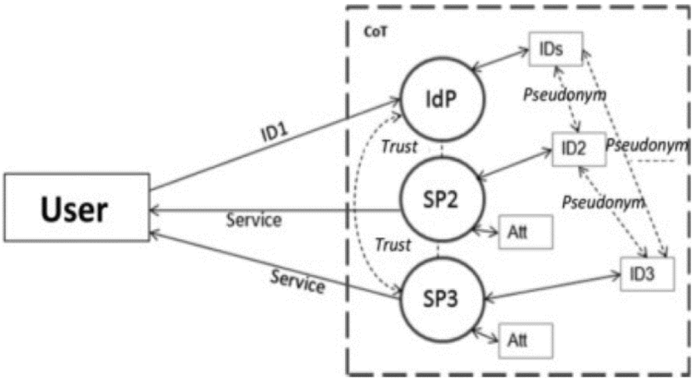


Figure 3.4 Federated Identity Model illustration

In contrast to the centralised model, SSO in this Federated model uses a pseudonym for its users. This model is commonly used in integrated systems that have many SPs and users.

4. User-Centric Identity Model

According to Jøsang and Pope (2005), this model prioritises the user in terms of controlling his privacy. This model places the user as the main actor who determines the rules in providing access to their personal information. The user can manage their digital identities to be used for several applications.

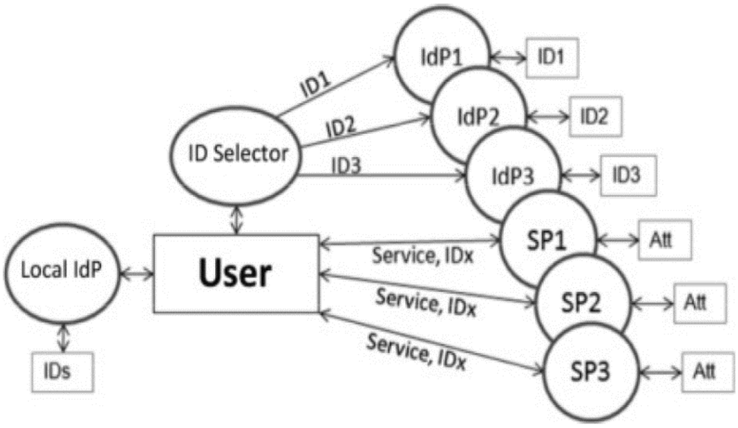


Figure 3.5 User Centric Identity Model illustration

Usually, the user can save the identity that comes from several issuers into a special hardware such as smartcards or other devices such as smartphones etc. What distinguishes this model from the federated model is that this identity is more concerned with the user than the service provider. One example of using this model is attribute-based identity. The main purpose of this model is to make it easier for users to access multiple service providers using the same identity and credentials.

5. Self Sovereign Identity Model

Based on Cameron (2005), Self Sovereign Identity (SSI) is a new concept model of user-centric digital identity that allows users as the identity holder to have direct control over their data. In the initial issuance of the digital identity, users will need a digital certificate or digital signature from the verified authority to certify that their digital identity has been verified. In the future, this digital identity will become valid and can be used for various SPs. Figure 3.6 illustrates that the user has control over their credentials on his device based on the certificates or credentials issued by the issuer. Their credentials are registered by both the user and issuer in the identity registry to ensure their validity. Whenever any SPs acting as a verifier request any certificates from the user, the user can selectively present the proof, and then the verifier can check its validity from the identity registry.

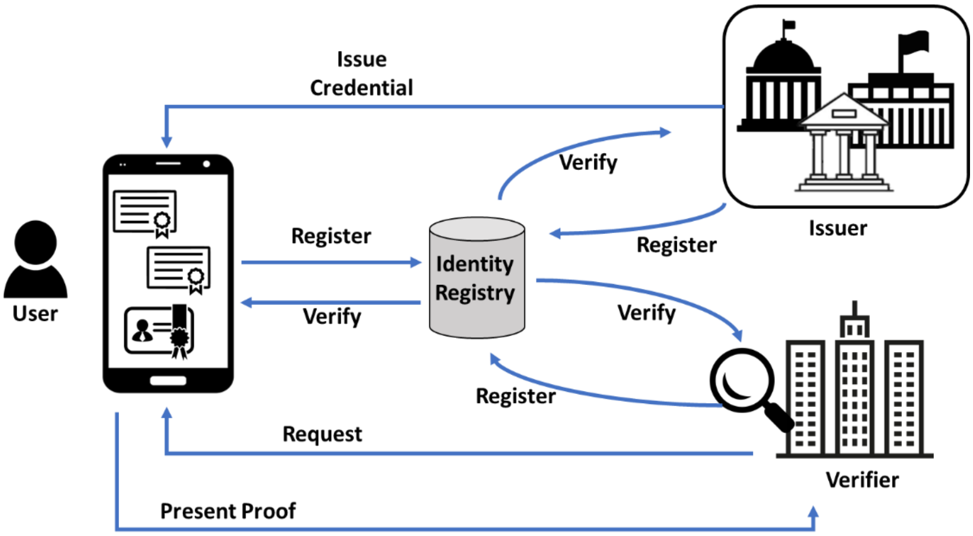


Figure 3.6 Self Sovereign Identity Model illustration

Another goal of SSI is the transparency and portability of data. Transparency refers to the user's ability to know how the data is managed and stored by the system. While portability is how this digital identity can be attached to the user and not tied to one IdP or SP. According to Allen (2016), there are ten specific principles are the main characteristics of SSI:

1. Existence: Entities do not depend on digital identity alone; they must exist and be independent of any party.

2. Control: The user must have control over their identity. They can update, hide it or reference it.
3. Access: Users must have direct access to their identity and any data related to their identity. Every data must be visible to the owner, and no other party is in the middle.
4. Transparency: The workings of the system that regulates this digital identity must be transparent, including how the data updating works.
5. Persistence: Identity must exist as long as the user wants but must also fulfil the “right to be forgotten” principle.
6. Portability: Any information related to the identity must be easily transferred and not only stored by one third party entity.
7. Interoperability: Every data contained in the identity must be easy to use anywhere.
8. Consent: Users must have consent before their identity and data can be shared on related systems or parties.
9. Minimisation: Disclosure of user data must be as minimal as possible so that parties that require certain digital attributes do not need to know other data.
10. Protection: the rights of the user must be protected and prioritised if there is a conflict with the network.

Based on these characteristics, one technology capable of realising the SSI is Blockchain technology. Blockchain exhibits several properties that coincide with some desirable traits of self-sovereignty identity. For example, blockchain provides a decentralised domain that is not controlled by any single entity. Data stored on any blockchain is readily available (portability and interoperability characteristic) to any authorised entity (access characteristic). The owner of certain data has full control and determine how the data can be shared with other users in the blockchain domain, thereby fulfilling the disclosure characteristic (Ferdous et al., 2019).

3.4 Conclusion on Digital Identity

In short, digital identity is a digital representation that contains a compilation of information indicating that a digital entity is truly owned by an individual. There are usually several properties in digital identity, namely: Entity, Attribute, Lifecycle and Policy. Digital identity is essential for users who want to carry out online activities because aspects of policy and security are used to ensure that only authorised people can carry out certain activities.

There are currently four main digital identity models widely used in the digital world, namely Isolated, Centralised, Federated and User-centric models. The most commonly found digital identity model, especially in finance, is currently the isolated identity model. On the one hand, this makes it easier for SPs to manage their own user data, but on the other hand, this model is vulnerable to cyber-attacks and reduces user control over data. The study by Mertens and Rosemann (2015) stated that people feel that they do not have control over their data with most digital identity implementation. People feel the need for transparency in digital identity management, and they also want to have complete control over their own data.

Based on this condition, self-sovereign identity (SSI), the newest digital identity model, is expected to solve the problems above. Based on several studies (Naik & Jenkins, 2020; Liu et al., 2020), the role of Blockchain technology is very important to realise the SSI model because it can provide transparency, portability, privacy and security into digital identity. Chapter 3 will further discuss how blockchain can realise this model.

4 Blockchain Technology

4.1 Blockchain Technology Overview

At first, the blockchain concept was introduced by the whitepaper from by Nakamoto (2008) as the basis for the alternative peer-to-peer electronic money transactions. The initial study discussed how peer to peer technology can work without a central authority or a bank that can regulate bitcoin transactions and issuance. The main essence of the study is how consent can occur between members of a network and ensures an audit trail that can identify every transaction that occurs therein.

In simple terms, blockchain can be described as a database that decentralized, without trust between participants. Digital assets (such as units, credit, bonds, holdings, or fundamental rights) are managed as a block list contains ordered transactions. Every and each block in the blockchain is connected using hash based on its previous block. Thus, the transaction record and history within the blockchain ledger cannot be edited or deleted without changing the entire contents of the blockchain (Xu, 2017). This makes the blockchain safe from attacks hacker. The fundamental difference with today's databases is the omission of central element; consequently, data is distributed and decentralized. It means that there is no central control unit that can check the accuracy of the information. Therefore, blockchain uses a consensus mechanism. This allows the submitted information to be integrated into blockchain only after approval (consensus). If the relevant requirements fulfilled, transactions confirmed by consensus can be tracked and secured from manipulation or forgery by third parties.

Several studies stated that the use of blockchain technology for cryptocurrency is just one of the many potentials that can be developed from technology capability (Dresher 2017; Hawlitschek et al., 2018). They stated that blockchain architecture has several advantages compared to the traditional system architecture. The difference between the traditional ledger system architecture and the blockchain architecture lies in the absence of a trusted 3rd party central node as the master record. Each node on the blockchain network has an identical copy ledger and can transact with each other without the need for a trusted 3rd party node (Hawlitschek et al., 2018; Lacity, 2018).

In this chapter some of the blockchain technology concepts will be explained followed by its implication to the development of Self Sovereign Identity. The detailed component of the blockchain technology and its concepts will be explained in Appendix C – Blockchain Technology.

4.2 Blockchain Technology Concepts

4.2.1 Blockchain Types and Taxonomies

Blockchain technology has several types to be implemented in the expected conditions. There are three types of Blockchain, namely:

a. Public Blockchain: Public blockchain is a Blockchain that anyone can access and use. Public blockchain is not controlled by any individual or organization. The ledger on the Blockchain is open and transparent. However, there are drawbacks to public blockchains, namely high operating and maintenance costs, as well as slow transaction speeds. Examples of its use are Bitcoin, Ethereum, and Hyperledger.

b. Private Blockchain or Permissioned Blockchain: Private blockchain is formed to facilitate private data exchange among a group of individuals or organizations. Unknown users cannot access this Blockchain network without a special invitation. An example of its use is on R3 Corda.

c. Consortium Blockchain: The blockchain consortium is a combination of public and private blockchains, where no single organization in charge can control the network but several predetermined nodes. This node can decide who can be part of the network and who can become a miner. For block validation, a multisignature scheme is used, where a block is considered valid only if it is signed by some of the nodes. An example of its use is on Fabric.

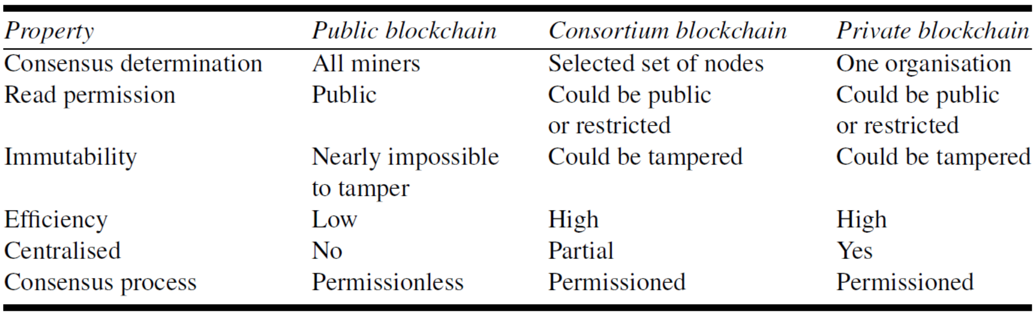
The choice of blockchain type is very important in blockchain-based application development. because there are several attributes that also affect the degree of decentralization and privacy. Various literatures categorized blockchain types based on the taxonomy in them (Swanson, 2015; Zheng et al.,2018), namely:

1. The type of consensus applied: on a public blockchain, every node in the network can participate in the validation of the new block. Whereas on a

consortium type blockchain, only a few nodes are allowed to validate the block. lastly, on the private blockchain, new block validation is controlled by only one entity or organization.

2. Types of permission to read: Every transaction that occurs on the public blockchain will be visible to the public, on the other hand, on private and blockchain consortia, permission to read this information can be granted or restricted.
3. Immutability: generally stored transactions will be distributed to all members on the network so that it is almost impossible to modify the public blockchain. On the other hand, in the consortium, the blockchain will be able to be modified if it is in accordance with the consortium majority agreement. The same is true for the organizations responsible for the private blockchain.
4. Efficiency: the time required to distribute blocks safely to each node on the public blockchain network is quite high. This will result in limited throughput and high latency. Whereas on consortium and private blockchain, this will be more efficient because only a few validators are involved.
5. Centralized structure: what distinguishes the network structure on these three blockchains are: the public blockchain is fully decentralized, the consortium is partially centralized and the private blockchain will be fully centralized.
6. consensus process: On a public blockchain, all network members will be involved in the consensus process. whereas in the consortium and private blockchain only a few licensed and certified members are involved.

Table 4-1Types of blockchain Comparison (Zheng et al., 2018)



Property	*Public blockchain*	*Consortium blockchain*	*Private blockchain*
Consensus determination	All miners	Selected set of nodes	One organisation
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralised	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

During its development, various studies stated that the public blockchain, which first emerged as a bitcoin enabler, has a large and quite active community. Meanwhile, the blockchain consortium is currently being explored to be applied to various business processes. Choosing the right blockchain type depends on the main purpose of making an application system. The literature from Roubini (2018) discusses how much political influence an application has on the level of decentralization.

4.2.2 Blockchain Characteristics

Various studies characterized blockchain differently based on their view on each of the attributes (Puthal et al., 2018; Lakhani ,2017; Treiblmaier, 2019; Drescher, 2017) hence, in general the principles of blockchain can be summarized as follows:

1. **Decentralization** (Distributed ledger and database): each block in the chain has the access to the entire records and enables the audit of the entire transaction. every node in the network can verify records without the need for a central node or a trusted third party.
2. **Transparency**: this feature is highly related with the auditability of the data. Each node in the blockhchain network will keep the same records as the distributed ledger so that every transaction that occurs is transparent. however, for permissioned type blockchains, the privacy aspect is more prioritized, therefore it will reduce transparency.
3. **immutability**: Whenever a new transaction entered into the ledger, it will be replicated to all nodes in the network and it cannot be modified. The data will be stored permanently and sorted chronologically (cannot be changed or re-ordered). By using the consensus mechanism, an invalid transaction will not be admitted, and the existing record will not be able to be deleted, modified, or copied. This feature enables the data consistency and ownership assurance.
4. **time stamped**: every record on the blockchain is time stamped. This allows for a built-in audit trail that can be accounted for for each member of the network.
5. **Programmability**: Activity inside the blockchain can be programmed to trigger automatically (via smart contracts) using a secure algorithm

without any intervention of a central third party. blockchain allows an action to be executed if the conditions are met. When compared in terms of the type of platform that implements it, Ethereum and Kadena allows for fully programmable smart contracts, this approach is quite different from bitcoin which limits the smart contract programming. However, the more complex the smart contract is, the higher the burden on the blockchain system, because it will affect data storage, throughput, and network latency.

6. **Secure**: Any additions to the blockchain are governed by secure algorithm using public key encryption, thereby reducing fraud and data corruption. Some of the studies also mentioned cryptography hashing as the means of the security measure (Gervais et al., 2016)

Given these characteristics, blockchain technology has a lot of potential beyond its application to cryptocurrency, where this attribute can provide advantages compared to traditional architectures.

4.3 Blockchain Based Digital Identity

Maesa and Mori (2020) studied that the identity management is currently silos and isolated among information providers. As a result, users are required to rely on different central providers to manage their identity data that stored in different domains. This condition force users to memorize several methods of verification and filling the same data redundantly. To overcome this, studies that supported the federated identity systems (Tobin and Reed, 2016) proposed a solution: a self-sovereign identity where the identity manager are still centralized on their own domain, but the user are allowed to use one of the identities within the domain to access all the federated ones. This allows data portability that allows the sharing of data between identity managers. although this solution can relieve users, control over their identity data is still silos and centralized in each domain of the identity manager. On the other hand, studies from Cameron (2009) propose a different solution. Identity management system is seen as a user-centered system. this can solve the privacy problems that occur in federated identity management. With this approach, the user will be responsible for their own data and not a 3rd party. The implementation of this solution is also similar to the self-sovereign identity system method offered by previous researchers, but the personal data from the user is not stored on each the identity manager instead the identity manager will be the one who request the data to the user.

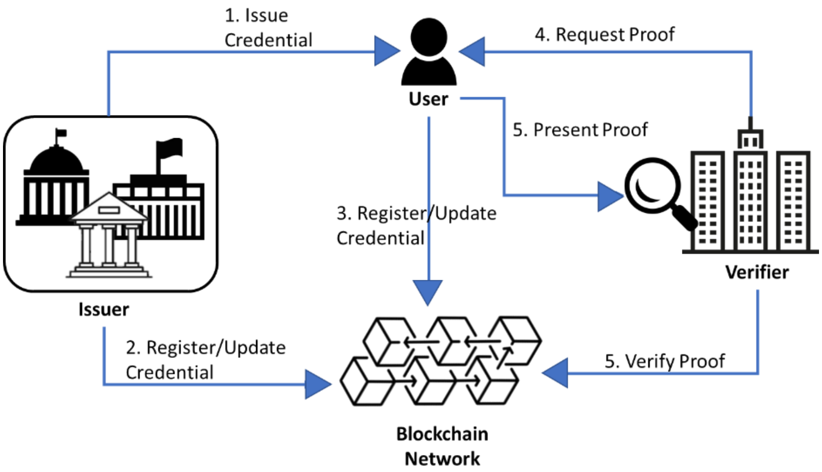
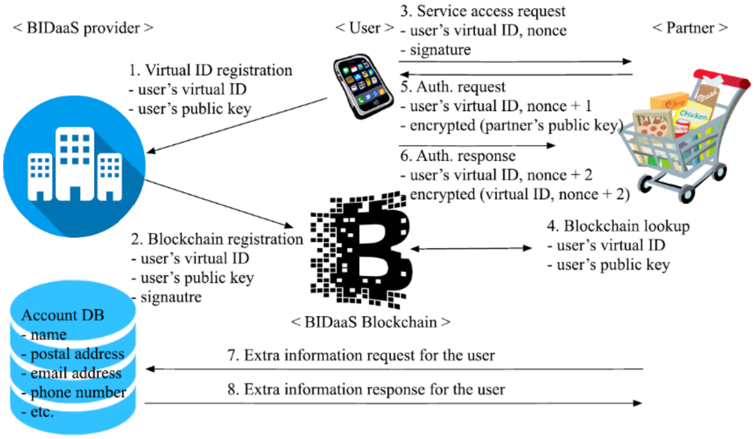


Figure 4.1 Illustration on Blockchain-enabled digital identity

Several proposed solutions for the use of blockchain based identity management have been identified by several researchers and service providers. Several studies that are considered representative of this topic include: Tobin & Reed (2016) with Sovrin, Jacobovitz (2016) with uPort, and blockchain Based Identity as a Service (BIDaaS) by Lee (2017). In Sovrin, the self-sovereign identity (SSI) system is created in the public domain but with a permissioned ad-hoc blockchain. The ones responsible for consensus on this solution are trusted miners called stewards. They are controlled directly by the Sovrin Foundation on a non-profit basis to ensure their validity. Although data can be stored in chains, they advocate storing it locally and only accessible by trusted parties via cryptographic side channels. On the other hand, the approach by uPort is slightly different with Sovrin. Uport implements its self-sovereign identity through smart contracts on the Ethereum blockchain (Jacobovitz, 2016). User has a uPort identifier which is based on an Ethreum address. User data is not stored in the chain but through the hash of the original data stored in the Interplanetary File System (IPFS).

Lastly another paradigm that also shaping the blokchain adoption for identity management presented by Lee (2017). On his paper, he introduces the blockchain enabled ID as a service (IDaaS) for the digital identity management. This approach is presented as a solution to mitigate the privacy and security risk within the current IDaaS infrastructure, where user outsource all of the identity data and authentication process to the third party. The proposed blockchain based IDaaS (BIDaaS) solution involving three entities as follows: BIDaaS provider: the one who responsible with the identity management, Partner: business or service provide that will make use of user identity; and lastly User: a registered user on the BIDaaS provider that has control over identity data that can be provided to Partner.



< BIDaaS provider >
< User >
< Partner >
3. Service access request
- user's virtual ID, nonce
- signature
1. Virtual ID registration
- user's virtual ID
- user's public key
5. Auth. request
- user's virtual ID, nonce + 1
- encrypted (partner's public key)
6. Auth. response
- user's virtual ID, nonce + 2
- encrypted (virtual ID, nonce + 2)
2. Blockchain registration
- user's virtual ID
- user's public key
- signautre
4. Blockchain lookup
- user's virtual ID
- user's public key
Account DB
- name
- postal address
- email address
- phone number
- etc.
< BIDaaS Blockchain >
7. Extra information request for the user
8. Extra information response for the user

Figure 4.2 Example of BIDaaS use case

The main idea of the BIDaaS are: everytime a user trying to register into a Partner, the Partner will request the identity data of the user to the BIDaaS provider, and the BIDaaS provider will share the required data if the user authenticate the request by the Partner. With this approach, user can ensure that their personal data is safe because they are fully responsible for their own data. Furthermore, Partner can carry out KYC more efficiently by requesting data from the BIDaaS provider without having to burden users to fill out forms.

4.4 Conclusion

In this chapter, it can be concluded that the use of blockchain technology in digital identity is represented by the SSI model, where the blockchain technology capability can meet the principles of the SSI. With blockchain technology, digital identity will become easier to control for users. Users are no longer dependent on third parties in administering their identity. In addition to that, SPs also get benefits in terms of certainty in the user authentication and authorization process. The immutability of the blockchain can make it easier for SPs and regulators to ensure that the credentials owned by the user are genuine credentials and cannot be manipulated.

In addition, this chapter is also intended to identify what technology components are contained in blockchain technology. It also explains how the selection of the design architecture for this component can affect business processes and governance in a blockchain-based system. Furthermore, the information in this chapter will be used to formulate the requirements and design architecture of a blockchain-based digital identity in the form of PaymentID.

5 Indonesia Payment System ID Case Study

5.1 Development of Payment Ecosystem in Indonesia

Based on Indonesian Regulation Number 23 of 1999, the payment system is a system that includes a set of rules, institutions and mechanisms used to transfer funds to fulfill obligations arising from an economic activity. The payment system, which is one of the pillars of support for financial system stability, has developed rapidly in line with technological developments. The development of this payment system is driven by the increasing capacity and value of transactions, increased risk, and also technological developments. A payment system is needed to facilitate efficient, safe and fast transfer of funds. The transformation of electronic payment transactions consists of several models, among others; direct transfers (electronic funds transfer), using payment cards, using electronic money (electronic money) and digital money (digital money). This is different from card-based payment system, (with ATM / debit cards or credit cards), where the value of money is stored in the card owner's account instead of their bank account.

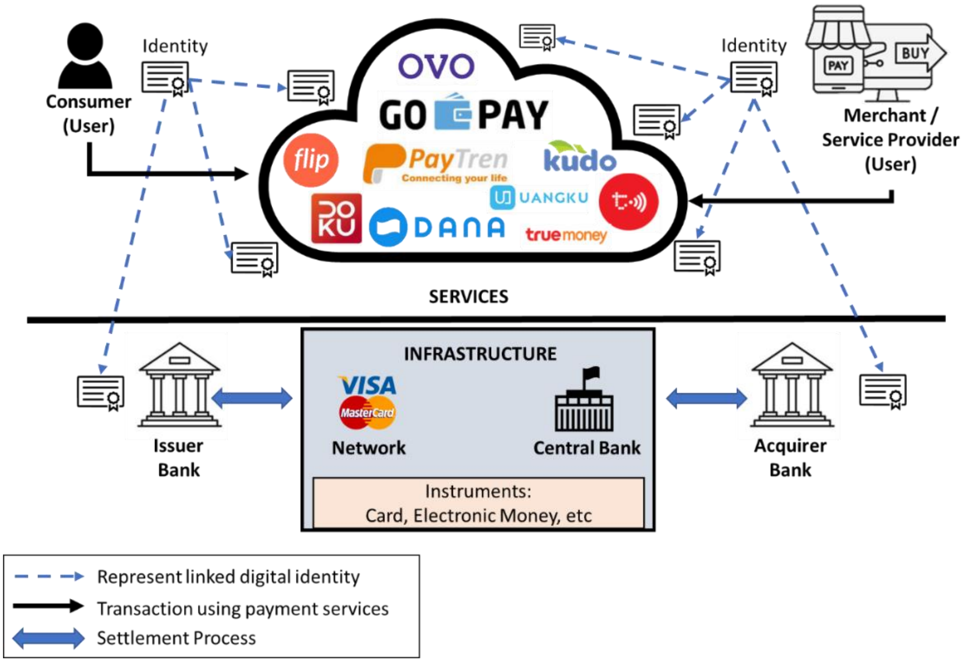


Figure 5.1 Simplified Indonesia Payment Ecosystem

Figure 5.1 visualize the simplified Indonesia Payment Ecosystem and the relationship among its main stakeholders. It is divided into the services layer and the infrastructure layer. In the services layer we can see the interaction between Consumer and Service Providers or Merchants via payment service provider (PJSP), while in the infrastructure layer we can see the interaction on the banking side where the settlement is processed. The Issuer bank or the consumer's bank transfer their money to the acquirer bank (merchant's bank) through the infrastructure provided by the Payment gateway provider (Visa, Mastercard, etc) and the Indonesian Central Bank settlement system (Clearing, RTGS, etc). In this part, the central bank role is not only as the infrastructure provider but also as the regulator that set the governance of the payment system and monitor the transaction processes. The picture also shown that Identity is present in every contact point that related with the users. In the current situation, these digital identities is still siloed, where each digital identity that is managed by PJSPs and banks is not directly interconnected.

Table 5-1 Stakeholders of Payment Ecosystem in Indonesia

Role	Description
Payment System Regulator	BI as a government institution that is responsible for supervising the implementation of the payment system
Payment System Infrastructure Provider	Switching networks that focus on providing the payment network for banks. However, as the business keep growing, the member inside this category is not limited only for the switching services but also any other service provider that can provide the network for payment system related services.
Banks	Payment system members and operators can act as issuer or acquirer for payment system settlement. -Issuer: bank that issue cards, e-money or claims that related to the consumer ownership of an account -Acquirer: bank that holds the merchant's account, may act as an organization that requires specific claims of for settling the payment
Payment Service Provider (PJSP)	Payment system member and operator, it includes bank, or other e-money and e-wallet fintech. Majority of the PJSP act as IdP and SP within the payment ecosystem
User	Person or organization that utilize payment system to make transactions
Consumer	Person or organization that spend their money to buy goods or services

Merchant	Person or organization that receive money from selling goods or services
Digital Identity Provider	IdP that has collaboration with some PJSP. They manage the digital identity of the user that registered with some PJSP
Related Authority	Government organization that may have relation with the payment system such as: - Ministry of Communication and Information Technology: carrying out government affairs in the field of communication and informatics -Ministry of Home Affairs: responsible in maintaining the citizen data (for KYC purposes by Banks and PJSP)

5.2 Development of Payment System Regulation in Indonesia

Starting from July 2009, electronic money fintech companies have begun to develop with products from server-based and chip-based banking institutions and non-bank institutions after obtaining permission from Bank Indonesia based on the Regulation concerning e-money in Bank Indonesia Regulation Number 11/12 / PBI / 2009 concerning Electronic Money.

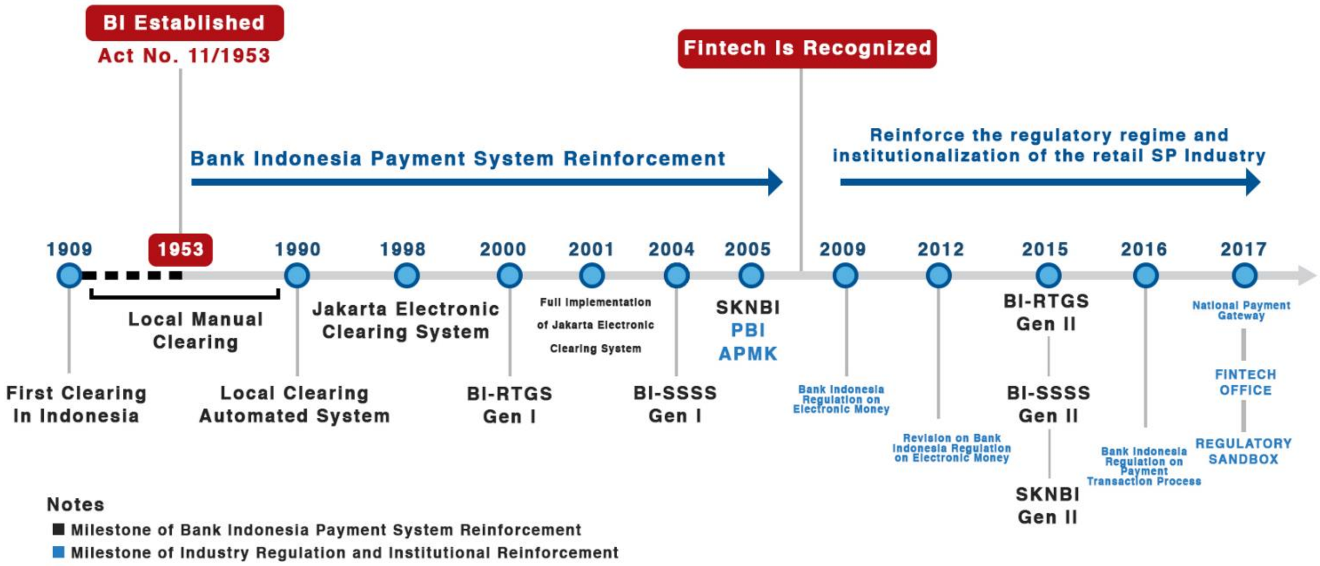

BI Established
Act No. 11/1953
Fintech Is Recognized
Bank Indonesia Payment System Reinforcement
Reinforce the regulatory regime and institutionalization of the retail SP Industry
1909
1953
1990
1998
2000
2001
2004
2005
2009
2012
2015
2016
2017
Local Manual Clearing
Jakarta Electronic Clearing System
Full Implementation of Jakarta Electronic Clearing System
SKNBI
PBI
APMK
BI-RTGS Gen II
National Payment Gateway
First Clearing In Indonesia
Local Clearing Automated System
BI-RTGS Gen I
BI-SSSS Gen I
Bank Indonesia Regulation on Electronic Money
Revision on Bank Indonesia Regulation on Electronic Money
BI-SSSS Gen II
SKNBI Gen II
Bank Indonesia Regulation on Payment Transaction Process
FINTECH OFFICE
REGULATORY SANDBOX
Notes
■ Milestone of Bank Indonesia Payment System Reinforcement
■ Milestone of Industry Regulation and Institutional Reinforcement

Figure 5.2 Payment System Regulation Timeline

To further supporting the non-cash transactions, BI has issued several regulations such as Bank Indonesia Regulation (PBI) No.18/17/PBI/2016 concerning Electronic Money and PBI No.19/8/PBI/2017 concerning National Payment Gateways. BI has also reformed the payment system regulation through the issuance of Bank Indonesia Regulation No.22/23/PBI/2020 concerning Payment System (PBI Payment System) which will take effect on July 1, 2021 (Beritasatu.com id, January 8, 2021). Since this PBI was issued until July 2021, BI will follow up on this policy by drafting more detailed implementing regulations for each type of industry to support the implementation of these regulatory reforms. In the other hand, with regard to digital identity, Bank Indonesia is issued the regulation number 19/10/PBI/2017 concerning the Implementation of Know Your Customer Principles through the continuous customer due diligence.

The latest regulations from Bank Indonesia that related with the Payment Ecosystem and Digital Identity in terms of KYC can be summarised in the table 5.2.

Table 5-2 Regulations related with Fintech and Digital Identity

No.	Issuer	Regulation	Description
22/23/PBI/2020	Bank Indonesia	Payment System Arrangement	Bank Indonesia issues a PBI on the Payment System which is expected to be able to reorganize the structure of the SP industry, as well as to provide an umbrella policy for the overall Payment System implementation ecosystem in line with the development of the digital economy and finance.
20/6/PBI/2018	Bank Indonesia	Electronic Money	This regulation regulates the operation of Electronic Money (EM) in Indonesia. it contains the principles and scope of the implementation of the EM; licensing and approval for the operation of the EM, the operation of the EM,

			including the application of risk management, information system security standards, processing of EM transactions in Indonesian territory, interconnection and interoperability, application of anti-money laundering and prevention of terrorism financing, application of consumer protection principles, implementation of EM activities, and implementation of Digital Financial Services (LKD); merger, consolidation, separation, and takeover; reporting and supervision;
19/12/PBI/2017	Bank Indonesia	Financial Technology Management	The provisions in this Bank Indonesia Regulation apply to Financial Technology Operators operating Financial Technology in the payment system sector. The scope of regulation in this PBI includes: registration; Regulatory Sandbox Provision; permits and approvals; monitoring and supervision; cooperation between Payment System Service Providers and Financial Technology Operators; coordination and cooperation; and penalty.
19/10/PBI/2017	Bank Indonesia	Anti-money laundering	This Regulation apply to Providers in the form of Payment System Operator (PJSP) other than Banks, namely Fund Transfer providers, Card issuers, electronic money

			issuers, and electronic wallet operators, as well as non-bank money exchange operators. It is required that the PJSP must carry out Customer Due Diligence (CDD) against Service Users, prospective Service Users and Beneficial Owners of Service Users, which includes identification, verification, continuous monitoring (on going due diligence). The CDD obligation here also include the procedure and the required KYC activites that should be done by financial services organizations.
22/20/PBI/2020	Bank Indonesia	Consumer Protection	This regulation concerning the awareness of business actors about the importance of Consumer Protection, increasing the level of consumer empowerment so that consumers can protect themselves, reducing the imbalance in position between business actors and consumers, eliminating the delivery of misinformation, abuse of authority, and fraud, and encouraging responsible and efficient development of innovative financial products and services
Law Number (No). 11 of 2008	Ministry of Home Affairs	Citizen Administration	Arrangement and Regulation for the issuance of Citizenship documents and data through Citizen Registration and personal data records. It also regulates the

			administration information management and utilization of the citizen data for public services and other sector development.
Ministerial Decree No. 20 of 2016	Ministry of Communication and Information Technology	Protection Of Personal Data in Electronic Systems	This Ministerial Regulation that regulates the protection of personal data in electronic systems. The Protection of Personal Data in this case includes protection against the acquisition, collection, process, analysis, storage, disclosure, publication, transmission, dissemination, and destruction of Personal Data.

5.3 Importance of Digital Identity

Digital transformation also requires stakeholders to face new challenges related to managing trust and identity between transacting parties. A financial transaction is a transfer of resources between two endpoints or entities: the original owner of the resource and the beneficiary entity. This control over financial flows depends on two important elements: Known identities of the source (original owner) and destination (recipient entity). The adoption of technologies that facilitate digital transactions has created an imbalance in the ecosystem, as the processes used to identify transacting parties still rely on names, inappropriate text processing techniques, and manual intervention. For example, in a payment transaction, the original owner and the receiving entity can be identified by account number and name, neither of which is a unique identifier that would allow efficient communication with the other banks involved in the transaction. This means that digital transactions are hampered because the parties cannot perform analog elements with the same speed, security and cost efficiency. This not only creates an imbalance that negatively affects the user experience of transactions and processing fees, but also opens up opportunities for fraudsters to exploit the system.

Banks are responsible for controlling the flow of finance between entities in the ecosystem and they do so based on a watch list of sanctioned entities issued by the financial supervisory authority. Banks analyze their transactions looking for the names of sanctioned entities to reduce fraud and other illicit transactions. The fact that it remains an analogue and text-based process means low data control, frequent false alerts, and widespread opportunities for error. As a result, regulatory controls have become increasingly stringent and often now require banks to seek additional enriched data before they can authorize a transaction. Ultimately, compliance costs have increased substantially and efficiency in financial transactions has decreased.

5.4 Payment ID Overview

The PaymentID initially developed because there is a need by the financial system authority to supervise the transaction patterns of the payment channel in Indonesia so that they can make analysis and policies that are in accordance with the conditions of digital transactions of the people in Indonesia. This idea formed because there is a shift in people's consumption patterns whose transactions are turning to digital payments, one example of which is the growing volume and value of electronic money transactions. However, the idea grew bigger than that, because the Bank Indonesia also wants to also emphasize the importance to the security and confidentiality aspects of transaction activities in the digital era. Furthermore, for the final goal of this system, it is expected that users and the public can access financial facilities more easily by using a digital identity. It is also hoped that the government can take advantage of PaymentID in order to facilitate the distribution of social benefits to the appropriate targets. With a unique and verified PaymentID for each individual and organization, Bank Indonesia aspire that its utilization can be utilized by various payment channels, from bank accounts to electronic money. This can improve payment interoperability at the individual scale more safely and securely.

5.4.1 Payment ID Initial Driver

Based on the Literature study and Interviews from the Bank Indonesia it can be identified that there are several main drivers for the development of the Payment ID:

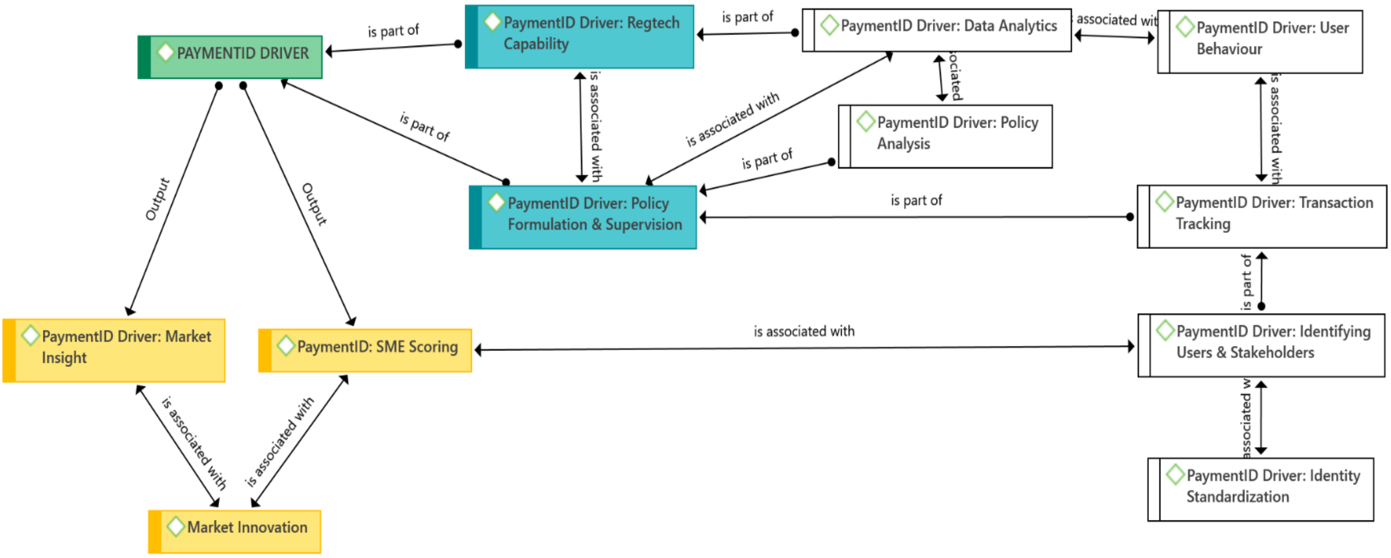

PAYMENTID DRIVER
is part of
PaymentID Driver: Regtech Capability
is part of
PaymentID Driver: Data Analytics
associated wit
PaymentID Driver: User Behaviour
is associated with
ociated
PaymentID Driver: Policy Analysis
is part of
is associated with
is part of
is associated with
PaymentID Driver: Policy Formulation & Supervision
is part of
PaymentID Driver: Transaction Tracking
Output
Output
is part of
PaymentID Driver: Market Insight
PaymentID: SME Scoring
is associated with
PaymentID Driver: Identifying Users & Stakeholders
associated w
is associated with
is associated with
PaymentID Driver: Identity Standardization
Market Innovation

Figure 5.3 Payment ID Initial Driver from Bank Indonesia

From the figure 4. The main driver of the current PaymentID development from the point of view Bank Indonesia as the payment system regulator is mainly to maintain its role as the policy maker to create a better suited policy following the rise of financial technology company that may disrupt the financial stability.

5.4.1.1 Regtech Capability & Data Standardization

One of the main driver of the PaymentID is to increase the central bank capability to response the rapidly growing financial technology company in Indonesia. This statement stated by one of the interviewees from the Bank Indonesia:

> *"there is a need for the central bank to remain relevant in its role as a policy maker. ..... there is a motivation from the regulator that this system can be utilized to monitor the rapidly growing fintech ecosystem so that it will not become an entity that is too big to fail" (Regulator, 33:26)*

This statement is in line with Arner et al., (2017) which stated that the regulatory technology (regtech) development is necessary for regulators to response the market innovation by improving the monitoring on the financial services risk and behaviour. BI believe that the current policy analysis tool is not sufficient to cover the activites that has already happened within the fintech companies. With the rise of the fintech company that is capable to run as an alternative for banks, it is expected that shadow banking activity may happen. Shadow banking is an activity where non-bank organizations can operate and act just like bank, it can provide services like storing money, transfers, giving loan etc. Shadow banking considered as unhealthy for the economics because they bear the same risks as banks, but they are not directly regulated by the financial authority, they also do not have a strong safety net, such as public guarantees deposit insurance or last resort facility lender from central bank (Collier, 2017).

> *For example, the PBOC was totally overwhelmed because it couldn't stop Alibaba and the tencent group from expanding into banking activities. because people are very dependent on them, it has come to that, so now almost all of their banking services are accommodated although they are not banks…. Fintech companies are very tempting, if you learn, starting with Payment Service, Always, they started with Payment Services. People are spoiled for their convenience, it's easy to get there without a charge which is usually charged by a bank, then they (fintech companies) can get data from there. So, they gather data indirectly, and its user data collection is so big, tha it become very exclusive for them (Regulator, 33:26)*

BI presume that by the time more user is engaged in that activity it will be too late for BI to regulate the fintech ecosystem. In order to prepare for that condition, BI considers the need of sophisticated regulatory technology that enables them to capture more data and create new analysis framework based on the new technology. To create a robust regulatory technology system, Bank Indonesia feel the need to have the big data that contains highly detailed data of the digital identity and the real time transaction data. To make things easier for the data analytics, Bank Indonesia also need data standardization. One of them is the standardization of the digital identification. Bank Indonesia realize that the digital identity data in the current fintech ecosystem is not standardized, every Banks and PJSP has their own set of digital identity data besides the obligatory KYC data that has been regulated by Bank Indonesia in PBI NO. 19/10/PBI/2017.

5.4.1.2 Policy Formulation and Supervision

In order to create a quick adapting policy, Bank Indonesia as a regulator feels the need to have highly available supervision tools that can supervise the transaction over the new technology especially in the form of digital transaction and electronic money. It is to be expected by Bank Indonesia because based on their electronic money transaction data, the amount and the usage of fintech as the means of transaction has increased significantly from 2017 (Bank Indonesia). Furthermore, as the regulatory and supervisory functions expand, Bank Indonesia feel the need of a highly available digital identity data so that they can match them with the Banks and PJSPs transaction data that has already captured by their system. This combination of data further will be used to create a profile based on the people’s attribute and spending pattern.

> *“So we want a granular identity data at the individual level so that it can be combined with the available transaction data to see people's profiles and spending patterns. With this profiling, Bank Indonesia hoped to learn more about the people’s behaviour and finding the suitable policy according to the people’s needs” (Regulator,37:8)*

Furthermore the aggregate data that gathered from the PaymentID will not only be used solely by BI, but also processed as an anonymous statistic data that will be used by another regulatory institution to support the policy making and supervision activity that is related with the people’s spending behaviour.

> *“Granular data from various sources will support a more detailed and comprehensive analysis for the needs of policy making & supervision, both within BI and for other authorities. This includes supporting technology-based surveillance” (Regulator,37:3)*

5.4.1.3 Healthy Competition and Market Insight

Besides supporting the regulatory part of the ecosystem, BI also planned to use the data analytics gathered from PaymentID to foster the growth of the SMEs and digital industry. BI realizes that with the rise of the data economy, information asymmetry is bound to happen and may cause unbalanced competition between the fintech companies. For example, fintech companies with more extensive capital may have more access to the user’s data than emerging fintech startups or SMEs. They can provide more promotion and marketing benefits to gather more users and exploit their data. This condition may cause instability to the economy, and new businesses will find it difficult to compete with big companies.

“Granular data is processed to produce useful insights as feedback for the industry, a.l. for analysis of potential business development and product development, in order to encourage innovation and healthy competition.” (Regulator,37:10)

With the comprehensive data from the users and SMEs, it is also expected that banks can make use of the data to assess the creditworthiness of the the loan activity. By analyzing the standardized KYC in conjunction with user’s or SMEs transaction profile and history BI expect banks can make a suitable decision for funding or loans.

Granular data that utilizes a unique key identifier (a.l. Payment ID) can produces individual financial information to support credit worthiness assessments. (Regulator,37:11)

5.4.2 Payment ID Market Driver

Based on the interview with banks, fintech companies and users, it can be concluded that the current digital identity used in the payment ecosystem are still using the siloed model of digital identity, it means that the same organization act as SP and the IdP at the same time. It means that the PJSP, in this case the banks and fintech companies also act as the identity provider, where they record and maintain the identity of the users by themselves and not directly connected with any other financial institutions nor make use of the Digital Identity Service Provider or external digital identity service provider.

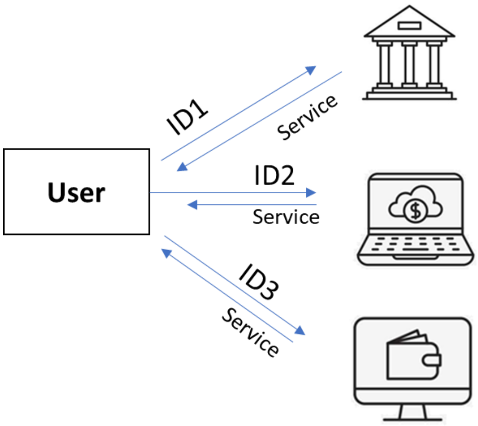


Figure 5.4 Current Digital Identity in Payment System

The banks and fintech company perceived the digital identity as the record of user that is registered on their system. The stored user data at least contains the required attribute based on Bank Indonesia's KYC policy, but they also mention that each of the company has their own policy and required data to be filled besides the initial KYC data.

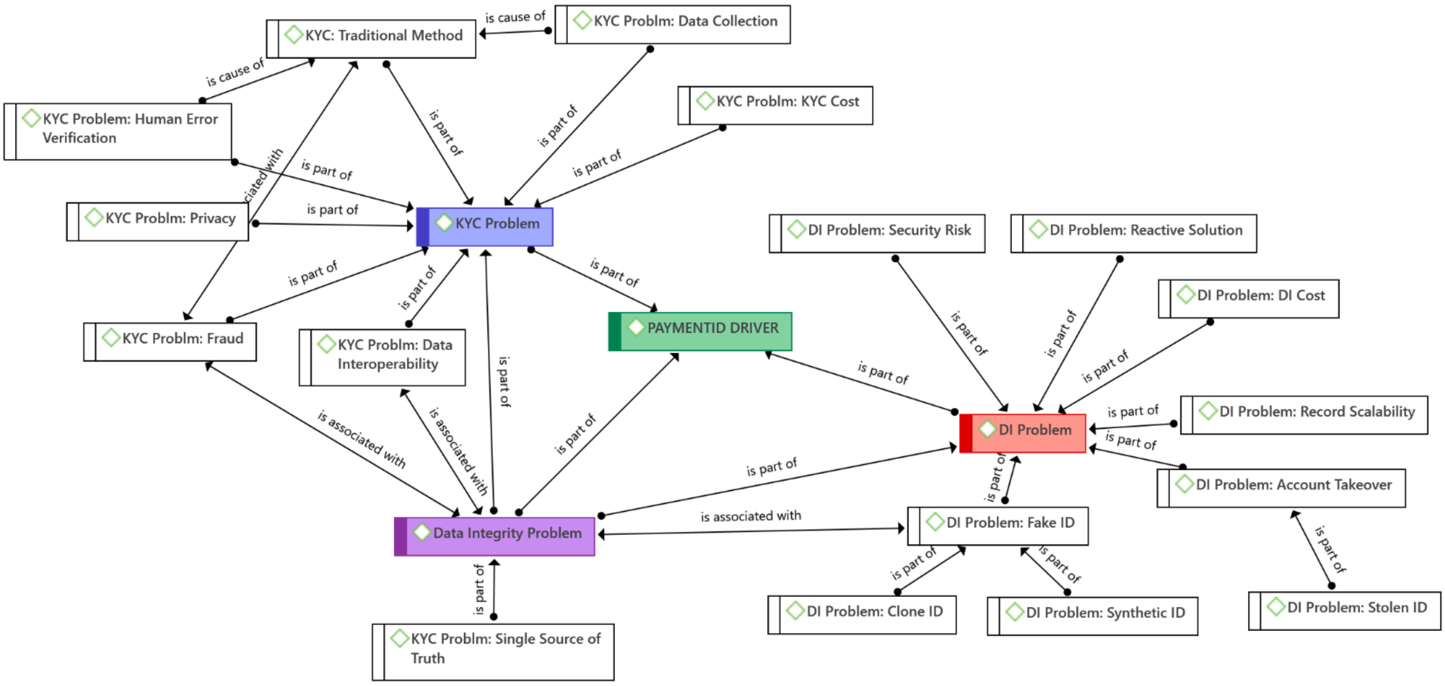


Figure 5.5 PaymentID Driver From the Market Perspective

From the market perspective, the interview from various company that provide payment system services (Banks and PJSPs) explained that there are 2 main drivers that require the creation of a new and standardized digital identity for the payment system. The first one is the problems with the siloed digital identity that they currently manage and secondly the problems with the KYC process when onboarding new users on their system.

5.4.2.1 Current Digital Identity Challenge

The current state of the digital identity approach by the banks and PJSPs are still using the centralized identity model resulting in giving less control for the user and making the users more dependent to the service providers. From the user point of view, the more account that user has in more than one service provider, user will also overloaded with memorizing different identity and authentication method. Not to mention that the centralized IdP is prone to the single point of failure, where the compromised user identity can be exploited by the irresponsible party. In order to explore more on the challenge with the current digital identity in the payment ecosystem, The details of the problems will be explained further in this section.

Security Risk

By using the centralized digital identity model, having full control of the user data is deemed beneficial from the perspective of the PJSP. It is because they can make use of the data that they have for the analytics and create new product based on the user's demography and spending pattern, however they also mention that it has its own disadvantages such as they will have to manage the risks of the user's data security all by themselves.

> For us data is very important for personal decisions for customization, promotions. But at least we know more about our consumer in a very granular level...Well of course it comes with a price. Because we act as both SP and IdP, we also have to put in more effort in protecting our user's data or digital identity, because we also don't want our customer's data to be reached, and stolen (Fintech, 36:22)

Fake ID

Further, From figure 5.2 it is explained that one of the problem with the current siloed digital identity is the potential frauds that occur due to fake identity. The fake identity firstly caused by Synthetic ID where the perpetrator creates an identity by combining the real identity and the false identity. Another form of the fake identity is by using the clone ID, where the prepetator is using a loophole in the system to create a new identity using individual data that has been previously recorded on the system. This occurrence mostly happens to the PJSP because their onboarding process is not as rigid as bank.

> The hole in the identity awareness is used for the perpetrator for them to copy, for example, the user’s account is banned because of illegal activities or suspicious activites, that account will be suspended by the ride hailing company. Now they will have to make another account if they want to do their activities such as money transfers etc. Well, the way they make that account, they will ask brokers or insiders that has the list of unused citizen identity number to create account using the same identity and attributes but with different identifier. So that they can make transfers to the bank account that has already registered with their original account. (Fintech, 36:26)

Another e-wallet fintech also stated that the digital identity creation using the synthetic ID method is commonly happen whenever they announce new promotion deals on their platform. Although the users are required to register by entering the citizen identity number and taking picture with the Indonesian citizenship card, this does not rule out the possibility that the newly registered user is using another person’s citizenship identity.

> Yes, for example, when there is an interesting promo, users use the wallet for the first user promo, but then There are so many wallets registration, so many, I think it's really that easy for that person to ask someone for an ID card to make it, or he just pays someone to take my picture, for example. So sometimes even though the person roughly matches the face in the citizen identity card, we are not sure if it is the user. (Fintech, 41:8)

It happens mostly for the e-wallet fintech companies because of 2 reasons: Firstly, The lack of awareness from the user regarding the data privacy. It causes people to lend people their identity card without paying attention on what will happen with their identity data. Secondly, the current KYC onboarding method that still has vulnerability in the human checking and the blind spot of the face recognition software that they use to identify the citizenship identity card.

Account Takeover

while other problems also include account take over, whether it is intentional or due to identity theft. This is happening because of the low awareness of users in Indonesia in protecting their personal data. Not a few users who voluntarily lend their digital identity accounts to be used by others such as friends and family. In this case there is a chance for the irresponsible people to be able to take over their account and do things beyond the knowledge of the original owner of the account.

> Educating people for not sharing OTP is really difficult, you know. There are many people in Indonesia who are still easily deceived. For example, many people are still fall for the trap when random people called and asked for an OTP claiming that they are from the administrator. This kind of activites caused a lot of take-over accounts. (Fintech, 41:11)

Besides the problem with people awareness of data privacy, the account takeover can also happen because user do not have full control of their account, where they are relied on the IdP to provide the security measure. Not only that, when there is single point of failure occur in the IdP database, the information and the digital identity of the users will be compromised and can be taken over by the unauthorised person. This is why, there is a need in the self-sovereign identity where people can take control over their own digital identity.

Record Scalability

The PJSP also mentioned record scalability as one of the current problem that they have, because they have to limit the number of attribute that they can record. One of the PJSP mention that in order to increase the security the company used to also record the device that is used by the users, however nowadays they do not do it anymore because of the scalability issues.

> Yes, in the old days it was true, in the past it was still recorded but it wasn't scalable. If we had to do this…, in the past we did record device IDs and others, but it's a bit impossible because the users are changing their mobile phone and devices quite frequently nowadays (Fintech, 36:6)

Digital Identity Service Cost

Another problem stated by the PJSP are the cost of using the Digital Identity services. Although they realize that by using the service provided by the Digital Identity service provider will be beneficial for them in terms of managing the user's identity, they said that it is over their operational budget and may cause a significant drop in their revenue if they decide to use it.

> We believe that their service (Digital Identity Serivce Provider) is very complete, actually. And indeed, if based on the testimony, it is credible, yes, and their performance is promising. However, if we look at it from an economic point of view, or the business, the price they offer is actually very, very high…. For a bank that goes digital, it might work, but for startup e-wallet fintech, it is a bit difficult because the margin is very small. (Fintech, 40:11)

5.4.2.2 Current KYC Process

Problems that occur in the KYC process for onboarding new users at Banks and PJSPs are one of the reasons why they need a standardized and integrated digital identity payment system. the KYC process which is currently being carried out separately and differently by each service provider has it weaknesses. Every service provider at least performs KYC based on the regulaiton imposed by Bank Indonesia. However, the current registration process causes a lot of effort for both PJSP and users. Every time the user registering for on the new Banks and PJSP, KYC process will always be carried out using the same process.

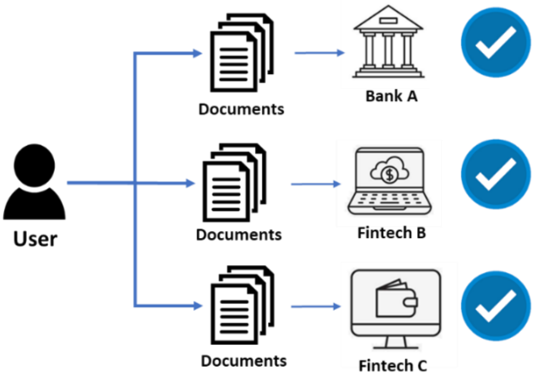


Figure 5.6 Current KYC Process

Users will have to fill out the same KYC form and submit the same required documents that they have already submit if they have already registered in another financial institutions. On the Banks and PJSPs side, they will also do the same KYC process even though another financial institution has already done that previously for the same person. The KYC Regulation that currently issued by Bank Indonesia is part of the anticipation for money laundering activities. Financial institutions are required by the regulator in this case Bank Indonesia to perform KYC to avoid customers using financial institutions for illicit activities.

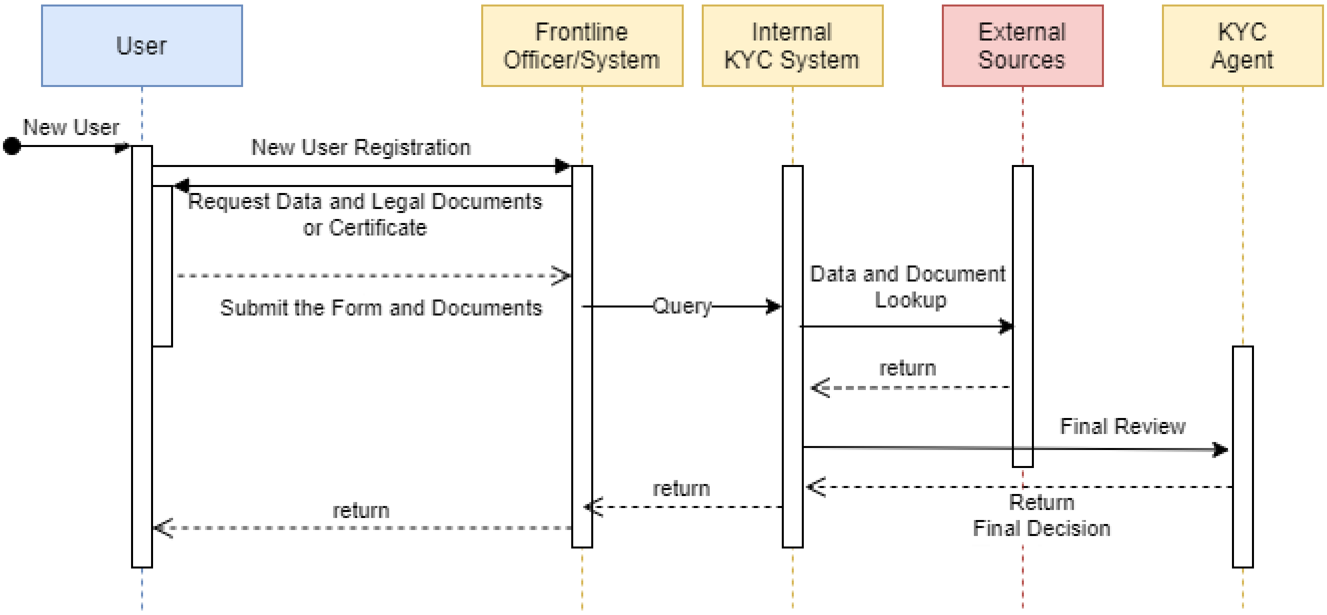


Figure 5.7 Commonly found KYC Process in Financial Institutions

The KYC process currently being carried out consists of checking documents between customers and financial institutions who want to collaborate. The core process of this KYC is the collection of basic identity information from each related organization or institutions to check for suspicious activities and how much exposure the customer has to political activities. Review of transactions, and risk management are also carried out in this process. Some institutions also admit that the KYC process is quite costly and if they do not carry out this process in accordance with applicable regulations, they will also be subject to penalties. Chronologically, the applicable KYC process is described as follows:

1. Customers and financial institutions agree to cooperate.
2. The customer sends the documents requested by the bank.

3. The bank verifies the KYC document and analyzes whether the customer can be trusted to be able to onboard the organization.
4. The financial institutions will issue a certification indicating that the KYC process has been carried out and they will also issue a certificate to the regulator stating that this customer has been validated or rejected according to the KYC process.

This process will be repeated every time the customer will cooperate or onboarding the financial institutions. In figure 5.6 a customer will do onboarding at 3 different financial institutions; the customer is required to submit the document 3 times and core KYC checking process must be done 3 times as well. Here we can see the redundancy of the process that would lead to several weaknesses in the process.

Data Integrity Problem

Several interviewees stated that eventhough they have already done the core KYC process completely, there is still an issue that occur during the process. One of them is the data integrity problem. From the customer or user perspective, this problem happens when he try to register into one of the PJSP. He said that the citizenship identity record that they submit to the PJSP is rejected because the data is different from the data that is currently recorded in on the database of Ministry of Home Affairs where the PJSP would do the checking for the KYC purposes.

> ” There’s a problem when I am registering in one of the fintech, they rejected my form because my citizenship identity number is not recorded on their system. Maybe it is related with my recent move to the new place. Actually, I have done all the move procedure long time ago, and they also have issued the new identity card, but I wonder why my data is not updated yet on the citizenship database.” (User, 41:1)

The same problem is also stated by one of the PJSPs who carry out the KYC validation process. Data integrity is considered to be one of the obstacles that need to be solved in validating citizenship data. In some cases, there are differences in individual data between the national citizenship database and the district database where the person is registered. This of course makes PJSP questioning the validity of data or documents submitted by customers. They doubt whether the customer entered the wrong data, or the citizenship database and the district database are not well integrated.

> So he's still on the registration list, then when we checked thoroughly, there are two sources of ID card data in Indonesia besides the national citizenship database, there's the district database. Some of the data is different. The individual data such as the name, date of birth is still the same, but the address is different. The details of the address that we retrieve is not the same at all, it's different, started from the district, the street name, the neighbourhood etc. (Fintech, 41:15)

Manual Verification Problem

In the current KYC process, in addition to using an automated system to crosscheck customer data, manual checking is also carried out by KYC officers. Human intervention here is needed as a final judgment whether the documents and evidence or claims that have been submitted by the user are really valid.

> Actually, there is still a manual activity for the validation. There are agents behind the KYC system who will logging into the system and doing the final check whether ID card is genuine or not and everything is submitted according to the regulation. (Fintech, 40:13)

However, one fintech interviewee stated that this manual verification process has the potential for problems and fraud, especially if the number of customers doing onboarding increases significantly. Firstly, the PJSP will not be able to satisfy the SLA for the KYC because of the limited human resources.

> “At one time the problem happens because of the large number of disbursements from government program. Every time there is a new pre-employment batch, the KYC registration level immediately goes up and our agents are not prepared to process a large batch of KYC like that, so the SLA will be late. Furthermore, if there is an invalid or late approval, many users will complain.” (Fintech, 41:26)

It is not uncommon for KYC verification officers to make human errors when they are asked to complete a large number of KYC verification processes in a short time. In addition to human error, fraud can occur if the KYC verification officer states that the new customer has been validated even though they have not checked it first, they done this because they want to pursue the target number of new registrants.

> “The agents are paid based on the incentive, on how much they finish the tasks. So in post evaluation we found a lot of photos and identity with the same name that didn't match, but the agents kept mark it as valid. When this happen, our only solution is just by looking at their transaction pattern, when we found a suspicious transfer activity deemed as money laundry, we trace it back to the KYC, and because of that we found out that our agents did not perform accordingly.”

5.5 Payment ID Requirements

To develop a blockchain-based platform that can facilitate PaymentID's digital identity, regulators need to design the technology architecture. However, before the technology architecture can be designed, a list of requirements is needed as a reference. In this section, the research question “What are the core requirements of the Payment ID as the primary digital identity in Indonesian payment system? This section will explain what objectives are expected from the PyamentID system to answer the challenges that have been described in the PaymentID Driver section.

In general, this collection uses the Requirement Engineering method, which is a systematic process for developing and validating requirements in collaboration with stakeholders (Shukla et al., 2015, Hull et al., 2010). This RE is carried out through 3 main stages, namely: Requirement Elicitation, Requirement Specification and lastly Requirements Validation.

1. Requirement Elicitation: carried out by collecting information and knowledge related to the main problems from stakeholders. This stage is carried out in the interview process
2. Requirement Specification: Identify key aspects of the information that has been collected from the user. In this process, it is carried out using content analysis
3. Requirements Validation: Re-confirm to stakeholders related to the requirements that have been prepared.

5.5.1 PaymentID Objective and Requirements

There are several main Objectives that will be the goals of the requirements formulation. Each objective will be considered solved as long as the PaymentID can meet the requirements.

a. Objective 1: PaymentID can support the main task of the Regulator in terms of policy formulation and supervision.

   The main objective of this objective is to facilitate the regulator as the initiator of this project to access granular user digital identity data as input for policy formulation and monitoring of payment system activities.

No.	Description	Concerned Actor
Req.1	The Payment System Regulator (BI) have access to the digital identity data on granular level	Regulator

   This requirement ensures that the initial purpose of the PaymentID development is still intact, that Regulators can gain access to payment system user data for data analysis purpose and supervision of payment system activities. This is necessary to support the making of policies that are suitable for user profiles in Indonesia and prevent money laundering activities using the payment system platform.

b. Objective 2: PaymentID can facilitate the KYC process to meet compliance in the payment ecosystem.

   Reflecting on the KYC Challenges currently faced by PJSPs and existing financial institutions, a digital identity is needed that can be used as a reference for the KYC process. In this KYC process, PaymentID is expected to become a digital identity that has data integrity so that it will minimize the potential for errors in the KYC process. On the other hand, by utilizing Blockchain technology, the KYC process can be shortened by utilizing KYC history and attestations from institutions that can validate related to certificates and claims from users.

No.	Description	Concerned Actor
Req.2	Initial registration process should satisfy the regulator's KYC principle	Regulator, PJSP, User
Req.3	PJSP can access digital identity data that related with their services (e.g. registered users data on their system or KYC purpose)	PJSP
Req.4	Whenever a user wants to onboard a PJSP services, PJSP and Regulator can access the user's data, claim and certificate for KYC purposes to verify the validity of their data	User, PJSP
Req.5	Only selected and verified institution can issue and validate user's claims and certificates	Regulator, PJSP, User
Req.6	Service Provider can verify the validity of user's claim	PJSP, SP

c. Objective 3: PaymentID can be a digital identity that can preserve the confidentiality and privacy of the user.

This can be made possible by making Payment ID a Self-Sovereign Identity, so that users have full control over their data and digital identity. Users can limit what information can be shared with other parties. Users can also give consent to PJSPs to access their KYC history when they onboard on new banks or PJSPs.

No.	Description	Concerned Actor
Req.7	User's digital identity data can only be accessed by the consent of the identity owner	User
Req.8	User can limit or choose which data that can be shown to specified PJSP	User
Req.9	User can have access to the information on their own digital identity informations, and the information on which service provider and government institutions that has access to it	User

d. Objective 4: PaymentID should have high degree of data integrity.

It can be used as the main source that can ensure the accuracy, consistency, accessibility, and high quality of data or the identity that it holds. Furthermore, by having data integrity, the authority that will require to validate the digital identity can ensure that the data that it holds is consistent, certified and referable. Data integrity means the accuracy and truth of the data. Data integrity must be maintained to ascertain the truth of the data stored.

No.	Description	Concerned Actor
Req.10	individual and organization should be registered as a unique digital identity	Regulator, PJSP, SP, User,
Req.11	There should be one single source of truth that responsible in providing the correct digital identity data	Regulator, PJSP, User, SP
Req.12	There should be data governance mechanism to ensure the data integrity	Regulator, PJSP, User, SP

e. Objective 5: Availability and interoperability capability of PaymentID.

With interoperability, the data recorded on PaymentID can be easily connected to platforms owned by service providers and legacy systems in the payment ecosystem. With interoperability capabilities, it is also hoped that PaymentID can easily connect with other digital identities that have the potential to be developed in the near future in Indonesia, such as Health and Citizenship Digital Identity.

No.	Description	Concerned Actor
Req.13	The PaymentID can be used by SP within payment ecosystem, and able to create linkage with the existing or future digital identity	Government, PJSP, SP, User
Req.14	The transition from current Siloed digital identity to the PaymentID should be carried out smoothly by ensuring the data interoperability	PJSP, User
Req.15	The system should be available 24/7 or during payment system working hour	Regulator, PJSP, User, SP

f. Objective 6: The Security Aspect of PaymentID

. To ensure the security of user identity data, authentication, access control and security in securing PaymentID need to be considered. Sensitive data needs to be encrypted and stored in a safe place. When the authorities want to access the data, the information will be shared in a secure manner. It should also be ensured that this sensitive data can only be accessed by authorized parties. There should be a governance to mitigate the lost identity case so that it remain secure and can be recovered by the authorised user

No.	Description	Concerned Actor
Req.16	A secure authentication method is needed and should require at least 2-factor authentication	User, PJSP
Req.17	Digital identity data should be stored securely	Regulator, PJSP, User
Req.18	There should be a mechanism to mitigate lost identity	User, PJSP

5.5.2 Conclusion on PaymentID Requirements

In this section, each objective that has been mentioned represents the purpose for which PaymentID was developed. Details of the requirements are compiled to support the objectives and answer the challenges identified in the previous section. The table below will provide an overview of the requirements that have been compiled.

Table 5-3 PaymentID Requirements

No.	Description	Concerned Actor
Req.1	The Payment System Regulator (BI) have access to the digital identity data on granular level	Regulator
Req.2	Initial registration process should satisfy the regulator's KYC principle	Regulator, PJSP, User
Req.3	PJSP can access digital identity data that related with their services (e.g. registered users data on their system or KYC purpose)	PJSP
Req.4	Whenever a user wants to onboard a PJSP services, PJSP and Regulator can access the user's data, claim and	User, PJSP

No.	Description	Concerned Actor
	certificate for KYC purposes to verify the validity of their data	
Req.5	Only selected and verified institution can issue and validate user's claims and certificates	Regulator, PJSP, User
Req.6	Service Provider can verify the validity of user's claim	PJSP, SP
Req.7	User's digital identity data can only be accessed by the consent of the identity owner	User
Req.8	User can limit or choose which data that can be shown to specified PJSP	User
Req.9	User can have access to the information on their own digital identity informations, and the information on which service provider and government institutions that has access to it	User
Req.10	individual and organization should be registered as a unique digital identity	Regulator, PJSP, SP, User,
Req.11	There should be one single source of truth that responsible in providing the correct digital identity data	Regulator, PJSP, User, SP
Req.12	There should be data governance mechanism to ensure the data integrity	Regulator, PJSP, User, SP
Req.13	The PaymentID can be used by SP within payment ecosystem, and able to create linkage with the existing or future digital identity	Government, PJSP, SP, User
Req.14	The transition from current Siloed digital identity to the PaymentID should be carried out smoothly by ensuring the data interoperability	PJSP, User
Req.15	The system should be available 24/7 or during payment system working hour	Regulator, PJSP, User, SP

No.	Description	Concerned Actor
Req.16	A secure authentication method is needed and should require at least 2-factor authentication	User, PJSP
Req.17	Digital identity data should be stored securely	Regulator, PJSP, User
Req.18	There should be a mechanism to mitigate lost identity	User, PJSP

5.6 Proposed Blockchain Architecture For Payment ID

5.6.1 Design of the architecture

In this section, we will discuss the design of a blockchain based digital identity architecture that is suitable to meet the requirements of PaymentID so that this can be a solution to the problems identified in the PaymentID Driver. In the preparation of this design architecture, the selection of blockchain networks will be explained followed by a consensus mechanism for recording new digital identities, data storage and security aspects.

5.6.1.1 Network Configuration

The network configuration will determine the structure and control of the blockchain network and the form of member participation in the network. By paying attention to the requirements and conditions of the current payment ecosystem, regulators, banks and PJSPs are the parties that can be used as nodes in this blockchain network. This means that other actors other than regulators, banks and PJSPs cannot be entered directly into this network. Reflecting on the literature study on blockchain networks, previously mentioned there are 3 main types of network configurations that can be implemented on blockchain networks, namely: public, private and consortium. When viewed from its use, public blockchain is not suitable as an option because this type has no restrictions for anyone who joins the network and becomes a node. On the other hand, private blockchains are also not suitable because this digital identity model will be centralized and every stakeholder who joins this network will depend on only one central entity. The consortium blockchain is a suitable choice to form a digital identity for this payment ecosystem because only a select few nodes can join the network. By using a permissioned blockchain, the confidentiality of the digital identity will be maintained. This is made possible by the provision of access control that cannot be facilitated by the public blockchain. On the other hand, because PaymentID involves digital identity which requires credibility from certificates and claims owned by users, trusted and responsible authorities and organizations are needed in authorizing the identities of users and organizations that are onboard into this Digital Identity.

Component	Description
Blockchain Network	Consortium Blockchain (Private Permissioned) because the payment system regulator need to have control over the data and ensuring the compliance within the digital identity

5.6.1.2 Consensus Mechanism

The consensus mechanism here concerns the mechanism on how a blockchain ledger is verified before being stored in a series of blocks in the blockchain network. To prevent problems with data integrity, an appropriate consensus mechanism is needed. In section 3 we have described several consensus mechanisms in blockchain networks. In relation to the payment ecosystem, trust and reputation of the nodes that are members of the blockchain network play an important role in the validation process of data changes and new data recorded on PaymentID, in this case new data changes are represented by storing new blocks in the ledger. So PoA can be a suitable consensus mechanism because only certain and trusted authorities can validate new blocks.

Component	Description
Consensus Mechanism	Proof of Authority

5.6.1.3 Data Storage

Whenever new data is added or data changes, the records will be recorded in the block stored in the ledger on-chain. This process runs so that nodes that have duplicates of the ledger have access to the data change records. On the other hand, documents, certificates and claims can be stored on-chain or off-chain. Using off-chain storage will lighten the storage load on the platform, making it easier to increase scalability and increase the confidentiality of the document. In this case, if it is associated with PaymentID, then using off-chain storage for documents, certificates and claims is better. With this method, references to documents will be recorded on-chain so that they are accessible to nodes and authorized parties. This reference will have a URI (Unified Resource Identification) which will be used as a link to access documents from off-chain storage. To ensure document integrity, the hash of the document needs to be included in the reference. When an authorized party wants to access the document, a new hash will be degenerated and used to match the hash stored in the reference.

Component	Description
Data Storage	Hashed Identifier or the reference of users identity stored on-chain, while the identity details such as certificate, claims, or documents is stored off-chain. This approach is used to facilitate the scalability of the blockchain network.

5.6.1.4 Data Security and access control

Because PaymentID contains sensitive data such as usernames, addresses, personal data and references containing addresses of documents and claims, access to this entity should be restricted. With a consensus form of blockchain, of course every node that has the right to read the data will be able to access the information, so to protect the confidentiality of the data, the document needs to be encrypted before being stored. In this case, Symmetric encryption will be used to encrypt information and references stored on-chain due to adapting to the scalability of the system. With symmetric encryption, only one key is needed to encrypt and decrypt data, so this method is suitable for facilitating systems with high volume of data changes on-chain. To be able to share keys securely, an access control is needed. The current access control consists of two methods, namely RBAC and ABAC, in this case RBAC is more suitable for use because access to on-chain information will only be accessible by users with certain roles.

On the other hand, documents belonging to users that are stored off-chain will be encrypted using Asymmetric encryption so that a pair of private and public keys will be required to access them. This is necessary so that the information contained in the document can only be accessed by a specific authorized party.

Component	Description
Security	The reference that stored on chain will be encrypted using asymmetric cryptography, while the identity details will be encrypted using symmetric cryptography.
Access Control	Using RBAC (Role Based Access Control), the access to digital identity data will be restricted based on the role of the user; i.e. only selected government institution can have access to the data, SP can access data only for onboarding user and registered user under their system

5.6.1.5 PaymentID Blockchain Architecture Conclusions

The consortium blockchain is a suitable choice to form a digital identity for this payment ecosystem because only a select few nodes can join the network. By using a permissioned blockchain, the confidentiality of the digital identity will be maintained. This is made possible by the provision of access control that cannot be facilitated by the public blockchain. For the consensus mechanism PoA can be a suitable consensus mechanism because only certain and trusted authorities can validate new blocks. The information changes of the records will be recorded in the block stored in the ledger on-chain. This process runs so that nodes that have duplicates of the ledger have access to the data change records. On the other hand, documents, certificates and claims can be stored on-chain or off-chain. Using off-chain storage will lighten the storage load on the platform, making it easier to increase scalability and increase the confidentiality of the document. Lastly for the security requirement, Symmetric encryption will be used to encrypt information and references stored on-chain due to adapting to the scalability of the system. With symmetric encryption, only one key is needed to encrypt and decrypt data, so this method is suitable for facilitating systems with high volume of data changes on-chain. This symmetric encryption will be accompanied with Role Based Access Control to make sure that only user with certain roles can access the key. On the other hand, documents belonging to users that are stored off-chain will be encrypted using Asymmetric encryption so that a pair of private and public keys will be required to access them. This is necessary so that the information contained in the document can only be accessed by a specific authorized party.

Table 5-4 PaymentID Blockchain Architecture Suggestion

Component	Description
Blockchain Network	Consortium Blockchain (Private Permissioned) because the payment system regulator need to have control over the data and ensuring the compliance within the digital identity
Consensus Mechanism	Proof of Authority
Data Storage	Hashed Identifier or the reference of users identity stored on-chain, while the identity details such as certificate, claims, or documents is stored off-chain. This approach is used to facilitate the scalability of the blockchain network.
Security	The reference that stored on chain will be encrypted using asymmetric cryptography, while the identity details will be encrypted using symmetric cryptography.
Access Control	Using RBAC (Role Based Access Control), the access to digital identity data will be restricted based on the role of the user; i.e. only selected government institution can have access to the data, SP can access data only for onboarding user and registered user under their system

5.7 Challenge in Adopting the Blockchain based Payment ID

In addition to interviews to gather the main reasons for the need for PaymentID as a digital identity for the payment system, interviews were also conducted to identify what challenges have the potential to arise when developing a blockchain based PaymentID. In this interview, questions related to challenges were asked based on an approach to the Integrated Process, Institutional, Market, Technology (PIMT) framework (Janssen et al., 2020). Challenge aspects are grouped into 3 things: Technical, Institutional and Market. Based on the results of the interview, the description of the challenge is as follows:

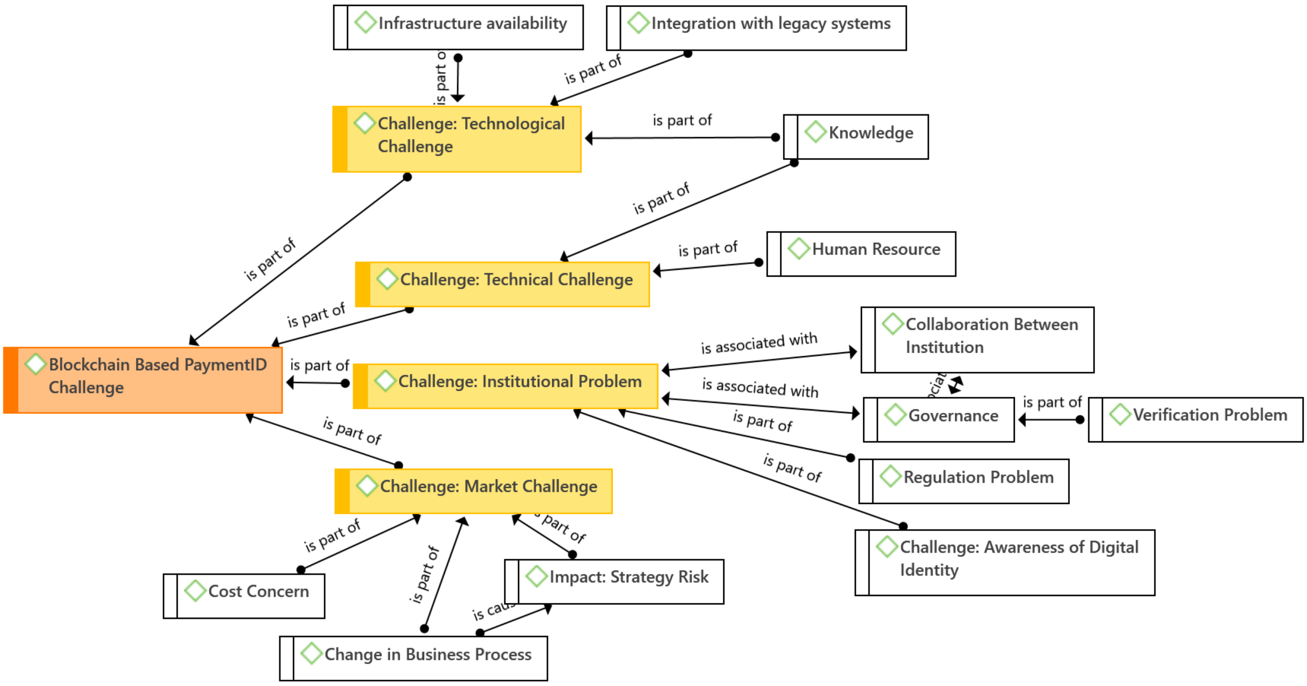

Infrastructure availability
Integration with legacy systems
is part of
is part of
Challenge: Technological Challenge
is part of
Knowledge
is part of
is part of
Human Resource
is part of
Challenge: Technical Challenge
is part of
Collaboration Between Institution
is associated with
Blockchain Based PaymentID Challenge
is part of
Challenge: Institutional Problem
is associated with
Governance
is part of
Verification Problem
is part of
is part of
Regulation Problem
is part of
is part of
Challenge: Market Challenge
Challenge: Awareness of Digital Identity
is part of
is part of
part of
Impact: Strategy Risk
Cost Concern
is cau
Change in Business Process

Figure 5.8 Blockchain Based PaymentID Implementation Challenge

5.7.1 Technical Challenge

In the technical challenge aspect, it is known that until now blockchain technology is still rarely implemented in Indonesia. From the blockchain consultants we interviewed, it was stated that there are only 5 consultants who are capable of doing blockchain programming in Indonesia. Meanwhile, companies that have used blockchain technology in their business processes are still few or below 10 companies. Therefore, it can be concluded that the development of blockchain technology in Indonesia is still at the early stage. This can mean 2 things, namely: the opportunity to develop blockchain innovation is still very large in Indonesia but on the other hand, limited resources are one of the main obstacles to enabling this technology in industries in Indonesia.

Apart from the results of interviews with blockchain consultants, similar statements were also found in both regulators and PJSPs. The regulator said that understanding of blockchain technology is still very minimal and a more in-depth study needs to be done regarding its potential use, security and other aspects if it is to be implemented in the organization. Meanwhile, the PJSP stated that until now there is still no urgency from companies to adopt blockchain technology in their business processes

5.7.2 Technological Challenge

The challenge in the technological side is still related with the technical challenge. The knowledge possessed by both regulators and market players in Indonesia regarding blockchain is still considered low, this is confirmed by the results of the interviewees' statements when conducting an overview related to blockchain technology.

> “understanding related to blockchain technology in both of the regulator and market side is still low, people are still referring to blockchain as another form of bitcoin or cryptocurrency.” (Regulator, 3:11)

> "I don't think the technology can be implemented easily, especially when the knowledge of the technology implementation is not common for the industry player." (Bank, 35:19)

On the other hand, there are also questions about the infrastructure requirements of this blockchain technology. Because this technology is still not common in Indonesia, the infrastructure requirement is also one of the challenges questioned by stakeholders. Lastly, because there is still lack of knowledge about this technology, stakeholders are also afraid that the Blockchain technology is incompatible with the legacy systems that they currently have. One of the blockchain consultant stated that integration with legacy system is possible, however it is a complex activity, therefore a transition procedure into the new technology will be needed.

5.7.3 Institutional Challenge

From the institutional side, there are several main challenges, including Governance, regulation, collaboration between institutions and awareness related to digital identity in the community.

Starting from the Governance side, the Regulator stated that there will be many changes related to the process that applies when the registration and use of this digital identity is carried out. The governance of the payment system work process will be changed, and this will be related to the regulations issued by the regulator to PJSP and stakeholders in the payment ecosystem. It is necessary to conduct a study on how to formulate the governance in order to comply with the existing regulations. Governance and Policy are also related to the inter-institutional authority. It is necessary to see how big the scope of PaymentID is and how many other government institutions will be involved in the implementation of PaymentID. For example, if this business process is directly related to citizenship data in the Ministry of Home Affairs, collaboration between institutions is necessary. Similar collaboration is also needed with the Ministry of Communication and Information Technology regarding the technology standards used and how they affect personal data protection laws.

> “In terms of authority, we think that the Ministry of Home Affairs has higher precedence to regulate it. Therefore, before we can develop the system or regulation, we have to make sure that the Ministry of Home Affairs is onboard with this idea.” (Regulator, 37:13)

> “From my point of view as industry player, I think the political aspect related to digital identity is very high, therefore the division of roles within the government institutions should be clear before they plan to collaborate with the industry.” (Fintech, 40:27)

The last one needs to be addressed as well as institutional challenges related to the public. The awareness related to the confidentiality and security of digital identities are still low in within the Indonesian users, so it is also necessary to strengthen the education side on the use of digital identities for the users.

5.7.4 Market Challenge

Challenges on the market side are closely related to business processes that are currently being developed in the industry. In addition to technical challenges, changes in business processes are also one of the main challenges faced by market players, banks, PJSPs and merchants who are connected to the payment ecosystem. This is a challenge for the market because they have to make a transition from existing business processes. This also affects the strategy they have to plan after the implementation of the PaymentID based blockchain. The work process of assigning a risk rating to the user as well as data analytics related to the user's identity will also impacted. There are also doubts from one of the PJSPs regarding the user's full control over their personal data.

> “For some reason I feel that the existence of this blockchain network will limit service providers from being able to retrieve data from users. I think it will results in changes in many business processes in our company.”(Fintech, 40:52)

They do not want this new PaymentID to reduce their access to data and information that they have been using as the main input in providing service innovations to users.On the cost aspect, they also said that if the KYC process changes and becomes more effective and efficient, there will be potential for cost reductions.

On the other hand, costs are a concern for them in terms of transitioning to a new system. Of course, both the market and regulators are required to prepare costs for infrastructure preparation and development of a system that is able to accommodate blockchain-based PaymentID.

> “Of course there is a cost here, therefore we need to see whether the costs we spend to maintain this blockchain network are less than the costs we have to spend on end-to-end KYC and digital identity security.” (Fintech, 40:53)

The new form of digital identity infrastructure also needs to be maintained to ensure that the end to end process from the registration, verification and deregristration working synchronously for every institutions. The maintenance cost for this infrastructure should also be discussed among the stakeholders that utilizing the services.

> “Because this certificate will be stored in the cloud and the private e the public is talking about who should do this because there are costs involved.” (Digital Identity Expert, 42:2)

From the government point of view, cost can be other aspects that will become a challenge when they want to implement the new system. Depending on the scope of the new system, if the government decided to recreate the whole digital identity ecosystem it will become very costly both for the government and the existing digital identity provider and users.

Collaboration with the existing digital identity service provider and giving them option to do the research on the new digital identity that fits the existing business can be a solution for both the government and the market.

“They don't try to develop your own digital I.T. and verification services because that's a costly process and you need to fulfill thousands of audit norms. And it's going to be difficult for you. Let the market who specializes in this do it.” (Digital Identity Expert, 42:9)

6 Blockchain-Based Payment ID Analysis

6.1 The Issues With Current Digital Identity

the current digital identity used in the payment ecosystem are still using the siloed model of digital identity, it means that the same organization act as SP and the IdP at the same time. It means that the PJSP, in this case the banks and fintech companies also act as the identity provider, where they record and maintain the identity of the users by themselves and not directly connected with any other financial institutions nor make use of the Digital Identity Service Provider or external digital identity service provider.

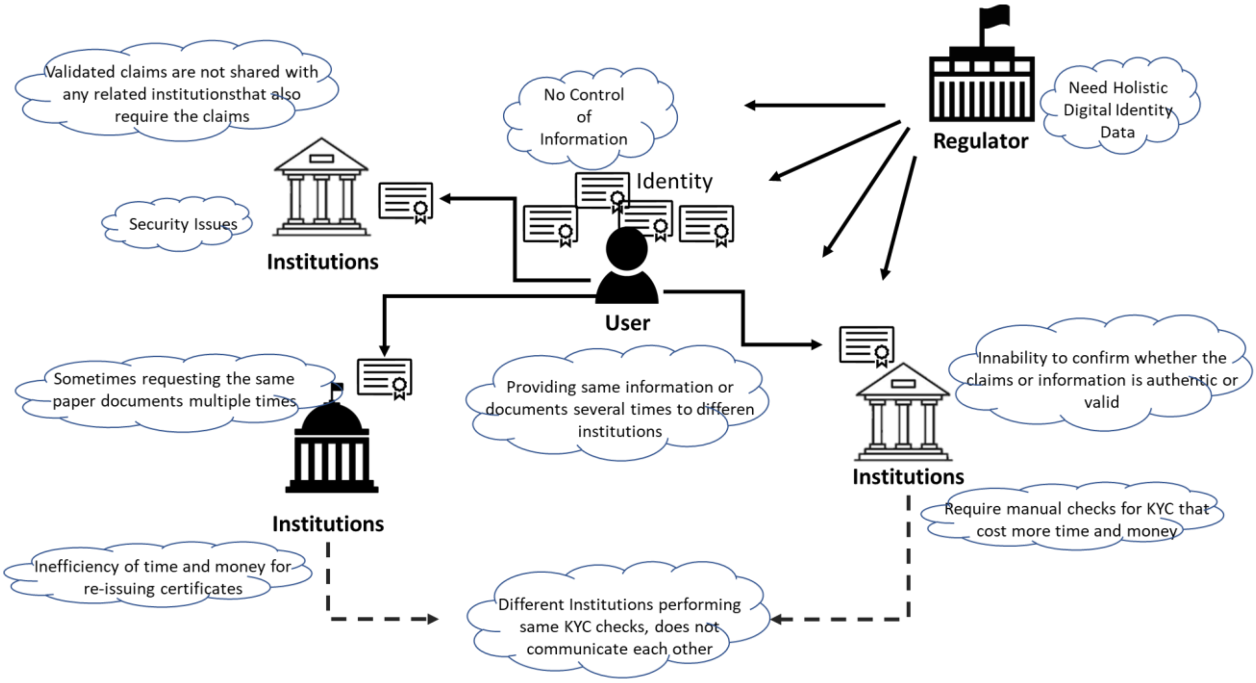

Validated claims are not shared with any related institutionsthat also require the claims
No Control of Information
Regulator
Need Holistic Digital Identity Data
Security Issues
Institutions
Identity
User
Sometimes requesting the same paper documents multiple times
Providing same information or documents several times to differen institutions
Innability to confirm whether the claims or information is authentic or valid
Institutions
Institutions
Require manual checks for KYC that cost more time and money
Inefficiency of time and money for re-issuing certificates
Different Institutions performing same KYC checks, does not communicate each other

Figure 6.1 Issues with Current Digital Identity illustrated

1. **Lack of Data Availability**

The current state of digital identity has an impact on the availability of data held by the central bank. So far, the central bank only has aggregate transaction data and does not have detailed access to transactions that occur in the community, this has reduced the ability of the central bank to be able to make policies that are specific to the public. On the other hand, in terms of security to prevent money laundering, the process of monitoring customer identity has also not been effective due to the availability of data and the integrity of public data. Bank Indonesia feel the need to have the big data that contains highly detailed data of the digital identity. Beside that In order to avoid information asymmetry and unbalanced competition between the fintech companies, BI also planned to use the data analytics gathered from PaymentID to foster the growth of the SMEs and digital industry.

2. **Data Integrity Problem**

Data integrity is another aspect that causes data availability problem in Indonesia. Some data stored in several government institutions are not connected to each other, causing mismatches in citizen's data. Data integrity is considered to be one of the obstacles that need to be solved in validating citizenship data for KYC. This condition raises question in the validity of data or documents that is provided by users. In this case it is difficult to differentiate between falsified data and the outdated data. Banks and PJSPs find it difficult to find the reliable source of data to check the validity of user's data.

3. **Security Risk**

By using the centralized digital identity model, having full control of the user data is deemed beneficial from the perspective of the PJSP. It is because they can make use of the data that they have for the analytics, however they also mention that it has its own disadvantages such as they will have to manage the risks of the user's data security all by themselves. Another problem with the current siloed digital identity is the potential frauds that occur due to fake identity and account take over. Although this problem caused by the weakness of their own system, the user's lack of awareness for digital identity security is also become one of the most influential factors.

4. **Redundant KYC**

Problems that occur in the KYC process for onboarding new users at Banks and PJSPs are one of the reasons why they need a standardized and integrated digital identity payment system. They feel that there is redundancy in the current KYC process, and it is costly, because they have to employ tools and resources every time, they do the KYC processes. Furthermore, Data Integrity is one of the most important things that become an issue either for banks, PJSP and users. There is no data integration between institution which causes confusion everytime banks or PJSP wants to do a more detailed KYC.

5. **User Data Control**

With siloed digital identity, the first problem that users have is that they are required to memorize different authentication methods to access their digital identities in several institutions. In addition, users also experience problems related to data control because their digital identities are attached to the different institutions, and they do not have them on their own or any devices. Users cannot control how the data they share with these institutions will be used and utilized. From the user's point of view, they also cannot confirm whether the digital identities currently stored in these different institutions have been manipulated or modified. This causes users to lose control over their digital identity data.

6. **Cost**

Ultimately, everything will come down to the cost concern. With the weakness in the security of the current digital identity model, this can be detrimental to PJSP and banks if their security is compromised. Imagine how much loss the organization will suffer if its data is leaked. The occurrence of Fake Identity also has the potential to cause losses in terms of financial fraud. On the other hand, KYC activities also very costly, according to the banks and PJSPs. The cost may come from developing and maintaining KYC software to the expenses incurred for manually checking KYC activities. The cost of checking KYC manually here can include the cost of document printing and fees for hiring 3rd party KYC services. On the other hand, PJSP actors also mentioned that the cost of managing services from a 3rd party digital identity provider is also relatively high.

6.2 Impact Analysis of Blockchain Based PaymentID

6.2.1 Solving Digital Identity Problem

1. **Data Availability**

By having blockchain based digital identity, the regulator can have access to detailed payment system user data without having to know the personal data of each user with the help of ZKP encryption. In this way, regulators can use the data for policy analysis and supervision purposes. They can assign risk ratings and scoring to payment system actors which can later be useful for other government institutions that require such data, one of which is to monitor potential fraud and money laundering in more detail. The quality of the data captured by the regulator can improve because digital identity data is standardized among the PJSP. Historical data related to user membership status in financial institutions can also be tracked and audited better

2. **Security**

Firstly, the security can be guaranteed by using the blockchain technology because every data that is stored in the blockchain is hashed and does not contain any personal data of the users. The data in each block is linked and immutable which means that the data inside the block is tamper-proof. Secondly the digital identity data is not recorded solely on each of the banks or PJSPs therefore the digital identity will not have the single point of failure, making it more robust from cyber-attacks that threaten the data integrity. The blockchain network also integrated with claim issuers, therefore PJSPs and banks can also easily verify the claims that provided by the user to them. This way it will reduce the rate of security issues such as Fake ID and synthetic identity because any data provided by the users will be validated first within the blockchain network to ensure its authenticity and its validity.

3. **Data Integrity**

With the existence of a blockchain network that connects various institutions, the data that is distributed in the peer-to-peer network will always be synchronized and checked for its validity between institutions. Data integrity will be maintained because every data change that occurs in a digital identity will be recorded and auditable in the blockchain. Both users and institutions will be able to access the latest data and if there is a data change there will be records of the change.

4. **User Data Control & Efficiency**

With this blockchain based digital identity, it can actually make it easier for the users to register or board on the PJSP platform. Users no longer have to fill out forms every time they register on the PJSP platform. they only need to register the claim and administrative documents required by PJSP on the blockchain based PaymentID. In terms of privacy and security, users will have full control over the information that they will share with institutions and SP. This is also called as the selective attribute disclosure and it satisfy the principles of the SSI. Furthermore, regulator and other government instiutions will not have full control of the users data, this way, there is a balance in the data control.

5. **Operational Efficiency**

There will be efficiency in the KYC process, especially when banks and PJSPs need to check the claims on the user's digital identity who want to onboard their system or platform. With the existence of a blockchain based digital identity, there will be change in the business processes and the relationship between the actors.

In the current business processes, the identity of the user was spread across various institutions. At the time of registration at bank or PJSP, they must collect proof of the certificates and documents that they has scattered from various certificate issuers. There are 3 main problems that occur in the current process:

a. Proof is usually in the form of unstructured data, in various forms, it can be in the form of photocopies, images and writings. This causes an additional process that must be carried out by the bank or PJSP in converting the unstructured document into digital data that is in accordance with their system for processing.
b. Changes in data that occur in real life such as changes in address, changes in ownership of goods can occur at any time and are not recorded in real time on paper based proofs. It will take time for this proof document to be updated and not necessarily reflected in the user's proof
c. Some proofs, such as photocopies and pictures, are very easy to forge, so to determine their authenticity, the bank and PJSP need to take more sophisticated steps such as notarizing proof, etc., which takes a lot of time and money.

To illustrate the current KYC activity, the process can be described in figure 5.1

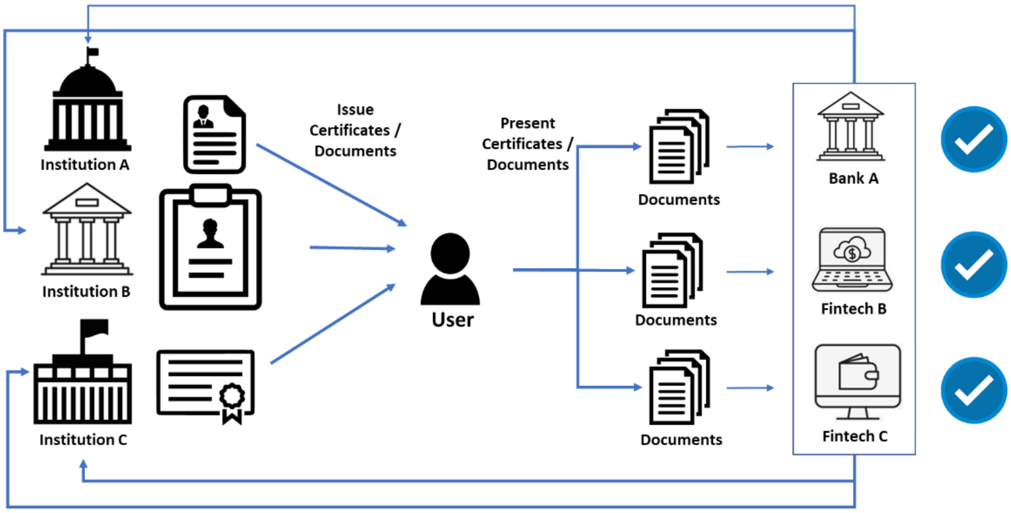


Figure 6.2 Illustration on Current KYC Process in Payment Ecosystem

*In this scenario we assume that The first time users receive certificates from the Institution that issued them, users will store the physical documents on their own.

1. User and financial institutions agree to cooperate.
2. Financial institutions requires user to submit their data and the proof, such as citizenship identification, ownership certificates, passports and etc.
3. The customers gather the documents that they have from the institutions that issue the documents.
4. The customer sends the documents requested by the bank.
5. The financial institutions verifies the KYC document and analyzes whether the customer can be trusted to be able to onboard the organization.
6. The financial institutions will issue a certification indicating that the KYC process has been carried out and they will also issue a certificate to the regulator stating that this customer has been validated or rejected according to the KYC process.
7. Whenever the user wants to onboard another financial institution he will required to do the KYC process all over again and the new financial institution will need to verify the data claimed by the user by doing another the KYC process based on their regulation

The current business process can be concluded that it is quite time consuming and requires costs both from the user side and the bank and PJSP who will do the onboarding of new users.

On the other hand, by utilizing the Blockchain based Digital Identity, The government institutions, the users and the service provider will be interconnected through the Blockchain Network.

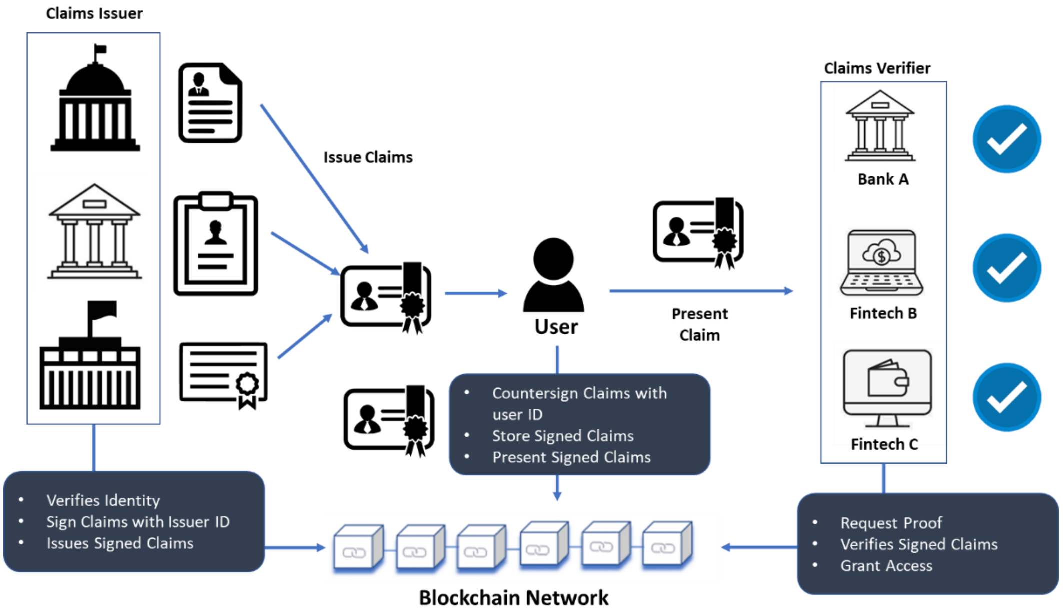


Figure 6.3 KYC Process using Blockchain Based Digital Identity

In the new KYC scenario, blockhain based PaymentID is used as the container or a wallet that can store claims that owned by the users. By using this PaymentID users can easily onboard to any banks or PJSP without having to gather the physical proof of their certificates or documents. The process can be broken down into these steps:

* In this scenario we assume that initially when users receive a certificate, they store them into their wallet. The certificates that issued by the claims issuer will be signed by both the issuer and the users and then it is stored into the blockchain.

1. User and financial institution agree to cooperate.
2. Financial Institution request the documents that they need to check for KYC to the user.
3. User presents the PaymentID to the financial institutions containing the detailed documents and claims.
4. Financial institution verifies the claims from the blockchain network

5. Financial institution grants or reject the onboarding process based on the verification result and records the KYC result into the blockchain to be used by other financial institution.
6. Whenever the user wants to onboard another financial institution, he only need to present their PaymentID without having to gather any physical documents again. On the financial institution side, they will not need to do the KYC process from the beginning because they will have access to the latest KYC result by the previous financial institution and the documents that is stored in the user's PaymentID

With this efficiency, Blockchain Based PaymentID is expected to cut a lot of KYC costs and shorten the user onboarding process. In addition, because the user claim verification process in the blockchain can be traced and audited, this can potentially reduce fraud that often occurs in this payment ecosystem such as fake id, clone id account take over and etc.

6.2.2 Concern Related With Blockchain-based PaymentID

1. **Technical challenges**

From a technical point of view, blockchain technology is still rarely implemented in Indonesia. The understanding of blockchain technology is still very minimal in the industry and a more in-depth study needs to be done regarding its potential use, security and other aspects if it is to be implemented in the organization. It is also related with the availability of the human resources that is capable to develop the blockchain-based system. There is also problem when the government wants to do a benchmarking of this technology to another country since there is still low number of countries that has implement blockchain into its government process.

2. **Technological challenges**

The challenge in the technological side is still related with the technical challenge. The knowledge possessed by both regulators and market players in Indonesia regarding blockchain is still considered low. the knowledge about the infrastructure requirements of this blockchain technology is also questionable. Because this technology is still not common in Indonesia, the infrastructure requirements is also one of the issues that commonly discussed by the stakeholders. The issue with infrastructure requirements also related to the scalability aspect which is still often discussed in several studies such as (Zheng et al, 2018; Swan, 2015) as well as the energy consumption of blockchain technology (O'Dwyer et al., 2014; Monrat et al., 2019). Lastly, because there is still lack of knowledge about this technology, stakeholders are also afraid that the Blockchain technology is incompatible with the legacy systems that they currently have.

3. **Organizational Concerns**

The development of Blockchain-based PaymentID requires the participation of many stakeholders, ranging from the regulator to the market player. Each stakeholder has its own role. On the other hand, stakeholders also have different goals, interests, challenges, and opportunities. Collaboration between government institutions is a very important factor because the authority in managing blockchain-based digital identity is spread across various institutions. In terms of recording citizenship data, the main authority lies with the Ministry of Home Affairs, only this ministry has the authority to organize community data. Meanwhile, from the aspect of data privacy and security, the main authority lies with the Ministry of Communication and Information Technology. The collaboration between institution is necessary so that there is no conflict of interest between these authorized institutions. In terms of market players, their contribution is also needed to ensure that this digital identity can solve the problems they are currently experiencing and to make sure that the new digital identity is suitable and can be implemented in the current industry.

It is also necessary to think about how to form the blockchain consortium that can satisfy the needs of each stakeholder. BI as a regulator must also think about how the form of the initiative will be implemented, whether BI as a regulator will also act as a provider of blockchain network infrastructure or BI will only become the governing body. If the regulator choose to become the governing body, they need also to think on how to cooperate with existing IdPs and other related authorities to build this blockchain network. Then BI also needs to think about whether there will be additional operational costs that need to be incurred by either the regulators or market players to maintain the blockchain network.

4. **Regulatory**

Regulation concerns are still linked with the organizational concerns. With the new system and the new business process, it will certainly lead to regulatory changes. Regulations that related to PaymentID are at least related to the data protection law owned by the Ministry of Communication and Information Technology, the citizenship law regulated by the Ministry of Home Affairs and the anti-money laundering law that regulated by Bank Indonesia. In this regard, collaboration between related institutions is also needed so that there is compatibility between blockchain-based PaymentID and the current law and regulation.

5. **Cost Consideration**

Cost has become one of the concerns among PJSPs and banks. They are unsure on how much is the investment costs that they need to pay to adjust their existing system so that it will be interoperable with blockchain network in the future. They also questioning the operational costs that they need to pay to utilize the blockchain network infrastructure, and the potential recurring costs for members of the blockchain consortium.

6. **Identity Data Control Dillema**

There are concerns from stakeholders namely government, market players and users related to the digital identity data control. Firstly, The zero knowledge proofing that can be utilized in the blockchain technology will enable users to limit SPs access to their information. If this happens, SP needs to adjust their data captuing strategy since it will affect their business processes. Meanwhile from the point of view of the regulator, they will have dillemas in managing the digital identity data. The dillema is: should this data be stored centrally, distributed among the respective and authorised institutions or entirely decentralized. The more centralized of the data storage the regulator will have more control over the data but the more it will lose data transparency, on the other hand if blockchain technology is used fully in a decentralized manner, there will be the potential that the regulator will lose control over the data. The same thing also concerns the verification process of data changes, where regulators can choose to be the central party that can verify or they can appoint certain parties or the public as part of the consensus. If they choose to be the central party, of course, the verification process of data changes can occur quickly, but their transparency will also be questioned in the eyes of the market and the public. The control mechanism of this PaymentID will be described in the table 6-1.

Table 6-1 Digital Identity Data Governance Tensions

	Identity Data Governance Tensions	
	Centralized	**Decentralized**
Data Control	Fully controlled and managed by the one organization, the payment system regulator. Easier for the regulator to monitor and supervise the data or even modify the data. But the user will not have control over their own data	Identity data is kept by the user along with the claims that have been signed by the issuer institutions. User has control over their own digital identity. There is a potential that user can tamper their digital identity, however if they connected to the blockchain network, the the tampered data will be rejected because it is not valid
Data Accesibility	Regulator can access the data easily. Users need to authenticate themselves with the centralized system to access their own data. Service Provider need to request permission to access the data either to the regulator or users, depends on the regulation.	Regulator may have access to the user's data or they will have to request the user's consent, depends on the regulation. Users can easily access their own data because it is saved on their device, but they still need to authenticate themselves to ensure the security of the data. Service provider will have to ask the user's consent to access teir data

Security Risk	The risk is centralized in one institution. The organization can become the honeypot of cyber attacks. Once the security is compromised the attacker will have access to the user’s data	The risk is not centralized to one institution. The decentralized blockchain network will be able maintain the integrity of user’s data
Responsibility	The government will be responsible for the governance and the scurity of the user’s data	The responsibility governing the user’s data will be distributed among the member of the blockchain network consortium
Reputation	The reputation of the institution is undisputed and does not have any effect to the institutions. Users will always rely on the institution	Reputation of the members within the blockchain network consortium plays huge role especially during the consensus process and giving attestation over user’s claim
Transparency	The transparency of the data (how it is stored and managed) is questionable since the users cannot have control of their data	Since the users have full control of their data, it is considered transparent

The tensions presented from the table above shows that both centralized and decentralized control for the digital identity has its own advantages and disadvantages. This dilemma raises concerns for stakeholders as each of the stakeholders has their own view related with data utilization.

Government Control Concern

government point of view, the centralized control over the digital identity data is needed on order to preserve the validity of the users’ data. From this sentiment, it can be assumed that government still has doubt over the security within the blockchain network. Based on this concern there should be a trust mechanism that can ensure the validity of the user's digital identity even though they are registered and stored in a decentralized manner.

SP Data Availability Concern

From the SP perspective, the decentralized data will have both positive and negative impact on their business. In one hand, since the important digital identity data is not solely recorded on their own database, they will be freed from the single point of failure risk. Having said that, it means that SP will not have all the users' data that they used to have on their storage, and they will have a limited accessibility. The change of business process will cause them to readjust their strategy and it will potentially cost them more resources in order to gather the users' data. Hence there is a need to have a mechanism that can enable the SP to gather data from the users without causing a lot of changes on their businesses.

Users Privacy and Responsibility Concern

While from the user's perspective, privacy and the ease to control their own data become the main concern from them. By having a decentralized identity data storage, it will enable the users to manage their own data and preserving their privacy. However, the ease of control also has its own price, it means that users have full responsibility over their own data. When there are problems and omissions in data management users will not be able to put the responsibility to the governments. It will also cause risks of losing the digital identity become more apparent. In order to mitigate these unwanted consequences, users need to be equipped with the sufficient knowledge and the tools needed to manage the digital identity. Furthermore, there's also a need to have a middle ground solution or discussion that can facilitate the concern between the governments, market players and the users.

6.3 Payment ID Governance Area

In order to facilitate the the needs of the regulator, the market players and the users. There is a need to set the required area of responsibility of the Blockchain-based PaymentID. The area of resonsibility that will be recommended in this study is formed by four main governance processes, namely: Governance on block creation, governance on PaymentID Registry, Governance on trusted list, and finally governance on governance on user keys and credentials.

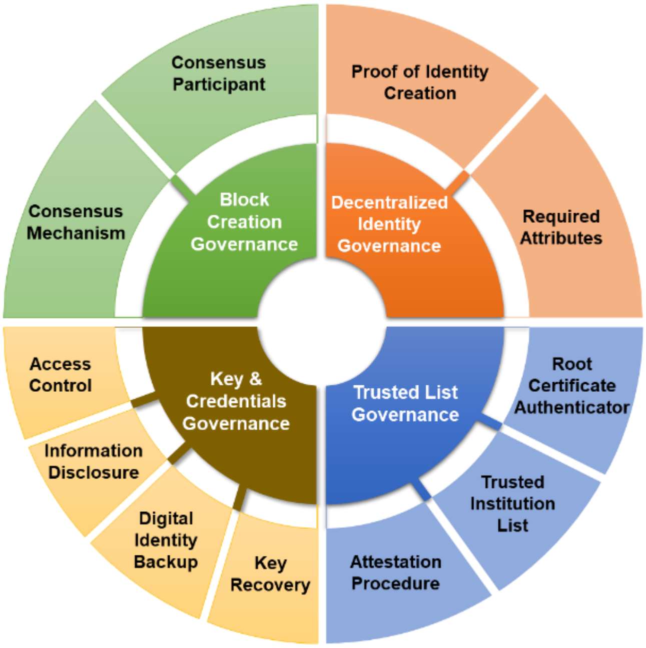


Figure 6.4 PaymentID Area of Responsibility Diagram

The area of responsibility will not fully solve the dillema that is presented from the previous point but it will serve as the recommendation on the governance process that will be needed to be discussed furhter by the stakeholders to support the development of the PaymentID while also facilitating in solving their main concerns.

The interaction between stakeholders on the area of responsibilities are recommended based on the table 6-2. This table utilize RACI matrix based on Simonsson, Johnson, & Wijkstrom, (2007) in relation with the the IT Governance based on CobiT 5. However, in this recommendation table only Responsible (R), Consulted (C), and Informed (I) roles are used to simplify the interaction between the stakeholders. The roles in the matrix explained as follows:

1. R = Responsible, meaning that the individual or organization is responsible for actively formulate the governance process of the specified area and become the part of decision maker of the governance process formulation.
2. C = Consulted, meaning the the individual or organization is not fully responsible in the formulation of the governance area but they are consulted by the responsible party for their input that will be useful in

formulating the governance process but not actively act as the decision maker.

3. I = Informed, meaning the individual or organization is not responsible or included in the discussion for the governance formulation process but they are informed of the process and the outcome of the decision.

Table 6-2 Area of Responsibility Matrix

Area of Responsibility	Payment System Regulator	Payment System Infrastructure Provider	Payment Service Provider (PJSPs & Banks)	Digital Identity Provider	User	Related Government Institution
Block Creation Governance	**R**	**R**	**C**	**C**	**I**	**C**
Decentralized Identity Governance	**R**	**I**	**C**	**C**	**C**	**R**
Trusted List Governance	**R**	**R**	**R**	**R**	**I**	**R**
Key and Credentials Governance	**R**	**I**	**R**	**R**	**C**	**C**

6.3.1 Block Creation Governance

This governance is another term for the consensus protocol that will be used by this blockchain network. If viewed from the main purpose of forming a Payment ID, it can use proof of authority which also involves banks and PJSP as authorized nodes. With the proof of authority, only certain nodes can authorize the creation of new blocks. The selection of proof of authority is necessary considering that PaymentID is a digital identity in which it stores sensitive information so that credible organizations are needed to be able to maintain this blockchain network. In addition, by involving regulators, bank representatives and PJSP representatives, decentralization can run decentralized and the process of creating new blocks does not depend on one party alone. In this process, the government and the payment system infrastructure provider are expected to discuss how the block creation will be performed and decide the suitable governance of the process

6.3.2 Decentralized Identifier (DID) registration Governance

The registration of the new PaymentID will be done by determining the components and attribute that will be required in making the DID document. This DID document is the main document that is stored in the blockchain that determines the ownership of a decentralized identity. According to the NIST standard (Lesarve, 2019), a DID document contains at least a set of authentication methods to prove ownership of the DID document, timestamp of creation and update of the DID and an encrypted proof of identity. In this area of responsibility, there is a need for the regulator and the related government institution to decide on what kind of attributes that should be stored in the digital identity. They are expected to also consult this to the service providers to get the insight of what kind of data that the service providers typically need from their users.

6.3.3 Trusted List Governance

This governance is needed to determine which authorities can be trusted in issuing certificates and verifying user claims for these certificates. In this case, the regulator or government can become the root certificate authenticator (CA) which becomes the trust anchor. On the other hand, the government can also create frameworks or provisions that allow other entities to get truss and become the root CA. The trusted list governance is one of the important area of responsibility that need to be discussed by the majority of the stakeholders. It is very important to reach the the agreement between stakeholders because it is the main mechanism that can ensure the validity of the registered users. Therefore, if the regulators decide to let the digital identity data to be stored decentrally, they will not have to be worry of the validity of the users data because there are trusted institutions that will be responsible to ensure its validity.

6.3.4 Key and Credentials Governance

By using the self-sovereign identity model, a digital wallet is the main component that will be required to store, manage and share identities and credentials. Ideally, control over this wallet is entirely in the hands of the users. This wallet can be in the form of hardware or objects they have, such as cards, or it can be in the form of software installed on the user's personal device. With this, users can control how they store and share the information contained in their digital identity. In this governance, several aspects need to be regulated, including:

a. Who has access to the user key and credentials
b. Under what conditions the user needs to display his credentials to other parties
c. How to backup this digital identity

d. Who can recover the key from the user's digital identity
e. And lastly, who is responsible if there is a loss or theft of keys and credentials

In this area of responsibility, the government, service providers and users are responsible to form the suitable process that can satisfy the needs of each party. The discussion between these parties are important so that there are clear roles on which organization are responsible in managing the credentials and data, including how the user can responsibly control their own data.

7 Conclusion

In this chapter, the results of the study carried out will be presented again to answer the main research question: “How can blockchain-based digital identity management be managed for Payment System in Indonesia?” In 7.1 the conclusions of the study will be described in order based on the previous chapters. These conclusions then also serve as answers to the research questions that have been set at the beginning of the study. In 7.2 we will discuss reflections and recommendations that can be given to actors who can play a role in the realization of payment ID. Then proceed with the study contribution in 7.3. The limitations of the study will be discussed in 7.4. Finally the study will be closed future research recommendations at 7.5.

7.1 Revisiting the research questions

The main objective of this research is to explore on how to manage and implement the blockchain-based digital identity in the payment ecosystem. This study begins with finding the main reasons for the need for an integrated digital identity in the payment ecosystem in Indonesia, what are the requirements needed, and what configurations are possible to realize it. Furthermore, this research is closed with how it impacts on the payment ecosystem that has been running and suggestions on the governance for the digital identity management.

RQ1: What are the Payment ID’s core requirements as the primary digital identity in the Indonesian payment system?

The purpose of this question is to find the design requirements that will be needed to find the type of blockchain approach that is suitable for implementing blockchain-based digital identity in the payment ecosystem. This RQ is answered by conducting a literature study on payment system regulations in Indonesia and interpreting the results of interviews collected as the main driver of the payment ID from both the regulator and market and user side. In formulating this requirement, the parties that are taken into account include: BI as regulator, Bank and Fintech Company as payment system service provider (PJSP), service provider like merchants (SP) and users.

No.	Description	Concerned Actor
Req.1	The Payment System Regulator (BI) have access to the digital identity data on granular level	Regulator
Req.2	Initial registration process should satisfy the regulator's KYC principle	Regulator, PJSP, User
Req.3	PJSP can access digital identity data that related with their services (e.g. registered users data on their system or KYC purpose)	PJSP
Req.4	Whenever a user wants to onboard a PJSP services, PJSP and Regulator can access the user's data, claim and certificate for KYC purposes to verify the validity of their data	User, PJSP
Req.5	Only selected and verified institution can issue and validate user's claims and certificates	Regulator, PJSP, User
Req.6	Service Provider can verify the validity of user's claim	PJSP, SP
Req.7	User's digital identity data can only be accessed by the consent of the identity owner	User
Req.8	User can limit or choose which data that can be shown to specified PJSP	User
Req.9	User can have access to the information on their own digital identity informations, and the information on which service provider and government institutions that has access to it	User
Req.10	individual and organization should be registered as a unique digital identity	Regulator, PJSP, SP, User,
Req.11	There should be one single source of truth that responsible in providing the correct digital identity data	Regulator, PJSP, User, SP

No.	Description	Concerned Actor
Req.12	There should be data governance mechanism to ensure the data integrity	Regulator, PJSP, User, SP
Req.13	The PaymentID can be used by SP within payment ecosystem, and able to create linkage with the existing or future digital identity	Governmen t, PJSP, SP, User
Req.14	The transition from current Siloed digital identity to the PaymentID should be carried out smoothly by ensuring the data interoperability	PJSP, User
Req.15	The system should be available 24/7 or during payment system working hour	Regulator, PJSP, User, SP
Req.16	A secure authentication method is needed and should require at least 2-factor authentication	User, PJSP
Req.17	Digital identity data should be stored securely	Regulator, PJSP, User
Req.18	There should be a mechanism to mitigate lost identity	User, PJSP

RQ2: What type of blockchain architeture is suitable for the PaymentID?

This section is intended to look for an approach that can be used as a reference to create a blockchain-based PaymentID. This implementation approach is prepared by considering the requirements that have been defined in the answer to the previous research question. Based on literature studies on taxonomy and blockchain components, this implementation approach will be seen from the main components of blockchain, namely: blockchain network types, consensus mechanisms, data storage methods, security.

Component	Description
Blockchain Network	Consortium Blockchain (Private Permissioned) because the payment system regulator need to have

Component	Description
	control over the data and ensuring the compliance within the digital identity
Consensus Mechanism	Proof of Authority
Data Storage	Hashed Identifier or the reference of users identity stored on-chain, while the identity details such as certificate, claims, or documents is stored off-chain. This approach is used to facilitate the scalability of the blockchain network.
Security	The reference that stored on chain will be encrypted using asymmetric cryptography, while the identity details will be encrypted using symmetric cryptography.
Access Control	Using RBAC (Role Based Access Control), the access to digital identity data will be restricted based on the role of the user; i.e. only selected government institution can have access to the data, SP can access data only for onboarding user and registered user under their system

RQ3: How will the actors and stakeholders in the payment ecosystem be impacted by implementing the blockchain-enabled PaymentID?

Impact analysis on the actor side will be described based on potential benefits and risks, this is done because this technology has not yet been implemented and is still in the ideation stage.

1. Payment System Regulator: benefits that will be obtained by payment system regulators, especially Bank Indonesia, one of which is access to detailed payment system user data without having to know the personal data of each user. In this way, regulators can use the data for policy analysis and supervision purposes. They can assign risk ratings and scoring to payment system actors which can later be useful for other government institutions that require such data, one of which is to monitor potential fraud and money laundering in more detail. The quality of the data captured by

the regulator can improve because digital identity data is standardized among the PJSP. Historical data related to user membership status in financial institutions can also be tracked and audited better. Security and data security can be guaranteed with encryption on the blockchain network. With digital KYC verification on user identity, regulators can minimize the use of physical documents in conducting CDD audits on PJSPs. This affects the efficiency of the regulatory work process in supervising PJSP activities.

2. Meanwhile, the challenges and dilemmas in implementing blockchain based digital identity are:

   In terms of data transparency, regulators have a choice, whether it is stored centrally, distributed among related institutions or decentralized. The more centralized the regulator will have more control over the data but the more it will lose data transparency, on the other hand if blockchain technology is used fully in a decentralized manner, there will be the potential that the regulator will lose control over the data. The same thing also concerns the verification process of data changes, where regulators can choose to be the central party that can verify or they can appoint certain parties as part of the consensus mechanism. If they choose to be the central party, of course, the verification process of data changes can occur quickly, but their transparency will also be questioned in the eyes of the market and the public.
3. Organizationally, it is necessary to think about how to form this blockchain consortium. BI as a regulator must also think about how the form of the initiative will be implemented, whether BI as a regulator will also act as a provider of blockchain network infrastructure or BI will only be the governing body and will cooperate with existing IdPs and other related authorities to build this blockchain network. Then BI also needs to think about whether there will be additional operational costs that need to be incurred by either BI or PJSP to maintain this blockchain network.
4. On the banking side and non-bank PJSPs (including e-wallet and e-money fintech) it is estimated that there will be many benefits, including: A more efficient KYC process, namely by checking claims on the digital identity of users who want to onboard their system or platform. With this efficiency, Blockchain Based PaymentID is expected to cut a lot of KYC costs and

shorten the user onboarding process. This KYC efficiency process also stated by Lootsma (2017) . In addition, because the user claim verification process in the blockchain can be traced and accounted for, this can potentially reduce fraud that often occurs in this payment ecosystem such as fake id, clone id account take over and etc. In terms of data security, PJSPs will also benefit because user data storage will be encrypted with public key cryptography and stored in a decentralized manner. With the blockchain network integrated with claim issuers, PJSPs also don't have to worry about the validity of the data provided by the user, because they can easily verify the claim issuer for the data provided by the user to them.

5. Apart from the benefits they get, there is also concern from PJSP regarding control over their user data, because with zero knowledge proofing, users can limit PJSP's access to their information. If this happens, PJSP also needs to adjust their strategy in terms of capturing user data which will also have an impact on their business processes. On the other hand, PJSP is also concerned with the costs they have to pay. The first is the investment costs they need to incur to adapt their existing system to the blockchain network in the future, the second is the operational costs they need to spend if there will be recurring costs for members of the blockchain consortium.
6. With this blockchain based digital identity, it can actually make it easier for the users to register or board on the PJSP platform. Users no longer have to fill out forms every time they register on the PJSP platform. they only need to register the claim and administrative documents required by PJSP on the blockchain based PaymentID. Furthermore, PJSP will perform KYC by verifying user claims through the blockchain network, matched with cryptographic proof from the authority issuing claims from the user. In this way users will have the convenience of being able to join the Payment System Platform thus enabling the financial inclusion. Daily transactions with merchants or service providers are also easier because users don't need to log in to various IdPs or SPs, they only need to use their PaymentID to authenticate payments, of course, provided that users have recorded their bank account ownership claims on PaymentID. this. On the other hand, this digital identity can also make it easier for users to apply for financial support to the government. They just need to show their paymentID along with the

claims they have without having to fill out paperwork. In terms of privacy and security, users will have full control over the information that they will share with institutions and SP it is called selective attribute disclosure.

7. Challenges that may hinder the adoption of this technology as well as the risks that may occur, is the resistance of users in registering themselves with PaymentID, this can occur because changes in business processes usually cause inconvenience and need for an adjustment process in managing this digital identity. Not to mention the low user awareness of data security, especially in Indonesia, which can lead to a low level of urgency for users to register themselves with PaymentID.

RQ4: What are the required governance process that needs to be formulated for PaymentID?

The governance processes that need to be formulated are divided 4 main area of responsibility, namely: Governance on block creation, governance on Payment ID Registry, Governance on trusted list, and finally governance on user keys and credentials.

- Governance in Block creation is another word for the consensus protocol that will be used by this blockchain network. If viewed from the main purpose of forming a Payment ID, it can use proof of authority which also involves banks and PJSP as authorized nodes. With the proof of authority, only certain nodes can authorize the creation of new blocks. The selection of proof of authority is necessary considering that PaymentID is a digital identity in which it stores sensitive information so that credible organizations are needed to be able to maintain this blockchain network. In addition, by involving regulators, bank representatives and PJSP representatives, decentralization will continue and the process of creating new blocks does not depend on one party alone.
- Governance in the decentralized identifier (DID) registration is done by determining what components are needed in making the DID document. This DID document is the main document that is stored decentralized in the blockchain that determines the ownership of a decentralized identity. According to the NIST standard, a DID document contains at least a set of authentication methods to prove

ownership of the DID document, timestamp of creation and update of the DID and an encrypted proof of identity.

- Meanwhile, Governance on the trusted list is needed to determine which authorities can be trusted in issuing certificates and verifying user claims for these certificates. In this case, the regulator or government can become the root certificate authenticator (CA) which becomes the truss anchor. On the other hand, the government can also create frameworks or provisions that allow other entities to get truss and become the root CA.
- Lastly the key and credentials governance is needed to ensure the accesibility of the digital Identity. In this governance, several aspects need to be regulated, including: Who has access to the user key and credentials, Under what conditions the user needs to display his credentials to other parties, How to backup this digital identity, Who can recover the key from the user's digital identity and lastly, who is responsible if there is a loss or theft of keys and credentials.

MRQ4: How can blockchain-based digital identity be managed for the Payment System in Indonesia?

Based on the current situation of the Indonesian payment ecosystem, requirements were identified and developed to determine the suitable blockchain architecture for implementing the blockchain-based PaymentID. Consortium Blockchain (Private Permissioned) with the Proof of Authority Consensus was chosen as the blockchain type as payment system regulators have to control and supervise the data, ensuring compliance within the digital identity. However, this decision also sparked a dilemma: centralising digital identity may give the regulators more control over the data, but it might lose data transparency in the public’s eye. On the other hand, if blockchain-based digital identity is stored decentrally, the regulators may lose control over the data.

Subsequently, to facilitate the needs of each stakeholders, we need to identify the area of responsibility on several governance processes in the blockchain-based PaymentID. The four main governance processes that are recommended in this study are: governance on block creation, governance on Payment ID Registration, governance on the trusted list, and finally, governance on user keys and credentials.

Furthermore, this study also reflects that implementing a blockchain-based identity in an established ecosystem is a complex task, not merely an IT project but also a change in the whole ecosystem. Therefore, collaboration between government institutions and stakeholders is critical.

7.2 Reflections

- The existing digital identity model commonly applied in most financial services in Indonesia is still silos or centralized in each financial service provider. In this model, the service provider stores sensitive data and user transactions centrally, doubling as the identity provider. Users are given access to their data by using login credentials and identity tokens, either through an application or physically. However, this model is vulnerable to cyber-attacks as the IdP also acts as SP. On the other hand, with too many digital identities spread over several SPs and IdPs, users are also burdened with having to adapt to various authentication methods. The KYC process when users onboard financial services also becomes redundant because they are required to fill in the same information repeatedly; on the other hand, the government is also challenged in supervising and conducting policy analysis as there is no standardization of digital identity- making it difficult to collect standard and granular transaction data in on digital platforms.
- Managing digital identity in Indonesia is challenging because the main problem is the integrity of citizen data. The silo nature of the responsible organizations is a leading cause of differences in citizen data among institutions. The low level of personal data security also causes low data integrity as it prompts fake IDs originating from stolen identities and synthetic identities. The public’s low awareness about the importance of personal data security also incites fake identity fraud often encountered during the onboarding process at fintech payment system companies in Indonesia.

- Technical factors are essential if governments want to implement this blockchain-based digital identity. Blockchain technology is still relatively new in Indonesia; few companies implement blockchain technology as a solution in their companies. This stems from the lack of information technology consultants in Indonesia who can do blockchain programming. This is why the lack of knowledge in blockchain technology remains a significant obstacle in adopting the technology within the industry (Cagigas et al., 2021).
- To realize a blockchain-based digital identity in the Payment System, a collaboration between government institutions is critical, as supported by the findings from (Yeoh, 2017). Collaboration is vital as the authority in managing blockchain-based digital identity is spread across various institutions in Indonesia. For example, in recording citizenship data, the central authority lies with the Ministry of Home Affairs. Meanwhile, the central authority lies with the Ministry of Communication and Information Technology regarding data privacy and security. With this in mind, collaboration is necessary to avoid conflict of interest between these authorized institutions.
- Governance on the operational side also needs to be discussed because maintaining a blockchain network is not easy. It needs to be decided which institution will be responsible for maintaining the system and ensuring the SLA of the blockchain network is fulfilled-otherwise, forming a new institution or organization to maintain the blockchain network can also be done. The decision related to this responsibility and governance should also be consulted among the stakeholders.
- This study only shows one scenario of blockchain-based digital identity for the payment ecosystem; however, many scenarios can be given on how it will be realized in the financial field. The results of this study also only represent the view of digital identity in Indonesia- thus, other countries may experience a different situation and may point to another direction.

7.3 Contribution

1. Academically, this discussion can provide an initial idea of using blockchain-based digital identity in the payment ecosystem setting in developing countries. This research also exploring the main driver that caused the need of a blockchain based digital identity. This research also trying to find out the main challenges that may arise during its development plan.
2. From the managerial perspective, this research contributes to identify what high level requirements are needed in developing blockchain based digital identity. In addition, discussions related to governance are also one of the aspects that need to be identified in developing a blockchain based digital identity, and in this study it is discussed based on the needs of the relevant actors and the scope of the payment ecosystem.
3. Furthermore this study shows another aspects of blockchain based digital identity besides its technical considerations. This study illustrates that implementing a blockchain based identity in an established ecosystem is a complex task where it is not merely an IT project but also a change in the whole ecosystem, ranging from the regulation, governance relationship between institutions and preparing resources that is capable in developing and maintaining blockchain based ecosystem. Therefore a whole transformation in the payment ecosystem is needed.
4. Digital identity is a digital representation of individuals and the key to the digital world, the fact that there is still lack of accesibility, data integrity and security awareness in utilizing the digital identity is a problem that a country should not oversee in the digital era. This study also try to add another perspective on how a digital identity can influence businesses in a certain field.
5. In terms of societal relevance, the results of this study are expected to help provide an overview to policy makers, regulators and public regarding the potential advantages and challenges of using blockchain based digital identity. The technical aspect of blockchain is not discussed in detail in this study, but we argue that this study can be a relevant part of the building block for governments in other developing countries like Indonesia to start developing blockchain-based technologies.

7.4 Research Limitations & Future Research Recommendation

1. The first limitation of this study is the number of country that is investigated is only one, which is Indonesia. Not to mention that the implementation of similar technologies in developing countries such as Indonesia is quite rare, so it is difficult to find a suitable implementation case as benchmark.
   - Recommendation: Future research on blockchain based digital identity can be done by involving more country that has similar condition and background. Furthermore research on benchmarking and comparing the development process of blockchain based digital identity in several countries can also be useful to identify the challenges or key factors for the digital identity development.
2. Secondly, the quality of the case studies is closely related to the quality of the researchers. This can lead to bias from the researcher's side which can affect the formation of conclusions from this study. However this challenge is mitigated by having a structured research methodology and carefully selecting the participants and interviewee so that the result can represent the condition that is currently happening in the payment ecosystem.
   - Recommendation: Future research on blockchain based digital identity for the payment system by including researchers from different background and point of view in approaching the case. For example studying the cost and benefit of blokchain based digital identity for the industries in the country that has already implement it.
3. Thirdly, there are some limitations in terms of collecting the interview data. Only limited number interviewee is interviewed because the topic is very specific and it requires respondents with a certain background and qualification. Some institutions, especially the government, also have a strict requirements to be able to conduct interviews. In addition, some interviewees answer the quesition very carefully and not openly express

their opinion, therefore it causes the transcription process become more time-consuming, because of the need to interpret their vague statement.

- Recommendation: Future research on blockchain based digital identity for the payment system can be done by including more diverse stakeholders and discuss the broader topics, such as the transformation in the regulation and governance process of related institutions.

4. Lastly, The results from research that are quite high level are not necessarily applicable to real world cases because there are still many factors that are not covered in this study. The interview method is carried out with semi-structured and open-ended questions so that a multitude of factors and aspects that influence the motivation and challenges of applying this technology are immeasurable.

    - Recommendation: several research on blockchain based digital identity for the payment system can be done further with in depth topics such as:

        i. Research to develop the design of a blockchain based digital identity platform that is suitable for the payment ecosystem with prototyping and experimenting approach to observe the socio-technical complexity of the system

        ii. Research related to the performance of blockchain based digital identity to find out what type of blockchain technology and configuration that has sutable performance for nationwide scale

        iii. Research on How change management is implemented in the transition process from the current digital identity to blockchain based digital identity.

Bibliography

Alsayed Kassem, Jamila & Sayeed, Sarwar & Marco-Gisbert, Hector & Pervez, Zeeshan & Dahal, Keshav. (2019). DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network. Applied Sciences. 9. 2953. 10.3390/app9152953.

Al-Riyami, S. S., & Paterson, K. G. (2003, November). Certificateless public key cryptography. In International conference on the theory and application of cryptology and information security (pp. 452-473). Springer, Berlin, Heidelberg.

Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the open blockchain. " O'Reilly Media, Inc.".

Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. European Business Organization Law Review, 20(1), 55–80. https://doi.org/10.1007/s40804-019-00135-1

Atzei, N., Bartoletti, M., & Cimoli, T. (2017, April). A survey of attacks on ethereum smart contracts (sok). In International conference on principles of security and trust (pp. 164-186). Springer, Berlin, Heidelberg.

Auernheimer, B. and Tasi, M.J. (2005), “Biometric authentication for web-based course examinations”, Proceedings of the 38th Annual Hawaii International Conference on System Science (HICSS'05), Big Island, HI, USA, pp. 294-300.

Ayed, Ghazi Ben. (2014). Architecting User-centric Privacy-as-a-set-of-services: Digital Identity related Privacy Framework. Springer.

Bank Indonesia. (2019). Indonesia Payment Systems Blueprint 2025 Bank Indonesia : Navigating the National Payment Systems in the Digital Era. 1–49. Retrieved from https://www.bi.go.id/.../Indonesia-Payment-Systems-Blueprint-2025-Presentation.pdf

Balasubramaniam, S., Lewis, G. A., Morris, E., Simanta, S., & Smith, D. B. (2009, March). Identity management and its impact on federation in a system-of-systems context. In 2009 3rd annual IEEE systems conference (pp. 179-182). IEEE.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.

Buchmann, J. (2013). Introduction to cryptography. Springer Science & Business Media.

Cameron, K., Posch, R., & Rannenberg, K. (2009). Appendix d. proposal for a common identity framework: A user-centric identity metasystem. The Future of Identity in the Information Society, 477.

Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernández-Gutiérrez, M. (2021). Blockchain for public services: a systematic literature review. *IEEE Access*, *9*, 13904-13921.

Castillo-Montoya, M. (2016). Preparing for Interview Research: The Interview Protocol Refinement Framework. Qualitative Report, 21(5).

Chadwick, D. W. (2009). Federated identity management. In Foundations of security analysis and design V (pp. 96-120). Springer, Berlin, Heidelberg.

CGI. White Paper : Public Key Encryption and Digital Signature - How do they work? (2004). url: https://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf.

Clark, Julia et al. A joint World Bank Group – GSMA – Secure Identity Alliance

Collier, Andrew. (2017). Shadow Banking and the Rise of Capitalism in China. 10.1007/978-981-10-2996-7.

Common Terminological Framework for Interoperable Electronic Identity Management," modinis IDM. [Online]. Retrieved from: https://www.cosic.esat.kuleuven.be/modinis�idm/twiki /bin/view.cgi/ Main/GlossaryDoc#4_13_Digital_Identity. [Accessed: Apr-2021].

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: beyond bitcoin. Appl. Innov. Rev.(2016). Sutardja Center for Entrepreneurship & Technology Report, Berkeley University. http://scet. berkeley. edu/wp-content/uploads/AIR-2016-Blockchain. pdf.

Dabrowski, M. and Pacyna, P.(2008). "Generic and complete three-level identity management model," in Emerging Security Information, Systems and Technologies. SECURWARE'08. Second International Conference on, 2008, pp. 232–237.

Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain enabled applications. Apress, Berkeley, CA, 72.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366-1385.

Digital Identity Towards Shared Principles for Public and Private Sector Cooperation. url: http : / / www . gsma . com / mobilefordevelopment / wp - content/uploads/2016/07/Towards- Shared- Principles- for- Public- and- Private-Sector-Cooperation.pdf.

Drescher, D. (2017). Blockchain basics (Vol. 276). Berkeley, CA: Apress.

Experian. (2019). 2019 Global Identity and Fraud Report . Retrieved from https://www.experian.com.sg/wp-content/uploads/2019/04/2019-APAC-Identity-and-Fraud-Report.pdf

Ferdous, M. S., Chowdhury, F. and Alassafi, M. O. "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

Garfinkel, S., Spafford, G., & Schwartz, A. (2003). Practical UNIX and Internet security. " O'Reilly Media, Inc.".

Given, L. M. (Ed.). (2008). The Sage encyclopedia of qualitative research methods. Sage publications.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic commerce research and applications, 29, 50-63.

Jacobovitz, O. (2016). Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva.

Jøsang, A., & Pope, S. (2005, May). User centric identity management. In AusCERT Asia Pacific information technology security conference (p. 77).

Keele, Staffs. (2007). “Guidelines for performing systematic literature reviews in software engineering”. Technical report, Ver. 2.3 EBSE Technical Report. EBSE.

K. Cameron, “The laws of identity, May 2005,” Microsoft Corp., 2005.

Kogure, J., Kamakura, K., Shima, T., & Kubo, T. (2017). Blockchain technology for next generation ICT. Fujitsu Sci. Tech. J, 53(5), 56-61.

Lakhani, K. R., & Iansiti, M. (2017). The truth about blockchain. Harvard Business Review, 95(1), 119-127.

Lamport, L., & Fischer, M. (1982). Byzantine generals and transaction commit protocols (Vol. 66). Technical Report 62, SRI International.

Laurance, T. (2017). Blockchain for Dummy.

Laurent, M., & Bouzefrane, S. (2015). Digital identity management. Elsevier.

Lee, J. H. (2017). BIDaaS: Blockchain Based ID As a Service. IEEE Access, 6, 2274–2278. https://doi.org/10.1109/ACCESS.2017.2782733

Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2019). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. https://doi.org/10.6028/NIST.CSWP.07092019-draft

Li, X., Niu, J., Khan, M. K., & Liao, J. (2013). An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, 36(5), 1365-1371.

Liu, Y., Lu, Q., Paik, H. Y., Xu, X., Chen, S., & Zhu, L. (2020). Design pattern as a service for blockchain-based self-sovereign identity. *IEEE Software*, *37*(5), 30-36.

Logical access security: The role of smart cards in strong authentication. 2004.

Lootsma, Y. (2017). Blockchain as the newest regtech application—the opportunity to reduce the burden of kyc for financial institutions. *Banking & Financial Services Policy Report*, *36*(8), 16-21.

Mukhopadhyay, M. (2018). Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity. Packt Publishing Ltd.

Maesa, D. D. F., & Mori, P. (2020). Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing, 138, 99-114.

Menkus, B. (1998). Understanding the Use of Passwords. Computers & Security, 7(2), 132-136.

Mertens, W., & Rosemann, M. (2015). Digital identity 3.0: the platform for people.

Modinis. (2005). Study on Identity Management in eGovernment. Common terminological framework for interoperable electronic identity management. European Commission / University of Leuven; 2005. (https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc)

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134-117151.

Mukhopadhyay, M. (2018).Ethereum Smart Contract Development: Build Blockchain-Based Decentralized Applications using Solidity. Birmingham: Packt.

Naik, N., & Jenkins, P. (2020, April). Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology. In 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) (pp. 90-95). IEEE.

Narayanan, A., J. Bonneau, E. Felton, A. Miller and S. Goldfeder (2016) Bitcoin and Cryptocurrency Technologies. Princeton University Press, Princeton, NJ.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 34(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Olson, Eric T. (2016). “Personal Identity”. The Stanford Encyclopedia of Philosophy. Ed. by Zalta, Edward N.

O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint.

Pernul, G. (1995). Information systems security: Scope, state-of-the-art, and evaluation of techniques. International journal of information management, 15(3), 165-180.

Pervan, G., & Maimbo, M. (2005). Designing a case study protocol for application in IS research. In Proceedings of the Ninth Pacific Asia Conference on Information Systems (pp. 1281-1292). PACIS.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking beyond banks and money (pp. 239-278). Springer, Cham.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. IEEE Consumer Electronics Magazine, 7(2), 18-21.

Rawat, D. B., Chaudhary, V., & Doku, R. (2019). Blockchain: Emerging Applications and Use Cases. arXiv preprint arXiv:1904.12247.

Richardson, B., & Waldron, D. (2019). Fighting back against synthetic identity fraud. McKinsey on Risk, 7, 1-6.

Robert K Yin. Case Study Research: Design and Methods. SAGE Publications, Thousand Oaks,

CA, 5th edition, 2014. ISBN 978-1-4522-4256-9.

Roubini N (2018) The Big Blockchain Lie by Nouriel Roubini - Project Syndicate. In: Proj. Synd. https://www.project-syndicate.org/commentary/blockchain-big-lie-by-nouriel-roubini-2018-10?barrier=accesspaylog.

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. John Wiley & Sons.

Sharman, R. (2011). Digital Identity and Access Management: Technologies and Frameworks: Technologies and Frameworks. Premier reference source. Information Science Reference. isbn: 9781613504994. url: https://books.google.nl/books?id=rAjoyoTv6qcC.

Simon, H. SAML: The Secret to Centralized Identity Management. 2004.

Simonsson, M., Johnson, P., & Wijkstrom, H. (2007). Model-Based IT Governance Maturity Assessments with COBIT.

Sriram Balasubramaniam et al. (2009). “Identity management and its impact on federation in a system-of-systems context”. In: Systems conference, 2009 3rd annual IEEE. IEEE., pp. 179–182.

Swanson, T. (2015). Explore the Blockchain, Ignore the Bitcoin Maximalists. American Banker, 1(170).

Tapscott, D., & Tapscott, A. (2016). The impact of blockchain goes beyond financial services. Harvard Business Review (Retrieved from https://hbr.org/2016/05/the-impact-of-the-blockchaingoes-

beyond-financial-services).

Tasca, P., & Tessone, C. J. (2019). A taxonomy of blockchain technologies: principles of identification and classification. Ledger 4 (2019).

Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. The Sovrin Foundation, 29(2016).

Treiblmaier, H. (2019). Combining blockchain technology and the physical internet to achieve triple bottom line sustainability: a comprehensive research agenda for modern logistics and supply chain management. Logistics, 3(1), 10.

Windley, P. J. (2005). Digital Identity: Unmasking identity management architecture (IMA). " O'Reilly Media, Inc.".

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. (2017, April). A taxonomy of blockchain-based systems for architecture design. In 2017 IEEE international conference on software architecture (ICSA) (pp. 243-252). IEEE.

Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security*, *99*, 102050.

Yin, Robert K. (2014). Case Study Research Design and Methods . Thousand Oaks, CA: Sage. 282 pages. Canadian Journal of Program Evaluation, 30(1).

Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. (2016) Where Is Current Research on Blockchain Technology? A Systematic Review. PLOS ONE 11(10): e0163477.https://doi.org/10.1371/journal.pone.0163477

Zhang, Y., Zheng, J., and Ma, M. (2008). Handbook of Research on Wireless Security. Handbook of Research on Wireless Security. Information Science Reference, 2008. isbn: 9781599048994. url: https://books.google.nl/books?id=b3r81GCpOnYC.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

Zīle, K., & Strazdiņa, R. (2018). Blockchain use cases and their feasibility. Applied Computer Systems, 23(1), 12-20.

Appendices

Appendix A. Interview Questions for Bank Indonesia

General Questions:

1. What are the main objectives of the implementation of the Payment ID?

2. What are the triggers/reason behind the implementation of this Payment ID?
3. Can you tell us the involved actors and stakeholders of the Payment ID?
4. Are there any milestones in the Payment ID implementation? which milestone is the current status?
5. What are the benefits for the organization to implement the Payment ID? How?
    1. Cost reduction,
    2. Competitive advantage,
    3. Faster business processes,
6. Who is the one who will operate and maintain the system (if any)? Does your organization consider being more active in this case? Why?
7. What are the main socio-and technical challenges?

Questions about realizing paymentID

1. What are technological barriers in implementing the PaymentID? How can your organization overcome such barrier? Is there any help from the system owner? If yes, how?
2. What are the impacts of the barrier(s) toward the implementation process? Is there any additional cost to overcome this kind of barrier(s)?
3. What is the architecture of the system (if any)? Do you know why such architecture is chosen for this system? What are its advantages and disadvantages?
4. Is there any specific software and hardware required to implement the system? Who is/are the provider(s)? Who is responsible to ensure the interoperability of the system?
5. Would you like to describe the activities/use case of PaymentID?
6. Who is responsible for developing the Payment ID system (if any)?
7. How are users involvement in the development process? Do you think this is important for end-users to be involved in the development?
8. How will user data be stored? Will it be kept by your organization?
9. How the system ensures the privacy and security of the users or sensitive data shared by users?

    -What type of security that will be incorporated in PaymentID?
10. What is needed before you can implement the system?
    a. Technological knowledge? -so far its okay, text mining, entity resolution
    b. Clear responsibilities between stakeholders?
    c. Collaborations between organizations?
    d. Regulations?
    e. Stakeholder?
11. Can you please explain how the PaymentID can verify the identity of payment system user?
12. Are there any standards or compliance that should be followed when implementing the PaymentID?
13. Is there any need to maintain the KYC or maintain or trace the digital identity data of the user? If so, how do you think PaymentID enables this activity?

14. If the PaymentID is implemented, who do you think will be the Identity Issuer?
15. If the PaymentID is implemented, who do you think will be the Identity verifier?
16. Is there a risk of fraud in the use of digital identity? Do you have any approach to avoid fraud within the digital identity?

Organizating paymentID questions:

1. How is the implementation of the PaymentID related to your organization's strategy?
2. How many users or department will utilize the PaymentID system/data in your organization?
3. With which partners or stakeholders do you need to collaborate for the initiation of PaymentID?
4. How is the resource management for the system's implementation? How do you deal with the skills and knowledge required to operate the system? Does your organization need to make changes to implement the system? Why and how?
5. What are the organizational barriers to implementing the system? How can your organization overcome such barrier?
6. What are the impacts of the barriers to the implementation process?
    a. Any new measurements?
    b. Is there any additional cost?
7. What organizational changes are needed before you can implement the system?
    a. New department?
    b. New regulations?

Blockchain-Based Digital Identity context questions:

1. Related to the benefits of Blockchain technology, in your opinion, will it bring any benefit if it were implemented as the basis for PaymentID?
2. If the blockchain technology were going to be implemented for the PaymentID, What are the organizational barriers in implementing the system? How can your organization overcome such barrier?
    a. Technical knowledge?
    b. Law & Regulations?
    c. Organizations?
    d. Inter-organization collaboration?
3. How do you think the data of the users will be maintained? Is it okay if the user data is not kept by your organization but by another party or governmental organization?
4. In your opinion, what are the risk of implementing digital identity using blockchain technology?

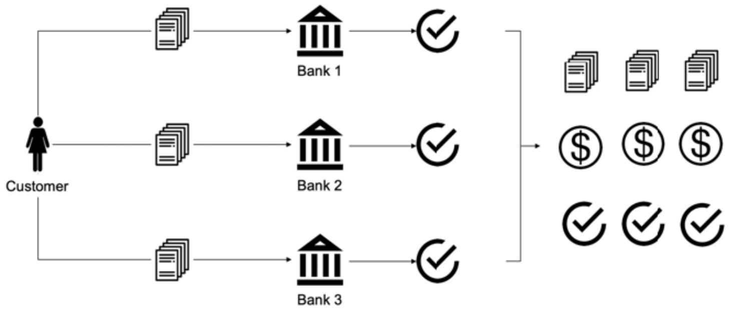
Appendix B. Interview Questions for Bank and PJSP

1. What is your organization's type of business?
2. During this time, how was the user onboarding process on the platform in your organization?
3. How is the KYC process carried out during the onboarding process?
4. Does your organization use a digital identity platform to identify or KYC new users in your application?
5. Have you ever experienced or heard of challenges or problems related to users on your platform? Example:
    a. Registration difficulties
    b. Identity theft
    c. Fraud
    d. Misuse of personal data
6. If yes, what is the solution?

7. So far, how does your organization verify users?

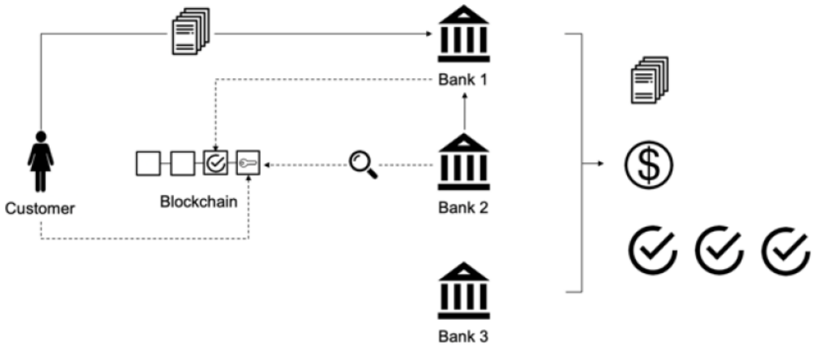
8. So far, how does your organization protect user identity?

9. Look at the diagram below:
    a. Scenario 1: Registration & KYC user existing condition



Source: Adapted from Parra-Moyano and Ross (2017)

    b. Scenario 2: User registration & KYC with blockchain technology:



Do you have any idea on what is the change in this process? How it diffes with the existing business process?

10. In your opinion, what are the conveniences that can be obtained with the above concept:
    a. Cost reduction?
    b. Competitive advantage?

c. Faster business processes?

11. To realize the Payment Ecosystem above, what aspects need to be considered?
    a. Socio-technical factors?
    b. Technical knowledge/skills?
    c. Laws & Regulations? There needs to be a change in regulations
    d. Organization?
    e. Collaboration between organizations?
    f. Interoperability?
    g. Standardization?
    h. Service Level Agreements?

12. What risks might occur in the above scenario?

Appendix C. Blockchain Technology

Blockchain Structure

Behind how the Blockchain process works, of course there are important parts that are structured so that Blockchain can be used. According to Laurance (2017), the structure of Blockchain consists of 3 main component parts, namely:

a. Block

Blockchain is composed of many blocks that represent a list of valid and stored transactions. Each block has a cryptographic hash as a pointer or as the identity of each block so that they can be connected to each other. According to Antonopoulos et al., (2017) the structure of a block consists of a header, followed by metadata and a list of stored transactions. The following is an explanation of the components that exist in each block on the Blockchain network:

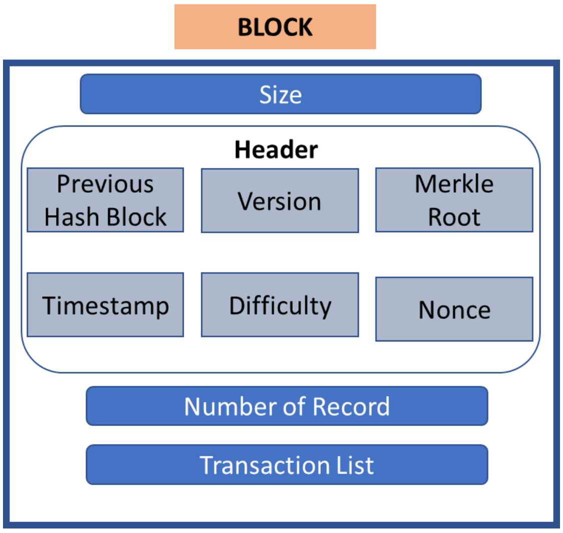


Figure 0.1 Block Structures

1. Block Size is the first part of the block structure that stores information related to the size of a block in bytes.
2. The Block Header is part of a block that has a size of 80 bytes and stores a set of metadata, such as:
   a. Version: Stores version information of a block and has a size of 4 bytes.
   b. Previous Block Hash: Metadata that stores the hash of the previous block, also functions as a “chain” that links the block with the previous block and has a size of 32 bytes.

c. Merkle Root: It is a collection of information from all transactions that have been hashed on the block with a size of 32 bytes and aims to provide conclusions from all transactions carried out by the block.

d. Timestamp: Stores information related to timestamp or when the block was created with a size of 4 bytes.

e. Difficulty Target: Stores information related to the difficulty level of the PoW (Proof of Work) algorithm used and has a size of 4 bytes.

f. Nonce: This is a random number stored with a size of 4 bytes and used in the process of mining new blocks.

3. The number of records is the part of the block that counts the number of transactions carried out and usually has a size of 1-9 bytes.
4. Transaction List is a section that stores a collection of transaction data that has been carried out on a block with varying data sizes.

b. Chain

So that each block on the Blockchain is connected to each other, a "chain" in the form of a hash is needed that connects one block to another block. The hash mechanism is one of the mathematically complex concepts to be applied to Blockchain. Although Blockchain is considered the latest technological innovation. However, not with hashes. The concept of hashing has certainly been around for about 30 years, and is used in the Blockchain concept because hashes can only create one-way functions that cannot be decrypted. A hashing function creates a mathematical algorithm that maps data of all sizes into character bits which are usually 32 characters long, where the length of the bit size represents the hashed data. Secure Hash Algorithm (SHA) is one of the hash functions used by Blockchain, while the algorithm commonly used to hash on Blockchain uses the SHA-256 algorithm which can change the length of any data size into a hash character with a size of 256 bits (32 bytes). , so that on the Blockchain, the hash can be considered as a unique digital fingerprint of the data on a block to lock the block so that it remains sequential in the Blockchain.

c. Network

The term network on Blockchain is a representation of the number of nodes or computers that are connected to each other and run an algorithm to secure the network. Each node has a record of all transactions recorded on the Blockchain.

These nodes are located all over the world and are managed by everyone who is part of the Blockchain network. It is very clear related to the network topology used by Blockchain, namely Peer-to-Peer, in which all nodes can communicate with each other from one node to another to receive and send messages.

Blockchain Ledger Storage

On-Chain Storage

The blockchain ledger satisfies the ground rules related to internal consistency. Internal consistency that described as creating 'internally coherent data structures that can keep consistent records of transactions' (Dhillon, Metcalf, & Hooper, 2017, p. 15). Blockchain ledger Reflects the 'historical and current state is managed by blockchain' (Dinh et al., 2018, p. 1368). Transactions in blockchain ledgers are stored in blocks linked to cryptographic hash pointers. each block that has made a transaction will be stored on the Blockchain and each transaction has a hash value obtained from the hash value of the previous block then entered into the block, then to calculate the new hash value, so that the hash can be considered as a pointer or link from each of these blocks. However, the hash value obtained must meet certain requirements called difficulty in order to get a valid block.

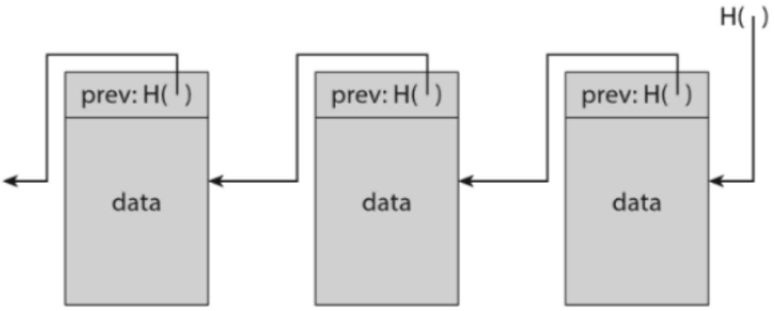


Figure 0.2 Blockchain and Hash Pointers
(Zheng et al., 2017)

For example, if a block is likened to the notation 'i', then block i+1 contains the hash of block i, as well as block i in which there is a hash of block i+1 This structure allows for tamperproof capabilities, because if the information contained in a block has been modified, the hash associated with that block will be different, so that inconsistencies can be detected.

Off-Chain Storage

Data can not only be stored in the blockchain ledger. By storing data outside the chain (Off-chain). This method can increase the performance of a system and it is more efficient than on-chain storage. By storing data off-chain, the computational load of a platform will be reduced (Xu et al., 2017). Moreover, this can increase the confidentiality aspect of the data because this data is not directly accessible to the nodes connected to the blockchain system. Off-chain storage can be done by storing the pointer or reference address of the data on-chain (inside the blockchain network). This reference also needs to be hashed to ensure the integrity of the document so that those who have access to this document can ensure its integrity.

Security

Security is an important component of blockchain technology, especially in the cryptographic aspect, so it is often mentioned in the literature (Dinh et al., 2018). Cryptography is a way to hide data and display data through encryption and decryption. The general purpose of cryptography is to ensure the security of data in the blockchain network. In blockchain technology, the use of cryptography is divided into 2, namely to validate transactions and link blocks to ensure the integrity of the blockchain ledger (Narayan et al., 2016).

Cryptography

Based on Buchmann et al. (2013) cryptography is a set of algorithms and keys. This cryptographic algorithm is divided into 2, namely:

- Symmetric Key Algorithm: in this method the encrypted information will be a cyper text. This cyper text can only be read by the party who has the key. The number of keys in this algorithm is only 1 and this key will be shared by the sender to the recipient so that the recipient can access the encrypted info.
- Asymmetric Algorithm: Unlike the symmetric Key Algorithm, in this algorithm each entity will have a pair of public and private keys. In the encryption process, the data will be encrypted using a public key sender. While in the decryption process, the key used is the private key of the recipient. Furthermore, to ensure that the data sent is valid data, the

sender must also encrypt it using its private key, so that the recipient can check by decrypting it using the sender's public key.

In general, asymmetric algorithms are more complicated than symmetric algorithms, however, asymmetric algorithms can provide higher security.

Hash

Hashing is a process to convert all input data into output data consisting of random characters with a predetermined length and can be determined as a unique character for each data that has been processed. Regardless of the length of the string that is entered, the output data has a fixed length, and the hashing process ensures that if there is a slight change in the data that has been entered, it will change and affect the results of the output data. Based on Buchmann et al. (2013) the hash function can be described as follows:

- Consistent: because a hash will always refer to the same message or information
- Unique: the probability that two different messages will have the same hash is almost zero
- Cannot be inverted so it is very difficult to find out the original message or information just by having the hash result

In addition, the hash on the Blockchain is also used as a pointer or link between blocks and is used to generate and validate new blocks. For example, the Sender of information can perform calculations from a hash and attach it to the message. The recipient who receives it can recalculate the hash that was pasted with the same function, if the results are similar then the message is still safe, otherwise it means that there has been manipulation by another party before the message is received by the recipient.

Zero Knowledge Proof

According to Yang & Li (2020) Zero-knowledge proof (ZKP) is one of the cryptographic techniques on blockchain technology that is used in the interaction between the profer and verifier. By using ZKP Profer can prove the truth of a specific information without having to display the details of the information. For example, when an SP requires the user to be 21 years old and over to be able to utilize one of their facilities, the user can prove that he or she has met the requirements without having to reveal how old he is. This way users will have control over what information they can display to the SP acting as a verifier. With the ZKP method, blockchain technology can fulfill one SSI requirement, namely *minimization*, where, users only need to display minimal data to be able to prove credentials.

Smart Contract

A smart contract is a set of agreements that is converted into digital form so that violations of the agreement are difficult to do. The Ethereum smart contract is a computer protocol that functions to facilitate, verify, or enforce digital negotiations written through program code. Smart contracts work without going through a third party and has a credible transaction process so that it cannot be hacked or changed (Atzei et al., 2017). Smart contracts are stored along with their transactions on the Blockchain. Blockchain uses distributed peer-ro-peer network technology, so Blockchain is the most secure storage place for digital data such as cryptocurrency, smart contracts, property, stocks, files, or any other valuable data with confidentiality, integrity and authenticity. Blockchain consists of several lists of blocks that are constantly growing and linked by cryptographic algorithms. It is based on Distributed ledger Technology (DLT) which is a system for recording digital transactions in distributed storage without having centralized storage (Atzei et al., 2017). By using smart contracts, we can exchange data, money, property, shares or anything in a transparent way, without conflict and without intermediaries. Smart contracts can provide more security over traditional contract law while also reducing other transaction costs associated with the contract. Various cryptocurrencies have implemented this type of smart contract (Mukhopadhyay, 2018). What's more, smart contracts don't just explain rules and penalties like those in traditional contracts. But also automatically ensure that the things in the contract are enforced (Mukhopadhyay, 2018).

Consensus Mechanism

The consensus mechanism is the process by which nodes validate transactions on the ledger. The consensus mechanism is the main characteristic of blockchain because there is no central authority that does validation but nodes.

This is commonly discussed as the Byzantine Generals Problem (Lamport et al., 1982). It is said that a group of generals who led the Byzantine army did not agree on war because some generals wanted to attack but some wanted to retreat. It is said that they will be successful in the war if all the generals agree to attack. To reach this point, a consensus is needed. Similar to this incident, in the process of determining consensus, the parties who are members of the blockchain network do not necessarily know each other, but they must reach a consensus to validate new transactions. In this regard, because there is no central node that controls this, a protocol is needed. The consensus protocol will be discussed further in this part.

Proof Of Work (PoW)

Proof of work was first put forward by Satoshi Nakamoto to solve the problem of double spend on Bitcoin. This Proof of Work is commonly found on the Public Blockchain because every node incorporated in it has the right to be able to participate in the consensus process. Nodes that are members of the Public Blockchain can also be referred to as miners. Miners need to solve complex math puzzles in new blocks before passing the blocks to the ledger. After completing the puzzle, the final solution is passed on to the other nodes and validated by them before being accepted into their respective ledger copies. The PoW rule defines that nodes must adopt a working fork, and it is highly unlikely that two competing forks will produce the next block together. The blockchain core suite protects against double-shopping by authorizing each transaction using a Proof-of-Work (PoW) mechanism. Transactions are finalized and approved by minors after ratification. If anyone tries to duplicate a transaction, it will show in the series that it is fake and will not be accepted. You may not double spend, once the transaction is passed.

Proof of Stake (PoS)

PoS is a surrogate approach to PoW that requires less CPU computation for mining. While this is also an algorithm, and the purpose is the same as PoW, the process is quite different here. As in the case of PoW, miners are rewarded by solving mathematical problems and creating new blocks, in Proof-of-Stake, the creator of a new block is selected in a certain way, depending on his wealth. The higher the stakes or in this case the value or the coins that a nodes have the more likely they will be chosen as the validator of the new block. This approach is more efficient than PoW as it discards the heavy computation. The downside of this method is there is a risk that the network will be controlled by some wealthy nodes that has heavy stakes.

Practical Byzantine Fault Tolerance (PBFT)

PBFT is a consensus algorithm based on voting. Transactions are executed on a round basis. Each round will determine a node that acts as a leader whose role is to order transactions, while the rest are treated as backup nodes (Xu et al., 2017; Zheng et al., 2017). In this PBFT, at least if 2/3 of the total nodes in the network approve the addition of a block, the block will be added to the blockchain. In PBFT the identity of the nodes must be transparent in order for transactions to be validated. This can complete the solution if there are 1/3 of the total nodes showing faulty behavior that resembles the Byzantine general problem

Proof of Authority (PoA)

Proof-of-Authority (PoA) is a consensus protocol that can solve the Byzantine General Problem by selecting trusted parties to participate in the consensus (Dinh et al., 2018). With the POA, the identity of the joining nodes must be known and have a reputation. There is also a need for standards and governance in selecting validator nodes. This consensus method is commonly used in private consortium blockchains because it is easier to determine a trusted authority in order to maintain system integrity (Tasca and Tessone, 2019). Since the number of validators is fixed and is not affected by the number of nodes on the network, this solution is highly scalable. On the other hand, the main challenge in PoA is to find and maintain validators that are trusted by participants.