IMPACT OF BLOCKCHAIN SYSTEM ON PRIVACY AND SECURITY OF USER'S DATA AND TRANSACTIONS IN FINTECH INDUSTRIES OF NEPAL

SURYA RAJ BISTA

A thesis submitted in fulfilment of the

requirements for the award of the degree of

M.Sc. in Information Technology Management

Asia Pacific University of Technology & Innovation (APU)

School of Computing and Technology

SEPTEMBER 2023

IMPACT OF BLOCKCHAIN SYSTEM ON PRIVACY AND SECURITY OF USER'S DATA AND TRANSACTIONS IN FINTECH INDUSTRIES OF NEPAL

surya raj bista

Asia Pacific University of Technology and Innovation

(APU)

# DECLARATION OF THESIS CONFIDENTIALITY

Author’s full name: Surya Raj bista

IC No./Passport No.: np000689

Thesis/Project title: **THE IMPACT OF BLOCKCHAIN SYSTEM ON PRIVACY AND SECURITY OF USER'S DATA AND TRANSACTIONS IN FINTECH INDUSTRIES OF NEPAL**

I declare that this thesis is classified as:

CONFIDENTIAL

RESTRICTED

OPEN ACCESS

I acknowledged that Asia Pacific University of Technology & Innovation (APU) reserves the right as follows:

1. The thesis is the property of Asia Pacific University of Technology & Innovation (APU).
2. The Library of Asia Pacific University of Technology & Innovation (APU) has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

|  |  |
| --- | --- |
| Author’s Signature: | …………………………… |
| Date: | 12 September 2023 |
|  |  |
| Supervisor’s Name: | Suman bhattacharya |
| Date: | 12 September 2023 |
| Signature: | …………………………… |

# 

# DECLARATION OF SUPERVISOR(S)

“I hereby declare that I have read this thesis and in my

opinion this thesis is sufficient in terms of scope and quality for the award of the degree of

Master of Science in Information Technology Management”

|  |  |
| --- | --- |
| Name of Supervisor: | suman bhattacharya |
| Signature: | …………………………… |
| Date: | 12 September 2023 |

# DECLARATION OF ORIGINALITY AND EXCLUSIVENESS

I declare that this thesis entitled

THE IMPACT OF BLOCKCHAIN SYSTEM ON PRIVACY AND SECURITY OF USER'S DATA AND TRANSACTIONS IN FINTECH INDUSTRIES OF NEPAL

is the result of my own research work except as cited in the references. This thesis has not been accepted for any degree and it is not concurrently submitted in candidature of any other degree.

|  |  |
| --- | --- |
| Signature: |  |
| Name: | Surya Raj Bista |
| Date: | …………………………… |

# DEDICATION

I dedicate this thesis to my beloved sisters "Bhubi" and "Puspa", and my mom who has been instrumental on inspiring throughout the thesis writing process. They made me much motivated and supported in the encouraging way whenever I felt the difficult in time and they added the confidence on me.

# **ACKNOWLEDGEMENTS**

First of all, I would like to thank The Lord Buddha Campus and The ASIA PACIFIC UNIVERSITY for providing me the opportunity to pursue Masters in Science and Information Technology Management.

With the completion of the report, there are many people to whom I would like to express my gratitude and appreciation for the efforts they have provided me to throughout my journey.

My indebtedness goes to my supervisor Mr. Suman Bhattacharya for constantly putting his efforts into his kind direction, valuable suggestions, and proper guidance. I would also like to thank Mrs.Hiru and Mrs. Janaki for supporting me on the primary data collection.

Finally, I would like to thank each and everyone who has been supporting and encouraging me to complete this thesis.

# **ABSTRACT**

The Fintech industry is currently a booming industry. With the growing digitization and modernization, various threats have arisen as a result of which the fintech industry has become vulnerable and prone to data and information breaches and hacks. Hence, in order to find a solution to this problem, quantitative research was conducted among 402 participants to find out the perceived value of security and privacy among Fintech users and also to find out whether blockchain solves privacy and security issues in Fintech.

A detailed questionnaire was prepared for each variable i.e., privacy, security and blockchain and then they were distributed among the employees of Fintech and IT organizations and responses were collected. During the research, Blockchain was considered to be the independent variable and privacy and security were the dependent variables.  The results were analyzed with the help of SPSS tools. In addition, a detailed literature review was done by comparing and analyzing research done in the past.

The results showed that privacy and security have a strong positive correlation to blockchain, which means that whenever we implement a blockchain in the fintech industry, the perceived value of a user in terms of privacy and security increases. Thus, Hyperledger fabric, a type of private blockchain, was proposed for better privacy and security of the personal and financial information of the fintech users.

**Keywords**: Blockchain, security, privacy, Hyperledger Fabric

# **LIST OF ABBREVIATIONS**

**Fintech**                                             Financial Technology

**NRB**                                                   Nepal Rastra Bank

**KYC**                                                    Know Your Customer

**QR** **code**                                           Quick Response Code

**BT**                                                       Blockchain Technology

**MSP** Membership Service Provider

**PBFT** ` Practical Byzantine Fault Tolerance

**WFC** Worldwide Financial Community

**DC** Data Centers

**DR** Data Recovery

**HLF** Hyperledger Fabric

**POW** Proof-of-Work

**POS** Proof-of-Stake

**PBFT** Practical Byzantine Fault Tolerance

**IPFS** Interplanetary File System

**SPSS** Statistical Package for Social Sciences

**ANOVA** Analysis of variance

**DLT** Distributed Ledger Technology

**CA** Central Authority

**STR** Suspicious Transaction Report

**SAR** Suspicious Activity Report

**DLT** Distributed Ledger Technology

TABLE OF CONTENTS

[DECLARATION OF THESIS CONFIDENTIALITY i](#_Toc145413200)

[DECLARATION OF SUPERVISOR(S) ii](#_Toc145413201)

[DECLARATION OF ORIGINALITY AND EXCLUSIVENESS iii](#_Toc145413202)

[DEDICATION iv](#_Toc145413203)

[ACKNOWLEDGEMENTS v](#_Toc145413204)

[ABSTRACT vi](#_Toc145413205)

[LIST OF ABBREVIATIONS vii](#_Toc145413206)

[LIST OF FIGURES xi](#_Toc145413207)

[LIST OF TABLES xii](#_Toc145413208)

[CHAPTER 1 INTRODUCTION AND BACKGROUND 1](#_Toc145413209)

[1.1 Introduction to Fintech 1](#_Toc145413210)

[1.2 Fintech Flow, Security and Privacy 4](#_Toc145413211)

[1.3 Blockchain 5](#_Toc145413212)

[1.3 Problem statement 9](#_Toc145413213)

[1.5 Research Questions 10](#_Toc145413214)

[1.6 Objectives and Aims 10](#_Toc145413215)

[1.7 Scope 10](#_Toc145413216)

[1.8 Significance of the Research 11](#_Toc145413217)

[1.9 Structure of the Thesis 11](#_Toc145413218)

[1.10 Summary 12](#_Toc145413219)

[CHAPTER 2 LITERATURE REVIEW 13](#_Toc145413220)

[2.1 Introduction 13](#_Toc145413221)

[2.2 Current Scenario of Fintech 14](#_Toc145413222)

[2.2.1 Gaps in the Fintech Industry 14](#_Toc145413223)

[2.2.2 Shortcomings led by the gaps 16](#_Toc145413224)

[2.2.3 Consequences of a data breach 20](#_Toc145413225)

[2.3 Role of Blockchain in the sustainability of fintech 22](#_Toc145413226)

[2.3.1 The Blockchain technology 23](#_Toc145413227)

[2.3.2 Blockchain for private and secured financial records and transaction 27](#_Toc145413228)

[2.3.3 Security Benefits of Blockchain Over Traditional Methods 29](#_Toc145413229)

[2.3.4 Blockchain as a Solution 30](#_Toc145413230)

[2.4 Related Work 30](#_Toc145413231)

[2.5 Research Gap 41](#_Toc145413232)

[CHAPTER 3 RESEARCH METHODOLOGY 42](#_Toc145413233)

[3.1 Methodology 42](#_Toc145413234)

[3.2 Independent and Dependent Variable 43](#_Toc145413235)

[3.3 Research Strategy 43](#_Toc145413236)

[3.4 Types of Data 44](#_Toc145413237)

[3.5 Research design 45](#_Toc145413238)

[3.6 Sampling type and size 45](#_Toc145413239)

[3.7 Data collection methods 45](#_Toc145413240)

[3.8 Analysis of Data 45](#_Toc145413241)

[3.9 Research timeframe 46](#_Toc145413242)

[3.10 Ethics and Confidentiality 47](#_Toc145413243)

[CHAPTER 4 DATA ANALYSIS AND INTERPRETATION 48](#_Toc145413244)

[4.1 Case Processing Summary 48](#_Toc145413245)

[4.2 Reliability Testing (Cronbach’s Alpha) 48](#_Toc145413246)

[4.3 Descriptive Analysis 53](#_Toc145413247)

[4.3.1 Background of the Respondents 53](#_Toc145413248)

[4.4 Correlation Analysis 58](#_Toc145413249)

[4.4.1 Correlation between Privacy and Blockchain 58](#_Toc145413250)

[4.4.2 Correlation between Blockchain and Security 60](#_Toc145413251)

[CHAPTER 5 FINDINGS AND DISCUSSIONS 68](#_Toc145413252)

[5.1.1 Challenges Faced During the Responses Collection 68](#_Toc145413253)

[5.1.2 Demographic Data 68](#_Toc145413254)

[5.1.3 Interpretation of Findings 69](#_Toc145413255)

[5.2 Conceptual Framework 73](#_Toc145413256)

[CHAPTER 6 CONCLUSION AND RECOMMENDATIONS 80](#_Toc145413257)

[6.1 Conclusion 80](#_Toc145413258)

[6.2 Recommendations 80](#_Toc145413259)

[6.3 Further Contributions 82](#_Toc145413260)

[6.4 Summary 83](#_Toc145413261)

[APPENDICES 89](#_Toc145413262)

# LIST OF FIGURES

[Figure 1: Rise of QR payments in Nepal 12](#_Toc144908606)

[Figure 2: Fintech ecosystem in Nepal 14](#_Toc144908607)

[Figure 3: Current Fintech Mechanism 14](#_Toc144908608)

[Figure 4: The mechanism of blockchain 16](#_Toc144908609)

[Figure 5: Key components of blockchain 17](#_Toc144908610)

[Figure 16:Types of blockchain 18](#_Toc144908611)

[Figure 6: Gaps in Fintech to Blockchain as a solution 23](#_Toc144908612)

[Figure 7: Global fraud and payment survey report 2022 26](#_Toc144908613)

[Figure 8: Yearly receipt of STR/SAR report in the finance sector of Nepal 28](#_Toc144908614)

[Figure 9: Percentage of STR/SAR received in 2021/2022 in various finance sectors of Nepal 28](#_Toc144908615)

[Figure 10: Financial Offences in the financial year 2021/2022 29](#_Toc144908616)

[Figure 11: Percentage spread of costs after suffering from a data breach 31](#_Toc144908617)

[Figure 12: Cost of global data breach by industry 32](#_Toc144908618)

[Figure 13: Hash algorithm in blockchain 33](#_Toc144908619)

[Figure 14:Key characteristics of blockchain 34](#_Toc144908620)

[Figure 15: Shared network in a blockchain 35](#_Toc144908621)

[Figure 17: Consensus algorithms 36](#_Toc144908622)

[Figure 19: Analysis of blockchain features and fintech requirements 37](#_Toc144908623)

[Figure 20: Components and phases of Hyperledger Fabric 38](#_Toc144908624)

[Figure 21: Five phases of the empirical cycle 52](#_Toc144908625)

[Figure 22: Relationship between dependent and independent variable 53](#_Toc144908626)

[Figure 24: Gantt Chart Representing Project Timeline 57](#_Toc144908627)

[Figure 25: Total questionnaire case summary 58](#_Toc144908628)

[Figure 26: Conceptual framework using the Hyperledger Fabric blockchain 84](#_Toc144908629)

[Figure 27: Detailed view of the Hyperledger Fabric architecture for private and secure payment and record of transactions 87](#_Toc144908630)

# LIST OF TABLES

[Table 1: Key 1 Literature Review Overview 41](#_Toc144908640)

[Table 2: Key 2 Literature Review Overview 41](#_Toc144908641)

[Table 3: Key 3 Literature Review Overview 42](#_Toc144908642)

[Table 4: Key 4 Literature Review Overview 43](#_Toc144908643)

[Table 5: Key 5 Literature Review Overview 44](#_Toc144908644)

[Table 6: Comparison of Related works 45](#_Toc144908645)

[Table 7: Research Matrix of 30 research articles 51](#_Toc144908646)

[Table 8: Project Timeline 56](#_Toc144908647)

[Table 10: Reliability test and statistics for total case summary 59](#_Toc144908648)

[Table 11: Reliability for privacy 60](#_Toc144908649)

[Table 12: Overall statistics for all items 60](#_Toc144908650)

[Table 13: Reliability test for security 61](#_Toc144908651)

[Table 14: Reliability test for blockchain 62](#_Toc144908652)

[Table 15: Age-Based Distribution of Respondents 63](#_Toc144908653)

[Table 16: Pie chart of total age-Based Distribution of Respondents 64](#_Toc144908654)

[Table 17: Gender-based distribution of respondents 64](#_Toc144908655)

[Table 18: Pie-chart of gender-based distribution of total respondents 65](#_Toc144908656)

[Table 19: Occupational background of respondents 65](#_Toc144908657)

[Table 20: Pie-chart of occupational background of total respondents 66](#_Toc144908658)

[Table 21: Occupation statistics of respondents 66](#_Toc144908659)

[Table 22: Pie-chart of occupation of various respondents 67](#_Toc144908660)

[Table 23:Monthly income statistics of all respondents 67](#_Toc144908661)

[Table 24: Pie-chart of monthly income of respondents 68](#_Toc144908662)

[Table 25: Statistical representation of correlation between privacy and blockchain 69](#_Toc144908663)

[Table 26: Statistical representation of correlation between blockchain and security 70](#_Toc144908664)

[Table 27: Statistical representation of regression between blockchain and privacy 72](#_Toc144908665)

[Table 28: Statistical representation of regression between blockchain and security 73](#_Toc144908666)

[Table 29: Q-Q plots for Privacy 74](#_Toc144908667)

[Table 30: Q-Q and histogram plots for Security 75](#_Toc144908668)

[Table 31: Q-Q and histogram plots for Blockchain 75](#_Toc144908669)

[Table 32: Mean analysis of privacy and security 77](#_Toc144908670)

[Table 33: Relationship of blockchain with privacy and security 79](#_Toc144908671)

# **CHAPTER 1** **INTRODUCTION AND BACKGROUND**

*This section presents and outlines the research point of view. Additionally, it includes a historical background, explains the main probles and highlights objectives of the thesis including the scope and significance.*

## **Introduction to Fintech**

Gone are the days of excess paperwork, long queues and a hectic environment while making a transaction. With the help development of internet connectivity, information technology, and smartphones and digital devices, there has been an influencing rise in the banking and financial services giving rise to the Fintech sector.

Fintech also referred to as Financial Technology improves traditional finance using new technologies. Fintech is a new way of handling money through data and transactions through various digital smart devices with the help of the internet. In other words, Fintech simplifies and makes financial transactions and services faster and more convenient.

Fintech, an emerging concept, is backed up by diverse cutting-edge technologies. They include innovative business models, various applications and fresh contributions of products and services, which in turn influence the entire financial market and provide financial services.

The land space of Fintech in Nepal is diverse and is in a growing phase. Over the last few years, the use of Fintech has shown a significant rise and has thus made a remarkable impact on various sectors of finance. The main ecosystem areas of Nepal where Fintech is used are as follows:

1. Banks and digital payment services

Fintech has revolutionized banking in Nepal as it has expanded its scope beyond the traditional Internet and electronic banking. Now with the use of mobile banking and various digital payments such as Quick Response(QR) payment, eSewa, Khalti and IME Pay, the rise of Fintech is only promising in the future. The growth of QR payments from the last two financial years has been shown below in Figure 1.

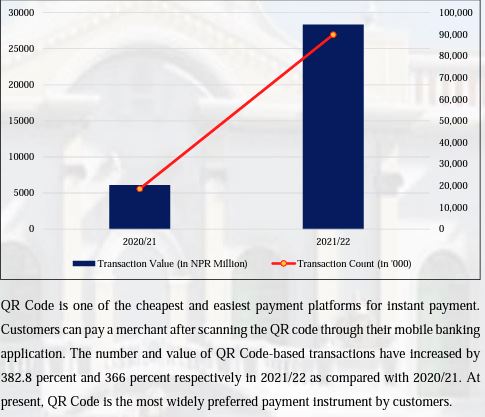


Figure 1: Rise of QR payments in Nepal

Source: (*FIU-NEPAL: ANNUAL REPORT 2021/22*, 2022)

The NRB report shows the growth of QR payments has soared and there is a substantial increase of 382.8% in 2022 when compared to the previous year, 2021. This makes the Quick Response (QR) code payment the most preferred fintech method of payment in Nepal. The figure below shows the rise of QR payments in Nepal from the year 2021 to 2022 (*FIU-NEPAL: ANNUAL REPORT 2021/22*, 2022).

ii) Insurance

The use of Fintech in the insurance industry has been in a flourishing trend and has improved insurance methods and companies. Along with the integration of predictive tools and databases, insurance companies can now study customer behavior through data analysis and forecasting. The insurance companies in Nepal have noticed a need to transition into digital platforms as digital transformation has been helpful for customers to explore diverse insurance offers available. Progressive fintech solutions are moreover imperative in the insurance industries of Nepal.

iii) Financing and Lending

The financial and lending sector facilitates the borrowing and delivery of services and resources for better trade. In recent years, the growth of finance companies has seen promising growth have been categorized as 'Class C' by NRB, and have been providing digital financial services.

iv) Markets and Exchanges

Fintech has revolutionized the trade of bonds and equity and provided traders within the marketplace to sell and buy shares. Nepal Stock Exchange (NEPSE) is currently the most prominent marketplace for securities exchanges. Nepal has now fully digitalized the trading platform and traders no longer have to queue to purchase the initial public offerings (IPO) and for other businesses, thanks to the fintech advancements.

v) Law and Governance

Fintech applications are regulated using various sets of rules and regulations with the law and governance. These regulations are important to ensure standards are met and fintech activities are monitored and documented for audit purposes. Know your Customer (KYC) is a standard followed by Fintech applications in Nepal for any transactions involving money (Joshi & Shah, 2020).

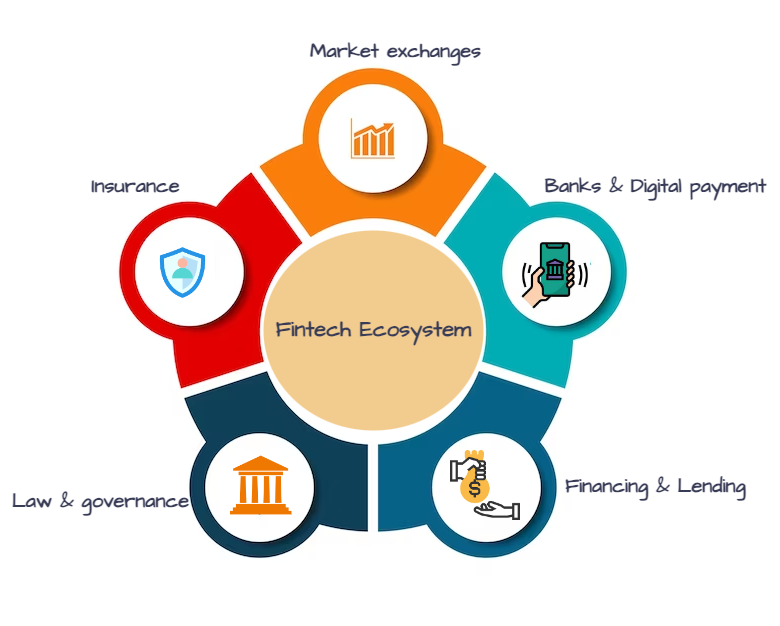


Figure 2: Fintech ecosystem in Nepal

Source: (Nelaturu et al., 2022)

## **1.2 Fintech Flow, Security and Privacy**

Nowadays, traditional paper-based processes have been replaced by digital means in the field of Fintech. This means allowing users to conduct transactions without being limited to a single bank. In Nepal, the NRB is the major regulatory body of Fintech Service Providers.

To ensure proper customer identification and to prevent fraud and anti-money laundering cases, the NRB has authorized the use of Know Your Customer (KYC) forms. The regulatory body has now made it mandatory for fintech service providers to collect consumer information via KYC forms which include basic and all-important personal information. This information is very sensitive and a breach of this data in some way may lead to huge financial losses as well as cause breach of privacy.

The current flow of fintech transactions and storage of information is shown below in Figure 3.

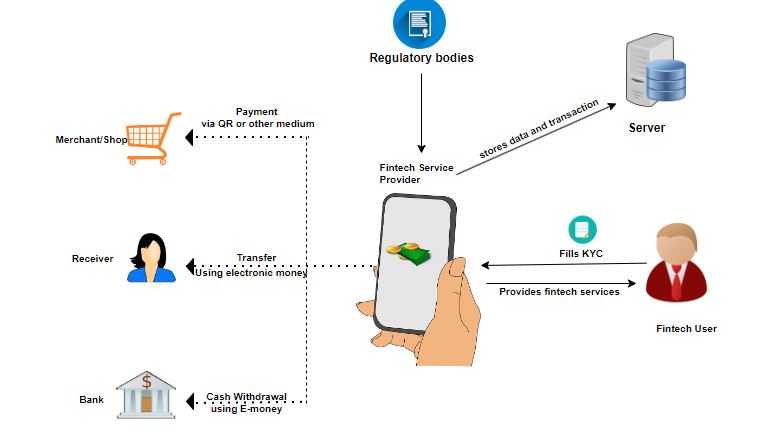


Figure 3: Current Fintech Mechanism

Source: (Nelaturu et al., 2022)

In the current Fintech system of Nepal, whenever a Fintech user wants to make a payment or share data, they are required to fill up a KYC form online for registration which is further stored in the provider's database. Some may also use the Data Centers(DC) and Data Recovery(DR) sites to secure and maintain the data. This KYC is regulated by the NRB which also regulates the fintech providers. When a registered user makes a payment through their device to another merchant or a bank, the transactional data is again then stored in the database (Nelaturu et al., 2022).

But despite this, there are rising security issues such as unauthorized access, data breaches and money theft that occur in the fintech industry. Therefore, better privacy and security measures are in demand to protect users' information and money more than ever in the context of Nepal.

A blockchain-based system has therefore been proposed as a solution to secure user information and money, avoiding access to unauthorized parties and protecting users from cyber-related threats.

## **1.3 Blockchain**

Blockchain is a system that allows storing of data in a secure way. (Nelaturu et al., 2022). The operation of blockchain is shown in Figure 4.

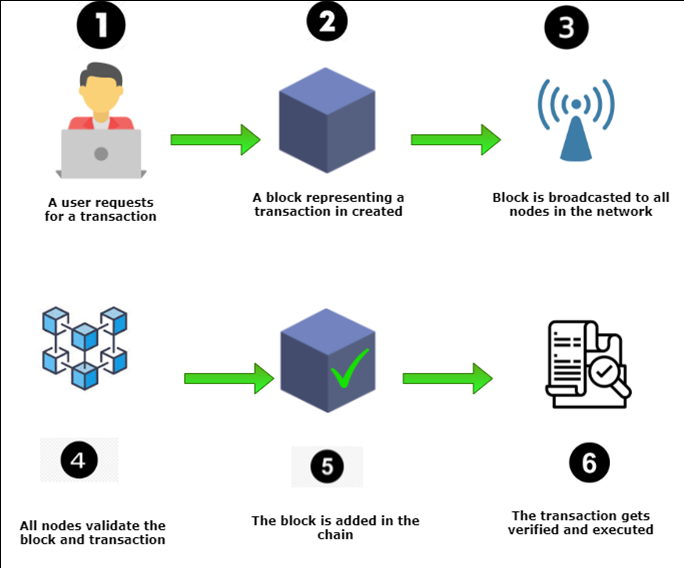


Figure 4: The mechanism of blockchain

(Hegde et al., 2023)

The figure above is the explanation of a blockchain mechanism. Whenever a user requests a transaction, a block is created on a blockchain. These blocks are secured with the help of cryptography, which helps to validate every block, and form a chain within the network. A transaction is executed and verified through this process. Every block comprises a unique hash of either 512 or 256 bits, and together the chain of blocks creates a sequential record (Gad et al., 2022).

All these key components of blockchain technology have been depicted in Figure 5.

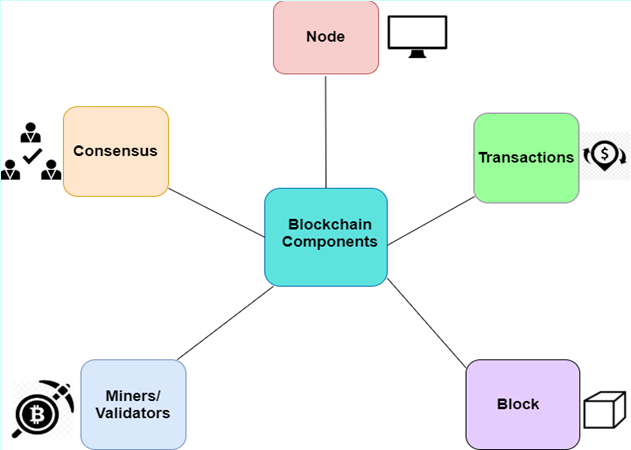


Figure 5: Key components of blockchain

(Muntaha et al., 2023)

* Nodes

The physical devices such as computers or servers within a network where transactions occur are referred to as nodes. Nodes are vital as they create a copy of the distributed ledger whenever a transaction is created or transmitted making the network immutable (Muntaha et al., 2023).

* Transactions

All the operations such as data transfers, modifications and deletions recorded in the blocks are referred to as transactions. They are further validated by the miners and validators.

* Block

A block is a space within a blockchain where data and information are stored. Whenever data is stored in a block or a group of blocks as a transaction, a chain of blocks is secured through the previously added hash.

* Miners/Validators

The secured transactional data backed up by a hash function are gathered by miners to verify the authenticity of blocks to make sure all the transactions across the nodes are valid and prevent any invalid transactions (Guo & Yu, 2022).

* Consensus

Consensus uses an algorithm in a blockchain to validate the transactions and make them authentic. They usually update the shared ledger and are further discussed in the Literature Review.

**Types of blockchain**

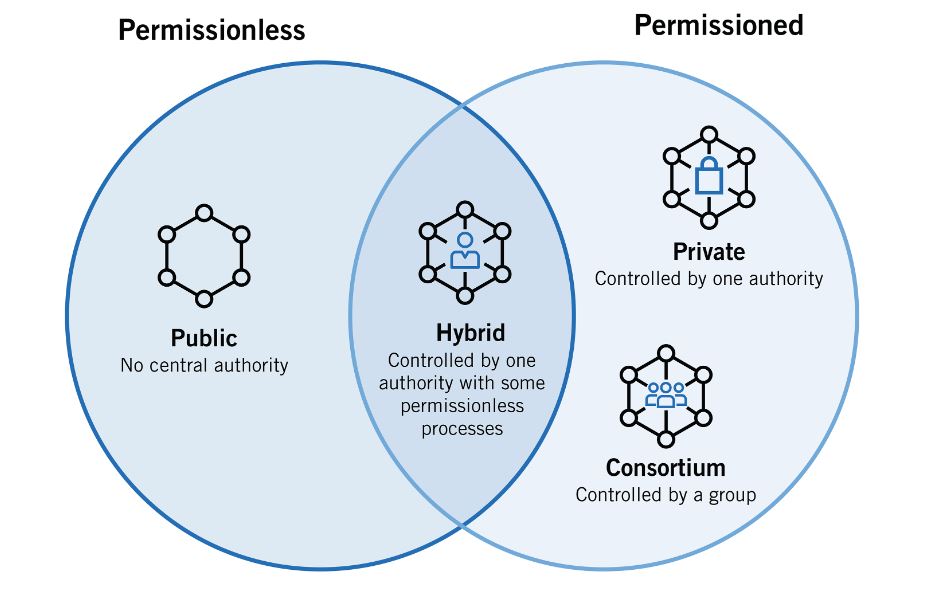


Figure 6:Types of blockchain

(Qian et al., n.d.)

Blockchains can be permissioned, permissionless and hybrid. The permissionless blockchain is usually public in nature and does not restrict the sharing of data within the blockchain network.

Bitcoin and Ethereum are some crucial public blockchains. Permissioned, on the other hand, include private and Consortium blockchain. Private blockchains are used to limit access to specific groups and also limit the participants to join and maintain the network (Nelaturu et al., 2022).

In summary, blockchain is an emerging technology that provides a secure way of storing transactions and this applies to the Fintech sector which will be discussed in chapter 2 in detail.

* 1. **Background Rationale**

Paper records and physical means of storage were used in the past to store financial transactions within bank vaults, and banks acted as the mediators. This process was vulnerable as there were cases of paper and financial documents being stolen or lost through the breakage of the vault or even due to natural causes. With the rise of technology, there was a shift to Fintech where digital records were created and electronic databases were used to store this information and transactions.

In recent years, the volume of data and money circulation in the fintech ecosystem has been immensely increasing. Privacy and Security of every transaction are equally important and each user's personal and financial information must also be protected at any cost. Failure to do so can lead to challenges such as data breach, identity theft, money laundering and hacking of the information, which can further lead to serious damage such as financial, personal and reputational damages. And this fear is only getting worse as there are increasing cases of fraud and data breaches in the fintech sectors.

Fintech firms and regulatory bodies must therefore mitigate these challenges and improve the privacy and security of the personal and transactional data.

## **Problem statement**

One of the primary motives of Fintech services is to manage money and data with a strong focus on privacy and security. To achieve this, the fintech companies have used measures like access control, encryption, firewalls, and audit. Despite these measures, the industry still has privacy and security challenges.

The biggest concern is the risk of cybercriminals targeting the fintech companies to gain unauthorized access to sensitive personal and financial information which can lead to the breach of the data. This breach of data can lead to financial fraud, identity theft and reputational damage. Money laundering and other financial crimes are also a result of this breach. The rising technological vulnerabilities and collaboration of the third-party service providers are a contributor to risks. Therefore, fintech companies need to implement new solid measures for security and prioritize privacy to build better trust and avoid threats.

In summary, the Fintech industries of Nepal face the following challenges:

* The Fintech sector in Nepal is susceptible to privacy and security risks as the Fintech industry is vulnerable to attacks, making it difficult to maintain adequate security and privacy.
* There is a lack of a robust framework to secure payments and maintain data privacy in the Fintech industry in Nepal.

## **1.5 Research Questions**

The research will address these questions:

1. What is the current state of the fintech industry in Nepal in terms of the privacy and security of users' personal and financial information?
2. Is there any significant relationship between the privacy of user data and the Blockchain system used?
3. Is there any significant relationship between the implementation of the Blockchain system and the Security of transactions and data in Fintech?
4. Is there any suitable conceptual framework that addresses the gap of privacy and security in the Fintech industries of Nepal?

## **1.6 Objectives and Aims**

The primary objective of this research is to examine the procedures involved in implementing blockchain technologies in the fintech industry of Nepal. To achieve this goal, the following objectives have been established:

1. To investigate relevant research papers, journals, and books and to survey to identify the current situation of the Fintech Industry in Nepal.
2. To examine where there is a significant relationship between the privacy of user data and the Blockchain system used.
3. To examine where there is a significant relationship between the security of user’s data and transactions and the Blockchain system used.
4. To propose a blockchain framework specifically tailored for the fintech industry of Nepal.

## **1.7 Scope**

The research focuses on the impact of blockchain on Privacy and security of the user's data in the Fintech Industries of Nepal.

## **1.8 Significance of the Research**

This research offers a distinctive approach on exploring challenges in Fintech industries and the use of blockchain to maintain privacy and security across the Fintech ecosystem in Nepal and globally. This dissertation makes a significant contribution to the various areas mentioned below.

* Fintech users
* Fintech Providers
* Fintech Institutions
* Fellow Researchers

## **1.9 Structure of the Thesis**

This dissertation has been divided into six main chapters.

**1.9.1 Chapter 1: INTRODUCTION AND BACKGROUND**

This chapter gives an overview of the fintech and blockchain technology along with the current flow and data privacy and security. The main research questions along with the aims, objectives, problem statement and significance are also mentioned in this chapter.

**1.9.2 Chapter 2: LITERATURE REVIEW**

All the theories and concepts underlying the blockchain and fintech are included in this chapter. These concepts are retrieved mostly from the prior journal articles, and some from books, government reports and newspaper articles.

**1.9.3 Chapter 3: RESEARCH METHODOLOGY**

The methodologies to find the current situation of Fintech in Nepal, the relationship between privacy and blockchain systems used and security and blockchain systems used are included in this chapter. All the data and information utilized in the survey, characteristics, and procedures for data collection, tools and various analyses involved are mentioned in this chapter.

**1.9.4 Chapter 4: DATA ANALYSIS**

The collected data from the questionnaires are analyzed and calculated with the help of the SPSS tool in this chapter. Through various analyses, the relationship between the various independent variables and dependent variables is found.

**1.9.5 Chapter 5: DISCUSSION AND FINDINGS**

This chapter includes an examination of the significant discussion of the primary survey. They include both the theoretical and statistical findings.

**1.9.6 Chapter 6: CONCLUSION AND RECOMMENDATIONS**

This chapter explores the findings and proposes solutions.

## **1.10 Summary**

Personal information and transactional data are both important in the fintech world and due to their increasing vulnerability to risk, they must be protected at any cost. In addition, any kind of payments made through Fintech should be secure. Blockchain technology helps to provide privacy to users' information and also makes transactions secure and improves the entire fintech ecosystem in Nepal.

# **CHAPTER 2 LITERATURE REVIEW**

*Prior journaal articles have been carefully chosen to deliver more valuable insights to ensure a systematic and clear view of the literature.Top of Form*

## **2.1 Introduction**

The literature marks the current state of privacy and security in the Fintech industry of Nepal and then explores the blockchain for privacy and security of financial information. Overall, it covers past and existing vulnerabilities and consequences within the fintech and various blockchain frameworks and tools to overcome those issues.

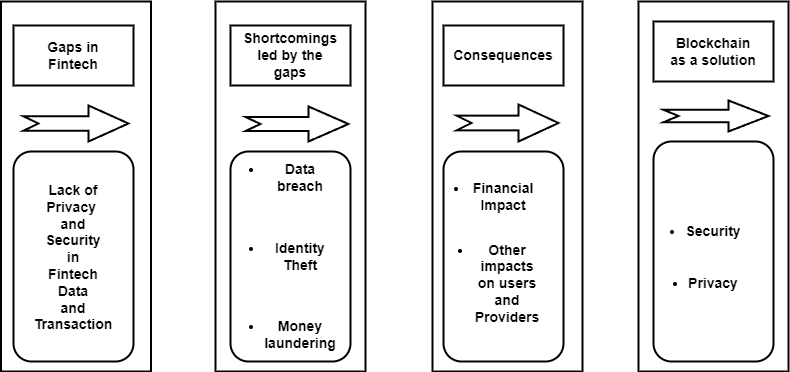


Figure 7: Gaps in Fintech to Blockchain as a solution

The figure above illustrates the gaps in the fintech industry, which are the lack of privacy and security in the fintech data and transactions, and these gaps can result in serious shortcomings such as data breaches, identity theft and money laundering. These shortcomings have significant impacts such as financial loss and other negative impacts on the users and providers. The blockchain technology has been proposed as a solution to increase the privacy and security of the user's personal and financial data.

## **2.2 Current** Scenario **of Fintech**

The current scenario of Fintech industries in Nepal can be understood through the identification of gaps.

### **2.2.1 Gaps in the Fintech Industry**

A kind of financial service innovation that amplifies the traditional ways of financial services via technology is referred to as Fintech (Thakur & Sharma, 2023).In the past, whenever a transaction was made, the user had to provide their personal information to the employee of the financial provider by filling out a paper-based form, and the employee then simply stored them in their register book. The users could then be registered and were allowed to make a transfer of funds through the bank by filling up cheques. This method of transfer of payments and storage of personal information was at high risk as they were often stolen and lost. Moreover, there were other issues such as long waiting times, chaotic environment and identity disputes. A need to digitalize the financial industry was indeed necessary to overcome these challenges and thus traditional financial systems started switching to Fintech (Jakhiya et al., 2020).

Although this shift in the storage of personal data and transactions have improved the work efficiency in the financial world, they are often vulnerable to disastrous attacks from malicious actors, ultimately leading to irreversible damage (Song & Chen, 2021). Our reliance on information technology has only increased over time in critical fields such as healthcare, finance and management. However, due to the increasing incidents of data breaches, storing private and valuable information on internet-connected devices is now a matter of concern.

The rise of fintech has both advantages and disadvantages for both users and fintech providers. The consequences of digitization and globalization in various business models have led to an increase in data vulnerability (Dorfleitner et al., 2021). Fintech makes the availability of financial services, providing customers with economical and easy way of making a transaction. Additionally, the rise of fintech has reduced costs and improved services which have further fostered the competition within the finance industry. Despite this, the widespread integration of fintech has further generated issues surrounding the protection and confidentiality of personal and transactional information. While making the transactions, the cases of cyber-attacks and data breaches have significantly increased. Personal and transactional information breach could lead to critical consequences for both of them (Rehman et al., 2023).

Similarly, all the personal and transactional data are stored in a centralized system using a database, necessitating many intermediaries and compromising the need for transparency. This method of storage of data is highly vulnerable to data breaches and hacking (Javaid et al., 2022). The consequences of these include more complex security issues, as a result of imbalance in a financial system not getting noticed due to lack of transparency.

Today's technology-driven financial services are convenient but the rising cybercrimes are also a result of the rising technology. These have generated more negative than positive perceptions due to the limitations in the network, cyber threats, high cost and security issues (Durai & Stella, 2019).

#### **Financial information records vulnerabilities**

Vulnerability means being in a weak state and likely to be negatively affected by various factors (Gordon, 2020).  In the current fintech industry, there are many internal and external threats leading to countless data harm. Some of these include the sharing of passwords and demographic information that most likely cause a threat to financial information.

The regulatory bodies are solely responsible for making financial policies but they are not solely responsible for the increasing worry about cyber security. Sometimes the financial sector falls into the top game of cyber-attacks. Cyber security is often considered the topmost concern within the realm of fintech by the finance communities across the world (Marqués et al., 2021). The reason for this is that the risks to Fintech are linked to its infrastructure, and when the whole infrastructure is corrupted, it affects other financial institutions and the whole Fintech ecosystem. Therefore, the gaps need to be addressed to better understand financial services and their extent.

According to recent research, there are rising concerns among individuals in the USA who are using mobile payments to financial failure than those who do not use such services. (Seldal & Nyhus, 2022).

### **2.2.2 Shortcomings led by the gaps**

In the present fintech industry, the involvement of third parties and lack of secure methods to control cyber security crimes has become a major reason for privacy and security concerns and escalation of financial vulnerabilities and risks. Let us now delve into the major issues caused by the gaps in fintech.

#### 2.2.2.1 Security Issues in Fintech Sectors

Various types of fraud attacks have taken place across the world. The data below is the most recent report of global payment fraud in 2022, which is given below in the Figure 7.



Figure 8: Global fraud and payment survey report 2022

Source: (Cybersource et al., 2022)

In the above figure, it is clear that several cybercrimes took place recently in the financial sectors. Among them, the highest recorded cybercrime was phishing, which accounted for 35%. This was followed by card testing and identity theft, and more challenges such as money laundering and triangular schemes were also among the most committed crimes. (CyberSource et al., 2022)

#### **2.2.2.2 Breaches across the world**

Breach of data is an event or an intended cyber security attack that leads to significant consequences and losses for both individuals and organizations(Wang et al., 2019). Cyber attackers usually target the fintech industry because the fintech institutions have the storage of most valuable data including both transactional as well as personal data. Cyber attackers can immensely benefit from these activities (Kost, 2023).

Data Breaches give rise to privacy issues in most cases, leading to the revelation of users’ sensitive data to bad-intentional people for the sake of selling it on the dark web and releasing it publicly (Saleem & Naveed, 2020). In March 2019, more than 100 million customer accounts of Capital One were impacted due to a data breach. Valuable information including social security numbers, credit card scores, name and address were exposed publicly. The exploitation of an unmanaged Web Application  
 A firewall was the reason behind this breach which allowed the attacker to get inside the system through the public cloud servers (Nadeau, 2021).

The fintech users are now worried about their personal and transactional information being stolen from online fintech platforms, which has therefore compelled the fintech institutions, providers, and regulators to address these issues to gain the trust of the users (Aldboush & Ferdous, 2023).

#### **2.2.2.3 Data breaches in Nepal**

According to the annual report of NRB 2022, there are currently many new cases of online fraud in the financial sector. Additionally, complaints related to financial crimes have increased in Nepal. The report presented the STR/SAR, which stands for Suspicious Transaction and Activity in Nepal. The STR/SAR shows the vulnerabilities in the transactions that directly or indirectly link to the data breach (*FIU-NEPAL: ANNUAL REPORT 2021/22*, 2022).

A 10-year report on STR/SAR activities in the Finance sector of Nepal is shown in the Figure 10.

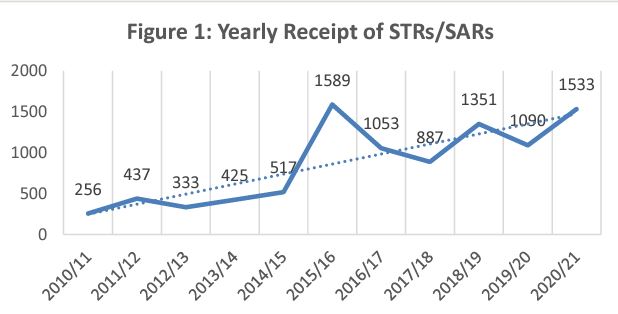


Figure 9: Yearly receipt of STR/SAR report in the finance sector of Nepal

(*FIU-NEPAL: ANNUAL REPORT 2021/22*, 2022)

The above line graph showed a rise in STR/SAR activities every year, with a 12.77% average annual increase over the last decade. This is a big concern for all fintech users as well as institutions. Hence, this makes the financial industry more vulnerable to risks. (*FIU-NEPAL: ANNUAL REPORT 2021/22*, 2022).

The report also covered major areas of finance where most STR and SAR are recorded as shown in Figure 9.

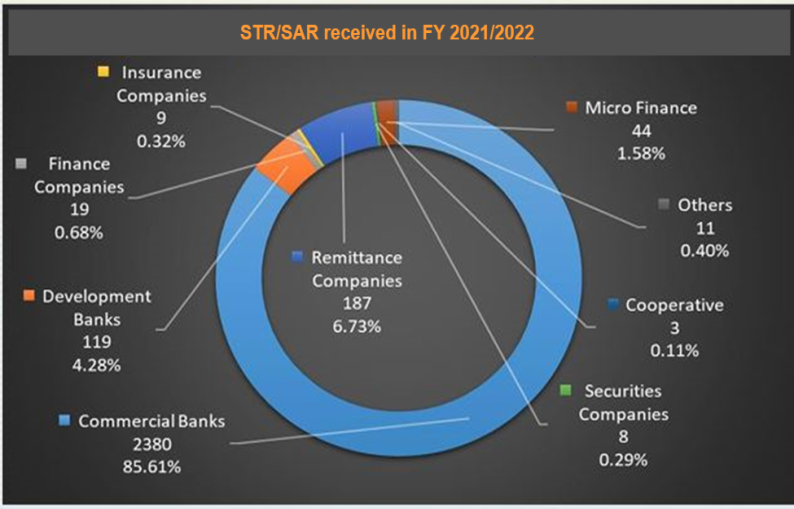


Figure 10: Percentage of STR/SAR received in 2021/2022 in various finance sectors of Nepal

(FIU, 2022)

The report above highlights a significant increase in suspicious transactions and activities, with banks registering the highest number of suspicious transactions. Additionally, the insurance industry, securities companies, microfinance institutions, and remittance companies have also exhibited noteworthy levels of suspicious activities (*FIU-NEPAL: ANNUAL REPORT 2021/22*, 2022).

The suspicious activities and transactions have resulted in financial offences in Nepal which is shown in the Figure 10.

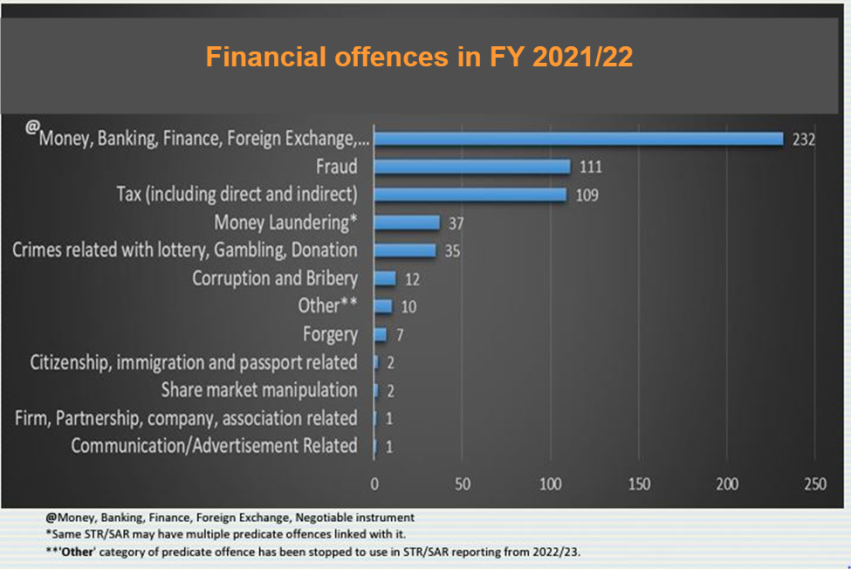


Figure 11: Financial Offences in the financial year 2021/2022

(FIU, 2022)

The above figure from the NRB's report reveals the financial offences within the financial sectors of Nepal, with the highest number of offences related to money, banking, finance and foreign exchanges. This is closely followed by other offences such as fraud, money laundering and tax evasion.

In 2020, various cybercrimes took place in Nepal that cost the fintech industry huge losses. A hacker named Narapichas leaked the data and information of 170,000 users of Vianet Communication. In the same year, the Foodland Delivery app was hacked by another hacker named "Mugger". The following year, Mercantile Communications experienced a data breach through its webpages (Aryal, 2020).Top of Form

#### **2.2.2.4 Privacy and Security in Nepal**

The potential of Fintech is promising in Nepal, and there are an increasing number of businesses adopting financing technologies. However, there are privacy and security challenges within the industry that have impacted its growth and scalability. Although there are wide areas of fintech services, which includes digital banking and payment, they are also among the most vulnerable area to data breach. There has been a tremendous increase in these areas of fintech. Simply implementing the KYC is not enough to effectively regulate and prevent data breaches.

Security breaches expose confidential information of the users without their consent, jeopardizing their privacy of the information. Due to this several countries have safeguarded the personal and financial data of the users in their topmost priority, and have also implemented and proposed effective legislation over the last few years. For example, General Data and Protection and Regulation, also termed at GDPR is one such act focused on maintaining transparency of the data of the users (Dorfleitner et al., 2023). This regulation has been implemented in many fintech companies across the globe.

However, in Nepal, global data privacy measures are still not enforced, despite the presence of the Privacy Act and Privacy Regulation, which align with the constitutional Right to Privacy. Therefore, it is important to limit the valuable information to authorized individuals or institutions, even when fintech companies may try to access it for legitimate reasons. Privacy and security issues in fintech must be addressed to improve quality within the industry.

### **2.2.3 Consequences of a data breach**

There are serious consequences of data breaches. According to the fintech times report, the major consequences of a data breach may involve information loss, equipment damage, revenue loss, and business disruption as given in the figure below.

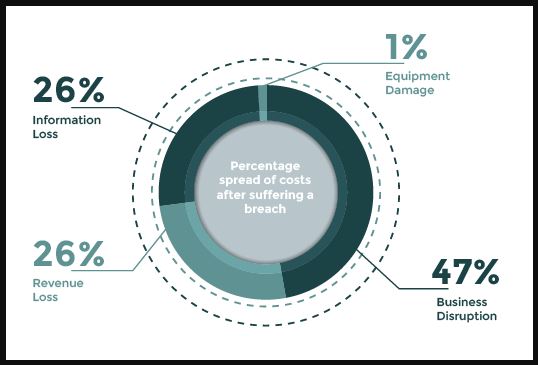


Figure 12: Percentage spread of costs after suffering from a data breach

(Patel, 2017)

According to the figure, business disruption contributes to 47% of the total financial loss caused by a data breach, making it the most important motivator for cybercrime prevention. This is followed by information and revenue loss, both constituting 26% of total financial loss. Overall, all these losses contribute to the financial loss and have serious financial consequences. (Patel, 2017)

#### **2.2.3.1 Financial Consequences**

An occurrence of a data breach leads to an increase in expenses within the banking and financial sectors (Nadeau, 2021).

According to (IBM, 2022), the financial industry covers the second highest position for having faced financial loses from data breach nearing 6 million dollars as shown in the figure below.



Figure 13: Cost of global data breach by industry

(*IBM*, 2022)

Big companies like ‘Sony’, ‘TalkTak’, and Ashley Madison were a victim of high-profile cyber-attacks and have suffered serious damage to their clients, share prices, and reputations. According to the TalkTalk case study, the company has to allocate and spend tens of millions of dollars following a cyber-attack to pay for the compensation of damages to their customers due to data breach (Saleem & Naveed, 2020).

Fintech advancements have the potential to strengthen the effectiveness of anti-money laundering (AML) initiatives through the incorporation of sophisticated algorithms, data analysis, and machine learning techniques to identify potentially suspicious transactions (Faccia et al., 2020). However, the swiftness and user-friendliness characteristic of fintech can also be manipulated by illicit actors to facilitate money laundering activities. Cryptocurrencies, digital wallets, peer-to-peer payment networks, and online trading platforms present opportunities for the movement and masking of unlawfully obtained funds.

## 2.3 Role of Blockchain in the sustainability of fintech

In the domain of financial technology, personal and financial data play a vital role. Nevertheless,

upon transferring and handling this information with inadequate security measures, severe repercussions can occur. Various security and privacy-related measures may arise when people have limited control over their data and money. Also, this has been made worse by the advent of money laundering, shadow banking, and data theft. The consequences of this result in the adoption of blockchain technology as a possible remedy by the fintech industry (Ozili, 2023).

### **2.3.1 The Blockchain technology**

Blockchain technology is the database or protocol that has been designed to save digital records across various computers. With the help of the series of interconnected blocks, a network of blockchains is established as shown in Figure 13 below.

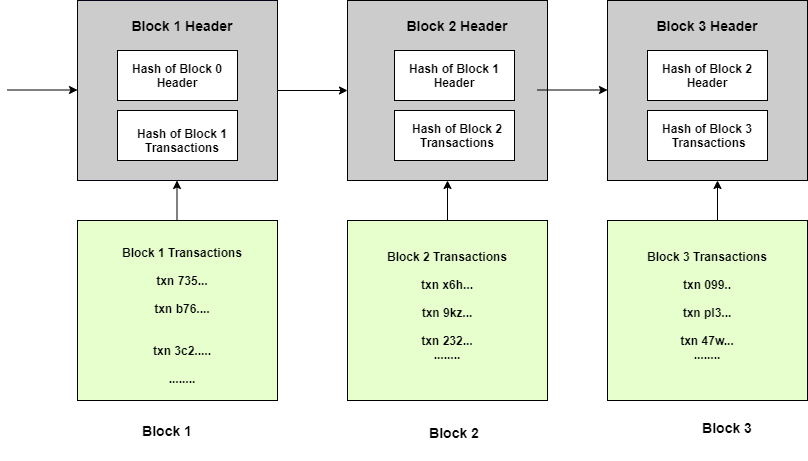


Figure 14: Hash algorithm in blockchain

Source: (Bellaj et al., 2022)

The above figure shows the working mechanism of hashing in blockchain. The first block comprises of hash of transactions. Each block that is added to the chain links its hash to the previous one, which results in the creation of an unchangeable chain. Because of this peer-to-peer setup, it is ensured that the data stored is immutable (Mamun et al., 2020). All the nodes operate together to confirm the transactions and sustain network integrity in the blockchain, which is a distributed and trustless mechanism (Shrimali & Patel, 2022).

Blockchain comprises an important element known as the digital signature, which has considerably enhanced transparent online cooperation and set up trust among clients and merchants (Nelaturu et al., 2022)

Digital signatur secures the data or digital messages against unwarranted changes, both internally and externally, after putting in a digital signature. The users have a private-public key pair with the private key for transaction signing. Also, the process of digital signature comprises signing with private and public key. This allows simple detection of data tampering throughout the transmission (Renduchintala et al., 2022)

The multiple qualities of blockchain are as follows:

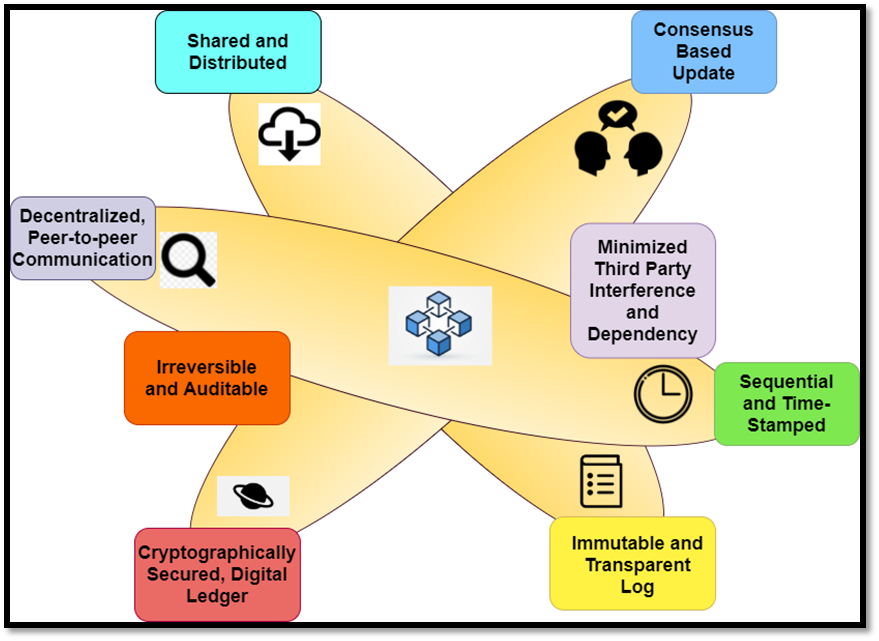


Figure 15:Key characteristics of blockchain

(Singh, 2023)

* **Shared and Distributed**

Blockchain utilizes a shared ledger over a decentralized web of nodes, ensuring the verification of transparent and trusted transactions. It works without a central authority where each node possesses a ledger copy. Transactions are validated through consensus mechanisms POW and POS, bolstering data security and immutability. Alliance of a majority of nodes is important for the manipulation of the ledger. (Singh, 2023)

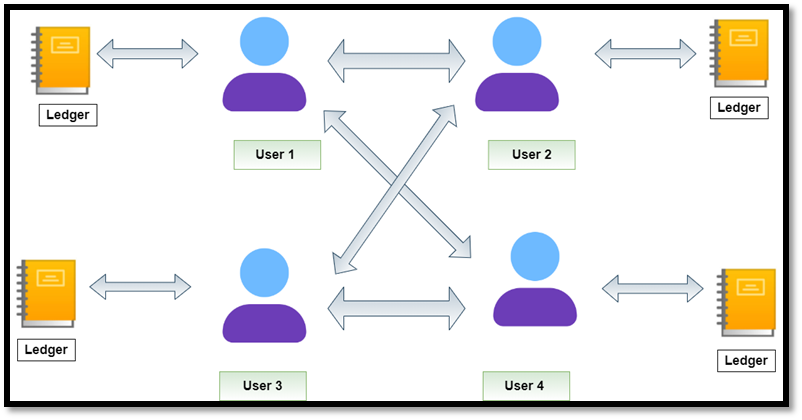


Figure 16: Shared network in a blockchain

(Singh, 2023)

* **Decentralized**

Blockchain supports peer-to-peer networks. With the help of this structure of peer-to-peer, users can interchange and share information directly. This reduces the requirement for intermediaries and increases security and trust via a consensus mechanism. This decentralized feature of blockchain enables tamper-resistant and censorship-resistant communication (Peres et al., 2023).

* **Consensus-based update**

Blockchain uses consensus algorithms for the verification of transactions and verification is completed when every node validates. Similarly, validation from peers is required whenever any change is required during the process. A block is permanently stored in a blockchain every time the validation process is complete.

There are various consensus algorithms available in the blockchain network, and their selection varies on the complexity and nature of the task. Popular blockchains such as Bitcoin, Ethereum and Hyperledger use different consensus mechanisms. are employed in Bitcoin, Ethereum and Hyperledger. These choices are constructed on the basis of type of blockchain, the speed of transaction, scalability, the cost of participation and the trust requirements. (Islam et al., 2023).

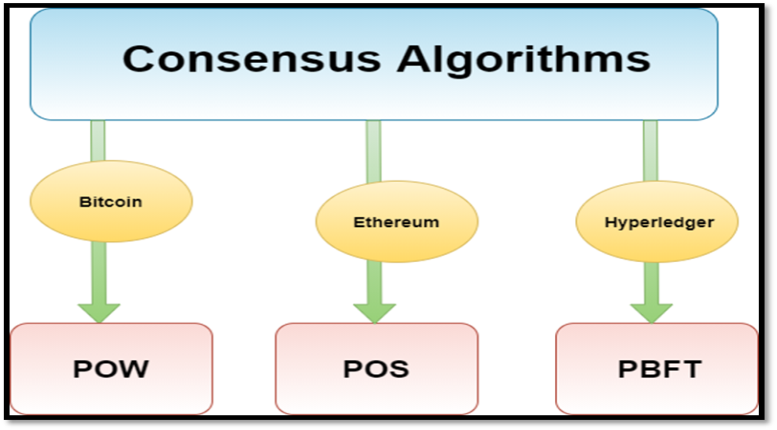


Figure 17: Consensus algorithms

(Islam et al., 2023)

* **Irreversible and Auditable**

Whenever an error or a mistake occurs in one node, a cross-referencing process can be used to correct the situation. This process not only maintains blockchain record consistency but also ensures data permanence.

* **Cryptographically Secured, Digital ledger**

Cryptographic measures involve the hashing technique, which helps to secure the financial records within a blockchain from external threats.

* **Minimized third-party interference and dependency**

The involvement of third-party providers is usually susceptible to privacy and security concerns due to cyber-attacks (Aslan et al., 2023).

Blockchain solves this issue by reducing the need to involve any third-party provider. This is facilitated by smart contracts, which make direct agreements between two parties possible without needing to involve a third party (Taherdoost, 2023). The smart contracts not only validate transactions but also avoid data tampering, are cost-effective and ensure high security

* **Immutable and transparent log**

Only authorized users are allowed to inspect the transactions and if not verified, they face a block rejection. Blockchain offers tamper-resistant designs for better security of financial records and prevents unauthorized modification of the data. Moreover, blockchain allows the sharing of data, preserves the integrity of the record, and promises a secure record of transactions.

### **2.3.2** **Blockchain for private and secured financial records and transaction**

Blockchain uses a distributed node network, depending on digital signatures, consensus techniques, and a sequence of hash functions for strong storage of data. The fintech sector, as shown in the figure below, has definite demands regarding user financial data privacy and security.

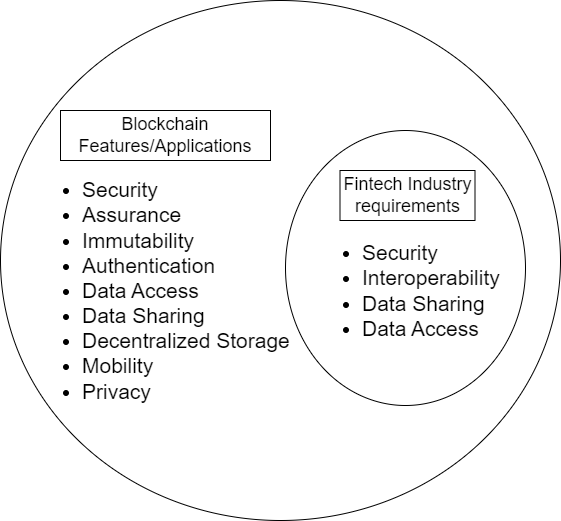


Figure 18: Analysis of blockchain features and fintech requirements

As shown in the figure above, fintech industry requirements include security, interoperability, data access, and data sharing. All of these features are fulfilled by a blockchain. Blockchain eliminates the need for a central administrator, replacing traditional security with cryptographic methods to reduce data risks. (Nelaturu et al., 2022).

Whenever a transaction is carried out in a blockchain, the transactions are distributed to every node. This leads to the formation of a new ledger without having to involve a third-party administrator. Blockchain also confronts the confidentiality of financial records through public key cryptography. This ensures that only the authorized network can access financial information, keeping up with the privacy.

Blockchain, specifically the permissioned Hyperledger Fabric (HLF) Platform, confirms the security of the sensitive and confidential nature of financial records. HLF works as a closed ledger that can be accessed only via user invitations, resulting in the maintenance of record confidentiality. Financial institutions generate a permissioned consortium, establishing a private network. The new member is granted with permission only when the consensus among existing members is achieved (Ghosh et al., 2023). The HLF system increases privacy and security with the help of primary components and consensus phases, as shown in the figure provided below.

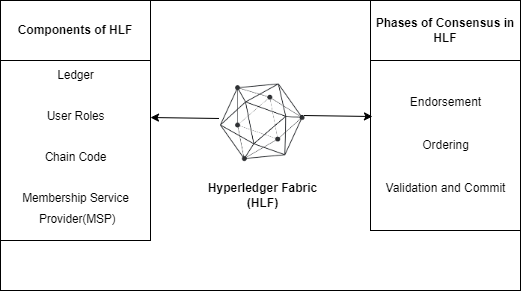


Figure 19: Components and phases of Hyperledger Fabric

(Ghosh et al., 2023)

The above figure showcases the Hyperledger fabric, and its key components, which include the User Role, Ledger, Chain Code, and Membership Service Provider (MSP). Similarly, there are four phases in the consensus stage of this blockchain, which are endorsement and order, followed by validation and commitment.

In short, the cryptographic proof measure in blockchain helps to validate records, and increase trustworthiness. This makes a blockchain a secure and interoperable tool for the management of personal and financial records. The Public-key cryptography on the other hand maintains confidentiality and privacy through its private and public keys.

### **2.3.3** **Security Benefits of Blockchain Over Traditional Methods**

Banks and governments serve as a facilitator for transaction security in the current fintech system. This has led to trust issues in online transactions. Contrarily, the blockchain uses decentralized controlled measures and grants ownership of personal and financial records. Moreover, this measure also guarantees a permanent and immutable record resulting in the secure transactions and protection of transactional and identity data in the Fintech Industries.

The decentralization nature of blockchain depends on the consensus mechanism, which not only helps to authenticate the transactions but also keeps a record of all participants in a network.

If two-thirds of peers agree on the consensus, a transaction is appended to the blockchain. This safeguards against unauthorized and unwarranted entries. On the other hand, the transactions in traditional methods are delayed if the central authority is compromised. (Yadav et al., 2023).

Whenever required, a blockchain provides users with the integration of dynamic Access Control Lists. Additionally, it facilitates full data ownership to the users. This feature of blockchain handles the gaps present in the traditional system, shaping blockchain into a decentralized and immensely secure remedy (Sarfaraz et al., 2023).

When any user is involved with the fintech institution for the registration process or any transaction-related activity, the user’s financial data, along with their KYC, is employed in the organization’s data server for keeping the record. Nevertheless, if the same person chooses to register with any other fintech company, the second company will not have the authority to the records from the first company. This guarantees that anytime a block needs to be appended to the network, it is copied and distributed in every node, resulting in the remedy of data fragmentation across fintech sectors.

To preserve the fintech data from hackers, public-key cryptography is used. When a user sends data to the provider, the public key is sent along the way. Now, only the authorized individual or an entity, who has the right private key for that particular public key can decrypt and get access to the data. A central system directs the access control in traditional databases whereas cryptographic measures secure the ledger in blockchain.

### **2.3.4 Blockchain as a Solution**

Blockchain aims to achieve data storage and access control for network applications with security and reliability in a distributed network environment (Zhao & Meng, 2019). Blockchain has offered a remedy to remove emerging security and privacy problems that are becoming more challenging as the rise in the privacy risk increases (Wylde et al., 2022). The technology of blockchain prospects to maintain long-standing challenges in several sectors which include fraud detection and money laundering prevention via smart contracts. It allows secure efficient record-keeping, accounting, and auditing processes can be obtained which ensures accuracy and trust (Ndung’u, 2022). Also, it can decrease the cost of transactions and increase transaction speed resulting in the revolution of conventional financial processes.

## **2.4 Related Work**

Previously many authors have studied blockchain technology to use it effectively in the fintech industry. The critical reviews of the related works of implementation of blockchain in the fintech industry will now be done in this section.

|  |
| --- |
| **Key Literature 1** |

|  |  |
| --- | --- |
| Title | Applications of Blockchain in FinTech |
| Authors and Year of Publication | Christian Baliker, 2023 |
| Features | * Analyze and discuss various architectures that are proposed for different areas in Fintech. * Overview of various sectors of Fintech * Overview of blockchain based fintech applications in future researches. |
| Techniques | Hyperledger Fabric, blockchain technology, fintech |
| Advantages | * Provides insights on the current cyberattacks in the fintech and security and privacy issues in Fintech. * Provides insights on the blockchain technologies. * Suggests hyperledgerblockchain to secure the fintech applications in future |
| Limitations | * Research dependency only on secondary data. |
| Method of Research | Survey based empirical study |
| Model Used | Quantitative and Qualitative |

Table 1: Key 1 Literature Review Overview

|  |
| --- |
| **Key Literature 2** |

|  |  |
| --- | --- |
| Title | A Comparative Analysis of Advanced Security Algorithms |
| Authors and Year of Publication | Nikita Thakur, Vandana Sharma , 2023 |
| Features | * various security-based algorithms |
| Techniques | Hash algorithm, blockchain encrption |
| Advantages | * Paper stresses advanced security in fintech, compares algorithms, and urges research on optimization, collaboration, and countering threats. |
| Limitations | * Only relies on cryptography but has not used full blockchain potential. |
| Method of Research | Empirical Based |
| Model Used | Qualitative |

Table 2: Key 2 Literature Review Overview

|  |  |
| --- | --- |
| **Key Literature 3** | |
| Title | Secure and Transparent KYC for Banking System |
| Authors and Year of Publication | Abdullah AI Mamun, 2020 |
| Features | * Implementation of platform for an easier verification of the KYC document. * Different PCs with different operating systems were used. |
| Techniques | Interplanetary File System (IPFS) and Blockchain. |
| Advantages | * Easy and secure sharing of KYC between financial organizations. * Overview of KYC and blockchain technology. |
| Limitations | Only latency test and stress test used. |
| Method of Research | Empirical method |
| Model Used | Quantitative and Qualitative |

Table 3: Key 3 Literature Review Overview

|  |
| --- |
| **Key Literature 4** |

|  |  |
| --- | --- |
| Title | SecuredInsuranceFrameworkUsingBlockchainand SmartContract |
| Authors and Year of Publication | Abid Hassan, Iftekhar Ali, Rifat Ahammed, 2021 |
| Features | * This proposed framework solves security and trust issues. * Testing of the scalability Is done with the addition of number of peers. * With a greater number of validators, the security increases. |
| Techniques | This paper introduces a framework that employs smart contracts stored on a blockchain for insurance agreement. |
| Advantages | * Framework uses Solidity for smart contracts * It enhances trust and security in insurance by cancelling faulty claims. * Paper explains about the Proof of Authority consensus, internal workflows, system flowchart, and clarifies PoA algorithm. |
| Limitations | * The proposed framework is not domain-specific. * It focuses on insurance policies only. * Dependent only on secondary data. |
| Method of Research | Empirical based |
| Model Used | Qualitative and Quantitative |

Table 4: Key 4 Literature Review Overview

|  |
| --- |
| **Key Literature 5** |

|  |  |
| --- | --- |
| **Title** | Implementation of a Blood Cold Chain System with blockchain |
| **Authors and Year of Publication** | Dongsoo Kim, 2020 |
| **Features** | * Previous research papers on blood cold chain system have been reviewed. * Interactive blood supply system with the medical systems have been proposed. |
| **Techniques** | An innovative cold blood system established on the private blockchain technology using the architecture of Hyperledger Fabric is proposed in this research to secure information visibility and deduct the supply time of the blood. |
| **Advantages** | * Counterfeiting and information tampering is prevented. * Increases transparency. * Reduces supply time. * Secure information. |
| **Limitations** | Evaluation of the proposed system has not been done to prove the effectiveness of the system. |
| **Method of Research** | Empirical method |
| **Model Used** | Qualitative and Quantitative |

Table 5: Key 5 Literature Review Overview

**Comparison of the related works**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Title** | Application of blockchain in fintech | Enhancing Fintech Security | Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology | SecuredInsuranceFrameworkUsingBlockchainand SmartContract | Implementation of a Blood Cold Chain System with blockchain |
| **Authors** | (Baliker et al., 2023) | (Thakur & Sharma, 2023) | (Mamun et al., 2020) | (Hassan et al., 2021) | (Kim et al., 2020) |
| **Year** | 2023 | 2023 | 2020 | 2021 | 2020 |
| **Features** | * Analyze and discussion of various architectures in Fintech * Overview of various sectors of Fintech   and blockchain based fintech applications in future researches. | Comparative Analysis between various advanced security-based algorithms. | Improvement of the proposed system by analyzing testing such as latency test and stress test. | * Framework uses a private Ethereum network, Solidity smart contracts. * Paper distinguishes itself with Proof of Authority consensus and clarifies PoA algorithm. | Previous research papers on blood cold chain system have been reviewed.  Interactive blood supply system with the medical systems have been proposed. |
| **Limitations** | Research dependency only on secondary data. | Only relies on cryptography but has not used full blockchain potential | Enhancement of the proposed system with latency test | * The proposed framework is not domain-specific. * It focuses on insurance policies only. * Dependent only on secondary data. | Evaluation of the proposed system has not been done to prove the effectiveness of the system. |
| **Advantages** | Provides insights on the current cyberattacks in the fintech  Provides insights on the blockchain technologies.  Suggests hyperledgerblockchain to secure the fintech applications in futureSecure, including easy KYC sharing in finance. | Paper focuses on advanced security in fintech, compares algorithms, to counter threats.  Researchers can now improve these algorithms to counter fraudulent activities and cyberattacks. | Easy and secure sharing of KYC between financial organizations. | * This proposed framework solves security and trust issues. * Testing of the scalability is done with a greater number of validators to increase security. | An innovative cold blood system established on the private blockchain technology using the architecture of Hyperledger Fabric is proposed in this research to secure information visibility and deduct the supply time of the blood. |
| **Method of research** | Survey based empirical study | Empirical based | Product Based | Empirical based | Product Based |
| **Models used** | Qualitative / Quantitative | Qualitative | Qualitative/ Quantitative | Qualitative/ Quantitative | Quantitative / Qualitative |

Table 6: Comparison of Related works

Various researchers have conducted their investigations, and interestingly, their discoveries exhibit interconnectedness. The table provided below illustrates the comparison of these related studies.

The other 30 research articles have been listed below in the literature review matrix.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No | Journal title | Authors and Year of Publication | Quotations | DVs | IVs | Research Gap |
| 1 | A review of Blockchain in financial services | Mohd Javaid, Rajiv Suman, 2022 | Blockchain technology is found to enhance  security and authenticity in Fintech | privacy, Security | blockchain | This research is only limited to the theoretical review of blockchain-based financial services. |
| 2 | Digital Financial Transaction Security Based on blockchain | Yansheng Chen, 2021 | To study the ftransaction security in Fintech with blockchain technology | Digital financial transaction security | Blockchain | Framework has not been proposed |
| 3 | Data Defense: Examining Fintech’s Security and Privacy Strategies | Fasih Ur Rehman, Hafiz Muhammad Attaullah, Failsal Ahmed, Sundus Ali, 2023 | To discuss advantages and security along with the vulnerability of data among Fintech users and providers | Data Protection Security, Privacy | Blockchain | No quantitative survey done |
| 4 | Blockchain as a Solution of Information Security and Data Privacy Issues: Review | Ndung’u Rachael Njeri, 2022 | To provide an overview of privacy and security of data with blockchain | Information security, data privacy | Blockchain | No quantitative survey done |
| 5 | DIGITAL FINANCE AND ITS IMPACT ON FINANCIAL INCLUSION | Tabitha Durai, Stella G., 2019 | To study the financial inclusion impact | Financial inclusion,security, adaptability, affordability | Digital Finance | No framework proposed |
| 6 | Digital finance research and developments around the world: a literature review | [Peterson K. Ozili, 2023](https://www.inderscienceonline.com/doi/abs/10.1504/IJBFMI.2023.127698) | To provide an overview of key drivers in fintech such as efficiency, financial inclusion and efficiency of payment | digital finance, sustainability, financial inclusion, payment efficiency | artificial intelligence, machine learning, mobile money, blockchain | Research limited to comparison with earlier researches, methodological gap |
| 7 | Policy report on FinTech data gaps | José Manuel Marqués, 2021 | To determine key issues on data gaps in fintech and monitoring the challenges with statistics | Fintech, data breach, payment systems | cybersecurity, monitory policy, | Limited to a particular geographical area |
| 8 | Financial Vulnerability, Financial Literacy, and the Use of Digital Payment Technologies | [M. M. Naeser Seldal, & Ellen K. Nyhus , 2022](https://link.springer.com/article/10.1007/s10603-022-09512-9#auth-M__M__Naeser-Seldal-Aff1) | To study the relation between online digital payment and financial vulnerability | money transfer, payment, data breach | Digital payment technologies | Research limited to comparison with earlier researches, methodological gap |
| 9 | ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES | Ping Wang, hubert D Cruz, 2019 | To explore the factors of data breach and its impact on economy | Economic costs | Data Breach | Limited to a particular geographical area |
| 10 | Emergence and Growth of Mobile Money in Modern India: A Study on the Effect of Mobile Money | Mukund Jakhiya,Malini Mittal Bishnoi,Harsh Purohit, 2020 | To analyze mobile payments in developing countries | Economy, privacy, security | Mobile money | The research is limited only to small area – India. |
| 11 | Building Trust in Fintech | Marah Ferdous, 2023 | To study the ethical considerations of fintech privacy | Customer trust, privacy | Big Data, AI | Only qualitative research done, methodological gap |
| 12 | Promise not fulfilled: FinTech, data privacy, and the GDPR | Gregor, Dorfleitner, Lars Hornuf | To analyze the effects of GDPR to improve privacy practices in fintech firms | Data privacy | GDPR | Evidence gap |
| 13 | SoK:AnatomyoDataBreaches | Hamza Saleem, Muhammad Naveed, 2020 | To understand the various data breach methods . | Data breach, data security | Security Defences | Only qualitative research done, methodological gap |
| 14 | Electronic Money Laundering, the Dark Side of Fintech: An Overview of the Most Recent Cases | Alessio Faccia, narcisa Roxana , 2020 | To understand the the dark side of Fintech and various problems including money layndering | Money laundering, data breach, privacy, security | Electronic money | Only qualitative research done, methodological gap |
| 15 | Decentralized web, distributed ledgers, and build-up to blockchain | harjot Singh, 2023 | Study of various types of blockchain | privacy and security | Distributed ledger, privacy | Only qualitative research done, methodological gap |
| 16 | Review of Cyber Security Vulnerabilities, and Solutions | Omer Aslan, 2023 | To summarize security issues and blockchain solution for cyber crime. | Cybersercurity, cyberattacks, cyber threats , Phising, malware, | Blockchain | Methodological gap, only qualitative comparisons done |
| 17 | AccessChain: An access control framework to protect data access in blockchain-enabled supply chain | Aaliya Sarfaraz, 2023 | To create a framework for access control | Data access protection | Blockchain | Methodological gap, only qualitative comparisons done |
| 18 | A Review of Blockchain in Fintech | Duc-Phong Le, 2022 | To discuss challenges that are linked with the blockchain protocols and application layers. | Security and Privacy | Blockchain | Qualitative Research Only |
| 19 | Blockchain meets marketing: Opportunities, threats, and avenues for future research | Renana Peres, Martin Schreier, David A. Schweidel, Alina Sorescu, 2023 | To integrate blockchain technology into marketing industry | Security | Blockchain | Only Literature reviews compared |
| 20 | A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues | Saminur Islam, Mohammad Jaminur Islam, Mahmud Hossain, Shahid Noor, 2023 | To provide the comparative analysis between various consensus protocol. | Privacy and security | Blockchain | Only comparative analysis of past researches |
| 21 | Research on Innovation and Development of Blockchain Technology in Financial Field | Chenxi Zhao, Xianyong Meng, 2019 | To provide security of data storage in finance | Big data, cloud storage, fintech | Blockchain | Only literature review is involved. |
| 22 | Cybersecurity, Data Privacy and Blockchain | Vinden Wylde, Nisha Rawindaran, John Lawrence, 2022 | To provide overview on privacy and security of data in blockchain | Cybersecurity, big data, machine learning | Blockchain | Only literature reviews compared |
| 23 | Blockchain state-of-the-art | Bela Shrimali, Hiren B Patel, 2022 | To study the use cases of consensus mechanism | Security | Blockchain | Only literature reviews compared |
| 24 | A Survey of Blockchain Applications in the FinTech | Tara Rendenduchintala, Haneen Alfauri, Zebo Yang | To study financial solutions in Fintech through blockchain and DLT, and permissioned blockchain method. | Payment, Lending | Blockchain | Only limited to the theoretical review, the framework has not been discussed |
| 25 | Evolution of Blockchain and consensus mechanisms & its real-world applications | Armendra Singh Yadav, Nikita Singh, Dharmendra, 2023 | To explore existing algorithm and processes of blockchain  in Finance, Healthcare and food safety. | Food safety, data security | Distributed Ledger Technology(DLT), Merkle tree, Block, Hash , encryption | Based on only statistical data, no framework |
| 26 | Smart Contracts in Blockchain Technology: A Critical Review | Hamed Taherdoost, 2023 | To discuss the advantages of smart contracts | Security, reliability | Smart contracts in blockchain | Limited to journal articles, books |
| 27 | The Applications of Blockchain in FinTech: Advancements and Opportunities | Christian Baliker, Mohamed Baza, Abdullah Alourani, 2023 | To study the opportubnities and challenges in Fintech industries and maintain pricacy and security with the blockchain | Cyber attack, privacy , security | hyperledger fabric (blockchain) | Limited to journal articles, books |
| 28 | Enhancing Fintech Security - A Comparative Analysis of Advanced Security Algorithms | Nikita Thakur; Vandana Sharma, 2023 | To analyze security algorithms for privacy and authenticity of data | data privacy, security, hash algorithm, blockchain, transaction | Secure Hash algirithm(SHA),  Cryptography, security algorithms, | Only relies on cryptography but has not used full blockchain potential |
| 29 | Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology | Abdullah AI Mamun, M. Shamim Kaiser, Mohammad Abu Yousuf 2020 | To implement blockchain technology along with IPFS for secure KYC in banks | security, data privacy, transparency | Blockchain, smart contract, IPFS, Decentralization, payment | Limited to a certain geographical area |
| 30 | SecuredInsuranceFrameworkUsingBlockchainand SmartContract | Abid Hassan, Iftekhar Ali, Rifat Ahammed, 2022 | To implement blockchain technology for secure insurance industry data. | Data security, secure payment | Blockchain, smart contract | Framework only limited to insurance, findings not supported by data, smart contract may have been customized |

Table 7: Research Matrix of 30 research articles

## **2.5 Research Gap**

While comparing and analyzing past literatures and articles, it was found that most of the articles related to the relationship between blockchain and privacy and security were done in a qualitative aspect i.e., by comparing other literatures. There were extremely less quantitative research articles on these topics. In addition, these research articles did not provide or propose a framework for the solution of privacy and security issues in fintech.

Thus, in order to cover these gaps in previous research works, research was carried out in a quantitative manner and also a Blockchain-based framework was proposed in order to solve the issues of privacy and security.

In addition, there was almost nil quantitative research done in Fintech in the context of Nepal in relation to privacy and security. So, this research aims to bridge these research gaps through a quantitative research to show the blockchain, privacy and security relationship of data in the Fintech industry of Nepal.

# **CHAPTER 3 RESEARCH METHODOLOGY**

*We will now discuss the research methods that are used for this survey. The data collection methods and the techniques used will be discussed. Moreover, we will also discuss the total timeframe for the research and also bring into the limelight the ethical considerations associated with the study.*

## 3.1 Methodology

Empirical cycle was followed using direct and indirect observation.

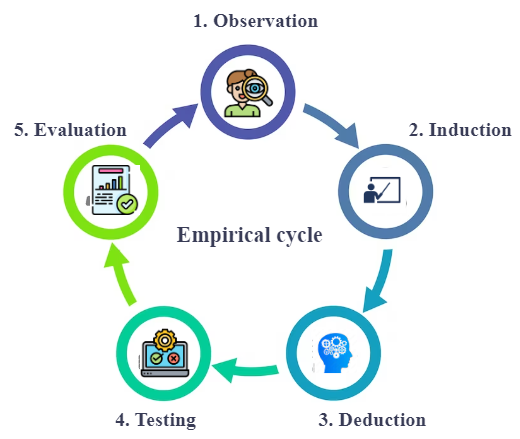


Figure 20: Five phases of the empirical cycle

As shown in the above figure, the research has followed the five stages of the empirical cycle during the thesis conduction. The five stages in the research article are implemented as follows:

I.               Observation - Initially, the existing problems or gaps prevalent in the Fintech industries in Nepal were addressed and the research topic was discussed under the observation step.

II.             Thereafter, the questions that this research seeks to answer along with the objectives as a part of Induction.

III.           Likewise, the relevant literature to understand the current theories, various concepts and findings that are associated with the research topic was also reviewed under deduction.

IV.          As a part of Testing, methods used in data collection and their analysis were described along with the proposal of the Hyperledger Fabric framework used to address the current problem.

V.            Finally, under evaluation, data analysis using SPSS along with the interpretation/ analysis of data collected was also presented.

## **3.2 Independent and Dependent Variable**

In this research paper, the independent variable is the blockchain whereas the dependent variables are privacy and security. The relationship between blockchain and privacy and security and blockchain will be discussed.

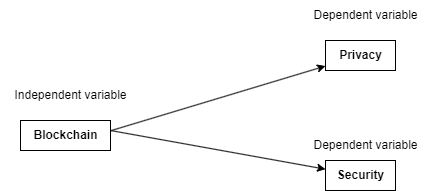


Figure 21: Relationship between dependent and independent variable

## **3.3 Research Strategy**

This research can be called a contemporary topic since the use of blockchain in fintech in Nepal has not been uncovered yet. There are many related researches done outside of Nepal, but the focus has been limited to a single industry of Fintech and not Fintech as a whole. Through the previous jourrnals, the current gaps of fintech that cause privacy and security concerns in Nepal as well as outside Nepal were uncovered. Similarly, the possibility of improvement in privacy and security of financial information with the help of blockchain was also uncovered. This research focuses on improving and strengthening the privacy and security of the financial world. Thus, it can be generalized in any financial entity or any country with privacy and security concerns of the information. Quantitative as well as qualitative method have been used for research outcome. 35 research papers related to blockchain and fintech have been analysed thoroughly. Similarly, the survey questionnaires and analysis of the collected data have been analysed with the SPSS tool. Correlation and regression models found relationship of independent variables with dependent.

## **3.4 Types of Data**

Primary and secondary data were used as a methodology for this research, and survey questionnaires have been prepared and distributed online survey. Similarly, prior journal articles, books and journal articles have been studied extensively for the collection of secondary data.

**Primary data**

To understand the current status of privacy and security, the collection of primary data was done through online survey questionnaires using Google Forms. Both the fintech users and the fintech employees in all public and private sectors were targeted to help get a better understanding and feedback from all perspectives. A Likert scale questionnaire has been used to collect responses. It is often believed that the primary data can give a better insight of the situation and collecting responses using a questionnaire is one good way of collecting responses.  Since fintech and blockchain both are new and emerging terminologies, through the prior research on these topics, it was found that past review of literature was alone not enough to determine the present o status of fintech in Nepal. Therefore, there was a need for the collection of primary data from the participants.

**Secondary Data**

The secondary data was collected in the Literature review section through the various prior journal articles, books, reports and newspaper articles, also included real data and statistics. The journal articles used are no older than the last five years. The major areas included the gaps in Fintech, the shortcomings led by the various gaps, their consequences and their solution using blockchain technology. Moreover, the secondary data was useful as the information regarding the use of blockchain technology in fintech was explored and the alternative solutions to make the personal and transactional data more secure and private.

## 3.5 Research design

Since the research has used both qualitative and quantitative approaches, it has followed a blend of exploratory and descriptive methods.

## 3.6 Sampling type and size

Since the research involves technical terms such as fintech and blockchain, most users may not be familiar with these terminologies' names. Therefore, for this research, only employees of the Fintech and IT companies of Nepal have been asked to participate. Since the study is centred in Kathmandu, Nepal, participants were chosen from among the fintech employees across the city. These employees possess knowledge about the fintech industry and are well-informed about future opportunities associated with the technology.

A total of 32 questionnaires have been developed, and a set of questionnaires have been developed for each variable. The sample size for participants is 402.

## 3.7 Data collection methods

The development of the questionnaire was based on the five Likert-type questions. This helped to gain the viewpoint of the respondents in a fun way. To collect the data, the questionnaires were sent and distributed via email and the HR representatives of the companies.

## 3.8 Analysis of Data

SPSS, a statistical tool was used for data analysis. Reliability Testing of the questionnaires covering privacy security and blockchain was done. Similarly, descriptive analysis including the background of the participants was done. The regression along with the correlation were conducted to determin relationship between blockchain and privacy and blockchain and security. Along with the SPSS, related kinds of literature also supported the analysis.

## 3.9 Research timeframe

The research timeframe and the Gantt chart of the research timeline have been shown below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TASK NAME** | **START DATE** | **END DATE** | **START ON DAY\*** | **DURATION\* (WORKDAYS)** |
|  |
| Research area identification | 10/8/2022 | 10/12/2022 |  | 5 |  |
| Literature review | 10/13/2022 | 11/30/2022 | 5 | 49 |  |
| Planning research methodology | 12/1/2022 | 1/25/2023 | 54 | 56 |  |
| Preparing the questionnaires | 1/26/2023 | 2/15/2023 | 110 | 21 |  |
| Distributing the questionnaires/Data Collection | 2/16/2023 | 3/10/2023 | 131 | 23 |  |
| Data analysis with SPSS | 3/11/2023 | 4/6/2023 | 154 | 27 |  |
| Report Writing | 4/7/2023 | 5/7/2023 | 181 | 31 |  |
| Proposing the blockchain framework | 5/8/2023 | 6/8/2023 | 212 | 32 |  |
| Discussion and Findings | 6/9/2023 | 7/9/2023 | 244 | 31 |  |
| Conclusion and Recommendations | 7/10/2023 | 8/10/2023 | 275 | 32 |  |
| Dissertation Final Submission | 8/11/2023 | 9/7/2023 | 307 | 28 |  |
|  |  |  |  |  |  |

Table 8: Project Timeline

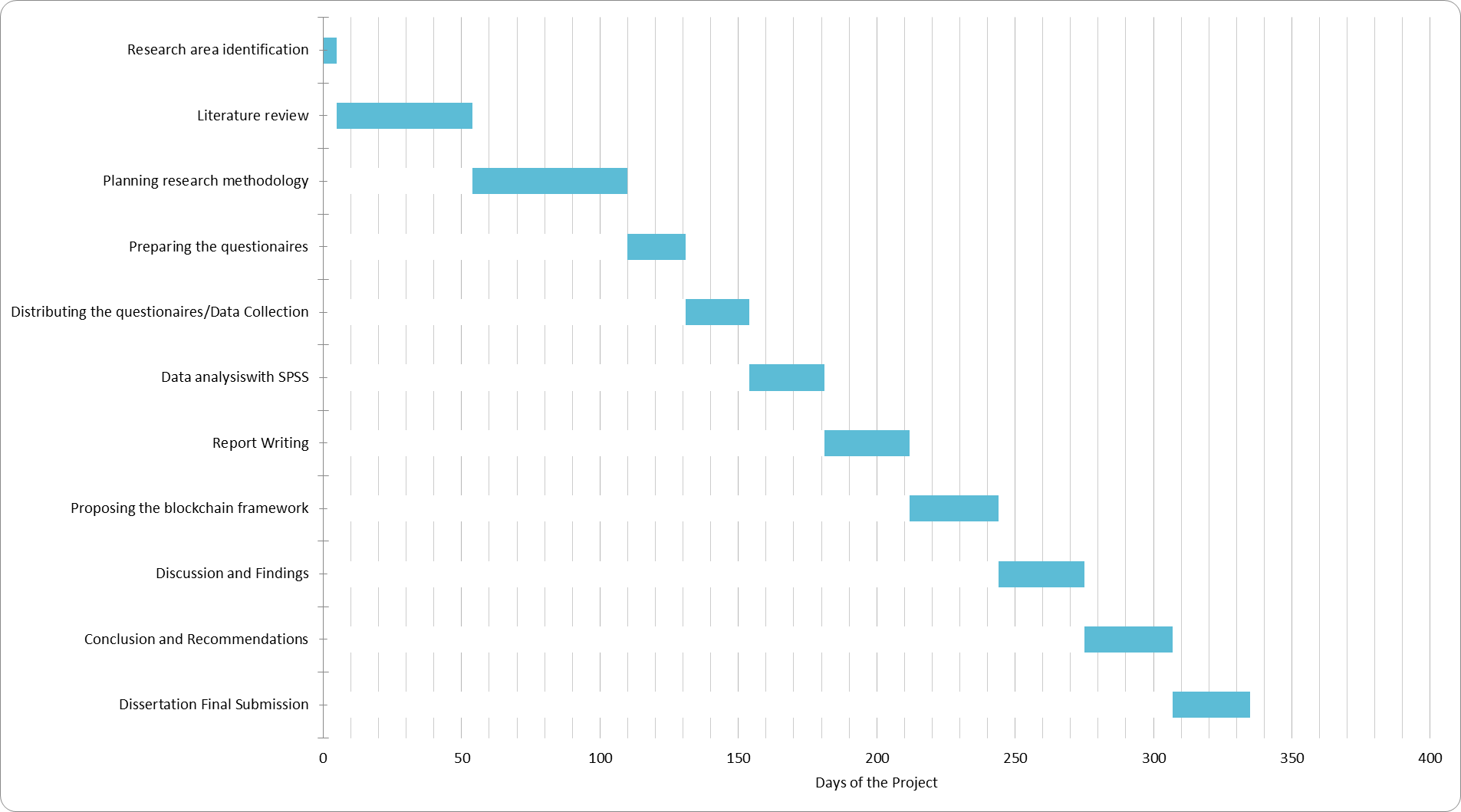


Figure 22: Gantt Chart Representing Project Timeline

## 3.10 Ethics and Confidentiality

University Regulation is adhered to during the conduction of research and moral principles are kept in mind. Ethics being an important aspect of the research ensured that only lawful and moral methods were used. The participants of the questionnaire were approached professionally without any compulsion to participate. Participants' privacy and confidentiality were respected and made sure no personal information would be disclosed under any circumstances.

# **CHAPTER** **4 DATA ANALYSIS AND INTERPRETATION**

*This section covers the analysis of survey responses from the survey participants. Survey questions were prepared in alignment with research objectives, pre-mapped, and averaged for each objective. The data collected were analysed, organized and reported using the SPSS tool.*

## **4.1 Case Processing Summary**

The survey questionnaires were specifically distributed to employees in the Fintech and IT industries of Nepal. This decision was made due to the presence of technical terms like "Fintech" and "blockchain," which might not be easily understood by the general public. Ensuring targeted participants was crucial to obtaining the most relevant feedback for the thesis and identifying current issues and data vulnerabilities in Nepal's Fintech industry. Additionally, the survey aimed to assess the current state of user's perception towards privacy and security in Fintech.

## **4.2 Reliability Testing (Cronbach’s Alpha)**

Reliability analysis is performed to find the relevancy of the survey questionnaire. The survey analyses impression of blockchain in the fintech industry of Nepal in consideration of privacy of data and security of transactions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Case Processing Summary** | | | |
|  | | N | % |
| Cases | Valid | 398 | 99.0 |
| Excluded | 4 | 1.0 |
| Total | 402 | 100.0 |
| a. List-wise deletion based on all variables in the procedure. | | | |

Figure 23: Total questionnaire case summary

A reliability test ensures the quality of questions used in a survey questionnaire. To analyse the consistency of the chosen variables in the survey, a Cronbach's alpha test was carried out through the SPSS tool.

The Cronbach's alpha coefficient of reliability, which can vary between 0 and 1, shows whether a question set is dependable or not. The high value of Cronbach's alpha indicates that the response values for each participant across the questionnaire set are similar or consistent while a low value indicates that they are not consistent across a question set. The statistics below, extracted from SPSS, display the reliability of each independent variable along with a comprehensive alpha coefficient representing the gathered responses.

**Reliability analysis for all the variables:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Case Processing Summary** | | | | | |
|  | | | N | | % |
| Cases | Valid | | 379 | | 94.3 |
| Excluded | | 23 | | 5.7 |
| Total | | 402 | | 100.0 |
|  | | | | | |
| **Reliability Statistics** | | | | | |
| Cronbach's Alpha | | N of Items | |
| .967 | | 25 | |

Table 9: Reliability test and statistics for total case summary

The reliability statistics show that the questions included in the survey are highly reliable. As Cronbach’s alpha value is 0.967. The high Cronbach’s alpha value shows a high level of reliability. That means the questionnaire for the survey will yield reliable results. This also indicates a high level of consistency of responses of each participant in a set of survey items.

**Reliability Test for Privacy**

|  |  |  |
| --- | --- | --- |
| **Reliability Statistics** | | |
| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
| .922 | .937 | 8 |

Table 10: Reliability for privacy

The above reliability statistics for Privacy and Security show a high reliability of 0.922. This high value shows a high reliability. That means the questionnaire for the survey will yield reliable results. This also indicates a high level of consistency of responses of each participant in a set of survey items. Hence, the questions included for Privacy are highly reliable.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Questionaires for privacy** | | | | | |
|  | Scale Mean | Scale Variance | Corrected Correlation | Squared Multiple Correlation | Cronbach's Alpha |
| I often use Digital Banking, wallet or any other fintech services for my transactions. | 29.04 | 32.348 | .300 | . | .960 |
| I am hesitant to share my personal information with Fintech service providers. | 28.44 | 30.101 | .720 | . | .913 |
| The personal information that I provide to Fintech organizations is important to me. | 28.27 | 29.992 | .818 | . | .906 |
| I feel insecure when I provide my personal information to Fintech organizations. | 28.32 | 29.901 | .826 | . | .905 |
| I think that someone else is accessing my personal and financial information besides the fintech. | 28.31 | 28.863 | .926 | . | .897 |
| I am concerned that my personal information might be stolen or intercepted | 28.41 | 30.440 | .755 | . | .910 |
| The fintech service providers ask for sensitive information from users | 28.31 | 28.863 | .926 | . | .897 |
| The fintech service provider does not disclose how they plan to use our personal information | 28.31 | 28.863 | .926 | . | .897 |

Table 11: Overall statistics for all items

**Reliability test for Security**

|  |  |  |
| --- | --- | --- |
| **Reliability Statistics** | | |
| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
| .860 | .894 | 8 |

Table 12: Reliability test for security

The above reliability for Security show a high value of 0.860. That means the questionnaire for the survey will yield reliable results. This also indicates a high level of consistency of responses of each participant in a set of survey items. Hence, the questions included for Security are extremely reliable.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Questionaires for security | | | | | |
|  | Scale Mean | Scale Variance | Total Correlation | Squared Multiple Correlation | Cronbach's Alpha |
| I feel that the current system in Fintech Nepal is not mature enough to make the electronic identity records secure. | 27.19 | 25.485 | .818 | .727 | .821 |
| I do not feel secure making a high amount of transactions through Fintech. | 27.13 | 25.451 | .840 | .771 | .819 |
| I have often become a victim of Digital Fraud. | 27.51 | 25.864 | .486 | .412 | .864 |
| I doubt that Fintech services will become more secure in the future in Nepal. | 27.14 | 25.327 | .838 | .756 | .819 |
| I feel that the transactions that I perform through Fintech are not secure. | 27.12 | 25.666 | .826 | .764 | .821 |
| I feel that the Fintech industry in Nepal is immature and insecure compared to other developed countries in the world. | 27.08 | 26.001 | .824 | .770 | .823 |
| I feel that the information I provide to Fintech organizations is prone to hacking. | 27.07 | 25.756 | .793 | .754 | .824 |
| I don't trust Fintech organizations because of lack of security while making transactions through Fintech | 28.76 | 32.985 | -.047 | .074 | .931 |

**Reliability test for Blockchain**

|  |  |  |
| --- | --- | --- |
| **Reliability Statistics** | | |
| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
| .956 | .957 | 9 |

Table 13: Reliability test for blockchain

The above statistics for Blockchain show a high reliability of 0.956. That means the questionnaire for the survey will yield reliable results. This also indicates a high level of consistency of responses of each participant in a set of survey items. Hence, the questionaires are highly reliable for blockchain.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Questionaires related to Blockchain** | | | | | |
|  | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Squared Multiple Correlation | Cronbach's Alpha if Item Deleted |
| Blockchain is an emerging concept in Nepal | 31.83 | 42.967 | .649 | .536 | .960 |
| I feel that the blockchain use in the Fintech can make my personal information secure. | 31.65 | 41.221 | .853 | .787 | .949 |
| I feel that the blockchain use in the Fintech can help organizations win the trust of their customers by securing payment. | 31.58 | 41.390 | .867 | .793 | .948 |
| I feel that the use of blockchain can help organizations prevent their system from being hacked. | 31.60 | 41.311 | .850 | .741 | .949 |
| I feel that blockchain can minimize latency in Fintech. | 31.65 | 41.888 | .854 | .763 | .949 |
| I feel that blockchain can create a higher scope in Fintech. | 31.67 | 41.287 | .852 | .769 | .949 |
| I feel that blockchain is the ultimate solution to data privacy and security in Fintech. | 31.61 | 41.457 | .846 | .750 | .949 |
| I would use Fintech services more often if they used a Blockchain system for data security and privacy. | 31.61 | 41.256 | .841 | .749 | .950 |
| I think the use of Blockchain is the future of the Fintech industry's security and privacy | 31.71 | 41.842 | .787 | .632 | .952 |

Above table shows that value of Cronbach’s alpha for all the questions is more than 0.9 if any of the items are deleted. This also shows that the reliability of the questionnaire is quite high.

On the other hand, when we ran a correlation and validity test for all the questionnaires, the result showed that all the questions used in the survey were valid as the correlation was less than or equal to 0.01 for all the questions. This value for all the questions shows that the questions included in the questionnaires are valid.

## **4.3 Descriptive Analysis**

### **4.3.1 Background of the Respondents**

The demographic data collected pertained to the respondents' background, encompassing information such as occupational background, age, income group, and gender.

**4.3.1.1 RESPONDENT'S AGE**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Age** | | | | | |
|  | | Frequency | Per cent | Valid Percent | Cumulative Percent |
| Valid | 15-24 | 64 | 15.9 | 15.9 | 15.9 |
| 25-34 | 180 | 44.8 | 44.8 | 60.7 |
| 35-44 | 129 | 32.1 | 32.1 | 92.8 |
| 45-54 | 23 | 5.7 | 5.7 | 98.5 |
| 55 and above | 6 | 1.5 | 1.5 | 100.0 |
| Total | 402 | 100.0 | 100.0 |  |

Table 14: Age-Based Distribution of Respondents

Table 15: Pie chart of age distribution

The above frequencies represent the proportion of individuals within each age group accounted for in the dataset, progressing from the lowest age group (15-24) to the highest age group (55 and above). There are the highest number of respondents from the age group 25-34 and the lowest respondents are from the age group 55 and above. There are 180 respondents in the age group 25-34 and 129 respondents in the age group 35-44, making these the highest respondent categories. There are only 6 respondents in the age group 55 and above.

**4.3.1.2 RESPONDENTS GENDER**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Gender** | | | | | |
|  | | Frequency | Per cent | Valid Percent | Cumulative Percent |
| Valid | Female | 157 | 39.1 | 39.1 | 39.1 |
| Male | 245 | 60.9 | 60.9 | 100.0 |
| Total | 402 | 100.0 | 100.0 |  |

Table 16: Gender Statistics

Table 17: Pie-chart of genderof respondents

The figure shows the pie chart of the majority of the respondents in the research were male. 60.9%, i.e., 245 male respondents participated in the survey while only 39.1%, i.e., 157 female respondents participated in the survey.

**4.3.1.3 OCCUPATIONAL BACKGROUND OF RESPONDENTS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Occupational Background** | | | | | |
|  | | Frequency | Per cent | Valid Percent | Cumulative Percent |
| Valid | Non-technical | 33 | 8.2 | 8.2 | 8.2 |
| Technical (IT/ computer science and other related background) | 369 | 91.8 | 91.8 | 100.0 |
| Total | 402 | 100.0 | 100.0 |  |

Table 18: Occupational background of respondents

Table 19: Pie-chart of occupational background of total respondents

The pie chart in the above figure shows that 91.8% of respondents are from an IT background or have another related technical background while only 8.2% people are from a non-technical background. Only 33 respondents were from non-technical backgrounds while all other 369 respondents were from the technical background.

**4.3.1.4 OCCUPATION**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Occupation** | | | | | |
|  | | Frequency | Per cent | Valid Percent | Cumulative Percent |
| Valid | Employed (Full-time/Part-time) | 328 | 81.6 | 81.6 | 81.6 |
| Others | 2 | .5 | .5 | 82.1 |
| Self-employed | 56 | 13.9 | 13.9 | 96.0 |
| Student | 9 | 2.2 | 2.2 | 98.3 |
| Unemployed | 7 | 1.7 | 1.7 | 100.0 |
| Total | 402 | 100.0 | 100.0 |  |

Table 20: Occupation statistics of respondents

Table 21: Pie-chart of occupation of various respondents

The majority of the participants who responded to the survey were employed full time and the remaining were either self-employed, unemployed, or students. The pie chart shows that 81.6% of employees were working as full-time employees which constituted 328 respondents.

**Income**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Monthly Income (in NRs)** | | | | | |
|  | | Frequency | Per cent | Valid Percent | Cumulative Percent |
| Valid | 50001 to 200,000 | 139 | 34.6 | 34.6 | 34.6 |
| Above 200,000 | 24 | 6.0 | 6.0 | 40.5 |
| Between 15000 and 50000 | 216 | 53.7 | 53.7 | 94.3 |
| Less than 15000 | 23 | 5.7 | 5.7 | 100.0 |
| Total | 402 | 100.0 | 100.0 |  |

Table 22:Monthly income statistics of all respondents

Table 23: Pie-chart of monthly income of respondents

The above table shows that the respondents earning between 15000 to 50,000 are highest. The second highest earn between 50,000 to 200,000.

## **4.4 Correlation Analysis**

The research study has three major variables namely Privacy (p\_total) and Security (s\_total  
), Blockchain (B\_total). Here, Blockchain is the independent variable, and Privacy and Security are the dependent variables.

### **4.4.1 Correlation between Privacy and Blockchain**

The correlation analysis between two variables, Privacy and Blockchain, yields the following results:

|  |  |  |  |
| --- | --- | --- | --- |
| **Correlations** | | | |
|  | | P\_Total | B\_Total |
| P\_Total | Pearson Correlation | 1 | .776\*\* |
| Sig. (2-tailed) |  | <.001 |
| N | 402 | 402 |
| B\_Total | Pearson Correlation | .776\*\* | 1 |
| Sig. (2-tailed) | <.001 |  |
| N | 402 | 402 |
| \*\*. Correlation is significant at the 0.01 level (2-tailed). | | | |

Table 24: Statistical representation of correlation between privacy and blockchain

Pearson Correlation for Privacy and Blockchain: The Pearson correlation coefficient between Privacy and Blockchain is 0.776. This value represents the significance and strength of relationship between the variables.

Sig. (2-Tailed) with B\_Total: The p-value associated with the correlation coefficient for P\_total with B\_total is <0.001. This p-value shows the significance of the observed correlation. In this case, the p-value is below 0.001, and thus suggests a highly significant relationship between Privacy and Blockchain.

N value: The N value represents the sample size, which in this case is 402. It indicates the number of data points or observations used to calculate the correlation coefficient.

Interpretation: Based on the results, we can interpret the correlation analysis as follows:

Privacy and Blockchain have a strong correlation, as the correlation coefficient is 0.776. The positive sign implies that as the implementation of Blockchain exists or increases, privacy tends to increase as well. In statistical analysis, the p-value helps us determine whether the relationship we found in our data is a real and meaningful relationship or just a result of random variation. A p-value of less than 0.001 is considered very small, indicating that there is very strong evidence against the idea that the correlation took place only by chance.

Therefore, we can confidently say that the correlation that we observed between privacy and blockchain is not just a coincidence. It shows a genuine and meaningful relationship between these variables in the larger population from which the data was collected. The relationship of Privacy and Blockchain is likely to hold beyond our specific sample and can be considered a reliable finding.

To conclude, there is a strong and highly positive correlation (r = 0.776, p < 0.001) of Privacy and Blockchain in the given set of observations. This shows that if we make use of Blockchain Technology privacy will also increase in Fintech industries which in turn creates a perception among users that their data and information are safe.

### **4.4.2 Correlation between Blockchain and Security**

The correlation analysis between two variables Security and Blockchain in Nepal, yields the following results:

|  |  |  |  |
| --- | --- | --- | --- |
| **Correlations** | | | |
|  | | B\_Total | S\_Total |
| B\_Total | Pearson Correlation | 1 | .845\*\* |
| Sig. (2-tailed) |  | <.001 |
| N | 402 | 402 |
| S\_Total | Pearson Correlation | .845\*\* | 1 |
| Sig. (2-tailed) | <.001 |  |
| N | 402 | 402 |
| \*\*. Correlation is significant at the 0.01 level (2-tailed). | | | |

Table 25: Statistical representation of correlation between blockchain and security

Pearson Correlation for Blockchain and Security: The Pearson correlation coefficient between Blockchain and security is 0.845. This value represents a positive relation between these variables.

Sig. (2-Tailed) with B\_Total: The p-value associated with the correlation coefficient for S\_total with B\_total is <0.001. In this case, the p-value is below 0.001, which suggests a strong relationship between Security and Blockchain.

N value: The N value represents the sample size, which in this case is 402. It indicates the number of data points or observations used to calculate the correlation coefficient.

Interpretation: Based on the results, we can interpret the correlation analysis as follows:

Security and Blockchain, have a correlation coefficient of 0.845, which is strongly positive. The positive sign implies that as the implementation of Blockchain exists or increases, security tends to increase as well. In statistical analysis, the p-value helps us determine whether the relationship we found in our data is a real and meaningful relationship or just a result of random variation. A p-value of less than 0.001 is considered very small, indicating strong evidence against the idea that the correlation occurred by chance alone.

Therefore, we can confidently say that the correlation we observed between security and blockchain is not just a coincidence. It shows that a real and meaningful relationship between these variables in the larger population from which the data was collected. The relationship exists between Security and Blockchain is likely to hold beyond our specific sample and can be considered a reliable finding.

Overall, we can conclude that there is a strong and highly significant correlation (r = 0.845, p < 0.001) of Security and Blockchain in the given set of observations. This shows that if we make use of Blockchain Technology security will also increase in Fintech industries which in turn creates a perception among users that the transactions that they make through fintech are secure.

**Regression**

**Regression between Blockchain and Privacy**

|  |  |  |  |
| --- | --- | --- | --- |
| **Variables Entered/Removed** | | | |
| Model | Variables Entered | Variables Removed | Method |
| 1 | B\_Totalb | . | Enter |
| a. Dependent Variable: P\_Total | | | |
| b. All requested variables entered. | | | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Model Summary** | | | | | | | | | |
| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate | Change Statistics | | | | |
| R Square Change | F Change | df1 | df2 | Sig. F Change |
| 1 | .776a | .602 | .601 | .48974 | .602 | 603.833 | 1 | 400 | <.001 |
| a. Predictors: (Constant), B\_Total | | | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ANOVAa** | | | | | | |
| Model | | Sum of Squares | df | Mean Square | F | Sig. |
| 1 | Regression | 144.824 | 1 | 144.824 | 603.833 | <.001b |
| Residual | 95.936 | 400 | .240 |  |  |
| Total | 240.761 | 401 |  |  |  |
| a. Dependent Variable: P\_Total | | | | | | |
| b. Predictors: (Constant), B\_Total | | | | | | |

Table 26: Statistical representation of regression between blockchain and privacy

In the above model summary table, it is seen that the valur of R square is 0.602. This shows that a 60.2% change or variance in privacy variables can be accounted for by the implementation of the blockchain system.

In addition, the ANOVA shows that the positive value for regression is less than 0.001. This shows that there is a significant impact of Blockchain on privacy in the fintech industry.

**Regression between Blockchain and Security**

|  |  |  |  |
| --- | --- | --- | --- |
| **Variables Entered/Removed** | | | |
| Model | Variables Entered | Variables Removed | Method |
| 1 | B\_Totalb | . | Enter |
| a. Dependent Variable: S\_Total | | | |
| b. All requested variables entered. | | | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Model Summary** | | | | | | | | | |
| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate | Change Statistics | | | | |
| R Square Change | F Change | df1 | df2 | Sig. F Change |
| 1 | .845a | .714 | .714 | .39386 | .714 | 1000.563 | 1 | 400 | <.001 |
| a. Predictors: (Constant), B\_Total | | | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ANOVAa** | | | | | | |
| Model | | Sum of Squares | df | Mean Square | F | Sig. |
| 1 | Regression | 155.215 | 1 | 155.215 | 1000.563 | <.001b |
| Residual | 62.051 | 400 | .155 |  |  |
| Total | 217.266 | 401 |  |  |  |
| a. Dependent Variable: S\_Total | | | | | | |
| b. Predictors: (Constant), B\_Total | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Coefficients** | | | | | | |
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| B | Std. Error | Beta |
| 1 | (Constant) | .852 | .099 |  | 8.644 | <.001 |
| B\_Total | .772 | .024 | .845 | 31.632 | <.001 |
| a. Dependent Variable: S\_Total | | | | | | |

Table 27: Statistical representation of regression between blockchain and security

In the above model summary table, it is seen that the value of R square is 0.714. This shows that a 71.4% change or variance in the Security variable can be accounted for by the implementation of the blockchain system.

In addition, the ANOVA shows the regression value is below 0.001. This shows that there is a significant impact of Blockchain on the security in the fintech industry.

**Q-Q plots**

The Q-Q plots show some differences in expected normal as well as detrended normal plots of privacy and security.

Q-Q plots for Privacy

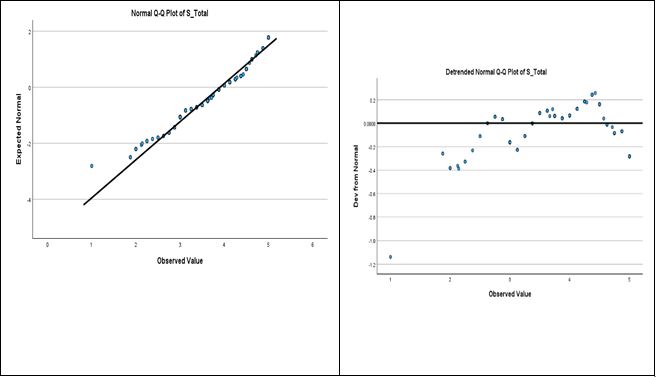


Table 28: Q-Q plots for Privacy

**Q-Q plots for Security**

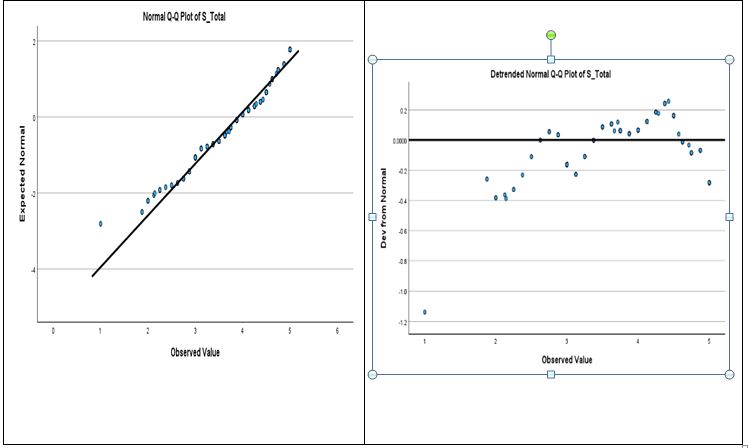


Table 29: Q-Q plot for Security

The Q-Q plots show some differences in expected normal as well as detrended normal plots of the Security variable.

**Q-Q plot of Blockchain**

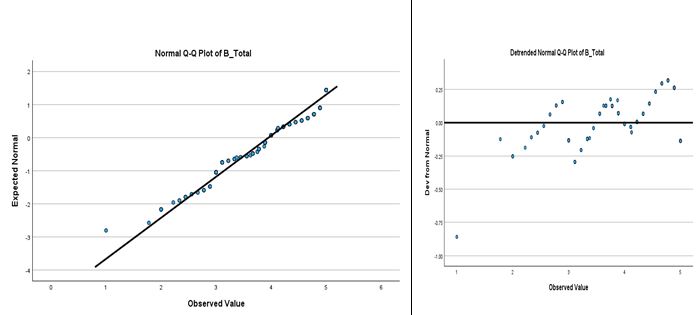


Table 30: Q-Q and histogram plots for Blockchain

The Q-Q plots show some differences in expected normal as well as detrended normal plots of Blockchain

**Mean Analysis of the Privacy and Security**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Mean analysis | | | | | |
|  | N | Minimum | Maximum | Mean | Std. Dev |
| I often use Digital Banking, wallet or any other fintech services for my transactions. | 402 | 1 | 5 | 3.45 | 1.326 |
| I am hesitant to share my personal information with Fintech service providers. | 402 | 1 | 5 | 4.04 | .967 |
| The personal information that I provide to Fintech organizations is important to me. | 401 | 1 | 5 | 4.21 | .880 |
| I feel insecure when I provide my personal information to Fintech organizations. | 400 | 1 | 5 | 4.16 | .880 |
| I think that someone else is accessing my personal and financial information besides the fintech. | 402 | 1 | 5 | 4.18 | .900 |
| I am concerned that my personal information might be stolen or intercepted | 402 | 1 | 5 | 4.07 | .886 |
| The fintech service providers ask for sensitive information from users | 401 | 1 | 5 | 4.18 | .899 |
| The fintech service provider does not disclose how they plan to use our personal information | 401 | 1 | 5 | 4.18 | .899 |
| I feel that the current system in Fintech Nepal is not mature enough to make the electronic identity records secure. | 402 | 1 | 5 | 4.10 | .926 |
| I do not feel secure making a high amount of transactions through Fintech. | 401 | 1 | 5 | 4.16 | .915 |
| I have often become a victim of Digital Fraud. | 402 | 1 | 5 | 3.76 | 1.316 |
| I doubt that Fintech services will become more secure in the future in Nepal. | 399 | 1 | 5 | 4.14 | .937 |
| I feel that the transactions that I perform through Fintech are not secure. | 400 | 1 | 5 | 4.17 | .905 |
| I feel that the Fintech industry in Nepal is immature and insecure compared to other developed countries in the world. | 402 | 1 | 5 | 4.20 | .875 |
| I feel that the information I provide to Fintech organizations is prone to hacking. | 400 | 1 | 5 | 4.22 | .924 |
| I don't trust Fintech organizations because of lack of security while making transactions through Fintech | 401 | 1 | 5 | 2.52 | 1.321 |
| Valid N (list wise) | 390 |  |  |  |  |

Table 31: Mean analysis of privacy and security

The above results obtained from the survey show that most of the participants of the survey used some kind of Fintech service. This is likely because the respondents are from IT and Fintech backgrounds so it’s obvious that few from this population often used Fintech services. However, the results also show that though they use Fintech services, most are hesitant to share their personal information with the Fintech service providers. They also feel that the Fintech industry in Nepal is not mature enough to make electronic identity records secure, thus, they are hesitant to make a high amount of transactions through Fintech. On the other hand, most people responded that they have also become a victim of some kind of Digital Fraud. Moreover, most of the respondents feel that someone else also has access to their personal and financial information which they have given to the Fintech organizations. The majority of the respondents also responded that they feel that the information that they provide to Fintech organizations is prone to hacking.

Thus, the above survey results show that though people in IT and Fintech organizations use Fintech services, they are not yet very sure about the security system in these organizations. They are still sceptic that the information that the Fintech has about them might be insecure, might be duplicated, and might be hacked.

# **CHAPTER 5** **FINDINGS AND DISCUSSIONS**

*The process of data analysis and findings are now discussed. It delves into the correlation between the selected variables and offers conclusions that address the initial research questions.*

### **5.1.1 Challenges Faced During the Responses Collection**

* Restricted to an online survey
* Few responses not received as anticipated

### **5.1.2 Demographic Data**

The statistical analysis showed that there were significantly more male respondents than female respondents. This is possible because the research respondents are from IT and fintech backgrounds and we know that in Nepal there is a high number of male populations working in the IT sector. The number of females in the IT industry is slowly increasing however, the number is still very low compared to the number of male members in the IT sector.

The statistical results also showed that most respondents were 25-34 age group. This shows that the IT and fintech industries are mostly populated with youth. This is because the fintech industry is just emerging in Nepal so the younger generation is more attracted towards the Fintech as well as the IT industry. Also, this is generally the age group that takes responsibility for the family or themselves and uses digital wallets and other fintech services more than people of other age groups.

In addition, the majority of the respondents are from an IT background. This is because the research questionnaires have been distributed only in the IT and Fintech industry assuming that the majority of the people from nontechnical backgrounds would not be able to know the technical terms associated with blockchain, its usage, and its advantages and disadvantages.

The majority of respondents in the survey responded that their salary ranged from 15000 to 50000.  This might be a true figure because the majority of the staff in these organizations are young and in entry-level positions thus not earning more than 50,000. However, few responded that they have a salary of less than 15000 range. This might either be because few people do not want to disclose their salary range and have randomly chosen false data or interns might have been given to fill up the research data because normally IT and Fintech organizations hire several interns.

### **5.1.3 Interpretation of Findings**

The major outcomes derived from the statistical data analysed are briefly discussed in this chapter.

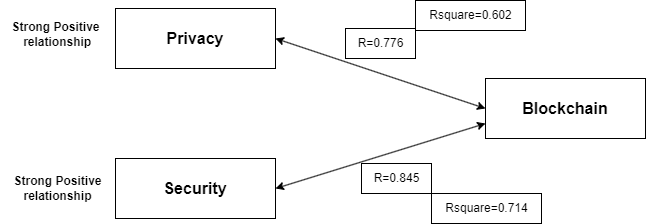


Table 32: Relationship of blockchain with privacy and security

The major intent of the research was to identify whether a blockchain system of the model can change the privacy and security status of Fintech services in Nepal. A thorough data analysis was done using SPSS and the following results were witnessed for the questions below.

**RQ1. What is the current state of the fintech industry in Nepal in terms of the privacy and security of users' personal and financial information?**

**Findings:**

A survey was carried out among 402 participants to identify the state of the Fintech industry in terms of privacy and security and the participant’s perception regarding the same variables were measured.

The outcome from the survey depicted that more than half of the respondents were users of Fintech services and it was found that the privacy and security perceived by these respondents were significantly lower because they do not trust the Fintech services much.

The findings showed that crucial portion of the respondents were users of various Fintech services. This might be because all the respondents are either from Fintech or IT organizations, hence, there is a high chance that most of these respondents have used Fintech in their daily lives.

A majority of the respondents responded that they are not quite comfortable sharing their details with the fintech service provider because they do not trust fintech with their sensitive personal information. In addition, the results of the survey also showed that people do not think that the infrastructure in Nepal is mature enough to safeguard the records of the users properly.

Consequently, these respondents hesitate to engage in substantial financial transactions through Fintech platforms. A handful of respondents also said that they have become victims of digital fraud in some way.

Furthermore, a majority of the participants feel that their personal and financial information might also be accessible to unauthorized parties. This in turn leads to a belief that the information that they disclose might be prone to hacking attempts.

In addition, the report of NRB also showed that there were an increasing number of suspicious transactions and activities in the financial sector of Nepal, with banks, financing and lending companies and insurance companies being at high risk. These activities have further led to finance offences involving banking fraud and money laundering (FIU, 2022). Further proving that the perception of the respondents regarding privacy and security was correct.

**RQ2.  Is there any significant relationship between the implementation of the Blockchain system and the privacy of data in Fintech?**

Findings: A correlation and regression analysis was carried out between the two variables ‘Privacy’ and ‘Blockchain’ system and it showed a highly positive correlation between these two variables.

A solid positive connection exists between Privacy and Blockchain, as shown by a Pearson correlation coefficient of 0.776. The positive coefficient indicates that an increase in the implementation of Blockchain is associated with increased levels of privacy. The significance of this relationship is assessed through the p-value in statistical analysis. A p-value below 0.001 is known to be very small, citing that the correlation did not happen merely due to chance.

To sum up, the data set of 402 observations indicates a highly noteworthy correlation (r = 0.776, p < 0.001) of Blockchain and privacy variables. This establishes that the adoption of Blockchain Technology leads to an increase in data privacy, particularly within the realm of Fintech industries.

During the process of performing the regression analysis, it was found that the coefficient of determination (R-squared) is 0.602. This shows that 60.2% of the discrepancies in the privacy variable can be explained by the presence of the blockchain system.

Furthermore, the analysis of variance (ANOVA) table shows that the p-value associated with the regression is below 0.001. This outcome shows the significant influence of the blockchain on privacy within the fintech sector.

Additionally, previous research also shows that the use of blockchain can increase privacy in Fintech. Algorithms such as hash algorithms can be used to counter cyberattacks on fintech by maintaining privacy and security (Thakur & Sharma, 2023). Similarly, a research conducted by (Baliker et al., 2023) has used a hyperledger fabric blockchain , a private blockchain framework to increase privacy in Fintech sector.

**RQ3.  Is there any significant relationship between the implementation of the Blockchain system and the Security of data and transactions in Fintech?**

Findings: A correlation and regression analysis was carried out between the two variables ‘Security’ and ‘Blockchain’ system and it showed a highly positive correlation.

A strong positive connection exists between Security and Blockchain, as shown by a Pearson correlation coefficient of 0.845. The positive coefficient indicates that an increase in the implementation of Blockchain is associated with increased levels of security. The significance of this relationship is assessed through the p-value in statistical analysis. A p-value below 0.001 is known to be very small, citing that the correlation did not happen merely due to chance.

A robust and favourable connection exists between Security and Blockchain Systems, as demonstrated by a Pearson correlation coefficient of 0.845. The positive coefficient indicates that an implementation of Blockchain or a heightened level of use in Blockchain is associated with heightened levels of security.

To sum up, the data set of 402 observations indicates a highly noteworthy correlation (r = 0.845, p < 0.001) between Blockchain and privacy variables. This establishes that the adoption of Blockchain Technology leads to an increase in data security, particularly within the area of Fintech industries.

During the process of performing the regression analysis, it was found that the coefficient of determination (R-squared) stands at 0714. This shows that 71.4% of the discrepancies in the privacy variable can be acgieved through Blockchain.

Furthermore, the analysis of variance (ANOVA) table shows that the p-value associated with the regression is below 0.001. This outcome shows the significant influence of the blockchain on privacy within the fintech sector.

In addition, research conducted by (Mamun et al., 2020) states that the implementation of Blockchain along with the IPFS can secure the financial system, financial data and transactions. Other researchers have used smart contracts and blockchain to secure fintech transactions (Hassan et al., 2021).

**RQ4. Is there any suitable conceptual framework that addresses the gap of privacy and security in the Fintech industries of Nepal?**

**Findings**: Yes, there is a conceptual framework based on a Hyperledger Fabric blockchain. that helps to improve the privacy and security of the Fintech system.

Hyperledger Fabric, a private blockchain framework can be used to make secure payments and privately share and store the information. They can also involve various participants, including fintech users, regulators, providers and researchers. Each participant needs to register themselves to create their digital identity through the MSP. Whenever a fintech user executes a transaction, it is shared only within a selected channel, thus maintaining privacy and confidentiality among involved parties. The transactions are carried out through smart contracts or chain codes that define the transaction logic and rules. The fintech provider then validates the transaction, making sure it is compliant with the rules of that particular smart contract.

The consensus mechanism guarantees agreement among ordering nodes before the transaction is committed to the ledger by committer peers. Furthermore, KYC information can be securely stored on the network, accessible only to authorized entities like fintech regulators and institutions. Researchers can leverage the blockchain for data analysis, while still keeping privacy. This process ensures secure, compliant, and private financial transactions in the fintech ecosystem(Wylde et al., 2022).

## **5.2 Conceptual Framework**

To identify and record the fintech users within a firm, the fintech employees get complete access to the personal and financial data of the users. This information is sensitive as it may include very personal or card details. Oftentimes, the users are unaware of the potential access to their information by other individuals, employees, financial institutions and researchers. This makes the user's information highly vulnerable to risks as there are privacy and security concerns.

To address and overcome this issue, the implementation of a blockchain-based architecture can be a potential solution. This conceptual framework ensures and safeguards security and privacy measures for the fintech records. A visual representation of this proposed architecture is presented in the Figure.

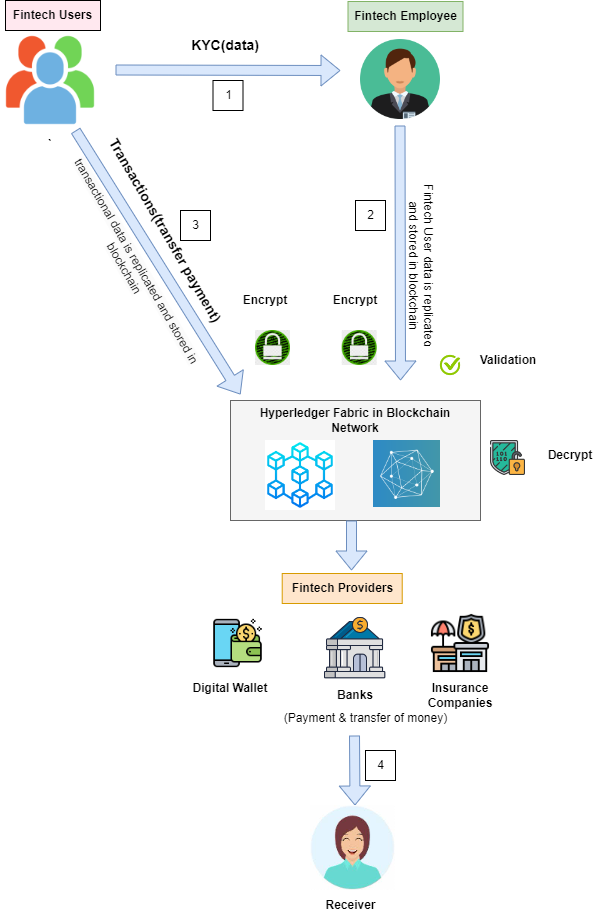


Figure 24: Conceptual framework using the Hyperledger Fabric blockchain

Whenever an individual registers with the fintech institution by filling out the KYC form, they provide their personal information, which is then stored securely within a blockchain network. After the successful documentation of the KYC in the blockchain, the fintech users are then eligible to make a payment or transaction. The transaction log and the KYC include the financial and personal information of the users. The users have a strong desire to store their personal and financial information privately and accessible to only authorized parties. Hence, to address this concern, blockchain technology can be utilized in conjunction with the Hyperledger Fabric for a better remedy to the issues.

A Hyperledger blockchain is known for its private nature, which can allow the employment of networks with restricted access. This is a unique feature as it differs from blockchain such as Bitcoin and Ethereum, which allows everyone to become a part of a network and get access to the data by simply downloading the application. Furthermore, this blockchain uses a distributed Ledger Technology (DLT), and with this feature, the financial data of users are duplicated across the blockchain network. Additionally, no central authority exists to govern the data as the blockchain is decentralized.

Whenever a participant, whether it be a user, provider, regulator or researcher in a fintech, joins the blockchain network, each participant is provided with public and private keys. The visibility of public key is open to all whenever execution of a transaction takes place whereas a private key is only accessed by the key holder.

When a request is made to access the information from the user, the public key of the provider is sent to the user. The user then encrypts the data and transmits it using the provider's public key. This procedure makes sure only the designated provider accesses the records. The provider then uses their private key to decrypt and access the data. This public-key cryptography is an asymmetric method that guarantees no data can be accessed without the authorization of users.

Data security can be achieved through this approach as users can monitor any unauthorized data access attempts. Moreover, a secure communication channel between the fintech users and other entities is also established through this technique.

Along with the establishment of channels, the Hyperledger fabric also allows the creation of sub-networks within a node network. This makes the information solely accessible to a specific channel. When new blocks are added to the network, they are channelled through the Membership Service Provider (MSP). The same ledger is shared by nodes in the same sub-network.

To illustrate, think about a scenario where the fintech companies solely necessitate access to a specific fintech user. For this, a unique channel is created along with the requirements. This Hyperledger fabric-based blockchain framework ensures the privacy and security of the user’s record.

**Detailed architecture of the HyperLedger Fabric conceptual research framework**

A complete and detailed view of the proposed architecture is given below.

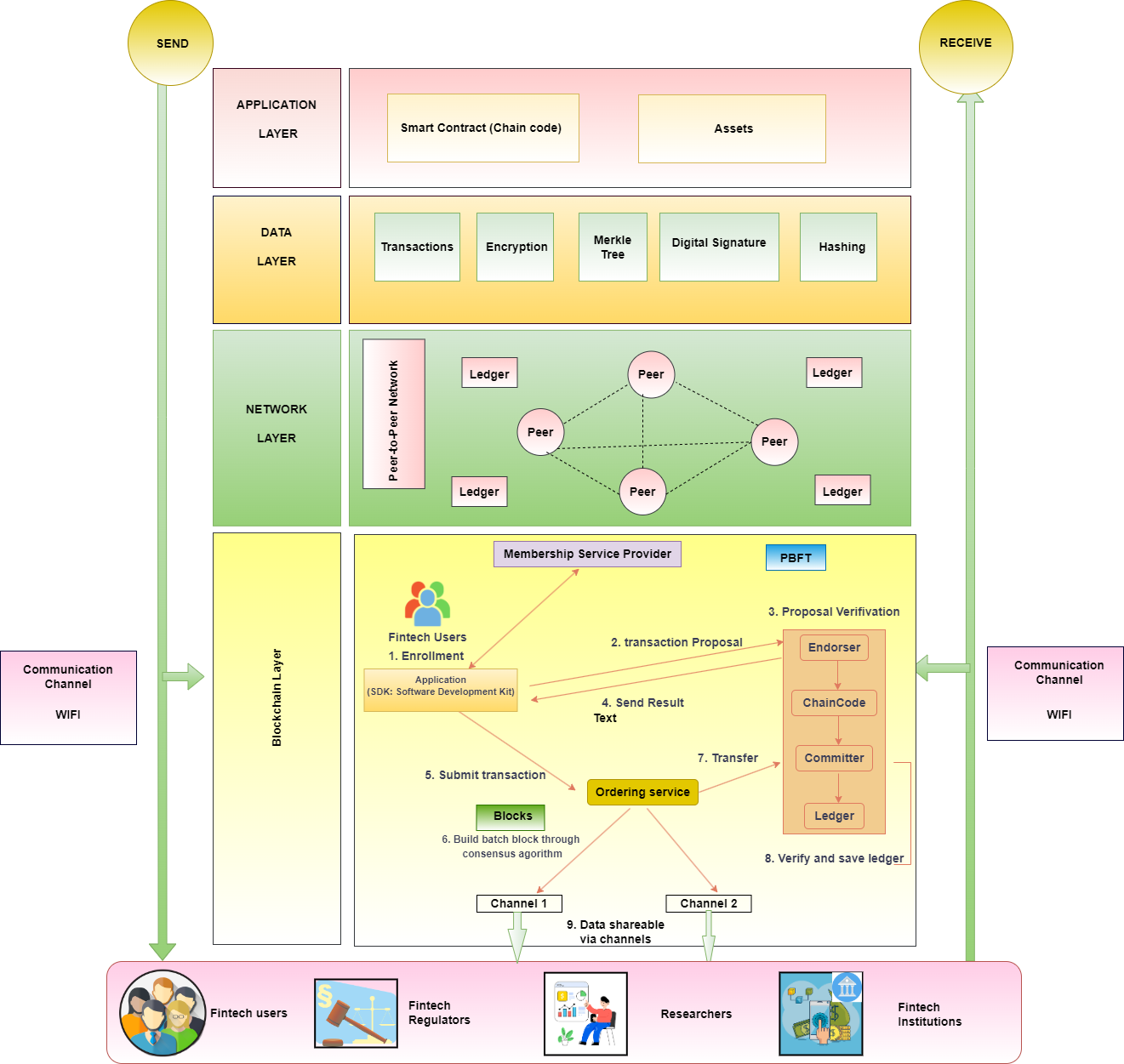


Figure 25: Detailed view of the Hyperledger Fabric architecture for private and secure payment and record of transactions

These include various layers in the blockchain which are discussed below.

* **Application Layer**

The application layer stands in the highest tier and comprises smart contracts and assets. The assets refer to the collection of key-value pairs stored as transactions on each ledger. The smart contract, on the other hand, encapsulates the operational logic of transactions within the fintech network. The chain code or smart contract embody a set of protocols, and utilize many different programming languages such as Java, Golang or Python. In Ethereum however, they are mostly written in Solidity language.

* **Data layer**

Various blockchain elements such as encryptions, transactions, Merkle tree, hashing and digital transactions are included within the data layers. With the help of these components, transactions are recorded inside the block, ensuring a high level of security.

* **Network Layer**

The network layer involves the configuration of the peer-to-peer network. Each peer serving as a node in this layer establishes a connection with all other nodes in the network. And if there is a need to establish, alter or delete a new financial record, each peer within the network records the transaction inside the ledger, ultimately replicating the user’s data within that blockchain network. At times when any node attempts to introduce a different value, the ledger is not modified.

* **Blockchain layer**

This layer comprises consensus mechanism, blocks and other important components of the Hyperledger fabric such as MSP, Ledger and consensus. The framework employs the PBFT consensus algorithm for its transactional operation. Ledger plays an equally important role in managing the transaction log and database and archiving the history of this information.

Hyperledger also uses the concept of creating sub-networks or channels, which exclusively gives visibility of transactional information to the member participants engaged within it. Participants including an individual or an entity can register for a membership through the MSP request and enrolment process. This allows all the fintech institutions, users, regulators, researchers and other entities to get a verified digital membership identity through the MSP. MSP can help with the validation of the certificate, authorization of users and issuance. Upon request, these certificates are granted by the Central authority (CA). The MSP and CA combine to manage and secure participants’ identities and offers authentication, authorization and validation process within the blockchain network.

So, when a peer is authenticated through the MSP and CA, they forward the transaction to the ordering service, which validates the transactions. The ledger is then automatically modified after the validation process and this modification is distributed among all peers. The remaining peers then authenticate and acknowledge the modifications, and update their respective ledgers. The Ordering Service Nodes are responsible for assuming the task of upholding consensus within the peer network.

**The Pool of Fintech Stakeholders**

The pool of stakeholders within the fintech sector includes the fintech users, regulators, researchers and financial institutions. These stakeholders connect with the blockchain network either through a web application or a mobile application via WIFI, which serves as a communication conduct.

The financial institutions and regulators establish and share a designated channel to access the user's data, whereas other stakeholders such as researchers, who don’t need access to the financial data, create a different channel. This way of segregation of data access through channels gives access privileges within the blockchain network.

Unlike in Bitcoin and Ethereum blockchain, where all nodes observe every transaction log publicly, the Hyperledger allows the privacy of this transaction through separate channels and also enables private data viewing. Similarly, the cryptographic elements within the blockchain further boost data security. Thus, the proposed Hyperledger fabric framework utilizes a unique blockchain network to effectively address the privacy and security of financial information.

# **CHAPTER 6** **CONCLUSION AND RECOMMENDATIONS**

*The findings are now summarized and recommendations are discussed for stakeholders and future researchers, and includes researchers' perspectives on the achieved results.*

## **6.1 Conclusion**

The research presents the problem of high vulnerabilities in fintech-related security and privacy, especially in a developing country like Nepal. The tremendous rise in the digitalization of finance has intensively exposed the industry itself to various risks. Fintech users are now worried the misuse of their financial information due to the increasing global fintech breaches and cybercrime incidents.

Hyperledger Fabric, a private blockchain is thus proposed as a solution, to secure financial information. It secures and privately allow sharing of data by utilizing cryptographic measures and also creates multiple channels to separate information that allows the fintech users to control their data access to a third party. Moreover, it aims to improve privacy data security, and trust among the fintech users, ultimately enhancing Nepal's fintech industry.

The statistical analysis results clearly showed that though the majority of people are users of Fintech services, the privacy and security perceived by the users is much lower and they feel that Fintech services are still not secure to use.

A correlation and regression analysis were carried out between the two variables ‘Privacy and Security’ and ‘Blockchain’ system and it showed a highly positive correlation between of the variables.

## 6.2 **Recommendations**

This research has been able to present various gaps and challenges in the current Fintech system and successfully propose blockchain solutions for better privacy and security of the user's financial information across the industry. The below-mentioned areas are some recommendations of this research.

* **Fintech Start-ups**

Fintech Startups should refer to privacy and security measures using blockchain technology. This can help them improve their trust towards their clients in the future.

* **Regulators and Government authorities**

Regulators and government agencies need to stay updated with the new technologies to build up better policies for fintech companies. This research can be studied for the development of regulatory frameworks for the secure share of data. Smart contracts in blockchain can be further studied to resolve conflicts between two parties.

* **Researchers**  
  Researchers should conduct more quantitative research and include conceptual frameworks. There is still not much quantitative research done in the blockchain sector.
* **Blockchain Developers**
* Blockchain developers could get insights on the blockchain algorithms and census, which could be useful to improve the smart contracts in various sectors.
* **Fintech users**

The users within the fintech industries can be aware of the various risks and vulnerabilities to their personal and financial information. Moreover, they may benefit from the increased privacy and security measures of their information from the blockchain implementation.

* **Financial Institutions and Banks**:

Traditional banks and financial institutions should be aware of the various cyberattacks happening in Fintech. They can also introduce secure data storage methods using blockchain to improve the privacy and security of their client's personal and financial data.

* **Blockchain Technology Providers**: Blockchain companies can develop their products and improve the trust of their clients toward their products through the use of smart contracts, various consensus mechanisms and algorithms.
* **Cyber security Experts**: Cyber-security people should understand the various cyber-attacks in Fintech, including different blockchain methods and cryptographic measures for improved privacy and security.

## 6.3 **Further Contributions**

Future researchers can refer to this research and conduct further studies in the same area to validate that the results from this research are actually valid and can be generalizable across a wider geography, wider population and in a number of industries. There has been extremely limited quantitative research on privacy, security and blockchain and most of the previous studies are based on analysing literature reviews of past research. Thus, there is enough scope for future researchers to propose new frameworks and new solutions to privacy and security in the Fintech industry.

The research work has been conducted only in the fintech and IT industry and the participants are employees only from fintech and IT organizations. The views obtained from these participants might not be generalizable to people from all industries. Future researchers can take a wider population and sample and replicate the research or carry out research in new ways.

This research could also be referred to by the research workers and further improve and develop an enhanced model for better privacy and security of financial information.

The survey conducted was restricted to Kathmandu Valley only which provides a biased result and is difficult to generalize in the whole context of Nepal as the rural parts of Nepal are still not well-equipped with internet facilities and do not know about the possibilities of blockchain in Fintech. The researchers in days to come can conduct surveys in different parts of Nepal and also outside the country for generalized research outcomes.

The survey had a limited response option, and respondents were constrained by the provided options for each question, which may not fully capture their perspectives or experiences. Future researchers can try out new questionnaires and new methodologies in order to bring the best and most accurate responses from Fintech users.

## **6.4 Summary**

The above sections conclude the dissertation work along with the possible recommendations for the engaged stakeholders to address the blockchain implementation in the fintech industry of Nepal. All of the related stakeholders could work collectively towards improving the fintech industry in Nepal with positive direction from the blockchain implementation. The section also provides areas for future work, which could not be covered in the dissertation work with its limitations.

**References**

1. Aldboush, H. H., & Ferdous, M. A. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. 11(3), 90. https://doi.org/10.3390/ijfs11030090
2. Aryal, M. (2020). The Story Of Vianet’s Data Breach | The Full Case Story. ICT Frame. https://ictframe.com/the-story-of-vianets-data-breach-the-full-case-story/
3. Aslan, O., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. MDPI, 12(6). https://doi.org/10.3390/electronics12061333
4. Baliker, C., Baza, M., Alourani, A., Alshehri, A., & Alshahrani, H. (2023). On the Applications of Blockchain in FinTech: Advancements and Opportunities. https://doi.org/10.1109/TEM.2022.3231057
5. Bellaj, B., Ouaddah, A., & Bertin, E. (2022). SOK: A Comprehensive Survey on Distributed Ledger Technologies. IEEE. https://doi.org/10.1109/ICBC54727.2022.9805533
6. cybersource, MRC, & Verifi. (2022). Global fraud and payments report 2022. Global fraud and payments report 2022
7. Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2021). Promise not fulfilled: FinTech, data privacy, and the GDPR. 30(1). https://doi.org/10.1007/s12525-023-00622-x
8. Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2023). Promise not fulfilled: FinTech, data privacy, and the GDPR. SpringerLink. https://doi.org/10.1007/s12525-023-00622-x
9. Durai, T., & Stella, G. (2019). DIGITAL FINANCE AND ITS IMPACT ON FINANCIAL INCLUSION. 6(1). https://www.jetir.org/papers/JETIRV006018.pdf
10. Faccia, A., Moşteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020). Electronic Money Laundering, The Dark Side of Fintech: An Overview of the Most Recent Cases. 29–34. https://doi.org/10.1145/3430279.3430284
11. FIU. (2022). FIU-Nepal Newsletter.
12. FIU-NEPAL: ANNUAL REPORT 2021/22. (2022). https://www.nrb.org.np/contents/uploads/2022/12/FIU-Nepal-Annual-Report-2021.22.pdf
13. Gad, A. G., Mosa, T. D., Abualigah, L., & Abohany, A. A. (2022). Emerging Trends in Blockchain Technology and Applications: A Review and Outlook. ScienceDirect, 34(9). https://doi.org/10.1016/j.jksuci.2022.03.007
14. Gordon, B. G. (2020). Vulnerability in Research: Basic Ethical Concepts and General Approach to Review. 20(1), 34–38. https://doi.org/10.31486/toj.19.0079
15. Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. ScienceDirect, 3(2). https://doi.org/10.1016/j.bcra.2022.100067
16. Hassan, A., Ali, Md. I., Ahammed, R., & Monirujjaman, M. (2021). SecuredInsuranceFrameworkUsingBlockchainand SmartContract. https://doi.org/10.1155/2021/6787406
17. Hegde, S., Aishwarya, G., Hugar, A., & Suneeta, V. B. (2023). Bank Management System Using Blockchain Technology. Springer. https://doi.org/10.1007/978-981-19-0098-3\_22
18. Islam, S., Islam, M. J., Hossain, M., Noor, S., & Kwak, K.-S. (2023). A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues. IEEE, 11. https://doi.org/10.1109/ACCESS.2023.3267047
19. Jakhiya, M., Bishnoi, M., & Purohit, H. (2020). Emergence and Growth of Mobile Money in Modern India: A Study on the Effect of Mobile Money. IEEE. https://doi.org/10.1109/ASET48392.2020.9118375
20. Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. 2(3). https://doi.org/10.1016/j.tbench.2022.100073
21. Kim, S., Kim, J., & Kim, D. (2020). Implementation of a Blood Cold Chain System Using Blockchain Technology. 10(9). https://doi.org/10.3390/app10093330
22. Kost, E. (2023). 10 Biggest Data Breaches in Finance [Updated August 2022]. https://www.upguard.com/blog/biggest-data-breaches-financial-services
23. Mamun, A., Kaiser, M. S., & Yousuf, M. (2020). Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology. https://doi.org/10.1109/TENSYMP50017.2020.9230987
24. Marqués, J. M., Ávila, F., Rodríguez-Martínez, A., Morales-Reséndiz, R., Marcos, A., & Godoy, T. (2021). Policy report on FinTech data gaps. 2(3). https://doi.org/10.1016/j.latcb.2021.100037
25. Muntaha, S. T., Lazaridis, P. I., & Hafeez, M. (2023). Blockchain for Dynamic Spectrum Access and Network Slicing: A Review. IEEE. https://doi.org/10.1109/ACCESS.2023.3243985
26. Nadeau, J. (2021). Banking and Finance Data Breaches: Costs, Risks and More To Know. https://securityintelligence.com/articles/banking-finance-data-breach-costs-risks/
27. Ndung’u, R. N. (2022). Blockchain as a Solution of Information Security and Data Privacy Issues: Review. International Journal of Computer Applications Technology, 11(8), 337–340. https://doi.org/10.7753/IJCATR1108.1007
28. Nelaturu, K., Du, H., & Le, D.-P. (2022). A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions. MDPI. https://doi.org/10.3390/cryptography6020018
29. Ozili, P. K. (2023). Digital finance research and developments around the World: A literature review. 8(1), 31–35.
30. Patel, M. (2017). Real Risk for fintech: The Growth in the Cost of Cyber Attacks. https://thefintechtimes.com/fintech-insurance-elmore-growth-cost-cyber-attacks/
31. Peres, R., Schreier, M., Schweidel, D., & Sorescu, A. (2023). Blockchain meets marketing: Opportunities, threats, and avenues for future research. ScienceDirect, 40(1). https://doi.org/10.1016/j.ijresmar.2022.08.001
32. Qian, K., Liu, Y., He, X., & Du, M. (n.d.). HPCchain: A Consortium Blockchain System based on CPU-FPGA Hybrid PUF for Industrial Internet of Things. IEEE. https://doi.org/10.1109/TII.2023.3244339
33. Rehman, F. U., Attaullah, H. M., Ahmed, F., & Ali, S. (2023). Data Defense: Examining Fintech’s Security and Privacy Strategies. 32(1). https://doi.org/10.3390/engproc2023032003
34. Renduchintala, T., Alfauri, H., Yang, Z., Pietro, R. D., & Jain, R. (2022). A Survey of Blockchain Applications in the FinTech Sector. MDPI, 8(4). https://doi.org/10.3390/joitmc8040185
35. Saleem, H., & Naveed, M. (2020a). SoK: Anatomy of Data Breaches. 4, 153–174. https://doi.org/10.2478/popets-2020-0067
36. Saleem, H., & Naveed, M. (2020b). SoK:AnatomyofDataBreaches. Sciendo. https://doi.org/10.2478/popets-2020-0067
37. Sarfaraz, A., Chakrabortty, R. k, & Essam, D. L. (2023). AccessChain: An access control framework to protect data access in blockchain enabled supply chain. 148. https://doi.org/10.1016/j.future.2023.06.009
38. Seldal, M. M. N., & Nyhus, E. K. (2022). Financial Vulnerability, Financial Literacy, and the Use of Digital Payment Technologies. 45(2), 281–306. https://doi.org/10.1007/s10603-022-09512-9
39. Shrimali, B., & Patel, H. B. (2022). Blockchain state-of-the-art: Architecture, use cases, consensus, challenges and opportunities. ScienceDirect, 34(9). https://doi.org/10.1016/j.jksuci.2021.08.005
40. Singh, H. (2023). Chapter 1—Decentralized web, distributed ledgers, and build-up to blockchain. ScienceDirect. https://doi.org/10.1016/B978-0-323-96146-2.00004-8
41. Song, H., & Chen, Y. (2021). Digital Financial Transaction Security Based on Blockchain Technology. https://doi.org/10.1088/1742-6596/1744/3/032029
42. Thakur, N., & Sharma, V. (2023a). Enhancing Fintech Security—A Comparative Analysis of Advanced Security Algorithms. https://doi.org/10.1109/ICECAA58104.2023.10212129
43. Thakur, N., & Sharma, V. (2023b). Enhancing Fintech Security—A Comparative Analysis of Advanced Security Algorithms. IEEE. https://doi.org/10.1109/ICECAA58104.2023.10212129
44. Top Takeaways from IBM’s 2022 Cost of a Data Breach Report. (2022). Bluefin. https://www.bluefin.com/bluefin-news/top-takeaways-ibm-2022-cost-data-breach-report/
45. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., & Prakash, E. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. 3(127). https://link.springer.com/article/10.1007/s42979-022-01020-4
46. Yadav, A. S., Singh, N., & Kushwaha, D. S. (2023). Evolution of Blockchain and consensus mechanisms & its real-world applications. SpringerLink. https://doi.org/10.1007/s11042-023-14624-6
47. Zhao, C., & Meng, X. (2019). Research on Innovation and Development of Blockchain Technology in Financial Field. 315. https://www.atlantis-press.com/article/125907072.pdf

# APPENDICES

## APPENDIX A

**Survey Questionaire**

**Greetings!**

I kindly request your assistance in completing the enclosed questionnaire, taking just a few minutes of your valuable time. The purpose of this questionnaire is to investigate the implementation of blockchain technology in the fintech sector of Nepal. Your input is vital in enabling me to analyze the topic effectively. I highly value your personal viewpoints on the subject, and it is important to note that there are no correct or incorrect answers. Please rest assured that all your responses will remain completely confidential, accessible solely to the research team. The provided information will be strictly utilized for academic purposes only. Thank you sincerely for your cooperation and for contributing to the advancement of this research project. Your support is greatly appreciated.

Age

* 15-24
* 25-34
* 35-44
* 45-54
* 55 and above

Gender

* Male
* Female
* Others

Occupational Background

* Technical(IT/Computer Science and other related background)
* Non-technical

Occupation

* Student
* Employed(Part time/Full time)
* Self Employed
* Unemployed
* Others

Monthly Income(In NRs)

* less than 15000
* Between 15000 and 50,000
* 50,001 to 200,000
* Above 200000

Which of the following fintech services have you used before?

* Digital Wallet
* Digital banking
* Finance & Lending
* Insurance
* Others
* None

Have you filled up the Know Your Customer Form (KYC) in order to use Fintech services?

* Yes
* No

|  |
| --- |
| I often use Digital Banking, wallet or any other fintech services for my transactions? |
| I am hesitant to share my personal information with Fintech service providers. |
| The personal information that I provide to Fintech organization is important to me. |
| I feel insecure when I provide my personal information to Fintech organizations. |
| I think that  someone else is accessing my personal and financial information besides the fintech. |
| I am concerned that my personal information might be stolen or intercepted. |
| The fintech service providers ask sensitive information to users |
| The fintech service provider does not disclose how they plan to use our personal information. |
| I feel that the current system in Fintech in Nepal is not mature enough to make the electronic identity records secure? |
| I do not feel secure to make high amount of transaction through Fintech. |
| I have often become the victim of digital fraud. |
| I doubt that Fintech services will become more secure in the future in Nepal.    I feel that the transactions that I perform through Fintech are not secure. |
| I feel that the Fintech industry in Nepal is immature and insecure compared to other developed countries in the world. |
| I feel that the information that I provide to Fintech organizations are prone to hacking. |
| I don't trust Fintech organizations because of lack of security while making transactions through Fintech. |
| Blockchain is an emerging concept in Nepal |
| I feel that use of blockchain in Fintech industry can make my personal information secure. |
| I feel that use of block chain in Fintech industry can help organizations win the trust of their customers by securing payment. |
| I feel that use of blockchain can help organizations prevent their system from being hacked. |
| I feel that Block chain can minimize latency in Fintech. |
| I feel that the blockchain can create higher scope in Fintech. |
| I feel that block chain is the ultimate solution to data privacy and security in Fintech. |
| I would use Fintech services more often if they can use Block chain system for data security and privacy. |
| I think use of Block chain is the future of Fintech industry's security and privacy. |

## APPENDIX B

Turnitin Report



