8-2024

Exploring the Integration of Blockchain in IoT Use Cases: Challenges and Opportunities

Ivannah George

Recommended Citation

George, Ivannah, "Exploring the Integration of Blockchain in IoT Use Cases: Challenges and Opportunities" (2024). *Electronic Theses, Projects, and Dissertations*. 2001.
https://scholarworks.lib.csusb.edu/etd/2001

EXPLORING THE INTEGRATION OF BLOCKCHAIN IN IOT USE CASES: CHALLENGES AND OPPORTUNITIES

A Project
Presented to the
Faculty of
California State University,
San Bernardino

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
in
Information Systems & Technology
Cybersecurity

by
Ivannah George
August 2024

EXPLORING THE INTEGRATION OF BLOCKCHAIN IN IOT USE CASES: CHALLENGES AND OPPORTUNITIES

A Project

Presented to the

Faculty of

California State University,

San Bernardino

by

Ivannah George

August 2024

Approved by:

Dr. Conrad Shayo, Committee Member, Co-Chair

Dr. Oluwatosin Ogundare, Committee Member, Co-Chair

Dr. William Butler, Committee Member, Reader

ABSTRACT

Blockchain and The Internet of Things (IoT) is a significant paradigm which has gained traction in today’s digital age as two complimentary technologies. The combination of IoT's connectivity with blockchain's security creates new opportunities and solves problems associated with centralized systems. This culminating project aims to delve deeper into the integration of blockchain technology in IoT applications based on select use cases to uncover potential benefits and significant challenges of blockchain integration across different sectors. The research objectives to be addressed are: (RO1) How emerging vulnerabilities manifest in the implementation of blockchain within current IoT ecosystems. (RO2) How current opportunities and challenges are influencing the successful integration of blockchain in IoT ecosystems. The findings from the case studies are: (RO1) Significant vulnerabilities exist within core blockchain features such as smart contracts which could lead to cascading failures and widespread system disruption within an IoT ecosystem. Additionally, difficulty in quickly patching smart contract vulnerabilities due to blockchain immutability further exacerbates this risk. (RO2) The successful integration of blockchain in IoT has the potential to provide enhanced trust, performance and security however significant bottlenecks such as interoperability challenges between various IoT devices and blockchain protocols, effective consensus mechanisms suited for resource constrained IoT devices and scalability challenges must be navigated to achieve a seamless integration of the technologies The conclusions are: (RO1) IoT-blockchain convergence introduces new potential attack vectors that must be analyzed and secured, especially at the intersection of resource-constrained IoT devices and computationally intensive blockchain protocols. (RO2) Blockchain integration in IoT requires specific considerations related to the heterogenous nature of IoT devices, resource limitations for traditional IoT ecosystems, scalability of blockchain solutions in the diverse nature of IoT ecosystems and standardization and compatibility of different blockchain platforms across IoT applications.

Areas of further study include researching minimum security requirements in software development of IoT devices which can support complex computational requirements needed for successful integration of blockchain in IoT applications and improving blockchain security against quantum attacks. Public-key cryptography, a cornerstone of blockchain security, is particularly susceptible to such threats.

ACKNOWLEDGEMENTS

I would like to acknowledge my family and loved ones for their encouragement and support throughout my graduate studies. Without their support, this would not have been possible. I also want to thank Drs. Oluwatosin Ogundare, William Butler, and Conrad Shayo, Chair of the IST Department, dedicated Committee Members, whose encouragement and insightful feedback helped me tremendously throughout the completion of this culminating experience project.

TABLE OF CONTENTS

ABSTRACT iii

ACKNOWLEDGEMENTS v

LIST OF TABLES viii

LIST OF FIGURES ix

CHAPTER ONE: INTRODUCTION 1

Background of study 1

Problem Statement 5

Research Objectives 6

CHAPTER TWO: LITERATURE REVIEW 7

Literature Review Identified Gaps 16

CHAPTER THREE: RESEARCH METHOD 18

Multiple Case Study Approach 18

Selection of Case Studies 19

CHAPTER FOUR: CASE STUDY ANALYSIS AND FINDINGS 21

Case Study 1: THE DAO Attack 2016 22

Case Analysis 23

Findings and Mitigation Strategies 24

Smart Contract Vulnerabilities 25

Exploitation of IoT Oracles 26

Case Study 2: Walmart's Blockchain Quest with IBM 29

Case Analysis 30

Findings and Mitigation Strategies 31

Interoperability Challenges 32

Adoption & Collaboration 33

Scalability Challenges 34

Cost of Implementation 35

Energy Consumption 36

Regulatory Compliance 36

Integration of Legacy Systems 37

CHAPTER FIVE: DISCUSSION, CONCLUSION AND AREAS FOR FURTHER STUDY 39

Discussion 39

Conclusion 44

APPENDIX A BLOCKCHAIN - IOT REAL WORLD USE CASES 45

REFERENCES 47

LIST OF TABLES

Table 1. Comparison of Different Blockchain Technologies (Singh & Kumar 2022)………………………………………………………………………………….15

Table 2. Selection of Case Studies.. 19

Table 3. Case Study Analysis Criteria (Yin 2017).. 20

Table 4. Losses and Occurrences across Different Blockchains (Tsai et al., 2023)………………………………………………………………………………….23

Table 5. Blockchain-IoT Security Vulnerabilities and Mitigations........................ 27

LIST OF FIGURES

Figure 1: Internet of Things Connected Devices Worldwide from 2019 to 2023 (Statista, 2024) 2

Figure 2:Edge-Fog-Cloud Architecture of IoT Systems 9

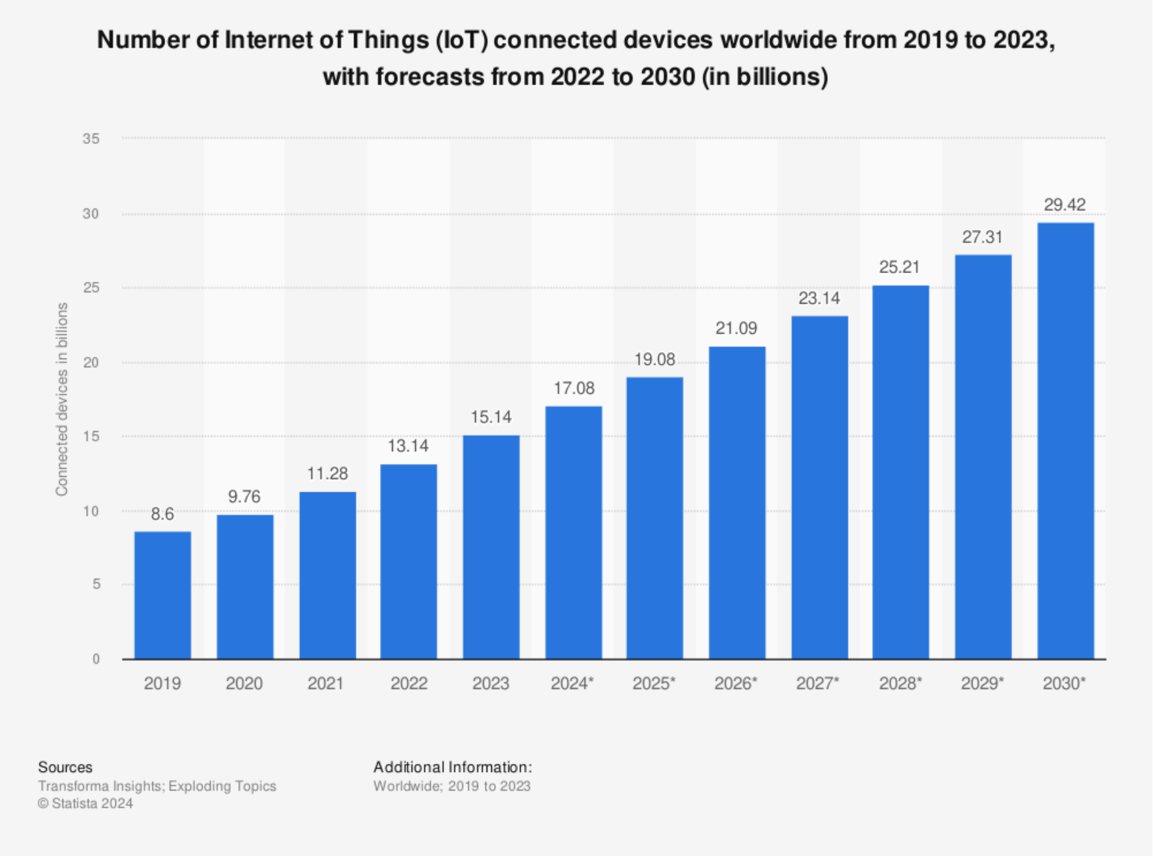
Figure 3:Timeline of Walmart's Blockchain-based Food Tracking Initiative 30

CHAPTER ONE

INTRODUCTION

Background of study

The Internet of Things (IoT) is a digital nervous system connecting everyday physical devices such as smartphones, sensors, and appliances, which gather and exchange data across the internet. The IoT ecosystem transforms ordinary devices into smart, interconnected tools that enhance efficiency and convenience in various aspects of life and has transformed how we interact with technology introducing increased levels of connectivity and automation across various domains, including healthcare, transportation, agriculture, smart cities, and supply chain management. However, as IoT devices become more widespread, concerns about the security mechanisms in place and data privacy surrounding significant amounts of data which they collect have grown (Singh & Kumar 2022). Traditional security mechanisms are often inadequate for IoT due to its unique resource constraints and requirements. This has led to increasing interest in integrating blockchain to bolster security and trust in IoT ecosystems. Blockchain, a decentralized ledger technology known for its secure, transparent, and immutable transaction features and offers promising solutions to IoT's inherent vulnerabilities. (Singh & Kumar 2022)



Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 (in billions)

Sources
Transforma Insights; Exploding Topics
© Statista 2024

Additional Information:
Worldwide; 2019 to 2023

Figure 1: Internet of Things Connected Devices Worldwide from 2019 to 2023 (Statista, 2024)

According to Statista (2024), The number of IoT devices is forecasted to grow to more than 17 billion by 2030 as shown in Fig 1. The expansive reach of IoT calls for a deep dive into the architecture and landscape of IoT devices and ecosystems to analyze inherent complexities and vulnerabilities and how they can be mitigated. Given that the IoT paradigm comprises interconnected networks and diverse devices, it inherits traditional security challenges from computer networks. Additionally, the presence of constrained resources in IoT devices exacerbates security issues, as small devices or sensors possess limited power and memory. Therefore, security solutions must be tailored to accommodate these constrained architectures.

Blockchain technology, which was originally developed for cryptocurrencies like Bitcoin and Ethereum, offers better security, decentralized, transparent storage and transaction verification mechanisms (Singh & Kumar, 2022). Since the inception of the pioneering blockchain system Bitcoin, the evolution of blockchain technology has unfolded across two distinct phases: blockchain 1.0 and blockchain 2.0(Li et al., 2020). In its infancy, blockchain 1.0 primarily focused on establishing decentralized digital currencies like Bitcoin, laying the groundwork for peer-to-peer transactions without the need for intermediaries. Subsequently, blockchain 2.0 emerged, introducing more sophisticated functionalities such as smart contracts (Li et al., 2020). These smart contracts leverage the decentralized consensus mechanism inherent in blockchain technology, enabling parties with mutual distrust to engage in data exchange or transactions without reliance on a trusted third party. Ethereum, as of May 2017, emerged as the predominant blockchain platform supporting smart contracts (Li et al., 2020).

As the possibilities of Blockchain technology has been seen in various IoT domains, multiple studies (Reyna et al., 2018; Wang et al., 2019; Fei et al., 2023; Hassan et al., 2019; Dorri et al., 2019; Liang & Kim 2021) have delved into understanding the inherent complexities and vulnerabilities within IoT ecosystems and the integration of blockchain to address those challenges. In one such work, (Wang et al., 2019) highlighted the blockchain technologies which can be used to address the potential challenges introduced by IoT. Privacy preservation has also been discussed as a potential challenge in successful blockchain integration due to the public nature of blockchain technology (Hassan et al., 2019). In a comprehensive survey conducted by (Fei et al., 2023) a detailed review of IoT architecture, infrastructure, and wireless technology in IoT provide a detailed analysis of current IoT security vulnerabilities and the mitigation strategies provided by recent research. However, the authors highlighted areas for further research directions for IoT security which focused on analyzing resource constraints of IoT devices and vulnerabilities emerging in edge computing and blockchain. This culminating project seeks to contribute practical insights and solutions that can enhance the security, scalability, interoperability, and governance of blockchain-IoT integrations, while also addressing economic feasibility and privacy concerns.

Problem Statement

The integration of blockchain technology into Internet of Things (IoT) ecosystems presents a promising solution to enhance security, transparency, and trustworthiness. However, despite the potential benefits, there remain significant challenges and gaps in investigation into emerging vulnerabilities specific to new IoT technologies, such as edge computing and blockchain integration (Liang & Kim 2021), there is also a need to address privacy preservation in blockchain based solutions for IoT security. (Hassan et al., 2019). Exploration of novel attack vectors and exploitation techniques targeting IoT and blockchain ecosystems, including 51% attacks, physical-layer attacks and side-channel vulnerabilities (Fei et al., 2023) and research into the scalability and practical feasibility of implementing robust blockchain security measures across heterogeneous IoT device deployments. (Banerjee et al., 2018)

This culminating project seeks to conduct a comprehensive analysis of real-world use cases and deployments where these technologies are employed to enhance IoT security and performance. By synthesizing insights from existing case studies based on the case study research strategy (Yin, 2017), this culminating project will identify common challenges, success factors, and lessons learned in implementing emerging technologies for IoT security. This holistic understanding gained from the analysis of case studies will help inform the development of practical guidelines and frameworks for effectively addressing pertinent challenges in integration of emerging technologies in diverse IoT applications and environments.

Research Objectives

The gaps identified in existing research remain in exploring the practical implementation, scalability, and real-world implications of blockchain integration in IoT industry specific use cases. Specific challenges include handling the high volume of IoT data, managing resource-constrained devices, mitigating security vulnerabilities, and establishing trust among diverse stakeholders (Tran et al., 2021). Based on the examination of existing research, the objective of this culminating experience project is to use qualitative research case study techniques (Yin, 2019, Miles & Huberman, 2019, & Corbin & Strauss, 2015) to explore the following research objectives:

Research Objective 1: How emerging vulnerabilities manifest in the implementation of blockchain within current IoT ecosystems. (Liang & Kim 2021)

Research Objective 2: What current opportunities and existing challenges influence the successful integration of blockchain in IoT ecosystems. (Qureshi et al., 2022)

CHAPTER TWO

LITERATURE REVIEW

In reviewing the literature for this research project, numerous theories have been identified to elucidate the concepts of the Internet of Things (IoT), blockchain, and their integration. Common themes emerged, particularly concerning IoT security and potential solutions. Key themes such as blockchain technology, smart contracts, consensus mechanisms, and edge computing frequently appear in the literature. Examining these themes will help address the research questions of this study. This review aims to synthesize the current scholarly works in this emerging field, concentrating on the period from 2017 to 2024. This timeframe encompasses the rapid development and widespread adoption of blockchain and IoT technologies, offering a thorough understanding of the latest advancements, challenges, and opportunities.

The reviewed literature is gathered from multiple academic journal databases such as Google Scholar, Science Direct, IEEE Xplore and ACM Digital Library. These databases allowed for the refinement of search parameters tailored to the specific research topic. Along with limiting the language to English, Open Access, and a date range of 2017-2024, additional filters are applied. Keywords and logical operators AND/OR were employed to refine the search, focusing on themes such as "blockchain, "smart contracts”, “consensus mechanisms”, "Internet of Things, "blockchain scalability”, "IoT security", and combinations thereof. The keywords selected in this process are chosen based on their relevance to answering the research questions in this project. To ensure a comprehensive and balanced review, the review encompasses a diverse range of sources, including peer-reviewed journal articles, conference proceedings, industry reports, and authoritative publications from credible organizations. The selected literature covers various aspects of blockchain-IoT integration, such as security vulnerabilities, scalability challenges, interoperability issues, and potential applications across different sectors.

Research Objective 1: How emerging vulnerabilities manifest themselves in the implementation of blockchain within current IoT ecosystems (Liang & Kim 2021)

The Internet of Things (IoT) is an evolving technology that's gaining considerable attention lately. Despite its popularity, the definition of an IoT system remains varied and elusive (Atzori et al., 2010). Tran et al. (2021) discusses three perspectives on defining IoT systems: thing-oriented, Internet-oriented, and semantic-oriented. Described practically, they consider IoT systems as physical devices that utilize electronic tags, sensors, and actuators to communicate over the Internet. IoT systems often employ a three-tier architecture consisting of edge, fog, and cloud components (Tran et al., 2021). The cloud tier simplifies the interactions and management of IoT devices by hosting digital representations of the physical devices. Many blockchain-based IoT (BC-IoT) systems deploy blockchain elements on the cloud infrastructure or treat blockchain networks as remote cloud services, referred to as Cloud Deployment.

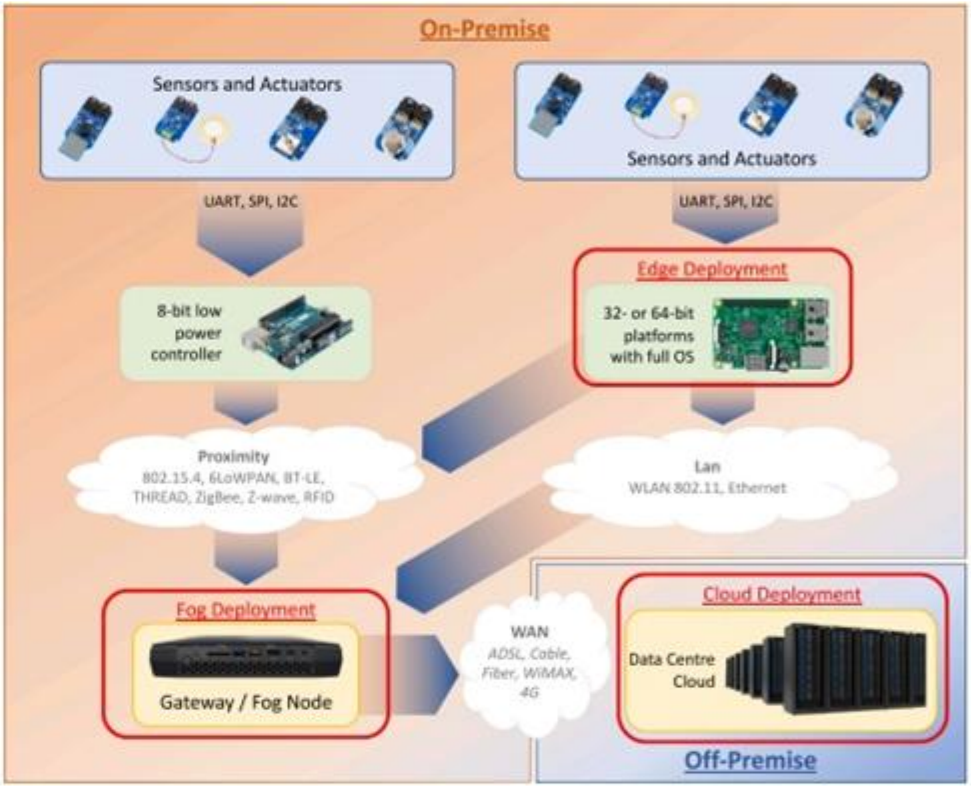


Figure 2:Edge-Fog-Cloud Architecture of IoT Systems

Emerging technologies such as edge computing, fog computing, cloud computing, and blockchain have been developed to address various IoT challenges, including load balancing, storage, and reducing costs by moving data away from the cloud (Fei et al., 2023). However, while potential solutions to IoT security issues using these technologies have been explored, significant problems remain unresolved. A major issue in edge computing is the security of user data (Liang & Kim, 2021). For instance, researchers highlighted a scenario where hackers could exploit a user's absence from their home—detected through monitoring power or water usage—to gain unauthorized access (Liang & Kim, 2021). This situation emphasizes the necessity for robust security measures to protect user data at the edge computing level. Users must ensure their network connections are secure to prevent such intrusions (Liang & Kim, 2021). Another study by researchers' states:

"Although, using edge computing can mitigate spoofing attacks, the limited power capacity of edge IoT devices must be considered in future research, because attackers can perform many operations on the CPU to reduce battery life" (Fei et al., 2023).

Consequently, blockchain has been introduced to improve performance challenges in IoT whilst also addressing security concerns in IoT ecosystems. However, this technology is still not without its own vulnerabilities (Shammar et al., 2021). One of the main vulnerabilities associated with blockchain integration in IoT is the scalability limitations of blockchain technology (Shammar et al., 2021). The decentralized and distributed nature of blockchain often struggles to keep pace with the massive volumes of data generated by IoT devices, leading to performance bottlenecks and potential system congestion.(Hassan et al., 2019) This mismatch in scalability can create vulnerabilities, as the blockchain network may become overwhelmed, compromising the overall reliability and responsiveness of the IoT-blockchain ecosystem (Qureshi et al., 2022).A survey on security attacks and solutions in the IoT networks (Liang & Kim 2021), discusses significant security and privacy challenges that must be addressed for blockchain implemented in IoT to reach their full potential and meet user expectations. The study identifies the unique problems faced by IoT networks, including issues around privacy, authentication, scalability and storage, and data processing speeds (Liang & Kim 2021). To better understand these security challenges, the literature outlines a three-layered IoT architecture, comprising the physical layer, network layer, and application layer (Liang & Kim 2021). It further delves into the various types of attacks that can target each of these layers, such as physical attacks on hardware, network layer attacks like man-in-the-middle and spoofing, and application layer attacks involving code injection and data theft (Liang & Kim 2021). This multilayered view of IoT security highlights the complexity and breadth of the attack surface.

In another such work on the security of blockchain systems (Li et al., 2020), provide a comprehensive overview of the security risks and vulnerabilities associated with blockchain technology. Researchers refer to the development stages of blockchain as blockchain 1.0 for cryptocurrencies and blockchain 2.0 for smart contracts (Li et al., 2020). Significant vulnerabilities exist in blockchain like the 51% vulnerability which occurs when a single miner controls more than 50% of the total mining power of the blockchain, they can potentially take control of the entire blockchain and manipulate the blockchain to perform double spending attacks (Li et al., 2020). Real-world attacks on blockchain systems, such as selfish mining attacks, the DAO attack on Ethereum, BGP hijacking attacks, eclipse attacks, liveness attacks, and balance attacks are surveyed which demonstrate the practical implications of these security vulnerabilities (Li et al., 2020). There are also additional privacy vulnerabilities related to blockchain solutions in IoT due to the inherently public nature of blockchain transactions which raises the risk of private information being leaked (Liang and Kim 2021). Smart contracts, which automate interactions and enforce predefined rules within blockchain ecosystems, present a notable vulnerability. While they offer efficiency, flaws in the smart contract code can lead to unexpected behaviors, financial losses, and exploitation by hackers (Atzei et al., 2017; Li et al., 2020).

Additionally, governance issues in blockchain networks can pose additional risks. Decentralized governance often makes it challenging to swiftly address emerging threats or agree on updates and fixes, leaving IoT-blockchain systems exposed to potential vulnerabilities for extended periods (Zwitter et al., 2020). Also, the scalability issues that can arise as the blockchain grows and more miners are added, leading to increases in storage requirements, costs, and the speed of data distribution across the network is a significant vulnerability for blockchain in IoT. These scalability challenges must be addressed when designing and implementing blockchain-based IoT security architectures (Tran et al., 2021).

Research Objective 2: What current opportunities and challenges influence the successful integration of blockchain in IoT ecosystems (Qureshi et al., 2022)

Researchers have been exploring the integration of blockchain technology into IoT systems in recent years, emphasizing the opportunities it presents for enhancing security and performance. For instance, Qureshi et al. (2022) offer a comprehensive overview of this integration, detailing various strategies to leverage blockchain effectively within IoT environments. They highlight blockchain's redundant data storage as crucial for maintaining data integrity and resilience against breaches or data loss (Qureshi et al., 2022; Bhushan et al., 2020), which meets the high availability needs of IoT control mechanisms. The study underscores blockchain's potential to improve scalability in IoT by its decentralized structure, accommodating diverse devices and protocols (Qureshi et al., 2022), thus addressing interoperability challenges common in IoT deployments. Furthermore, blockchain's fault-tolerant consensus mechanisms ensure reliability and security, overcoming the limitations of centralized architectures and ensuring uninterrupted operation (Qureshi et al., 2022).

In another review, (Tran et al., 2020) examines the motivations and approaches for integrating blockchain technology into Internet of Things (IoT) systems, highlighting amongst many other benefits such as increased transparency, immutability, key vulnerabilities that blockchain aims to address. Existing IoT systems face challenges ensuring the integrity and authenticity of data like sensor readings, device configurations, and firmware updates, which blockchain's immutable ledger can help protect against tampering (Tran et al., 2021). IoT systems currently rely heavily on centralized cloud services for operation and security, creating single points of failure and trust issues that decentralized blockchain networks could mitigate by enabling decentralized security mechanisms like authentication and access control (Khan et al., 2018). Establishing secure communication channels within and across IoT systems is difficult, but blockchain can provide a trusted environment for auditable communication (Khan et al., 2018). As autonomous IoT systems engage in machine-to-machine exchange of resources like data, energy and services, blockchain offers secure recordkeeping and cryptocurrency-based incentivization models to control these transactions (Khan et al., 2018). By addressing this integrity, trust, security and incentive issues, blockchain integration aims to enhance the robustness and decentralization of IoT ecosystems (Christidis & Devetsikiotis, 2016)

A review on blockchain technologies for the Internet of Things (Ferrag et al., 2018) highlights three main types of blockchain technologies in literature: *public blockchain, consortium blockchain* and *private blockchain*. Public blockchains allow anyone to join the blockchain network and participate in the consensus process (Singh & Kumar 2022). Private blockchains are typically owned and controlled by a single entity or organization with restricted access to the distributed ledger and consensus process. Consortium blockchains, also known as federated blockchains, share a lot of similarities to private blockchains and are typically used in business domains for cross-organizational collaboration (Singh & Kumar 2022). The adequate type of blockchain technology to be used in IoT use cases will be based on the specific applications required for the IoT ecosystem. Table 1 shows a comparison of the different types of blockchain technologies.

Table 1. Comparison of Different Blockchain Technologies (Singh & Kumar 2022)

	Public Blockchain	**Private Blockchain**	**Consortium/Federated Blockchain**
Participation in Consensus	Every node	Solo organization	Some specified nodes in multiple organizations
Access	Read/write access allowed to all	High access restriction	Comparatively lower access restriction
Identity	Pseudo-anonymous	Accepted participants	Accepted participants
Immutability	Fully immutable	Partially immutable	Partially immutable
Transaction Processing Speed	Low	High	High
Permission Required	No	Yes	Yes

A significant concept in the blockchain phenomena is the consensus mechanisms. This is the mechanism used by peers in the blockchain network to come to a consensus on transactions in the blockchain network (Nakamoto 2008). Evaluating consensus algorithms like Proof-of-Work, Proof-of-Stake, Practical Byzantine Fault Tolerance (PBFT), and Directed Acyclic Graph (DAG)-based consensus is crucial to find the right balance for specific IoT use cases (Qureshi et al., 2022). Challenges such as data management and specialized skill requirements are also noted, suggesting the need for robust frameworks and skill-building initiatives to drive BCIoT adoption. Furthermore, the study highlights privacy concerns related to personal data collection by IoT devices to be addressed through blockchain-based privacy-preserving mechanisms to foster user trust and widespread BCIoT acceptance (Qureshi et al., 2022, Fei et al., 2023). Additionally, it has been observed that the processing power required for public blockchain network and associated energy costs will be a challenge (Banerjee et al., 2018). “Essentially, the Bitcoin network consumes enough energy to power more than 1.3 million U.S.

Literature Review Identified Gaps

The review of existing literature on the integration of blockchain with Internet of Things (IoT) ecosystems has unveiled several gaps warranting further investigation. These gaps identified directly correlate with the research questions and serve as driving forces behind the need for blockchain-based solutions to tackle vulnerabilities and intricacies within current IoT ecosystems. A significant gap illuminated in the literature is the insufficient understanding of how emerging vulnerabilities and security risks stemming from the rapid adoption of new technologies within IoT ecosystems can be identified early on (O1). As IoT devices and systems interconnect and grow in complexity, there's an urgent need to pinpoint and address potential vulnerabilities that could jeopardize the integrity, privacy, and reliability of these ecosystems. Furthermore, the literature review has brought to light gaps in exploring the practical opportunities and challenges linked with integrating blockchain technology into IoT ecosystems (O2). While the benefits of blockchain are widely acknowledged, there exists a need for deeper insights into practical implications, scalability concerns, and potential obstacles that might arise in real-world implementations. Through a thorough investigation of these identified gaps, this culminating project aims to offer invaluable insights to guide the integration of blockchain in IoT use cases. This project's findings can shape the future development and deployment of secure, transparent, and accountable IoT ecosystems.

CHAPTER THREE

RESEARCH METHOD

Multiple Case Study Approach

This culminating experience project employs the case study research method to address the research objectives, following the guidance of Yin (2017). The objective of this method is to explore the complex landscape filled with both challenges and opportunities in integrating blockchain technology with Internet of Things (IoT) ecosystems. To examine this intricate relationship, a multi-case study methodology is identified as the most suitable approach. This aligns with Yin's (2017) recommendation, which highlights case studies as essential tools for investigating complex phenomena within their real-world contexts, especially when the boundaries between the phenomenon and its context are not clearly defined. According to Yin (2017), the components of case study research design include the study's:

1.Questions (How, Why) and (What) if necessary.

2.Propositions or Justification (for Exploratory Study)

3.Unit(s) of analysis

4.Logic linking the data to the research question

5.Criteria for interpreting the findings

Selection of Case Studies

The primary case studies reviewed for this project were sourced from databases including the Harvard Business Review, Hyperledger Fabric Foundation, and Google Scholar. Selected studies needed to contain empirical data or quantitative analyses related to the performance, scalability, or security aspects of blockchain-IoT integration; discussions on the challenges encountered during implementation and the strategies used to address them; and insights into future directions or potential improvements for the specific use case. Furthermore, the case studies had to be published in scholarly journals, conference proceedings, or by reputable organizations, written in English or another widely understood language, with the most recent versions being prioritized.

Table 2. Selection of Case Studies

Database Searched	**Search Words**	**Number of Relevant Cases found**	**Number of Cases Selected**	**Authors**
Google Scholar	"Blockchain Vulnerability", "Blockchain Attack", "Blockchain - IoT Security"	10	1	(Tsai et al., 2023)
Harvard Business Review	"Blockchain IoT Integration", “Blockchain- IoT challenges",	16	1	Hoffman (2021)
Hyperledger Fabric Foundation	“Blockchain” ‘Hyperledger” “Supply chain”	25	1	Hyperledger Foundation (2019)

Table 3. Case Study Analysis Criteria (Yin 2017)

1	Questions	How do emerging vulnerabilities manifest in the implementation of blockchain within current IoT ecosystems?	What are current opportunities and challenges influencing the successful integration of blockchain in IoT ecosystems?
2	Propositions or Justification (for Exploratory Study	Blockchain vulnerabilities such as 51% attacks, smart contract vulnerabilities, and consensus mechanism flaws can compromise data integrity, disrupt operations, and undermine trust among stakeholders.	Conducting an analysis of real-world case studies can provide valuable insights into unrealized opportunities and potential challenges that arise when integrating blockchain into IoT ecosystems.
3	Unit(s) of Analysis	The unit of analysis will focus on vulnerabilities in blockchain technology, smart contract codes and the broader implications of blockchain attacks for IoT-blockchain implementations.	The unit of analysis will focus on specific projects or initiatives within organizations adopting blockchain for IoT. The analysis will also consider the roles and interactions of the various stakeholders involved in the ecosystem.
4	Logic Linking the Data to the Research Question	Thematic analysis is used to identify patterns and themes related to vulnerabilities and integration challenges across various blockchain-IoT deployments.	Cross-case synthesis is used to compare different case studies and draw broader conclusions about the opportunities and challenges influencing the integration of blockchain in IoT ecosystems.
5	Criteria for Interpreting the Findings	The findings are interpreted in the context of degree of vulnerability mitigation in IoT-blockchain vulnerabilities, and the challenges associated with secure and resilient implementation.	The findings of the case study are interpreted in the context of the successful implementation indicators of blockchain integration in IoT ecosystems, challenges encountered and overcome, and opportunities realized in blockchain implementations.

CHAPTER FOUR

CASE STUDY ANALYSIS AND FINDINGS

This section will analyze case studies of real-world implementation of blockchain in IoT domains. The scope of the case studies targeted security vulnerabilities in new technologies being implemented in IoT ecosystems, the integration of blockchain to address security and performance vulnerabilities in IoT and privacy preservation strategies in blockchain based solutions.

Research Objective 1: How emerging vulnerabilities manifest in the implementation of blockchain within current IoT ecosystems (Liang & Kim 2021)

To support research objective 1, The 2016 DAO (Decentralized Autonomous Organization) hack will be reviewed as a notable case study of how significant vulnerabilities can manifest in real-world applications, highlighting the importance of addressing security flaws in both blockchain and IoT contexts. This is because, although blockchain technology is instrumental in providing a more secure way of storing IoT data, Blockchain networks are also susceptible to various attacks. Methods such as 51% attacks, Sybil attacks, double-spending, and selfish mining can undermine the security and reliability of the blockchain (Saad et al., 2019). These attacks can have serious repercussions for IoT devices and applications that depend on the integrity of the blockchain.

Case Study 1: THE DAO Attack 2016

[1]In 2016, a decentralized autonomous organization known as "The DAO" launched on the Ethereum blockchain, raising over $150 million worth of Ether (ETH) through a token sale (DuPont, 2017). The DAO was created by the company Slock.it as a decentralized investment platform operating through smart contracts on the Ethereum blockchain (Jentzsch, 2016). In theory, The DAO would enable a transparent, crowdsourced model for funding projects without centralized control (Jentzsch, 2016). However, on June 17, 2016, a hacker began exploiting a "recursive call" vulnerability in The DAO's smart contract to withdraw funds repeatedly before the contract could update its balance (Merre, 2016). Over $60 million in ETH was drained into a "child DAO" controlled by the attacker (DuPont, 2017). This attack alone accounts for a substantial portion of the total losses on the Ethereum chain, as shown in Table 4. The Ethereum community scrambled to respond, eventually implementing a controversial "hard fork" to the Ethereum blockchain to roll back the malicious transactions and restore the stolen funds (Merre, 2016). This case study examines The DAO hack to explore emerging vulnerabilities that can arise when implementing blockchain solutions in the context of Internet of Things (IoT) ecosystems.

[1] https://library.oapen.org/bitstream/handle/20.500.12657/29557/1000376.pdf#page=172

Table 4. Losses and Occurrences across Different Blockchains (Tsai et al., 2023)

Chain	**Loss**	**Percentage**	**Event**	**Percentage**
Ethereum	1306.15	82.75%	37	68.51%
Solana	117.00	7.41%	1	1.85%
Arbitrum	80.62	5.10%	5	9.25%
Fantom	46.40	2.93%	3	5.55%
Polygon	16.45	1.04%	2	3.70%
Gnosis	6.20	0.39%	1	1.85%
zkSync Era	3.40	0.21%	1	1.85%
BSC	2.09	0.13%	4	7.40%

Case Analysis

The DAO hack illustrated that smart contract, like all software, can contain exploitable coding flaws (DuPont, 2017). The "recursive call" bug in The DAO's withdrawal mechanism allowed the repeated withdrawals that facilitated the theft (Jentzsch, 2016). As IoT ecosystems increasingly leverage blockchain and smart contracts for applications like supply chain tracking or M2M transactions, such code vulnerabilities could enable attacks disrupting physical processes (Huckle et al., 2016). Additionally, the DAO hack exemplified governance risks posed by fully decentralized, automated decision-making (DuPont, 2017). The DAO lacked a clear governance mechanism to swiftly intervene and halt the draining of funds, prolonging the incident (Merre, 2016). Implementing blockchains within IoT environments will require designing governance frameworks to promptly respond if vulnerabilities arise in smart contracts controlling critical infrastructure. Immutability challenges of blockchains when vulnerabilities are discovered post-deployment is also observed and undoing The DAO hack necessitated a divisive hard fork which resulted it in a divide in the Ethereum community (DuPont, 2017). Enabling controlled mutability will be vital for blockchain IoT applications to address emergent issues without relying on hard forks.

Findings and Mitigation Strategies

The DAO hack was not a singular event but a series of attacks exploiting multiple vulnerabilities. While the "recursive call" bug in the withdrawal mechanism is often cited as the primary vulnerability (Jentzsch, 2016), further analysis reveals that the attacker(s) leveraged several additional exploits, including a "race to empty" flaw and a "split to 0 ether" vulnerability (Mehar et al., 2019). This finding highlights the complexity of securing smart contracts and the potential for compounding vulnerabilities in blockchain systems. The Ethereum community's response to The DAO hack, particularly the decision to hard fork, exposed governance vulnerabilities in decentralized systems. The hard fork was controversial, with some arguing that it undermined the immutability and censorship-resistance of blockchain (Dhillon et al., 2017). This debate revealed the challenge of achieving effective decentralized governance and the potential for contentious decision-making in crisis scenarios. Despite its decentralized aspirations, token ownership in The DAO was highly concentrated. Analysis shows that just 50 addresses held over 40% of all tokens. This concentration of voting power undermines the principle of decentralized governance and makes the system vulnerable to manipulation by large token holders which exposed the gap between the promise and reality of decentralization. While marketed as a decentralized entity, The DAO's governance and operations were not as distributed as initially believed. This raises questions about the true level of decentralization achievable in practice in blockchain-IoT integrations.

Smart Contract Vulnerabilities

These findings highlight the multifaceted nature of vulnerabilities in blockchain systems and their relevance to IoT implementations. The presence of multiple exploits in The DAO's code emphasizes the importance of comprehensive specialized security audits and testing that simulates various IoT device states and interactions to identify potential vulnerabilities in the smart contract's logic (Stellios et al., 2018). To mitigate vulnerabilities like the recursive call that led to the DAO 2016, we can apply secure coding practices, such as implementing reentrancy guards (Tsai et al., 2023). In the DAO's case, the attack leveraged a flaw in the `withdraw` function, allowing repeated withdrawals before updating the balance, leading to a significant loss of funds. If we quantify this, assuming an attacker can initiate n recursive calls without a guard, where n could be a large number limited only by gas costs and transaction constraints, the potential for fund depletion is substantial. By implementing a `nonReentrant` guard in the `withdraw` function, the execution is limited to one call per invocation, effectively reducing n to 1. This mitigation drastically lowers the risk by ensuring that each function call completes before another begins (Tsai et al., 2023). Additionally, adhering to the check-effects-interactions pattern, where [2]internal state changes are made before any external call, further strengthens the contract against such attacks.

Exploitation of IoT Oracles

Consequently, as IoT devices increasingly rely on IoT oracles to feed real-world data into blockchain systems, the risk of oracle manipulation leading to smart contract exploits becomes a critical concern (Boudguiga et al., 2017). This can be mitigated by creating a network of multiple, independent IoT data oracles and the use of consensus mechanisms to aggregate and validate the data before it's used in smart contracts (Boudguiga et al., 2017). The use of cryptographic proofs to validate IoT data integrity can also be a beneficial mitigation strategy. This can be implemented in systems where IoT devices sign their data with secure hardware modules, allowing oracles to verify the authenticity and freshness of the data before submitting it to the blockchain (Chainlink 2021). The governance challenges exposed by The DAO hack also have significant implications for IoT ecosystems, contentious hard forks or delayed decision-making due to governance disputes could have severe consequences in these environments, potentially disrupting essential services or causing physical damage (Huckle et al., 2016). Furthermore, the reputational and legal fallout from

[2] https://research.chain.link/whitepaper-v1.pdf

The DAO attack highlights the broader risks associated with blockchain vulnerabilities. In IoT implementations, a loss of trust or legal uncertainties could hinder adoption and investment in blockchain solutions (Atlam et al., 2018) and consequently, clarity around liability and regulatory frameworks will be crucial for fostering confidence in IoT blockchain applications. Additionally secondary analysis has been conducted and significant vulnerabilities which could have an impact on blockchain-IoT integration has been highlighted alongside recommended mitigation strategies in Table 5.

Table 5. Blockchain-IoT Security Vulnerabilities and Mitigations

Vulnerability	**Mitigation Strategies**	**References**
51% Attack	Implement an algorithm that adjusts the mining difficulty based on the total computational power of the IoT network, making it harder for an attacker to suddenly overwhelm the system.	(Sayeed et al., 2019)
	Implement a proof-of-stake (PoS) consensus mechanism instead of proof-of-work (PoW) to reduce the risk of 51% attacks.	
Double Spending	Implement a confirmation mechanism that requires multiple blocks to be added to the chain before a transaction is considered final.	(Pérez-Solà et al., 2019)
	Use a consensus mechanism that prioritizes transaction finality, such as practical Byzantine fault tolerance (PBFT).	

Table 5. Blockchain-IoT security vulnerabilities and mitigations continued

Sybil Attack	Implement a reputation system that assigns higher weights to nodes with a proven track record of honest behavior	(Li et al., 2020)
	Use a proof-of-authority (PoA) consensus mechanism that requires nodes to be approved by a central authority before joining the network.	
Replay Attack	Implement a nonce or timestamp mechanism to ensure that each transaction is unique and cannot be replayed	(Yang et al., 2019)
	Use a secure communication protocol, such as transport layer security (TLS), to prevent attackers from intercepting and replaying messages	
Quantum Computing Threat	Use a post-quantum cryptographic algorithm, such as lattice-based cryptography, to secure the blockchain against quantum computing attacks	(Fernández-Caramés et al., 2019)
	Implement a hybrid approach that combines classical and post-quantum cryptography to provide both short-term and long-term security	
Firmware Vulnerabilities	Use blockchain to store and verify cryptographic hashes of firmware versions.	(Boudguiga et al., 2017)
	Implement smart contracts to manage the firmware update process, including version control and authorization.	

Case Study 2: Walmart's Blockchain Quest with IBM

To support research objective 2, this case study examines Walmart's innovative effort to integrate blockchain technology into its food supply chain management system in collaboration with IBM. The case study examines how the strategic [3]application of blockchain technology, combined with IoT devices, can transform the tracking and tracing of food products from farm to shelf. The goal is to illustrate how these technologies enable real-time monitoring, greater transparency, and improved decision-making for Walmart and its supply chain partners.

In 2016, Walmart partnered with IBM to develop a blockchain-based food traceability system using Hyperledger Fabric, a robust, enterprise-level blockchain framework. The primary goals were to increase transparency, reduce the time required to trace the origins of food products, and facilitate swift actions in response to food safety incidents. The Walmart-IBM partnership began with two proof-of-concept (PoC) projects aimed at tracing the sources of mangoes in the US and pork in China. These PoCs utilized IoT devices to gather real-time data at various points in the supply chain, including temperature, humidity, and location. This data was recorded on the blockchain, creating an immutable and transparent record of each food product's journey from farm to store.

[3] https://www.hyperledger.org/case-studies/walmart-case-study

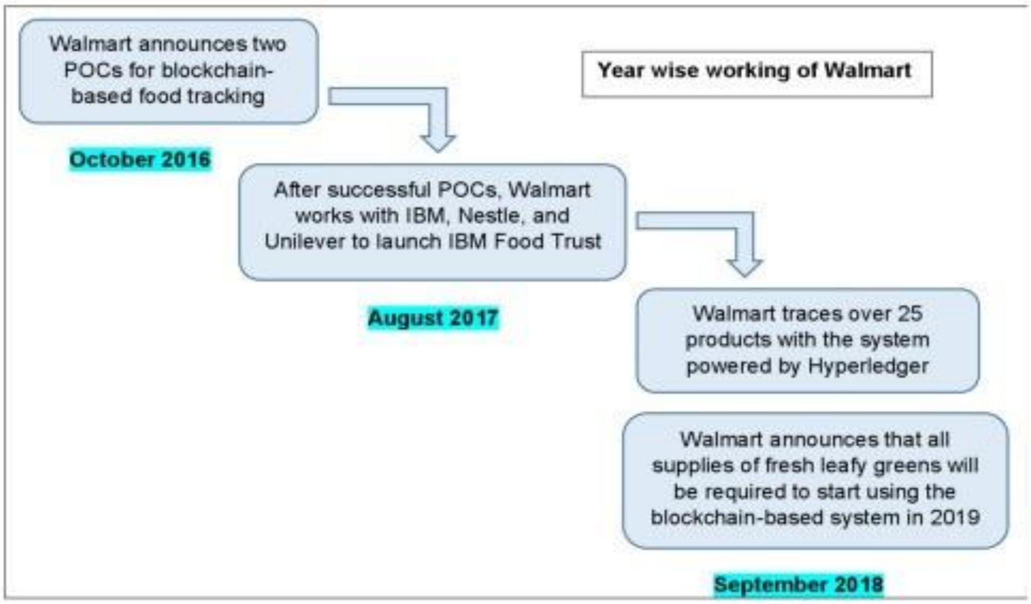

Walmart announces two POCs for blockchain-based food tracking
Year wise working of Walmart
October 2016
After successful POCs, Walmart works with IBM, Nestle, and Unilever to launch IBM Food Trust
August 2017
Walmart traces over 25 products with the system powered by Hyperledger
Walmart announces that all supplies of fresh leafy greens will be required to start using the blockchain-based system in 2019
September 2018

Figure 3:Timeline of Walmart's Blockchain-based Food Tracking Initiative

Case Analysis

Walmart's adoption of blockchain technology for its food traceability system showcases the strategic implementation of Hyperledger Fabric, a permissioned blockchain framework that offers a modular architecture for customization. The system leverages smart contracts, referred to as "chain code" in Hyperledger Fabric, to automate transactions and encode business logic specific to Walmart's requirements. To ensure data consistency and interoperability among supply chain participants, Walmart collaborated with GS1, a global standards organization, to define the data attributes for blockchain upload. The company's technology team played a crucial role in integrating the blockchain application with existing enterprise systems, enabling seamless data flow and compatibility with legacy infrastructure. Hyperledger Fabric's permissioned and private nature allows Walmart to control network access, ensuring that only authorized participants can view and transact on the blockchain, thereby protecting sensitive business information while maintaining transparency. The architecture of Hyperledger Fabric is designed for scalability, enabling Walmart to expand the system to more products and suppliers, while the use of channels and parallel transaction execution ensures high performance and throughput.

Research Objective 2: What are current opportunities and challenges influencing the integration of blockchain in IoT ecosystems? (Qureshi et al., 2021)

The Walmart-IBM case study highlights findings that offer valuable insights into both the potential benefits of integrating blockchain within IoT ecosystems. However, the case study also revealed several challenges influencing the integration of blockchain in IoT ecosystems which are discussed below.

Findings and Mitigation Strategies

Blockchain and IoT integration at Walmart significantly revolutionized traceability within the food supply chain, reducing the time to trace product origins from 7 days to just 2.2 seconds. This innovative approach leverages IoT devices to capture real-time data at every stage of the supply chain, securely recording it on an immutable blockchain ledger. This enhanced traceability ensures unprecedented transparency, enabling swift responses to food safety incidents by pinpointing product origins swiftly. Moreover, the synergy between blockchain and IoT technologies enhances food safety measures by continuously monitoring environmental conditions. IoT sensors detect fluctuations in temperature, humidity, and other factors that affect food quality, with blockchain recording this data to identify potential risks early and reduce food waste. The integration also optimizes supply chain operations, automating data sharing among stakeholders and minimizing manual intervention. This efficiency not only reduces administrative costs but also accelerates decision-making processes through smart contracts that automate transactions and compliance checks. Walmart's collaboration with IBM Food Trust, which includes major players like Nestle and Unilever, exemplifies the potential for industry-wide standardization and collaboration. This collective effort promises a more transparent and efficient food supply ecosystem, demonstrating the scalability of blockchain technology across a global, complex supply chain.

Interoperability Challenges

The case study highlights significant challenges in blockchain-IoT integration such as interoperability and standardization across diverse supply chain participants. Different blockchain platforms and IoT devices must seamlessly communicate and exchange data, necessitating industry-wide standards and protocols to overcome integration barriers which can be particularly challenging. Developing cross-chain communication protocols is essential for addressing interoperability issues in blockchain-IoT integration (Belchior et al., 2021). Cross-chain solutions like Polkadot can reduce interoperability issues by up to 40% in complex IoT environments. These advancements are crucial for creating a cohesive blockchain-IoT ecosystem where different devices and platforms can interact without friction (Belchior et al., 2021).

Adoption & Collaboration

Widespread adoption of blockchain in IoT in the supply chain domain hinges on convincing suppliers, distributors, and other stakeholders of the benefits of blockchain and IoT integration, this requires fostering a collaborative ecosystem, providing necessary training and support, and demonstrating tangible advantages such as improved efficiency and transparency. To overcome adoption barriers and manage the organizational changes required for blockchain-IoT integration, comprehensive educational resources and phased implementation strategies are essential. Walmart's supplier onboarding program for blockchain adoption in the case study serves as a practical example of this approach. The program provided targeted training and support to suppliers, helping them understand the benefits of blockchain technology and guiding them through the implementation process. Kamble et al. (2020) found that such comprehensive training programs increased blockchain adoption rates by 60% among supply chain participants. A phased implementation approach allows organizations to gradually introduce blockchain-IoT solutions, starting with pilot projects and scaling up based on lessons learned. This strategy helps in managing resistance to change, allows for iterative improvements, and provides tangible proof of concept to stakeholders, thereby facilitating wider adoption.

Scalability Challenges

As the Walmart network grew to include thousands of suppliers, ensuring the blockchain could handle the increased transaction volume without compromising performance became a significant challenge. IoT networks generate vast amounts of data, blockchain systems must be capable of processing and storing this information efficiently. Current blockchain architectures often struggle with the high transaction volumes and real-time processing requirements of IoT environments (Shammar et al., 2021). This scalability issue can lead to slower transaction confirmation times and increased costs, potentially undermining the benefits of integration. To address the scalability challenges in blockchain-IoT integration, sharding techniques and layer-2 solutions have emerged as promising mitigation strategies (Xu et al., 2019). Sharding involves dividing the blockchain network into smaller, more manageable segments, allowing for parallel processing of transactions.

[4]Ethereum 2.0's implementation of sharding is a prime example of this approach (Xu et al., 2019).

Cost of Implementation

The initial investment required for blockchain implementation, including hardware, software, and training, was substantial, potentially creating barriers for smaller participants in the supply chain (Hoffman 2021). To mitigate the high costs associated with blockchain-IoT implementation, developing consortium models for cost-sharing has proven effective. The IBM Food Trust consortium model exemplifies this approach, where multiple organizations in the food supply chain collaborate and share the costs of blockchain infrastructure. Consortium models reduced individual implementation costs by up to 50% for small and medium-sized enterprises (Lacity 2020). By distributing the financial burden across multiple participants, consortium models make blockchain-IoT integration more accessible to a wider range of organizations, including smaller players who might otherwise be priced out. Additionally, these collaborative models often lead to shared standards and best practices, further enhancing the overall efficiency and effectiveness of the blockchain-IoT ecosystem.

[4] https://static1.squarespace.com/static/563240cae4b056714fc21c26/t/5bc13eb5b208fcee0e8ad937/1539391159544/LacityMISQEBlockchains2018.pdf

Energy Consumption

It is also commonly known that many blockchain consensus mechanisms, particularly those used in public blockchains, are energy intensive. This poses a significant challenge when integrating with IoT devices, which are often designed to be energy-efficient and may have limited power resources. Transitioning to more energy-efficient consensus mechanisms, such as Proof of Stake (PoS), is a crucial strategy for addressing the energy consumption concerns in blockchain-IoT integration. Ethereum's ongoing transition to PoS, known as Ethereum 2.0, is a prime example of this approach.

Regulatory Compliance

Governance and regulatory compliance become more complex in the decentralized, cross-border environments typical of IoT ecosystems. Implementing compliance-by-design architectures is essential for navigating regulatory challenges in the integration of blockchain and IoT systems. Hyperledger Fabric’s use of private channels provides a practical example, especially for adhering to GDPR requirements. These private channels enable the creation of isolated sub-networks within the blockchain, where sensitive information is shared only among authorized parties, effectively addressing data privacy concerns. Research by (Lima et al., 2022) shows that compliance-by-design strategies can reduce regulatory issues in blockchain-IoT systems by up to 70%. By embedding regulatory compliance into the initial design of blockchain-IoT solutions, organizations can preemptively ensure their systems meet legal standards, avoiding the need for costly retrofits later. This proactive methodology not only mitigates legal risks but also fosters trust among users and regulators, promoting broader adoption and acceptance of blockchain-IoT technologies.

Integration of Legacy Systems

Integrating legacy IoT systems with blockchain frameworks presents both technical and financial challenges because many industries rely on established IoT infrastructure that may not be readily compatible with blockchain technology. The cost and complexity of integrating or replacing these legacy systems can be a significant barrier to adoption. Mitigation strategies for this challenge include the development of middleware solutions and the implementation of hybrid architectures. Hybrid architecture allows organizations to gradually migrate to blockchain-IoT solutions while maintaining critical legacy functionalities. Organizations implementing hybrid blockchain architectures were able to reduce integration costs by up to 30% compared to full system overhauls (Gartner 2019). However, it's important to note that while these solutions can facilitate integration, they also introduce additional complexity and potential points of failure. Samaniego and Deters (2016) found that poorly implemented middleware in IoT-blockchain systems could introduce latency of up to 15%, highlighting the need for careful design and optimization.

The findings from the Walmart-IBM case study highlight the considerable impact of both the opportunities and challenges in integrating blockchain with IoT ecosystems. The findings demonstrate the potential for blockchain-IoT integration to revolutionize IoT domains like supply chain. Blockchain in supply chain management provides enhanced security, traceability, improving food safety, and optimized efficiency. However, the case study also reveals the need to address challenges related to interoperability across diverse IoT deployments and blockchain protocols, data quality which is essential for the effectiveness of blockchain-based solutions due to the immutable nature of the technology and stakeholder collaboration to fully harness the power of these technologies. As Walmart and other industry players continue to explore and implement blockchain-IoT solutions, they must navigate these challenges while leveraging the opportunities to drive positive change across various domains.

CHAPTER FIVE

DISCUSSION, CONCLUSION AND AREAS FOR FURTHER STUDY

Chapter five provides a discussion and conclusions of the findings in Chapter 4 and offers recommendations of areas for further study for each research objective.

Discussion

The case studies reviewed in this culminating project illustrate the transformative potential of blockchain technology within IoT ecosystems. The 2016 DAO attack revealed significant vulnerabilities in blockchain implementations, especially regarding smart contracts and governance mechanisms. This incident underscored the necessity for thorough IoT-specific security audits, robust governance frameworks, and the complexities tied to blockchain's immutability. Conversely, Walmart's collaboration with IBM highlighted the strategic application of blockchain technology combined with IoT devices to revolutionize supply chain management. The successful deployment of a blockchain-based food traceability system demonstrated the potential for greater transparency, enhanced food safety, and improved efficiency within IoT ecosystems.

Research Objective 1: How do emerging vulnerabilities manifest in the implementation of blockchain within current IoT ecosystems?

The DAO attack case study revealed that emerging vulnerabilities in blockchain implementations within IoT ecosystems can manifest in the form of exploitable coding flaws in smart contracts, governance risks posed by decentralized decision-making, and immutability challenges when vulnerabilities are discovered post-deployment. The attack demonstrated the complexity of securing smart contracts and the potential for compounding vulnerabilities in blockchain systems. As IoT ecosystems increasingly leverage blockchain and smart contracts for various applications, such vulnerabilities could enable attacks that could lead to cascading failures due to the decentralized nature of IoT deployments. The findings from the DAO attack case study amongst many other things emphasize the importance of comprehensive security audits and testing for smart contracts deployed in IoT environments. The decentralized governance models often employed in blockchain systems present another vulnerability vector. While decentralization offers benefits, it can also lead to decision-making paralysis or conflicts when critical security issues need to be addressed swiftly. This is especially problematic in IoT environments where real-time response to threats may be crucial to prevent physical damage or service disruptions. To mitigate these risks, it's essential to incorporate robust security analysis and design principles throughout the system development lifecycle of blockchain-IoT systems. This includes conducting thorough code audits, employing formal verification techniques, and implementing comprehensive testing protocols that account for the unique characteristics of decentralized systems. Furthermore, the reputational and legal fallout from the attack underscores the broader risks associated with blockchain vulnerabilities and the importance of establishing clear liability and regulatory frameworks for IoT blockchain applications.

Areas for further study in this research question include investigating the development of formal verification methods for smart contracts to identify and eliminate vulnerabilities before deployment in IoT environments. Exploring the use of advanced cryptographic techniques in edge computing nodes for security and software defined networking for optimized network performance in blockchain-IoT deployments.

Research Objective 2: What are current opportunities and challenges influencing the integration of blockchain in IoT ecosystems?

The Walmart-IBM case study highlighted several opportunities and challenges influencing the integration of blockchain in IoT ecosystems. Walmart’s successful implementation of a blockchain-based food traceability system demonstrated the potential for enhanced traceability, improved food safety, and increased efficiency. By leveraging IoT devices to capture data at various points and recording this information on an immutable blockchain ledger, stakeholders can achieve unprecedented levels of transparency and traceability. The combination of blockchain and IoT technologies enables continuous monitoring, early issue detection, and waste reduction. Furthermore, blockchain-IoT integration streamlines supply chain processes, reduces manual intervention, and enables automated data sharing among stakeholders, leading to increased operational efficiency and cost savings. In the supply chain domain, companies like Maersk and FedEx have leveraged blockchain-IoT integration to optimize logistics operations and improve cargo tracking. In the energy sector, firms such as Power Ledger and LO3 Energy are utilizing blockchain and IoT devices to create decentralized energy trading platforms, enabling peer-to-peer transactions and more efficient grid management.

However, the case study also revealed significant challenges related to interoperability, scalability, cost of implementation, energy consumption and integration of legacy systems. Integrating blockchain and IoT technologies successfully across diverse IoT ecosystems and blockchain protocols requires standardization. The lack of industry-wide standards and protocols can hinder the successful integration of these technologies. Ensuring the accuracy and reliability of data captured by IoT devices is equally crucial for the effective functioning and increased trust in the blockchain-IoT ecosystem. Additionally, integrating blockchain and IoT technologies requires the participation and collaboration of multiple stakeholders, which can be challenging, especially for smaller entities with limited resources. Recommendations are for the design of standardized protocols which can be compatible across various IoT deployments and blockchain protocols, design of robust data validation mechanisms and reliable connectivity solutions to ensure the accuracy and reliability of data captured by IoT devices in blockchain ecosystems and the consideration of legacy IoT systems and the feasibility of blockchain integration in that use case. Efficient consensus mechanisms to support scalability and faster transaction processing times in IoT environments are also recommended.

Areas for further study in this research question include investigating the development of industry-wide standards and protocols for blockchain-IoT integration to enhance interoperability and data exchange and improving blockchain security against quantum attacks. Additionally, exploring blockchain integration in legacy systems which will be more challenging to match up with complex computational algorithms required by blockchain and which will be more vulnerable in the coming years. Finally, to expand on the findings of this qualitative study, an area for further study can be an experimental study on the integration of blockchain on an IoT device.

Conclusion

In conclusion, the case studies in this research project underscore the significant impact that blockchain technology can have on IoT systems. As IoT continues to expand across various industries, strategically implementing blockchain will be crucial for enhancing the security, reliability, and efficiency of these systems. These case studies pave the way for further exploration into several key areas: defining minimum security requirements for IoT software development that can support the complex computational needs of blockchain integration, verifying the accuracy of smart contracts before their deployment in blockchain-IoT environments, and developing adaptable governance models. Additionally, understanding the legal and regulatory issues surrounding blockchain implementation, and establishing standards and protocols to ensure interoperability across diverse IoT devices and use cases are essential. Improving data validation methods in blockchain transactions within IoT systems and fostering collaboration among stakeholders in the IoT ecosystem are also critical areas for further research and development. By addressing these challenges, researchers and practitioners can help create secure, transparent, and efficient blockchain-IoT ecosystems, setting the stage for transformative innovations in the IoT landscape.

APPENDIX A

BLOCKCHAIN - IOT REAL WORLD USE CASES

Industry	Company/Project	Use Case
Supply Chain	IBM & Maersk	TradeLens blockchain platform for transparent efficient global shipping information sharing
Agriculture	Bayer Crop Science & BlockApps	IoT-integrated blockchain platform for transparent, efficient crop management
Energy	Brooklyn Microgrid	P2P energy trading using IoT and blockchain
Healthcare	Chronicled	IoT-blockchain for pharmaceutical product integrity and traceability
Manufacturing	IOTA & Jaguar Land Rover	Secure data sharing between vehicles and IoT devices using blockchain
Insurance	Aon & Ninepoint Partners	Usage-based insurance models leveraging IoT data on blockchain
Recycling	Plastic Bank	Incentivized plastic recycling using blockchain and IoT-enabled collection machines
Logistics	Modum	Temperature monitoring of pharmaceuticals in transit using IoT and blockchain
Smart Cities	CityXChange	IoT data integration for smart city applications

REFERENCES

Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2023). Blockchain and COVID-19 pandemic: applications and challenges. *Cluster Computing*, *26*(4), 2383–2408. https://doi.org/10.1007/s10586-023-04009-7

Atlam, H., Alenezi, A., Alassafi, M., Willis, G.(2018). Blockchain with Internet of Things: benefits, challenges, and future directions - ePrints Soton. (2018, June 1). https://eprints.soton.ac.uk/421529/

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In *Lecture notes in computer science* (pp. 164–186). https://doi.org/10.1007/978-3-662-54455-6_8

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Banerjee, M., Lee, J., & Choo, K. R. (2018, August 1). *A blockchain future for internet of things security: a position paper*. Digital Communications and Networks. https://doi.org/10.1016/j.dcan.2017.10.006

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A Survey on Blockchain Interoperability: Past, Present, and Future Trends. ACM Computing Surveys, 54(8), 1–41. https://doi.org/10.1145/3471140

Benarroche, A. (2022). Jaguar Land Rover to Reward Drivers for Sharing Data via IOTA Blockchain. CoinDesk. Retrieved from https://www.coindesk.com/business/2022/04/28/jaguar-land-rover-to-reward-drivers-for-sharing-data-via-iota-blockchain/

Brent, L., Jurisevic, A., Kong, M., Liu, E., Gauthier, F., Gramoli, V., Holz, R., & Scholz, B. (2018, September 11).*Vandal: A Scalable Security Analysis Framework for Smart Contracts*arXiv.org. https://arxiv.org/abs/1809.03981

Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., & Debnath, N. C. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*, *61*, 102360. https://doi.org/10.1016/j.scs.2020.102360

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017, May). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 772-777). IEEE.

Borrero, J. D. (2021). Smart farming: A holistic approach towards sustainable agriculture using blockchain and IoT technologies. Journal of Cleaner Production, 298, 126783.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017). Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain. (2017, April 1). IEEE Conference

Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7966970

Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, *20*(4), 398–461. https://doi.org/10.1145/571637.571640

Christidis K., & Devetsikiotis R.(2016) *Blockchains and Smart Contracts for the Internet of Things*. (2016). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7467408

Douceur, J. R. (2002). The Sybil Attack. In *Lecture notes in computer science* (pp. 251–260). https://doi.org/10.1007/3-540-45748-8_24

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing*, *134*, 180–197. https://doi.org/10.1016/j.jpdc.2019.08.005

DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. Bitcoin and beyond, 157-177.

Fei, W., Ohno, H., & Sampalli, S. (2023, November). *A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions*. ACM Computing Surveys. https://doi.org/10.1145/3625094

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2019). *Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum*

Computing Attacks. (2020). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8967098

Ferrag, M., Derdour, Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018) *Blockchain Technologies for the Internet of Things: Research Issues and Challenges*. (2019, April 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8543246

Gonczol, P., Katsikouli, P., Herskind, L., & Dragoni, N. (2022). *Blockchain Implementations and Use Cases for Supply Chains-A Survey*. (2020). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8952728

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019a, August 1). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2019.02.060

Hyperledger Foundation Case Study. (2019). Case Study. How walmart brought unprecedented transparency to the food supply chain with hyperledger fabric Hyperledger Foundation.

Jentzsch, C. (2016). Decentralized autonomous organization to automate governance. White paper, November.

Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. International Journal of Information Management, 52, 101967.https://www.sciencedirect.com/science/article/pii/S0268401218312118

Kamilaris, A., Fonts, A., & Prenafeta-Boldύ, F. X. (2019). The rise of blockchain technology in agriculture and food supply chains. Trends in Food Science & Technology, 91, 640-652.

Khan, M. A., & Salah, K. (2018, May 1). *IoT security: Review, blockchain solutions, and open challenges*. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2017.11.022

Li, X., Jiang, P., Chen, T., Wang, L., & Wen, Q. (2020). *A survey on the security of blockchain systems*. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2017.08.020

Lacity, M. C. (2020). Addressing key challenges to making enterprise blockchain applications a reality. MIS Quarterly Executive, 19(1), 65-77.

Liang, X., & Kim, Y.(2021). *A Survey on Security Attacks and Solutions in the IoT Network*. IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9376174

Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., ... & Palombini, M. (2019). 'Fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine, 17(1), 1-17.

Mao, D., Hao, Z., Wang, F., & Li, H. (2018). Innovative Blockchain-Based Approach for Sustainable and Credible Environment in Food Trade: A

Case Study in Shandong Province, China. *Sustainability*, *10*(9), 3149. https://doi.org/10.3390/su10093149

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Applied Energy, 210, 870-880

Merre, M. (2016). $50 Million Hack Shows the Dangers of 'Smart Contracts'. Vice. June 18, 2016

Nguyen, T. C., Hoang, T.D., Niyato, D, Nguyen, T.H., Dutkiewicz, E., (2019). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and *Opportunities*. (2019). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8746079

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT Integration: A Systematic Survey. *Sensors*, *18*(8), 2575. https://doi.org/10.3390/s18082575

Pérez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2018). Double-spending prevention for Bitcoin zero-confirmation transactions. *International Journal of Information Security*, *18*(4), 451–463. https://doi.org/10.1007/s10207-018-0422-4

Qureshi, J. N., Farooq, M. S., Abid, A., Umer, T., Bashir, A. K., & Zikria, Y. B. (2022). *Blockchain applications for the Internet of Things: Systematic* *review and challenges*. Microprocessors and Microsystems. https://doi.org/10.1016/j.micpro.2022.104632

Ralph, O. (2021). Aon and Ninepoint launch $50m blockchain and crypto insurance fund. Financial Times. Retrieved from https://www.ft.com/content/1e4e2e3f-8a5f-4e5e-b8c0-0f1f9c3d8b2e

Reyna, A., Martin, C. L., Chen, J., Soler, E., & Díáz, M. (2018). *On blockchain and its integration with IoT. Challenges and opportunities*. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2018.05.046

Robert K. Yin. (2017). Case Study Research Design and Methods (7th ed.) . Thousand Oaks, CA: Sage. 282 pages. (ISBN 978-1-4522-4256-9).

Samaniego, M., & Deters, R. (2016, December). *Blockchain as a Service for IoT*. (2016, December 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7917130

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences*, *9*(9), 1788. https://doi.org/10.3390/app9091788

Shammar, E. A., Zahary, A. T., Amgad, A., & Elshakankiry, O. (2021). *A Survey of IoT and Blockchain Integration: Security Perspective*. (2021). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9622256

Singh, S. K., & Kumar, S. (2022, June 30). *Blockchain Technology: Introduction, Integration, and Security Issues with IoT*. Apple Academic Press eBooks. https://doi.org/10.1201/9781003231332-2

Tran, N. K., Babar, A., & Boan, J. (2021, January 1). *Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs*. Journal of Network and Computer Applications. https://doi.org/10.1016/j.jnca.2020.102844

Tsai, C., Lin, C., Liao, S. (2023) *Unveiling Vulnerabilities in DAO: A Comprehensive Security Analysis and Protective Framework*. (2023, December 17). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/10411467

Wang, X., Zha, X. F., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019, February 1). *Survey on blockchain for Internet of Things*. Computer Communications. https://doi.org/10.1016/j.comcom.2019.01.006

Wohrer, M., & Zdun, U. (2018).*Smart contracts: security patterns in the ethereum ecosystem and solidity*. (2018, March 20). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8327565

Xu, Q., Su, Z., Yang, Q.(2019) Blockchain-Based Trustworthy Edge Caching Scheme for Mobile Cyber-Physical System. (2020, February 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8889686

Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019) *Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges*. (2019, January 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8624417

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, *29*(2), 105–117. https://doi.org/10.1016/j.infoandorg.2019.03.001

Zarrin, J., Phang, H. W., Saheer, L. B., & Zarrin, B. (2021). Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Computing*,*24*(4), 2841–2866.https://doi.org/10.1007/s10586-021-03301-8

Zwitter, A. J., & Hazenberg, J. (2020). Decentralized Network Governance: Blockchain Technology and the Future of Regulation. *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.00012