

2021

Security Strategies Information Technology Security Mangers Use in Deploying Blockchain Applications

PRINCE NANA YAW GYEDU NKRUMAH
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>



Part of the [Databases and Information Systems Commons](#)

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Prince Nkrumah

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee

Dr. Bob Duhainy, Committee Chairperson, Information Technology Faculty
Dr. Cheryl Waters, Committee Member, Information Technology Faculty
Dr. Jon McKeeby, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2021

Abstract

Security Strategies Information Technology Security Mangers Use in Deploying

Blockchain Applications

by

Prince Nana Yaw Gyedu Nkrumah

MS, Walden University, 2017

EMBA, Kwame Nkrumah University of Science and Technology, 2010

BS, Kwame Nkrumah University of Science and Technology, 1994

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

October 2021

Abstract

Blockchain is seen as a potential game-changer in many industries and a transformational technology in the 21st century. However, security concerns have made blockchain technology adoption relatively slow. Massive security breaches in cryptocurrency, an example of blockchain technology, have caused organizations to lose \$11.3 billion in illegal transactions, exacerbating these security concerns for information technology (IT) security managers who are worried about the safety of blockchain. Grounded in the routine activity theory, the purpose of this multiple case study was to explore strategies used by IT security managers to deploy blockchain applications securely. The participants were 4 IT security managers from companies in Ghana, the United States, and Europe with experience in implementing blockchain applications securely. Data collection was done using semistructured interviews and a review of organizational documents for triangulation. A thematic analysis produced three themes: (a) cryptographic key management, (b) comprehensive software auditing, and (c) traditional IT security controls. A critical recommendation is for security managers to implement the National Institute of Technology (NIST) key management and cybersecurity frameworks. The implications for positive social change include the potential to alter people's negative perceptions of blockchain security and giving security assurance to individuals and organizations on their digital assets stored in a blockchain system. In addition, a secured blockchain system could improve people's confidence in blockchain applications for an increased adoption rate of this useful technology development.

**Security Strategies Information Technology Security Mangers Use in Deploying
Blockchain Applications**

by

Prince Nana Yaw Gyedu Nkrumah

MS, Walden University, 2017

EMBA, Kwame Nkrumah University of Science and Technology, 2010

BS, Kwame Nkrumah University of Science and Technology, 1994

Doctoral Study Submitted in Partial Fulfillment
of the Requirements for the Degree of
Doctor of Information Technology

Walden University

October 2021

Dedication

I dedicate this work to my late father, who always encouraged me to hit my academic pyramid, and my immediate family (Genevieve, Princess, Phoebe) for supporting me throughout the program. Also to my siblings and extended family for supporting me in various ways during this program.

Acknowledgments

I thank the Almighty God for the gift of life, health, and resources to enable me to complete this course successfully. I am incredibly grateful to Dr. Duhainy, Dr. Waters, and Dr. Mackeeby for their guardianship and mentoring throughout the course. Great appreciation also goes to the entire faculty and staff of Walden University for their help and direction during my academic time with the school. To my wife and children, I say a big thank you for the time and peace you gave me during this Doctor of Information Technology educational journey.

Table of Contents

List of Tables.....	v
List of Figures	vi
Section 1: Foundation of the Study	1
Background of the Problem.....	1
Problem Statement.....	1
Purpose Statement	2
Nature of the Study.....	2
Research Question	4
Interview Questions	4
Theoretical or Conceptual Framework	5
Definition of Terms	5
Assumptions, Limitations, and Delimitations	7
Assumptions	7
Limitations.....	7
Delimitations	8
Significance of the Study	8
Contribution to Information Technology Practice.....	8
Implications for Social Change	9
A Review of the Professional and Academic Literature.....	10
Routine Activity Theory and Cyber Crime	11
Routine Activity Theory and Information Technology	16

Supporting Theories	19
Contrasting Theories	21
Criticism of Routine Activity Theory	21
Blockchain	22
Blockchain Information Technology Architecture	33
Blockchain Applications	37
Blockchain Application Security Concerns	44
Blockchain Security Strategy	49
Transition and Summary	54
Section 2: The Project.....	56
Purpose Statement	56
Role of the Researcher	56
Participants	58
Research Method and Design.....	60
Research Method	60
Research Design	63
Population and Sampling	66
Ethical Research	67
Data Collection	69
Instruments	69
Data Collection Technique	71
Data Organization Techniques	74

Data Analysis Technique	75
Reliability and Validity.....	78
Reliability	79
Validity.....	80
Credibility.....	81
Transferability.....	82
Confirmability/Dependability.....	83
Transition and Summary	83
Section 3: Application to Professional Practice and Implications for Change	85
Introduction	85
Overview of Study.....	85
Presentation of the Findings	86
Theme 1: Cryptographic Key Management	87
Theme 2: Software Auditing	94
Theme 3: Traditional Security Controls.....	97
Application to Professional Practice.....	102
Implications for Social Change	104
Recommendations for Action.....	106
Recommendations for Further Study.....	108
Reflections.....	108
Summary and Conclusions.....	109
References.....	111

Appendix A: Interview Guide.....	146
Appendix B: Permissions to Reuse Figures and Tables	149

List of Tables

Table 1. Blockchain Attacks Over the Years and Estimated Cost of Cryptocurrency	
Stolen	45
Table 2. Blockchain Categories of Security Concerns and Related Vulnerability	47
Table 3. Major Theme Cryptographic Key Management With Supporting Metrics	87
Table 4. Major Theme Software Auditing With Supporting Metrics	93
Table 5. Major Theme Traditional Security Control With Supporting Metrics	97

List of Figures

Figure 1. Blockchain Diagram	24
Figure 2. Proof of Work Process Flow	28
Figure 3. Proof of Stake Process Flow	29
Figure 4. PBFT Stages.....	32
Figure 5. Three-Layer Blockchain Architecture	34
Figure 6. Six-Layer Blockchain Architecture.....	35
Figure 7. Two-Layer Generic Blockchain Information Technology Architecture	37
Figure 8. Blockchain Application Implementation in a Microgrid.....	40
Figure 9. Typical Use of Blockchain for a Hospital.....	42
Figure 10. Blockchain in Public Sector, March 2017.....	44
Figure 11. Blockchain Application Vulnerabilities.....	46
Figure 12. Stacked Model of Reference Architecture	51
Figure 13. ThreatóRisk Assessment Model of Reference Architecture	52
Figure 14. Proposed Hybrid Blockchain Security Framework.....	54

Section 1: Foundation of the Study

Background of the Problem

Many in computing and business circles see blockchain technology as the next big development after the internet. Weber (2018) explained that blockchain is a shared, decentralized, secure, unchangeable digital ledger that will increase trust and efficiency to business networks. Bitcoins is the most popular cryptocurrency run on blockchain technology. Other potential applications of blockchain technology that could be game changers in most industries exist. At a U.S. House of Representatives hearing, Cuomo of IBM explained that blockchain is a revolutionary technology that can enable a reimagination of many of the world's most fundamental business processes and open the door to new styles of digital interactions (Government Publishing Office, 2018). Blockchain technology, however, attracts a fair amount of criticism, fear, and opposition due to recent security breaches in cryptocurrency exchanges, which caused the loss of millions of dollars (Catalini, 2018). CypherTrace, a U.S. security firm, reported that over \$927 million was stolen from exchanges and trading platforms running on blockchain technology within the first 9 months of 2018 (Chavez-Dreyfuss, 2018). If skeptics are to be convinced of the benefits of adopting blockchain technology, then information technology (IT) managers must have solid security strategies in place to avert the hacking of blockchain applications. In this study, I explored the security strategies IT managers have used in deploying blockchain applications to protect against breaches.

Problem Statement

Even though blockchain is a burgeoning technology that could affect many industries and transform technology in the 21st century, security concerns have

slowed its adoption (Government Publishing Office, 2018). These concerns have been exacerbated by massive security breaches in cryptocurrency exchanges, the best-known example of blockchain technology, that have caused governments and businesses to lose \$11.3 billion in illegitimate transactions and revenue taxes (Bischoping, 2018). The general IT problem is that some businesses and organizations who deploy blockchain technology without a security strategy could expose the application to breaches. The specific IT problem is that some IT security managers lack security strategies to deploy blockchain applications securely.

Purpose Statement

The purpose of this qualitative, multiple case study was to explore the security strategies IT security managers use to deploy blockchain applications securely. The population consisted of IT security managers from blockchain application companies in Ghana, the United States, and Europe with experience in security and blockchain applications. The findings from this study may benefit information security practice by improving the understanding of the nature of blockchain and the security implementation requirements. The implications for social change include the potential to protect users' private digital assets and data in the blockchain.

Nature of the Study

In considering which was appropriate for my research, I looked at the three research methods— qualitative, quantitative, and mixed— in terms of their fit in the context of this study. I concluded that a qualitative research method was the most appropriate method that aligned with my study because qualitative methods aim to provide in-depth insights and understanding of real-world problems, as explained by Moser and Korstjens (2017). Qualitative methods are also seen as an interpretive

technique that can describe, decode, translate, and otherwise come to terms with the meaning of certain occurring phenomena in the social world (Bandara et al., 2012). In other words, a researcher relies on subjectivism, which is an epistemological position that argues that human subjects create the meaning of a phenomenon (Hathcoat & Nicholas, 2014). I did not consider the quantitative method because, according to Everett et al., (2015), quantitative researchers build on the positivist epistemology and use theory to formulate and test hypotheses. I was not seeking to test a hypothesis, and consequently, my choice of qualitative method. Mixed-method research is built on pragmatism and uses a combination of qualitative and quantitative methods (Onwuegbuzie & Corrigan, 2014). Mixed methods also include formulation and testing of a hypothesis, as argued by Green et al. (2015). My study did not involve a combination of two research methods, neither was there a formulation of hypothesis, hence my decision of not using mixed methods.

Among the five qualitative research designs I evaluated, case study was the most appropriate design for my research topic. Park and Park (2016) articulated that a case study entails understanding the intricate complexity and idiosyncrasy of one particular case investigation of a situation that is worthy of being analyzed. In addition, Harwati (2019) explained that a case study involves studying the practices or beliefs of an organization or phenomenon in its real-life context. Harwati also articulated that, in a case study, the respondents are seen as experts and not just objects that inform or produce the data. These antecedents supported my intentions for the research because I intended to understand security strategies from experts.

I considered other approaches such as ethnography, phenomenology, and narrative research. As described by Cupit et al. (2018), ethnography entails adopting a

cultural lens to observe and interpret the activities and behaviors of people in their natural settings. My research focused on the experiences of individuals about their knowledge concerning blockchain security strategies and not their culture, beliefs, and behaviors; therefore, this approach was not relevant for my study. Although phenomenology research is used to study the lived experiences of individuals in a phenomenon (Zahavi, 2019), the approach did not align with my study because I was not seeking to understand a lived experience but rather focused on security strategies IT security managers use in protecting blockchain applications. The narrative design involves systematically coding individual differences in how they tell their stories about significant events in their lives to understand the extent to which they create meaning and purpose (Grysmen & Lodi-Smith, 2019). My study was not about an individual's life, and narrative design would have been counterproductive to the study.

Research Question

What strategies do IT security managers use in deploying blockchain applications securely?

Interview Questions

1. Describe the security threats that you encounter on blockchain applications.
2. Describe the nature of these attacks.
3. Why do you think blockchain applications are under attack?
4. In your opinion, are blockchain security threats different from traditional IT threats?
5. Explain the strategies that you used successfully against these threats.
6. Explain other strategies, if any, you tried but did not work.

7. How did you implement these strategies?
8. Explain the challenges, if any, in the implementation.
9. Do you have any additional information you think might help the study that you do not mind sharing?

Theoretical or Conceptual Framework

The conceptual framework I adopted for this study was the routine activity theory (RAT), developed by Cohen and Felson (1979). The framework states that crime occurs when three elements come together in time and space: (a) the presence of a motivated offender, (b) an accessible target, and (c) the absence of capable guardians that could intervene (New South Wales Government, 2018). Even though RAT is used to formulate policies and programs for crime prevention in the terrestrial world, the theory's tenets can also be used to address criminality in cyberspace (Leukfeldt & Yar, 2016). Leukfeldt and Yar (2016) further argued that the four elements of RAT—value, inertia, visibility, and accessibility—that make a victim attractive to a motivated offender have their equivalent in the cyber world. For example, a terrestrial offender's value on a physical dollar bill is no different from the value on cryptocurrency in the cyber world. This framework was suited for my study wherein I sought to understand the strategies IT security managers use in deploying blockchain applications securely to prevent motivated offenders from breaching blockchain applications to access valued digital assets.

Definition of Terms

Bitcoin mining: The process of adding transaction records to Bitcoin's public ledger of past transactions or blockchain by using specialized computer hardware to

find a particular mathematical hash function and being rewarded for success with new bitcoins (Easley et al., 2019).

Blockchain: A shared, decentralized, secure, unchangeable digital ledger, bringing increased trust and efficiency to business networks (Weber, 2018).

Blockchain as a service: A cloud platform that enables developers to develop blockchain applications in a cloud environment without worrying about the underlining infrastructure, which is managed by the cloud provider (Zheng et al., 2019).

Cryptocurrency: A digital cash that uses cryptography to secure its transactions and to verify the transfer of digital assets through blockchain and over the internet without the use of a centralized banking system (Andriole, 2020).

Cryptocurrency wallet: A collection of private keys and public keys through which transfer of cryptocurrencies or tokens can be accomplished (Volety et al., 2019)

Distributed ledger: A record of transactions maintained by consensus among a network of peer-to-peer nodes that may be geographically dispersed (Kuhn et al., 2019).

Initial coin offerings (ICOs): A way entrepreneurs raise funds to finance innovative ventures that use distributed application technology (DLT) or a blockchain (Fisch, 2019).

Smart contract: An electronic contract involving digital assets and two or more parties; some or all parties invest in the assets that are automatically redistributed among those parties when certain conditions are met after the initiation of the contract (Hu et al., 2019)

Tokens: Given in exchange for relatively liquid cryptocurrency (like Bitcoin) or fiat currency in an ICO to fund the development of a distributed ledger project or jumpstart an ecosystem of users in a DAP (Crosser, 2018)

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are opinions accepted as valid without proof or argument (Hufford, 1996). In the case of research, assumptions are portions of information considered valid for a theory to be tested (Foss & Hallberg, 2014). Assumptions also allow a researcher to know roughly what kinds of observation and explanation will be accepted or rejected (Hufford, 1996). In this study, I focused on understanding the strategies IT security managers use in protecting blockchain applications, and I assumed that the security managers who participated would have the requisite experience in the research area. I assumed that all participants' responses to interview questions would be accurate and candid. I also assumed that the participants had a sincere and voluntary desire to participate in the study.

Limitations

While research assumptions are normally under the control of the researcher, limitations, on the other hand, are outside the power of the researcher but exist and may influence the outcome of the study. Theofanidis and Fountouki (2019) postulated that limitations are potential weaknesses generally beyond a researcher's control and closely related to the kind of research design selected. For this qualitative study, some participants may have responded in a particular way to please me, which is a limitation in case study research (Yin, 2014). I was also limited by the number of

cases I was able to study in the given stipulated time, which may not have been enough to reach data saturation.

Delimitations

In my study, I set up some delimitations to ensure that my aims and objectives were possible. Delimitations are boundaries and scope of a study set by the researcher (Marshall & Rossman, 2016). Theofanidis and Fountouki (2019) argued that delimitations are in the control of the researcher and help the researcher stay on course in objectives. A delimitation for my study was the use of only four cases and the use of only IT security managers with experience in blockchain application. I also restricted myself with IT security managers in Ghana, the United States, and Europe.

Significance of the Study

Contribution to Information Technology Practice

This study may be valuable to IT security managers because the outcomes could produce best practice security strategies for protecting blockchain applications. This might provide IT security managers a list of actions the IT practitioner can use in assessing security in a blockchain application deployment. Additionally, the study's findings may contribute to IT practices by enriching the body of knowledge on blockchain security threats and effective strategies IT security managers can use in mitigating the threats.

The objective of my study was to develop a blockchain application security strategy template for IT security managers grounded in RAT, which has been used to successfully fight crime in terrestrial space (Drawve et al., 2014). Having such a template, IT managers will have similar tools and strategies used by terrestrial crime officers to deter crime. For example, the core strategies used by terrestrial crime

managers to fight crime is to eliminate one of the elements of the crime triangle, such as accessible target, proposed in the RAT. The equivalent in cyberspace could be a hardened firewall, which makes accessibility to the application difficult for would-be attackers.

Implications for Social Change

The implications for positive social change includes the potential to provide an underling data integrity platform for several areas of society, such as democracy and governance, finance, health, energy, and agriculture. Blockchain will be among the top 10 strategic technology trends that will disrupt business in the next 5 years (Holotescu, 2018). Galen et al. (2018) found that 55% of social-good blockchain initiatives were estimated to impact their beneficiaries by early 2019. These were blockchain based projects on governance, land rights, health, financial-inclusion, agriculture, environment, education, and energy.

For example, Estonia uses e-governance based on blockchain to deliver 99% of government services online to its populace. Tkachuk (2018) articulated the use of blockchain in fighting societal corruption and promoting of fair value by ensuring transparency in transactions. For example, Weber (2018) illustrated that blockchain can be used to hold the complete medical history for each patient, with multiple levels of control by the patient, doctors, regulators, hospitals, insurers, and other stakeholders with a secure mechanism to record and maintain a comprehensive medical history for every patient. With such a system in place, clients and medical practitioners benefit from a single record that can prevent conflicts in drug recommendations and/or conflicting side effects in certain drug combinations.

A Review of the Professional and Academic Literature

To provide an encompassing literature review, I searched for and performed a critical analysis of various sources and content for relevant literature ranging from reports, seminal books, presentations, journals from ACM Digital Library, EBSCOhost, Google, Google Scholar, ProQuest Central, ResearchGate, Science Direct, and the Walden University Library. To ensure I used peer-reviewed articles for the study references, I used the Ulrich enabled search engine system to crosscheck and confirm scholarliness. The in-depth research and analysis I conducted empowered me with knowledge on past and present information on the conceptual theory and application of RAT. In addition, the research gave me the opportunity to explore blockchain applications, blockchain application security concerns, and blockchain security strategies.

I collected 206 articles for the literature review, of which 195 were peer-reviewed and six were seminal authors. In searching for academic materials for the paper, I used broad terms such as *crime theories*, *cybersecurity*, *blockchain*, *information security*, and *strategies*. I then narrowed the search down to more specific terms such as *RAT*, *cybercrime*, *cyberattacks*, *cyber victimization*, *cybersecurity strategies*, *data breaches*, *blockchain applications*, *blockchain breaches*, *blockchain security concerns*, *cryptocurrency theft*, *online crime theories*, *information security strategies*, and *blockchain security strategies*. In the analysis of the various articles and journals found, I looked out for themes of RAT and cyberspace, information security strategies, blockchain application threats, and blockchain security strategies.

The literature review gave me a strong academic foundation to enable me to investigate and explore existing blockchain applications security strategies from

experienced IT security managers. I used security managers who have skills, knowledge in deploying blockchain enabled applications securely to ensure that information and strategies were practical and implementable. The literature review has three parts: the first part covers information regarding crime theories and their application to cybersecurity; in the second part I analyze blockchain, its applications and related security issues; and the third part is a discussion of information security strategies.

Routine Activity Theory and Cyber Crime

RAT is a concept originally used in fighting environmental terrestrial crime. The theory states that for crime to occur three elements— an accessible target, the absence of a capable guardian that can intervene, and the presence of a motivated offender— must come together in time and space (Cohen & Felson, 1979). RAT as a crime prevention method is focused on the three elements that make up the theory (Kigerl, 2012). The approach is to deal with at least one of the elements to prevent crime, but the most effective measure is to address all three elements. However, Eck (2003) proposed that a controller who can reduce the potential of the problem could influence each of the three RAT elements that form the crime triangle (offender, target, and guardian). Eck argued that handlers can control offenders, place managers can control places, and guardians can control the targets. Sampson et al. (2010) extended the controllers to include super controllers who can exert influence on handlers, managers, and guardians to prevent the underlying problem. According to Sampson et al., super controllers make cost benefits decisions to manage crime through formal, diffuse, and personal mechanisms.

In the formal mechanism framework, super controllers exercise their authority through an institutional setting that defines who influences whom, in which ways, and under what circumstances. Systems, such as organizations, contracts, financial commitments, regulations, and the courts provide the settings for formal super controllers to function while the diffuse mechanism indirectly influences the controllers in a general and nonspecific way via political institutions, the markets, and the media (Sampson et al., 2010). Sampson et al. further explained that personal super controllers rely on personal and informal connections from groups and families to alter the behavior of a controller. For example, a family member or a trusted friend using their connection to an offender could convince the offender from performing an act of malicious intent.

Even though RAT was proposed for terrestrial crime, researchers have proposed its usefulness in fighting cybercrime. William (2016) articulated that RAT focuses on criminal events rather than the criminal; this is an important fact for cybercrime because in cyberspace, there is rarely access to the criminals to study their motivations. The focus is on cybercriminal events that occur often and leave behind digital signatures that can be analyzed. Hawdon et al. (2017) articulated that RAT could be applied to cyberspace because online routine activity could bring individuals or assets and potential offenders together in cyberspace where there are no capable guardians to confront offenders. Hawdon et al. argued that, with regard to time and space, where the RAT triangle converge, evidence suggests that virtual contact can occur asynchronously; therefore, convergence at a specific time becomes irrelevant as postulated in the original theory. Potential offenders and victims or digital assets meet asynchronously in a virtual space through their network devices. Thus, the theory

proposed by Cohen and Felson (1979) is applicable in virtual and real-world situations.

Leukfeldt and Yar (2016) argued that distance between target and offender is a factor for crime occurrence in the physical world, but in cyberspace, distance does not exist between offender and victim. Thus, applying RAT in virtual offenses may be problematic. Leukfeldt and Yar cautioned that the distance factor alone could not be used to determine the viability of RAT theory in addressing cybercrime. An empirical study conducted on RAT and cybercrime was inconclusive but indicated that most cybercrime could be explained with the theory (Leukfeldt & Yar, 2016). In the case of this qualitative study grounded in the conceptual framework of RAT, I examined various elements of RAT and its equivalent in cyberspace to make the case for the use of the theory in this research.

According to RAT, an accessible target could be a person, an object, or a place. Attributes such as available, concealable, disposable, enjoyable, inertia, valuable, visible, and removable have been used for accessible targets. Cohen and Felson (1979) articulated that a suitable target is any object or person that meets and fulfills the needs and wants of a motivated offender. In addition, Felson and Clarke (1998) argued that the suitability of a target depends on their assessed value, inertia, visibility, and access. *Value* is defined as the actual value or perceived value placed on an object by the offender, and *inertia* determines the physical properties of the item that can either encourage or discourage the offender. *Access* describes the prospects of the offender in attaining the object or person, and *visibility* is the ability of the offender to see or know about the object or person. These antecedents of target

suitability, according to Hawdon et al. (2017), are interrelated and influenced by the extent to which people or objects are in contact with motivated offenders.

In support of Hawdon et al.'s (2017) claim, Newman and Clarke (2003) argued that, in cyberspace, the frequency and variety of online routine activities differentiates a target from nontarget of cybercrime. In other words, users who are active online become closer to being cybercrime victims than those who spend less time online. Aside from people as targets online, Leukfeldt and Yar (2016) suggested that suitable targets in cyberspace include proprietary data, personal information, credit card data, online financial transaction services, and computer systems. In addition, cryptocurrency and crypto mining are becoming attractive targets for cybercriminals (Network Security, 2018). These targets have value, inertia, visibility, and accessible in cyberspace.

Regarding RAT, Cohen and Felson (1979) explained that a capable guardian is someone who can come to the aid of the target when the offender and target come together in time and space. A capable guardian can be a person whose mere presence would deter potential offenders from perpetuating a crime (Hollis et al., 2013). Cohen and Felson (1979) proposed that a capable guardian could also be an object in place of a person, such as CCTV that is being monitored from a remote location. Other guardians include police patrols, security guards, door staff, vigilant staff and coworkers, and friends and neighbors (Cohen & Felson, 1979). Drawve et al. (2014) articulated that other security measures, such as alarms, locks, and electric fencing, could also be considered guardians because even though these security measures will not come to the aid of the victim, they act as a deterrent. Studies have proven that things or people perceived as guardians have averted countless crimes. For example,

Murray and Roncek (2008) found that there is less crime in the immediate area of a bar compared to adjacent blocks because potential offenders saw bar patrons as capable guardians.

Moreover, Felson and Boba (2010) suggested that the mere presence of another person could serve as a warning of a potential capable guardian. Miró-Llinares (2014) indicated that guardians, to a greater extent, are owners who guard properties. In cyberspace, guardianship can be seen as target hardening or any action that prevents an offender from having access to the target. Hawdon et al. (2017) pointed out that those who have operationalized online guardianship use firewalls, antivirus programs, filtering, and blocking software. In addition, systems such as intruder detection and prevention systems and any related intervention in the cyberspace that prevents digital targets from being accessed by a motivated offender can be considered a guardian.

A motivated offender is an individual who has the capacity to carry out criminal intent (Cohen & Felson, 1979). The extent to which a target is in an offender's reach relates to the likelihood that an attack will take place (Hawdon et al., 2017). RAT theory can be used to assume that potential motivated offenders already exist; they act rationally with their criminal intent, and therefore the magnitude and source of offender motivation is irrelevant (Nikitkov et al., 2014). The low attention given to offenders in RAT theory has been highlighted by Navarro and Jasinski (2015), who argued that a motivated offender is rarely investigated because it is assumed there a plethora of offenders in society. The focus of RAT is on the localized situated assembly of offenders, targets, and capable guardians in a market or social ecology (Nikitkov et al., 2014). Therefore, a well-planned ecological design of social

and market places can reduce crime and make its displacement to other target owners or objects difficult (Nikitkov et al., 2014). In testing motivated offenders' applicability to online, Leukfeldt and Yar (2016) found there are an abundance of offenders online in the form of online fraudsters, hackers, pirates, stalkers, and others.

Routine Activity Theory and Information Technology

RAT was originally developed to explain terrestrial crime, but the theory has seen success in the study of cybercrime. For example, Van-Wilsem (2011) used RAT to study online victimization and concluded the theory could be used to explain both online and traditional face-to-face victimization. Williams et al. (2019) used RAT in a study to predict insider cyber victimization and concluded that both routine activity in the handling of confidential data and guardianship processes were significant to predict insider cyber victimization. Shaikh and Oliveira (2019) used RAT as a theoretical lens to investigate how situational and environmental features influence insider risks, and their study provided a foundation for future research in securing digital assets.

William (2016) conducted an empirical study on online identity theft using RAT and concluded that risky online routine activity correlates with people who often engage in online routine activities. Some of the risky online activities revealed by William's study included using public internet access and selling on online auction sites. Reyns and Henson (2016) studied online identity theft using RAT as the theoretical framework. The researchers investigated the relationship between routine online activities and identity theft victimization in England and Wales (Reyns & Henson, 2016). Reyns and Henson found that several online routines were positive predictors of identity theft, including online banking, online shopping, emailing,

instant messaging, and downloading music and videos. The researchers explained that the risk of identity theft in the cyberworld does not depend on individuals' exposure but rather information about the individual, directly related to online activities (Reyns & Henson, 2016). Reyns and Henson argued that time spent in chat rooms or online is an indicator of exposure to online offenders.

In a study to determine why some nations have high cybercrime, Kigerl (2012) used RAT and determined that countries with high internet use per capita have high cybercrime rates. Oni et al. (2019) investigated the increase in cybercrime because of e-governance implementation in Nigeria and used RAT as the conceptual framework. The researchers examined the effect of cybercrimes on implementing the digital government in Nigeria's public sector and argued that the daily use of information and communications technology (ICT) to conduct government processes by citizens and institutions increases the routine online activities that expose them to online criminals. Therefore, by analyzing secondary data from peer-reviewed publications and other authentic sources using RAT as the foundation, Oni et al. discovered a significant threat posed by an increase in cybercrime against the digital governance implementation in the Nigerian public sector.

Abhishta et al. (2019) studied victims' routine influence on distributed denial of service attacks (DDoS) using the RAT framework. Abhishta et al.'s work explicitly answered why DDoS targeted academic institutions and if the attacks were random or planned. The authors hypothesized the attacks were motivated and used the RAT tenets to analyze the data. According to RAT, changes in crime rates are related to days that affect the routine. Therefore, for an academic institution, when most teaching-related activities are halted during holidays, an attacker whose aim is to

interrupt teaching activities will not be motivated to launch an attack during these periods. Abhishta et al. (2019) concluded that, based on RAT, the change in the victims' daily activities would influence the attack pattern. In the academic environment, a motivated attacker would target the network infrastructure when school is in session. Hawdon et al. (2020) used RAT to examine the effect of the COVID-19 pandemic on cyberattacks. The research suggests the pandemic altered people's routine activities and could influence cyberattacks. Hawdon et al. compared prepandemic and postpandemic rates of victimization using a data set designed to monitor cyberattacks. The researchers concluded that the pandemic has not radically changed cyber routines nor altered cyber victimization rates. Nevertheless, the use of RAT to predict cyber victimization gave explicit support for the theory's ability both before and after the pandemic.

Whitty (2019) investigated people's susceptibility to falling for cyber fraud and used RAT as a theoretical lens to understand the situation. The researcher examined if users' demographic characteristics and their online routine influenced their exposure to cyber fraud. Whitty explained that users' demographic characteristics tend to shape their routine online activities in a way that provides indicators in determining the probability of being targeted for online fraud. According to the article, computer use was an essential predictor of receiving a phishing email used for fraud attacks. In general, Whitty concluded that routine online activity, such as making online purchases, engaging in social networking, and posting information, makes one vulnerable for cyber fraud that includes phishing, hacking, and malware infection.

Choo (2011) suggested in his article that some crime theories can be used as strategies in addressing cybercrimes. Choo argues that because RAT proposes that crime occurs when a suitable target is in the presence of a motivated attacker and the absence of a capable guardian, cybercrime can be prevented by targeting these three areas. That is (a) increasing the effort required to offend, (b) increasing the risk of being caught and (c) reducing the reward of offending. Choo suggested that in the case of making offending difficult, content providers could integrate security into their software, hardware and system development life cycle. On the other hand, a study by Nguyen (2020) analyzes the current situation of cybercrime in Vietnam using RAT framework. The research analyzed published and unpublished reports of international and domestic organizations using RAT's three factors, namely, likely offenders, suitable targets, and the absence of capable guardians. The study aimed to answer how much the dimensions of each RAT factor influences cybercrime in Vietnam, and what factor is the most important in solving the cybercrime. Besides, the study examined whether the RAT can be applied to cybercrime. The research concluded that government, organizations, and personal guardianship are necessary to frustrate motivated offenders to reduce cyber-attacks. Also, the study confirmed the use of RAT in understanding cybercrime and prevention.

Supporting Theories

Convenience theory is one of the theories that has also been used to explain crimes in cyberspace but uses different elements from RAT. The convenience theory explains that three dimensions, namely economic dimension, organizational dimension and, behavioral dimension facilitate white-collar crime (Nolasco Braaten, & Vaughn, 2019). The economic dimension is what drives the financial desire of the

offenders to crime as a convenient way of satisfying personal needs and organizational profit (Adam et al., 2005). The organizational dimension is what gives the offenders the convenient access to corporate resources and personnel to commit the crime. The behavioral dimension enables the offenders to conveniently justify and rationalize their deviant behavior (Gottschalk, 2018). Nolasco Braaten and Vaughn (2019) confirmed the convenience theory's support for cybercrime by empirically examining cases of white-collar crimes and fraud involving cryptocurrency in U.S. federal district and circuit courts, which indicated offenders exhibited antecedents of the theory. I did not use this theory because it focuses on mainly white-collar crimes, which is just a subset of crimes committed in cyberspace.

Situational crime prevention (SCP) theory, like RAT also focuses on the environment within which certain crime occurs. According to the theory, crime can be prevented by manipulating the environment in a way that increase the risk to the offender and reduces the potential reward for the crime (Mandala & Freilich, 2018). Meaning, crime occurs when the environment creates the opportunity for the offender to commit an offence (Freilich et al., 2020). According to Freilich et al. (2020), the environment differ as to whether it create provocation or entice the offender to commit crime, therefore putting in interventions that reduces these opportunities will reduce ability of the offender to commit crime. Hinduja et al. (2013) articulated that the SCP theory can be applied to cyberspace because space in virtual world can be designed to prevent crime by target hardening, access control, deflecting offenders, and controlling facilitators. For example, in target hardening the asset such as sensitive digital data is encrypted to make it difficult for the offender to access (Hinduja et al., 2013).

Contrasting Theories

Social learning theory (SLT) is a general theory of crime that has been used to explain all manners of criminal behaviors by focusing on the offender instead of the environment or situations as RAT does. Burruss et al. (2012) postulated that SLT is based on the idea that individuals are influenced and motivated to commit crime by association or being exposed to others who are already committing the crime. The SLT originally proposed by Akers in 1966 has four fundamental premises that include differential association, definitions, differential reinforcement, and imitation (Burruss et al., 2012). Akers (1998) proposed that exposure to deviate behavior gave individuals the definitions that are seen as either approving or rejecting the behavior. These definitions once accepted by the individuals becomes the rationalization for them when they want to commit crime. The differential reinforcement on the other hand indicates the rewards that are associated to a particular criminal behavior. However, this behavior is originally leant by imitating deviant behaviors of others through watching and listening to them. Therefore, individuals commit crime by putting into action what they have seen others do (Burruss et al., 2012). The use of SLT in cyberspace is supported by the software piracy study conducted by Burrussø team. They discovered that individuals who are associated with peers that are into software piracy learn and eventually fall into the same deviant behavior. Software piracy requires a skill set and knowledge that must be leant and these individuals learns them from their deviant peers.

Criticism of Routine Activity Theory

As indicated, RAT has been used to successfully explain and addressed a number of criminal issues but has also been criticized especially for its neglect of the

social aspect of committing crime, for example the social-economic and educational status of the offender. Also the general theory of crime postulate that individuals with low self-control are risk takers, shortsighted, impulsive, and like taking simple and easy task (Stylianou, 2002). According to the theory, these characteristics hinders the individual's ability to analyze the consequences of their behavior critically and so the offenders cannot be rational as RAT assume (Stylianou, 2002). In support, Jeffery (1993) argued that the theory only describes but does not explain a crime. Another reason the theory has been criticized for is the fact that the theory does not take into consideration the behavioral expectations associated with type of settings the victims engage their routine activities (Tewksbury & Mustaine, 2010).

Having discussed RAT and its application to cybercrime, I will want to synthesize elements of blockchain to justify the use of RAT as an underling theory to investigate blockchain application security strategies that IT security managers use. I will start by defining blockchain, detailing its components and its current use cases. I will then examine blockchain applications security issues and prior researches that have been done on the subject matter.

Blockchain

The blockchain system has many explanations and definitions. For example, Roberts and Karras (2019), defined blockchain system in the context of economics as a distributed ledger that ensures data integrity once the data is stored. Roberts and Karras elaborated that the data set could be a bank account details or a complete software that is stored in a ledger, also known as a block, and distributed across many computer nodes in the blockchain system. Knirsch et al. (2019), on the other hand, described blockchain technology as a trustless and fully decentralized peer-to-peer

storage system scattered across all participants known as nodes in the blockchain system. Another definition made by Hughes et al. (2019) is that blockchain system is a distributed public ledger made up of chains of blocks of the current transaction and previous transactions ever made in a blockchain system. Dai et al. (2017), on their part, see a blockchain as an underlying technical framework of a distributed network that allows users to maintain a reliable database in a decentralized manner collectively.

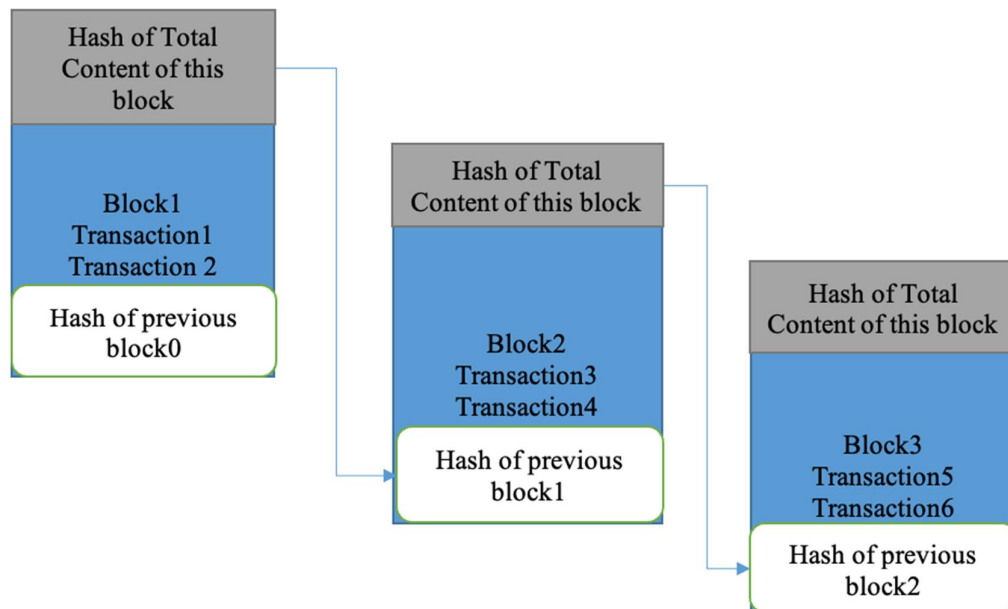
According to Wilczynski and Widlak (2019), there are three Blockchain architectures, namely Public, Private, and Permissioned. In public Blockchain architecture, any external entity can join, read, and modify the Blockchain; an example of such a Blockchain is Bitcoin and Litecoin systems. While in the permissioned Blockchain, some consortium members or a privileged user of the network decides which next node to have read or write access to the network. Private Blockchain, on the other hand, is owned by an entity (Company, Society, or a public entity), and it is not decentralized. Therefore it is the owner who decides on who participates in the chain (Wilczynski, & Widlak, 2019). Even though the Private architecture is centralized and may defeat a vital attribute of a blockchain, which is mostly decentralized, the private architecture uses cryptographic protocols of traditional blockchain to secure transactions in the network (Ismail, & Materwala, 2019).

For this paper, I will define the blockchain as a technology that enables immutability, decentralization and distributed digital assets. By putting them in cryptographically linked blocks of data in a way that only when there is a consensus among the participating nodes will a new block be added. The arrangement of the

blocks is, as shown in Figure 1. In the definitions of Blockchain technology, there are three main themes, namely cryptography hash, distributed, and consensus, that will be discussed further.

Figure 1

Blockchain Diagram



Hash Function

Each block is linked to the preceding block through a cryptography hash function to ensure immutability, as indicated in Figure 1, which makes it difficult for one to change the content of the block without affecting the preceding and the subsequent blocks. According to Raikwar et al. (2019), a hash function is a mathematical procedure that takes any size of data at the input and produces a fixed size at the output. For example, Secure Hashing Algorithm 256 (SHA256) used by the bitcoin blockchain produces an output of 256 bits for any number of bits as input

(Raikwar et al., 2019). Raikwar et al. articulated that there are several types of hash functions, but for cryptography, hash (H) must satisfy these conditions.

A collision resistance: which means to find two inputs x and y such that $H(x) = H(y)$ will be very difficult.

Preimage resistance: meaning for a given output z , it is hard to find an input x such that $H(x) = z$.

Second preimage resistance: that is for a given input x and output $z = H(x)$, it is hard to find a second input y such that $H(y) = z$.

Therefore, when the content of a block is hashed, any future change in it will produce a different hash, which will be detected. For a blockchain, the blocks are chained by including the hash of a block in the next block as indicated in Figure 1, and by so doing any change in any of the blocks content affects all the blocks preceding the block and subsequent blocks after. Roberts and Karras (2019) articulated that making a change in a blockchain will require a tremendous effort because it will require an astronomical amount of computing power and other resources. This property is one of the attributes that make the blockchain immutable.

Distributed Ledger

Blockchain data is also distributed across multiple nodes, meaning the chain is deployed on many nodes or computers that participate in the blockchain system.

Technically such an arrangement is referred to as a distributed ledger technology (DLT). Chowdhury et al. (2019) defined DLT as a ledger stored on nodes of peer-to-peer (P2P) network where each block (Ledger) is added upon agreement between all the nodes. In other words, DLT consensually spreads a shared and synchronized database across multiple sites, countries, or institutions without a central administrator

(Khan et al., 2017). According to Chowdhury et al., DLT has some unique properties that are appealing to several potential applications. These properties include the following.

- **Distributed consensus on the ledger state:** This property of the DLT is a critical one because it enables the participating parties to agree on the state of the ledger without involving any third party. This property opens up opportunities for the development of applications that requires transparent verification of transaction that has occurred on the ledger by all authorized entities.
- **Immutability and irreversibility of ledger state:** This means when a consensus is achieved with a large number of participants, it is practically impossible to reverse a transaction after a certain period. Most importantly, if the content of a block is a computer program, then once it has committed and executed, it becomes immutable and will deliver all instructions as designed. It is this property that is spearheading programs called smart contracts that delivers a response once agreed conditions are met just like a traditional legal contract.
- **Data (transaction) persistence:** DLT stores data in a distributed fashion, which ensures its persistence so long as there are participating nodes in the P2P network.
- **Data Origin:** In the DLT data storage process is done utilizing a mechanism called a transaction. This mechanism ensures that every transaction is digitally signed using public-key cryptography (PKI), which ensures the authenticity of the source. When this is combined with immutability and irreversibility properties of DLT, the data in the ledger becomes immune to repudiation.

- Distributed data control: This attribute of DLT ensures that data is retrieved or stored in the ledger is done in a distributed fashion, which removes a single point of failure in that operation.
- Accountability and transparency: In the DTL, the state of the ledger and all other activities among the participating nodes can be verified by any other authorized entity, which promotes transparency and accountability.

Consensus

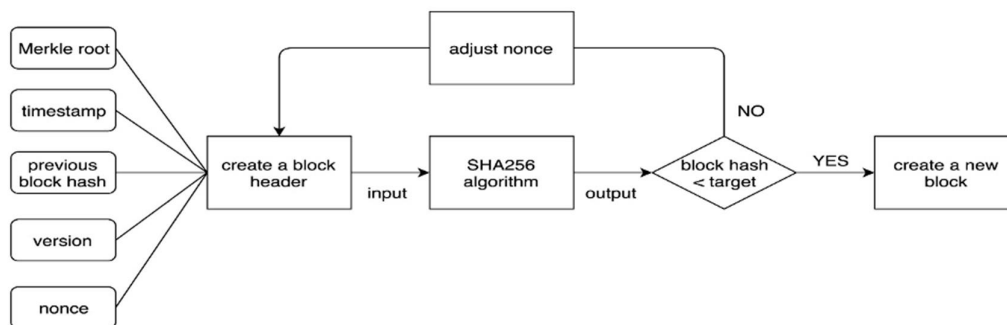
Consensus reaching is a critical and fundamental feature in a distributed ledger technology. As indicated above, it enables the participating nodes to agree on the state of the ledger. Wilczynski and Widlak (2019) articulated that adding a new block to a chain is done through a consensus protocol that all the participating nodes agree. According to Zhang and Lee (2019), there are two broad categories of consensus protocols; the probabilistic-finality consensus protocol and the absolute-finality consensus protocols. There are exist different types of consensus models within these categories for different blockchains. However, the main ones include proof of work (PoW), proof of stake (PoS), practical byzantine fault tolerance (PBFT) and round robin consensus models (Wilczynski & Widlak, 2019).

PoW, which uses a probabilistic-finality protocol, is used by bitcoin blockchain and enables the distributed nodes to come to a consensus by competition of computation powers that is open to all participating nodes on the blockchain network. Zhang and Lee (2019) explained that in the competition, the participating nodes need to solve a complicated mathematical cryptography puzzle. The first node that solves the puzzle is given the right to add a new block to the chain. Kumar et al. (2019) explicates that this process of competing and adding a new block to the chain

by participants in a blockchain network is known as mining in Bitcoin parlance. They are mining because the participants earn virtual coins in exchange for using their computational power to execute the task involved in the process. Figure 2 illustrates the workflow of the puzzle-solving process, as indicated by Zhang and Lee.

Figure 2

Proof of Work Process Flow



Note. From “Analysis of the main consensus protocols of Blockchain,” by S. Zhang and J. H. Lee, 2019, *ICT Express*, 6(2), (<https://doi.org/10.1016/j.ict.2019.08.001>).

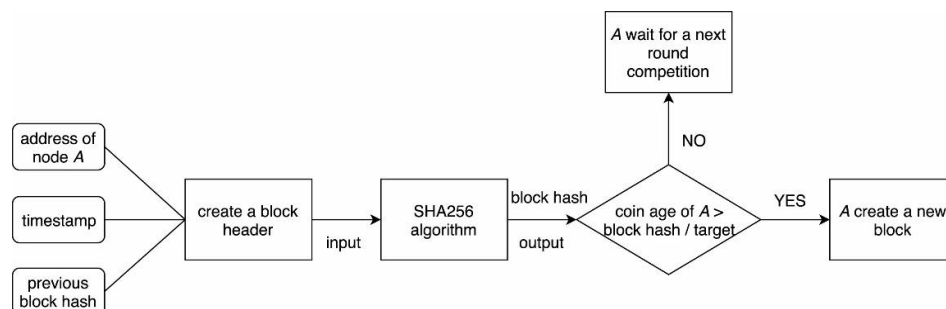
Copyright 2019 by Elsevier. Reused with permission (see Appendix B).

Zhang and Lee articulate that the PoW starts by grouping the block metadata such as Merkle root, timestamp, previous block hash, version (of the blockchain), and nonce to create the block header. The block header and transaction data are then hashed; the output of the hash function is then compared with a known target. If the output of the hash is less than or equal to the known target, then the node acting wins and is allowed to create a new block. However, if the hash output is higher than the known target, the node repeats the process by changing the nonce value for another try. The nonce is the only variable in the content of the block which miners have to find to get a solution to the mathematical puzzle, according to Kumar et al. (2019), it is only by using a brute force with a vast number of tries can the nonce be found.

PoW being a probabilistic-finality protocol have the advantage of fault-tolerant of 50%. Meaning to compromise the blockchain network, one would have to accumulate 50% or more of the computation power of the entire network, which will require a tremendous amount of resources as articulated by Zhang and Lee (2019). This assertion is reinforced by Panda et al. (2019), who argued that the probability of getting PoW is very low. Therefore, it will be challenging for any miner to control the blockchain network exclusively. In terms of scalability, Zhang and Lee argue that PoW scale very well even though transactions per second is low, there are offline interventions such as the Lightning network for bitcoin blockchain that improves the scalability. However, the most significant criticism and a disadvantage of the PoW is its high level of power consumption, Andoni et al. (2018) articulated that PoW consensus being used in bitcoin consumes about \$1 million worth of electricity in a day and by 2020 could guzzle as much as total Denmark electricity.

Figure 3

Proof of Stake Process Flow



Note. From “Analysis of the main consensus protocols of Blockchain,” by S. Zhang and J. H. Lee, 2019, *ICT Express*, 6(2), (<https://doi.org/10.1016/j.ict.2019.08.001>).

Copyright 2019 by Elsevier. Re-used with permission (see Appendix B).

An alternative to PoW is PoS, another Probabilistic-finality algorithm which is designed to cut down the consumption of electricity. In PoS, the appointment of a node to create a new block depends on its stake rather than its computational power. Andoni et al. (2018) explain that in PoS computation work is replaced with a random selection process where the chance of successful mining depends on the wealth of validators. Meaning the ability of a node to succeed in mining depends on its investment in the network such as coin ownerships and duration of the hold. Zhang and Lee (2019) further explicated that even though the hash puzzle has to be solved, the node does not need to change the nonce several times as is done in PoW consensus model but rather the key to solve the puzzle is the amount of stake (coins) in the network. This is so because the difficulty level of the puzzle is reduced for the node with a more significant stake in the network, which reduces the amount of energy used in the computation (Tang et al., 2019). The process flow is as indicated in Figure 2.

According to Sayeed and Marco-Gisbert (2019), the PoS algorithm begins with a random selection of a node to create the next block. During the selection process of a node, the details of the coins at stake and duration for which the coin has been kept is taken into consideration. The node selected then hash the contents of the block, and the output of the hash function is compared with a target value, as illustrated in Figure 3. If the target value is higher than the hash of the block, the node wins the competition and creates the new block. Otherwise, the node will have to wait for the next round of the competition.

$$\text{SHA256}(\text{timestamp, previous block hash, } \dots) < \text{Target} \times \text{Coins}.$$

PoS has the same 50% fault-tolerant as PoW, but it is more energy-efficient than PoW. Wang et al. (2020) stated that mining in the PoS algorithm does not waste electricity, and block confirmation is fast because PoS uses proof of equity and not physical calculations. However, one critical disadvantage of the PoS algorithm highlighted by Cao et al. (2019) is the fact that wealthy miners benefit more and may lead to oligopolies or near-monopolies. Another issue with PoS raised by Sayeed and Marco-Gisbert (2019) is that PoS also suffers from weak subjectivity, and its implementation process is very complex and challenging.

Another consensus, which will be discussed, is the practical byzantine fault tolerant (PBFT) model. This model falls within the Absolute Finality category and solves the challenges of the high computation requirement of PoW and oligopolies of PoS. Ismail and Materwala (2019) described PBFT as an algorithm that allows a blockchain network to reach consensus even if some of the nodes becomes faulty or malicious. According to Andoni et al. (2018), the network is secure as long as the faulty nodes are less than a third of the total nodes. Meaning the network tolerance increases as more nodes are added or joined to the system. Unlike PoW and PoS, PBFT is a permissioned blockchain; therefore, a central entity authorizes membership and so cannot be used as a public Blockchain (Feng et al., 2018).

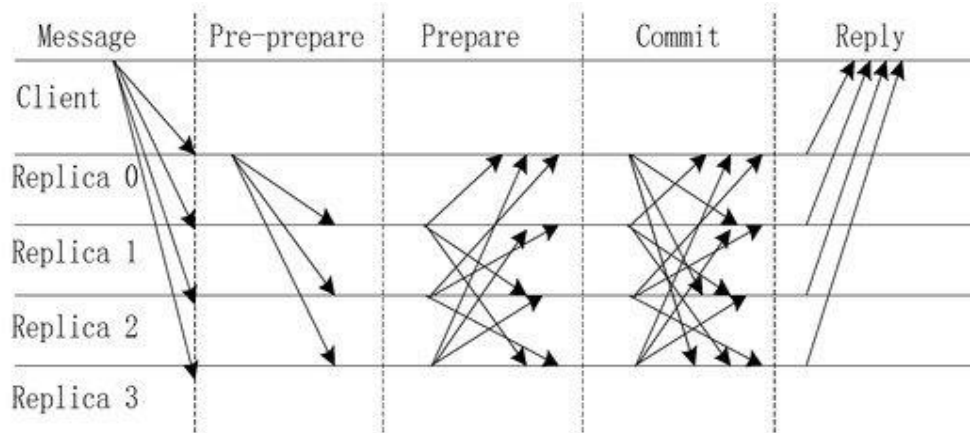
According to Ismail and Materwala (2019), generating a block in PBFT can be broken into four main phases, as illustrated below.

1. Client A sends a transaction request to a node appointed as the Leader Node.
2. The leader node collects all transactions and groups them into a block. The leader node then broadcasts the block to all back nodes that can be reached.

3. The backup nodes that receive the broadcast then verify each transaction in the block and create a block of verified transactions. The node then computes the hash of the block and broadcast to other nodes.
4. Each node waits for replies with the same hash from at least Two-Thirds of the total nodes in the network. If the replies received are the same, the block is then added to the node's ledger.

Figure 4

PBFT Stages



Note. From “Scalable Dynamic Multi-Agent Practical Byzantine Fault-Tolerant Consensus in Permissioned Blockchain,” by L. Feng, H. Zhang, Y. Chen and L. Lou, 2018, *Appl. Sci.* 8(10), p. 1919 (<https://doi.org/10.3390/app8101919>). Copyright 2018 by MDPI. Reused with permission (see Appendix B).

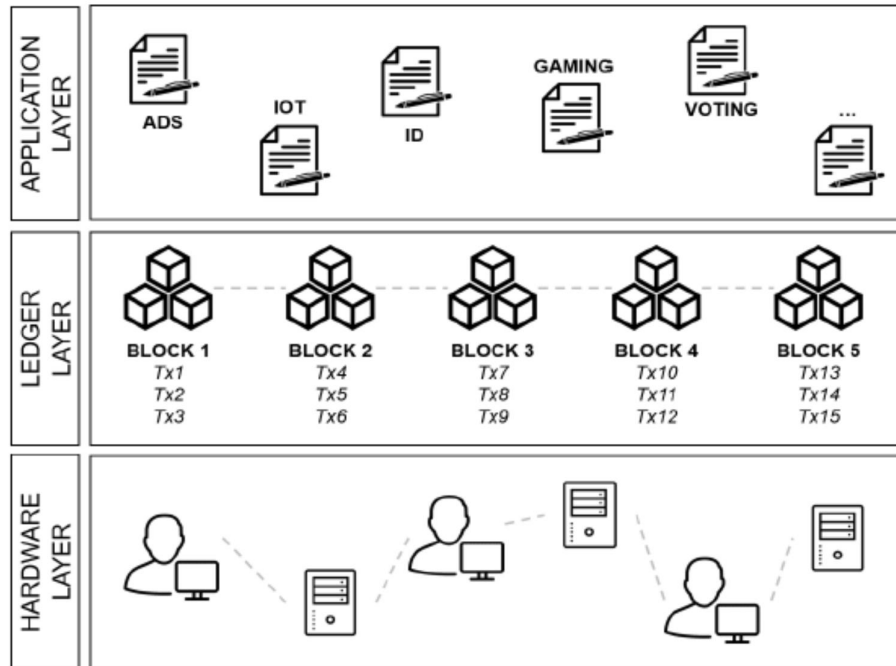
Even though PBFT solves the energy wastage and monopoly challenges of PoW and PoS, respectively, it has scalability shortcomings.

Gao et al. (2019) articulated that PBFT suffers from low scalability or low Byzantine fault rate. On PBFT scalability, Feng et al. (2018) demonstrated that to obtain consensus results, the nodes send $2n^2$ messages across the network, where n is

the number of nodes. Therefore, if the nodes reach 100, the total messages generated will be 20,000, which will burden the communication network.

Blockchain Information Technology Architecture

De Rossi et al. (2019) postulated that to appreciate the business and organizational impact of blockchain, one must understand its IT architecture. De Rossi et al. proposed three-layer architecture made up of a Top layer, Middle layer, and the Bottom layer. The top layer represents the application layer, which provides the interface through which organizations derive services from the blockchain. While the middle layer is the blockchain ledger that supports the application layer; the bottom layer consists of all the hardware representing the network and nodes. Figure 5 illustrates the layers and functions.

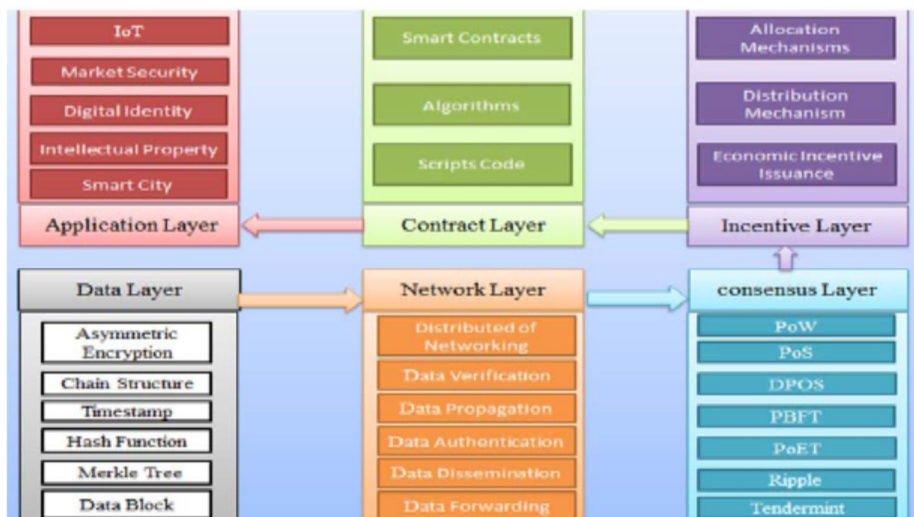
Figure 5*Three-Layer Blockchain Architecture*

Note. From "Towards a Comprehensive Blockchain Architecture Continuum," by L.

M. De Rossi, N. Abbate-marco and S. Gianluca, 2019, ScholarSpace

(<https://doi.org/10.24251/HICSS.2019.557>). Copyright by Hawaii University (HU).

Reused with permission (see Appendix B).

Figure 6*Six-Layer Blockchain Architecture*

Note. From "Blockchain Technology: Characteristics, Security and Privacy: Issues and Solutions," by M. B. Yassein, F. Shatnawi, S. Rawashdeh and W. Mardin, 2019, IEEE (<https://doi.org/10.1109/AICCSA47632.2019.9035216>). Copyright 2019 by IEEE. Reused with permission (see Appendix B).

Yassein et al. (2019), on the other hand, argued that the Blockchain architecture could have several layers depending on the type of application and requirements of the users. However, Yassein et al. proposed a general six-layer architecture illustrated in Figure 6 that could satisfy most application requirements. In Yassein et al. six-layer architecture, the bottom layer is the data layer followed by the network, consensus, incentive, contract, and application layers. The function of these layers is as follows.

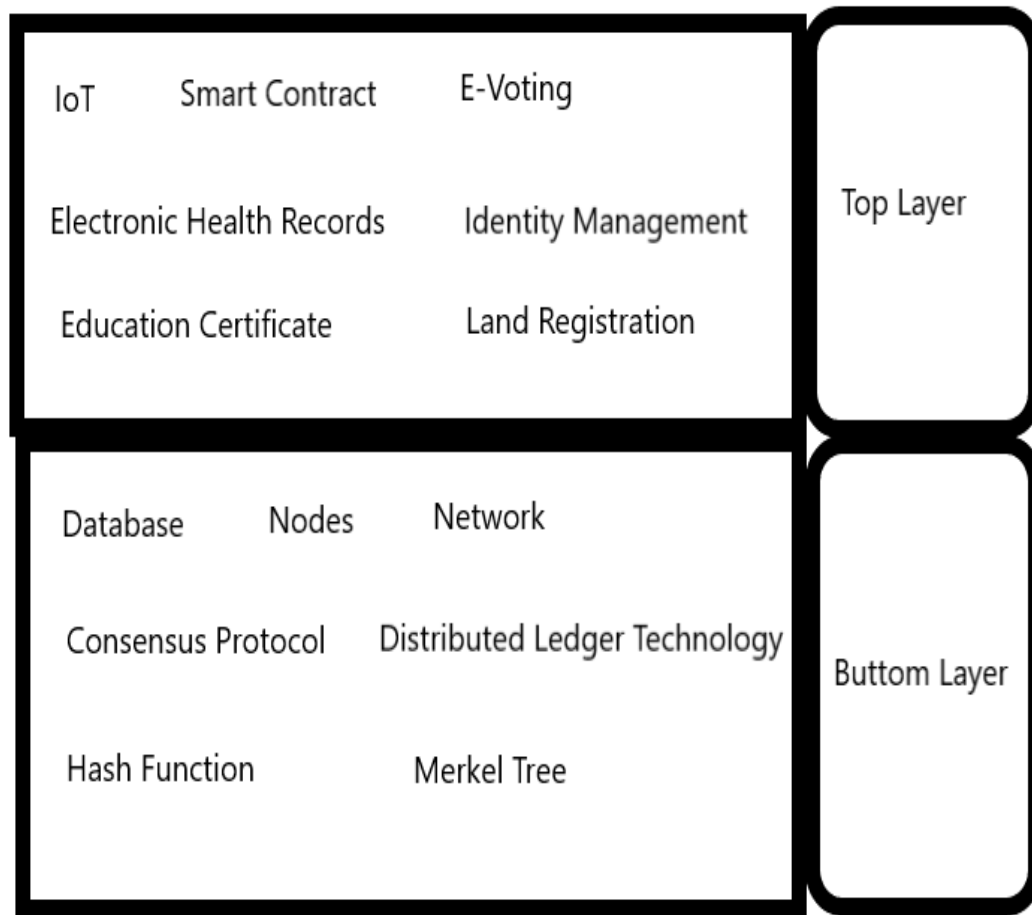
- Data layer: this layer performs the hashing function, asymmetric encrypting, timestamping, saving of data, and establishing new blocks.

- Network layer: the layer is responsible for data propagation, data verification, distributed networking, data authentication, data dissemination, and data forwarding.
- Consensus layer: Blockchain depends on consensus algorithm to achieve its decentralization nature; this layer provides that functions.
- Incentive layer: this layer provides the necessary economic motivation to ensure participation in a blockchain network. Without it, the blockchain will cease to grow and eventually collapse.
- Contract layer: the contract layer is fundamental to blockchain smart contracts applications. It provides the necessary environment for the program code that executes the contract to run.
- Application layer: The topmost layer is the application layer, where users on the blockchain interfaces with the chain. Computer scientists and engineers have developed several blockchain applications, which include IoT, digital identity, cryptocurrency, smart contract, electronic health records, and e-voting.

From both discussions, one could see two distinct layers, the application layer, and the infrastructure layer. Therefore, in the lens of IT, this paper will adopt the two-layer IT architecture approach, as shown in Figure 7. The top layer will represent all blockchain applications, and the bottom layer will comprise of the nodes, network, ledger, consensus protocols, and DLT

Figure 7

Two-Layer Generic Blockchain Information Technology Architecture



Blockchain Applications

Blockchain, originally designed for the trustless cryptocurrency, is seen by many as a great technology to provide an alternative solution for existing business problems and can disrupt matured industries. A study by Jaoude and Saade (2019) on the current trend of blockchain applications in both industries and academia identified five major application domains. These application domains include the internet of things (IoT), energy, finance, healthcare, and government. According to Jaoude and

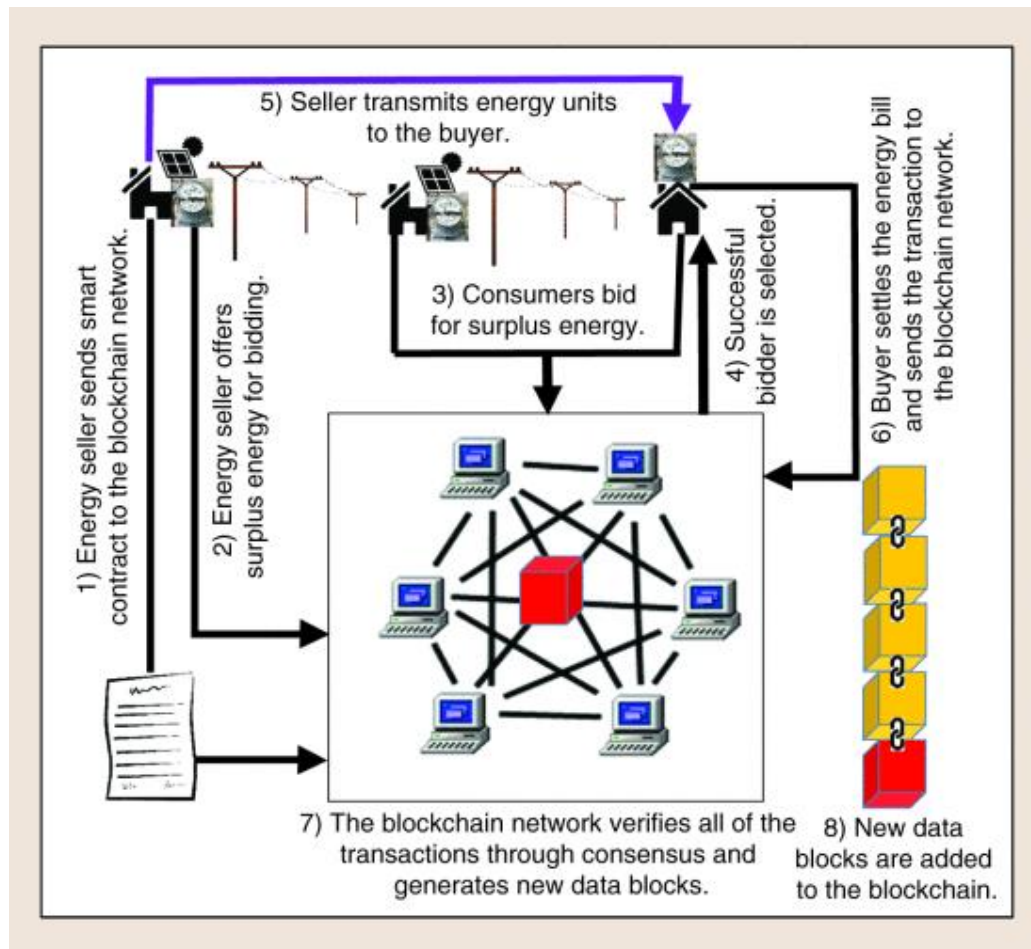
Saade, these application areas account for about 53% of the 151 blockchain related articles reviewed. Other areas of application domains postulated by Monrat et al. (2019) are identity management and education. From the research, one could see strong growth in other use of blockchain aside its initial use in cryptocurrency since 2008. The following paragraphs will illustrate the details of the major application areas.

IoTs are internet-enabled gadgets such as cameras, smart-lights, smart-bins, and a whole host of others being used in the smart environment, including homes and industries. Reyna et al. (2018) describe IoT as a set of technologies involving Wireless Sensor Networks (WSN) to Radio Frequency Identification (RFID) that have the ability to sense, actuate and communicate over the internet and is empowering cities, homes, and factories into smart entities. According to Sivanathan et al. (2020), over 10 Billion IoT devices are currently connected in homes, buildings, enterprises, campuses, and cities. However, Wang et al. (2019) articulated that inadequate data security and trust are limiting IoTs adoption and stressed that blockchain has the potential to address these IoT data security concerns. Reyna et al. acknowledged the enormous potential blockchain would have on IoT, indicating that blockchain technology will enrich IoT by providing trusted sharing service, information reliability, data immutability, and generally increasing the IoT security. These interventions by blockchain technology will, therefore, leverage IoT applications to provide the necessary security that has been lacking in IoT technology, which in recent times, is dominating all aspects of society.

The application of blockchain in the Energy sector has also seen consistent activity in academia and industries. The energy domain ranked second to IoT in terms

of blockchain application research, according to the study by Jaoude and Saade (2019). One of the primary uses of blockchain application in the energy domain is in the area of the microgrid. The microgrid is localized integrated sources and loads of electric power, which is managed to enhance efficiency and reliability (Monrat et al., 2019). Zhang et al. (2020) explained that microgrid energy sources are made up of independent coordinated distributed renewable energy, local co-generators, and energy storage devices owned by different organizations and power providers. According to Monrat et al., one of the main advantages of the microgrid is the ability to sell excess energy into the primary grid. Due to the decentralized nature of microgrid, Monrat et al. argued that blockchain application will be a fit for facilitating, recording, and validating the buying/selling microgrid energy transactions. Di Silvestre et al. (2019) also justified the use of blockchain in the energy domain by arguing that the microgrid energy market has an environment that is suited for blockchain application. Di Silvesre et al. explained that it is a multiparty environment that does not need a trusted authority but needs transparency and immutability, which blockchain technology can offer. Figure 8 illustrates a typical flow of Blockchain application implementation in a microgrid.

Figure 8

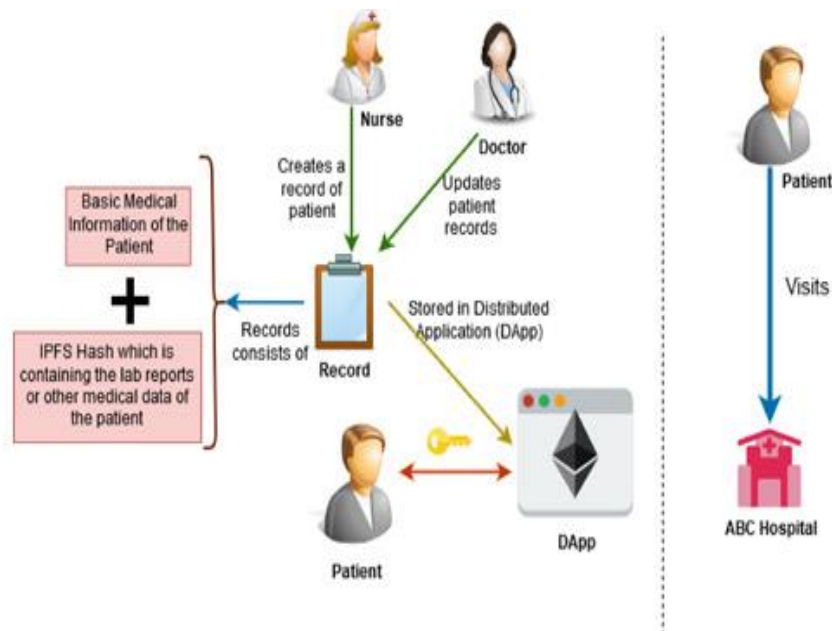
Blockchain Application Implementation in a Microgrid

Note. From “Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges, and Solutions,” by N. Ul Hassan, C. Yuen, and D. Niyato, 2019, IEEE (<https://doi.org/10.1109/MIE.2019.2940335>). Copyright 2019 by IEEE. Reused with permission (see Appendix B).

The health domain is one of the promising areas for blockchain application, especially in the storage and management of electronic health records (EHRs). According to Shahnaz et al. (2019), existing electronic medical records (EMRs) improved paper-based medical records management by adding some level of security

and better user experience. However, the existing EMR faced some challenges such as data breaches, lack of data integrity, user ownership, and interoperability. Tang et al. (2019) articulated that current EHR hosted in the cloud, even though solved the interoperability challenges, the problem of centralization and user ownership still existed because when the cloud server is compromised, privacy and data integrity become an issue. For example, when there is a dispute between a patient and the hospital, the hospital authorities could connive with the cloud provider to temper with the data.

Both Tang et al. and Shahnaz et al. postulated that Blockchain could be a panacea to the existing problems of the traditional EHR due to its use of cryptography and its distributed database. Mertz (2018), on the other hand, reasoned that Blockchain is what can take EHR from where it is to where it is needed and empower the patient to take control of his/her records. A study and a prototype application by Quaini et al. (2018) proved that Blockchain could be used to solve the interoperability problem exhibited by current EHR systems. The prototype confirmed the effectiveness of Blockchain for distributed EHR integration by allowing another healthcare institution to access an EHR previously added by a different health institution.

Figure 9*Typical Use of Blockchain for a Hospital*

Note. From “Using Blockchain for Electronic Health Records,” by A. Shahnaz, U. Qamar, and A. Khalid, 2019, IEEE (<https://doi.org/10.1109/ACCESS.2019.2946373>). Copyright 2019 by IEEE. Reused with permission (see Appendix B).

In Figure 9, a typical blockchain application for a hospital is illustrated. The process, as illustrated by Shahnaz et al., goes like this: a patient goes to a hospital where a nurse creates a record of the patient, which is then stored in a distributed application (DApp). The DApp is a blockchain based EHR system with all the characteristics of a Blockchain, as explained in the paragraphs above. Once the record is stored, it becomes available to only doctors and patients through their cryptographic keys.

Governments have shown keen interest in blockchain technology applications; several countries have explored the use of technology to make governance more efficient and transparent. Reddick et al. (2019) articulated that as of 2018, forty out of

213 countries had initiated over 200 blockchain related projects. Olnes et al. (2017) stressed the potential of blockchain in e-governance due to blockchain's ability to enable reduced costs and complexity, shared trusted processes, improved traceability of audit trails and ensured trusted recordkeeping. According to Razzaq et al. (2019), UK government is now using blockchain as a service, Estonia government is using the technology for providing public notary services for the citizens, and the Danish political parties use a blockchain voting application for their voting. Other prominent areas using blockchain application in government sectors include digital payments/currency, land registration, identity management, and supply chain management (Reddick et al., 2019). Figure 10 below indicates countries' implementation levels of the top ten blockchain applications.

Figure 10

Blockchain in Public Sector, March 2017



Note. From “An Overview of Blockchain Applications and Attacks,” by R. R.

Vokerla, B. Shanmugam, S. Azam, A. Karim, F. D. Boer, M. Jonkman, and F. Faisal, 2019, IEEE (<https://doi.org/10.1109/ViTECoN.2019.8899450>). Copyright 2019 by IEEE. Reused with permission (see Appendix B).

Blockchain Application Security Concerns

Blockchain at the core is a database system with unique features, so like a traditional database, it contains digital assets and, therefore, prone to the same security issues that confront these databases. Besides, blockchain has some peculiar security concerns that are unique to its underlining technologies. Moubarak et al. (2018) argued that despite DLT’s advantages and huge potential in several applications, it has quite many flaws that threaten security and privacy. Averin and

Averina (2019), in their presentation, reported that current interest in blockchain is not only about its application or investment but also about unprecedented attacks on blockchain, especially cryptocurrency blockchains. Table 1 below lists the recent attacks on existing blockchains and the cost of the attack.

Table 1

Blockchain Attacks Over the Years and Estimated Cost of Cryptocurrency Stolen

Blockchain	Year of attack	Lost
Bitcoin	2014	\$473,000,000
Mt.Gox	2015	\$5,100,000
Shapeshift	2016	\$130,000
Gatecoin	2016	\$2,000,000
DAO	2016	\$50,000,000
Steemit	2016	\$85,000
Bitfinex	2016	\$72,000,000
CoinDash	2017	\$7,000,000
Parity	2017	\$32,000,000
Veritaseum	2017	\$8,000,000
Enigma	2017	\$500,000
Blockchian.io	2017	\$50,000,000
TetherThere	2017	\$30,900,000

Note. Adapted from "Review of Blockchain Technology Vulnerabilities and

Blockchain-System Attacks," by A. Averin and O. Averina, 2019, IEEE

(<https://doi.org/10.1109/FarEastCon.2019.8934243>). Copyright 2019 by IEEE.

Reproduced with permission (see Appendix B).

A survey by Li et al. (2020) identified nine security issues in blockchain and Moubarak et al. (2018) illustrated seven attack scenarios on DLT. Vokerla et al. discussed six different attacks and variations on blockchain, indicating related applications that are prone to these vulnerabilities as shown in Figure 11. The security concerns raised by the authors, suggests two categories of vulnerabilities that confront blockchain applications. These categories are blockchain specific exposures and

Traditional security challenges as indicated in Table 2 but the main ones that pertain to blockchain technology flaws will be discussed in this paper. The weaknesses include a 51% vulnerability Consensus mechanism, Private Key security encryption scheme, and vulnerabilities in the Smart Contract Program that are detailed in the subsequent paragraphs.

Figure 11

Blockchain Application Vulnerabilities

	IoT	Government Services	Smart Contracts	Identity	Financials
Attacks					
Double Spending	✗	✓	✓	✗	✓
Finney	✗	✓	✓	✗	✓
Brute Force	✗	✓	✓	✗	✓
Vector 76	✗	✓	✗	✗	✓
Selfish Mining	✓	✓	✓	✓	✓
Block Withholding	✓	✓	✓	✓	✓
Bribery	✓	✓	✓	✗	✓
Sybil	✗	✓	✓	✗	✓
Eclipse	✗	✓	✓	✗	✓
Tampering	✗	✗	✗	✗	✗

Note. From "An Overview of Blockchain Applications and Attacks," by R. R.

Vokerla, B. Shanmugam, S. Azam, A. Karim, F. D. Boer, M. Jonkman, and F. Faisal, 2019, IEEE (<https://doi.org/10.1109/ViTECoN.2019.8899450>). Copyright 2019 by IEEE. Reused with Permission (see Appendix B).

Table 2*Blockchain Categories of Security Concerns and Related Vulnerability*

Security concern category	Types of vulnerability
Blockchain specific security concern	<ol style="list-style-type: none"> 1. 51% attack vulnerability 2. Private key management 3. Smart contract flaws 4. Sybil attack 5. Anonymity 6. Selfish mining 7. Spam attacks 8. Timejacking 9. Forks
Traditional security concern	<ol style="list-style-type: none"> 1. DDos attacks 2. Phishing attacks 3. BGP hijacking attack

The classic 51% attack, also known as the Majority attack, is one of the main threats to blockchain (Saad et al., 2020). This 51% attack is a result of the way some blockchain consensus mechanism is designed to work. As explained by Li et al. (2020), blockchain depends on a distributed consensus mechanism to establish a shared trust. Therefore, an entity with 51% of the hashing power of the entire blockchain can compromise the network. This attack is more pronounced in blockchain using PoW and PoS consensus algorithm. However, with the PoS algorithm, the attacker must gain 50% of the stake (coins) in the network instead of hashing power. Lin and Liao (2017) articulated that the Majority attack can empower the attacker to modify the blockchain data to result in a double-spending attack; it could also stop the block verifying transaction process and mining of any available block. Averin and Averina (2019), in their review of blockchain vulnerability, shared several recent 51% attacks on known blockchains such as Electroneum, BitcoinGold, Litecoin, Zencash, Bitcoin Private, Vertcoin, Callisto, Monaco, and Ethereum. An

indication that the 51% attack has moved from the theoretical realm to practical attacks.

Much research has been done to mitigate the 51% blockchain attack. For instance, Anita and Vijayalakshmi (2019) indicated a solution by PirlGuard Protocol implemented in Ethereum. As explained by Sayeed and Marco-Gisbert (2019), the PirlGuard modifies the consensus protocol to punish any peer node that tries to take over the network by enforcing the node to mine a specified amount of blocks. Another mitigation method suggested by Sayeed and Marco-Gisbert is the delayed PoW (dPoW), which is offered by Komodo. The Komodo strategy prevents attackers from changing and erasing transactions by replicating the hashes of the blocks onto the Bitcoin chain, which is immune to 51% attack due to its current size (Anita & Vijayalakshmi, 2019).

Management of cryptographic private keys is another threat to blockchain applications; the existing blockchain application uses private keys to confirm a user's identity to complete a transaction. Dai et al. (2017) argued that unlike traditional public key management, which is centrally controlled, blockchain users are responsible for their private keys, and losing it will mean loss of digital assets. Additionally, the cryptographic key algorithm can have unknown vulnerabilities that could be used in the future to compromise the blockchain. For example, a vulnerability discovered in Elliptic Curve Digital Signature Algorithm (ECDSA) allows an attacker to recover a user's private keys because the system does not generate enough randomness during the key producing process (Li et al., 2020).

Smart contract (SC) are programs deployed in a decentralized blockchain and are executed when it receives a triggered instruction to automatically honor the

agreement like a traditional contract without a third party (Sayeed et al., 2020). When the SC is deployed in the blockchain, it cannot be changed or updated due to the immutability properties of blockchain. However, programs running in blockchain SC, like any other program, could have security vulnerability caused by program defects. Li et al. (2018) identified six vulnerabilities caused by the SC source code, three vulnerabilities caused by the EVM bytecode, and another three caused by the blockchain mechanism, all in the Ethereum blockchain. According to Destefanis et al. (2018), the Ethereum chain suffered a vulnerability labeled as Parity Wallet hack, which caused over \$160 million to be frozen.

Moubarak et al. (2018) suggested that mitigation of SC flaws should include an auditing mechanism to review and check SC functions to eliminate programming bugs before deployment and adding an induced validity date of the SC after which it will expire. Sayeed et al. (2020) proposed ten security analysis tools that could be used to audit and identify flaws in SC. These software tools include Slither, MythX, Mythril, Manticore, Smartcheck, Echidna, Oyente, Vandal, and Zeus. Each of these tools has unique properties in identifying the flaws in SC to enable the programmer to rectify them before deployment.

Blockchain Security Strategy

This DIT applied study is about security strategies for blockchain application, so I sought existing research on the topic to investigate if there are gaps that needed to be the focus on in this paper. However, a search on the various academic libraries and search engines produced very few research papers directly related to security strategies or security framework for blockchain application. This observation was reiterated by Shrivastava et al. (2020), who reviewed several academic research on the

same topic and came to a similar conclusion. However, seven of the academic papers reviewed by the team showed some limited details of various security concerns scattered across different areas of the blockchain system without any comprehensive security framework or strategy.

A paper by Wilczynski and Widlak (2019), on the other hand, suggested a simple strategy for blockchain security. In the paper, they articulated that security in a blockchain is mainly the protection of transaction and data related information against internal and external attacks. Because of that, Wilczynski and Widlak suggested the following four safety procedures as a security strategy against attacks on blockchain application.

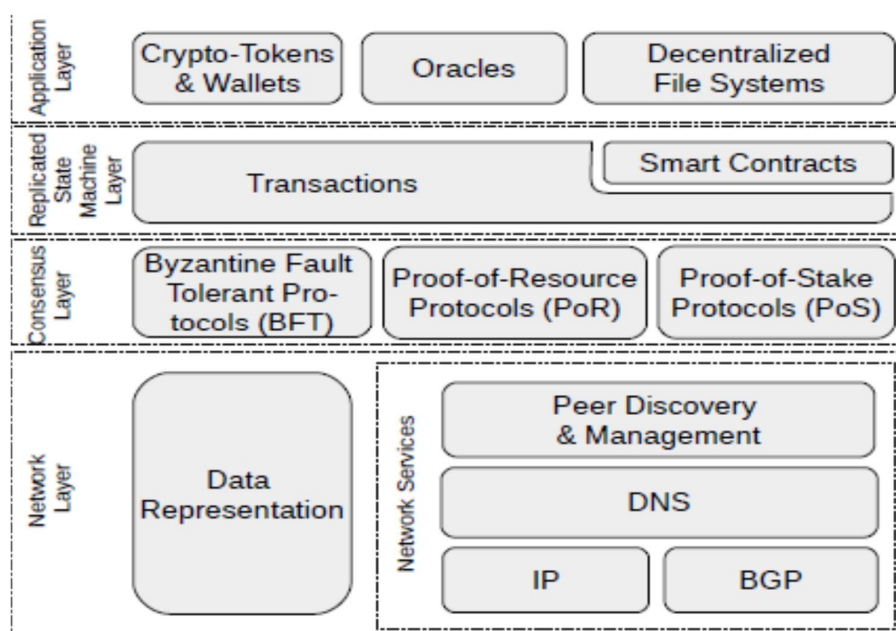
- Penetration defense: Using many data protection measures with the view that multiple layers are more effective than a single layer of protection.
- Minimum privilege: A conscious effort is made to limit access to data as minimum as possible.
- Manage vulnerabilities: A continues evaluating and checking of security vulnerabilities so as to patch them early enough before an attack,
- Manage risks: Risks in the environment are identified and evaluated in other that appropriate control measures can be put in place.
- Manage patches: Program developers critically analyze the application source code for faulty parts and bugs before deployment.

Homoliak et al. (2019), on their part, attempted a more detailed strategy by developing security architecture for blockchain application. Homoliak et al. proposed a four-layer architecture, made up of network layer, consensus layer, replicated state machine layer (RSM), and application layer. The paper then used Threat-Risk

ISO/IEC 15408 template to capture the security aspect of the blockchain through layered architectures shown in Figure 12 and Figure 13. By using the layered security architecture, the authors identified the risks at each layer and its related mitigation methods to focus on.

Figure 12

Stacked Model of Reference Architecture

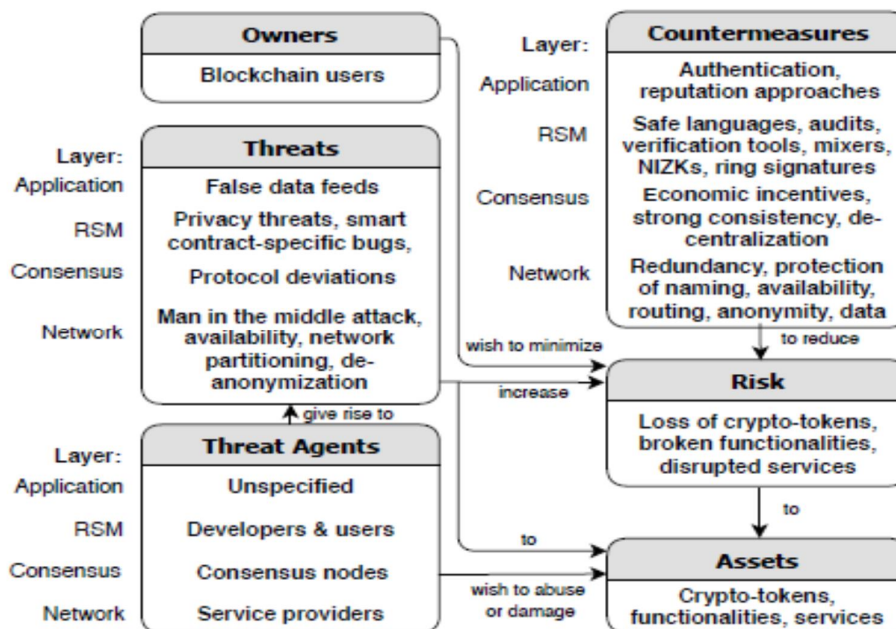


Note. From "A Security Reference Architecture for Blockchains," by I. Homoliak, S.

Venugopalan, Q. Hum and P. Szalachowski, 2019,

(<https://doi.org/10.1109/Blockchain.2019.00060>). Copyright 2019 by IEEE. Reused

with permission (see Appendix B).

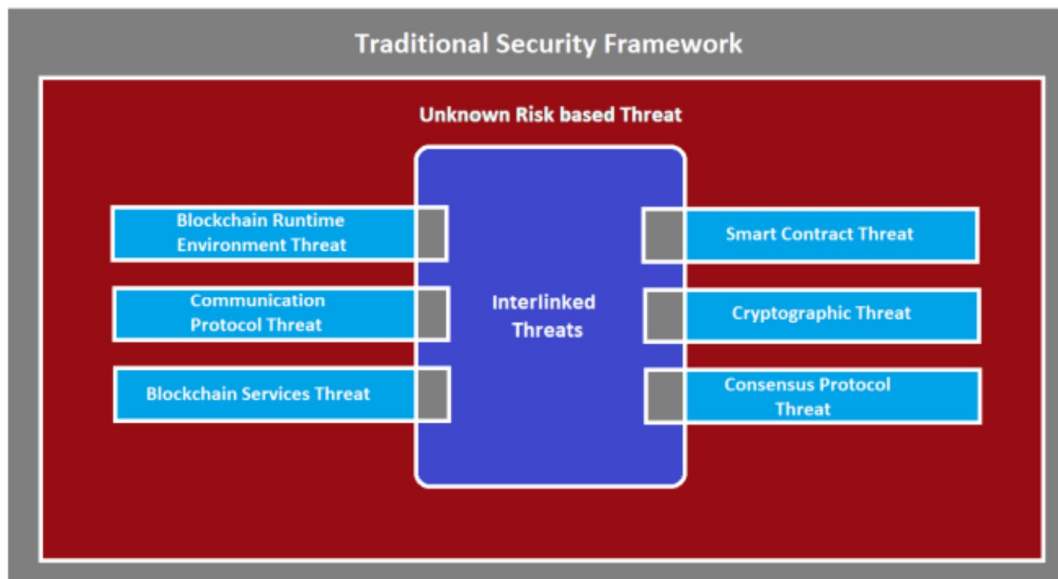
Figure 13*Threat–Risk Assessment Model of Reference Architecture*

Note. From “A Security Reference Architecture for Blockchains,” by I. Homoliak, S. Venugopalan, Q. Hum and P. Szalachowski, 2019, (<https://doi.org/10.1109/Blockchain.2019.00060>). Copyright 2019 by IEEE. Reused with permission (see Appendix B).

Homoliak et al. paper explains that at the network layer threats includes man-in-the-middle (MITM) attacks, network partitioning, de-anonymization, and availability attacks. Countermeasures suggested against these threats comprise of protection of availability, naming, routing, anonymity, and data. At the consensus layer, malicious nodes may want to alter the outcome of the consensus protocol by not sticking to the rules. The mitigation against this attack includes economic incentives, strong consistency, and decentralization. Vulnerability on the RSM layer includes threats agents such as developers who intentionally or accidentally introduce semantic bugs in a smart contract. Protection against such includes safe languages,

static/dynamic verification, and audits. Finally, at the application level, threats are unknown since any user at that layer could be a threat. Threats at that level are mainly false data feeds, which can be mitigated by authentication or reputation systems.

Shrivastava et al., (2020) deepened the security architecture by categorizing the blockchain security into traditional and blockchain specific security concerns as indicated in Figure 14. Their approach differs from that of Homoliak et al. (2019), which had no separation between traditional and blockchain security issues. Shrivastava et al. argued that traditional security framework alone cannot address blockchain security threats and therefore proposed a framework that takes into consideration both the traditional security and blockchain security threats. The team reasoned that the combination was necessary because the blockchain platform uses traditional computing resources. In the suggested framework, two additional categories labeled Interlinked threats and Unknown Risk-based threats, were added. The Interlink threats are a combination of blockchain known threats, while the Unknown Risk-based threats are blockchain security issues that are yet to be discovered but are capable of affecting any blockchain platform component. Shrivastava et al. explained that the framework layers allow blockchain security issues at each layer as well as the underlining IT infrastructure to be identified so that mitigating strategies can be adopted to address the issues. For example, at the traditional security layer, existing accepted security frameworks such as ISO/IEC 27000 series or NIST cybersecurity framework could be used and at the unknown risk-based threats layer NIST's risk management framework (RMF) along with cybersecurity framework (CSF) and ISO/IEC 27001:2013 can also be used (Shrivastava et al., 2020).

Figure 14*Proposed Hybrid Blockchain Security Framework*

Note. From "Hybrid Security Framework for Blockchain Platforms," by M. K.

Shrivastava, T. Yeboah and S. S. Brunda, 2020,

(<https://doi.org/10.1109/ICPC2T48082.2020.9071477>). Copyright 2020 IEEE. Reused

with permission (see Appendix B).

Transition and Summary

In this section, Routine Activity Theory (RAT) was discussed as the conceptual framework underlying this research. Cohen and Felson originally developed RAT to explain the dynamics of criminal events, patterns in criminal victimization, and predictions of crime in a terrestrial environment. The RAT theory postulates that crime occurs when these three elements (motivated offender, valuable target, and absence of capable guardian) coincide in time and space. The theory concludes that managing crime involves controlling these three elements of the RAT. The equivalents of these RAT elements in cyberspace identified in the discussion

justified the applicability of RAT to cybercrime, which relates to the topic of this research paper. This section reviewed blockchain technologies, applications, and security issues against user digital assets and transactions in the blockchain cyberspace. Most importantly, the section reviewed existing security strategies that identified gaps that were focused on when answering the study's research question. The remaining sections will address the data gathering and analysis methods used in answering the research question in an ethical and quality manner.

Section 2: The Project

Purpose Statement

The purpose of this qualitative, multiple case study was to explore strategies IT security managers use in deploying blockchain applications securely. The population consisted of IT security managers from blockchain application companies in Ghana, the United States, and Europe with experience in security and blockchain applications. The findings from this study may benefit information security practice by improving the understanding of the nature of blockchain and security implementation requirements. The implications for positive social change include the potential to protect users' private digital assets and data in the block chain.

Role of the Researcher

I have been in the computer industry since 1996. I started as a data communication engineer and progressed as a network administrator, and I am currently the ICT deputy director of my company. My job role covers ICT security policy design and implementation. Over the years, I have gained experience in computer security matters and have implemented several IT security solutions for many organizations. However, I have not had the opportunity to work on blockchain systems and their protection. I became interested in blockchain first as a financial investor in bitcoins and subsequently bought a peer-to-peer bitcoin exchange website, which I intended to operate.

The various breaches of cryptocurrency exchanges resulting in the loss of vast sums of cryptocurrencies (Bischooping, 2018) caught my attention. Therefore, I decided to research bitcoins and realized there was more to the technology than cryptocurrencies. My interest then grew from financial investment in cryptocurrency

to academic curiosity into the technology and security implications. These motivations played a significant role in selecting a qualitative research topic that relates to security strategies for blockchain applications. I did not have any working relationship with the participants in this study. Nevertheless, some are people I contacted through social media on LinkedIn or who I met at a seminar or through other contacts.

As a qualitative research, the researcher's potential bias can be high. Sanjari et al. (2014) articulated that in a qualitative study, the researcher is personally involved in various stages of the research, which puts the researcher in an awkward ethical position for bias. Mackieson et al. (2019), argued that all research methods in practice may have some biases due to explicit or implicit value assumptions, which may be evident in one or multiple parts of the study. For example, value assumptions can be found in the framing of the research question, the choice of a theoretical model, the selection of the subjects or sources of data, and the nature of questions asked during interviews. Due to such possibilities, Karagiozis (2018) suggested that the researcher should acknowledge potential biases by his role and critically analyze them to give credibility to the research. Given these potential biases, the study adopted these mitigation measures to reduce bias.

As indicated by Johnson et al. (2020), data collection is a potential source of researcher bias. For this study, an interview was the main instrument for data collection, which was prone to researcher bias as Birt et al. (2016) articulated. Johnson et al. (2020) suggested that interviews should be recorded and transcribed verbatim before coding and analysis to reduce bias and improve trustworthiness. I acknowledged that my background in IT and my particular interest in the subject

matter could trigger confirmation bias. Therefore, I used member checking to avoid misinterpreting of the participants' answers. Member checking is used to validate, verify, or assess the trustworthiness of qualitative results (Birt et al., 2016). I also used data triangulation to improve the validity of the study. Farquhar et al. (2020) recommended that triangulation in a case study offers validity through a convergence of findings, sources, or methods. Thus, I used multiple triangulation methods involving more than one data collections method. For this study, I collected data through interviews and review of company documents related to IT security. These company documents, such as IT security policies, were requested from participants before interviews.

To ensure strictly ethical research, I prioritized the recommendations of the Belmont report: respect for persons, beneficence, and justice (Adashi et al., 2018). The recommendations were implemented by ensuring that each participant who agreed to participate did so freely with full consent and without coercion. In addition, participants were told they could withdraw from the interview at any point. The risks associated with the study were analyzed to ensure they far outweighed any risk to participants. The information on the analysis of the risks was communicated to the subjects to enable them to decide whether to participate. Justice is served by ensuring that the selection of interviewees is purely based on the ability to answer the research question and the burden of the interview process is shared equally by all participants (Kamp et al., 2019).

Participants

The study participants were IT security managers with at least 3 years of experience in security strategies used in blockchain application deployment. Because

the study is a multiple case study, I selected participants from different organizations in different geographical areas. I also ensured diversity in knowledge by interviewing IT security professionals in both academia and industry domains. Participants' experiences were not restricted to blockchain-specific security, but also to general IT security. As Reybold et al. (2012) articulated that purposeful selection in qualitative research is necessary because it is the most significant difference between qualitative and quantitative methods. Reybold et al. explained that information-rich cases and in-depth understanding could not be obtained through random sampling. Therefore, the purposeful selection strategy allows access to the right knowledge that fits the purpose of the study, the resources available, the constraints being faced, and the correct type of interview questions. Arsel (2017) suggested that a researcher should know their participants by purposely seeking specific individuals based on the topic of inquiry. Such a selection is vital and will inform the vocabulary and type of questions used in the interview (Arsel, 2017). Cleary et al. (2014) pointed out that participants' selection should be based on specific purposes related to the research question, and therefore, a knowledgeable interviewee on the topic under study is critical.

To establish contact with participants, I used my network established through social media such as LinkedIn and conferences attended on the subject matter. Many researchers have successfully used social media to recruit participants. Sikkens et al. (2017) used Facebook to recruit participants who are hard to find offline in research on youth and radicalization. In research on youth e-cigarette use, Keamy-Minor et al. (2019) used social media to recruit participants. Barratt et al. (2015) articulated the usefulness of internet-mediated participants and recommended it for sensitive topics.

I developed a working relationship by making initial contact through email or phone calls to as many potential participants as possible. Those interested were shortlisted and categorized by the qualities I had defined for my participants. I acknowledged the fact that I may face challenges in establishing this relationship. Recruiting research participants is challenged by the time constraint of the participant due to work overload and may put a higher priority on work than the interview (Daly et al., 2019). Khatamian Far (2018) also amplified the recruitment challenge and pointed out that failure in engaging participants can lead to severe threats to the validity and quality of the research. In mitigating these recruitment challenges, I took a cue from Mandava and Millum (2013) and sought to understand the factors that affect potential participants' decisions to help design recruitment strategies that would encourage participants to join. Mandava and Millum suggested use of persuasion and offers as strategies grounded in respect of autonomy but avoid manipulation and coercion.

Research Method and Design

Research Method

I adopted a qualitative research method for my study. In this section, I explained the choice and why I did not choose quantitative and mixed methods. From a philosophical point of view, a qualitative study is seen as interpretive research, which assumes there is no single or observable reality but multiple realities or interpretations of a single event (Nicholls, 2009). Also, interpretivism or constructivism means that researchers do not find knowledge but construct it or develop subjective meaning from experiences (Singh, 2015). Merriam and Tisdell (2016) explained that these relative meanings are not simply imprinted on individuals

but are socially constructed through interactions with others and through historical and cultural norms that exist in an individual's life. However, in constructing these meanings, Petty et al. (2012) illuminated that qualitative researchers use inductive reasoning strategies instead of deductive strategies to build patterns, themes, and categories in the data, which lead to a detailed understanding of the phenomena of interest or a theory.

Mather et al. (2018) articulated that qualitative method addresses how, what, and why questions, whereas quantitative concerns the how much questions. In my research, I sought to document security strategies used by IT security managers. Therefore, a qualitative study was the most appropriate. Moreover, qualitative research aims to develop concepts that will help understand a social phenomenon in a natural setting as against experimental, focusing on the meanings, experiences, and views of the participants (Pope & Mays, 1995). The keywords *meanings*, *ideas*, and *expertise* were my focus. However, these elements cannot be quantified and this ruled out quantitative methods for the study.

Collecting data on the keywords (views, meanings, and experiences) is usually through qualitative data acquisition—mainly, interviews, focus groups, and observations (Bleiker et al., 2019). Bleiker et al. posited that research aiming to explore an individual perception in rich detail and depth should use interviews instead of a quantitative survey. According to Aarsand and Aarsand (2019), there are four main types of qualitative interview techniques: structured interviews, semistructured interviews, open interviews, and group interviews. Kallio et al. (2016) pointed out that a semistructured interview is a commonly used type because it has a researcher's participant reciprocity advantage, which means the researcher can improvise follow-

up questions based on participants' responses to ensure clarity. The semistructured interview requires that the researcher know the subject matter because the interview questions are based on previous knowledge (Kallio et al., 2016). The qualitative philosophical views and the properties of semistructured interviews relate to my study, in which I sought to develop knowledge in security strategies on blockchain application deployment through inductive analysis of data collected through semistructured interviews with IT security managers.

I considered quantitative research methods but realized the method would not be appropriate for the study from both philosophical and theoretical perspectives. Quantitative research is based on a positivist philosophy that has an ontological view that reality is one and is socially ordered, which can be observed and measured (Petty et al., 2012). The epistemological quantitative method only accepts what can be directly observed by the senses, and objective knowledge is possible through observation (Petty et al., 2012). Park and Park (2016) posited that the quantitative method uses deductive reasoning to test hypotheses using numerical data and measurable variables. The data I gathered from the participants were not numerical, not measurable, and could not be observed directly. Additionally, the study was not deducing information from data to test for a hypothesis. Therefore, the use of the quantitative method would have been counterproductive for the research.

I also analyzed the possibility of using a mixed method for the study. Sahin and Öztürk (2019) explained that mixed methods use a pragmatic approach in combining both qualitative and quantitative methods to better respond to research questions under investigation. According to Headley and Plano Clark (2020), mixed methods can produce sophisticated and robust results that cannot be derived from

either quantitative or qualitative results alone. Mixed methods also allow the researcher to generate new knowledge and insights in responding to their research question (Plano Clark, 2019). Plano Clark illustrated three types of mixed methods approaches: convergent mixed methods, explanatory sequential mixed methods design, and exploratory sequential mixed methods. In all three, a researcher must have adequate knowledge of both quantitative and qualitative research methodology. As a novice researcher, I did not have the skills in both methods and could only use one method that could answer my research question adequately. In addition, mixed methods are time consuming (Popescul & Jitaru, 2017) and because the study was a time-constrained project, using mixed methods would have been inappropriate.

Research Design

I selected multiple case studies as the appropriate qualitative method approach for the study. My study's objective was to understand specific strategies used by experienced IT security managers in protecting real-life blockchain applications, for which a case study approach was appropriate. A case study is a qualitative approach used to explore a real-life contemporary bounded system or systems over time through an in-depth analysis of data collected by the investigator acting as the instrument (Alpi & Evans, 2019). To understand a complicated situation, one either experiences it or learns from the experiences of others (Lucas et al., 2018); therefore, using a case study, one can use participants' perspectives to understand more about a specific case. A case study provides answers and exploration for a phenomenon, and what is learned can be put into practice (Alpi & Evans, 2019).

A case study provides an in-depth understanding of a situation and its meanings (Campbell, 2015). The case study also highlights the context rather than a

specific variable and is focused on discovery rather than confirmation. Results from a case study can directly influence policy, practice, and future research (Campbell, 2015).

Case study research has flexibility not available in other approaches, such as grounded theory and phenomenology (Ebneyamini & Moghadam, 2018). Additionally, a case study is designed to fit the case and research question, evidenced by the vast diversity of study designs in published case studies. Ebneyamini and Moghadam (2018) suggested that a case study can play a prominent role in studying the dynamics of technology implementation: "The essence of a case study, the central tendency among all types of the case study, is that it tries to illuminate decision or set of decisions, why they were taken, how they were implemented, and with what results" (Ebneyamini & Moghadam, 2018, p. 2). Therefore, using a case study furnished me with participants' actions and inactions taken to protect a blockchain application deployment successfully.

I considered phenomenology and ethnography qualitative research approaches, but none was appropriate for my research question. Both phenomenology and ethnography study are about lived experience of a phenomenon. However, ethnography focuses on group or community experience; whiles phenomenology centers on individualistic experience. I did not want to study the lived experience of a group or individuals but rather document strategies to implement a case. According to Ploeg (1999), the objective of the phenomenological approach is to describe the lived experience of the participant accurately and not to develop theory or models of the phenomena. The focus of phenomenology is on the lived experience and not on the individual having the experience (Kruth, 2015). Mohajan (2018) explained that in a

phenomenology study, the researcher attempts to understand how participants make sense of their lived experiences in a phenomenon. Alase (2017) posited that data collection in the phenomenology approach is mostly by interviews. Participants are mostly two or more subjects who have lived similar experiences. Even though the collection methods are similar to a case study, the focus is on lived experience and not on decisions taken on a case.

In ethnography research, the aim is to study the lived experiences of a group or community in their natural settings about a phenomenon (Kian & Beach, 2019). According to Koskull (2020), researchers usually immerse themselves among the group of participants in the context of a phenomenon. To generate knowledge from within and understand meanings put on the phenomenon by those studied. The mode of data capturing in ethnography study is mostly observation, field notes, and narrative interviews. Sorce (2019) articulated that the advantage of the observation method is that it illustrates people's actions and behaviors, telling them more than their spoken words. The participants' behavior or actions was not the focus of my research, and I was not interested in a group lived experience. Therefore, ethnography study would have been detrimental to my research purpose.

To ensure confidence in the research I employed data saturation strategy. Guest et al. (2020) posited that researchers should reach data saturation in a qualitative study to answer the research question adequately. A failure to reach data saturation will jeopardize the quality of the research and content validity (Fusch & Ness, 2015). Guest et al. explained that saturation is reached by gathering data until a point of diminishing returns is reached where no new knowledge is added to the data set. To reach saturation, I used Tibben (2015) strategy, that is adding cases to the

study until a new case fails to offer substantial new insights. In addition, I took a cue from Huang et al. (2020), who used the method of concurrently conducting interviews and analysis continuously until no new themes emerged to confirm saturation. Finally, Fusch and Ness (2015) suggested that there is a direct link between data triangulation and data saturation. Therefore, data triangulation is a method to get to data saturation. I used interviews, documents, and field notes as data sources for data triangulation to test for data saturation.

Population and Sampling

My research was a multi-case study, so I used four cases. My selection of four cases was based on a recommendation by Omona (2013). Omona recommended that a sample size between three to five cases is right enough for a case study's data saturation. My participants were IT Security managers with experience in blockchain application deployment. Therefore, the population were four IT security managers; each one was purposely selected and represented one case study. As explained by Farrugia (2019), in purpose sampling the researcher deliberately selects participants based on a criterion the researcher set to ensure the data collection for information needed in answering the research question is optimized. With a small sample of four IT security managers, I employed a census method of data collection to take advantage of its benefit in the data collection process. The census sampling method is a non-probabilistic purposeful method that makes use of all the participants in a universe for data collection (Jacobson et al., 2015). Khosravan et al. (2014) suggested that when the sample size is small, the use of census is more beneficial, but it becomes expensive when the population is large. One of the key advantages of the census method is accuracy because every knowledgeable and expert in the subject

matter identified is used in the study to collect data before conclusions are drawn (Poggrund et al., 2015).

In collecting the research data, Fusch and Ness (2015) postulated that failure to reach saturation will put the research quality and content validity into jeopardy. Fusch and Ness explained that data saturation is reached when there is enough data to replicate the study, and no new information is coming out of additional interviews and data coding. Fusch and Ness (2015) suggested that interview questions should be the same for all participants to enhance data saturation. Therefore, my study, a multiple case study, ensured that the participants in the cases selected were asked the same interview questions using the interview guide in Appendix A.

Ethical Research

Gelling (2020) articulated that ignoring ethics may cause various types of harm, including physical, social, psychological, and economic harm to participants. For these reasons, participants should consent to participate in a study. Metselaar (2019) posited that it should be an informed consent, which means the participant is aware of the purpose, benefits, and potential risks to participants or organization before agreeing to partake. Metselaar explained that three crucial conditions, namely, full disclosure, capacity, and voluntariness, must exist for acceptable informed consent. Full disclosure meaning getting all the information to make an independent decision. Capacity, which is having the ability to understand the information to form a reasonable judgment, taking into consideration the outcome of the decision. Voluntariness, which means the right to make a decision freely without any influence or pressure (Barsdorf & Wassenaar, 2005).

Based on the conditions illustrated, my participants were given full disclosure, and ensured they voluntarily decided to participate in the study. I also adhered to the Belmont report, which preaches respect for persons, benevolence, and justice. Also, I debriefed participants on their freedom to opt out of the study by informing me or a Walden University contact through email or telephone of their desire to do so at any point in time if they become uncomfortable during the study. Schaefer and Wertheimer (2010) articulated that the right to withdraw from a research is a universal accepted policy by all modern institutions conducting research involving human participants and it is to protect participants from any harm during a trial. Participant's consent was captured on the consent form and was signed before the interview process.

Among what were discussed before the consent form was signed is the fact that the interview had no financial benefits. Zutlevics (2016) suggested that financial incentives undermine autonomous decision making and compromise the scientific integrity of the research. Participants were, however, encouraged to join the study voluntarily and informed that their inputs may help improve the protection of blockchain application and add to the IT body of knowledge by partaking in the study. In addition, the consent form made it clear that participants were only required to share their knowledge on the research topic, which was free from any risks to them. Participants were assured of the privacy and confidentiality of any sensitive information that were collected, including their names. According to Surmiak (2018), assuring confidentiality may serve as a guarantee for the participant's statements' authenticity. As suggested by Surmiak, anonymization was used to hide the identities of the participants. The anonymization was done by representing participant's names

with codes such as participant A, participants B etc. The code key was kept in a password protected excel sheet which was encrypted by MacAfee data encryption program during storage. Also, all data collected were encrypted and stored in google drive and an offline drive for protection against theft and damage but will be destroyed after five years as posited by Schmidlin et al. (2015). Finally, to assure participants of the university's involvement and supervision, the Walden IRB approval number has been indicated in the final doctoral manuscript.

Data Collection

Instruments

I used the interview collection method to seek the information needed to answer the research question. Kallio et al. (2016) articulated that the interview method is the most common data collecting method in qualitative data collection. According to Moser and Korstjens (2018), qualitative interview involves the researcher asking the participants questions either via face-to-face, telephone, or online. In a qualitative research interview, the researcher aims to understand what the participants say to gather their experiences, perceptions, thoughts, and feelings (Moser & Korstjens, 2018). Broom (2005) indicated that an in-depth interview is about giving and receiving even though the researcher is not a councilor he/she should be prepared to be supportive. I used semistructured interview questions to solicit for the data needed. According to Megan et al. (2015), it is suitable for exploring the perception and opinions of participants regarding complex issues and probing further to enrich the data. One of the main advantages of semistructure is that the researcher can improvise follow-up questions based on the participant's responses to deepen the understanding (Kallio et al., 2016). Moser and Korstjens (2018), in their guide, suggested that to get

more details from an interview question, there should be a follow-up question. Apart from using interviews, the organization's policies and documents were my secondary source of data that also formed the bases for data triangulation. According to Bowen (2009), print or electronic documents can be analyzed as part of qualitative data collection to combine with other sources as a means of triangulation to seek convergence and collaboration. Bowen explained that document analysis is a systematic procedure to review or evaluate documents on a research topic.

In the interview method of data collection, the researcher becomes the main instrument, and therefore potential self-bias may exist. As the primary data collection instrument, I was mindful of my biases and ensured that I was as objective as possible. Barrett (2018) warned that in qualitative interviews, researchers should be mindful of their biases in order to preserve the study's integrity. Clark and Vealé (2018) indicated that qualitative researchers must understand that their biases may influence the outcome of the study. Using a semistructured interview, I was guided by an interview protocol or guide located in Appendix A. It was designed specifically to mine information that answers my research question. Yeong et al. (2018), postulated that interview protocol should contain the predetermined questions that participants will be asked. Moser and Korstjens (2018) suggested that sequence of these questions should be predetermined in the interview guide or protocol. Moser and Korstjens further explained that interview guide helps to collect the same information from all the participants, which is an effective way of collaborating and confirming data. However, on their part, Kallio et al. (2016) advised that even though interview guide gives a focused structure to the process, it should not be followed strictly. Rather, it should be used as a means of exploring the research area by collecting similar

information from each participant. Interviews were to be face-to-face wherever possible, but I used telephone and online methods due to the COVID-19 pandemic. As articulated by Namey et al. (2020), qualitative data collection is no longer synonymous with face-to-face but a variety of online platforms for individuals and group interview exist. I recorded and transcribed the interview for thematic analysis to make sense of participants' answers.

FitzPatrick (2019) suggested that validation should be ongoing throughout the study process to improve the validity of qualitative research. FitzPatrick pointed out some validation approaches, which I adopted for my research. The approaches included purposeful sampling, keeping the audio recording and transcript for reference, data triangulation, member checking, debriefing sessions with participants and other researchers. In addition, a suggestion by Leung (2015) to enhance research validation that I used included a well-documented audit trail of material and processes and respondent verification.

Data Collection Technique

My research question was: What strategies do IT security managers use in deploying blockchain applications securely? I sought to answer the research question by using cases of experienced IT security managers who have deployed or have experience in the subject matter. I intended to understand the strategies the security managers have used to protect the blockchain applications by interviewing them and analyzing organizational documents relating to IT security. I used a semistructured interview strategy suggested by Kallio et al. (2016) to operationalize the interview. The main advantage of this semistructured interview data collection is the reciprocity between the interviewer and interviewee, enabling the interviewer to improvise

follow-up questions based on answers from the participants (Kallio et al., 2016).

Opdenakker (2006) indicated that face-to-face interviews also have the advantage of giving the interviewer social cues such as body language, voice, intonation, and other nonverbal information. According to O'Keefe et al. (2016), a significant advantage of semistructured interviews is that, opportunity for new information to emerge from the interview with experts is high because the interviewer spends more quality time with the participants. On the other hand, face-to-face semistructured interviews come with cost as a disadvantage, especially if the interviewer will have to travel to the location of the interview (Kallio et al., 2016).

The first phase of my data collection strategy was identifying the prerequisite for using a semistructured interview. This phase enabled me to confirm the appropriateness of the use of a semistructured data collection method for my research question. As Moser and Korstjens (2018) articulated, a semistructured is suitable for eliciting the participant's experiences, perceptions, thoughts, and feelings. My study sought to understand security strategies used by IT security managers with experiences in protecting blockchain. Therefore, semistructured questions were able to unearth such knowledge from my participants. The second phase of my data collection strategy was to update my knowledge on the subject matter through literature and seminar papers. This second phase of the data collecting strategy was necessary to create a predetermined framework and a conceptual basis for the interview, as explained by (Kallio et al., 2016). The third phase of the data collection strategy was developing a semistructured interview guide, which contained a list of predetermined interview questions. A listing of the interview question is in Appendix A. The interview guide steers the conversation towards the research question during

the interview (Cridland et al., 2015). The semistructured interview guide had two levels of open-ended questions, the central theme and follow-up questions. The main theme focused on the main content of the research subject while the follow-up questions were used to clarify answers from participants and direct the interview towards the study subject (Baumbusch, 2010). The fourth phase of the data collecting strategy was testing of the interview guide to ensure the questions have no ambiguity. As Chenail (2011) articulated, testing the interview guide makes it possible to make informed changes, adjust to the interview questions, and improve the quality of the data collections.

The final stage of the data collecting strategy was the interview itself. Before starting the interview, the participants were briefed about the interview and the details of the consent document. After ensuring that they understood the consent document and what was required of them for the interview, I sought their signatures to be appended to the consent form. The open-ended questions were then asked for the participant to answer. When necessary, I used probing questions to get clarification on the response. As articulated by Arsel (2017), probing questions illuminate an answer for clarity. I scheduled another meeting with participants to have a member checking and shared a summary of their answers to the open-ended question to validate their responses. According to Birt et al. (2016), member checking is used to validate, verify, or assess the fidelity of qualitative results. During this meeting, all other unclear issues were discussed with participants. Any new information that popped up during this section was discussed in another member checking session until no new information came up.

Data Organization Techniques

Alase (2017) articulated that managing data in qualitative research is vital to the study's success. Alase explained that the data must be analyzed to give meaning to the research but must be kept securely during the study period and disposed of after a while. Therefore, the researcher must provide adequate security for the protection of the data collected. Data that I generated from the study interviews were encrypted with the McAfee Complete Data Protection software product. The files were stored in Google drive cloud place for additional data protection against damage or theft. For hard copies of data, I locked them in a safe during the study and will return them to participants on completion of the research. After 5 years, all the transcribed data will be destroyed as demanded by Walden University URR. Additionally, Alase (2017) suggested that the video and audio recording should also be destroyed after transcribed to protect the participants.

The recorded interview and other data forms, such as field notes, organization documents, and any data collected, were upload into MAXQDA 2020 software. The MAXQDA 2020 software organized all my research data in one central location and allowed efficient coding, labeling, categorization, and development of themes in the same software environment (Galan-Diaz, 2017). In addition, MAXQDA software provided a logbook, which I used as a research diary for recording the study process. For instance, Elaldi and Yerliyurt (2017) used MAXQDA successfully in organizing and analyzing their data.

I uploaded my interview audio files and any other related data, such as field notes, with the software in my initial step. The software had transcription capabilities, which I used to produce verbatim text from the audio. I began data exploration as the

data was collected and loaded in MAXQDA. The software provided a memo function that enabled adding notes and comments as I went along. The software also provided a coding and categorization function, that I used. As I continue to code and categorize using the software, the themes gradually emerged. Using the inbuilt logbook, I documented all processes and steps taken throughout the study.

Data Analysis Technique

As stated in the purpose statement, the objective of the research was to know and understand the strategies IT security managers use in protecting blockchain applications. Meanings and understandings are qualitative and can be obtained using a semistructured interview and other sources of qualitative data such as an organization's policy documents, as illustrated by Kallio et al. (2016). I used the MAXQDA software to gather all the collected data and stored them at one location for ease of access for analysis. Lester et al. (2020) suggested that data gathered by a researcher be structured and stored at a single location for better data management. Lester et al. explained that storing the data in a structured manner with names of sources and other metadata enables the development of the corpus data for analysis. The recorded interview audio was transcribed verbatim to ensure all the spoken words were captured. According to Halcomb and Davidson (2006), verbatim transcription produces a replica of what the interviewee said and guarantees accuracy in the interview data set. Organization documents such as policies were captured and stored. These documents included both electronic and paper documents. However, paper documents were scanned and converted into electronic format. These documents were examined, and those that had the potential to answer the research questions were analyzed. As explained by Bowen (2009), document analysis, like any other

qualitative data source, requires that data be examined and interpreted to solicit meaning and understanding of the phenomenon in question.

To ensure the truthfulness of the analysis and rigor in the research, I used method and data triangulation in the study. As Carter et al. (2014) puts it; triangulation enables the use of multiple data to gain a comprehensive understanding of a phenomenon and to ensure the validity of the research through the convergence of the different data sources. Carter et al. explained that, in method triangulation, the researcher uses different data collections methods from the same phenomenon. In my study, I used a semistructured interview and documents to collect the data. Data triangulation uses different individuals or groups to collect the data to gain different perspectives and validation of data (Carter et al., 2014). Bowen (2009) sees data triangulation to provide convergence of proof that produces credibility and reduces biases. As my study is a multiple case study, which involved interviews of different individuals in various cases, the use of data triangulation was appropriate. According to Stavros and Westberg (2009), multiple case studies put confidence and robustness in a study.

In analyzing the data set, I used a five-step procedure proposed by Akinyode (2018). The steps included data logging, anecdotes, vignettes, data coding, and thematic network. Data logging involves simultaneously documenting the raw data collected from all the sources and identifying all issues by iteratively confirming with original data. Anecdotes of the collection were then made to comprehend the data that helped develop the themes. Lester et al. (2020) explained this step as the stage when the researcher starts becoming familiar with the data and helps build an initial understanding so that gaps in the data set can be identified and worked on. The next

step in the Akinyode proposed process was developing the vignette of the investigation or meanings of the interview to produce a more profound sense of understanding about the phenomenon to make it convincing to readers. According to Lester et al., this step allows memos to be written to indicate initial reflection about the data and any emerging interpretation. The fourth step was to code the data collected by putting tags to related themes from different sources. As explained by Akinyode, coding helps separate data into categories or themes, so the data from different sources can be harmonized and reduced to a manageable size. According to Williams and Moser (2019), coding is the key to organizing data in qualitative research. Lester et al. explained that coding is an essential element of thematic analysis and involves assigning a short, descriptive, or phrase representing meanings to data related to the researcher's analytic interest. In coding my data, I made use of the MAXQDA qualitative software. Williams and Moser suggested that qualitative software reduces coding errors and makes the process more efficient.

The final step was using thematic analysis to make sense of the data collected, as articulated by Lester et al. (2020); thematic analysis is more convenient and appropriate for novice researchers like myself. Kuruppuge and Gregar (2020) successfully used a similar thematic analysis in multiple case study research. According to Moser and Korstjens (2018), the analysis should begin as soon as the first interview is done to refine the subsequent interview questions. The thematic analysis aims at identifying patterns in a qualitative dataset (Lester et al., 2020). Akinyode (2018) explained that the thematic analysis objective is to explore a subject's understanding or make sense of an idea. The nature of the main themes that emerged was defined using knowledge gained from the literature. Peel (2020)

suggested that themes should be conceptualized from the categories of codes to create meanings that can be defined based on literature and interpreted beyond the categories of data for larger meaning by linking the raw data to research literature. In discussing my major themes, I considered inputs from current studies related to my research topic since the development of my proposal.

Reliability and Validity

Reliability and validity in research are essential to ensure that the research outcome's application produces a quality knowledge base or utilitarian function in the subject area of concern. Aguinardo (2004) explained that a qualitative study's ability to deliver emancipatory goals or promote social action is determined by its validity. Aldhouse and Kitchen (2018), on the other hand, posited that poor quality in the qualitative study may contribute to unreliable data, which will lead to inaccurate conclusions and a false understanding of issues such as disease burden. Golafshani (2003) articulated that, unlike quantitative research, where the validity and reliability of a study depend on the instrument's design, qualitative research validity and reliability depend on the researcher because the researcher acts as the instrument in qualitative research. Golafshanni further explained that validity and reliability are not separated; therefore, words such as credibility, transferability, and trustworthiness represent quality. In support, Noble and Smith (2015) suggested that due to the qualitative research philosophical view, an alternative measure of rigor must be used and proposed truth-value, consistency, neutrality, and applicability as a criterion to determine rigor in a qualitative study. Other criteria proposed by Moser and Korstjens (2018) are credibility, transferability, dependability, and confirmability. Moser and Korstjens argued that criteria used for quality in quantitative research could not be

used for qualitative research because the two methods have different epistemological and ontological views.

For example, Leung (2015) explained that reliability, as used in a quantitative study, cannot be applied to qualitative study, but consistency should preferably be used. Regarding validity in qualitative studies, Leung posited that it should be determined by the appropriateness of the tools, processes, and data used in the study. According to Leung, this means that the research question should be valid for the desired outcome, the kind of methodology to be used should be a fit for the research question, the study design is valid for the methodology, the sampling and data analysis is proper, and finally, the results and conclusion drawn are valid for the sample and context.

In ensuring credibility for my study, I adopted strategies proposed by FitzPatrick (2019) and another by Noble and Smith (2015). These strategies incorporate most of the definitions by Leung (2015) and Golafshani (2003). According to FitzPatrick, validation procedures should be part of the ongoing study process rather than after so that threats to validity can be reconciled during the study period. The credibility transferability, dependability, and confirmability strategies I used are as follows.

Reliability

FitzPatrick (2019) indicated that a thick description of the participants, events, and themes with detailed reports and facts brings credibility to the reader. Besides, Moser and Korstjens (2018) explained that thick description makes the study transferable. Noble and Smith (2015) explained that thick and rich extracts assist readers in determining the study's truth-value. According to Cypress (2017), a

detailed description of the entire process that makes room for inter-subjectivity indicates a good quality in a qualitative study and makes the research reliable. FitzPatrick (2019) explained that having both the audio and transcript strengthens the descriptive validity. The recording will indicate gestures such as the tone of the voice that cannot be presented in the transcript. Besides, listening to the interview audio and reading the transcript will strengthen a researcher's conclusion.

In some cases, readers can be given excerpts of the interview audio to give them confidence in the study's inferences and conclusions. Cypress (2017) asserted that because the researcher is the main instrument in a qualitative study, he should have adequate training in a qualitative study to ensure a reliable study. As a novice researcher, I acquired the requisite knowledge in my doctoral study through professional and experienced mentors that guided me to produce a reliable study.

Validity

Cypress (2017) explained that validity in qualitative research is related to meticulous recording and constant data verification during the study. Cypress cautions that one of the dangers to validity is researcher bias since the researcher is the study instrument in qualitative research. Explicitly acknowledging my roles in the research, my biases, feelings, and assumptions, and how they will influence the study's analysis, results, and conclusions will strengthen the validity of the inferences drawn. Shufutinsky (2020) articulated that use-of-self (Awareness, mindfulness, and self-knowledge) by the researcher and consciously controlling biases is critical to the study's validity and credibility.

Engaging participants for an extended period provides more complete data because it enables trust and rapport between the participants and the researcher.

FitzPatrick (2019) suggested that such a validation approach is constructivist as it is not predetermined. Therefore, it allows the participants' voices to play a substantial role in interpreting the data. According to Moser and Korstjens (2018), a lasting presence with participants in an interview helps build trust and enriches the collected data. The use of purposeful sampling ensures validity because the selected participants are knowledgeable in the research subject area to give quality information that will aid in answering the research question. As explained by Söylemez (2018), purposeful sampling enhances the validity of the research. Both Green et al. (2015) and Suri (2011) agree that purposeful sampling leads to data saturation, improving the research quality.

Credibility

To increase credibility and reduce study biases, researchers use a triangulation technique whereby researchers try to use multiple and different sources of data to reach convergence (FitzPatrick, 2019). FitzPatrick suggests combining multiple methods such as case study and document analysis provides richer data and increases authenticity. According to Noble and Smith (2015), triangulation produces a comprehensive set of findings. Moser and Korstjens (2018) proclaimed that triangulation is a reliable strategy to ensure the credibility of the research. Fusch and Ness (2015) argued that there is a direct link between data saturation and triangulation. Fusch and Ness explained that data triangulation is a method to ensure data saturation.

FitzPatrick (2019) articulated that member checking is a sure way to eliminate misinterpretation of the meaning of what participants illustrated. The member checking involves giving participants the data and your interpretation to confirm or

correct what they meant. According to FitzPatrick, this is a critical check for validation because qualitative research reveals that reality is socially constructed and represents what the participants perceived. As explained by Moser and Korstjens (2018), one benefit of member checking is its ability to strengthen the data and make the study more credible.

Collecting varied and detailed data will ensure a complete understanding of participants. These data include what participants say, do, write, or produce. In my case, I used interviews, documents, and field notes. According to FitzPatrick (2019), sufficient data generate a full picture of the phenomenon. Also, ensuring rich data gives detailed insight into cases or phenomena under study (Barrett & Twycross, 2018). Having debriefing sessions with a trusted peer reduces research biases and improves the study (FitzPatrick, 2019). In addition, researchers share the study reports with the participants after the research to explain the results to reinforce the researcher's understanding and interpretation. According to Noble and Smith (2015), such sessions reduce biases and improve the truth-value.

Transferability

Moser and Korstjens (2018) explained that a thick description makes the study transferable. On the other hand, Noble and Smith (2015) explained that thick and rich extracts assist readers in determining the study's truth-value. Noble and Smith further explained that rich detail of context enhances transferability. Cypress (2017) also articulated that transferability is enhanced by using purposeful sampling and a thick description of the process. In addition, Cypress suggested that transcription of the interview should be done verbatim for future reference, and the rich documentation of

the analysis process should be ensured. To ensure transferability, I meticulously adopted the suggestions made by these writers above.

Confirmability/Dependability

Noble and Smith (2015) explained that a transparent and precise description of the research process from the initial outline through the development of the method and finally reporting of findings makes the study confirmable. In addition, keeping a research diary and documenting issues and challenges encountered during the process and how they were resolved improved the cohesion between the study's aim, design, and methods (Noble & Smith, 2015). Also, emerging themes should be discussed with experts in an open process to challenge assumptions and reach a consensus. To enhance dependability and confirmability, I kept track of and documented my research processes from beginning to end, which empowered me to give detailed and transparent reports at the end of the study. Moser and Korstjens (2018) suggested that having an excellent transparent report of the research steps taken throughout the project makes the study credible and dependable. Also, keeping an audit trail is one of the critical strategies for establishing the confirmability of qualitative findings (Cutcliffe & McKenna, 2004). Carcary (2009) illustrated that confirmability of a study could be built into a study to improve trustworthiness by developing an audit trail of the research to demonstrate that the research was carried out with substantial care.

Transition and Summary

In section two, I discussed the methodology used in my research. I chose the qualitative method, and case study approach, which I am confident, answered my research question. The chosen methodology and approach were suitable for collecting

data from experienced IT security managers to understand the strategies used in securely deploying blockchain applications. I also explained the strategies I used to ensure trustworthiness in the study by detailing my actions to ensure credibility, transferability, dependability, confirmability, and reflexivity. In Section 3, I will use the data collected to detail the result of the study and my conclusions.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative, multiple case study was to explore the strategies IT security managers use to securely deploy blockchain applications. I collected data for this research by conducting semistructured interviews with four IT security managers from blockchain-related companies and reviewing company documents. Three themes emerged from the data analysis: (a) cryptographic key management, (b) comprehensive software auditing, and (c) strong traditional IT security controls. In this section, I discussed the findings, applicability to professional practice, the implications for social change, the recommendations for action, recommendations for future research, and a conclusion.

Overview of Study

I undertook this study to understand how some organizations protect blockchain applications. Blockchain applications have experienced many recent attacks despite their security (Saad et al., 2020). The information I gathered indicated that even though blockchain has inherent integrity, it is challenged by other common lapses in traditional IT security control. In fact, Extance (2015) made a similar observation and stated that blockchain is not secure out of the box. One of the biggest challenges that emerged is the limited knowledge and experience in blockchain technology, which has resulted in insecure investment and implementations. Blockchain technology has no common framework and regulations to govern its implementation or operations to assure security. By ensuring good cryptographic key management, a firm primary IT security control, a comprehensive software auditing

system, a more profound understanding of blockchain, and a blockchain security framework will make blockchain applications more secure.

Presentation of the Findings

My overarching question for this study was: What strategies do IT security managers use in protecting blockchain applications? My target population was IT security managers in blockchain-related companies in Ghana, the United States, and Europe. I employed purposeful sampling to identify and interview four security managers in blockchain-related companies who have experience in blockchain systems and IT security. Data were collected using semistructured interviews and a review of company documents to ensure triangulation. Member checking was done with participants to validate interpretations of their input. I confirmed data saturation by collecting data until no new themes emerged. The conceptual framework for the study was RAT. In analyzing the data collected, I used a five-step procedure: (a) data logging, (b) anecdotes, (c) vignettes, (d) data coding, and (e) thematic network (Akinyode, 2018).

Voluntary participants gave consent to participate in the study by stating their desire in response to my consent email. Pseudonyms were used to protect participants' names (PT1 to PT4) and their company names (CP1 to CP4) for confidentiality. Each participant was interviewed for about 45 minutes using Zoom online meeting software. Follow-up questions were asked via phone calls or emails where necessary. Company documents were acquired through their authorized company representative by signing a partnership letter of cooperation. To ensure data saturation and that findings were dependable, credible, confirmable, and trustworthy, I used method and data triangulation (FitzPatrick, 2019). The audio interviews were

transcribed using MAXQDA. All other documents and transcripts were then uploaded into the MAXQDA document system to analyze and develop themes (Elaldi & Yerliyurt, 2017). The themes developed aligned with the RAT conceptual framework and literature review discussed in Section 1.

According to RAT, crime occurs when three elements come together in time and space: (a) absence of a capable guardian, (b) attractive target, and (c) a motivated offender (Mohammad & Nooraini, 2021). Leukfeldt and Yar (2016) explained that even though RAT was developed for terrestrial crime, these three elements have their equivalent in the cyber world. Leukfeldt and Yar indicated that, when it comes to motivated offenders, countless cybercriminals are attracted to targets in the cyber world such as information and digital money. Leukfeldt and Yar also reiterated that capable guardians could be equated to IT security controls in the cyber world.

Theme 1: Cryptographic Key Management

Cryptographic key management implementation was one of the themes that surfaced from the data collected from the interviews. All participants indicated that having a sound key management system was useful in protecting blockchain applications. Thirty-four elements of cryptographic key management were mentioned by the participants during interviews, and in a review of 12 company documents, 36 references were found for cryptographic key management.

Table 3

Cryptographic Key Management and Supporting Metrics

Participants	References frequency	Documents	Reference frequency
4	34	12	36

Cryptography key management is a collective technique and procedure in handling keys throughout a system's life cycle (Kbean & Sadkhan, 2020). Kbean and Sadkhan explained that the objective is to maintain an acceptable level of security throughout the life cycle of a cryptographic system. Key management is essential in cryptography because it is the basis for securing cryptographic techniques and providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures (Ali & Alaa, 2018). PT1 indicated that it all comes to key management when protecting blockchain applications:

The last thing we do to keep this secure is key management. If you feel that someone has compromised your keys, you have to be able to rotate them in a twinkle of an eye, rotate all the keys, and make yourself secure, and this all comes down to key management.

PT2, PT3, and PT4 agreed with this assertion and made similar statements. PT2 stated, "It's not about the technology or the chain and the fancy peer-to-peer network. It all comes down to cryptography keys, so a solid key management system is needed." PT3 stated that key management is the core of their protection on their Blockchain applications: "To ensure a secure key environment, we have put in place National Institute of Standards and Technology (NIST) key management framework." This statement corroborated information captured in CP3's key management policy, which states,

The purpose of this policy is to provide the top-level framework of governance and direction to ensure a secure cryptography management, i.e., the provision or issue, storage, use and recovery or revocation and decommissioning, of cryptographic products and key material (Keymat) for the Department.

All four companies the participants represented have policies in place that govern cryptographic keys. Going through the policies, I discovered those policies corroborated the verbal statements made in the interviews. PT4 stated, "Encryption key management is a crucial part of the company's application protection strategy, inadequate encryption key management can result in the loss of valuable digital assets and can lead to severe penalties and legal liability."

Pal et al. (2021) detailed that efficient and secure key management is a challenge for any cryptographic system. If an intruder can steal the keys by any mechanism, like brute force, side-channel attack, physical access of the system, weak encryption, or replay attack, the intruder has access to everything from the targeted system. For example, in the case of blockchain, the security of the asymmetric encryption technology used depends on the management of the private keys (Cai et al., 2018). As PT2 stated, "The biggest thing there is, it always goes back to the private key, exposing it. You don't want to expose a private key, and that's the biggest threat." More importantly, some blockchain, such as bitcoin blockchain private keys, grant access to private data and cryptocurrency, which is of great value (Zaghloul et al., 2020).

Therefore, the cryptographic keys of blockchain are attractive to would-be offenders, as predicted by RAT (Cohen & Felson, 1979). RAT posits that motivated offenders will take advantage of opportunities when they encounter suitable targets that lack capable guardianship. Lee and Choi (2021) explained that cybercrimes rely on computer networks to connect motivated cybercriminals with potential targets in the absence of capable guardianship in the cyber world. According to Xu (2016), user anonymity, cyberspace low entry barriers, spatial and temporal separation between

users exacerbate cyberspace crime. In cyberspace, personal information such as cryptographic keys naturally carry valuable assets into cyberspace, which attract computer criminals (Lee & Choi, 2021). PT2 and PT3 agreed with the assertion that blockchain attracts cyber attacks because of its value. PT3 stated,

blockchain is mostly used for critical data and assets. Another reason why blockchain is a viable target to threat actors is the fact that 95% of its applications is important data such as money, private information, etc. The sheer value of these assets motivates hackers to attack blockchain systems as they see a large value being reaped if hacking is successful.

Therefore, if cryptographic keys are not well managed, the system becomes easy prey for motivated offenders. Several blockchain companies have lost millions of dollars because of inefficient management of cryptographic keys (Zamani et al., 2020).

Three types of management came up during the interview: offline (cold wallet), hardware security module (HSM), and multisignature private key management systems for enhanced security. Offline management systems, as described by PT2, are systems that stores the private key of a blockchain off the Internet. PT2 stated,

The biggest advice is typically is to have a cold storage wallet, typical machines or cold storage systems that are off the internet is not exposed to the internet. That is the safest way you can protect your crypto assets.

In an attempt to explain offline key storage, PT1 stated, "It is a randomly generated key, it has never seen a computer, never been anywhere near the blockchain so typically harder for people to you know, and attack that."

PT1's statements aligned with Pal et al. (2021), who explained that offline key storage avoids the possibility of online hacking and stealing of keys through malicious software and physical access of the device that stores the keys. Pal et al. further indicated that private keys are stored in offline portable media like USB or in the form of a paper wallet in offline storage.

However, Conti et al. (2018) caution that offline wallets' usability is low even though they are more secure than other options. Therefore, a balance should occur between usability and security when selecting offline key management options. PT1 said that most digital assets are stored offline, and a few that are regularly used are stored online:

One thing you can do here to separate what is a cold asset from a hot asset - a hot asset is a bitcoin you use every day for a transaction, so if I have one million, I split it into two. I put 500,000 Euros into a cold storage, which means it's in a bitcoin wallet that has never seen a computer.

PT2 made the same suggestion. In his case, the use of private blockchain is used as offline media:

If I were to run Coinbase, I would have offline storage site that has a majority of that money sitting there, probably have a private blockchain so that you have more control on it before it gets to the public blockchain so that some can move it around.

Offline storage strategies satisfy the tenets of RAT. According to the theory, if all three RAT elements meet in time and space, the potential is high for crime to occur. If motivated offenders, suitable targets, and the absence of a capable guardian coincide in time and space, crime may occur; manipulating any of the three elements could

control crime (Schaefer & Mazerolle, 2017). Therefore, by using the offline key management system, the distance between the target and the offender is being separated to make the meeting of the three elements more difficult.

Even though offline storage gives a higher level of security, Boireau (2018) explained that they remain vulnerable to various hacks, including fault injections. A fault injection attack happens when malware is intentionally introduced in the security hardware (offline wallet) during production to prevent either a legitimate operation of the hardware or corruption of the data to leak the stored private key (Boireau, 2018).

PT1 mentioned the use of HSM key as one of the best ways of managing private keys:

The next thing is how will you store your keys. For this, we use HSM. These are like hardware devices, and they are specialized for storing keys, creating keys even for our signatures. This is really really preferable to trying to do it on your own on some server.

Boireau (2018) articulated that HSM is the best option for key management because HSM has long been used by banks and has stood the test of time. Boireau explained that HSM is built with a high level of security in mind and is cryptoprocessor-based, which securely generates, protects, stores keys, and typically guarantees a level of regulatory assurance that meets compliance requirements by either the Federal Information Processing Standard (FIPS) certification or common criteria international standards.

The last key management system mentioned in the interviews was a multisignature system. PT1 and PT 2 explained that a multisignature key management system requires two or more authorizations before a transaction can occur, which improves the security of the blockchain. For example, PT2 stated,

You could have a big bitcoin wallet, say your treasury bond, and this is big wallet, big bankô you only have to give one or two people the private key, and you need all the two or three people to authorize this before money can be taken out.

This was corroborated by a statement from PT1:

The other thing is you can use things like multisig, so you require two signatures to make a transaction, which means that, you kind of spread your risk there and acts like a dual control. This is what they call it. Someone has to have one key, and another person has to have one key before they can have the money.

Singh and Singh (2016) and di Angelo and Salzer (2020) explained that multisignature wallets ensure two or more signatures before a transaction can occur. The authors highlighted that such arrangements are generally referred to as M-of-N, meaning the transaction is associated with N private keys but requires at least M keys before it can be implemented, ensuring security and corporate governance.

Table 4

Software Auditing and Supporting Metrics

Major Theme	Participants Count	References Frequency	Documents (ITPolicy, Cybersecurity Policy, Standards Manual, Operational Manuals)	References Frequency
Software Auditing	4	20	16	32

Theme 2: Software Auditing

Another theme that emerged from the interviews is Software Auditing. The participants made Twenty (20) references on software auditing, and which was collaborated by Thirty-Two (32) references in the company documents as indicated in Table 4. According to He et al. (2020), vulnerabilities in smart contracts or blockchain applications can lead to severe financial loss and legal problems. He et al. explained that code audit could detect any security vulnerability before publishing the application or smart contract. Participants PT1, PT2, and PT3 expressed a solid need to audit blockchain applications before deploying them because most of the recent hacks on blockchain were due to faulty software codes. For instance, PT1 cautioned that once Smart Contract is deployed, it becomes immutable, and so is any security vulnerability and bugs embedded in it. He cited a software vulnerability in the Ethereum blockchain smart contract which caused Decentralized Autonomous Organization (DAO) to lose millions of dollars.

This DAO hack is also confirmed by Xu (2016), who articulated that even though it is challenging to hack the blockchain records, the programming codes and systems that implement the technology can be vulnerable. Xu mentioned that MtGox and DAO were hacked off over \$750 million due to poorly implemented codes. PT2 also pointed out that software that generates the crypto keys or wallets could also be vulnerable and, therefore, must be critically audited for bugs and intentionally inserted malware designed to steal the keys, as captured in his statement below.

So if you lockdown your master key, you sure to take the adapted principles but you also have to be careful now, because the private key has money on it right now, so you have to be extra careful about the code, get third party to

audit the code or get someone in house to audit the code, you have to be careful because developers write code straight lines all day, they may write it with standards or meet some requirement, but you need a third party to audit the code to determine if its vulnerable or if something weird was being done with the private key.

PT3, on his part, articulated that all software is prone to vulnerability, so regular penetration testing and other security assessment should be done to determine the security posture of the application and the network. As captured in his statement below, PT3 suggested that regular audit would help discover new threats so that solutions can be designed to address the problem.

Furthermore, regular security audit help reduce vulnerabilities. All software is prone to vulnerabilities and as such it is advisable to have regular penetration testing and other security operations to assess the security posture of the application and network. This helps discover new vulnerabilities in the dependencies or the underlying language or system to be patched with the latest update.

Ghosh et al. (2020), numerated several attacks on the Ethereum blockchain due to vulnerability in the smart contract code. A more detailed analysis of code vulnerability in blockchain applications has been published by Ahmed and Pathan (2020). In the article, Ahmed and Pathan posited that software and web application vulnerabilities are a genuine concern in smart contracts. The authors pointed out that to date, the blockchain research community has identified 34,200 vulnerabilities in smart contracts, among which hackers can exploit a set of 3000 to steal \$6 million worth of cryptocurrency. Therefore, any organization that plans to deploy blockchain

applications should ensure the design of a secure smart contract, ways of identifying vulnerabilities, and how to mitigate zero-day vulnerabilities.

The literature revealed several ways to audit blockchain application codes. He et al. (2020) classified them into two groups that are the manual auditing and automated auditing. He et al. explained that manual auditing heavily relies on experienced security engineers who will study the code and quickly identify vulnerabilities and possibly patch them before launch. On the other hand, automated auditing uses software tools to increase the efficiency and speed of the auditing process. The downside of automated auditing is its inability to address logical loopholes (Perez & Livshits, 2019). He et al. identified and detailed three smart contract automated tools currently used, namely Oyente, Mythril, and Porosity. Other tools presented by Perez and Livshits (2019) include ZEUS, Maian, SmartCheck, ContactFuzzer, Securify, Vandal, MadMax, Sereum, Vormal verification, and teEther.

Blockchain applications mostly hold valuable assets, and for example, smart contracts hold cryptocurrency and tokens. According to Zou et al. (2019), smart contract applications control and manage sensitive digital assets. Therefore, according to RAT, such applications are considered valuable targets, and without a capable guardian, they could be victims of crime. As postulated by Wang et al. (2015), IS application's value increases its risks of being accessed by unauthorized people. According to RAT, a target's suitability depends on its value, inertial, visibility, and availability (Lee et al., 2018). Felson and Clarke (1998) defined inertial as how easy it will be for offenders to remove or overcome the target. Lee et al. further explained that inertia is negatively related to a suitable target. Meaning if the inertia is high chances of the item becoming a target is low. Concerning applications, the strength of

application controls can make it difficult for an attacker to either steal the application's data/functionality or achieve a malicious purpose within an application (Wang et al., 2015). Therefore, auditing a blockchain application to remove bugs and malicious codes can be seen as hardening and increasing the inertia to make it a difficult target, as theorized by RAT. As Yar (2005) pointed out, files and technical specifications can be seen as a form of inertial that can control the level of suitability a target can offer.

Table 5

Major Theme Traditional Security Control With Supporting Metrics

Major Theme	Participants Count	References Frequency	Documents (IT Policy, Cybersecurity Policy, Standards Manual, Operational Manuals)	References Frequency
Traditional Security Control	4	59	16	48

Theme 3: Traditional Security Controls

Traditional security controls are one of the themes that interviewees discussed. As indicated in Table 6, the theme was the most referenced by participants. In their view, traditional security control is critical in the protection of blockchain applications. They articulated that security managers assume blockchain is secure, and so IT controls are lax at the basic level. For example, PT1 in the interview stated: "I think the final thing I will leave with this is, bitcoin although very secure is not secure out of the box right, you still have to do your due diligent as a security manager."

As explained by Radhakrishnan et al. (2019) in the literature, users of the blockchain assume it is secure and tend to have excess confidence about its security; therefore, attackers try to focus on the traditional ways of attacks such as phishing, dictionary attacks, and vulnerable signatures. The interviewees iterated that traditional security controls such as antimalware deployment, physical protection of systems, and cybersecurity awareness programs are all needed to protect blockchain applications. For example, PT3 said,

Installation of antimalware software help prevents hacking. As mentioned earlier, a threat to blockchain applications is the compromise of the components of the blockchain network. A way to mitigate this is to install up to date antimalware software that may recognize signature of payloads sent by threat actors to take over the system.

PT2 said,

People are scammers, you have to watch out for scammers who will try to phish out your private keys, they will try to get you to a scheme like that, using phishing emails, there are other ways too.

According to Baker and Wallace (2007), traditional security controls have advanced to a stage where a holistic approach is needed. Baker and Wallace articulated that having a structured way of managing security controls standards such as the National Institute of Standards and Technology (NIST) are critical for information security control. The NIST standard classifies Information Security controls into three main categories. The categories are Technical Controls, Operational Controls, and Management Controls. Baker and Wallace further explained the categories as follows;

- Technical controls; traditionally include products and processes (such as firewalls, antivirus software, intrusion detection, and encryption techniques) that focus mainly on protecting an organization's ICTs and the information flowing across and stored in them.
- Operational controls; include enforcement mechanisms and methods of correcting operational deficiencies that various threats could exploit; physical access controls, backup capabilities, and protection from environmental hazards are examples of operational controls.
- Management controls; involve using policies, employee training, business continuity planning, target information security's nontechnical areas.

Even though these standards were designed for non-blockchain systems, it plays a significant role in protecting blockchain applications because they are intertwined with traditional systems. Shrivastava et al. (2020) proposed a hybrid security framework for blockchain systems that involved traditional security control standards and blockchain-specific standards. The hybrid framework has an outer layer managed with traditional security controls and an inner layer governed by blockchain-specific security standards. According to Shrivastava et al., traditional information security control standards such as NIST, International Electrotechnical Commission (IEC), and the International Organization for Standardization (ISO) can be considered. The latter group of standards is jointly known as ISO/IEC 2700 series. Homoliak et al. (2019), on the other hand, illustrated a layered blockchain security reference model, which uses a template based on ISO/IEC 15408 standard to identify risk and mitigation at various levels. Homoliak et al. indicated that at the application layer, where most of the

attacks have occurred in recent times, mitigation methods include traditional security controls.

PT1 also revealed the use of equivalent European standards such as IT-Grundschutz Compendium and BSI-101 by his company for traditional security controls in their blockchain systems. In fact, PT1 was very emphatic on the use of these standards and made the profound statement below.

The documents and standards I provided form a crucial part of the general information security principles. My claim is that these core principles of security transcend new technologies such as blockchain. In fact, with the proper suggested principles in these standards such as Dual Control, Role Based Access Control, Proper risk Management, etc., many of the blockchain-specific risks can be effectively mitigated.

As at this time of writing this paper, limited literature exists for internationally accepted security standards for blockchain. However, PT2 recommended a standard that can be considered for blockchain protection. He made this statement.

Following the Information Security standards is beneficial; however, organizations and startups looking to secure their blockchain and wallet private keys should primarily look at the following standard that is more relevant or ðtunedö for blockchain protection - Cryptocurrency Security Standard (CCSS)

PT2 indicated that CCSS is broken into ten sections focused on private keys protection. The ten sections covered by CCSS are Key/Seed Generation, Wallet Creation, Key Storage, Key Usage, Key Compromise Policy, Keyholder

Grant/Revoke Policies & Procedures, Third-Party Security Audits/Pentests, Data Sanitization Policy, Proof of Reserve, and Audit Logs

Some crypto companies have started implementing this standard in addition to their traditional security standards. A news media article by PR Newswire (PR Newswire, 2019) confirmed that Crypto.com, a cryptocurrency platform, has officially achieved Level 3 compliance with the Cryptocurrency Security Standard (CCSS); the highest and strictest level achievable. The paper explained that CCSS is designed to complement existing information security standards such as ISO 27001:2013 by introducing additional security best practices for cryptocurrencies. A statement attributed to the Chief Information Security Officer of Crypto.com in the publication reads, "A key component of any cybersecurity strategy is the ability and willingness to adapt existing security controls to incorporate new technologies and processes."

The statement made above is in tune with what my interviewees have articulated. My conceptual theory very much supports traditional security controls. Capable guardians in RAT are seen as technical controls, management controls, and operational controls in cyberspace. For example, Hsieh and Wang (2018) articulated that cyber guardianship has a broad spectrum, which can be from informal guardians such as in-house network administrators, ethical private and public computer users to formal guardians like antivirus software, firewalls, antivirus, IT staff, security monitors and supervisors. According to Hsieh and Wang, these are necessary to deter motivated offenders and control and prevent convergence of targets and motivated offenders. Leukfeldt and Yar (2016) explained that guardianship comes in other forms, namely technical and personal. . Leukfeldt and Yar cited installing antivirus as

a technical capable guardian. Leukfeldt and Yar also argued that persons with adequate technical knowledge and aware of the risks they face online can be considered personal capable guardians.

Application to Professional Practice

The research collated the knowledge of IT security managers with a combined practical experience of over 20 years on blockchain applications security. The practical experience captured may guide practicing IT security managers in implementing or maintaining blockchain applications that could reduce the risk of security breaches. In general, the study will add to the body of knowledge of blockchain application security. Specifically, the research findings may increase the understanding of blockchain application security requirements and may also act as a guide to securely deploy Blockchain applications. Also, the study may be used as a security reference framework in administering blockchain application systems. The themes that emerged from the study could be used as focused areas that security managers can consider in implementing blockchain application systems to reduce security breaches. For example, if security managers focused on traditional security control, which is the third theme, most blockchain risks could be eliminated. For instance, Zhang et al. (2019) argued that although by design, blockchain has the three basic security properties, consistency, tamper-resistance, and resistance to DDoS attacks, additional traditional security control is critical for successful protection against threats. Another observation by Erfani and Ahmadi (2019) is that although blockchain protocols may be secure, their security does not extend to all parts and services that deal with the blockchain applications. Erfani and Ahmadi proposed additional security layers that incorporate non-blockchain specific structures such as

traditional security control. In fact, according to Chia et al. (2018), common operational security-related incidents accounted for 66% of current blockchain security breaches.

The first theme, which is cryptographic key management as a focus area for IT security managers, cannot be over-emphasized. According to Boireau (2018), in blockchain applications, the digital assets and their protection are combined into one token. No one can have access to digital assets unless they have private keys. Boireau further explained that protection for cryptographic keys remains at the top of security concerns raised by companies and individuals in blockchain applications. A survey by Greenwich Associates indicated that 58% of participants agreed that HSMs are an essential part of addressing blockchain security concerns (Boireau, 2018). The survey result supports the cryptographic key management focus area discussed in the findings of the study.

The second theme, which is software auditing, a focus in the area is critical to ensure both intentional and accidental errors are eliminated before a blockchain application is published or used. As illustrated by He et al. (2020), software vulnerability has caused hackers to steal several millions of dollars from blockchain applications such as smart contracts. He et al. suggested that audit is the surest way to detect any security vulnerability before publishing a Smart contract. Once a Smart Contract is published, it is impossible to correct bugs due to the immutability property of the blockchain system. In a paper, "Blockchain Is not as Unbreakable as You Think," Madnick (2020) articulated that adding information or using existing information in a blockchain requires software codes. Like any other software, the code is prone to flaws. IT security managers should therefore use the same level of

care that professional developers have established for conventional systems (Madnick, 2020). In that regard, he suggested that an independent software firm should review and verify blockchain application software before it is put to use.

Implications for Social Change

Organizations and individuals can use the study's findings to drive a positive change in society by ensuring that their clients' information and assets in blockchain application are protected. The positive change that can be derived in the findings is three fold, which are: (a) improving the confidence in the blockchain technology, (b) reducing data breaches in blockchain, and (c) reducing cryptocurrencies theft in blockchain.

Blockchain technology have the ability to support an endless number of innovative use in finance, trading, healthcare, governance, and other critical, valuable applications that will positively help society. However, recent high-profile breaches of blockchain systems represent a security weakness in the technology that must be addressed before the technology can reach its full potential (Boireau, 2018). Using the study's findings will help address these security concerns, which will then propel the blockchain technology acceptance by the mainstream users.

For example, using a secure blockchain application for the health industry will help ensure the security of the EHR systems, which will significantly benefit patients, doctors, and health institutions. According to Shi et al. (2020), exiting EHR systems is prone to a single point of failure. However, with a secure blockchain-based EHR, the risk of a single point of failure will be eliminated due to the distributed nature of blockchain. Aside from the single point of failure, Sharma and Balamurugan (2020) pointed out that current EHR systems have become more vulnerable to attacks by

unauthorized users due to advancements in technology. Sharma and Balamurugan proposed that a blockchain-based EHR will efficiently store the records and secure them over the network due to the inherent properties of blockchain.

The findings can also be used to reduce data breaches. Data breaches have a severe negative impact on society. According to Klaus and Elzweig (2020), the average cost of data breaches to organizations is about \$3.6 Million. In addition to the direct cost, there may be indirect costs such as loss of customer trust and heavy toll on the support team who work long hours addressing the data breach. Also, customers whose data has been leaked become anxious about the impact of their leaked data on their lives. Therefore, addressing data breaches may positively impact organizations, individuals, and society.

Application of the findings could also be used to prevent or reduce cryptocurrency theft. In recent times, there has been massive theft of digital assets, specifically cryptocurrencies. Theft of cryptocurrencies have severe replications for society. For example, companies could go bankrupt, causing many employees, dependents, and individuals to lose their livelihood. Bischooping (2018) argued that cryptocurrencies theft has a crippling effect on individuals, institutions, and the economy. According to Zaytoun (2019), cryptocurrencies theft in the last four years is well over \$3.5 billion and has the potential for colossal economic loss. Besides, cryptocurrencies theft undermines the universal principle of any organized society. Therefore, a reduction in cryptocurrencies theft incidents will have a positive impact on society as a whole.

Recommendations for Action

My participants posited that, even though blockchain systems have some inherent security features, organizations and individuals should be mindful that blockchain systems are prone to the same security risks as traditional systems. Besides, blockchain systems have blockchain-specific security threats. Therefore, Information system professionals who are deploying Blockchain applications should combine traditional security controls and Blockchain-specific security controls in the following ways.

- Security frameworks have structures containing processes and technologies that organizations can use to protect their networks and computer systems from security threats at the primary level. The study suggests that organizations should put traditional IT security controls in place by following established standards such as NIST and ISO/IEC 2700 series, or any equivalent standard that is suitable for the institution in question. IT security managers should also apply blockchain-specific security frameworks such as the IBM blockchain framework or CCSS. However, at the time of writing this paper, there were no national or global standards for the blockchain security framework, but the IBM and CCSS framework can be used as a starting point.
- Cryptographic features used in blockchain technology give it inherent security properties such as data integrity. An essential component of the security feature is the cryptographic keys used in signing and as a claim of ownership to a digital asset. Once one loses the key, especially the private key, either through theft or accident, all assets will be lost and inaccessible, sometimes for good. Because blockchain transactions are traceable but not reversible, IT

security managers should use key management system to reduce unauthorized access to digital assets. The study's findings suggested a key management system that makes use of HSM. Applying standards such as The Federal Information Processing Standards (FIPS) and CCSS will significantly improve cryptographic key protection.

- Server, Infrastructure, and software vulnerabilities account for about 90% of recent attacks on blockchain systems (Zamani et al., 2020). The findings suggested that IT security managers and software developers should establish a comprehensive software auditing system to test and ensure all software related to the blockchain is safe from vulnerabilities and malware before deployment. Existing standards such as Consortium for IT Software Quality (CISQ) could be used to support secure software development. Blockchain-specific applications such as smart contracts could benefit from HashEx smart contract audit framework and ConsenSys best practices guide to audit smart contract applications. Automated software auditing tools such as Oyente, Mythril, and Porosity can also make the auditing efficient.
- Blockchain is a novel technology, and not many experts exist; it is still an evolving technology. Therefore, if developers, users, and implementers are not knowledgeable on the subject matter, grave mistakes could be made. Therefore, I will recommend training all stakeholders in a blockchain-related project to ensure both the technical team and administrators understand the technology, risks, and mitigation methods.

I aim to communicate the findings of the study through academic publications, personal blogs, and websites. I will also give seminars in colleges in my home country

Ghana and beyond when the opportunity arises. Finally, I will share the findings with the partnering organizations for this research.

Recommendations for Further Study

Blockchain technology is relatively new and still evolving; not much information exists on the technology. From the study, I identified a lack of standards and awareness training for the blockchain technology that should be further researched. Because there are no universally accepted standards, organizations try to use existing standards that are not meant for blockchain technology and may lead to inefficiencies and vulnerabilities in deployed blockchain systems. A standard or framework that is blockchain specific and accepted by the blockchain community will significantly help the body of knowledge. As indicated, the technology is new to users, implementers, and developers, and without in-depth training, mistakes are bound to happen. Further research into training and awareness programs that will provide requisite standardized knowledge for various stakeholders in the Blockchain eco system will reduce risks associated with errors made by individuals and organizations. Also, one of my limitations is the limited number of organizations that were used for the research. I believe the number of organizations using blockchain technology will increase with time and therefore a further research with increased number of partnering organizations will ensure a more trustworthy outcome.

Reflections

The research journey has been an exciting one, especially amid a pandemic. Initially, I underestimated the recruitment phase of the study, and it turned out to be very challenging. Getting organizations to participate was very challenging. What made it worse is that the blockchain industry is at its infant stage, and not many

companies are into it. The initial plan was to meet some of the participants physically. However, due to the pandemic, the interview had to be done online in both asynchronous and synchronous modes. Therefore, one could not capture the nonverbal communications, which are essential to complement the verbal data collection. Nevertheless, I took steps to ensure credible data was collected by asking the same question from different angles and ensuring verbatim transcription. To control the personal biases, I remained open-minded to assimilate any new idea that might crop up. For example, I discovered that blockchain-specific vulnerability accounted for far less of the total attacks on blockchain than I expected. Even though the online mode of interviewing was largely successful, there were some pertinent issues like not getting immediate responses and delays in confirming meanings, especially with the asynchronous meetings. These issues prolonged the data collection phase.

Summary and Conclusions

Blockchain technology is a game-changer in many industries, but security concerns must be addressed before the technology can reach its full potential. Organization leaders must be aware that even though blockchain systems have some fundamental security properties, it is not enough to make blockchain secure out of the box. Blockchain systems have the same antecedents as other entities that attract cybercriminals, as theorized by the routine activity theory. That is to say, the blockchain systems have value and therefore can attract motivated criminals if no capable guardian exists to prevent the attack. IT security managers' strategies in deploying secure Blockchain applications include traditional security controls, cryptographic key management systems, and a comprehensive software auditing

system. These measures act as capable guardians to prevent attacks on blockchain systems. To implement these controls, organization leaders must adopt relevant traditional IT security frameworks and standards in addition to an acceptable blockchain-related security framework. A secured blockchain application system gives assurance to organizations and users who have less worry knowing that their digital properties are safe in the blockchain.

References

- Aarsand, L., & Aarsand, P. (2019). Framing and switches at the outset of qualitative research interviews. *Qualitative Research, 19*(6), 635-6652.
<https://doi.org/10.1177/1468794118816623>
- Abhishta, A., Junger, M., Joosten, R., & Nieuwenhuis, L. J. M. (2019). Victim routine influences the number of DDoS attacks: Evidence from Dutch educational network. 2019 IEEE Security and Privacy Workshops, 242-247.
<https://doi.org/10.1109/SPW.2019.00052>
- Adam, T., Marquart, J., & Mullings, J. (2005). Fraud and the American dream: Toward an understanding of fraud victimization. *Deviant Behavior, 26*(6), 601-620. <https://doi.org/10.1080/01639620500218294>
- Adashi, E. Y., Walters, L. B., & Menikoff, J. A. (2018). The Belmont Report at 40: Reckoning with time. *American Journal of Public Health, 108*(10), 1345-1348. <https://doi.org/10.2105/AJPH.2018.304580>
- Aguinaldo, J. P. (2004). Rethinking validity in qualitative research from a social constructionist perspective: From 'is this valid research?' to 'what is this research valid for?' *Qualitative Report, 9*(1), 127-136.
<https://doi.org/10.46743/2160-3715/2004.1941>
- Ahmed, M., & Pathan, A. (2020). Blockchain: Can it be trusted? *Computer, 53*(4), 316-35. <https://doi.org/10.1109/MC.2019.2922950>
- Akers, R. L. (1998). Social learning and social structure: A general theory of crime and deviance. Northeastern University Press.
- Akinyode, B. F. (2018). Step by step approach for qualitative data analysis. *International Journal of Built Environment and Sustainability, 5*(3).

<https://doi.org/10.11113/ijbes.v5.n3.267>

- Alase, A. (2017). The interpretative phenomenological analysis: A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies*, 5(2), 9619. <https://doi.org/10.7575/aiac.ijels.v.5n.2p.9>
- Aldhouse, N. V., & Kitchen, H. (2018). Assessing quality in qualitative research to understand disease burden: What tools are available? *Value in Health*, 21, S230. <https://doi.org/10.1016/j.jval.2018.04.1556>
- Ali, R. S., & Alaa, F. A. K. (2018). Security protocol of keys management system for transmission encrypted data. *International Journal of Computer Network & Information Security*, 10(1), 10617. <https://doi.org/10.5815/ijcnis.2018.01.02>
- 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), 165. <https://doi.org/10.5195/jmla.2019.615>
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallen, P., & Peacock, A. (2018). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, 100, 1436174. <https://doi.org/10.1016/j.rser.2018.10.014>
- Andriole, S. J. (2020). Blockchain, cryptocurrency, and cybersecurity. *IT Professional*, 22(1), 13616. <https://doi.org/10.1109/MITP.2019.2949165>
- Anita, N., & Vijayalakshmi, M. (2019). Blockchain security attack: A brief survey. 2019 10th International Conference on Computing, Communication and Networking Technologies, 166. <https://doi.org/10.1109/ICCCNT45670.2019.8944615>
- Arsel, Z. (2017). Asking questions with reflexive focus: A tutorial on designing and

conducting interviews. *Journal of Consumer Research*, 44(4), 9396948.

<https://doi.org/10.1093/jcr/ucx096>

Averin, A., & Averina, O. (2019). Review of blockchain technology vulnerabilities and blockchain-system attacks. 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 166.

<https://doi.org/10.1109/FarEastCon.2019.8934243>

Baker, W. H., & Wallace, L. (2007). Is information security under control?

Investigating quality in information security management. *IEEE Security & Privacy, Security & Privacy*, 5(1), 36644.

<https://doi.org/10.1109/MSP.2007.11>

Bandara, W., Fernandez, W., & Rowlands, B. (2012). Qualitative methods in IS/IT research: Issues, contributions and challenges ? Forward. *Australasian Journal of Information Systems*, 17(2). <https://doi.org/10.3127/ajis.v17i2.784>

Barratt, M. J., Potter, G. R., Wouters, M., Wilkins, C., Werse, B., Perala, J., Pedersen, M. M., Nguyen, H., Malm, A., Lenton, S., Korf, D., Klein, A., Heyde, J., Hakkarainen, P., Frank, V. A., Decorte, T., Bouchard, M., & Blok, T. (2015). Lessons from conducting trans-national Internet-mediated participatory research with hidden populations of cannabis cultivators. *International Journal of Drug Policy*, 26(3), 2386249.

<https://doi.org/10.1016/j.drugpo.2014.12.004>

Barrett, D. (2018, July 1). Data collection in qualitative research. *Evidence-Based Nursing*, 21(3), 63664. <https://doi.org/10.1136/eb-2018-102939>

Barsdorf, N. W., & Wassenaar, D. R. (2005). Racial differences in public perceptions of voluntariness of medical research participants in South Africa. *Social*

Science & Medicine, 60(5), 108761098.

<https://doi.org/10.1016/j.socscimed.2004.06.039>

Baumbusch, J. (2010). Semi-structured interviewing in practice-close research.

Journal for Specialists in Pediatric Nursing 15(3), 2556258.

<https://doi:10.1111/j.1744-6155.2010.00243.x>

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member Checking:

A Tool to Enhance Trustworthiness or Merely a Nod to Validation?

Qualitative Health Research, 26(13), 180261811.

<https://doi.org/10.1177/1049732316654870>

Bischooping, G. (2018). Prosecuting Cryptocurrency Theft with the Defend Trade

Secrets Act of 2016. *University of Pennsylvania Law Review*, (1), 239.

<https://www.pennlawreview.com/wp-content/uploads/2020/04/167-U-Pa-L-Rev-239.pdf>

Bleiker, J., Morgan-Trimmer, S., Knapp, K., & Hopkins, S. (2019). Navigating the maze: Qualitative research methodologies and their philosophical foundations.

Radiography, 25 Suppl 1, S46S8. <https://doi.org/10.1016/j.radi.2019.06.008>

Boireau, O. (2018). Securing the Blockchain against hackers. *Network Security*,

2018(1), 8611. [https://doi.org/10.1016/S1353-4858\(18\)30006-0](https://doi.org/10.1016/S1353-4858(18)30006-0)

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method.

Qualitative Research Journal (RMIT Training Pty Ltd Trading as RMIT Publishing), 9(2), 27640. <https://doi.org/10.3316/QRJ0902027>

Broom, A. (2005). Using qualitative interviews in CAM research: A guide to study

design, data collection and data analysis. *Complementary Therapies in*

Medicine, 13(1), 65. <https://doi.org/10.1016/j.ctim.2005.01.001>

- Burruss, G. W., Bossler, A. M., & Holt, T. J. (2012). Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy. *Crime and Delinquency*, 59(5), 1157-1184.
<https://doi.org/10.1177/0011128712437915>
- Cai, Z., Du, C., Gan, Y., Zhang, J., & Huang, W. (2018). Research and Development of Blockchain Security. *International Journal of Performability Engineering*, 14(9), 204062047. <https://doi.org/10.23940/ijpe.18.09.p12.20402047>
- Campbell, S. (2015). Conducting Case Study Research. *Clinical Laboratory Science*, 28(3), 2016205. <https://doi.org/10.29074/ascls.28.3.201>
- Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2019). Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digital Communications and Networks*.
<https://doi.org/10.1016/j.dcan.2019.12.001>
- Carcary, M. (2009). The Research Audit Trial -- Enhancing Trustworthiness in Qualitative Inquiry. *Electronic Journal of Business Research Methods*, 7(1), 11623.
https://www.researchgate.net/publication/228667678_The_Research_Audit_Trial-Enhancing_Trustworthiness_in_Qualitative_Inquiry
- Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). *The Use of Triangulation in Qualitative Research*. *Oncology Nursing Forum*, 41(5), 5456547. <https://doi.org/10.1188/14.ONF.545-547>
- Catalini, C. (2018). Blockchain Technology and Cryptocurrencies: Implications for the Digital Economy, Cybersecurity, and Government. *Georgetown Journal of International Affairs*, 19, 36642. <https://doi.org/10.1353/gia.2018.0005>

- Chavez-Dreyfuss, G. (2018, October 10). Cryptocurrency theft hits nearly \$1 billion in first nine months: Report. <https://www.reuters.com/article/us-cryptocurrency-crime/cryptocurrency-theft-hits-nearly-1-billion-in-first-nine-months-report-idUSKCN1MK1J2?il=0>
- Chenail, R. J. (2011). Interviewing the Investigator: *Strategies for Addressing Instrumentation and Researcher Bias Concerns in Qualitative Research*. *The Qualitative Report*, 16(1), 255-262. <http://nsuworks.nova.edu/tqr/vol16/iss1/16>
- Chia, V., Hartel, P., Hum, Q., Ma, S., Piliouras, G., Reijnsbergen, D., Staalduinen, M. V., & Szalachowski, P. (2018). Rethinking Blockchain Security: Position Paper. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1273-1280, https://doi.org/10.1109/Cybermatics_2018.2018.00222.
- Choo, K.-K. R. (2011). The cyber threat landscape: *Challenges and future research directions*. *Computers & Security*, 30(8), 7196731. <https://doi.org/10.1016/j.cose.2011.08.004>
- Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A. S. M., Alazab, M., & Watters, P. (2019). A Comparative Analysis of Distributed Ledger Technology Platforms. *IEEE Access*, Access, IEEE, 7, 1679306-167943. <https://doi.org/10.1109/ACCESS.2019.2953729>
- Clark, K. R., & Vealé, B. L. (2018). Strategies to Enhance Data Collection and Analysis in Qualitative Research. *Radiologic Technology*, 89(5), 482CT6-485CT.

- Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing*, 70(3), 4736475. <https://doi.org/10.1111/jan.12163>
- Cohen, L. E., & Felson, M. (1979). "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44:5886608.
- Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE COMMUNICATIONS SURVEYS AND TUTORIALS*, 20(4), 341663452. <https://doi.org/10.1109/COMST.2018.2842460>
- Cridland, E. K., Jones, S. C., Caputi, P., & Magee, C. A. (2015). Qualitative research with families living with autism spectrum disorder: recommendations for conducting semi-structured interviews. *Journal of Intellectual & Developmental Disability* 40(1), 78691. <https://doi.org/10.3109/13668250.2014.964191>
- Crosser, N. (2018). Initial Coin Offerings as Investment Contracts: Are Blockchain Utility Tokens Securities? *University of Kansas Law Review*, (2), 379. <https://doi.org/10.17161/1808.27486>
- Cupit, C., Mackintosh, N., & Armstrong, N. (2018). Using ethnography to study improving healthcare: reflections on the "ethnographic" label. *BMJ Quality & Safety*, 27(4), 2586260. <https://doi.org/10.1136/bmjqs-2017-007599>
- Cutcliffe, J. R., & McKenna, H. P. (2004). METHODOLOGICAL ISSUES IN NURSING RESEARCH Expert qualitative researchers and the use of audit trails. *Journal of Advanced Nursing (Wiley-Blackwell)*, 45(2), 1266133. <https://doi.org/10.1046/j.1365-2648.2003.02874.x>
- Cypress, B. (2017). Rigor or Reliability and Validity in Qualitative Research:

Perspectives, Strategies, Reconceptualization, and Recommendations.

Dimensions of Critical Care Nursing, 36, 253-263.

<https://doi.org/10.1097/DCC.0000000000000253>

Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. 2017 4th International Conference on Systems and Informatics (ICSAI), Systems and Informatics (ICSAI), 2017 4th International Conference On, 9756979.

<https://doi.org/10.1109/ICSAI.2017.8248427>

Daly, D., Hannon, S., & Brady, V. (2019). Motivators and challenges to research recruitment ó A qualitative study with midwives. *Midwifery*, 74, 14620.

<https://doi.org/10.1016/j.midw.2019.03.011>

De Rossi, L. M., Abbatemarco, N., & Gianluca, S. (2019). Towards a Comprehensive Blockchain Architecture Continuum. Proceedings of the 52nd Hawaii International Conference on System Sciences.

<https://doi.org/10.24251/HICSS.2019.557>

Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., & Hierons, R. (2018). Smart contracts vulnerabilities: a call for blockchain software engineering? 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Blockchain Oriented Software Engineering (IWBOSE), 2018 International Workshop On, 19625.

<https://doi.org/10.1109/IWBOSE.2018.8327567>

di Angelo, M., & Salzer, G. (2020). Characteristics of Wallet Contracts on Ethereum. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Blockchain Research & Applications for

Innovative Networks and Services (BRAINS), 2020 2nd Conference On, 2326
239. <https://doi.org/10.1109/BRAINS49436.2020.9223287>

Di Silvestre, M. L., Gallo, P., Ippolito, M. G., Musca, R., Riva Sanseverino, E., Tran, Q. T. T., & Zizzo, G. (2019). Ancillary Services in the Energy Blockchain for Microgrids. *IEEE Transactions on Industry Applications, Industry Applications*, IEEE Transactions on, IEEE Trans. on Ind. *Applicat*, 55(6), 731067319. <https://doi.org/10.1109/TIA.2019.2909496>

Drawve, G., Thomas, S., & Walker, J. (2014). The Likelihood of Arrest: A Routine Activity Theory Approach. *American Journal of Criminal Justice*, 39(3), 4506
470. <https://doi.org/10.1007/s12103-013-9226-2>

Easley, D., O'Hara, M., & Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134(1), 916109.
<https://doi.org/10.1016/j.jfineco.2019.03.004>

Ebneyamini, S., & Moghadam, M. R. S. (2018). Toward Developing a Framework for Conducting Case Study Research. *International Journal of Qualitative Methods*, 17(1). <https://doi.org/10.1177/1609406918817954>

Eck, J. E. (2003). Police problems: The complexity of problem theory, research and evaluation. *Crime Prevention Studies* 15: 796113.
https://www.researchgate.net/publication/228531940_Police_problems_The_complexity_of_problem_theory_research_and_evaluation

Elaldi, S., & Yerliyurt, N. S. (2017). The Efficacy of Drama in Field Experience: A Qualitative Study Using MAXQDA. *Journal of Education and Learning*, 6(1), 10626. <https://doi.org/10.5539/jel.v6n1p10>

Erfani, S., & Ahmadi, M. (2019). Bitcoin Security Reference Model: An

- Implementation Platform. 2019 International Symposium on Signals, Circuits and Systems (ISSCS), Signals, Circuits and Systems (ISSCS), 2019 International Symposium On, 165.
<https://doi.org/10.1109/ISSCS.2019.8801796>
- Everett, J., Neu, D., Rahaman, A. S., & Maharaj, G. (2015). Praxis, doxa and research methods: Reconsidering critical accounting. *Critical Perspectives on Accounting*, 32, 37644. <https://doi.org/10.1016/j.cpa.2015.04.004>
- Extance, A. (2015). The future of cryptocurrencies: Bitcoin and beyond. *Nature*, 526(7571), 21623. <https://doi.org/10.1038/526021a>
- Farquhar, J., Michels, N., & Robson, J. (2020). Triangulation in industrial qualitative case study research: Widening the scope. *Industrial Marketing Management*, 87, 1606170. <https://doi.org/10.1016/j.indmarman.2020.02.001>
- Farrugia, B. (2019). WASP (write a scientific paper): Sampling in qualitative research. *Early Human Development*, 133, 69671.
<https://doi.org/10.1016/j.earlhumdev.2019.03.016>
- Felson, M., & Boba, R. L. (2010). *Crime and Everyday Life* (4th ed.). Sage.
<https://doi.org/10.4135/9781483349299>
- Felson, M., & Clarke, V. (1998). *Opportunity Makes a Thief*. Police Research Series, Paper 98. British Home Office Research Publications.
<https://doi.org/10.4324/9781315060965-14>
- Feng, L., Zhang, H., Chen, Y., & Lou, L. (2018). Scalable Dynamic Multi-Agent Practical Byzantine Fault-Tolerant Consensus in Permissioned Blockchain. *Applied Sciences-Basel*, 8(10). <https://doi.org/10.3390/app8101919>
- Fisch, C. (2019). Initial coin offerings (ICOs) to finance new ventures. *Journal of*

Business Venturing, 34(1), 1622.

<https://doi.org/10.1016/j.jbusvent.2018.09.007>

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning*, 11(2), 2116217.

<https://doi.org/10.1016/j.cptl.2018.11.014>

Foss, N. J., & Hallberg, N. L. (2014). How symmetrical assumptions advance strategic management research. *Strategic Management Journal*, 35, 903-913.

<https://doi.org/10.1002/smj.2130>

Freilich, J. D., Chermak, S. M., & Klein, B. R. (2020). Investigating the applicability of situational crime prevention to the public mass violence context.

Criminology & Public Policy, 19(1), 2716293. <https://doi.org/10.1111/1745-9133.12480>

Fusch, P. I., & Ness, L. R. (2015). Are We There Yet? Data Saturation in Qualitative Research. *Qualitative Report*, 20(9), 140861416.

<https://doi.org/10.46743/2160-3715/2015.2281>

Galan-Diaz, C. (2017). Conference Report: 18th Conference on Computer-Assisted Qualitative Data Analysis (CAQD) 2016: MAXQDA User Conference.

Forum: *Qualitative Social Research*, 18(1). <https://doi.org/10.17169/fqs-18.1.2786>

Galen, D. J., Brand, N., Boucherle, L., Davis, R., Do, N., El-Baz, B., Kimura, I., Wharton, K., & Lee, J. (2018, April 11). Blockchain for Social Impact.

https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype_0.pdf

Gao, S., Yu, T., Zhu, J., & Cai, W. (2019). T-PBFT: An EigenTrust-based practical

Byzantine fault tolerance consensus algorithm. *China Communications, Communications, China, China Commun*, 16(12), 1116123.

<https://doi.org/10.23919/JCC.2019.12.008>

Gelling, L. (2020). Research ethics in real world research. *Journal of Clinical Nursing (John Wiley & Sons, Inc.)*, 29(7/8), 101961022.

<https://doi.org/10.1111/jocn.15083>

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, 163.

<https://doi.org/10.1016/j.jnca.2020.102635>

Golafshani, N. (2003). Understanding reliability and validity in qualitative research.

The Qualitative Report, 8(4), 597-606. <http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf>

Gottschalk, P. (2018). "Approaches to the Empirical Study of Convenience Theory for White-Collar Crime." *Deviant Behavior* 39:1600614.

<https://doi:10.1080/01639625.2017.1410623>.

Government Publishing Office. (2018). Beyond bitcoin: Emerging applications for Blockchain technology. Joint Hearing.

<https://docs.house.gov/meetings/SY/SY21/20180214/106862/HHRG-115-SY21-20180214-SD004.pdf>

Green, C. A., Duan, N., Gibbons, R. D., Hoagwood, K. E., Palinkas, L. A., & Wisdom, J. P. (2015). Approaches to mixed methods dissemination and implementation research: Methods, strengths, caveats, and opportunities. *Administration and Policy in Mental Health and Mental Health Services*

Research, 42, 508. <https://doi.org/10.1007/s10488-014-0552-6>

- Grysmen, A., & Lodi-Smith, J. (2019). Methods for Conducting and Publishing Narrative Research With Undergraduates. *Frontiers in Psychology*.
<https://doi.org/10.3389/fpsyg.2018.02771>
- Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLoS ONE*, 15(5), 1617.
<https://doi.org/10.1371/journal.pone.0232076>
- Halcomb, E. J., & Davidson, P. M. (2006). Is verbatim transcription of interview data always necessary? *Applied Nursing Research*, 19(1), 38642.
<https://doi.org/10.1016/j.apnr.2005.06.001>
- Harwati, L. N. (2019). Ethnographic and Case Study Approaches: Philosophical and Methodological Analysis. *International Journal of Education and Literacy Studies*, 7(2), 1506155. <https://doi.org/10.7575/aiac.ijels.v.7n.2p.150>
- Hathcoat, J., & Nicholas, M. (2014). Epistemology. *The Sage Action Research*, 5, 303-307. Sage Publications Ltd. <https://doi.org/10.4135/9781446294406.n108>
- Hawdon, J., Costello, M., Ratliff, T., Hall, L., & Middleton, J. (2017). Conflict Management Styles and Cybervictimization: Extending Routine Activity Theory. *Sociological Spectrum*, 37:4, 250-266,
<https://doi.org/10.1080/02732173.2017.1334608>
- Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. *American Journal of Criminal Justice*, 45(4), 5466562. <https://doi.org/10.1007/s12103-020-09534-4>
- He, D., Deng, Z., Zhang, Y., Chan, S., Cheng, Y., & Guizani, N. (2020). Smart

- Contract Vulnerability Analysis and Security Audit. *IEEE Network, Network, IEEE*, 34(5), 2766282. <https://doi.org/10.1109/MNET.001.1900656>
- Headley, M. G., & Plano Clark, V. L. (2020). Multilevel Mixed Methods Research Designs: Advancing a Refined Definition. *Journal of Mixed Methods Research*, 14(2), 1456163. <https://doi.org/10.1177/1558689819844417>
- Hinduja, S., Kooi, B., Reynolds, B. W., & Henson, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, 4, 383. <https://doi.org/10.1057/sj.2013.25>
- Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The Capable Guardian in Routine Activities Theory: A Theoretical and Conceptual Reappraisal. *Crime Prevention and Community Safety* 15(1):65679. <https://doi.org/10.1057/cpcs.2012.14>
- Holotescu, C. C. (2018). Understanding Blockchain Opportunities and Challenges. *ELearning & Software for Education*, 4, 2756283. <https://doi.org/10.12753/2066-026X-18-253>
- Homoliak, I., Venugopalan, S., Hum, Q., & Szalachowski, P. (2019). A Security Reference Architecture for Blockchains, 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, pp. 390-397. <https://doi.org/10.1109/Blockchain.2019.00060>
- Hsieh, M., & Wang, S. K. (2018). Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree. *International Journal of Cyber Criminology*, 3336352. <https://doi.org/10.5281/zenodo.1467935>
- Hu, W., Fan, Z., & Gao, Y. (2019). Research on Smart Contract Optimization Method on Blockchain. *IT Professional, IT Prof*, 21(5), 33638.

<https://doi.org/10.1109/MITP.2019.2923604>

Huang, Y. C., Lei, R. L., Lei, R. W., & Ibrahim, F. (2020). An exploratory study of dignity in dementia care. *Nursing Ethics*, 27(2), 433.

<https://doi.org/10.1177/0969733019849458>

Hufford, D. J. (1996). Culturally grounded review of research assumptions.

Alternative Therapies In Health And Medicine, 2(4), 47653.

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin:

What blockchain and distributed ledger technologies mean for firms. *Business*

Horizons, 62(3), 2736281. <https://doi.org/10.1016/j.bushor.2019.01.002>

Ismail, L., & Materwala, H. (2019). A Review of Blockchain Architecture and

Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry*, 10,

1198. <https://doi.org/10.3390/sym11101198>

Jacobson, R. M., Hanson, W. E., & Zhou, H. (2015). Canadian psychologists' test

feedback training and practice: A national survey. *Canadian Psychology*, 56,

394-404. <https://doi.org/10.1037/cap0000037>

Jaoude, A. J., & Saade, R. G. (2019). Blockchain Applications ó Usage in Different

Domains. *IEEE Access*, *Access, IEEE*, 7, 45360645381.

<https://doi.org/10.1109/ACCESS.2019.2902501>

Jeffery, C. R. (1993). Obstacles to the development of research in crime and

delinquency. *Journal of Research in Crime & Delinquency*, 30:491-497.

<https://doi.org/10.1177/0022427893030004010>

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A Review of the Quality Indicators

of Rigor in Qualitative Research. *American Journal of Pharmaceutical*

Education, 84(1), 1386146. <https://doi.org/10.5688/ajpe7120>

- Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72(12), 2954-2965. <https://doi.org/10.1111/jan.13031>
- Kamp, K., Herbell, K., Magginis, W. H., Berry, D., & Given, B. (2019). Facebook Recruitment and the Protection of Human Subjects. *Western Journal of Nursing Research*, 41(9), 1270. <https://doi.org/10.1177/0193945919828108>
- Karagiozis, N. (2018). The Complexities of the Researcher's Role in Qualitative Research: The Power of Reflexivity. *International Journal of Interdisciplinary Educational Studies*, 13(1), 19631. <https://doi.org/10.18848/2327-011X/CGP/v13i01/19-31>
- Kbean, N. A. W., & Sadkhan, S. B. (2020). A Survey on Key management for SCADA. 2020 6th International Engineering Conference on Sustainable Technology and Development (IEC), Sustainable Technology and Development (IEC), 2020 6th International Engineering Conference, 976102. <https://doi.org/10.1109/IEC49899.2020.9122853>
- Keamy-Minor, E., McQuoid, J., & Ling, P. M. (2019). Young adult perceptions of JUUL and other pod electronic cigarette devices in California: a qualitative study. *BMJ Open*, 9(4), 1. <https://doi.org/10.1136/bmjopen-2018-026306>
- Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., & Thompson, C. (2017). A Distributed-Ledger Consortium Model for Collaborative Innovation. *Computer*, 50(9), 29637. <https://doi.org/10.1109/MC.2017.3571057>
- Khatamian Far, P. (2018). Challenges of Recruitment and Retention of University Students as Research Participants: Lessons Learned from a Pilot Study.

Journal of the Australian Library & Information Association, 67(3), 2786292.

<https://doi.org/10.1080/24750158.2018.1500436>

Khosravan, S., Mazlom, B., Abdollahzade, N., Jamali, Z., & Mansoorian, M. R.

(2014). Family participation in the nursing care of the hospitalized patients.

Iranian Red Crescent Medical Journal, 16(1), 1-6.

<https://doi.org/10.5812/ircmj.12868>

Kian, M., & Beach, D. (2019). Implications of Ethnography Research Method in

Educational and Health Studies. *Social Behavior Research & Health*, 3(2),

4196427. <https://doi.org/10.18502/sbrh.v3i2.1788>

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime

Countries. *Social Science Computer Review*, 30(4), 4706486.

<https://doi.org/10.1177/0894439311422689>

Klaus, T., & Elzweig, B. (2020). The impact of data breaches on corporations and the

status of potential regulation and litigation. *Law & Financial Markets Review*,

14(4), 2556260. <https://doi.org/10.1080/17521440.2020.1833432>

Knirsch, F., Unterweger, A., & Engel, D. (2019). Implementing a blockchain from

scratch: why, how, and what we learned. *EURASIP Journal on Information*

Security, 1, 1. <https://doi.org/10.1186/s13635-019-0085-3>

Koskull, C. V. (2020). Increasing rigor and relevance in service research through

ethnography. *Journal of Services Marketing*, 34(1), 74677.

<https://doi.org/10.1108/JSM-03-2019-0143>

Kruth, J. G. (2015). Five qualitative research approaches and their applications in

parapsychology. *The Journal of Parapsychology*, 2, 219.

Kuhn, R., Yaga, D., & Voas, J. (2019). Rethinking Distributed Ledger Technology.

Computer, 52(2), 68672. <https://doi.org/10.1109/MC.2019.2898162>

- Kumar, G., Saha, R., Rai, M. K., Thomas, R., & Kim, T. (2019). Proof-of-Work Consensus Approach in Blockchain Technology for Cloud and Fog Computing Using Maximization-Factorization Statistics. *IEEE Internet of Things Journal*, *6*(4), 683566842. <https://doi.org/10.1109/JIOT.2019.2911969>
- Kuruppuge, R. H., & Gregar, A. (2020). Strategic, Tactical and Operational Decisions in Family Businesses: A Qualitative Case Study. *The Qualitative Report*, *25*(6), 1599-1618. <https://doi.org/10.46743/2160-3715/2020.2945>
- Lee, H., & Choi, K.-S. (2021). Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework. *Victims & Offenders*, *16*(3), 3636384. <https://doi.org/10.1080/15564886.2020.1835764>
- Lee, J., de Guzman, M. C., Talebi, N., Korní, S. K., Szumigala, D., & Rao, H. R. (2018). Use of online information and suitability of target in shoplifting: A routine activity based analysis. *Decision Support Systems*, *110*, 1610. <https://doi.org/10.1016/j.dss.2018.03.001>
- Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to Do Qualitative Data Analysis: A Starting Point. *Human Resource Development Review*, *19*(1), 94. <https://doi.org/10.1177/1534484320903890>
- Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 2636280. <https://doi.org/10.1080/01639625.2015.1012409>
- Leung, L. (2015). Validity, reliability, and generalizability in qualitative research.

Journal of Family Medicine and Primary Care, 4(3), 3246327.

<https://doi.org/10.4103/2249-4863.161306>

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of blockchain systems. *Elsevier BV*. <https://doi.org/10.1016/j.future.2017.08.020>

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 8416853.

<https://doi.org/10.1016/j.future.2017.08.020>

Lin, I., & Liao, T. (2017). A Survey of Blockchain Security Issues and Challenges. *I. J. Network Security*, 19, 653-659.

[https://doi.org/10.6633/IJNS.201709.19\(5\).01](https://doi.org/10.6633/IJNS.201709.19(5).01)

Lucas, P., Fleming, J., & Bhosale, J. (2018). The Utility of Case Study as a Methodology for Work-Integrated Learning Research. *International Journal of Work-Integrated Learning*, 19(3), 2156222.

<https://files.eric.ed.gov/fulltext/EJ1196748.pdf>

Mackieson, P., Shlonsky, A., & Connolly, M. (2019). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work*, 18(6), 9656980.

<https://doi.org/10.1177/1473325018786996>

Madnick, S. (2020). Blockchain Isn't as Unbreakable as You Think. *MIT Sloan Management Review*, 61(2), 66670. <https://doi.org/10.2139/ssrn.3542542>

Mandala, M., & Freilich, J. D. (2018). Disrupting Terrorist Assassinations Through Situational Crime Prevention. *Crime & Delinquency*, 64(12), 151561537.

<https://doi.org/10.1177/0011128717718488>

Mandava, A., & Millum, J. (2013). Manipulation in the Enrollment of Research

Participants. *Hastings Center Report*, 43(2), 38647.

<https://doi.org/10.1002/hast.144>

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Sage.

Mather, M. W., Hamilton, D., Robalino, S., & Rousseau, N. (2018). Going where other methods cannot: A systematic mapping review of 25 years of qualitative research in Otolaryngology. *Clinical Otolaryngology : Official Journal of ENT-UK ; Official Journal of Netherlands Society for Oto-Rhino-Laryngology & Cervico-Facial Surgery*, 43(6), 144361453.

<https://doi.org/10.1111/coa.13200>

Megan, L. R., Zachary, F. M., Esther, K. C., Aris, C. G., Comilla, S., Kate Morrow, G., & Craig, N. (2015). Interview-based Qualitative Research in Emergency Care Part II: Data Collection, Analysis and Results Reporting. *Academic Emergency Medicine*, 9, 1103. <https://doi.org/10.1111/acem.12735>

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative Research : A Guide to Design and Implementation: Vol. Fourth edition*. Jossey-Bass.

Mertz, L. (2018). (Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution. *IEEE Pulse*, *Pulse, IEEE*, 9(3), 467. <https://doi.org/10.1109/MPUL.2018.2814879>

Metselaar, S. (2019). Commentary 1: Informed consent of research participants: The gap between regulations and reality. *Journal of Empirical Research on Human Research Ethics*, 14(5), 4336435. <https://doi.org/10.1177/1556264619831589a>

Miró-Llinares, F. (2014). Routine Activity Theory. *The Encyclopedia of Theoretical Criminology*, 167 <https://doi.org/10.1002/9781118517390.wbetc198>

Mohajan, H. K. (2018). *Qualitative Research Methodology in Social Sciences and*

Related Subjects. *Journal of Economic Development, Environment and People*, 7(1), 23648. <https://doi.org/10.26458/jedep.v7i1.571>

Mohammad, T., & Nooraini, I. (2021). Routine activity theory and juvenile delinquency: The roles of peers and family monitoring among Malaysian adolescents. *Children and Youth Services Review*, 121.

<https://doi.org/10.1016/j.childyouth.2020.105795>

Monrat, A. A., Schelen, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access*, 7, 1171346117151.

<https://doi.org/10.1109/ACCESS.2019.2936094>

Moser, A., & Korstjens, I. (2017). Series: Practical guidance to qualitative research.

Part 1: Introduction. *The European Journal Of General Practice*, 23(1), 2716-273. <https://doi.org/10.1080/13814788.2017.1375093>

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), 9618. <https://doi.org/10.1080/13814788.2017.1375091>

Moubarak, J., Filiol, E., & Chamoun, M. (2018). On blockchain security and relevant attacks. 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Communications Conference (MENACOMM), IEEE Middle East and North Africa, 166.

<https://doi.org/10.1109/MENACOMM.2018.8371010>

Murray, R. K., & Roncek, D. W. (2008). Measuring diffusion of assaults around bars through radius and adjacency techniques. *Criminal Justice Review*, 33(2),

1996220. <https://doi.org/10.1177/0734016808316777>

Namey, E., Guest, G., O'Regan, A., Godwin, C. L., Taylor, J., & Martinez, A. (2020).

How Does Mode of Qualitative Data Collection Affect Data and Cost?

Findings from a Quasi-Experimental Study. *Field Methods*, 32(1), 58674.

<https://doi.org/10.1177/1525822x19886839>

Navarro, J. N., & Jasinski, J. L. (2015). Demographic and Motivation Differences

Among Online Sex Offenders by Type of Offense: An Exploration of Routine Activities Theories. *Journal of Child Sexual Abuse*, 24(7), 7536771.

<https://doi.org/10.1080/10538712.2015.1077363>

Network Security. (2018). Crypto-currencies hit by hacking attacks, theft and fraud.

Network Security, 2018(2), 162. [https://doi.org/10.1016/S1353-](https://doi.org/10.1016/S1353-4858(18)30011-4)

[4858\(18\)30011-4](https://doi.org/10.1016/S1353-4858(18)30011-4)

Newman, G. R., & Clarke, R. V. G. (2003). Superhighway robbery. Willan.

<https://doi.org/10.4324/9781843924876>

New South Wales Government. (2018). Routine Activity Theory. Crime Prevention.

http://www.crimeprevention.nsw.gov.au/Documents/routine_activity_factsheet_nov2014.pdf

Nguyen, T. V. (2020). Cybercrime in Vietnam: An Analysis based on Routine

Activity Theory. *International Journal of Cyber Criminology*, 14(1), 1566173.

<https://doi.org/10.5281/zenodo.3747516>

Nicholls, D. (2009). Qualitative research: part one -- philosophies. *International*

Journal of Therapy & Rehabilitation, 16(10), 5266533.

<https://doi.org/10.12968/ijtr.2009.16.10.44562>

Nikitkov, A. N., Stone, D. N., & Miller, T. C. (2014). Internal Controls, Routine

Activity Theory (RAT), and Sustained Online Auction Deception: A

Longitudinal Analysis. *Journal of Information Systems*, 28(1), 3116337.

<https://doi.org/10.2308/isys-50708>

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative.

Research Evidence-Based Nursing, 18, 34-35. <https://doi.org/10.1136/eb-2015-102054>

Nolasco Braaten, C., & Vaughn, M. S. (2019). Convenience theory of cryptocurrency crime: A content analysis of US Federal court decisions. *Deviant Behavior*.

<https://doi.org/10.1080/01639625.2019.1706706>

O'Keefe, J., Buytaert, W., Mijic, A., Brozovic, N., & Sinha, R. (2016). The use of semi-structured interviews for the characterization of farmer irrigation practices. *Hydrology and Earth System Sciences*, 20(5), 191161924.

<https://doi.org/10.5194/hess-20-1911-2016>

Olmes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.

Government Information Quarterly, 34(3), 3556364.

<https://doi.org/10.1016/j.giq.2017.09.007>

Omona, J. (2013). Sampling in Qualitative Research: Improving the Quality of Research Outcomes in Higher Education. *Makerere Journal of Higher*

Education, 4(2), 169-185. <https://doi.org/10.4314/majohe.v4i2.4>

Oni, S., Araife Berepubo, K., Oni, A. A., & Joshua, S. (2019). E-Government and the Challenge of Cybercrime in Nigeria. 2019 Sixth International Conference on EDemocracy & EGovernment (ICEDEG), EDemocracy & EGovernment (ICEDEG), 2019 Sixth International Conference On, 1376142.

<https://doi.org/10.1109/ICEDEG.2019.8734329>

- Onwuegbuzie, A. J., & Corrigan, J. A. (2014). Improving the quality of mixed research reports in the field of human resource development and beyond: A call for rigor as an ethical practice. *Human Resource Development Quarterly*, *25*, 273. <https://doi.org/10.1002/hrdq.21197>
- Opdenakker, R. (2006). Advantages and Disadvantages of Four Interview Techniques in Qualitative Research. *Forum: Qualitative Social Research*, *7*(4). <http://nbn-resolving.de/urn:nbn:de:0114-fqs0604118>.
- Pal, O., Alam, B., Thakur, V., & Singh, S. (2021). Key management for blockchain technology. *ICT Express*, *7*(1), 76680. <https://doi.org/10.1016/j.ict.2019.08.002>
- Panda, S. S., Mohanta, B. K., Satapathy, U., Jena, D., Gountia, D., & Patra, T. K. (2019). Study of Blockchain Based Decentralized Consensus Algorithms. TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Region 10 Conference, TENCON, 2019 - 2019 IEEE, 9086913. <https://doi.org/10.1109/TENCON.2019.8929439>
- Park, J., & Park, M. (2016). Qualitative versus Quantitative Research Methods: Discovery or Justification? *Journal of Marketing Thought*, *3*(1), 167. <https://doi.org/10.15577/jmt.2016.03.01.1>
- Peel, K. L. (2020). A beginner's guide to applied educational research using thematic analysis. *Practical Assessment, Research & Evaluation*, *25*(2), 1615. <https://doi.org/10.7275/ryr5-k983>
- Perez, D., & Livshits, B. (2019). Smart Contract Vulnerabilities: Does Anyone Care? *arXiv, abs/1902.06710*. <https://arxiv.org/pdf/1902.06710v1.pdf>
- Petty, N. J., Thomson, O. P., & Stew, G. (2012). Ready for a paradigm shift? Part 1:

- Introducing the philosophy of qualitative research. *Manual Therapy*, 17(4), 2676274. <https://doi.org/10.1016/j.math.2012.03.006>
- Plano Clark, V. L. (2019). Meaningful integration within mixed methods studies: Identifying why, what, when, and how. *Contemporary Educational Psychology*, 57, 1066111. <https://doi.org/10.1016/j.cedpsych.2019.01.007>
- Ploeg, J. (1999, April 01). Identifying the best research design to fit the question. Part 2: Qualitative designs. September 27, 2020, <http://dx.doi.org/10.1136/ebn.2.2.36>
- Poggrund, R. L., Darst, S., & Munro, M. P. (2015). Initial validation study for a scale used to determine service intensity for itinerant teachers of students with visual impairments. *Journal of Visual Impairment & Blindness (Online)*, 109, 433. <https://doi.org/10.1177/0145482x1510900602>
- Pope, C., & Mays, N. (1995). Reaching the parts other methods cannot reach: an introduction to qualitative methods in health and health services research. *British Medical Journal*, 6996, 42. <https://doi.org/10.1136/bmj.311.6996.42>
- Popescul, L. F., & Jitaru, L. (2017). Research Methods Used in Studies on Management and International Affairs. *Journal of Public Administration, Finance & Law*, 11, 1576162.
- PR Newswire. (2019). Crypto.com Achieves Cryptocurrency Security Standard (Level 3) Compliance. <https://www.prnewswire.com/news-releases/crypto-com-achieves-cryptocurrency-security-standard-level-3-compliance-300922284.html>
- Quaini, T., Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2018). A Model for Blockchain-Based Distributed Electronic Health Records. IADIS International

Journal on WWW/Internet, 16(2), 66679.

https://doi.org/10.33965/ijwi_2018161205

Radhakrishnan, B. L., Joseph, A. S., & Sudhakar, S. (2019). Securing Blockchain based Electronic Health Record using Multilevel Authentication. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Advanced Computing & Communication Systems (ICACCS), 2019 5th International Conference On, 6996703.

<https://doi.org/10.1109/ICACCS.2019.8728483>

Raikwar, M., Gligoroski, D., & Krlevska, K. (2019). SoK of Used Cryptography in Blockchain. *IEEE Access*, *Access, IEEE*, 7, 1485506148575.

<https://doi.org/10.1109/ACCESS.2019.2946983>

Razzaq, A., Khan, M. M., Talib, R., Butt, A. D., Hanif, N., Afzal, S., & Raouf, M. R. (2019). Use of Blockchain in Governance: A Systematic Literature Review. *International Journal of Advanced Computer Science and Applications* 10(5).

<https://doi.org/10.14569/IJACSA.2019.0100585>

Reddick, C. G., Cid, G. P., Ganapati, S., Bolívar, R., & Scholl, H. J. (2019).

Determinants of blockchain adoption in the public sector: An empirical examination. *Information Polity: The International Journal of Government & Democracy in the Information Age*, 24(4), 3796396.

<https://doi.org/10.3233/IP-190150>

Reybold, L. E., Lammert, J. D., & Stribling, S. M. (2012). Participant selection as a conscious research method: thinking forward and the deliberation of emergent findings. *Qualitative Research*, 13(6), 6996716.

<https://doi.org/10.1177/1468794112465634>

- Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 88, 1736190. <https://doi.org/10.1016/j.future.2018.05.046>
- Reyns, B. W., & Henson, B. (2016). The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *International Journal of Offender Therapy & Comparative Criminology*, 60(10), 111961139. <https://doi.org/10.1177/0306624X15572861>
- Roberts, J., & Karras, J. (2019). What is blockchain? *Economic Development Journal*, 18(4), 5610. <https://www.proquest.com/scholarly-journals/what-is-blockchain/docview/2510531714/se-2?accountid=201395>
- Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020). Exploring the Attack Surface of Blockchain: A Comprehensive Survey [Abstract]. *IEEE Communications Surveys & Tutorials*, 22(3), 1977-2008. <https://doi.org/10.1109/comst.2020.2975999>
- Sahin, M. D., & Öztürk, G. (2019). Mixed Method Research: Theoretical Foundations, Designs and Its Use in Educational Research. *International Journal of Contemporary Educational Research*, 6(2), 3016310. <https://doi.org/10.33200/ijcer.574002>
- Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: a routine activity explanation of crime prevention success and failure. *Security Journal*, 1, 37. <https://doi.org/10.1057/sj.2009.17>
- Sanjari, M., Bahramnezhad, F., Khoshnava Fomani, F., Shoghi, M., & Ali Cheraghi, M. (2014). Ethical challenges of researchers in qualitative studies: the

necessity to develop a specific guideline. *Journal of Medical Ethics & History of Medicine*, 7(14), 166.

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences*, 9, 1788.

<https://doi.org/10.3390/app9091788>

Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020). Smart Contract: Attacks and Protections. *IEEE Access, Access, IEEE*, 8, 24416624427.

<https://doi.org/10.1109/ACCESS.2020.2970495>

Schaefer, G., & Wertheimer, A. (2010). The Right to Withdraw from Research. *Kennedy Institute of Ethics journal*. 20. 329-52.

<https://www.muse.jhu.edu/article/413517>.

Schaefer, L., & Mazerolle, L. (2017). Putting process into routine activity theory: Variations in the control of crime opportunities. *SECURITY JOURNAL*, 30(1),

2666289. <https://doi.org/10.1057/sj.2015.39>

Schmidlin, K., Clough-Gorr, K. M., & Spoerri, A. (2015). Privacy preserving probabilistic record linkage (P3RL): A novel method for linking existing healthrelated data and maintaining participant confidentiality. *BMC Medical Research Methodology*, 15(1), 1. <https://doi.org/10.1186/s12874-015-0038-6>

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. *IEEE Access, Access, IEEE*, 7, 1477826147795.

<https://doi.org/10.1109/ACCESS.2019.2946373>

Shaikh, A., & Oliveira, D. (2019). Informal IT and Routine Activity Theory -A Theoretical Review. 2019 SoutheastCon, SoutheastCon, 2019, 164.

<https://doi.org/10.1109/SoutheastCon42311.2019.9020557>

- Sharma, Y., & Balamurugan, B. (2020). Preserving the Privacy of Electronic Health Records using Blockchain. *Procedia Computer Science*, 173, 1716180.
<https://doi.org/10.1016/j.procs.2020.06.021>
- Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, 97.
<https://doi.org/10.1016/j.cose.2020.101966>
- Shrivastava, M. K., Yeboah, T., & Brunda, S. S. (2020). Hybrid Security Framework for Blockchain Platforms. 2020 First International Conference on Power, Control and Computing. <https://doi.org/10.1109/icpc2t48082.2020.9071477>
- Shufutinsky, A. (2020). Employing Use of Self for Transparency, Rigor, Trustworthiness, and Credibility in Qualitative Organizational Research Methods. *OD Practitioner*, 52(1), 50658.
- Sikkens, E., Van San, M., Sieckelinck, S., Boeije, H., & de Winter, M. (2017). Participant Recruitment through Social Media: Lessons Learned from a Qualitative Radicalization Study Using Facebook. *FIELD METHODS*, 29(2), 1306139. <https://doi.org/10.1177/1525822X16663146>
- Singh, K. D. (2015). Creating Your Own Qualitative Research Approach: Selecting, Integrating and Operationalizing Philosophy, Methodology and Methods. *Vision (09722629)*, 19(2), 1326146.
<https://doi.org/10.1177/0972262915575657>
- Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Contemporary Computing and Informatics (IC3I), 2016

2nd International Conference On, 4636467.

<https://doi.org/10.1109/IC3I.2016.7918009>

Sivanathan, A., Habibi Gharakheili, H., & Sivaraman, V. (2020). Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning. *IEEE Transactions on Network and Service Management, Network and Service Management*, IEEE Transactions on, *IEEE Trans. Netw. Serv. Manage*, 17(1), 60674. <https://doi.org/10.1109/TNSM.2020.2971213>

Sorce, G. (2019). Institutional ethnography for communication and media research. *Communication Review*, 22(4), 2966308. <https://doi.org/10.1080/10714421.2019.1659703>

Söylemez, Y. (2018). The Development of the Text Evaluation Scale for Child Rights: A Study of Validity and Reliability. *World Journal of Education*, 8(5), 1396159. <https://doi.org/10.5430/wje.v8n5p139>

Stavros, C., & Westberg, K. (2009). Using triangulation and multiple case studies to advance relationship marketing theory. *Qualitative Market Research: An International Journal*, 12(3), 3076320. <https://doi.org/10.1108/13522750910963827>

Stylianou, S. (2002). the relationship between elements and manifestations of low self-control in a general theory of crime: two comments and a test. *Deviant Behavior*, 23(6), 5316557. <https://doi.org/10.1080/01639620290086512>

Suri, H. (2011). Purposeful Sampling in Qualitative Research Synthesis. *Qualitative Research Journal (RMIT Training Pty Ltd Trading as RMIT Publishing)*, 11(2), 63675. <https://doi.org/10.3316/QRJ1102063>

Surmiak, A. (2018). Confidentiality in Qualitative Research Involving Vulnerable

- Participants: Researchers Perspectives. *Forum: Qualitative Social Research*, 19(3), 393. <https://doi.org/10.17169/fqs-19.3.3099>
- Tang, F., Ma, S., Xiang, Y., & Lin, C. (2019). An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records. *IEEE Access*, 7, 41678641689. <https://doi.org/10.1109/ACCESS.2019.2904300>
- Tewksbury, R., & Mustaine, E. (2010). Cohen, Lawrence E., and Marcus K. Felson: routine activity theory. In F. T. Cullen & P. Wilcox (Eds.), *Encyclopedia of criminological theory* (pp. 187-192). SAGE Publications, Inc. <https://doi.org/10.4135/9781412959193.n52>
- Theofanidis, D., & Fountouki, A. (2019). Limitations And Delimitations In The Research Process. *Perioperative nursing (GORNA)*, E-ISSN:2241-3634, 7(3), 1556162. <http://doi.org/10.5281/zenodo.2552022>
- Tibben, W. J. (2015). Theory Building for ICT4D: Systemizing Case Study Research Using Theory Triangulation. *Information Technology for Development*, 21(4), 6286652. <https://doi.org/10.1080/02681102.2014.910635>
- Tkachuk, R. (2018). How Blockchain is becoming instrumental to social change [Blog Post]. <https://www.cio.com/article/3246629/how-blockchain-is-becoming-instrumental-to-social-change.html>
- Van-Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, 8(2), 1156127. <https://doi.org/10.1177/1477370810393156>
- Volety, T., Saini, S., McGhin, T., Liu, C. Z., & Choo, K.-K. R. (2019). Cracking Bitcoin wallets: I want what you have in the wallets. *Future Generation*

Computer Systems, 91, 1366143. <https://doi.org/10.1016/j.future.2018.08.029>

- Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly*, 39(1), 91-A7. <https://doi.org/10.25300/misq/2015/39.1.05>
- Wang, Q., Huang, J., Wang, S., Chen, Y., Zhang, P., & He, L. (2020). A Comparative Study of Blockchain Consensus Algorithms. *Journal of Physics: Conference Series*, 1437(1), 1. <https://doi.org/10.1088/1742-6596/1437/1/012007>
- Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. *Computer Communications*, 136, 10629. <https://doi.org/10.1016/j.comcom.2019.01.006>
- Weber, R. M. (2018). An Advisor's Introduction to Blockchain. *Journal of Financial Service Professionals*, 72(6), 49653.
- Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 2776292. <https://doi.org/10.1108/JFC-10-2017-0095>
- Wilczynski, A., & Widlak, A. (2019). Blockchain Networks - Security Aspects and Consensus Models. *Journal of Telecommunications & Information Technology*, 2, 46. <https://doi.org/10.26636/jtit.2019.132019>
- William, M. L. (2016). Guardians upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology*, 56(1), 21648. <https://doi.org/10.1093/bjc/azv011>
- Williams, M., & Moser, T. (2019). The Art of Coding and Thematic Exploration in Qualitative Research. *International Management Review*, 15(1), 45655.
- Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the Corporate

- Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior*, 40(9), 11196-1131. <https://doi.org/10.1080/01639625.2018.1461786>
- Xu, J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(1), 169. <https://doi.org/10.1186/s40854-016-0046-5>
- Yar, M. (2005). The Novelty of "Cybercrime." *European Journal of Criminology*, 2(4), 407-427. <https://doi.org/10.1177/147737080556056>
- Yassein, M. B., Shatnawi, F., Rawashdeh, S., & Mardin, W. (2019). Blockchain Technology: Characteristics, Security and Privacy; Issues and Solutions. 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Computer Systems and Applications (AICCSA), 2019 IEEE/ACS 16th International Conference On, 168. <https://doi.org/10.1109/AICCSA47632.2019.9035216>
- Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview Protocol Refinement: Fine-Tuning Qualitative Research Interview Questions for Multi-Racial Populations in Malaysia. *Qualitative Report*, 23(11), 2700-2713. <https://doi.org/10.46743/2160-3715/2018.3412>
- Yin, R. K. (2014). Case study research: Design and methods. Sage
- Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and Blockchain: Security and Privacy. *IEEE Internet of Things Journal, Internet of Things Journal, IEEE, IEEE Internet Things J*, 7(10), 10288-10313. <https://doi.org/10.1109/JIOT.2020.3004273>
- Zahavi, D. (2019). Getting it quite wrong: Van Manen and Smith on phenomenology. *Qualitative Health Research*, 29(6), 900-907.

<https://doi.org/10.1177/1049732318817547>

Zamani, E., He, Y., & Phillips, M. (2020). On the Security Risks of the Blockchain.

Journal of Computer Information Systems, 60(6), 4956506.

<https://doi.org/10.1080/08874417.2018.1538709>

Zaytoon, H. S. (2019). Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft. *North Carolina Law Review*, 97(2), 395.

<https://scholarship.law.unc.edu/nclr/vol97/iss2/4>

Zhang, G., Shen, Z., & Wang, L. (2020). Online Energy Management for Microgrids With CHP Co-Generation and Energy Storage. *IEEE Transactions on Control Systems Technology*, Control Systems Technology, IEEE Transactions on, IEEE Trans. *Contr. Syst. Technol*, 28(2), 5336541.

<https://doi.org/10.1109/TCST.2018.2873193>

Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, 52(3), 1634. <https://doi.org/10.1145/3316481>

Zhang, S., & Lee, J.-H. (2019). Analysis of the main consensus protocols of blockchain. *ICT Express*. <https://doi.org/10.1016/j.ict.2019.08.001>

Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., & Chen, R. (2019). NutBaaS: A Blockchain-as-a-Service Platform. *IEEE Access*, Access, IEEE, 7, 1344226-134433. <https://doi.org/10.1109/ACCESS.2019.2941905>

Zou, W., Lo, D., Kochhar, P. S., Le, X. D., Xia, X., Feng, Y., Chen, Z., & Xu, B. (2019). Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*.

<https://doi.org/10.1109/TSE.2019.2942301>

Zutlevics, T. L. (2016). Could Providing Financial Incentives to Research Participants

Be Ultimately Self-Defeating? *Research Ethics*, 12(3), 137-148.

<https://doi.org/10.1177/1747016115626756>

Appendix A: Interview Guide

My Research Topic

Security strategies for deploying Blockchain applications.

Research Questions

What security strategies do IT managers use in deploying Blockchain applications?

Assurance to the Interviewee

1. Thank you for agreeing to this interview, your participation is very important for the study about Blockchain security. It will help organizations to secure their Blockchain applications.
2. I will like to say that your participation is purely voluntary, if you will want to stop along the way or do not want to answer a question, please let me know.
3. This is for academic purpose and may be used for conferences or publications but your identity and institution will be confidential by replacing them with pseudonym.
4. I will be recording this interview for reference's sake.
5. After the interview, I will share my transcript and recording with you so that you can confirm or clarify any of the information that you gave.
6. The interview will take 60 to 120 minutes.
7. Should there be a need for a follow-up interview, I will discuss with you for a convenient time. This second interview will not take more than 30 minutes.
8. Ready to go?

Initial Probe Questions

What is your professional and academic background?

What is your experience as far as Blockchain technology is concerned?

What is your experience in IT security ?

Targeted Concept Questions

1. Describe the security threats that you encounter on Blockchain applications.
2. Describe the nature of these attacks.
3. Why do you think Blockchain applications are under attack?
4. In your opinion, are Blockchain security threats different from traditional IT threats?
5. Explain the strategies that you used successfully against these threats.
6. Explain other strategies if any you tried but did not work.
7. How did you implement these strategies?
8. Explain the challenges if any in the implementation.

Targeted Follow-up Questions

1. Why these threats?
2. To be decided during interview (I heard you mention x, tell me more about that)
3. To be decided during interview (I heard you mention x, tell me more about that)
4. Explain the differences if there is. If there is no difference, explain why they are the same.
5. Why did these strategies work?
6. Explain why the strategies did not work.
7. Depends on answer to question seven (I heard you mention z, tell me more about that).
8. How did you deal with the challenges in the implementation of the strategies?

Targeted Wrap-up Question

Do you have any additional information you think might help the study that you do not mind sharing?


Appendix B: Permissions to Reuse Figures and Tables

Rightslink® by Copyright Clearance Center - Mozilla Firefox

https://s100.copyright.com/AppDispatchServlet#formTop

Copyright Clearance Center RightsLink®

Home ? Help Email Support Sign in Create Account



Requesting permission to reuse content from an IEEE publication

Review of Blockchain Technology Vulnerabilities and Blockchain-System Attacks
 Conference Proceedings: 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)
 Author: A. Averin
 Publisher: IEEE
 Date: Oct. 2019
 Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Type here to search

3:34 PM 21/09/2020



RightsLink®



Home



Help



Email Support



Sign in



Create Account



An Overview of Blockchain Applications and Attacks

Conference Proceedings: 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (VITECoN)

Author: Rahul Rao Vokerla

Publisher: IEEE

Date: March 2019

Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK

CLOSE WINDOW



RightsLink®



Home



Help



Email Support



Sign in



Create Account

Analysis of the main consensus protocols of blockchain



ELSEVIER

Author: Shijie Zhang, Jong-Hyuk Lee

Publication: ICT Express

Publisher: Elsevier

Date: June 2020

© 2020 The Korean Institute of Communications and Information Sciences (KICS). Publishing services by Elsevier B.V.

Creative Commons Attribution-NonCommercial-No Derivatives License (CC BY NC ND)

This article is published under the terms of the [Creative Commons Attribution-NonCommercial-No Derivatives License \(CC BY NC ND\)](#).

For non-commercial purposes you may copy and distribute the article, use portions or extracts from the article in other works, and text or data mine the article, provided you do not alter or modify the article without permission from Elsevier. You may also create adaptations of the article for your own personal use only, but not distribute these to others. You must give appropriate credit to the original work, together with a link to the formal publication through the relevant DOI, and a link to the Creative Commons user license above. If changes are permitted, you must indicate if any changes are made but not in any way that suggests the licensor endorses you or your use of the work.

Permission is not required for this non-commercial use. For commercial use please continue to request permission via Rightslink.

[BACK](#)

[CLOSE WINDOW](#)

Open Access Article

Scalable Dynamic Multi-Agent Practical Byzantine Fault-Tolerant Consensus in Permissioned Blockchain

by Libo Feng¹, Hui Zhang^{1,2,*}, Yong Chen¹ and Liqi Lou³¹ State Key Laboratory of Software Development Environment, Beihang University, Beijing 100191, China² Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing 100191, China³ State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

* Author to whom correspondence should be addressed.

Appl. Sci. 2018, 8(10), 1010; <https://doi.org/10.3390/app8101919>

Received: 10 September 2018 / Revised: 30 September 2018 / Accepted: 30 September 2018 / Published: 15 October 2018

View Full-Text

Download PDF

Browse Figures

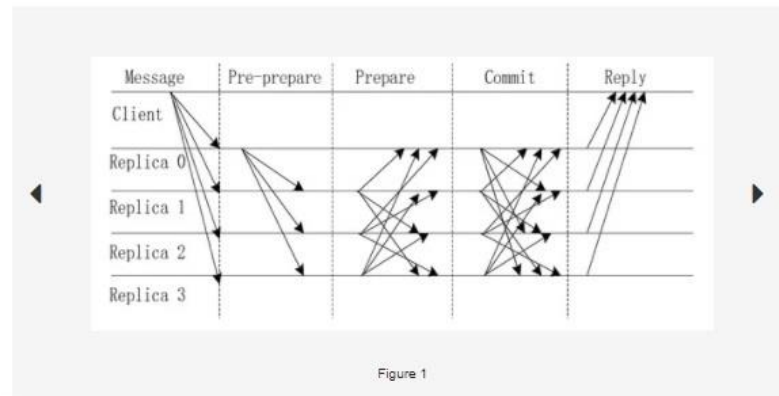
Cite This Paper

Abstract

The permissioned blockchain system has recently become popular in a wide range of scenarios, such as artificial intelligence, financial applications and the Internet of things, due to its dominance in terms of distribution, decentralization, reliability and security. However, the Practical Byzantine Fault-Tolerant (PBFT) algorithm, which is currently adopted in such systems, sparks communication bottlenecks when the number of consensus nodes increases sharply, which seriously hinders large-scale applications. In this paper, we propose a scalable dynamic multi-agent hierarchical PBFT algorithm (SDMA-PBFT), which reduces the communication costs from $O(n^2)$ to $O(n \times k \times \log_k n)$. Specifically, SDMA-PBFT forms multiple autonomous systems at each agent node in which message multicasting can be efficiently carried out and the internal voting results can be effectively collected. Therefore, the design of these agent nodes facilitates the in-and-out operations of consensus nodes in the blockchain system. Simulation results show that our proposed algorithm substantially outperforms the PBFT algorithm in terms of latency. Hence, it can be applied to the permissioned blockchain system effectively and efficiently. [View Full-Text](#)

Keywords: permissioned blockchain; byzantine fault tolerance; multi-agent; consensus; distributed systems; state machine replication

▼ Show Figures



© This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

https://outlook.office.com/mail/deeplink?version=20200914002.05&popoutv2=1

Reply all Delete Junk Block

Fwd: Permission to use diagram

HICSS <hics@hawaii.edu>
Mon 9/21/2020 4:56 PM
To: Prince Nirumah

Dear Prince,

Please find below a message from the author of the paper titled Towards a Comprehensive Blockchain Architecture Continuum.

Best regards,
Thayanan

----- Forwarded message -----
From: **Nico Abbatemarco** <nico.abbatemarco@sdabocconi.it>
Date: Mon, Sep 21, 2020 at 6:16 AM
Subject: R: Permission to use diagram
To: Daniel Ishimitsu <daniel20@hawaii.edu>, HICSS <hics@hawaii.edu>
Cc: Leonardo Maria De Rossi <leonardo.derosi@sdabocconi.it>


Dear Thayanan, dear Daniel,

absolutely no problem on our side! We are happy that our work proves useful for other scholars.

Unfortunately, the pandemic emergency prevented us from applying to HICSS this year; we will dearly miss the conference and we hope to be there again for the future editions!


Have a good day, best regards,

https://s100.copyright.com/AppDispatchServlet#formTop



RightsLink®

[Home](#)
[Help](#)
[Email Support](#)
[Sign in](#)
[Create Account](#)



Requesting
permission
to reuse
content from
an IEEE
publication

Blockchain Technology: Characteristics, Security and Privacy; Issues and Solutions

Conference Proceedings: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)

Author: Muneer Bari Yassein; Farah Shatnawi; Saif Rawashdeh; Wail Mardin

Publisher: IEEE

Date: 3-7 Nov, 2019

Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK
CLOSE WINDOW



RightsLink®



Home



Help



Email Support



Sign In



Create Account



Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges, and Solutions

Author: Naveed Ul Hassan

Publication: IEEE Industrial Electronics Magazine

Publisher: IEEE

Date: Dec. 2019

Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[BACK](#)
[CLOSE WINDOW](#)



RightsLink®



Home



Help



Email Support



Sign In



Create Account



An Overview of Blockchain Applications and Attacks

Conference Proceedings: 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)

Author: Rahul Rao Vokerla; Bharanidharan Shanmugam; Sami Azam; Asif Karim; Friso De Boer; Mirjam Jonkman; Fahad Faisal

Publisher: IEEE

Date: 30-31 March 2019

Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[BACK](#)
[CLOSE WINDOW](#)



RightsLink®



Home



Help



Email Support



Sign In



Create Account



A Security Reference Architecture for Blockchains

Conference Proceedings: 2019 IEEE International Conference on Blockchain (Blockchain)

Author: Ivan Homoliak

Publisher: IEEE

Date: Jul 2019

Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.


If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[BACK](#)
[CLOSE WINDOW](#)

https://s100.copyright.com/AppDispatchServlet#formTop

Copyright Clearance Center RightsLink®

Home Help Email Support Sign in Create Account



Hybrid Security Framework for Blockchain Platforms
 Conference Proceedings: 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)
 Author: Mahendra Kumar Shrivastava
 Publisher: IEEE
 Date: Jan. 2020
 Copyright © 2020, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW