CRYPTOCURRENCY AND FINANCIAL RISKS

by

Avin M.Sharma

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

December 2020

Abstract

Since its inception, the cryptocurrency's exceptional growth has put financial institutions at high risk of exposure to money laundering. In financial institutions, specifically banks, Anti-Money Laundering and Bank Secrecy Act (AML/BSA) risk specialists, bank managers, and compliance officers get challenged in identifying cryptocurrency-related transactions and customers who conceal illegal funds. Interviews conducted with the AML/BSA risk specialists, bank managers, and compliance officers were analyzed to understand how banks combat the cryptocurrency-related money laundering in the USA banking system. Interview with the Director of Financial Investigations & Education at CipherTrace as an expert in blockchain forensics was evaluated to recognize bank regulation and compliance. The case studies were assessed to understand the banks' program and regulation deficiencies and their inability to identify suspicious accounts. Interviews and case studies findings suggest that cryptocurrency-related money laundering is a risk for banks who lack proper tools, programs, and adequate well-trained and well-educated staff in mitigating cryptocurrency-related risks. Support provided by FinCEN regulation and guidance and external vendors is seen as critically valuable in assisting banks to combat cryptocurrency-related money laundering financial crimes.

Key words: cryptocurrency, banks, regulation, money laundering

CRYPTOCURRENCY AND FINANCIAL RISKS

by

Avin M.Sharma

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

December 2020

____

Dr. David Bosch, Dissertation Chair

____

Dr. John Halstead, Dissertation Committee Member

____

Dr. Ed Moore, DBA Director

____

Dr. David Calland, School of Business

Dedication

Dedicated to my parents, Abhay and Praneeta, who emigrated from the Fiji Islands in 1995 for their children to achieve and live the American Dream. In lieu of better life their daily struggles bestowed in me of never giving up to achieve my dream no matter how difficult it became. Thank you for teaching me the value of hard work and perseverance always. I love you both.

Acknowledgments

I am grateful to my wife Monita, and daughters Yashi and Dipal, for allowing me to purse this dream. I appreciate your sacrifices that you have made to support me in my pursuit. I love you!

To my Chair. Dr. Bosch – thank you is just not enough to describe your influence. Your continuous encouragement, guidance, and prayer enabled me to overcome all challenges. I am eternally grateful for your presence in my journey.

Nothing is possible without God! Jeremiah 29:11 resonates with me deeply for God only knows the plans to the future and to give hope along the way. I am thankful for His blessings on me and my family.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

As a result of a rapid increase in cryptocurrency money laundering, financial institutions struggle to address financial crimes that come with it. According to Böhme et al. (2015), fighting cryptocurrency crimes have become a critical issue as it gives rise to money laundering. While regulations such as the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) are available to combat cryptocurrency money laundering, there are significant gaps in these existing laws as the cryptocurrency has many advanced features such as decentralization (Nabilou, 2019). Although banks are continuously implementing anti-money laundering standards against cryptocurrency, many banks feel the strain due to cryptocurrency's decentralized and anonymity feature along with its forever changing nature (Demertzis & Wolf, 2018). This chapter discusses the background of cryptocurrency, its threat to financial institutions, the regulations and their impact, problem statement, and purpose statement. The significance of the study, research questions, and a list of terms are also included in this chapter.

Background of the Problem

Money laundering is one of banks' biggest challenges and is often a key element in financial crimes that banks cannot completely understand and address (Slutzky et al., 2018). It is defined as the process for disguising illicitly obtained money and converting it into legal proceeds, thus corrupting the financial system and giving criminals undeserved power (Ardizzi et al., 2014). The United States government estimates, based on the 2015 analysis, approximately $300 billion of laundered money was generated (U.S. Department of the Treasury, 2018).

Laws such as the anti-money laundering law and the bank secrecy act exist to help banks combat money laundering (Anderson & Anderson, 2015); however, due to an increase in money laundering, many banks lag in compliance monitoring. As a result, the money laundering regulations' restrictions create threats, vulnerability, and risks for the financial sectors (U.S. Department of the Treasury, 2018). Additionally, the lack of money laundering regulations challenges law enforcement to outline guidelines to combat money laundering (Alsaif & Ramo, 2018).

As Sarigul (2013) stated with increased in financial crimes such as drug dealing, terrorist groups, and arms traffickers, money laundering has permitted the criminals to extend their criminal network globally. Criminals filter and funnel illicit funds through banks, who usually lack the compliance and economy of scale needed to implement anti-money laundering programs (Saperstein et al., 2015). The ineffectiveness of money laundering regulations has failed to stop money laundering, promoting financial crimes such as corruption and bribery (Gjoni et al., 2015). Isa et al. (2015) described money laundering as one of the most significant financial risks resulting in banks unintentionally being a part of financial crimes.

Research by Mabunda (2018) showed that with an increase in virtual currencies, money laundering raises new challenges for banks. Cryptocurrency, such as Bitcoin, has become the currency of choice for many criminal activities in the form of money laundering by allowing individuals to hide behind alleged privacy and anonymity, where CipherTrace reported that in the second quarter of 2018, cryptocurrency-related money laundering rose to around $1.2 billion (Kethineni & Cao, 2019). While cryptocurrency is not an easy technology to use, the lack of technological know-how can constrain banks and agencies' ability to battle with money laundering (Arias-Oliva et al., 2019). The pseudo-anonymity feature of cryptocurrency has also caused the banks to struggle to identify and investigate both the sender and the cost of crime transactions (Dyson et al., 2018).

Due to the regulation's weakness against money laundering encouraged by cryptocurrency and its advanced technology, banks may lack the appropriate regulation to combat the increase in money laundering. Consequently, they end up paying hefty fines (U.S. Government Accountability Office, 2016). Governments, law enforcement agencies, and banks have been asked over the years to explore a risk-based policy from a rule-based model (Savona & Riccardi, 2019). As a result, to create and promote safe cryptocurrency exchange, specific regulations may be needed for consistency and accountability within the cryptocurrency market where banks can diligently monitor criminal activities (Obie & Rasmussen, 2018).

Problem Statement

The general problem to be addressed was the challenge of banks to understand and combat risks of financial crime resulting in laundered money entering the banking system. According to Slutzky et al. (2018), it is estimated that the volume of money laundered globally is anywhere between 2% and 5% per year. This increase in money laundering leaves the banks with challenges such as lack of supervision, resources, time, and cost to combat crime (Al-Qadi et al., 2012). Recently, some cryptocurrencies, such as Bitcoin, have played a significant role in spreading money laundering as it possesses features that attract criminals (Mabunda, 2018). According to Forgang (2019), $266 million was laundered through cryptocurrencies in 2017, increasing to $761 million in early 2018. Since there is no government or financial industry control for conducting cryptocurrency transactions, the requirement for no verification under specific limits increases the financial crimes and criminal activities, almost blocking criminal identification (Dyntu & Dykyi, 2018). The specific problem to be addressed was the challenge posed by cryptocurrency to banks within the U.S. in how they understand and combat risks of financial crime resulting in money laundering entering the banking system.

Purpose Statement

The purpose of this qualitative case study was to understand the challenges posed by cryptocurrency for banks within the U.S. in order to identify and combat risks of financial crimes resulting in laundered money entering the banking system. This more significant problem was explored through in-depth case studies of banks within the U.S. The cumulative case studies were collected from CipherTrace and several sites allowing for the higher generation of data without spending time on new or possibly repetitive studies. The case studies demonstrated how money laundering through cryptocurrency presents banks with issues in identifying financial crimes. The case studies also focused and expanded on other financial crimes such as terrorist funding through money laundering influenced by cryptocurrency. The data were used to determine if there are justifications and strategies for implementing regulations to combat financial crimes in the banking industry.

Nature of the Study

This research study used a qualitative method and case study design. Hammarberg et al. (2016) described the qualitative method as a suitable method for recording 'factual' data to answer the research questions. The case study design applied to the research study enabled the researcher to collect data from multiple sources within a specific context. According to Rashid et al. (2019), case study design allows researchers to collect in-depth data through various data sources, revealing multiple facets of the study. The research study utilized research questions within a specific context intended to gather data from the bank employees and the Director of Financial Investigations & Education at CipherTrace. In addition, case studies were evaluated and analyzed.

Discussion of Method

According to Hammarberg et al. (2016) qualitative methods are exploratory research used to reveal theoretical framework problems. The qualitative method is used to detect trends in thinking and opinion by understanding the problem (Sutton & Austin, 2015). For this study, the qualitative research method was utilized, as the study planned to produce subjective and detailed data by “non-standardized” practice rather than using numbers and statistics, in addition to interacting with participants through interviews (Rahman, 2016). Data from bank personnel was collected on the challenges they face with financial crimes risk, how they report those suspicious transactions, and what can help the banks minimize those financial crime risks. The qualitative method did not utilize any numbers, but data were based on trends, opinions, and developing an understanding of the problem.

According to Salvador (2016), the quantitative method is concise and uses fixed approaches, numerical data, and closed-ended questions; therefore, it is not an appropriate method for exploring the challenges posed by banks' cryptocurrency. The quantitative method comes with structured predetermined variables, hypothesis, and design, which do not enable critical thinking (Daniel, 2016), as is not the case in this research study. The mixed-method can be an option; however, the integrating both quantitative and qualitative approaches should only be used where the combined data fully answers the research questions (Halcomb, 2018). For this study, there was no hypothesis; therefore, the mixed method was not appropriate, as the method only answered qualitative research questions.

Discussion of Design

The most appropriate design for this study was a case study. Starman (2013) defined case studies as a detailed analysis of a project, policy, institution, program, financial organizations, and websites allowing for the greater generation of data without time being spent on new or possibly repetitive studies. The study included interviews from selected bank personnel who specialize in AML/BSA. These individuals are certified and trained to identify, detect, and report suspicious transactions involving financial crimes.

The qualitative method also comprises of phenomenology, ethnography, grounded theory, and narrative designs. According to Eddles-Hirsch (2015), phenomenology design attempts to understand a phenomenon's essence from the participants' environment. The grounded theory explains the theory using interviews and coding systems (Tie et al., 2019). According to MacLeod (2016), ethnography design focuses on culture, understanding the participants' cultures, rather than relying on surveys or studies, but experiencing the environment first. Wang and Geale (2015) explained that the narrative method helps understand the events' sequence to form a cohesive story, trying to understand the relationships, rather than the truth. However, these designs were not suitable for gaining understanding and insight into the challenges posed by banks' cryptocurrency as these methods are more focused on the participants' environment, their culture, and relationships forming stories.

Summary of the Nature of the Study

The qualitative method allows researchers to access the thoughts and feelings of participants (Sutton & Austin, 2015) as in this case, the bank personnel’s thoughts on how the money laundering has affected their process and ability to perform their job. Additionally, this qualitative method's data can help the banks and bank personnel update their compliance programs to match current regulations and develop a concordant and reliable relationship with their clients to gain their trust by fighting money laundering successfully. Case study as a design for the qualitative method, on the other hand, focuses on a particular unit where they are used to explore a setting to understand links and pathways and to compare different types of facts (Gustafsson, 2017). Moreover, data collected from case studies are more abundant and greater than other experimental designs (Starman, 2013). In this case, the case study worked best for the crafted research questions. It may allow banks to revisit their compliance regulations, make improvements in successfully identifying suspicious accounts, and minimize the financial crime risks and challenges they face when dealing with cryptocurrency money laundering.

Research Questions

This qualitative study sought to develop an in-depth understanding of the financial risks and challenges posed by cryptocurrency for banks within the U.S. According to Böhme et al. (2015), cryptocurrency money laundering can be difficult in being tracked by law enforcement. The rise in cryptocurrency challenges banks to identify cryptocurrency-related financial crimes (Peprah et al., 2018). The following designed research questions derived from the general and specific problem were addressed through interviews and case studies:

RQ1. What are the financial crime risks and challenges faced by banks when dealing with cryptocurrency?

RQ2. How do banks identify and report suspicious account activities related to cryptocurrency?

RQ3. What would help banks to minimize the financial crime risks and challenges that they face when dealing with cryptocurrency?

Conceptual Framework

Due to weak regulations, financial institutions are usually the target for many different types of financial crimes resulting in money laundering entering the banking system (Campbell-Verduyn, 2018). According to Comben (2019), since the financial crisis of 2008, the weak regulations and anti-money laundering laws have cost banks up to $243 million making them the hub for money laundering practices. The foundation of this research study was built on the advantages of regulating cryptocurrency. Within this conceptual framework, two theories, as illustrated in Figure 1, was utilized to guide this research study; Burrus' (2018) theory identifying cryptocurrency-related financial crimes supported by no regulations and Marian's (2015) conceptual framework for the regulation of cryptocurrency.

Burrus Theory of Cryptocurrency-Related Financial Crimes

Burrus (2018) has identified financial crimes as money laundering, corruption, illicit market, illegal drug, and arms dealings, caused by the decentralized and anonymous cryptocurrency characteristic. Thus, it is used as a source of financial payments where criminals are looking to hide illicit money and profit. Furthermore, according to Burrus (2018), banks suffer from money laundering, which arises from drug and arms trafficking, giving criminals the ability to profit. Burrus (2018) pointed out that the cause of financial crimes is due to the lack of appropriate regulations. Kethineni and Cao (2019) supported Burrus (2018) by pointing out that cryptocurrency-related crimes such as illegal weapons, illegal drugs, defrauding people, drug trafficking, and money laundering is on the rise while operating in anonymity without regulations, as depicted in Figure 1. Kethineni and Cao (2019) also faulted the oversight and lack of appropriate regulations and monitoring due to no identity revelation to banks for financial crimes growth.

Marian’s Theory of Regulation Framework

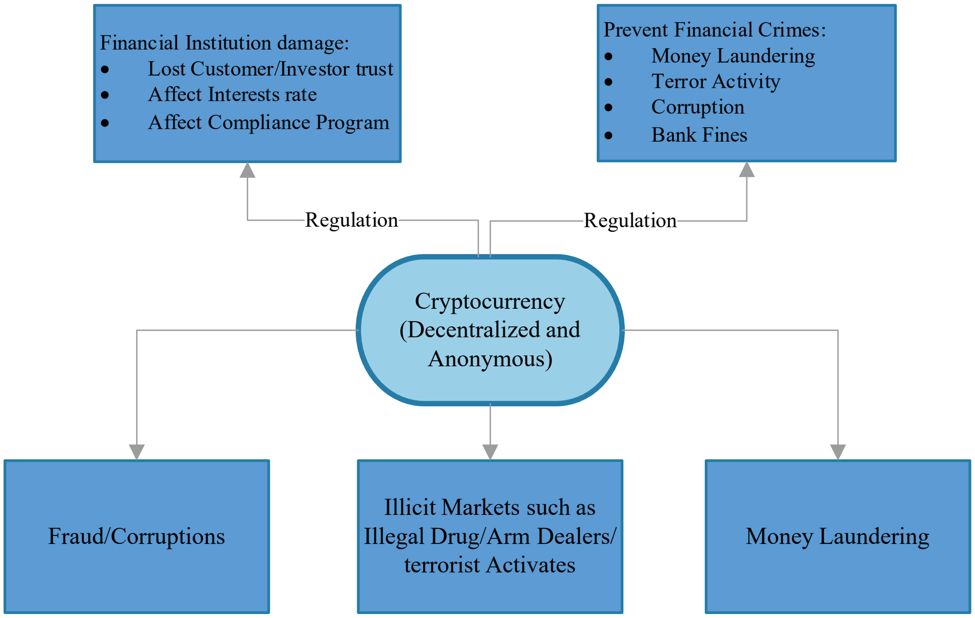
Marian's (2015) conceptual theory proposing cryptocurrency regulation branches of Burrus' (2018) theory. Marian's (2015) literature focused increasingly on the interest of cryptocurrency regulation and mentions that the high level of anonymity and decentralized feature of cryptocurrency has prompted illicit transfers, specifically money laundering challenging the financial institutions in identifying criminal activities. The "Know Your Customer” rules have limited the financial institutions in preventing money laundering; thus a better and new intermediary regulation needs to be imposed on cryptocurrency exchanges in banks. Marian (2015) further emphasized that new regulations can help lower cryptocurrency-related money laundering financial crimes as criminals can find the regulations hard to circumvent.

Supporting Marian's theory, Massed (2019) noted that it is time to strengthen cryptocurrency regulations, which can help decrease money laundering, terrorist activities, corruption, and bank fines, as illustrated in Figure 1. The breach and the weakness in cryptocurrency regulations have led many financial institutions to pay penalties due to their inability to appropriately identify and report money laundering activities through digital assets (U.S. Government Accountability Office, 2016). Goodell and Aste (2019) and Perkins (2018) further noted that lack of regulations causes damage to financial institutions where they lose customer and investor trust, and impact their interest rate and compliance programs as depicted in Figure 1.

Without regulations, money laundering, fraud, corruption, and illicit funds can reside in the banking system, causing enormous damages. With appropriate regulations, banks can monitor suspicious accounts and transactions that can be detrimental to financial crimes, as shown in Figure 1. According to Sidanius (2018), organizations lost an average of 3.5% of their global turnover because of financial crimes such as money laundering. Marian's (2015) theory strongly calls for a need to have regulatory requirements to discourage criminals from utilizing cryptocurrency for the wrong reasons. The section below discusses cryptocurrency, financial crime, money laundering, and the impact of cryptocurrency and regulations on money laundering.

Figure 1

Relationships between Cryptocurrency, Financial Crime, and Regulation


Financial Institution damage:
Lost Customer/Investor trust
Affect Interests rate
Affect Compliance Program
Prevent Financial Crimes:
Money Laundering
Terror Activity
Corruption
Bank Fines
Regulation
Regulation
Cryptocurrency (Decentralized and Anonymous)
Fraud/Corruptions
Illicit Markets such as Illegal Drug/Arm Dealers/ terrorist Activates
Money Laundering

Note. Relationships between Cryptocurrency and Regulations

Cryptocurrency

Cryptocurrency, defined as a decentralized digital currency in Figure 1, was initially designed and developed in 2008 to make a peer-to-peer transaction without bank involvement (Kethineni & Cao, 2019). According to the BIS Annual Economic Report 2018, cryptocurrency promises to replace long-standing and trusting financial institutions with a new, fully decentralized system. As the internet becomes universal, many find cryptocurrency convenient by avoiding financial fees associated with the traditional banking system (Peprah et al., 2018). As of 2018, over 1,800 different cryptocurrencies are available (Kethineni & Cao, 2019). At its peak in January 2018, Bitcoin, one of the leading cryptocurrencies, had a market cap of $310 billion, while Ethereum's market cap was around $24 billion (Toscher & Stein, 2018).

Numerous articles have stated that cryptocurrency has played a significant role in increasing financial crimes, leading to billions of dollars' worth of losses (Faridi, 2019). According to an anti-money laundering report from CipherTrace, during Q2 2019, around $125 million was lost to crypto-related hacks and $227 million stolen in various other security breaches. Since cryptocurrency is pseudonymous, it allows for money transfer with no cost low barriers (Dyntu & Dykyi, 2018). According to van Wegberg et al. (2018), since transactions can potentially be linked to illegal activities, enhanced technology associated with cryptocurrency can break the link between cryptocurrency transactions and illegal money laundering.

Financial Crimes

As shown in Figure 1, financial crime is defined as any crime related to finances, such as fraud, theft, tax evasions, money laundering, and terrorist funding carried out by either an individual, an organization, or a group of people (Houben & Snyers, 2018). It has led to wide-spread distress for individuals, organizations, and financial institutions (Jung & Lee, 2017).

Money Laundering

Money laundering is the process of obtaining illegal funds and allowing criminals to control their money (Kumar, 2012). It is a severe global crime as it affects the financial system's integrity and stability, eventually impacting countries' economic stability (Mabunda, 2018). According to Cao (2019), cryptocurrency has created a haven for money laundering, making the crime easy as it gets challenging for financial institutions to relate transactions to criminal activities. Money launderers use numerous ways to accomplish their tasks as they are becoming skilled in deploying new techniques to perform illegal activities (Abel & MacKay, 2016).

One of the banking institutions’ enormous financial risks is money laundering because banks struggle to accurately to assess it at the beginning (Isa et al., 2015). In a case study by the

Financial Action Task Force (Financial Action Task Force [FATF, 2018b), Altaf Khanani illegally laundered billions of dollars to fund illegal drug dealings, weapons dealings, and many terrorist groups. Similarly, in another case study by the FATF (2018b), money was laundered to support a criminal proceeding in Nigeria, where the individual received funds and distributed it over multiple accounts with 12 fraudulent wire transfers within six weeks.

Impact of Cryptocurrency on Money Laundering

The increase in different cryptocurrency types noted a 6-fold increase in financial crimes from 2015 to 2018 (Malwa, 2018). Nowadays, cryptocurrency is commonly used in financial and cybercrimes such as money laundering, tax evasion, and terrorism, where the criminals do not need to reveal their identity, resulting in difficulty for banks to detect and investigate money laundering (van Wegberg et al., 2018). CipherTrace states that misuse of funds from cryptocurrency holders caused around $4.3 billion in losses in 2019 (Alexandre, 2019). Due to the advanced technological features of cryptocurrencies, financial institutions have been facing obstacles in combatting cryptocurrency crimes since lack of understanding of the system constraints banks and the agency's ability to battle money laundering (Arias-Oliva et al., 2019).

Financial Regulation and Acts

Financial institutions, such as banks, have regulations that help them regulate money laundering and identify suspicious activities. Anderson and Anderson (2015) noted that anti-money laundering laws such as BSA/AML help banks identify suspicious account activities and report them. The Bank Secrecy Act created by the Financial Crimes Enforcement Network (FinCEN, n.d.) aims to help the US banks prevent money laundering by making the process difficult. Similarly, the Anti-Money Laundering Act was created to identify and report suspicious transactions to fight money laundering and other frauds (Kemal, 2014). Likewise, the Sarbanes-

Oxley Act was created to help banks identify illegal securities fraud, wire fraud, and bank fraud by ensuring adequate controls are taken in the banking institutions (Morelli, 2015). This act forces banks to hire auditors who oversee methods implemented for addressing bank accounting and auditing issues (Falanga, 2006).

However, due to the increase in cryptocurrency and money laundering activities, regulations are not up to par (Anderson & Anderson, 2015). Although BSA and AML laws have been successful in fighting against money laundering and terrorist financing, criminals are steps ahead of regulations as they try to navigate around reporting thresholds to avoid identification (Anderson & Anderson, 2015). In response to constant changes in the money laundering process and criminal's ability to defraud, banks have doubled their staff in the financial crime unit by 30% but adding to banks' annual cost by up to 2%, totaling approximately $100–200 million each year (Durner & Shetret, 2015). Given the pseudonymous nature of cryptocurrency transactions, BSA and AML compliance are at risk, making it challenging to identify suspicious activities (King, 2015). Furthermore, new advanced technologies such as cryptography and computer science associated with cryptocurrency have enhanced programs that enforcement entities have not yet fully caught up to (Rueckert, 2019).

With the absence of the appropriate regulatory oversight, cryptocurrency has increased money laundering schemes, moving money smoothly without any challenges (Cumming et al., 2019). Following the lack of regulations, cryptocurrency schemes are subject to the security breach's legal risk (Cvetkova, 2018). Cryptocurrencies and blockchain technology have gained so much popularity that the government cannot merely forbid them, but advanced regulation and supervision should be created to safeguard the financial system to avoid financial institution damages (Spithoven, 2019). These relationships are presented in Figure 1.

Data Collection

Data to support the study was collected from case studies and from interviews with bank personnel who are certified money laundering risk specialists by the Association of Certified Anti-Money Laundering and specialize in the BSA/AML Laws. The expected findings helped answer research questions on financial crimes risks and challenges faced by banks when dealing with cryptocurrency, how banks can identify those activities, and what regulations or acts can help banks minimize the financial risk caused by cryptocurrency.

Definition of Terms

Anti-money laundering. According to Savona and Riccardi (2019), anti-money laundering is a set of laws and policies to control crime and reporting on those customers who are suspected of obtaining funds and laundering.

Bank Secrecy Act. Olsen (2019) defined Bank Secrecy Acts as a comprehensive federal anti-money laundering and counter-terrorist financing that requires financial institutions to surveil their customers by providing their information to Financial Crimes Enforcement Networks.

Commodity Futures Trading Commission (CFTC). Chen (2019) defined the "Commodity Futures Trading Commission (CFTC) as an independent U.S. federal agency recognized by the Commodity Futures Trading Commission Act of 1974, who controls the commodity futures and options markets." Retrieved from https://www.investopedia.com/terms/c/cftc.asp

Cryptocurrency. Kethineni and Cao (2019) defined Cryptocurrency as a decentralized digital currency that was originally designed and developed in 2008 to make a peer-to-peer transaction without bank involvement.

Decentralized. Chuen et al. (2018) defined decentralized in cryptocurrency network as where there is no single group or institution that controls the cryptocurrency network. An algorithm governs its supply, and anyone can have access to it via the Internet.

Financial crime. Houben and Snyers (2018) defined financial crime as any crime related to finances, such as fraud, theft, tax evasions, money laundering, and terrorist funding, carried out by either an individual, an organization or a group of people.

Money laundering. According to Zali and Maulidi (2018), money laundering is a method utilized by criminals to disguise the source of illegally obtained money, usually by transfers involving banks or authentic business without the interference of enforcement agencies or any regulation.

Pseudonymous. According to Dyntu and Dykyi (2018), pseudonymous is when someone sends an amount to someone else, but without any tracking or linking relationship.

Regulation. According to regulation.gov, regulations are the standards and rules that are responsible for governing and enforcing the laws created by the government. Retrieved from https://www.regulations.gov/docs/FactSheet_Rules_and_Regulations_The_Basics.pdf

Securities and Exchange Commission. According to the U.S. Securities and Exchange Commission site, the U.S. Securities and Exchange Commission (SEC) is an independent federal government agency responsible for protecting investors, maintaining fair and orderly functioning of the securities markets, and facilitating capital formation. Retrieved from https://www.sec.gov/about.shtml.

Assumptions, Limitations, Delimitations

Assumptions are important in every research study, as it acts as a guide for conducting research (Cleland, 2017). For this research study, the assumptions focused on cryptocurrency's relation to increased money laundering risks, case studies providing unbiased and reliable data, and the bank employee's understanding of the cryptocurrency-related money laundering transactions. However, the assumptions came with limitations that represented the possibility of a limited number of cryptocurrency-related cases and small bank employee sample sizes, which could have influenced study outcome, impacting the research's conclusion. The research study's scope to interview bank employees, the Director of Financial Investigations & Education at CipherTrace, and analyze case studies were the researcher's delimits.

Assumptions

The first assumption was that cryptocurrency influences money laundering through financial crimes. This assumption was based on thorough literature reviews by the researcher. According to van Wegberg et al. (2018), since cryptocurrency clients do not have to reveal their identities, it presents difficulty for banks to detect any money laundering activities, thus giving rise to cryptocurrency-related money laundering.

The second assumption was the case studies utilized will not be biased towards any group, individual, or financial institution. By manipulating research questions and data collection, including sample recruitment and registration, bias may distort the study results (Galdas, 2017). This assumption ensured that the researcher reviewed literature and case studies to understand the influence of cryptocurrency on money laundering.

The third assumption was that the data obtained from the case studies would be reliable. A detailed analysis of the case studies and their originality would minimize this presumption. Data reliability is important as it provides data consistency, data integrity, and data accuracy (Leung, 2015). Additionally, reliability eliminates biases through data consistency, influencing the study findings (Noble & Smith, 2015).

The last assumption was that the bank personnel interviewed will fully understand the interview questions and respond to their ability best. This assumption was based on a detailed analysis of the questions of semi-structured interviews with bank staff in the development of useful study information. The semi-structured interview questions are the most frequent qualitative data source guided by flexible and supplementary follow-up questions, collecting open-ended rich data where the participant's thoughts and feelings are explored to the best of their ability (DeJonckheere & Vaughn, 2019).

Limitations

Since cryptocurrency is still a new system, case studies had potential limitations identifying all cryptocurrency-related money laundering and other financial crimes. Additionally, very few companies specialize in cryptocurrency-related financial crimes, so the case study sample size was limited. Therefore, the researcher reviewed several case studies and thoroughly evaluated each case study. The impact of cryptocurrency money laundering negatively affects the banks and the economy (Kumar, 2012); however, with limited data to show the negative effect on the economy, the data sample size could be small. The loss in revenue, the effect on the socioeconomic cost, the effect on currencies, interest rates, capital flows, interest, exchange rates, economic instability, and risks to privatization are some of the few economic effects to watch out for a while reviewing articles (McDowell & Novis, 2001).

The sample size from the AML/BSA risk specialists was small, as not many bank personnel were able to share and describe their experiences or disclose bank information. Moreover, since cryptocurrency limits the bank's ability to track the movement of funds and comply with anti-money laundering laws (Cheng, 2018), the data gathered from bank personnel was not rich and reliable. For this limitation, open-ended semi-structured interview questions were developed, leading to other effective and probing questions, obtaining richer, more in-depth information from the participants encouraging them to speak more freely. The open-ended semi-structured interview questions closed the gap and limit on sample size. This was also an example of saturation, where one does not have to interview a large number of participants to gain new information as enhancing or change the findings of a study (Weller et al., 2018).

Delimitations

This qualitative study's scope was to focus on case studies as it is more productive and of greater depth compared to other experimental designs, such as ethnography, phenomenology, and grounded theory (Starman, 2013). Each research question chosen helped answer banks' challenges when dealing with cryptocurrency and financial crimes such as money laundering, ways to identify and report suspicious activities, and how banks can minimize these financial crimes. The research participants were certified bank representatives who specialize in BSA/AML Laws. The case studies from CipherTrace Company were studied. CipherTrace identifies money laundering and allows for regulatory monitoring of exchanges of cryptocurrencies, and works with banks to minimize financial risks and exposure. Other financial institutions did not qualify for this study, as not all have case studies or were willing to share case studies or confidential data.

Significance of the Study

This qualitative study's findings are significant for banks to set additional rules and regulations to help identify suspicious money laundering activities. Due to cryptocurrency’s pseudo-anonymity characteristic, banks have struggled to combat financial crimes such as money laundering (Lansky, 2018). The popularity of cryptocurrency justifies the need for additional regulations as, currently, it does not provide the comprehensive framework needed (Massad, 2019). This study intended to help banks minimize the risk of financial crimes and the challenges posed by cryptocurrency resulting in laundered money. Hopefully, the banks that apply the recommended regulations found in this study will have the capability to train their employees more effectively and efficiently in identifying financial crimes and reporting suspicious activities about cryptocurrency.

Reduction of Gaps

The United States Congress has passed anti-money laundering laws such as the Bank Secrecy Act, which implements the Anti-Money Laundering rules that all banks are supposed to comply with. According to the FinCEN (n.d.) the anti-money laundering law was established to protect financial institutions from financial crimes like terrorist funding, money laundering, and other criminal activities in 1970. Financial institutions are actively tracking the rise in cryptocurrency activities; however, due to regulatory gaps in the cryptocurrency system, it is nearly impossible for banks to eliminate money laundering (Massad, 2019). This qualitative study aims to increase the bank's understanding and knowledge of cryptocurrency, leading to money laundering, reducing the gap between money laundering challenges, and increasing understanding of regulations and the types of technology utilized to launder the money. The knowledge behind the advanced technology to crack encryption software can allow the banks to solve challenges against money laundering and increase efficiency gains in clearing cryptocurrency settlement (Bech & Garratt, 2017).

Implications for Biblical Integration

Money laundering simply means to obtain illegal money. According to the bible, illegal money is greed, the greed that only “brings destruction” (Bernock, 2019). As 1 Timothy 6:9-10 states, “those who want to be rich, fall in the temptations, ruining others, wandering away from the faith." Accordingly, money laundering performed for one's benefit and greed has made the society self-centered, defeating God's purpose of business on earth. Due to money laundering, banks, government, and many businesses tend to spend money on investigations and on regulations, which can be costly and time-consuming. According to Bedrock (2019), greed makes individuals self-centered, unsatisfied, and increases their appetite for money, which gives them short-lived happiness. As Proverbs 20:17 states, "Bread gained by deceit is sweet to a man, but afterward, his mouth will be full of gravel." The advanced technology supposedly used to enhance the peer-to-peer transaction has been misused in money laundering (Dion-Schwarz et al., 2019). The Bible recommends the practice of technology to connect to the audience and the community, not to conduct fraud or mislead (Nickel, 2019). Therefore, government regulations, laws, and rules are needed to avoid such criminal acts. Romans 13:1-2 says, "Obey the government, for God is the one who has put it there. So those who refuse to obey the law of the land are refusing to obey God, and punishment will follow."

Relationship to Field of Study

Finance is one of the most critical features of any financial institution. It is a term that describes the study of money, helping acquire, and manage funds, and increasing the financial economy. However, the same financial industry can be in danger if money laundering is not regulated. Money laundering, known as illegally obtaining money, harms the financial industry by disguising the source of illegal funds and creating a severe threat to the banks and the economy (Zali & Maulidi, 2018). Financial crime in the form of money laundering has a significant effect on the economy by making the financing industry fragile, encouraging crime and corruption, and affecting economic growth and productivity (Hetemi et al., 2018). Effective and explicit anti-money laundering regulations can help reinforce various laws and regulations and help sustain the financial industry (Lansky, 2018).

The financial sector is negatively affected by money laundering associated with cryptocurrency. According to Cumming et al. (2019), cryptocurrency has already impacted the bank's competitiveness and reduced its revenues and profits. If widely accepted, pseudonymous and decentralized cryptocurrency could threaten banks’ long-term viability and financial network (Perkins, 2018). As the current financial system is complex, the decentralized financial system through cryptocurrencies could be more straightforward, adding to various types of financial products, making the process simple for customers (Ito et al., 2017). The authors further add that numerous financial product choices will further weaken the current complex financial system.

The emerging and innovative technology utilized by cryptocurrency could add expenses to the financial industry, limiting their ability to track fund movement and increase financial crimes (Rueckert, 2019). Unconventional cryptocurrency technology may add to the financial sector's expense to modify or adapt to new products to attract and retain clients, reduce net interest margin and revenues from their fee-based products and services. Many governments around worldwide are looking to monitor cryptocurrencies for this purpose, offering an opportunity to audit their vulnerabilities (Dyson et al., 2018).

Summary of the Significance of the Study

This qualitative study's findings can enable banks to set additional rules and regulations to help identify suspicious money laundering activities. By minimizing the risks of financial crimes through recommended regulations, banks can combat money laundering triggered by cryptocurrency. Although Anti-Money Laundering laws are available, the rise in cryptocurrency usage needs additional regulations to reduce the gap and lack of understanding of the relationship between the Anti-Money Laundering laws regulations and financial crimes. There needs to be better communication between the financial industries and employees regarding the risks, damages, and harms caused by cryptocurrency.

A Review of the Professional and Academic Literature

Money laundering is a crime that plays a critical role in the distribution of illegally attained money. The entire process efficiently moves funds from one location to another by disguising illegal money and converting it into legitimate assets (Qureshi, 2017). Global Financial Integrity's December 2015 study reported that $7.8 trillion in money laundering was lost by developed and emerging economies from 2004 to 2013 (Kepli & Nasir, 2016). In the U.S. during the same period, this number reached $2 trillion (United Nations [UN], n.d.). Financial institutions are the primary target of money laundering crimes, as banks are essential for transferring money between multiple entities (Ardizzi, 2014). However, due to weak regulations and many financial institutions' inability to fully understand the money laundering process, it has hindered the institutions to accurately monitor money laundering (Kemal, 2014). Additionally, the banks' regulatory compliance program's weakness and breach challenge the banks' ineptness in identifying money laundering cases (Saperstein et al., 2015).

Since cryptocurrency is unrecognized by banks, they do not worry about being a complaint against their digital currency programs (Battistini, 2016). Due to the nature of cryptocurrency being undetected, with no identity check, coupled with enhanced technology and the banks' failure to detect money laundering, cryptocurrency has become common amongst criminals conducting unlawful activities (Cvetkova, 2018). For example, the cryptocurrency Monero has a privacy feature of being efficient in mixing previous invalid transactions to complicate the current transactions (Burrus, 2018). This practice has increased banks' challenges of investigating money laundering as criminals can easily hide financial crime footprints by defending against their transactions and actions of being non-financial (Dyson et al., 2018). Furthermore, the technical process associated with cryptocurrency crime challenges banks' implementation of an appropriate anti-money laundering guideline (Houben & Snyers, 2018). Consequently, the gap and fragility in the current anti-money laundering and bank secrecy acts have limited the banks to trace and regulate cryptocurrency, resulting in increased money laundering risks (Obie & Rasmussen, 2018).

Cryptocurrency and Financial Risk Crimes

Money Laundering

Money laundering is defined as a method utilized by criminals to disguise the source of illegally obtained money, usually by transfers involving banks or authentic businesses without the interference of enforcement agencies or any regulation (Zali & Maulidi, 2018). The method involves the process of gaining illegal money, causing many ill-effects to the economy by increasing crime and corruption, and negatively impacting and weakening the financial institutions (Arafeen et al., 2016). According to Gjoni et al. (2015), the name “money laundering” came from the twentieth century when criminals used laundry businesses to rationalize large amounts of illegal income from regulated agencies as legit. Anderson and Anderson (2015) described money laundering as taking illegal money and “washing” it to appear as legal. Masjedi (2015) characterized money laundering as a secondary offense where the crime is organized by crime experts and run in a specific geographic area, eventually impacting the country’s economic and financial stability.

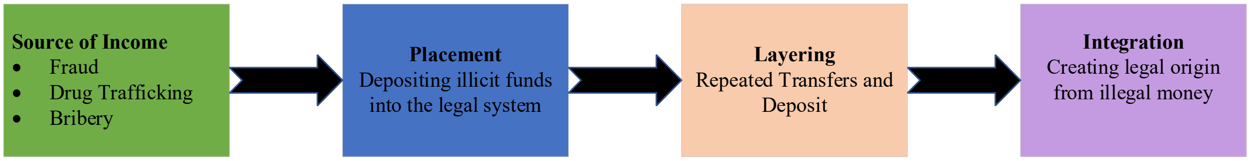
Every year, money laundering practices increase as it incorporates various methodologies such as digital money transfers, cash transactions, credit card payments, offshore property buildings, wire transfers, bulk cash smuggling, and trade-based money laundering (Qureshi, 2017). The United Nations Office on Drugs and Crimes projected that each year the amount of money laundered is 2-5% of global GDP or $800 billion-USD $2 trillion (UN, n.d.). Qureshi (2017) added that money laundering invites social costs advancing the promotion of other crimes, including drug trafficking, smuggling, arms trafficking, and terrorism financing.

Stages of Money Laundering

According to Zali and Maulidi (2018), money laundering is divided into three phases: (a) placement, (b) layering, and (c) integration. These stages can happen simultaneously or appear as a separate transaction (Cindori & Slović, 2017). The three stages of money laundering comprise illicitly attained money from fraud, drug trafficking, and bribery, such as a legal fund that enters the economic cycle (Gjoni et al., 2015). Figure 2 below shows the different stages of money laundering.

Figure 2

The Three Stages of Money Laundering


Source of Income
• Fraud
• Drug Trafficking
• Bribery
Placement
Depositing illicit funds into the legal system
Layering
Repeated Transfers and Deposit
Integration
Creating legal origin from illegal money

Note. Stages of Money Laundering

First Stage. Masjedi (2015) explained that placement is depositing the illegitimately gained funds into a legal, financial system at the first stage. The depositing stage converts the funds into an appropriate form to avoid law enforcement suspicion by inserting it into the financial flow (FATF, 2018b). However, the placement stage is only necessary if the cash obtained will be deposited into the financial system (Kepli & Nasir, 2016). For instance, the use of illegally obtained money to pay for illegal immigrants, purchasing assault weapons, and bribery purposes does not require the placement step, as the money does not need to go through banks or any financial institutions.

Second Stage. During this stage, layering, dirty money will be filtered through various banks to make the funds untraceable (Anderson & Anderson, 2015). The step is called layering as different layers of financial transactions go undetected, complicating the money trail to hide the source of funds (Kepli & Nasir, 2016). Sundarakani and Ramasamy (2013) added that once the placement step is completed, the layering step separates the illegal money by fulfilling the objective of concealing the audit trail and making it difficult for the regulators to trace the proceeds.

Third Stage. The last phase, integration, helps moves the illegitimate money back into the mainstream economy, mainly primarily to be used in business (Masjedi, 2015), for example, investing money in foreign financial institutions through financial or commercial operations (Brenig et al., 2015). Gilmour (2014) explained that the integration stage is when “black money” can be used to make a legal purchase, where the money appears as a legit business income. Areas of property dealing, fraudulent loans, integrating funds in banks, and presenting false import and export invoices are integration methods.

Money Laundering Indicators

Money laundering is indicated by many as suspicious activities such as a “sleeping” account containing minimum funds but suddenly receiving a large deposit or a business transferring a large amount of money with no legitimate business purpose (Beqiri & Beqiri, 2018). Additional money laundering indicators are incomplete or inconsistent information or reluctance to provide information or negative information about a client (Murray-West, 2017). Politzer (2019) described the red flag for money laundering as the unusual suspicious and unverified identification documents, especially customers' inability to explain their transactions or the lack of transparency on the wealth generated.

In a study conducted by Soudjin (2015), clients do not reveal their identity when money laundering occurs, especially when a large sum of money is involved. Importantly, money laundering transactions do not follow a pattern, and usually, there is a large amount of cash from unexplained sources, where multiple individuals send funds to a single beneficiary (Soudjin, 2015). During the money laundering process, individuals keep multiple accounts under the same name, depositing cash in it and creating a large sum of deposit (Alsaif & Ramo, 2018). Another money laundering indicator is when a large volume of money is wired to and from banks in countries known for money laundering and illegal financial irregularities (Alsaif & Ramo, 2018).

Economic Effects of Money Laundering

The United States Government has estimated that annually around $300 billion of proceeds gets generated in money laundering (U.S. Department of the Treasury, 2018). Most of these transactions come from fraud, drug dealing, organized crimes, and corruption. These crimes generate the bulk of illicit funds in the United States, which is integrated into the financial economy, impacting the country’s economy (Mugarura, 2016). The United States is seen as an attractive destination for illegal funds generated overseas (U.S. Department of the Treasury, 2018). Financial crime has damaged the economy by deformation of consumption, artificial price growth, and negatively affecting the growth rate (Gjoni et al., 2015).

Similar findings by Beqiri and Beqiri (2018) stated that money laundering negatively affects a state's budget by decreasing budget inflows from taxes and consumers. This decline in the state budget reduces state investment opportunities and capital investments, eventually resulting in detrimental economic development. The authors also mention that a country's privatization is affected as money launderers usually utilize privatization to help clean illegal business and give a country a bad reputation. The negative reputation from money laundering diminishes legitimate global opportunities while increasing the rate of international crimes, affecting a country's economic growth and development (Sarigul, 2013). These hazardous effects directly affect an economy by impacting legitimate businesses where legal transactions become less attractive for foreign investors who are suspicious that every business deals with money laundering (Gjoni et al., 2015).

As more funds are generated from money laundering, the process negatively affects a country's economy through disruptions and instability, leading to a deterioration of the financial markets, reduction in government revenue, reduction in government control over economic policies, and destruction of the private sector (Masjedi, 2015). Money launderers are finding new ways to launder money, while developing financial centers with uncontrolled regulations are helpless to do anything (Financial Action Task Force [FATF], 2018a). The promotion of corruption and bribery through money laundering demoralizes a country's economy, as money laundering is the most significant hurdle leading to lifting people from poverty and hardship by diverting from public resources (Ahmad, 2019). For this reason, one of the most substantial economic costs of money laundering as corruption is that it damages the reputation and international consequences of a country in terms of its development and progress (Arafeen et al., 2016).

Consequences of Money Laundering on Financial Institutions

Banks and other financial institutions are the hubs for finance flow, and as a result, they have been direct victims of money laundering and terrorist financing (Sundarakani & Ramasamy, 2013). Criminals heavily utilize the banking sector for terrorist funding by undermining the banks' integrity (Sundarakani & Ramasamy, 2013). Hence, the banks' cost of investing in to fight against the criminal process has increased immensely due to technology investment in trying to identify money laundering transactions. As banks' scale and reliability on money laundering increase, banks' failure to understand the crime results in severe reputational risks for banks where foreign investors and customers lack trust in the financial institutions (Oluwadayisi & Mimiko, 2016). Banks tainted reputation due to money laundering makes customers lose confidence and value in the financial institutions, fearing their funds' safety, leading to funding withdrawal (Omolara et al., 2018).

Intentionally or unintentionally, banks are part of criminals obtaining and concealing illegal money. Arafeen et al. (2016) presumed that many banks unintentionally become part of money laundering with numerous fund withdrawals, causing bank liquidity problems, loan losses, asset seizures, and loss of profits. Banks that intentionally rely on criminal's earnings also encounter significant liquidity, asset, and operation problems as money moves from one bank to another, appearing and disappearing through wire transfers (Sarigul, 2013).

Zali and Maulidi (2018) stated that criminals use a "legal" trick with the help of financial employees as "dirty" money is moved into different accounts as soon as law enforcement becomes aware of any possible money laundering. As such, banks end up paying fines due to the lack of stringent anti-money laundering policies. For instance, Standard Chartered Bank was fined $340 million for breaking the United States money laundering laws while managing an Iranian customer's transactions (Isa et al., 2015). The United States Government Accountability Report (2016) investigated that from January 2009 to December 2015, federal agencies evaluated about $5.2 billion for bank secrecy act and anti-money laundering law violations and collected about $5.1 billion in penalties and fines from various banks in violation of the regulations. These bank penalties lead to an attenuating financial sector's role in the growing economy that serves as a bridge between the government and the people (Sundarakani & Ramasamy, 2013). Table 1 shows penalties paid by some US banks for their failure in reporting suspicious accounts in violation of the bank secrecy act and anti-money laundering compliance and regulations.

Table 1

BSA/AML Penalties Paid by USA Banks

Bank	Date	Penalty Paid ($)
HSBS Bank	12/11/12	1.92B
JPMorgan Chase	01/07/14	2.05B
Banamex (Citigroup)	07/22/15	140M
Banamex (Citigroup)	05/22/17	97M
Citibank NA	01/04/18	70M
U.S. Bank NA	02/15/18	613M
California Pacific Bank [a]	10/17/19	225,000

Note. From "Cleaning up money laundering compliance aftermath", by BE Banking Exchange, 2018, (http://m.bankingexchange.com/bsa-aml/item/7399-cleaning-up-money-laundering-compliance-aftermath).

[a] From BSA-AML Civil Money Penalties, by BankersOnline.com, 2019, (https://www.bankersonline.com/penalty/penalty-type/bsa-aml-civil-money-penalties)

Ways to Tackle Money Laundering

Apart from anti-money laundering policies and bank secrecy act, many economic laws, tax laws, and financial regulations have been established to tackle money laundering (Rueckert, 2019). While the government is adding additional explicit regulations in terms of anti-money laundering regulations, the purpose is to strengthen the current and existing laws while adding new methodologies in fighting money laundering (Ferwerda et al., 2019). After the September 11th attacks, the government has added additional regulations to contest money laundering, where the cooperation between the authorities and the financial organization can be effective (Fernandez, 2014). Even the U.S. regulatory agencies have encouraged banks and other financial institutions to try and adapt new technologies to combat money laundering (Rubenfeld, 2018). These innovative technologies act as a safeguarding tool against an array of threats by money laundering. In particular, the enhanced technologies can expose and fill existing gaps where banks can identify suspicious accounts more effectively (Rubenfeld, 2018). Alsaif and Ramo (2018) concluded that a lack of technology can cause a high rate of money laundering in many banks by affecting the banking sector's power infrastructure. Many banks' advanced technology and robotics have reduced the number of false alerts for suspicious activities (Curry, 2019). The utilization of the internet and enhanced and updated technology skills can easily identify suspicious and false transactions (Kemal, 2014).

Agencies require a structured training of all anti-money laundering staff, demonstrating the commitment and ability to know what to look for (Curry, 2019). Specifically, a senior management's primary role as the implementer of the policies is to communicate and deliver compliance policies, demonstrating the vision to fight money laundering. Curry (2019) also suggested effective employee training in identifying suspicious transaction reporting and reiterating the importance of ethical and compliant culture can combat money laundering. Kemal (2014) discovered that implementing anti-money laundering techniques and employee training can significantly reduce money laundering practices. The rigorous training on "Know Your

Customer" can help anti-money laundering staff match the suspicious behavior sooner in the money laundering process (Battistini, 2016).

Data mining techniques utilized by anti-money laundering specialists can help them recognize questionable patterns, analyze the customer's "real-time", and detect fraud as part of a routine financial audit (Salehi et al., 2017). Salehi et al. (2017) further argued that the clustering technique can help the bank staff detect suspicious transaction patterns by grouping transactions with bank accounts in different clusters with most parallels. Rohit and Patel (2015) indicated that the clustering-based approach helps bank staff build patterns of suspicious transactions and detect risk patterns of clients' accounts. The model-based approach has also been identified as a potential approach in tackling money laundering, where the proposed use of transaction flow analysis and customer behavior analysis helps identify the customer's money laundering (Rohit & Patel, 2015).

Money Laundering Regulations

Currently, there are two financial regulations, anti-money laundering (AML), and bank secrecy act (BSA). Anti-money laundering refers to preventing criminal manipulation of financial sectors to conceal and control illicit proceeds and funds (Miller & Rosen, 2017). The bank secrecy act's purpose is to make money laundering difficult by preventing US banks from becoming victims of unknown crimes such as money laundering (Anderson & Anderson, 2015). Both laws were established by FinCEN (n.d.) to protect and prevent financial institutions from criminal activities leading to adverse effects on the financial factor (Howard, 2017). The FATF created these regulations in 1990 to combat money laundering, and according to Kemal (2014), these regulations are the best way to fight money laundering.

AML. Anti-Money Laundering (AML) law was established in 1970 to safeguard financial institutions from financial crimes such as terrorist financing, money laundering, and other illicit activities (FinCEN, n.d.). The AML law aids in detecting and reporting suspicious activities, including felonies to money laundering and terrorist financing (Miller & Rosen, 2017). Tsingou (2017) explained that AML compliance is a regime built to target criminal proceeds based on coordination and competition among regulation and law enforcement professional networks in the formulation of AML standards.

BSA. Bank Secrecy Act (BSA) is designed to help identify the source, volume, and the conversion to illegal currency (FinCEN, n.d.). Through this act, the banks are required to report cash transactions over $10,000 using the Currency Transaction Report to identify individuals conducting transactions and maintain a paper trail by keeping appropriate financial transactions (FinCEN, n.d.). The Office of the Comptroller of the Currency [OCC] (n.d.) elucidates that banks are required to establish effective BSA compliance, effective customers due diligence systems, and an effective suspicious activity monitoring and reporting process.

Financial Crimes

According to Eisenberg (2017), financial crime is any offense involving fraud or misconduct associated with the financial market or sector. The offense leads to distress for individuals, organizations, and financial institutions, only benefiting oneself (Jung & Lee, 2017). Per Nice Actimize (2019), financial crime is a regulatory or monetary act against financial sectors to manipulate and cause threats and instability of the system. Based on the literature review by Lord et al. (2018), the most common types of financial crimes are money laundering, tax evasion, terrorist activities, theft, and bribery. The financial institutions have been one of the biggest financial crime victims as ATMs, credit and debit cards, and wire transfers easily get accessed using bank accounts (Hasham et al., 2019). Sidanius (2018) found that many organizations have lost an average of 3.5% of their global turnover as a result of financial crimes, where the World Economic Forum shows that in 2018, financial crimes rose to a trillion-dollar industry, where companies spent about $8.2 billion on AML controls in 2017 (Hasham et al., 2019).

Relationship Between Financial Crime and Money Laundering

Money laundering is common for criminals, be it drug dealers, terrorist groups, or arms traffickers (Sarigul, 2013). To fund illicit activities, terrorist groups launder money through financial sectors such as banks. Stankiewicz (2015) affirmed that money laundering sustains and enables the extension of the criminal network and their activity globally, allowing criminals to enjoy profit without jeopardizing their sources (Sarigul, 2013). The connection between money laundering and financial crime negatively impacts the countries laws, economy, and damages the financial system. In addition, money laundering encourages and promotes corruption and bribery, affecting the financial institutions in addition to the economic sectors (Gjoni et al., 2015). Money laundering and corruption are closely linked as corruption hinders the effective use of the anti-money laundering system, aiding corruption in hiding money, and bribing the financial institutions against regulated actions towards them (Kemal, 2014). The relationship between corruption and money laundering helps generate profit, where money laundering allows criminals to hide stolen money and enables them to enjoy their corrupted earned money without the fear of being prosecuted (Mugarura, 2016). A study by Compin (2018) validated that since the traceability between terrorist money remains meek, the terrorist groups are increasingly making use of money laundering to raise the obsessive theme of "terror." Money laundering and terrorist financing have numerous similarities, where both by nature are private financial activities on an international scale (Compin, 2018). The similarity and connection between terrorist funding and money laundering results in the criminals providing terrorist organizations money through “laundered” funds, utilizing the secrecy and mobility attributes of both money laundering and terrorist financing schemes with no requirement of concealment or integration justice (The Organisation for Economic Co-operation and Development [OECD], 2019).

Cryptocurrency

Characteristic of Cryptocurrency

Cryptocurrency is characterized as a digital asset designed to work as a medium of exchange where users can send and receive money without the involvement of banks. (ElBahrawy et al., 2017). Furthermore, digital currency allows for exchanging of transactions and value without third-party oversight (DeVries, 2016). Many users find cryptocurrency as a convenient way to avoid financial fees associated with the traditional banking system (Peprah et al., 2018). This digital currency uses cryptography to transfer and exchange digital tokens securely by applying the currencies distributed and decentralized features (Gikay, 2018). Delgado-Segura et al. (2018) also complemented that security and robustness are some of the most critical cryptocurrency characteristics by utilizing cryptographic techniques and a decentralized approach. Cryptocurrency is a digital currency created by "mining and solving automatically generated mathematical puzzles towards processing users' transactions" (Gikay, 2018, p. 4).

Some of the unique features of cryptocurrency are their inability to be centralized to any authority with no physical representation or any tangible assets (Ferreira & Pereira, 2019). The digital currency not issued by a central authority is highly secured as it uses cryptography techniques to identify and verify transactions and is transparent in storing transactions in detail while keeping the users anonymous (Yuneline, 2019). The network's decentralized feature is based on the fact that there is no single group that controls it, making the digital assets available to those who want it (Chuen et al., 2018). Besides, blockchain's decentralized characteristic creates the idea of a token economy in which revenue gets allocated to the actual service users who create value (Lee, 2019).

The pseudo-anonymity capability of cryptocurrency makes transactions publicly available but relatively anonymous. This method assures anonymity, including transactional integrity, and non-repudiation (Litchfield & Herbert, 2018). Their actual names cannot easily identify the users who follow the relevant rules, but as account numbers, only allowing partial identification voluntarily or when needed (Lansky, 2018). Some cryptocurrencies try to attain full anonymity, such as Monero and Bitcoin use protocol, allowing users' identities to be seen by the sender and recipient only, where Dash tries to mix cryptocurrency units with different owners, targeting full anonymity (Lansky, 2018).

History of Cryptocurrency

Bitcoin is one of the first cryptocurrencies invented in 2008 by a programmer Satoshi Nakamoto (Hassani et al., 2018). Initially, it was not of interest to the general public, as only cryptographers, hackers, and mathematicians understood its importance (Rose, 2015). The Bitcoin network is supported by computers, where every time a transaction is made, the nodes in the network verify the transaction in order to avoid double transactions (Turpin, 2014). Although Bitcoin was introduced in 2008, it gained interest in the mainstream media in 2012 (Gandal & Halaburda, 2016). The United States has shown a positive approach towards the acceptance of cryptocurrency, and for example, Dish Network has already started accepting payment on Bitcoins and making its way to other U.S. derivative markets (Thakur & Banik, 2018). Currently, the market for cryptocurrency has reached about $260 billion as of May 2019 (Ferreira & Pereira, 2019). After Bitcoin's acceptance since 2009, around 1,500 other cryptocurrencies have entered the market, of which around 600 are actively in trade today (ElBahrawy et al., 2017). Up until April 10, 2019, 1027 new currencies were initially introduced, out of which 458 currencies folded.

Although Bitcoin is the largest cryptocurrency, Namecoin is the first decentralized domain cryptocurrency, with Ethereum as the first most active cryptocurrency (Liang et al., 2018). The emergence of Ethereum has been close to Bitcoin, as the upcoming digital currency has the additional powers of "Turing-completeness, value-awareness, blockchain-awareness" (Jani, 2017, p. 1). By the end of 2013, all virtual currencies were based on the Bitcoin protocol, providing alternatives to Bitcoin, and trying to fix Bitcoins shortcomings, often called altcoin (Gandal & Halaburda, 2016). However, Rose (2015) thought that Bitcoin is still the most popular cryptocurrency, and the majority of the merchants use and support this virtual currency. Other common and highly valued cryptocurrencies are Ripple (XRP), Litecoin (LTC), Bitcoin Cash (BCH), Dash (DASH), and privacy coins including ZCash (ZEC) and Monero (XMR; McBride & Gold, 2019). As of February 7, 2020, Bitcoin has a market capitalization value that exceeds $177 billion. Table 2 below shows the market capitalization of the top 5 cryptocurrencies in the market.

Table 2

Cryptocurrency by Market Capitalization as of 07 February 2020

Rank	Cryptocurrency	Market Cap ($)	Established
1	Bitcoin	177B	2009
2	Ethereum	24B	2013
3	XRP	12B	2012
4	Bitcoin Cash	7B	2011
5	Tether	5B	2017

Note. From "Top 100 Cryptocurrencies by Market Capitalization" by CoinMarketCap, 2019, (https://coinmarketcap.com).

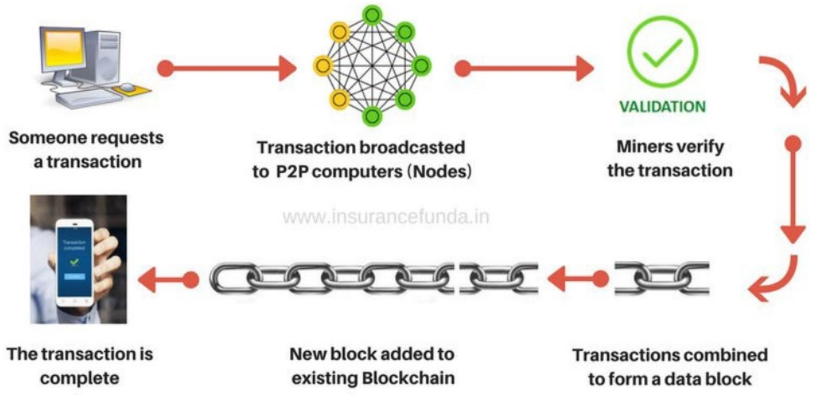
How Cryptocurrency Works

Cryptocurrency works when transactions are confirmed (Thakur & Banik, 2018). Initially, the transactions are sent between peers, and the funds get transferred, which are encrypted to the cryptocurrency network (Afzal & Asif, 2019). Secondly, the transactions get recorded on a digital public ledger known as the blockchain, which then makes the digital currency available to the owner, who owns a unique set of keys (DeVries, 2016). The transaction can be forged until a confirmation is received or pending; however, as soon as the transaction is received by the network and confirmed, there is no reversing back, nor can the transaction be forgeable anymore (Thakur & Banik, 2018). The whole process involves the initiators, codebase, programmers, miners, intermediaries, and customers (Spithoven, 2019).

The initiator or the "cryptocurrency user" creates a transaction whose information is received by the network, which validates the transaction becoming part of the blockchain Mittal et al. (2018) as depicted in Figure 2. The codebase is the software where the rules for sending, receiving, and recording value using cryptographic methods are enclosed (Spithoven, 2019). The programmer makes and promotes the currency, coordinating the protocol while regulating the cryptocurrency (Abramowicz, 2016; Spithoven, 2019). The miners provide network security by proof of work or proof of stake, where the middlemen provide finance, and the customers feed the network (Spithoven, 2019).

Figure 3

Cryptocurrency Workflow


Someone requests a transaction
Transaction broadcasted to P2P computers (Nodes)
VALIDATION
Miners verify the transaction
www.insurancefunda.in
The transaction is complete
New block added to existing Blockchain
Transactions combined to form a data block

Note. How Bitcoin Transaction Works. From “Atomic Wallet, 2019.” (https://atomicwallet.io/cryptocurrency-wallet)

Benefits of Cryptocurrency

Cryptocurrency has been drawing significant interest due to its key advantages, such as decentralization, pseudo-anonymity, security, and automation (Spencer, 2017). Since cryptocurrency uses advanced technology, they offer alternatives to traditional banking such as zero transaction fee, weak regulations, anonymity, and cash-like electronic transfers, which solves the issue of involving a trusted third party (Chuen et al., 2018). The flexibility to exclude each transaction's supervision, setting up a digital wallet with little or no background checks, and with no bank applications, makes the digital currency system better than the banks (Ng &

Griffin, 2018; Peprah et al., 2018). According to Thakur and Banik (2018), cryptocurrency makes the fund transfers easier, with a minimal processing fee, allowing the users to avoid the high fees charged by most banks, making any settlement faster, allowing the cryptocurrency holder to send what is needed with secured transactions. According to DeVries (2016), in countries where the inflation is high with a high population of unbanked citizens, cryptocurrency such as Bitcoin performs better where the need for banks, background checks, and bank applications are eliminated; from 2014 to 2015, South America has seen a big jump in Bitcoin transactions, increasing to 510%.

As the Internet of Things (IoT) and artificial technologies develop, the virtual currency can help stabilize and lead to large scale data markets through data security for personal information protection while increasing the validity of artificial technologies (Lee, 2019). Chuen et al. (2018) believed that cryptocurrency has an investment opportunity because it outperforms traditional asset class in terms of the daily return of 8.54. Businesses also see the benefits of quicker international transactions compared to traditional transactions, connecting buyers and sellers, and eliminating traditional card-based fees (DeVries, 2016).

In contrast, some studies show cryptocurrency as very volatile with fluctuations in prices (Bunjaku et al., 2017). The price fluctuations fear investors investing in cryptocurrency and making it difficult for users to accept and use the digital asset. Hacking is also known to be a threat to cryptocurrency, as the virtual location for storing cryptocurrency can be compromised: thus, private keys of the users can be stolen (Subramanian & Chino, 2015). The authors further observe that the lack of proper infrastructure of the system, where there is no central issuer, can be attacked by miners, gaining complete control of the cryptocurrency market. However, based on these journals, the benefits outweigh the disadvantages, where the easy to use, anonymous and decentralized feature, transparency, and the speed of transaction makes cryptocurrency attractive to the users, willing to take some risks associated with the virtual asset.

Cryptocurrency in Money Laundering

Cryptocurrency holds a vital role in money laundering, where criminals are switching to technology to launder money without having to "Know Your Customer" (KYC) requirements with fewer audit trails (Ng & Griffin, 2018). Given that cryptocurrency transactions are between decentralized networks of users, rather than the centralized networks like banks the cryptocurrency characteristic makes it convenient to conduct money laundering via the network (Campbell-Verduyn, 2018; Dyntu & Dykyi, 2018). To offer further privacy, cryptocurrency clients do not have to reveal their identity; as such, this presents a difficulty for banks to detect any money laundering activities (van Wegberg et al., 2018). Moreover, because the transactions do not have to move through regulated banks, money can freely move without having the purpose or legitimacy of the transactions verified (Forgang, 2019). From 2009 to 2018, approximately $2.5 billion were laundered, and 97% of it was laundered using unregulated cryptocurrency exchanges (Canellis, 2018). The fact that virtual currency is the preferred payment for illicitly obtained drugs and other goods online, criminals are being attracted to it by using it as a money-laundering vehicle (U.S. Department of the Treasury, 2018).

Decentralized and Anonymity

The role of decentralization and anonymity in cryptocurrency is profound as it allows individuals or groups to operate without being detected from authorities (Lansky, 2018). Even though cryptocurrency is not legal in any nation yet, it is highly recognized for its decentralized and anonymity feature capable of altering the financial system (Adeleke et al., 2019). With no central authority, cryptocurrency lacks a central point's oversight, strengthening the planning and controlling, making cryptocurrencies less susceptible to failure (Gikay, 2018). Rueckert (2019) points out that without any central administration to track the users with an indefinite number of accounts, the identification of criminals and money laundering efforts fail. The decentralized technology allows the blockchain to increase the transactions' capacity and security with a faster settlement with no regulatory oversight (Ng & Griffin, 2018). Due to banks' absence, the direct transaction between the peers maximizes the traders' security, making the transaction records for each participant, and data structured and accurate (Hassani et al., 2018).

Although some articles argue that cryptocurrency such as Monero is not entirely anonymous, it still has the characteristics to prevent illegal transactions from being adequately monitored, enabling criminals to get their hands on “clean cash” using cryptocurrency (Houben & Snyers, 2018; Ng & Griffin, 2018). The anonymous transfer and movement of funds make cryptocurrency operation easy, as no person can be identified in the transfer record (McBride & Gold, 2019). The anonymity feature allows criminals to cover their crimes and tracks (Mandjee, 2015). Goodell and Aste (2019) wrote that the possibility of anonymity in cryptocurrency increases money laundering transactions as people value privacy, and the criminals are misusing this privacy. The untraceable virtual currency links the chain of transactions, making it look like they are sent from different addresses, making it tougher for law enforcement to track and regulate (Piazza, 2017).

The combination of decentralized and anonymity features of cryptocurrency attracts criminals' interest in conducting illegal transactions (Brenig et al., 2015). The decentralized and anonymous feature makes the cryptocurrency market vulnerable and remunerative, keeping the trend unaltered (Hassani et al., 2018). Furthermore, this combination leads to an unstable economy and challenges banks to fight money laundering (Mugarura, 2016).

Difficulty in Catching up With Cryptocurrency

Due to the decentralized and anonymous cryptocurrency feature, and the forever changing process, it is quite challenging to compete with cryptocurrency leading to money laundering (Durner & Shetret, 2015). Coupled with low cost, high-speed transfer of funds, and with a decentralized tracking network providing secure transactions and anonymity, cryptocurrencies have been accepted as faster growth in the society, making it difficult for the traditional banking system to catch up with the progress (Afzal & Asif, 2019). Additionally, the unregulated and weak laws associated with cryptocurrency and the greater technology utilized to commit the crime make it even harder for the regulators to match the criminal's activities (Massad, 2019).

Fragility in the Law

Massad (2019) argued that the Securities and Exchange Commission (SCE) has limits where the most widely traded crypto-assets are not likely ever to be deemed securities, as not many crypto trading platforms are registered with the SEC. Obie and Rasmussen (2018) add that including stocks, even government currencies are regulated except for cryptocurrency, which is a leading factor in money laundering. Since the federal government has yet to classify Bitcoin, the lack of classification promotes the usage in money laundering, decreasing its chances of being regulated by any law or compliance programs (DeVries, 2016).

The law gap and because financial sectors can be eliminated during this process, the financial sector laws and regulations are not applied to Cryptocurrency (Cvetkova, 2018). The anti-money laundering laws are "short-sighted" where the criminals find new ways to bypass the law and conduct the crime of money laundering (Qureshi, 2017). While cryptocurrency firms do not have the infrastructure in place yet to follow anti-money laundering law standards, compliance could be costly for many startups (Broughton, 2019). Sending and receiving decentralized and anonymous safe data in a standardized way is still a challenge for regulators (Broughton, 2019). As such, DeVries (2016) proposes that outside of the Bitcoin framework specifications, the American National Standards Institute may need to establish security standards.

Technology

Cryptocurrency, leading to money laundering, is highly sophisticated and equipped with the latest technology that allows criminals to continually adapt and change to accomplish and increase money laundering (Dion-Schwarz et al., 2019). Battistini (2016) claimed that it is not the cryptocurrency but the blockchain, the technology, associated with cryptocurrency that has the actual value. The blockchain technology behind the Cryptocurrency is the digital currency's backbone and is essential for greater security and privacy for each participant (Miraz & Ali, 2018). Each transaction is tied to a new account, making it impossible to associate the number of transactions to a single client; hence, the crime footprints are covered appropriately, where the data and account holder is unknown (van Wegberg et al., 2018).

According to van Wegberg et al. (2018), transactions can potentially be linked to illegal activities, and enhanced technology associated with cryptocurrency can break the link between cryptocurrency transactions and illegal money laundering. Hence, enhanced technology is needed to make money laundering reliable, trustable, and efficient (Chen et al., 2018). Cryptocurrency technology enables users to make and enforce rules by circumventing the government made regulations (Afzal & Asif, 2019). The disruptive cryptocurrency technology challenges many bank regulations and laws that banks are not prepared for and are unlikely will be prepared for in the near future (Bryans, 2014).

Regulation

Why is Cryptocurrency Regulation Necessary?

The suitability of cryptocurrency and its advantages such as low transaction cost, privacy, means to buy goods, and a substitute for bank accounts (Brenig et al., 2015) poses a serious threat to banks. Therefore, as Cvetkova (2018) states, if Cryptocurrency is to be used as a means of payment for goods and services or any settlements, it should be considered money and regulated. Otherwise, the process can expose banking systems to anti-money laundering risk (Cvetkova, 2018). Idaho, Louisiana, New York, and Washington have adopted virtual currency as objects of money transmission, where, if not regulated, the cryptocurrency can pose a challenge to the financial institutions, public, and have a negative impact on the reputation of central banks (Cvetkova, 2018). A study conducted by CipherTrace in 2019 found that all significant U.S. banks have illicit cryptocurrency transmitting funds on their network, but often go undetected (CipherTrace, 2019).

Cryptocurrency with enhanced technology, widely promoted over the years (CipherTrace, 2019) may become the future by promising means of payment, and if companies are increasingly planning to use cryptocurrency in the future, then the regulation should be correspondingly and appropriately applied. The main benefit cited by Forgang (2019) is the lack of proper regulations on cryptocurrency has created new opportunities for money laundering. In 2013, the U.S. Department of Justice charged Liberty Reserve of transferring illegal funds using "Liberty Dollars" worth up to $6 billion, of which around 200,000 were U.S. users. Broughton (2019) mentioned that stronger cryptocurrency regulation can allow the collection of customer information, sharing with other institutions, potentially combating, and minimizing money laundering.

Anonymity by cryptocurrency is one of the biggest reason's regulation is required to counter terrorist financing as a lack of appropriate monitoring allows for questionable transactions permitting criminals to utilize cryptocurrencies (Houben & Snyers, 2018). Making account holder's information unidentifiable makes it difficult for accounts to be traced (Rueckert, 2019). Additionally, the decentralized structure of cryptocurrency allows for multiple account creation with multiple locations and no single party to administer, existing only on the internet or "virtual wallets" (Nabilou, 2019; Rasul, 2018) which is missed by regulators, consequently making the regulation harder (Nabilou, 2019). Although the government can never go away from a decentralized cryptocurrency, regulating this feature can decrease Cryptocurrency's illegal growth and usage (Nabilou, 2019). The lack of oversight makes cryptocurrencies less susceptible, leading to many financial crimes such as corruption, bribery, and money laundering (Gikay, 2018).

Massad (2019) identified that the inadequate regulations to address cryptocurrency lead to fraud and a weak economy, increasing illicit payments resulting in collateral damage to the financial system. The increase in cryptocurrency use and the failure to hold cash can affect the bank's interest rate by impacting the economy (Perkins, 2018). As well, the lack of regulation for the enhanced technology precludes the government from prohibiting criminal activities, increasing harm for the country and the world (Rasul, 2018). Not only the financial institutions but many cryptocurrency exchanges have been penalized as well. In 2015, Ripples Labs, Inc., a California based digital exchange developer and exchanger, was fined $700,000 in fines as they failed to implement and maintain proper anti-money laundering law obligations under the bank secrecy act (Sykes & Vanatko, 2019). The company's lack of regulation landed them in negotiating around $250,000 transaction without adhering to its “Know Your Customer,” where the transactions were overseen and not reported as suspicious activities.

In contrast, some authors have argued that regulating cryptocurrency might not be too beneficial as the enhanced technology associated with the process can drive financial globalization, resulting in an economic boom (Ducas & Wilner, 2017). By regulating cryptocurrency, the right to own a property, the right to pursue a profession, and the right to freedom of association can be violated and interfere with the right to data protection and private life (Rueckert, 2019). Since cryptocurrency is a new and upcoming industry, it is not recommended to overburden it with regulations that will affect the industry and its participants (Mandjee, 2015). Through various research, Rasul (2018) added that Bitcoin should be allowed to be an experiment as it can be an innovation adding to a country’s technological advances.

Sonderegger (2015) thought that cryptocurrency’s self-regulated peer-peer transactions can only grow and reach its potential only with fewer government interferences. Devlin (2017) added that regulation can slow down cryptocurrency adoption, study, and plans for future innovations enormously. In this case, the type of regulation applied to cryptocurrency should be well thought of as costly and complicated compliance regulation, and the overlapping regulations by federal, state, and bank laws can overwhelm startups (Mandjee, 2015). Therefore, “loose” regulation should be applied to cryptocurrency, permitting the virtual currency to develop (Sonderegger, 2015).

However, lack of regulation has served as a “fertile ground” for criminals inside and outside the country, causing instability, deflation, and security concerns about a country's citizens (Guadamuz & Marsden, 2015). Due to its anonymity feature, cryptocurrency cannot be tracked to any individual, nor can any illegal transaction be seized, contributing to crimes where their actions can be unstoppable (Rasul, 2018). Furthermore, lack of formal regulation means the rules can be changed anytime by the programmers to their desire but having a structured legal format and regulation can ensure accordance with the legal system (Afzal & Asif, 2019). Regulating cryptocurrency can help entrepreneurs and startups implement and facilitate a quicker operation from anywhere in the world, enabling economic growth, protecting investors from liquidity issues while encouraging innovation, and continuing the facilitation of entrepreneurial financing (Cumming et al., 2019). ***How to Regulate Cryptocurrency***

Massad (2019) believed that Congress should create strict and relevant laws to combat cryptocurrency leading to money laundering by requiring companies to comply with U.S. standards, and by increasing the authority of the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC). These laws will permit the law enforcement to set more core principles rather than just the regulations on recordkeeping and periodic reporting of transactions and disclosures to platform users. The comprehensive laws and regulations around money laundering practices can increase financial crime awareness; however, government enforcement should include all relevant voices in developing national anti-money laundering programs (FATF, 2018a).

Through the valid legislation and cooperation with anti-money laundering agencies and implementation of anti-money laundering laws can help fight illicit money crimes averting money laundering (Qureshi, 2017). The combination of law enforcement and financial regulatory agencies should enable the team to combat money laundering by enforcing financial institutions to deal with the problem (FATF, 2018a). To date, regulations have been concerned mostly with illicit transactions; however, a quota-based system offering transparency while ensuring that desired limits to money can regulate the use of cryptocurrency (Mandeng, 2018). The quota-based system can guard against undue cryptocurrency issuance, assuming that no other no extension of cryptocurrency is warranted (Mandeng, 2018).

Nabil (2019) referenced that one way to regulate cryptocurrency is by indirect regulations through banks that can have oversight powers without jeopardizing the benefit of the innovation. Cryptocurrency can be directly regulated by regulating the code and protocols, the design features of blockchain, node operators, and the users (Nabilou, 2019). Due to the growing popularity of cryptocurrency, there is a need for regulation, thence, for an innovative payment system, and to maximize its potential benefits, users should obtain a license for operating with virtual currency (Afzal & Asif, 2019). This approach can help set up specific guidelines and make cryptocurrency more transparent (Afzal & Asif, 2019). The authors further complement that allowing central banks to buy Bitcoin can ensure strict regulation just like cash, and to eliminate the virtual currency circulation; however, this approach does not stop other virtual currencies from being circulated without regulation.

As Cryptocurrency seems to empower the federal government, Bryans (2014) suggested the lawmakers should regulate the “fiat-to- cryptocurrency” exchanges given the exchanges already fall under the existing money regulations. Fiat-to-cryptocurrency is a legalized tender back up by the government, meaning, it is easier to regulate in comparison to cryptocurrency that is not approved by the government. Likewise, Turpin (2014) believed since cryptocurrency is likely to grow, regulating the transactions is more effective instead of restricting the virtual currency. Marian (2015) endorsed the government should enact “elective anonymity tax”, forcing a high tax on unknown cryptocurrency holders and users. Passing the “elective anonymity tax” will force the customers to reveal the identity, providing the regulators with a history of the transactions. The “elective anonymity tax” law not only allows the clients to continue using cryptocurrency but also has the financial benefit of registering their virtual currency, highlighting the illegal transactions, making the network less anonymous (Marian, 2015).

According to Q3 Cryptocurrency Anti-Money Laundering Report released on December 5, 2019, by CipherTrace, $4.4 billion in crypto crime was reported, and 65% of these crimes occurred due to the lack of "Know Your Customer" guidelines. Due to the challenges in "Know Your Customer" regulation, cryptocurrency poses as a primary challenge in money laundering, suggesting regulation around "Know Your Customer" should be implemented, and employees trained on the topic appropriately, where law enforcement can easily track and obtain information about illegal transfers (Forgang, 2019). Although anti-money laundering concepts focus on the due diligence and compliance of "Know Your Customer" regulations, banks can only utilize this concept if there is a bank account or an identity associated with the customer (Rueckert, 2019).

CipherTrace Report also indicates that out of the 120 most popular crypto exchanges, about two-thirds of those have poor or weak "Know Your Customer" instructions. Considering that cryptocurrency holders are not required to follow financial service provider account creation guidelines, where they can create multiple accounts on their device, the "Know Your Customer" regulation falls short. Making the "Know Your Customer" more rigorous can effectively detect and prevent money laundering (Sprenger & Balsiger, 2018) and guarding the banks against the flow of “dirty money” into the financial system (See et al., 2019). Rueckert (2019) proposed restricting and limiting access to Cryptocurrency or the mining hardware, and restricting the exchange of Cryptocurrency with real money by authorities can control illegal money laundering. Sprenger and Balsiger (2018) also advocated that to regulate cryptocurrency money laundering, financial institutions should focus more on the interchange between financial institutions and primary crypto exchange, distinguishing normal customer behavior from the ones performing money laundering. Hughes and Middlebrook (2014) mentioned that regulating cryptocurrency earlier than needed may hinder its development, mainly caused by innovative blockchain technology. The authors also reason that adopting and applying incorrect regulations may hamper the distributed computing technology potentially used for future applications. Regulating the decentralized system may give more power to the centralized system, enabling them to track the client's personnel information (Massad, 2019). Moreover, the regulation might inhibit the development of the decentralized system improving the existing financial market infrastructure.

While there may be concerns regulating the fast-moving innovative technology, the proposed regulations can directly target terrorist and criminal groups, ensuring money laundering reductions while helping banks take an improved control of their money laundering laws and rules (Moran, 2018). The weak regulation has attracted many different types of financial crimes, centered on the privacy feature of a cryptocurrency, which, if not regulated, can bring instability to the financial institutions (Campbell-Verduyn, 2018). For example, the "Know Your Customer" principles can help minimize the possibility of operational and legal risk, in addition to financial institutions concentration and reputational risks (See et al., 2019). The different regulation approaches adopted can potentially increase the comfort level for both virtual currency users and the customers using cryptocurrency while ensuring none or minimal illegal funds obtained through the process (Hughes & Middlebrook, 2014).

Current US Regulations Against Cryptocurrency

Currently, there are no formal regulations against cryptocurrency (Forgang, 2019). Hughes and Middlebrook (2014) reference that in 2013, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN, n.d.) issued guidance that the cryptocurrency should follow regulations under the Federal Bank Secrecy Act (BSA). FinCEN issued specified guidance in the United States that decentralized digital currencies should comply with money laundering regulations (Guadamuz & Marsden, 2015). Clear regulations and guidelines on AML, BSA, and "Know Your Customer" policies will help minimize criminal activities (Global Legal Insights, 2019). Some exchange services that do not fall in the current regulatory section have voluntarily developed robust procedures to verify their customers' identities and funding source (Global Legal Insights, 2019). For example, the state of New York has implemented "BitLicence," a new form of regulation that imposes a license requirement for cryptocurrency exchange (Massad, 2019).

In March 2013, the FinCEN identified Bitcoin as decentralized, placing it under the bank secrecy act laws (Stankovic, 2019). Thus, any cryptocurrency used for exchange purposes should be required to register with FinCEN and comply with strict regulatory rules. In the United States, cryptocurrency is undergoing regulations where the exchange companies must comply with BSA laws by making the identity requirement mandatory (Piazza, 2017). Although there are laws like the anti-money laundering law and the bank secrecy act, both fall short in this case as cryptocurrency is anonymous. Hence the "Know Your Customer" rule does not fully apply here as the identity is unknown in many cryptocurrency-related fund transfers. There are more regulations on money laundering in the US than cryptocurrency, but if cryptocurrency continues to grow, then clear regulations and guidelines may be necessary (Sonderegger, 2015).

Breach in Regulation

Many institutions have adopted different opinions due to cryptocurrency's ever-changing nature and varying views, leading to a breach in the regulation (Demertzis & Wolf, 2018). The authors further argue that the approach to regulation due to cryptocurrency's decentralized feature where it is just a software code that exists on the internet makes regulation difficult. The lack of definition for cryptocurrency has provided different regulations, consequently forming a breach in regulation and security (Piazza, 2017).

Hard Fork (2018) mentioned that currently, the United States has no real direction on the cryptocurrency regulation. Therefore, many cryptocurrency firms are not required to be registered and are not adequately supervised, leading to undetected illegal transactions (PYMNTS.com, 2019). Since the scope of anti-money laundering laws is limited to certain virtual currencies, the anti-money laundering laws leave a blind spot, still enabling money laundering (Houben & Snyers, 2018). Huang (2015) claimed that current regulations are weak and ill-equipped to address illicitly obtained funds, making money laundering prevalent. In order to address this, the U.S. judicial system should create new criminal standards that will regulate and target cryptocurrency use. Although the laws make the identity requirement during exchange necessary, diverse regulation involving cryptocurrency can result in non-transparency leading to a lack of disclosure requirements as well as anonymous accounts (Piazza, 2017).

Considering the interaction between cryptocurrency, specifically, Bitcoin and anti-money laundering are fragile, where the financial institutions are not fully knowledgeable and well prepared for the enhanced and disruptive technology, regulating technology can be tough (Bryans, 2014). Moreover, the "Know Your Customer" rule from anti-money laundering laws do not fully apply to cryptocurrency holders as they can create their account and as many as they want, leading to the mass market (Rueckert, 2019). Also, these users' tendency is not to be transparent in providing fund sources, which makes it difficult for financial institutions to mitigate risks (See et al., 2019).

Furthermore, if criminals find platforms outside of the anti-money law regulation, then they do not need to follow any regulations, where the exchange platforms appear and disappear so quickly on the internet that law enforcement lacks the ability to follow and regulate these (Rueckert, 2019). Given "Know Your Customer" regulation is not fully applicable to cryptocurrency, the anonymity feature of cryptocurrency complicates the financial system, where the task of identifying an individual is difficult (Campbell-Verduyn, 2018). If a transaction is not tied to an individual, a transaction cannot be traced, forming a breach of the current anti-money laundering regulations, causing obstacles for banks in obtaining appropriate account information. "Know Your Customer" is the due diligence that financial institutions must perform and not having up to the par regulation in this section, leads bank employees to miss many customers with the intention of money laundering, especially with anonymous cryptocurrency exchanges (Arasa & Ottichilo, 2015). The continued threat and lack of consistent regulatory oversight because of weak "Know Your Customer" compliance has led to cryptocurrency thefts up to $4.4 billion in 2019 (CipherTrace, 2019).

Negative Impact of Regulation on Financial Institutions

In a study conducted by Kemal (2014), the author finds that there is a negative relationship between the effectiveness of anti-money laundering regulations and money laundering. The author also finds that excessive regulation enforced by government regulations has forced banks to allocate a special budget just for employee training. The money laundering process and training implementations directly affect the financial institution's costs, indirectly increasing customer service costs and limiting customer choices (Meinert, 2016). JP Morgan Chase revealed that in 2013, the bank hired around 8,000 employees just to focus on the bank secrecy act and anti-money laundering laws, where these employees went through 800,000 hours of training (Aluise, 2017). Annually each bank spends up to $18 billion in anti-money laundering costs, where they are continually trying to innovate the technology and compliance (Aluise, 2017). Likewise, Bouheni et al. (2014) showed there is a negative relationship between tighter restrictions and regulations imposed by banks. The frequent changes in regulation to combat money laundering have impacted many banks (Kovner & Tassel, 2019). The forever changing regulations also increase the capital cost, where bank managers continuously have to change the financial institution's characteristics and resources to meet new regulations in keeping up with money laundering.

The gap in the U.S. regulation shows that regulations may not be an efficient approach to money laundering (Tysiac, 2016). In July 2015, Citigroup paid $140 million in penalties for anti-money laundering weakness in their subsidiary, where the regulators failed to identify a single instance of money laundering (Saperstein et al., 2015). Similarly, in 2016, the New York Department of Financial Services was fined $300 million for the same reason that existing regulation was found to be weak in identifying money laundering activities (Saperstein et al., 2015). These cases have proved that there is no indication that the anti-money laundering laws are effective in reducing the fight against money laundering. Not just the regulations, but the technology and infrastructure regulations related to money laundering also impact banks' financially (Bounds, 2016). While the new technology can help collect data and provide security, the new technology platform and regulations' gaps impose problems and complications for banks

(Gikay, 2018). The cost of increased new technology adds to the bank's expense in addition to training its employees on the new technology (Aluise, 2017).

The current anti-money laundering regulation is overly complicated, costing around $4.8 billion to $8 billion annually; however, these expensive laws result in less than 700 convictions yearly, where each conviction costs approximately $7 million (Mitchell, 2016). The higher compliance cost to combat money laundering has added to increased employee training, which has caused many small banks to fold. Also, the compliance cost associated with employees to compliance-related tasks has lowered the bank's services, raised fees, and damaged customer reputation (Mitchell, 2016). The United States Department of the Treasury Financial Crimes Enforcement Network in May 2018 asked banks to share the names of individuals with money laundering accounts, which ultimately increased compliance cost (Bounds, 2016). The data showed that many banks of the same size end up spending almost the same amount on punitive regulations and compliance (Bounds, 2016). The observation was also that it is hard to find compliance to combat money laundering, and while looking for pros of regulations, banks lose customers who fear being victimized (Bounds, 2016).

The rise in money laundering due to cryptocurrency has kept the banks on edge. Due to the pseudonymous and decentralized features of cryptocurrency, the regulations are uncertain and do not sufficiently protect consumers dealing in cryptocurrencies (Perkins, 2018). The lack of "Know Your Customer" leads to a bank's inability to collect individual account holder's information and data, resulting in severe noncompliance penalties (Goodell & Aste, 2019). The authors also discuss that in recent years the banks have dedicated a significant amount of resources to building and maintaining compliance structure in fighting money laundering impacted by cryptocurrency. Additionally, many larger firms have hired many employees to screen transactions making expensive customer calls in refreshing the “Know Your Customer” documents and training (Goodell & Aste, 2019).

Given the increase in money laundering activities due to cryptocurrency, the banking industry might be burdened with excessive regulations, losing anonymity with over-regulation, and causing more damage without knowing their customers (Subramanian & Chino, 2015). If individuals can move money into cryptocurrency with the anonymous feature, then the banks lose those customers, as bank regulations can be expensive for cryptocurrency-related transactions (Abramowicz, 2016). The anonymity feature of cryptocurrency makes it difficult for regulators to identify individuals with illicit money, leading fines for banks over money laundering charges and penalties (Marian, 2015).

Recent Cases

On January 30, 2020, the first cryptocurrency-related action was taken against M.Y. Safra Bank (MYSB). MYSB, which is based in New York City, had deficient anti-money laundering practices for compliance and monitoring for cryptocurrency exchanges and Bitcoin ATM operators (Clegg, 2020). The bank was charged for failing to comply with anti-money laundering laws for more than two years by not appropriately and thoroughly vetting cryptocurrency customers and associated transactions. The lack of anti-money laundering controls led the bank to open many accounts without adequate customer due diligence including, "Know Your Customer" practices and failing to identify and link them to suspicious crypto-related accounts and activities. While no monetary penalties were enforced on MYSB bank, it now has to implement many measures to update its anti-money laundering and bank secrecy act compliance programs. This will add to MYSB’s cost, where it has to hire appropriate individuals to oversee compliance programs and ensure no suspicious accounts go undetected.

Khatri (2019) analyzed a case between 2013 and 2018 involving two men, Callaway Crain, and Mark Sanchez, who sold steroids across the U.S. via their website. The pair sold over 10,000 packages of the controlled substance and received all payments in cryptocurrency. They laundered $2.8 million earned through these sales using Western Union, which was later converted to US dollars and deposited in legal bank accounts. Seeing that cryptocurrency regulations are still under development, the Western Union payments were laundered through false identities where the "Know Your Customer" verifications are weak or completely lacking (Piazza, 2017; Sprenger & Balsiger, 2018).

In 2019, a terrorist group called Hamas, Al-Qassam Brigades, started soliciting funding for their group using Bitcoin (CipherTrace, 2019). They started raising money for their organization using Bitcoin as a payment rail, asking supporters to use social media to send donations using Bitcoin, which comes with “anonymity and safety” features. The terrorist groups used videos to show funders how to utilize Bitcoin and send payments via telegram without getting exposed by regulators and authorities. To further tighten the anonymity issue, each donor was given a unique Bitcoin address.

In 2019, The United States Attorney for Southern District arrested Hugh Brian Haney in Ohio, for money laundering charges from illegal drug and other illicit goods and services (U.S. Department of Justice, 2019a). Haney, who was a drug dealer, laundered his profit of $19 million through cryptocurrency. In 2017 and 2018, Haney transferred Bitcoin derived from drug selling profit, to a Bitcoin exchange company, falsifying that the Bitcoin was from his own “mining”. Moreover, Haney was able to use a Bitcoin exchange company to open an account with different Bitcoin addresses, and as a result, was able to conceal his identity. The crypto-related laundered money worth $19 million was detained from a bank located in the Southern District of New

York. Haney was under the impression that cryptocurrency would keep his illegal proceeds anonymous, which it did, but he could not remain anonymous; therefore, his arrest came as a surprise to many cryptocurrency holders.

In 2018, Jacob Burrell Campos, a California Bitcoin dealer was charged with selling about $750,000 worth of Bitcoin to 900 individuals in the U.S. through his Bitcoin exchange service (Zhao, 2018). Campos, who failed to register the exchange and implement anti-money laundering laws, was charged with at least one count of money laundering from January 2015 to April 2016, where he wired at least $900,000 in 30 different transactions. Campos' legal trading account was closed in the U.S., despite which he used the cryptocurrencies no verification idea to launder money. His alleged activities challenged the legal U.S. regulated framework, where cryptocurrency regulation has a breach with no identity needed to create multiple transactions (Zhao, 2018).

Houben and Snyers (2018) discussed a 17-year Virginia teenager, Ali Shukri Amin's case, who supported a terrorist group, Daesh, by providing material using social media. In 2015, Ali Shukri Amin utilized the anonymity feature of cryptocurrency by masking the provision of funds to Daesh by providing instructions over Twitter on how to use Bitcoin. The anonymity feature and use of social media allowed Ali Shukri Amin to mask the shady transactions with limited regulations and breach around cryptocurrency and money laundering (Houben & Snyers, 2018).

Similarly, in a case study by the FATF (2018b), Altaf Khanani Money Laundering Organization (MLO) illegally laundered billions of dollars to fund illegal drug business, weapons to many terrorist groups. Due to the anonymity feature and the lack of cryptocurrency regulation, the Khanani organization facilitated money between Pakistan, the United Arab Emirates, USA, Canada, and other countries, funding many terrorist organizations. Altaf Khanani, the head of the organization, moved funds using wires to conceal transactions' nature. The multiple wires from various accounts and companies went undetected as cryptocurrency and money laundering regulations are weak in detecting several transactions from different account holders. Because cryptocurrency is pseudonymous and not tied to any individual gives many organizations the capability to conduct illegal activities (Rueckert, 2019). In a case against Michell Espinoza, accused of money laundering using Bitcoin, the presiding judge argued there was no strict regulation on Bitcoin along with no accurate definition of Bitcoin, so, cryptocurrency is not monetary (Price, 2016). The judge defined Bitcoin money as property but not as a means of exchange and ruled that a property can be laundered.

In 2012, HSBS was charged $1.92 billion for its US affiliate HBUS. HBUS operates in the US with over 470 branches, with an estimated 3.8 million customers was involved in bulk cash transfers, limited due diligence in "Know Your Customer" in anti-money laundering laws, and failing to track 17,000 suspicious accounts (Naheem, 2016). The bank failed to fully comprehend anti-money laundering regulations, where the high-risk accounts associated with money laundering and drug trafficking were categorized as low-risk accounts. HBUS also cleared about $2.9 million worth of traveler's checks that was disguised as money laundering for Russian criminal gangs in addition to offering 2,000 share accounts to high-risk customers, despite the high risk of money laundering due to anonymous accounts. The investigation revealed HBUS had weak anti-money laundering laws and breaches in their regulations and a high employee turnover rate with limited resources leading to many suspicious accounts bypassing the regulations (Naheem, 2016).***Potential Themes and Perceptions***

KYC, technology, decentralization, anonymity, regulation, and FinCEN guidance are the potential themes and perceptions from the literature review. The KYC process helps identify cryptocurrency-related red flags and customers and practices to assess and monitor customer risks. With the decentralized and anonymous feature, the virtual currency offers privacy towards customer identification, making it difficult for banks to detect illicit activities. The perception is that KYC effectively identifies customers with red flags, knowing a customer, their financial activities, and the risks they pose. The literature review emphasizes regulation and FinCEN guidance as ultimate solutions in dealing with cryptocurrency-related money laundering and combatting financial crime.

Summary of the Literature Review

The literature review summarized cryptocurrency-related money laundering as an illegal activity and crime conducted by customers to conceal illicitly obtained money. The practice involves multiple digital money transfers, cash transactions, wire transfers, and bulk cash smuggling. Due to the anonymous feature of the cryptocurrency, banks struggle to identify potential customers and the red flags accompanying the transactions. The KYC processes utilized at banks are effective; however, when it comes to virtual assets, the KYC process seems weak and needs improvement to help banks inappropriately identify and mitigate risks associated with cryptocurrency money laundering.

The illegally obtained money by damaging a bank's reputation also damage a country's economy. The illegitimate money flow entering the financial economy negatively affects economic growth. Additionally, the gap in banks AML/BSA programs due to the enhanced technology utilized by cryptocurrency prohibit the banks from correctly identifying suspicious accounts. The literature review indicates the banks need continuous improvement in AML/BSA programs and recommends the banks to follow regulations and FinCEN guidance.

Transition and Summary of Section 1

This study intended to understand the challenges faced by US banks to combat the risks of financial crimes leading to money laundering. Financial institutions are the primary contact for money laundering as it provides multiple services such as deposits, loans, and foreign exchange (Isa et al., 2015). This practice increases with the introduction of cryptocurrency as the digital currency can eliminate the bond between virtual currency and the real person by creating multiple accounts with anonymity, which leads to the impossibility of tracking and controlling all transactions promoted by the fragile regulation (Dyntu & Dykyi, 2018). Since many financial institutions lack the advanced technology associated with cryptocurrency to track virtual currency users, there is a need for a better approach and robust regulation to combat cryptocurrency leading to money laundering (McBride & Gold, 2019). Section two describes the researcher's role in this study, along with the participants' roles and the type of research method and design utilized. The section also outlines the population, sample size, and the tools and techniques employed to collect the data. Data organization and data analysis techniques are also discussed.

Section 2: The Project

This study's objective was to understand the challenges banks face while dealing with cryptocurrency-related money laundering transactions. This section defines the purpose statement for this study. The section also describes the researcher's role, procedures for gaining access to participants, their role in the study, and discusses the research method and design identified and justified. The qualitative case study method and design were applied to understand the challenges banks face while combating money laundering crimes posed by cryptocurrency. Data collection and organization methods were explained in this section, along with data analysis methods and processes.

Purpose Statement

The purpose of this qualitative case study was to understand the challenges posed by cryptocurrency for banks within the USA in order to identify and combat risks of financial crimes resulting in laundered money entering the banking system. This larger problem was explored through in-depth case studies of banks within the USA. The cumulative case studies were collected from organizations and several sites allowing for the greater generation of data without time being spent on new or possibly repetitive studies. These case studies demonstrated how money laundering through cryptocurrency presents banks with issues in identifying financial crimes. The case studies also focused and expanded on other financial crimes such as terrorist funding through money laundering influenced by cryptocurrency. The data were used to determine if there are justification and strategies for regulations that can be implemented to combat financial crimes for the banking industry.

Role of the Researcher

When conducting a qualitative study, the researcher is a human instrument. Only a human being as the instrument can learn and understand other humans, as it is not an easy task to ask people to relive past experiences and try to answer questions (Sutton & Austin, 2015). However, the researcher must be aware of his or her biases that can influence the study results. To minimize bias, the researcher considered all obtained data and analyzed them with unbiased minds by re-evaluating the participant's responses, ensuring no pre-existing assumptions interfered. This process, known as bracketing, helped the researcher set aside any prior knowledge, understanding, and assumptions on the research topic, minimizing the potential bias and influence (Neubauer et al., 2019). The researcher also avoided the halo effect as it can increase researcher bias. Halo effect leads to human judgment errors, increasing bias producing positive or negative research participants (Soper, 2014).

The researcher identified study participants in the study, developed interview questions, determined the study population, contacted potential participants, determined data collection techniques and methods, and conducted data analysis. Additionally, the researcher determined the most effective process to determine the research's validity and reliability. Reliability and validity add to the study's strength by providing accuracy, adding credibility to the study.

The researcher made the participants aware of the study's intentions, explained the interview process while ensuring their protection and confidentiality. Human protection is an important factor in any research as confidentiality affects respect, justice, and beneficence of subjects (Al Tajir, 2018). The interviews occurred virtually via zoom and phone. During the interview, the researcher transcribed the interview while trying to understand the interviewee's tone and modulations throughout the interview process. After the interview, the researcher reviewed and analyzed the interview questions with the participant's responses and checked with them for accuracy. The researcher also collected data from different case studies to answer research questions and reviewed and analyzed recent cryptocurrency-related money laundering cases and reports. Additionally, the researcher collected and analyzed data from case studies on what regulations or acts can help banks minimize the financial risk caused by cryptocurrency.

Participants

The bank employees from three different banks, the certified AML/BSA risk specialists, bank management, and bank compliance officers, were the study participants. Access to participants was by contacting the participants through LinkedIn or mutual relationships. The Director of Financial Investigations & Education at CipherTrace, experts on crypto laundering risks, was also a participant contacted via email to seek permission for the interview.

Participants were selected using purposive and selective sampling. Purposive and selective sampling produces a better and robust understanding of the problems by screening different participants for the same answer, seeking the complexity of the research problems (Beenot et al., 2016). The research participants were invited to participate in the study virtually (e.g., Zoom, Teams, Skype, Google Meet, etc.) or via phone and were made aware of the recorded interviews for accuracy if they consent. The ethical protection of the bank's participants was considered, and the participants were made aware of the anonymity and that their names and other related information will be excluded from the study. The bank participants were referred to as bank personnel.

The interviews were conducted via zoom and phone, and the number of certified AML/BSA risk specialists targeted ranged from 15-20, along with at least one bank management and one bank compliance officer. The saturation method was used for the study. According to

Vasileiou et al. (2018), there is no straightforward answer to how many participants are needed in a qualitative study; rather, reaching saturation is important. The more specific characteristics of the participants are, and the more specific questions are, the smaller the sample dialogue with the participant, the better the data; hence, more interviews do not depict stronger study data (Vasileiou et al., 2018). Sim et al. (2018) also added that saturation is essential in the qualitative study as the specificity of questions, quality of data, and strategy analysis is an important element. The participants were asked not to answer questions they were uncomfortable answering; however, they had the freedom to add information as needed or not asked during the interview.

A different set of interview questions were presented to the Director of Financial Investigations & Education at CipherTrace. Since CipherTrace is an external source, it does not directly deal with cryptocurrency-related money laundering, but its purpose is to educate and help financial institutions gain crypto entity knowledge. The Director of Investigations & Education at CipherTrace was made aware of the interview's research and process. The interview occurred via zoom, and following the interview, the Director was given a copy of the completed interview to confirm responses for accuracy. The Director of Investigations & Education had the freedom to add information as needed or not asked during the interview.

Research Method and Design

The researcher utilized the qualitative research method for this study. Qualitative research study helps develop an understanding of the research questions by detecting trends and opinions by experts. Qualitative research methods are exploratory and explain "how" and "why," describing and interpreting issues from the population studied to generate new theories (Mohajan, 2018). In this qualitative research method, the AML/BSA risk specialists, bank management, bank compliance officers, and the Director of Investigations & Education at CipherTrace were the experts, as they brought value to the study while offering insight into how each financial institution detects financial crimes related to money laundering entering the banking system.

This qualitative research study, utilizing the interview questions, focused on the in-depth questions via zoom and phone, some of the preferred qualitative study data collection methods (Sutton & Austin, 2015). The advanced preparation of the interview questions helped the researcher prepare for the interview. The interviewee's responses set the stage for the next set of questions or determined the number of participants. Sutton and Austin (2015) mention that in the qualitative research method process, one participants' narrative can inform the next, and the interview can continue until nothing new can be obtained, where saturation has reached. As the interviewees answer the questions, other effective questions might arrive, leading to detailed observations in the financial institutions and the expert's opinions.

There might be other issues in the financial institution that the researcher might be unaware of hence the AML/BSA risk specialists, bank management, bank compliance officers, and the Director of Investigations & Education at CipherTrace can help the researcher gain a thorough clarification and understanding of cryptocurrency-related money laundering problem. Qualitative research seeks to find meaning and understanding of participant's answers by utilizing open-ended and unstructured formats, leading to other useful questions (Creswell, 2018). Along with the interviews, case studies were used to obtain the research answers, which helped understand the research questions. Long-Sutehall et al. (2010) suggested that archived and existing data can strengthen the base of the social knowledge base. Ruggian and Perry (2019) added that utilization of archived and existing data allows for the generation of new knowledge without additional data collection but maximizes data output, increasing the sample size. Thus, the qualitative research method was appropriate to accomplish the purpose of this study.

The most appropriate design for this study is a case study. A case study analyzes projects, policy, institutions, programs, financial organizations, and websites in detail, allowing for the greater generation of data without time being spent on new or possibly repetitive studies (Starman, 2013). According to Alpi and Evans (2019), case studies should include evidence from interviews, archival records, or retrospective studies, which can help solve business problems by building and testing business theories and processes (Ebneyamini & Moghadam, 2018). In this case, data generated from interviews and case studies allowed the researcher to understand how criminals promote and use cryptocurrency-related money laundering.

Often financial crimes such as cryptocurrency-related money laundering happen at many different levels, and many times bank employees are far removed from these transactions, as the banks lack a proper system in place to detect money laundering. Therefore, apart from the expert's opinions, multiple case studies were reviewed and analyzed for different types of cryptocurrency-related money laundering crimes. Heale and Twycross (2017) explained a case study as an intensive study or investigation about a person or a group, where the researcher examines in-depth data relating to several variables about a topic.

The investigation may include reviews of literature articles, media, reports, and multiple studies. The collection of different data types helps with understanding the cases by informing the development of research questions. The multiple case studies and data allows for a more exhaustive understanding of the cases, comparing similarities and differences, where the evidence from multiple case studies are suggested to be stronger and more reliable. Since cryptocurrency-related money laundering is a growing concern, data from every variable increases data collection for the researcher while answering the research questions.

Discussion of Method

The qualitative method was the most appropriate method for this research study. The designed research study interview focused on the research participants' experiences and feelings on cryptocurrency-related money laundering cases and their suggestions on mitigating risks. The data collection was non-standardized and non-statistical. According to Rahman (2016), qualitative research is not statistical but incorporates multiple realities in analyzing meaning or issues rather than numbers; therefore, it is multiple aspects. The in-depth interview developed enabled the researcher to access the participant's thoughts and feelings on the specified topic with probing questions to gather in-depth data.

Although the research study questions are not explicitly stated in qualitative studies, they are frequently embedded in the problems and purposes (Kross & Giust, 2019). For this research study, the stated purpose described the researcher's intention to understand the challenges posed by cryptocurrency for US banks when dealing and combatting the financial crimes resulting in laundered money entering the banking system. The problem statement explained the increase in money laundering through cryptocurrency and how it damaged banks' reputation leading to fines. Both purpose statements and problem statements were used to derive the specific interview questions; hence the qualitative method helps narrow the study's focus, providing a structure to the research (Kross & Giust, 2019).

The anticipated detailed description of participants' responses helped achieve more in-depth insights into the research questions and purpose and problem statement. Rahman (2016) mentions the qualitative method helps understand the human experience in a specific setting, including individual case studies. The research also focused on case studies; hence, the researcher understood different participants and events and their abilities and perspectives. Additionally, the qualitative study enables the researcher to describe, decode, translate, and analyze, coming in terms with the data (Rahman, 2016).

Discussion of Design

The case study was a suitable design for the designed research study. The case study investigates a phenomenon within its real-life framework, relying on several sources of evidence (Ebneyamini & Moghadam, 2018). For this study, besides interviewing the bank employees and the Director of Financial and Education from CipherTrace, case studies were evaluated and analyzed. The case studies selected focused on real-life criminal cases to understand how banks combat cryptocurrency-related transactions and possible money laundering cases. Case studies are built to support research questions and published case studies to demonstrate the data diversity in a study (Ebneyamini & Moghadam, 2018). Furthermore, the detailed data from the case study design enabled the researcher to study different aspects of the research, examining them in relation to each other.

According to Harrison et al. (2017), case studies advance effective research to investigate and understand complicated issues in the real world and businesses. As money laundering is a growing concern, the case study design can help address a wide range of research questions with existing and new data obtained. Ridder (2017) added that a case study investigates real-life situations, and within its environmental context, it focuses on the similarities and differences between different case studies with similar theories. Penn and Currie (2016) reiterated that the case study emphasizes similar real-life problems and examples; therefore, this design worked the best for this research as cryptocurrency-related money laundering is a real-life problem with significant challenges to the financial institutions.

A case study allows for rich and detailed data collection, normally not obtainable in other research designs. Moreover, the design helps obtain a detailed description of answers while gaining a better understanding of “how” and “when” (Ridder, 2017). Once the detailed and rich data are obtained, the case study design enables the discussion to open further discussions. As the research questions arise from the research gap, the case study focuses on the research question relevance giving rise to many solutions as an outcome of the study, impacting the workplace. Case studies provide an enhanced understanding of the study of interest regarding context-dependent knowledge (Ridder, 2017).

Summary of Research Method and Design

Qualitative research methods and case study designs were best suited for this research study. As a qualitative research method allows for an in-depth interview as one of the preferred data collection methods, a case study enables in-depth interviews to generate detailed and rich data. Other effective questions can arise from the interview questions, opening the questions for further and deeper causes as an advantage of qualitative and case study design. With a complicated and complex cryptocurrency-related money laundering topic, the case study design is an effective design helping solve complex issues by emphasizing the real-life problem.

Population and Sampling

According to Sargeant (2012), research participants selected in a qualitative study are critical as they best inform the research questions, enhance phenomenon understanding, and generate quality data, as they are most familiar with the topic. In this qualitative study, the participants were certified bank AML/BSA risk specialists, bank management, and bank compliance officers. The Director of Financial Investigations & Education at CipherTrace, a company that consults banks on crypto laundering risk, was a participant as well. The researcher utilized purposeful sampling in selecting the participants who were experts in their field with rich information. Purposeful sampling was also be applied while selecting the case studies providing study relevant and information-rich cases while using limited resources.

Discussion of Population

The certified AML/BSA risk specialists are certified by the Association of Certified Anti-Money Laundering specializing in the Anti-Money Laundering Laws and Bank Secrecy Act. The AML/BSA risk specialists are certified to monitor, target, and report any wary activities related to illegal money laundering transactions. They are also responsible for implementing policies, procedures, and systems for banks to ensure complete customer identification and customer due diligence preventing suspicious activity (Miller & Rosen, 2017). Therefore, their role was valuable in answering research questions on how they investigate, identify, and report suspicious account activities.

Bank management and bank compliance officers as participants helped answer research questions on the financial crime risks and challenges faced by banks when dealing with cryptocurrency. The bank management's primary responsibility is to define and implement anti-money laundering policies (Curry, 2019). They must also ensure to include compliance programs, and employees are well trained to understand compliance programs. The bank compliance officer's responsibility includes managing and maintaining procedures related to money laundering activities. They are also accountable for designing, evaluating, maintaining, and overseeing compliance programs throughout the financial institution (Miller & Kohr, 2016). Additionally, they play a role in developing training on AML processes.

Cryptocurrency business linked to banks has increased over the years, posing many compliance challenges for financial institutions. Bank management and bank compliance officers as suitable candidates helped the researcher understand the decisions and strategies to minimize cryptocurrency-related money laundering. They also need to be aware of the monitoring tools to stay ahead of the "tech-savvy criminals" for "Know Your Customer" to enhance due diligence for full BSA/AML compliance (Richardson et al., 2019). The approach they take will have a direct influence on the AML/BSA risk certified specialist roles and how they help identify and report suspicious activities related to cryptocurrency money laundering.

The Director of Financial Investigations & Education at CipherTrace, a company that is an expert on crypto laundering risk, helped add to the compliance issues banks face with cryptocurrency-related money laundering. Banks often have a difficulty controlling their employees, processes, and choosing the right clients for cryptocurrency-related money laundering (Davies, 2018). Additionally, since cryptocurrency money laundering is relatively new to the financial institutions, many banks may lack the bandwidth, skills, knowledge, and experts (Isa et al., 2015), leading them to turn to external sources to help gain the crypto entity knowledge. Therefore, CipherTrace can help banks be complaint in investigations of criminal activity, fraud, and sanctions evasion while helping them understand new threats. As a participant, the Director of Financial Investigations & Education at CipherTrace helped shed light on important AML/BSA factors and how banks can better understand and track cryptocurrency-related money laundering.

The focused cryptocurrency-related money laundering case studies added to the new data, makes the research more robust. According to Antes et al. (2018), more knowledge will be added through the secondary sources to support the participant's answers, maximizing evidence gathered. Ruggiano and Perry (2019) mentioned that using secondary data such as case studies and reports increases the sample size, increasing the knowledge without additional data collection. The case studies and third-party reports chosen will have access to rich data and data and hard to reach to the population (Dufour & Richard, 2019).

Discussion of Sampling

For this study, the purposive sampling method was utilized. Purposive examining is a broadly used strategy in the subjective investigation because of the distinguishing proof and choice of the technique for data rich cases (Palinkas et al., 2013). This means identifying and selecting participants knowledgeable in the study field, willing to participate in the study, and answering the interview questions. Besides, the information-rich cases can yield an in-depth understanding of the problem, searching for trends, rather than generalizing the answers. The researcher ensured that participants were willing to take part in the study and can communicate experiences. Using a purposive sampling method in the study will ensure issues with time constraints, resources, and access to information (Beenot et al., 2016).

Access to purposive samples was obtained by applying criterion sampling. Criterion sampling is where the study participants meet predefined criteria, have the participants' characteristics, and meet the study objective (Moser & Korstjens, 2018). Criterion sampling, with predefined criteria, identifies participants of importance to the study, making access to participants easier. According to Palinkas et al. (2013), from the perspective of the qualitative research method, criterion sampling increases the research knowledge by the participants' experience, generating rich data.

For this study, the predefined participants were certified AML/BSA risk specialists, bank management, bank compliance officers, and the Director of Financial Investigations & Education at CipherTrace. These participants are the money laundering field experts, understand the anti-money laundering laws, and "Know Your Customer" policy. The "Know Your Customer" policy increases the banks due diligence activities for customer identification while attempting to decrease money laundering (Arasa & Ottichilo, 2015). CipherTrace's Financial Investigations & Education Director's experience in cryptocurrency-related money laundering brings information other than someone directly involved in the banking process. Having participants who share a similar experience but vary in characteristics can help the researcher understand the phenomena with divergent opinions (Moser & Korstjens, 2018).

Case studies had a similar trend, where the studies were selected with a predefined criterion. The researcher selected case studies that represent real-world examples, reports from agencies dealing with cryptocurrency-related money laundering, and with the knowledge of anti-money laundering laws. Using predefined cases elaborated on the study findings, adding the rich and in-depth data with credibility. According to Sargeant (2012), in a qualitative study, the sample size is not predetermined as it depends on the research design, and the number of participants needed to fully answer the research questions. Therefore, this study's sample size came from at least three different banks. CipherTrace's Financial Investigations & Education Director was the only sample size that was predetermined, as the Director had the capability to answer research questions based on the experience and role in the company. The number of case studies and reports analyzed also depended on how informative the sources were.

This qualitative study utilized the saturation method. The saturation method uses a small sample size but supports in-depth data fundamental to the study (Vasileiou et al., 2018). Furthermore, the saturation method supports not repeating data and gathering new data until no new data are available. Once the researcher felt no new data can be obtained, the researcher stopped interviewing the participants. In a qualitative study, the fewer the participants, the more profound the inquiry per person; hence, fewer resources can generate rich data.

Saunders et al. (2018) added that the saturation method indicates that further data collection may be unnecessary based on data collected and analyzed. The sample size determinant for this study depended on how powerful and relevant every certified AML/BSA risk specialists, bank managements, and bank compliance officers' responses were to the questions. Guest et al. (2020) defined saturation as the data collection point where no or little new information is collected to answer the research question. As interviews are a better method to reach saturation, the selected participants' characteristics can help the study reach data saturation quickly with enhanced rich data (Fusch & Ness, 2015).

A predetermined sample size was used for different case studies. The case studies can provide different information; therefore, the more focused case studies are, the quicker the saturation will be reached. At some point, every report will have similar information relayed differently; hence, the researcher must be careful not to repeat information. Case studies support primary data collection (Dufour & Richard, 2019), and depending on how much information is obtained from the participants, the case study sample size can be small.

Summary of Population and Sampling

The AML/BSA risk specialists, bank managers, compliance managers, and the Director of Financial Investigations & Education at CipherTrace, were the study participants. The researcher selected these participants as they were the experts in their field. The selected participants with rich and detailed information about the research topic can answer the interview questions and the overarching research questions. The purposeful sampling used helps identify study participants based on the knowledge of cryptocurrency-related money laundering cases.

Additionally, purposeful sampling helps select information-rich and in-depth cases, providing data relevant to the study. The information-rich and in-depth cases provide insights and a better understanding of the situation rather than generalizations (Beenot et al., 2016).

Data Collection

This study data were collected through interviews conducted via zoom and phone. The researcher started data collection once permission from the Institutional Review Board (IRB) was received, and upon successful proposal defense. The researcher played an instrumental role in the study to design and tested the research questions and its theory. In the qualitative study, the researcher provides factual and descriptive information on the research questions and data collection (Daniel, 2016). The facts and information collected through interviews represented the participant's thoughts, feelings, and opinions; therefore, the participants' presentation was critical. Since the researcher is the observer and establishes relationships with the participants, the researcher is instrumental in encouraging the participants to speak freely (Moser & Korstjens, 2018).

Instruments

According to Majid et al. (2017), the interview guide is important as it helps the researcher with consistency throughout the interview. Therefore, the interview guide should be prepared well in advance and is critical to in-depth interviews. The semi-structured in-depth interview includes developing an effective interview guide, with open-ended, clear, and neutral questions, accompanied by follow-up and probing questions (DeJonckheere & Vaughn, 2019). The interview guide also helps determine how banks identify and report suspicious accounts related to cryptocurrency-related money laundering and how they can minimize financial crime risks and challenges related to cryptocurrency.

The interview guide Appendix A and Appendix B consisted of an introductory statement, research questions, interview questions, and the closing statement. In the introductory statement, the researcher informed the participants about the research purpose and objective, and how and where the information available from the interview will be used. Appendix A outlined interview questions for bank employees, and Appendix B outlined interview questions for the Director of at CipherTrace. Disclosing the study's purpose helps build trust with the participants and clarifies the research objective (Qu & Dumay, 2011). The introductory statement also included the approximate time needed to finish the interview and the flexibility the participants are given to refuse to answer any uncomfortable interview questions. Majid et al. (2017) recommend keeping the interview well within 90 minutes to consider other study participants' commitments. The participants were encouraged to ask clarifying questions. Not all participants necessarily understand the questions in the same manner; hence encouraging them to ask clarifying questions, making the interviewee relaxed and unjudged (Qu & Dumay, 2011).

The research questions were listed, followed by interview questions that help in answering the overarching research questions. The opening questions are simple to make the participant comfortable with the interview and familiarize themselves with the research subject (McGrath et al., 2018). These questions were followed by open-ended and probing interview questions created to obtain more data from the participants. The open-ended, more in-depth probing interview questions created help obtain additional information from the participants, collecting the most salient answers and reaching saturation quicker (Weller et al., 2018). Moreover, the open-ended and probing questions within each topic can be used to follow up on the critical questions (Ranney et al., 2015). The interview questions concluded with a closing question. McGrath et al. (2018) suggested closing the interview with a closing question to ensure the participants have an opportunity to add information based on their knowledge and expertise the researcher misses during the interview.

The closing statement included statements on confidentiality and the plan to safeguard interview transcripts securely. Confidentiality is important in any research as it protects the research participants from harm, exposure, and risk, while breaking the confidentiality rule reduces collecting valuable data, showing a lack of respect, and disregarding the participant's privacy (Surmiak, 2019). Additionally, in the qualitative study, breaking the participant's confidentiality undermines the researcher's ability and credibility to conduct studies. Saunders et al. (2015) explained confidentiality as keeping conversation between the researcher and participant private, only achieved by keeping participant's identity secret. The closing statement also ensures a copy of the transcript is shared with the participant for data accuracy, allowing the participants to clarify or add further data if needed (Ranney et al., 2015).

Data Collection Techniques

For this qualitative research method, the researcher collected data through interviews. The interviews occurred via zoom and phone. Interviews are the preferred way for qualitative study data collection as interviews with participants are a direct and easy approach for collecting rich data (Barrett & Twycross, 2018). Data gathering identifies the participants, creates an interview guide with predetermined questions, and directly asks the participant's interview questions. The predetermined samples, however, were semi-structured, open-ended, and probing. The semi-structured interview for data collection with open-ended questions gives participants the flexibility to bring in their own opinions and add supplementary information not encountered in the interview (Barrett & Twycross, 2018). The data were collected at the end of the study, transcribed, and checked with the participants for accuracy. The participants were followed-up via emails with clarification questions or any additional interview questions the researcher had. The follow-up procedures are important as it helps increase research effectiveness. The follow-up questions also ensure data accuracy and help avoid any researcher bias. Data accuracy maintains data integrity, avoiding data misinterpretations and assumptions, providing accurate data representation (Cai & Zhu, 2015).

Interviews are a good way to gather data using a set of predetermined questions where interviewees can freely express themselves (Paradis et al., 2016). Barrett and Twycross (2018) added that the interviews shape the conversation in real-time, leading to other clarifying and probing questions, which can be hard to achieve in a prewritten schedule. The researcher conducted in-depth interviews with as many participants as possible to gather as much data as possible. In-depth interviews generate rich data, and rich data are credible, providing strength to the qualitative studies (Schultze & Avital, 2011). The interview will be a critical data collection method as interviews give rise to many different results and trends interpreted through conversation with the participants (Fritz & Vandermause, 2017).

Research data were also derived from secondary sources, such as case studies. Since the secondary sources can be readily available, there was no specific data collection method for these. The process involved considering different data types already collected on the research topic, how recent the data were, data collection techniques, data quality, data efficiency, and how sufficient and relevant data were to the research topic. For case studies, different reports on cryptocurrency-related money laundering were reviewed and analyzed, and notes were taken. The advantage of using secondary data is there is no hassle of data collection since data were collected by someone else (Kabir, 2016). For the case studies reports, data were gathered by reading the various reports generated and published on cryptocurrency-related money laundering. Relevant case studies related to cryptocurrency-related money laundering was gathered.

Data Organization Techniques

Data organization is vital to making data discoverable, understandable, and accessible, bringing success to qualitative study, producing high-quality data (Surkis & Read, 2015). To produce the highest quality data, the researcher organized the collected interview data into categories. The interview questions were grouped by organizations and their job titles. Categorizing data by organization and job titles helped data retrieval and sorting easy. The copies of the completed interview were maintained, and the data accuracy checked with the participants. The researcher grouped all the interview questions with missing answers, and interview questions with additional information were congregated together. This data organization technique of narratives emerged themes. Creswell (2018) suggested that researchers can use emerging themes from the interview narratives.

The interview data are stored in a central location. The researcher is the only person with access to the interview, including the participant's identity. The secured data are stored on a password-protected computer, which only the researcher has access to. The data are used only for the intended use, and published data will not reveal any participant's identity. Maintaining participants' confidentiality includes keeping information private or not sharing data, ensuring participants' protection from judgment (Saunders et al., 2015). After a period, the researcher will destroy all the interviews and any other data related materials.

Data from secondary sources were organized similarly as the interviews. Case studies from Ciphertrace, FinCEN, FINRA, U.S. Department of Justice, Financial Technologies Forum, and Financial Post were collected and classified. Research logs were also utilized to organize data from secondary sources. Research logs are a comprehensive list of sources already searched for, helping organize and track research articles (Elder, 2019). It helps document where the information was searched, what was searched, and what was found or not found. While keeping the researcher informed about the research process, the research log keeps a detailed record of each article, organizes the researcher's time, avoids repetitive searches, and duplicated efforts.

Summary of Data Collection

Through interviews, the data collection helped the researcher collect detailed information with a direct and easy approach where the interviewees can freely express themselves. The interview questions developed grouped by organizations, and their job titles allow for more detailed questions to achieve a high response rate. The semi-structured, probing, and open-ended questions for a predetermined sample size gave participants the flexibility to add information missed by the researcher. The secondary data from case studies benefitted the researcher by answering new research questions by relying on the already collected data.

Data Analysis

Data analysis began after data collection. The data analysis process is time-consuming and requires reading transcriptions repeatedly word-for-word (Barrett & Twycross, 2018). It allows the researcher to systematically organize the interview questions, review and understand the data, transcribe the interviews, type the notes, and assign codes to different interviews to identify emerging themes or patterns. Working systematically through the entire data set and paying attention to each response can help form and recognize themes across the collected data set (Nowell et al., 2017). Additionally, searching for emerging themes can help the researcher interpret the emerging themes answer and support the research questions.

Watkins (2017) added that the qualitative data analysis can be time-consuming as the amount of data generated from the qualitative study can be extensive; thus, getting familiarized with the data helps identify common themes and organize the interviews in categories subcategories. Interview categorization will define and compare themes that reflect the phenomenon of interest (Nowell et al., 2017). According to Elliot (2018), tagging interviews and structuring them into categories helps data mapping, provides an overview of similar and dissimilar data, and allows the researcher to makes sense of all the interviews conducted relevant to the research questions. Categorizing or coding organizes data and identifies different themes and relationships between the data.

Secondary data analysis using case studies from Ciphertrace, FinCEN, FINRA, U.S. Department of Justice, Financial Technologies Forum, and Financial Post FinCEN were analyzed by spending significant time reading and learning about the data origin, reviewing, and analyzing the data. The researcher ensured secondary data were accurate, relevant to the research questions, and contained the study's information. Similar types of case studies were organized, coded in similar themes, and categorized to find themes, increasing the data collection, providing detailed information needed for the research study. The researcher summarized the case studies in main points and analyzed in the review.

Coding Process

The researcher used the MAXQDA coding system to organize, analyze, and transcribe interviews. MAXQDA allows for organization, evaluation, analysis, and interpretation of textual data in interviews. MAXQDA helps researchers organize the interview data while performing content analysis and thematic analysis, making the research successful (Marjaei et al., 2019). Moreover, the system can organize and manage many interviews quickly. According to Elaldi and Yerliyurt (2016), MAXQDA helps interpret collected data by generating themes, summarizing the predefined themes, and aligning them with common themes. MAXQDA can pull all sufficient data together, using codes to identify what is relevant to the given question, code them with particular codes, and make the review process accessible, hence bringing sufficient data for the study (Elliott, 2018). Sapat et al. (2017) added that MAXQDA lets the researcher import data from interviews, organizing them into groups, and linking to each other for themes. In comparison, Neale (2016) added that MAXQDA codes, identify themes, and isolate them into common and different patterns, explaining the consistencies and inconsistencies in the data gathered. According to Oswald (2017), MAXQDA helps the researcher streamline the research process by keeping the study material organized, and keeping the participant's information confidential, secured by a password. Protecting participant's information helps establish trust between the researcher and the interviewer while increasing the data collection.

Summary of Data Analysis

Data analysis through MAXQDA enhances data organization and analysis by analyzing multiple interviews at once. MAXQDA interprets data collection by creating, identifying, and aligning with the research questions. The generated themes organize the questions into a common and different pattern, explaining the difference between gathered data. Secondary data analysis occurs by reading and evaluating case studies to find themes and increase data collection by providing detailed information for the research study.

Reliability and Validity

Reliability and validity are critical aspects of qualitative analysis, where the data can be subjective and misinterpreted (Cypress, 2017). Hence, the researcher must create strong research, choose appropriate methods and samples, maintain data consistency, and rigor to avoid misinterpretation. Reliability and validity help evaluate quality research and demonstrate data reproducibility with accuracy. According to Taherdoost (2016), reliability is about consistency in data collection, and validity measures the intended outcome; hence they go hand in hand. Since qualitative research data are challenging to explain, demonstrating rigor using different reliability and validity methods leads to building trustworthiness (Amin et al., 2019). Zamanzadeh et al. (2015) added that measuring reliability can be impossible if there is no appropriate measurement of content validity; hence validity and reliability are linked.

Reliability

Reliability is a repeated measurement of the method, producing the same result, providing stable and reliable data (Cypress, 2017). For this qualitative study, to show data reliability, the researcher used pre-developed structured interview questions for all the participants. Using structured interview questions among the participants helps the researcher increase data consistency and reduce errors, making the data more reliable (Doll, 2017). The structured interview questions standardize the way questions are asked, and holding the questions constant increases research data reliability (Hofisi et al., 2014). Additionally, the structured and standardized interview questions help data reproducibility with the highest quality data possible (Wass et al., 2019). The researcher's decision to keep the questions specific, clear, consistent, and transparent brings reliability to the data (Noble & Smith, 2015).

For this research study, data collection comprised of case studies from Ciphertrace, FinCEN, FINRA, U.S. Department of Justice, Financial Technologies Forum, and Financial Post. Therefore, to enhance data reliability, the triangulation method was used. Triangulation involves utilizing multiple external methods for data collection and data analysis (Fusch & Ness, 2015). The rich and in-depth data from triangulation increases data saturation and data reliability, where data saturation aids in obtaining enough data to produce reliable data (Fusch & Ness, 2015). Triangulation helps achieve a comprehensive data understanding, enriches the data result, adds to study depth, supports the researcher in the document, and interviews analysis increasing data quality (Fusch et al., 2018). Fusch et al. (2018) emphasized that using various resources in the research study helps dissertation studies explore different levels and perspectives of the same phenomenon, extending theory knowledge and revealing several commonalities. Moreover, triangulation can enrich research studies by offering various datasets and confirming a hypothesis (Noble & Heale, 2019).

Validity

According to Mohamad et al. (2015), validity is how well the research questions get answered and how meaningful, useful, and purposeful they are. To ensure the research study has valid data, the researcher ensured data accuracy with the participants to avoid misinterpretations, increasing data validity (Leung, 2015). Cai and Zhu (2015) explained that checking data accuracy increases data validity, avoiding ambiguity and assumptions. According to Noble and Smith (2015), lack of data accuracy decreases trustworthiness, increasing personnel bias, and influencing the study data.

In a qualitative research study, trustfulness, trustworthiness, and accuracy are the main concerns for validity (Cypress, 2017). Several types of validity, such as content validity and face validity, are critical to qualitative study; however, in this study, content validity was essential. Content validity is where the data generated includes a review of published articles, data, and interviews from the targeted population (Anthoine et al., 2014). The appropriate targeted sample gives an accurate picture of the process, providing information on the representativeness and clarity, measuring the intended (Zamanzadeh et al., 2015). The strong focus on the selected population represents currently available knowledge, developing meaningful, understandable, practicable, and valid data measurements (Halek et al., 2017).

Transferability, referred to as generalizability, increases data validity by providing thick and rich descriptive text applying the findings to other contexts or populations (Nowell et al., 2017). Morse (2015) described transferability as a thick description of findings to transfer to other contexts or individuals or someone interested in the original findings. The evidence provided by the researcher ensures that other researchers can justify the knowledge provided and apply it to other settings and situations (Carminati, 2018). The researcher presented a detailed and thick description of the research process and data, where the transferability was achieved by purposive sampling. Cypress (2017) mentioned that transferability can be enhanced by a purposive sampling method, providing a thick, wide range of detailed information from participants, including accurate research descriptions and robust data.

Like reliability, triangulation plays a critical role in the validity. Adams et al. (2015) described triangulation as a relationship between the validity of conclusions and different approaches producing convergent findings. When one or more methods get utilized for the data collection on the same topic of interest using different sample types, it captures different dimensions of the same topic, assuring validity. Therefore, the sample size brings in data validity, bringing a better understanding of the research questions by mixing different methods, and providing more convincing and accurate data (Ashour, 2018). The qualitative study's appropriate sample size brings in new and rich data to validate the data with trustworthiness (Vasileiou et al., 2018), while inappropriate sample sizes are prone to errors lowering data validity (Blackford, 2017).

Summary of Reliability and Validity

Data reliability achieved through specific, clear, and concise interview questions helps the researcher with data reproducibility from different participants with similar responses, increasing data saturation and data reliability. Validity by data accuracy decreases ambiguity and assumptions. Data accuracy evades data misinterpretations, specifically content validity, by reviewing published articles and interviews from the targeted population, while transferability validity will increase data validity with the thick and rich descriptive text from the research participants. Triangulation adds to data reliability and data validity by obtaining data from different scopes of the same topics with rich data assuring data quality.

Transition and Summary of Section 2

Section 2 detailed the researcher's role, the participants' information, and the research method and design employed by the researcher. The section also discussed how the study population was selected and how many participants were needed to reach the study saturation to collect enough data to support the study. In qualitative studies, saturation emerged as the "gold standard" when redundancy was reached during data collection with no further issues identified (Vasileiou et al., 2018). The section identified participants for the study and how their experience and knowledge can increase data reliability and validity. Data reliability and validity depends on the appropriate research sampling and their consistency (Leung, 2015). The researcher also discussed the instruments used during data collection and process techniques.

Section 3 describes how the qualitative data from interviews and case studies was organized, analyzed, and presented. The themes or patterns recognized from the data were linked to the research and conceptual frameworks. The section also presents any issues during the research and how they were addressed. Saturation and triangulation was also addressed in detail, providing a summary of the data analysis. The study findings discussed any potential benefit to the financial institutions to enhance their business practices and how the findings are related to the biblical framework. Recommendations for actions, recommendations for future study, study reflections, study summary, and conclusions was also discussed.

Section 3: Application to Professional Practice and Implications for Change

The purpose of this qualitative study was to understand the knowledge banks and CipherTrace possess about cryptocurrency-related money laundering transactions and their roles and responsibilities in mitigating those risks. CipherTrace is a blockchain analytics cryptocurrency intelligence company that protects financial institutions from virtual asset laundering risks and cryptocurrency-related assets. Founded in 2015, it has grown to have seven offices worldwide in Menlo Park, Toronto, New York, Washington, London, Frankfurt, and Singapore. CipherTrace currently has 150 customers comprising of banks, agencies, regulators, and Virtual Asset Service Providers (VASPs) and is funded by the U.S. Department of Homeland Security.

In this section, the researcher provides detailed findings from the interview process with the BSA/AML risk specialists, including bank managers, and compliance managers. The interview findings from the Director of Financial Investigations & Education at CipherTrace was presented as well. The findings discuss how the research study can be applied to professional practice and the implication for change.

Overview of the Study

The challenges posed by cryptocurrency for banks within the USA in order to identify and combat risks of financial crimes resulting in laundered money entering the banking system has increased since cryptocurrency came into existence. Since the inception of Bitcoin in 2009, its market capitalization has grown to over $200B, compared to American Express at $85.85B. With a news release on July 22, 2020, from the OCC (2020) all federally charted banks in the U.S. can provide custody services cryptocurrency; the challenge is now on banks. Following this, The State of Wyoming approved Karken’s application to be a crypto bank in September 2020.

The expectation is that Karken's clients in the US will be able to use the bank to conduct transactions in virtual and national currencies.

The BSA/AML risk specialists, including bank managers, compliance managers, and the Director of Financial Investigations & Education at CipherTrace, were the focus of this study. Some banks were unwilling to participate in the study due to potential reputational risks, although they were aware of the interview process and the confidentiality around the research study. As such, the researcher reached out to bank personnel directly through LinkedIn and mutual relationships; however, due to the bank employees' concerns and the bank's privacy, they declined recorded interviews. A consented recorded zoom interview was only conducted with the Director of Financial Investigations & Education at CipherTrace.

After receiving the approval from the Institutional Review Board (IRB), bank participants were sent recruitment letter/e-mail messages (Appendix C) followed by a consent form (Appendix D). Interviews were conducted using listed questions (Appendix A), while an interview for the Director of Financial Investigations & Education at CipherTrace was conducted using a different set of interview questions (Appendix B). Both sets of interviews were conducted with probing questions as needed.

The complete data from each interview were coded using a software program, MAXQDA (designed for computer-assisted qualitative analysis) with a great deal of emphasis on maintaining participants' confidentiality throughout the research study (Appendix E). MAXQDA helps streamline the research process by organizing the interview themes while keeping the participant's information confidential and secured with passwords (Oswald, 2017). The questions asked were intended to provide the researcher with emergent themes related to research questions (RQ):

RQ1 - What are the financial crime risks and challenges faced by banks when dealing with cryptocurrency?

RQ2 - How do banks identify and report suspicious account activities related to cryptocurrency?

RQ3 - What would help banks to minimize the financial crime risks and challenges that they face when dealing with cryptocurrency?

Each interview transcript ensured that the accuracy of data were maintained. Additional data for this study included some case studies obtained by the researcher through the Director of Financial Investigations & Education at CipherTrace. The data analysis process comprised of identifying themes that emerged from the interviews conducted with bank personnel. Although bank personnel positions varied, all participants responded to the interview questions through which data saturation occurred. MAXQDA software was used to code and identify emergent themes from the data. While responses to the interview varied in length and detail from each participant, it did not preclude the researcher from defining and analyzing themes. The researcher analyzed the data identifying several themes and sub-themes.

The research findings indicated that the bank personnel were not fully immersed in specifically identifying cryptocurrency transactions. At the same time, almost all bank personnel stated that they had never come across cryptocurrency transactions and were not aware of their banks, allowing such transactions. During the interview with the Director of Financial Investigations & Education at CipherTrace, it seemed banks were fully aware that cryptocurrency money laundering cases have been conducted using traditional banking products such as demand deposits and withdrawals. During the review of case studies, this was further validated that a majority of cryptocurrency cases resulting in Internal Revenue Service (IRS) indictment have been through peer-to-peer transactions. Throughout the findings section, the research participants are referred as RP.

Presentation of the Findings

The presentation of findings focused on interviews and case studies. Research participants were six BSA/AML Risk Specialists, one Financial Intelligence Unit (FIU) Manager, one Director of Due Diligence, one Financial Crimes Investigator, one Investigator, one Policy Implementation Manager, two Compliance Managers, and three Managers. Six research participants were from Bank #1, seven from Bank #2, and three from Bank #3, as shown in Table 3.

Table 3

Research Participants Demographic Information

Research Participant	Job Title	Bank No.	Bank Location	Number of Years at Current Position
1	Financial Intelligence Unit (FIU) Manager	1	San Francisco	3 years
2	Director of Due Diligence	1	San Francisco	4 years
3	BSA/AML Risk Specialist	2	San Francisco	32 years
4	BSA/AML Risk Specialist	1	San Francisco	3
5	BSA/AML Risk Specialist	3	San Francisco	1
6	Investigator	2	San Francisco	16
7	BSA/AML Risk Specialist	2	San Francisco	3
8	BSA/AML Risk Specialist	2	San Francisco	1
9	Financial Crimes Investigator	2	San Francisco	10
10	Policy Implementation Manager	3	San Francisco	3
11	BSA/AML Risk Specialist	3	San Francisco	7
12	Manager	1	San Francisco	2

13	Compliance Manager	2	San Francisco	12
14	Manager	2	San Francisco	1.5
15	Compliance Manager	1	San Francisco	6
16	Manager	1	San Francisco	4
N/A	Director of CipherTrace	N/A	Texas	2

Note. A total of 16 bank employees and one Director of Financial Investigations & Education at CipherTrace were interviewed.

Interviews - Banks

The research study results were analyzed using MAXQDA, which organized the data into different emerging themes. The interview responses collected from the study participants were uploaded in MAXQDA, which grouped and analyzed themes as depicted in Appendix E. The different themes produced were reviewed and linked to each other. A thorough discussion was given of each emerging theme dealing with saturation and triangulation. The findings include supporting direct quoted responses from the participants to support emerging themes. Each research question was linked to the obtained theme, conceptual framework, and previously published literature identified by the researcher in Section 1.

In qualitative research, triangulation by comprising data sources contributes to data saturation (Fusch et al., 2018). In this research study, the researcher attained triangulation by collecting data from multiple research participants from numerous banks with different job titles and CipherTrace. The researcher also utilized data from case studies, evaluating different money laundering and cryptocurrency-related money laundering cases across the U.S. Any differences between the attained themes of the researchers were highlighted and discussed in detail.

Qualitative Data Analysis

Data collection and analysis from the bank employees identified Know Your Customer (KYC) per Section 326 of USA Patriot Act, red flags-related to cryptocurrency, regulatory requirements including Financial Crimes Enforcement Network (FinCEN) guidance, transactions-related to cryptocurrency, Suspicious Account Reports (SARs), training, and advanced technology for transaction monitoring as emerging themes. Each theme was evaluated as they were critical in understanding the challenges banks face when dealing with cryptocurrency-related money laundering cases. Additionally, each theme that emerged from the research study was consistent with the conceptual framework conducted by Burrus (2018) and Marian (2015) in Section 1. Both theories highlighted the lack of knowledge about regulations, KYC policies (Customer Information Program and Customer Due Diligence), and the failure to identify suspicious activity accounts. The red flags associated with cryptocurrency-related accounts and transactions were additional themes identified in the conceptual framework. The literature reviews showed similar themes, along with the lack of advanced technology to identify inappropriate transactions.

Relationship of Interview Themes to Research Questions. At least one theme was related to the research questions. The emergent themes were verification, out of pattern, multiple transactions in a short period, SARs regulation, training, guidance, and advanced technology.

Research Question One: The theme of verification and purpose for accounts emerged from responses to interview questions (Appendix A), RQ1: What are the financial crime risks and challenges banks face when dealing with cryptocurrency.

Every research participant mentioned a similar process to verify documents for KYC as indicated in Appendix E. The bank customers are asked to provide documents such as country of citizenship, employment verification, and identification card for new bank accounts. The purpose of the account was a similar theme across the participants. To ensure account holders had legitimate documents and business, the purpose of transactions, and the reason for the movement of funds were required from the customers.

Research question one comprised of five different sub-questions. The first two sub-questions focused on the research participant’s role with the AML/BSA and the length of their current employment in respective roles. The three other questions focused on the KYC documents verification process and dealings with cryptocurrency-related cases.

All participants understood the verification process. Although participants represented different banks, all banks follow a similar process when verifying the KYC process and ensuring due diligence before a new account is opened. RP2 specifically mentioned a large amount of withdrawal as a concern with new account holders:

> There are various means to identify before allowing any large transactions. For example, at a retail office, for a large withdrawal, a customer may make a request ahead of time. If they are coming in to pick the cash, then proper government ID is required. For large transfers, a customer can initiate that at a retail office which requires identifying the signers. If requested via email or call, then the retail office or back office calls the customer to verify identity before processing the transaction.

RP3 mentions "proof of identity by using driver's license, country of citizenship, nature of business or account opening, employment letter" as some ways to verify KYC documents. The customer may be asked for a written explanation and proof of negotiated funds such as evidence of deposits or transfers, including relationships with the funds originator and funds beneficiary. RP12, RP13, RP14, RP15, and RP16 added social security number and debit and credit cards as other ways for KYC verification.

When asked about dealing with cryptocurrency-related money laundering cases, all except one participant mentioned they do not have much experience as cryptocurrency is new, and their banks do not have experience with clients with cryptocurrency accounts. RP2 stated that their bank "prohibited such client types as their bank is conservative and the new market and new trend was still under development for regulation and standards." RP13 did mention that "the cryptocurrency is trending and the bank is looking into expanding the guidance, and regulation to implement the process for crypto."

However, participant RP1 noted:

I have participated in cases where cryptocurrency transactions were identified and deemed to be unusual or suspicious. Generally, we review these cases with the same intent to understand the purpose of the transactions, to understand the pattern of the overall movement of the funds and to determine if the transactions make sense for the client.

Research Question Two: Themes such as structuring in a short period, and SARs emerged from RQ2: How do banks identify and report suspicious account activities related to cryptocurrency?

All participants named transactions out of pattern and multiple transactions known as structuring as one of the key red flags for any money laundering case, whether crypto-related or non-crypto-related. The unusual activity triggers additional customer verification, where sometimes the customers fail to verify reasons for large and multiple transactions. Once the account gets reviewed and analyzed, the banks file SARs to FinCEN.

Research question two contained three sub-questions that focused on the red flags pertaining to cryptocurrency cases, actions were taken against the suspicious activities, and the process followed for report suspicious activity. All of the participants representing different banks stated a high rate of transactions in a short period and a large amount of money as the key red flags for money laundering cases in general, as depicted in Appendix E.

Participant RP7 added that:

> Red flags are high volume of transactions, multiple and unusual transactions on a short period of time, and transactions across borders involving large amount of money are the main concerns for their banks. Once the banks spot these types of patterns, the account holders are questioned and SAR is filed to FinCEN following which the bank recommends to close the accounts.

Similarly, according to Participant RP8:

> Red flags are size and frequency of transaction, making multiple transaction in a short period of time and sending to users without recent activity, unverified documents, and inability of customers to explain transactions behind reason for large amount transferred in and out of accounts.

RP5 stated that in their banks, "the red flags for money laundering cases are unusual transactions for clients, multiple high-value transactions, no link to the client's business or home address, accepting funds from the unknown account." RP’s11 bank has not dealt with cryptocurrency money laundering. However, the participant thinks the red flags should be "the same as any other money laundering red flags, which are unusual transactions, a high volume of money transfer to unknown accounts. RP16 and RP17 also note that any red flags of cryptocurrency money laundering cases should be similar to traditional money laundering red flags.

When asked about actions taken against suspicious accounts recognized by the red flags and process followed to report the suspicions account, every participant noted SARs. SARs are filed when the account is deemed suspicious; hence, every bank follows the same process. Few research participants mentioned that law enforcement could get involved depending on the severity of the cases. RP1 said that in their bank when a suspicious account is tagged, "We follow our standard procedures – alert review, case review, and summary (if not suspicious) or SAR filed (if suspicious)."

According to RP15, when a suspicious account is identified, written policies and procedures are followed, cases are reviewed with appropriate managers, and eventually SARs are filed. RP4 stated that "banks standard procedures and processes are followed, reviewed, and a report is generated based on the findings. If the account is at high risk for suspicious, then a SAR is filed."

RP5 said, "I notify my manager, and as a team, bank procedures are followed to review the case, create report, and file SARs if needed." RP13 also files SARs and reports the case to FinCEN while involving law enforcement and closing the client's relationship if needed. RP2, RP7, and RP8 also stated that if the account is suspicious and filing a SAR, they have the right to close the relationship with the account holder. RP5 added that they are trained to "complete SAR and report to FinCEN and law enforcement if needed. The client's account can be closed, and they are put on a watchlist by the bank."

RP7 mentioned, “the bank follows FinCEN guidance and immediately reports any suspicious activities involving a large sum of money.” RP2 adds that if the cases are "egregious in nature and if an institution does not feel comfortable with the client, then the relationship should be closed to mitigate the risk." RP3 states that even though their bank has not experienced a cryptocurrency-related suspicious account, "as with any unusual activities, a suspicious report is filed with FinCEN." RP16 adds they "complete SAR and report to FinCEN and if the risk is too high close the account and involve law enforcement as needed."

Research Question Three: Training, guidance, and regulations were emergent themes from RQ3: What would help banks to minimize the financial crime risks and challenges that they face when dealing with cryptocurrency?

All participants mentioned that more in-depth training and guidance on cryptocurrency could help banks analyze and minimize cryptocurrency-related money laundering crimes, as depicted in Appendix E. As virtual currency is on the rise, the bank and its staff should have more guidance on dealing with the new threat to the financial industry. Following regulations and keeping up to date also helps banks protect them from cryptocurrency money laundering crimes.

Research question three comprised of four sub-questions. The first three questions are about how the banks are proactive in minimizing financial crimes in their organizations against cryptocurrency, some of the suggested ways to minimize financial crimes dealing with cryptocurrency, and how they stay in current compliance according to FinCEN's guidance to combat crime. All bank participants highlighted training, regulation, and guidance that the banks utilize to minimize cryptocurrency money laundering activities.

RP10 states that in order to minimize any potential cryptocurrency-related challenges, the bank "trains staffs on the recent trends relating to it, especially on case examples to see what alerts, transactions are involved, and what is suspicions." RP9 cites that "training could be given by the law enforcement who share red flags from real cases and elaborate when working on cases what to look for to identify a potential cryptocurrency case." According to RP1, the bank "has alerts that are designed to detect certain patterns of activity, including cryptocurrency transactions, and have additional monitoring and review for clients/business entities that are involved in the cryptocurrency space." RP11 also thinks cryptocurrency-related training can help banks fight crime.

RP5 states explicitly that:

> Training and conferences on ongoing issues can help. The banks can also have detailed case study trainings for new hires. Furthermore, the banks can provide trainings on advanced cryptocurrency, ways to detect them, and the regulations needed to conduct due diligence. The bank can also implement technology to fight high-risk crimes.

RP12 mentions training, conferences, and up to date regulation meetings as few ways to minimize the crime against cryptocurrency transactions. However, RP3 brings in a different perspective and states, "as with any other financial institution, there has to be possible consumer protection against fraud if any of the property (cryptocurrency) transactions are lost or stolen." Protection of customers is a way to minimize the banks from being made the target for cryptocurrency money laundering; hence, the banks can assure their full protection. Like all other research participants, RP10 added that "training staff, investigators, analysts/data analytics on cryptocurrency case" can help banks become more aware of cryptocurrency money-laundering.

On how banks are staying current with compliance regulations, all research participants suggested FinCEN regulations that banks can refer to and use as guidance. The participants suggest using FinCEN guidance to strengthen their regulatory policies, as depicted in Appendix E. RP10 states they stay current by "reading the financial crimes related to trends published on FinCEN's site, and regulators share some cases during seminars identifying the trend, red flags."

RP9 also thinks staying up-to-date with FinCEN's news on financial crimes and guidance is helpful and "the external training where law enforcement educates on cryptocurrency trend." RP12 frequently stated their staff attends training and conferences. RP11 shares that the bank has "various policies, procedures, and regulations to help the staff understand the process better." RP5 mentioned that the banks continuously update bank policies and tries to be in sync with regulations. RP8 also stated that staying current with FinCEN's guidance is how the banks are up-to-date with current regulations. RP16 added regulations and FinCEN as guidance in order to keep current with compliance regulations. Across the interviews, the regulation was a common theme.

RP1 shared their bank stays current with regulation where "the policy and procedure group regularly review our policies and procedures to look for any gaps in our structure to enhance our monitoring systems." RP3 shared that "as any other financial institution, there has to be a possible central authority monitoring the monetary and economic impact, including the exchange rate policy related to cryptocurrency transactions." According to RP4, "the banks has policies and regulation in place to help employees identify the suspicious account, have regular meetings to keep the employees aware of the new regulations and policies that will come in effect." RP13 shared that as the compliance manager role, they take compliance seriously, "We take compliance seriously at the bank. Every employee is supposed to follow the policies. The compliance operations team has oversight of the process, and the bank is always audit ready."

When asked about the challenges in identifying cryptocurrency cases, various types of responses were received. Although many research participants from AML/BSA risk specialists to managers and compliance managers had no experience with cryptocurrency cases, they think identifying the source of funds is the biggest challenge. RP5 said the challenges lie in "identifying fund source and client's information due to anonymous function of cryptocurrency." According to RP4, "some challenges are identifying the source of funds, identifying the real client as most of the virtual account holders can be anonymous," while RP2 states that "some of the challenges lack information about the parties engaged in a transaction and what was purchased." Although responding differently, the answers lead to the main issue of lacking essential information in identifying the cryptocurrency-related cases. The advanced technology to manage such cases is challenging the banks, and according to RP2, "some banks do not have the right infrastructure and controls to manage and identify such cases. The industry has seen some significant cases such as Silk Road."

In describing the challenges, RP1 thinks there are many challenges in obtaining information about the source of funds, "we participate in the 314(b) program and some other digital wallet providers also participate, but not all. If more of the cryptocurrency wallet providers participated in the 314(b) programs, the collaboration would be beneficial." This statement shows that not many financial institutions or wallet providers participate in the required programs; hence, it is challenging to understand the source of funds.

RP4 thinks some of the challenges in identifying the criminals are account holders being anonymous, where RP5 states that "identifying fund source and client’s information due to anonymous function of cryptocurrency" can be difficult for banks. RP6 also thinks that the "lack of client identification and senders and receiver's information" is challenging for banks to identify. Similarly, RP14 said, "some challenges can be identifying the source of funds and account holders due to their anonymous feature." RP7 and RP8 also see that lack of client identification makes it challenging for banks and employees to identify the cryptocurrency cases. Furthermore, according to RP7, "the lack of client identification and the lack of technology that the clients use to launder cryptocurrency" has been the hardest for banks. Moreover, RP7 added that "many banks still lack proper staff with cryptocurrency knowledge." RP7 is the only participant who thinks lack of staff is a challenge for banks to identify cryptocurrency cases.

Interview – CipherTrace

Data collection and analysis from the Director of Financial Investigations & Education of CipherTrace suggested banks fail to identify cryptocurrency-related money laundering transactions. As traditional money laundering has similar phases such as placing, layering, and integration, many banks do not understand the difference between traditional and cryptocurrency-related money laundering. Hence, they fail to implement proper tools and regulations to combat money laundering crimes. Responses from the Director of Financial Investigations & Education aligned with theories of Burrus (2018) and Marian (2015) which highlight lack of regulation, lack of KYC policies, and the inability of banks in identifying suspicious accounts and red flags associated with cryptocurrency-related accounts and transactions mentioned in Section 1.

Research Question One: What are the financial crime risks and challenges banks face when dealing with cryptocurrency?

Research question one comprised of five different sub-questions. The sub-questions focused on CipherTrace's perspective on money laundering, and the greatest risk banks face with cryptocurrency, and bank's knowledge on cryptocurrency-related cases. The Director was also asked to comment if cryptocurrency cases can be conducted using traditional money laundering.

During the interview, the Director of Financial Investigations & Education indicated that banks still lack the proper tools and training for cryptocurrency money laundering.

According to the Director:

> Cryptocurrency has three phases of money laundering crypto that you have in any other type of traditional money laundering scheme. Placement; How did they even get into the crypto system? Where did they acquire the crypto from? Where we can place it in some type of entity that can launder that, whether an exchange or P2P? Still there is layering and integration. It's all there but it is just done with different type of currency.

The Director's strong assertion in the interview was that the banks are still lacking the right tools, training, and education and therefore are at the most significant risk with cryptocurrency-related money laundering. The Director who joined CipherTrace from a bank understands banks structure and thinks many cryptocurrency money laundering transactions have similar features as traditional money laundering. The Director further states that the banks are not adequately staffed to handle cryptocurrency cases:

> Crypto is a full-time job for me, to keep up with crypto it's hard. It's a dynamic technology. You can't have somebody at the bank who is a BSA officer or head of investigation wearing the hat. It's impossible for them to do their daily work and keep up with crypto and then also train everyone else on crypto so banks need to engage third parties to help the banks manage cryptocurrency cases.

The Director also thinks that the Association of Certified Anti-Money Laundering Specialists (ACAMS) has a bigger role to play since it cannot teach virtual currency the way it teaches because a lot of information is incorrect. In a recent seminar attended by the Director, one of the ACAM representatives incorrectly said, "virtual currency is not regulated. But it has been regulated since 2013." By engaging the experts, the banks can obtain correct education, training, and information, minimizing any risks. Since traditional banking can be used to launder cryptocurrency, banks are at high risk. The Director highlighted the case example of Kunal Karla, who used traditional banking system to launder $25 million in cash and cryptocurrency.

Research Question Two: How do banks identify and report suspicious account activities related to cryptocurrency? Is their process efficient?

Research question two comprised of two different sub-questions. The sub-questions talked about steps banks can take in identifying cryptocurrency, and if, according to the Director of Financial Investigations & Education at CipherTrace, banks are compliant ready for KYC. If the banks are not complaint ready, the Director was asked to comment on the strategies and processes they can implement.

According to the Director, banks are not compliant ready as they cannot understand and identify cryptocurrency-related transactions. Recently, Director Kenneth Blanco, in a recent seminar, shared similar sentiments. As a result, the Director thinks banks should engage third parties to conduct due diligence and educate their employees on identifying cryptocurrency-related transactions.

The Director further states:

> Not all crypto is bad. There is good crypto and bad crypto. Step 1 is to identifying them which we have already said they can't efficiently do. No2 is accessing the proper risk to those transactions. If you can't identify the transaction then you can't do the due diligence.

Research Question Three: What would help banks to minimize the financial crime risks and challenges that they face when dealing with cryptocurrency?

Research question three consisted of four different sub-questions. The sub-questions focused on how banks can minimize the risks of cryptocurrency-related money laundering transactions, and if current regulations are sufficient to combat crime. Additionally, the questions were on how banks can stay current with regulations and the challenges in identifying cryptocurrency cases.

The Director reiterated that since banks are not efficiently identifying cryptocurrency-related money laundering transactions, they fail to conduct due diligence. To address this issue, banks should use external vendors while "educating and training the employees." Currently, CipherTrace is working with NICE Actimize (AML software) and CaseWare in helping banks identify suspicious wire transfers.

The Director further adds:

> It is impossible for banks to know if VASP A is high risk, VASP B is medium risk, and VASP C is low risk without understanding it better. Therefore, the banks are still at high risk and still not compliant. Even though many tools are available, banks need to utilize them appropriately and use external resources to help train their staff to identify cryptocurrency transactions.

Case Studies

Two sets of themes emerged from data collection and analysis of the case studies; KYC and Regulations, as depicted in Table 4. The sub-themes emerging from the main themes were appropriate AML laws, policies and procedures, technology, lack of knowledge, training, and lack of sufficient customer due diligence. Each theme was essential in understanding the challenges and issues banks encounter when combatting cryptocurrency-related money laundering. Burrus' (2018) and Marian's (2015) theories highlighted the lack of regulation, lack of KYC policies, and the inability to identify suspicious accounts and red flags associated with cryptocurrency-related accounts and transactions. The literature reviews expanded on utilizing appropriate technology to compete with the decentralized and anonymous feature of cryptocurrency.

Table 4

Emergent Theme Related to Research Questions from Case Studies

Research Question	Emergent Theme from Case studies
What are the financial crime risks and challenges banks to face when dealing with cryptocurrency?	Main theme: Regulation and KYC Sub-theme: Lack of Knowledge, Training, Lacking sufficient customer due diligence, and Technology
How do banks identify and report suspicious account activities related to cryptocurrency?	Main theme: Know Your Customer Sub-theme: Appropriate AML laws, Policies, Procedures and Technology
What would help banks minimize the financial crime risks and challenges they face when dealing with cryptocurrency?	Main theme: Regulation Sub-theme: Technology, Policies, Procedure and Training

Note. Research questions and related emergent themes from case studies.

Case Study Summaries

Case #1. On October 1, 2020, CipherTrace reported that the U.S. Department of Justice fined BitMEX, a cryptocurrency exchange and derivative trading platform, for violating the BSA and failing to maintain AML laws (Jevans, 2020). BitMEX executives intentionally failed to establish, implement, and maintain AML programs and procedures while generating transaction fees in USD 1B. The company had been under investigation since 2019, where they claimed to have improved the Customer Identification Program excluding U.S. persons effectively; however, the Commodity Futures Trading Commission (CFTC) found that not to be true.

BitMEX was found to have a deficiency in their AML policies and procedures, in addition to failing to comply with record-keeping and deleting critical customer identification information. The records were usually deleted to conceal the user's information in the U.S. or other restricted jurisdictions. Moreover, the company failed to file SARs and report suspicious accounts and activities. BitMEX was not just charged for deficiency in their laws but also fined for money laundering charges, where they allegedly operated an 'off-shore' crypto exchange while deliberately failing to implement and maintain necessary anti-money laundering policies.

In the light of all the charges, BitMEX was asked to improve their AML compliance programs, increase AML procedures, and monitor global compliance activities. The company hired a specialist to improve all the recommended process and report the progress to BitMEX's CEO and COO. After evaluation of BitMEX’s KYC, CipherTrace found that the crypto exchange company has improved on the practices, moving exchange from a porous score to a more robust KYC process.

Case #2. On February 27, 2020, CipherTrace, reported that on January 30, 2020, M.Y. Safra Bank (MYSB), with headquarters in New York City, was cited for having deficient anti-money laundering practices and monitoring of bank's customers (Clegg, 2020). The practice included cryptocurrency exchanges, Bitcoin ATM operators, virtual OTCs, and other crypto-related businesses. The bank was blamed for not thoroughly vetting its customers and transactions, lacking sufficient customer due diligence, and deficiency in investigating. The bank lacked KYC practices and deficient in the AML, and BSA policies prevented the bank from correctly identifying cryptocurrency-related transactions leading to money laundering customers. Although the bank was not fined for the absence of regulations, they were enforced to implement appropriate laws and regulations to detect the future's suspicious account.

Within the 90 days, the bank's board was asked to assign a compliance committee team for monitoring and overseeing the bank's compliance program, adhere to training programs educating their employees under the BSA, and train their employees to monitors and report suspicious activity appropriately. They were also asked to have policies to file SARs and develop an institution-wide BSA/AML Risk Assessment. Within 180 days, the authorities enforced M.Y.

Safra Bank to have qualified and experienced BSA Officer and adequate staff to correctly identify and rate customers who buy, sell, exchange, or administer cryptocurrency.

Case #3. In March 2020, FinCEN fined a former Chief Operational Risk Officer at U.S. Bank National Association (U.S. Bank) for $450,000 for failing to avert violations of the BSA (Financial Crimes Enforcement Network, 2020). Under his tenure at U.S. Bank as the former Chief Operational Risk Officer, the bank utilized an automated transaction monitoring software to spot potential money laundering suspicious activities; however, the system improperly capped the number of alerts. The automated monitoring system had limitations in targeting criminal activity. Additionally, the bank had limited resources and failed to efficiently assess the reduced number of accounts tagged for money laundering the automated transaction monitoring software. The regulators warned the Chief Operational Risk Officer that capping the number of alerts was not a proper way to access accounts, which prevented the proper filings of many SARs, restricting the regulators and law enforcement to combat the crimes fully, protecting others against the crime.

The law enforcement warnings and inquires stretched the resources thin by increasing the number of SARs and AML/BSA risk specialist workload; however, the former Chief Operational Risk Officer ignored those warnings and memos from his internal team. In 2018, the bank was fined for $185 million for ineffective BSA/AML programs and failed to file SARs promptly. In cases like these, FinCEN advises that banks use innovative technologies to help combat money laundering crime; however, the technology must be utilized proficiently.

Case #4. In 2019, Kunal Karla of Westwood was fined and sentenced to 18 months of possessing and operating an unlicensed money transmitting business, enabling the exchange of up to $25 million in cash and virtual money (U.S. Department of Justice, 2019b). Kunal Karla laundered money through unlicensed money transmitting business and not maintaining an effective anti-money laundering program. From 2015 to 2017, Kunal knowingly operated virtual currency, exchanging U.S. dollars for Bitcoin, charged commissions for exchanges costing at least $5000 per transaction, and dealt only with customers who were willing to exchange for $5000 per transaction, which mostly included criminals known to sell narcotics.

For the process, Kunal established bank accounts under fake business names, concealing his illicit business. Additionally, he operated ATMs for exchanging Bitcoins, profiting from each transaction. Furthermore, Kunal intentionally failed to identify his customers, and he failed to install cameras for customer identification. The law enforcement seized his bank account with almost $889,000, in addition to approximately 54.3 Bitcoin and other cryptocurrencies. Kunal committed similar money laundering crimes in Texas, supporting a drug trafficking network. His case was investigated by numerous authorities, including Drug Enforcement Administration, U.S. Immigration and Customs Enforcement's Homeland Security Investigations, the U.S. Postal Inspection Service, IRS Criminal Investigation, and the Los Angeles Police Department.

Case #5. In a similar case in 2018, Morgan Stanley Smith Barney LLC was charged a penalty of $10 million for deficiency in their AML programs and management failure for more than five years (Financial Industry Regulatory Authority [FINRA], 2018). FINRA discovered that the bank failed to properly conduct surveillance of the transactions while using several automated systems, where the systems did not capture wires and foreign transfers of more than tens of billions of dollars. The financial institution also failed to dedicate adequate employees to review accounts and transactions with red flags generated by the automated systems. Also, the AML staff closed many cases without performing due diligence.

Additionally, Morgan Stanely's AML department lacked experience monitoring customers' deposits and trades in a penny stock for possible suspicious activities, although the customers deposited large amounts, for example, 2.7 billion shares of penny stock, resulting in doubling the customers' profits. Moreover, FINRA found that Morgan Stanley was unsuccessful in implementing appropriate policies, procedures, and laws to control periodic reviews of foreign institutions' accounts. As a control measure, Morgan Stanley had to expand its AML-related programs, ensuring the financial institution dedicated sufficient trained staff to detect red flags. They improved the usage of automated transaction monitoring systems, revising its policies and procedures.

Case #6. In 2018, U.S. Bancorp paid $613 million in fines and penalties for inadequate anti-money laundering policies, where the criminals were able to launder a large amount of money successfully (Sweet, 2018). A customer Scott Tucker moved $2 billion in revenue to his illegal payday lending scheme. The crime was easily overlooked as the bank employees deliberately ignored the red flags in his case and neglected to not file the appropriate suspicious activity reports. The bank was held responsible for running an inadequate anti-money program from 2009 to 2014, failing to detect various suspicious transactions, and concealing their missteps from regulators. The U.S. Bank eventually restructured and broadened its anti-money laundering programs to identify red flags and trained their employees to identify and file anti-money laundering cases.

Case #7. Similarly, in 2018, Bank of America was fined $13 million by SEC and another $13 million by FINA for mismanaging their anti-money laundering responsibilities (Chunvoic, 2018). From 2006 to 2015, Bank of America lacked proper monitoring of nearly 12 million accounts and transactions where they failed to apply Mantas, the AML system that monitors the money flow. These accounts were later found to move around $105 billion to and from the bank in cash deposits and wires.

In 2011, Bank of America was fined $400,000 for a weak AML compliance program and written procedures on accepting checks from third parties for depositing into customers' accounts with no names on the checks. As a result, one of the customers moved $9 million from one account to another. The inadequate AML program was unsuccessful in detecting and reporting suspicious accounts related to such transactions. There were deficiencies in their automated monitoring programs, missing many accounts with red flags. Since then, the Bank of America has enhanced AML tools, added procedures for investigators related to red flags, and incorporated employee training programs regarding AML schemes and laws.

Case #8. In 2018, the U. S Treasury Department's Financial Crimes Enforcement Network FinCEN discussed their cryptocurrency approach and its innovation on financial institutions (JJ, 2018). Simultaneously, the agency highlighted the issues and complaints regarding suspicious transactions received by the agencies. Regulations were the common theme and key discussion points in many of the meetings. FinCEN has seen a surge in SAR filling over the years due to an increase in cryptocurrency-related money laundering. As a result, many financial institutions have been advised to develop, implement, and maintain AML programs to prevent money laundering.

Relationship of Case Study Themes to Research Questions. At least one theme from each case study was related to the research questions. The emergent themes were AML laws, policies and procedures, technology, and lack of knowledge. Additional themes were training and lacking sufficient customer due diligence.

Research Question One

The theme of regulation and KYC and sub-themes of lack of knowledge, training, lacking sufficient customer due diligence, and technology emerged from the first research question, as shown in Table 4, What are the financial crime risks and challenges banks to face when dealing with cryptocurrency?

Case 1, 3, 4, 6, and 7 demonstrated that banks lack knowledge of cryptocurrency and KYC training. The rising interest in cryptocurrency by criminals has hindered the bank's ability to have a robust investigation and customer due diligence procedures, leading the banks to pay a hefty penalty. The banks' challenge with advanced technology prevented them from correctly identifying cryptocurrency-related transactions leading to money laundering customers. The banks were blamed for not thoroughly vetting their customers and transactions, lacking sufficient customer due diligence, and deficiency in investigating.

Research Question Two

The theme of KYC and sub-themes appropriate AML laws, policies, procedures, and technology are related to the second question, How do banks identify and report suspicious account activities related to cryptocurrency?

Cases 1, 2, 4, 5, and 6 discussed how banks identify and report suspicious accounts. Having a well-established KYC policy is one way many banks identify and verify their customers and clients to ensure customer details are verified. A robust KYC policy can help banks identify accounts intended for criminal purposes early. Technology such as automated systems or software plays a key role in helping with KYC policies. Banks frequently use automated transaction monitoring software to identify potential money laundering suspicious activities, wires, and foreign transfers of more than tens of billions of dollars. Additionally, the

AML laws, policies, and procedures and policies help the employees identify suspicious cases and file SAR.

Research Question Three

The theme of regulation with sub-theme technology, policies, procedures, and training was linked to the third research question, What would help banks minimize the financial crime risks and challenges they face when dealing with cryptocurrency?

As cryptocurrency becomes more common, the decentralized and pseudonymous currency can easily hide behind advanced technology to continue the trade and increase illicit money flow. Banks fined for weak regulations for cryptocurrency-related money laundering lacked innovative technologies to combat money laundering crime, or the technology was utilized incompetently. The banks were asked to utilize adequate technology, automated software, or systems to identify money laundering cases and transactions. The improved usage of an automated transaction monitoring system was suggested.

Due to insufficient knowledge on cryptocurrency-related money laundering, the banks suffered monetary loss; however, they increased effective training, monitoring systems, and staff to combat money laundering crime. Furthermore, the anonymous and decentralized feature of the virtual asset prevented banks from tightening the KYC verification process. The case studies presented highlight the regulations and KYC policies as the main issues with many banks. The deficiency in the regulations around KYC increased the banks' fines, leaving them behind the innovative features of cryptocurrency. The deficiency in anti-money laundering practices and monitoring of bank customers were discussed in almost every case, and banks were blamed for not accurately monitoring transactions and showing a lack of due diligence when verifying customers.

According to the spring 2020 CipherTrace report, in the first five-months of 2020, cryptocurrency thefts totaled $1.36 billion, which is already more than $169 million in 2016. In the past four years cryptocurrency has seen a steep increase in the theft and money laundering associated with the virtual currency. The coronavirus pandemic has not slowed down the crime or the criminals, as the criminals successfully sold cryptocurrency on the dark web through phishing sites. The percent of funds sent from U.S. Bitcoin has doubled since 2017.

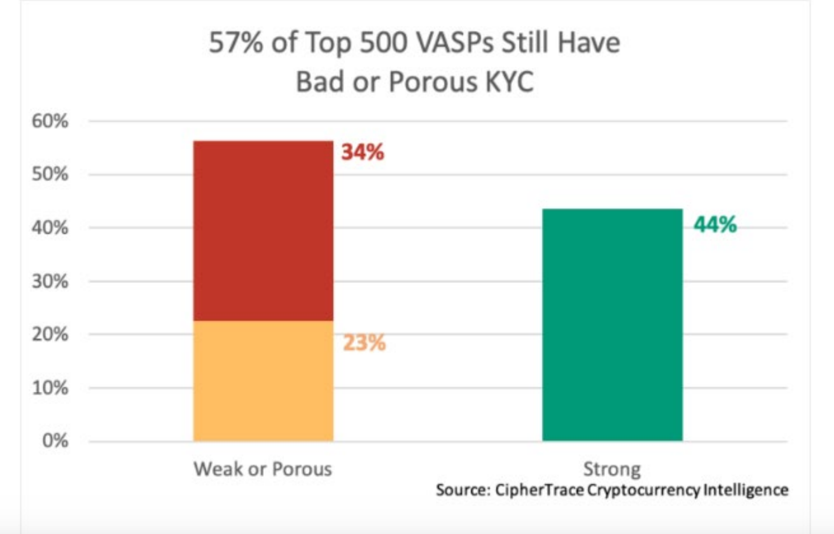
However, criminals have increased the cross-border exchange, underlining the importance of global AML/BSA and cryptocurrency regulations. As cryptocurrency has tightened the KYC and AML laws and policies, the technology-savvy criminals layered funds through multiple private accounts. Research presented by CipherTrace in the fourth quarter of 2019 Cryptocurrency Anti-Money Laundering (CAML) report shows that even though cryptocurrency can be exchanged through the dark web, banks increase the crime as 8 out of 10 U.S. retail banks harbor illicit cryptocurrency accounts and transactions. According to the report, a top 10 U.S. retail bank can process up to $2 billion in cryptocurrency-related transactions annually without being detected.

Banks must identify any cryptocurrency transactions, just like identifying any regular money laundering cases. The digital customer, in particular, should be carefully monitored as not identifying them can lead to operational, legal, and financial risks to the banks. Hence, utilization tools like CipherTrace Armada can help financial institutions identify virtual customers, flag cryptocurrency transactions, and perform due diligence. The utilization of such tools can enable banks to grow their clients' base by understanding the transactional risk associated with cryptocurrency accounts.

The KYC is still weak in VASPs, and financial institutions are still lacking robust KYC policies and processes. CipherTrace has analyzed all exchange and bank processes and rated them either by weak, porous, or good based on money laundering after opening virtual accounts. The weak KYC process makes it difficult for banks to identify cryptocurrency-related money laundering and terrorism financing. CipherTrace has also found that 57% of VASPs are weak or porous, as shown in Figure 4.

Figure 4

Know Your Customer VASPs



Source: CipherTrace Cryptocurrency Intelligence

Note. North America still lacks knowledge on KYC, and more than 50% of VASPs are weak, with less than 50% VASPs with strong knowledge.

The weak KYC process oversees the collection and verification of customer's personal information, including a government-issued ID, phone numbers, email address, and physical address (CipherTrace, 2020). Once these identities are overlooked, the criminals find ways to increase money laundering activities without being under the bank's surveillance. The criminals are well aware of the different KYC jurisdictions and procedures; therefore, when the financial institutions are weak, they try to complicate their funds' flow, making it harder for banks to track them.

The cryptocurrency money laundering process can weaken KYC laws making the VASP a go-to place, allowing the criminals to operate freely without any monitoring or regulations. Additionally, the decentralized feature of cryptocurrency increases peer-to-peer trading, lacking many KYC processes, as not many financial institutions are advanced or understand the decentralized process. In contrast, robust KYC can mitigate money laundering by obtaining users' real identities involved in suspicious accounts and transactions. The robust KYC also prevents criminals from registering with fake or stolen identities, making money laundering much tougher. The strenuous KYC process requires numerous identification and verification processes, making the depositing, and withdrawal process easy.

Research Finding Summary

The qualitative case study research findings focused on interviews from the bank employees, the Director of Financial Investigations & Education at CipherTrace, and case studies. A summary of each theme was analyzed, presented, and linked to the study research questions. The emergent themes of lack of knowledge about KYC policies (Customer Information Program and Customer Due Diligence), regulations and failure to identify suspicious activity accounts were consistent with the literature review and Burrus' (2018) and Marian's (2015) conceptual theories mentioned in Section 1.

Relationship of Research Findings Themes to Research Questions. The emergent themes from bank employees, CipherTrace, and case studies were verification, out of pattern, multiple transactions within a short period, SAR regulations, training, guidance, and advanced technology. Additional themes were AML laws, policies and procedures, lack of knowledge, and lacking sufficient customer due diligence.

Research Question One

The theme of verification, the purpose for account, regulation and KYC, sub-themes of lack of knowledge, training, lack of sufficient customer due diligence, and technology emerged from RQ1, What are the financial crime risks and challenges banks face when dealing with cryptocurrency?

The bank interviews and case studies demonstrated that even though banks have KYC policies, they still lack knowledge of cryptocurrency, KYC training, and appropriately identifying cryptocurrency suspicious accounts. During the interview, almost all bank employees had little to no experience in cryptocurrency cases; hence, the employees lacked sufficient knowledge and training on cryptocurrency-related transactions. Although employees participated in cryptocurrency-related cases, they did not deal with cryptocurrency related money laundering transactions directly. In contrast, CipherTrace believes banks have encountered cryptocurrency-related transactions; however, they lack the proper tools in identifying money laundering cases.

According to JJ (2020) every bank should hold themselves accountable for any cryptocurrency-related transactions. They should be able to identify and report suspicious activities. Through research, CipherTrace discovered that many banks do not have the right education and guidance on monitoring cryptocurrency-related transactions accurately. Since issuing the guidance on virtual currency regulation, FinCEN has received around 10,000 cryptocurrency-related SARs from at least 1,900 entities.

JJ (2020) further added that many banks and financial institutions try to use internally built systems to identify clients with cryptocurrency-related accounts and transactions. In comparison, other banks try to match names from the cryptocurrency exchanges and other VASPs compared to their customer base. The matching process often gives false positive where the banks internal matching system misses many actual cryptocurrency-related money laundering activities and transactions. Also, many lists are incomplete, leaving out many exchanges. For example, out of 700, only 100 exchanges are detected. Additionally, many cryptocurrency exchanges do not do business under their popular name; hence, name matching is insufficient to identify all red flags, missing 70% or more of the crypto exchanges, including 90% of the actual transactions.

Research Question Two

Themes such as out of pattern, multiple transactions in a short period, SAR regulations, education including training the employees, KYC, AML laws, policies, procedures, and technology emerged from RQ2, How do banks identify and report suspicious account activities related to cryptocurrency?

Bank employees named red flags related to money laundering as out of pattern, multiple transactions in a short period as few of the ways to identify suspicious accounts. Once the red flags were identified, FinCEN guidance were followed, and SARs were created as needed. Although many bank employees did not directly experience cryptocurrency related money laundering transactions, they mentioned any case egregious in nature is treated as a risked case, and the relationship with the clients can be closed. CipherTrace thinks banks need external vendors and education on identifying cryptocurrency-related money laundering transactions. As banks are not complaint ready, the Director of Financial Investigations & Education pointed out banks cannot identify the cryptocurrency-related transactions; hence they lack due diligence.

Case study findings showed that automated systems could identify suspicious accounts, although many automated systems are limited to identifying and targeting the criminals; hence many cases were not tagged as suspicious accounts. In the case studies, banks failed to proficiently evaluate the number of accounts tagged for money laundering due to a lack of knowledge on cryptocurrency and limited resources with sufficient knowledge. Numerous banks lacked the implementation of proper laws, policies, and procedures to review accounts with due diligence. Some showed banks intentionally ignoring the red flags in some cryptocurrency-related money laundering cases; hence no one filed the suspicious activity reports as required. The investigations process was weak, with banks weak regulations and guidelines. The banks frequently have inadequate anti-money laundering programs with limited resources or with staff lacking the required knowledge to identify the red flags associated with the money laundering cases.

Research Question Three

Training, FinCEN guidance, regulations, advanced technology, and engaging third parties were emergent themes from RQ3, What would help banks minimize the financial crime risks and challenges they face when dealing with cryptocurrency?

Bank employees cited regulation, training, and FinCEN guidance needed to minimize the financial crime risks and challenges they face when dealing with cryptocurrency. Considering lack of exposure to cryptocurrency cases, bank employees mentioned receiving training and education, attending seminars and conferences on existing cases as ways in identifying cryptocurrency-related cases. Training on ways to detect cryptocurrency and regulation was needed to conduct due diligence, as highlighted in the findings. In contrast, the Director of Financial Investigations & Education strongly recommended engaging a third party in minimizing risks of cryptocurrency-related money laundering transactions. CipherTrace has relations with NICE Actimize (AML Software) and CaseWare to help banks integrate into AML solutions and identify cryptocurrency-related transactions.

According to the Director of Financial Investigations & Education at CipherTrace, many bank personnel may not be aware that their banks have conducted cryptocurrency-related transactions using traditional banking methods such as demand deposits and withdrawals. Case #4 is one recent example where Kunal Karla laundered $25 million using traditional bank accounts. Although the banks followed the KYC process, they lacked due diligence in Kunal's case. Because many banks lack appropriate tools to identify such cases, makes the banks susceptible.

Sharing a personal experience, the Director of Financial Investigations & Education at CipherTrace buys and sells cryptocurrency through Coinbase and uses a personal bank to transfer funds. Since Coinbase has a well-structured AML program, the bank does not need to worry about cryptocurrency transactions. However, unregulated systems such as BitQuick allow anyone to buy and sell Bitcoins instantly for cash deposits into banks or credit unions without regulations. As shown in Appendix F, one can purchase Bitcoin in four steps at any of the fourteen banks and credit unions. In the example shown, it can be seen in step 4 that Bitcoin can be purchased after selecting Bank of America and depositing in a business account. This simplicity in purchasing Bitcoins shows ineptness by banks and credit unions in monitoring transactions relating to cryptocurrency.

Findings from the bank research participants also supported this statement. RP1 and RP2 both work for the same bank; however, RP1 was exposed to cryptocurrency cases, but RP2 was not. Both research participants from the same bank had different experiences in dealing with cryptocurrency-related transactions, especially in their respective roles. This difference shows that banks have internal gaps in training and educating their employees thus failing to understand cryptocurrency and associated regulations.

Case studies showed how banks can enhance their regulations, policies, and procedures by adhering to effective training programs while educating their employees under AML/BSA to successfully report suspicious activities. Hiring experienced, adequate, and dedicated staff and training the current employees to identify money laundering cases was suggested by regulators in order to decrease suspicious account activities by tightening banks policies and procedures and following regulations and laws. Case studies also illustrated that failure to understand and identifying cryptocurrency-related money laundering activities have resulted in significant penalties and fines to banks.

Applications to Professional Practice

Bank's unawareness of unregulated systems like BitQuick, Luno, and Binance allows anyone to buy and sell Bitcoins for cash deposit into bank accounts, enabling them to engage in cryptocurrency-related transactions unwillingly. With the emergence of Kraken, a cryptocurrency exchange trading platform attaining a U.S. Banking license, banks now need to consider cryptocurrency-related transactions as risks. Since cryptocurrency-related transactions are now part of many banks through unregulated systems resulting from deposits in bank accounts, the challenge lies in efficient and robust regulations to mitigate money laundering and financial risks. The research findings present an opportunity for banks to venture into cryptocurrency-related transactions guided by stringent regulated policies and procedures.

According to Rexrode (2018), since many big banks refuse to deal with cryptocurrency, this opens an opportunity for small banks such as Silvergate Bank. San Diego-based Silvergate

Bank, a three-branch lender heavily focused on local businesses, doubled its assets to $1.9 billion from $978 million, mainly from cryptocurrency-related business. According to Castillo (2020), Silvergate Bank's initial risks in dealing with cryptocurrency has resulted in its cryptocurrency assets increasing to $2.1 billion as of September 30, 2020, compared to $1.5 billion as of June 30, 2020. The high risk and high reward strategy by Silvergate suggest that banks who are conservative about cryptocurrency should progressively venture towards accepting the virtual currency.

The findings from this study identified training, KYC, and regulations as the foundations that can help bank personnel to understand the nature of cryptocurrency. Additionally, utilizing third-parties such as CipherTrace could assist banks in adequately identifying and reporting suspicious accounts. Compared to traditional money laundering, cryptocurrency-related money laundering has advanced features such as ensuring pseudo-anonymity and independence from central authority (Lansky, 2018), prompting banks to seek the expertise of third parties.

The study's finding indicated that bank employees only have experience with traditional money laundering cases, making it challenging for banks to address cryptocurrency-related cases. As suggested by most bank employees, training can enhance their knowledge of cryptocurrency cases from presentations and exposure to crypto-related cases. Additionally, ongoing training, attending seminars and conferences can develop bank employees, making them competent to combat cryptocurrency-related accounts and transactions. Curry (2019) recommends that formal training assessment and AML training are needed to stay abreast of any trends, acting as a powerful strategic tool to banks. He further adds that the strategy can also help determine appropriate staff to train.

The interviews and case study findings demonstrated KYC as a critical process for banks in understanding to combat cryptocurrency-related money laundering. As KYC laws and FinCEN guidance get updated and restructured, the banks should adapt to new laws to avoid their program deficiencies. According to the case studies, robust KYC policy, programs, and systems utilized caused banks failure to identify cryptocurrency-related transactions leading to money laundering. KYC ensures transaction transparency, confirming accounts legitimacy by monitoring money movement. Customer validation is essential to ensure no client is involved in any money laundering activities, and a robust KYC process reiterates that banks have to confirm the account holder's identity as the financial institutions need to know fund source (Arasa & Ottichilo, 2015).

The Director of Financial Investigations & Education at CipherTrace suggested banks should work with external vendors to identify cryptocurrency cases and transactions as they may lack proper tools, expertise, and experienced staff to understand cryptocurrency transactions adequately. FinCEN has stated that it is the financial institution's responsibility to identify and report suspicious accounts (JJ, 2020); however, if the banks do not participate in cryptocurrency transactions, they may be unaware of the programs and tools needed to identify the cases. As cryptocurrency emerges in the market, external vendors can play a crucial role in helping banks educate their staff in understanding and reducing cryptocurrency money laundering risks. Some bank employees mentioned that law enforcement could share red flags from real cases to educate the employees in identifying probable cryptocurrency cases. Therefore, applying the current programs, right tools, appropriate system, and knowledge from external vendors can improve bank practices towards cryptocurrency money laundering cases.

As suggested by many bank employees, regulations play a critical role in money laundering cases. The Office of the Currency's Comptroller hopes the agency can develop more regulatory guidance helping banks transition from traditional banks to cryptocurrency adopting institutions (Sun, 2020). During the interview, bank employees and the Director of Financial Investigations & Education stated following guidance from FinCEN makes banks effective and efficient in combatting cryptocurrency-related money laundering. Ineffective regulations have caused many banks to struggle with money laundering cases resulting in paying hefty fines (U.S. Government Accountability Office, 2016). Additionally, the damage caused to financial institutions by lack of regulations can be a source of customer loss. Specific regulations and guidance may help financial institutions diligently monitor accounts and transactions, reducing money laundering risks (Obie & Rasmussen, 2018). The outcome of applying regulation and guidance can effectively and proficiently improve banks knowledge of cryptocurrency.

As Paul wrote to the Romans, “Everyone must submit himself to the governing authorities, for there is no authority except that which God has established.” To improve the financial institution's laws, policies, and procedures, following government instructions are crucial. Romans 13:1 state, “Let every person be subject to the governing authorities. For there is no authority except from God, and those that exist have been instituted by God.” The demonstration of obeying laws and government is outlined in the Bible. The Bible mentions the relationship between believer and government and states that one should obey the government, as he created government and laws (GotQuestions.org, 2010). Therefore, obeying and following government created laws is a way to be obedient to God. Similarly, banks following regulations and guidance created by regulatory authorities illustrate following the authority established by God.

Recommendations for Action

Cryptocurrency has developed a reputation of having questionable challenges to financial institutions. Although it brings in many opportunities such as independence from traditional banking to having no access to bank accounts (Dyntu & Dykyi, 2018), it challenges the banks in identifying suspicious accounts and flagging accounts for potential money laundering. While banks are continually working to improve their AML/BSA programs, the decentralized and anonymous virtual currency feature and its changing features threaten the banks in keeping up with updated regulations (Demertzis & Wolf, 2018).

To reduce the challenges faced by cryptocurrency, banks should effectively implement training processes. Cryptocurrency is a complex, fast-growing market; hence a robust and effective training process ensures bank employees are prepared for cryptocurrency money laundering cases. This research study's findings showed that almost all bank employees think the traditional money laundering process can be applied to cryptocurrency-related cases.

The study results indicated that training and exposure to cryptocurrency cases could effectively increase bank employees' education and knowledge. Comprehensive training and employee development augment employee quality, increasing job satisfaction, morale, motivation, and efficiency in strategy and process (Kumar & Siddika, 2017). Both authors further add training as a crucial component that provides significant emphasis and information needed to perform the job. As the bank employees also indicated, training and conferences can help close the gap, improving the organization's approach towards cryptocurrency-related money laundering cases.

This study's results demonstrated that training describes an employee's ability to accomplish roles and responsibilities in financial institutions. Therefore, training on important factors in identifying a suspicious case, such as KYC, would benefit AML/BSA specialists, managers, and compliance managers as nearly all research participants from all three banks lack sufficient training and exposure to cryptocurrency accounts. The improved process most likely can increase bank reputation, attracting customers with cryptocurrency accounts for secure transactions. Data shows that banks dealing with cryptocurrency are more profitable over banks who refused to deal with cryptocurrency (Rexrode, 2018).

Case studies demonstrated a robust KYC process as another way to reduce cryptocurrency-related money laundering. According to all the case studies, banks were penalized for lacking KYC practice with a deficiency in their AML and BSA policies. The lack of KYC policies does not allow banks to identify cryptocurrency-related transactions appropriately. When banks utilize a robust KYC policy, they combat crimes better to ensure their customers' safety while understanding and addressing the potential of money laundering (Arasa & Ottichilo, 2015). According to Rueckert (2019), standard KYC programs might be too weak for the pseudonymous digital virtual asset outside the current jurisdiction. Therefore, the financial institutions have to strengthen their policies and maintain a sophisticated KYC program capturing pertinent information about account holders (Forgang, 2019).

Additionally, to reduce the high number of cryptocurrency-related money laundering cases, regulations and guidance are essential. Falling out of both regulation and guidance indicates an institution's weakness in being compliant. Complying with BSA and AML laws and implementing regulations help detect and report suspicious activities. With cryptocurrency's enhanced technology, the virtual asset has gained new opportunities in the market (Forgang, 2019); therefore, the regulation should be appropriately applied. According to the Director of

Financial Investigations & Education at CipherTrace, banks are not compliant ready, and if they cannot identify suspicious transactions, then there is no due diligence.

Adding stringent regulations can ease the bank's fear of accepting virtual currency accounts to reduce the gap between proper transaction identification and cryptocurrency-related money laundering. As the case study findings presented, banks should be up-to-date with the FinCEN guidance. The senior management and compliance managers running the department must be up-to-date with regulations by attending conferences, seminars and educating them and their staff on financial crime trends. Improved training, KYC process, and regulations can eliminate the bank's fear of dealing with cryptocurrency-related accounts.

Money laundering can have a corrosive effect on banks; thus, providing training, being in compliance, and following recommended guidance and regulations can lower money laundering risks, specifically cryptocurrency-related money laundering. The price paid for training, conferences, and regulation will have a positive impact on banks. Similarly, engaging in third parties can enable banks to better implement appropriate laws, tools, and programs in mitigating cryptocurrency-related money laundering risks.

Recommendations for Further Study

The research study's scope focused on the bank employees and CipherTrace's knowledge of cryptocurrency-related money laundering transactions and mitigating associated risks. The research participants included BSA/AML risk specialists, bank managers, compliance managers, and the Director of Financial Investigations & Education at CipherTrace. The outcome from the research findings suggested that further studies should be conducted in this field to understand the challenges banks face when dealing with cryptocurrency-related money laundering.

Financial institution's relationship with cryptocurrency is not new, but banks remain uncertain about their role in preventing cryptocurrency-related money laundering. As long as the banks knowledge of cryptocurrency-related money laundering is limited, they will continue to be deficient in their AML policies and procedures. The banks lack awareness in training, implementing proper systems and programs, and regulations prevent them from thoroughly mitigating cryptocurrency money laundering risks. Additionally, the lack of appropriately trained employees further exposes the banks to cryptocurrency-related money laundering risks.

Opportunities exist for further research in this field if banks discard fear of reputational risks by allowing their employees to participate in research studies. The knowledge gained from the research studies can help banks improve their internal processes to mitigate cryptocurrency risks. In this research study, many banks refusal to participate due to fear of disrepute, limited the researcher from obtaining insight into banks experience, process, and procedures in combating cryptocurrency-related money laundering. Future studies should include banks support without fear of reputational risks, increasing their employees' participation, while sharing their experiences with cryptocurrency-related money laundering transactions, training, and knowledge.

Reflections

The research findings on investigating banks processes and experience in combating cryptocurrency-related money laundering surprised the researcher. The researcher had preconceived expectations that banks would play an active role in allowing bank employees to participate in the research study. Moreover, the researcher anticipated more bank employees to be involved in cryptocurrency-related money laundering cases. However, the outcome was that

AML/BSA risk specialists, bank managers, and compliance managers lacked experience in dealing with cryptocurrency transactions or accounts.

The researcher had no bias towards the study but expected detailed responses from the research participants. Due to bank employees' lack of participation and experience in cryptocurrency money laundering cases, their responses were limited but analogous during the interview. The researcher feels the banks can improve on cryptocurrency knowledge from the research findings if they are aware of the tools available in identifying cryptocurrency-related transactions.

Banks explicitly limit themselves in the world of virtual currency by impacting their employees' ability to address cryptocurrency-related money laundering. Furthermore, as the banks deny service to cryptocurrency customers, their chances of generating additional profit are limited. As the Bible says, all hard work brings a profit. Proverbs 21:5 states, "The plans of the diligent lead to profit as surely as haste leads to poverty." For banks, the cost of educating and training employees and implementing appropriate tools to combat money laundering crimes can be worth an investment.

Summary and Study Conclusions

The research findings demonstrated that bank employees are not exposed to cryptocurrency-related money laundering and lack knowledge of cryptocurrency challenges that banks may face. The findings indicated that training and exposure to cryptocurrency-related cases and transactions do not exist in many banks, especially with increasing risks from unregulated systems that allow Bitcoins to be purchased through bank accounts. However, according to the Director of Financial Investigations & Education at CipherTrace, banks are exposed to cryptocurrency-related money laundering, but the lack of proper tools and well-trained employees hinders them from identifying cryptocurrency money laundering transactions.

According to FinCEN, failure to have appropriate compliance staff to meet regulatory requirements can result in fines up to $25,000 each day. In order to mitigate such risks, the Director of Financial Investigations & Education at CipherTrace suggested that banks either utilize external vendors to help them identify suspicious cases or implement appropriate tools and build cryptocurrency in their training modules to help identify such cases. Supporting the Director of Financial Investigations & Education's statement, case study findings also demonstrated evidence of bank's lack of knowledge about KYC policies (Customer Information Program and Customer Due Diligence) in identifying cryptocurrency-related money laundering transactions.

The case studies found a deficiency in several banks' AML/BSA programs and their failure to implement and follow proper AML/BSA regulations and FinCEN guidance. Additionally, the inexperienced employees' failure to correctly identify clients with the intent to launder money led many banks to pay hefty penalties. Furthermore, case study findings showed that innovative technology and stricter regulations could be new ways to address and transform AML/BSA challenges and processes.

The research findings indicated that attention to cryptocurrency transactions and education and training on cryptocurrency-related cases should be a stronger focus from all banks. Furthermore, utilizing technology and following FinCEN guidance and regulations for cryptocurrency-related transactions may benefit the banks. With appropriate education and training, the bank employees will be more knowledgeable and experienced in dealing with cryptocurrency-related accounts. Understanding the banks experience in cryptocurrency-related money laundering can be developed further through detailed research studies, with cooperation from banks without fear of reputational risks, resulting in improved programs and systems to identify cryptocurrency accounts.

References

Abel, A. S., & MacKay, I. A. (2016). Money laundering: combating a global threat. *Journal of Accountancy*, *222*(3), 44–49. https://search.proquest.com/openview/d812d456a6ed41f3487a77c0fdeea4e9/1?pq-origsite=gscholar&cbl=41065

Abramowicz, M. (2016). Cryptocurrency-based law. *Arizona Law Review*, *58*, 359–420. https://arizonalawreview.org/pdf/58-2/58arizlrev359.pdf

Adams, J., Bateman, B., Becker, F., Cresswell, T., Flynn, D., McNaughton, R., Oluboyede, Y., Robalino, S., Ternent, L., Sood, B., Michie, S., Shucksmith, J., Sniehotta, F. F., & Wigham, S. (2015). Effectiveness and acceptability of parental financial incentives and quasi-mandatory schemes for increasing uptake of vaccinations in preschool children: Systematic review, qualitative study, and discrete choice experiment. *Health Technology Assessment*, *19*(94), 1–176. https://doi.org/10.3310/hta19940

Adeleke, I., Zubairu, U. M., Abubakar, B., Maitala, F., Mustapha, Y., & Ediuku, E. (2019). A systematic review of cryptocurrency scholarship. *International Journal of Commerce and Finance*, *5*(2), 63–75. http://oaji.net/articles/2019/2748-1570514344.pdf

Afzal, A., & Asif, A. (2019). Cryptocurrencies, blockchain and regulation: A review. *The Lahore Journal of Economics*, *24*(1), 103-130. http://lahoreschoolofeconomics.edu.pk/EconomicsJournal/Journals/Volume%2024/Issue%201/05%20LJE01%20Afzal%20ED%20AAC%20ttc.pdf

Ahmad, S. (2019). Corruption and money laundering. *International Journal of Government Auditing*, 29–30. http://intosaijournal.org/site/wp-content/uploads/2019/04/INTOSAI-Journal-Spring-2019_Corruption-and-ML-Nexus_SAI-Pakistan.pdf

Alexandre, A. (2019, August 12). Cyber criminals netted $4.3B from crypto-related crime in 2019: Study. COINTELEGRAPH. https://cointelegraph.com/news/cyber-criminals-netted-43b-from-crypto-related-crime-in-2019-study

Alpi, K. M., & Evans, J. J. (2019). Distinguishing case study as a research method from case reports as a publication type. *Journal of the Medical Library Association*, *107*(1), 1–5. https://doi.org/10.5195/jmla.2019.615

Al-Qadi, N. S., Al Haj, A. A., Matar, M. M., & Hathloul, M. (2012). The positive and negative role for banks in money laundering operations. *Canadian Social Science*, *8*(5), 13–23. https://doi.org/10.3968/j.css.1923669720120805.1742

Alsaif, K. I., & Ramo, R. M. (2018). The role of banks in reducing the phenomenon of money laundering. *International Journal of Computer Applications*, *180*(17), 21–26. https://doi.org/10.5120/ijca2018916386

Al Tajir, G. K. (2018). Ethical treatment of participants in public health research. *Journal of Public Health and Emergency*, *2*(1). https://doi.org/10.21037/jphe.2017.12.04

Aluise, D. M. (2017). Financial regulation case study: bank secrecy act, anti-money laundering law compliance, and blockchain technology [Harvard Law School Case Study]. https://www.google.com/search?q=Aluise%2C+D.+M.+(2017).+Financial+regulation+case+study%3A+bank+secrecy+act%2C+anti-money+laundering+law+compliance%2C+and+blockchain+technology&oq=Aluise%2C+D.+M.+(2017).+Financial+regulation+case+study%3A+bank+secrecy+act%2C+anti-money+laundering+law+compliance%2C+and+blockchain+technology&aqs=chrome..69i57.380j0j8&sourceid=chrome&ie=UTF-8

Amin, M., Nørgaard, L., Cavaco, A. M., Witry, M. J., Hillman, L., Cernasev, A., & Desselle, S. P. (2019). Establishing trustworthiness and authenticity in qualitative pharmacy research. *Research in Social and Administrative Pharmacy*, 1–11. https://doi.org/10.1016/j.sapharm.2020.02.005

Anderson, M. J., & Anderson, T. A. (2015). Anti-money laundering: history and current developments. *Journal of International Banking Law and Regulation*, *30*(10), 521–531.

Antes, A. L., Walsh, H. A., Strait, M., Hudson-Vitale, C. R., & DuBois, J. M. (2018). Examining data repository guidelines for qualitative data sharing. *Journal of Empirical Research on Human Research Ethics*, *13*(1), 61–73. https://doi.org/10.1177/1556264617744121

Anthoine, E., Moret, L., Regnault, A., Sebille, V., & Hardouin, J. B. (2014). Sample size used to validate a scale: a review of publications on newly-developed patient reported outcomes measures. *Health and Quality of Life Outcomes*, *12*(176), 1–10. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4275948/pdf/12955_2014_Article_176.pdf

Arafeen, Q., Arifeen, N., & Ahmed, M. S. (2016). Money laundering in Pakistan-its effects and negative outcomes. *International Journal of Advance Engineering and Research Development*, *3*(4), 109–111. http://52.172.159.94/index.php/theijbm/article/view/126286/87220

Arasa, R., & Ottichilo, L. (2015). Determinants of know your customer (KYC) compliance among commercial banks in Kenya. *Journal of Economics and Behavioral Studies*, *7*(2), 162–175. https://doi.org/10.22610/jebs.v7i2.574.g574

Ardizzi, G., Petraglia, C., Piacenza, M., Schneider, F., & Turati, G. (2014). Money laundering as a crime in the financial sector: A new approach to quantitative assessment, with an application to Italy. *Journal of Money, Credit and Banking*, *46*(8), 1555–1590. https://doi.org/10.1111/jmcb.12159

Arias-Oliva, M., Pelegrín-Borondo, J., & Matías-Clavero, G. (2019). Variables influencing cryptocurrency use: A technology acceptance model in Spain. *Frontiers in Psychology*, *10*(4), 1–13. https://doi.org/10.3389/fpsyg.2019.00475

Ashour, M. L. (2018). Triangulation as powerful methodological research technique in technology-based services. *Business & Management Studies: An International Journal*, *6*(1), 193–208. https://doi.org/10.15295/v6i1.209

Barrett, D., & Twycross, A. (2018). Data collection in qualitative research. *Evidence Based Nursing*, *21*(3), 63–64. https://doi.org/10.1136/eb-2018-102939

Battistini, D. J. (2016, August 31). *Using blockchain technology to facilitate anti-money laundering efforts* [pdf]. La Salle University Digital Commons. http://digitalcommons.lasalle.edu/ecf_capstones/15

Bech, M., & Garratt, R. (2017). Central bank cryptocurrencies [Report]. https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf

Beenot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology*, *16*(21). https://doi.org/10.1186/s12874-016-0114-6

Beqiri, V., & Beqiri, N. (2018). Negative effects on the domestic economy caused by money laundering. *International Journal of Knowledge*, *27*, 87–92. https://www.researchgate.net/publication/330971707_negative_effects_on_the_domestic_economy_caused_by_money_laundering

Bernock, D. (2019). Christianity.com. https://www.christianity.com/wiki/christian-terms/what-is-greed-definition-and-bible-verses-about-greed.html

Blackford, J. (2017). Leveraging statistical methods to improve validity and reproducibility of research findings. *JAMA Psychiatry*, *74*(2), 119–120. https://doi.org/10.1001/jamapsychiatry.2016.3730

Bouheni, F. B., Ameur, H. B., Cheffou, A. I., & Jawadi, F. (2014). The effects of regulation and supervision on European banking profitability and risk: a panel data investigation. *Journal of Applied Business Research*, *30*(6), 1665–1670. https://doi.org/10.19030/jabr.v30i6.8881

Bounds, J. (2016). How banks are fighting money laundering [Magazine]. *D magazine*. https://www.dmagazine.com/publications/d-ceo/2016/november/how-banks-are-fighting-money-laundering/

Broughton, K. (2019, September 16). Crypto firms assess how to comply with anti-money-laundering standards. *WSJ*. https://www.wsj.com/articles/crypto-firms-assess-how-to-comply-with-anti-money-laundering-standards-11568626200

Bryans, D. (2014). Bitcoin and money laundering: mining for an effective solution. *Indiana Law Journal*, *89*(1), 1–32. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj

Bunjaku, F., Gjorgieva-Trajkovska, O., & Miteva-Kacarski, E. (2017). Cryptocurrencies – advantages and disadvantages. http://eprints.ugd.edu.mk/18707/1/Cryptocurrencies.pdf

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Brenig, C., Accorsi, R., & Muller, G. (2015). Economic analysis of cryptocurrency backed money laundering. *AIS Electronic Library* (AISeL). http://aisel.aisnet.org/ecis2015_cr/20

Burrus, J. (2018). Fighting financial crime in the age of cryptocurrencies. *REFINITIV.* https://www.refinitiv.com/content/dam/marketing/en_us/documents/expert-talks/world-check-expert-talk-fighting-financial-crime.pdf

Cai, L., & Zhu, Y. (2015). The challenges of data quality and data quality assessment in the big data era. *Data Science Journal*, *14*(2), 1–10. https://doi.org/10.5334/dsj-2015-002

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, *69*(2), 283–305. https://doi.org/10.1007/s10611-017-9756-5

Canellis, D. (2018, October 10). Criminals used Bitcoin to launder $2.5B in dirty money. *HARD FORK.* https://thenextweb.com/hardfork/2018/10/10/bitcoin-money-laundering/

Cao, S. (2019, August 5). Is bitcoin a haven for financial crimes? New MIT study finds surprising answer. *OBSERVER.* https://observer.com/2019/08/bitcoin-use-illegal-finance-mit-study-blockchain-ai/

Carminati, L. (2018). Generalizability in qualitative research: A tale of two traditions. *Qualitative Health Research*, *28*(13), 2094–2101. https://doi.org/10.1177/1049732318788379

Castillo, M. D. (2020, October 26). Silvergate takes $586 million in cryptocurrency deposits. *Forbes*. https://www.forbes.com/sites/michaeldelcastillo/2020/10/26/silvergate-breaks-record-with-586-million-in-cryptocurrency-deposits/

Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1), 1–10. https://doi.org/10.1186/s40561-017-0050-x

Chen, J. (2019, April 9). Commodity futures trading commission (CFTC). *Investopedia*. https://www.investopedia.com/terms/c/cftc.asp

Cheng, E. (2018, February 23). Bank of America is worried about the threat of cryptocurrency to its business. *CNBC*. https://www.cnbc.com/2018/02/23/bank-of-america-worried-about-threat-of-cryptocurrency-to-its-business.html

Chuen, D. L., Guo, L., & Wang, Y. (2018). Cryptocurrency: a new investment opportunity? *The Journal of Alternative Investments*, *20*(3), 16–40. https://doi.org/10.3905/jai.2018.20.3.016

Chunvoic, L. (2018, January 4). Merrill Lynch fined $26m on AML deficiency charges. *FTF*. https://www.ftfnews.com/merrill-lynch-fined-26m-on-aml-deficiency-charges/19765

Cindori, S., & Slović, J. (2017). Identifying money laundering in business operations as a factor for estimating risk. *International Journal of Innovation and Economic Development*, *3*(3), 7–16. https://doi.org/10.18775/ijied.1849-7551-7020.2015.33.2001

CipherTrace. (2019). Q2 2019 Cryptocurrency anti-money laundering report [Report]. https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

CipherTrace. (2019). Q3 2019 Cryptocurrency Anti-Money Laundering Report [Report]. https://ciphertrace.com/ciphertrace-q3-2019-caml-press-release/

CipherTrace. (2020, February 10). Q4 2019 cryptocurrency anti-money laundering report [Report]. https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/

CipherTrace. (2020). 2020 geographic risk report: Vasp kyc by jurisdiction [Report]. https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/?utm_campaign=Newsletter

CipherTrace. (2020). Spring 2020 cryptocurrency crime and anti-money laundering report [Report]. https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/

Clegg, P. (2020, February 27). OCC hits New York based bank with first-ever enforcement action... CipherTrace. https://ciphertrace.com/occ-hits-new-york-based-bank-with-first-ever-enforcement-action-for-lack-of-crypto-aml-compliance/?utm_campaign=Newsletter

Cleland, J. A. (2017). The qualitative orientation in medical education research. *Korean Journal of Medical Education*, *29*(2), 61–71. https://doi.org/10.3946/kjme.2017.53

Comben, C. (2019, March 27). Anti-bitcoin banks paid over $243 billion fines since the financial crisis. https://bitcoinist.com/bank-fines-243-billion-bitcoin/.

Compin, F. (2018). Terrorism financing and money laundering: Two sides of the same coin?. *Journal of Financial Crime*, *25*(4), 962–968. https://doi.org/10.1108/jfc-03-2017-0021

Creswell, J. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.

Cumming, D. J., Johan, S., & Pant, A. (2019). Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty. *Journal of Risk and Financial Management*, *12*(3), 126. https://doi.org/10.3390/jrfm12030126

Curry, F. (2019, July 30). The role of corporate leaders in fighting money laundering. *The Wall Street Journal.* https://deloitte.wsj.com/cfo/2019/08/25/the-role-of-corporate-leaders-in-fighting-money-laundering/

Cvetkova, I. (2018). Cryptocurrencies legal regulation. *BRICS Law Journal*, *5*(2), 128–153. https://doi.org/10.21684/2412-2343-2018-5-2-128-153

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research. *Dimensions of Critical Care Nursing*, *36*(4), 253–263. https://doi.org/10.1097/dcc.0000000000000253

Daniel, E. (2016). The usefulness of qualitative and quantitative approaches and methods in researching problem-solving ability in science education curriculum. *Education and Practice*, *7*(15), 91–100. https://eric.ed.gov/?id=EJ1103224

Davies, P. J. (2018, October 5). Banks are getting squeezed by the fight against dirty money. *WSJ.* https://www.wsj.com/articles/banks-are-getting-squeezed-by-the-fight-against-dirty-money-1538731802

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health*, *7*(2), 1–8. https://doi.org/10.1136/fmch-2018-000057

Delgado-Segura, S., Pérez-Solà, C., Herrera-Joancomartí, J., Navarro-Arribas, G., & Borrell, J. (2018). Cryptocurrency networks: A new P2P paradigm. *Mobile Information Systems*, 2018, 1–16. https://doi.org/10.1155/2018/2159082

Demertzis, M., & Wolf, G. B. (2018). *The economic potential and risks of crypto assets: is a regulatory framework needed?.* (No. 2018/14). Bruegel Policy Contribution. https://bruegel.org/2018/09/the-economic-potential-and-risks-of-crypto-assets-is-a-regulatory-framework-needed/

Devlin, F. (2017). Blockchain, revolution, regulation, and the way forward. *The RMA Journal*, *100*, 48–51. http://wwc.rmany.org/documents/1709BlockchainRevolution.pdf

DeVries, P. D. (2016). An analysis of cryptocurrency, bitcoin, and the future. *International Journal of Business Management and Commerce*, *1*(2), 1–9. https://www.researchgate.net/profile/Peter_Devries2/publication/316656878_An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future/links/590a0af90f7e9b1d0823c253/An-Analysis-of-Cryptocurrency-Bitcoin-and-the-Future.pdf

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). Terrorist use of cryptocurrencies [Report]. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

Doll, J. L. (2017). Structured interviews: Developing interviewing skills in human resource management courses. *Management Teaching Review*, *3*(1), 46–61. https://doi.org/10.1177/2379298117722520

Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: regulating emerging technologies in Canada. *International Journal: Canada's Journal of Global Policy Analysis*, *72*(4), 538–562. https://doi.org/10.1177/0020702017741909

Dufour, I. F., & Richard, M. C. (2019). Theorizing from secondary qualitative data: A comparison of two data analysis methods. *Cogent Education*, *6*(1), 1–15. https://doi.org/10.1080/2331186x.2019.1690265

Durner, T., & Shetret, L. (2015). Understanding bank de-risking and its effects on financial inclusion [Report]. https://www-cdn.oxfam.org/s3fs-public/file_attachments/rr-bank-de-risking-181115-en_0.pdf

Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies*, *4*(5), 75–81. https://doi.org/10.30525/2256-0742/2018-4-5-75-81

Dyson, S., Buchanan, W., & Bell, L. (2018). The challenges of investigating cryptocurrencies and blockchain related crime. *The Journal of the British Blockchain Association*, *1*(2), 1–6. https://doi.org/10.31585/jbba-1-2-(8)2018

Ebneyamini, S., & Moghadam, M. R. (2018). Toward developing a framework for conducting case study research. *International Journal of Qualitative Methods*, *17*(1), 1–11. https://doi.org/10.1177/1609406918817954

Eddles-Hirsch, K. (2015). Phenomenology and educational research. *International Journal of Advanced Research*, *3*(8), 251–260. http://www.journalijar.com/uploads/287_IJAR-6671.pdf

Eisenberg, P. (2017). Financial crime – is there any way out of the theoretical deadlock?. *Journal of Financial Crime*, *24*(4), 529–540. https://doi.org/10.1108/jfc-06-2016-0043

Elaldi, S., & Yerliyurt, N. (2016). The efficacy of drama in field experience: A qualitatıve study using MAXQDA. *Journal of Education and Learning*, *6*(1), 1–17. https://doi.org/10.5539/jel.v6n1p10

ElBahrawy, A., Alessandretti, L., Kandler, A., Pastor-Satorras, R., & Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. *Royal Society Open Science*, *4*(11). https://doi.org/10.1098/rsos.170623

Elder, D. (2019, March 8). Research logs: A key to organized genealogy. https://familylocket.com/research-logs-a-key-to-organized-genealogy-by-diana-elder-at-rootstech-2019/

Elliott, V. (2018). Thinking about the coding process in qualitative data analysis. *The Qualitative Report*, *23*(11), 2850–2861. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=3560&context=tqr

Falanga, S. (2006). Sarbanes-Oxley impact on banks under review. *Corporate Counsel Business Journal*. https://ccbjournal.com/articles/sarbanes-oxley-impact-banks-under-review

Faridi, O. (2019, August 13). $4.3 billion lost due to cryptocurrency crimes: Cipher trace report. *Ethereum World News*. https://en.ethereumworldnews.com/4-3-billion-lost-due-to-cryptocurrency-crimes-ciphertrace-report/

Fernandez, C. M. (2014). Fighting against financing of terrorism and money laundering. *Global Journal of Management and Business Research: B Economics and Commerce*, *14*(6), 42–48. https://globaljournals.org/GJMBR_Volume14/5-Fighting-Against-Financing.pdf

Ferreira, P., & Pereira, É. (2019). Contagion effect in cryptocurrency market. *Journal of Risk and Financial Management*, *12*(3), 1–8. https://doi.org/10.3390/jrfm12030115

Ferwerda, J., Deleanu, I., & Unger, B. (2019). Strategies to avoid blacklisting: The case of statistics on money laundering. *PLoS One*, *14*(6). https://doi.org/10.1371/journal.pone.0218532

Financial Action Task Force. (2018a). Annual Report 2017-2018 [Report]. www.fatf-gafi.org/publications/fatfgeneral/documents/annual-report-2017-2018.html

Financial Action Task Force. (2018b). Professional Money Laundering [Report]. http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf

Financial Crimes Enforcement Network. (n.d.). Anti-Money Laundering. Retrieved March 4, 2020, from https://www.fincen.gov

Financial Crimes Enforcement Network. (2020, March 4). FinCEN penalizes U.S. bank official for corporate anti-money laundering failures. https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-official-corporate-anti-money-laundering-failures

Financial Industry Regulatory Authority. (2018, December 26). FINRA fines Morgan Stanley $10 million for AML program and supervisory failures. https://www.finra.org/media-center/news-releases/2018/finra-fines-morgan-stanley-10-million-aml-program-and-supervisory

Forgang, G. (2019, January 15). *Money laundering through cryptocurrencies.* La Salle University Digital Commons. https://digitalcommons.lasalle.edu/ecf_capstones/40/

Fritz, R. L., & Vandermause, R. (2017). Data collection via in-depth email interviewing: lessons from the field. *Qualitative Health Research*, *28*(10), 1640–1649. https://doi.org/10.1177/1049732316689067

Fusch, P. I., Fusch, G. E., & Ness, L. R. (2018). Denzin’s paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*(1), 19–32. https://doi.org/10.5590/josc.2018.10.1.02

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408–1416. https://nsuworks.nova.edu/tqr/vol20/iss9/3

Galdas, P. (2017). Revisiting bias in qualitative research. *International Journal of Qualitative Methods*, *16*(1), 1–2. https://doi.org/10.1177/1609406917748992

Gandal, N., & Halaburda, H. (2016). Can we predict the winner in a market with network effects? Competition in cryptocurrency market. *Games*, *7*(3), 1–21. https://doi.org/10.3390/g7030016

Gikay, A. A. (2018). Regulating decentralized cryptocurrencies under payment services law: lessons from the European Union. *Journal of Law, Technology & the Internet*, *9*(1), 1–35. https://scholarlycommons.law.case.edu/jolti/vol9/iss1/1/

Gilmour, N. (2014). Understanding money laundering – a crime script approach. *The European Review of Organized Crime*, *1*(2), 1–18. https://standinggroups.ecpr.eu/sgoc/understanding-money-laundering-a-crime-script-approach/

Gjoni, M., Gjoni, A., & Kora, H. (2015, November 6). Money laundering effects [Paper]. International Conference on Management, Business and Economics, Durres, Albania.

Global Legal Insights. (2019). Blockchain & cryptocurrency regulation. https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

Goodell, G., & Aste, T. (2019). Can cryptocurrencies preserve privacy and comply with regulations?. *Frontiers in Blockchain*, *2*. https://doi.org/10.3389/fbloc.2019.00004

GotQuestions.org. (2010, April 15). What does the bible say about government? https://www.gotquestions.org/Bible-government.html

Guadamuz, A., & Marsden, C. (2015). Blockchains and bitcoin: regulatory responses to cryptocurrencies. *First Monday*, *20*(12). https://doi.org/10.5210/fm.v20i12.6198

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLoS One*, *15*(5), 1–17. https://doi.org/10.1371/journal.pone.0232076

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study. [Literature Review]. http://www.diva-portal.org/smash/get/diva2 :1064378/FULLTEXT01.pdf

Halcomb, E. J. (2018). Mixed methods research: The issues beyond combining methods. *Journal of Advanced Nursing*, *75*(3), 499–501. https://doi.org/10.1111/jan.13877

Halek, M., Holle, D., & Bartholomeyczik, S. (2017). Development and evaluation of the content validity, practicability and feasibility of the innovative dementia-oriented assessment system for challenging behaviour in residents with dementia. *BMC Health Services Research*, *17*(554), 1–26. https://doi.org/10.1186/s12913-017-2469-8

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction*, *31*(3), 498–501. https://doi.org/10.1093/humrep/dev334

Hard Fork. (2018). Cryptocurrency regulation in 2018: where the world stands right now [Magazine]. https://thenextweb.com/hardfork/2018/04/27/cryptocurrency-regulation-2018-world-stands-right-now/

Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017). Case study research: foundations and methodological orientations. *Forum Qualitative Socila research Sozialforschung*, *18*(1). https://doi.org/10.17169/fqs-18.1.2655

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity.* McKinsey & Company. https://www.mckinsey.com/~/media/McKinsey/Business Functions/Risk/Our Insights/Financial crime and fraud in the age of cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.ashx

Hassani, H., Huang, X., & Silva, E. (2018). Big-crypto: Big data, blockchain and cryptocurrency. *Big Data and Cognitive Computing*, *2*(4), 1–15. https://doi.org/10.3390/bdcc2040034

Heale, R., & Twycross, A. (2017). What is a case study? *Evidence Based Nursing*, *21*(1), 7–8. https://doi.org/10.1136/eb-2017-102845

Hetemi, A., Merovci, S., & Gulhan, O. (2018). Consequences of money laundering on economic growth – The case of Kosovo and its trade partners. *Acta Universitatis Danubius Œconomica*, *14*(3), 113–125. https://www.ceeol.com/search/article-detail?id=731637

Hofisi, C., Hofisi, M., & Mago, S. (2014). Critiquing Interviewing as a data collection method. *Mediterranean Journal of Social Sciences*, *5*(16), 60–64. https://doi.org/:10.5901/mjss.2014.v5n16p60

Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain (PE 619.024) [Report]. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Howard, C. (2017). The applicability of the BSA/AML regulatory regime to indirect lending business models. *The Tennessee Journal of Business Law*, *19*, 45–77. https://trace.tennessee.edu/cgi/viewcontent.cgi?article=1417&context=transactions

Huang, A. (2015). Reaching within silk road: The need for a new subpoena power that targets illegal bitcoin transactions. *Boston College Law Review*, *56*(5), 2093–2125. https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3476&context=bclr

Hughes, S. J., & Middlebrook, S. T. (2014). *Regulating cryptocurrencies in the United States: current issues and future directions*. https://www.repository.law.indiana.edu/facpub/2096/

Isa, Y. M., Sanusi, Z. M., Haniff, M. N., & Barnes, P. A. (2015). Money laundering risk: from the bankers' and regulators perspectives. *Procedia Economics and Finance*, *28*, 7–13. https://doi.org/10.1016/s2212-5671(15)01075-8

Ito, J., Narula, N., & Ali, R. (2017, March 8). The blockchain will do to the financial system what the internet did to media. *Harvard Business Review*. https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

Jani, S. (2017). An overview of Ethereum & its comparison with Bitcoin. *International Journal of Scientific & Engineering Research*, *10*(8), 1–7. https://www.researchgate.net/publication/323078799_An_Overview_of_Ethereum_Its_Comparison_with_Bitcoin/link/5a7ea3c14585154d57d53d5d/download

JJ. (2018, September 8). *FinCEN director lauds crypto innovation while citing need to reign in bad actors.* CipherTrace. https://ciphertrace.com/fincen-director-lauds-crypto-innovation/

JJ. (2020, September 9). *Best practices for monitoring virtual currency-related transactions at your bank.* CipherTrace. https://ciphertrace.com/best-practices-for-banks-to-monitor-virtual-currency/

Jevans, D. (2020, October 13). CFTC, DOJ Charge BitMEX Owners with Illegal Operations and Anti-Money Laundering Violations. *CipherTrace.* https://ciphertrace.com/cftc-doj-charge-bitmex-owners-with-illegal-operations-and-anti-money-laundering-violations/

Jung, J., & Lee, J. (2017). Contemporary financial crime. *Journal of Public Administration and Governance*, *7*(2), 88–97. https://doi.org/10.5296/jpag.v7i2.11219

Kabir, S. M. (2016). *Basic guidelines for research: An introductory approach for all disciplines*. Book Zone Publication.

Kemal, M. U. (2014). Anti-money laundering regulations and its effectiveness. *Journal of Money Laundering Control*, *17*(4), 416–427. https://doi.org/10.1108/jmlc-06-2013-0022

Kepli, M. Y., & Nasir, M. A. (2016). Money laundering: analysis on the placement methods. *International Journal of Business, Economics, Law*, *11*(5), 32–40.

Kethineni, S., & Cao, Y. (2019). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review*, 1–20. https://doi.org/10.1177/1057567719827051

Khatri, Y. (2019, April 24). *New York State sees first conviction for crypto money laundering*. Coindesk. https://www.coindesk.com/new-york-state-sees-first-conviction-for-crypto-money-laundering

King, D. (2015). Banking bitcoin-related businesses: A primer for managing BSA/AML risks [Report]. https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/2016/banking-bitcoin-related-businesses.pdf/

Kovner, A., & Tassel, P. (2019). *Evaluating regulatory reform: bank's cost of capital and lending* [Report]. Federal Reserve Bank of New York. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr854.pdf

Kross, J., & Giust, A. (2019, January 6). *Elements of research questions in relation to qualitative inquiry* [Report]. TQR. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=3426

Kumar, D., & Siddika, H. (2017). Benefits of training and development program on employees' performance: A study with special reference to banking sector in Bangladesh. *International Journal of Research*, *5*(12), 77–88. https://doi.org/10.29121/granthaalayah.v5.i12.2017.475

Kumar, V. A. (2012). Money laundering: concept, significance and its impact. *European Journal of Business and Management*, *4*(2), 113–119. https://pdfs.semanticscholar.org/b1a4/6c10a40dfc2d653dea3d34c235ca2b09befd.pdf

Lansky, J. (2018). Possible state approaches to cryptocurrencies. *Journal of Systems Integration*, *9*(1), 19–31. https://doi.org/10.20470/jsi.v9i1.335

Lee, J. (2019). A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Business Horizons*, *62*(6), 773–784. https://doi.org/10.1016/j.bushor.2019.08.003

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324. https://doi.org/10.4103/2249-4863.161306

Liang, J., Li, L., & Zeng, D. (2018). Evolutionary dynamics of cryptocurrency transaction networks: An empirical study. *PLoS One*, *13*(8). https://doi.org/10.1371/journal.pone.0202202

Litchfield, A., & Herbert, J. (2018). Resolv: Applying cryptocurrency blockchain methods to enable global cross-platform software license validation. *Cryptography*, *2*(2), 1–24. https://doi.org/10.3390/cryptography2020010

Long-Sutehall, T., Sque, M., & Addington-Hall, J. (2010). Secondary analysis of qualitative data: a valuable method for exploring sensitive issues with an elusive population. *Journal of Research in Nursing*, *16*(4), 335–344. https://doi.org/10.1177/1744987110381553

Lord, N., Wingerde, K., & Campbell, L. (2018). Organising the monies of corporate financial crimes via organisational structures: Ostensible legitimacy, effective anonymity, and third-party facilitation. *Administrative Sciences*, *8*(2), 1–17. https://doi.org/10.3390/admsci8020017

Mabunda, S. (2018, August 6). Cryptocurrency: The new face of cyber money laundering. [Paper presentation]. 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa. https://doi.org/10.1109//ICABCD.2018.8465467

MacLeod, A. (2016). Understanding the culture of graduate medical education: The benefits of ethnographic research. *Journal of Graduate Medical Education*, *8*(2), 142–144. https://doi.org/10.4300/jgme-d-15-00069.1

Majid, M., Othman, M., Mohamad, S., Lim, S., & Yusof, A. (2017). Piloting for interviews in qualitative research: operationalization and lessons learnt. *International Journal of Academic Research in Business and Social Sciences*, *7*(4), 1073–1080. https://doi.org/10.6007/ijarbss/v7-i4/2916

Malwa, S. (2018, July 5). *$1.2 billion in cryptocurrency laundered through bitcoin tumblers, privacy coins.* Yahoo! Finance. https://finance.yahoo.com/news/1-2-billion-cryptocurrency-laundered-224521652.html

Mandeng, O. J. (2018). *Cryptocurrencies, monetary stability and regulation*. Research Gate. https://www.researchgate.net/publication/323417307_cryptocurrencies_monetary_stability_and_regulation_Germany’s_nineteenth_century_private_banks_of_issue

Mandjee, T. (2015). Bitcoin, its legal classification and its regulatory framework. *Journal of Business & Securities Law*, *15*(2), 1–62. https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1703&context=facultypub

Marian, O. Y. (2015). *A conceptual framework for the regulation of cryptocurrencies*. UF Law Scholarship Repository. https://scholarship.law.ufl.edu/facultypub/695/

Marjaei, S., Yazdi, F. A., & Chandrashekara, M. (2019). *MAXQDA and its Application to LIS research* [Report]. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5740&context=libphilprac

Masjedi, E. (2015). Electronic money laundering and data mining methods in investigating money laundering prevention. *International Academic Journal of Science and Engineering*, *2*(10), 29–46.

Massad, T. G. (2019). *It's time to strengthen the regulation of crypto-assets* [Report]. https://www.brookings.edu/wp-content/uploads/2019/03/Economis-Studies-Timothy-Massad-Cryptocurrency-Paper.pdf

McBride, M., & Gold, Z. (2019). *Cryptocurrency: implications for special operations forces.* (CNA) [Report]. https://www.cna.org/CNA_files/PDF/CRM-2019-U-020186-Final.pdf

McDowell, J., & Novis, G. (2001). The consequences of money laundering and financial crime. *Economic Perspective*, *6*(2). https://web-archive-2017.ait.org.tw/infousa/zhtw/DOCS /ijee0501.pdf

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2018). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, *41*(9), 1002–1006. https://doi.org/10.1080/0142159x.2018.1497149

Meinert, M. (2016). ABA highlights harmful effects of excessive regulation. *ABA Banking Journal*. https://bankingjournal.aba.com/2016/06/aba-highlights-harmful-effects-of-excessive-regulation/

Miller, R. S., & Rosen, L. W. (2017). *Anti-money laundering: an overview for Congress.* (R4476) [Report]. https://fas.org/sgp/crs/misc/R44776.pdf

Miller, Z., & Kohr, L. (2016). Senior management training, accountability and oversight for anti-money laundering compliance. *Journal of Financial Compliance*, *1*(1), 81–88. https://www.henrystewartpublications.com/sites/default/files/JFC00006_MILLER_KOHR_1_1.pdf

Miraz, M. H., & Ali, M. (2018). Applications of blockchain technology beyond cryptocurrency. *Annals of Emerging Technologies in Computing*, *2*(1), 1–6. https://arxiv.org/ftp/arxiv/papers/1801/1801.03528.pdf

Mitchell, D. J. (2016). *Money laundering laws: ineffective and expensive*. CATO Institute. https://www.cato.org/blog/money-laundering-laws-ineffective-expensive

Mittal, R., Arora, S., & Bhatia, M. P. (2018). Automated cryptocurrencies prices prediction using machine learning. *Ictact Journal on Soft Computing*, *8*(4), 1758–1761. https://doi.org/10.21917/ijsc.2018.0245

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23–48. https://www.ceeol.com/search/article-detail?id=640546

Mohamad, M., Sulaiman, N., Sern, L., & Salleh, K. (2015). Measuring the validity and reliability of research instruments. *Procedia - Social and Behavioral Sciences*, *204*, 164–171. https://doi.org/10.1016/j.sbspro.2015.08.129

Moran, J. D. (2018). The impact of regulatory measures imposed on initial coin offerings in the United States market economy. *Catholic University Journal of Law and Technology*, *26*(2), 213–258. https://scholarship.law.edu/jlt/vol26/iss2/7

Morelli, C. F. (2015). *An effectiveness review of section 404 of the Sarbanes Oxley Act* (2002). University of New Hampshire Scholars' Repository. https://scholars.unh.edu/honors/262/

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), 1212–1222. https://doi.org/10.1177/1049732315588501

Moser, A., & Korstjens, I. (2018). Series: practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, *24*(1), 9–18. https://doi.org/10.1080/13814788.2017.1375091

Mugarura, N. (2016). Uncoupling the relationship between corruption and money laundering crimes. *Journal of Financial Regulation and Compliance*, *24*(1), 74–89. https://doi.org/10.1108/jfrc-01-2014-0002

Murray-West, R. (2017, February 10). *Recognizing the warning signs of money laundering*. The Telegraph. https://www.telegraph.co.uk/money/criminal-activities/money-laundering-checks-5-warning-signs/

Nabilou, H. (2019). How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency. *International Journal of Law and Information Technology*, *27*(3), 266–291. https://doi.org/10.1093/ijlit/eaz008

Naheem, M. A. (2016). Risk of money laundering in the US: HSBC case study. *Journal of Money Laundering Control*, *19*(3), 225–237. https://doi.org/10.1108/jmlc-01-2015-0003

Neale, J. (2016). Iterative categorization (IC): A systematic technique for analyzing qualitative data. *Addiction*, *111*(6), 1096–1106. https://doi.org/10.1111/add.13314

Neubauer, B. E., Witkop, C. T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on Medical Education*, *8*(2), 90–97. https://doi.org/10.1007/s40037-019-0509-2

Ng, D., & Griffin, P. (2018). The wider impact of a national cryptocurrency. *Global Policy*, 1–18. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=6879&context=lkcsb_research

Nice Actimize. (2019). *Understanding and managing financial crime risk* [White Paper]. https://www.niceactimize.com/Lists/WhitePapers/Fighting_WhitePaper_Understanding_Managing.pdf

Nickel, K. (2019, March 6). *4 Bible verses that encourage technology in ministry.* https://www.boxcast.com/blog/4-bible-verses-that-encourage-technology-in-ministry

Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence Based Nursing*, *22*(3), 67–68. https://doi.org/10.1136/ebnurs-2019-103145

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing*, *18*(2), 34–35. https://doi.org/10.1136/eb-2015-102054

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), 1–13. https://doi.org/10.1177/1609406917733847

Obie, S. J., & Rasmussen, M. (2018, July 17). How regulation could help cryptocurrencies grow. *Harvard Business Review*. https://hbr.org/2018/07/how-regulation-could-help-cryptocurrencies-grow

Office of the Comptroller of the Currency. (n.d.). *Bank Secrecy Act* (BSA). https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html

Office of the Comptroller of the Currency. (2020, July 22). *Federally chartered banks and thrifts may provide custody services for crypto assets* [News Release 2020-98]. OCC. https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-98.html

Olsen, C. (2019). *Blockchain and cryptocurrency regulation 2019* (1st ed.) [Report]. https://www.careyolsen.com/sites/default/files/CO_Blockchain-and-Cryptocurrency-Regulation-2019-1st-Edition_3-19.pdf

Oluwadayisi, A., & Mimiko, M. (2016). Effects of money laundering on the economy of Nigeria. *Beijing Law Review*, *7*(2), 158–169. https://doi.org/10.4236/blr.2016.72017

Omolara, A. E., Jantan, A., Abiodun, O. I., Singh, M. M., Anbar, M., & Dada, K. V. (2018). State-of-the-art in big data application techniques to financial crime: A survey. *International Journal of Computer Science and Network Security*, *18*(7), 6–16. http://paper.ijcsns.org/07_book/201807/20180702.pdf

Oswald, A. G. (2017). Improving outcomes with qualitative data analysis software: A reflective journey. *Qualitative Social Work*, *18*(3), 436–442. https://doi.org/10.1177/1473325017744860

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2013). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Paradis, E., O'Brien, B., Nimmon, L., Bandiera, G., & Martimianakis, M. (2016). Design: selection of data collection methods. *Journal of Graduate Medical Education*, *8*(2), 263–264. https://doi.org/10.4300/jgme-d-16-00098.1

Penn, M., & Currie, C. S. (2016). The use of case studies in or teaching. *Higher Education Pedagogies*, *1*(1), 16–25. https://doi.org/10.1080/23752696.2015.1134201

Peprah, W. K., Afriyie, A. O., Abandoh-Sam, J. A., & Afriyie, E. O. (2018). Dollarization 2.0 a cryptocurrency: Impact on traditional banks and fiat currency. *International Journal of Academic Research in Business and Social Sciences*, *8*(6), 341–349. https://doi.org/10.6007/ijarbss/v8-i6/4213

Perkins, D. W. (2018). *Cryptocurrency: The economics of money and selected policy issues* (R45427) [Report]. https://fas.org/sgp/crs/misc/R45427.pdf

Piazza, F. (2017). Bitcoin in the dark web: a shadow over banking secrecy and a call for global response. *Southern California Interdisciplinary Law Journal*, *26*, 521–546. https://gould.usc.edu/why/students/orgs/ilj/assets/docs/26-3-Piazza.pdf

Politzer, M. (2019, September 3). *Watch out for these bribery risk red flags.* FM Magazine. https://www.fm-magazine.com/news/2019/sep/bribery-risk-red-flags-201921561.html

Price, R. (2016, July 26). *A Florida judge ruled bitcoin isn't money*. SLATE. https://slate.com/business/2016/07/florida-judge-rules-that-bitcoin-isnt-money.html

PYMNTS.com. (2019). *Global regulatory firm to tighten rules on cryptocurrency*. https://www.pymnts.com/cryptocurrency/2019/fatf-rules-cryptocurrency/

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management*, *8*(3), 238–264. https://doi.org/10.1108/11766091111162070

Qureshi, W. A. (2017). An overview of money laundering in Pakistan and worldwide: causes, methods, and socioeconomic effects. *University of Bologna Law Review*, *2*(2), 300–345. https://doi.org/10.6092/issn.2531-6133/7816

Rahman, M. S. (2016). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language “testing and assessment” research: A literature review. *Journal of Education and Learning*, *6*(1), 102–112. https://doi.org/10.5539/jel.v6n1p102

Ranney, M. L., Meisel, Z. F., Choo, E. K., Garro, A. C., Sasson, C., & Morrow Guthrie, K. (2015). Interview-based qualitative research in emergency care part ii: Data collection, analysis and results reporting. *Academic Emergency Medicine*, *22*(9), 1103–1112. https://doi.org/10.1111/acem.12735

Rashid, Y., Rashid, A., Warraich, M., Sabir, S., & Waseem, A. (2019). Case study method: A step-by-step guide for business researchers. *International Journal of Qualitative Methods*, *18*, 1–13. https://doi.org/10.1177/1609406919862424

Rasul, H. (2018). Does bitcoin need regulation?: An analysis of bitcoin's decentralized nature as a security and regulatory concern for governments. *Political Analysis*, *19*(9). https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1045&context=pa

Rexrode, C. (2018, May 22). Small banks' new money maker: Bitcoin. *WSJ.* https://www.wsj.com/articles/bitcoin-needs-bankers-too-a-handful-of-community-banks-say-yes-to-crypto-1526997601

Richardson, B., Williams, D., & Mikkelsen, D. (2019, August 15). *Network analytics and the fight against money laundering.* McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/network-analytics-and-the-fight-against-money-laundering

Ridder, H. G. (2017). The theory contribution of case study research designs. *Business Research*, *10*, 281–305. https://doi.org/10.1007/s40685-017-0045-z

Rohit, K. D., & Patel, D. B. (2015). Review on detection of suspicious transaction in anti-money laundering using data mining framework. *International Journal for Innovative Research in Science & Technology*, *1*(8), 129–133.

Rose, C. (2015). The evolution of digital currencies: Bitcoin, a cryptocurrency causing a monetary revolution. *International Business & Economics Research Journal (IBER)*, *14*(4), 617–621. https://doi.org/10.19030/iber.v14i4.9353

Rubenfeld, S. (2018, December 3). U.S. encourages banks to innovate in anti-money laundering compliance. *WSJ*. https://www.wsj.com/articles/u-s-encourages-banks-to-innovate-in-anti-money-laundering-compliance-1543878973

Rueckert, C. (2019). Cryptocurrencies and fundamental rights. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz004

Ruggiano, N., & Perry, T. E. (2019). Conducting secondary analysis of qualitative data: Should we, can we, and how? *Qualitative Social Work*, *18*(1), 81–97. https://doi.org/10.1177/1473325017700701

Salehi, A., Fathian, M., & Ghazanfari, M. (2017). Data mining techniques for anti money laundering. *International Journal of Applied Engineering Research*, *12*(20), 10084–10094.

Salvador, J. (2016). Exploring quantitative and qualitative methodologies: A guide to novice nursing researchers. *European Scientific Journal*, *12*(18), 107–122. https://doi.org/10.19044/esj.2016.v12n18p107

Sapat, A., L, Schwartz, Esnard, A. M., & Sewordor, E. (2017). Integrating qualitative data software into public administration. *Journal of Public Affairs Education*, 959–979. https://par.nsf.gov/servlets/purl/10057044

Saperstein, L., Sant, G., & Ng, M. (2015). The failure of anti-money laundering regulation: Where is the cost-benefit analysis?. *Notre Dame Law Review Online*. https://scholarship.law.nd.edu/ndlr_online/vol91/iss1/4/

Sargeant, J. (2012). Qualitative research part ii: Participants, analysis, and quality assurance. *Journal of Graduate Medical Education*, *4*(1), 1–3. https://doi.org/10.4300/jgme-d-11-00307.1

Sarigul, H. (2013). Money laundering and abuse of the financial system. *International Journal of Business and Management Studies*, *2*(1), 287–301.

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Anonymising interview data: challenges and compromise in practice. *Qualitative Research*, *15*(5), 616–632. https://doi.org/10.1177/1468794114550439

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Savona, E., & Riccardi, M. (2019). Assessing the risk of money laundering: Research challenges and implications for practitioners. *European Journal on Criminal Policy and Research*, *25*(1), 1–4. https://doi.org/10.1007/s10610-019-09409-3

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*(1), 1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

See, B. R., Miru, A., Muhadar, & Paserangi, H. (2019). Know Your Customer (KYC) principles relates to bank confidentiality as an effort to prevent money laundering crimes. *Journal of Law, Policy and Globalization*, *81*, 101–108. https://doi.org/10.7176/JLPG

Sidanius, C. (2018, May 30). *Financial crime report: Costs & fighting back*. REFINITIV. https://www.refinitiv.com/perspectives/financial-crime/financial-crime-report-the-true-costs-and-how-to-fight-back/

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology*, *21*(5), 619–634. https://doi.org/10.1080/13645579.2018.1454643

Slutzky, P., Villamizar-Villegas, M., & Williams, T. (2018). Drug money and firms: The unintended consequences of anti-money laundering policies. *SSRN Electronic Journal*, 1–46. https://doi.org/10.2139/ssrn.3280294

Sonderegger, D. (2015). A regulatory and economic perplexity: bitcoin needs just a bit of regulation. *Journal of Law & Policy*, *14*(175), 175–216. https://openscholarship.wustl.edu/law_journal_law_policy/vol47/iss1/14

Soper, D. S. (2014). *User interface design and the halo effect: some preliminary evidence* [Research Paper]. https://pdfs.semanticscholar.org/561a/487386fbd067b675ad9a82426c7408ee0e53.pdf

Soudjin, M. (2015). Hawala and money laundering: Potential use of red flags for persons offering Hawala Services. *European Journal on Criminal Policy and Research*, *21*(2), 257–274. https://doi.org/10.1007/s10610-014-9238-6

Spencer, J. (2017, November 2). *The risks and benefits of digital currency.* Entrepreneur. https://www.entrepreneur.com/article/302778

Spithoven, A. (2019). Theory and reality of cryptocurrency governance. *Journal of Economic Issues*, *53*(2), 385–393. https://doi.org/10.1080/00213624.2019.1594518

Sprenger, P., & Balsiger, F. (2018). *Laundering in times of cryptocurrencies. Cryptocurrencies-game changers in many ways*. https://assets.kpmg/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of-cryptocurrency.pdf

Stankiewicz, N. (2015). Using anti-money laundering measures in the financial world to combat organized crime. *Inquiries Journal*, *7*(10). http://www.inquiriesjournal.com/a?id=1268

Stankovic, S. (2019). *US cryptocurrency regulation: policies, regimes & more*. Unblock. https://unblock.net/us-cryptocurrency-regulation/#h3

Starman, A. B. (2013). The case study as a type of qualitative research. *Journal of Contemporary Educational Studies*, 28–43. https://pdfs.semanticscholar.org/1cc2/7a1b28050194da8bef5b2ab807386baa286e.pdf?_ga=2.136503024.1791628593.1589914003-1268466600.1589914003

Subramanian, R., & Chino, T. (2015). The state of cryptocurrencies, their issues and policy interactions. *Journal of International Technology and Information Management*, *24*(3), 25–40. https://scholarworks.lib.csusb.edu/jitim/vol24/iss3/2

Sun, M. (2020, October 6). This regulator wants to help banks embrace cryptocurrency. *WSJ*. https://www.wsj.com/articles/this-regulator-wants-to-help-banks-embrace-cryptocurrency-11601976600

Sundarakani, S., & Ramasamy, M. (2013). Consequences of money laundering in banking sector. *Journal Technology*, *64*(2). https://doi.org/10.11113/jt.v64.2243

Surkis, A., & Read, K. (2015). Research data management. *Journal of the Medical Library Association*, *103*(3), 154–156. https://doi.org/10.3163/1536-5050.103.3.011

Surmiak, A. (2019). Should we maintain or break confidentiality? The choices made by social researchers in the context of law violation and harm. *Journal of Academic Ethics*, 1–19. https://doi.org/10.1007/s10805-019-09336-2

Sutton, J., & Austin, Z. (2015). Qualitative research: data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3), 226–231. https://doi.org/10.4212/cjhp.v68i3.1456

Sweet, K. (2018, February 15). US bank pays $613 million over money laundering charges. *Financial Post*. https://financialpost.com/pmn/business-pmn/us-bank-pays-613-million-over-money-laundering-charges

Sykes, J. B., & Vanatko, N. (2019). *Virtual currencies and money laundering: legal background, enforcement actions, and legislative proposals* (R45664). https://crsreports.congress.gov/

Taherdoost, H. (2016). Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in a research. *International Journal of Academic Research in Management*, *5*(3), 28–36. https://doi.org/10.2139/ssrn.3205040

Thakur, K. K., & Banik, G. G. (2018). Cryptocurrency: Its risks and gains and the way ahead. *Journal of Economics and Finance*, *9*(2), 38–42. https://doi.org/10.9790/5933-0902013842

The Organisation for Economic Co-operation and Development. (2019). Tax Crime. *OECD.* www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-taxauditors.pdf

Tie, Y. C., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. *SAGE Open Medicine*, *7*, 1–8. https://doi.org/10.1177/2050312118822927

Toscher, S., & Stein, M. R. (2018). *Cryptocurrency—FinCEN and discovery of hidden wealth*. https://www.taxlitigator.com/wp-content/uploads/2018/10/Hidden_Wealth.pdf

Tsingou, E. (2017). New governors on the block: The rise of anti-money laundering professionals. *Crime, Law and Social Change*, *69*(2), 191–205. https://doi.org/10.1007/s10611-017-9751-x

Turpin, J. B. (2014). *Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework*. Digital Repository @ Maurer Law. http://www.repository.law.indiana.edu/ijgls/vol21/iss1/13

Tysiac, K. (2016). U.S. anti-money laundering regulations well-developed, analysis finds. *Journal of Accountancy*. https://www.journalofaccountancy.com/news/2016/dec/us-anti-money-laundering-regulations-201615620.html

U.S. Department of the Treasury. (2018). *National Money Laundering Risk Assessment*. https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf

U.S. Department of Justice. (2019a). *U.S. Attorney announces arrest and money laundering charges against dark web narcotics trafficker*. https://www.justice.gov/usao-sdny

U.S. Department of Justice. (2019b, August 23). *Westwood man agrees to plead guilty to federal narcotics, money laundering charges for running unlicensed bitcoin exchange and ATM.* https://www.justice.gov/usao-cdca/pr/westwood-man-agrees-plead-guilty-federal-narcotics-money-laundering-charges-running?fbclid=IwAR00w960NzjHX4BcGjn9cro6mxvd0PLhQsKieEaU6QTJJSvlOm4Egy25zhw

U.S. Government Accountability Office. (2016). *Financial Institutions Fines, Penalties, and Forfeitures for Violations of Financial Crimes and Sanctions Requirements* (GAO-16-297). https://www.gao.gov/assets/680/675987.pdf

United Nations. (n.d.). *Money-laundering and globalization.* https://www.unodc.org/unodc/en/money-laundering/globalization.html

van Wegberg, R., Oerlemans, J. J., & van Deventer, O. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, *25*(2), 419–435. https://doi.org/10.1108/jfc-11-2016-0067

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterizing and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology*, *18*(1). https://doi.org/10.1186/s12874-018-0594-7

Wang, C. C., & Geale, S. K. (2015). The power of story: Narrative inquiry as a methodology in nursing research. *International Journal of Nursing Sciences*, *2*(2), 195–198. https://doi.org/10.1016/j.ijnss.2015.04.014

Wass, M. N., Ray, L., & Michaelis, M. (2019). Understanding of researcher behavior is required to improve data reliability. *GigaScience*, *8*(5), 1–8. https://doi.org/10.1093/gigascience/giz017

Watkins, D. C. (2017). Rapid and rigorous qualitative data analysis: The "raadar" technique for applied research. *International Journal of Qualitative Methods*, *16*(1), 1–9. https://doi.org/10.1177/1609406917712131

Weller, S. C., Vickers, B., Bernard, H., Blackburn, A. M., Borgatti, S., Gravlee, C. C., & Johnson, J. C. (2018). Open-ended interview questions and saturation. *PLoS One*, *13*(6), 1–18. https://doi.org/10.1371/journal.pone.0198606

Yuneline, M. (2019). Analysis of cryptocurrency's characteristics in four perspectives. *Journal of Asian Business and Economic Studies*, *26*(2), 206–219. https://doi.org/10.1108/jabes-12-2018-0107

Zali, M., & Maulidi, A. (2018). Fighting against money laundering. *BRICS Law Journal*, *5*(3), 40–63. https://doi.org/10.21684/2412-2343-2018-5-3-40-63

Zamanzadeh, V., Ghahramanian, A., Rassouli, M., Abbaszadeh, A., Alavi-Majd, H., & Nikanfar, A.-R. (2015). Design and implementation content validity study: Development of an instrument for measuring patient-centered communication. *Journal of Caring Sciences*, *4*(2), 165–178. https://doi.org/10.15171/jcs.2015.017

Zhao, W. (2018, August 20). *21-year-old trader prosecuted over bitcoin money laundering - Coindesk*. Coindesk. https://www.coindesk.com/21-year-old-trader-prosecuted-over-bitcoin-money-laundering

Appendix A: Interview Questions for Bank Employees

RQ1 - What are the financial crime risks and challenges faced by banks when dealing with cryptocurrency?

Interview Question 1– How long have you been working here, and how long have you been in BSA/AML related role?

Interview Question 2– What is your role in the anti-money laundering process?

Interview Question 3– What are the documents you verify for "Know Your Customer" when dealing with large money transfers or withdrawals? And how would you verify them?

Interview Question 4– Have you dealt with any cryptocurrency-related money laundering cases? If yes, how did you deal with them?

Interview Question 5- If you answered “Yes” to the above question, then could you please explain how each case differs from one another and what are the lessons you learned from each one?

RQ2 - How do banks identify and report suspicious account activities related to cryptocurrency?

Interview Question 6–What are some of the key signs or red flags pertaining to cryptocurrency cases? Can you explain?

Interview Question 7– What actions do you take when suspicious activity is identified?

Interview Question 8– What process do you follow to report the suspicious account activity?

RQ3 - What would help banks to minimize the financial crime risks and challenges that they face when dealing with cryptocurrency?

Interview Question 9– How is your organization proactive in minimizing financial crime risks and challenges that they face when dealing with cryptocurrency?

Interview Question 10– What are some of the suggested ways your organization can minimize these financial crimes dealing with cryptocurrency transactions? Can you elaborate?

Interview Question 11– How is your organization staying current with compliance regulation to combat cryptocurrency-related money laundering?

Interview Question 12– What are some of the challenges in identifying cryptocurrency cases?

Closing Question: Is there anything else you would like to add that I have not covered in my interview?

Appendix B: Interview Questions for the Director of Financial Investigations & Education

CipherTrace

RQ1 - What are the financial crime risks and challenges faced by banks when dealing with cryptocurrency?

Interview Question 1– How long have you been employed with CipherTrace, and how long have you been in your current role?

Interview Question 2– As someone not associated with any financial institution, how will you describe money laundering?

Interview Question 3– In your opinion, what is the greatest risk banks face with cryptocurrency-related money laundering? Are banks aware of these risks? If not, then why not?

Interview Question 4– Do you think banks have proper knowledge and training cryptocurrency-related cases? If they do not, what is the resolution?

Interview Question 5– Has any cryptocurrency cases being conducted using traditional banking products (demand deposits, withdrawals etc.)?

RQ2 - How do banks identify and report suspicious account activities related to cryptocurrency? Is their process efficient?

Interview Question 6– What are some of the steps banks can take in identifying cryptocurrency-related money laundering transactions? And how can they take these steps?

Interview Question 7–Are banks complaint ready in "Know Your Customer" when dealing with cryptocurrency-related money laundering? If not, what are the strategies and processes they can implement?

RQ3 - What would help banks to minimize the financial crime risks and challenges that they face when dealing with cryptocurrency?

Interview Question 8 – What are some of the suggested ways banks can minimize risks of cryptocurrency-related money laundering transactions?

Interview Question 9 – Do you think banks are current with compliance regulation to combat cryptocurrency-related money laundering? If not, why so?

Interview Question 10 – What do you think banks need to do to stay current with compliance regulation to combat cryptocurrency-related money laundering?

Interview Question 11 - What are some of the challenges in identifying cryptocurrency cases?

Closing Question: Is there anything else you would like to add that I have not covered in my interview?

Appendix C: Recruitment Letter

Dear [Recipient]:

As a graduate student in the School of Business at Liberty University, I am conducting research as part of the requirements for a doctoral degree. The purpose of my research is to understand the challenges posed by cryptocurrency for banks within the USA in order to identify and combat risks of financial crimes resulting in laundered money entering the banking system, and I am writing to invite eligible participants to join my study.

Participants must be 18 years of age or older; Anti-Money Laundering and Bank Secrecy Act (AML/BSA) risk specialists, bank managers, or bank compliance officers; and have been in their respective roles for a minimum of 6 months. Participants, if willing, will be asked to participate in a virtual (Zoom, Teams, Skype, Google Meet, etc.) or phone interview. It should take approximately 45-60 minutes to complete the study procedures. Names and other identifying information will be requested as part of this study, but the information will remain confidential. Following the interview, I may review your responses to the interview questions with you to validate them for accuracy if time permits; otherwise, I will email you the responses to check for accuracy.

In order to participate, please contact me at asharma5@liberty.edu to schedule a time for the interview. A consent document, which contains additional information about my research, is attached. If you choose to participate, you will need to sign and date the consent form and return it at any time between scheduling a time for the interview and when the interview occurs.

Participants will receive VISA gift cards of $25.00 electronically as compensation for taking part in my research.

Sincerely,

Avin Sharma
Doctorate Student
asharma5@liberty.edu

Appendix D: Consent

Title of the Project: CRYPTOCURRENCY AND FINANCIAL RISK CRIMES: A QUALITATIVE STUDY
Researcher: Avin Sharma

Invitation to be Part of a Research Study

You are invited to participate in a research study. In order to participate, you must be 18 years old or older; an Anti-Money Laundering and Bank Secrecy Act (AML/BSA) risk specialist, bank manager, or bank compliance officer; and have been in your respective role for a minimum of 6 months. Taking part in this research project is voluntary.

Please take time to read this entire form and ask questions before deciding whether to take part in this research project.

What is the study about and why is it being done?

The purpose of the study is to understand the challenges posed by cryptocurrency for banks within the USA, resulting in money laundering. The research questions will address the issues banks face while dealing with increasing cryptocurrency-related money laundering and the compliance gaps they have in their systems, prohibiting them from successfully monitoring all money laundering activities.

What will happen if you take part in this study?

If you agree to be in this study, I would ask you to do the following things:

1. Participate in a virtual (Zoom, Teams, Skype, Google Meet, etc.) or phone interview, which should take approximately 45-60 minutes.
2. Following the interview, I may review your responses to the interview questions with you to validate them for accuracy if time permits; otherwise, I will email you the responses to check for accuracy.

How could you or others benefit from this study?

Participants should not expect to receive a direct benefit from taking part in this study.

Benefits to society include the possibility for banks to understand the gaps in the compliance system to help them successfully track and monitor all cryptocurrency-related money laundering.

What risks might you experience from being in this study?

The risks involved in this research are minimal, which means they are equal to the risks you would encounter in your daily life.

How will personal information be protected?

The records of this study will be kept private. Published reports will not include any information that will make it possible to identify you as the participant. Research records will be stored securely, and only the researcher will have access to the records.

- Participant responses will be kept confidential through the use of pseudonyms/codes.
- Data will be stored on a password-locked computer and may be used in future presentations. After three years, all electronic records will be deleted.
- Participants will be protected at every level. The participant's confidential information will not be released to anyone except the researcher.

How will you be compensated for being part of the study?

Participants will be compensated for participating in this study. Each participant will receive a Visa gift card of $25.00 after they have completed the study process.

Is study participation voluntary?

Participation in this study is voluntary. Your decision whether to participate will not affect your current or future relations with Liberty University. If you decide to participate, you are free to not answer any question or withdraw at any time.

What should you do if you decide to withdraw from the study?

If you choose to withdraw from the study, please contact the researcher at the email address included in the next paragraph. Should you choose to withdraw, data collected from you will be destroyed immediately and will not be included in this study.

Whom do you contact if you have questions or concerns about the study?

The researcher conducting this study is Avin Sharma. You may ask any questions you have now. If you have questions later, **you are encouraged** to contact him at asharma5@liberty.edu. You may also contact the researcher's faculty sponsor, David Bosch, at dbosch1@liberty.edu.

Whom do you contact if you have questions about your rights as a research participant?

If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher, **you are encouraged** to contact the Institutional Review Board, 1971 University Blvd., Green Hall Ste. 2845, Lynchburg, VA 24515 or email at irb@liberty.edu

Your Consent

By signing this document, you are agreeing to be in this study. Make sure you understand what the study is about before you sign. You will be given a copy of this document for your records. The researcher will keep a copy with the study records. If you have any questions about the study after you sign this document, you can contact the study team using the information provided above.

I have read and understood the above information. I have asked questions and have received answers. I consent to participate in the study.

□ The researcher has my permission to audio record or video record me as part of my participation in this study.

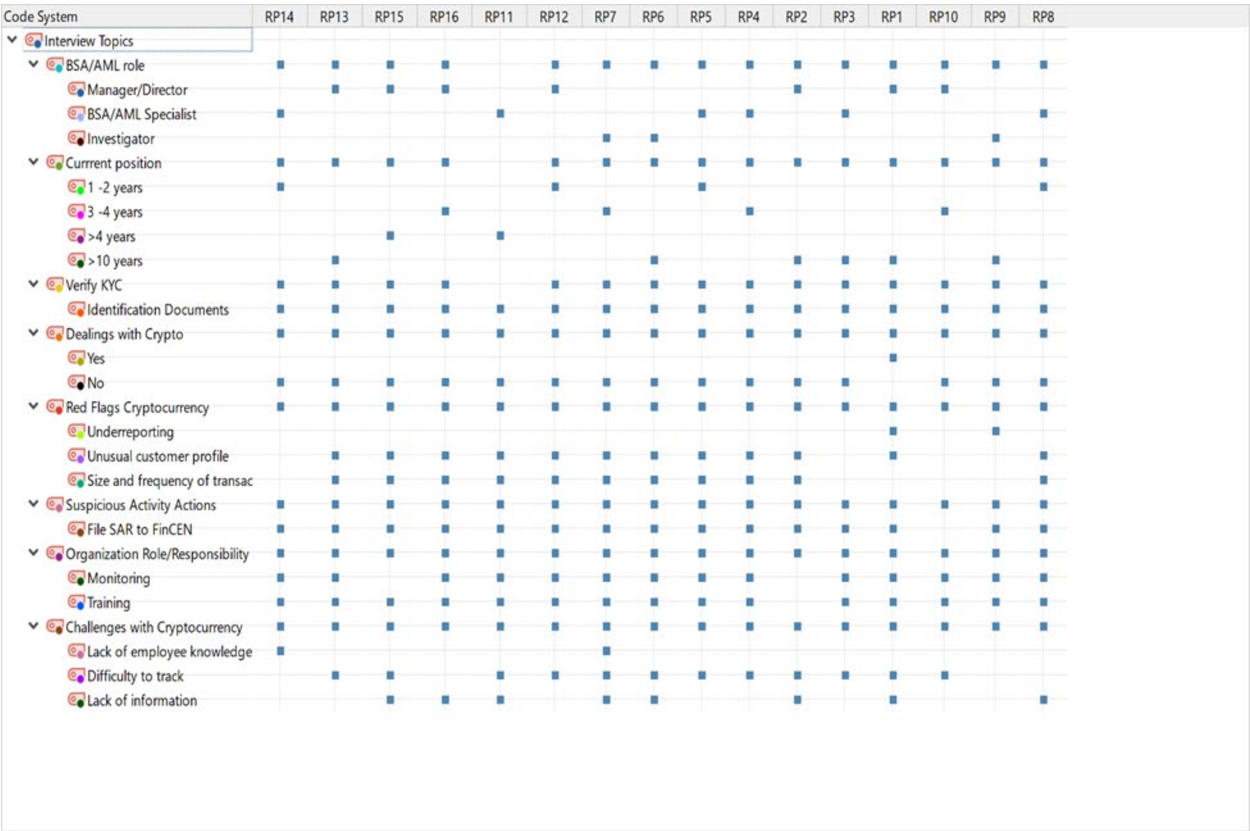
____

Printed Subject Name

____

Signature & Date

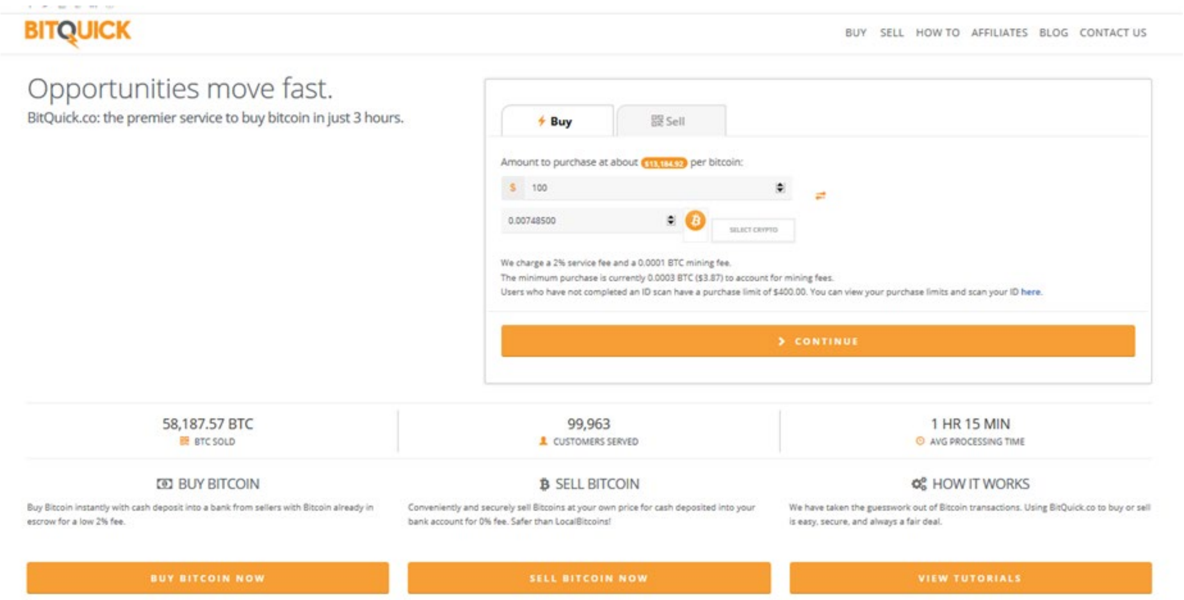
Appendix E: Coded Matrix - MAXQDA



Code System	RP14	RP13	RP15	RP16	RP11	RP12	RP7	RP6	RP5	RP4	RP2	RP3	RP1	RP10	RP9	RP8
Interview Topics																
BSA/AML role	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■
Manager/Director		■	■	■		■					■		■	■		
BSA/AML Specialist	■				■				■	■		■				■
Investigator							■	■							■	
Currrent position	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■
1 -2 years	■					■			■							■
3 -4 years				■			■			■				■		
>4 years			■		■											
>10 years		■						■			■	■	■		■	
Verify KYC	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■
Identification Documents	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Dealings with Crypto	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Yes													■			
No	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■
Red Flags Cryptocurrency	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Underreporting													■		■	
Unusual customer profile		■	■	■	■	■	■	■	■	■	■		■			■
Size and frequency of transac		■	■	■	■	■	■	■	■	■	■					■
Suspicious Activity Actions	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
File SAR to FinCEN	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■
Organization Role/Responsibility	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Monitoring	■	■		■	■	■	■	■	■	■		■	■	■	■	■
Training	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■
Challenges with Cryptocurrency	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Lack of employee knowledge	■						■									
Difficulty to track		■	■		■	■	■	■	■	■	■	■	■	■		
Lack of information			■	■	■		■	■			■		■			■

Appendix F: Cryptocurrency Purchase - BitQuick

Step 1



Opportunities move fast.

BitQuick.co: the premier service to buy bitcoin in just 3 hours.

Amount to purchase at about $13,184.92 per bitcoin:

$ 100

0.00748500

We charge a 2% service fee and a 0.0001 BTC mining fee.
The minimum purchase is currently 0.0003 BTC ($3.87) to account for mining fees.
Users who have not completed an ID scan have a purchase limit of $400.00. You can view your purchase limits and scan your ID here.

58,187.57 BTC
BTC SOLD

99,963
CUSTOMERS SERVED

1 HR 15 MIN
AVG PROCESSING TIME

BUY BITCOIN

Buy Bitcoin instantly with cash deposit into a bank from sellers with Bitcoin already in escrow for a low 2% fee.

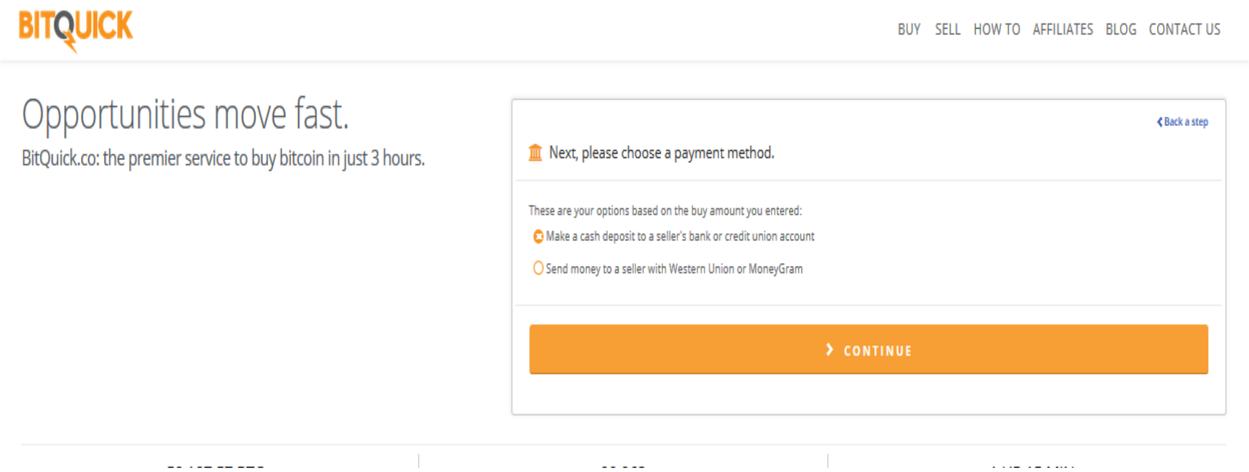
SELL BITCOIN

Conveniently and securely sell Bitcoins at your own price for cash deposited into your bank account for 0% fee. Safer than LocalBitcoins!

HOW IT WORKS

We have taken the guesswork out of Bitcoin transactions. Using BitQuick.co to buy or sell is easy, secure, and always a fair deal.

Step 2



Opportunities move fast.

BitQuick.co: the premier service to buy bitcoin in just 3 hours.

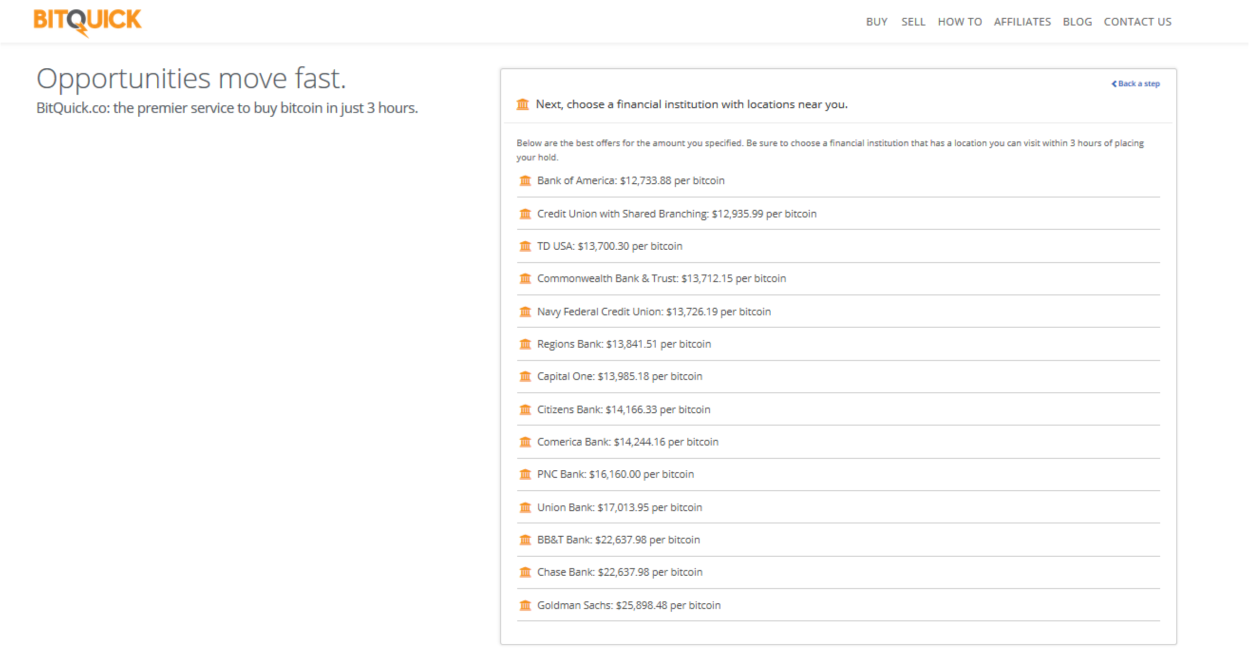
Next, please choose a payment method.

These are your options based on the buy amount you entered:

● Make a cash deposit to a seller's bank or credit union account

○ Send money to a seller with Western Union or MoneyGram

Step 3



Opportunities move fast.

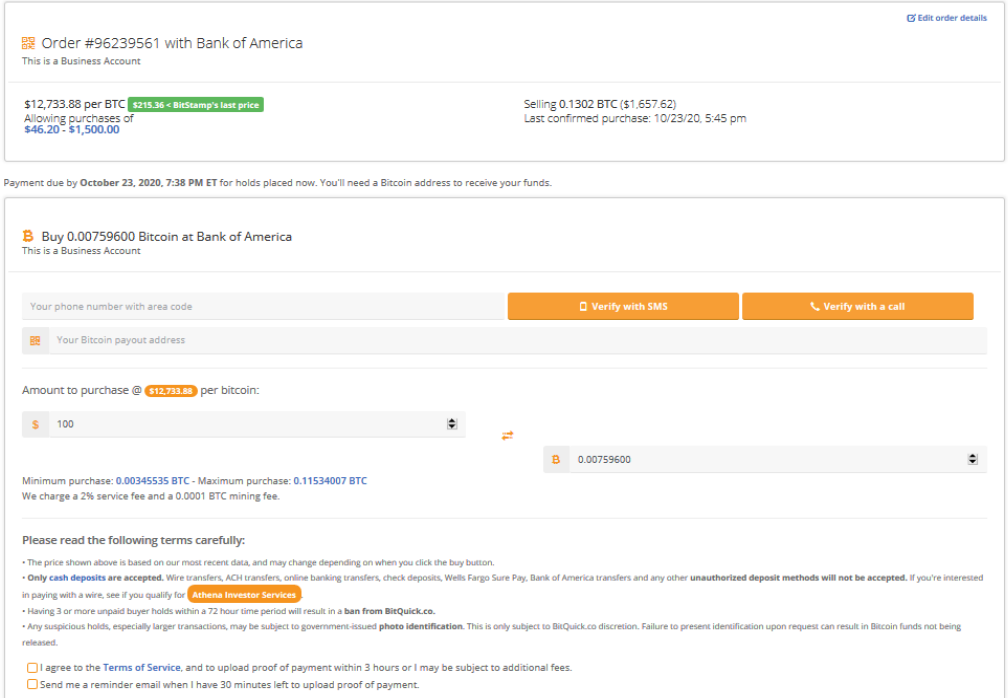
BitQuick.co: the premier service to buy bitcoin in just 3 hours.

Next, choose a financial institution with locations near you.

Below are the best offers for the amount you specified. Be sure to choose a financial institution that has a location you can visit within 3 hours of placing your hold.

- Bank of America: $12,733.88 per bitcoin
- Credit Union with Shared Branching: $12,935.99 per bitcoin
- TD USA: $13,700.30 per bitcoin
- Commonwealth Bank & Trust: $13,712.15 per bitcoin
- Navy Federal Credit Union: $13,726.19 per bitcoin
- Regions Bank: $13,841.51 per bitcoin
- Capital One: $13,985.18 per bitcoin
- Citizens Bank: $14,166.33 per bitcoin
- Comerica Bank: $14,244.16 per bitcoin
- PNC Bank: $16,160.00 per bitcoin
- Union Bank: $17,013.95 per bitcoin
- BB&T Bank: $22,637.98 per bitcoin
- Chase Bank: $22,637.98 per bitcoin
- Goldman Sachs: $25,898.48 per bitcoin

Step 4



Order #96239561 with Bank of America
This is a Business Account

$12,733.88 per BTC $215.36 < BitStamp's last price
Allowing purchases of
$46.20 - $1,500.00

Selling 0.1302 BTC ($1,657.62)
Last confirmed purchase: 10/23/20, 5:45 pm

Payment due by **October 23, 2020, 7:38 PM ET** for holds placed now. You'll need a Bitcoin address to receive your funds.

Buy 0.00759600 Bitcoin at Bank of America
This is a Business Account

Your phone number with area code

Your Bitcoin payout address

Amount to purchase @ $12,733.88 per bitcoin:

$ 100

B 0.00759600

Minimum purchase: 0.00345535 BTC - Maximum purchase: 0.11534007 BTC
We charge a 2% service fee and a 0.0001 BTC mining fee.

Please read the following terms carefully:

- The price shown above is based on our most recent data, and may change depending on when you click the buy button.
- **Only cash deposits are accepted.** Wire transfers, ACH transfers, online banking transfers, check deposits, Wells Fargo Sure Pay, Bank of America transfers and any other **unauthorized deposit methods will not be accepted.** If you're interested in paying with a wire, see if you qualify for Athena Investor Services.
- Having 3 or more unpaid buyer holds within a 72 hour time period will result in a **ban from BitQuick.co.**
- Any suspicious holds, especially larger transactions, may be subject to government-issued **photo identification**. This is only subject to BitQuick.co discretion. Failure to present identification upon request can result in Bitcoin funds not being released.

□ I agree to the Terms of Service, and to upload proof of payment within 3 hours or I may be subject to additional fees.
□ Send me a reminder email when I have 30 minutes left to upload proof of payment.