



The University of Trinidad and Tobago

UNIVERSITY OF TRINIDAD AND TOBAGO (UTT), year (2025)
CENTRE FOR INFORMATION AND COMMUNICATION
TECHNOLOGY

Master of Science in Cybersecurity

PROJECT TITLE:

*(Enhancing Law Enforcement's Preparedness: A Study on Cryptocurrency Awareness
in the TTPS)*

Jason Ricardo Ramlal

Student ID#: 92068

Year of Submission (2025)

**This work is being submitted in partial fulfilment of the requirements for a
Master of Science**

Supervisor Name: Ms. Lisa Wharwood
Coordinator: Mr. Mahindra Persad Koon

Abstract

Cryptocurrencies have transformed traditional financial systems globally whilst simultaneously creating complex challenges for law enforcement. The Trinidad and Tobago Police Service (TTPS) faces increase problems as it relates to financial crimes and issues surrounding cryptocurrencies. Yet no systematic evaluation to determine its preparedness to combat these issues has been done. This research investigates the level of cryptocurrency awareness within the TTPS management and evaluates the institution's readiness to address crimes involving digital assets.

A mixed-methods research design was adopted that combined aspects of phenomenology and included survey data from 95 TTPS officers across all management levels, interviews from officials in key investigative units and institutional stakeholders. The research revealed stratified awareness, with lower management demonstrating greater familiarity with cryptocurrency concepts than their senior counterparts. Consequently, significant gaps were identified across all management tiers in technical knowledge, regulatory understanding, investigative training, and inter-agency coordination. Most significantly, despite a sharp increase in crypto-related crimes and monetary losses, there were no prosecutions. The study determines that the TTPS is critically underprepared to address the rising threat of cryptocurrency-enabled crime.

Based on this the proposal of a strategic implementation plan was developed, focusing on six pillars: structured training, policy and SOP development, technical tool acquisition, inter-agency collaboration, information sharing protocols, and public engagement. Overall, the findings discovered offer vital insights for institutional reform and advocate for a proactive, coordinated, and informed response by law enforcement in the digital age.

Table of Contents

CHAPTER 1: (Introduction)	1-3
CHAPTER 2: (Methodology)	4-5
CHAPTER 3: (Literature Review)	6-24
CHAPTER 4: (Survey, Interviews and Analysis).....	25-38
CHAPTER 5: (Discussions).....	39-43
CHAPTER 6: (Implementation).....	44-51
CHAPTER 7: (Conclusion).....	52-54
REFERENCES.....	55-59
APPENDICIES	
A: (Project proposal)	60-66
B: (Interview guide FIB).....	67-69
C: (Interview guide PTA).....	70-71
D: (Interview guide CSMU).....	72-74
E: (Interview guide Fraud Squad).....	75-76
E: (Survey questionnaire).....	77-78

Chapter 1

Introduction

Assassinated 35th president of the United States of America *John F Kennedy* quoted over sixty years ago “*Change is the law of life and those who look only to the past or present are certain to miss the future*”. This interesting quote had certainly set the tone for what was yet to be realized in the distant future. Enter cryptocurrency, emerging over fifteen years ago (Nakamoto, 2008), cryptocurrency revolutionized financial technology and the digital landscape. Features such as secure and decentralized transactions coupled with the removal of traditional banking intermediaries are some of the reasons why cryptocurrencies have gained significant popularity within society. Conversely, even though cryptocurrency has seen widespread adoption for genuine endeavors, its pseudonymous nature has also made it attractive for illicit activities, including fraud, money laundering, ransomware attacks, and dark web transactions. Ultimately, this evolving landscape has placed law enforcement agencies globally in a precarious position as traditional methods of investigations are often ineffective in addressing cryptocurrency-related crimes.

Recently, in Trinidad and Tobago there is an apparent growing concern as it relates to cybercrime involving cryptocurrency (Carrington, 2023). This being the case, there appears to be limited specialized training, resources, and legislative tools available to TTPS to effectively investigate and mitigate such instances. It is evident that there is an evolution of the digital landscape as it concerns financial crimes and this occurrence demands that there must be heightened awareness and more specialized training among TTPS officers. Further, a lack of awareness and technical understanding within the TTPS can hinder investigative efforts,

reducing the likelihood of successful prosecutions ultimately undermining public trust and confidence. Globally, efforts are being made to regulate cryptocurrency from a law enforcement perspective. However, in Trinidad and Tobago its law enforcement framework does not provide a structured approach to address crimes within this sphere. Moreover, there exists no data or systematic assessment that can speak to preparedness or knowledge levels of TTPS's personnel, particularly its managerial population. Importantly, this gap must be bridged as modernization is a crucial noun to the TTPS in its approach towards financial crimes and ensuring they are equipped to navigate the complexities of cryptocurrency investigations.

In my study, the central aim was to assess the current level of cryptocurrency awareness among management personnel within the TTPS with a view to enhancing their capabilities through the exploration of contemporary strategies. More specifically, I had several interests—they included developing a comprehensive understanding of cryptocurrency technologies and their key components, investigating the levels of awareness across TTPS management tiers, and identifying reported instances of cryptocurrency-related crime in Trinidad and Tobago. I was desirous of proposing an awareness and capacity-building programme tailored to TTPS's needs. In my contemplations, the main question was “How prepared is the Trinidad and Tobago Police Service (TTPS) to address cryptocurrency-related crimes and how can a targeted awareness programme improve their investigative capacity?” The former directed me to four (4) sub-questions that offered support; “what is the current level of cryptocurrency awareness among TTPS personnel?”, “what are the key challenges faced by TTPS in investigating cryptocurrency-related crimes?”, “what training, tools, or resources are currently available, along with what gaps exists?”, and “how a structured awareness and capacity-building strategy could improve the TTPS's overall effectiveness?”.

My justification is to suggest practical insights that may enhance law enforcement readiness, support the development of tailored training programmes and strengthen inter-agency collaboration whilst contributing to academic knowledge on policing cryptocurrency crimes in small island developing states like Trinidad and Tobago. Notably, I have chosen a unique sample and decided to focus on assessing cryptocurrency awareness from the management levels within the TTPS. I have also considered several limitations in this study namely, gaps in available crime data, reliance on self-reported survey responses, possible biases and the rapidly evolving nature of cryptocurrency technologies, which may affect the longevity of the findings. In executing my thesis report I propose the following outline of my project: Chapter 1: Introduction (project background, problem statement, research aim, significance, and scope). Chapter 2: Methodology (research design, data collection methods, and analysis approach). Chapter 3: Literature Review (overview of cryptocurrency, law enforcement challenges and synthesis and implications). Chapter 4: Survey and Analysis (key research findings and considerations). Chapter 5: Discussions (presentation and interpretation of survey results and other data, critical reflections, and recommendations for frameworks). Chapter 6: Implementations (action plan and challenges). Chapter 7 Conclusions (summary of key findings and areas for future research).

Chapter 2

Methodology

In this section, the methodology employed in this study will be outlined as follows.

- Research Design
- Data Collection Methods
- Analysis Techniques

The above will ensure that the research objectives are met and that findings are valid and reliable.

1. Research Design (mixed)

- The study will adopt a quantitative and qualitative research approach, utilizing surveys and interviews to collect data from TTPS personnel.
- A descriptive analysis will be used to assess cryptocurrency awareness levels.
- The qualitative component is informed by phenomenological principles, aiming to explore the lived experiences and perceptions of officers regarding cryptocurrency-related crimes and institutional preparedness.

2. Data Collection Methods

- A structured questionnaire will be administered to TTPS officers at various management levels.
- Interviews with senior TTPS officials responsible for key areas within the organization.
- Secondary data, including crime reports and regulatory documents, will be analyzed.

3. Data Analysis Techniques

- Descriptive statistics will be used to summarize survey responses.
- Correlation analysis will examine relationships between cryptocurrency knowledge and law enforcement effectiveness.

This methodology ensures a systematic and objective approach to investigating cryptocurrency awareness in TTPS.

Chapter 3

Literature Review

‘The illiterate of the twenty-first century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn.’ (Alvin Toffler, 1970) A digital asset can be described as a digital representation of something of value, for example, cryptocurrency (Yuming, 2022) which is a central topic in this review. This study captioned; “Enhancing Law Enforcement's Preparedness: A Study on Cryptocurrency Awareness in the TTPS” is pertinent to the Trinidad and Tobago Police Service (TTPS) as empirical data collected shows that there exist several gaps as it relates to the technology within the organization. The relevancy of this research cannot be overstated as several factors such as rising cryptocurrency crimes, public protection, judicial and legal support, institutional modernization, and operational breaches can generate meaningful conversations. Ultimately this leads to the questions of How prepared is the TTPS to address cryptocurrency-related crimes and how can a targeted awareness program enhance their capacity to effectively manage such cases?

A quintessential intention of this study encompasses adding to the awareness and understanding of the cryptocurrency ecosystem (Garewal, 2020) not from a law enforcement perspective solely but for assisting in academic endeavors as well as general educational capacity building. To achieve this the study would generate conversations on several subject areas such as *Understanding Cryptocurrency* within its ecosystem which would encapsulate historical perspectives and the components behind the technology, *the Regulatory Framework and Legal Considerations*, *TTPS’s position* in relation training, knowledge and contemporary policing, *the Role of Actors* within the ecosystem and finally *Synthesis and Implications* for the TTPS. It is

hoped that on completion of this research the knowledge gaps that exist within the TTPS will be bridged effectively.

Understanding Cryptocurrency and Its Ecosystem

The term cryptocurrency was first used sometime in 2009 just about a year after the popular white paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto, 2008) was published online via at “metzdowd.com” a website that it is dedicated to the discussion of cryptographic technology and its influence on politics (“Cryptography”, n.d.). There is a plethora of components that are rudimentary in relation to cryptocurrencies’ operation (Malik & Rana, 2020) however based on the scope of this study only the following will be discussed succinctly via following subheadings, Blockchain Technology, Digital Assets, Smart Contracts, Wallets, and their Security Risks.

Blockchain Technology: an integral component of a cryptocurrency systems is blockchain-technology (What is blockchain?, n.d.). Its unique engineering has been a catalyst for development in the context of digital transactions. Blockchain technology, with their decentralized architecture is crucial to digital currencies (Ilham, Erlina, Fachrudin, Silalahi, & Saputra, 2019). It (Rebel, 2021) was first conceptualised and introduced by Satoshi Nakamoto sometime in 2008 (Nakamoto, 2008). Typically, the technology involves a sophisticated database mechanisms known as blockchains (Khanfar, 2021) that enables seamless and transparent sharing of information within a business network. Within a blockchain database, data is organized into interconnected blocks forming a chronological chain. This structure ensures the integrity of the data as it cannot be deleted or modified without consensus from the network participants (Nicholas Kolokotronis, 2019). Consequently, blockchain technology offers the ability to establish an immutable ledger for tracking various transactions such as orders,

payments, and accounts. The system incorporates inherent measures that safeguard against unauthorized transaction entries and promote consistency across the network's shared view of these transactions. They can also facilitate criminal activity as in blockchains such as Monero that allows full anonymity. Furthermore, when discussing blockchain technology, the term “Digital Assets” will form part of the conversation and will be explained next.

Digital Assets: Next, according to research during this study, digital assets can be described as a digital representation of something of value, for example, logos, artwork, music, tokens, and digital currency/ cryptocurrency (Yuming, 2022). The Securities and Exchange Commission of Trinidad and Tobago suggests cryptocurrencies may be defined as a digital decentralized variation of currency that utilizes cryptography to afford secure transactions by users (Cryptocurrencies, 2019). Cryptocurrencies, a popular digital asset, has been realized by most of the world and in some jurisdiction functions as a contemporary form of payment for goods as services. They can be either a stable coin (Bhattacharya, Vasilyev, & Villafuerte, 2023) in that they are regulated by a central authority and pegged to something of value or not, where their value is determined by a combination of market sentiment and supply and demand for example bitcoins. Non-Fungible Tokens (NFTS), another classification of digital assets, can be described as unique digital tokens that exist on blockchains, for example Ethereum. They were quite popular in 2021, can possess significant value and are used in the representation of artwork or some type of digital identity (Ehrlich, 2023). Even though NFTs have created opportunities for creators and collectors alike, they prove worrisome for law enforcement as they can facilitate money laundering and wash trading violations (Team C. , 2022). None the less there is a considerable number of NFTs and cryptocurrency in circulation in the world today including private coins (Li, et al., 2021) that are cryptocurrencies engineered to enhance transaction

anonymity and privacy of users. Collectively, they are subsets of digital assets and are all reliant on smart contracts which will be introduced next.

Smart contracts are self-executing contracts that enable parties to enter into agreements without the need for intermediaries or traditional legal frameworks, thus mitigating costs. They operate on the blockchain, enabling automatic execution of transactions once predefined conditions are met. They afford several benefits including enhancing trust and ensuring transparency through automated transactions that are irreversible and immutable (J. Gilcrest, 2018). Even though smart contracts offer numerous advantages, challenges persist (Nzuva, 2019) such as scalability issues and security vulnerabilities. In parallel, the secure storage and management of digital assets have become paramount, leading to the emergence of crypto wallets which serve as essential tools for individuals to securely store, manage and engage in transactions with their digital currencies as will be debated hereafter.

Wallets and Their Security Risks: Cryptocurrency wallets as latter suggest hold the same purpose as a conventional wallet. They are managed by private keys (Powell & Curry, 2023) and provide a secure gateway to digital asset it secures. Essentially, there two popular types of cryptocurrency wallets; hot wallets that requires the internet and cold wallets that does not. Although both wallets do afford certain benefits in the context transactional speed and basic security mechanism (not online no threat) respectively they both are not without certain security risk. Hot wallets by nature of their connectivity are more susceptible to hacking as reliance on third party security may pose a risk. Additionally, lost or damage to device hosting wallet can preclude access to funds. Cold wallets lack convenience as spending funds requires multiple steps that can deter traders, hardware devices can be costly and learning curve issues can be significant as setting up may require some technical knowledge and time to realize. Whether hot

or cold wallets the absence of regulatory framework and legislative backing managing these risks can prove detrimental to the ecosystem.

Regulatory Framework and Legal Considerations

Suggested as the greatest economic catastrophe in the world's history The Great Depression was a decade long economic contagion that originated in the United States in August 1929. It was attributed to several accumulating factors, namely, the stock market crash, banking failures, and the collapse of world trade. Consequently, in 1934 United States President Franklin D. Roosevelt established the United States Securities and Exchange Commission (SEC) under the Securities Exchange Act of 1934. It is argued that it is the first modern financial regulatory body with mandates that include enforcement of securities laws, regulatory oversight of stock exchanges and the protection of investors from fraud. Regulatory bodies and policy makers play a significant role within the cryptocurrency environment. Whilst decentralization embodies it, the presence of an effective regulatory oversight is crucial to ensure integrity, stability, and protection within the cryptocurrency business. Hence, it is essential to understand how regulatory frameworks and legal considerations are interconnected to cryptocurrency awareness.

In the Bahamas, the Digital Assets and Registration (**DARE**) act of 2024 is a prime example of how regulatory frameworks have evolved to accommodate the cryptocurrency landscape. Unlike some jurisdictions that attempt to retro fit laws to address concerns and challenges surrounding cryptocurrency. This nation took the initiative and enacted legislation specifically to regulate cryptocurrency and blockchain technology influence and adoption. The act operates within the limits of the Securities Commission of the Bahamas and boast of key features such as (Director, 2024): enhanced digital asset exchange requirements, robust custody framework, staking and stable coin regulations, investor and consumer protection measures, digital asset issuers and NFT

classification. On January 21st, 2025, the U.S Securities and Exchange Commission established the **SEC Crypto Task Force**. The Task Force's essential aim is to deliver clarity on the application of US Federal laws with respect to cryptocurrency (SEC Crypto Task Force to Host Four More Roundtables, 2025). Again, the nation of Singapore recognizes cryptocurrency as "digital payment token" and as such has incorporated it in its Payment Services Act (2019). Additionally, *the Virtual Assets and Related Activities Regulation of 2023* and *Law No. (4) of 2022* are legislations that govern Dubai's **Virtual Assets Regulatory Authority (VARA)**, the entity responsible for regulating and overseeing the provision, use, and exchange of virtual assets in and from United Arab Emirates. Moreover, **article (5) 2** and **(6) 9 of Law No. (4) of 2022** states "*Objectives of VARA...to increase awareness on investment in the Virtual Asset services and products sector and encourage innovation in this sector*" and "*Functions of VARA...educate Beneficiaries, and raise their awareness, on dealing and trading in Virtual Assets and the risks arising therefrom*" respectively. The legislation was also conscious of the significance to law enforcement as **article (21)** pronounces "*VARA employees nominated pursuant to a resolution of the Director General will have law enforcement capacity to record the acts committed in breach of the provisions of this Law...*". The specifics of these excerpts were clear as they are necessary to ensure protection and control within the digital landscape. Most important consideration was given to the aspect of awareness which is essential to adoption. Lastly, the **Markets in Crypto-Assets Regulation (MiCA)** (Hall, 2023) is a bonding legal framework crafted by the Europe Union and all its 27 member states to regulate cryptocurrencies and even though currently it doesn't provide for decentralize finance (DeFi) and non-fungible tokens (NFTs) (Gaur, 2021) the framework affords legal volume that can improve clarity for both law enforcement and the courts (Linden & Shirazi, 2023). In Trinidad and Tobago there is not any

specific legislation to directly address crimes evolving cryptocurrency. On the contrary, there were certain efforts made by way of the introduction of the ‘The Cybercrime Bill’ on March 21st, 2014, which at the time was intended to provide for the creation of offences related to cybercrime and other related matters. However, the bill lapsed even after several reintroductions in 2015 and 2017 respectively (Bills, 2020). Interestingly, Trinidad and Tobago Cyber Security Incident Response Team (TT-SCIRT) the entity tasked with securing the Nation’s cyber security infrastructure reported, during the period **2019-2025** there were **53** cyber security incidents that included extortion and ransomware where cryptocurrency was demanded (TT-SCIRT, personal communication, April 4, 2025). Chainalysis a blockchain data platform that provides data, services, and research to government agencies worldwide, suggested in its 2024 Crypto Crime Report. Crypto crime was worth an estimated \$24.2 billion (Team, 2024). The table below includes some infamous cases attributed to cryptocurrency crimes.

Table 1

High profile cryptocurrency crime convictions (2015-2024)

Note: Data compiled by author from public court records and news releases from the U.S. Department of Justice, BBC, CoinDesk, and other media sources (2015–2024).

Name	Year Of Crime	Year Of Conviction	Court Of Which Country	Role	Crime	Years
Ross Ulbricht	2013	2015	USA	Founder of Silk Road	Money laundering, computer hacking, narcotics trafficking	90
Sam Bankman-Fried	2019-2022	2024	USA	Founder of FTX	Fraud, conspiracy	25
Roger Thomas Clark	2013	2023	USA	Senior advisor to Silk Road	Narcotics trafficking	20
Karl Sebastian Greenwood	2014	2023	USA	Co-founder of OneCoin	Fraud	20
Mark Scott	2015	2024	USA	Lawyer for OneCoin	Money laundering	10

Michael Aaron Lord	2013-2015	2017	USA	Unlicensed money service operator	Operating an unlicensed money transmitting business	9
Randall Crater	2013	2022	USA	Founder of My Big Coin Pay	Wire fraud & operating an unlicensed money transmitting business	8
Ryan Salame	2019-2021	2024	USA	FTX Executive	Fraud	8
Stefan Qin	2017-2020	2021	USA	Virgil Capital	Securities fraud	8

TTPS's specialist units such as the Fraud Squad, Financial Investigation Unit (FIB) and the Cyber and Social Media Unit all indicated their interaction with investigations involving cryptocurrency however, each echoed similar sentiments in relation to hurdles due to legislative authority, tools, and training. Based on these revelations it is clear that there exist concerns as to TTPS's readiness when addressing cryptocurrency issues.

Law Enforcement and Cryptocurrency

To being, an interrogation of the TTPS's website (<https://www.ttps.gov.tt/>) suggested that media releases were achieved as far back as 2016 however, when executing a query on the term cryptocurrency awareness or cryptocurrency nothing relating was apparent. Similar checks were made on the "safety tips" section and results returned no information on the topic. Interestingly, compared to other stakeholders that can be associated with this space the results painted a different picture. The Trinidad and Security Exchange Commission's (TTSEC) website provided several articles about the topic that can assist in creating or building on awareness (Bachan, 2021), analogous information can be also found on the websites of the Central Bank as well as certain commercial banks such as First Citizens Bank (Mohammed, 2024). Data obtained from the Trinidad and Tobago Police Academy's Faculty of Advanced Law Enforcement Education

and Training presented a curriculum consisting of a range of general and specialised policing subject categories. However, as it relates to programs on cryptocurrency the Academy did not specifically offer any program (Simon Alexis, 2025) instead included courses that would touch on the topic as illustrated below.

Table 2
Excerpt of current Curriculum provided by the Police Academy (April 3rd, 2025)

Title:	Cyber Crime Investigations
Type of Training:	Course
Duration:	30 hours
Description:	Designed to equip participants with the necessary knowledge, skills, and attitude to be aware of vulnerabilities to cyber-attacks, detecting and investigating cybercrimes and securing technological assets. Participants are exposed to recent case studies on cyber-attacks for critical analysis, application of tools and techniques used to check vulnerabilities, and performance of a digital investigation. Additionally, the investigative process and legislative requirements of a country is discussed.
Modules:	Concepts of Cyber Security and Cyber Crimes Managing Cyber/Digital Incidents Cyber Crime Investigations Legislative Considerations
Objectives:	Learning Outcomes: At the end of this course, participants will be able to: a) Discuss concepts of cyber security and cyber crimes b) Identify cyber and digital incidents c) Explain the investigative process for cyber crimes d) Identify the legislative and other considerations for cybercrime investigations

Consequently, the Academy did signal its intention to target cryptocurrency awareness and investigation in the future for the subject matter to be a more substantial offering on its curriculum. The Fraud Squad, one of the TTPS's white collar units, provided that for period **2022 – 2024** there were **41** reports involving cryptocurrency where over **\$2.2 million TTD** was obtained by criminals through scams on social media platforms such as Metta. The reports were classified by the Fraud Squad using existing or combination of existing laws such as the **Larceny**

Act 11:12 and the *Computer Miss Use Act 2000*, others that did not meet the threshold under legislation were classified as either information or irregularities. More concerning was the absence of any charges or prosecutions and in some cases reports were either closed or filed. Evidence reveals that the ability to advance these cases proves difficult as the necessary tools were not available. Additionally, investigative training dedicated to the subject was scarce. Further data provided that for the mentioned period only 5 officers were specifically trained. In comparison to the Financial Intelligence Branch (FIB) another White Collar unit within the TTPS provided for the mentioned period only 3 reports associated with cryptocurrency that were linked to money laundering were recorded; no monetary figures were provided, and they remain inactive due to similar reasons echoed by Fraud Squad. The FIB produced a documented standard operating procedure (SOP) that provided guidance on the seizure, retention, and disposal of cryptocurrencies and other virtual assets. However, it was ineffective as there exist no laws to specifically treat cryptocurrency related crimes. TTPS's Cyber and Social Media Unit, a unit that provides technical support for other arms of the TTPS, stipulated that there was one cyber related incident they assisted with during **2019-2025**. The incident involved the compromise of a private key to a crypto wallet where millions of USDs were stolen. Further information suggested that the Unit also suffered from the lack of cryptocurrency investigative training and tools. Additionally, the Unit suggested the absence of legislative framework to cope with potential crimes within this environment is an added burden to the TTPS as suspected deviant behavior or criminal conduct is either reliant on existing laws or aligned to suit them (Balewah, 2025). Even more concerning is that the Crime and Problem Analysis Branch (CAPA), the TTPS's entity that is tasked primarily with data-processing and analysis information (Crime And Problem Analysis, n.d.) disclosed that there was no recorded data in relation to

cryptocurrency crimes. In continuing, whilst the use of present legislation to address crime within this environment is resourceful and commendable they should complement modern laws that provide specificities that speak to the vernacular of the cryptocurrency space as opposed to being their substitutes.

“...I am grateful to the U.S. Attorney’s Office for the Southern District of New York and the FBI for their outstanding work in bringing Mr. Bankman-Fried to justice.” This was the pronouncement of U.S. District Judge Lewis A. Kaplan during the sentencing of Samuel Bankman-Fried on March 28th, 2024, at the Southern District of New York Court (Justice, 2024). Bankman-Fried founder and chief executive officer of FTX, an international cryptocurrency exchange, was sentenced to a 25-year prison term and ordered to pay \$11 billion (about \$34 per person in the US) in forfeitures. The success of this investigation was not brought about by a conservative policing approach but rather a contemporary one. This research revealed that technical competencies and resources were items lacking in the toolbox of TTPS in coping with issues associated with cryptocurrency and by nature of their profession successful outcomes of their responsibilities would be reliant on them. A Cryptocurrency investigation would require several steps. Firstly, investigators should understand what types of crimes are being investigated, such as investment fraud, ransomware attacks, malware attacks, or phishing scams. Additionally, once classified the requisite tools or resources can be applied to progress an investigation. For example, Chainalysis is a popular blockchain data platform that provides data, services, and research to government agencies worldwide (Willmer & Voreacos, 2023). The platform tracks and analyses cryptocurrency transactions on the blockchain, connecting them to real-world entities and events. Techniques such as Asset Tracing Methodologies that apply the *Proceeds-In-First-Out* (PIFO) principle which enables investigators to determine when illicit

funds are entered into wallets can be useful. Other key strategies in the process included Asset Freezing (QC & Maguire, 2020), Asset Confiscation (Balthazor, 2019) and Asset Disposal (Christiansen & Jarrett, Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset, 2019). During this study, the commonality discovered in these cases was interagency collaboration as efficient cryptocurrency investigation is reliant mostly on cooperation between various bodies. No data provided by any of TTPS's agencies studied within this research reveals that there was meaningful collaboration among bodies. Best practices dictate law enforcement build technical expertise, foster cooperation across borders and deploy advanced investigative tools (COPOLAD, 2025) again none other these recommendations were obvious when scrutinizing the TTPS's capacity to realize cryptocurrency related incident. Standardization of this process should be a priority to the TTPS as it would ensure consistency across units, support training and professional development, facilitate Inter-Agency Cooperation (locally/internationally) and it is vital for emerging crime types. Moreover, as crimes involving digital assets such as cryptocurrency are becoming increasingly sophisticated, a uniform investigative approach is critical to the TTPS in ensuring the organization remains contemporary in its efforts to uphold its mandate.

People and Actors in the Ecosystem

Throughout history, people have always taken risks in pursuit of discovery. After all this behavior provided the realization, the world was not round (through trial and error of course). This natural inclination to push boundaries is why, as of authoring this review, the cryptocurrency industry is worth \$2.63 trillion USD (Cryptocurrency Prices Today By Market Cap, n.d.).

The cryptocurrency ecosystem in the perception of some has generated numerous exciting possibilities. However, it is people and other actors that are comprised of miners, investors, developers, and traders who form the heart of the ecosystem, driving its growth, innovation, and adoption.

Who are miners and how do they intersect in the cryptocurrency landscape? To illustrate, a miner is the intransitive verb of the word mine which according to Merriam Webster includes an excavation in the earth where mineral substances are extracted, for example gold. It is a tedious process, however, and can be quite rewarding. Theoretically, within the cryptocurrency space, the endeavors of miners are typically the same. In their efforts to acquire new cryptocurrencies (mining) and validate transactions, miners dedicate their computational power and resources to solving complex mathematical puzzles (Drescher, 2017). Once successful new cryptocurrencies (Narayana, 2016) are created and added to the blockchain as a new block of data along with validated transactions.

Investors are individuals or entities who provide capital and liquidity to the market with the expectation of reaping some rewarding return on initial investments. They can be classified as either **retail** or **institutional investors**. The first are typically people using their personal finances to engage in buying, holding, or trading digital assets such as Bitcoin, Ethereum, or non-fungible tokens (NFTs). Retail investors are normally motivated by market sentiments, diversification, or an interest in emerging technologies. The latter, however, are cooperative and associated with magnanimous contributions in relation to market investment. Retail investors are known to influence market trends through strategic investments in cryptocurrency projects, blockchain startups, and decentralized finance platforms. Overall, given their economic significance, these parties may be considered key stakeholders within this digital sphere. They

contribute significantly towards stimulating innovation, driving adoption, and providing liquidity to cryptocurrency markets. Their financial participation is necessary as it fosters blockchain development, funds new protocols, and underpins token economies. Their decisions can influence token valuations, project credibility, and add to market dynamics. Hence maintaining investor confidence through effective regulatory oversight cannot be overstated as law enforcement agencies, such as the TTPS, must contribute proactively to this environment by investigating fraud, tracing illicit activity, and contributing to public education and investor protection efforts.

Next, the developers are notably considered the architectural engineers at the center of blockchain technology that powers cryptocurrencies. Whether individual driven or team centered, developers are instrumental in designing, building, and maintaining the software infrastructure that are central in digital currencies, decentralized applications (dApps), smart contracts, and blockchain protocols. The role of developers can vary within the cryptocurrency environment and can be categorized as follows: **Core developers** (contribute to the foundational code of blockchain networks), **Application developers** (build decentralized finance (DeFi) platforms) and **Smart contract developers** (write and audit the code that governs automated, self-executing agreements). Innovation and technological advancement are both symptomatic of crypto space and for this reason the role of developers is vital. Their involvement creates a conduit for faster transactions, stronger cryptographic protection, improved user experience, and even interoperability between different blockchain systems. Additionally, developers can act as a catalyst in influencing governance mechanisms in decentralized communities. In the end, one can appreciate the role of developers in this topic.

Finally, traders facilitate the buying and selling of cryptocurrencies which drives market liquidity. Contrary to long-term investors, traders prefer a short-term strategy geared towards profit from market volatility and liquidity opportunities. Even though people play a key role in the cryptocurrency landscape, they are not insulated from exploits or bad actors bent on deviant behavior. The proliferation of cryptocurrencies has not only created a habitat of creativity and innovation but also conditions that exploit technological loopholes and human psychology. Some notable abuses that are synonymous with bad actors are Initial Coin Offering (ICO) scams and rug pulls, both of which blend technical deception with sophisticated social engineering tactics to defraud unsuspecting investors. ICO scams such as '*pumps and dump*' (Li, Shin, & Wang, 2021) involves the artificial inflation of a cryptocurrency by a bad actor through fabricated positive statements about the expected future values. This causes a surge in investments (the pump). Subsequently, the actor then sells off the assets, locking profits. To salvage their investments victims are subject to a fire sale (the dump) situation upon realization of the scheme (Corbet, The danger of cryptocurrency pump-and-dumps: Analysing the development of research & regulation, 2021). A rug-pull on the other hand occurs when a crypto project developer suddenly abandons the project and vanishes taking with them all capital that was invested by unsuspecting victims (Garnett & Ashburn, 2024). Nonetheless, these schemes can be facilitated using social media and other avenues as they can impact the behavior of people. Online communities and social media platforms can also influence public perception, drive market sentiment, and facilitate mass adoption within the crypto space. However, it can also operate as the proverbial '*double edged sword*' as negative perception and unscrupulous behavior towards cryptocurrencies can be induced by it (Corbet, 2021).

Synthesis and Implications for TTPS

In this research, it was revealed that while there is a general recognition of the growing significance of cryptocurrency in criminal activity, TTPS lacks the institutional preparedness to effectively respond. Survey results attested that most officers across various management levels possess only limited to moderate competence of blockchain technology, cryptocurrency wallets, decentralized platforms, and the legal classification of virtual assets. The absence of standardized operating procedures (SOPs), specialized training, and technical investigative tools presents a significant obstacle to effective intervention. Findings also suggested that there was uncertainty about the proper procedures in reporting and classifying cryptocurrency matters. Additionally, a lack of interagency coordination and limited exposure to live cases involving cryptocurrency was also obvious. Despite serious cyber incidents and criminal activity associated with cryptocurrencies, the TTPS has not yet fully integrated cryptocurrency considerations into its investigative strategies or crime prevention frameworks. When reviewing the potential implications this subject can have on the TTPS, several outcomes can be rationalized. However, the following will be discussed: Training and Capacity Building, Policy Development and SOPs, Specialized Units or Focal Points, Inter-agency and International Cooperation and Public Engagement and Investor Protection.

Training and Capacity Building: TTPS must adopt a stance that prioritizes a structured training programme in cryptocurrency fundamentals, blockchain analysis, and digital asset investigations that is continuous. Special emphasis should be given particularly to officers within the Fraud Squad, Cyber and Social Media Unit, and the Financial Investigations Branch. These personnel should be equipped with forensics tools such as Chainalysis and afford the technical knowledge and practical skills in using them. Training should also be extended to legal officers and prosecutors, to ensure proper case presentation and prosecution of crypto-enabled crimes.

Policy Development and SOPs: There is an urgent need to develop formal SOPs and internal policy documents governing the classification, investigation, seizure, and reporting of cryptocurrency-related offenses. Even though one section within TTPS generated an SOP, it is faced with challenges due to lack of legislative support.

Specialized Units or Focal Points: Given the complexity of cryptocurrency crimes, the TTPS should establish a dedicated crypto investigations team or appoint cryptocurrency liaison officers within high-priority divisions or sections. Based on their capacity they can serve as internal subject matter experts and lead coordinated responses to incidents involving digital assets.

Inter-agency and International Cooperation: the effective response to crypto crimes is reliant on active collaboration between the TTPS international and national agencies such as the Financial Intelligence Unit (FIU), Trinidad and Tobago Securities and Exchange Commission (TTSEC), and TT-SCIRT.

Public Engagement and Investor Protection: The TTPS in its mandate must incorporate an aggressive approach in public education, issuing alerts and advisories on emerging scams and best practices for cryptocurrency safety. Collaborating with regulators and civil society to develop preventative awareness campaigns will empower citizens to recognize and avoid fraudulent schemes. The mentioned areas, once operationalized, can be helpful to TTPS in addressing cryptocurrency concerns. However, failure to target these gaps may result in increased victimization of the public, loss of confidence in law enforcement, and greater difficulty in prosecuting financially motivated cybercrimes.

Nonetheless, the outlook looks favorable for the TTPS as potential benefits can be realized through further research in areas such as *measuring the effectiveness of crypto training in law*

enforcement, public perception and victimology in crypto scam and legal framework assessment in Trinidad and Tobago.

In conclusion, the reviewed literature explained that cryptocurrency is not a novel technology but rather an evolving one. It provided the potential of this technology and articulated how it has transformed societies and economies globally through realization, awareness, and adoption of it. The research also reveals that there can be a dark side to this technology. This exploitation is brought about by the endeavors of individuals who seek to maximize the vulnerabilities of people within the ecosystem who may have been fed a diet of fallacies or suffer from confirmation biases brought about by cognitive overload, knowledge gaps or financial incentives. Albeit several jurisdictions internationally and even regionally have adopted a proactive attitude towards cryptocurrency by implementation of legislation, awareness strategies and institutional steps. The studied material still found that in developing countries such as Trinidad and Tobago its premier law enforcement body the TTPS is positioned in a bog in relation to awareness. The relevance of this gap is crucial as studies that can assess officers' readiness to address crimes or general awareness within the cryptocurrency ecosystem are unfounded. Sincere efforts should be made by the TTPS to raise the level of awareness as the research show that entities as the TTSEC, FIUTT, Central Bank of Trinidad and Tobago and TTCSIRT has taken steps to provide relevant information to create or enhance awareness and build capacity within the area of study. However, without any direct interdictory powers alleviating issues would pose a challenge. The findings unearthed in this review further reiterate the relevance and timeliness of this research as the TTPS being the focal point of this study should place more effort in how they view cryptocurrency within the crime triad. It is anticipated that this investigation will rectify the knowledge gaps that exist within the organization and be

the catalyst for change through calculated and informed recommendations. Ultimately, this review justifies the need for an empirical assessment and policy development to enhance TTPS's preparedness for cryptocurrency-related challenges.

Chapter 4

Survey, Interviews and Analysis

The Tobago Police Service (TTPS) comprises several managerial positions that further comprise a ranking system. The specific performance requirements attached to each rank will be an indicator as to whether they lie within the top, middle, and lower management levels of the organization. In this chapter, the results of a survey conducted to evaluate the level of cryptocurrency awareness and preparedness among officers of various managerial levels within the TTPS will be presented. Also, interviews with key personnel within TTPS will be discussed along with data collected from other relevant institutions.

The Survey: The question of how well TTPS understands cryptocurrency technologies and the extent to which the organization is institutionally prepared to respond to arising challenges provided valuable guidance on the results that were achieved on the completion of this survey. The three managements levels Top, Middle, and Lower were the participants represented in this questionnaire which was administered electronically. Assessments of participants focused on several key competencies such as knowledge, perceptions, and engagement with various dimensions of cryptocurrency, technical concepts (e.g., blockchain, smart contracts), market understanding (e.g., price volatility, trading volume), regulatory awareness, and security practices. Responses were rated using standardized Likert scale to measure levels of understanding (from 1: Low to 5: High) and frequency of behavior or engagement (from 1: Never to 5: Always). The results are presented thematically across five major areas: Demographic Profile of Respondents, Awareness of Cryptocurrency Concepts, Understanding of Blockchain Technology and Functionality, Security Practices and Risk Perception and Regulatory Awareness and Engagement. The sections allude to descriptive statistics, frequency

distributions, and comments on factors that may relate to trends, gaps, and areas of concern among TTPS personnel. The chapter concludes with a summary of the key findings. 95 officers took part in the survey.

Demographic Profile of Respondents: 95 officers within the TTPS access and completed the survey. The participants represent a cross-section of the organization's management tiers and age demographics, setting a rational stage for assessing the level of awareness and preparedness regarding cryptocurrency.

Age Distribution: The respondents between the ages **45–54** years dominated the exercise, comprising most of the sample. **The 35–44** age group followed next, resulting in a smaller number of respondents falling outside these categories. Based on the age profile, it is plausible that most participants are in their mid to late career stages, and this may influence their exposure to or interest in emerging digital technologies.

Management Level Distribution: Participants represented all three management tiers within the TTPS

- Middle Management accounted for the largest group, particularly in the 45–54 age range, with 47 respondents.
- Lower Management followed with 14 respondents in the 45–54 category and 7 in the 35–44 group.
- Top Management contributed 8 respondents, all within the 45–54 range.

This demographic mix ensures a balanced view of operational, tactical, and strategic perspectives regarding the Service's cryptocurrency readiness.

Table 3: Age and Management Level Distribution

Age Group	Top Management	Middle Management	Lower Management
35–44	–	9	7
45–54	8	47	14

The table shows that middle management personnel, who are often responsible for executing policies and leading operational teams, are the most represented group in this survey. Their views, therefore, are particularly important for understanding TTPS's capacity to adapt to cryptocurrency-related challenges on the ground. However, it must be noted that lower management displayed slightly higher awareness levels than their counterparts with an average score of **2.08** compared to **1.89** and **1.60**, respectively.

Awareness of Cryptocurrency Concepts

The above caption analyzes TTPS respondents' understanding of key cryptocurrency market concepts, namely market capitalization, trading volume, price volatility, and sentiment analysis. These concepts are vital for recognizing unusual market behavior that may signal fraud, money laundering, or other criminal activity involving digital assets.

Market Capitalization: When asked about their understanding of market capitalization; the total value of a cryptocurrency's circulating supply, **34%** of respondents rated their understanding as low and **25%** as limited. Only **16%** reported good or high comprehension (ratings 4 or 5), suggesting that the majority are unfamiliar with this core metric used to assess asset significance in financial investigations.

Trading Volume: Trading volume awareness, that intimates the liquidity and activity level of a cryptocurrency, showed a similar trend: **38%** reported low understanding and **23%** indicated limited awareness. While **16%** had good or high understanding, this leaves a substantial portion

of officers without a working knowledge of how trading activity could indicate criminal behavior or market manipulation.

Price Volatility: Price volatility; a key feature of cryptocurrency that affects risk and criminal exploitability was understood at a low level by **42%** of respondents, with another **18%** rating their familiarity as limited. Only **18%** claimed a good or high level of understanding. This result is critical, as price swings are often used in pump-and-dump schemes or other investment frauds.

Market Sentiment Analysis: Interestingly, a considerable number of officers (55%) indicated low confidence in interpreting market sentiment, with an additional **19%** reporting limited capability. This simply suggests that nearly **three-quarters** of the sample are not equipped to recognize social or media-driven market manipulation, an increasingly common tactic used in cryptocurrency scams.

Understanding of Blockchain Technology and Functionality

This caption assesses respondents' familiarity with key technical components of blockchain systems. Namely: consensus mechanisms, decentralization, immutability, and smart contract elements critical to detecting, understanding, and disrupting illicit uses of blockchain technology.

Consensus Mechanisms: More than half **56%** of respondents rated their understanding of consensus mechanisms as low, while an additional **16%** selected limited. Only **13%** rated themselves as having good or high comprehension. This indicates a widespread unfamiliarity with the very systems that validate transactions, an essential feature for understanding how blockchain network functions and can be exploited.

Decentralization: A combined **67%** of respondents expressed *low* or *limited* familiarity with decentralization. Decentralization is a core feature of blockchain that limits control and

jurisdictional oversight. This lack of understanding could hinder strategic responses to crimes committed on distributed networks.

Immutability of Blockchain Ledgers: Knowledge about immutability, the inability to alter recorded data once validated—was the lowest among all indicators in this section. Over **59%** of officers selected *low*, and another **17%** chose *limited*. This is especially important as immutability underpins the evidentiary integrity of blockchain records, which is relevant in prosecution and asset recovery.

Smart Contracts: A total of **61%** of participants reported *a low* understanding of smart contracts, with another **17%** indicating *limited* familiarity. Smart contracts are used in various schemes, including decentralized finance (DeFi) frauds and automated money laundering. Only **8%** of respondents claimed good or high understanding, pointing to an urgent need for knowledge enhancement in this area.

Security Practices and Risk Perception

This section evaluates the TTPS respondents' awareness of essential security practices associated with cryptocurrency use. Indicators that were assessed included secure storage, private key management, risk awareness, and wallet backup procedures as these competencies are crucial for officers tasked with handling digital evidence, conducting cyber investigations, or safeguarding institutional digital assets.

Secure Storage Solutions: Questioned about selecting and using secure storage options (such as hardware wallets or secure exchanges), **59%** of respondents rated their awareness as *low*, and an additional **14%** as *limited*. Only **14%** reported *good* or *high* familiarity, suggesting that most

officers lack the basic knowledge needed to secure or interpret the safekeeping of seized digital assets.

Private Key Management: Similarly, **58%** of officers indicated *a low* understanding of private key security practices, and **15%** reported limited awareness. Private keys are central to controlling access to cryptocurrency wallets. With only **10%** of respondents indicating *good* or *high* understanding, the TTPS may face serious challenges in evidence handling and cyber asset security.

Security Risks in Crypto Transactions: While still low overall, this category reflected slightly better awareness: **42%** reported *a low* understanding, and **19%** reported *limited*. Around **20%** of respondents claimed *good* or *high* knowledge, showing some emerging awareness of vulnerabilities associated with cryptocurrency storage and transfers.

Wallet Backup and Recovery Procedures: **54%** of respondents reported *low* familiarity with how to back up wallets and recover lost funds, and another **18%** selected *limited*. Only **17%** had *a good* or *high* understanding of an issue that could compromise investigations involving wallet access or forensic recovery efforts.

Regulatory Awareness and Engagement

Within this segment, the level of awareness and involvement of TTPS respondents in regulatory matters related to cryptocurrency was evaluated. This is necessary because law enforcement must understand their importance as they require legal frameworks and collaboration with other agencies to be effective within this space.

Awareness of Regulatory Requirements: A significant **55%** of respondents rated their understanding of local cryptocurrency regulations as *low*, with another **16%** selecting

rarely/limited. Only **10%** reported *good* or *high* awareness. This indicates that more than two-thirds of officers lack sufficient familiarity with existing legal requirements given the legal sensitivity of cryptocurrency investigations.

Understanding of Regulatory Impact: Quizzed about the impact of regulatory changes on cryptocurrency activity, **53%** indicated *low* understanding, and **19%** selected *limited*. A small fraction (**13%**) rated their knowledge as *good* or *high*, underscoring a widespread unawareness of how legal shifts could affect investigations, asset seizure, or prosecutorial strategy.

Knowledge of Global Regulatory Differences: A total of **61%** of officers did not understand how regulatory approaches vary between jurisdictions, while **15%** selected *limited*. Just **8%** indicated *good* or *high* understanding. Given the international nature of cryptocurrency crime, this knowledge gap weakens TTPS's ability to work with cross-border partners or respond to transnational threats.

Engagement with Stakeholders: This subtitle recorded the lowest scores: **69%** of officers reported *never* engaging with regulatory authorities or industry stakeholders, while another **14%** said they *rarely* do. Only **5%** said they *often* or *always* participate in such discussions, highlighting a major disconnect between frontline law enforcement and key regulatory entities.

The Interviews: TTPS consists of several departments that vary in their functions within the organization's scope. However, based on this investigation four (4) were chosen on the following rationale: **Financial Investigations Branch (FIB)**, responsibility in financial crime investigation and its pivotal role in tracing illicit financial flows that may involve digital assets, **Police Academy**, to assess the current training curriculum and identify gaps in cryptocurrency awareness within TTPS officer development, **Cyber and Social Media Unit**, for its operational

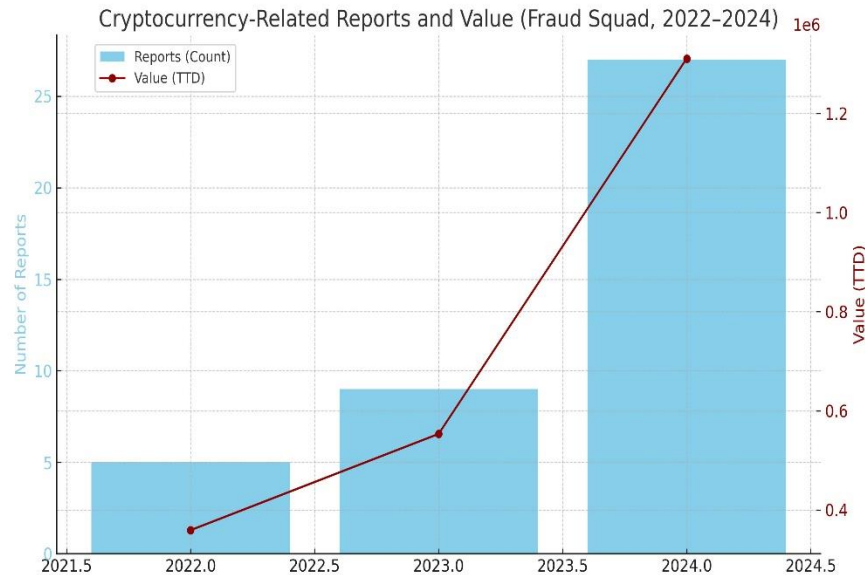
relevance providing support in cyber related crimes with the digital landscape and the **Fraud Squad** due to its mandate to investigate fraud, scams and financial deception areas increasingly exploited through cryptocurrency.

Senior Superintendent of the FIB on whether the technical and human resources presently available to the FIB are sufficient to conduct in-depth cryptocurrency investigation. *“No, I would say at this time no —additional training is needed for the human resource requirement and the technical requirement because we don't have the software (Chainalysis)....”* Additionally, it was revealed that there was no collaboration between the FIB and internal or external agencies in relation to cryptocurrency investigations and the lack of regulatory framework in relation to cryptocurrency was also a concern of the department’s head. He agreed that a specialized unit would be beneficial in addressing cryptocurrency reports. Recommendations were centered around the need for training and specific investigative tools such as the Chainalysis software. In closing, the head of the branch opined that law enforcement must be *“in tune”* in relation to the new and emerging trends surrounding digital currencies. During an interview with the provost of the Police Academy, it was shared that the academy did not have any formal initiatives or discussions about incorporating cryptocurrency related topics in officer training. Conversely, when asked whether such training is important to all levels within TTPS the provost stated *“It is very important that police officers be at least sensitize on the aspect of cryptocurrency. We believe that at the trainee level, sensitization is also important, but specific training should be given to the units or sections that are dealing with what we consider to be financial crimes.”* In relation to existing training gaps on officer’s preparedness to handle cryptocurrency crimes, the provost was monosyllabic in the affirmative. Data suggested some partnerships with internal and external stakeholders regarding training, but none covered specific programs addressing

cryptocurrency and connecting issues. When asked about recommendations concerning the growing use of cryptocurrency and criminality, similar sentiments were expressed about the need for specialized training. Additionally, it was explained during an interview with the officer in charge of the Cyber and Social Media Unit that awareness was present when interrogated about his unit's technical capacity with respect to cryptocurrency technology. However, he remarked "... *but the training to actually perform that type of investigation we lack.*" It was revealed that officers of the unit had introductory training on the mechanism surrounding how cryptocurrencies are traced but these instances of training "*were far and few*" as they were reliant on the sponsorship of external stakeholders. In terms of investigation, it was reported that there was only one investigation within the last five years that the unit had an active involvement but due to the lack of legislation that specially addressed crimes within the ecosystem the investigation lapsed. There were no SOPs or internal guidelines on how the unit handles cases involving cryptocurrency and recommendations by the unit's head repeated those of previous interviewees. "*It comes right back to training and tools. You provide the training and the tools; we can do the work*" Inspector Cyber and Social Media Unit. Interviews culminated with a designation from the Fraud Squad. Data suggested that this section of the TTPS was the most active in relation to crime associated with cryptocurrency, as illustrated below

Chart 1: Reports involving cryptocurrency 2022-2024

Data provided by TTPS's Fraud Squad



During the period **2022 to 2023**, it was observed that reports increased from **5 to 9**, which represented a **60%** increase. The value of reported losses rose by **54%**, from **\$359,390.00 TTD to \$553,485.00**

TTD. Subsequent period **2023 to 2024** reports rose from **9 to 27**, representing a **200%** increase in figures. Further analysis was indicative of financial losses more than doubling to the sum of **\$1,310,491.55 TTD**, an increase of **137%**. Across the three-year period, over **\$2.2 million TTD** in cryptocurrency-related losses were reported to the Fraud Squad. More concerning, no prosecutions were apparent to date despite this significant increase in both volume and monetary value. This obvious trend not only signals the expanded use of cryptocurrency in criminal activity but also exposes critical gaps in investigative capability, legal readiness, and inter-agency collaboration. Additionally, the designate provided that the most common fraud scheme that involve digital currency was investment types, Inspector Fraud Squad “*what is happening is that fraudsters are using persons lack of knowledge about cryptocurrency and telling persons—well we can if you should invest in cryptocurrency and what they do is they generally take the person’s money and then that’s it they don’t hear anything about—from the person again*”. Ironically, the description offered in this scheme suffers from similarities that were earlier discussed in the study associated with ICO scams. It was also revealed that equally to the other

respondents interviewed, the Fraud Squad in the opinion of the Inspector has “*limited capacity*” to investigate crime synonymous with cryptocurrency. Remarkably, recommendations by the designate not only included legislation, tools, and training but training and sensitization should be extended to non-specialist officers within the TPPS as they would be the primary contact for victims before such cases are referred to specialist sections.

Reports: Several entities responded to questions submitted to help with the progression of this study, and an analysis of these reports will be discussed later. TTSCIRT asserted cryptocurrency is predominately demanded in instances of ransomware and in some instances of extortion via phishing as illustrated below.

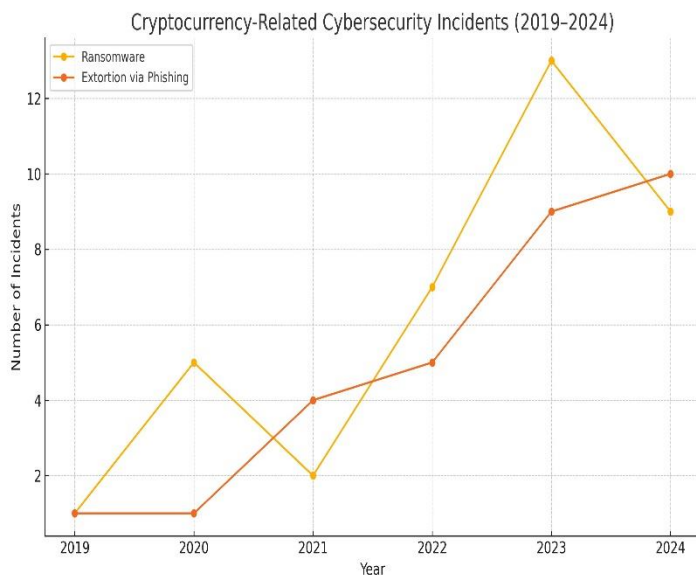


Chart 2: cryptocurrency related incidents 2019-2024

Data provided by TTCSIRT

In Ransomware's case, 37 incidents were recorded that saw 14 Public sector and 23 Private sector entities affected. Notable increases included in 2020 a **200%** rise from **1** to **3** incidents and 2023 a **117%** increase from 2022 (**7** to **13** cases). There was a slight decline

observed in 2024 (from **13** to **9** cases, **-31%**). Extortion via Phishing totaled **30** incidents for the period under review. This saw **13** Public and **17** private sector entities affected. Significant growth was observed in 2021 with a **300%** increase from 1 to 4 cases and a further rise of **66%** in 2022 from **4** to **7** cases. However, for the 2023–2024 period there was some stabilization with **9** and **10** cases respectively, a modest **1%** increase. Sectoral impact showed the following were mostly affected: government, public health, manufacturing, retail, and logistics. CAPA, TPPS’s

data repository, was asked to report on the number of reported cryptocurrency-related crimes within the last 3 to 5 years and interestingly they replied that there were no reports. Lastly, significant data was submitted by the TTSEC that identified several revelations. First, there were **10** Fintech service providers in Trinidad and Tobago offering the following: *buying and selling cryptocurrency on behalf of clients, trading in forex and cryptocurrency on behalf of clients, managing investment portfolios backed by cryptocurrency on behalf of clients and pooling client investments for the purchase of cryptocurrency* despite there exist no laws or regulations approving the operation of cryptocurrency or digital asset business. During the period **2022-2024** TTSEC recorded **75** complaints involving cryptocurrency. The first year saw **18** complaints. This figure declined in the second to **15**, suggesting a **17%** decrease from the previous year. However, in the third the number of complaints almost tripled to **42**, marking a significant **180%** increase compared to the previous year. Further data suggested that some of these complaints involved “*prohibited schemes*” where no infractions were detected, but investigations are ongoing by TTSEC. The TTSEC has not hosted any public education or outreach programs on cryptocurrency risk awareness. However, there have been joint statements and panel discussions with various stakeholders excluding TTPS. On commenting on challenges and strategic outlook, the TTSEC position was the absence of a national mandate to govern actors within the ecosystem as this has affected the interest in developing legislative frameworks. Nonetheless, TTSEC asserts that the Virtual Assets (VAs) and Virtual Assets Services Providers (VASPs) Bill has been drafted. Additionally, there has been an undertaking of a national risk assessment of VAs and VASPs, that will be coordinated through the Office of the Attorney General and the Ministry of Legal Affairs to assess the money laundering and terrorist financing risks associated with VAs and VASPs.

Summary of findings

To begin, the evaluation of results realized in the survey was evident that there exists a general lack of awareness within the TTPS within key areas of the cryptocurrency ecosystem, namely, cryptocurrency operations, market fundamentals, blockchain technology, security practices, and regulatory frameworks. This collective deficiency places the organization at a strategic disadvantage in responding to digital financial crimes. Interviews reveal that certain specialist sections within the TTPS, for example, FIB, Fraud Squad, and the Cyber and Social Media task with investigating or assisting in reports involving cryptocurrency suffered from the absence of the requisite tools and training to progress investigations. Inadequate training was also an area of concern as introductory courses within this specific field did not provide many benefits to TTPS personnel. This was further compounded by fact that the TTPS's Police Academy a key internal stakeholder as it relates to training and development of all police officers did not specifically offer any training programs on cryptocurrency awareness or investigation. Additionally, there exist gaps when considering collaboration among the TTPS's department studied within this research as no evidence was adduced to prove otherwise. Communication in some instances was a grey area for example CAPA, the repository for statistics within TTPS, had no data on reports cryptocurrency related irrespective of data shared by the Fraud Squad, FIB and Cyber and Social Media Unit (to a lesser extent). Significant monetary losses have occurred to people who are victims of criminality perpetrated in the cryptocurrency landscape. This unfortunate situation is further exacerbated given the fact that there have never been any (at the time of this study) indictments against responsible parties. Most notably, legislation addressing criminal conduct or regulated cryptocurrency is nonexistent, and these sentiments were expressed by key subjects who participated in the research. More concerning for the TTPS's is the growing use of

cryptocurrency in deviant behavior within society as reported by TTCSIRT and TTSEC. Lastly, it was conspicuous that the TTPS, regardless of the current situation, has not bothered to engage in any campaign or other method to enhance public awareness and perception towards cryptocurrencies and associated issues that may surround them. These findings are clear indicators that there must be some intervention by TTPS to modify its attitude towards cryptocurrencies issues.

Chapter 5

Discussions

The findings discovered in this study provides that cryptocurrency awareness within the Trinidad and Tobago Police Service (TTPS) is not well defined. To begin, there was a significantly low moderate level of awareness towards cryptocurrency among the various management levels of the TTPS. In fact, based on the data analyzed there was a clear stratification of awareness, where Lower Management consistently reported higher familiarity with cryptocurrency concepts than their Middle and Top Management counterparts. This reality can be associated with **Rogers' Diffusion of Innovation Theory** (Lundblad, 2003) that describes the route of a new idea through stages of adoption by different people who participate in or begin using it. The theory does have some challenges linked to it such as assumptions about innovation, the role of individual characteristics, and possible negative impacts. Nonetheless, this trend is a point of concern given the strategic responsibilities and roles of top management as indicated by (Walsh & Vito, 2018). Their limited understanding could hinder decision-making related to digital crime prioritization, policy development, and resource allocation. Notwithstanding, it can be deduced that lower management's higher awareness may reflect more exposure to operational realities and informal learning; However, without institutional empowerment, this knowledge may remain underutilized.

The Police Academy did not offer any specific training on cryptocurrency awareness or investigations. This situation is curious and not in keeping with contemporary policing illustrated in the case of the South Dakota's Police Academy that added an extra ethics session within their module as a result of publicity (Hult, 2024) or as identified in a research report (Harkin & Whelan, 2021) where it is quoted "*a police officer who goes through the academy now gets a*

pretty decent introduction to cyber-crime". It was also intimated that specialized training units were reliant on external agencies as they may become available. This can have certain implications; hence it is necessary for the Police Academy to formulate conditions for training and retraining towards building capacity and sustaining relevancy in this ecosystem.

Next, the moderate level of cryptocurrency awareness and obvious deficiency in investigative capacity discovered across various specialized units within the TTPS was bothersome. During interviews it was disclosed that while some officers possess a general understanding of digital currencies, they lack both specialized training and investigative tools such as blockchain analytics software (e.g., Chainalysis) necessary to effectively trace illicit cryptocurrency transactions. This lends credence to an article published by the Canadian Financial Crime Academy titled "*The Role of Technology in Combating Financial Crime in Canada*" which emphasized the critical role of technological to law enforcement (Academy, 2024). Ironically, TTPS's situation echoes global trends observed in law enforcement. As noted by (Gundur, Levi, Topalli, & Ouellet, 2021) where it was suggested that police agencies worldwide are grappling with the complexity and speed of cryptocurrency adoption by criminals, particularly in money laundering and scam operations. However, the lack of tools should not be limited to the scope of software. Legislations and or regulations are other vital instruments in addressing cryptocurrency related issues in Trinidad and Tobago have not been established. Countries such as the USA, United Arab Emirates, Singapore, and neighboring Bahamas have all utilizes legislations to combat against cryptocurrency issues. According to an excerpt from article in the Denver Journal of International Law & Policy (Duchow, 2025) "*With standardized regulations and international agreements, authorities could more effectively combat financial crime and prevent illicit actors from exploiting loopholes in the financial system by using crypto*" is some justification of the

importance of legislation of cryptocurrency. Nonetheless, the unavailability of present legislation does not fall square on the TTPS's breast plate, and this is a rational assumption. However, some scintillas of responsibility should be attributed to it as the organization can stimulate new laws through feedback to legislators about what laws are working and what gaps exist.

Additionally, the idea that there were no prosecutions in relation to crime associated with cryptocurrency despite the data submitted by the TTPS's Fraud Squad and other respondents in the study was not reassuring. Globally, there exists immutable evidence where perpetrators within the cryptocurrency realm have been successfully prosecuted for criminal conduct. More interestingly, some of these cases were not reliant on specific cryptocurrency laws but rather robust existing ones or established frameworks. For example, United States of America and Canada where tax evasion on digital assets such as cryptocurrency is an offence subjected to penalties (Thompson, 2024). This reality can invite unhealthy implications to the TTPS when considering public trust and confidence — as it may lead to perceived ineptitude or police misconduct (Owen-Evans & Low, 2024).

Lastly, the attitude adopted by the TTPS in omitting any sort of public awareness campaign on realities faced by cryptocurrency or digital assets on whole within its operations can be debated at length. Internationally, in 2022 the US Secret Service launched a cryptocurrency public awareness hub (Relations, 2022) to provide awareness and information on digital asset security to the public. Law enforcement bodies in Canada (Charbonneau, 2024) and several Latin American (internacional, 2022) counties have also adopted this approached towards their citizenry. After all, even though the adage "*prevention is better than a cure*" is still applicable to the implications associated with this relatively modern technology.

To surmise the key findings discussed in this segment suggest there are some concerns as it relates to **Stratified Awareness by Rank** (Lower management shows higher cryptocurrency awareness than middle and upper management, possibly due to operational exposure), **Lack of Formal Training Infrastructure** (The Police Academy currently does not provide cryptocurrency-related training, contrary to global trends), **Inadequate Investigative Capacity** (There is a deficiency in investigative tools and expertise e.g., no access to Chainalysis software) and **Limited Strategic and Regulatory Engagement** (The TTPS lacks internal policies, legislative feedback loops, and proactive public awareness campaigns).

While this study offers valuable insights into cryptocurrency awareness within the TTPS, certain limitations must be acknowledged. Firstly, the sample size and composition—focusing on select units—may not fully represent the entire TTPS. Secondly, self-reported awareness can be subject to response bias, where participants overestimate or underestimate their competence.

Additionally, the use of interviews with senior officers may have limited openness due to institutional culture or fear of critique. Finally, the study did not account for external systemic factors such as political or economic constraints that may influence institutions. The TTPS is at a pivotal point where increasing exposure to cryptocurrency threats demands a coordinated, informed, and proactive institutional response. The study confirms that without structured training, access to investigative tools, and regulatory alignment, the service risks falling behind in the fight against digital financial crime. Bridging the current gaps requires not only internal reforms but also strategic foresight, leadership commitment, and inter-agency collaboration.

In closing, the ideas presented in this discussion highlighted several gaps the TTPS faces within the cryptocurrency ecosystem, namely, awareness, technical preparedness, regulatory engagement, and strategic foresight. The lack of proper tools, specific training, and laws has

applied certain limitations to the organization. Moreover, misalignments between internal stakeholders and regulatory bodies have compounded these limitations. Hence, these findings support why it is necessary for the TTPS to revise its approach to cryptocurrency and related threats to incorporate policy reform, inter-agency collaboration, and specialized training programs.

Chapter 6

Implementations

The findings unearthed in this research revealed several items that includes the TTPS possesses low to moderate institutional awareness of cryptocurrency with top management exhibiting the lowest level of awareness and low management showing slightly higher levels than its counterparts. It was also discovered that TTPS was without any formal framework or SOPs in place to assist with challenges faced by cryptocurrency. There was no operational procedure installed to investigate cryptocurrency crimes, making it difficult for specialized units within the organization to function. Training and curriculum gaps were also indicative of the TTPS readiness to respond to cryptocurrency issues. The Police Academy, the organization's training hub currently, did not include cryptocurrency awareness or blockchain fundamentals in its curriculum, nor was any consideration given to handling or identifying digital assets as part of investigations. Moreover, limited interagency collaboration was evident as interviews showed poor collaboration amongst TTPS units as well as key regulators like TTSEC and TT-CSIRT. Most interestingly, the findings evidenced that there was a rising cryptocurrency threat within Trinidad and Tobago. Data from TTCSIRT and TTSECT showed that there was a steady increase in incidents and complaints on cryptocurrency matters over the period 2022-2024. Also, for the same period Fraud Squad recorded over 2 million dollars in losses across major crypto-related cases. Finally, this investigation determined that the TTPS position as it relates to organizational readiness for cryptocurrency issues is critically low. They are not adequately prepared to investigate, prosecute, or manage cryptocurrency-related crimes. Survey data and stakeholder feedback show an urgent need for policy development, training programmes, and technical investments.

To mitigate these revelations, this proposed implementation plan would operationalize these findings into targeted institutional reform as set out in these **strategic goals**.

- Enhance institutional cryptocurrency awareness and investigative capacity.
- Improve interagency and regulatory alignment.
- Build public trust through proactive communication.
- Research and technology focus.

To further assist this implementation, the above interventions would be devised into pillars of success.

Pillar A: Training and Capacity Enhancement

- Objective: To design and implement a multilevel cryptocurrency training curriculum for various TTPS personnel within 12 months, resulting in a measurable increase in investigative competency and awareness.
- Key Actions: Develop curriculum, deliver multi-tier training, evaluate competency gains
- Responsible Units: TTPS Academy, UTT, Fraud Squad
- Dependencies: Training budget, curriculum approval, subject matter experts
- Expected Outputs: Crypto curriculum developed, 200+ officers trained across 3 ranks

Pillar B: Policy & SOPs

Objective: To develop and institutionalize standardized operating procedures (SOPs) for cryptocurrency-related investigations within 9 months to guide operational consistency across TTPS investigative units.

- Key Actions: Draft and implement SOPs for crypto investigations
- Responsible Units: Legal Dept, Fraud Squad, Cyber Unit
- Dependencies: Policy approval, internal review
- Expected Outputs: Approved SOP document, circulated to all investigative units

Pillar C: Technical Tools & Resources

- Objective: To acquire and operationalize at least one leading specialized blockchain forensic tool within one fiscal year, ensuring that trained TTPS officers have access to digital tracing and analytics capabilities for crypto-related crimes.
- Key Actions: Procure and deploy forensic tools (e.g., Chainalysis)
- Responsible Units: ICT Unit, Finance Branch
- Dependencies: Procurement approval, funding

Pillar D: Stakeholder Integration

- Objective: To establish formal inter-agency collaboration with TTSEC, TTCSIRT, and the FIU by signing three Memorandums of Understanding (MOUs) and initiating structured engagement by the end of the calendar year.

- Key Actions: Sign MOUs with TTSEC, TTCSIRT, and FIU
- Responsible Units: TTPS Executive, Legal Dept
- Dependencies: Stakeholder willingness, legal clearance
- Expected Outputs: 3 MOUs signed, quarterly meetings scheduled

Pillar E: Information Sharing Protocols

- Objective: To design, pilot, and assess an inter-agency data exchange system for crypto intelligence and incident reporting within 12 months, enhancing the speed and accuracy of multi-agency responses.
- Key Actions: Design and pilot inter-agency data exchange systems
- Responsible Units: ICT Unit, TTCSIRT
- Dependencies: Data privacy laws, IT compatibility
- Expected Outputs: 1 platform piloted, tested by 3 agencies

Pillar F: Public Awareness Campaigns

- Objective: To launch a national public education campaign on cryptocurrency fraud and safe digital practices within 6 months, aiming to reach 500,000+ citizens and decrease crypto scam reporting rates by 30% in one year.
- Key Actions: Design posters, ads, and videos on crypto fraud
- Responsible Units: Corporate Communications, Fraud Squad, FIB, CSMU
- Dependencies: Media partnerships, funding

- Expected Outputs: Campaign launched, 500,000+ people reached

These pillars represent clear pathways to achieving sustainable institutional readiness, operational effectiveness, and strategic alignment in the TTPS's response to cryptocurrency-related threats and opportunities. However, their timely deployment must be considered and illustrated next.

Table 4

Implementation Timeline

Phase	Activities	Responsible Entities	Timeframe	Output Indicator
Phase 1: Planning and Design	Develop cryptocurrency curriculum and SOP drafts	TTPS Academy, Legal Dept, UTT	Month 1–3	Draft training modules and SOPs completed
Phase 2: Resource Mobilization	Secure funding, procure tools, and finalize MOU templates	ICT Unit, Finance Branch, Executive	Month 4–5	Budget approved, 2 tools procured, 3 draft MOUs ready
Phase 3: Pilot Implementation	Deliver pilot training, circulate SOPs, begin inter-agency data exchange pilot	TTPS Academy, Cyber Unit, TTCSIRT	Month 6–8	50 officers trained, SOPs distributed, pilot data platform tested
Phase 4: Public Awareness Rollout	Launch national campaign and establish reporting portals	Corporate Communications, Fraud Squad	Month 7–9	Public campaign live, 10,000 visits to reporting portal
Phase 5: Monitoring and Evaluation	Conduct evaluation, publish findings, adjust programs	CAPA, ICT Unit, TTPS Executive	Month 10–12	M&E report published, strategy revised for next year

The metrics for success will be dependent on the following proposed monitoring and evaluation plan.

Table 5

Monitoring and evaluation plan

Success Indicator	Measurement Method	Responsible Entity	Frequency
% of TTPS officers completing crypto training	Attendance logs, post-training assessment scores	TTPS Academy, CAPA	Quarterly
Number of investigations using crypto forensic tools	Case file audits, usage logs from forensic platforms	Fraud Squad, Cyber Unit	Bi-annually
SOP compliance rate in case investigations	Internal audit reports, supervisory reviews	Legal Dept, CAPA	Annual
Number of public engagement and education sessions	Event reports, media analytics, community feedback	Corporate Comms, Community Unit	Quarterly
Level of stakeholder satisfaction with inter-agency MOU	Survey responses, meeting evaluations	TTPS Executive, TTSEC, TTCSIRT	Semi-annually
Reports produced by Research & Innovation Unit	Unit output logs, publications	ICT Unit, UTT	Quarterly

It is anticipated that there may exist several factors that can threaten the success of this implementation plan and to alleviate them a risk analysis with mitigation solutions was considered and presented hereunder.

Table 5

Risk analysis and Mitigation Plan

Strategic Risk	Mitigation Strategy	Ownership
Legislative Gaps – Absence of crypto-specific laws may hinder SOPs and enforcement.	Engage policymakers early; align with regional best practices.	Legal Department

Budget Constraints – Limited funding may delay training or tools.	Phase implementation; pursue external grants or donor support. Public Service Investment Programme (PSIP), Seize Asset Fund (POCA)	Executive Leadership
Low Stakeholder Buy-in – Resistance from internal or partner agencies.	Conduct awareness briefings; formalize partnerships via MOUs.	Executive Leadership
Technology Barriers – Incompatibility or delays in tool deployment.	Pilot tools in phases include the ICT team from the outset.	ICT Unit
Public Distrust – Low trust in reporting platforms or awareness campaigns.	Transparent communication; use trusted community channels.	Corporate Communications

In conclusion, these strategic steps outlined above represent a shift toward modernizing TTPS's capabilities in awareness and tackling cryptocurrency-related crime. Once the training, tools, legislation, and public communication factors are addressed, TTPS will be able to position itself as a proactive and competent entity in this evolving digital landscape. This transformation must be deliberate, data-driven, and aligned with both local and global best practices in law enforcement innovation.

The implementation plan outlined in this study represents a structured and actionable roadmap toward enhancing TTPS's capacity to respond to cryptocurrency-related threats. The pillars ranging from training and policy reform to inter-agency collaboration and public engagement encapsulate and interpret these research findings into tangible and deliberate interventions. Success of this transformation will not be relegated to a "quick fix" but heavily dependent on visionary leadership, that possesses the ability to drive institutional change and prioritize investment in people, tools, and partnerships. Data-driven monitoring and evaluation mechanisms embedded within the plan will ensure accountability and responsiveness, enabling the TTPS to adapt in real time to evolving digital threats. Ultimately, the plan aligns the TTPS

with the best international practices in law enforcement readiness, positioning it not just to respond, but to lead the region on matters of digital and financial crime.

Chapter 7

Conclusion

In this study an investigation was launched to examine the levels of cryptocurrency awareness within the Trinidad and Tobago Police Service (TTPS) and assess the organization's preparedness to respond to emerging digital financial threats within this emerging technology. Grounded in Rogers' Diffusion of Innovation Theory, the research explored how knowledge, tools, and institutional support differ across management levels and specialized units. The study also examined training availability, legal gaps, and public engagement.

The findings realized several critical concerns. Firstly, awareness of cryptocurrency was stratified across the management hierarchy, —an outcome linked to operational exposure rather than structured learning. Secondly, the TTPS lacks formal training pathways or investigative tools necessary to address cryptocurrency-related crime, a gap compounded by its reliance on external support and informal knowledge-sharing. Thirdly, the absence of legislation and internal policy frameworks was evident, as was the lack of prosecution in reported crypto-related incidents. Finally, public education and transparency were notably lacking in TTPS operations, contrasting sharply with international examples of proactive law enforcement.

These findings underscore a broader institutional unpreparedness. This study has not only diagnosed the gaps but has also proposed a structured implementation plan featuring thematic pillars—training, policy, inter-agency collaboration, technical tools, and public education—each supported by clear objectives, measurable outputs, and strategic oversight. These interventions offer a realistic path toward institutional transformation and sustained readiness and highlight the urgent need for organizational reform. Notwithstanding, while the TTPS cannot single-handedly enact legislation, it has an obligation to provoke dialogue, shaping policy, and championing the

need for change. Moreover, internal reform is within its control—particularly in areas of training, resource allocation, and inter-agency coordination.

The research, however, is not without limitations. The sample size was limited to selected units within the TTPS, and their responses could have been economical based on self-reporting bias and institutional conservatism. Other studies may benefit from broader representation, inclusion of civilian perspectives, or comparative analyses with other jurisdictions.

In looking ahead given the sensitive nature of digital investigations, the implementation of any crypto-related initiative must also be guided by strong ethical principles—particularly regarding privacy rights, data handling, and public transparency. Ensuring due process and accountability will be essential to maintaining public trust in a digital law enforcement environment.

In the future, other research can explore the intersection between law enforcement readiness and public trust in digital asset investigations, particularly in small island developing states like Trinidad and Tobago. Additionally, investigations into the effectiveness of crypto-related training modules, legal reform impacts, and cross-agency collaborations could offer more targeted recommendations. Longitudinal studies tracking the TTPS's progress over time would also be valuable in assessing institutional growth and adaptation.

This study reinforces that while the TTPS is central to this transformation, meaningful progress also requires engagement from key external stakeholders such as the Financial Intelligence Unit (FIU), the Ministry of Legal Affairs, the TTSEC, and TTCSIRT. Their cooperation is vital for legal reform, regulatory alignment, and intelligence sharing in combating cryptocurrency-related threats. The need for a proactive, technology-literate, and policy-aware law enforcement body in the era of digital finance is essential to any developing country. Hence TTPS must not only keep

pace with technological change but also shape its institutional environment to respond confidently, lawfully, and transparently to emerging threats as this transformation is essential for preserving public trust, operational integrity, and national security.

References

- "Cryptography". (n.d.). Retrieved from cryptography -- The Cryptography and Cryptography Policy Mailing List: <https://www.metzdowd.com/mailman/listinfo/cryptography>
- Academy, C. F. (n.d.). *The Role Of Technology In Combating Financial Crime In Canada*. Retrieved from Canadian Financial Crime Academy: <https://www.canadianfinancialcrimeacademy.ca/financial-crime-articles/the-role-of-technology-in-combating-financial-crime-in-canada>
- Alvin Toffler. (1970). *Future Shock*. New York: Random House.
- Bachan, N. (2021, April 14). *Is Cryptocurrency a Security?* Retrieved from Trinidad and Tobago Securities Exchange Commission: <https://www.ttsec.org.tt/is-cryptocurrency-a-security-2/>
- Balewah, I. (2025, April 9). Enhancing Law Enforcement's Preparedness: A Study on Cryptocurrency Awareness in the TTPS. (J. Ramlal, Interviewer)
- Balthazor, A. W. (2019). The Challenges of Cryptocurrency Asset Recovery. *FIU Law Review*, 1207.
- Bhattacharya, R., Vasilyev, D., & Villafuerte, M. (2023, June 22). *Interest in Central Bank Digital Currencies Picks Up in Latin America and the Caribbean While Crypto Use Varies*. Retrieved from International Monetary Fund: <https://www.imf.org/en/News/Articles/2023/06/22/cf-interest-in-cb-digital-currencies-picks-up-in-latam-the-caribbean-while-crypto-use-varies#:~:text=The%20Bahamas%20pioneered%20the%20introduction,and%20Jamaica%20have%20followed%20suit.>
- Bills. (2020). Retrieved from Parliament of the Republic of Trinidad and Tobago: <https://www.ttparliament.org/publication/the-cybercrime-bill-2017-4/>
- Blakstad, S., & Allen, R. (2018). *FinTech Revolution: Universal Inclusion in the New Financial Ecosystem*. New York: Springer.
- Blundell-Wignall, A. (2014). *The Bitcoin Question Currency Versus Trust-Less Transfer*. Paris: OECD.
- Carrington, O. (2023, November 15). *SWRHA battles European hacker to save its system*. Retrieved from Trinidad and Tobago Guardian: <https://www.guardian.co.tt/news/swrha-battles-european-hacker-to-save-its-system-6.2.1852801.718fb8c20d>
- Chan, K. (2024, November 6). *Trump's win ignites a crypto frenzy that sends bitcoin to a record high*. Retrieved from The Associated Press: <https://apnews.com/article/bitcoin-crypto-donald-trump-election-c2e2a1a895288c5e9c0df2721012a5bb>

- Charbonneau, D. (2024, November 21). *OPP launches 'Project Atlas' to fight cryptocurrency fraud*. Retrieved from CTV News: <https://www.ctvnews.ca/ottawa/article/opp-launches-project-atlas-to-fight-cryptocurrency-fraud/>
- Christiansen, N. B., & Jarrett, J. E. (2019). Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset. *DEPARTMENT OF JUSTICE JOURNAL OF FEDERAL LAW AND PRACTICE*, 155-180.
- Corbet, S. (2021). The danger of cryptocurrency pump-and-dumps: Analysing the development of research & regulation. In S. Corbet, *Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies (Batten-Corbet-Lucey Handbooks in Alternative Investments Book 2)* (p. 187). Berlin: De Gruyter.
- Corbet, S. (2021). *Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies (Batten-corbet-lucey Handbooks in Alternative Investments, 2)*. Berlin: De Gruyter.
- Crime And Problem Analysis*. (n.d.). Retrieved from Trinidad and Tobago Police Service: <https://www.ttps.gov.tt/Branches/Branches-A-E/Crime-And-Problem-Analysis>
- Cryptocurrencies*. (2019, March 12). Retrieved from Trinidad and Tobago Securities Exchange COMMISSION: <https://www.ttsec.org.tt/cryptocurrencies/>
- Cryptocurrency Prices Today By Market Cap*. (n.d.). Retrieved from Forbes: <https://www.forbes.com/digital-assets/crypto-prices/?sh=6443898d2478>
- Director, O. o. (2024, July 30). *MEDIA RELEASE*. Retrieved from The Securities Commission of The Bahamas: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scb.gov.bs/wp-content/uploads/2024/07/Media-Release-The-Bahamas-Introduces-Transformative-Digital-Asset-Legislation-The-DARE-Act-2024.pdf](https://www.scb.gov.bs/wp-content/uploads/2024/07/Media-Release-The-Bahamas-Introduces-Transformative-Digital-Asset-Legislation-The-DARE-Act-2024.pdf)
- Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. New York: Apress.
- Duchow, M. (2025). Crypto Crime and Punishment: The Case for Stronger International. *Denver Journal of International Law & Policy*, 1-6.
- Ehrlich, S. (2023, March 13). *What Are NFTs?* Retrieved from Forbes: <https://www.forbes.com/sites/digital-assets/article/what-are-nfts/>
- Forbes*. (2025, June 20). Retrieved from Cryptocurrency Prices Today By Market Cap: <https://www.forbes.com/digital-assets/crypto-prices/?sh=7968bb982478>
- Garewal, K. S. (2020). *Practical Blockchains and Cryptocurrencies*. New York: Apress.
- Garnett, A. G., & Ashburn, D. (2024, July 22). *Buyer beware: How to spot (and avoid) rug pulls and pump-and-dump schemes*. Retrieved from Britannica Money: <https://www.britannica.com/money/pump-and-dump-schemes>

- Gaur, N. (2021, April 2021). *The rising NFT tide lifts all tokens: So what is an NFT?* Retrieved from IBM: <https://www.ibm.com/think/topics/nft>
- Gundur, R., Levi, M., Topalli, V., & Ouellet, M. (2021, April). *Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context*. Retrieved from Research Gate: https://www.researchgate.net/publication/350937069_Evaluating_Criminal_Transactional_Methods_in_Cyberspace_as_Understood_in_an_International_Context
- Hall, I. (2023, April 25). *European Parliament backs crypto rules to put EU 'at forefront of token economy'*. Retrieved from Global government Fintech: <https://www.globalgovernmentfintech.com/european-parliament-backs-crypto-rules/>
- Harkin, D., & Whelan, C. (2021). Perceptions of police training needs in cyber-crime. *The International Journal of Police Science and Management*, 66-76.
- Hult, J. (2024, September 18). *Police academy adding extra ethics session due to heightened publicity, officer interest*. Retrieved from South Dakota Search Light: <https://southdakotasearchlight.com/briefs/police-academy-adding-extra-ethics-session-due-to-heightened-publicity-officer-interest/>
- Ilham, R. N., Erlina, Fachrudin, K. A., Silalahi, A. S., & Saputra, J. (2019). Comparative of the Supply Chain and Block Chains to Increase the Country Revenues via Virtual Tax Transactions and Replacing Future of Money . *International Journal of Supply Chain Management*, 1066-1069.
- internacional, E. y. (2022, March 30). *Police and prosecutors from 17 countries in Latin America and the European Union combine their efforts to raise awareness about the most common investment scams involving cryptocurrencies*. Retrieved from EL PAcCTO: <https://elpaccto.eu/en/news/police-and-prosecutors-from-17-countries-in-latin-america-and-the-european-union-combine-their-efforts-to-raise-awareness-about-the-most-common-investment-scams-involving-cryptocurrencies/>
- J. Gilcrest, A. C. (2018). Smart Contracts: Legal Considerations. *2018 IEEE International Conference on Big Data (Big Data)*, (pp. 3277-3281). Seattle.
- Justice, U. D. (2024, March 28). *Samuel Bankman-Fried Sentenced to 25 Years for His Orchestration of Multiple Fraudulent Schemes*. Retrieved from U.S Department of Justice: <https://www.justice.gov/archives/opa/pr/samuel-bankman-fried-sentenced-25-years-his-orchestration-multiple-fraudulent-schemes>
- Kacperczyk, M., & Neuefeind, M. (2018). *Cryptocurrency - a Trader's Handbook: A Complete Guide on How to Trade Bitcoin and Altcoins*. Independently Published.
- Li, T., Shin, D., & Wang, B. (2021, February 10). *Cryptocurrency Pump-and-Dump Schemes*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3267041

- Li, Y., Yang, G., Susilo, W., Yu, Y., ManHoAu, & Liu, D. (2021). Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability. *IEEE Transactions on Dependable and Secure Computing*, 679-691.
- Linden, T. v., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it. *Financial Innovation*, 1-30.
- Lundblad, J. P. (2003). A Review and Critique of Rogers' Diffusion of Innovation Theory as it Applies to Organizations. *Organization Development Journal*, 50-64.
- Malik, S., & Rana, A. (2020). A Brief Survey of Cryptocurrency Systems. *IITM Journal of Management and IT*, 77-82.
- Mohammed, D. (2024, December 24). *Money Laundering In the Caribbean*. Retrieved from First Citizens Bank: <https://www.firstcitizensgroup.com/tt/news-insights/money-laundering-in-the-caribbean/>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from Bitcoin: <https://bitcoin.org/bitcoin.pdf>
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from Bitcoin.org: <https://bitcoin.org/bitcoin.pdf>
- Narayana, A. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. New Jersey: Princeton University Press.
- Navigating Cryptocurrency-Driven Crime: A Guide for Law Enforcement*. (2025, February 2). Retrieved from COPOLAD: <https://copolad.eu/en/cryptocurrency-law-enforcement/>
- Nzuva, S. (2019). Smart Contracts Implementation, Applications, Benefits, and Limitations . *Journal of Information Engineering and Applications*, 63-75.
- Owen-Evans, R., & Low, N. (2024, October 31). *Public trust and confidence in the police*. Retrieved from UK Parliament: [https://post.parliament.uk/public-trust-and-confidence-in-the-police/#:~:text=There%20are%20multiple%20barriers%20to%20trust%20and,negative%20public%20perceptions%20of%20police%20performance%20\(PN693\).](https://post.parliament.uk/public-trust-and-confidence-in-the-police/#:~:text=There%20are%20multiple%20barriers%20to%20trust%20and,negative%20public%20perceptions%20of%20police%20performance%20(PN693).)
- Perez, M. F., & Ahmed, M. N. (2021). Cryptocurrencies, a Transformational Catalyst for the Philippines' Digital Economy: An Analysis. *2021 ASEAN University Network Business and Economics Virtual Conference* (p. 257). Yogyakarta: ASEAN University Network for Business and Economics.
- Pethuru, R., Kavita, S., & Chellammal, S. (2020). *Blockchain Technology and Applications 1st Edition*. Florida: Auerbach Publications.
- Powell, F., & Curry, B. (2023, May 1). *Best Crypto Wallets Of May 2023*. Retrieved from Forbes: <https://www.forbes.com/advisor/investing/cryptocurrency/best-crypto-wallets/>

- QC, R. R., & Maguire, A. (2020). Cryptoassets—Obtaining English Freezing and Proprietary Injunctions in Relation to Civil Fraud. *US-China Law Review*, 39-45.
- Relations, U. S. (2022, February 18). *U.S. Secret Service Launches Cryptocurrency Awareness Hub*. Retrieved from United States Secret Service: <https://www.secretservice.gov/newsroom/releases/2022/02/us-secret-service-launches-cryptocurrency-awareness-hub>
- SEC Crypto Task Force to Host Four More Roundtables*. (2025, April 11). Retrieved from U.S. Securities and Exchange Commission: <https://www.sec.gov/newsroom/press-releases/2025-57#:~:text=Launched%20on%20January%2021%20by,and%20deploy%20enforcement%20resources%20judiciously>.
- Simon Alexis, P. (2025, April 7). Porvost interview. (J. Ramlal, Interviewer)
- Team, C. (2022, February 2). *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class*. Retrieved from Chainalysis: <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/>
- Team, T. C. (2024). *The 2024 Crypto Crime Report*.
- Thompson, E. (2024, April 17). *Canada Revenue Agency gets more teeth to catch potential tax cheats*. Retrieved from CBC: <https://www.cbc.ca/news/politics/budget-2024-crypto-taxation-1.7175780>
- Walsh, W. F., & Vito, G. F. (2018). *Police Leadership and Administration A 21st-Century Strategic Approach*. New York: Routledge.
- What is blockchain?* (n.d.). Retrieved from Stanford: <https://online.stanford.edu/how-does-blockchain-work>
- Willmer, S., & Voreacos, D. (2023, September 14). *Wall Street-Backed Crypto Tracer Faces 'Junk Science' Attack*. Retrieved from Bloomberg: <https://www.bloomberg.com/news/articles/2023-09-14/bitcoin-fog-case-puts-spotlight-on-chainalysis-crypto-tracing?embedded-checkout=true>
- Yuming, L. (2022). *Sovereignty Blockchain 2.0 New Forces Changing the World of Future*. Singapore: Springer Nature Singapore.

APPENDIX A

Project Proposal

UNIVERSITY OF TRINIDAD AND TOBAGO (UTT), year (2022)
CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY

[Master of Science in in Cybersecurity]

PROJECT TITLE: Enhancing Law Enforcement's Preparedness: A Study on Cryptocurrency Awareness in the TTPS

Jason Ramlal

Student ID: 92068

Year of Submission (2025)

This work is being submitted in partial fulfilment of the requirements for a

Master of Science in
Cybersecurity
(MSc in Cybersecurity)

Supervisor Name: Ms. Lisa Wharwood

Coordinator Name: Mahindra Persad Koon

Project Proposal

This project is geared towards identifying the levels of understanding and awareness of cryptocurrencies within various management levels of the Trinidad and Tobago Police Service TTPS. The findings gathered may be used to assist the organization as a fact-finding tool that may assist in organizational changes. The project has several key objectives that would assist in its delivery. These would include collecting data. Proposed data collection would be conducted by online survey of the various management levels (top, middle and lower) of the TTPS and interviews to determine the level of awareness and understanding as it relates to cryptocurrency as well as assessing how prepared TTPS is as it relates to cryptocurrency challenges. Other objectives such as explaining the key components of cryptocurrency technologies and identifying whether there exists any relationship between criminal activity and cryptocurrency in our society. The final objective would be providing specific strategies for improving awareness, training, and organizational policy. In the end it is anticipated that this project would achieve and deliver on its purpose and aims. Student Profile

My name is Jason Ramlal; I am an Acting Assistant Superintendent of Police with the Trinidad and Tobago Police service. I have been serving for over twenty-four years, and I am the holder of Bachelor of Science degree in Information Technology from the College of Science, Technology and Applied Arts of Trinidad and Tobago. I am fascinated with the concept of cryptocurrency technologies, and I envision a rapid change in crime trends in Trinidad and Tobago soon. I have enrolled in this program chiefly, so I will be well prepared to assist my organisation when the threat arises.

Background Information

According to Forbes (Forbes, 2025) 3.31 trillion dollars is what the global cryptocurrency market is worth at time of preparing this research. Experts suggests this exponential gain was synonymous with the recent victory of United States president Donald Trump in November 2024 (Chan, 2024). This evidence is clear that cryptocurrency adoption is a significant factor in financial sector worldwide. However, with opportunities therein lies elements of threats. Ironically even though it may be perceived as an oxymoron the criminal elements within this space have seized the opportunity to exploit this technology to provide for their criminal enterprises such as the laundering of money, cybercrime, and terrorism financing. In Trinidad and Tobago, the TTPS may find it challenging combating crime within this ecosystem because of the lack or limited awareness and understanding by its members. This research will attempt to explore these limitations as it relates to the TTPS's management and propose strategies for the organization's improvement.

Problem Statement

Renowned fiction writer and inventor Arthur C. Clarke quoted "Any sufficiently advanced technology is indistinguishable from magic." This quote can be synonymous with cryptocurrencies as its emergence has brought about a new era of financial innovation/magic and disruption that have provided individuals to take control of their financial transactions and investments. However, this modern technology has also brought about a rise in cryptocurrency crimes, which can be costly on the victims. Despite some efforts to combat this through regulations and education there is no record of bad actors being prosecuted for crimes within this ecosystem. Hence it is crucial that there exist an elevated level of understanding and awareness as it relates to cryptocurrency within Trinidad and Tobago Police Service. The TTPS has limited

resources and training to address the complexities of cryptocurrency-related crimes. Despite the growing concerns of deviant behaviour and complexities surrounding cryptocurrency; the TTPS lacks the resources, training, and meaningful awareness to address issues within this thematic. This knowledge gap may hinder effective enforcement, investigation, and policy formulation. Hence this thesis will assess the current knowledge and perception of cryptocurrencies within the organization and explore opportunities for initiating organizational change to better address the challenges and opportunities posed by this emerging technology.

Project Goal/Aim of the Project

This research explores the level of awareness of cryptocurrency technologies within the various management levels of the TTPS. It examines the factors that contribute to the current attitudes towards cryptocurrencies among members of the organization.

These factors include:

1. **Lack of Knowledge:** With limited exposure to and understanding of cryptocurrency technologies within the TTPS an officer's ability to effectively identify and address cryptocurrency-related crimes can be compromised.
2. **Limited Access to Training and Resources:** Specialized training programs and access to resources are major factors in combatting cryptocurrencies crimes. In their absence an officer may be unable differentiate between accurate and misleading information.
3. **Lack of Regulation:** Without clear regulatory guidelines for cryptocurrencies in Trinidad and Tobago TTPS personnel may find it challenging to address cryptocurrency issues, thus limiting their ability to manage cryptocurrency-related cases effectively.

Additionally, this research would assist the society in making calculated and informed decisions as it relates to cryptocurrencies.

Project Purpose

The presence of cryptocurrency has attracted some concerns leading to certain impacts within our society. Hence, this thesis will endeavour to increase the level of awareness of cryptocurrency within the TTPS which can act as a catalyst to organizational change and by so doing increase the level of public trust and confidence in the country's premier law enforcement agency.

Objectives of the Project:

- To explore all literature as it relates to the cryptocurrency ecosystem that is applicable to the region.
- To investigate the levels of awareness of cryptocurrency as it relates to the various management levels of the TTPS.
- To propose an awareness programme for the TTPS as it relates to cryptocurrency.
- To develop an implementation plan to facilitate the awareness strategy.

Resources

Internet access: the internet would be essential for this project as it would provide a medium for original source of information as well as providing guidance in relation to fact finding endeavours. The internet would also facilitate communication with supervisors to provide feedback and counselling.

Surveys: this is a method that would be used in the research to gather data relating to a plethora of different fields. It would be important as this research would be studying the awareness levels of cryptocurrency within the various management levels of the TTPS. Additionally, data from other entities would be sourced to add credibility to the research.

Interviews: this strategy would be used to collate data from a smaller group within the environment, and it is normally a richer source. This strategy would be ideal as some of the actors within the environment would be required to be approached individually.

Supervisors: are needed as their role would be to provide the much need guidance for this project. They would ensure that the overall scope of the project remains within the curtilage of the area of research as well as providing feedback on changes or achievements.

Literature

Books, scholarly and journal articles are paramount to this research paper as they are a source of credible material which include some level of research written by experts. These items would form an integral part of this research.

Reference

There were several pieces of literature that assisted this paper to achieves its goal, however the most relevant had were isolated to include Cryptocurrency - a Trader's Handbook that provided material on how cryptocurrencies work and use within an economy etc (Kacperczyk & Neuefeind, 2018). Blockchain Technology and Applications provided the detailed concept of blockchain technology a key component of cryptocurrency (Pethuru, Kavita, & Chellammal, 2020). FinTech Revolution: Universal Inclusion in the New Financial Ecosystem this book was a guide to evolving financial environment. Moreover, it highlighted how our relationship with

money and financial technology, together with macroeconomic and societal change, is changing the paradigm of how conventional business is executed in emerging economies (Blakstad & Allen, 2018). The Bitcoin Question Currency Versus Trust-Less Transfer Technology this paper talked about the impacts of cryptocurrencies in relation to central banks in addition to some serious issues that may arise due the anonymity features inherent with cryptocurrencies (Blundell-Wignall, 2014). Cryptocurrencies, a Transformational Catalyst for the Philippines' Digital Economy: An Analysis. This study focused on the people of the Philippine in relation to their awareness and trust on the cryptocurrencies (Perez & Ahmed, 2021).

References

- Blakstad, S., & Allen, R. (2018). *FinTech Revolution: Universal Inclusion in the New Financial Ecosystem*. New York: Springer.
- Blundell-Wignall, A. (2014). *The Bitcoin Question Currency Versus Trust-Less Transfer*. Paris: OECD.
- Chan, K. (2024, November 6). *Trump's win ignites a crypto frenzy that sends bitcoin to a record high*. Retrieved from The Associated Press: <https://apnews.com/article/bitcoin-crypto-donald-trump-election-c2e2a1a895288c5e9c0df2721012a5bb>
- Forbes. (2025, June 20). Retrieved from Cryptocurrency Prices Today By Market Cap: <https://www.forbes.com/digital-assets/crypto-prices/?sh=7968bb982478>
- Kacperczyk, M., & Neuefeind, M. (2018). *Cryptocurrency - a Trader's Handbook: A Complete Guide on How to Trade Bitcoin and Altcoins*. Independently Published.
- Perez, M. F., & Ahmed, M. N. (2021). Cryptocurrencies, a Transformational Catalyst for the Philippines' Digital Economy: An Analysis. *2021 ASEAN University Network Business and Economics Virtual Conference* (p. 257). Yogyakarta: ASEAN University Network for Business and Economics.
- Pethuru, R., Kavita, S., & Chellammal, S. (2020). *Blockchain Technology and Applications 1st Edition*. Florida: Auerbach Publications.

APPENDIX A: Interview Guide – Head of the Financial Investigations Branch (FIB)

1. Introduction

Good day and thank you for participating in this interview. This study seeks to evaluate the preparedness of the TTPS, with a focus on the Financial Investigations Branch (FIB), in addressing crimes involving cryptocurrency. Your expert perspective will significantly contribute to understanding institutional gaps and opportunities. This interview is voluntary and confidential. With your permission, I would like to record this session for accuracy.

2. Interviewee Information

Rank/Position: Senior Superintendent

Division/Unit: Financial Investigations Branch

Years of Service: 26

3. Interview Questions

Section 1: Strategic Awareness & Understanding

1. From your perspective, how would you define the role of cryptocurrencies in the context of financial investigations within Trinidad and Tobago?
2. How aware do you believe FIB officers are regarding cryptocurrency operations such as blockchain technology, crypto wallets, and exchanges?
3. Has FIB developed any internal definitions, protocols, or frameworks specifically to address cryptocurrency-related financial crimes?

Section 2: Investigation Trends & Experience

4. Could you provide an overview of how frequently FIB encounters cryptocurrency-related cases over the past 3 to 5 years?
5. Are there specific trends or patterns emerging in the types of financial crimes involving cryptocurrencies (e.g., fraud, ransomware, money laundering)?
6. What are some key challenges FIB has encountered in bringing cryptocurrency-related investigations to successful resolution or prosecution?

Section 3: Resources, Tools & Technical Capacity

7. Does FIB currently utilize any specialized blockchain forensic tools or investigative platforms (such as Chainalysis, Elliptic, CipherTrace)?
8. Do you consider the technical and human resources presently available to FIB sufficient to conduct in-depth cryptocurrency investigations?
9. Are there any gaps in technical capability that you believe need to be addressed to strengthen the unit's effectiveness?

Section 4: Training & Capacity Development

10. What types of training, if any, have been provided to FIB personnel concerning cryptocurrency and blockchain investigations?
11. Are there existing partnerships or programs (locally or internationally) that support FIB's officer training in this area?
12. From a leadership standpoint, what further capacity-building initiatives would you recommend enhancing the unit's readiness to handle cryptocurrency-related financial crimes?

Section 5: Policy, Regulation & Legal Framework

13. Do you believe the existing laws and policies in Trinidad and Tobago sufficiently empower FIB to investigate and prosecute cryptocurrency-related offenses?

14. Are there any legislative or regulatory barriers that limit FIB's ability to access information from cryptocurrency exchanges or financial intermediaries?

15. In your view, how effective is inter-agency cooperation (e.g., FIU, Cyber Units, Fraud Squad) when dealing with cryptocurrency investigations?

Section 6: Regional & International Collaboration

16. Has FIB engaged in collaborations with regional or international bodies (such as Interpol, FATF, or other law enforcement agencies) in the area of cryptocurrency investigations?

17. How valuable do you find these partnerships in strengthening FIB's ability to trace, intercept, or prosecute cryptocurrency-related crimes?

Section 7: Emerging Threats & Preparedness

18. What emerging threats do you foresee with the increasing use of cryptocurrencies in Trinidad and Tobago, particularly concerning financial crimes?

19. Do you believe establishing a specialized cryptocurrency-focused unit or task force within TTPS would enhance overall law enforcement preparedness?

APPENDIX B: Interview Guide – Provost of the Police Training Academy

1. Introduction

Good day and thank you for participating in this interview. This study explores the state of awareness and preparedness within the TTPS to address crimes involving cryptocurrency. Your role as Provost of the Police Training Academy provides vital insights into the training and curriculum aspects. This interview is voluntary and confidential. With your permission, I would like to record this session for accuracy.

2. Interviewee Information

Name: Simon Alexis Ph.D.

Position: Provost, Police Training Academy

Years of Service at TTPS: 30

Years' experience in Training/Curriculum Development: 20

3. Interview Questions

Section 1: General Awareness & Curriculum Integration

1. What do you know about cryptocurrency and blockchain technology?
2. Is cryptocurrency awareness currently integrated into the Police Training Academy curriculum?
3. Does the Academy provide training specifically focused on cybercrime investigations or digital threats?

4. Has there been any formal initiative or discussion about incorporating cryptocurrency-related topics in officer training programs?

5. In your opinion, how important is it for police officers, at all levels, to be trained on cryptocurrency-related issues?

Section 2: Current Training & Capacity

6. What existing courses or modules (if any) touch on financial crimes, cybercrime, or digital investigations?

7. Have any officers received external training or certifications specifically focused on cryptocurrency investigations?

8. Are there challenges (budgetary, expertise, resources) that the Academy faces in offering cryptocurrency-related training?

Section 3: Collaboration & Resources

9. Has the Academy collaborated with external agencies (local, regional, international) to provide training on cryptocurrency awareness?

10. Are there any partnerships in place with institutions such as universities, financial intelligence units, or cybersecurity bodies?

Section 4: Training Gaps & Future Plans

11. From your perspective, do you believe there is a training gap in terms of officers' preparedness to handle cryptocurrency-related crimes?

12. Are there plans to revise or update the Academy's curriculum to include cryptocurrency, blockchain, or emerging technologies?

APPENDIX C: Interview Guide – Cyber & Social Media Unit

1. Introduction

Good day and thank you for participating in this interview. This study aims to evaluate the preparedness of the TTPS in addressing cryptocurrency-related crimes. As a key player in cyber investigations, your insights are critical. This interview is voluntary and confidential. With your permission, I would like to record this session for accuracy.

2. Interviewee Information

Rank/Position: _Inspector in Charge

Division/Unit: Cyber & Social Media Unit

Years of Service: 25

3. Interview Questions

Section 1: Awareness & Technical Capacity

1. How would you assess the Cyber Unit's awareness of cryptocurrencies and blockchain technology?
2. What specific cyber threats involving cryptocurrency has the unit encountered (e.g., ransomware, crypto scams, darknet transactions)?
3. Are officers in the unit familiar with digital wallets, exchanges, and how cryptocurrency transactions are traced?

Section 2: Investigative Experience

4. Can you share examples of cyber investigations handled by the unit that involved the use of cryptocurrency?
5. What are the most common online platforms or tactics used by offenders in these cases?
6. Does the unit work with blockchain analysis tools to trace transactions?

Section 3: Training & Tools

7. Have team members received training specific to cryptocurrency tracking, investigation, or forensic analysis?
8. What types of tools or platforms does the unit use to detect or analyze crypto-related cybercrime?
9. What limitations, if any, affect your ability to pursue cryptocurrency-related investigations effectively?

Section 4: Inter-Unit & External Collaboration

10. Does the Cyber Unit collaborate with other TTPS departments (e.g., Fraud Squad, FIB, CAPA) or agencies (e.g., FIU, Interpol) in cryptocurrency-related investigations?
11. Are there data-sharing or coordination protocols in place when cryptocurrency is involved?

Section 5: Policy, Challenges & Recommendations

12. Are there any internal guidelines or SOPs specific to handling cryptocurrency in cybercrime cases?

13. What challenges does the unit face in investigating crimes where cryptocurrency is the medium of exchange?

14. What improvements or resources would you recommend enhancing TTPS's ability to respond to cryptocurrency-facilitated cybercrimes?

4. Closing Script

Thank you for your time and valuable input. Your responses will be used solely for academic purposes and will remain anonymous. If you would like to review your responses or have any follow-up questions, feel free to contact me.

APPENDIX D: Interview Guide – Fraud Squad

Section 1: Case Handling & Classification

1. Can you describe the Fraud Squad's process for handling reports that involve cryptocurrency?
2. What criteria must be met for a cryptocurrency-related report to be classified as a fraud case?
3. Are there challenges or delays due to the need for classification before investigations can proceed?
4. Is there a standardized method for identifying and flagging cryptocurrency involvement in initial reports?

Section 2: Investigative Experience

5. How frequently does the Fraud Squad encounter cases involving cryptocurrency (e.g., scams, Ponzi schemes, phishing)?
6. Could you share any insights on the types of fraud schemes that most commonly involve digital currencies?
7. What challenges are typically faced when investigating these cases (e.g., tracing funds, accessing exchange data, lack of cooperation)?

Section 3: Training, Tools & Preparedness

8. Have Fraud Squad officers received any formal training on cryptocurrency-related investigations?
9. Does the unit have access to blockchain analysis tools or partnerships with agencies that support such work?
10. How confident are you in the unit's current capability to effectively investigate cryptocurrency-based fraud?

Section 4: Policies & Inter-Agency Cooperation

11. Are there internal policies or guidelines that govern how cryptocurrency fraud cases are approached?
12. Are there any statutes that guide the Fraud Squad in relation to cryptocurrency?
13. How effective is collaboration with other TTPS units (e.g., Cyber Unit, FIB, CAPA) or external agencies (e.g., FIU, Interpol) in these cases?
14. Are there any recommendations you would make to improve how TTPS or the Fraud Squad handles cryptocurrency-related fraud investigations?

Appendix E: Survey Questionnaire

This instrument was developed to assess the awareness, knowledge, and preparedness of TTPS personnel regarding cryptocurrency and related technologies. Respondents were asked to indicate their level of understanding or engagement on a 5-point Likert scale as follows:

- 1 – Low/Never
- 2 – Limited/Rarely
- 3 – Moderate/Sometimes
- 4 – Good/Often
- 5 – High/Always

The questionnaire is structured around key thematic domains relevant to cryptocurrency awareness and readiness.

Market Dynamics

1. How well do you understand the concept of market capitalization in the cryptocurrency market?
2. Do you understand the significance of trading volume in determining market activity within the cryptocurrency space?
3. To what extent are you familiar with the concept of price volatility and its impact on cryptocurrency investments?
4. How confident are you in interpreting market sentiment analysis towards specific cryptocurrencies?

Blockchain Basics

1. How well do you understand the concepts of the consensus mechanisms used in blockchain technology?

2. How familiar are you with the concept of decentralization and its importance in blockchain networks?
3. What you think is your level of understanding regarding the immutability of blockchain ledgers
4. How familiar are you with the functionality and applications of smart contracts in blockchain ecosystems?

Security & Wallet Management

1. Are you aware of how to select and use secure storage solutions for cryptocurrency holdings?
2. Are you familiar with best practices for managing private keys to ensure the security of cryptocurrency assets?
3. How well do you understand the potential security risks associated with cryptocurrency transactions and storage?
4. Are you familiar with the procedures for backing up wallet data and recovering funds in case of loss or theft?

Regulatory Understanding

1. How well do you stay informed about and comply with regulatory requirements governing cryptocurrency transactions in your jurisdiction?
2. How familiar are you with the potential impact of regulatory changes on cryptocurrency activities and investments?
3. Do you understand the differences in regulatory approaches to cryptocurrencies across different jurisdictions?
4. How often do you engage in discussions with regulatory authorities or industry stakeholders regarding cryptocurrency regulations?