Conference Paper

QR Code Payment in Indonesia and Its Application on Mobile Banking

Ruslan[1], Gusti Made Karmawan[3], Suharjito[1], Yudi Fernandoand[2], and Anderes Gui[3]

[1]Computer Science Department. BINUS Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta, 11480, Indonesia
[2]Faculty of Industrial Management, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Gambang, Pahang, Malaysia
[3]Information Systems Department, School of Information Systems, Bina Nusantara University, Jakarta, 11480, Indonesia

Abstract

The technology innovation makes it easy for us to connect to various services. Banking transactions that previously could only be served only at Branch Offices, ATMs (Automatic Teller Machines) and EDC (Electronic Data Capture), now they can be accessed online. Balance information, fund transfers, credit purchases, PLN tokens, payment of PAM and BPJS bills, all can be done through Mobile Banking application from smartphones. This study aims to find out how QR Code on Mobile Banking provides convenience in making payment transactions and how it can be used safely. The research was conducted through literature study, observation, and distribution of questionnaires to 30 respondents to identify the system acceptance. Payment Model QR Code on Mobile Banking can be widely used as an alternative of cash payment through a smartphone. The developed system does not only for merchant payment but can be used for person to person payment. The result of this research is a prototype for QR Code Payment on OCBC NISP Mobile Banking which can be used as an alternative payment system and integrated with fund source account without the need to top up the transfer.

Keywords: Mobile Technology, QR Code. Code Payment, Banking.

Corresponding Author:
Anderes Gui
anderesgui@binus.edu

Received: 5 August 2019
Accepted: 14 August 2019
Published: 18 August 2019

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FGIC2019 Conference Committee.

1. Introduction

How smartphones and internet technology have changed our lives. They help us connect to various activities including banking service which previously only be served in Branch Offices, ATM machines or through EDC. Banking today can be accessed from a smartphone. We can inquiry the balance, bank transfer, and pay the bills. All those processes can be done through Mobile Banking application. (Robson, Lee, East, Lim, & Chia, 2017). Currently, the global landscape payment system also continues to evolve following the trend of technological improvement.

How to cite this article: Ruslan, Gusti Made Karmawan, Suharjito, Yudi Fernandoand, and Anderes Gui, (2019), "QR Code Payment in Indonesia and Its Application on Mobile Banking" in *FGIC 2nd Conference on Governance and Integrity 2019*, KnE Social Sciences, pages 551–568. DOI 10.18502/kss.v3i22.5073

The National Non-Cash Movement, which has been initiated by Indonesia's Central Bank in 2014, aimed to build public awareness of non-cash payment instruments. Then continued to launch the National Payment Gateway (NPG) in December 2017, for all domestic payment transactions by card can be processed domestically interconnected and interoperable for all EDC or ATM owned by other banks. NPG is removing the barriers that have been created through the rules of each bank. To support NPG Movement, such as Toll Road Transactions, Transjakarta and Commuter Line Payment have been shifted to the non-cash payment transaction, and now we can pay by e-money. By regulation, according to PBI Number 11/12/PBI/2009, the Financial Services Authority (OJK) has allowed electronic money to be issued by the non-bank institution. Telkomsel as the telecommunication company, also participated in developing e-money through a product called Tcash Wallet that a server-based non-cash payment system which can be used for payment at the merchant. Online transport modes such as GoJek and Grab by using mobile applications have implemented server-based non-cash payment systems (Robson, Lee, East, Lim, & Chia, 2017).

In the Digitalization Age, smartphones are ubiquitous and have become a primary requirement. We can find various services and get the benefits in every activity. Including the payment process, it is becoming easier with a smartphone. Payment through a mobile application is also known as mobile payment. Here is the type of mobile payment based on technology (Stiphout & Nausea, 2017):

1. Proximity Payments also called Contactless Payments or Close Payments. We can use Near-Field Communications (NFC) technology and QR Codes (Quick Response Code). NFC needs the contactless reader to communication between devices. QR Code does not require a reader but needs a smartphone camera to scan the QR Code for communicating between devices;

2. Remote Payments, also known as Distant Payments, for example, SMS Banking and USSD (Unstructured Supplementary Service Data). The SMS format sent, and the USSD instruction (e.g., * 141 * 28 #) from the smartphone will be processed on the server.

PCI Security Standards Council as one of the official security agencies recommends to secure the online transaction have to use the Multi-Factor Authentication method from 2 (two) different channel authentication or more. This process will prevent, if one of the authentication sources is not available or provides an incorrect response, then the transaction cannot be processed (PCI Security Standards Council, 2017). NFC, QR

Code or Biometric are categorized have technology maturity and can be alternative for the authentication process. However, NFC and Biometric require the availability of NFC Reader and Biometric requires Scanner. But not all smartphones support NFC Reader and Biometric Scanner. That is the difference for QR Code, support for all types of smartphones because QR Code only needs of the camera for the scan (Stiphout & Nausea, 2017). This research is focused on QR Code on Mobile Banking. How can provide convenience on payment transactions? How can be secured to use?

2. Literature Review

2.1. Mobile Banking

It is one of the channels provided by the Bank to make it easier for customers to access online banking services through smartphone applications. The main services available on Mobile Banking are the same as those available at branch offices, ATMs and EDCs (Sachdev, 2014), among others:

1. View Account Balance
2. Transfer Funds
3. View Monthly Statement
4. Locate an ATM or Branch
5. Bill Payments

2.2. Mobile Payment Technology

Mobile Payment is the transaction payment through a mobile application or mobile banking. By 2020, multiple devices will be connected to an integrated ecosystem payment with improvised authentication process (Shah, Roongta, Jain, Kaushik, & Awadhiya, 2016). Mobile Banking application has become the flagship channel of banking. Customers can use the banking service without having to come to a branch office. Payment method on Mobile Banking application is divided into 2 (two) categories, namely: Proximity Payment and Remote Payment. Proximity is the payments made without requiring a direct contact (contactless payment). Use NFC sensors to detect the other close objects. Example MasterCard® PayPass ^{TM} and Visa® payWave ^{TM}, which enables to make payments through smartphone apps without the need for physical use of MasterCard cards /Visa. Also, Remote Payment is the payment transactions will be processed on the server. For examples: transaction on a web application with security authentication will directly send the token to a smartphone to authorize payment transactions.

2.3. Quick Response Code

Known as QR Code is a two-dimensional barcode type that can be used to represent information into square-shaped patterns that can be read by using QR Scan through a smartphone camera. QR Code stands for Quick Response, which can be decoded with high speed. Designed by a Japanese company called Denso Wave in September 1994 to track inventory vehicle manufacturing in the automotive industry. QR Code consists of a black module arranged in a rectangular pattern that represents a good 2-dimensional information, which can be read from both vertical and horizontal directions. This is what distinguishes the 1-dimensional barcode with only one-way data, which is generally vertical. The advantages of QR Code in addition to having a large data storage capacity of 7.089 for the numbers, 4.296 for the data of both letters and numbers, 2, 953 bytes of binary (8 bits) and 1.817 Kanji / Kana Japanese symbols, extensive encoding coverage, can be printed with mini size, hypervelocity / very fast readability, strong error correction capabilities, resistance to damage and can remain legible with 360 degrees conditions (Liu & Liu, 2006). QR code systems are also accepted outside the automotive industry due to the ease of use and speed of the reading process and greater storage capacity compared to standard UPC barcodes. (Dennehy & Sammon, 2015).

Currently, with existing developments, the QR Code has become an effective alternative that can be scanned through any smartphone camera. The error correction ability can facilitate data repair even under conditions with most cases of corrupted code. Smartphones are now equipped with QR Code decoding software. Additionally, QuickMark and i-nigma are cost-free tools available for many models and production devices to decode QR Code. (Chang, 2014).

2.4. One Time Password (OTP)

OTP is a mechanism for accessing system services by using a unique password that can only be used once. This mechanism is a powerful form of authentication and offers more effective security to corporate networks, online applications, and other systems that contain sensitive data. This can prevent identity theft by making sure passwords cannot be used a second time. (Chang, 2014).

2.5. Multi Factor Authentication (MFA)

As shown in Fig. 1. a basic concept with a combination of authentication channels can be defined with one of three categories below:

1. Something you know: secret, like password, PIN.
2. Something you are: biometrics, like fingerprint, face, eyes, sound.
3. Something you have: device or object or the like, such as ATM / Debit card, mobile phone.

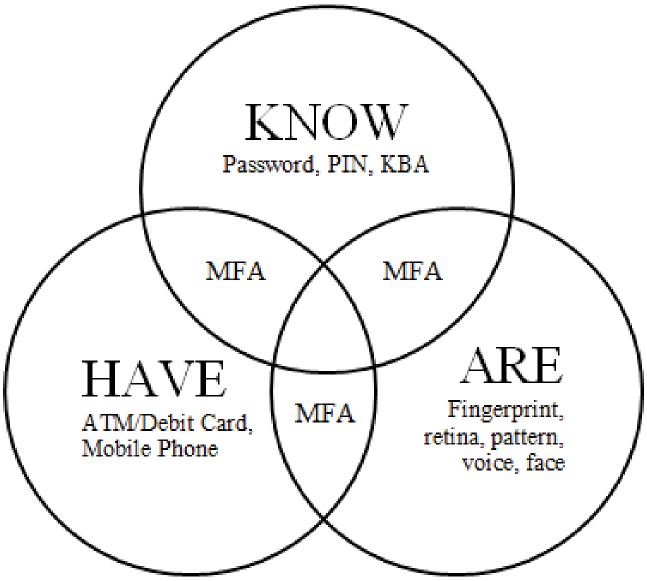


Figure 1: Security Concept Mobile Phones.

This approach can be easily identified when phishing occurs, and the root cause of overreliance in the first category is something you know. The solution is to switch from dependency using static credentials to dynamic credentials. To get strong authentication, we can use in parallel two or more different authentication credentials with different categories. This is a process known as Multi-Factor Authentication (MFA). (Dmitrienko, Liebchen, Rossow, & Sadeghi, 2014). Moreover, if the authentication credential comes from 2 different channels, then it is called Two Factor Authentication (2FA).

Online Banking is a powerful example of authentication, using the MFA as the standard. In the current application, the first factor uses a PIN or password to log into the application. So the second factor is obtained from OTP automatically generated as Token which is then sent with SMS format to the registered mobile phone number (if using internet banking, OTP can also be obtained from Hardware Token which then displayed to Token screen). Next, the customer returns OTP to the bank by inputting to the OTP confirmation screen in the application. If appropriate, then this second authentication factor is considered to be successfully verified, and the transaction may proceed. (Gandhi, Salunke, Ithape, Gawade, & Chaudhari, 2014).

2.6. Technology Acceptance Model (TAM)

TAM consists of several supporting factors to assess whether the application is acceptable and usable by the user. User Acceptance is the factor that determines the success or failure of an information system project. TAM can be used to find out why a user accepts or rejects a specific information technology or application system and how its acceptance is affected by system characteristics. Supporting factors for assessing user acceptance of the application can be seen in Figure 2:

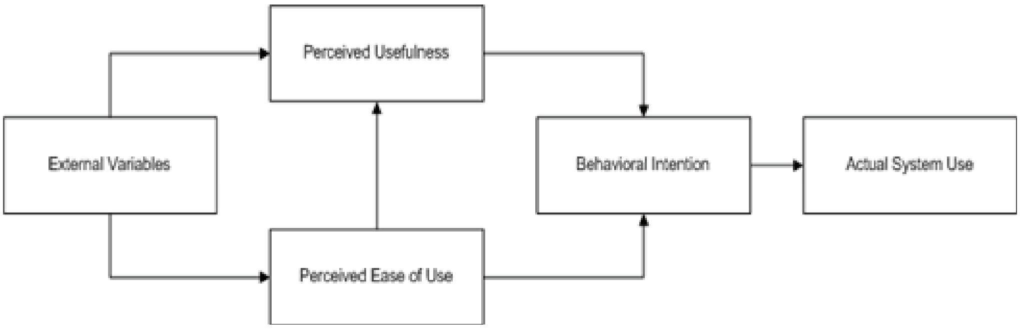


Figure 2: Technology Acceptance Model (TAM).

Here is the explanation of the supporting factors above:

1. External Variables, an external factor of the system that influences Perceived Usefulness (PU) and Perceived Ease of Use (PE), e.g., training system usage, implementation process, user involvement in system development, documentation, support from the consultant and so on.

2. Perceived Usefulness (PU), is the level at which a person believes by using a system to improve the performance of his work. This factor is a major factor that determines a person's desire to use a system. So this factor directly affects the Behavioral Intention of Use (IU). With the increase in job performance, a person

has been using automated systems will instantly increase his desire to continue using the system.

3. Perceived Ease-of-Use (PE), the degree to which a person believes by using a system can reduce the effort required to complete a job. This factor is the second factor after Perceived Usefulness (PU) so that this factor directly affects Perceived Usefulness (PU). With minimal effort in completing the job automatically, the performance of a person's work will increase.

4. Behavioral Intention to Use (IU), the degree to which a person feels a system can have a positive impact on the job and believe using a system can improve performance and reduce the effort in completing its work and have a desire to continue to use it. This factor is influenced by Perceived Usefulness (PU) and Perceived Ease of Use (PE).

5. Actual System Use (AT), is the actual use of the system by the user.

2.7. Related Research

Hayashi, et al. (2014), describes the implementation of the QR Code on the Starbucks Prepaid program in 2011 has increased the use of smartphones for Starbucks in-store purchases. Merchants put QR Code on posters and advertisements to inform customers of QR scans via smartphone to get coupons or promotional and product information. In this research, it is submitted that QR Code Technology can be applied with very low cost.

Sachdev (2014) defines the Four Pillars of Mobile Payment to help financial institutions determine mobile payment strategy:

1. Self-Paying: intended for transfer to bank account itself through mobile deposit and funds transfer capabilities feature

2. Paying Other People: uses Person to Person Payment / P2P features for individual or group payments.

3. Paying Biller: making a payment to the biller through a mobile application owned by financial institutions or applications owned by the biller.

4. Paying Merchant / Retailer: is for payment transactions on purchases at merchants using NFC sensors, QR code, cloud, or online.

Zlot Bezhovski (2016), found that the frequency of use of mobile payment for online purchases increased the high number of transactions. The method of payment has shifted through the evolution from the use of cash, debit cards, credit cards, and now Mobile Banking. Changes in consumer behavior from the use of the traditional way into the online payment system are evident in banking and retail services. Bezhovski's research results conclude that the future payment system will be integrated with telecommunications infrastructure and financial institutions for compatibility across a range of services, including its security solutions. (Bezhovski, 2016)

Mobile Payment currently has several payment methods, such as NFC, QR Code, and Online. Security development continues to be adopted to ensure mobile payment security. The results of Wang et al. (2016) stated that there are 4 (four) Security Challenges for Mobile Payment, namely: malware detection, multi-factor authentication, data breach prevention, and fraud prevention. Mobile Payment security issues, both service providers and users require ongoing security measures to ensure data security and prevent data breaches. (Wang, Hahn, & Sutrave, 2016)

In contrast to Hayashi et al. (2014), the QR Code Payment model in this study builds on the Mobile Banking platform and is not limited to certain merchants but can be used generally. Based on the mapping of four pillars of mobile payment strategy from Sachdev (2014), the purpose of QR Code Payment in Mobile Banking builds a non-cash ecosystem that can be used easily and ultimately can reduce the volume of cash withdrawal transactions. In addition to its use as an alternative method of payment transactions offline merchant (Paying Merchant / Retailer), QR Code Payment on Mobile Banking can also be used for service (Person to Person) (Paying Other People). Regarding one of the security challenges, namely: fraud prevention delivered by Wang et al. (2016), in the current study using the method of close payment where QR Code Payment transactions can only be done after the customer and merchant have logged into Mobile Banking. While the authentication of QR Code Payment transactions using Multi-Factor Authentication (MFA) method.

3. Methodology

As shown in Figure 2, the stages in this study begin by identifying and formulating problems. Then a literature study and observation were carried out to clarify the problem, understand theories and concepts, and get alternative solutions. The next steps are needs analysis, system design and prototyping, and system evaluation. In the system design process, a use case diagram is designed, process flow diagrams, and system prototypes. Next, the developed system will be evaluated using Beta Testing, Security Testing, and TAM analysis to measure user acceptance.

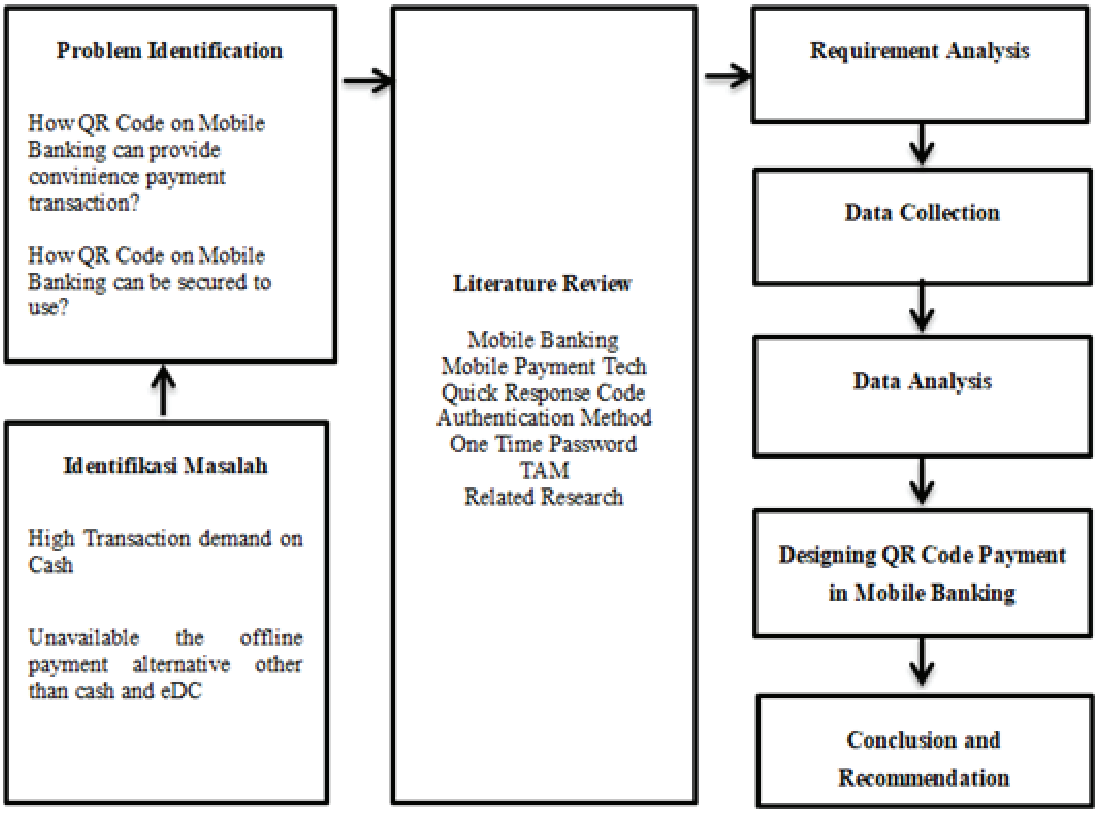

Problem Identification
How QR Code on Mobile Banking can provide convinience payment transaction?
How QR Code on Mobile Banking can be secured to use?
Identifikasi Masalah
High Transaction demand on Cash
Unavailable the offline payment alternative other than cash and eDC
Literature Review
Mobile Banking
Mobile Payment Tech
Quick Response Code
Authentication Method
One Time Password
TAM
Related Research
Requirement Analysis
Data Collection
Data Analysis
Designing QR Code Payment in Mobile Banking
Conclusion and Recommendation

Figure 3: Research Procedures.

4. Results and Discussion

4.1. Requirement Analysis Results

Currently, payment transaction services from Mobile Banking OCBC NISP still use basic banking service features, namely Purchase and Biller Transactions, Payment, Virtual Account Transfers or Interbank Transfers. The use of Purchase and Biller Payment transactions is still limited to non-retail transactions and is related to regular monthly purchases or payments. Whereas Virtual Account or Interbank transfer transactions are more flexible with the mandatory information, namely the destination account number and the nominal value inputted by the customer. Bank OCBC NISP continuously identifies problems in the customer service process and repairs necessary processes.

At present, one of the problems that arise is how banks can provide a secure and safe way to be able to make payment transactions at merchants through Mobile Banking.

Here are some of the existing mobile technologies that can be used to develop payment systems through Mobile Banking, including Near Field Communication (NFC), Biometric, and QR Code. NFC and Biometric technology requires a mobile device that has a reader and writer feature, while the QR Code only requires a camera and without the need for a reader and writer feature. So that the application of QR Code compared to NFC and Biometric can be achieved more broadly with a smaller investment value than the application of NFC and Biometric. Currently, the camera is an essential feature available on all types of mobile devices. To be able to facilitate payment transactions and provide security, the QR Code feature is an option to add to the Mobile Banking OCBC NISP application as an alternative payment system that is easy to use and can reduce cash withdrawal transactions at ATMs and can be used by merchants not to provide EDC machines.

In contrast to some similar applications that have been mentioned above, the system built from this research is integrated with the main data source accounts so that it does not require a top-up of funds through the interbank transfer process. The list of requirements for QR Code Mobile Banking OCBC NISP can be described as follow:

1. QR Code Payment is built on the Mobile Banking platform
2. Customers can determine their source of funds account and can make account changes later.
3. Customers and Merchants are required to log in to Mobile Banking to be able to make transactions.
4. Merchants can display the QR Code generated by the system to be informed to the Customer.
5. The customer scans the QR Code from the Merchant
6. The customer enters a nominal value
7. OTP generate system
8. Customer input OTP PIN and press process instructions.
9. Customers and Merchants receive payment complete notifications from the Mobile Banking application.

4.2. Design System

As shown in Figure 4, the system design of the QR code payment consists of 3 entities, namely:

1. Customer's Device is a customer-owned device that is used as a media scan, input, and confirm with a user interface that is easy to understand.
2. Mobile Banking Application, A banking application that can be run via a smartphone and used for banking transactions.
3. Merchant's Device, It is a device belonging to the merchant that is used as a medium to display the QR Code and confirm the payment received.

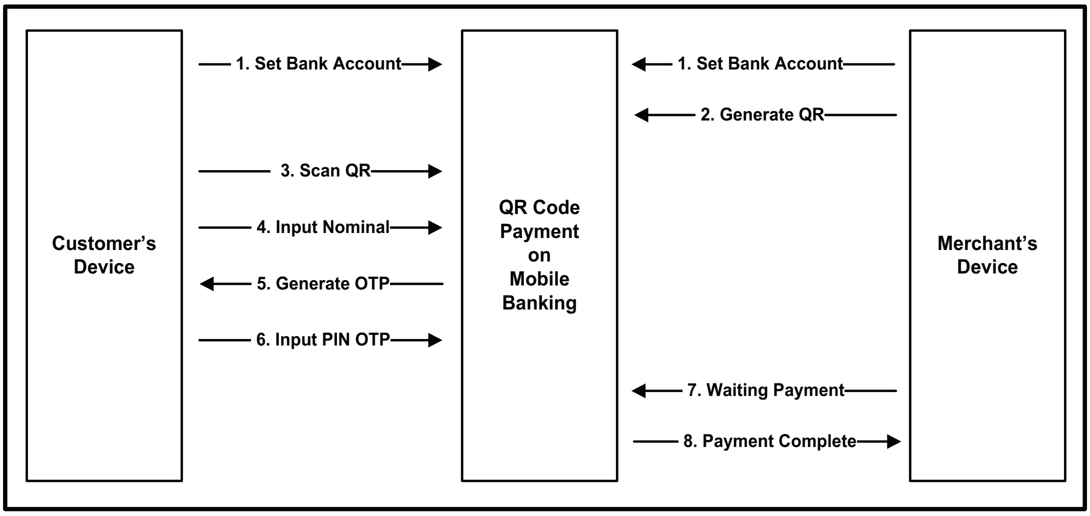


Figure 4: The Proposed QR Code Payment System Design.

Based on Figure 4, for the initial process after the Mobile Banking login, the Customer and Merchant are required to determine the account number of the source of funds to be used. If no account number has been linked, the transaction cannot be done yet. Finished from the process of linking the source fund account number, then when the transaction, the Customer will be asked to scan the QR Code from the Merchant that has been generated by the previous system according to the Merchant's data. Then proceed with the process of the nominal input paid and the OTP input that the system has sent after the nominal input. At the end of the process, the payment transaction status will be informed to the Customer and Merchant devices.

Figure 5 describes the use case diagram for QR Code Payment Mobile Banking, which shows that there are 2 main types of users interact with the system, namely Customers and Merchants.

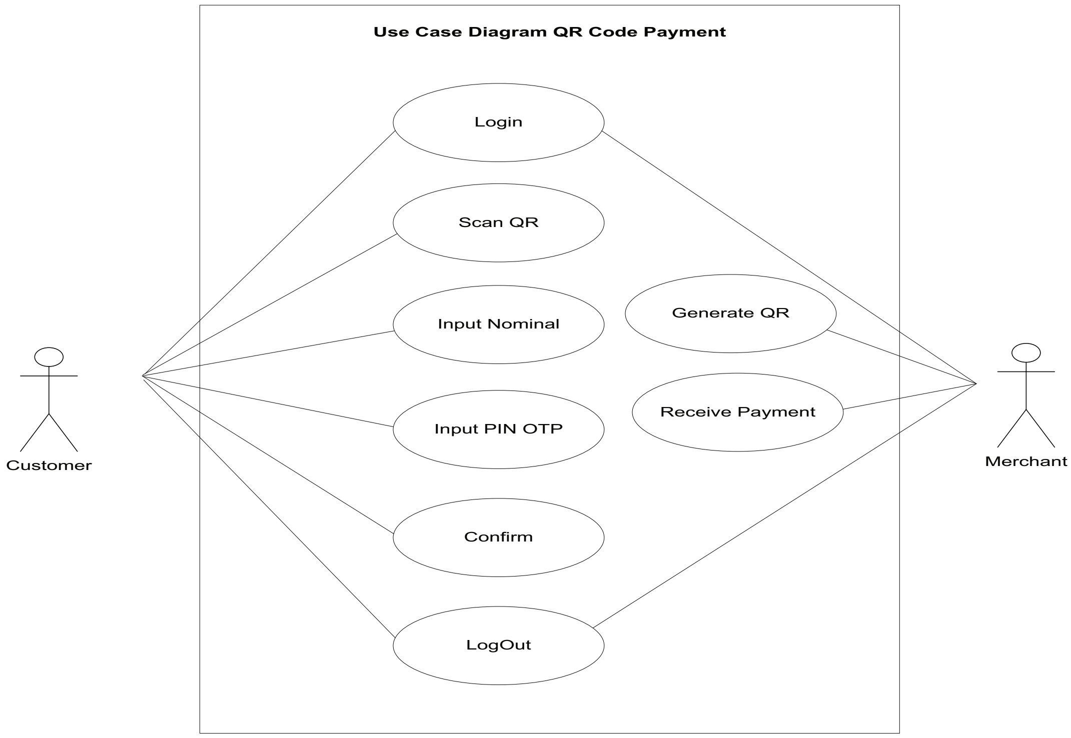


Figure 5: The Use Case Diagram of QR Code Payment.

Figure 6 describes a process flowchart for QR Code payment using Mobile Banking.

Based on Figure 6, at the beginning of the transaction with the QR Code, Mobile Banking will generate a QR Code and display it on the Merchant device. The customer will scan the QR Code, and Mobile Banking will send detailed information to the Customer device to display the detailed payment information on the Customer device screen, then enter the nominal value and the input PIN sent separately by the system. The confirmation process, the system will ensure that the inputted PIN is valid and proceed with processing and saving transactions. The process results are displayed on the device belonging to the Customer and Merchant.

Unlike other similar applications that have been submitted before, the system designed is unique based on:

1. Built-in the Mobile Banking application. Strict regulation in the banking industry makes high trust in banks, including every bank-owned system and its development, the rigorous selection of testing processes and periodic review of the application of the system used.

2. Integrated with the main account of the source of funds without the need for a top-up process and if it is still needed later, it can still be changed to another account easily when needed.

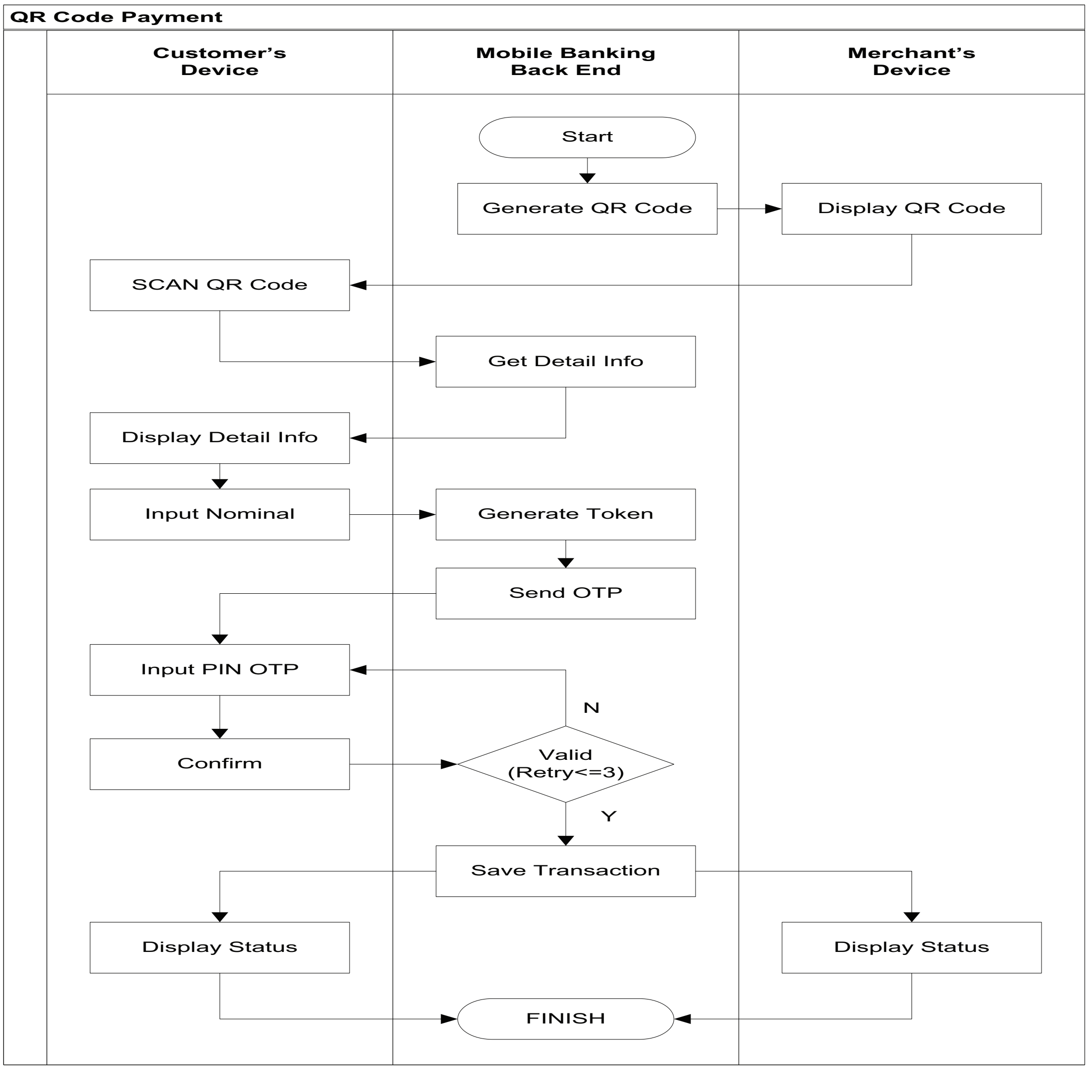


Figure 6: The Flow chart for the QR Code Payment Process Using Mobile Banking.

Here are some display of the prototype QR Code Payment features on Mobile Banking:

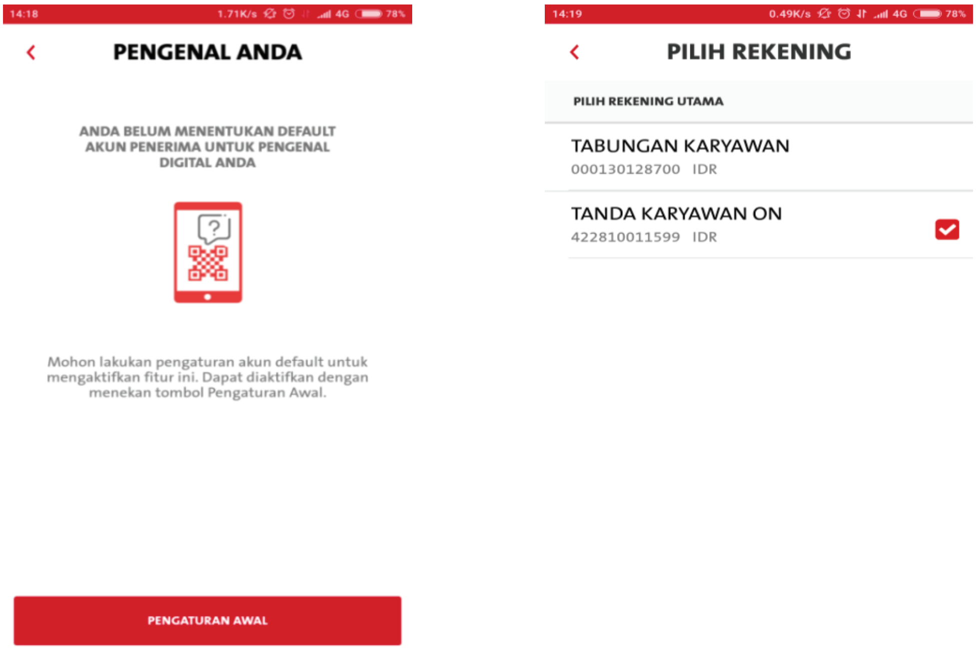
i. Linking of Fund Source Account

ii. Generate QR for Fast Transfer

This form is the main form which will appear when the user will use the application for the payment process.

iii. QR Scan for Fast Transfer

Serves for selection at the time the data input is completed, the user can directly upload data if they feel that the inputted data is complete or can store data temporarily with the later will complete the data.



14:18 1.71K/s 4G 78%

PENGENAL ANDA

ANDA BELUM MENENTUKAN DEFAULT AKUN PENERIMA UNTUK PENGENAL DIGITAL ANDA

Mohon lakukan pengaturan akun default untuk mengaktifkan fitur ini. Dapat diaktifkan dengan menekan tombol Pengaturan Awal.

PENGATURAN AWAL

14:19 0.49K/s 4G 78%

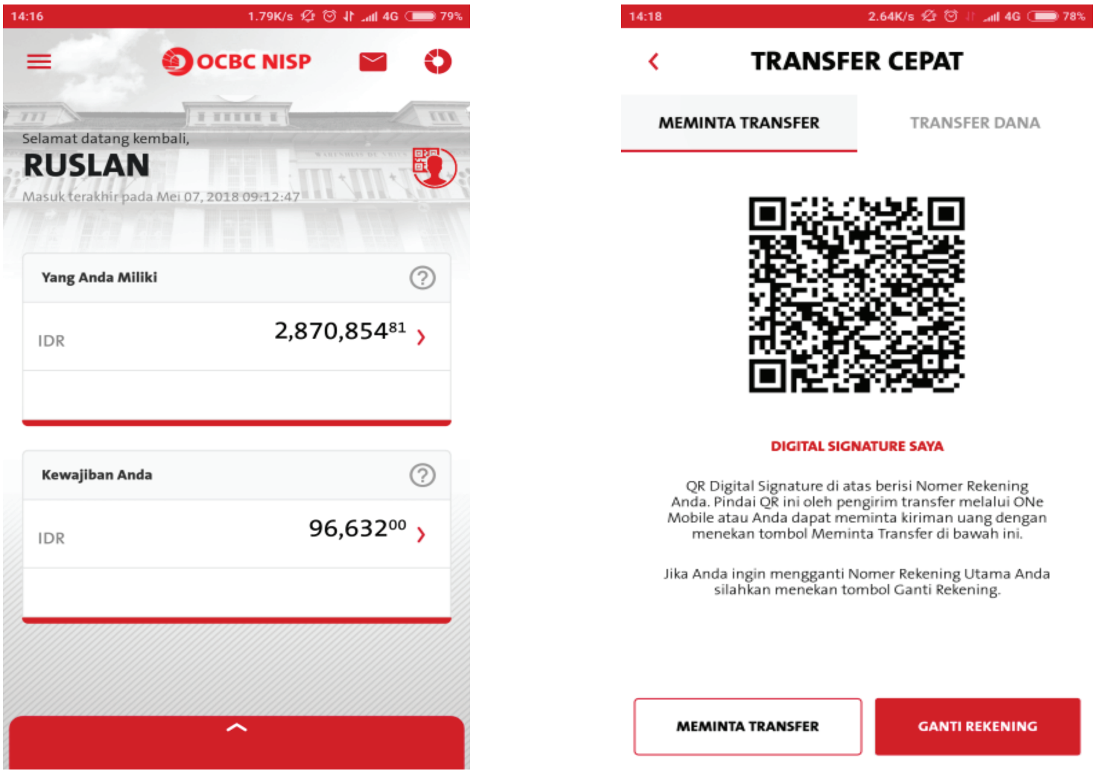
PILIH REKENING

PILIH REKENING UTAMA

TABUNGAN KARYAWAN
000130128700 IDR

TANDA KARYAWAN ON ☑
422810011599 IDR

Figure 7: Display Screen of Main Account Linkage.



14:16 1.79K/s 4G 79%

OCBC NISP

Selamat datang kembali,
RUSLAN
Masuk terakhir pada Mei 07, 2018 09:12:47

Yang Anda Miliki	
IDR	2,870,854^{81}

Kewajiban Anda	
IDR	96,632^{00}

14:18 2.64K/s 4G 78%

TRANSFER CEPAT

MEMINTA TRANSFER | TRANSFER DANA

DIGITAL SIGNATURE SAYA

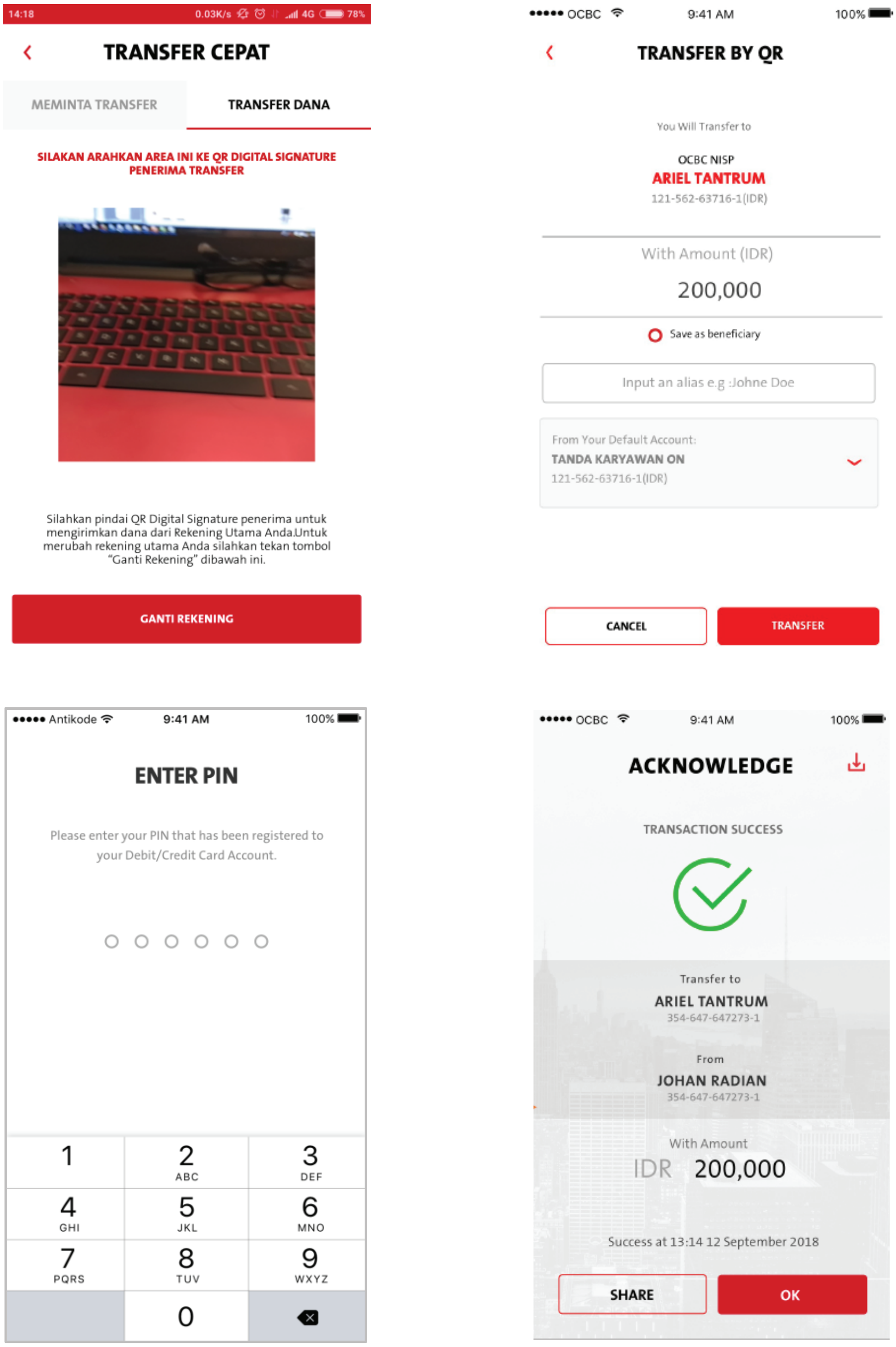
QR Digital Signature di atas berisi Nomer Rekening Anda. Pindai QR ini oleh pengirim transfer melalui ONe Mobile atau Anda dapat meminta kiriman uang dengan menekan tombol Meminta Transfer di bawah ini.

Jika Anda ingin mengganti Nomer Rekening Utama Anda silahkan menekan tombol Ganti Rekening.

MEMINTA TRANSFER | GANTI REKENING

Figure 8: Screen Display of Generate QR for Fast Transfers.

iv. Receive Payment



SILAKAN ARAHKAN AREA INI KE QR DIGITAL SIGNATURE PENERIMA TRANSFER

Silahkan pindai QR Digital Signature penerima untuk mengirimkan dana dari Rekening Utama Anda.Untuk merubah rekening utama Anda silahkan tekan tombol "Ganti Rekening" dibawah ini.

You Will Transfer to

OCBC NISP
ARIEL TANTRUM
121-562-63716-1(IDR)

With Amount (IDR)
200,000

○ Save as beneficiary

Input an alias e.g :Johne Doe

From Your Default Account:
TANDA KARYAWAN ON
121-562-63716-1(IDR)

Please enter your PIN that has been registered to your Debit/Credit Card Account.

TRANSACTION SUCCESS

Transfer to
ARIEL TANTRUM
354-647-647273-1

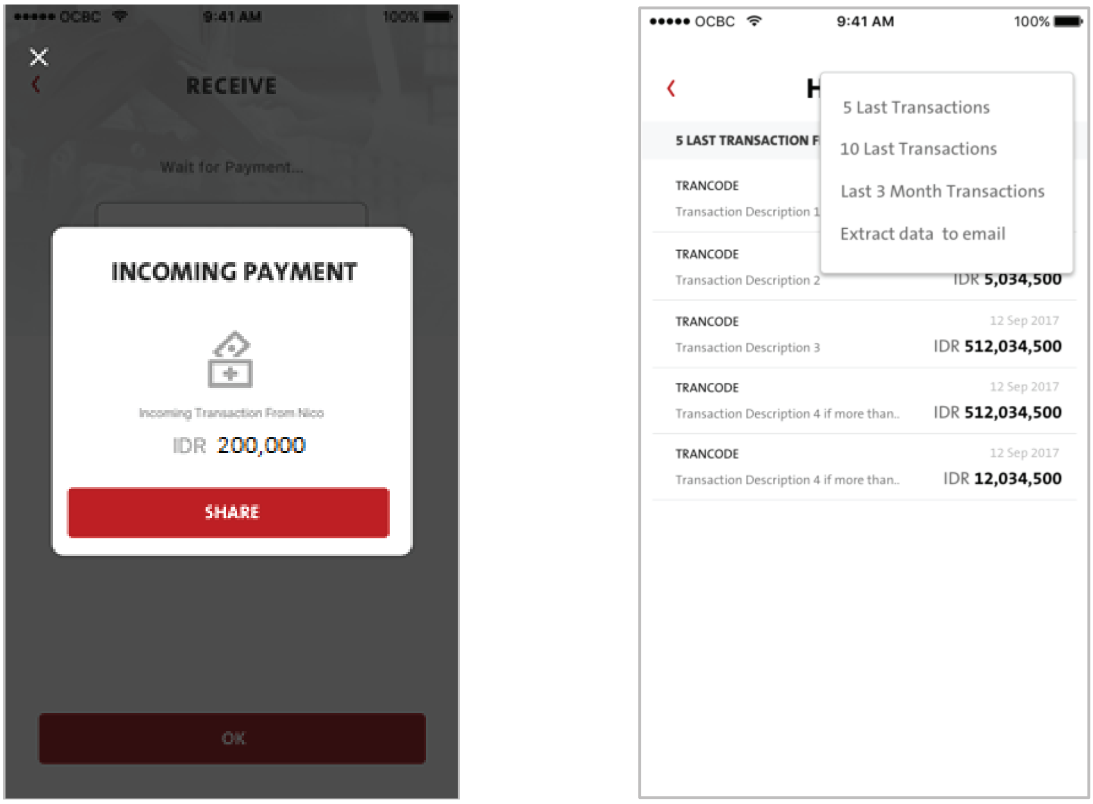
From
JOHAN RADIAN
354-647-647273-1

With Amount
IDR 200,000

Success at 13:14 12 September 2018

Figure 9: Screen Display to Scan QR code for Fast Transfers.

Serves for selection at the time the data input is completed, the user can directly upload data if they feel that the inputted data is complete or can store data temporarily with the later will complete the data.



TRANCODE
Transaction Description 1

TRANCODE
Transaction Description 2 IDR 5,034,500

TRANCODE 12 Sep 2017
Transaction Description 3 IDR 512,034,500

TRANCODE 12 Sep 2017
Transaction Description 4 if more than.. IDR 512,034,500

TRANCODE 12 Sep 2017
Transaction Description 4 if more than.. IDR 12,034,500

Figure 10: Screen Display Incoming Payment Notification.

4.3. Evaluation System Result

The functional testing system is done using beta testing. This test is intended to ensure that each menu and features of the QR Code payment application are running according to user requirements. Based on the results of testing with the Beta Testing scenario, QR Code Payment on Mobile Banking has been functioning properly according to the application requirements.

The QR Code payment on Mobile Banking prototype generated from this research was then tested by the Technology Acceptance Model (TAM) method to measure the influence and acceptance of the QR Code payment system using Mobile Banking. This TAM test is assessed from the variables Perceived Ease of Use (PE), Perceived Usefulness (PU), Attention toward Using (AT) and Intention to Use (IU). The evaluation results on the PE variable show a relatively small data deviation because the value is less than the Mean value. Thus it can be concluded that the variable PE data is useful. This can explain that respondents get the convenience of using the developed QR Code Mobile Banking OCBC NISP feature. The evaluation results in the PU variable show a relatively small data deviation because the value is less than the Mean value. The user's perception of the benefits of the QR Code Mobile Banking OCBC NISP feature can be represented by variables PU1, PU2, PU3, and PU4. The mean value of the four variables tends to approach the maximum value. Thus it can be concluded that the respondents benefit from the use of the developed QR Code Mobile Banking OCBC NISP system features.

5. Conclusion and Implications

The prototype QR Code Payment on Mobile Banking has been able to answer the background of problems and research objectives. These include:

1. The QR Code Payment model on Mobile Banking can be used widely as a non-cash payment alternative through a smartphone. Developed not only for Paying Merchants / Retailers but can be used for Paying Other People (Person to Person).
2. For transaction security, login to Mobile Banking is required to access QR Code, then the QR Code is generated by an application. From the customer side, each transaction using QR will receive OTP according to the Multi-Factor Authentication (MFA) method applied.
3. QR Code on Mobile Banking provides convenience to the customer to make payment in the simplest way possible, namely: Scan, Input Nominal, Input OTP, and Confirm.
4. Customers can determine the source of funds used for transactions using this QR Code Payment, so indirectly also reduces cash withdrawal transactions.

Prototype QR Code Payment on Mobile Banking is still not perfect and is still being developed to improve the ease and security in transacting. Integration with other non-cash ecosystems can be considered. For interconnection and interoperability with other ecosystems, it is possible to have standardized QR Code Payment, so the way it works can follow the flow of interbank or ATM transfer process together. For this, it is awaiting the study and policy of OJK as a regulator in promoting non-cash movement.

References

[1] Bezovski, Z. (2016). The future of the mobile payment as electronic payment system. *European Journal of Business and Management*, *8*(8), 127-132.

[2] Chang, T. K. (2014). A secure operational model for mobile payments. *The Scientific World Journal*, *2014*.

[3] Dennehy, D., & Sammon, D. (2015). Trends in mobile payments research: A literature review. *Journal of Innovation Management*, *3*(1), 49-61.

[4] Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A. R. (2014). Security Analysis of Mobile Two-Factor Authentication Schemes. *Intel Technology Journal*, *18*(4).

[5] Gandhi, A., Salunke, B., Ithape, S., Gawade, V., & Chaudhari, S. (2014). Advanced online banking authentication system using one time passwords embedded in QR code. *International Journal of Computer Science and Information Technologies*, *5*(2), 1327-1329.

[6] Hayashi, F., & Bradford, T. (2014). Mobile payments: Merchants' perspectives. *Economic Review*, *99*, 5-30.

[7] Liu, Y., & Liu, M. (2006, October). Automatic recognition algorithm of quick response code based on embedded system. In *Sixth International Conference on Intelligent Systems Design and Applications* (Vol. 2, pp. 783-788). IEEE.

[8] Robson, B., Lee, H., East, D., Lim, L., & Chia, T. (2017). *Retail Payments in Indonesia - Who will Drive the cashless transaction?* KPMG Siddharta Advisory.

[9] Sachdev, S. (2014). *The Four Pillars of Mobile Payments - Immediate Opportunities.* Brookfield: Fiserv, Inc.

[10] Shah, A., Kaushik, V., Roongta, P., Jain, C., & Awadhiya, A. (2016). Digital payments 2020: The making of a $500 billion ecosystem in India. *The Boston Consulting Group*.

[11] Stiphout, M. v., & Mual, M. (2017). *Payment Methods Report 2017.* The Paypers BV.

[12] Wang, Y., Hahn, C., & Sutrave, K. (2016, February). Mobile payment security, threats, and challenges. In *2016 second international conference on mobile and secure services (MobiSecServ)* (pp. 1-5). IEEE.