

University of Central Florida

STARS

Electronic Theses and Dissertations, 2020-

2020

Assessing the Potential of Implementing Blockchain in Supply Chains using Agent-Based Simulation and Deep Learning

Mohammad Obeidat
University of Central Florida



Part of the [Industrial Engineering Commons](#)

Find similar works at: <https://stars.library.ucf.edu/etd2020>

University of Central Florida Libraries <http://library.ucf.edu>

This Doctoral Dissertation (Open Access) is brought to you for free and open access by STARS. It has been accepted for inclusion in Electronic Theses and Dissertations, 2020- by an authorized administrator of STARS. For more information, please contact STARS@ucf.edu.

STARS Citation

Obeidat, Mohammad, "Assessing the Potential of Implementing Blockchain in Supply Chains using Agent-Based Simulation and Deep Learning" (2020). *Electronic Theses and Dissertations, 2020-*. 390.
<https://stars.library.ucf.edu/etd2020/390>

ASSESSING THE POTENTIAL OF IMPLEMENTING BLOCKCHAIN IN SUPPLY CHAINS
USING AGENT-BASED SIMULATION AND DEEP LEARNING

by

MOHAMMAD OBEIDAT

B.S. Mathematics Jordan University of Science and Technology, 2003

M.S. Business Administration Phoenix University 2013

M.S. Mathematics University of Central Florida, 2017

M.S. Industrial Engineering University of Central Florida, 2019

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Industrial Engineering & Management Systems
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Fall Term
2020

Major Professor:
Luis C. Rabelo

© 2020 Mohammad Obeidat

ABSTRACT

In this decade, with the rise of data science accompanying the growth of e-commerce, many technologies have been developed. An example of these technologies is Blockchain, which has appeared to overcome security problems potentially.

This research assesses Blockchain's implementation in supply chains through a methodology that uses deep learning and agent-based simulation. A case study was utilized to observe and validate research developments.

The unique method predicts intrusions by using deep learning, and agent-based modeling reproduces artificial but convincing agents (e.g., customers, companies, hackers, and cyber pirates) in a computer-generated market. Trust and other relationships are systematically captured to represent Blockchain additions. Once again, the agent-based simulation model's environment permits hypothetical interactions and emergent features by coordinating supply and demand for business-to-consumer e-commerce events. The case study based on a real environment shows that the proposed method can determine the feasibility of the business model and Blockchain implementation's potential contributions.

I dedicate this work to:

My great father, **Ziad**, for his support

My beloved mother, **Amal**, for her ongoing love, sacrifices, and support

My lovely wife, **Rasha**, for her love, patience, and ongoing support

My beautiful kids, **Jennah, Danya, Ziad**, and **Omar**, for the happiness that they bring to my life

All my brothers and sisters for their encouragements

ACKNOWLEDGMENTS

I thank Allah Almighty first and foremost for giving me the health, courage, and wisdom to fully resolve my Ph.D. journey.

Special thanks to Dr. Luis Rabelo for his vision, help, patience, and directions. His continuous reviews, suggestions, feedback, and comments were significant factors to complete this dissertation. Also, I am very thankful to my committee members, Dr. Gene Lee, Dr. Ahmad Elshennawy, and Dr. Ahmad Rahal for their support and instructions. I also would like to thank all faculty and staff members in the Department of Industrial Engineering and Management Systems at UCF.

TABLE OF CONTENTS

LIST OF FIGURES	xi
LIST OF TABLES	xv
LIST OF ACRONYMS/ABBREVIATIONS	xvi
CHAPTER 1. INTRODUCTION	1
1.1 Background	1
1.2 Problem Statement	5
1.3 Potential Solution	5
1.4 Research Objectives	6
1.5 Potential Contributions	7
1.6 Outline	7
CHAPTER 2. LITERATURE REVIEW	9
2.1 Complex Systems (Supply Chains)	10
2.2 Blockchain	13
2.2.1 Introduction to Blockchain	13
2.2.2 History of Blockchain	15
2.2.3 Advantages of Blockchain network	16
2.2.4 Types of Blockchains	18
2.2.5 Blockchain Structure	20
2.2.6 Trust effect model with Blockchain Technology	21
2.2.7 Blockchain Effect on Industry	22

2.2.8 Cryptography Algorithms	23
2.2.9 Cryptocurrency (Bitcoin).....	26
2.2.10 Smart Contracts.....	29
2.2.11 Ethereum	31
2.2.12 Honeypots in Ethereum.....	32
2.3 Decision Making.....	34
2.4 Artificial Intelligence	36
2.4.1 Introduction.....	36
2.4.2 Artificial Neural Networks	37
2.4.3 Back Propagation.....	38
2.4.3 Deep Learning.....	39
2.4.3.1 Deep Neural Network	40
2.4.3.2 Recurrent Neural Network (RNNs)	48
2.4.3.3 Deep Belief Networks (DBNs).....	49
2.4.3.4 Convolutional Neural Networks (CNNs).....	51
2.4.3.5 Deep Boltzmann Machines (DBMs).....	51
2.4.3.6 Restricted Boltzmann Machines (RBMs).....	52
2.4.3.7 Generative Adversarial Nets (GANs).....	53
2.5 Simulation and Modeling.....	54
2.6 Recent Research.....	57
2.7 Gap Analysis.....	63
CHAPTER 3. RESEARCH METHODOLOGY	66

3.1 Introduction.....	66
3.2 Research Methodology	66
3.3 Research Idea	68
3.4 Literature Review.....	68
3.5 Research Gap	69
3.6 Methodology Development	69
3.7 Case Study	70
3.8 System Simulation	70
3.9 Validation and Analysis.....	71
3.10 Conclusions and Future Work	73
CHAPTER 4. DEVELOPMENT OF METHODOLOGY	74
4.1 Introduction.....	74
4.2 Proposed Methodology	74
4.2.1 Supply Chains	74
4.2.1.1 Stakeholder Identification.....	75
4.2.1.2 System Characterization	76
4.2.1.3 Supply chains challenges	77
4.2.2 Blockchain	86
4.2.3 Simulation.....	87
4.2.3.1 Justification of using Agent-based simulation.....	87
4.2.3.2 Agent-based Simulation.....	94
4.2.4 Artificial Intelligence	97

4.2.4.1 Justification for using Deep Learning.....	97
4.2.4.2 Deep Learning.....	102
4.3 Conclusion	104
CHAPTER 5. CASE STUDY.....	106
5.1 Introduction.....	106
5.2 Peer-to-Peer Economy	107
5.3 Peer-to-Peer Lending	109
5.4 Lending Club	109
5.4.1 Borrowers and Lenders Activities	110
5.4.2 Lending Club Challenges.....	115
CHAPTER 6. IMPLEMENTATION, VALIDATION, AND RESULTS.....	117
6.1 Introduction.....	117
6.2 Initial Model.....	119
6.3 Addition of a Deep Learning IT Security System	130
6.3.1 IT Environment Development of Lending Club.....	130
6.3.2 KNIME	134
6.3.3 Agent-Based Simulation	139
6.4 Addition of Blockchain.....	141
6.5 Agent-Based Model Results	142
6.6 Blockchain Breaches and Analysis.....	148
6.7 Conclusion	161
CHAPTER 7. CONCLUSIONS AND RECOMMENDATIONS	163

7.1 Conclusions.....	163
7.2 Research Limitations	170
7.3 Future Research	170
7.4 Research Contribution	171
LIST OF REFERENCES	172

LIST OF FIGURES

Figure 1: Higher-order that capture path in complex systems.....	2
Figure 2: Cause and Effect Analysis of the Current Supply Chain Management	3
Figure 3: Implementation of DL and ABS to facilitate blockchain for Supply chain	6
Figure 4: Traditional transfer of funds process.....	18
Figure 5: Transfer of funds process after implementation of Blockchain	18
Figure 6: Three types of Blockchain.....	19
Figure 7: Representation / Structure of a Blockchain.....	21
Figure 8: Path of a Hash Value	24
Figure 9: GP-Hash Ad-hoc function comparison	25
Figure 10: Phases of a Honeypot utilization.....	33
Figure 11: Honey Badger to Capture Honeypots in Ethereum.....	34
Figure 12: Artificial intelligence and its subsets.....	37
Figure 13: Simple Neural Networks versus Deep Neural Networks (DNN).....	40
Figure 14: Development of Data Representation and Neural Networks	42
Figure 15: DNN model to test Financial mining approach.....	48
Figure 16: Recurrent Neural Networks (RNNs).....	49
Figure 17: Structure of a Deep Belief Network (DBN).....	50
Figure 18: Structure of a Deep Boltzmann Machine (DBM)	52
Figure 19: Generative Adversarial Network (GAN)	53
Figure 20: Discrete System (Left) & Continuous System (Right).....	56

Figure 21: Traditional Generic Supply Chain.....	61
Figure 22: Utilization of Smart Contracts in an Open Source Supply Chain	62
Figure 23: Relationship map of Literature Review.....	65
Figure 24: High-Level Research Methodology	67
Figure 25: A model validation methodology and simulation process	72
Figure 26: Challenges in the Supply Chains.....	77
Figure 27: Network-Based Intrusion Detection and Prevention System	79
Figure 28: Implementing Transparency and Trust in the Supply Chains	86
Figure 29: Deploying the smart contracts to the blockchain	87
Figure 30: Complexity of implementing blockchain in a generic supply chain system.....	89
Figure 31: Process of creating a block on the blockchain	91
Figure 32: Causal Loop / Relationships of an Autonomous Operation in Blockchain.....	93
Figure 33: Flow chart to conduct a simulation study.....	95
Figure 34: Structure of Agents characteristics in an agent-based simulation.....	97
Figure 35: Vulnerability points and security attack points (adapted from Lee,2019)	99
Figure 36: Reputation Management Model	101
Figure 37: Deep Neural Network Architecture.....	103
Figure 38: System Methodology.....	105
Figure 39: Peer to Peer Platforms across different Industries.....	107
Figure 40: Lending Club Loan Issuance Mechanism	113
Figure 41: Flow Chart representing the behaviors of Borrower activities.....	114
Figure 42: Flow Chart representing the behaviors of Investor activities.....	114

Figure 43: Initial ABM Environment and Agent Interactions	119
Figure 44: Borrower and Lender's State-Charts	120
Figure 45: Lending Club Trust's State-Chart	121
Figure 46: Loan Amount Custom Distribution.....	122
Figure 47: Borrower Grade Custom Distribution	122
Figure 48: Term Distribution by Grade	123
Figure 49: Interest Rate Distribution for Grade A	123
Figure 50: Interest Rate Distribution for Grade B	124
Figure 51: Interest Rate Distribution for Grade C	124
Figure 52: Interest Rate Distribution for Grade D	124
Figure 53: Interest Rate Distribution for Grade E	125
Figure 54: Interest Rate Distribution for Grade F.....	125
Figure 55: Interest Rate Distribution for Grade G.....	125
Figure 56: Overview of the Lending Club environment.....	131
Figure 57: Current Model and Proposed Mode	133
Figure 58: Deep Learning Network	134
Figure 59: Loss function values after three epochs	135
Figure 60: The Accuracy Results.....	138
Figure 61: KNIME Model	138
Figure 62: Upgraded ABM Environment and Agent Interactions.....	139
Figure 63: IT Security System' State-Chart.....	140
Figure 64: Numerical Results Example	142

Figure 65: Graphical Results Example	143
Figure 66: Sample ongoing Parameter Variation run	144
Figure 67: Number of funded applications	145
Figure 68: Number of Attackers	146
Figure 69: Blocked Non-Attackers	146
Figure 70: Repeat Lenders	147
Figure 71: Trust change over time under different scenarios	147
Figure 72: Application Process Duration.....	148
Figure 73: The Blockchain system security domains (adapted from Lee,2019)	151
Figure 74: Breakdown of the 78 recent blockchain cyberattacks	159
Figure 75: Domain's Loss by Year	160
Figure 76: Total Loss by Year	161
Figure 77: Concept map reflecting information about agent-based simulation.....	166
Figure 78: Three scenarios conclusion	169

LIST OF TABLES

Table 1: Blockchain Networks.....	20
Table 2: Results of the R/S analysis in various cryptocurrency markets.....	29
Table 3: Disadvantages in using these types of detection approaches in IDS	82
Table 4: Disadvantages of the types of IPS	84
Table 5: State Types.....	118
Table 6: Transition Types	118
Table 7: Originating Fee by Grade	126
Table 8: Repeat Lender Probability	128
Table 9: findInvestment function overview – Willingness to fund grades based on Trust Level and Lenders’ Risk Aversion.....	129
Table 10: Attribute.....	132
Table 11: Classes	133
Table 12: Output Example of the DL4J Feedforward Learner node	137
Table 13: Lending Club Models Metrics	144

LIST OF ACRONYMS/ABBREVIATIONS

ABM	Agent- Based Modeling
ABMS	Agent- Based Modeling and Simulation
ANN	Artificial Neural Network
C	Ciphertext
CI	Computational Intelligence
CNN	Convolutional Neural Networks
CRM	Customer Relationship Management
D	Decryption
DNN	Deep Neural Network
DLNN	Deep Learning Neural Networks
E	Encryption
E-Commerce	Electronic Commerce
EVM	Ethereum Virtual Machine
FDIA	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
GAN	Generative Adversarial Nets
HHM	Hidden Markov Models
IPsec	Internet Protocol Security
IoT	Internet of things

K	Key
KNIME	Konstanz Information Miner
P	Plaintext
P2P	Peer-to-Peer
PESTLE	Political, Economic, Social, Technological, Legal, Environmental
PD	Probability of Default
PGP	Pretty Good Privacy
R/S	Rescaled Range
RF	Random Forest
RNN	Recurrent Neural Networks
ROI	Return on Investment
SHA-2	Secure Hash Algorithms
S/MIME	Secure/Multipurpose Internet Mail
SPN	Sum-Product networks
SSH	Secure Shell
SWOT	Strengths-Weaknesses-Opportunities-Threats
TLS	Transport Layer Security
WAROIC	Weighted Average Return on Invested Capital

CHAPTER 1. INTRODUCTION

1.1 Background

The field of complex systems spans throughout all of the traditional science, engineering, and management disciplines. Complex systems carry various independent but interconnected and interlinked components. According to Weisbuch (2018), the behavior of a complex system is unpredictable. Complex systems are critical because of everything from politics, organizations, technology, weather, economic markets, and the environment functions within a complex system. Complex systems approach sociology, economics, computer science, data theory, and non-linear dynamics with a research-based approach to problem-solving. It is essential to learn how complex system components are interrelated and their effect on other components (Weisbuch, 2018).

The study of the interaction between the components in a complex system requires a network of scientific methods. A complex system's complexity features are the actions resulting from the complex system. They cannot be easily modeled. Those models representing a complex system will consider a complex system's properties as noise, making the model not accurate or suitable (Arthur, 2018). A complex system's interacting components form a network. It is far too complicated to understand the complexity of interactions between components by using a simple standard network in a complex system. It does not regard how links contribute to paths. Instead, a higher-order model of paths or a path-centric view of data must be used (Davis, 2018).

The ideal higher-order model that should be used in understanding the paths and interactions is the Markov Chain Model. The Markov Chain Model is a type of Markov Process that uses a memory type of network to showcase the nodes representing states in a continuous or countable state space and links that have been coded to display transitions between the states. The

Markov Chain Model is most commonly used as a statistical model (Davis, 2018). Figure 1 below shows the models of the higher-order that capture path topology in complex systems.

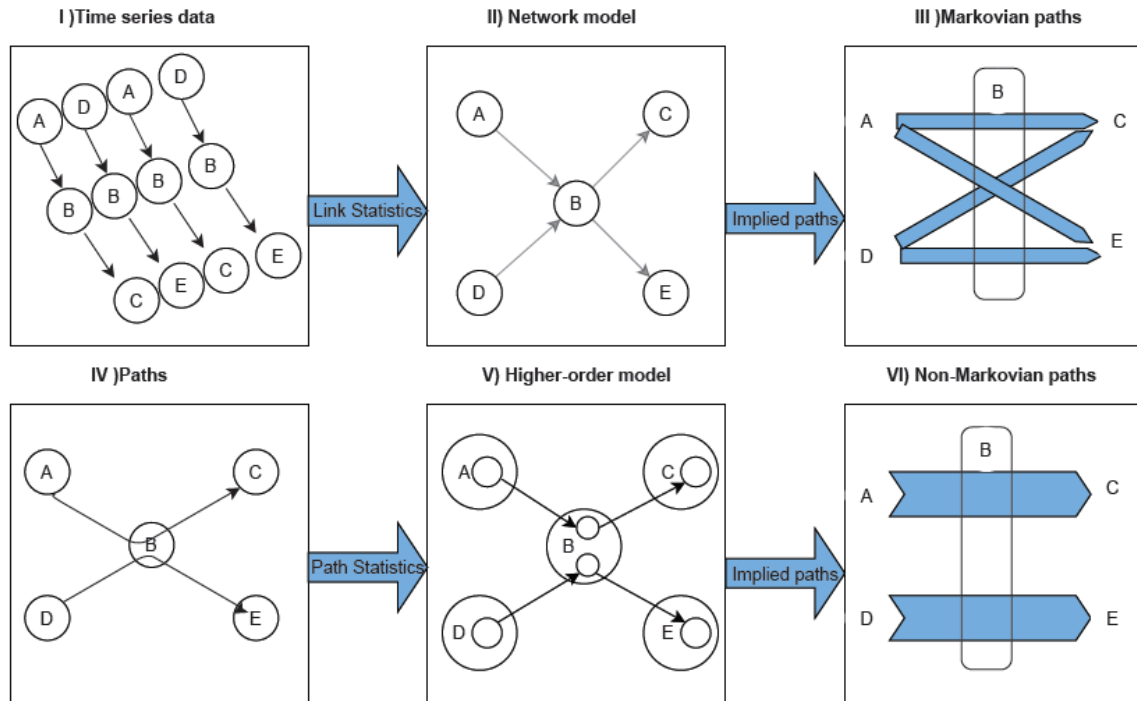


Figure 1: Higher-order that capture path in complex systems

One example of a complex system is a supply chain. A supply chain is a system of components, entities, functions, information, and resources engaged in moving a good or service from supplier to customer. According to Law (2017), a supply chain is a system process that incorporates all the network of activities and resources that links manufacturer to suppliers and suppliers to consumers. The principles of the complexity of a supply chain include procurement of raw materials, design, fabrication, technology, network logistics, delivery, and consumer sales to make a supply chain a complex system (Law, 2017). Due to its complexity of the supply chain components, which contain many characteristics, it makes a supply chain system a complex

system. Supply chain systems and value chain systems are complex systems due to their nature. Despite proposed research work that attempts to utilize systems to solve the challenges of integration and collaboration roles that add value, there are still problems with consistency, transparency, and security.

Blockchain is a new technology that appeals to solve the issues observed in the present supply chain system. Blockchains are ledgers that can be autonomously managed to exchange data between parties. Blockchain is an attached block that records transactional data, the previous block's encrypted hash, and the transaction's timestamp. According to Bryk (2017), Blockchain technology can offer many potential benefits and expectations in the supply chain system. Some of these benefits include decentralization, integrity, transparency, immutability, and confidentiality. The Blockchain public ledger will also provide immediate updates as information changes in the system (Bryk, 2017).

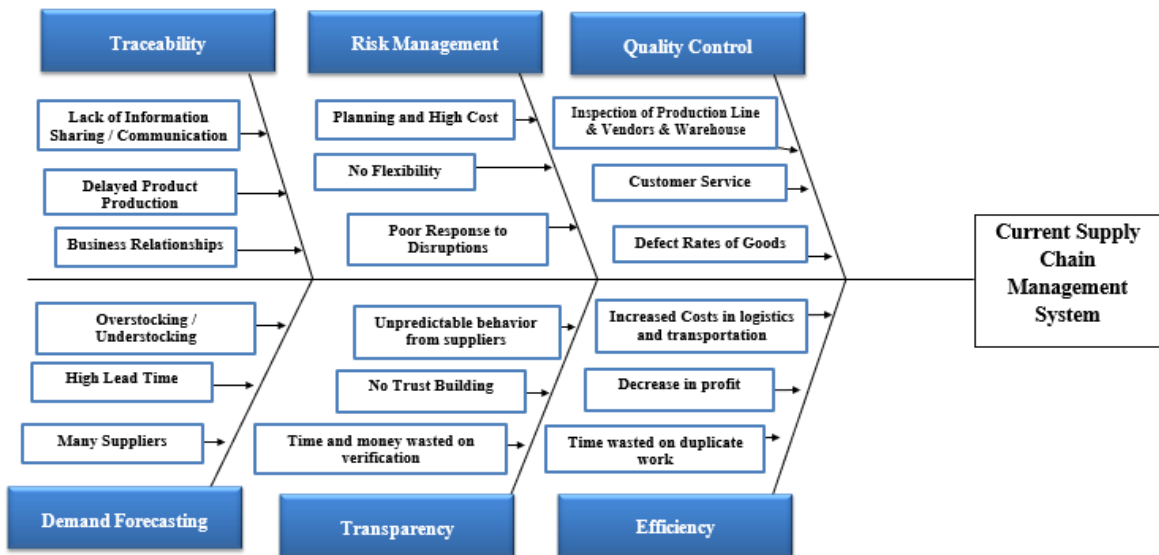


Figure 2: Cause and Effect Analysis of the Current Supply Chain Management

Figure 2 illustrates the many different causes of the problems in the traditional supply chain. The sources of conflict within the current supply chain are essential to get beneficial outcomes (Giannakis et al., 2016).

Initially founded by Nick Szabo, computer scientist, and scholar, Smart Contracts are associated with the self-executing and self-enforcing transaction and computer protocol. Smart Contracts are trackable, making it ideal for merging within Blockchain Technology (Cong et al., 2019). The computation of Smart contracts takes place in the Blockchain distributed ledger, making it a more secure and trusting way to conduct transactions in the Peer-to-Peer network. Smart Contracts and Blockchain technology are at the forefront of the financial services industry's technological development and can be utilized by virtually any industry. They aim to create a system that meets standard terms and decreases the necessity for third parties in transaction processing.

Smart contracts will solve many complex systems, such as the current traditional financial transaction market (P2P). When it is introduced in the complex system, it will create many benefits for the parties involved. Smart Contracts will create a basis for trust. The encryption capability of Smart Contracts will enable transaction data to be embedded and encrypted on a shared ledger to carry out any transaction securely. Smart Contracts on the Blockchain technology are guarded with hard to tamper with cryptography that ensures the Smart Contracts are safe and secure among the collection, storage of data, and transaction process. Also, the Smart Contract and Blockchain technology will eliminate the errors that can happen with human interference of traditional handling of physical Contracts (Serrano-Cinca, 2016).

Due to high-security issues of money laundering, credit fraud, security, and even the public's safety, the above problem can be eliminated by introducing and using the Blockchain

technology of Smart Contracts. It is essential to understand that Blockchain is a decentralized ledger, unlike the current traditional way of conducting transactions with a third party as a centralized transaction. Blockchain is introduced to become a new way of conducting business, specifically with complex system processes. It becomes transparent to both parties and creates trust by using cryptography and hashing algorithms to store data. Blockchain is also tamper-proof and has an immutability factor that creates trust between parties. This trust is because no one has the authority to change or alter any information within the data stored on the Blockchain, making it very secure and a safe way to be embedded in the complex system, for example, P2P (Gonzalez, 2018).

1.2 Problem Statement

Supply chains are complex systems because of the amount of suppliers, amount of consumers, amount of interactions, changing rules, and different decisions and actions. Other factors include uncertainty, transparency, traceability, information, currency exchanges, risk management, and reputation. Blockchain is an evolving technology that has shown success in securing financial transactions among trading partners. When applied to a supply chain, blockchain technology can enhance transparency and traceability in data, monetary exchanges, and building trust and reputation between various entities; however, there is no method to assess blockchain's implementation to enhance a supply chain.

1.3 Potential Solution

This study proposes to use Agent-Based Simulation (ABS) and Deep Learning to assess the implementation of blockchain in a supply chain. The agents are composed of individuals or collective entities and provide insight into how each entity affects the entire system. The ABS approach allows for observing each supply chain entity's behavior over time and the entire supply

chain. On the other hand, Deep Learning can identify trends, patterns, and behaviors of stakeholders and hackers within a supply chain network. These modeling will evaluate a supply chain system performance with and without blockchains concerning transparency and traceability in data. It will also allow for monetary exchanges, trust, and reputation between various entities. Figure 3 illustrates the current supply chain and the utilization of ABS and Deep Learning to assess Blockchain technology's future supply chain.

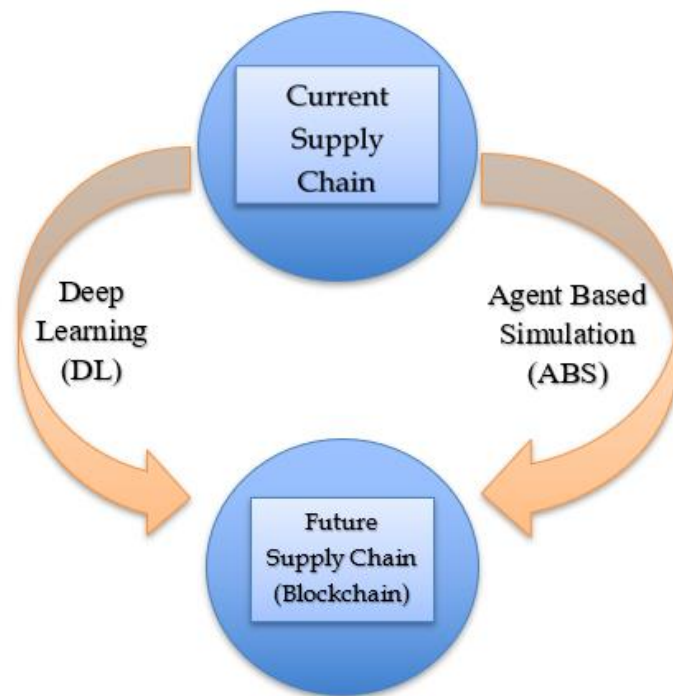


Figure 3: Implementation of DL and ABS to facilitate blockchain for Supply chain

1.4 Research Objectives

The key research objectives are:

1. Recognize the options to make the current process more secure and create trust between parties by utilizing Smart Contract technology.

2. Compare the proposed process with the current traditional process from the Industrial Engineering perspective, such as Return on Investment (ROI), Process Time, Security, Trust, etc.
3. Develop a methodology to analyze the feasibility of using Blockchain in supply chains.

1.5 Potential Contributions

Many real-world problems will benefit from merging the proposed technologies and implementing them to supply chain management and any other complex system. This research will contribute to many fields, precisely the field of Engineering and Computer Science. First, the research will help organization decision-makers rely on the Blockchain and Smart Contract to improve their supply chain system process. Secondly, stakeholders will benefit since Blockchain technology offers trust and security in the lending and financial field's transaction process.

1.6 Outline

This dissertation proceeds as follows:

- **CHAPTER 1** provides an outline of the research study.
- **CHAPTER 2** reviews relevant literature on five main areas and the research gap, as follows:
 1. Complex systems (Supply chains).
 2. Blockchain Technology
 3. Decision Making.
 4. Artificial Intelligence.
 5. Simulation and Modelling.

6. Research gap.

- **CHAPTER 3** describes the research methodology to address the research objectives.
- **CHAPTER 4** explores the development of the methodology.
- **CHAPTER 5** includes the details of the case study.
- **CHAPTER 6** is a presentation of the methodology's implementation using the case study and , Blockchains breaches, then validating the methodology's results.
- **CHAPTER 7** includes conclusions, limitations, and suggestions for future research.

CHAPTER 2. LITERATURE REVIEW

This chapter presents a review of research in the fields mentioned below as well as related literature and studies on five main categories, recent research, and gap analysis as follows:

- Complex Systems (Supply Chains): This part defines complex systems, provides its functions, behaviors, examples, and applications.
- Blockchain: This part covers History of the Blockchain, Disadvantages of the Blockchain Network, Types of Blockchain, The Blockchain Structure, Blockchain effect of Industry, the trust effect with the Blockchain technology, cryptography algorithms, Secure Hash2 Algorithms, Cryptocurrency Bitcoin, Smart Contracts, Ethereum, Honey Pots in Ethereum.
- Decision Making: This part covers the decision-making process, its three main properties, and the relation to simulation and modeling.
- Artificial intelligence: This part covers Artificial neural networks and Deep Learning with its algorithms.
- Simulation and Modeling: This part covers simulation research, presents its importance, and types of simulations
- Recent research: This part covers the latest studies that combined the previous categories that led to the research gap.
- Gap Analysis: This part identifies the gap based on the literature review.

2.1 Complex Systems (Supply Chains)

The supply chain is an interconnected system of entities, companies, services, processes, operations, and technologies engaged in the development and deployment of a good or service. The supply chain is an important function of so many industries and is important for the sustainability of organizations and customer loyalty (Swift et al. 2019). The supply chain is an essential complex system because it offers the availability of goods, inventory control, cost controls, and opportunity for market growth.

Although traditional supply chain processes and procedures are essential to the supply chain, they are no longer the only way a supply chain can efficiently function. Information technology is now essential to the performance of operations, social engineering, data sharing, optimization, and programming of the supply chain. According to Zhang (2019), Evolving dynamics and innovations in the supply chain must meet organizations' needs, which require technical training based on emerging procedures and processes of the supply chain (Zhang, 2019).

An interesting approach in a complex system is presented by Koczy et al. (2019). This paper suggests that three main elements make computational intelligence: population-based algorithms, artificial neural networks, and fuzzy systems. Complex systems have a place in the engineering industry as an asset to economic models, computer science, and social and agricultural engineering. This paper covers the real-life problem of “cat and mouse” using an automated algorithm. Using the Mamdani type fuzzy system application, the fuzzy system is represented by the computational intelligence or the “cat,” and the model's object is to catch the “mouse.” In this complex system, there are three goals: for the cat to capture an image of the mouse, the CI or the

cat must then calculate the mouse's future position, then CI or the cat searches the future position for the mouse. The results conclude that using mathematical algorithms and computational Intelligence with hybrid approaches. The prediction model calculates the smaller the to be searched, the faster the prediction model can output a precise result (on the mouse's location) in this case (Koczy et al., 2019).

Johnson (2006) presents the challenges faced in engineering complex systems labeled as “emergent properties.” The issues stemming from the emergent properties explain how unexpected behavior comes from the interaction between the components and subsystems of a complex system. The challenges arise from stakeholders, the public, clients, construction crews, managers, agencies, and the government all have requirements for complex systems design, making the complexity of any situation difficult. One approach was to use the chaos theory of Weak and Strong Emergence, which is based on simulation and modeling developed by Mark Bedau (1977), which explains the modification that weak rise has and strong rise that causes a downwards interconnection (Johnson, 2006).

In the engineering aspect, Gott (2005) explains how important it is to understand the resulting design for engineers and must bear in mind to keep time for marketing and profit, which is a significant challenge embedded in the engineering industry (Gott, 2005). The dynamics and topology of complex systems are the governing factors in a complex system. Despite the advances I the technological networks in social and biological advances, there are still limitations to how much we can manipulate in predicting behaviors without using microscopic models to determine a system dynamically. A study presented by Barzel et al. (2015) analyzes the relationships and interactions that system components have with each other, which can predict the system's behavior.

It was found that it was a reliable method to measure the model under all expectations (Barzel et al., 2015).

Poddey et al. (2019) analyze the complex systems' autonomous functions in self-driving cars. In this case, the problem was to study the design and complex system for complete validation or “no risk” in the operation of self-driving automobiles. The experiment utilized algorithms for iterative advancement and validation to make the complex system less complex. In this study, it is concluded that additional quality control and integrating statistical and methodical aspects for society to fully trust and rely on autonomous vehicles and the complexity of its operations to be more widely used and accepted. This would require a demonstration of zero accident rates for the use of autonomous vehicles, which has not been reached yet (Poddey et al., 2019).

A case study presented by Farmer, J. D. Gallegati, M., Hommes, C. Kirman, A. Ormerod, P. Cincotti, S. & Helbing, D. (2012) titled “A complex systems approach to constructing better models for managing financial markets and the economy” proposes researching and applying new approaches in the finance and economic industry for modeling complex systems. This case presented an approach of using the old vision of how our economy is viewed as a complex non-linear system made up of people, cars, buildings, and states. A new analysis method was used, such as computational tools, new math concepts, models like network theories, and economic performance, and agent-based modeling to influence the economic growth and evolution using networks. The experiment was done by categorizing and aiming critical nodes within the complex system components, which allowed for effectiveness on the policy that influences the network. The proposed approach uses the FutureICT project as a platform. It develops the application for

the economical use of data mining, artificial intelligence, and computational data collection to create a larger information platform for our economy (Farmer et al., 2012).

A 2018 Cherry & Pidgeon case study called "Is the solution sharing? - Exploring the acceptance of the sharing economy by the public" examines the intention and motivation behind the shared economy industry and is testing the broader acceptance of the sharing economy. This case study also examines the population's wishes and fears about integrating the sharing economy and its position in a more viable and efficient future. Four driving strategies lead to the sharing economy: Business to Business (B2B), Profit versus Non-Profit, Online-based versus Offline-based, and Peer-to-Peer (P2P). The case study results concluded that there is a great interest in sharing the economy for the public, according to Cherry & Pidgeon, 2018. A complex system built for the economy will bring sustainability, fair business practices, social equality and promote an environment in which consumers are directly involved and communicate with providers of a complex system such as a P2P business. The promotion or growth of a sharing economy's environment will also strengthen local self-regulating societies (Cherry & Pidgeon, 2018).

2.2 Blockchain

2.2.1 Introduction to Blockchain

Blockchain is a potential solution platform that has proven to solve many security problems in technology. Blockchain technology is based on a system consisting of nodes that contain data and are distributed among many other nodes that make it extremely difficult to manipulate (Karam et al., 2018). If someone or a system wants to change the data in a node, thousands of nodes containing the same information would need to be updated or changed, making it detectable. The

data exposure in the nodes spread between them and recorded in thousands of other nodes enhances Blockchain's security feature (Wust et al., 2018).

In a high-security data storage need, Blockchain has revolutionized the financial world and the technology or computing community. J.P. Morgan's Treasury Services recently announced the Blockchain's use for its benefit and used in the banking industry. Since J.P. Morgan processes almost \$5 trillion in payments and transactions for its customers, the question arises of how secure its security features are. J.P. Morgan is committed to implementing Blockchain in its investment transactions, customer experience, Machine Learning, robotics, and helping its customers worldwide develop innovative products and solutions. Blockchain's purpose used by J.P. Morgan is aimed at reducing resistance in time with global payment processing time and improving security features for transactions such as money transfers, loan processing, reducing payment transfers time between customers, and international transactions (J.P. Morgan, 2017).

According to Khan et al., 2018, Blockchain has advantages, including the authenticity factor in Blockchain's security features and approval method. The cryptographic language allows any industry in its business processes to use Blockchain. Another advantage is that Blockchain allows easy data monitoring and transparency of data access and history for companies in different industries (Khan et al., 2018).

Blockchain's entire existence is to remove a third party or middle man from any transaction or data connection and decentralize data for additional security. The problem with the centralization of existing data or methods is that data can be altered, changed, and undetectable, which reduces confidence, authenticity, and security. Another problem with a centralized system

is that it requires high-powered and end-server-to-house data usually controlled by a third party (Ali et al., 2018). According to Huckle et al., 2016, there are still many problems with our current security that Blockchain does not use. Despite the security acknowledgment, the data currently stored is a significant setback and still has its limits, mainly because it lacks traceability, which means that any company or individual making changes to the data cannot be traced back to the user. The problem with a centralized infrastructure is the mismanagement of data. This data is at risk of being manipulated by a lack of traceability. This forces organization to blindly trust the cloud without knowing more information than a centralized system can offer. Blockchain has advantages to building systems with autonomy, immutability, traceability, security, and decentralization. These factors play a significant role in the advances of Blockchain. Data can be verified with integrity that it is not tampered with; not one user has access to all data but more universal access for many users across all data stored in the Blockchain capacity (Huckle et al., 2016).

2.2.2 History of Blockchain

Discussing Blockchain's history, it is crucial to understand where Blockchain originated from understanding the concept behind this technology. Stuart Haber and W. Scott Stornetta were among the leading people to introduce their idea on a cryptographically secured Blockchain in 1991. Blockchain was used in 1992 to collect several document data in one data block and improve efficiency. Blockchain's distributed concept was introduced in 2008 by a group called Satoshi Nakamoto (Dinh et al., 2018).

Abstractly, Blockchain is a decentralized distributed ledger that holds encrypted transactions across a network that provides a high-security level. Each Blockchain contains the data (information on the individual or transaction content), the hash (similar to a fingerprint), and the hash of the previous block, making it very difficult or virtually impossible for tampering happen since the block after will show the change. Any changes made to the block will make the “hash” change and record that change as well, and others will see that alterations to a block have been made (Stampernas, 2018).

According to Khoury et al., 2018, Blockchain transactions are available for public view making the block impossible to alter since any alteration will be exposed in the next block. The next block linked to the previous block will show any changes or alterations, making the Blockchain encryption censored and resistant to changes. The linking of two or more blocks is called the Blockchain. It is a very valuable component to have decentralization for that copyright protection can exist. Others can also think about a Blockchain as a protected database that also serves to have multiple handlers access the Blockchain concurrently. These same handlers or users can update each block with data in its database using cryptographic factors to validate the authenticity or credibility (Khoury et al.,2018).

2.2.3 Advantages of Blockchain network

Recent research has discovered the benefits or advantages of enterprise Blockchain versus traditional ledger technology. The Blockchain enterprise technology’s advantages are consistent, secure, and accurate, such as that found in cryptocurrency. Blockchain is also intelligent such as

that found in “Smart Contracts” which will be discussed later in this literature review (Cong et al., 2018).

According to Allayannis et al., 2017, the potential applications of Blockchain can be found in various processes within many different types of industries, such as supply chain management, medical recording in the healthcare industry, as well as passport and customs in our government (Allayannis et al., 2017). The level of potential services that Blockchain can offer to any industry is endless. For example, specifically to the financial industry, it can save and lower transaction costs for banks and customers, fewer errors made by human-made transactions, low cost in the administrative ledgers, and lower capital cost (Karam et al., 2018).

A research study in 2014 conducted by Allayannis, George (Yiorgos), Fernstrom, and Aaron in 2017 discusses Blockchain's future. Figure 5 shows the application of Blockchain. Blockchain technology eliminates the corresponding process and allowing the sender and receiver to process the transaction directly with the bank until the receiver receives the funds. Figure 4 below shows the traditional transfer of funds process versus the bottom Figure 5 illustrates the transfer of fund process after the enterprise Blockchain technology has been implemented (Allayannis et al., 2017)

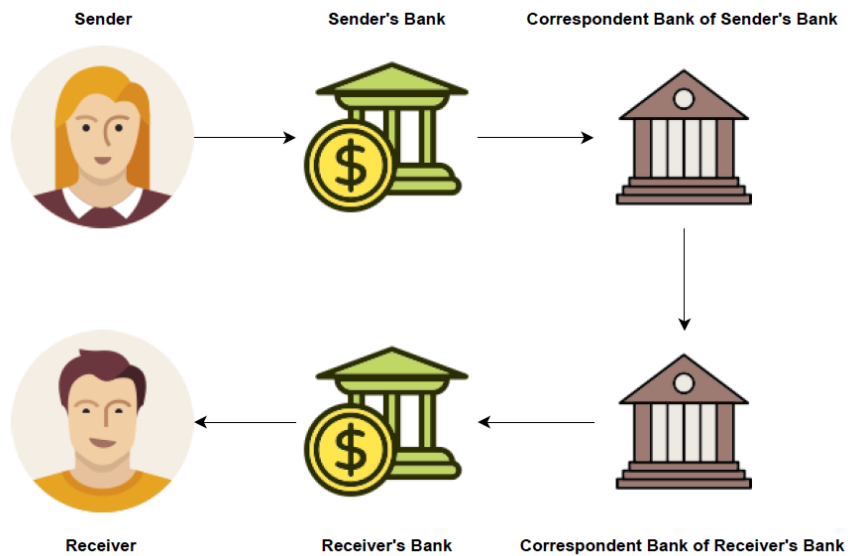


Figure 4: Traditional transfer of funds process

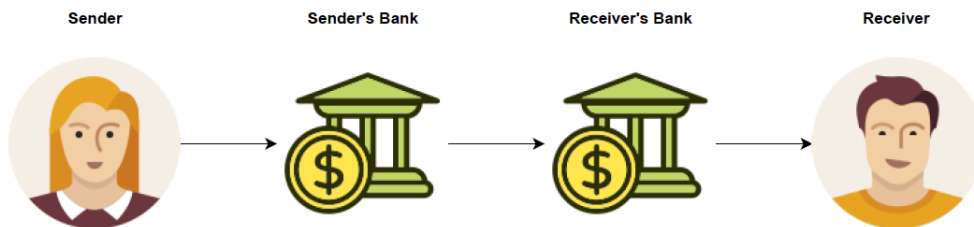


Figure 5: Transfer of funds process after implementation of Blockchain

2.2.4 Types of Blockchains

Buterin (2014) has characterized Blockchains into three categories: Public Blockchain, Private Blockchain, and Hybrid Blockchain. A public Blockchain is a Blockchain platform that anyone can access, including access to reading and writing. If the user has access to the network,

information can be accessed, and information can be added. Bitcoin, Monero, and Ethereum are an example of the public Blockchain system. In a public Blockchain system, the transactions conducted are transparent; however, the authors or users creating the transactions remain anonymous (Buterin, 2014).

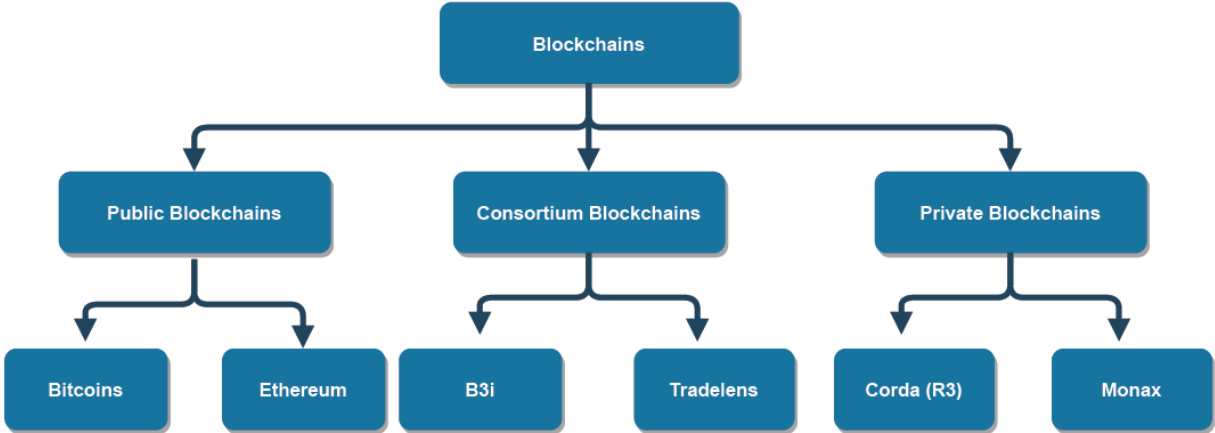


Figure 6: Three types of Blockchain

As shown above, in Figure 6, the three types of Blockchain are categorized. A private Blockchain is a Blockchain with some boundaries that cannot be overcome compared to a public Blockchain. In terms of modifying or reading the Blockchain, a private Blockchain has a stricter entry. In a compliance system with privacy and regulatory limits, private Blockchains are found more (Tinny, 2018).

A hybrid Blockchain system is a platform where Blockchain users are already predetermined or selected to access the block to read, write, and modify. The hybrid Blockchain is considered more flexible because it can be open to the public if necessary or locked or restricted

to some members. Table 1 below illustrates the different Blockchain networks' details concerning Access, Security, Transaction Speed, and Participants (Stampernas, 2018).

Table 1: Blockchain Networks

	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	<ul style="list-style-type: none"> • Anyone 	<ul style="list-style-type: none"> • Single Organization 	<ul style="list-style-type: none"> • Multiple selected organizations
Participants	<ul style="list-style-type: none"> • Permissionless • Anonymous 	<ul style="list-style-type: none"> • Permissioned • Known identities 	<ul style="list-style-type: none"> • Permissioned • Known identities
Security	<ul style="list-style-type: none"> • Consensus mechanism • Proof of Work/Proof of Stake 	<ul style="list-style-type: none"> • Pre-approved participates • Voting/multi-party Consensus 	<ul style="list-style-type: none"> • Pre-approved participates • Voting/multi-party Consensus
Transaction Speed	<ul style="list-style-type: none"> • Slow 	<ul style="list-style-type: none"> • Lighter and faster 	<ul style="list-style-type: none"> • Lighter and faster

2.2.5 Blockchain Structure

To fully understand Blockchain's structure, it is essential to research how a Blockchain is structured to understand its features. The Blockchain structure is based on complex transactions housed in each block. Every block is split into two sections, the title and the body of the block. Any transaction recorded is collected in the block or the cryptographic hash body. The header stores the previously created block's identifier or data, as illustrated in Figure 8 below. The transaction data that is stored within the body portion of the block is called the Merkle tree. This is where the name chain comes into reference. The chain refers to the linking of each block since

each block stores data from the previous block. This is the central concept of Blockchains security and tamper-proof feature (Koo et al., 2018).

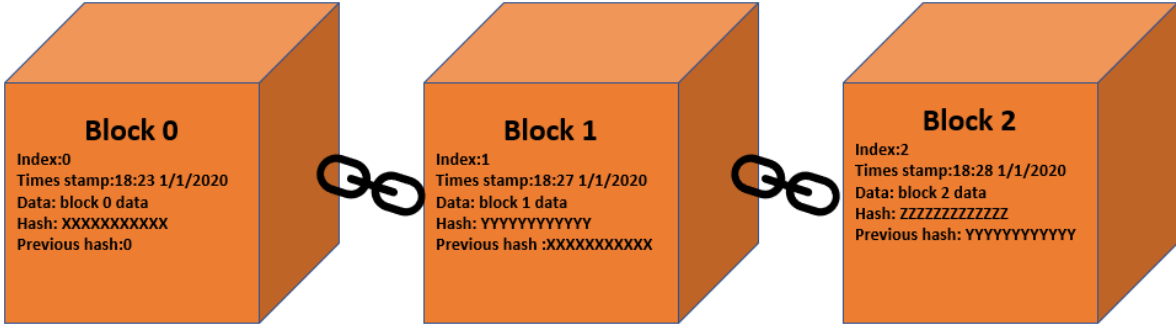


Figure 7: Representation / Structure of a Blockchain

Figure 7 above also illustrates two additional features of the Blockchain. The first is the immutability feature. Immutability allows for decentralization, making it tamper-proof and detectible to any changes. The second feature that Figure 8 above illustrates is the auditability of the Blockchain. The auditability is the timestamp of the recorded transaction or the “address” that verifies where the data came from, which can hold the data source responsible or accountable for the data input (Hartikka, 2017).

2.2.6 Trust effect model with Blockchain Technology

Trust effect concept in a complex system, according to Perren et al., 2018, “Trust Factor” in a complex system, and its effects have three factors. The first is integrity, then ability, then benevolence. Usually, organizations can create trust with their customers without previous

experience; however, the exchange is completed through binding contracts that are enforced. However, with the advancement in technology, even the binding contracts are eliminated. The platform has shifted towards conducting business based on technology and creating trust from the technology. The significance of the trust effect of social capital ascends in like-minded individuals' systems. It leads to mutual exchange, even without a solid presence of outdated institutions such as banks in the network, also defined as consociality. The theoretical implicating factor of trust in the Peer-to-Peer economy of Blockchain technology refers to three implications or dimensions: the ability to trust, the integrity available to trust, and the benevolence to trust transaction process in a Peer-to-Peer economy. The ability portion of the trust happens while the user initially has shopping intentions. The integrity and benevolence part happen as a behavior of the intention that affects the transaction (Perren et al., 2018).

Mehrwald et al. (2019) created a research model that looks at incorporating the trust-building concept in Blockchain using Qualitative and Quantitative research methods to identify which platform intermediation is needed when Blockchain is present. The results showed that the Blockchain-based systems provide ways to facilitate confidence in transaction-intensive contexts but could only work for now in the context of closed Peer-to-Peer platforms (Mehrwald et al., 2019).

2.2.7 Blockchain Effect on Industry

The latest research completed on Blockchain effect on the industry for debit and risk influences the digital and distributed ledgers in the Blockchain technology. The case study completed by Melanie Swan in 2019 argues that Crypto Tokens on Blockchain are digital assets

that can be executed instantly and pledged in new ways by the theory and idea of Crypto Tokens. The study reveals that Crypto Tokens might ultimately lead to a reform of debt problems in our society (Swan, 2019). Crypto Tokens are a new kind of currency that can be efficient in trading as well. It has a value and an intermediate of exchange and a unit of account that is required to be considered a monetary value and can be embedded on the Blockchain ledger (Conley, 2017). This new Crypto Tokens theory is a new way to facilitate financial interactions within an economic problem, such as deals with debt and risk specifically (Conley, 2017).

2.2.8 Cryptography Algorithms

Essentially, cryptography is a way of writing data or messages in a highly secure and secretive manner. Cryptography is considered an art form because it was used in history by the ancient Egyptians in 1900 B.C (Before Christ), like their hieroglyphic messages displayed by images. Taking this method of secret writing, we use cryptography in today's times to enhance the privacy and confidentiality of messages to only the intended receiver or accessor. It is also used for authentication purposes, integrity, key exchange, and non-repudiation, which is proof that the sender is a trusted sender (Sharma et al., 2016).

In cryptography, the start of this method contains using unencrypted data or can also be called plaintext. The plaintext is then coded into a ciphertext that is decoded back into a more available plaintext. The process for this formula usually looks like where: $C = E_k(P)$ and $P = D_k(C)$, where **P** = plaintext, **C** = ciphertext, **E** = the encryption method, **D** = the decryption method, and **K** = the key. This encryption method and idea lead to the development of the mathematical algorithms used to decode messages (Nadeem et al., 2005). Cryptography algorithms have 3 types

of characteristics: a private key, a public key, and hash functions. The blockchain contains a "hashing function" or cryptographic hashes or Secure Hash Algorithms (SHA2) that produces a bytes stream. The hashing method consists of converting variable value and passing through the hash function into something that transforms the value into a fixed hash value (Rogaway et al., 2004).

The hash function is categorized under the cryptographic hash function in the security field. SHA is the most used cryptographic hash function. Specifically, the SHA-2 is a hash algorithm accepted and used by the U.S Government in various government-protected programs. SHA-2 is used to protect sensitive data using cryptographic algorithms. The data content or messages in the SHA-2 consist of 256 bits versus the old SHA-1, which has 160 bits. In reality, the longer the hash structure, the more secure the data is (Rogaway et al., 2004). Figure 8 below illustrates the testing on the Hash function value with and without the "ad hoc" Genetic Programming (GP) to the hash function (KeyCDN, 2019).

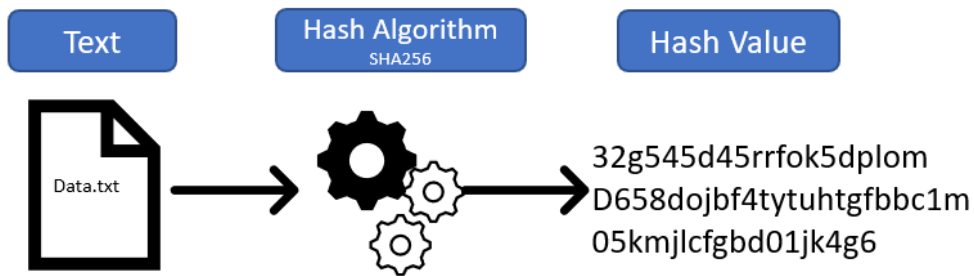


Figure 8: Path of a Hash Value

There are six hashing variations of the Secure Hash Algorithm or (SHA-2) algorithm family, which consists of SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. These can also be called hash values. Hash variations are essential when applying these functions to applications, databases, software programs, and networks. Saez et al. (2019) investigate an approach to design a tailor-made hash function to allow it to adapt to real-world environments by adding an “ad hoc” non-cryptographic hash function to the existing hash as illustrated below in Figure 9 (Saez et al., 2019).

This will allow for continuous evolution if necessary. Eight different scenarios were tested, and the results illustrated the new function hash that was designed outclasses the non-cryptographic hash (Grochol et al., 2018).

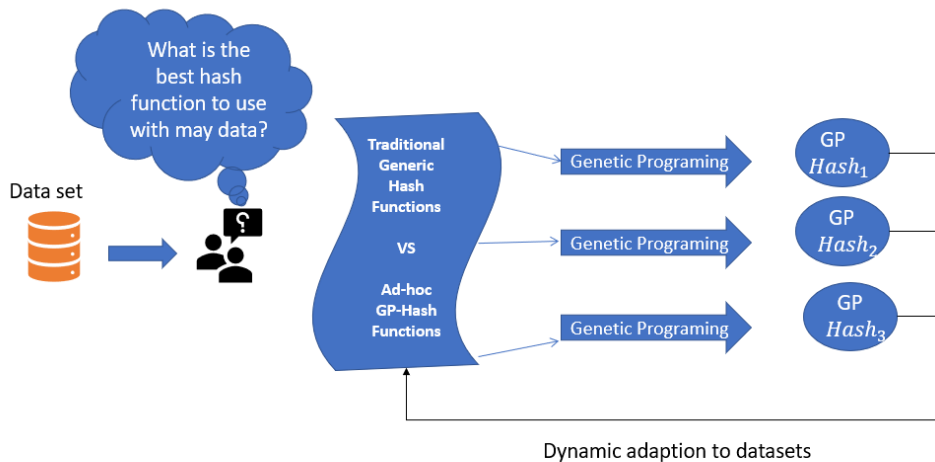


Figure 9: GP-Hash Ad-hoc function comparison

The SHA-2 function is widely used in password encryption, security, Transport Layer Security (TLS), Secure Sockets Layer (SSL), Pretty Good Privacy (PGP), Secure/Multipurpose

Internet Mail (S/MIME), Internet Protocol Security (IPsec), and Secure Shell (SSH). These security applications assist in the authentication process and message standards. SHA-2 is also commonly used to sign digital security certificates and documents, making it the most secure hash function (Grochol et al., 2018).

2.2.9 Cryptocurrency (Bitcoin)

Cryptocurrency is an alternative way to manage today's financial world. Cryptocurrencies can only work in a network of Blockchains. When these transactions are carried out, registered users of Bitcoin can remain anonymous. Cryptocurrency / Bitcoin is a digital currency type that does not resemble traditional paper bills and coins. Bitcoin operates on an open-source platform, where both a digital currency and Peer-to-Peer currency are considered (Hewitt, 2015). According to Partanen, 2018, Cryptocurrency is the first technology-driven system for payments and transactions after the traditional system of using paper bills and coins as money. The government is interested in how cryptocurrency can be incorporated into everyday life and how much the government can control such investments (Partanen, 2018).

Today transactions are still conducted with a third party somewhere present in the transaction history or money transfer. This can include a bank or other financial institution type to overlook any transaction and validate both sides' data due to the lack of trust between the two parties initiating the transaction. The concept then lies in removing the need for validation and creating a direct link between supplier and buyer. Satoshi Nakamoto introduced the idea of removing the “middle man” by creating a network where the transaction is completed and recorded

and visible/transparent to anyone. This creates a network where transactions are recorded as a code, creating faster transaction speed and tamper-proof (Hewitt, 2015).

A case study done by Partanen in 2018 looks at the viability of cryptocurrency / Bitcoin concerning how it is perceived and accepted by the use of large stakeholders. The stakeholder's studies included the government, financial institutions, and other countries interested in cryptocurrencies. To investigate the interest and viability, SWOT analysis, and PESTLE analysis was done on the cryptocurrency / Bitcoin (Partanen, 2018).

According to financial institutions, banks fear they will lose control of transactions if cryptocurrencies take over as the primary payment form and appear weak when banks are healthy. Meanwhile, some financial institutions want to keep their customers happy and have implanted or made available cryptocurrencies. The government or Wall Street fear missing out if they skip out on implementing cryptocurrencies / Bitcoin (Noonan, 2014).

Some financial institutions have swayed the other way about how they feel about Bitcoin. They feel it is part of a black market where its anonymous nature and highly illegal transactions can take place and can also be looked at as a "blood diamonds" market. Some banks do not want part of a network filled with criminals or any fraudulent activities. The results indicate that the government and banks have not fully taken on the cryptocurrency. The government would only be interested if they can regulate and control cryptocurrencies. Banks will not replace the current currency with Bitcoin. After performing the PESTLE and SWOT on Bitcoin, the author believes that cryptocurrencies will not threaten current legal tenders but will become a tender of their own as an asset or an investment option (Noonan, 2014).

Another study completed by Yaya, O. S., Ogbonna, E. A., & Mudida, R. in 2019 investigated the efficiency of the Market and volatility of cryptocurrency for Bitcoin. The study used fractional integration methods in linear and nonlinear methods to analyze if markets can be efficient in such circumstances of pre and post-crash of Bitcoin. The study revealed that cryptocurrency is efficient, and there is evidence of the Bitcoin values as Bitcoin values are unpredictable. Due to the unpredictability in cryptocurrencies future, investors cannot make stable and long-term profits from the cryptocurrency markets as suggested in the case study (Yaya et al., 2019)

Caporale et al. (2018) compared Bitcoin to other cryptocurrencies that are not as popular such as Litecoin, Ripple, and Dash cryptocurrency. The comparison was made to analyze the evolution and persistence in success in the current market over time. While the Litecoin, Dash, and Ripple cryptocurrency dropped over time, Bitcoin was also unpredictable in its efficiency. Using the Rescaled Range (R/S) analysis as illustrated below in Table 2, daily frequency data were analyzed between 2014 to 2017 and anomalies and any changes in the Hurst exponent. The results will help make decisions based on trading strategies in the cryptocurrency markets (Caporale et al., 2018).

Table 2: Results of the R/S analysis in various cryptocurrency markets

Period	Daily Frequency
Bitcoin	.59
LiteCoin	.63
Ripple	.64
Dash	.60

Cryptocurrencies have even merged with Machine Learning in its evolution of digital currency generation, relying on the cryptographic properties in transferring, generating, and distributing currencies. Machine Learning enhances cryptocurrency (Chang et al., 2009). Alessandretti et al. (2018) examined the hypothesis of how Machine Learning can be useful in simple exchange strategies by using Machine Learning algorithms to enhance efficiency in the market. The study used data that included Price, Market capitalization, Market share, Rank, Volume, and Age of the currency from November 2015 to April 2018, involving 1,681 cryptocurrencies transactions. The results showed viability in Bitcoin over time that can be measured through the return on investment or (ROI) (Alessandretti et al., 2018).

2.2.10 Smart Contracts

Smart Contracts essentially are not controlled by anyone and or anything. Smart Contracts are pieces of codes built inside the Blockchain that codify business logic, and at the core, they are meant to do three things, store rules, verify rule, and self-execute rules. Smart Contracts are being infiltrated in many industries since they are programmed inside a Blockchain, and applications like

the Internet of Things (IoT), supply chain, and financial sector. Smart Contracts have the potentials for solving problems without any person involved and create trust. A Smart Contract is the idea of allowing data to be collected, stored, and implemented within a distributed ledger in a Blockchain (Hassan, 2018).

Nick Szabo, a computer scientist, first coined the idea approximately in 1995 about Smart Contracts. He referenced the idea of taking the initiative to implement and store Smart Contracts in a ledger. One may ask, what exactly is a Smart Contract? They are digital data that is stored in a Blockchain that cannot be changed, altered, reversed, like a computer program. It also stores the terms of the negotiation or the rules between two or more parties. After it collects and saves those agreed terms, it automatically triggers a response when the terms have been reached and execute an order without human interference or a human making any changes (Green, 2018). For example, a crowdfunding site collects funds. The rules that are programmed into the “Smart Contract” for the site states to collect a certain amount. When the goal has been reached, the crowdfunding site should distribute the fund to the goal setter or user to initiate the funding goal. The next rule embedded into the Blockchain is that the funds do not reach the intended goal, all funds belonging to the sponsors or donors of the goal get returned to them. These rules are programmed within the Smart Contract, and no one can alter or change those rules since they are tied to a computerized hash code, and it is impossible to change the rules once set (Meadows, 2017).

Hassan Shah Zaib (2018) examines the use of a Blockchain platform to analyze the problems faced in education and technology while raising funds for their projects. Because of the change, the application requirements have been met. Thus the application has been deployed to the Blockchain, and the public can access it (Hassan, 2018).

2.2.11 Ethereum

Historically, Ethereum started as a computing platform introduced by Vitalik Buterin in 2013 when he was only 19 years old. The idea of Ethereum by Buterin was to leverage programs in general and across a system of distributed nodes. The way Ethereum was built was to be a host for Smart Contracts so the Smart Contracts can self-execute over the network and are immutably embedded in the Blockchain when they mean certain milestones or goals that are programmed in them (Vujičić, 2018). Ethereum, the world's second-largest cryptocurrency after Bitcoin, leads and paves the way for a digital decentralized money platform to become very popular. In 2018, Ethereum achieved more than \$ 133 billion in market capitalization (Torres et al., 2019). Ethereum is an open-source, public service that securely facilitates Smart Contracts and cryptocurrency trading not including a third party using Blockchain technology. Some developers even predict that Ethereum is leading towards an aggressive expansion to overpower Bitcoin in the next year and soon take over the Bitcoin usage market despite Bitcoins' growth and popularity (Marr, 2018).

According to a study by Moosavi et al., 2018, Ethereum is also an allocated technology available to the public. Ethereum is tied to Smart Contracts because it allows for the development of Smart Contracts in a decentralized system of applications and codes. This means anyone in the world can connect directly and access the Ethereum Blockchain to develop and maintain a network. Nearly the building blocks built within the Ethereum platform program are known as the Smart Contracts. The Smart Contracts then run on an Ethereum Virtual Machine or (EVM) platform. The EVM can be used to encrypt Contracts, move money allocation, impose honesty and trust in relationship environments between two or more parties. The question lies in whether

Ethereum will continue to make growth progress and change investor ideas about its volatility since there are still many investors who are cautious about (Moosavi et al., 2018).

An empirical case study was conducted by Vikram Saraph and Maurice Herlihy in 2019. The study looked at historical data to estimate the potential benefit of speculative techniques is similar to the implementation of Smart Ethereum Contracts. The study uses the replay traces of experimented blocks from the Ethereum Blockchain over time. The speculative technique studied yielded the terminated transactions executed sequentially and resulted from the speculative technique used concurrent execution (Saraph et al., 2019).

Ethereum provides Smart Contracts for all of its users, such as execution, recording of the transaction, and definition of the Contract rules. Amani et al. (2018) looked at the structure of the bytecodes sequences embedded into the Blockchain and how they can create a program that can logic with this reasoning. The study resulted in a step towards cost control of Smart Contracts in Ethereum and the Ethereum Virtual Machine (EVM) (Amani et al., 2018).

2.2.12 Honeypots in Ethereum

As Smart Contracts become more popular and added value, they become an intriguing new target for fraudulent perpetrators. It has been discovered in recent years that a few intelligent Contracts have been found susceptible and therefore been exploited. However, a new movement appears to be heading towards a more practical tactic in which fraudulent perpetrators no longer pursue critical Contracts. Instead, they try to trick their victims by arranging exposed Contracts with hidden traps (Andre et al., 2018).

These hidden traps or fraudulent Contracts are called “Honeypots.” The latest case study on Honeypots was completed by Torres and Steichen (2019), which investigates the Honeypots that may be found in the Ethereum Blockchain and how this can impact the frequency, conduct, and influence on the Ethereum Blockchain. Figure 10 illustrates a “Honeypot” phase in the path to its victim (Torres et al., 2019).

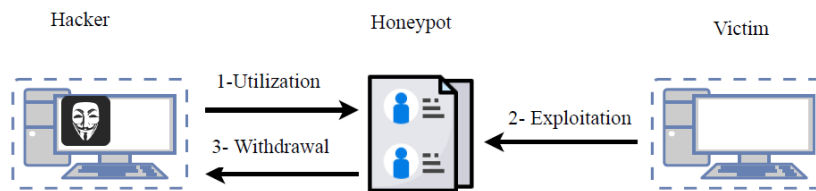


Figure 10: Phases of a Honeypot utilization

Figure 10 illustrates the attacker deploying a depiction of a so-called Smart Contract as bait to its victim. The next phase shows the victim attempts to transfer the funds required by the so-called fraudulent Contract, the third phase is where the attacker removes the bait or Contract with the funds that have been transferred, and the victim loses the funds transferred, which end up with the fraudulent attacker. The study concluded that a technology called Honey Badger would detect Contracts via an EVM bytecode on the Ethereum Blockchain. The Honey Badger runs a process for symbolic analysis, cash flow analysis, and honeypot analysis to determine which Smart Contract is a Honeypot, as illustrated in Figure 11. Honey Badger is executed in Python (Jacobsen et al., 2018).

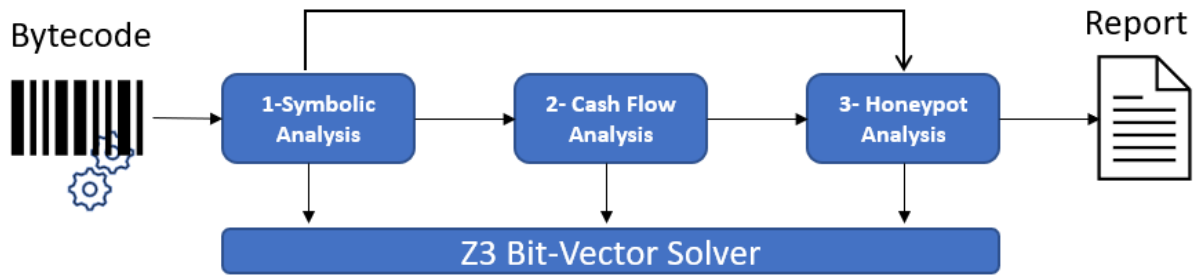


Figure 11: Honey Badger to Capture Honeypots in Ethereum

This case study examined 2 million Contracts currently in use on the Blockchain, with a total of 690 Contracts distinguished as honeypots. The results revealed that the usage of Honey Badger had a 91.32 % success rate in detecting a code coverage of Honeypots in Ethereum. Despite the results of the fraudulent activity of honeypots, it still retains a shallow success rate in the fraud department of Ethereum (Torres et al., 2019).

2.3 Decision Making

According to Gilbert, G., Ahrweiler, P., Barbrook-Johnson, P., Narasimhan, K., & Wilkinson, H, in 2018, a study called Computational modeling of the public policy describes the benefit of simulation and modeling helps organizations to make appropriate decisions based on the results of the presented simulation and modeling data. The task of organizations is to use simulation and modeling to test different solutions that help in the decision-making process when an organization has a problem. Simulation and modeling aim to offer organizations decisions based on organizations' results and challenges (Gilbert et al., 2018).

A study carried out by Abukhousa, Al - Jaroodi, Lazarova - Molnar, & Mohamed, 2014, and published in The Scientific Journal, which discusses simulation and modeling efforts to support decision - making in the supply chain management of healthcare. These advantages were to address the healthcare industry's challenges to find solutions to risk management, cost efficiency, and support the goal to decrease healthcare problems. According to the 2014 study by Abukhousa et al., decision-making is the benefit of simulation and modeling. This benefit is the objective of modeling simulation. With new technologies increasing, the objectives are to increase the impact and added value of the simulation modeling results to increase the healthcare industry's benefits (Abukhousa et al., 2014).

According to Beamon (2008), the decision-making process has three main properties. The first level of decision - making is strategic, based on the outcome and the impact it would have on the organization. For example, strategic decisions in healthcare are considered long-term and impact the entire organization's shape and direction, such as budgets set for the industry. The decision at this level affects the future of the organization.

The second level in decision-making is tactical, which later helps to implement the strategy. Research and studies are carried out to reach a tactical decision based on the received data. The objective is to achieve financial objectives to help decide where profitability and sustainability are located within the industry. The decision taken at the tactical decision-making level may lead to new purposes and procedures affecting the management and dispersal of inventories in any industry (Beamon et al., 2008).

The third level of decision-making is operational decisions. The decisions taken at this level are more specific to an organization's day - to - day operations. They can be routine decisions and can be made in the organization by lower or middle managers. The objectives covered by operational decisions are inventory, lower budget limits, the cost of opportunities, and excess stock. In any industry, the operational decision-making level faces challenges that affect the industry's factors. This can be due to poor planning and the failure to monitor the min/max inventory levels, leading to a split effect and cost the organization a large amount of its revenue and generate waste or overstock (Ramachandran et al., 2018).

2.4 Artificial Intelligence

2.4.1 Introduction

Artificial Intelligence (AI) is a powerful invention in technology that facilitates the social, economic, and daily activities of the world. It creates a key contribution to the economic progress of the world and addresses numerous societal issues. Machine learning (ML) is a subset of AI, which makes it possible for computers to learn without programming. Computers have developed as a result of the development of intelligent machines, so they can process data without a human being involved. A well-known American pioneer in the AI area, Arthur Samuel, coined the word "Machine Learning" back in 1959 (Vu et al., 2018).

Machine Learning has become a powerful technology used in various applications and sectors. For example, Machine Learning has been used in smart cars, healthcare, and handwritten and voice pattern recognition (Chen, Qin, Wang, Yu, & Gao, 2020). Figure 12 below shows artificial intelligence science and its subsets.

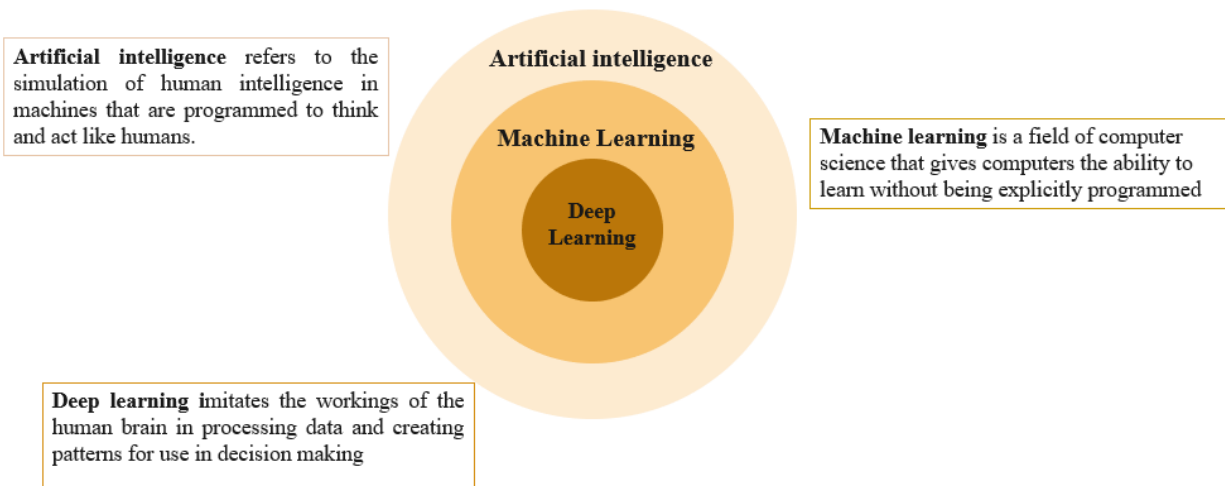


Figure 12: Artificial intelligence and its subsets.

2.4.2 Artificial Neural Networks

It is essential to understand neural networks to understand Deep Learning. Expert Maureen Caudill stated that an Artificial Neural Network (ANN) is a computing system comprised of numbers and unified managing elements that handle data by their reaction to the external inputs. Essentially, ANN is a framework that is useful for machine learning algorithms. These algorithms collaborate and process complex information that is received by the ANNs. ANNs are similar to the human brain, where interconnected neurons transmit and receive data via neurons. However, with the ANNs, these transmissions happen on a computational level. The artificial network receives data via a single vector and then takes that data or input and transfers it through a sequence of hidden layers until it reaches the output layer, the fully linked layer in an ANN (Berg et al., 2018).

2.4.3 Back Propagation

Backpropagation is a supervised learning algorithm that uses training an artificial neural network on how to accomplish a particular task. Backpropagation uses a method to calculate the “error function” related to the weights of the neural network caused by an ANN and an error function using a delta rule method. The network is prepared with weights added for all the neurons in the layer. The error factor is calculated for each neuron. When an error is located, the error is then backpropagated to assign the correct weight to minimize the error. The purpose of using backpropagation is to train the neural network for all the input patterns and layers until errors do not exist (Sundaram et al., 2016).

A case study completed by Sundaram, N. M., & Renupriya, V. in 2016 titled A Survey on Different Training Algorithms for Supervised Learning of Backpropagation Artificial Neural Networks utilized two different algorithm methods to test the performance of the network. The first method was the Mean absolute Percentage Error (MAPE) (as shown in Equation 1 below) metric using the Bayesian Regulation algorithm. It was concluded that using the Bayesian Regulation Algorithm proved to have the lowest MAPE. The next method used was the Levenberg-Marquardt algorithm, which proves that it was very efficient and had a high accuracy in training the network. However, they had a higher demand for computational efforts. In conclusion, the Bayesian Regulation Algorithm is best suited for more massive data sets input for a network. Equation (1) below was used to calculate the MAPE (Sundaram et al., 2016).

$$MAPE = \left(\sum_{j=1}^{j=n} \left[\frac{Estimate - Actual}{Actual} \right] \right) \div n \times 100 \quad (1)$$

2.4.3 Deep Learning

According to Samek et al. (2017) that explains the Deep Learning models and how it is used to explain artificial intelligence. Learning has been in many organizations' interest for quite some time now, a general topic in the Artificial Intelligence domain. In particular, it's known for its breakthroughs in fields such as computer vision and gameplay but has branched out to different industries and has gained popularity for the type of functions it can produce. Due to the nature of Deep Learning stemming from Artificial Intelligence, there are progressively complex algorithms that significantly impact an individual's life and businesses and the choices available (Samek et al., 2017).

The Deep Learning mechanisms and algorithms are surpassing the capabilities allied with our professionals today. A new provision that currently uses Deep Learning systems embraces computerized driving systems and hearing aids that benefit people to interpret languages instantaneously. Deep Learning has both good and bad outcomes, but it is based on how the technology is applied, and there is no inherent problem with the strategy or application of the algorithms (Marcus, 2018).

Deep Learning is a subset of Machine Learning in Artificial Intelligence, which requires a machine to learn via trends or patterns, possibly hundreds and thousands of stored trends or

patterns. Deep Learning allocates computers to be taught knowledge from data without human intervention or a human controlling the output data. This process is termed learning via unstructured, unsupervised, or unlabeled information. Humans will permit the machine to discover a learning algorithm to scan and learn on a deeper training level. Then, the machine utilizes the algorithm to solve problems from the learned trends or patterns. Deep Learning involves large quantities of information and learning patterns to learn and achieve an precise decision. The more accessible information Deep Learning has, the more precise the output (McClelland, 2017).

2.4.3.1 Deep Neural Network

According to McDonald (2017), Deep Learning is equivalent to Deep neural learning or system. It uses a non-linear method to go through numerous layers of data and learns to generate an intelligent output through the raw information. It is essential to understand that Deep Learning aims on learning data through numerous layers versus Machine Learning, that learns through a layer of data, as illustrated in Figure 13. Money laundering detection is an example of Deep learning. Machine Learning can identify a laundering attempt by the total amount of the transaction, meanwhile Deep Learning progresses deeper by learning the source (user) of the

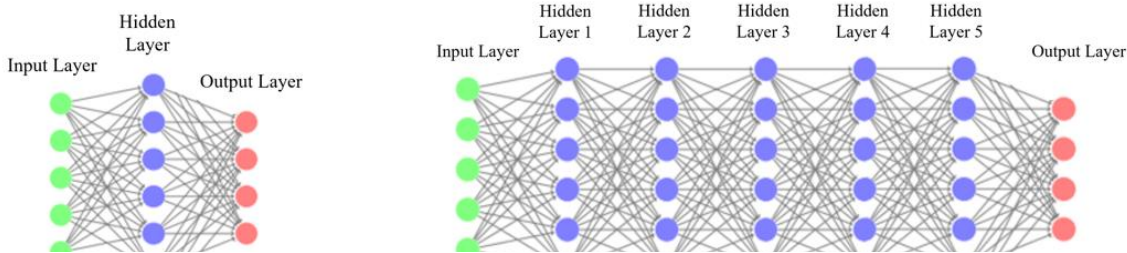


Figure 13: Simple Neural Networks versus Deep Neural Networks (DNN)

transaction, the user's location and IP address. The layers are termed as the Deep Neural Networks (DNN) process (McDonald, 2017).

Zhong et al. (2016) analyze the advancement in deep learning from traditional views and features to current deep learning methods used in finance and data science using data representation learning methods. Around the 1970's P. Werbos studied the backpropagation (BP) algorithms to train multi-layers in a neural network. He proved that using the BP algorithm method was suitable and beneficial in the internal representation of data found in neural networks' hidden layers. The development throughout data representation has been trying to merge with neural networks; however, data representation has become more complicated than neural networks. Figure 14 illustrates the evolution and the intended merge with neural networks overtime (Zhong et al., 2016). The study concluded that the future concepts of deep learning would use the fundamental theory and novel algorithms to create deep learning networks that can process cultured models using this technology (Zhong et al., 2016).

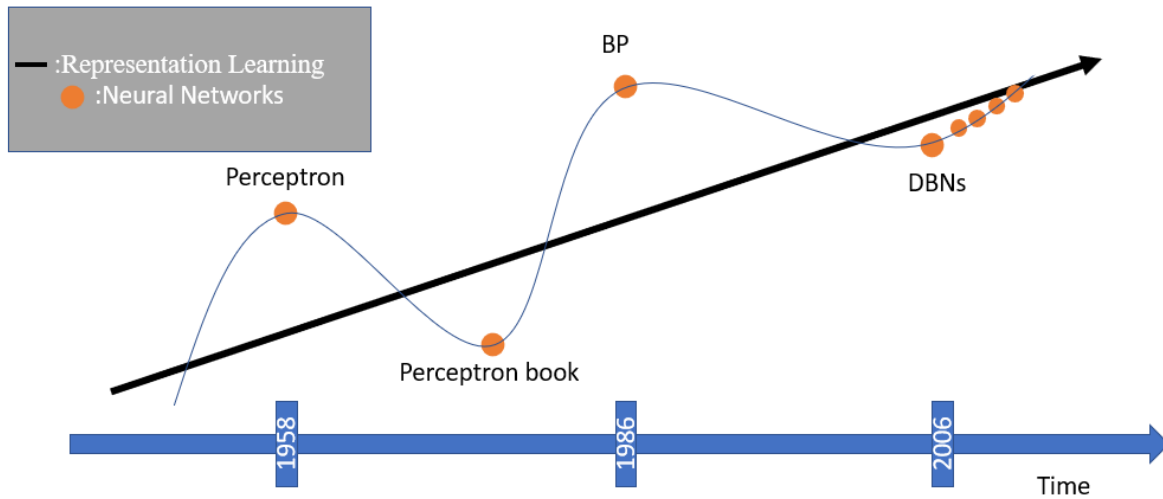


Figure 14: Development of Data Representation and Neural Networks

There are three major classes of deep learning architecture, which are generative, discriminative, and hybrid. Generative deep learning architecture categorizes the relationship in properties of visible information or data patterns for analytical purposes and depicts the information distribution to their respective class. The discriminative deep learning architecture provides pattern classification into classes. The hybrid deep learning architecture combines assisted generative and discriminative approaches to improve optimization and learning parameters. There are also various types of neural networks and/or machine learning structures such as Artificial neural networks (ANNs), Recurrent neural networks (RNNs), Deep belief networks (DBNs), Deep neural networks (DNNs), Convolutional neural networks (CNNs), Deep Boltzmann machines (DBMs), Restricted Boltzmann machines (RBMs), and Generative Adversarial Nets (GANs). These networks can be classified as deep generative models (RBMs,

DBNs, & DBMs) and deep discriminative models (DNNs, RNNs & CNNs) (Montavon et al., 2018).

Tishby and Zaslavsky (2015) analyze the Deep Learning concept and the information bottleneck principle with the relationship between the layers in Deep Learning and output received from the input layers variables among a simple versus Deep Neural Networks (DNN). This study also looked at the Neural Networks (NN) architecture. It argues that the input layer is relatively compressed to the output layer. The classified depictions in the layered network are parallel to the structural phase's evolutions along the data curve. It has been found that this new perception can lead to new ideal limitations and Deep Learning systems in Deep Learning (Tishby et al., 2015).

According to Schmidhuber, J., Deep Learning processes the input data and can generate more accurate choices by taking in large amounts of data. Deep Learning uses the learning algorithms and discovers a behavioral pattern that can prompt for an inspection in imminent fraudulent activity. The core of Deep Learning depend on layers of three linked neurons. The primary neuron is the input layer, and the subsequent neuron is the hidden layer(s). To take a more thorough look at Deep Learning is to first look at what Deep Learning is comprised of (Schmidhuber, 2015).

Deep Learning is considered learning of hundreds of Deep layers of representation. When looking at Machine Learning, it can also be noted that Machine Learning can be called shallow learning as it does not require Deep layers of data to learn. There are various paradigms of Deep Learning, which is the learning of Neural Networks with multiple layers. Examples of types of

Deep Learning techniques are Hidden Markov models (HMMs), Generative Adversarial Nets (GAN), Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Sum-Product networks (SPNs) (Liu et al., 2017).

Some methods and techniques used in Deep Learning are The Hidden Markov models (HMM), a way to calculate the probability for several sequences in an event(s). Generative adversarial nets (GAN), which copy the inputted data, outputs a similar model. A real-world example of this is text to image generator or image to image generator. Recurrent Neural Networks (RNNs) are algorithms that process a sequence of data such as a sensor or a language or sound and can model the data and classify the data or create a cluster of data depending on what is being presented. An example of RNN is various hand-written words, and that data is then translated into computer text. The data can be different every time, such as in the style a word is written. The more data is inputted, the better RNN can learn to translate and model the output (Liu et al., 2017).

Zheng et al. (2015) called Conditional random fields recurrent neural networks, explains that RNNs can also learn various sounds and categorize based on different sequences in the sound. Another method is Convolutional Neural Networks (CNNs), which analyze and classify images, sounds, texts, graphs, and documents categorized in a tensor number format using a matrix-like grid for use, such as for image search, face recognition, and sound recognition. Sum-Product Networks (SPN) is used to uncover the multiple hidden variables in a model. Algorithms can learn Deep Sum-Product Networks (SPN) using nodes (Zheng et al., 2015).

Salakhutdinov (2015) stated that Deep Learning and Data Science means the Deep structuring and un-structuring of the represented data that allows the platform to create a user-

optimized solution using the preset algorithms to create an intended output. Deep Learning has become the fastest advancing field in Neural Networks. Deep Learning has therefore become a growing inclination in the topic of Artificial Intelligence to draw better and more accurate data results when data is too large or multifaceted and complex to be extracted with artificial intelligence alone (Salakhutdinov, 2015).

A case study completed by Sun, T., & Vasarhelyi, M. A. in 2018 analyzes the Embracing Textual Data Analytics in Auditing with Deep Learning, specifically in financial data and the financial world. Deep Learning models can be created to use in the financial industry to predict financial fraud. It can also be used along with text mining to read millions of Contracts and complex documents and extract the intended information for the auditing and consulting processes for firms and organizations. However, Deep Learning is not perfect. Deep learning is more art than science.

It is essential to understand that the more data available for processing, the more useful and accurate Deep Learning becomes. Deep Learning is used in many industries and many aspects of businesses. Over the years, Deep Learning has improved through computerized infrastructure and has provided the industry with more precise data outputs over time. Back in the 1940s to 1960, Deep Learning was known as cybernetics due to its development. Then in the 1980s to 1990s, it was known as connectionism (Goodfellow et al., 2016).

The concept and inspiration of Deep Learning reside in neuroscience to mimic the intelligence of the brain as close as possible using computational units. This concept was introduced in 1975 by Kunihiko Fukushima under visual pattern recognition (Fukushima et al.,

2015). According to Xie (2018), Deep Learning enables complex systems to hold large amounts of trained data gathered from their consumer base and introduce outputs that the organization is looking for. For example, in the financial market, we can have an individual who wishes to obtain a loan from a financial institution can do using Deep Learning without a bank's interference. The real-world application that complex systems can have allowed individuals to make loan requests and the complex system can analyze which individual is creditworthy of such a loan (Xie et al. 2018).

Tan et al. (2018) explore solutions to challenging risks, charge-off, payment installments, and subsidized advances. The model used in this study consist of integrating qualitative and quantitative models in the grading system. This requires using Deep Neural Networks to characterize the loan risks in a complex system such as a P2P market. The results achieved an interesting investment outcome by modeling the risks between the investor and the potential loan dynamics (Tan et al., 2018). Another case study completed by Bastani (2018) discusses the current loan approaches and predictions using credit scoring. However, the case evaluates a method using profit scoring to determine which loan investment is the best for the financial institutions' benefit and customers. A Deep Learning predictive model in a two-stage process of simplification and memorization was developed successfully for a practical approach (Bastani et al., 2018).

In this case study, IRR predictive models depended on the training data and samples that were inputted. The results showed that Deep Learning was beneficial over other testing methods to determine the loan process's profit score. The case also utilized Deep Learning in TensorFlow. The results showed that the field of profit scoring is still to be explored as tests were inconclusive

and ignored the customer's demographics, which is useful in making loan decisions (Bastani et al., 2018).

Figure 15 illustrates the Deep Neural Networks (DNNs), which are known for their “depth” and having an input layer, one or more hidden layer(s), then an output layer. DNNs are considered part of a complex machine learning system that uses algorithms for regression and reinforcement learning. Data is then transmitted via the input layer all through the hidden layers and nodes. A recent study completed by Piao, G., & Breslin, J. G. in 2018, titled Financial aspect and sentiment predictions with deep neural networks, uses a Deep Learning approach to untangle the financial domain, which plays an essential part in forecasting a market response. This was done by feeding a Deep Learning Neural Network a sequence of words. Those words are given a sentiment score and aspect labels in the deep neural network and generate an output formula. This study was deemed successful in displaying an output text after using the DNNs (as shown in Figure 15), prediction, and lookup features of the proposed approach (Piao et al., 2018).

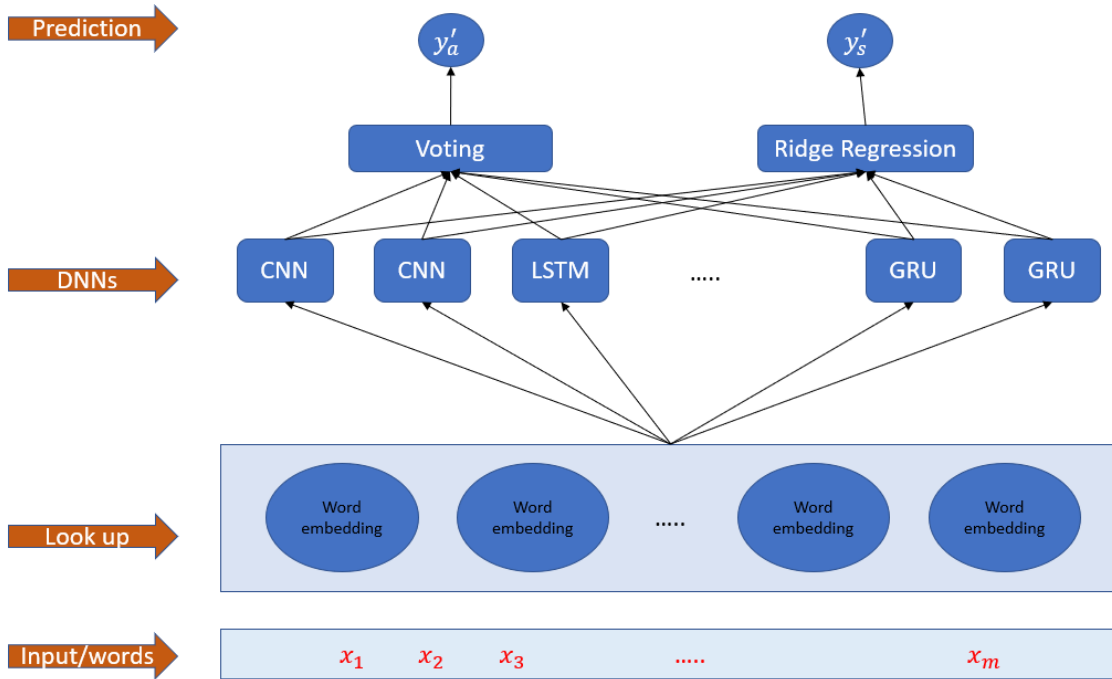


Figure 15: DNN model to test Financial mining approach

2.4.3.2 Recurrent Neural Network (RNNs)

Recurrent neural networks (RNNs) are networks that allow nodes to form connections along a sequence. RNNs illustrate the motivated behavior of a network and rely on their internal memory to develop inputs. They are used in deep learning such that models can be created using recurrent networks by helping in predicting an outcome, unlike other neural networks. They are also used mostly in speech recognition. RNNs are comprised of network nodes that are interconnected. The name recurrent comes from the neural network's ability to become layers of data and process data in two diverse directions (Yogatama et al., 2018). The latest study presented by Alemi-Neissi et al. (2019) approached Recurrent Neural Networks (RNNs) (as shown in Figure

16) with a goal, which was to create a learning rule for the RNN and have a maximal storage capacity. This was completed by learning thresholds and external inputs. A histogram was used to model the results of the before and after learning, which was successful. Regarding the storage capacity, the simulation test proved successful in that there were recalls of the simulation pattern (Alemi-Neissi et al., 2019).

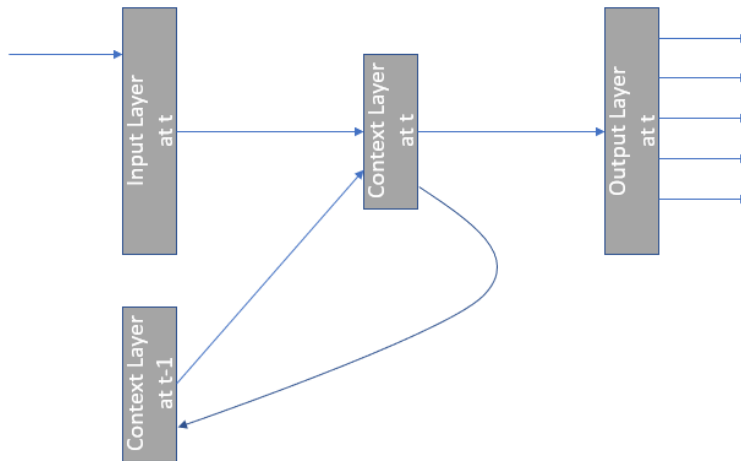


Figure 16: Recurrent Neural Networks (RNNs)

2.4.3.3 Deep Belief Networks (DBNs)

Deep Belief Networks (DBNs) are graphical-based models that have many layers. DBNs are also called generative models. DBNs are meant to extract the depiction of training data and model the combined dispersal between hidden layers and vectors. DBNs use Restricted Boltzmann machines that have layers that communicate with the previous layer and the succeeding layers. However, the nodes of the layers do not communicate with each other. The use of DBNs is to recognize, generate images, and are used in video sequences. They can have the capability of motion-capturing data (Tran et al., 2018).

Testolin et al. (2018) analyze the deep belief neural networks to depict the DBNs' structures after a learning process and its properties, which can be translated to computational graphs by using a sensibility analysis. The primary purpose of a deep belief network is the hope for the network to build more controlled and intellectual depictions of the input data. The study's neuron function seemed to be successful in the sense that it gave the approach a new insight into the structural properties of the Deep belief network and a non-linear system (Testolin et al., 2018). Figure 17 illustrates the Structure of a Deep Belief Network (DBN).

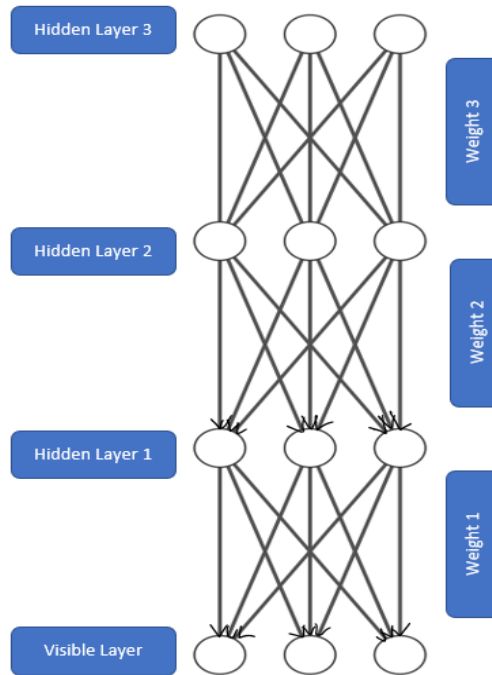


Figure 17: Structure of a Deep Belief Network (DBN)

2.4.3.4 Convolutional Neural Networks (CNNs)

Convolutional Neural Networks (CNNs) consists of a multi-layer network structured to have an Input, Output, and multiple hidden layers much similar to a regular Neural Network. However, CNN's are built to recognize visual trends or patterns directly from the input of images. CNN's can perform object detection tasks without the need for extensive data such as Neural Networks. They can use fewer parameters or “weights” to learn. The hidden layers include convolutional layers, pooling layers (Layer 1 and 2), and linked layers (Layer 3, 4, and 5). A recent study published by Cotter, F., & Kingsbury, N. in 2019 titled A Learnable ScatterNet: Locally Invariant Convolutional Layers analyzes a Scattering Transform approach CNN for image analysis. Previously ScatterNet was inserted at the beginning of a CNN in the hopes of better image analysis. However, after this study, it was determined that adding ScatterNet to CNN produces better results and improved accuracy in classification, recognition, and segmentation of image analysis (Cotter et al. 2019).

2.4.3.5 Deep Boltzmann Machines (DBMs)

Deep Boltzmann Machines (DBMs) is a deep learning model that consists of connections between layers that are hidden and have hidden units. Figure 18 depicts these undirected layers' connections, unlike those found in a Deep Belief Network (DBN). Voulodimos, A., Doulamis, N., Doulamis, A., & Protopapadakis, E. in 2018 titled Deep learning for computer vision proposes that DBMs and selecting the right type of interaction between the visible and hidden layers will display a more controllable form of the DBM model. A stochastic maximum likelihood (SML) approach was used to train the layers using the algorithms of the DBM. The unique feature of the DBM is

that there is no output layer. Each layer is trained by stacking RBMs. One advantage of the RBM is that it can hold many layers of intricate depictions from the input data. Another advantage is they can also be trained on unlabeled input data. The study concluded that using this computer vision approach has excellent success in using CNNs, DBNs, and DBMS (Voulodimos et al., 2018).

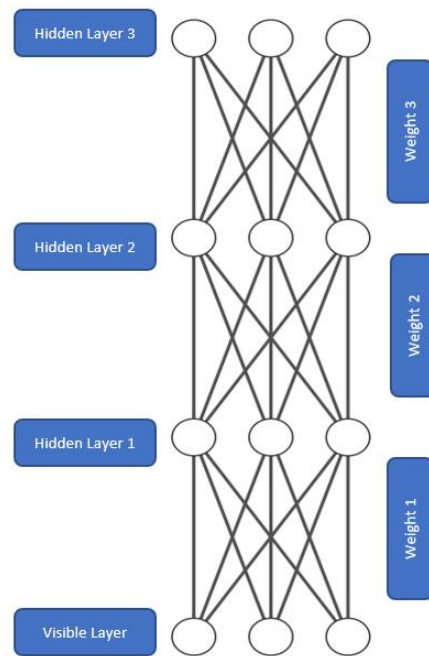


Figure 18: Structure of a Deep Boltzmann Machine (DBM)

2.4.3.6 Restricted Boltzmann Machines (RBMs)

Restricted Boltzmann machines (RBMs) consist of a total of two layers; one hidden layer and one visible layer. They can learn probability distribution regression, classification, and topic modeling. A study presented by Prosak, A., Gangopadhyay, A., & Garg, H. in 2019 titled A New Machine Learning Approach for Anomaly Detection Using Metadata for Model Training suggests

using RBMs as a way to detect sensitive data and inconsistent log records and for language processing. Using various Machine Learning models can cut down on training time and testing time (Prosak et al., 2019).

2.4.3.7 Generative Adversarial Nets (GANs)

Generative Adversarial Nets (GANs) are deep neural net architectures that help solve problems by training two distinct networks with objectives. The first network creates an output or an answer that makes it generative. The other network differentiates between a real answer and a generated answer that makes it adversarial, hence the name Generative Adversarial Networks GANs (Figure 19). The GANs are unique due to their ability to learn and copy any dispersal of information (Koshiyama et al., 2019).

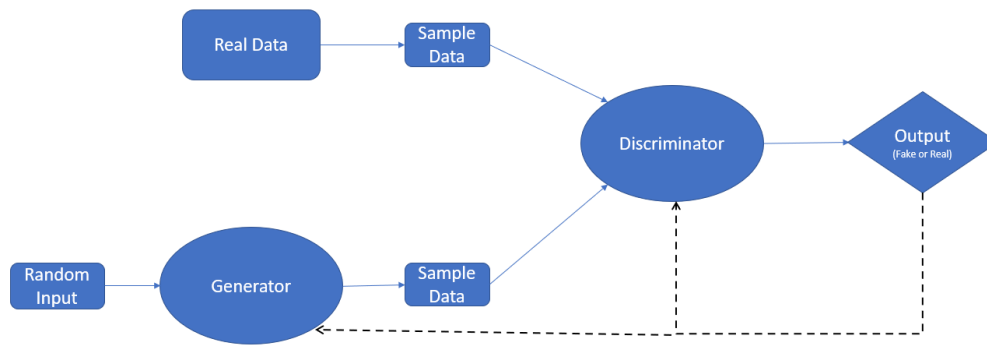


Figure 19: Generative Adversarial Network (GAN)

A recent study completed by Koshiyama et al. (2019) analyzes the trading market industry and a strategy that allows for an automatic or systematic trading strategy programmed using

algorithms to allocate assets using a standard. Trading analysts need to adjust the current systematic trading criteria to achieve the best or a desired performance in the trading market. The paper proposes using GANs as a substitute for strategies, which, in conclusion, outperformed current trading strategies (Koshiyama et al., 2019).

2.5 Simulation and Modeling

Simulation is used in gaming, education, safety engineering, testing, and training. When dealing with systems, models, and algorithms equations, modeling is essential to computing mathematical characterization in a system. Simulation is a broad term that refers to a methodology for mimicking the behavior of a real or projected physical experimentation. The terms reproduction and model, mainly quantitative and behavioral models, are linked. A model establishes the influences and characteristics of enthusiasm for the framework. A quantitative or behavioral model outlines an unraveled outlook of a portion of the items in a framework. A model employed as a part of a replica can catch many perceptions around a framework, how complicated the model is, or ought to relies on the incentive behind the reenactment that will be "run" utilizing the model. Proper modeling is a critical component in simulation, in which the capacity to acceptably predict practical simulation must encompass cooperation between complexity and precision (Ogrodzki, 2018).

According to research done by North, M. J., & Macal, C. M. (2007), there is agent-based modeling and simulation (ABMS) in the simulation world, which is a relatively new modeling paradigm. Human beings are better at relating behaviors and choices of the same system than mathematical models. The relationships between agents and the real world are more closely

matched as they describe combined behavior. ABMs uses a bottom-up approach to represent a system. It is also inspiring. The ABMS in this research covers the main impressions and applications of those approaches in emerging the agent representations in simulation. The agent has characteristics that include behavioral rules, resources, behavioral changes, rules, and attributes that are all experientially adaptive in behavior. The main impressions for modeling human, social, and structural behaviors and distinctive decision-making are artificial agents. A simulation model is comprised of conventional guidelines. These include equations, state machines, and flowcharts containing a system's future status (North et al., 2007).

For distributed simulation tools, computer-based simulations are used. Computer experiments are often used to investigate simulation models. Simulation modeling is also used in the scientific world, where human systems and natural systems allow the researcher to obtain simulation information about these scientific models' functions. There are still problems when a simulation is studied, such as the validation of the data source representing the simulation model's behaviors and characteristics and the fidelity of the simulation results. The need for more focus on simulation studies is present. Once the simulation field is in higher demand and is used by different industries, the advantages and benefits of simulation for usability in all industries will be further focused on and explored (Meng et al., 2018).

According to Gray, J., & Rumpe, B. (2016), modeling is categorized under the research branch of mathematical and computer science. The mathematical concept of modeling includes derivation, algebraic formulas, numerical techniques, and integration for the models to be used for simulation. Data science, networking, software, Machine Learning, and software architecture disciplines define the computer science concepts of modeling to enable the simulation to be applied

(Gray et al., 2016). The two categories under dynamic systems are continuous or discrete. These are the basis of time calculations in simulation.

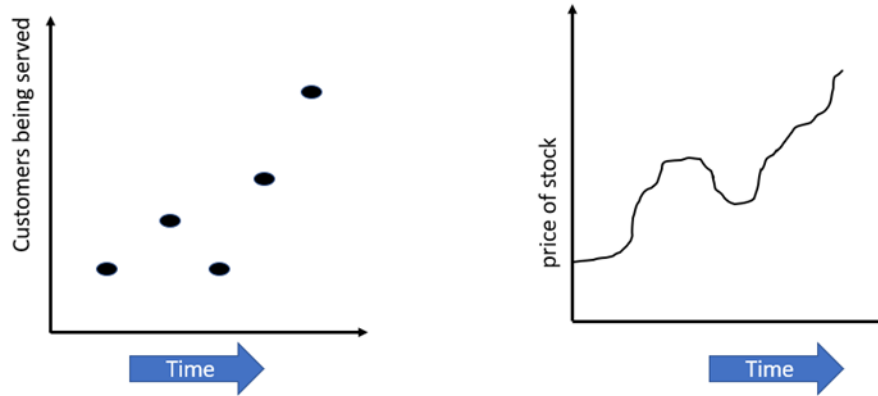


Figure 20: Discrete System (Left) & Continuous System (Right)

Banks, J., Nelson, B. L., Carson, J. S., & Nicol, D. (2007) conducted a study of their findings in discrete and continuous systems, as Figure 20 above illustrates. An example of this is a banking facility. The number of bank customers is discrete and only changes when a new customer enters the bank or leaves the bank after completing it. Continuous simulation is appropriate in the opposite spectrum for a system state that changes at a continuous rate where differential equations require mathematical computation. Fluids in a holding tank or fluid temperature are examples of a continuous system (Banks et al., 2007).

It is much smarter to use modeling software than to use a model presentation type to propose what will be simulated using a hybrid modeling approach. Using modeling software also reduces costs. Using AnyLogic (www.anylogic.com) simulation modeling tool is the best simulation modeling software for this research process. It allows modeling the three paradigms

and integrates System Dynamics, Agent-Based Modeling, and Discrete Event processing, which is then exported to a simulated environment presentation application. A recent study by Anderson (2016) completed in 2016 analyzed the complex modeling systems available for evolving system simulations and complex adaptive systems. His experiments concluded that the software was one of two modeling tools that successfully provided an extensible basis to support such simulation if further progress was made (Anderson, 2016).

This research will utilize the AnyLogic simulation tool as it is believed to be the best in displaying the simulation of smart contracts and Deep Learning and complex systems. Another study completed by Konczak, A., & Paslawski, J. in 2015, testing several simulation models for visual representation, concluded the same.

2.6 Recent Research

The concept of Smart Contracts to assist in the automatic process of security, trust, and time - to create a system where the digital assets of transactions are moved to a pre-specified rule for many purposes and encryption. This paper also addressed and identified the process of a complex system and the impact it can potentially have if more focus was embedded on the technology aspect of complex systems for the benefits of all organizations across the globe. Deep Learning can be used in the process of a complex system. An emphasis was also projected on the challenges in E-Commerce, Ethereum, and Cryptocurrency (Bitcoin). These topics are vital in discussing how smart contracts can enable the complex system to become a more efficient and reliable one using smart contracts in Blockchain (Kosba et al., 2016).

Smart Contracts can be used to solve the limitations of a traditional financial system or any system that creates financial transactions by tracking performance, reducing costs for the organization that turns into financial savings, and compliance in storing data in a highly secure system that is tamper-proof. The concepts behind the Smart Contracts such as self-checking, self-execution when terms match, and tamper resistance make Smart Contracts the best-automated data security process system. This helps organizations reduce reliance on untrusted intermediaries by eliminating third-party interferences and reducing transaction costs (Giancaspro, 2017).

Smart Contracts are placed to reduce the limitations of executing a third-party intermediary. This is the most significant focus on Smart Contracts' advantage, which reduces cost and processing time. For example, in a traditional transaction, a trust third party must be included in the sale transaction process of any goods or services such as purchasing an individual purchasing a vehicle from another individual. These individuals would need a trusted third party such as a Bank who can oversee the transaction process and act as an intermediary in the sale, as well as benefit from the sale by collecting fees or payment for the service rendered depending on the transaction type (Tasca et al., 2016).

In the Smart Contract world, the necessity for a third-party intermediary is removed, and the Smart Contract is then placed in the middle of the transaction as the trusted source of conducting the transaction without third party interference. The Smart Contracts verifies all information via nodes on the Blockchain network. If the Blockchain network agrees that all information is true and correct, the transaction is self-executed. The data is then registered and documented on the Blockchain network as a sale (Omohundro, 2014).

Kosba et al. (2016) analyze the ways a Smart Contract can be hidden from public view since it contains financial transaction information despite the security levels of a Smart Contract on a Blockchain. The purpose of this case was to find a way for a Hawk computer programmer to secure or retain the disclosure of financial information from the public using an operative cryptographic procedure where the prescribed individuals interrelate with the Blockchain by means of cryptographic primitives such as zero-information proofs (Kosba et al., 2016).

According to Watanabe (2016), the terms of Smart Contracts can reduce process time in any transaction due to eliminating the third party. There is a cryptographic apparatus placed on the Blockchain, which could be used to decrease the overhead related to manual data entry and verification process and overprocess time for the transaction (Watanabe et al., 2016). For example, in entering new data on a new customer or client on the Blockchain, the customer would be assigned and identified by a unique address or code. This code links the customer to their wallet, where additional data is stored or verified and linked to the client or customers' identity. This information is taken wherever the transaction is facilitated. If the Smart Contract needs data, it can pull and store the Blockchain's data and verify that information onto the Smart Contract (Watanabe et al., 2016).

To reduce processing time, this storage of data in the Smart Contract would house all the verified credentials; therefore, there would be no need for additional processing time in verifying additional documents. The benefits of Smart Contracts can be seen in this case as an advantage of utilizing the Smart Contract technology, which in return reduces time and cost to gather the necessary information needed (Watanabe et al., 2016).

Gatteschi et al. (2018) cover many aspects and advantages of the Smart Contract concept in a Blockchain and the benefit it serves specifically in reducing process time. For example, in the insurance industry, the Smart Contract is used to increase the claims processing process's speed time. Smart Contracts are also utilized to reduce the cost of any mistakes which happen or are associated with manual input of claims. This is proof of how Smart contracts have proven their excellence in utilization for privacy, cost reduction, usability, removing third parties, and security in other industries (Gatteschi et al., 2018).

The supply chain industry is another industry in which Smart Contracts can be used. The Supply Chain Industry is the collection of practices and procedures in which the business can transfer goods and products to the end-user being the consumer. Supply chains have become more complicated in recent years as a result of globalization. Every day the products we use and consume have parts and ingredients from all over the world. The best supply chain industry management allows organizations to minimize inventory use, cost reduction, and the time it takes to deliver goods to the open markets, enabling more flexibility in the company's entire production operations and activities. Good management of the supply chain can improve and optimize service flow in the most optimal way. They help to convey the value chain as it helps to understand people's needs to the provider. Today, both large corporations and small businesses rely on global supply chains to carry the products and parts that ultimately create their ultimate good (Bhandari, 2018).

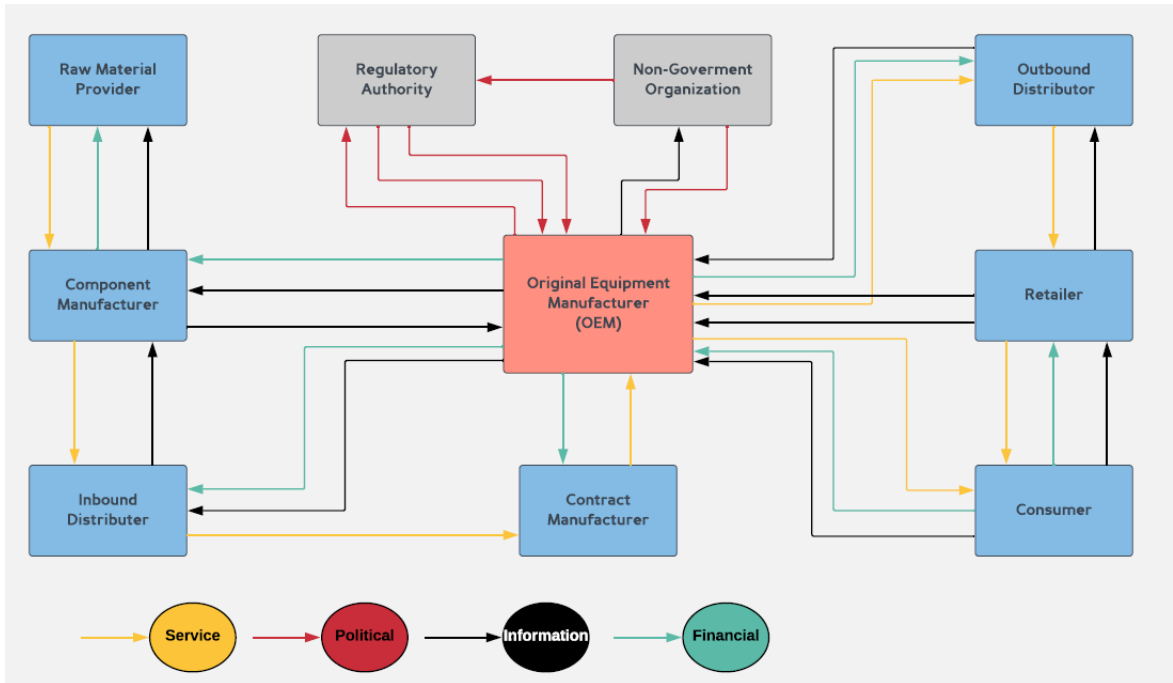


Figure 21: Traditional Generic Supply Chain

Figure 21 is an illustration that shows the current mapping in a typical generic supply chain. The mapping includes signing contracts, legalities, logistics, agreements, time schedules, project management, cost and financing, Original Equipment Manufacturer, Raw Material Provider, Component Manufacturer, Inbound Distributor, Contract Manufacturer, Outbound Distributor, Retailer, Consumer, Regulatory Authority, and Non-Governmental Organization, as well as stakeholders (Law, 2017).

Since the supply chain can be broken down into two main parts, the planning stage, and the execution or coordination stage, it all involves a high demand and supply level. The actual movement of the goods to consumers all are within the Supply Chain Management process. Below is an illustration that shows the elimination of all third parties by using Smart Contracts technology on the Blockchain and the Supply Chain after Smart Contracts are utilized in place of the traditional process. A case study completed by Angwei Law (2017) analyzes the Smart Contracts and the

application it serves in the Supply Chain Process and Management. The study claims that the utilization of Smart Contracts shows less waste in resources, high transparency among suppliers and buyers, a higher rate of trust in transactions and financial agreements, faster transaction time, and better internal reputation within each supplier (Law, 2017). Figure 22 shows the application of Smart Contracts in an open-source supply chain.

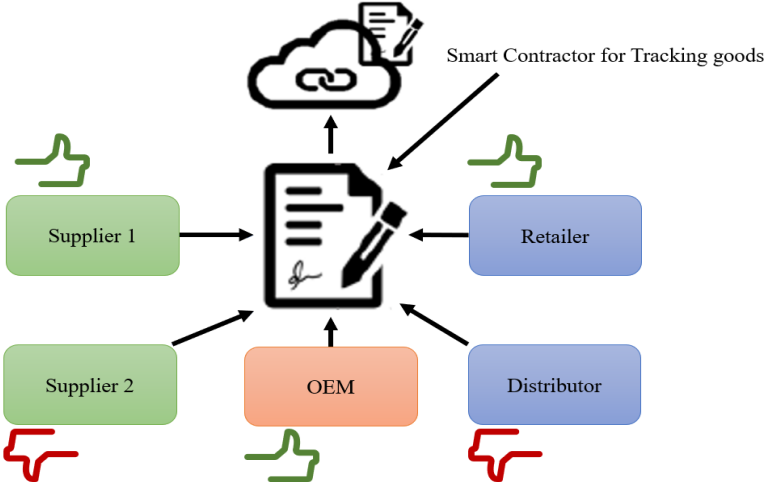


Figure 22: Utilization of Smart Contracts in an Open Source Supply Chain

According to Bahga et al. (2016), a Smart Contract will control the location of goods, the Leadtime, and handle all payments via Blockchain. By using Smart Contracts in the Supply Chain, it can handle the various exchanges between the different parties involved in the supply chain transaction process(es). The Blockchain and Smart Contract technology allows for a drastic change and improvement in the transparency, trust factors, and complexity and efficiency of the current supply chain process. Smart Contracts can also foster a more trusting and stronger business relationship among those involved in the business of the supply chain partners process; however, all of those are claims and not been tested (Bahga et al., 2016).

2.7 Gap Analysis

In this research, the Gap Analysis aims to analyze where necessary contributions are needed to contribute to the complete set of principles and knowledge. This research draws on previous work in supply chain systems, supply chain management, Blockchain, including Smart Contracts, which are processes and technologies that are complicated and need support in decision making. However, despite many industries already implementing Blockchain technology in their processes, no known studies assess and test the Blockchain application in the Supply Chain. There is a lack of comprehensive work in blockchain, security, and transparency (i.e., the next frontier to optimize and make the supply chain lean and secure). Simulation and deep learning can be the core of a decision-making platform to assess Blockchain's implementation in a supply chain.

After reviewing the literature, there are published research articles that discuss the importance of supply chains and Blockchain. The supply chains and its developments are essential to industries that want to improve the processes and effectiveness in the daily functions of the supply chains. For instance, a research study that was done by Zhang (2019) studied the elements of the supply chains and the essential role it plays for any organization. Also, another research that was done by Swift et al. (2019) revealed that supply chains play a critical role in many fields, and it is important for business efficiency and logistics.

On the other hand, according to a recent research study that was done by Karame & Capkun (2018), Blockchain is a new and promising technology that is believed to address several security issues in the supply chains. Blockchain technology can offer several possible advantages and benefits in the supply chain systems (Bryk, 2017). Transparency, security, and trust are some of

these advantages that the Blockchain can offer to the supply chain systems. However, there is still a concern regarding the utilization of the Blockchain in the supply chains based on the literature review, as it creates doubts about whether it can provide what the Blockchain promises to do. Recent studies have addressed the theories and implementation of Blockchain in the supply chains and their effects, but no study has been found to assess the implementation of Blockchain in the supply chain (Allayannis, 2017; Bagha et al. 2016; Law, 2017).

Throughout the literature review, we were unable to find any research that assessed the Blockchain's implementation in the supply chains, which led to the research gap, as shown in Figure 23 below.

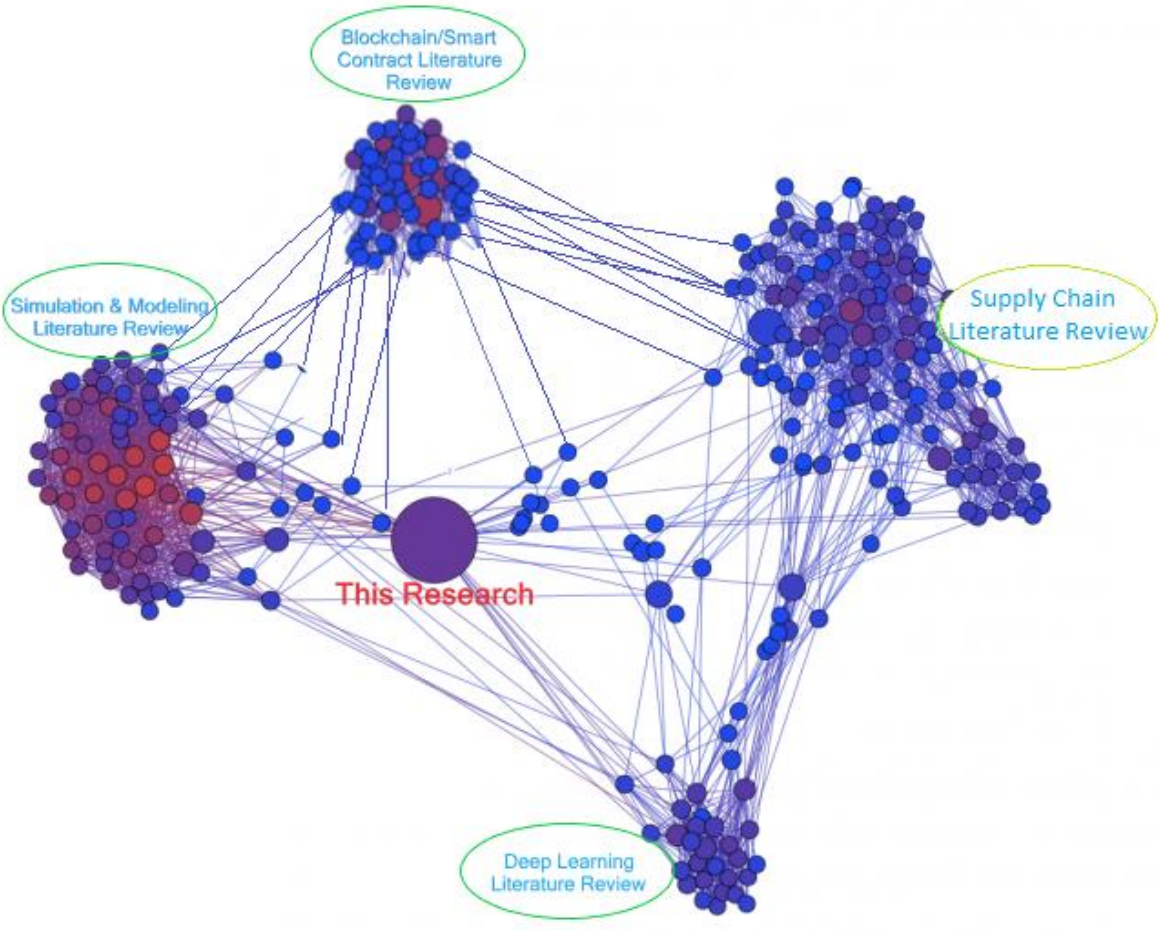


Figure 23: Relationship map of Literature Review

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the research methodology to develop and build a new decision-support system and justify and analyze blockchain implementation in supply chain systems using deep learning and agent-based simulation.

3.2 Research Methodology

A research methodology involves all practices, procedures, and approaches used in research, which is concerned with many ordered activities to be carried out. This research is conducted following the High-Level Research Methodology Chart shown in Figure 24, which shows the process and progress of this research. This research methodology includes different elements that include research ideas, literature review, gap analysis, methodology development, case study, an evaluation of the system simulation, validation of the research, and conclusion.

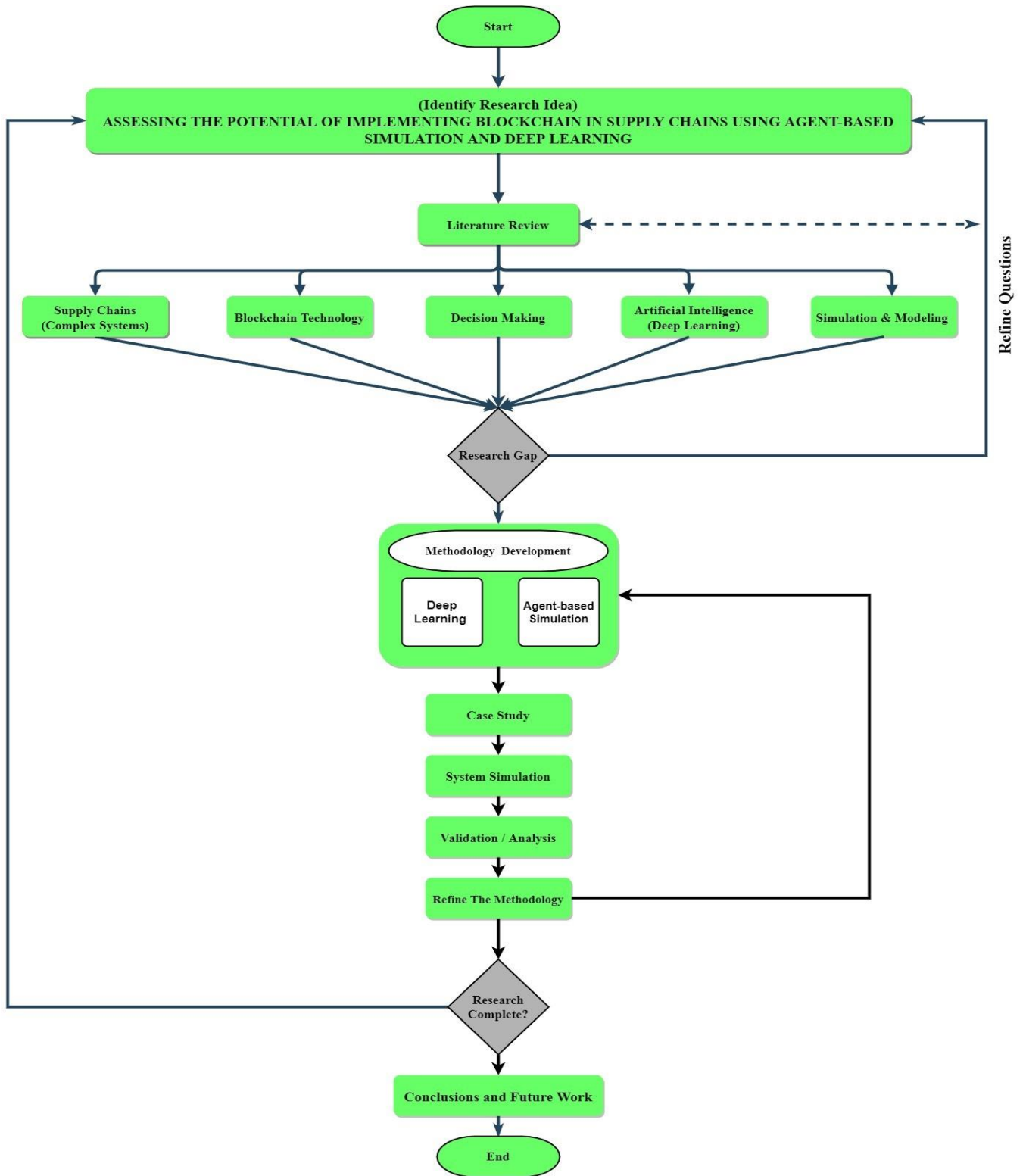


Figure 24: High-Level Research Methodology

3.3 Research Idea

This research idea stemmed from extensive research on Blockchain technology and supply chains. Supply chains are complex systems and have some challenges. Organizations are continuously developing their supply chains to remain competitive in the field. On the other hand, blockchain is an evolving and promising technology that claims it can enhance transparency, building trust and reputation between various entities, and traceability in data. The combinations of the two topics led to the following scenario, If the blockchain is implemented into supply chains, then will it:

1. Increase traceability?
2. Increase Transparency?
3. Improve data sharing?
4. Improve customer experience?
5. Improve trust among participants?
6. Detect and make decisions about unreliable suppliers?
7. Reduce risks and the potential for fraud, hackers, and security breaches?
8. Increase the supply chain visibility to help the organization react faster?

3.4 Literature Review

The next step, after getting a clear research idea, was to go through the literature and have a deep knowledge of the previous effort made and then begin to build on the previous knowledge. To establish a strong foundation in this research area, the literature review started on three areas directly related to this study: 1) Supply chains; 2) Blockchain technology, and 3) Decision making. The literature found that blockchains are hard and complicated to implement; therefore,

visualization and assessment tools are needed, which added two more research areas to the literature: 1) Simulation and modeling and 2) Artificial intelligence. Reviewing, understanding, and analyzing the literature led to and identified this study's research gap.

3.5 Research Gap

After reviewing and analyzing the literature, a research gap was identified. The research gap was there is no methodology to assess blockchain's implementation into supply chains. The current research and efforts are about how to implement the blockchain into supply chains and what it can offer. We are going to build a methodology to assess the implementation of the blockchain into supply chains.

3.6 Methodology Development

This dissertation proposes to build a methodology to justify and assess the implementation of blockchain into supply chains. The methodology provides a means of testing supply chains in the following elements: data sharing, planning decisions, performance evaluations, infrastructure enterprise (web), revenue sharing, business process integration, organizational culture, leadership style, accounting and cost control, information system and technology (IT), and communication, and joint planning. The methodology should be able to manage complex systems because supply chains are complex and implementing blockchain into it will add more complexity. To be able to fulfill the research gap with a suitable methodology, the steps below are needed:

- Identify all stakeholders(entities) in the system.
- Identify internal and external factors that influence the performance of the supply chain.

- Specify interactions between entities in supply chains and blockchain.
- Identify the behaviors of the entities and the system as a whole.
- Identify the function, needs, and objectives of each entity.
- Identify whether the system is stochastic or deterministic.
- Identify the causal relationship between entities.
- Identify success factors.

After these steps and analyzing the proposed system, agent-based simulation and deep learning will be a potential methodology to assess blockchain implementation into supply chains. However, this will be explained more in Chapter 4.

3.7 Case Study

To further examine and validate the research idea, it is essential to use a case study. According to Turner & Danks (2014), “The utilization of case study research is an effective way to identify the strengths and opportunities for the improvement of organizational procedures, policies, processes or programs. Case study research provides evidence of new emerging theories and helps to make sense of real-world problems”.

3.8 System Simulation

The simulation environment is essential due to the logical and symbolic factors that are present between entities or components. Thus, simulation modeling can be used both as a tool analysis to predict the effects of existing system changes and as a design tool to assess a new system's performance under various sets of circumstances. As explained in the methodology development

section, Agent-based simulation will be utilized as a simulation tool, and more justifications will be covered in Chapter 4.

3.9 Validation and Analysis

For effectiveness and accuracy, the results of the case study will be analyzed. Also, if applicable, the proposed structure will be refined and formed from the results attained from the case study. A sure way to establish a simulation model's validation is to compare the simulation results to historical data and test data that hasn't been used. According to Law (2009), "Validation is the process of determining whether a model is an accurate representation of the system, for the particular objectives of the study." Besides, the simulation model results will be assessed by the following criteria:

1. **Usefulness:** Observing if the model's applicability and usefulness in design will allow for the following evaluation methods 1) assess and forecast the effects of different strategic scenarios in the model 2) Witness the actions of the agents in response to drastic variations during the simulation, 3) observe model behavior when extreme parameters and input variables are set 4) analyzing model tasks and model goals, 5) Observe progression within the simulation
2. **Representation of Reality:** Evaluation of a simulation model should include representation of reality to evaluate if the models make mathematical and logical meaning or sense. Evaluating the simulation model is critical to determine if the model will behave as closely as reality should or cause a limitation.
3. **Scalability:** Choosing scalability as a performance metric by analyzing the direct relationship between the interacting components, the transition time of a simulation path, compared to the number of simulated entities, determines the model's scalability. (if the

simulation model grows, the scalability will be determined by accommodating a partitioning strategy)

4. **Replicability:** Replicability is vital in determining if a system is running identically to its prototype. Comparing the results from a replicated simulation determines the replicability of a model. A replicated simulation model can achieve an entirely matching result in all variables as those found in the original simulation model (prototype).
5. **Uniqueness:** In modeling agent components, simulating the model is unique in its form. The simulation model is analyzed and validated using simulation programming language and software, utilizing simulation concepts and inputting experimental parameters and decision-making metrics. Figure 25 is the model validation methodology and simulation process for this research.

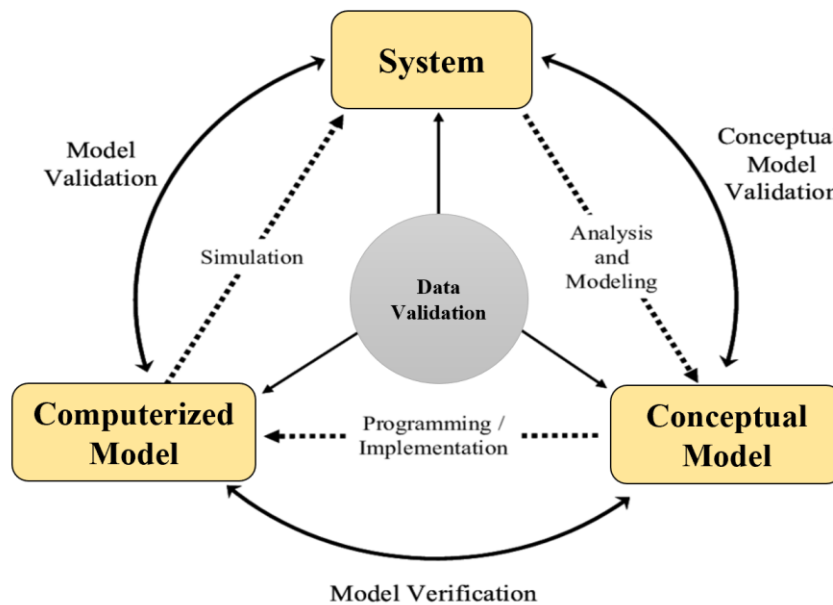


Figure 25: A model validation methodology and simulation process

3.10 Conclusions and Future Work

The conclusions of this research will include a summary of an in-depth comparison of the simulated models. Also, general and final conclusions about the proposed methodology will be illustrated. The conclusions section will also include the contributions to the body of knowledge, the research limitations, and further research that needs to be conducted.

CHAPTER 4. DEVELOPMENT OF METHODOLOGY

4.1 Introduction

The methodology aims to assess the strategic approach and guide in analyzing the actors/agents' respective interactions. This chapter provides a methodology that uses a core simulation environment to support the assessment of Blockchain's implementation in supply chains. As described in the literature review, a methodology to assess and analyze its validity does not exist.

4.2 Proposed Methodology

The proposed methodology consists of an approach to characterize and assess the implementation of blockchain into supply chains for the desired analysis. The methodology selection and its development are motivated by the research objectives defined in chapter 1. The major components of the proposed methodology are:

- Supply chains, including stakeholders' identifications, system characterization, and supply chain challenges.
- Blockchain, including component identifications and smart contracts.
- Simulation, including justification of a suitable tool.
- Artificial intelligence and the justification of the suitable technique.

4.2.1 Supply Chains

Success can be challenging to attain in a growing global economy. Integrated and strong supply chains will power any firm in the competitive industry forward. The global concept of streamlining a process effectively is essential to establish an efficient supply chain. A supply chain

comprises vendors, producers, distributors, wholesalers, and retailers who collaborate to accomplish common objectives. If proper tracking is absent from a supply chain, it poses a great challenge to validate the transfer, receiving, and destination of goods. This causes additional delays and derailments throughout the chain management process and damages internal and external operations (Emmett & Crocker, 2016).

Managing a supply chain is essential for companies who want to gain a competitive advantage in their corresponding industry. Using the Supply-Chain Operations Reference (SCOR) model in the supply chain allows for a comprehensive review of supply chain activities, efficiency indicators, continuous improvement, and optimization operations.

Supply chain visibility allows suppliers to check a company's inventory in real-time, which can help plan ahead for future fulfillment demands. A decrease or unfavorable changes in the supply chain can greatly affect a company's productivity and profitability. Supply chains need to be sufficient to meet customers' needs as rapidly as possible (Packowski, 2013). The complexity of any supply chain often varies depending on well-established standards to function properly. If these areas are threatened by increased competition or external instability, the quality and effectiveness of delivering products can struggle (F. Persson et al., 2012).

4.2.1.1 Stakeholder Identification

A stakeholder is a person who has involvement in a company that can either impact the business or be affected by it. The primary stakeholders in a traditional company are its owners, workers, consumers, and suppliers. In the lending industry, an excellent benefit for stakeholders is unity with the company; therefore, a widely recognized software that all stakeholders can use to

update important supply chain data can also benefit from the use of technology in the supply chain in the lending industry (Scheibe & Blackhurst et al. 2018). Technology such as automating critical supply chain processes can reduce and redesign inconsistencies within the supply chain and improve efficiency. A company's consistency standards can be achieved while adding value to the company when services are constantly being made available (Mishra & Sharma, 2014). The Lean and Six Sigma SIPOC (suppliers, inputs, process, outputs, and customers) method recognizes manufacturers, supplies, procedures, outputs, and consumers, offers a realistic solution for process improvement practice in a supply chain, and can help determine where deficiencies are located. SIPOC is a tool to recognize key components of a process from its vendors to its consumer.

4.2.1.2 System Characterization

The technology and system characteristics of e-commerce in the Peer-to-Peer (P2P) platform is becoming more apparent, and individuals have become connected. Businesses and consumers want their activities streamlined, and new market possibilities should be explored. The system characterization of an e-commerce economy consists of all business-related transactions in selling, buying, and or exchanging products or services in a virtual setting via a communication network (Bruce & Neely et al., 2002). An e-commerce platform is a data system that handles data and generates information 565 that facilitates the electronic transactions and activities and operation of an organization. There are four infrastructures for e-commerce networks; 1) vendor servers (e-catalog), 2) architecture for SET (e-payment function), 3) open market exchange (product information and order fulfillment), and 4) architecture for Open Buying on the Internet (OBI) (selection of supplier) (García-Cáceres, & Escobar, 2016). An ideal e-commerce model

should be a structured transaction that can provide an e-commerce network with an accurate, fail-free, and reliable transaction processing environment.

4.2.1.3 Supply chains challenges

Based on the literature review, Supply chains face several challenges, as shown in Figure 26.



Figure 26: Challenges in the Supply Chains

The supply chain consists of various compartments, including product design, product manufacturing, quality product production, and logistics. Supply chains have faced growing complexities in developing and sustaining a secure and reliable supply chain system. Each supply chain component interacts with one another, which can pose many challenges in possessing a streamline of processes and capacities in which they communicate (Santiteerakul et al., 2015). Some challenges the supply chain faces are cost inefficiencies, centralization, information sharing, hacking, lack of trust, lack of transparency and traceability, etc.

4.2.1.3.1 Cybersecurity

Supply chains offer a foundation for a vulnerable link for cybersecurity as the security controls taken by supply chain partners are not necessarily regulated by entities. This can offer cyber-criminals and hackers the opportunity to infiltrate an entity or organization by first invading a supply chain through many channels. One channel is by vulnerabilities in software platforms. Malicious hackers can detect applications and networks. Another track is by hacking the supply chain network by installing hardware encryption that comes with malware already configured on it. By using these vulnerabilities, hackers may manipulate and access other supply chain activities and components (Sturges & Norton, 2013). Supply chains currently utilize intrusion detection system (IDS), or intrusion prevention system (IPS) software, both in an attempt to control and monitor cyber threats and attacks or possible hacking operations in the supply chain network system. Figure 27 illustrates the utilization of a Network-Based Intrusion Detection and Prevention System in a supply chain.

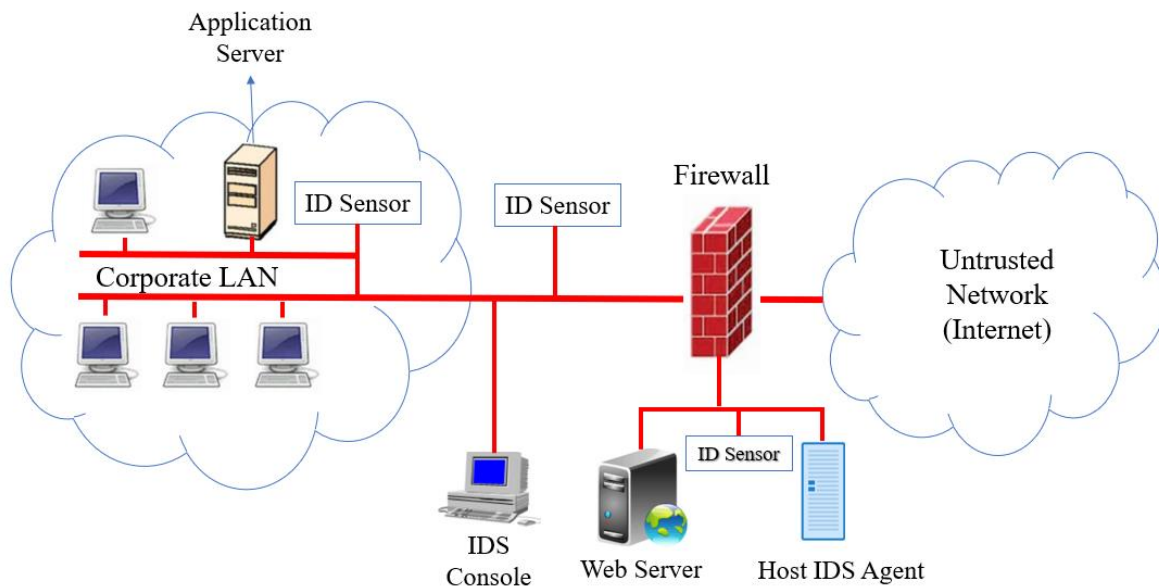


Figure 27: Network-Based Intrusion Detection and Prevention System

The role of an intrusion monitoring system is intended to protect the core security net principles such as privacy, credibility, operational efficiency of a network. Data breaches are today's main concern for all organizations. The scale of expense for the breaches continues to grow and negatively impacts organizations, which can impact it on a global level and cost \$3.62 million for just one breach and rising. Network security and consumer trust are also highly relevant for any company further than the financial ramifications. An attack can undermine the customers' confidence in the company and impact its image.

Precautionary security procedures such as firewall protection (for example, system encryption and blockaded zones) and protected variants of network control systems parameters have been formulated and implemented or introduced to defend control systems networks from security and network intrusions. Different criteria must be met when monitoring suspicious activity

and normal behaviors of a system (Hossain, E. et al., 2019). Intrusion detection and prevention systems are both distinct terms that describe data security protocols for implementation that are used to minimize strikes, threats, and block emerging risks. Recognizing how intrusion detection and prevention systems function is essential to keeping companies in many different industries, data, and network systems secure in our current times of potential threats that can come from any source. Despite their advantages, both types of monitoring systems have significant limitations, which indicate that threats escape detection.

4.2.1.3.1.1 Intrusion Detection System (IDS)

Intrusion Detection Systems (IDS) are routing algorithms that track and control network traffic and produce "trigger alarms" for actions that either fit recognized trends of suspicious activities or are not in the system standard of processes. An intrusion can happen in many ways on a network (Butun & Song et al. (2019). The intrusion operation involves disrupting the normal flow and overloading it with data, acquiring network information to invade it from a future vulnerable moment, or introducing information into the network to distribute and obtain control from inside. IDS may be network dependent or host-dependent. The information which is obtained anomaly is based on methodologies, rather than identities. An anomaly-based process uses identities or reference points that characterize the typical actions or behaviors of programs, server links, hosts, and users of the network and contrasts them to the actual activities to distinguish major variations. The signature-based method is another approach used in the Intrusion Detection System (Gharib & Sharafaldin et al., 2016). The signature-based process evaluates known malicious behaviors and trends (signatures) to the information collected or processed packets to identify potential invasions using comparative analysis. The third type of detection approach is the

Stateful protocol analysis, which detects abnormal responses in the network using fixed standardized profiles dependent on acceptable behavior and responses or abnormal activity or responses.

There are many disadvantages in utilizing these methods or approaches. Table 3 below lists the disadvantages of using these types of detection approaches in intrusion detection systems.

Table 3: Disadvantages in using these types of detection approaches in IDS

Intrusion Detection System (IDS)	Cons
Signature-based methodology	<ol style="list-style-type: none"> 1. Operates exclusively to common threats 2. Restricted to one event or behavior at a time 3. Does not work on variations
Stateful protocol analysis detection	<ol style="list-style-type: none"> 1. High in overhead, which exhausts resources 2. Cannot detect attacks that do not violate the attributes of commonly recognize system conduct 3. Conflicts within IDPS protocol layout and how protocols are currently applied
Anomaly-based method	<ol style="list-style-type: none"> 1. Large rate of false positives 2. Susceptible to invasions during the time of 'learning.' 3. Capability to be tricked over time by perfectly executed attacks 4. Difficulty in setting rules 5. Difficulty in assessing why incidents activated admin warning

4.2.1.3.1.2 Intrusion Prevention Systems (IPS)

Intrusion Prevention Systems (IPS) function protect network and data resources, inhibiting threats and intrusions, and protecting intangible resources for any company that relies on network security (Vuppala et al., 2016). The existence of an IPS device would not influence the normal

activity of the network. Intrusion Prevention Systems intended utilization on a network means restricting suspicious behavior or malicious data from connecting to the network and taking prompt remedial measures in relation to a potential attack or intrusion. Integrated and reflexive reactions can be immensely beneficial for organizations. However, there is a need for an intensive configuration and surveillance, which is necessary to ensure potential threats in the systems are automatically stopped (Agarwal & Hussain, 2018). There are four major types of systems for preventing intrusion, which has been designed.

1. Network-based intrusion prevention system (NIPS) screen the full network and scan for unusual activity by examining protocols' behavior.
2. Wireless intrusion prevention systems (WIPS) manage wireless networks by examining the wireless networking protocols for unusual behavior
3. Network behavior analysis (NBA) analyzes network congestion in an attempt to detect potential risks that trigger abnormal behavior in network flow, such as distributed denial of service (DDoS) intrusions and threats.
4. Host-based intrusion prevention (HIPS) scans the network for abnormal behavior or potential risk inside a single host.

Table 4 lists the disadvantages of the types of preventions used in the Intrusion Prevention System.

Table 4: Disadvantages of the types of IPS

Intrusion Prevention System (IPS)	Cons
Network-based Intrusion Prevention System	<ol style="list-style-type: none"> 1. High rates of false-positive and false-negative 2. Cannot recognize encryption 3. Not functioning properly during heavy loads
Wireless Intrusion Prevention System	<ol style="list-style-type: none"> 1. Cannot account for insecure or poor wireless standards 2. Cannot monitor application layer, transport layer, and network layer protocol behaviors
Host-based Intrusion System	<ol style="list-style-type: none"> 1. Delays observed in an alert generation 2. Unified reporting may interfere with existing security measures
Network behavior analysis	<ol style="list-style-type: none"> 1. Delay in recognizing intrusions 2. Does not allow for real-time flow

4.2.1.3.2 Transparency

Transparency in the supply chain allows enterprises to know the processes and activities in an upstream way. And to be able to share their data both to internal and external components and entities of the supply chain, which will encourage trust as well (Munir & Chatha et al., 2020). Shifting trends in technology and consumer expectations require industries to become even more transparent and build credibility, sustainability, and strategic goals across entities, which will produce more trust in the supply chain. Internal and external electronic transmission of communication enables trust to be established in the supply chain. Not having transparency and trust in the supply chain will cause the organization's image to suffer, decrease credibility, suffer in reputation, and increase costs for all supply chain entities. The supply chain should be transparent in terms of where users will measure product quality and the ethics of the goods produced.

The supply chain must be transparent as it can develop trust within entities and help them navigate risks. If there is transparency in a supply chain, it can eradicate dependency on foreign entities to promote trust (Kozma, 2017). Some of the benefits of facilitating transparency supply chains are improving the integrity and public confidence of shared data, minimizing the adverse risk of misconduct or fraud in public relations for companies, and encourage a take on approach for stakeholders. Figure 28 illustrates the transparency and trust implementation in the supply chain.

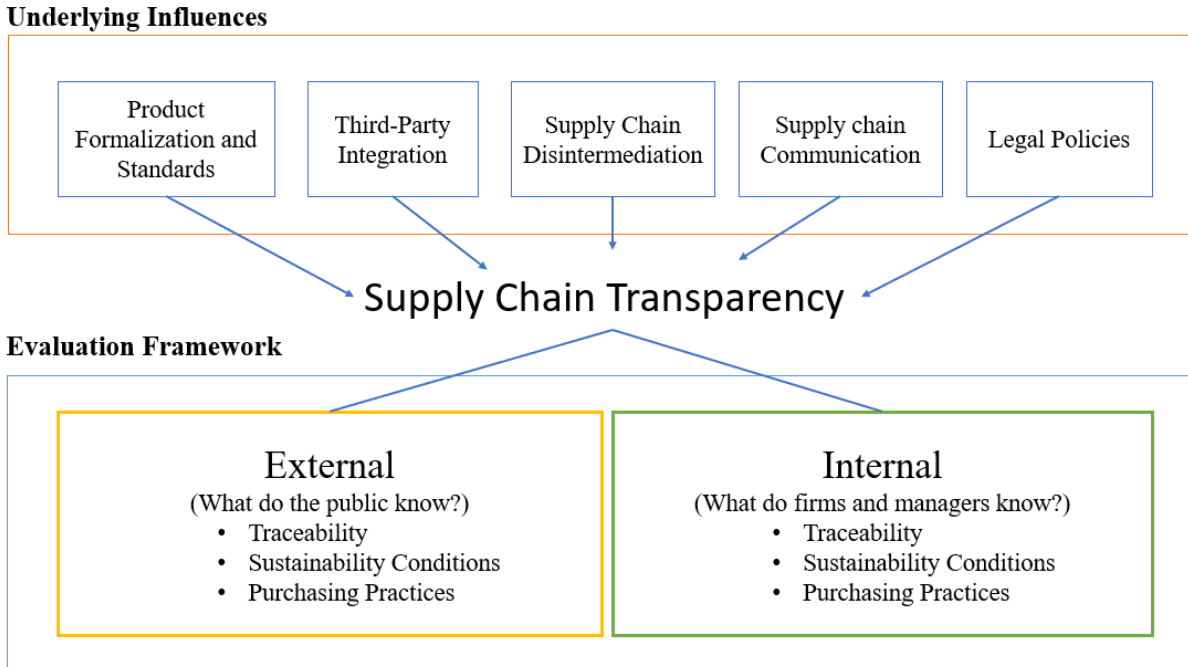


Figure 28: Implementing Transparency and Trust in the Supply Chains

4.2.2 Blockchain

A smart contract is a blockchain system consisting of a series of contracts, a digital network, protocols, and parties that have been implemented. The smart contract agreements are written between the parties involved using digital code and is executed when the conditions are met and incorporated into a blockchain network. An example of blockchain platforms is Ethereum, which includes accounts, and the network captures the interaction on the ledger for any occasion, and trade occurs among accounts (Saraf & Sabadra, 2018). To implement a smart contract, the interested parties must accept the opportunity to work together. After that, each must set and decide on the terms and conditions required to exchange products or services. The contract and its terms are written using computer code and deployed to the blockchain where either the relevant parties

or certain events can execute it. Figure 29 illustrates deploying the smart contracts to the blockchain.

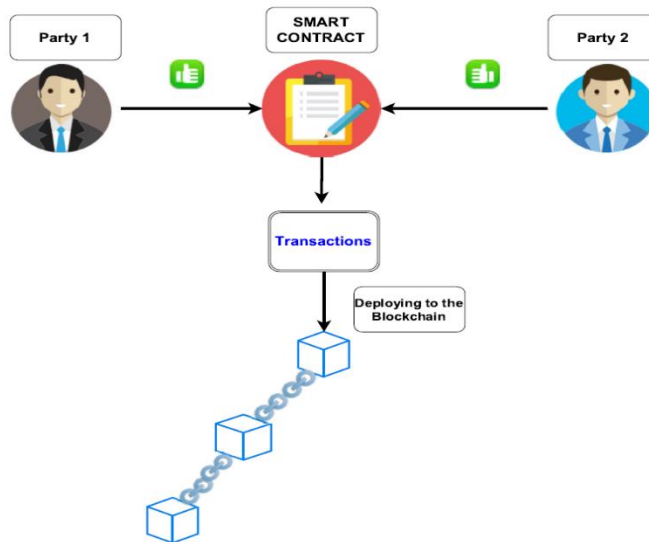


Figure 29: Deploying the smart contracts to the blockchain

4.2.3 Simulation

4.2.3.1 Justification of using Agent-based simulation

Agent-based technology is a computing paradigm where agents can perform tasks such as planning, decision-making, and reasoning. Those agents may be people, products, companies, software, or anything relevant to the system. Besides, they work independently or coordinate with each other to achieve tasks. The agent-based simulation agent has both methods (rules of interacting between the entity and the other agents) and attributes (features that control the interaction between the entity and the other resources in the system). In the proposed system, the

agent-based simulation will be a better fit than different paradigms such as Discrete event simulation and System dynamics for the following reasons:

1. Complex and stochastic system: The elements that define a supply chain's complexity rely on the operation between many interacting entities or agents. An agent is represented by anything that can act on the perceived data. An agent is an autonomous entity that can decide how it acts based on experience and can make decisions by different actions. An agent can also be motivated by rules and goals. The entities (agents) in a supply chain include suppliers, vendors, warehouses, manufacturers, stakeholders, business transactions, logistics, distribution, and retailers. Also, Blockchain technology contains technological elements that create a block on the blockchain. These pillars are complex within themselves and include cryptographic hash, header, digital signature, timestamp, transactions (Merkle tree/binary hash), and nodes (can take on different roles within the blockchain system). Other elements of a blockchain are hackers (agents). These components of the block in a blockchain also make the Blockchain a complex structure.

Each of these entities (agents) or components serve a function in the supply chain such as finance, operations, customer service, product development, and marketing. Supply chain performance can be measured using qualitative and quantitative techniques such as customer satisfaction, flexibility, data flow, product flow, risk managing, supplier performance, cost, stock levels, sales volume, profit margin, and return on investment.

Each of the components of a supply chain (agents) has different needs, objectives, and decision-making behaviors. The elements that make up a supply chain have different characteristics, considered to have diversity and countable entities. The elements act differently in both a social and physical environment. The behaviors displayed by these components or

entities(agents) are considered stochastic, which means their behavior is unpredictable. Discrete-event simulation (DES) contains no interactive entities that carry intelligence. Instead, the entities move through a pre-determined process. In System Dynamics (SD), no representation of these entities can be found. System Dynamics uses a “top-down” approach to modeling, which cannot be suitable for complex systems as it will be unable to model the diversity of a supply chain. Therefore, it is concluded agents can act on behalf of the stochastic components in an agent-based simulation. Using agent-based simulation is most suitable for this type of proposed system. Figure 30 below shows the complexity of implementing blockchain in a generic supply chain system (which contains one entity of suppliers of raw materials, manufacturer, OEM, distributor, retailer, consumer, and other components).

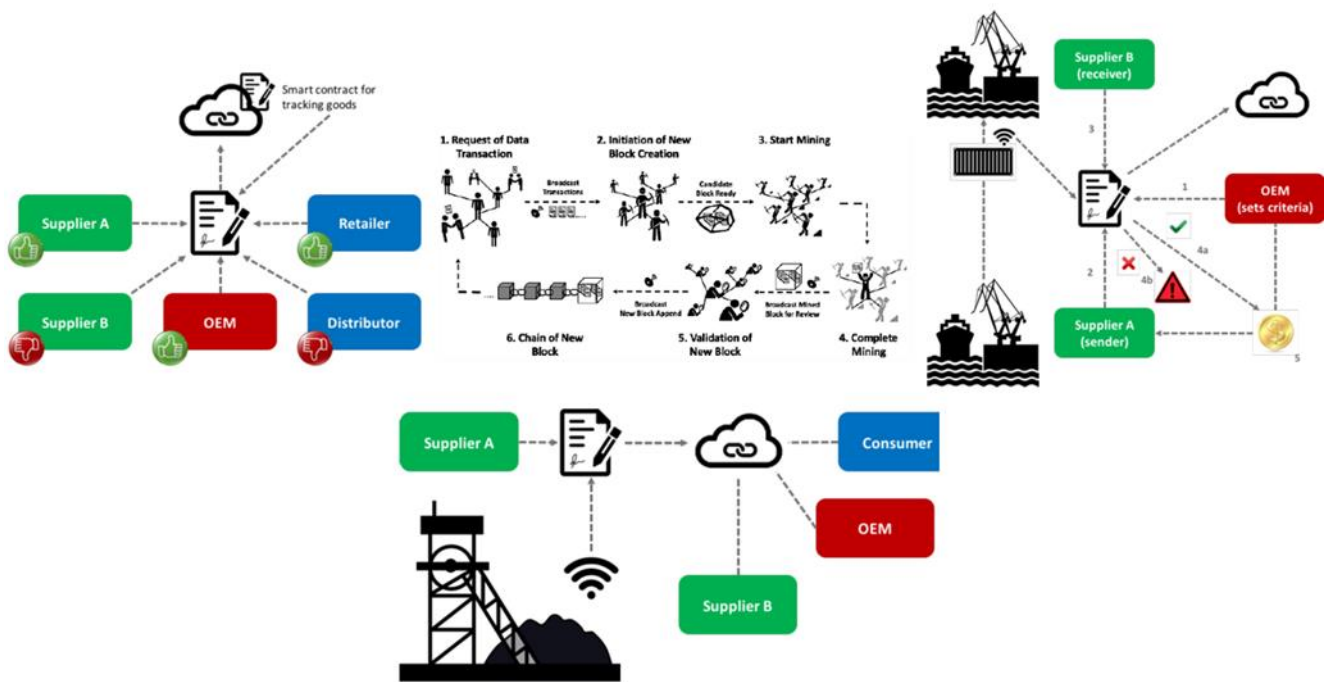


Figure 30: Complexity of implementing blockchain in a generic supply chain system

2. **Relationships between entities:** Implementing blockchain in the supply chain displays there are more entities involved and relationships that need to be addressed, which leads

to more complexity, such as entities behaviors (reputation), more interactions between entities, and provenance. For example, adding blockchain technology to a generic supply chain system (contains one entity of supplier of raw materials, manufacturer of individual components, OEM, distributor, retailer, and consumer) requires three smart contracts: to determine the provenance of goods, to track the progress of goods, and to build trust between the supply chain partners including their reputation. Each of these contracts produces new relationships, functions, entities, and interactions. There is a need for building trust and healthy relationships and interactions among stakeholders and all supply chain components. For instance, adding smart provenance contracts to a supply chain system will include the following relationships and functions:

1. Add a smart contract administrator
2. Allow each entity to record their details to the blockchain
3. Allow the administrator of the contract to add and remove a supplier
4. Verify that the supplier is certified and legitimate
5. Add and remove products from the supplier and the administrator
6. Allow any entity to display the details of the product and the transaction

These relationships add the emergence property to the proposed system. None of these characteristics can be allocated to a particular entity, but they are the outcome of the systems' actions and behaviors. The interactions between the components of a supply chain require various relationships consisting of participants and resources. The relationships found in a supply chain have the primary goal of building and maintaining those relationships and are also considered agents in a supply chain. For example, manufactures must maintain relationships with distributors, distributors towards manufacturers, distributors towards retailers, retailers towards distributors and consumers, and stakeholders towards consumers. In a blockchain system, the components work

together as autonomous agents that work independently and carry their characteristics and can make decisions without being influenced by other components.

A node (user/agent) in the Blockchain system interacts with non-system entities, such as when a user enters a financial transaction or when a user/agent sends or obtains money via an

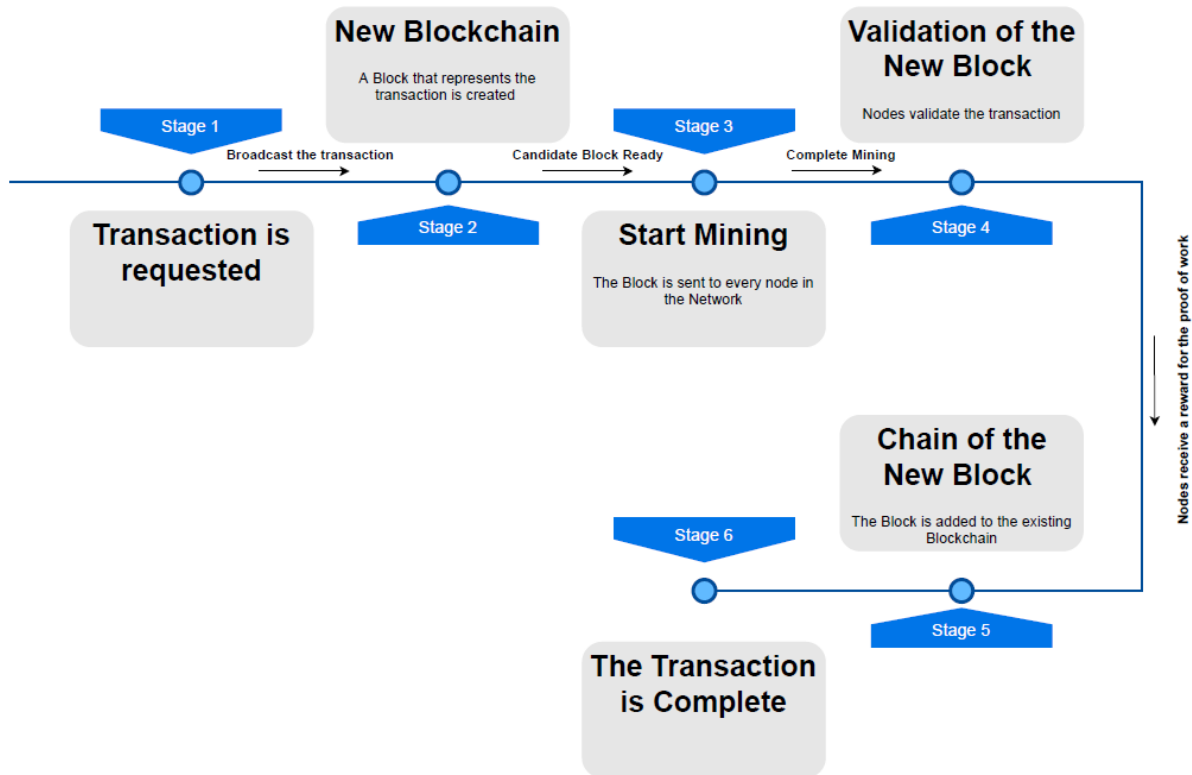


Figure 31: Process of creating a block on the blockchain

internet platform. These interactions also occur when funds are cashed in or out for buying or selling a transaction. Figure 31 below illustrates the relationship and interactions between a blockchain system's components in what it takes to create a block on the blockchain. Miners and the validators are also considered agents in the blockchain system. Therefore, it is concluded that using an agent-based simulation would be the best fit for our proposed approach.

3. **Time between actions (dynamic system):** Supply chain entities and blockchain elements can be modeled using agent-based technology to capture the interactions among several elements over time. Social entities and physical properties of a supply chain create an adaptive system. The changes occurring in one entity of a system can impact all other system components. The structural changes, such as new resources and suppliers to the supply chain, can cause change over time in its environment. Due to the structural and socio-technical changes (components that are active in both the social and technical side of a complex system), the adaptive supply chain system can change over time, making it a dynamic system.

For instance, a supplier's reputation score can be calculated and updated in the reputation smart contract as more transactions are made. This contract will encourage suppliers (agents) to establish and maintain a good reputation with manufacturers (agents) and help the system prevent or minimize transactions with low-reputation scores. Time handling using agent-based simulation is regarded as discreet, while time handling is continuous in System Dynamics. Therefore, using agent-based simulation for time entity is more suitable for this proposed system.

4. **Causal Relationships and Loops:** Causal relationships are the causation factor and degree of relationship between two components (agents). A causal relationship between two entities (agents) exists if the existence of the first entity or agent causes the other entity or agent. The causation of a causal relationship can be looked at as a cause and effect of related factors. For example, in the proposed system, when analyzing cyber-attacks, a causal analysis conducted may reveal an influence on the reasons for loss of security. This security loss could be matched with managing countermeasures to prevent future attacks and improve the system's operational and technological performance. A causal loop is another way to prove that there are causal

relationships in the supply chain entities (agents). A causal loop is a method to visualize the variables that influence each other in documenting systemic thinking, hence creating a dynamic system. However, agents can cover causal relationships as equal to system dynamics. Causal relationships exhibit correlations, influence, interactions, and consequences in a supply chain between entities (agents). Therefore, the agent-based simulation would be best suitable to model causal relationships in a supply chain due to the commonality of agents representing entities.

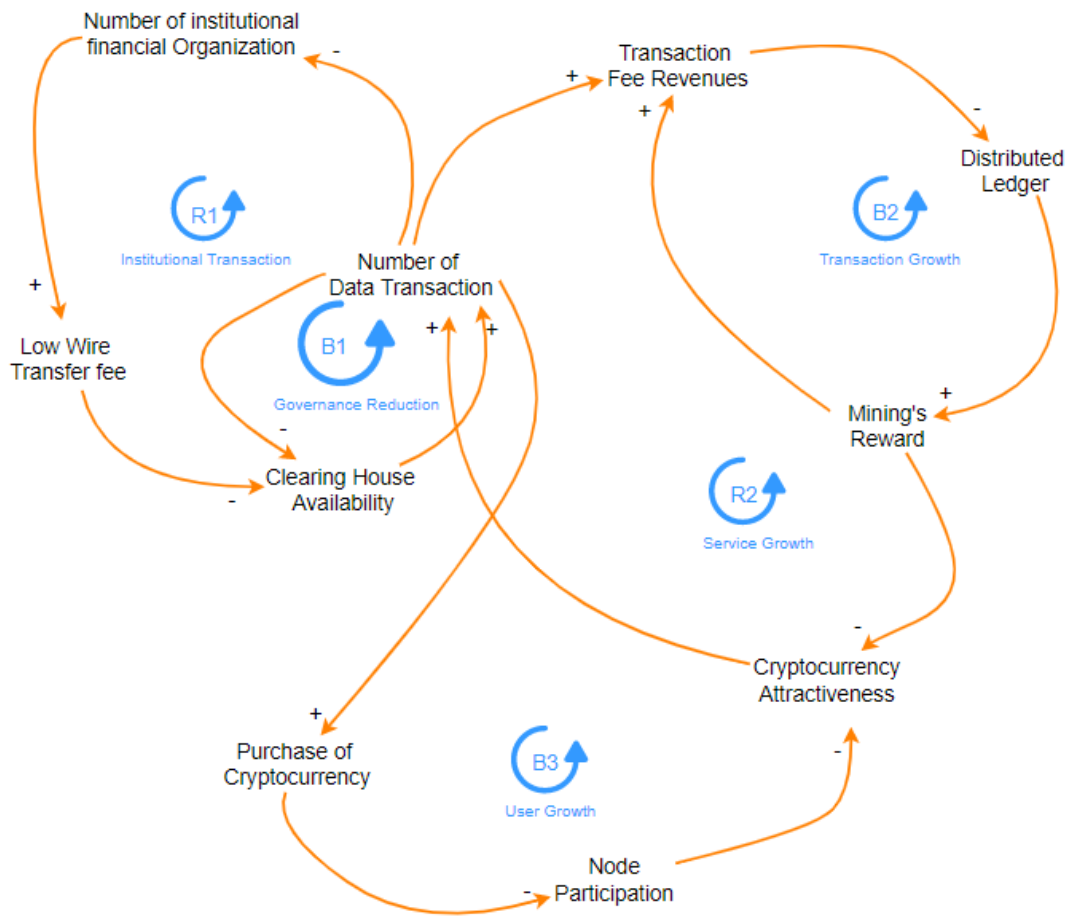


Figure 32: Causal Loop / Relationships of an Autonomous Operation in Blockchain

Figure 32 above illustrates a complex causal loop diagram that shows how diverse variables and components of a blockchain in a supply chain affect each other. It also depicts the connection between the system and its operating environment and interconnections among its components. The causal loops above display the variables linked by arrows representing the variables' causal effects if the variables change.

4.2.3.2 Agent-based Simulation

The concept of process mapping is essential in this research since it allows for a visual representation of the functions of events and objectives that must be completed for a simulation study. This process map displays the many processes and illustrates the interconnections from a practical aspect, and use the map to create a representation of each work process in designing and analyzing the system for agent-based design.

Set of rules such as statecharts, process flow, equations, and schedules form a simulation model. Those rules are statements defining operations and constraints that configure the overall system behavior. The steps for conducting a simulation study are shown in the flow chart in Figure 33 below.

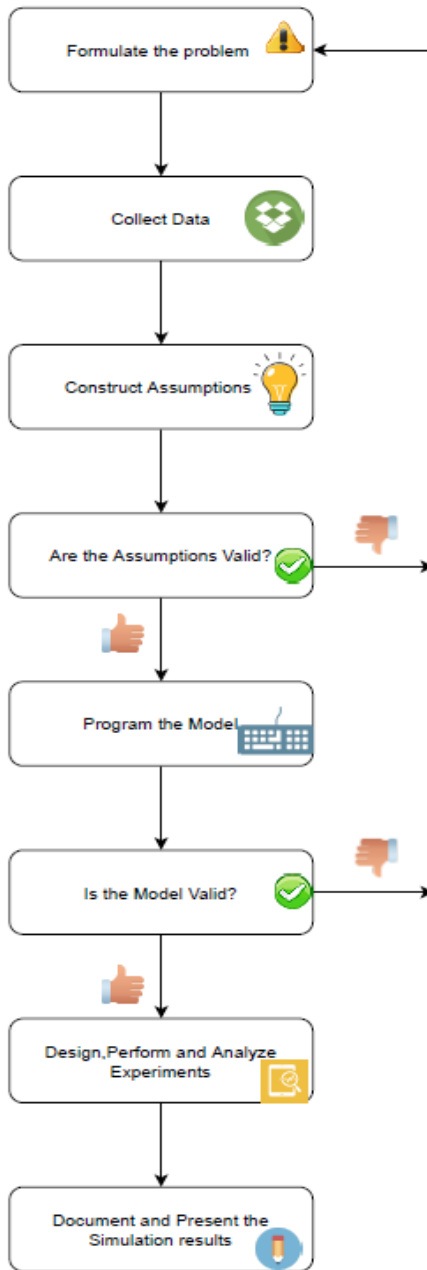


Figure 33: Flow chart to conduct a simulation study

Simulation models are designed for a specific analysis of research objectives. Concerning risk assessment, an integrated simulation approach is implemented utilizing agent-based simulation and process modeling to analyze the P2P operations. An agent-based simulation is utilized to obtain a distinct perspective into the behavior of a system, its primary components, interactions, and constraints. Every agent analyzes their role and conditions independently and makes decisions consisting of a set of standards for behavior (Mykoniatis & Angelopoulou, 2020). In a dynamic interacting system such as the supply chains, agents make the decisions for actions and activities that occur in the network. The agents have established behaviors and set characteristics within the simulation environment. The behaviors of agents can be sequences or functions which help to identify and model complex system interactions.

The agent-based simulation's interacting and autonomous characteristics are made up of roles and conditions that act independently and make decisions consisting of parameters for behavior. Agents may exhibit different behaviors suitable to the structure they reflect, such as complex behavior patterns that reflect the environment and components of the supply chain. Agent-based simulation provides important knowledge about the real-world complexities of the framework environment, such as the supply chain and its interactions and decision making (Tangpong & Hung, 2019). In turn, agents can transform, enabling the appearance of unplanned behaviors. To allow realistic modeling and adaptation, complex agent-based modeling often integrates neural networks, dynamic algorithms, or other computing techniques. Figure 34 demonstrates the different characteristics that agents in the agent-based simulation can have.



Figure 34: Structure of Agents characteristics in an agent-based simulation

4.2.4 Artificial Intelligence

4.2.4.1 Justification for using Deep Learning

In addition to using an agent-based simulation component, a Deep Learning component will be required. Deep learning (DL) is an exciting data technology inflated in popularity due to its capabilities in learning complex data. Deep Learning consists of multiple layers of neurons that extract useful information from complex data and detect and discover trends and (agents) patterns from millions of data points to produce the best possible solution or output. Deep learning is most efficient and effective when the data given to learn is unstructured and unlabeled. The justification for using Deep Learning comes from many elements Deep Learning offers in the proposed system that can't be achieved by other artificial intelligence such as machine learning and neural networks.

Concerning building the proposed system for simulation, Deep Learning is ideal for the following reasons:

1. Behavior and Trends: A common ground that Deep Learning can offer is detecting behavior and trends found in data. Some entities (agents) may display patterns of behavior that need to be captured. An example can be seen in hackers' behavior in emergent technologies; the more popular the technology, the inclinations of hacking and cyber-attacks incidents increase. Hackers use a process called reconnaissance to penetrate data and hack a centralized system, which takes much effort and time to achieve the attack. In a decentralized system (blockchain), hackers can easily access data due to the vulnerable blockchain properties of being an open-source and autonomous system that allows the hacker to dodge or deactivate specific authentication points. Deep Learning can capture and learn the trends, (agent) patterns, and behavior, detect potential threats, detect malicious activity, detect human mistakes, detect programming errors anywhere in the whole system, and implement updates to provide strong security protection. Therefore, Deep Learning is a suitable methodology for this system in capturing these trends and behaviors. The illustration in Figure 35 below displays the vulnerability points (front-end of the system) and security attack points, as well as how the hacker was able to breach the blockchain system exchange from a front-end entry point due to inadequate security measures such as internet host servers, Internet-based wallets, and two-factor validation process.

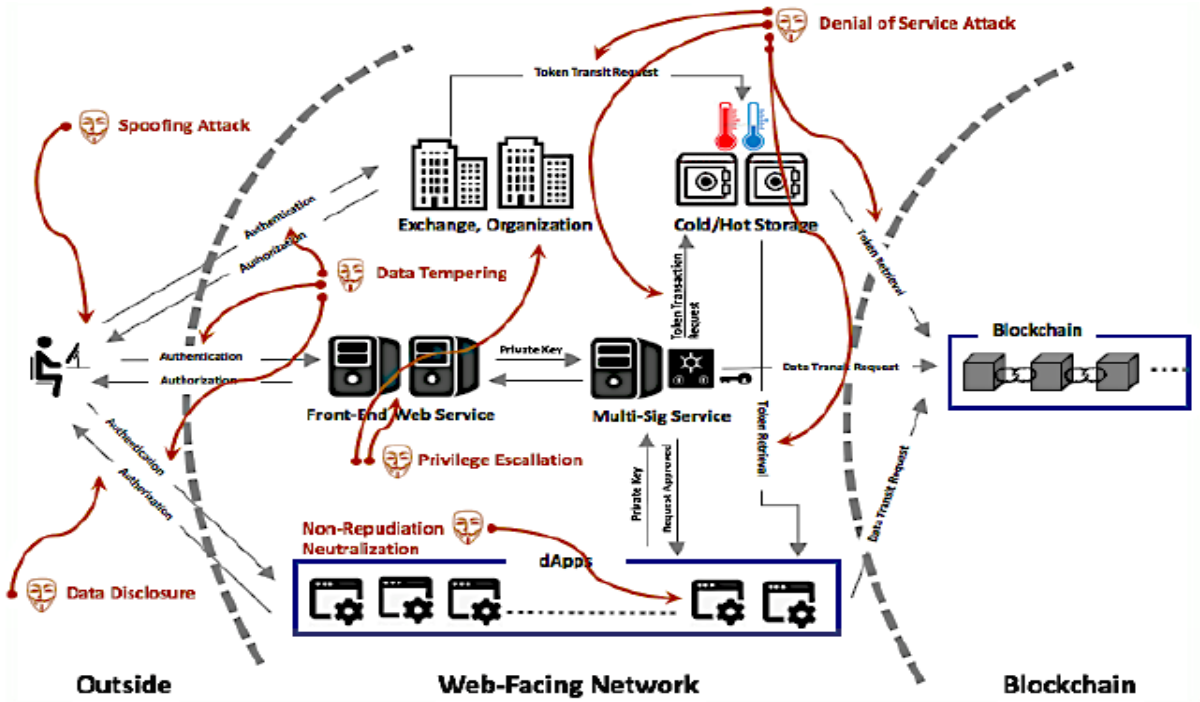


Figure 35: Vulnerability points and security attack points (adapted from Lee,2019)

2. Decision Making: Making accurate decisions is further possible with Deep Learning because Deep Learning Technology offers insight into what can occur next through scenario analysis. It also delivers precise results relative to the big, unstructured, complex, and dynamic data it learns. For example, Deep Learning can offer the financial market a technological lead in determining credit risk for businesses that apply for a loan by predicting loan default probability using algorithms. Information collected on businesses includes data found in financial statements, balance sheets, income statements, and cash flows. This data must meet specific criteria to trigger an outcome for a result (decision) of either a “low” default “probability or “high” default probability. The same concept can be applied to consumer loans issued by financial institutions (bank) towards the credit risk involved for banks. The criteria or (agent) patterns/trends used in

determining consumer credit risk are payment and credit history, outstanding debt, the pursuit of new credit, and the types of credit currently in use.

3. Reputation: Part of trust-building between supply chain partners is the reputation factor. One of the Deep Learning capabilities is learning over time with unstructured data; the more input, the “smarter” Deep Learning can produce accurate decisions with no preset limits. Sharing information between enterprises in the proposed supply chain will promote transparency. For example, suppliers in a supply chain need to create trust and maintain solid relationships with manufacturers over time, so suppliers can be trusted over time by demonstrating the reliability and manufacturing of high-quality goods. Manufacturers need to build a reputation by proving to keep their word with suppliers, and suppliers will trust them over time. The same reputation concept can be used by supply chain managers when selecting their suppliers and will choose suppliers who have a good track record and are reliable user experience to make informed decisions.

Deep Learning can be utilized to establish a reputation score for each entity (agent) in the supply chain (open database). Deep Learning will look for data that includes the number of shipments, location, number of correct items. Deep Learning will then analyze the (agent) patterns and behavior and produce which suppliers, manufacturers, distributors are most trustworthy and helps managers forecast who they are likely to have a business relationship. Figure 36 below displays the reputation management platform used to label each supplier, retailer, and distributor, while each entity (agent) behavior is recorded. Therefore, it can be implied that Deep Learning is an ideal solution in determining the behaviors and trends found in reputation management.

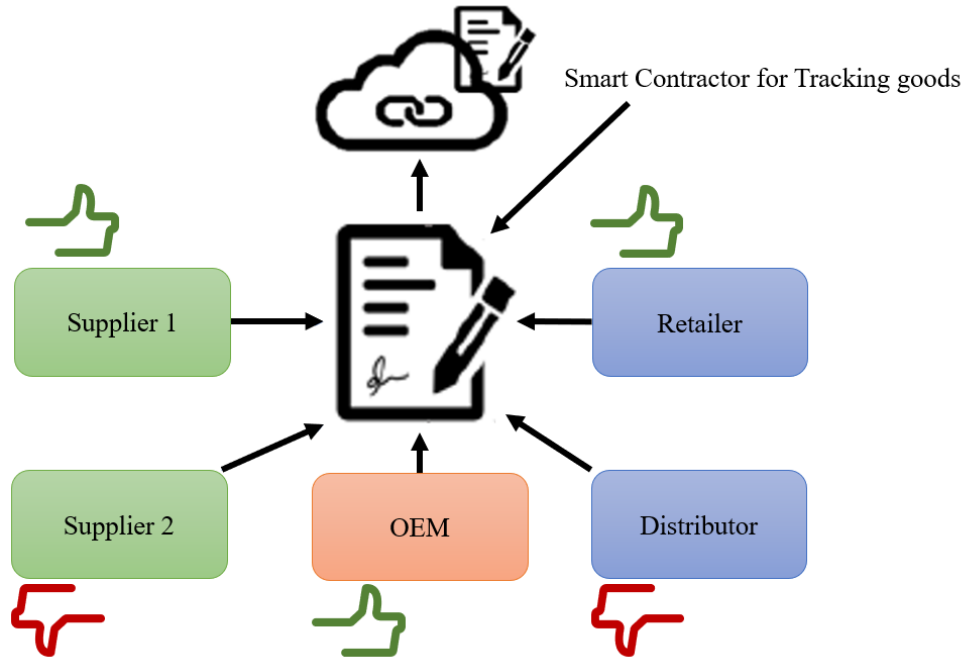


Figure 36: Reputation Management Model

Deep learning is more suitable for handling the proposed system since it can learn complex unstructured data and produce decision-making solutions. Deep learning is best used when large amounts of Big Data and a need to reduce human effort and input. Deep learning allows for capturing intricate patterns in the data, which may allow for adaptive agent behavior in real-time. Machine learning needs to be programmed with the criteria that define items and uses a smaller and simpler dataset. Neural Networks only contain only three layers of neurons that cannot dissect complex unstructured data. Due to the commonalities and compatibility of Deep Learning technology and its capability to detect (agent) patterns and behavior while the other technologies cannot, it is determined that Deep Learning is the best tool to utilize with Agent-Based Simulation the proposed system.

4.2.4.2 Deep Learning

The revolutionary advances in technology and artificial intelligence paves the way for discovering the possibilities of machine learning and artificial intelligence. Neural networks are a group of broadly constructed algorithms based on the human brain and developed to identify patterns. Deep learning is the very primary instrument of artificial (AI) intelligence. Rather than instructing systems to analyze and interpret the information (machine learning), the machine trains itself through the processes and understands from the information collected with deep learning (Chollet, 2017). Deep Learning is utilized to recognize facial expressions, recognize handwriting and texts, translate different languages, play games on a computer. It can have robotic control over self-driving cars and other technologies.

Deep Learning perceives information through a certain type of computer vision, classification, or direct content grouping. The variations of information that are recognized are numerical, stored in sequences, into which all real-world data must be interpreted, either in images, audio, and text, as well as time sequences. Deep learning typically involves the Neural Networks of several hidden layers (Zhang & Yang et al., 2018). Figure 37 illustrates a deep neural network to show the use of fully interconnected layers. Every link between the layers passes the output values node to the origin of the intended receiver or node; this happens from left to right sequence. The first deep layer is called the input layer, then hidden layer 1, then hidden layer 2, then hidden layer 3, followed by the output layer. For example, in recognizing pictures or data from texts, the neural network recognizes these images or texts and classifies them (Nielsen, 2018). The network layers illustrated below shows that every neuron in the neural network is connected to the adjacent neuron in the next layer to create an interconnected network of information transmittal.

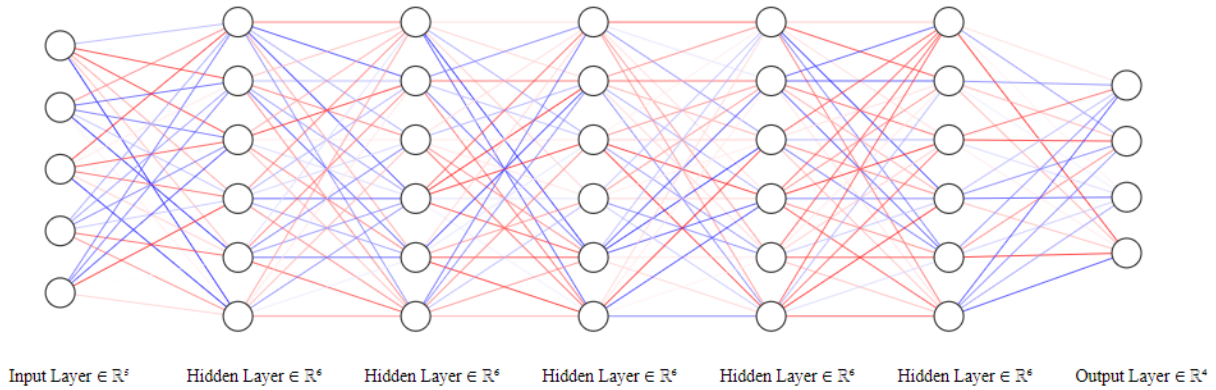


Figure 37: Deep Neural Network Architecture

The set of input data will be separated to two data sets, training and testing. The weights are calculated using the training data, and test data set is used to test the model. Through relation has its own weights, and each layer has its own value for the bias. The weights for the first connections among the input layer and the hidden layer 1 in addition to its bias value are used as inputs in the transfer function and produce outputs. Those outputs and the bias value for hidden layer 2 are used as inputs in the same or different transfer function to produce outputs, which will be considered inputs for the hidden layer 3 (Aggarwal, 2018). This algorithm will be repeated until calculating the final outputs. Deep learning learns and updates the weights of connections and bias values based on the equation (Equation 2), and the activation function is the sigmoid function (Equation 3)

$$\sum(\text{inputs} * \text{weights}) + \text{Bias} \quad (2)$$

$$y = \frac{1}{1+e^{-x}} \quad (2)$$

Neural networks offer an efficient way to select independent variables. Artificial neural networks are algorithms that is used to achieve variational mathematical analysis and offer a

modern approach to multiple linear regression models, a widely used approach for creating statistical models (Denoeux, 2019). Neural networks provide various benefits, such as having fewer rigorous mathematical learning, the capacity to indirectly identify dynamic nonlinear associations between different variables, the ability to detect all potential correlations between the regression model, and the utilization of several learning algorithms. Weaknesses include its "complex mechanical" characteristics, high computing burden, predisposition to over-fitting, and system construction's quantitative nature.

4.3 Conclusion

The key components of the developed model, which illustrates the different components needed for the simulation study, are illustrated in Figure 38. The proposed methodology is mapped to define the respective components, such as the supply chains, deep learning, blockchain, and how each of the components or modules correspond with each other in the proposed simulation environment. For this purpose, we are using the agent-based simulation environment for the components mentioned, combined with deep learning to assess the implementation of the blockchain in the supply chains.

To observe and assess the implementation of blockchain in the supply chain, three models are developed to compare the outcomes. The first model is the current supply chain, which features characteristics such as stakeholder identification, supply chain mapping, platform characterization, and challenges. The second model is adding deep learning to the previous model. The third model is the supply chain with deep learning and the implementation of the blockchain. The blockchain component features characteristics, such as entities (agents), types, and benefits.

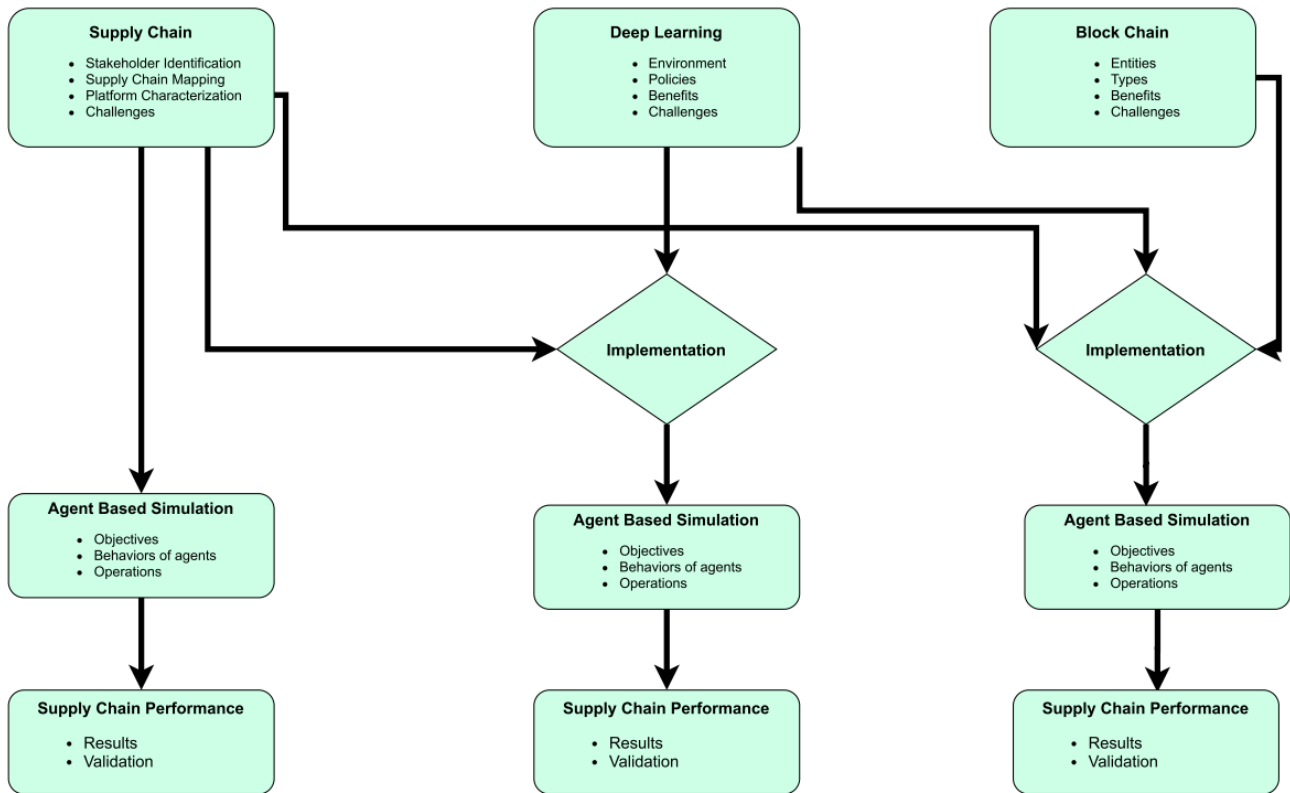


Figure 38: System Methodology

CHAPTER 5. CASE STUDY

5.1 Introduction

This chapter focuses on selecting and analyzing a case study to implement the methodology.

To be able to find a suitable case study, It requires to have the following features:

- Complex system.
- Has challenges.
- Technological based.
- Engineering based.
- Easy to visualize
- Data availability.
- Has the potential for creativity and innovation.
- Logical and meets the student's educational level.
- A service industry that needs a lot of security.

Peer to Peer lending is a complex system that has the features listed above. More precisely, the Lending Club (Peer to peer lending) will be used as a case study. The case study is used to describe the business model's suppliers, customers, and processes, as well as relevant internal and external factors. Data is used from the Lending Club website, Blogs, and the company's 10K report. The case study is discussed heavily in section 5.4.

5.2 Peer-to-Peer Economy

Peer-to-peer (P2P) markets like eBay, Uber, and home-sharing platform Airbnb allow small companies to compete with conventional companies of products or services and sell directly to the customer in a decentralized market without third party agent. As of 2014, the Peer-to-Peer sharing economy is projected to increase from \$14 billion to \$335 billion by 2025 (Anderson & Huffman, 2017). P2P markets allow for a platform for businesses to sell their goods and services in industries such as freelancing, consumer loans such as Prosper and Lending Club, payment processing, hospitality, currency exchange, e-commerce such as Amazon, craigslist, e-Bay, and delivery services such as Instacart, as well as on-demand ride-sharing services such as Uber and Lyft (Aslam & Shah, 2017). Figure 39 illustrates the P2P platforms in different sectors of the market.

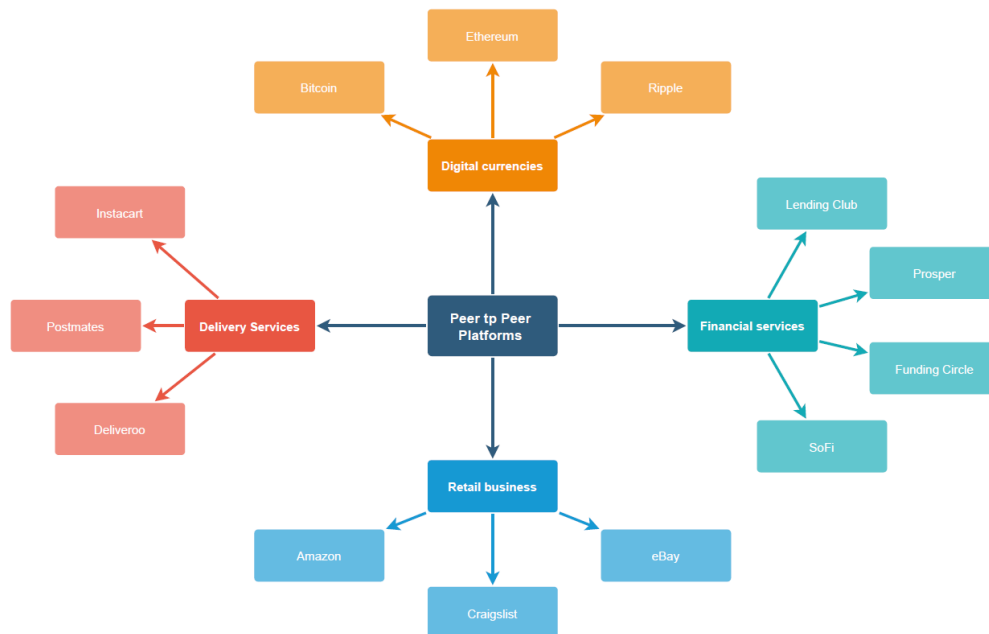


Figure 39: Peer to Peer Platforms across different Industries

The P2P online platforms offer consumers a way of conducting transactions virtually and give users or customers certain degrees of control, such as customers can utilize the P2P platform to search for exactly what they need and receive results and feedback. There are five virtual intermediate platforms in the P2P market economy which connect various types of consumer classes. The first platform is the resource-sharing platform such as Lyft or Uber, which connects customers or passengers in real-time that need transportation or ride-sharing services to their location with the closest driver.

The second platform is a matching platform such as loan lending or housing websites that match their customers according to the user's preset preferences. The third type of virtual platform is a crowdsourcing platform that involves receiving the task, knowledge, or thoughts of many participants sending their information through the Web, social media, and mobile apps. (Schor, J. B., & Fitzmaurice, 2015). For example, freelancing websites and traffic apps enable drivers to submit online real-time traffic information to update traffic accuracy for another user's knowledge.

The fourth type of virtual P2P platform is a review platform in which users submit online reviews of products and services for other users to benefit from. For example, Amazon offers reviews of its products for customers to read about before they decide to purchase (Chen et al., 2018). Yelp has a review platform where diners can read about restaurants and search for restaurants based on other people's experiences. The fifth platform is a crowdfunding platform where a seeker collects funds to finance a campaign from a wide range of donors or investors from the public, GoFundMe and Kickstarter are an example of crowdfunding platforms (Chen et al., 2018). The P2P platforms can be viewed as search and match functions for users. An advantage of the P2P market is many businesses have low barriers to overcome for entry into the P2P market. Buyers and sellers can switch roles as the P2P market is flexible. The scale of the Peer-to-Peer

economy is global such as alibaba.com is operating. Other companies, such as Uber and Airbnb, are spread globally in various countries (Aslam & Shah, 2017).

5.3 Peer-to-Peer Lending

The P2P lending market functions in the business mindset of "for profit." P2P firms earn income by obtaining a one-time fee from borrowers on financed loans and assessing a loan servicing fee to investors or borrowers (often a specific annual percentage or a percentage dependent on the loan amount) (Einav et al., 2016). In the peer to peer (P2P) lending market, investors bid on unprotected loans requested by potential borrowers. Online P2P transactions are increasing; however, creditors are also not professional investors in this type of industry. Consequently, investors must take huge risks since these loans are awarded without leverage in the P2P lending market. At first, an auction platform was developed by Prosper Lending Company, an early entrant in peer-to-peer lending of the virtual marketplace, whereby borrowers submitted a maximum interest rate they were willing to pay, and lenders were prepared to make lower offers accordingly to attract the borrowers (Lee et al., 2012). Then another company emerged into the P2P market called Lending Club. Lending Club uses a sophisticated formula to calculate the probability and risk of each prospective purchaser. It sets interest rates dependent on that scoring system, in accordance with the market conditions and competitive investment returns.

5.4 Lending Club

In the financial service industry, Lending Club offers its customers (agents) a virtual credit marketplace to promote and market its loan at a lower overall cost for borrowers or businesses rather than conventional lending programs, delivering added value in the form of reduced rates to

borrowers (agents), and giving investors (agents) the ability to gain attractive or promising returns (Yao, 2019). Renaud Laplanche first founded the lending Club in 2006, with its headquarters located in San Francisco, CA. As of 2017, it has issued \$50 billion in loans. The lending Club process starts with an individual looking for a loan to buy a home or a business applying for a loan. They will first apply for a loan online if they satisfy other conditions (660 + FICO score and income requirements); their loan is linked to the online portal (Wang et al., 2009). The online platform then assigns each borrow with a grade based on the overall criteria.

Investors (agents) can then sort through the borrowers/loans and grade on the portal using 30 different criteria and build a loan portfolio. Meanwhile, Lending Club starts the borrower's verification process; once the verification is cleared, the loan is then sent for processing for approval within a few days. The borrower's payments start 30 days after approval, and funds are split between the principal and interest on the loan (Lending Club, 2019). Interest on loans via Lending Club range between 10.68% to 35.89%. Investors behave in a way where their funds are spread across many different borrowers to lower their investment risk, which means an investor will more likely invest smaller amounts of money into a larger number of loans.

5.4.1 Borrowers and Lenders Activities

With the rise in the e-commerce market combined with the rapid growth of the virtual network, P2P loans are growing rapidly as an easy route to finance for individuals. The acceptance rates for loans in the P2P market are as good as the standard way of measuring loan grades and interest rates. Lending Club utilizes WebBank, an insured bank that is backed up by the FDIC

(FORM 10-K., 2019). WebBank is committed to all the laws and policies on federal and state-level banking as other online and traditional banks. Lending Club pays WebBank a monthly service fee that is dependent on the number of loan amounts that are issued by WebBank.

The loan origination for borrowers' cost is calculated by the loan's length and credit rating, which varies from 1.11% to 5.00 % of the first principal balance. Lending Club charges lenders (agents) a service fee that matches 1% of the balance, interest, and late fees collected from the borrower. The promissory note and the original contract encompass obligatory arrangements and commitments that necessitate the borrower to pay back the debt and recognize Lending Club's role as their servicer for the loan (Joledo et al., 2014). Borrowers (agents) allow WebBank to distribute the funds for the loan through an ACH transfer. The following steps are the Lending Club borrower and lender activities from when a potential borrower applies to when the lender funds the loan.

1. Applicant (Borrower) fills out an online application (Borrowers must be at least 18 years of age, must have valid email addresses, meet either the Standard Program or the Custom Program criteria, must have a social security number, and a bank account.)
2. Initial Screening, agent, (proprietary risk algorithms to analyze an borrower's risk profile based upon the issuing bank's underwriting guidelines). Each loan requested is assigned one of 20 loan grades, from A1 through D5. The base interest rates currently range between 6.46% and 28.80% (FORM 10-K., 2019).
3. If the applicant, agent, is initially approved, the applicant is presented with different loan options with various amounts, terms, and rates.
4. Once the Applicant chooses the loan option, the loan is then recorded on Lending Club's marketplace to draw in an investor, agent, commitments

5. During the search for investors, additional verifications on the borrower are completed. An applicant with a FICO score of 660+ is deemed to be a “prime” borrower. (verification includes; borrower’s income, employment, fraud checks, the debt-to-income ratio must be below forty percent, credit report (five or fewer credit queries in the last 6 months (excluding mortgages and auto loans, and minimum credit history of 36 months. Delinquencies of credit line balance and length of credit history, supplied names, social security numbers, addresses, and telephone numbers against the data in the records of a consumer reporting agency)
6. Once verifications and commitments are received, the issuing bank originates and issues the loan to the borrower. Borrowers pay an origination fee to WebBank upon the successful issuance of the loan, which ranges from 0% to 6.00% of the original principal amount (FORM 10-K., 2019).
7. If the borrower accepts the loan, the applicant agrees to be bound by the terms of a promissory note and authorizes Lending Club to debit the borrower’s designated account by ACH transfer for each loan payment due under the promissory note.
8. Loan Servicing (account maintenance, collections, processing payments from borrowers and distributions to investors)

Figure 40 illustrates the loan issuance mechanism and process for what both borrowers’ activity entails and lenders activity. The lending club obtains the capital from investors, then provides investors with notes, securities, certificates.

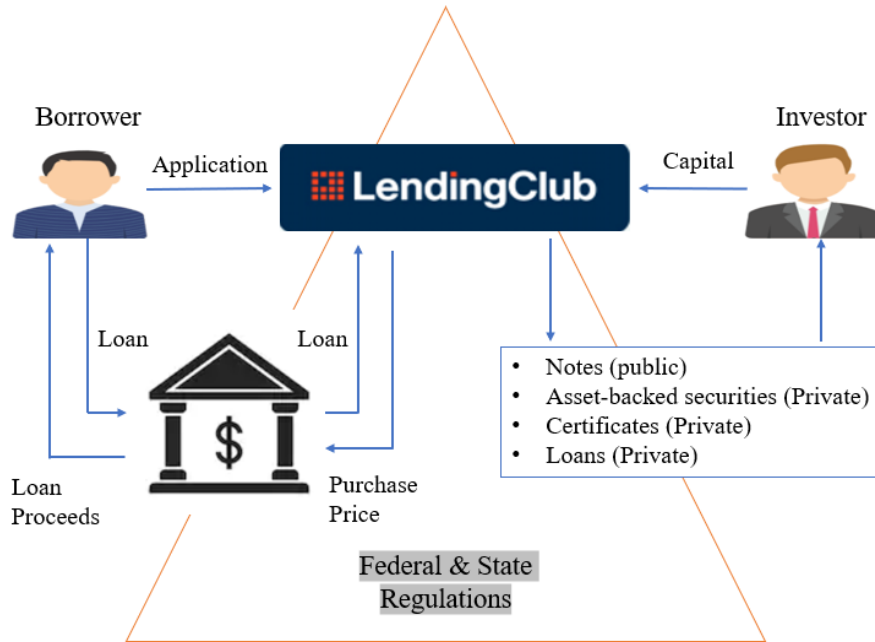


Figure 40: Lending Club Loan Issuance Mechanism

Figure 41 below illustrates the behaviors of the borrower’s activities for Lending Club. The potential borrower must go through each of the steps and verification processes and review them until they are approved.

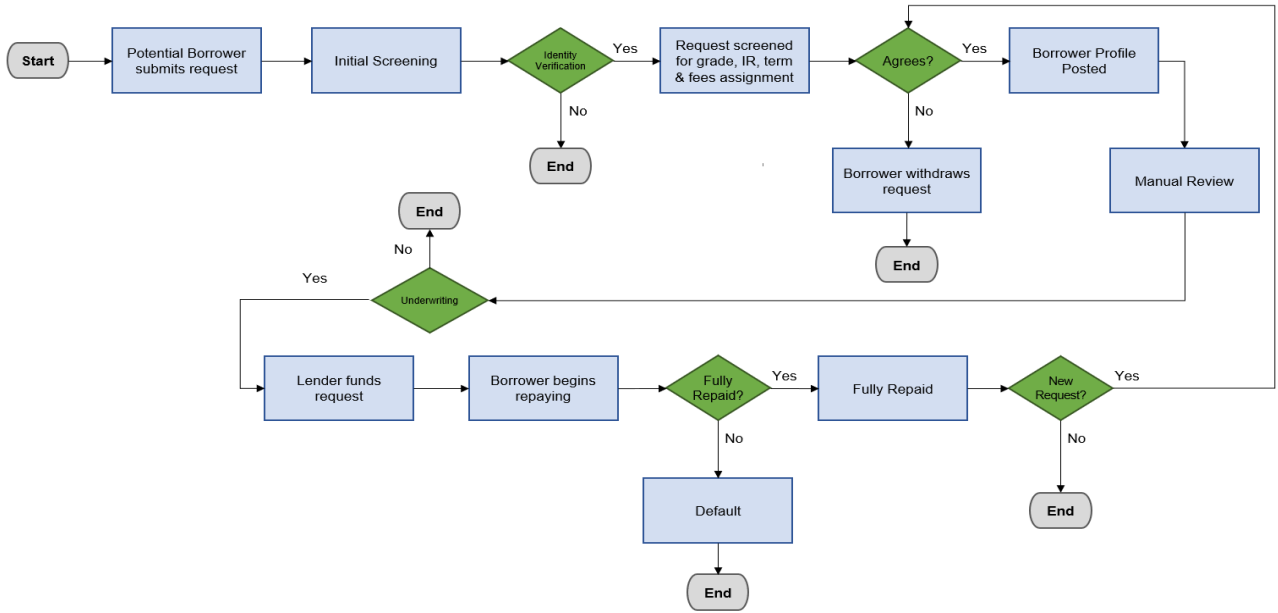


Figure 41: Flow Chart representing the behaviors of Borrower activities

Figure 42 illustrates the behaviors of the lender’s activities for Lending Club. The lender also passes through a process of choosing the right and secure investments that are suitable for funding.

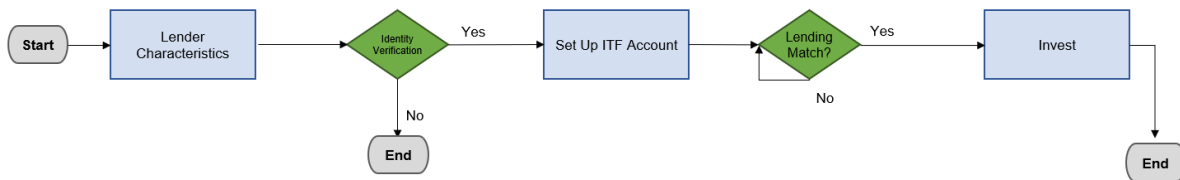


Figure 42: Flow Chart representing the behaviors of Investor activities

5.4.2 Lending Club Challenges

Lending Club faces many challenges since it is a different way of financing loans through a virtual network and platform made up of borrowers and investors. Some challenges include if the Federal Reserve increases the federal fund rate, it causes an increase in the market interest rate, which causes people to save their money in banks versus applying for loans. When this happens, there are fewer funds for loans for Lending Club to dispense (Chang, 2015). Another challenge is high operating costs due to competition and stricter regulations set, which causes Lending Club to increase marketing costs to compete for profit. Lending Club also faces challenges in its cybersecurity and transparency.

Lending Club does face many challenges; however, this study will focus on the challenges of cybersecurity and transparency/trust issues. Like other financial institutions, Lending Club faces challenges in cybersecurity as it relates to the financial gain for hackers and those who want to intrude into companies' data and extract what they can and cause corruption to their financial system for a reward. According to data gathered from Bitglass from Ponemon Institute, financial sector firms experienced 6.5 percent of all cyber-attacks and breaches (Carino & Del Giorgio et al., 2018). Leaked data and records are other cyber issues for financial firms, which 61.7 % of leaked data in hacking, in general, comes from finance firms. In the past years, the global threat framework has significantly increased. The intended motive for hackers to execute cyber-crime and hacking isn't always easy to identify. Hackers are looking for financial gain from selling sensitive data, consumer data, and information on business assets, which are all increasing with time.

In 2007, Lending Club was created as a peer-to-peer lending platform serving borrowers and investors. Borrowers can borrow up to \$40,000 from a platform of interested investors who buy the loan and then are promoted to institutional lenders who can make a profit from the interest on the loans. According to Lending Club, in the 4th quarter of 2019, the Lending club had issued more than 59 billion dollars in loans (Lending Club, 2019). A recent audit and investigation on Lending Club revealed a \$22.3 million discrepancy of loans granted to a sole investor, the loans that were fabricated were made to appear to qualify for the loan so that it can be marketed to the investor as qualified; however, the requirements were not met by the borrower. The case is still under legal proceedings and has not been assigned a judgment yet. However, Lending Club CEO Renaud Laplanche has been removed from his position. Two other class action lawsuits are active for Lending Club. The first lawsuit claims the company made a false statement about its operations, and the other lawsuit claims borrowers received loans that were above the states' lending limits.

CHAPTER 6. IMPLEMENTATION, VALIDATION, AND RESULTS

6.1 Introduction

An Agent-Based Model (ABM) is defined by a set of Agent Types with a population each, an environment in which they exist, and finally interactions between the different agents in the model. In AnyLogic, each Agent Type is defined by a state-chart (i.e., a combination of states and transitions between these states), functions, and attributes. As part of this study, three different Agent-Based Simulation Models are developed as follows:

1. Current Lending Club
2. Lending Club with the addition of a Deep Learning IT Security System
3. Same as above with the addition of Blockchain

In this section, a summary of the used software elements in the three models is presented. Three kinds of states and five kinds of transitions are introduced in the established Lending Club models. These are presented in tables 5 and 6, individually.

Table 5: State Types

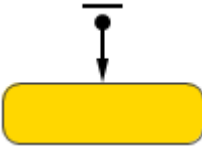



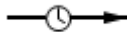


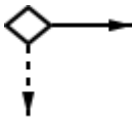
State	Presentation	Description
Initial State		The agent's first state when created
Regular State		Any state in the state-chart that is not the initial state or an end state.
End State		An agent cannot leave an end state. Once the agent reaches the end state, it will no longer change. A state-chart may have several end states.

Table 6: Transition Types

Transition	Presentation	Description
Message		This transition is triggered by a message that is usually sent by another agent or by the environment.
Timeout		The agent moves from a state to another state after a given period.
Condition		This transition is triggered by a pre-defined condition.
Rate		This transition is triggered at a certain rate (e.g., 1 / min)
Branch		The branch is used when more than one possible outcome may occur, depending on a condition or probability.

6.2 Initial Model

The Lending Club's initial simulation model contains three Agent Types: 1) Borrower, 2) Lender, and 3) Lending Club Trust. Unlike the Lending Club Trust type, which has a total population of only one, Borrower and Lender have large populations of variable size. On the one hand, two-way interactions exist between borrowers and lenders; on the other hand, one-way interactions exist between lenders and Lending Club Trust as well as between borrowers and Lending Club Trust. In fact, the lenders' decisions are impacted by the Lending Club's reputation and how much they trust funding borrowers on the platform. Moreover, borrowers' performance compared to the expectations may negatively impact the level of trust as well. A high-level summary of these interactions is presented in Figure 43.

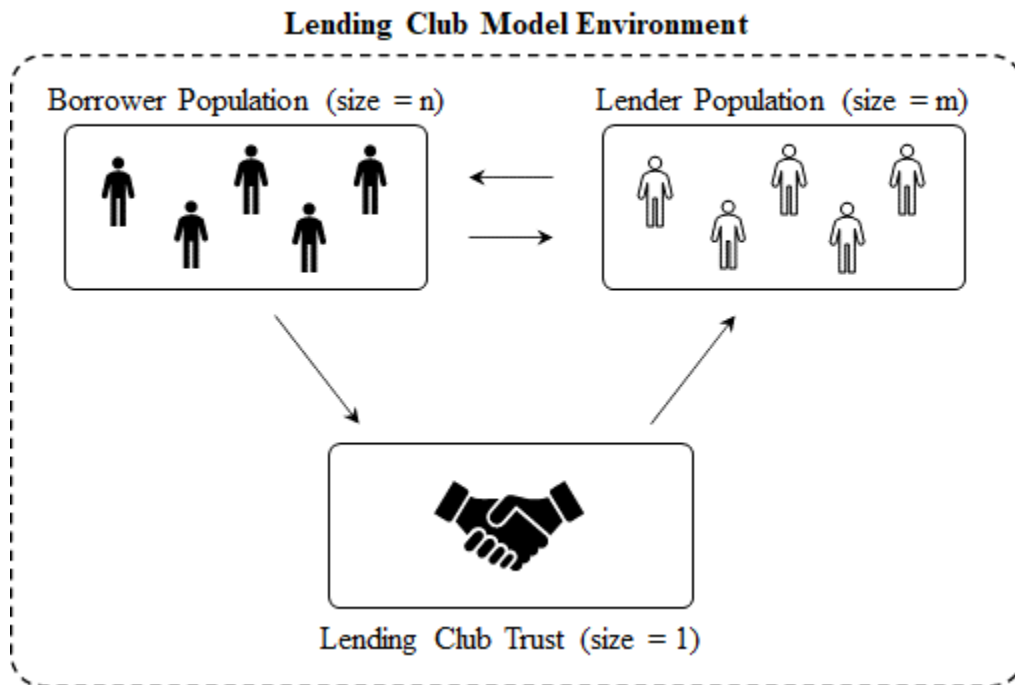


Figure 43: Initial ABM Environment and Agent Interactions

The Lending Club model's state-charts are presented in Figures 44 and 45.

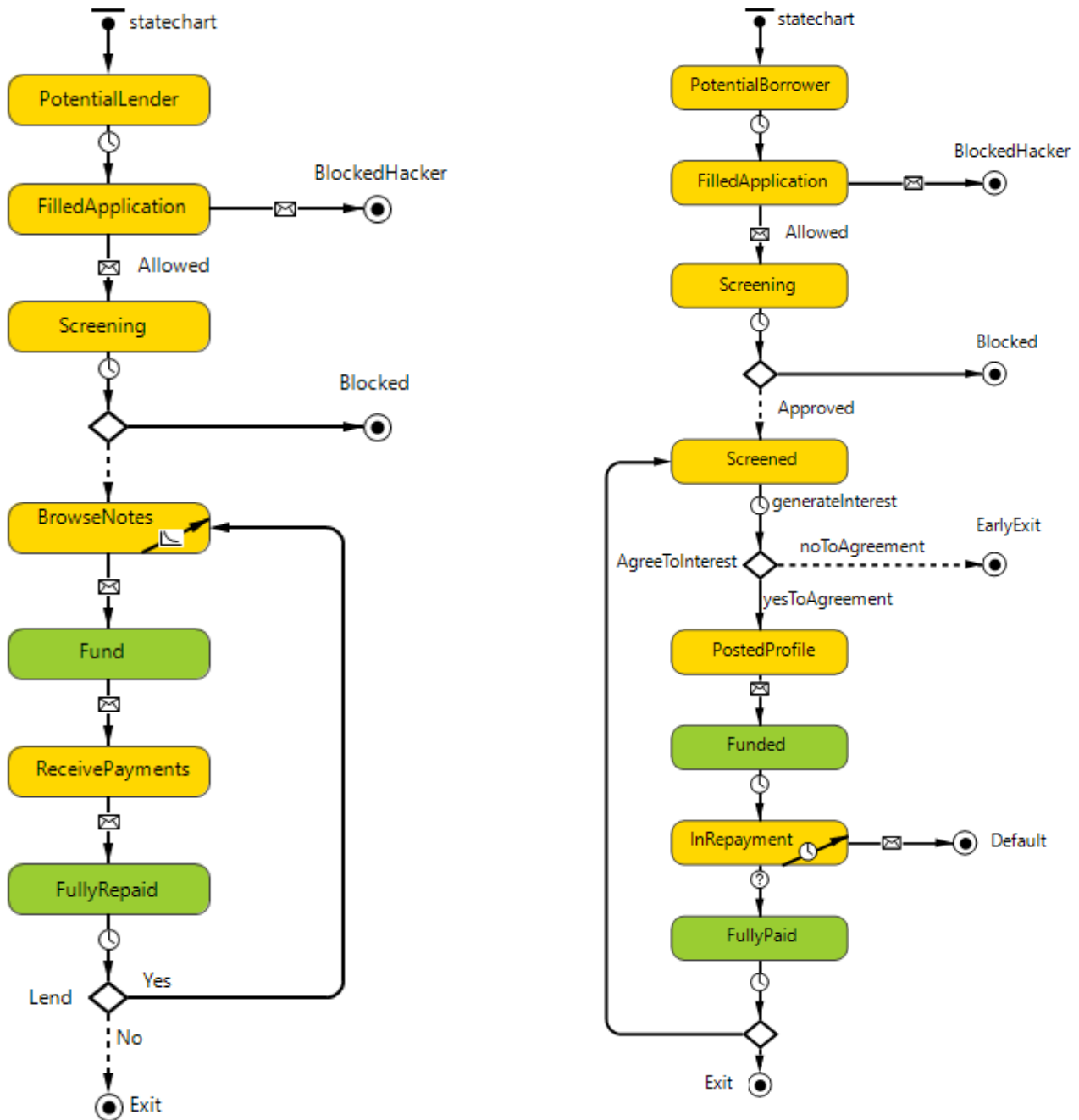


Figure 44: Borrower and Lender's State-Charts

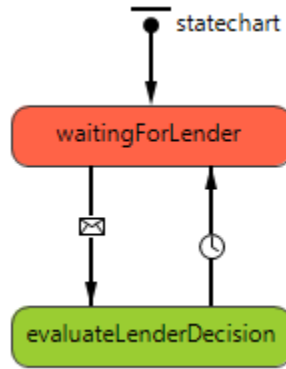


Figure 45: Lending Club Trust’s State-Chart

In addition to their state-charts, borrower and lender agents are characterized by several parameters and variables. Some are defined as the moment at which the agents are created, while others are generated as a result of agent interactions. The initial parameter is the agent’s class. The latter may take three values: 1) attacker, 2) suspicious, or 3) normal. Based on the Lending Club data, 2% of platform profiles are attackers, 24% are suspicious, and 74% are normal (Lending Club, 2020). Agents of class “suspicious” are not attackers; their profiles raise question marks but end up generally being accepted.

Another borrower parameter consists of the loan amount, which is randomly generated from a custom distribution defined using actual data from the Lending Club, which provides such information publicly (Lending Club, 2020). Over 100,000 entries were used to generate the distribution. The latter is shown in Figure 46, which is a simplification of the actually used distribution that has much smaller ranges. Ranges were grouped in the figure merely to give a clearer idea of the loan amounts distribution. The generated custom distribution is fed to AnyLogic as a stochastic input, thus assigning a loan amount to each borrower.

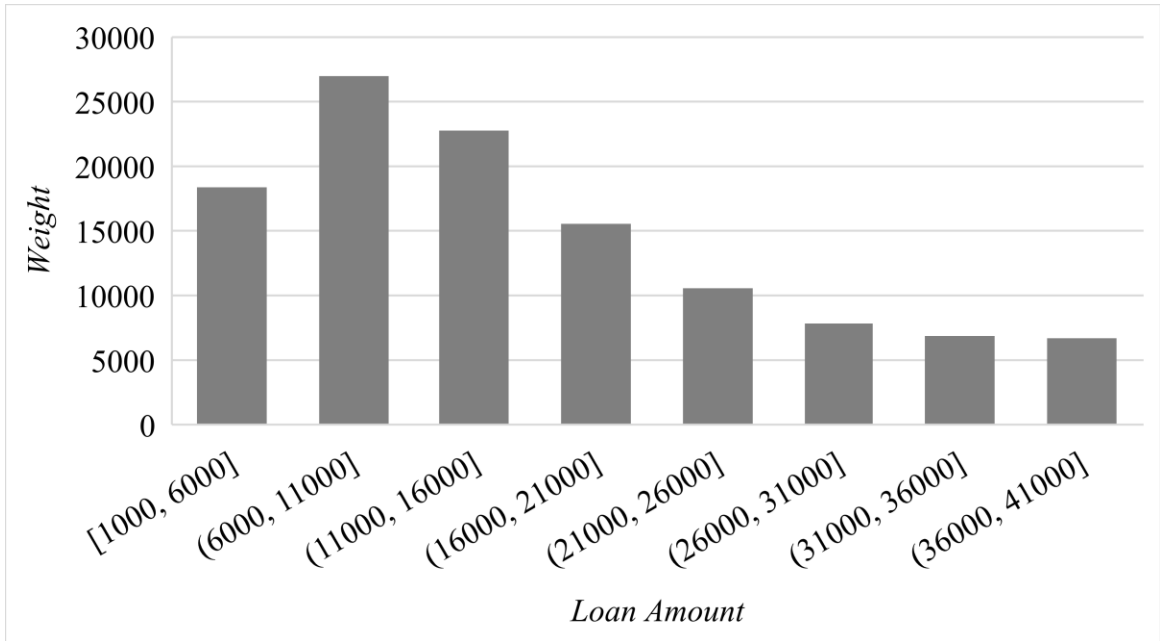


Figure 46: Loan Amount Custom Distribution

Another borrower parameter is the grade. It is also based on a custom distribution from the same actual data set acquired for the loan amount (Lending Club, 2020). Grade A represents the most reliable borrowers, while grade G corresponds to the riskiest profiles. The used grade custom distribution is presented in Figure 47.

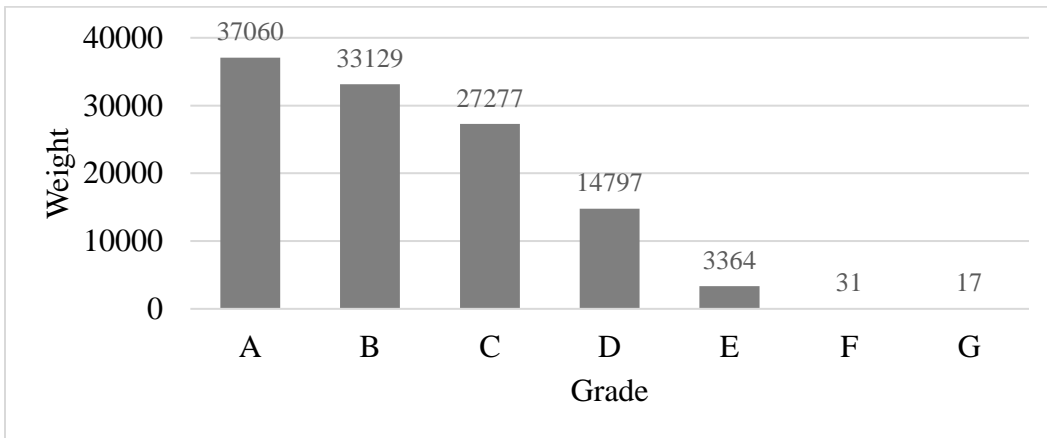


Figure 47: Borrower Grade Custom Distribution

Once the grades are defined, the last set of parameters for the borrowers are generated using custom distributions that are grade-dependent (i.e., each grade has its own distributions). These parameters include the interest rate, the loan term, and the originating fee. The distributions of interest rate and loan terms are presented in Figure 48 to Figure 55 by grade (Lending Club, 2020). The third parameter, which is the originating fee, falls between 1.10% and 5.00% (Joledo, 2016). It is assumed that the better the grade, the lower the fee, so uniformly distributed and equal ranges are defined as shown in Table 7.

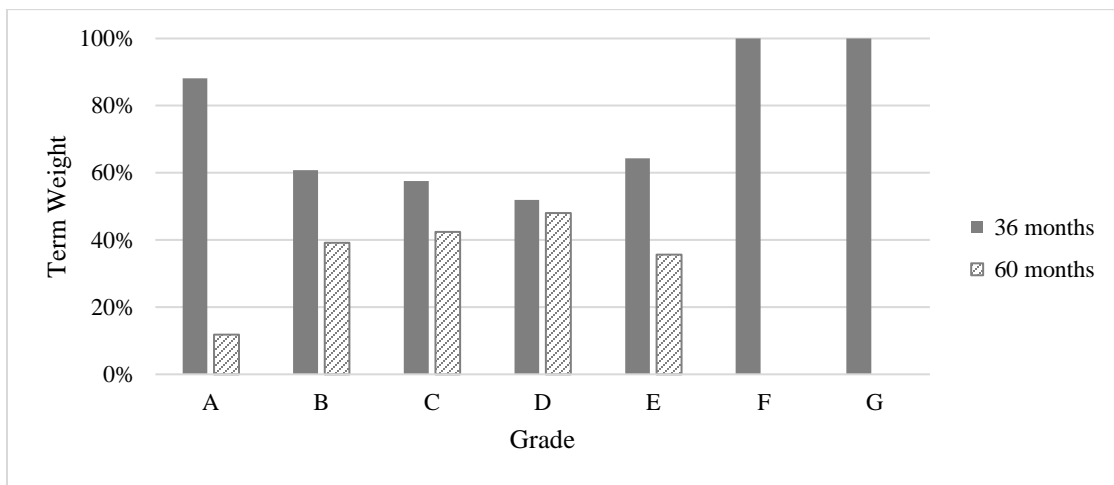


Figure 48: Term Distribution by Grade

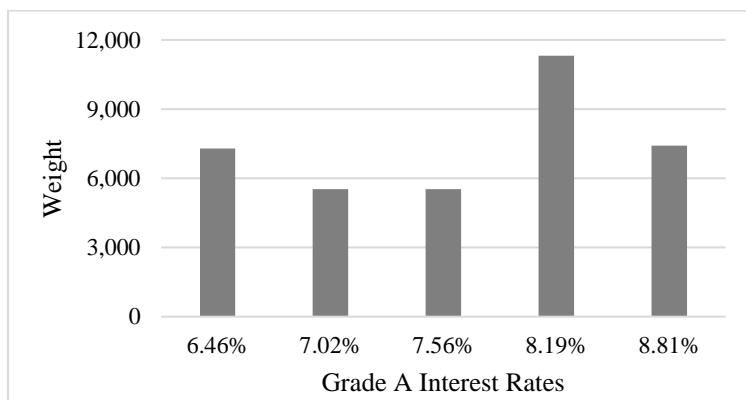


Figure 49: Interest Rate Distribution for Grade A

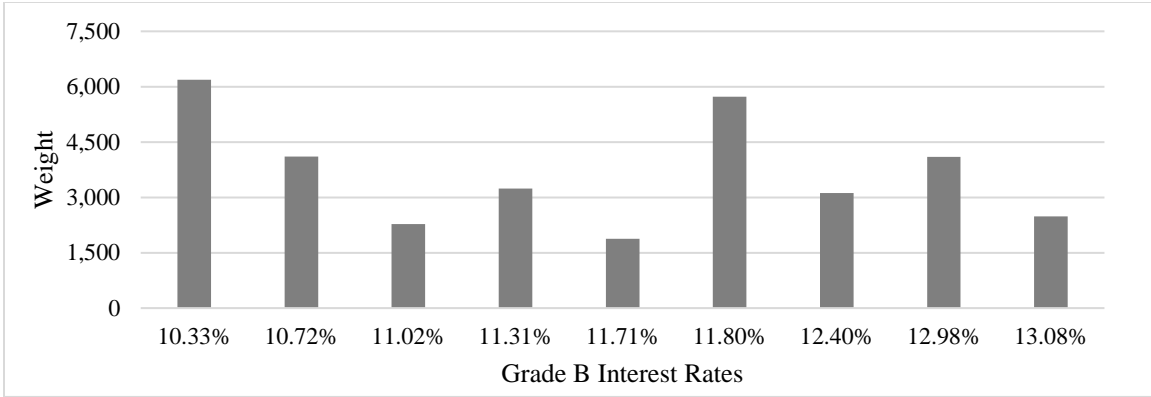


Figure 50: Interest Rate Distribution for Grade B

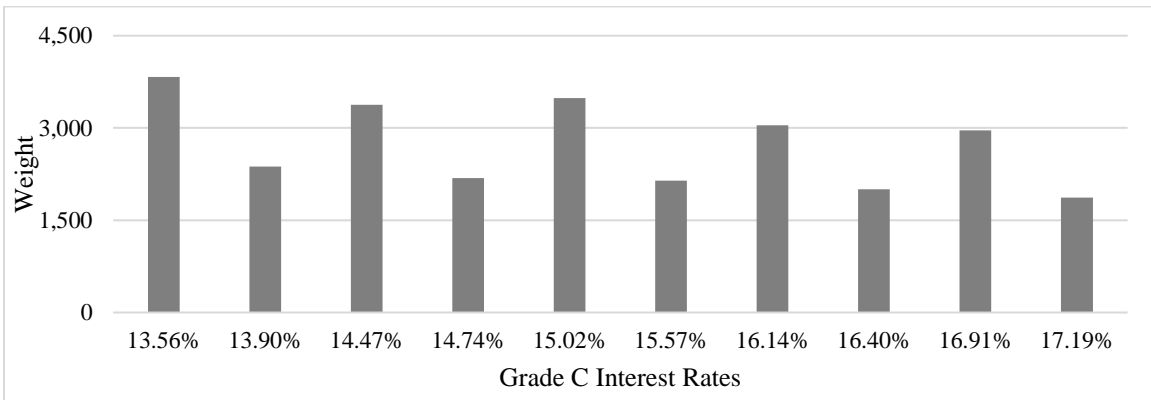


Figure 51: Interest Rate Distribution for Grade C

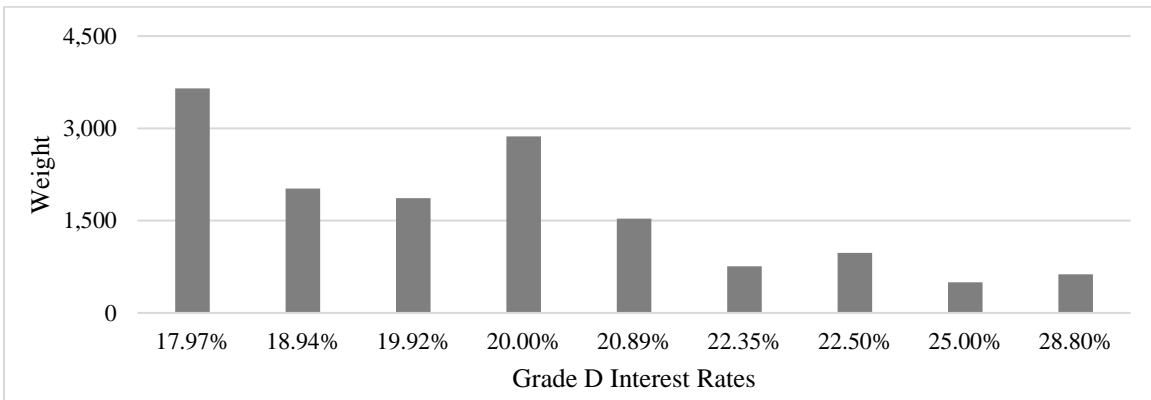


Figure 52: Interest Rate Distribution for Grade D

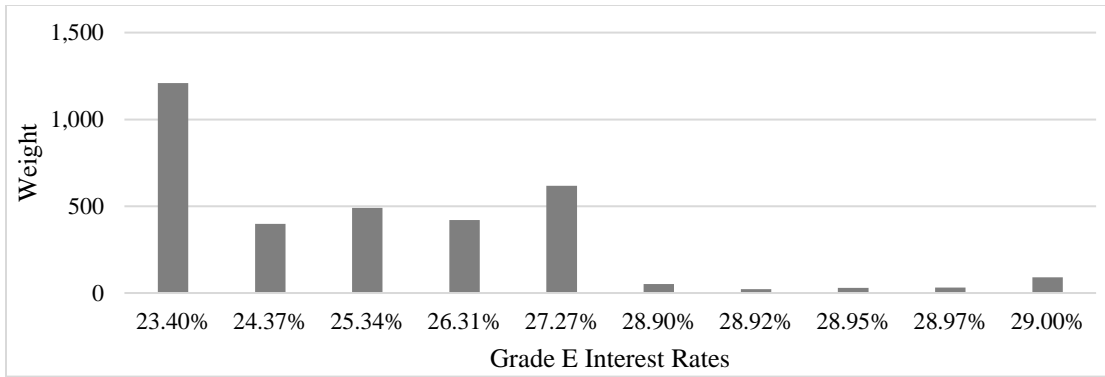


Figure 53: Interest Rate Distribution for Grade E

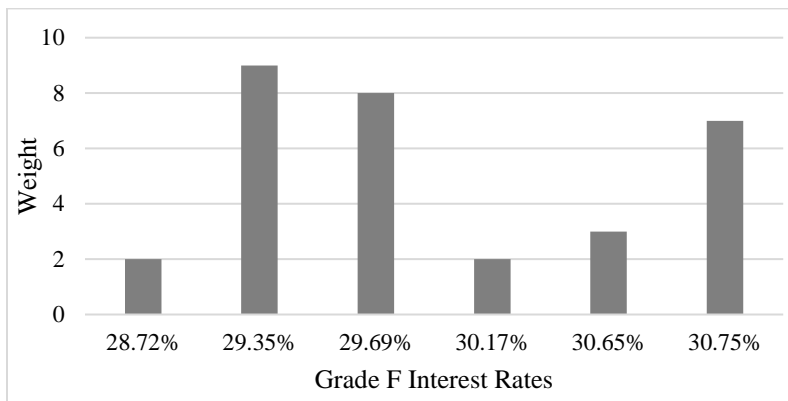


Figure 54: Interest Rate Distribution for Grade F

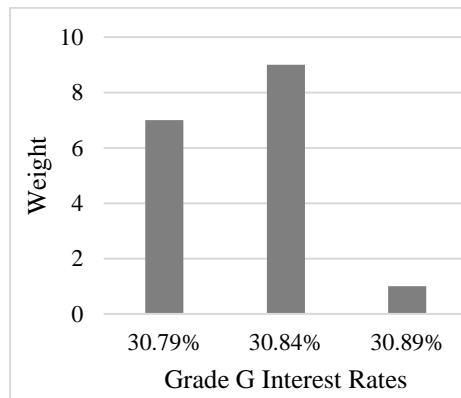


Figure 55: Interest Rate Distribution for Grade G

Table 7: Originating Fee by Grade

Grade	Originating Fee (%)
A	uniform(1.10, 1.66)
B	uniform(1.66, 2.21)
C	uniform(2.21, 2.77)
D	uniform(2.77, 3.33)
E	uniform(3.33, 3.89)
F	uniform(3.89, 4.44)
G	uniform(4.44, 5.00)

The lenders' main parameter is their risk aversion, which can be one of three values: High, Medium, or Low, representing the lender's willingness to take the risk of funding borrowers of poor grades. The grades that different risk aversion levels are willing to fund depend on the Lending Club's Trust Agent. For example, a lender with high-risk aversion may be willing to fund a borrower of grade C if trust levels are high but may not be willing to fund a borrower of grade B if trust levels are low. More details regarding this mechanism are presented later in this section.

Having presented the model's state-charts and main parameters, the model logic, rules, and functions behind the agents' interactions is now described (in reference to figure 44). At time 0, the populations of borrowers and lenders are created in addition to one single Lending Club Trust Agent. At that moment, all borrowers and lenders are in the states' *PotentialBorrower* and *PotentialLender*, respectively. After that, both the borrowers' and the lenders' applications are either blocked (as a result of being considered attackers) or approved. If blocked, the agent is sent to the end state *BlockedHacker*. Otherwise, the agent proceeds to the screening stage (applies to

both borrowers and lenders). In the initial model, given that the Deep Learning IT Security System is not implemented yet, it is assumed that a percentage of agents of class “attackers” and “suspicious” are blocked while the remaining ones are allowed to proceed. At this stage, based on the available data, it is assumed that 80% of attackers are blocked, while 5% of the suspicious profiles will be wrongly blocked, thus reducing the number of borrowers that could have been funded.

Screening, unlike the previous step, consists of reviewing the applicant’s loan/funding-related application components and not IT information. It is assumed that 5% of applications will be rejected for reasons such as missing information. Those rejected reach the end state *Blocked* (whether borrower or lender). Approved lenders can now start looking for borrowers to fund. As for approved borrowers, an additional step remains, which consists of the Lending Club generating the characteristics (i.e., grade, interest rate, term, and originating fee) for the requested loan amount based on the previously presented custom distributions. As a result, the borrower now faces the choice of either agreeing or refusing the assigned loan terms. If the borrower decides to refuse, another end state is reached (*EarlyExit*); otherwise, the borrower’s profile is finally posted publicly on the Lending Club platform.

With lenders having reached the state *BrowseNotes* and borrowers having reached the state *PostedProfile*, both agent types can now start matching. This is modeled through the use of a function called *findInvestment* that is dependent on the Lending Club’s Trust Agent. This function behaves differently depending on the established level of trust. The Lending Club may sometimes inaccurately represent the borrower’s grade by assigning one that is better than deserved to entice lenders to fund more borrowers. This is modeled using an additional parameter for borrowers called “*Posted Grade*.” It is assumed that borrowers of grade A will have a posted grade of A as

well. 50% of borrowers of grade B will be posted as A while the other 50% will be posted as B. Similarly, 50% of borrowers of grade C will be advertised as borrowers of grade B while the other 50% will be advertised as C. The same applies to the remaining grades.

As a result, lenders would often be disappointed given that their expectations would be higher. This negatively impacts the Lending Club’s reputation and the lenders’ trust. Trust is modeled as a variable within the Lending Club Trust Agent, which is initially equal to 100. Each time a misrepresented borrower is funded, the level of trust decreases by one. Trust is divided into three ranges: 0 to 50 (low trust); 50 to 80 (medium trust); 80 to 100 (high trust). With reference to Table 8, the lower the level of trust, the lower the chance of having repeat lenders (Business Model Zoo, 2015).

Table 8: Repeat Lender Probability

Trust Level	Repeat Lender Probability
High	18%
Medium	14%
Low	10%

Another impact of low trust is modeled through lenders' changing willingness to fund borrowers of different grades based on the trust level. The modeled idea is presented in Table 9

Table 9: findInvestment function overview – Willingness to fund grades based on Trust Level and Lenders’ Risk Aversion

Trust Level	Risk Aversion		
	High	Medium	Low
High	A, B, C	D, E, F	G
Medium	A, B	C, D	E, F, G
Low	A	B	C, D

Based on the presented trust dynamics, the *findInvestment* function within the Lending Club’s Trust Agent (refer to Figure 49) makes each approved lender go through each borrower and matches a lender with a borrower only if two conditions are both met:

1. The borrower is in the state *PostedProfile*
2. The lender’s risk aversion matches the borrower’s grade (as per Table 9)

Once matched, the borrower moves to the state *Funded*, and the lender moves to the state *Fund*. A delay of around a day is assumed for the money to be transferred, after which the borrower moves to the state *InRepayment* and the lender to the state *ReceivePayments*. In the *InRepayment* state, the borrower pays an installment every month, which is calculated based on the loan amount, the term, and the interest rate, with a probability of defaulting every month. The defaulting probability is grade-dependent and is identified from the actual data collected from the actual lending club. It varies between 0.0% and 3.0% every month (Lending Club, 2020). In case of default, the borrower goes to the end state *Default*. Otherwise, installments keep getting paid to the lender until the number of payments becomes equal to the loan term (i.e., 36 months or 60 months). At that point, both the lender and the borrower move to the *FullyPaid* and *FullyRepaid*

states, respectively. One day later, both borrowers and lenders have the option to exit the Lending Club platform or to enter it again for another loan/funding application. The lenders' probability of choosing to fund another borrower depends on the data presented in Table 8 (Business Model Zoo, 2015).

Finally, according to the Lending Club, the whole application, approval, and funding process take on average seven business days with a possibility of delays, so this number is represented in the transitions of type "timeout" (Lending Club, 2020).

6.3 Addition of a Deep Learning IT Security System

The deep learning model is used to map users' characteristics to the type of users, whether it be normal, suspicious, or attacker. The KNIME platform is used to build the Deep Learning model using Deeplearning4J Integration. The methodology of extracting the users' configurations of the Lending users is explained in section 6.3.1 below.

6.3.1 IT Environment Development of Lending Club

Based on experts' opinion, The IT environment of Lending Club is similar to the environment shown in Figure 56, it consists of two major categories, External and Internal. The external server (accessible from the internet) consists of borrowers, lenders, and hackers. The internal server offers two services, which are file synchronization and webserver. The internal network consists of three subnets management, server, and office. The two categories are separated by a firewall that filters the requests from the external network to the internal network. The traffic

flows from the external network through the firewall to the internal network, in which the traffic is serviced by the server.

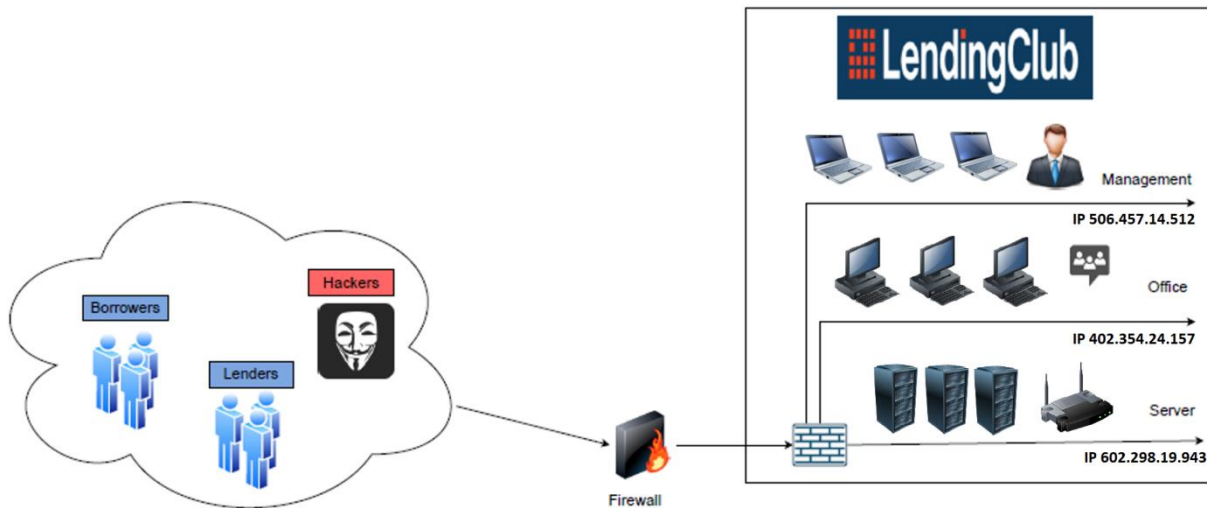


Figure 56: Overview of the Lending Club environment

On the other hand, CIDDS-001 (Coburg Intrusion Detection Data Set) is a data set that is resulted from a business environment for an anomaly-based intrusion detection system (Ring, Wunderlich et al., 2017). The business environment has both external and internal traffic. The internal server consists of four subnets internal servers, management, office, and developer. In contrast, the external server consists of users through the web, including hackers.

Clearly, the network structure of the Lending Club is similar to the network structure of the business environment where the CIDDS-001 dataset was collected. Note that having an internal network that is connected to the internet using a firewall is the most used network structure. Thus,

having the same vulnerabilities and exposing the system to the same types of attacks. Therefore, the CIDDs-001 data set can be used as users' configurations of Lending Club.

For the case study and building the deep learning model, we used three classes and five attributes shown and described in tables 10 and 11.

Table 10: Attribute

Attribute	Description
Proto	Transport Protocol (ICMP, TCP, or UDP)
SRC IP	Source IP Address
Dest IP	Destination IP Address
Bytes	Number of transmitted bytes
Flags	OR concatenation of all TCP Flags

Table 11: Classes

Class
Normal
Attacker
Suspicious

The data was vast and unbalanced; therefore, data preprocessing is needed. Approximately 13000 entries from each class were included to build the deep learning model. The proposed model is to use a deep learning function as an intrusion detection system names IT security system. Figure 57 below shows the proposed model and the current model, respectively.

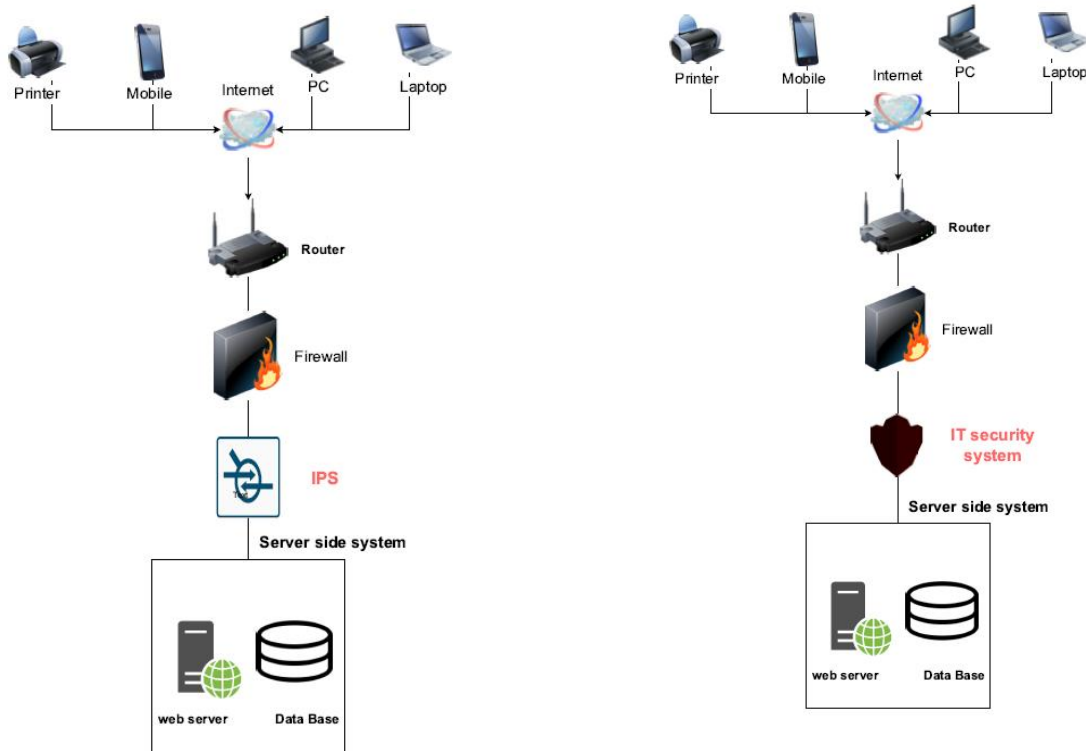


Figure 57: Current Model and Proposed Mode

6.3.2 KNIME

KNIME is used to build the deep learning model after installing the Deeplearning4J extension. The model started by reading the data from excel. After that, the data were normalized by using the Normalizer node; the used method is the Min-Max normalization method, i.e., every value gets transformed into a decimal between zero (Minimum) and one (Maximum). A partitioning node was used to divide the data into two groups, 75% for training and 25% for testing. The training data set was fed to the DL4J Feedforward Learner node. The deep learning model includes the input layer, hidden dense layers, and the output layer. Each dense layer has five hidden neurons, as shown in figure 58 below.

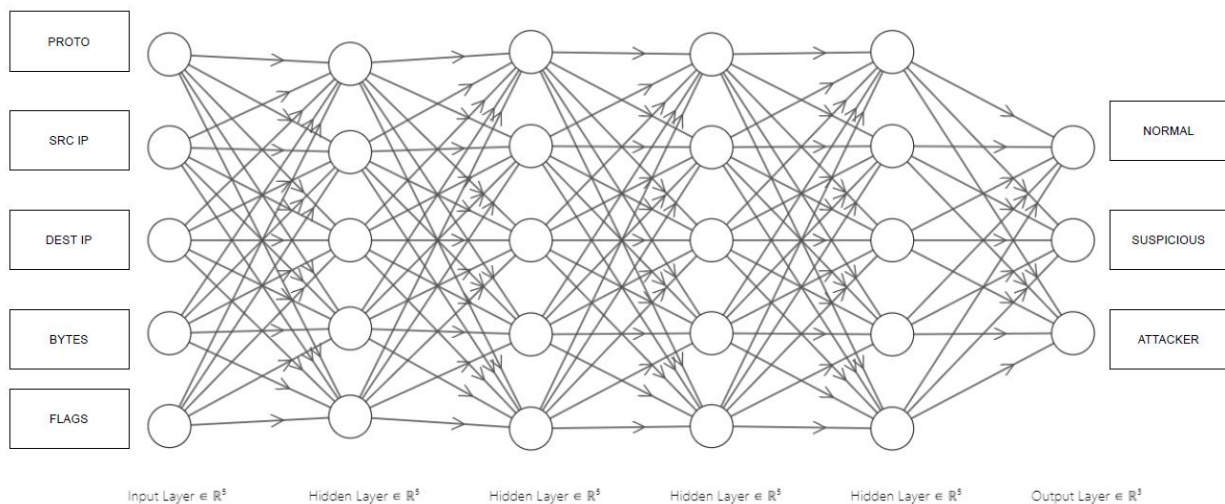


Figure 58: Deep Learning Network

Every connection in the figure has a weight value associated with it, and the weights are the coefficients of the equation, which the model is trying to solve. For example, $W_{(0,0) \rightarrow (1,0)} = 102.7967766$ means that the weight from the first entry in the input layer (PROTO-I) to the first neuron in the first hidden layer is equal to 102.7967766. In addition to the weight values, the Bias

values are calculated. The bias value is a constant that added to the sum of the multiplication of the input values and the weights for each layer using equation 6.1. At the last layer, the computed value is plugged into the activation function (Equation 6.2), which is the sigmoid function to calculate the output.

$$Y = \sum(inputs * weights) + Bias \quad (6.1)$$

$$y = \frac{1}{1+e^{-x}} \quad (6.2)$$

Figure 59 shows the learning status of the DL4J Feedforward learner after running the whole data three times (epochs)

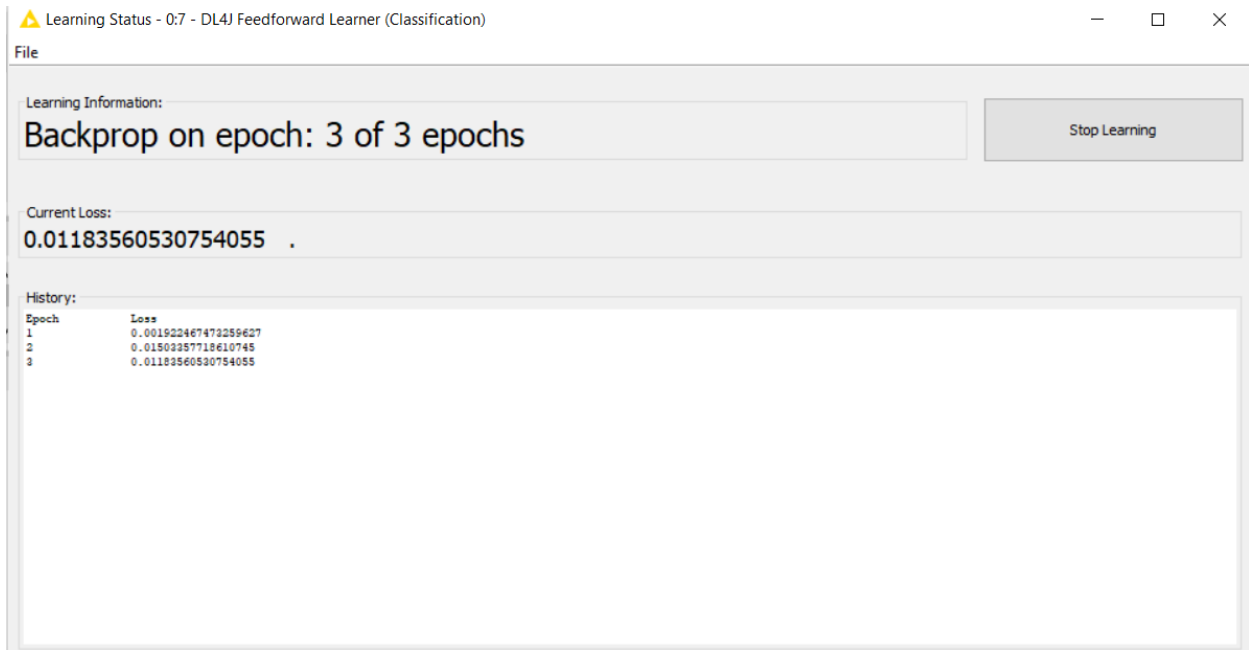


Figure 59: Loss function values after three epochs

The resulting structure of the network is given in matrices format below:

Weights from the input layer to the first hidden layer, 5x5 matrix;

```
wights1 = {  
    {394.3068322,-1.053311483,49.00497418,-0.167013476,-4.447019948},  
    {-118.9628701,66.30989775,411.7725691,-1.036308753,2.733838129},  
    {203.7897336,-40.2064447,-34.49233941,-3.950707989,3.042617236},  
    {-1161.506735,-516.5189531,120.7352643,677.4548411,-200.4279877},  
    {-79.38716773,-89.7745567,-275.7970629,-2.361262458,-1.48213827}  
};
```

The Weights from the first hidden layer to the second hidden layer, 5x5 matrix;

```
wights2 = {  
    {-9.43701466,8.253526339,-1.737350794,0.79112369,-4.988862106},  
    {-1.603391266,-7.468054011,-5.837837482,2.538804395,10.67340188},  
    {0.14706077,-6.803878604,0.661491803,-7.368886695,17.67319301},  
    {2.820723302,10.64427855,2.784906857,-0.557489512,-7.388670404},  
    {1.898568647,10.11958931,-2.874822041,7.666491127,-20.60661497}  
};
```

The Weights from the Second hidden layer to the output layer, 3x5 matrix;

```
wights3 = {  
    {11.09637648,56.5534078,15.4931129,-54.04836808,-15.21773749},
```

{10.85672239,-110.9493808,-43.82861688,5.852451855,39.54382006},
 {-36.49846778,-162.9104677,51.93593807,5.002416757,-38.10868111}

};

The biases values for each layer are given in the three metrics below;

bias1 = {-0.342678063,-2.194959016,-0.306286646,0.378097173,1.753450137};

bias2 = {0.248689595,-0.268876518,-0.718459265,-3.564570161,-0.276645481};

bias3 = {-0.093365573,-0.338820489,0.31561954};

The testing data set was fed into the DL4J Feedforward Predictor node to test it using the output model from the DL4J Feedforward Learner node. The classified data includes **P(class=normal)**, **P(class=Suspicious)** and **P(class=attacker)** As shown in table 12 below. For example, if the **P(class= normal)** is the maximum, then the **Prediction class** is normal.

Table 12: Output Example of the DL4J Feedforward Learner node

Class	P(class=normal)	P(class=Suspicious)	P(class=attacker)	Prediction (class)
normal	1	2.04E-05	1.28E-07	normal
attacker	0	1	1.40E-11	suspicious
attacker	0	3.90E-04	0.999613908	attacker

In the end, A scorer node was used to calculate the accuracy of the model by comparing the **Class** column to the **Prediction (class)** column. The accuracy of the model is 98.539%, as shown in figure 60 below. Also, Figure 61 is a screenshot of the complete model.

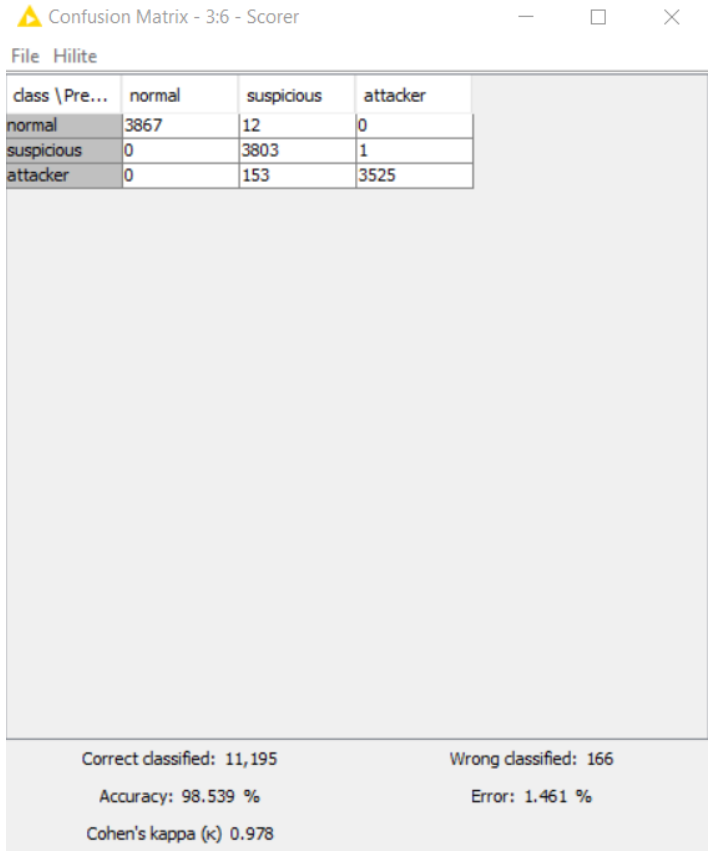


Figure 60: The Accuracy Results

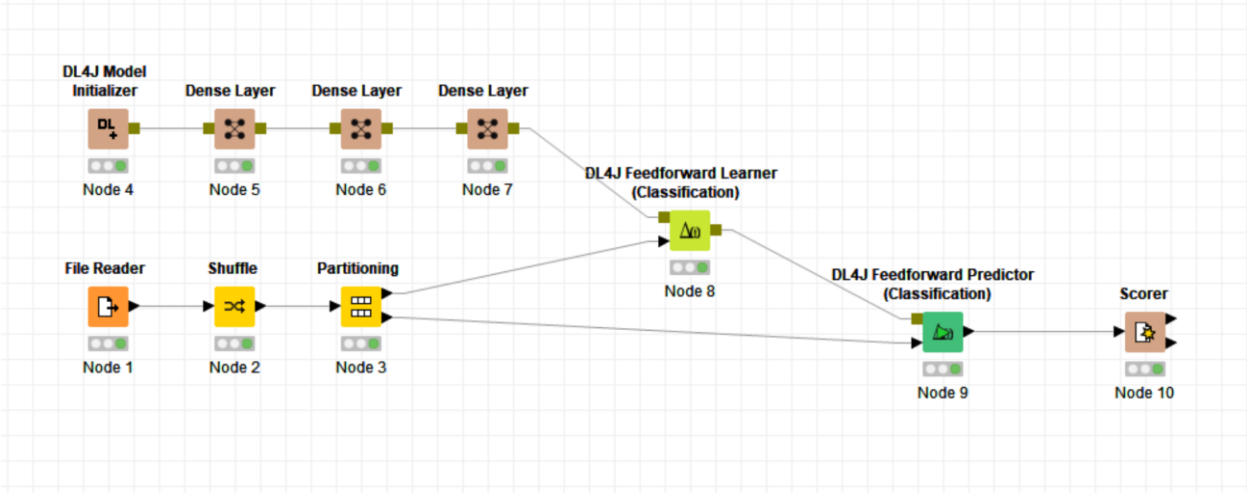


Figure 61: KNIME Model

6.3.3 Agent-Based Simulation

The main difference between the previously described model and the one in this section is the addition of a new Agent Type called the IT Security System with a population size of one. The interactions between agents, with the addition of this one, are presented in Figure 62.

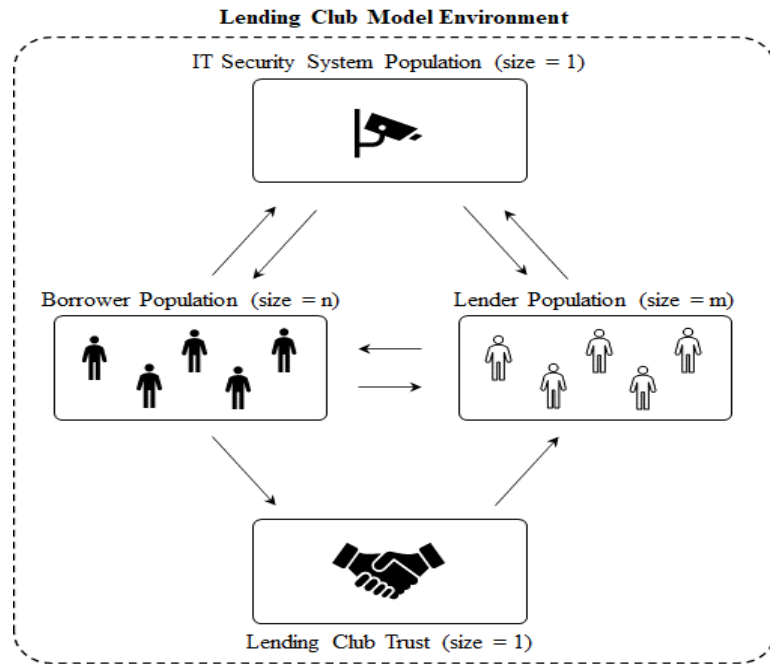


Figure 62: Upgraded ABM Environment and Agent Interactions

The difference between Figure 43 and Figure 62 is that now the borrowers and lenders are interacting with the new IT Security System agent with two-directional interactions. The new agent's state-chart is presented in Figure 63.

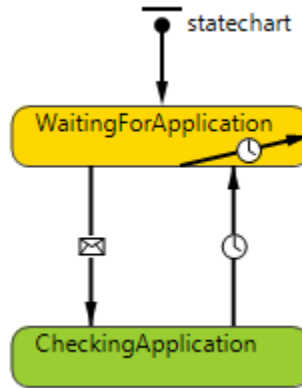


Figure 63: IT Security System' State-Chart

Referring to Figure 44, once borrowers and lenders reach the state *FilledApplication*, unlike in the previous model, the borrowers' and the lenders' applications are sent to the IT Security System Agent and stored in a list. Every minute through the timeout transition inside the *WaitingForApplication* state, the IT Security System Agent checks whether the list of applications is greater than 0. If so, it sends a message to itself to move from its initial state *WaitingForApplications* to the state *CheckingApplications*.

It is at this moment that the IT Security System uses its "Classifier" function, which is the reflection of the previously described Deep Learning exercise. This function takes as input borrower/lender parameters. Hence, in this model, new parameters are added at initialization, including the Port, Source IP, Destination IP, Bytes, and Flags. These parameters are defined using the Deep Learning exercise's normalized datasets. The java function runs the applicant's profile by taking the presented input parameters. The output is whether the applicant is blocked as an attacker or allowed to proceed in the Lending Club. This upgrade is expected to reduce the number of allowed attackers in the system and also reduce the number of blocked non-attacker applicants that could otherwise be value-adding borrowers/lenders that are not attackers.

6.4 Addition of Blockchain

The third proposed model is adding Blockchain on top of the Deep learning IT security System. The process flow of the proposed model is listed below:

- Borrower creates an account and uploads his data, FICO for the first time only, ID, employer, bank account ...etc
- A block is created for the user and added to the blockchain, which results in a private key and a public key (Crypto-currency method). The public key is used for viewing the applicant's history; the private key is used to access and modify the user data.
- The borrower submits a loan request with his public key; a smart contract is initiated, which holds the request and the borrower information.
- The interest rate is calculated, then the user is asked to agree or reject.
- Lenders create accounts in the same manner as users.
- Lenders view the loan requests and accept what he/she wants after checking the user data/history using the user public key.
- When the lender chooses to fund a borrower, the smart contract gets executed and withdraw money from a lender account and deposit the money into the borrower account.
- The smart contract then will keep withdrawing the monthly/weekly payments from the borrower account and deposit the payment into the lender account.

Blockchain's addition has two main impacts:

1. Transparency increases; hence, borrowers cannot be falsely advertised. This will result in a higher trust than the other two previous models. In modeling terms, the posted grade

variable is now always equal to the actual grade. As a result, the trust level variable within the Lending Club's Trust Agent will no longer be negatively impacted.

2. The duration of process applications becomes faster. Most processes are streamlined, and thus the 7 business days previously presented are no longer necessary.

6.5 Agent-Based Model Results

As the model is running, statistics are tracked. These include the different statuses of the borrowers in the system. Results are presented both numerically (Figure 64) and graphically (Figure 65).














 Potential Borrower	0	 Disagreed with Interest Rate	139
 Blocked Hacker	26	 Awaiting Lender	0
 Allowed Hacker	2	 Fully Paid	0
 Blocked non-Hacker	53	 Funded	292
 Under Review	0	 Repaying Loan	488
 Blocked Application	53	 In Default	0
 Screened	0		

Figure 64: Numerical Results Example

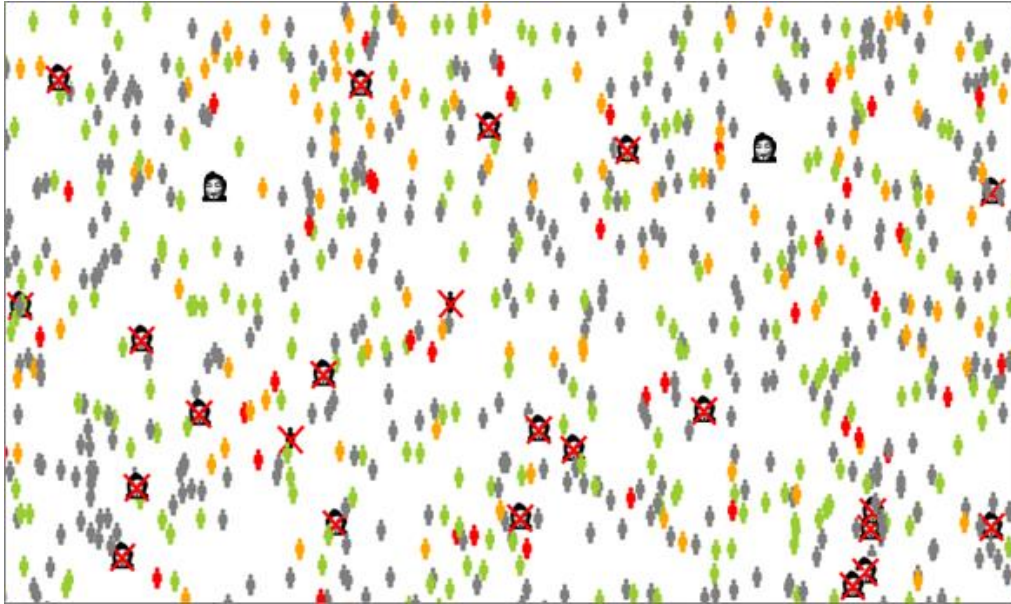


Figure 65: Graphical Results Example

The three scenarios are developed and run, and their results are compared. To be able to compare the results between the different models, a fixed number of initial borrowers and investors is assumed. One thousand of each is added to the model, and the model is left running until all agents reach end states. To achieve meaningful results, since the model contains several stochastic components, AnyLogic's Parameter Variation's freeform experiment type is used. The latter allows us to run each of the three models 100 times with different seeds, and the average of the 100 runs is used for analysis. Using radio buttons, the different scenarios can be interactively chosen through a friendly Graphical User Interface. Moreover, statistics elements are used, which allow us to collect the results with statistical information (e.g., mean, standard deviation, mean confidence, etc.). A sample of the run window is shown in Figure 66.

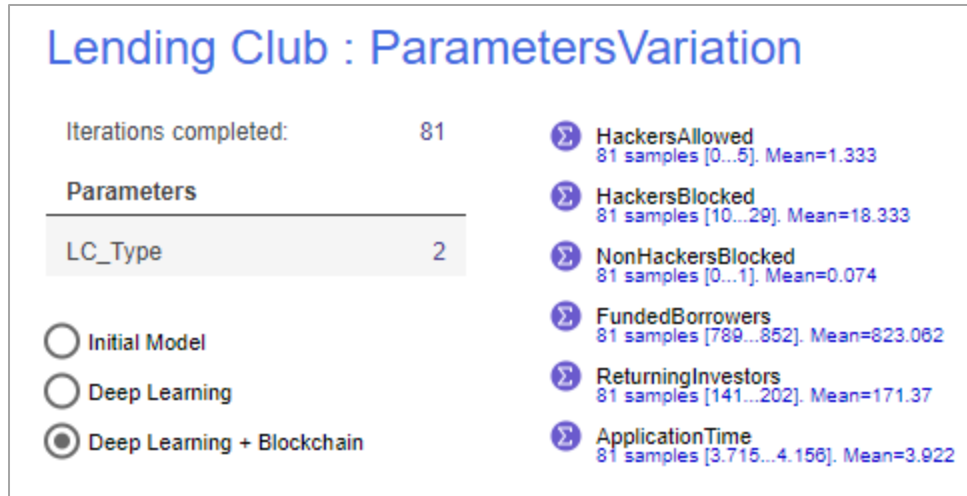


Figure 66: Sample ongoing Parameter Variation run

Five metrics are used to evaluate the performance of the Lending Club. These are summarized in Table 13.

Table 13: Lending Club Models Metrics

Metric	Description
Funded Applications	The Lending Club’s primary objective is to generate revenue. Naturally, the more applications are funded, the better the performance. Two main factors impacting the number of funded applications are the thoroughness of the blocking hackers' mechanism and the lending club's trust/reputation.
Blocked/Allowed Attackers	Allowing attackers in the system may result in stolen money or stolen ideas. Ideally, all attackers should be blocked.
Blocked Non-Attackers	Blocking non-attackers will have a negative impact mainly by reducing the number of opportunities for funded applications.
Repeat Lenders	Repeat lenders mainly reflect trust and Lending Club’s reputation. The higher the trust and the better reputation, the higher the tendency to have repeat lenders.
Application Process Duration	The application process takes time as it requires paperwork, internal review, etc. Using blockchain can streamline this process.

The above metrics are generated for each of the three models, and results are summarized below. The number of highest funded applications was found for the model combining both Deep Learning and Blockchain, followed by the one including Deep Learning, and finally followed by the current model. As deep learning results in higher accuracy in attacker detection (whether blocked attackers or allowed non-attackers), the number of applications making it to the system (whether borrowers or lenders) is higher. Moreover, the addition of blockchain, on top of deep learning, proved to improve results even further as it increases transparency and consequently trust/reputation, which increases the number of repeat lenders but also increases the chance of matching lenders and borrowers, given that lenders would feel more comfortable funding a larger number of borrower profiles instead of sticking only to the safest ones. The results of the three models are represented in Figure 67 to Figure 71.

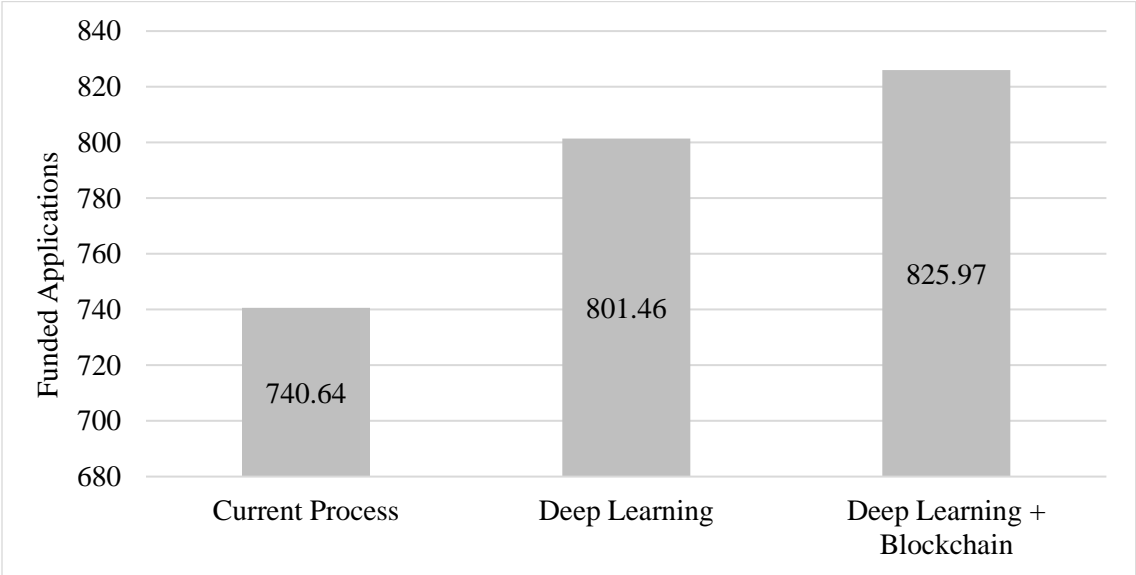


Figure 67: Number of funded applications

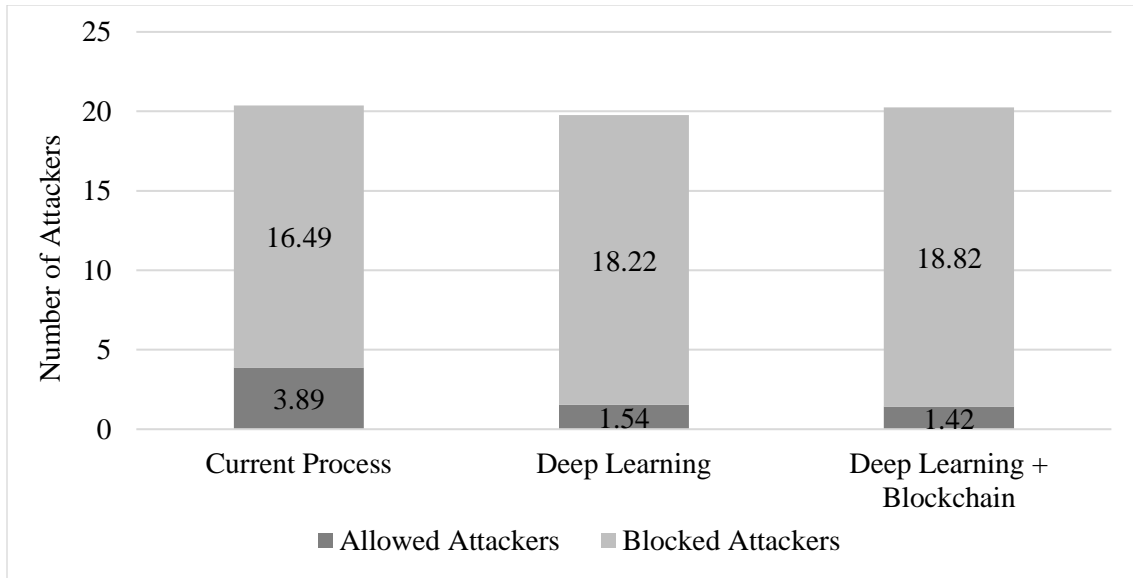


Figure 68: Number of Attackers

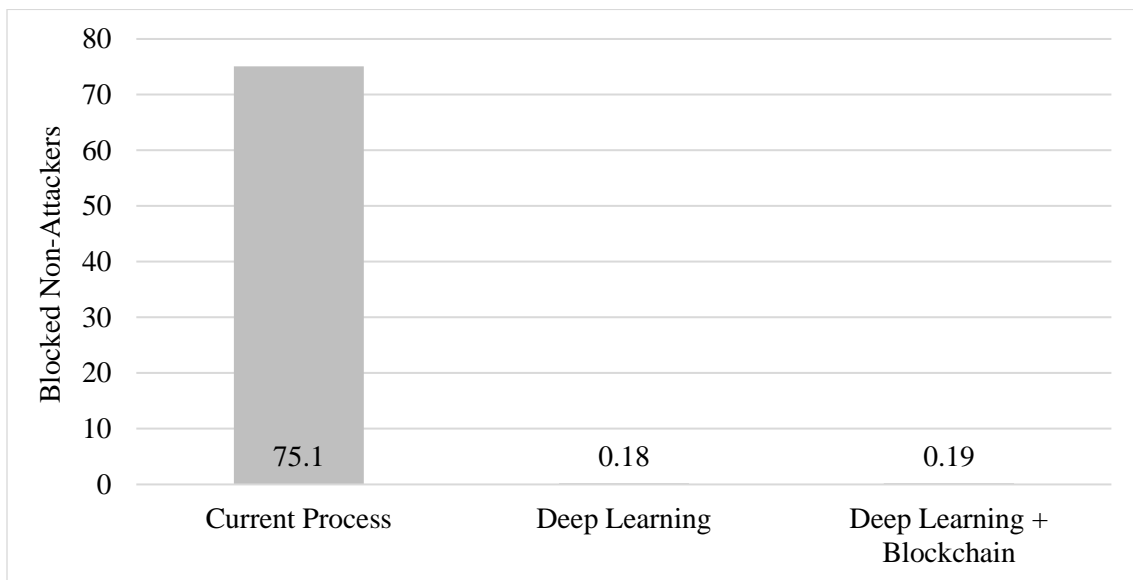


Figure 69: Blocked Non-Attackers

Regarding the number of blocked attackers and blocked non-attackers, it is the deep learning IT Security System that contributed the most given that the results differ between the second and the third model is minimal compared to the first model.

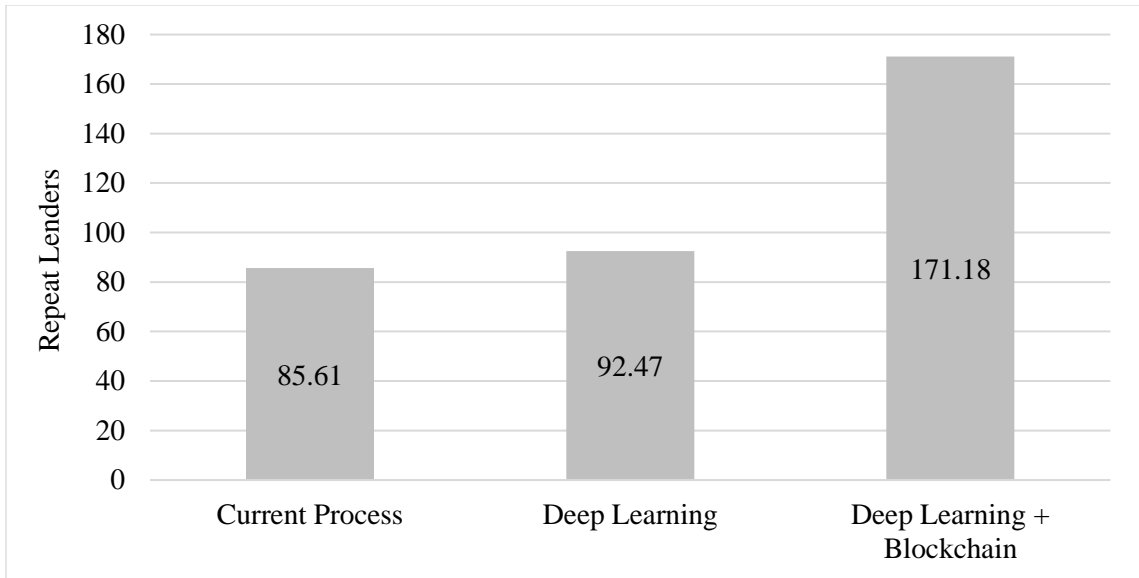


Figure 70: Repeat Lenders

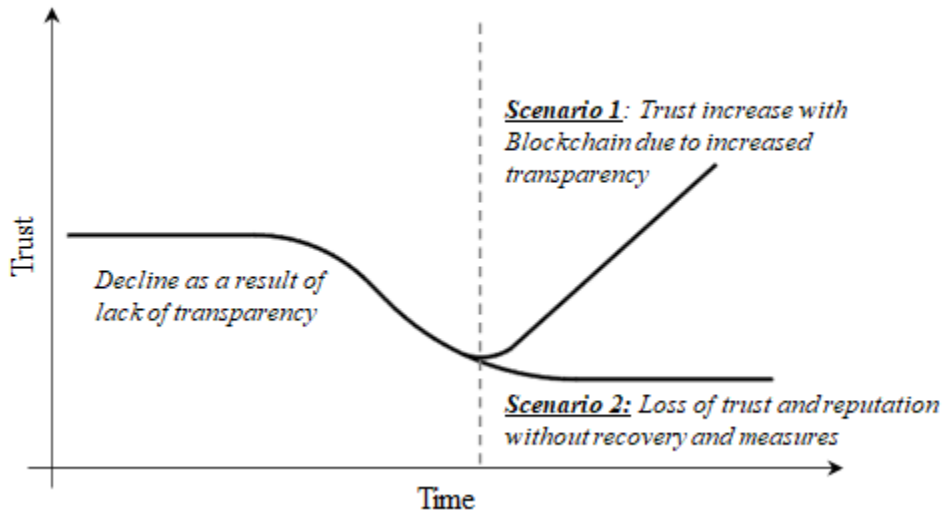


Figure 71: Trust change over time under different scenarios

As for repeat lenders, although improved as a result of the addition of the IT Security System, it was mostly improved as a result of blockchain's transparency, which improved trust.

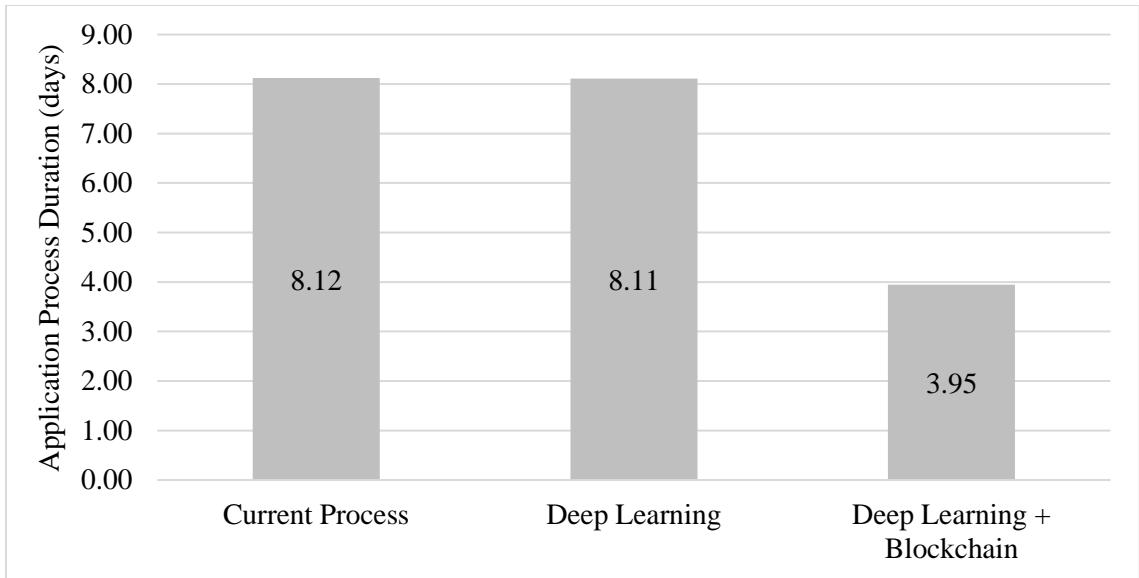


Figure 72: Application Process Duration

Lastly, blockchain also considerably improved the duration for applications to be processed, as shown in Figure 72.

6.6 Blockchain Breaches and Analysis

Since Blockchain emergence in 2008, blockchain technology has demonstrated tremendous opportunities for usage and implementation. Although Blockchain technology is considered to offer a safer and more transparent environment than other centralized systems, whether it should be implemented is still a legitimate question because the technology is relatively new.

There are several obstacles for the Blockchain to overcome the protection and privacy concerns in utilizing this technology and in potential developments. Blockchain can be used in various aspects, and it is important to tackle security and privacy issues in those industries that may use Blockchain in their field.

Different threats can be found on the blockchain system. These threats include double-spending, mining pool, blockchain network, and smart contract security threats. In addition, an example will be presented in the context of each threat. As the use of blockchain technology is embraced by more industries, there is an increasing need for recognizing the threats the blockchain system possesses (Mosakheil, 2018).

A double-spending attack threat is when there is a double usage of the same cryptocurrency amount in other transactions. Due to the transitional time between each transaction, the attacker can initiate a double-spending attack by sending the same cryptocurrency amount back to themselves in a very short amount of time, which can slip out of detection for this type of attack. For example, John sends William money to buy a product or service, William then ships the product to John; if the nodes create a longer trail until a confirmation is sent, then the node can contain a reversal of that same transaction, and William will be out of his money and the goods he just shipped (Karame et al., 2012).

A mining pool security threat is where there is an intrusion in the mining of cryptocurrency process. Digital coins can be electronically retrieved in the mining process using computer software. A community of miners create mining pools to operate collectively using high computation power, pool their resources and add to the creation of a block on the blockchain, and then divide the block payout accordingly. Multiple attack methods can exploit the vulnerabilities of the pool mining process, which can occur internally or externally (Conti et al., 2017).

In the mining process, the attack vectors originate from dishonest miners who are looking for a higher payout, which can be done by withholding a solution of the block to the network of miners or keeping a block private without publishing to the chain network. This can impede on the normal function of the pool mining process because it forces other miners to discard their blocks

and lose profit. The adversary goal of the vector attacks is to bankrupt the mining pool and retrieve all compensation for the attacker. For example, in an internal selfish mining attack, a miner identifies a block, the attacker decides to mine the block but keep it private, the honest miner can find the block and mine on top of it, the attacker now gains the reward. In-band payment through forking, in which an attacker attempts to bribe via Bitcoin by creating a fork containing bribe money to any miner accepting the fork, is a major external threat to the mining pool (Mosakheil, 2018).

The blockchain network threats can also be compromised if nodes on the blockchain network are attacked. The key responsibility of nodes is to store the most current transaction history that contributes in protecting the integrity of the Blockchain network. A major external threat to the blockchain network is distributed denial of service (DDoS), in which the attacker can flood the system by utilizing more than one server or IP address or can crash the system from legitimate users, therefore, denying service. Another possible attack on the blockchain is through transaction malleability (Mosakheil, 2018). Transaction malleability is an attack that allows an individual to change the unique number of a Bitcoin transaction prior to actual verification or confirmation. This modification allows the attacker to assume that a transaction has not occurred.

Smart contracts security threats are codes that are recorded and immediately activated on a blockchain when specified contract terms and agreements have been met. Ethereum is a platform that allows users to create and execute decentralized apps, including smart contracts as well as other applications. When a smart contract is added to the blockchain, it cannot be changed unless the smart contract is defective in the course code under which it becomes susceptible to attacks such as immutable bugs and additional hits to steal Ether or to render it unredeemable by

any individual. An example of a smart contract attack is the Decentralized Autonomous Organization (DAO) attack. The DAO was a project aimed at decentralizing the financial support of Ethereum projects. The DAO attack occurred when a hacker identified a flaw in the DAO's code and managed to drain 3.6 million ethers into their own account. The attack occurred when the smart contract gets stuck calling the "fallback function," which causes the contract to think no funds have been received by the attacker and allows the withdrawal of all the funds from the contract. This flaw and attack were also an effect of the attacker's balance not being updated automatically (Buterin, 2014).

A case study titled "Systematic Approach to Analyzing the Security and Vulnerabilities of Blockchain Systems" was completed by Jae Hyung Lee (2019) on the evolving cyber-attacks and hacks that occurred on the blockchain system between 2011 and 2018. The research examines 78 recent blockchain heists and lists the blockchain system vulnerabilities and possible security recommendations (Lee, 2019). Figure 73 below is an illustration of the four security domains of the Blockchain system and are categorized by their entry points.

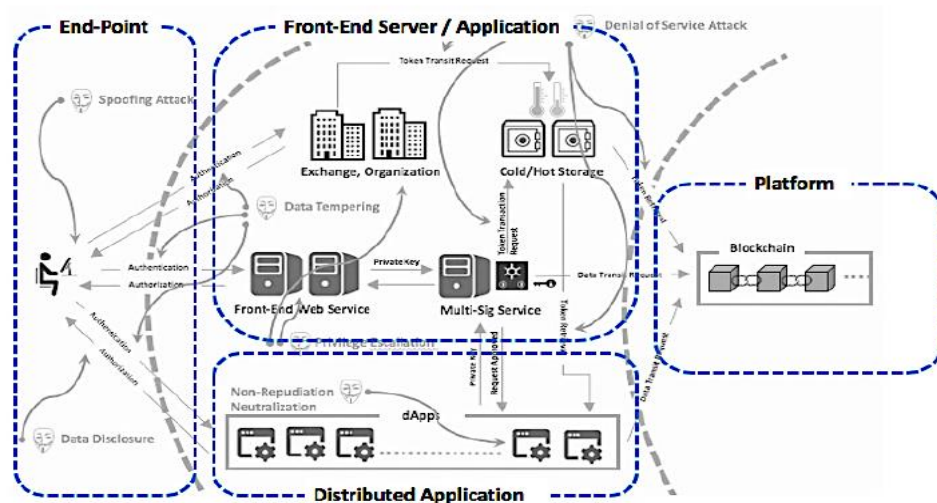


Figure 73: The Blockchain system security domains (adapted from Lee,2019)

The Platform domain includes the blockchain elements such as nodes (users) and shared data. This domain had a total of 17 attacks. The Front-end server domain includes a server and an application such as a web server for a digital wallet, or a third-party security solution, cryptocurrency exchange servers, and online-based storage; this domain had a total of 41 attacks. The Distributed application (dApps) domain includes mostly proprietary applications that run based on Blockchain; this domain had a total of 3 attacks. The End-point domain includes terminals, computers, or even mobile devices through which users communicate with a blockchain system for usage and services; this domain had a total of 17 (Lee, 2019).

To be able to understand the nature of the attacks, 25 of them are explained below:

1. In June 2011, Mt. Gox, the largest Bitcoin exchange at the time, was exploited through a computer of a system auditor, and the bitcoin amounts were changed to one penny. About 2,000 bitcoins were purchased by the attacker, then were sold for cash instantly. They estimated the loss at \$30,000. The attack happened on the Endpoint hacking domain.
2. In July 2011, Bitomat. Pl, a Poland based bitcoin exchange, lost \$222,000 when a breach caused the removal of the Bitcoin Wallet. Since the Bitcoin Wallet data was not backed up, the bitcoin exchange lost everything in the wallet. The breach happened on the Platform Breach domain.

3. In July 2011, MyBitcoin, a cryptocurrency wallet service provider, had security flaws, which caused an attacker to forge Bitcoin deposits through the Shopping Cart Interface and withdrew Bitcoins that amounted to \$833,000. The attack happened on the Platform Breach domain.

4. In October 2011, Bitcoin7, the 3rd largest Bitcoin Exchange, lost \$25,000 from cyber-attacks that occurred in Russia and Europe. The attackers hacked into the infrastructure and stole wallets and personal data from the database. The attack happened in the Access Point Attack domain.

5. In March 2012, Slush Pool, a Bitcoin mining pool, became a victim of a wallet hacking attack that caused a loss of \$14,760. The hackers attacked the Linode server (a cloud web host service provider) and hacked Bitcoin wallets of Slush Pool who were serviced by Linode. The hacking happened on the Access Point Attack domain.

6. In July 2012, BTC-E, a cryptocurrency exchange founded in Russia, was compromised through a broken API secret key. Due to the 16-digit key being an inadequate secret key, the attacker stole an estimated \$35,000 in forged deposits using the hacked API key and purchased large amounts of Bitcoin. The attack occurred on the Platform Breach domain.

7. In September 2012, Bitfloor, the 4th largest Bitcoin exchange, was hacked. The hacker was able to gain access to the cloud servers of the exchange and was able to acquire un-encrypted

wallet key backups. This resulted in a loss of approximately \$250,000. The hacking occurred on the Access Point Attack domain.

8. In March 2013, Bitinstant, a bitcoin brokerage, was hacked by DNS hijacking. After gaining control of the DNS registrar, the attacker gained control over the brokerage email and requested password resets for the exchange accounts. The attacker was able to extract the funds from the accounts, which resulted in a loss of \$12,000 worth of Bitcoins. The attack occurred on the Access Point Attack domain.

9. In May 2013, Vircorex, an alternative cryptocurrency exchange provider, was hacked and lost an estimated \$163,000. The intruder was able to gain login identifications and then accessed the VPS (Virtual Private Server) control account and sent a request to reset the password for all servers. The attacker then drained the reserved funds of the hot and warm wallets of the exchange, which caused a significant loss. The attack occurred on the Access Point Attack domain.

10. In July 2013, Bitfunder, a cryptocurrency platform, had flaws in the codes, which resulted in crediting accounts from multiple Bitcoin Exchanges. The loss was estimated at \$775,000. Jon Montroll, the creator of BitFunder, was charged with running unregistered trading of securities that defrauded consumers by suspected fraudulence of bitcoins. The incident occurred on the Access Point Attack domain.

11. In October 2013, Inputs.io, a bitcoin web wallet, was hacked and reported a loss of \$1,000,000 in two separate attacks. By resetting the password, the attacker could reach an old

email address in an unidentified way and take control of the account. Then, the attacker manipulated the company's two-factor authentication system and breached the database containing wallet info and account information by leveraging a server-side flaw. The incident occurred on the Endpoint Hacking domain.

12. In November 2013, Bitcash.cz, a Czech Republic-based bitcoin exchange, was hacked and lost \$100,000. The attacker sent phishing emails to users as a member of staff. The phishing email was accepted by about 4,000 recipients, who then transferred their bitcoins to the attacker's address. The hacking occurred on the Endpoint Hacking domain.

13. In November 2013, Picostock, a cryptocurrency exchange, was hacked, and it lost \$6,000,000. An old access key was used by the attacker, which had not been revoked and remained active for a long time. It allowed the attacker to transfer funds from hot and cold wallets to his own wallet address. The hacking occurred on the Endpoint Hacking domain.

14. In March 2014, FlexCoin, an electronic wallet provider, was attacked and lost all of the funds totaling \$700,000. Under a new account, the attacker was able to log into the flexCoin from the front-end and exploited a defect in the code that enabled transfers between users of Flexcoin. The attacker then transferred coins from one user account to another by submitting thousands of sequential requests before the sender account was overdrawn. Nothing was suspected due to the accounts not being updated at that time. This attack occurred on the Access Point Attack domain.

15. In March 2014, Poloniex, a cryptocurrency exchange, reported a loss of 12.3 % of its cryptocurrency supply, which totaled a loss of \$50,000. The hacker found a security issue in the withdrawal process of the company. When a customer puts many withdrawal orders quickly, the server processes the withdrawal without confirming the balance first, which caused the loss. This hacking occurred on the Platform Breach domain.

16. In October 2014, Justcoin, a Norway-based cryptocurrency exchange, was exploited because of the weakness of "tfPartialPayment" in the Ripple and Stellar roles. The loss was estimated to be \$300,000. This feature was designed to manage transactions by providing access to the hot wallet-stored funds of the network. Ripple imposes the responsibility on Justcoin's deployment and gateway validation. The gateway configuration directions from Ripple did not clarify the problem correctly. This incident occurred on the Platform Breach domain.

17. In October 2014, BTC-E, a cryptocurrency trading platform, reported its second attack. An attacker was able to take over 568,355 accounts and withdrew an estimated \$26,000,000. The attacker published a malware connection called Troll Box on the ajax chat program and distributed it to BTC-E users to steal login information. BTC-E's remediation effort to set rules for affected users was not successful in stopping the malware from spreading further because all communication methods was removed to reach and warn the affected users. This attack occurred on the Endpoint Hacking domain.

18. In December 2014, Bitpay, an Atlanta based cryptocurrency payment company, lost \$1,800,000 when it was hacked by a phishing attack. The hacker sent fake emails to the company's CEO from the CFO's email address asking for 5,000 BTC at three different times. In reaction, the company's CEO sent the crypto-currencies off without hesitation. This phishing attack occurred on the Endpoint Hacking domain.

19. In May 2016, Ethereum, TheDAO, being the most promising dApps at that time, were hacked and lost around \$70,000,000 worth of Ethers. A hacker found a way to steal most ICO funds and move them to his address while a developer repaired the dApps. This hacking occurred on the DApps Exploit Attack domain.

20. In May 2016, Gatecoin, a Hong Kong-regulated financial institution, reported it was attacked when the hacker gained access to its multi-sig system and was able to gain control of the cold storage and steal the funds. It is an unusual theft due to the origin of the theft being from the cold storage. The estimated loss is about \$2,000,000. This breach occurred on the Platform Breach domain.

21. In October 2016, Bitcurex, a Poland-based Bitcoin exchange in Europe, reported a hacking incident that caused a loss of \$1,500,000. To determine consumer risk and personal data security, Bitcurex upgraded to a third-party device service. The exchange posted a message that stated the incident management team is focusing on a network improvement and security fixes to back up the system to access their funds. The attacker was able to access the funds at a platform level within

a hot wallet, and in 3 seconds, after the hacker transferred all the funds. This hacking occurred on the Access Point Attack domain.

22. In February 2017, Zcoin, an open-source cryptocurrency exchange, reported an exploitation incident that caused a loss of \$600,000. Zcoin found that a malicious attacker was able to "double-spend" to receive Zcoin multiple times within one transaction initiation. The attacker manipulated the security flaw and exploited it over a few weeks; he stole around \$600,000. This attack occurred on the Platform Breach domain.

23. In June 2017, Jaxx, a Wallet software company, reported a hack which caused a loss of \$400,000. An attacker had targeted users who installed JAXX Wallet on a rooted android device, which disabled most of the mobile OS system's default security settings. Using this method after gaining access to the victims' phones, the hacker extracted a 12-word backup sentence from JAXX Wallets, and pulled out private keys, and then transferred all users' cryptocurrency away from them. This hacking attack occurred on the Endpoint Hacking domain.

24. In July 2017, Bithumb, one of the largest cryptocurrency exchanges based in the Republic of Korea, was hacked due to 31,506 customer data being stolen, which caused an \$870,000 loss. The attacker successfully breached 266 customer accounts, which caused customers to complain that they become victims of "voice phishing" and "identity theft. This hacking attack occurred on the Endpoint Hacking domain.

25. In July 2017, Coindash, a crypto-based social trading platform, was hacked through a discovery that the company's Ethereum address was changed to a fake one. As a consequence, the Ethers were moved from investors' accounts to an unknown party. The loss of this hack caused a \$7,000,000 loss for the company. This occurred on the Access Point Attack domain.

The results of the analysis below are driven for the major 78 attacks:

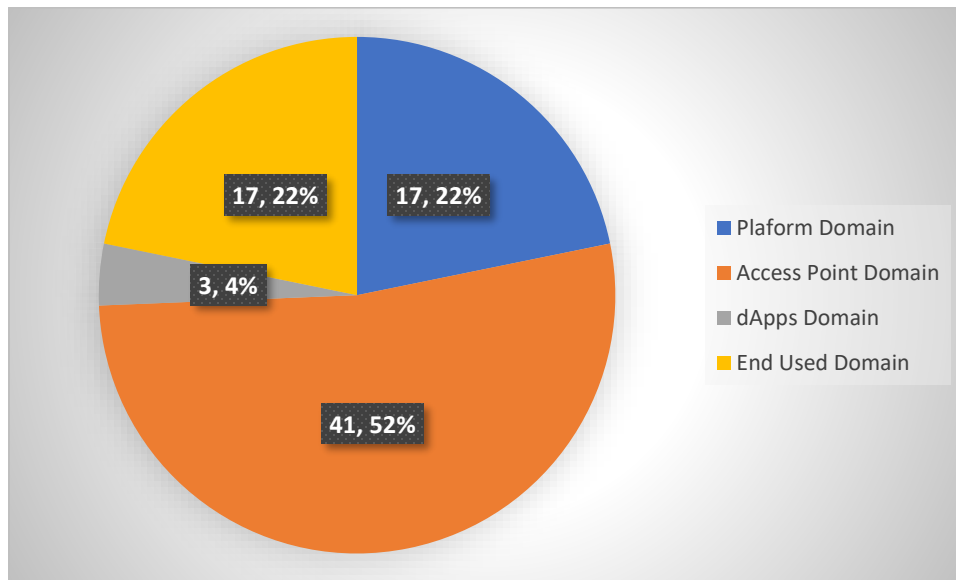


Figure 74: Breakdown of the 78 recent blockchain cyberattacks

Figure 74 above illustrates the percentage breakdown of the 78 recent blockchain cyberattacks and heists that were analyzed. As shown, the domain with the most attacks occurred within the end-point domain. Information is entered as input, sent as a query, then generated as an output in that field, which is considered to be the most vulnerable security point in the data access flow system.

Also, based on Figure 74, the domain with the least cyber-attacks was dApps. However, this does not imply that it is more secure than the rest of the domains. The dApps domain showed

more attacks after 2015, which is when smart contracts were launched. Figure 75 below illustrates the total loss for each domain by year. It is apparent that there is a major spike in the loss in the End-user and Platform domains in the year 2017 and the year 2018.

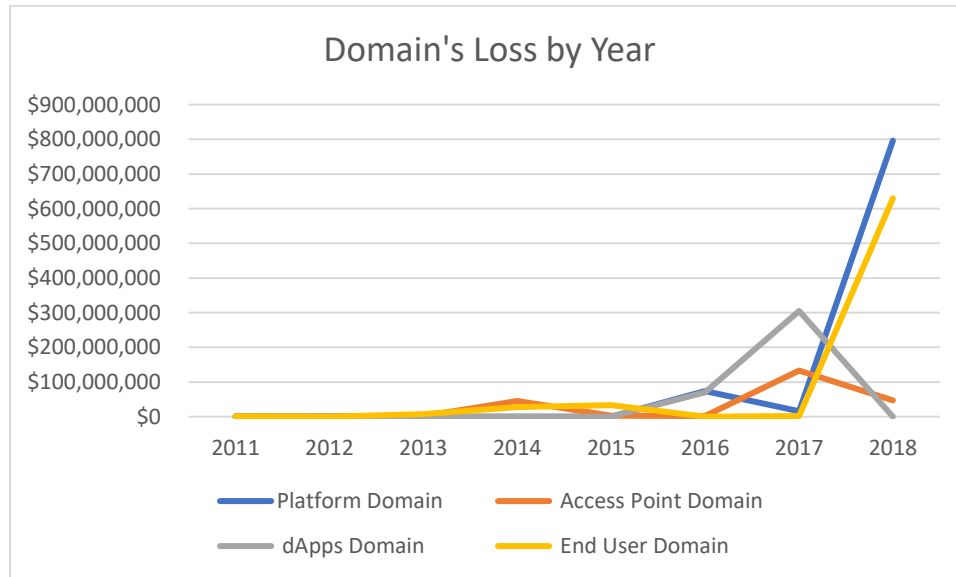


Figure 75: Domain's Loss by Year

Also, Figure 76 below illustrates the total loss every year.



Figure 76: Total Loss by Year

According to the Department of Homeland Security, approximately one-third of all cryptocurrency platforms were hacked. Furthermore, many blockchains systems experienced more than one cyberattack. The multiple cybersecurity attacks on the same system increased to 40% in 2017. Those multiple cyberattacks caused a shutdown of almost half of the affected cryptocurrency exchanges between the year 2009 -2016 (Chavez-Dreyfuss, 2016).

6.7 Conclusion

The success of the business model is dependent on tangible and intangible aspects. Examples of tangible aspects are the number of lenders, borrowers, employees, and services. Whereas examples of intangible aspects are trust, transparency, reputation ... etc. The framework offers a structured approach for integrated design that incorporates processes and technologies and stakeholders to complex systems problems.

The proposed methodology of this study suggests using ABM as a tool to test the implementation of Blockchain into the supply chains and use a case study. Three simulation models were created to conduct a comparison between them regarding cybersecurity and the trust relationship between the involved parties. The comparison results show a positive outcome of the potential implementation of blockchain into the supply chains.

CHAPTER 7. CONCLUSIONS AND RECOMMENDATIONS

This chapter provides a summary of this research, conclusions, limitations, suggested future work, and contributions. The main idea of this research is to assess the implementation of blockchain into supply chains. The supply chain is already complex, and adding such technologies will add more complexity to the system.

7.1 Conclusions

Organizations will be able to deal with big data issues in this era due to the rise of data science by influencing the growth of e-commerce and supply chain dynamics. These improvements have led many technologies to be developed, such as Blockchain and deep learning. Industrial engineers are capable of creating advanced methodologies to combine data from different sources and to deliver the vision needed to build and simulate complex systems and processes such as supply chains.

This research study's main objective is to develop a methodology to assess Blockchain's implementation into supply chains using Agent-based simulation and deep learning. Furthermore, the developed methodology is tested on a case study by using Agent-based simulation.

In this research study, an extensive literature review was conducted covering the main topics: blockchain technology, supply chains, assessment methodologies, simulation and modeling, deep learning. Also, other topics covered in this review covered elements of the Blockchain and smart contract technology. The literature reveals that Blockchain could improve transparency and traceability in data, monetary exchanges and build trust and reputation between

different entities when this technology is implemented in the supply chains; however, all of those are hypothetical claims, and there is no method for assessing that. There is a gap in the research of methodologies that assess Blockchain technology's implementation into supply chains; this gap led to this dissertation research gap.

After the research gap was identified, the research methodology was built to develop a new decision-support system and justify and analyze Blockchain's implementation in supply chain systems using deep learning and agent-based simulation. The methodology was then developed; however, Blockchain's implementation is not feasible and hard to do due to its immaturity, cost, and barriers to adoption. Therefore, a good method to do the assessment is to use agent-based simulation and deep learning.

The justifications for using Agent-based simulation are:

- Complex and stochastic system: Supply chains and blockchain are complex systems. Many interacting autonomous entities can decide how they act based on experience and can make decisions by different actions. Each entity has different needs, objectives, and decision-making behaviors.
- Relationships between entities: Copying entities behaviors: Implementing blockchain in the supply chains displays there are more entities involved and relationships that need to be addressed, which leads to more complexity, such as entities behaviors (reputation), more interactions between entities, and provenance.
- The time between actions: allows for capturing the interactions among several elements over time

- Causal relationships and loops: Diverse variables and components of a blockchain in a supply chain affect each other, and agents can cover causal relationships as equal to system dynamics

And the justifications for using deep learning are:

- Behaviors and trends: Deep learning can offer the detection of behavior and trends found in data. Also, Agents' behaviors and trends are unstructured and stochastic
- Decision Making: Deep Learning Technology offers insight into what can and will occur next through scenario analysis.
- Reputation: Deep learning is capable of learning over time with unstructured data

Figure 77 is a concept map reflecting information about agent-based simulation. To be able to build the simulation model of any supply chain, the steps below need to be followed:

1. Identify the agents, their types, and attributes: Identifying agents(decision-makers) and precisely defining their actions. Agents' interactions and adequate descriptions of them are the keys to a strong agent model structure.
2. Obtain and define every agent's behavior theory: A lot of historical data allows Deep learning to copy those behaviors, and agent-based modeling could reveal more information about agent behaviors.
3. Identify the agent relationships and get a theory of agent interaction by monitoring which, when, and how agents interact.
4. Get an Agent-Based Modeling development strategy.

5. Get the agent-related information needed.
6. Validation:
 - The agent behavior models
 - The model as a whole
7. Run the model and assess the performance from the point of view of connecting the agents' micro-scale behaviors to the system's macro-scale behaviors.

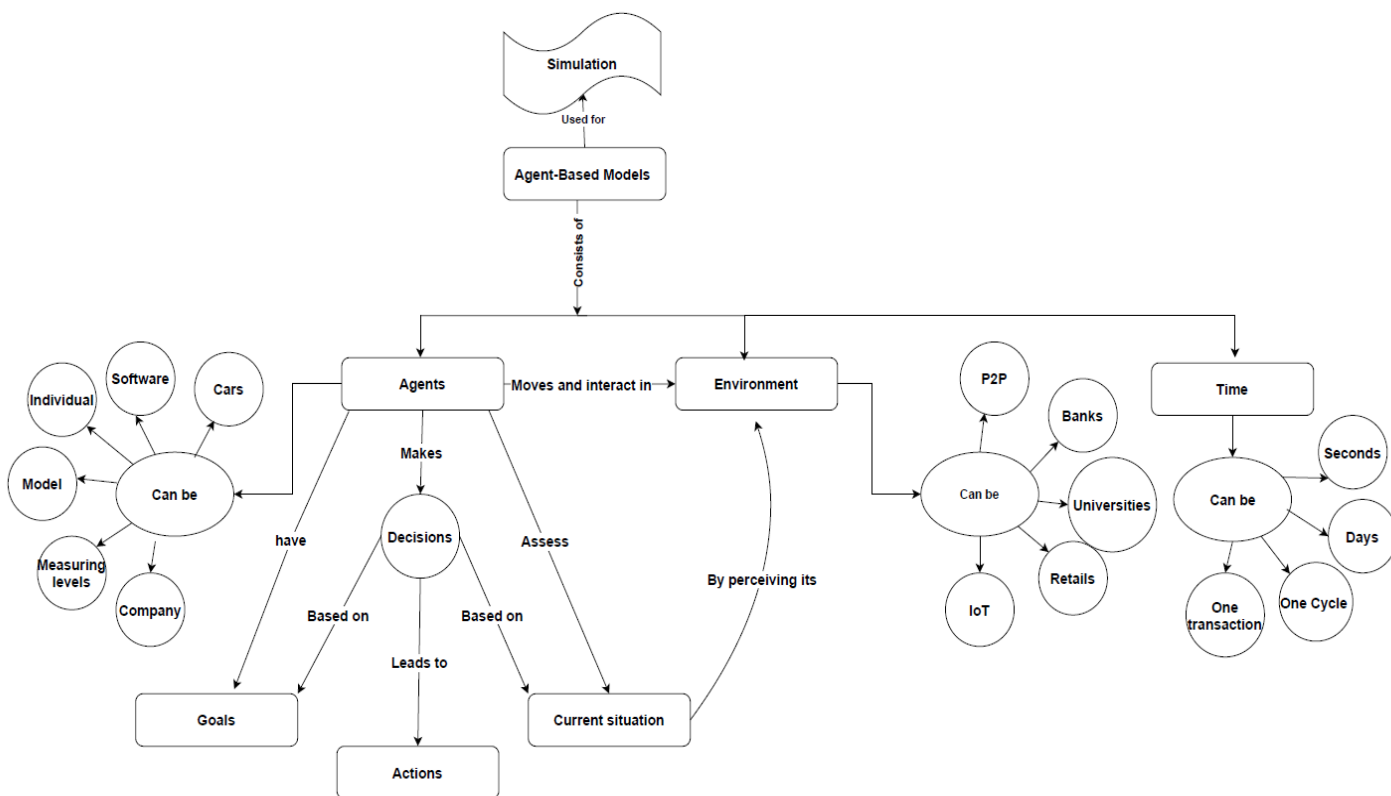


Figure 77: Concept map reflecting information about agent-based simulation

This research, with its combined tools and advanced topics, proved that the major benefit of implementing Blockchain into supply chains is trust, as it got increased between supply chain entities. That conclusion was derived from applying the proposed framework to a case study (Lending Club).

To assess different improvement measures on the Lending Club, the steps mentioned previously are followed to build the Agent-Based Model. To be able to make a comparison and to reach a conclusion, three simulation models are created to reflect three scenarios:

1. Current Lending Club
2. Addition of a Deep Learning IT Security System
3. Addition of Blockchain (on top of the IT Security System)

All developed models mainly represent the interactions between borrowers and lenders within the Lending Club environment, including screening process, loan application, loan funding, and loan repayment. The tracked metrics for scenario assessment include:

- The number of funded applications
- The number of blocked/allowed attackers
- The number of blocked non-attackers
- The number of repeat lenders
- The application process duration

While modeled as an Agent, the Deep Learning IT Security System was fed data from a similar business environment. Deep Learning capabilities were used to copy agents' behaviors and generate a function that can identify whether an applicant is an attacker, suspicious, or

normal based on the applicant's attributes (e.g., IP address). This added an extra layer of reliable security as opposed to the current scenario. In addition to the IT Security System, the third scenario incorporated Blockchain. Blockchain ensures a smooth, streamlined process that enhances transparency, thus highly enabling trust as the main factor. Other benefits are faster processing time for applications. The measure used to prove the increase of trust overtime is boosting the investors' willingness to fund more borrowers. In fact, the number of repeat lenders considerably increased after implementing Blockchain, and the total number of funded applications increased over 8% with the addition of an IT Security System and increased over 11% with the implementation of Blockchain on top of the security system.

The addition of the IT Security System, coupled with the implementation of Blockchain, proved to have great potential in improving the current Lending Process's overall performance and efficiency and enhancing the trust, which is essential to any P2P business. Figure 78 summarizes the conclusion based on the case study.

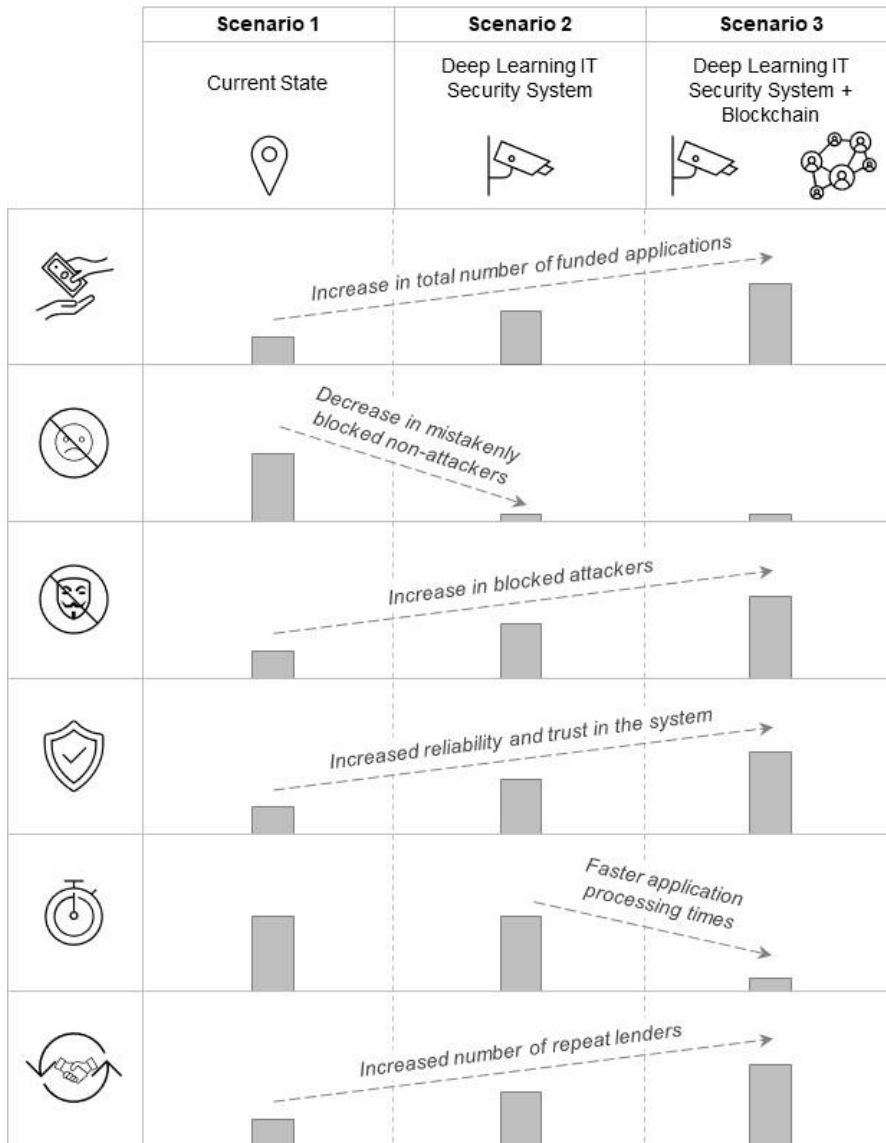


Figure 78: Three scenarios conclusion

7.2 Research Limitations

This research study provided a framework that filled a research gap by testing Blockchain's implementation into supply chains using Agent-based simulation and deep learning. However, like most cases, the researcher faced limitations, and the main limitations are:

1. This research studied only one case-study due to the difficulty and complexity of Blockchain and supply chains.
2. In this research, in consideration for future strategic decision making for companies, the large cost structure of adopting the blockchain is a limitation of this study, and its Return on Investment (ROI) is still up for research to examine whether it will be financially sound or financially profitable for an organization to use the technology.

7.3 Future Research

1. Limitations of using a single case study in this research include the issues of reliability, validity, and generalization. In future research, it is recommended to analyze multiple case studies. For future research, multiple cases should be used to allow for a broader exploration of research issues and theoretical methodologies.

2. Further research is needed to examine the ROI of Blockchain technology more thoroughly. Therefore, we recommend more research to concentrate on risk and to benefit from the flexibility gained in this technological investment to support any organization with strategies and decision-making. Focusing on ROI in the future study can add value to the research and should be embraced by the framework.

7.4 Research Contribution

It appears that there is an absence of an assessment of the implementation of Blockchain in supply chains. Therefore, this research explores Blockchain's application through a technique that combines deep learning and agent-based simulation in supply chains.

This research contributed to many fields, specifically in the field of Industrial Engineering, data analytics, and simulation. The contributions of this dissertation are as follows:

- 1- **Industrial Engineering:** The research provides a unique methodology using Industrial Engineering skills and tools that helps to assess blockchain and smart contract's implementation to improve supply chains and system processes.
- 2- **Data Analytics and Simulation:** This is the first study that presents a deep learning model inside agent-based modeling. In order to recreate trust, we modeled trust, cybersecurity, and processes in supply chains. The use of deep learning and agent-based modeling in that structure is unique.

LIST OF REFERENCES

- Abukhousa, E., Al-Jaroodi, J., Lazarova-Molnar, S., & Mohamed, N. (2014). Simulation and Modeling Efforts to Support Decision Making in Healthcare Supply Chain Management. *The Scientific World Journal*, 2014, 1-16. doi:10.1155/2014/354246
- Agarwal, N., & Hussain, S. Z. (2018). A closer look at Intrusion Detection System for web applications. *Security and Communication Networks*, 2018.
- Aggarwal, C. C. (2018). *Neural networks and deep learning*. Springer
- AgiraTech. (2018, May 30). 3 Types of Blockchain You Need to Know | Blockchain Technology. Retrieved from <https://www.agiratech.com/3-types-of-Blockchain-you-need-to-know/>
- Alcala-Fdez, J., Garcia, S., Fernandez, A., Luengo, J., Gonzalez, S., Saez, J. A., ... & Herrera, F. (2016). Comparison of KEEL versus open source Data Mining tools: Knime and Weka software.
- Alemi-Neissi, A., Baldassi, C., Brunel, N., & Zecchina, R. (2019). Input-driven unsupervised learning in recurrent neural networks.
- Alessandretti, L., Elbahrawy, A., Aiello, L. M., & Baronchelli, A. (2018). Anticipating Cryptocurrency Prices Using Machine Learning. *Complexity*, 2018, 1-16. doi:10.1155/2018/8983590
- Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*.
- Allayannis, George (Yiorgos) and Fernstrom, Aaron, An Introduction to Blockchain. Darden Case No. UVA-F-1810. Available at SSRN: <https://ssrn.com/abstract=3050049>
- Al-Salim, A. M., Lawey, A. Q., El-Gorashi, T. E., & Elmirghani, J. M. (2017). Energy efficient big data networks: Impact of volume and variety. *IEEE Transactions on Network and Service Management*, 15(1), 458-474.
- Amani, S., Bégel, M., Bortin, M., & Staples, M. (2018, January). Towards verifying Ethereum Smart Contract bytecode in Isabelle/HOL. In *Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs* (pp. 66-77). ACM.

- Anderson, K. E. (2016). An Evaluation of Complex Adaptive Evolvable System Simulation (Doctoral dissertation).
- Anderson, M., & Huffman, M. (2017). The Sharing Economy Meets the Sherman Act: Is Uber a Firm, a Cartel, or Something in Between. *Colum. Bus. L. Rev.*, 859.
- Andre, G., Alexandra, D., & Samuel, K. (2018, December). SmarTor: Smarter Tor with Smart Contracts: Improving resilience of topology distribution in the Tor network. In Proceedings of the 34th Annual Computer Security Applications Conference (pp. 677-691). ACM.
- Arthur, W. B. (2018). The economy as an evolving complex system II. CRC Press. *ArXiv:1706.00916 [Cs]*. Retrieved from <http://arxiv.org/abs/1706.00916>.
- Aslam, A., & Shah, M. A. (2017). Taxation and the peer-to-peer economy. International Monetary Fund.
- Ayal, S., Bar-Haim, D., & Ofir, M. (2018). Behavioral Biases in Peer-to-Peer (P2P) Lending.
- Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, 9(10), 533.
- Bailey, B. (2006, February 1). Consider as Many Design Alternatives as Possible: The Value of Parallel Design. Retrieved from <https://www.usability.gov/get-involved/blog/2006/02/parallel-design.html>
- Banks, J., Nelson, B. L., Carson, J. S., & Nicol, D. M. (2007). Discrete-event system simulation. (4th ed., Indian subcontinent adaptation. ed.) Delhi: Dorling Kindersley (India).
- Barzel, B., Liu, Y. Y., & Barabási, A. L. (2015). Constructing minimal models for complex system dynamics. *Nature communications*, 6, 7186.
- Bastani, K., Asgari, E., & Namavari, H. (2018). Wide and Deep Learning for Peer-to-Peer Lending Virginia Polytechnic Institute. Retrieved February 25, 2019, from <https://arxiv.org/ftp/arxiv/papers/1810/1810.03466.pdf>.
- Beamon, B. M. (2008). Sustainability and the future of supply chain management. *Operations and Supply Chain Management*, 1(1), 4-18.
- Berg, J., & Nyström, K. (2018). A unified deep artificial neural network approach to partial differential equations in complex geometries. *Neurocomputing*, 317, 28-41.
- Bhandari, B. (2018). Supply Chain Management, Blockchains and Smart Contracts.

- Bhiih, A., Johnson, P., & Randles, M. (2019). Decentralized iterative approaches for community clustering in the networks. *The Journal of Supercomputing*, 1-24.
- big data: Information measures, applications, and challenges. *IEEE Access*, 7, 100363-100382.
- Boariu, N. "Major Issues Facing Supply Chain Managers," Procurify, 10-Jun-2015. [Online]. Available: <https://blog.procurify.com/2015/06/10/4-major-issues-facing-your-supply-chainmanager/>. [Accessed: 13-Jul-2017].
- Bokhari, M. M. (2019). Credit Risk Analysis in Peer to Peer Lending Data set: Lending Club.
- Bozic, D. (2018, November 23). Supply Chains: Quantifying Social Transparency. Retrieved July 10, 2020, from <https://denisbozic.com/supply-chain-transparency/>
- Brown, C. (2019). Why and how to employ the SIPOC model. *Journal of business continuity & emergency planning*, 12(3), 198-210.
- Bruce, M., Neely, B., Schoeman, E., Veary, T., & Donovan, A. (2002). *U.S. Patent Application No. 09/917,810*.
- Bryk, A. (2017, October 31). Blockchain: Cyber Security Pros and Cons. Retrieved from <https://www.apriorit.com/dev-blog/462-blockchain-cybersecurity-pros-cons>
- Buterin, V. (2014). A next-generation smart contract and decentralized application platform.
- Buterin, V. (2014, January). Slasher: A Punitive Proof-of-Stake Algorithm. Retrieved February 13, 2019, from <https://blog.Ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/>
- Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, 22(1), 616-644.
- Caporale, G. M., Gil-Alana, L., & Plastun, A. (2018). Persistence in the cryptocurrency market. *Research in International Business and Finance*, 46, 141-148.
- Carino, F. M., Del Giorgio, H. R., Abeledo, M. C., Bullian, P., Gonzalez, J., & Hencsek, M. (2018, November). Detection and analysis of vulnerabilities in convergent network platforms. In *2018 Congreso Argentino de Ciencias de la Informática y Desarrollos de Investigación (CACIDI)* (pp. 1-5). IEEE.

- Chang, P. C., Liu, C. H., Fan, C. Y., Lin, J. L., & Lai, C. M. (2009, September). An ensemble of Neural Networks for stock trading decision making. In International Conference on Intelligent Computing (pp. 1-10). Springer, Berlin, Heidelberg.
- Chang, W. (2015). Growing pains: the role of regulation in the collaborative economy. *Intersect: The Stanford Journal of Science, Technology, and Society*, 9(1).
- Chavez-Dreyfuss, G. (2016, August 29). Cyber threat grows for bitcoin exchanges. Retrieved November 16, 2020, from <https://www.reuters.com/article/us-bitcoin-cyber-analysis-idUSKCN11411T>
- Chen, Y. J., Dai, T., Korpeoglu, C. G., Körpeoğlu, E., Sahin, O., Tang, C. S., & Xiao, S. (2018). Innovative online platforms: Research opportunities. *Manufacturing & Service Operations Management*, Forthcoming.
- Cherry, C., & Pidgeon, N. (2018). Is sharing the solution? Exploring public acceptability of the sharing economy. *Journal of Cleaner Production*, 195, 939-948. doi:10.1016/j.jclepro.2018.05.278
- Chollet, F. (2017). Xception: Deep learning with depthwise separable convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1251-1258).
- Cong, L. W., & He, Z. (2018). Blockchain disruption and smart contracts (No. w24399). National Bureau of Economic Research.
- Conley, J. P. (2017). Blockchain and the economics of crypto-tokens and initial coin offerings (No. 17-00008). Vanderbilt University Department of Economics.
- Conte de Leon, D., Stalick, A. Q., Jillepalli, A. A., Haney, M. A., & Sheldon, F. T. (2017). Blockchain: properties and misconceptions. *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(3), 286-300.
- Conti, M., E, S. K., Lal, C., & Ruj, S. (2017). A survey on security and privacy issues of Bitcoin.
- Cotter, F., & Kingsbury, N. (2019). A Learnable ScatterNet: Locally Invariant Convolutional Layers. arXiv preprint arXiv:1903.03137.
- Davis, M. H. (2018). *Markov models & optimization*. Routledge.
- Denoeux, T. (2019). Logistic regression, neural networks and Dempster–Shafer theory: A new perspective. *Knowledge-Based Systems*, 176, 54-67.

- Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7), 1366-1385.
- Distributed Ledger Technology (DLT). IntechOpen.
- Djennas, M., Benbouziane, M., & Djennas, M. (2012). *Agent-Based Modeling in Supply Chain Management: A Genetic Algorithm and Fuzzy Logic Approach*.
- Dos Santos, R. P. (2017). On the Philosophy of Bitcoin/Blockchain Technology: Is it a Chaotic, Complex System?. *Metaphilosophy*, 48(5), 620-633.
- Edwards, C. (2018, June 01). Deep Learning Hunts for Signals Among the Noise. Retrieved from <https://cacm.acm.org/magazines/2018/6/228030-Deep-learning-hunts-for-signals-among-the-noise/fulltext>
- Einav, L., Farronato, C., & Levin, J. (2016). Peer-to-peer markets. *Annual Review of Economics*, 8, 615-635.
- Einav, L., Farronato, C., & Levin, J. (2016). Peer-to-peer markets. *Annual Review of Economics*, 8, 615-635.
- Emmett, S., & Crocker, B. (2016). *The relationship-driven supply chain: creating a culture of collaboration throughout the chain*. CRC Press.
- Fakharzadeh-Naeini, H. (2011). *Integrated Tactical-Operational Supply Chain Planning with Stochastic Dynamic Considerations* (Doctoral dissertation, Université d'Ottawa/University of Ottawa).
- Farmer, J. D., Gallegati, M., Hommes, C., Kirman, A., Ormerod, P., Cincotti, S., ... & Helbing, D. (2012). A complex systems approach to constructing better models for managing financial markets and the economy. *The European Physical Journal Special Topics*, 214(1), 295-324.
- Fillbrunn, A., Dietz, C., Pfeuffer, J., Rahn, R., Landrum, G. A., & Berthold, M. R. (2017). KNIME for reproducible cross-domain analysis of life science data. *Journal of biotechnology*, 261, 149-156.
- FORM 10-K. (2019). *LendingClub Corporation* (United States, UNITED STATES SECURITIES AND EXCHANGE COMMISSION). Retrieved June 8, 2020, from http://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_LC_2019.pdf

- Fukushima, K., & Shouno, H. (2015, July). Deep convolutional network neocognitron: improved interpolating-vector. In 2015 International Joint Conference on Neural Networks (IJCNN)(pp. 1-8). IEEE.
- García-Cáceres, R. G., & Escobar, J. W. (2016). Characterization of supply chain problems. *Dyna*, 83(198), 68-78.
- Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and Smart Contracts for insurance: Is the technology mature enough? *Future Internet*, 10(2), 20.
- Gharib, A., Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2016, December). An evaluation framework for intrusion detection dataset. In *2016 International Conference on Information Science and Security (ICISS)* (pp. 1-6). IEEE.
- Giancaspro, M. (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Computer law & security review*, 33(6), 825-835.
- Giannakis, M., & Papadopoulos, T. (2016). Supply chain sustainability: A risk management approach. *International Journal of Production Economics*, 171, 455-470.
- Gilbert, G., Ahrweiler, P., Barbrook-Johnson, P., Narasimhan, K., & Wilkinson, H. (2018). Computational modelling of public policy: reflections on practice. *Journal of Artificial Societies and Social Simulation*, 21(1), 1-14.
- Gonzalez, L. (2018). Blockchain, Herding and Trust in Peer-to-Peer Lending. Available at SSRN 3297053.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT press.
- Gott, The challenge of complexity in product design and engineering, Cambashi Limited, Cambridge UK, 2005.
- Gray, J., & Rumpe, B. (2016). Models in simulation. *Software & Systems Modeling*, 15(3), 605-607. doi:10.1007/s10270-016-0544-y
- Green, S. (2018). Smart Contracts, Interpretation and Rectification. *Lloyd's maritime and commercial law quarterly*, (2), 234-251.
- Grochol, D., & Sekanina, L. (2018, April). Multi-objective Evolution of Ultra-Fast General-Purpose Hash Functions. In *European Conference on Genetic Programming* (pp. 187-202). Springer, Cham.

- Hartikka, L. (2017, March 04). A Blockchain in 200 lines of code – Lauri Hartikka – Medium. Retrieved February 11, 2019, from <https://medium.com/@lhartikk/a-Blockchain-in-200-lines-of-code-963cc1cc0e54>
- Hassan, S. (2018). Decentralized Research Funding Application: Utilizing Blockchain Technology to Ensure Transparency.
- Havlin, S., Kenett, D. Y., Ben-Jacob, E., Bunde, A., Cohen, R., Hermann, H., ... & Portugali, J. (2012). Challenges in network science: Applications to infrastructures, climate, social systems and economics. *The European Physical Journal Special Topics*, 214(1), 273-293.
- Hewitt, E. (2015). Bringing Continuity to Cryptocurrency: Commercial Law as a Guide to the Asset Categorization of Bitcoin. *Seattle UL Rev.*, 39, 619.
- Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Sunny, M. S. H. (2019). Application of big data and machine learning in smart grid, and associated security concerns: A review. *IEEE Access*, 7, 13960-13988.
- Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Sunny, M. S. H. (2019). Application of big data and machine learning in smart grid, and associated security concerns: A review. *IEEE Access*, 7, 13960-13988.
<http://eprint.iacr.org/2012/248>.
- Hu, X. B., Gheorghe, A. V., Leeson, M. S., Leng, S., Bourgeois, J., & Qu, X. (2016). Risk and safety of complex network systems. *Mathematical Problems in Engineering*, 2016.
- Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. *Procedia computer science*, 98, 461-466.
- J.P. MORGAN. (2017, October 16). J.P. Morgan deploys Blockchain with new correspondent banking network. Retrieved February 9, 2019, from <https://www.jpmorgan.com/country/US/en/detail/1320562088910>
- Jacobsen, H. A., Sadoghi, M., Tabatabaei, M. H., Vitenberg, R., & Zhang, K. (2018, December). Blockchain landscape and AI renaissance: The bright path forward. In *Proceedings of the 19th International Middleware Conference Tutorials* (p. 2). ACM.
- Johnson, C. W. (2006). What are emergent properties and how do they affect the engineering of complex systems?. *Reliability Engineering and System Safety*, 91(12), 1475-1481.

- Joledo, O. (2016). A Hybrid Simulation Framework of Consumer-to-Consumer Ecommerce Space.
- Joledo, O., Bernard, J., & Rabelo, L. (2014). Business Model Mapping: A Social Lending Case Study and Preliminary Work. In *IIE Annual Conference. Proceedings* (p. 1282). Institute of Industrial and Systems Engineers (IISE).
- Joledo, O., Bernard, J., Cisneros, J., & Laval, S. (2013, November). Lending Club - Case Study Analysis. EIN 6182: Engineering Management Final Report.
- Karame, G. O., Androulaki, E., & Capkun, S. (2012). *Two Bitcoins at the price of one? Doublespending attacks on fast payments in Bitcoin* (No. 248). Retrieved from
- Karame, G., & Capkun, S. (2018). Blockchain Security and Privacy. *IEEE Security & Privacy*, 16(4), 11-12.
- KeyCDN. (2019). SHA1 vs SHA256 - KeyCDN Support. Retrieved February 15, 2019, from <https://www.keycdn.com/support/sha1-vs-sha256>
- Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395-411.
- Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2018, November). Decentralized Voting Platform Based on Ethereum Blockchain. In *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)* (pp. 1-6). IEEE.
- KNIME Server. (2018). Retrieved from <https://www.knime.com/knime-software/knime-server>
- Koczy, L. T., Medina, J., Reformat, M., Wong, K. W., & Yoon, J. H. (2019). Computational intelligence in modeling complex systems and solving complex problems. *Complexity*, 2019.
- Konczak, A., & Paslawski, J. (2015). Decision support in production planning of precast concrete slabs based on simulation and learning from examples. *Procedia Engineering*, 122, 81-87.
- Koo, D., Shin, Y., Yun, J., & Hur, J. (2018). Improving Security and Reliability in Merkle Tree-Based Online Data Authentication with Leakage Resilience. *Applied Sciences*, 8(12), 2532.
- Koshiyama, A., Firoozye, N., & Treleaven, P. (2019). Generative Adversarial Networks for Financial Trading Strategies Fine-Tuning and Combination. arXiv preprint arXiv:1901.01751.

- Kozma, T. (2017). Cooperation in the supply chain network. In *Forum Scientiae Oeconomia* (Vol. 5, No. 3, pp. 45-58). Wydawnictwo Naukowe Akademii WSB.
- Lambiotte, R., Rosvall, M., & Scholtes, I. (2018). Understanding complex systems: From networks to optimal higher-order models. arXiv preprint arXiv:1806.05977.
- Landrum, G., & Meinel, T. (n.d.). The KNIME Analytics Platform -- Bringing Science to your Data. Retrieved from https://www.gdch.de/fileadmin/downloads/Veranstaltungen/Tagungen/2016_Tagungen/GCC_2016/Software_Workshop_KNIME.pdf.
- Lanio, K. (2018, August 01). Gartner Magic Quadrant for Data Science and Machine Learning Platforms. Retrieved from <https://rapidminer.com/resource/gartner-magic-quadrant-data-science-platforms/>
- Law, A. (2017). Smart contracts and their application in supply chain management (Doctoral dissertation, Massachusetts Institute of Technology).
- Law, A. M. (2009). How to build valid and credible simulation models. Winter Simulation Conference, 24.
- Lee, E., & Lee, B. (2012). Herding behavior in online P2P lending: An empirical investigation. *Electronic Commerce Research and Applications*, 11(5), 495-503.
- Lee, J. H. (2019). *Systematic approach to analyzing security and vulnerabilities of blockchain systems* (Doctoral dissertation, Massachusetts Institute of Technology).
- Lending Club. (2019, December 31). About Us. Retrieved July 12, 2020, from <https://ir.lendingclub.com/financials/Docs/Index/default.aspx?FilingId=13935526>
- Li, X., & Lau, S. K. (2005). A multi-agent approach towards collaborative supply chain management.
- Lieder, M., Asif, F. M., & Rashid, A. (2017). Towards Circular Economy implementation: an agent-based simulation approach for business model changes. *Autonomous Agents and Multi-Agent Systems*, 31(6), 1377-1402.
- Liu, W., Wang, Z., Liu, X., Zeng, N., Liu, Y., & Alsaadi, F. E. (2017). A survey of Deep Neural Networks architectures and their applications. *Neurocomputing*, 234, 11-26.
- Luo, Z., Li, K., Ma, X., & Zhou, J. (2013). A new accident analysis method based on complex network and cascading failure. *Discrete Dynamics in Nature and Society*, 2013.

- Malak Jr, R. J. (2005). A framework for validating reusable behavioral models in engineering design (Doctoral dissertation, Georgia Institute of Technology).
- Malekipirbazari, M. and Aksakalli, V., 2015. Risk assessment in social lending via random forests. *Expert Systems with Applications*, 42(10), pp.4621-4631.
- Marcus, G. (2018). Deep Learning: A critical appraisal. arXiv preprint arXiv:1801.00631.
- Marr, B. (2018, March 20). Blockchain: A Very Short History Of Ethereum Everyone Should Read. Retrieved from <https://www.forbes.com/sites/bernardmarr/2018/02/02/Blockchain-a-very-short-history-of-Ethereum-everyone-should-read/#57081cc51e89>
- McClelland, C. (2017, December 04). The Difference Between Artificial Intelligence, Machine Learning, and Deep Learning. Retrieved April 17, 2018, from <https://medium.com/iotforall/thedifference-between-artificial-intelligence-machine-learning-and-Deep-learning-3aa67bff5991>
- McDonald, C. (2017, August 23). Demystifying AI, Machine Learning, and Deep Learning - DZone AI. Retrieved April 17, 2018, from <https://dzone.com/articles/demystifying-ai-machinelearning-and-Deep-learning>
- Meadows, M. R. (2017). The Evolution of Crowdfunding: Reconciling Regulation Crowdfunding with Initial Coin Offerings. *Loy. Consumer L. Rev.*, 30, 272.
- Mehrwald, P., Treffers, T., Titze, M., & Welp, I. (2019, January). Blockchain Technology Application in the Sharing Economy: A Proposed Model of Effects on Trust and Intermediation. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
- Meng, X., & Liu, D. (2018). GeTrust: A guarantee-based trust model in Chord-based P2P networks. *IEEE Transactions on Dependable and Secure Computing*, 15(1), 54-68.
- Mikolov, T., Karafiát, M., Burget, L., Černocký, J., & Khudanpur, S. (2010). Recurrent neural network based language model. In *Eleventh annual conference of the international speech communication association*.
- Mishra, P., & Sharma, R. K. (2014). A hybrid framework based on SIPOC and Six Sigma DMAIC for improving process dimensions in supply chain network. *International Journal of Quality & Reliability Management*.

- Montavon, G., Samek, W., & Müller, K. R. (2018). Methods for interpreting and understanding deep neural networks. *Digital Signal Processing*, 73, 1-15.
- Moosavi, S., & Clark, J. (2018, February). Ghazal: toward truly authoritative web certificates using Ethereum. In *International Conference on Financial Cryptography and Data Security* (pp. 352-366). Springer, Berlin, Heidelberg.
- Mosakheil, J. H. (2018, May). *Security threats classification in blockchains*. Culminating Projects in Information Assurance. https://repository.stcloudstate.edu/msia_etds/48/
- Munir, M., Jajja, M. S. S., Chatha, K. A., & Farooq, S. (2020). Supply chain risk management and operational performance: The enabling role of supply chain integration. *International Journal of Production Economics*, 227, 107667.
- Mykoniatis, K., & Angelopoulou, A. (2020). A modeling framework for the application of multi-paradigm simulation methods. *SIMULATION*, 96(1), 55-73.
- Nadeem, A., & Javed, M. Y. (2005, August). A performance comparison of data encryption algorithms. In *2005 international Conference on information and communication technologies* (pp. 84-89). IEEE.
- Nielsen, A. A., & Voigt, C. A. (2018). Deep learning to predict the lab-of-origin of engineered DNA. *Nature communications*, 9(1), 1-10.
- Nielsen, M. (2018). Neural Networks and Deep Learning.[online] neuralnetworksanddeeplearning.com.
- Noonan, A. K. (2014). Bitcoin or Bust: Can One Really Trust One's Digital Assets. *Est. Plan. & Cmty. Prop. LJ*, 7, 583.
- North, M. J., & Macal, C. M. (2007). *Managing Business Complexity: Discovering Strategic Solutions with Agent-Based Modeling and Simulation* (1 edition). Oxford ; New York: Oxford University Press.
- Ogrodzki, J. (2018). *Circuit simulation methods and algorithms*. CRC Press.
- Okoye, M. C., & Clark, J. (2018, February). Toward Cryptocurrency Lending. In *International Conference on Financial Cryptography and Data Security* (pp. 367-380). Springer, Berlin, Heidelberg

- Omohundro, S. (2014). Cryptocurrencies, smart contracts, and artificial intelligence. *AI matters*, 1(2), 19-21.
- operating performance? Evidence from conflict minerals disclosures. *Journal of Operations Management*, 65(5), 406-429.
- Packowski, J. (2013). *LEAN supply chain planning: the new supply chain management paradigm for process industries to master today's VUCA World*. CRC Press.
- Packowski, J., & Francas, D. (2013). LEAN SCM: A paradigm shift in supply chain management. *Journal of Business Chemistry*, 10(3).
- Partanen, C. (2018). The viability of cryptocurrency in relation to the response of financial institutions and governments.
- Pavlou, P. A. (2002). Institution-based trust in interorganizational exchange relationships: the role of online B2B marketplaces on trust formation. *The Journal of Strategic Information Systems*, 11(3-4), 215-243.
- Perren, R., & Kozinets, R. V. (2018). Lateral exchange markets: how social platforms operate in a networked economy. *Journal of Marketing*, 82(1), 20-36.
- Persson, F., Bartoll, C., Ganovic, A., Lidberg, M., Nilsson, M., Wibaeus, J., & Winge, F. (2012, December). Supply chain dynamics in the SCOR model—A simulation modeling approach. In *Proceedings of the 2012 Winter Simulation Conference (WSC)* (pp. 1-12). IEEE.
- Piao, G., & Breslin, J. G. (2018, April). Financial aspect and sentiment predictions with deep neural networks: an ensemble approach. In *Companion of the Web Conference 2018 on The Web Conference 2018* (pp. 1973-1977). International World Wide Web Conferences Steering Committee.
- Pilkington, M. (2016). 11 Blockchain technology: principles and applications. *Research handbook on digital transformations*, 225.
- Poddey, A., Brade, T., Stellet, J. E., & Branz, W. (2019). On the validation of complex systems operating in open contexts. arXiv preprint arXiv:1902.10517.

- PricewaterhouseCoopers. (2015). Consumer Intelligence Series "The Sharing Economy", 1–30. Retrieved February 16, 2017, from: <https://www.pwc.com/us/en/technology/publications/assets/pwc-consumer-3intelligenceseries-the-sharing-economy.pdf>
- Prosak, A., Gangopadhyay, A., & Garg, H. (2019). A New Machine Learning Approach for Anomaly Detection Using Metadata for Model Training (No. 829). EasyChair.
- Ramachandran, K., Tereyağoğlu, N., & Xia, Y. (2018). Multidimensional decision making in operations: An experimental investigation of joint pricing and quantity decisions. *Management Science*, 64(12), 5544-5558.
- Rao, U. H., & Nayak, U. (2014). Intrusion Detection and Prevention Systems. *The InfoSec Handbook*, 225–243. doi:10.1007/978-1-4302-6383-8_11
- Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2017, January 01). Flow-based benchmark data sets for intrusion detection. Retrieved July 15, 2020, from <https://www.bibsonomy.org/bibtex/2c92848e1e32fa0a420c477b05a22b4e3/markus0412>
- Rogaway, P., & Shrimpton, T. (2004, February). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International workshop on fast software encryption* (pp. 371-388). Springer, Berlin, Heidelberg.
- Rowley, J. (2002). Using case studies in research. *Management Research News*, 25(1), 16-27. doi:10.1108/01409170210782990
- Saez, Y., Estebanez, C., Quintana, D., & Isasi, P. (2019). Evolutionary hash functions for specific domains. *Applied Soft Computing*, 78, 58-69. doi:10.1016/j.asoc.2019.02.014
- Salakhutdinov, R. (2015). Learning Deep generative models. *Annual Review of Statistics and Its Application*, 2, 361-385.
- Samek, W., Wiegand, T., & Müller, K. R. (2017). Explainable artificial intelligence: Understanding, visualizing and interpreting Deep Learning models. arXiv preprint arXiv:1708.08296.
- San Miguel, M., Johnson, J. H., Kertesz, J., Kaski, K., Díaz-Guilera, A., MacKay, R. S., ... & Helbing, D. (2012). Challenges in complex systems science. *The European Physical Journal Special Topics*, 214(1), 245-271.

- Santiteerakul, S., Sekhari, A., Bouras, A., & Sopadang, A. (2015). Sustainability performance measurement framework for supply chain management. *International Journal of Product Development*, 20(3), 221-238.
- Saraf, C., & Sabadra, S. (2018, May). Blockchain platforms: A compendium. In *2018 IEEE International Conference on Innovative Research and Development (ICIRD)* (pp. 1-6). IEEE.
- Saraph, V., & Herlihy, M. (2019). An Empirical Study of Speculative Concurrency in Ethereum Smart Contracts. arXiv preprint arXiv:1901.01376.
- Scheibe, K. P., & Blackhurst, J. (2018). Supply chain disruption propagation: a systemic risk and normal accident theory perspective. *International Journal of Production Research*, 56(1-2), 43-59.
- Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural networks*, 61, 85-117.
- Schor, J. B., & Fitzmaurice, C. J. (2015). Collaborating and connecting: the emergence of the sharing economy. In *Handbook of research on sustainable consumption*. Edward Elgar Publishing.
- Serrano-Cinca, C., & Gutiérrez-Nieto, B. (2016). The use of profit scoring as an alternative to credit scoring systems in peer-to-peer (P2P) lending. *Decision Support Systems*, 89, 113-122.
- Shaikh, F., & Faizan. (2017, June 15). Introductory guide to Generative Adversarial Networks (GANs). Retrieved from <https://www.analyticsvidhya.com/blog/2017/06/introductory-generative-adversarial-networks-gans/>
- shared vision for machine learning in neuroscience. *Journal of neuroscience*, 38(7), 1601-1607.
- Sharma, P., & Sharma, R. K. (2016, June). Design and implementation of encryption algorithm for real time speech signals. In *2016 Conference on Advances in Signal Processing (CASP)* (pp. 237-241). IEEE.
- She, R., Liu, S., Wan, S., Xiong, K., & Fan, P. (2019). Importance of small probability events in Siljak, D. D. (2011). *Decentralized control of complex systems*. Courier Corporation.

- Stampernas, S. (2018). "Blockchain technologies and Smart Contracts in the context of the Internet of Things". Digital Systems Security. Retrieved February 10, 2019, from http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11201/Stampernas_MTE1632.pdf?sequence=1&isAllowed=y
- Sturges, S., & Norton, M. (2013). *U.S. Patent No. 8,474,043*. Washington, DC: U.S. Patent and Trademark Office.
- Sun, T., & Vasarhelyi, M. A. (2018). Embracing Textual Data Analytics in Auditing with Deep Learning.
- Sundaram, N. M., & Renupriya, V. (2016). A Survey on Different Training Algorithms for Supervised Learning of Back Propagation Artificial Neural Networks. In International Conference on Systems, Science, Control, Communication, Engineering and Technology.
- Swan, M. (2019). Blockchain Economic Theory: Digital Asset Contracting reduces Debt and Risk. Blockchain Economics. London: World Scientific. Forthcoming.
- Swift, C., Guide Jr, V. D. R., & Muthulingam, S. (2019). Does supply chain visibility affect
- Tan, F., Wei, Z., He, J., Wu, X., Peng, B., Liu, H., & Yan, Z. (2018, November). A Blended Deep Learning Approach for Predicting User Intended Actions. In 2018 IEEE International Conference on Data Mining (ICDM) (pp. 487-496). IEEE.
- Tangpong, C., Hung, K. T., & Li, J. (2019). Toward an agent-system contingency theory for behavioral supply chain and industrial marketing research. *Industrial Marketing Management*, 83, 134-147.
- Tasca, P., Aste, T., Pelizzon, L., & Perony, N. (2016). Banking beyond banks and money. AG, Switzerland: Springer International Publishing.
- Testolin, A., Piccolini, M., & Suweis, S. (2018). Deep learning systems as complex networks. arXiv preprint arXiv:1809.10941.
- Tinny. (2018, March 01). Different Types of Blockchain Networks. Retrieved February 12, 2019, from <https://blog.xsolus.com/different-types-of-Blockchain-networks>
- Tishby, N., & Zaslavsky, N. (2015, April). Deep Learning and the information bottleneck principle. In 2015 IEEE Information Theory Workshop (ITW) (pp. 1-5). IEEE.

- Tran, K., Duong, T., & Ho, Q. (2016, December). Credit scoring model: A combination of genetic programming and Deep learning. In 2016 Future Technologies Conference (FTC)(pp. 145-149). IEEE.
- Turner, J. R., & Danks, S. (2014). Case Study Research: A Valuable Learning Tool for Performance Improvement Professionals. *Performance Improvement*, 53(4), 24–31. <http://doi.org/10.1002/pfi.21406>
- Vu, M.-A., Adalı, T., Ba, D., Buzsáki, G., Carlson, D., Heller, K., . . . Widge, A. (2018). A Vujičić, D., Jagodić, D., & Randić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-6). IEEE.
- Vuppala, R., & Farik, M. (2016). Intrusion Detection & Prevention Systems-Sourcefire Snort. *International Journal of Scientific & Technology Research*, 5.
- Wang, H., Greiner, M., & Aronson, J. E. (2009, August). People-to-people lending: The emerging e-commerce transformation of a financial market. In *SIGeBIZ track of the Americas Conference on Information Systems* (pp. 182-195). Springer, Berlin, Heidelberg.
- Warr, W. (2012). Scientific workflow systems: Pipeline Pilot and KNIME. *J Comput Aided Mol Des*. Retrieved from <https://link.springer.com/content/pdf/10.1007/s10822-012-9577-7.pdf>.
- Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016, January). Blockchain contract: Securing a blockchain applied to smart contracts. In 2016 IEEE International Conference on Consumer Electronics (ICCE) (pp. 467-468). IEEE.
- Weisbuch, G. (2018). *Complex systems dynamics*. CRC Press.
- White Paper.*
- Williams-Grut, O. (2016, May 17). After Firing Its CEO, Lending Club Is Facing a Crisis. Retrieved July 13, 2020, from <https://www.inc.com/business-insider/inside-lending-club-scandal.html>
- Xiang, Y., Mo, R., Chang, Z., Qiao, H., & Li, C. (2015). Stability analysis of process route based on weighted network. *Mathematical Problems in Engineering*, 2015.

- Xie, P., Ho, Q., & Xing, E. (2018). Efficient Peer-to-Peer Architecture for Distributed Machine Learning U.S. Patent Application No. 15/849,663.
- Yao, J. (2019). Valuation of a fintech company: Lending Club (Doctoral dissertation).
- Yaya, O. S., Ogbonna, E. A., & Mudida, R. (2019). Market Efficiency and Volatility Persistence of Cryptocurrency during Pre-and Post-Crash Periods of Bitcoin: Evidence based on Fractional Integration.
- Zhang, J. (2019). Deploying blockchain technology in the supply chain. In Blockchain and
- Zhang, Q., Yang, L. T., Chen, Z., & Li, P. (2018). A survey on deep learning for big data. *Information Fusion*, 42, 146-157.
- Zheng, S., Jayasumana, S., Romera-Paredes, B., Vineet, V., Su, Z., Du, D., ... & Torr, P. H. (2015). Conditional random fields as recurrent neural networks. In Proceedings of the IEEE international conference on computer vision (pp. 1529-1537).
- Zhou, Y., Chiu, D. M., & Ma, R. T. (2018). Modeling and Analysis of P2P Content Distribution Systems. CRC Press, Inc.