CHAPTER 1

INTRODUCTION

1.1 Rationale

The development of IT is increasingly accelerating in everyday life, and many fields or industries are utilizing it to provide convenience and practicality for their users. In recent years, people have benefited from the growth and advancement of information and communication technology (ICT) in many areas. One of these utilizations is the development of digital economy technology [1]. Based on research from the collection of results of the survey by APJII, Internet users in Indonesia reached 215 million people or 78.19% [2]. Many recent developments, such as e-commerce and online Taxis, are also prevalent in the business and trade sectors. The phrase Financial Technology (FinTech) is famous in the financial industry [3].

Fintech (Financial Technology) is a financial service that utilizes technology for business needs. Fintech services typically target people who are not served by the traditional financial industry and are looking for alternative funding. Fintech provides services that most people can use, such as payments, loans, investments, financial planning, and financing. Patrick [4] explains that fintech is a new financial industry that applies technology to increase economic activities. In Indonesia, the Fintech industry has experienced significant development. Based on a Bank Indonesia report for 2023, there are at least 187 payment service providers with License Category I license [5]. Over time, the fintech industry will continue to grow. Based on a report released by DailySocial [6, 7], the development of FinTech in Indonesia, primarily Electronic Wallet (E-Wallet), is good business.

The use of fintech e-wallet has been overgrown in recent years, as it offers many benefits, such as convenience, speed, and lower costs. However, this development turned out to be a problem and a risk associated with increasing fraud or theft in fintech services [8, 9], which:

1. Fraud: One of the most significant risks of fintech is the potential for fraud. Fraudsters can use various methods to steal personal and financial information, such as phishing scams, malware, or social engineering. They can then use this information to steal money or make unauthorized transactions. Fintech companies are responsible for protecting their customers' information and detecting and preventing fraudulent activities [10].

2. Hacking: Another risk of fintech is the potential for hacking. Hackers can gain access to fintech systems and steal sensitive information, such as personal and financial data. They can also disrupt services and cause economic losses. Fintech companies have

to secure their systems and have incident response plans in case of security breaches [11].

3. Money Laundry: Money laundry are individuals recruited to facilitate the movement of stolen money, often through their bank accounts. Fraudsters and hackers use them to launder stolen money and transfer it to other countries, making it more difficult to track and recover. Fintech companies must be aware of the potential for money laundering and have procedures to detect and prevent it [12].

4. Operational risks: Fintech companies are exposed to operational risks, relying on technology and infrastructure to provide their services. These risks include system failures, power outages, data breaches, and natural disasters. Business continuity and disaster recovery plans are crucial for fintech companies to minimize the impact of these risks [13].

5. Regulatory risks: Fintech companies are subject to a wide range of regulations, such as data protection, anti-money laundering, and consumer protection. Non-compliance with these regulations can result in fines, penalties, and reputational damage. Additionally, regulatory changes can affect fintech companies' operations and business models, requiring them to adapt or change their practices. Fintech companies must stay up-to-date with the regulations that apply to them and ensure that they comply with them [14].

This research was conducted as a form of consumer protection effort that emerged in accordance with OJK Regulation Number 10/POJK.05/2022 concerning Information Technology-Based Joint Funding Services [15, 16]. An example of a financial incident in the field of fintech technology occurred in the LinkAja digital wallet application, where six defendants were legally and convincingly sentenced to 4 years in prison for violating Articles 85 and 82 of Law Number 3 of 2011 concerning Fund Transfers in conjunction with Article 55 paragraph (1) to the 1 of the Criminal Code by taking advantage of an error in the LinkAja Top Up system that causes customers to transact through BRIVA BRI at ATMs. This causes the balance debited from the Top Up Link Aja transaction through the BRIVA ATM to be reversed or the balance returned due to a failed transaction [17].

In the case described, the investigator must have a robust explanation for the evidence the investigator gets. This is done to determine how the case can be analyzed. It can choose the flow of a forensic investigation to obtain evidence in interpreting the existing evidence and describing the investigation's findings [18]. However, unstructured data, textual or not, can cause difficulties in the forensic examination stage and waste time. Therefore, new tools and techniques are needed to detect, prevent, and investigate fraud against Fintech systems and provide the benefits of new methods and techniques to investigate Fintech crimes to identify crimes [19]. In court, the elements of the digital evidence examination are not directly accessible and are included in various conclusions and reports. Therefore,

from the findings and reports, the aspects of the investigation of digital evidence need to be researched and analyzed [20]. The selection of these four applications is based on the popularity of e-wallet applications on fintech services that are widely used by users in Indonesia in 2020 and 2021, according to DailySocial [6, 7].

To illustrate the scope of this research, consider a hypothetical e-wallet application on fintech services. This application is utilized on four distinct devices manufactured by different entities and acquired by four forensic applications. Consequently, the four resulting datasets will exhibit disparate characteristics, resulting in 16 unique combinations for a single application.

In a fintech investigation, investigators may encounter challenges due to the variability in the acquired data. Each acquisition application may yield distinct characteristics, leading to confusion and hindering the investigation process. This must be done because, in e-wallet applications on fintech services, regardless of the specific application, there must be similar data that is crucial for forensic activities.

This research can provide information about an incident involving an e-wallet application on fintech services and to what extent the data acquired can help investigate the incident. This is done because e-wallet applications on fintech services have the same data essence (having user, transaction, and merchant entities), but each application represents this data differently. The data that has been successfully acquired is grouped in a more general form to facilitate an understanding of what data plays an essential role in digital forensic activities and how an investigative question can be answered based on this data. Generalization of this data will show what data is available and the relationships between the data. This research can help determine policies regarding data that must be provided as digital evidence.

1.2 Theoretical Framework

Nikkel B presented the forensic analysis [19], where he conveyed the studies related to digital forensics for the Fintech incident investigation process. In addition, based on research of existing e-wallet application on fintech services in Indonesia in 2019 by Abdillah [21], it is suggested that Indonesian legal authorities should encourage the development of fintech-based applications in Indonesia.

Until now, no suitable forensics analysis model for the Fintech domain has existed. A basis is needed regarding what data can be used as concrete and generally accepted digital evidence. An analysis modeling is used to generalize the data in the Fintech application. This model should assist the investigator in the proceedings to help provide technological understanding to non-technical observers [22]. Based on the explanation, this research analyzes four e-wallet applications on fintech services in Indonesia.

1.3 Conceptual Framework/Paradigm

In conducting this research, it is necessary to understand the characteristics of the fintech system that runs as a reference and is the focus of attention in the forensic investigation results. To know the characteristics of the fintech system, there are several required understanding of the concept, such as:

1. Know what parameters are contained in the data in fintech services as digital evidence; and
2. The method/tool used must provide complete results related to the data needed in the e-wallet application on fintech services as digital evidence.

1.4 Statement of the Problem

To identify criminal acts in the e-wallet application on fintech services that have different representations. Investigators need a model to determine the data representation in each e-wallet application on fintech services. With this problem, several research questions occur, such as:

1. How to generalize the fintech data with its characteristics in each application?
2. How the data generalization can be built into an analysis model to help identifying digital evidence?

1.5 Objective and Hypotheses

This research aims to create a forensic analysis model by classifying existing data groups and generalizing digital evidence in technology-based financial services (Fintech). This analysis model is intended to help understand what data acquired from user device applications can be processed and used as digital evidence.

1.6 Assumption

There are several assumptions in this research. This assumption acts as a direction or foundation for research activities before something researched is proven true. Some of these assumptions are described as follows:

1. The generalization results of digital evidence in fintech services in this research can be used generally in other fintech services;
2. At the very least, the research can be applied to fintech services in Indonesia and

3. The value of research can provide information in the form of digital evidence that can help the trial process.

1.7 Scope and Delimitation

This research has a scope of 4 e-wallet applications on fintech services in Indonesia, including DANA, OVO, Gopay (in the Gojek application), and LinkAja. Other than that, several limitations need to be considered in this research. These include:

- Research focuses on client-base side media (Smartphone); and
- This model has only been tested on four e-wallet applications on fintech services in Indonesia, namely Gojek, OVO, LinkAja, and DANA, with the version determined in Table 3.1.

Limitations are established to narrow down the scope of the research and make it more feasible, focused, and manageable. Delimitations help researchers define the study's parameters, specify what will be included and excluded, and clarify the extent and limitations of their investigation.

1.8 Significance of the Study

The results of this study are expected to provide information to forensics investigator for making a basis for consideration, support, and input for their thinking to encourage revenue growth and business development. Therefore, the following contributions were made:

1. Organizing and structuring financial data in a consistent and meaningful way for financial investigations
2. Improving the searchability and understandability of financial data.
3. Providing greater context and meaning to financial transactions.
4. Facilitating collaboration and interoperability among forensic tools by providing a consistent data exchange and analysis framework.
5. Giving standardization and interoperability among different forensic tools and platforms, which can reduce costs and improve the quality of investigations.