INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY: APPLIED BUSINESS AND EDUCATION RESEARCH
2025, Vol. 6, No. 1, 180 – 200
http://dx.doi.org/10.11594/ijmaber.06.01.12

Research Article

An Assessment on The Role of Cryptocurrency in Modern Kidnapping for Ransom Cases in Cities of Pasay and Paranaque

Marceliano A. Desamito Jr., Leonardol O. Bautista III, Loreta R. Dela Cruz, Moises B. Garcia, Cecilio G. Tomas Jr, Elizabeth Buena Villa, Froilan D. Mobo, Nathaniel S. Golla

De La Salle University Dasmarinas, Philippines

Article history:
Submission 31 December 2024
Revised 07 January 2025
Accepted 23 January 2025

**Corresponding author:*
E-mail:
desamitomarcjr@gmail.com

ABSTRACT

The study aimed to address the influence of cryptocurrency on contemporary kidnapping for ransom in the cities of Pasay and Paraňaque as assessed by anti-kidnapping group personnel towards the development of a strategic proposal to combat kidnapping in the digital landscape.

This research employed a quantitative-descriptive methodology, utilizing stratified random sampling as the research design to carefully select respondents from the PNP office Anti-Kidnapping Group. A total of twenty (20) survey questionnaires will be distributed to gather data on the evaluation of PNP personnel regarding the role of cryptocurrencies in contemporary kidnapping for ransom, particularly in relation to investigation, negotiation, and operations. The study's findings indicate that: The Philippine National Police Anti-Kidnapping Group (AKG) should improve educational programs and strategies to address kidnapping for ransom. Mandatory training on proposed initiatives will be necessary for the PNP AKG. Additionally, the PNP AKG will oversee security in Pasay and Paranaque, and the BSP is actively monitoring developments in virtual currency, particularly regarding their potential use in money laundering and other illicit activities, and will take appropriate action as needed.

The findings emphasized that strong regulation, including the Anti-Fraudulent Activities in Financial Accounts Act (AFASA) and the suggested amendments to the Bank Secrecy Act, are essential and long overdue. The BSP and other regulatory authorities in the Philippines must actively oversee cryptocurrencies. Furthermore, the PNP AKG and ACG necessitate revised techniques to proficiently obstruct blockchain technology from enabling cross-border bitcoin transactions.

How to cite:
Desamito Jr., M. A., Bautista III, L. O., Dela Cruz, L. R., Garcia, M. B., Tomas Jr, C. G., Villa, E. B., Mobo, F. D., & Golla, N. S. (2025). An Assessment on The Role of Cryptocurrency in Modern Kidnapping for Ransom Cases in Cities of Pasay and Paranaque. *International Journal of Multidisciplinary: Applied Business and Education Research*. *6*(1), 180 – 200. doi: 10.11594/ijmaber.06.01.12

Keywords: *Assessment, Chainalysis, Blockchain Technology, Cryptocurrency, Kidnap-for-Ransom, Modern, Motivation, Philippine National Police*

Introduction

A financial system constitutes a structured framework facilitating the transfer of capital among lenders, investors, and borrowers. Financial systems function on both national and global scales. They comprise intricate, interrelated services, markets, and institutions designed to establish an efficient and consistent connection between investors and depositors. Monetary instruments, credit mechanisms, and financial resources serve as conduits for exchange within economic systems. The payment system has acquired considerable importance as nations engaged in digitization demonstrate enhanced efficacy in their financial inclusion initiatives. (Dewani et al., 2020).

A cryptocurrency (or crypto currency) is a digital asset meant to function as a means of exchange, employing powerful cryptography to safeguard financial transactions, restrict the creation of new units, and verify asset transfers. Cryptocurrencies, unlike centralized digital currencies and central banking institutions, operate on a decentralized basis. Cryptocurrencies use distributed ledger technology, such as blockchain, to provide decentralized control and a public record for financial transactions. Bitcoin, first released as open-source software in 2009, is widely regarded as the first decentralized cryptocurrency. Since the launch of Bitcoin, approximately 6,000 altcoins (alternative variations of Bitcoin or other cryptocurrencies) have been produced. (investopedia.com)

As of 2023, a survey conducted by the Pew Research Center indicates that approximately 17% of American adults have engaged in the ownership of cryptocurrency. As of September 2023, India occupies the foremost position in Chainalysis's global crypto adoption index, with Nigeria and Vietnam following closely to complete the top three rankings. According to Chainalysis, numerous high adopters are emerging in developing markets, including Ukraine, Indonesia, and the Philippines. (bankrate.com).

The Philippines, officially the Republic of the Philippines, is a unitary archipelagic nation in Southeast Asia. The Philippines has the 63rd greatest land area in the world and the 12th largest population. The Philippines is the world's 63rd largest country in terms of land area and the 12th most populous. The Philippines stands out as one of the world's most ethnically diverse countries, with a wide range of religious views. By the end of 2018, the Philippines had a GDP of $348 billion, making it the world's 34th largest economy. The economy is mostly made up of electronics, transportation machinery, petroleum and its derivatives, and agricultural products. Although agriculture employs 30% of the population, the Philippine economy is becoming more technologically oriented. Circular No. 944, released on June 2, 2017, set laws for Virtual Currency Exchanges, effectively legalizing cryptocurrencies in the Philippines. The Central Bank of the Philippines regulates Bitcoin transactions in the country. (BSP, 2017).

The utilization of cryptocurrency in the Philippines is facilitated through bank transfer transactions, which is considered essential for engaging with this form of currency. A number of investors engage with this technology, with notable cryptocurrencies including Bitcoin, Ethereum, Bitcoin Cash, and Ripple (XRP). This collection of literature reviews endeavors to propose solutions aimed at facilitating the adoption of this alternative currency system in the Philippines. In contemporary society, the insufficient understanding of cryptocurrency presents a significant challenge, particularly regarding the availability of essential blockchain wallets accessible online. The matter of security presents a significant concern; these wallets could serve to augment the concept and functionality of an individual's account or that of investors. The primary challenges associated with the adoption of cryptocurrencies encompass a nascent history characterized by illiquidity, significant volatility, and potentially ambiguous applications. The challenges associated

with the successful adoption of cryptocurrencies are often clouded by ambiguity regarding their classification as either digital or virtual currencies, which in turn raises questions about the mechanisms by which their values are established. (Harvey, 2015).

Internet-based payment methods and currencies have surfaced in recent years, eliminating the need for banks to handle payment processing. Bitcoin was the first and remains the biggest of these so-called cryptocurrencies. (Dwyer, 2015) & (Grinberg, 2011). In contrast to the majority of other currencies that are often kept in the central bank's foreign reserves, the supply of cryptocurrencies is managed by a very intricate mathematical proof rather than a central bank. Miners are network users who collect transaction blocks and compete to validate them. These users are compensated with any transaction costs and a fresh supply of the currency. Bitcoins are currently accepted as a final payment method by a number of companies worldwide. (Moore &Stephen, 2016).

The Philippines, Southeast Asia's (SEA) second-most populated nation, presents a favorable environment for blockchain development. The Philippines is one of Southeast Asia's most robust blockchain markets, with a population of over 107 million and a 71 percent internet penetration rate. However, the challenge of banking the unbanked, who make up a worrisome 77 percent of the population, comes along with its enormous population. Fortunately, there is Project i2i, which aims to provide financial services to rural residents, who make up a sizable percentage of the unbanked population in the archipelago. (Asia Blockchain Review, 2019).

By collaborating with Unionbank to develop the blockchain application bonds.ph for the sale of government bonds, the Philippine government has also gotten involved with bitcoin. Unionbank has recently set up a Bitcoin ATM in Makati (Metro Manila), illustrating the growing popularity of cryptocurrencies in the country. (Helms, 2020).

The payment system has undergone a significant number of changes as a result of technological advancements. As a result of the pandemic, the population of the Philippines has developed a better exposure to technological instruments. As a result of the surge in the value of bitcoin in the United States in 2009, most of the younger generation is becoming interested in alternative currencies. Blockchain technology is the foundation of cryptocurrency, which is a decentralized digital currency. Several cryptocurrencies, including Bitcoin, Ethereum, Cardano, Dogecoin, Litecoin, Bitcoin Cash, and Potcoin, are currently experiencing a surge in popularity. According to a report by Morning Consult, approximately 70 percent of cryptocurrency owners are male, despite their representation being only 48 percent of the overall population. Women represent 30 percent of cryptocurrency owners, while they account for 52 percent of the overall population. (pro.morningconsult.com).

Jadhav et al. (2022), the prevailing demographic of investors falls within the age range of 18 to 24 years. Investors acquire knowledge regarding cryptocurrency through their social circles and various social media platforms. It appears that males exhibit a greater level of awareness compared to females. An elevated degree of educational attainment significantly influences the advanced understanding of cryptocurrency.

Interest in cryptocurrencies, like Bitcoin and Ethereum, has recently intensified as several sectors investigate ways to leverage this emerging technology. As public awareness escalates, different uses for cryptocurrencies emerge almost daily. As fresh uses of cryptocurrencies arise, so do their potential legal liabilities. In accordance with the Freeman Law, they examine several prevalent legal issues about cryptocurrencies. (freemanlaw.com).

Contractual Issues

"Smart contracts" that run themselves are one of the most interesting things about blockchain technology and coins. Smart contracts are a list of promises, generally written in digital form, that set the rules for how the people involved in a deal will keep their promises. When one party follows through on their end of a smart contract, the other party is automatically paid. It's hard to say if smart contracts fit into the legal framework of standard contract law because they are so different and complicated. All of those who are in the United States

do not have to follow the same federal contract rule. Because of this, contract law is different in each state. Plus, as of October 2020, there is no federal law or advice that clearly defines what a "smart contract" is or whether it is legal. The only law that doesn't follow this is the Electronic Signatures in Global and National Commerce Act of 2000. This law gives smart contracts some legal authority. But because it's not clear whether smart contracts are legal or not, they are likely to lead to long court cases.

Jurisdictional Issues

The idea behind blockchain technology, which is what cryptocurrencies are built on, is that you can't be sure where a ledger is. These reasons mean that transactions on the blockchain are more private than transactions on traditional platforms. But this advantage makes it hard to decide who has authority. For starters, because the nodes of a crypto exchange are in different places, they may be subject to different laws. Second, it's hard to figure out the "residence country" for cryptocurrency software because the ledger doesn't have a physical place. Third, the fact that blockchain works across borders makes it very hard to figure out what laws apply and choose the right court for blockchain issues. Because blockchain can be used across borders, it is very hard for national regulators to enforce laws against blockchain users, transactions, or projects.

Data Theft and Financial Fraud

Other urgent legal issues with cryptocurrencies include financial crime and data theft. Many users who engage in illicit activities may be persuaded to adopt cryptocurrencies for their financial transactions by the blockchain's apparent regulatory exemption and anonymity promise.

A significant security vulnerability in the Ethereum blockchain was discovered by Cornell University researcher Matthew Leising in 2017, putting $250 million at risk of theft. In a similar vein, a data security breach at cryptocurrency wallet manufacturer Ledger recently exposed 1 million email addresses. The personal data of Ledger's 9,500 clients, including complete names, mailing addresses, and phone numbers, was also taken. It's unclear if current data rules can handle financial crime and data theft resulting from cryptocurrency.

Privacy Concern

Concerns about privacy are linked to data theft in the bitcoin space. It was one of the main goals of creating cryptocurrencies like Bitcoin so that users could make deals without being tracked. But Chainalysis showed that this privacy was in danger because blockchain analysis tools are always getting better. A company that studies blockchains said it can track most Zcash and Dash transfers, which means that the term "privacy coins" is not valid.

The United States lacks a comprehensive federal framework for data protection. Sector-specific privacy and data security laws and regulations are applicable, including the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA). The current privacy and data security laws and regulations in the United States fail to adequately address the privacy issues associated with blockchain technology. Blockchain technology's distributed peer-to-peer network architecture is often viewed as incompatible with the CCPA's conventional understanding of a centralized, controller-based data processing system. The CCPA's assumption of centralized controller-based processing does not apply to cryptocurrencies, as it overlooks the decentralized nature of this technology.

Legal and Regulatory Concerns for Investors

As of February 2020, cryptocurrencies, including Bitcoin, have been recognized as legal in the United States and in several other developed nations, including the United Kingdom, Japan, and Canada. Despite the IRS recognizing Bitcoin and other virtual currencies as legal, concerns regarding their legal validity persist.

Cryptocurrencies lack support from any centralized issuing authority, and their value is not based on intrinsic goods like gold or silver. Their value is entirely contingent upon the perceptions and valuations assigned by other owners and investors. Due to the absence of a centralized regulatory authority, investors might find themselves with limited legal recourse

should any issues emerge from their cryptocurrency transactions or ownership.

The legal challenges confronting cryptocurrencies are expected to intensify, as there is no single intermediary or authority with exclusive jurisdiction to resolve disputes related to this digital asset class. In a conventional financial transaction, when a party asserts that their account credentials have been compromised and that funds were illicitly transferred from their account, the financial institution, such as a bank, can act as an intermediary to address and resolve the issue. Nonetheless, if a similar situation arises on a blockchain platform, there is currently no established mechanism to resolve such disputes, as cryptocurrency operates in a decentralized manner and lacks financial institutions to serve as intermediaries. Consequently, individuals affected by cryptocurrency theft may find themselves without any legal recourse to recover their losses.

Criminals are expanding their knowledge of Bitcoin in a manner that is both gradual and consistent. Because of the increasing availability and utilization of cryptocurrencies, as well as the fact that they are attractive to illegal activity.

The first kidnapping for crypto-ransom that got a lot of attention happened on January 20, 2015, when someone abducted a Canadian living in San José, Costa Rica, and wanted USD 500,000 in Bitcoin. Since then, Control Risks has seen crypto-ransom kidnaps happen in 12 countries, and the number of cases is slowly rising every year. In 2017, there were an average of two cases involving cryptocurrency every three months. In the first half of 2018, that number rose to one case per month. (conrolrisk.com)

On the official website of the Office of Public Affairs (USDOJ), a federal jury in Greensboro, North Carolina, found a man from Florida guilty of being the leader of an international plot to break into the homes of U.S. citizens, kidnap and beat them, and steal their Bitcoin and other cryptocurrencies. Court papers and evidence show that 24-year-old Remy St Felix from West Palm Beach led a group of thieves who broke into the homes of cryptocurrency owners and stole their money. From September 2022 to July 2023, St. Felix helped plan and carry out a string of thefts in Florida, New York, Durham, North Carolina, and Texas. People whose homes were broken into in St. Felix were taken hostage and told to access and drain their cryptocurrency accounts.

In the report of Mangan (2024), Two young men accused of swindling a Washington, D.C., resident out of $230 million in bitcoin went on a spending spree, buying exotic cars and a $2 million watch and renting mansions, prosecutors said. The failed kidnapping of a couple from Connecticut may have been part of a conspiracy to demand ransom from their son, who is currently being investigated for probable involvement in the crypto theft, according to the police. (www.cnbc.com).

Bangkok, Sept. 27 (CNA) During a news briefing, Thailand's Immigration Bureau announced that a Taiwanese man and his Thai fiancée had just been freed in Bangkok following their kidnapping following a botched bitcoin transaction. After breaking into the house and saving the couple, Thai police detained nine Vietnamese suspects and confiscated a weapon and thirty-three rounds of ammunition. It was discovered by Thai authorities that Lee had consented to buy bitcoin from the Vietnamese males for about 1.7 million Thai Baht (US$52,462). After sending the cryptocurrency to Lee, the Vietnamese did not get paid, and it was only later discovered that he was acting as a middleman for a buyer named A-dong. Thai authorities found that Lee had overstayed his visa and was involved in another case in Taiwan. Nonetheless, Thai policy stipulates that Lee will be subject to judicial proceedings as an abduction victim before his deportation back to Taiwan. (Hsin-hui & Hsiao, 2024).

Bernama (2024), A married couple and four other individuals from Sepang, Malaysia were charged in the Sessions Court here today with the kidnapping of a Chinese national for a ransom of USDT1 million (RM4.44 million) in cryptocurrency last July 11, 2024. The charge document alleges that the six and four other people who are currently at large unjustly detained the Chinese citizen in exchange for USDT 1,007,696 in ransom. The accusations defined under Section 3 (1) of the Kidnapping Act 1961, when read in conjunction with Section 34 of the Penal Code, call for a minimum prison sentence of 30

years or a maximum of 40 years, as well as caning.

New Straits Times, in December 2023, Philippine police discovered the remains of a man believed to be a Malaysian individual who was recently kidnapped and held for ransom. The victim's brother reported to the Philippines police on October 22, 2023, according to Commercial Crime Investigation Department (CCID) director Datuk Seri Ramli Mohamed Yoosuf at a press conference in Kuala Lumpur, Malaysia. The money has been transferred to the kidnappers via cryptocurrency exchange in US dollars.

Philippines police had asked their Malaysian counterpart to help track down the suspect via the ransom transaction through crypto exchanges. The subsequent analysis effectively traced the flow of cryptocurrency transactions, which were sent to an unregistered exchange in Malaysia. The information obtained from that exchange revealed the identities of six foreign individuals who are currently under investigation.

Ramli said the police have received 10 police reports involving a forex investment scam involving RM4.7 million. Victims, in this case, were promised a return of capital and a monthly profit of 5% of the investment amount. Payments of investment amounts ranging from RM437,253.00 to RM864,303.00 were made through the Huobi platform (a cryptocurrency exchange application). (Noorshahrizam 2023).

A news article from Caixin Global highlights a recent kidnapping case in the Philippines involving two ethnic Chinese hostages who were lured to the country and ultimately killed. This incident underscores the growing use of cryptocurrencies in illegal activities. In this case, the abductors insisted that their ransoms be settled using the cryptocurrency USDT. Commonly referred to as Tether, USDT has gained notoriety as a means for individuals engaged in illicit activities to circumvent law enforcement, owing to its straightforward transfer process, anonymity, and consistent value. (Ran &Yukun, 2024).

GMA Integrated News, Police in Bustos, Bulacan said early Sunday morning October 20 that a Chinese national was kidnapped while fishing in the Angat River. According to witnesses, the victim was with other Chinese nationals when four unidentified males abducted and led him to a vehicle. The incident was reported by his live-in partner, who stated that she received a message from his cousin indicating that the abductors were demanding a ransom of $300,000.

Police Brigadier General Jean Fajardo, spokesperson for the Philippine National Police, announced during a press briefing that the victim, who was involved in Philippine Offshore Gaming Operators (POGOs), has been settled with a ransom of P5 million. One of the challenges faced by the Anti-Kidnapping Group was that the payment occurred outside of Philippine jurisdiction. The transaction was conducted using cryptocurrency. The police are currently collaborating with international counterparts to identify the recipients of the P5 million payment, which was disbursed in two installments. (Rita 2024).

The identified issues in kidnapping involving cryptocurrency as ransom payment indicate that numerous cases display shared characteristics. The kidnappers utilized open-source information in a calculated manner to pinpoint individuals with publicly disclosed cryptocurrency assets, ultimately choosing them as targets for abduction. Recent kidnappings are increasingly associated with ransom demands in cryptocurrencies specifically in the cities of Paraňaque and Pasay. This trend is emerging even in countries where the targeting patterns and methods of operation of kidnappers are less advanced. As apprehension increases regarding the evolution of the threat, it is evident that most kidnappers will not possess the required technical expertise and are improbable to act swiftly in seeking crypto-ransom payments. The lack of regulation surrounding cryptocurrencies, coupled with the difficulties law enforcement faces in monitoring transactions, identifying wallet holders, or freezing crypto-wallets as they do with other assets, presents a significant appeal to kidnappers.

This research study addresses the influence of cryptocurrency on contemporary kidnapping for ransom cases in Paraňaque and Pasay, the cities witnessing a significant rise in these occurrences. As traditional ransom payments face increased scrutiny, criminals are

increasingly adopting digital currencies due to their perceived anonymity and ease of transfer.

This research provides several comprehensive analyses of kidnap-for-ransom cases in cities of Paraňaque and Pasay that involved cryptocurrency. The results will show an intricate connection between technology and crime, showing how cryptocurrency makes a new wave of kidnapping easier while making it much harder to stop and deal with.

To provide recommendations for efficient strategies to combat kidnapping for ransom in a landscape that is becoming increasingly digital, the purpose of this study is to provide efficient methods to policymakers and law enforcement organizations about the consequences of cryptocurrencies in criminal activities.

Theoretical Framework of the Study

This study centers on the formal activation of the PNP Anti-Kidnapping Group (AKG) as per NHQ-PNP GO No. DPL-11-01 dated January 19, 2012, was approved by NAPOLCOM Resolution No. 2012-027.

In addition to being a serious crime, kidnapping-for-ransom (KFR) is a life-threatening situation that violates the victim's freedom and human rights. It is serious by definition, and because of its detrimental impact on security, peace, and order, it has turned into a social threat. The prevalence of kidnapping engenders widespread public anxiety and deters investment, thereby influencing the political and economic stability of the nation. The global trend of kidnap-for-ransom has emerged as one of the most prominent criminal activities in the Philippines, largely due to its financial allure. Those engaged in kidnapping orchestrate endeavors that yield substantial financial gains with each successful execution, all while maintaining a comparatively lower level of risk. The kidnappers profit from the archipelagic configuration of the Philippines, as they can move from island to island, rendering it challenging for the government forces to detect and pursue them. Consequently, kidnapping-for-ransom incidents have transpired in numerous regions of the nation, with a particular emphasis on the Greater Manila region and Mindanao.

Though the majority of the victims come from upper-income households, kidnappers also examine the following key factors when selecting a probable target.

- Ability to pay large ransom
- Capability for quick payment
- Noncompliance with the authorities
- Reluctant to inform the police about the incident

In order to combat crime in the nation, various task groups gave rise to the PNP Anti-Kidnapping Group. The first is the establishment of the Presidential Anti-Crime Commission (PACC) by Executive Order No. 3 on July 7, 1992, which was primarily tasked with overseeing and coordinating the actions of the several law enforcement organizations. This occurred when Vice-President Joseph Estrada was appointed PACC's leader by then-President Fidel V. Ramos. Executive Order No. 295 amended Executive No. 8 and established the Presidential Anti-Organized Crime Commission on September 28, 2000. On April 16, 2001, Executive Order No. 10 abolished the Presidential Anti-Organized Crime Commission and PAOCTF and activated STAG. Only three months later, Executive Order No. 23 dated July 6, 2001, established the National Anti-Crime Commission (NACC) to formulate policies, develop coordination methods, and monitor crime prevention and combat efforts. The Police Anti-Crime and Emergency Response (PACER) was operationalized on July 15, 2002, as detailed in the PNP Letter of Instruction LOI 12/02, which also outlines its operational thrusts and functions.

Pursuant to EO 522, PNP Letter of Instruction (LOI) 50/09 (PACER ALPHA) was established on January 27, 2010, mandating the augmentation of measures to be implemented by the Police Anti-Crime and Emergency Response (PACER) to combat the kidnap-for-ransom (KFR) issue. LOI 50/09, PACER ALPHA is the last phase of AKG's evolution since this is the period where paper and other documentation were created for PACER's justification for its activation to (PNP AKG) as a National Operational Support Unit (NOSU).

In accordance with the advice of the Incident Investigation and Review Committee

(IIRC) dated March 4, 2011, the functions of PNP AKG expanded from focusing just on kidnap-for-ransom to encompassing all types of kidnapping and hostage situations.

On January 19, 2012, Resolution No. 2012-027 established PACER as a regular national support unit of the PNP, designated as the PNP-Anti-Kidnapping Group (AKG). Further on February 19, 2012, PNP G.O. # DPL-11-01, Activation of the "PNP AKG" as the key unit of the PNP in addressing the kidnapping menace in the country and in handling hostage situations. (https://akg.pnp.gov.ph/).

As the PNP's main unit for carrying out anti-kidnapping operations, the Anti-Kidnapping Group (AKG) works closely with the LPU, other law enforcement organizations, and the community this will help researcher(s) interpret the data they gather, draw insightful conclusions, and fill in any gaps. Meanwhile, cybercrime response refers to the police intervention in a cybercrime or cyber-related occurrence, wherein the collection of evidential materials is identifiable inside the computer's hardware, software, and network. The First Responder (FR) must safeguard and maintain the integrity of the crime scene and request the aid of the station IOC to identify potential evidence, including the following: contraband or proceeds of a crime; instruments utilized in the perpetration of the crime; and/or additional objects that may facilitate the conduct of the crime. (PNP POP-Manual-2021).

Conceptual Framework of the Study

The following presented the conceptual framework of the study:

Based from Figure 1, the Input-Process-Output or the I-P-O Model will be applied for the present research. The use of the I-P-O Model will be deemed applicable by the researcher(s) in order to effectively show the different inputs, the processes or methods that will be used, and also the intended output of the study.

The INPUTS will be utilized to supply an answer to the statement of the problems, and the variables such as operations, negotiation, and investigation that will be utilized are all expected to be applied. Additionally, it seeks answers to the questions regarding the impact that cryptocurrencies have had on kidnapping for ransom, as well as the issues and challenges that the Anti-Kidnapping Group has encountered, such as pseudonymity, accessibility, regulatory deficiencies, and cross-border transactions, as evaluated by the two groups of respondents. Specifically, it seeks answers to these questions.

PROCESS employed a constructed survey questionnaire and statistical analysis of the data to provide the study's findings, conclusions, and recommendations that including the usage of percentage, weighted mean, or anova.

Lastly, the study's intended OUTPUT will suggest strategic measures for combating kidnapping for ransom using cryptocurrencies in the current era, as a result of technological advancements.

Statement of the Problem

The present study aims to address the influence of cryptocurrency on contemporary kidnapping for ransom in the cities of Pasay and Paraňaque.

Specifically, this study seeks answers to the following questions.

1 How do Police Personnel from the Anti Kidnapping Group (AKG) assess the role of cryptocurrency in modern kidnapping for ransom in terms of:
    1.1 Investigation;
    1.2 Negotiation; and
    1.3 Operations?
2 What will be the impact of cryptocurrency on ransom negotiations, issues and challenges faced by the Anti Kidnapping Group in terms of?
    2.1 Pseudonymity;
    2.2 Accessibility;
    2.3 Regulatory;
    2.4 Deficiencies; and
    2.5 Cross-border transactions
3 Based on the findings of the study, what strategic methods may be recommended to combat kidnapping in the digital landscape?

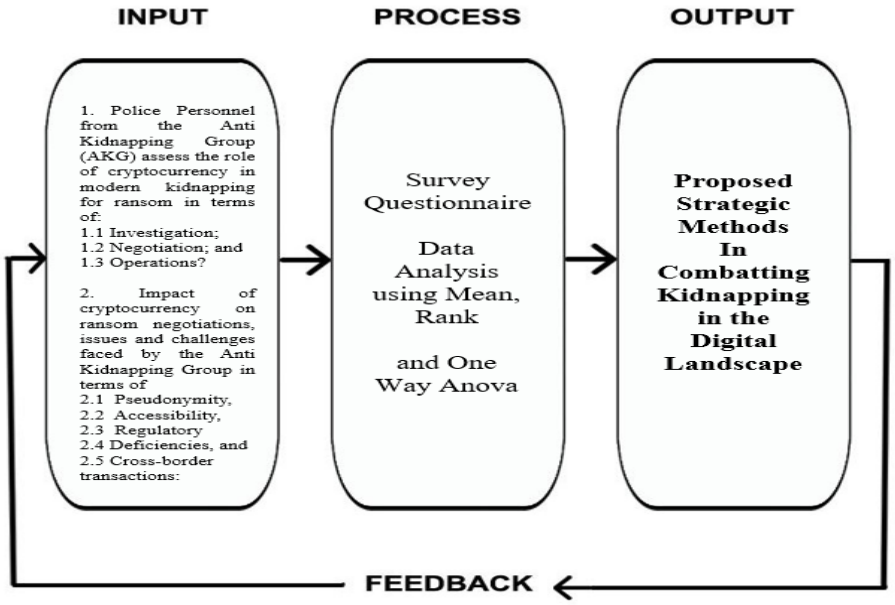

Figure 1. Conceptual Framework

Scope and Limitation of the Study

This study will examine the role of cryptocurrencies in modern kidnapping within the digital age, as evaluated by the two groups: AKG personnel. The study will be undertaken in the cities of Paraňaque and Pasay, which are the top two locations with the highest crime rate index for kidnapping using cryptocurrencies in paying the ransom. The study's timeline extends from January 2023 to November 2024.

Research Method

The study utilized a self-made survey questionnaire in conjunction with a descriptive comparative research framework. The research design employed was stratified random sampling, which meticulously selected respondents from the Anti-Kidnapping Group of the PNP. This study will involve a total of twenty participants. The development of this questionnaire is based on the research findings of Alincastre and Dalugdog (2022). The evaluation utilized a weighted mean to assess the perspectives of PNP personnel regarding the importance of cryptocurrencies in modern kidnapping for ransom, concentrating on investigation, negotiation, and operations. This study examined the impact of cryptocurrencies on ransom transactions and the difficulties faced by the Anti Kidnapping Group, such as pseudonymity, accessibility, regulatory shortcomings, and cross-border transactions. The research outlined systematic approaches to tackle kidnapping in the context of technological advancements.

Respondents of the Study

The main emphasis will be on the role of cryptocurrency in the context of kidnapping, no matter the specific kidnapping incident. The study will involve participants from the Anti Kidnapping Group, specifically the AKG Personnel, Field Unit, Operation, and Investigation. The scope of the study will focus on the cities of Paraňaque and Pasay, specifically targeting areas with the significant numbers reported incidents of kidnapping-related crimes where ransoms are being paid through cryptocurrency.

Table 1. Demographic Profile of the Respondents

Area	PNP (AKG)
Paranaque	10
Pasay	10
TOTAL	**20**

Population and Sampling Scheme

The study utilized stratified random sampling to select law enforcement personnel who

will be engaged in the kidnapping incident. Purposive sampling is a technique whereby the researcher(s) exercise their discretion to identify and select particular individuals for participation in the study. This phenomenon arises when the researcher meticulously evaluates the criteria that an individual must satisfy to qualify for inclusion in the population, with the belief that the sample effectively reflects the characteristics of the population.

Research Instrument

The researcher(s) prepared a survey questionnaire and then verify it to assess its validity before conducting the study. The questionnaire will be structured into three sections: the demographic profile of the respondents, an assessment of their capabilities in investigation, negotiation, and operations, and an exploration of the impact of cryptocurrencies on ransom exchanges. Additionally, it will address the concerns and challenges faced by the Anti Kidnapping Group, including issues related to pseudonymity, accessibility, regulatory deficiencies, and cross-border transactions. The degree of application will be assessed using a 4-point Likert Scale.

The following items were utilized:

4 – Highly Agree
3 – Agree
2 – Slightly Agree
1 – Disagree

Further, it will interpret using the following descriptions:

Quantitative Description	Qualitative Description	Interpretation
3.26 - 4.00	Highly Agree	Distinguished
2.51 – 3.25	Agree	Proficient
2.26 – 2.50	Not Agree	Beginning
1.00 - 1.25	Disagree	Poor

Data Gathering Procedure

A letter of approval will be drafted and emailed to the author prior to utilizing the survey questionnaire for this study. Upon receiving the author's approval, the team validates the instrument to confirm its suitability for the context and the characteristics of the respondents in the study area, incorporating feedback from three experts. A request letter will be submitted to the Office of the Director, AKG, seeking permission to distribute the questionnaires. Upon approval of the letter and receipt of the "go" signal, the researcher proceeded with the distribution of the questionnaire. On the day of questionnaire distribution, the researcher(s) elucidate the study's purpose and guarantee the confidentiality of respondents' answers. The study will take into account the anonymity of the respondents. All gathered data will be utilized solely for this purpose. The researcher(s) will retrieve the questionnaires and the data will be analyzed using various statistical tools.

Statistical Treatment of Data

Statistical analyses will be utilized to examine and understand the data collected from the participants. The following statistical analyses were conducted: 1.) Compute the percentage and frequency distribution to evaluate the demographic profile of the respondents. 2.) Apply the weighted arithmetic mean to sub-problem 2 and sub-problem 3 for the development of strategic methods.

Ethical Consideration

To uphold privacy measures, the papers will be shredded after a period of three years. Furthermore, strict adherence to the important sections of Republic Act 10173, otherwise known as the Data Privacy Act of 2012, will be ensured. All gathered information will be treated with the highest level of confidentiality and solely used for academic research only

The researcher(s) take into account the subsequent ethical guidelines during the collection of raw data:

The researcher(s) will survey with careful consideration of the respondents' demographic profiles and make a personal commitment to safeguarding the identities of individuals will observe or interact with, even in informal settings. Confidentiality will be upheld consistently throughout the research project, encompassing all phases from data collection to data analysis.

The sensitivity checks on the questions in the questionnaires will be designed and verified.

Results and Discussions

The respondents from the Anti Kidnapping Group (AKG) have the following demographic characteristics: age, gender, civil status, level of education, duration of service and trainings attended.

Table 1. Age of the Respondents

Age	Frequency	Percentage
20-30 years old	2	10%
31-40 years old	2	10%
41-50 years old	9	45%
51-60 years old	5	25%
Total	**20**	**100%**

The profile of the respondents categorized by age is presented in Table 1. Forty-five (45) percent of the respondents fall within the age range of 41 to 50. Individuals aged 51 years and older account for 5 respondents, representing 25%, whereas those in the 20-30 and 31-40 age brackets each have 2 respondents, equating to 10%.

Table 2. Sex of the Respondents

Sex	Frequency	Percentage
Male	19	95%
Female	1	5%
Total	**20**	**100%**

The data presented in Table 2 indicates that most respondents are male. 19 individuals have been identified, accounting for 95% of the studied population. Nonetheless, one (1) participant (5%) reported being female. The presence of males suggests a prevailing influence within the PNP workforce. Nonetheless, this study encompasses participants from all genders.

Table 3. Educational Attainment of the Respondents

Educational Attainment	Frequency	Percentage
College Graduate	17	85%
MA/MS Degree Graduate	2	10%
PhD Units	1	5%
Total	**20**	**100%**

The analysis of educational attainment is presented significantly in Table 3. The majority of respondents, comprising 85% (17), are College Graduates. Additionally, 10% (2) hold a Master's Degree, whereas 5% (1) have completed PhD coursework.

Table 4. Civil Status of the Respondents

Civil Status	Frequency	Percentage
Married	18	90%
Single	2	10%
Total	**20**	**100%**

The profile of the respondents based on Civil Status is presented in Table 4. The majority of respondents are married, comprising 18 individuals or 90%, while single respondents account for 2 individuals or 10%.

Table 5. Length of Service of the Respondents

Length of Service	Frequency	Percentage
11 years above	17	85%
2 – 5 years	3	15%
Total	**20**	**100%**

The characteristics of respondents are outlined in Table 5, organized by their length of service. A substantial percentage of the police personnel has been in service for 11 years or longer, leading to 17 respondents, accounting for 85% of the total. A total of 3 respondents, accounting for 15%, have been in service for a period of 2 to 5 years.

Table 6. Seminars and Trainings Attended for Anti-Kidnapping

Seminars and Training Attended for Anti-Kidnapping	Frequency	Percentage
Yes	13	65%
No	7	35%
Total	**20**	**100%**

Table 6 indicates that 13 out of 20 respondents, or 65%, have engaged in specialized training courses centered on Anti-Kidnapping with a focus on cryptocurrency as a mode of payment. Conversely, 35%, which equates to 7 out of 20 respondents, reported that they have not participated in any basic seminars focused on anti-kidnapping.

Sub-problem No. 1. Police Personnel (AKG) assessed the role of cryptocurrency in modern kidnapping for ransom.

Table 7 illustrates the respondents' assessment on the role of cryptocurrency in modern kidnapping for ransom in terms of investigation.

Table 7. Respondents' Assessment on the Role of Cryptocurrency in Modern Kidnapping for Ransom in terms of Investigation

Indicators	Weighted Mean	Interpretation
1. Every transaction submitted to the messaging app will be thoroughly examined by a knowledgeable cryptocurrency investigator. The investigator will then attempt to determine which address the money should be delivered to.	3.45	Highly Agree
2. The investigator is to attempt to uncover the identity of the person who owns the address, which comes after the identification of the address.	3.30	Agree
3. An investigator will find the owner of a cryptocurrency address by using Open-Source Intelligence (OSINT) and Know Your Customer (KYC) data that the exchanges receive. After that, the police can issue orders and try to get the victim back.	3.00	Agree
4. Investigations into cryptocurrency have been conducted in numerous high-profile cases, prompting the authorities to initiate a crypto investigate to trace the ransomware payment.	3.25	Agree

Indicators	Weighted Mean	Interpretation
5. The investigation discovered that the funds were transmitted to an e-wallet application. The police subsequently executed a seizure and retrieved the ransom.	3.00	Agree
Total	**3.20**	**Agree**

Legend:
3.26 - 4.00 Highly Agree
2.51 – 3.25 Agree
2.26 – 2.50 Not Agree
1.00 - 1.25 Disagree

The result shows that the overall assessment of the respondents is Agree, with mean score of 3.20.

The AKG personnel group has a Highly Agree assessment regarding the indicator: "Every transaction submitted to the messaging app will be thoroughly examined by a knowledgeable cryptocurrency investigator." The investigator will then try to ascertain the appropriate address for the delivery of the funds, with the lowest mean of 3.00 coming from indicator numbers 3 and 5, which state: "An investigator will identify the owner of a cryptocurrency address by utilizing Open-Source Intelligence (OSINT) and Know Your Customer (KYC) data obtained from exchanges." Following that, the police may issue directives and attempt to recover the victim," and "The investigation revealed that the funds were sent to an e-wallet application. The police then carried out a seizure and recovered the ransom.

Table 8 illustrates the respondents' assessment on the role of cryptocurrency in modern kidnapping for ransom in terms of negotiation.

Table 8. Respondents' Assessment on the Role of Cryptocurrency in Modern Kidnapping for Ransom in terms of Negotiation

Indicators	Weighted Mean	Interpretation
1. Investigators support the negotiator in the process by monitoring stolen or concealed ransom cryptocurrency money.	3.20	Agree
2. Senior PNP authorities, in conjunction with the victim's family, will defer the decision regarding payment and will await the outcome of negotiations from the investigator or a third party.	3.1	Agree
3. If the negotiator fails to act and the victim dies or is injured, the victim or his family may sue the PNP.	1.85	Not Agree
4. It is essential to develop contingency plans throughout the negotiation process.	3.35	Highly Agree
5. During negotiations, it is impractical to impose any definite limitations on the sum required to ensure the release of a kidnapping victim.	2.70	Agree
Total	**2.84**	**Agree**

Legend:
3.26 - 4.00 Highly Agree
2.51 – 3.25 Agree
2.26 – 2.50 Not Agree
1.00 - 1.25 Disagree

The result shows that the overall assessment of the respondents is Agree, with mean score of 2.84.

The AKG personnel group has an overwhelming agreement on the indicator: "It is essential to develop contingency plans throughout the negotiation process." The mean score stands at 3.35, indicating a highly agree. The indicator 3 has the lowest mean score of 1.85, indicating a response of not agree. "Should the negotiator neglect to take action and the victim suffers injury or death, the victim or their family may pursue legal action against the PNP."

Table 9 illustrates the respondents' assessment on the role of cryptocurrency in modern kidnapping for ransom in terms of operation.

The findings indicate that respondents' overall assessment is Highly Agree, with a mean score of 3.42.

The AKG personnel group exhibits strong consensus regarding indicators 4 and 6, with both receiving a mean score of 3.60. Indicator 4 states, "AKG will immediately activate the Anti-Kidnapping Action Team (AKAT) to investigate, negotiate, operate, and gather intelligence on the case," while indicator 6 emphasizes, "If a foreign national is kidnapped, identify their nationality and personal circumstances." Indicator 1 states that upon receiving the kidnapping report at the police station, the Chief of Police (COP) and the investigator will conduct a preliminary review of the provided information. Indicator 3 indicates that the Anti-Kidnapping Group (AKG) will engage the Anti-Cybercrime Group (ACG) in assessments related to kidnapping for ransom, particularly when cryptocurrency is used as the payment method. The weighted mean of 3.20 indicates agreement.

Table 9. Respondents' Assessment on the Role of Cryptocurrency in Modern Kidnapping for Ransom in terms of Operation

Indicators	Weighted Mean	Interpretation
1. Following receipt of the kidnapping report at the police station, the COP and investigator, will perform a preliminary review of the supplied information.	**3.20**	Agree
2. The AKG will assemble a team consisting of quad personnel and the duty officer of the day. The dispute will be evaluated to determine the operational action.	**3.45**	Highly Agree
3. AKG will involve the ACG as the assessment relates to kidnapping for ransom utilizing cryptocurrency as the method of payment.	**3.20**	Agree
4. AKG will immediately activate the Anti-Kidnapping Action Team (AKAT) to investigate, negotiate, operate, and gather intelligence on the case.	**3.60**	Highly Agree
5. AKG will seek for the Critical Incident Management Task Group (CIMTG) to be activated if the case is determined to be a kidnapping committed by TGs. The PNP will offer complete assistance and collaboration as the situation may be activated.	**3.50**	Highly Agree
6. If a foreign national is kidnapped, identify their nationality and personal circumstances.	**3.60**	Highly Agree
Total	**3.42**	**Highly Agree**

Legend:

3.26 - 4.00	Highly Agree
2.51 – 3.25	Agree
2.26 – 2.50	Not Agree
1.00 - 1.25	Disagree

Sub-problem No. 2. Police Personnel (AKG) assessed the impact of cryptocurrency on ransom negotiations, issues and challenges faced by the Anti Kidnapping Group.

Table 10 illustrates the respondents' assessment on the impact of cryptocurrency on ransom negotiations, issues and challenges faced by the Anti Kidnapping Group in terms of pseudonymity.

The results reveal that the participants' general evaluation is Highly Agree, reflected in a mean score of 3.29.

The AKG personnel group demonstrates a notable agreement concerning indicator 1, which states that police personnel face difficulties in analyzing information due to their inability to verify the identity of users who employ pseudonyms. Additionally, indicator 3 asserts that it is possible to identify the identity of a kidnapper, even when a pseudonym is utilized. Nonetheless, this procedure necessitates the amalgamation of diverse data sources and technologies, a task that can be intricate and labor-intensive, with both achieving a mean score of 3.35.

Indicator 2 articulates that "PNP personnel are limited in their capacity to assist with the investigation, as pseudonymization serves to safeguard privacy and enhances the protection afforded to the kidnappers." The weighted mean of 3.10 signifies a consensus, representing the lowest indicator within the group.

Table 10. Respondents' Assessment on the Impact of Cryptocurrency on Ransom Negotiations, Issues and Challenges faced by the Anti Kidnapping Group in terms of Pseudonymity

Indicators	Weighted Mean	Interpretation
1. Police personnel encounter challenges when analyzing information since they cannot verify the identity of any user because they utilize pseudonym names.	3.35	Highly Agree
2. PNP personnel cannot do much help with the investigation since pseudonymization protects privacy and increases protection for the kidnappers.	3.10	Agree
3. Identifying the identity of a kidnapper, even when a pseudonym is used, is feasible. However, this process requires the integration of various data sources and technologies, which can be complex and time-consuming.	3.35	Highly Agree
4. Pseudonymized personal data that can be linked to an individual through additional information should be submitted to the AKG and ACG for real-time processing.	3.30	Agree
5. Pseudemys personal data, which is protected by encryption, access control, and other safeguards against privacy violations, has imposed a significant burden on the ACG group in processing information.	3.35	Agree
Total	**3.29**	**Highly Agree**

Legend:

3.26 - 4.00	Highly Agree
2.51 – 3.25	Agree
2.26 – 2.50	Not Agree
1.00 - 1.25	Disagree

The findings indicate that the participants' overall assessment is Agree, as evidenced by a mean score of 3.19.

The AKG personnel group exhibits significant consensus regarding indicator 1, which asserts that the contemporary kidnapper possesses the requisite skills to obtain wireless access (WiFi), employ internet-enabled devices, access energy, and has a technical education. Furthermore, indicator 2 indicates that the

kidnapper is proficient in evaluating accessibility in terms of usability and expense. Analogous to a credit card, kidnappers necessitate a cryptocurrency wallet and an exchange platform to transact and employ virtual currencies.

Meanwhile indicator number 3 "Coinbase, a leading bitcoin trading platform, generates revenue through transaction fees. Access to the bitcoin marketplace is predominantly inaccessible without platforms like Coinbase", which had the lowest weighted mean of 3.05, understood as agreement.

Table 11. Respondents' Assessment on the Impact of Cryptocurrency on Ransom Negotiations, Issues and Challenges faced by the Anti Kidnapping Group in terms of Accessibility

Indicators	Weighted Mean	Interpretation
1. The modern kidnapper is equipped with the necessary skills to acquire wireless access (WiFi), utilize devices with internet connectivity, access electricity, and possess a technical education.	3.30	Highly Agree
2. The kidnapper is skilled in assessing accessibility regarding ease of use and cost. Similar to a credit card, kidnapper require a cryptocurrency wallet and an exchange platform to trade and utilize virtual currencies.	3.30	Highly Agree
3. Cryptocurrencies are truly accessible; they can be used by anyone without the need for verification.	3.10	Agree
4. Coinbase, a prominent cryptocurrency exchange platform, derives its money from transaction fees. Access to the cryptocurrency marketplace is mainly unavailable without platforms such as Coinbase.	3.05	Agree
5. After overcoming entry challenges and obtaining digital wallets through virtual platforms, kidnappers are ready to engage in digital currency transactions.	3.20	Agree
Total	**3.19**	**Agree**

Legend:

3.26 - 4.00	Highly Agree
2.51 – 3.25	Agree
2.26 – 2.50	Not Agree
1.00 - 1.25	Disagree

The results demonstrate that the participants' overall evaluation is Agree, supported by a mean score of 3.19.

The AKG personnel group demonstrates a strong agreement concerning indicator 2, which states that there are no current legislation specifically safeguarding victims who utilize cryptocurrencies in cases where virtual currencies are employed as a payment method for kidnapping for ransom, reflected by a high weighted mean of 3.30, interpreted as Highly Agree.

Additionally, indicator 4 demonstrates that a central bank neither issues nor guarantees virtual currencies. Virtual currencies lack backing by cash, gold, or silver, unlike electronic money, which has a weighted mean of 3.25, indicating agreement. Indicator number 1 has a weighted mean of 3.05, interpreted as agree, and received the lowest mean score in the group, which states that "The BSP and other regulatory bodies in the Philippines do not yet oversee cryptocurrencies."

Table 12. Respondents' Assessment on the Impact of Cryptocurrency on Ransom Negotiations, Issues and Challenges faced by the Anti Kidnapping Group in terms of Regulatory

Indicators	Weighted Mean	Interpretation
1. The BSP and other regulatory bodies in the Philippines do not yet oversee cryptocurrencies.	3.05	Agree
2. There are no existing legislation that particularly protect victims from using cryptocurrencies if the kidnapping for ransom uses virtual currencies as a means of payment.	3.30	Highly Agree
3. The BSP is closely observing developments in virtual currencies, especially regarding their potential use in money laundering and other illicit activities, and will implement necessary measures as required.	3.20	Agree
4. A central bank does not issue or guarantee virtual currencies. Virtual currencies are not backed by cash, gold, or silver like electronic money is.	3.25	Agree
5. Virtual currencies offer clients a significant level of confidentiality, which can facilitate money laundering and other illegal activities.	3.15	Agree
Total	**3.19**	**Agree**

Legend:

3.26 - 4.00	Highly Agree
2.51 – 3.25	Agree
2.26 – 2.50	Not Agree
1.00 - 1.25	Disagree

The findings indicate that the participants' overall assessment is Agree, corroborated by a mean score of 3.12.

The AKG personnel group exhibits substantial consensus about indicator 3, which posits that enhanced legal compliance may result in market concentration, favoring only larger, more resourceful users (hackers), as seen by a high weighted mean of 3.40, interpreted as Highly Agree. Furthermore, indicator 2 illustrates that local bitcoin exchanges and enterprises may encounter increased regulation, perhaps imposing fees on the user (hacker), with a weighted mean of 3.15, signifying concurrence.

Indicator number 1 possesses a weighted mean of 3.00, interpreted as agreement, and attained the lowest mean score within the group, which asserts that "The Philippines collaborates with the Financial Action Task Force (FATF) to address strategic deficiencies in money laundering, terrorist financing, and proliferation finance."

Table 13. Respondents' Assessment on the Impact of Cryptocurrency on Ransom Negotiations, Issues and Challenges faced by the Anti Kidnapping Group in terms of Deficiencies

Indicators	Weighted Mean	Interpretation
1. The Philippines works with the Financial Action Task Force (FATF) to solve strategic shortcomings in money laundering, terrorist funding, and proliferation finance.	3.00	Agree
2. Local bitcoin exchanges and businesses may face additional regulation, which may impose costs on the user (hacker).	3.15	Agree

Indicators	Weighted Mean	Interpretation
3. Increasing legal compliance could lead to market concentration where only larger, more resourceful user (hacker) survive.	3.40	Highly Agree
4. Leading the National Money Laundering/Terrorist Financing Risk Assessment Working Group helps the AMLC work with government and business to address bitcoin use in illegal operations.	3.00	Agree
5. It's also important to have laws like the Anti-Fraudulent Activities in Financial Accounts Act (AFASA) and the planned changes to the Bank Secrecy Law.	3.05	Agree
Total	**3.12**	**Agree**

Legend:

3.26 - 4.00	Highly Agree
2.51 – 3.25	Agree
2.26 – 2.50	Not Agree
1.00 - 1.25	Disagree

The results show that the participants' general evaluation is Agree, supported by a mean score of 3.15.

The AKG personnel group demonstrates significant agreement regarding indicator 3, which states that cryptocurrencies facilitate faster, cheaper, safer, and untraceable cross-border money transfers, evidenced by a high weighted mean of 3.30, interpreted as Highly Agree. Additionally, indicator 4 reveals that the PNP (ACG) is deficient in advanced technologies necessary to prevent the utilization of blockchain technology for facilitating cross-border transactions using bitcoin, reflected by a weighted mean of 3.25, indicating agreement.

Indicator number 1 has a weighted mean of 3.05, which is interpreted as agree, and it achieved the lowest mean score within the group. This indicates that transacting cryptocurrency across international borders lacks legal jurisdiction concerning the PNP or the country.

Table 14. Respondents' Assessment on the Impact of Cryptocurrency on Ransom Negotiations, Issues and Challenges faced by the Anti Kidnapping Group in terms of Deficiencies

Indicators	Weighted Mean	Interpretation
1. Transacting cryptocurrency over international borders has no legal jurisdiction over the PNP or the country.	3.05	Agree
2. International partners interact voluntarily with Filipino crypto companies, because they have no understanding about the unlawful use of cryptocurrency in the country.	3.00	Agree
3. Cryptocurrencies provide faster, cheaper, safer, and untraceable cross-border money transfers.	3.30	Highly Agree
4. The PNP (ACG) lacks advanced technologies to prevent the use of blockchain technology to promote cross-border transactions utilizing bitcoin.	3.25	Agree
5. Cryptocurrency Cross Border transfers can cut down on fees and processing times by getting rid of middlemen. This speed is especially helpful for international transactions, which are famously slow and pricey when done through traditional banking channels.	3.15	Agree
Total	**3.15**	**Agree**

Legend:

3.26 - 4.00	Highly Agree
2.51 – 3.25	Agree
2.26 – 2.50	Not Agree
1.00 - 1.25	Disagree

Conclusions

Based from the findings of the study, the following conclusion were drawn:

1 The findings of the investigation, negotiation, and operations are in agreement, as evidenced by the observations made by the respondents regarding the role that cryptocurrency plays in contemporary kidnapping for ransom.

2 The participants in the study demonstrate a general understanding of the investigation procedure, suggesting that transactions sent through the messaging app will be thoroughly analyzed by an experienced cryptocurrency investigator, who will then attempt to identify the correct address for fund delivery.

3 Overall, the respondents concurred that it is imperative to establish contingency plans during the negotiation process. Additionally, the Anti-Kidnapping Action Team (AKAT) will be activated immediately by the Anti-Kidnapping Guard (AKG) in order to investigate, negotiate, operate, and acquire intelligence regarding the case.

4 The respondents perceive those police personnel encounter challenges in analyzing information due to the inability to verify user identities, as individuals employ pseudonyms and pseudonymous personal data. The protection of this data through encryption, access control, and other privacy safeguards has significantly burdened the AKG group in their information processing efforts.

5 The AKG faced challenges in obtaining the necessary skills to access energy, and they have a technical education that prepares them for overcoming obstacles and difficulties, as the kidnapper is adept at assessing accessibility regarding usability and expense. Kidnappers are adept at trading and utilizing virtual currencies, employing a cryptocurrency wallet and an exchange platform with the same proficiency as they do with credit cards.

6 Enhancing existing legislation provides targeted protection for victims in cases where cryptocurrencies are employed as a payment method in kidnapping for ransom situations.

7 Increased legal compliance could lead to market dominance, benefiting primarily larger and more resourceful users (hackers), as cryptocurrencies facilitate faster, cheaper, safer, and untraceable cross-border money transfers.

8 Emphasized strong regulation, including the Anti-Fraudulent Activities in Financial Accounts Act (AFASA) and the suggested amendments to the Bank Secrecy Act, are essential and long overdue.

9 The BSP and other regulatory authorities in the Philippines must actively oversee cryptocurrencies.

10 PNP AKG and ACG necessitate revised techniques to proficiently obstruct blockchain technology from enabling cross-border bitcoin transactions.

11 Lastly, it is advisable to conduct a triangulation study to further verify the findings and conclusions, particularly regarding the use of qualitative research.

Recommendations

Based on the conclusions of the study, the researcher strongly recommends the following:

1 PNP AKG delivered informative lectures and seminars on the prevention of kidnapping. These sessions emphasized the importance of awareness regarding common tactics used by kidnappers, early warning signs, and effective measures for prevention. By equipping police officers with this knowledge, the AKG aims to improve their capacity to recognize and address potential threats.

2 PNP AKG will implement a comprehensive media awareness initiative centered on the prevention of kidnapping, with hotline numbers and emergency contacts strategically placed throughout the Pasay and Paranaque. These awareness campaign serves as a persistent reminder and readily available resource for community to swiftly seek assistance should they notice any suspicious activities or signs of potential threats.

3 Highlights the significance of collaborative efforts between law enforcement agencies and private organizations in addressing the issue of kidnapping for ransom, thereby broadening the outreach and fortifying the collective response to criminal activities.

4 The BSP is actively monitoring developments regarding these virtual currencies, especially their potential use for money laundering and other illicit purposes, and will take appropriate action when necessary. In the meantime, the BSP has publicly urged to become familiar with some basic information regarding cryptocurrencies that are used in illegal activities.

5 The PNP AKG and ACG require modern technologies and training in the use of equipment that hinders the implementation of blockchain technology, which could enable cross-border transactions using bitcoin.

Acknowledgement

The researcher(s) would like to acknowledge the following individuals who gave support and served as inspiration for her study:

THE GOD ALMIGHTY who gave the researcher(s) wisdom, courage, patience and good health in accomplishing her study;

TO OUR FAMILIES who gave us untiring support all the way from the start to end of our study;

PBGEN ROEL CUEVAS RODOLFO, Director of Anti-Kidnapping Group, for his clever opinions, comments, sharing his time and intelligent ideas to the researcher(s) to complete the study; and recommendations for the enhancement of the paper for international presentations;

ELIZABETH BUENA-VILLA, PhD. Director CCJEGS, professional Lecturer of the De La Salle University – Dasmariñas Cavite, for being compassionate and for always reminding the researcher(s) to finish the research study;

FROILAN D. MOBO, PhD. for his smart recommendations and opinions for the enhancement of the researcher(s) study;

Finally, **THE AKG COMMAND GROUP,** for their support and cooperation to the researcher(s).

References

Alincastre, G. D., & Dalugdog, W. D. (2022). Internal stakeholders' evaluation of the Philippine National Police Electronic – Project Systems. *International Journal of Academe and IndustryResearch*, *3*(1), 93–109. https://doi.org/10.53378/352859

Aznan, A. H., Ridzuan, A. R., Amri, A. L. M.S., Hamim, M. a. F. M., Mustazar, M. a. D., Djuyandi, Y., Wahab, S. A., & Zailani, M. H. Z. (2023). THE LEVEL OF EFFECTIVENESS OF UNITY GOVERNMENT IN MALAYSIA. *Deleted Journal*, 495–503. https://doi.org/10.33102/iiecons.v10i1.23

Executive No. 8 and established the Presdential Anti-Organized Crime Commission

Executive Order No. 23 dated July 6, 2001, established the National Anti-Crime Commission (NACC)

Jadhav, G. G., Gaikwad, S. V., & Bapat, D. (2023). A systematic literature review: digital marketing and its impact on SMEs. *Journal of Indian Business Research*, *15*(1), 76–91. https://doi.org/10.1108/jibr-05-2022-0129

Jadhav, S. D., Raghunath, C. P. S., Hamid, W., & Anil, M. V. (2022b). A study on awareness of college students about cryptocurrency and Its relation to Level of Education. *Indonesian Journal of Educational Research and Technology*, *3*(2), 155–160. https://doi.org/10.17509/ijert.v3i2.50083

NAPOLCOM Resolution No. 2012-027. Office of Public Affairs (USDOJ) (2024). Foreign National Pleads Guilty to Laundering Millions in Proceeds from Cryptocurrency Investment Scams

PNP Anti-Kidnapping Group (AKG) as per NHQ-PNP GO No. DPL-11-01
PNP Letter of Instruction LOI 12/02
PNP POP-Manual-2021
Presidential Anti-Crime Commission (PACC) by Executive Order No. 3
LOI 50/09, PACER ALPHA
bankrate.com
conrolrisk.com
freemanlaw.com
investopedia.com