HYBRID BLOCKCHAIN FRAMEWORK FOR SECURED TRANSACTION SYSTEM IN SMALL AND MEDIUM ENTERPRISE SECTOR

A Thesis Submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

COMPUTER APPLICATION

By

SAUGATA DUTTA

17SCSE302002

Supervisor

DR. KAVITA
Associate Professor

SCHOOL OF COMPUTING SCIENCE & ENGINEERING
GALGOTIAS UNIVERSITY
Plot No 2, Sector 17-A Yamuna Expressway
Greater Noida, Uttar Pradesh
INDIA

OCTOBER, 2021

CERTIFICATE

This is to certify that **SAUGATA DUTTA (Reg. No. 17SCSE302002)** has presented his pre-submission seminar of the thesis entitled **"HYBRID BLOCKCHAIN FRAMEWORK FOR SECURED TRANSACTION SYSTEM IN SMALL AND MEDIUM ENTERPRISE SECTOR"** before the committee and summary is approved and forwarded to School Research Committee of Computing Science & Engineering, in the Faculty of Engineering & Technology, Galgotias University, Uttar Pradesh.

Dean - SCSE

Dean – PhD & PG

The Ph.D. Viva-Voice examination of **SAUGATA DUTTA,** Research Scholar, has been held on_____.

Supervisor

External Examiner

CANDIDATE DECLARATION

I hereby declare that the work which is being presented in the thesis, entitled "**HYBRID BLOCKCHAIN FRAMEWORK FOR SECURED TRANSACTION SYSTEM IN SMALL AND MEDIUM ENTERPRISE SECTOR**" in partial fulfillment of the requirements for the award of the degree of **Doctor of Philosophy** in Computer Application and submitted in Galgotias University, Uttar Pradesh is an authentic record of my own work carried out from September 2017 under the supervision of **Dr. Kavita,** Associate Professor, School of Computing Science & Engineering, Galgotias University. The matter embodied in this thesis has not been submitted by me for the award of any other degree or from any other University.

SAUGATA DUTTA

17SCSE302002

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

DR. KAVITA

Supervisor
SCSE
Galgotias University

APPROVAL SHEET

This Thesis entitled **HYBRID BLOCKCHAIN FRAMEWORK FOR SECURED TRANSACTION SYSTEM IN SMALL AND MEDIUM ENTERPRISE SECTOR** by **SAUGATA DUTTA** is approved for the Degree of Doctor of Philosophy.

Examiner Supervisor Chairman

ACKNOWLEDGEMENTS

I would like to express my gratitude to my guide **Dr. Kavita** for her guidance, kindness, motivations, suggestions and insight throughout this PhD research, as without her this thesis would not have been completed. I offer my sincere thanks to my family members for their inspiration and moral support. Thank you all for your strong support.

I must owe a special debt of gratitude to Hon'ble Chancellor **Mr. Suneel Galgtotia,** CEO **Mr. Dhruv Galgotia,** Hon'ble Vice-Chancellor **Dr. Preeti Bajaj** and Dean **Dr. Munish Sabharwal**, Galgotias University for their valuable support throughout my research work.

Nothing is possible without the constant support of my family. I would like to convey my deep regard to my parents for their wise counsel and indispensable advice that always encouraged me to work hard for the completion of my research work. My highest gratitude goes to my parent's and all my family members for their relentless support, blessings and encouragement. Special mention goes to my wife, **Navita Dutta** and my kid **Arshia Dutta**. My final thanks to all my friends, and to all those who stood behind by me like a support and helped me in completing this dissertation.

SAUGATA DUTTA

ABSTRACT

Blockchain technology is no longer a nascent buzzword in digital cryptocurrencies and has matured a long way through innovation over the years. The journey of evolution has been long starting from the days of Merkle tree to Bitcoin development, blockchain transaction, development of Ethereum blockchain, innovation of smart contracts and hyperledger, development and implementation of decentralized applications, Blockchain as a Service (BaaS) and so on and so forth.

It has come a long way since its incubation. The technology has shown the world its benefits in securing data and gradual acceptance in every industry. The technological growth in recent years has been inviting threats and vulnerabilities both internally as well as externally. Well aside internal threats, corruption, scams and money laundering cases are increasing day by day. Data transparency has been declining and the data speculated may not be necessarily correct. Data can be changed, altered or hacked for various monetary gains, personal enmity. Wrong data can be portrayed to evade complications. In most of the cases, data is managed centrally, requires an intervention of central authority.

This research has played a crucial role in developing a hybrid blockchain framework, which can be implemented preferably in small and medium sized enterprises (SME) as against the model of traditional client server approach followed in most of the industries. The framework can be used in cloud, on-premise or both. The Hybrid nature of the framework not only holds true in implementation platform but also in balancing performance, can be integrated with traditional databases. The aim of the research is to solve potential risks identified especially in SME sectors in terms of data security and develop a secure, affordable and robust framework for data transaction. The potential challenges identified in SME sectors are as follows:

- Primarily data security
- Centralized management
- Vulnerable database (prone to alter, change, delete)
- Corruption
- Maintenance of high IT infrastructure cost, high IT fault tolerance cost, inflated software license cost

- Lack of data transparency and integrity, vulnerability to virus, ransomwares, malwares and hacking attacks.

The HBSTS (Hybrid Blockchain Secured Transaction System) framework aims to address these aforesaid issues with its secured features in the following ways:

- Data security, integrity and transparency of data
- Reduced or no hacking attacks
- Minimal or no software license cost
- Better fault tolerance with no investment
- Interoperability between various breeds of operating systems
- Cohesive model approach, which can also take advantage of traditional model to balance the performance.

This framework does not require any third party intervention and validates transactions by peer nodes. This can be used as a PaaS (Platform as a Service). This model tends to solve the potential risk identified in the SME sector and has gathered an enormous amount of acceptance across the industries. The HBSTS framework is evaluated in different organizations with the existing traditional approach and has been compared by different lobbies of officials and executives. The HBSTS framework has been accepted with permanence after being foreseen and compared with the existing traditional client server approach in terms of security features, cost benefit, data transparency, overall execution time and manageability. The result of final evaluation of this framework showed an encouraging curve of acceptance and can be a secured choice, which tends to solve the purpose of the problem statement of my research. The experimental research has culminated to somewhat a conclusive answer through this.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

HBSTS	Hybrid Blockchain Secured Transaction System
SME	Small and Medium Enterprise
Baas	Blockchain as a Service
SME	Small and Medium Sized Enterprise
IT	Information Technology
Paas	Platform as a Service
RPoW	Research Proof of Work
RSA	Rivest–Shamir–Adleman
DApp	Decentralized Application
NONCE	Number Only Used Once
PWC	PricewaterhouseCoopers
AI	Artificial Intelligence
IoT	Internet of Things
MPLS	Multiprotocol Label Switching
VPN	Virtual Private Network
OS	Operating System
iOS	iPhone operating system
DDoS	Distributed Denial-of-Service
AWS	Amazon Web Services
TCP	Transmission Control Protocol
IP	Internet Protocol
HTML	Hyper Text Markup Language

TON	Telegram Open Network
US	United States
SQL	Structured Query Language
I/O	Input Output
ID	Identity
OTP	One Time Password
SSL	Secured Socket Layer
MD5	Message-Digest
SHA	Shell Hash Algorithm
MFA	Multi-Factor Authentication
JSON	JavaScript Object Notation
URL	Uniform Resource Locator
DOM	Document Object Model
XSS	Cross-Site Scripting
UDP	User Datagram Protocol
ISP	Internet Service Providers
BPO	Business Process Outsourcing
ANOVA	Analysis of Variance
TLS	Transport Layer Security

CHAPTER 1

INTRODUCTION

This chapter discusses blockchain technology since its inception, its application and its current state in use. The traditional approach followed and its constraints in the SME sector. The hybrid blockchain secure transaction system (HBSTS) framework model is defined and compared with the traditional approach. The research's goal is clearly stated, as is the motivation for developing this HBSTS framework.

1.1 INTRODUCTION TO BLOCKCHAIN

Bitcoin is arguably the primary buzzword since its inception when we talk about blockchain technology. Bitcoin or any other digital cryptocurrencies uses the underlying technology of blockchain. Blockchain is a secured distributed ledger in a decentralized distributed network. It uses consensus algorithms without the intervention of central authority. It is resilient and has fault tolerance. As against the centralized client server architecture hosting a centralized database, blockchain uses distributed network to maintain a shared database. Bitcoin is the first used case of blockchain technology. Crypto currency operates on blockchain technology with a distributed ledger. The name Blockchain is a time stamped append only log. Blocks are added on an average of every ten minutes. There are, however, varieties of designs that can vary by up to ten seconds. Blockchain database is auditable and secured by a hash function for tamper resistance and integrity. Digital signatures are used for consent. Blockchain as the name suggest is a block of hash data and various technical contributors are time-stamp, append only logs, block headers and Merkle tree, cryptographic hash functions, asymmetric cryptography, digital signatures, addresses, network of nodes and consensus algorithm.

The blockchain network's nodes contain a complete copy of all transactions that have ever occurred. Although ledger technologies have been in place for quite some time blockchain takes the advantages of having a single source of truth where nodes share the same copy. Instead of one company holding an entire database of transactions information here is distributed to multiple people equally, transactions are validated

by multiple nodes of blockchain, and information is updated constantly. The creation of block is an irreversible process.

The interface is similar to any common applications but at the backend, an inter-network of multiple nodes operating as an underlying pillar of the technology. The technology uses cryptography that helps and code all transactions. As a result, the information is safe and cannot be tampered with. Blockchain technology is currently being used in a variety of industries, not just digital currency.

1.2 HISTORY OF BLOCKCHAIN

Although blockchain may appear to be a novel concept, it has a long history. Ralph Merkle was given the name Merkle tree, also known as hash tree, in 1979. The treelike structure concept, in which both leaf and non-leaf nodes are hashed from the very first child nodes, provides efficiency and security for data contents. This has formed a fundamental concept for the blockchain.

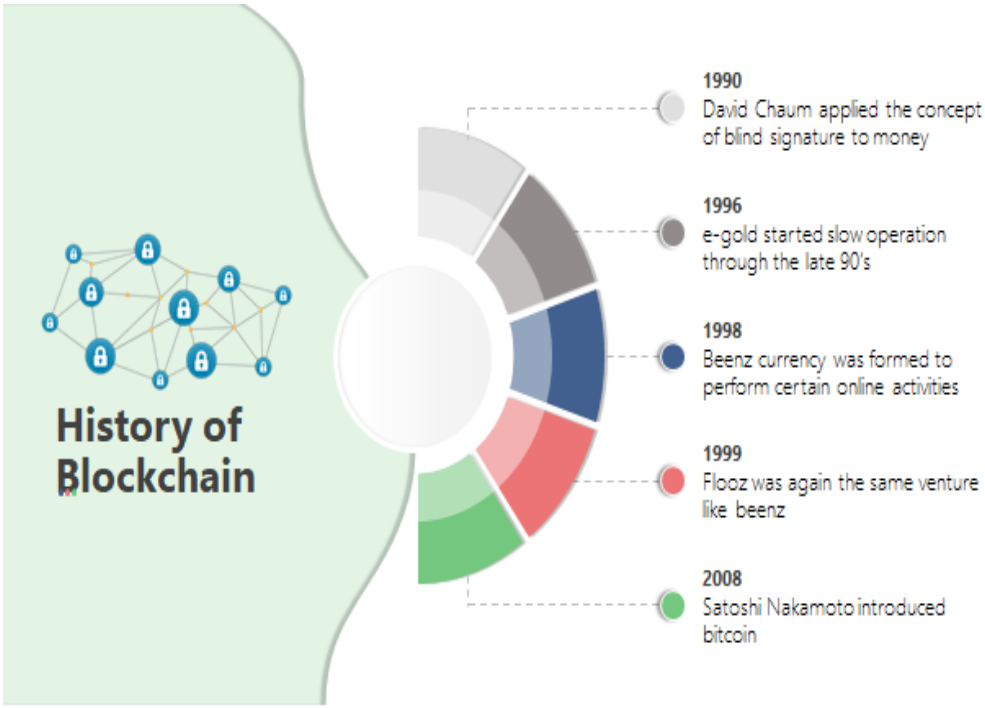

Figure 1.1 History of Blockchain

Figure1.1 explains the historical time lines of blockchain. The first work was done by Stuart Haber and W. Scott Stornetta to create a secure chain of blocks in 1991. However, in the following year (1992), they upgraded the system but the work did not yield much result.

The work was based on the concept of Merkle tree where each block of chain is hashed to store the time stamped documents as the technology was not used then and the patent was lapsed in 2004.

However, in the same year (2004) again, a scientist named Hal Finney introduced the concept of RPoW (Research Proof of Work). It is a hash based token which is non-exchangeable and in return creates a RSA (Rivest–Shamir–Adleman) signed token that can be transferred between individuals.

It solves the double spend problem which keeps the ownership of tokens by keeping the transactions in a trusted server. RPoW can be considered as an early prototype and an early step towards the blockchain.

In 2008, Satoshi Nakamoto (Person or group) introduced bitcoin white paper articulating peer-to-peer, decentralized electronic cash systems. Based on the hash cash, the proof of work algorithm, however, uses consensus algorithms for integrity and verifications.

In 2009, bitcoin came to existence when the first bitcoin was mined by Satoshi Nakamoto, which has a reward of 50 bitcoins. The first bitcoin transfer was done to Hal Finney.

In 2013, Vitalik Buterin, a programmer and a co-founder of Bitcoin magazine, experimented that blockchain can be used to create decentralized applications which will foster security and transparency. He also stated that the Ethereum platform, which is a distributed computing platform, can be used to create decentralized applications. The evolution of blockchain can be divided in phases.

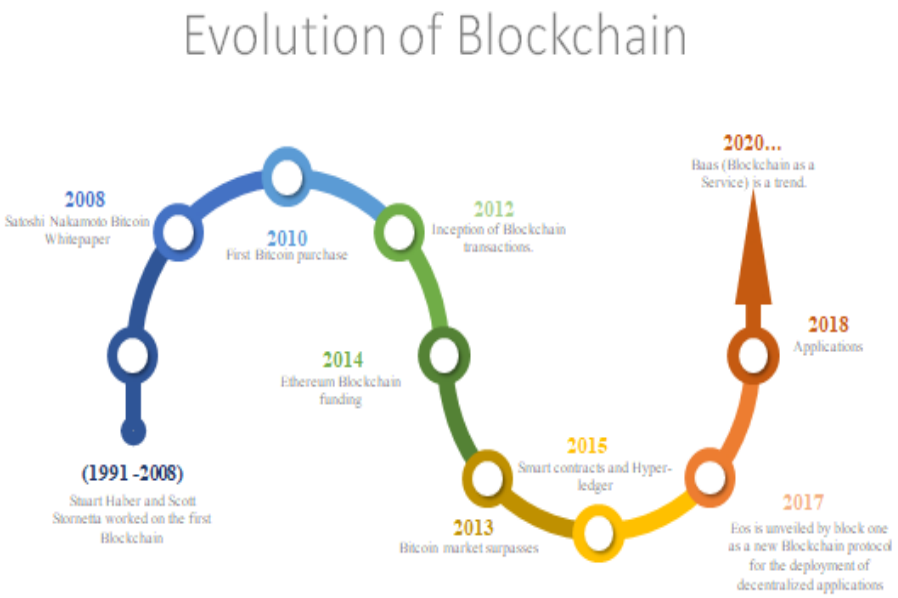

Figure 1.2 Evolution of Blockchain

Figure 1.2 shows how blockchain evolved year wise. Phase I can be attributed as the emergence of the technology "Blockchain 1.0" from 2008 to 2013. During this phase, bitcoin came into play, adoption and usage. The majority of people could not identify the difference between bitcoin and blockchain at the time. Bitcoin was supposed to be the digital crypto currency where blockchain is the underlying layer being used.

Phase II "Blockchain 2.0" is the inception of contracts from 2013 to 2015. The concept of smart contracts was established with the launch of Ethereum, which was a software program deployed on the Ethereum platform that was used to make a transaction when a certain condition was satisfied. Smart contracts were written in a certain programming language called solidity.

Phase III "Blockchain 3.0" since 2018 that is the future generation blockchain is being used primarily for creating decentralized applications and scalable projects keeping blockchain as an underlying layer. This concept of blockchain is being studied for sharing and sidechain for enhancing the performance and scalability features. It's worth noting that numerous centralized applications are being developed to investigate the usage of this technology in various business areas. Cardano, Zilliqa and EOS are some of the platforms used to create DApp (Decentralized Application) over blockchain. This phase has been designed keeping high transaction speed in mind.

1.3 HOW BLOCKCHAIN WORKS

A blockchain is an append-only database or a growing list of records created by blocks and which are linked with each other by hashes. Each block has the cryptographic hash of the previous block. It is resistant to alteration and deletion of data. Blockchain is an open distributed decentralized peer-to-peer ledger, which does not require any third party intervention. A block header's composition contains the majority of the information for the blocks.

Table 1.1 Block header

Version Number
Previous Block Hash
Root hash merkle tree
Time stamp
Difficulty target
Nonce

Table 1.1 shows the structure of block header.

A Block header consists of the following items:

a. Version Number: It is a software version number. This information is required by miners in some cases
b. Previous Block Hash: It is the hash of the preceding block, as the name implies. It is a connection and chronology between each block as the hash of the previous block is put on the hash of new block
c. Root Hash (Merkle Tree): The root hash is the aggregation of all the transactions in the block.
d. Time Stamp: The time stamp of the transaction
e. Difficulty Target: The objective specifies how short the new hash must be in order to be considered legitimate. The smaller the aim, the more difficult it is to locate a suitable match. A hash that starts with more zeroes is smaller than one that starts with none.
f. Nonce: A miner estimates a valid hash that is smaller than the objective for a number called the Nonce.

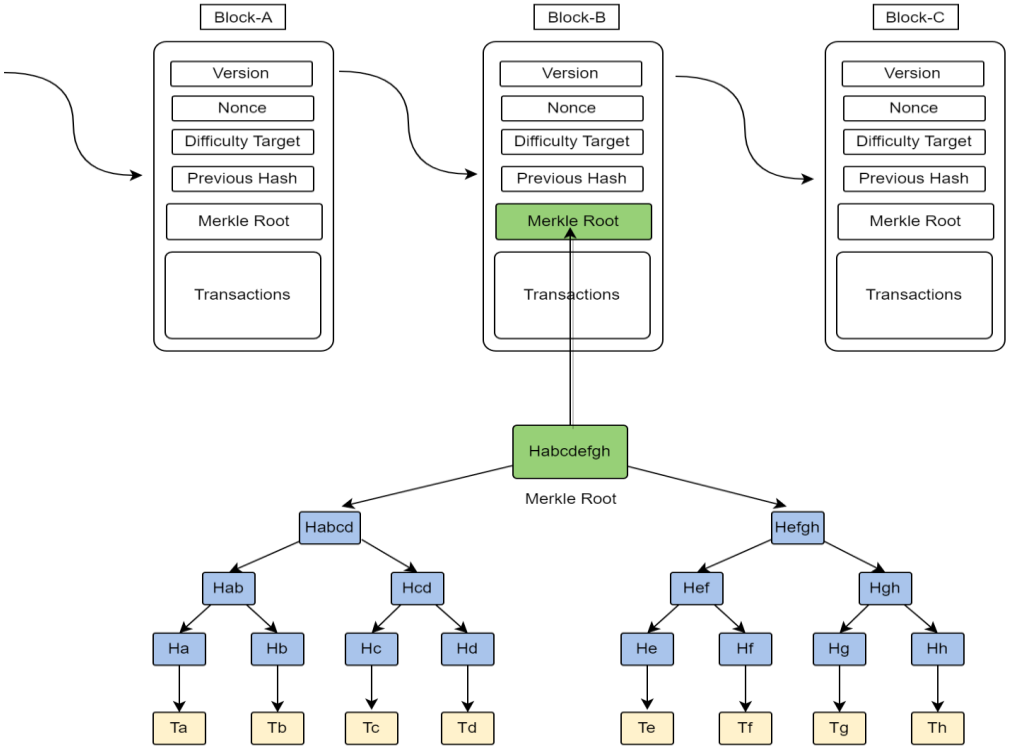

Figure 1.3 Merkle tree concept

Figure 1.3 explains the concept of Merkle tree and the way it works. Merkle trees are the bedrock of the blockchain system as a whole. In a Merkle tree, the data is first hashed, and then the hashes are merged. The Merkle tree is then combined into a single hash. The Root hash is the chain's most important hash. Individual transactions are called as leaves, and the hashes of the leaves are known as branches. Creating a hash only works in one way, which implies that if the root hash is known but the transaction information is unknown, guessing the transactions is impossible.

In blockchain technology, each individual block is linked to the previous block, with the exception of the "Genesis Block," which cannot be linked to any prior block. For example, in a blockchain, if block 3 is tampered then the hash value of that particular block will change and thereafter all the following blocks will be invalid. However, this alone cannot pose a protection layer as our systems nowadays are inherently more empowered with higher computing ability with retrospective effect to recalculate those hashes backward and make it look valid again. Hence, public blockchain is susceptible and are prone to many such similar attacks.

Essentially the blockchain mining is the gap arrangement to address this type of issue. The proof of work concept in mining is a computation done for protection. The blockchain header consists of five constants, which are as follows - one variable version number of the software, hash of the previous block, the root hash, timestamp and the target size. Nonce is a variable, which can be incremented by one. The abbreviation of NONCE is “Number only used once”. The Nonce value must be increased whenever the hash or encrypted block is changed. Once miners have successfully completed the mining process, they may earn a payment if they are accurate in their predictions. To check whether the goal has been accomplished, the new number is hashed and added to the target value. It is further analyzed whether the recirculated data matches the expected value. The procedure will continue to append nonce values one larger than the current hash value. The uniqueness of each result is guaranteed with a fresh hash for each result. This procedure is repeated for a fresh block. A new Bitcoin block is generated every 10 minutes. Mining is a physically hard profession, and needs the use of specialist equipment with a high processing capacity. Since it cannot be predicted how much it will cost to energize the system, it is a risky investment. To confirm transactions and to receive paid on a blockchain network, miners must use the proof of work technique.

It slows down the block generation process. Taking bitcoin as an example, on an average, it takes ten minutes to create an additional block. It makes it nearly impossible to tamper a block, as the recalculations of proof of work for all following blocks need to be done.

Another protection layer of blockchain is based on a distributed network rather than depending on a central authority. A blockchain copy is stored on each node in the distributed network, allowing it to verify the integrity of the network. In order to operate the protective layer, a consensus method is used. Each node verifies the integrity of a newly introduced block before adding it to its own node collection. To tamper with a blockchain, one must tamper with all subsequent blocks, recalculate the proof of work, and gain control of more than half of the dispersed network's nodes. Blockchain database is a distributed ledger, which is consensually shared and synchronized across multiple nodes. As these transactions are publicly exposed, it becomes difficult to suppress the data. Any changes or additions in the ledger are reflected across all the nodes in the blockchain.

Smart contracts are lines of code, which get executed when certain criteria are being met. These are self-executional and do not require any involvement or authorization from any central authority or legal system. Smart contracts render all transactions traceable, irreversible and transparent.

1.4 BLOCKCHAIN ON CURRENT AGES

Blockchain technology adoption has had a gradual growth story amid various lobbies of industries. Data transparency and security have been the most crucial aspects and trend in recent years. Data security cannot be compromised and data events should be transparent. With the development of smart contracts and hyperledger applications blockchain technology, as a service, has not only spread its wings across various industries but also tends to have a stronger presence in social media. The benefits are high while the motto of the blockchain remains the same with its high transparency on data, data leak proof and various other perks in posting threads.

The digital transformation across global markets in recent years has contributed to the growth of blockchain in manifold ways. The COVID-19 pandemic, in particular, has been a big reason for its acceleration. Global acceptance of digital transaction has created a wide adoption of digital technology over physical exchange. Smart contracts, decentralized applications focus on creating business, which is more secure and transparent. Customized blockchain solutions, specifically tailor made for industries, tend to gain popularity and dominate the digital exchange space gradually. This opens the door for more corporations where the data keeping is secured and kept confined within few trusted professionals. More and more industries have been focusing on performance and scalability of blockchain technology. In recent years, blockchain as a service or platform has become a trend. There are various exciting startups on blockchain like Abra, Bluzelle, Brave, Credit Dream, Enigma, Plex and Zcash.

Blockchain organizations can be delegated: Private, Public, Federated or Hybrid. This term can be alluded to as a standout amongst other blockchain most recent patterns in the business. It is simply an overhauled type of the essential blockchain model, which brands it ideal for some, particular use cases. It is interrelated with numerous organizations while these valid blockchain nodes from different authorities will

validate the transactions. This type of united blockchain will gain momentum in usage where it gives private blockchain networks a more adjustable viewpoint.

PWC (PricewaterhouseCoopers) reports 80% of monetary establishments to embrace Blockchain innovation as a component of transaction. To cater the traditional financial task, various monetary organizations have started considering the practice of digital cryptocurrency as an alternative.

With the harmonization of AI (Artificial Intelligence), Blockchain revolution will make for a superior turn of events. This coordination will show Blockchain innovation with a satisfactory degree of operations and progress. The International Data Corporation recommends that worldwide spending on AI will reach $60 billion in coming years and 52% of establishments will make the change to AI with Blockchain reconciliation. Moreover, Blockchain can likewise make AI more intelligible and justifiable. Blockchain can record all information and factors that go through a choice made under AI. In addition, AI can immensely help blockchain productivity over any human interference or standard process. A look by which blockchain currently runs on systems demonstrate that an excessive contract of handling power is expected to perform even fundamental assignments. Integration of artificial intelligence in Blockchain bolsters system power in smart computing, trusted decision-making, monetization and protection of diverse data set.

Blockchain interoperation is the mechanism to segment data across various multi Blockchain networks. A blockchain copy is stored on each node in the distributed network, allowing it to verify the integrity of the network. In order to operate the protective layer, a consensus method is used. Each node verifies the integrity of a newly introduced block before adding it to its own node collection.

A recent forecast by Gartner states that blockchain based digital cryptocurrencies will invite more than a billion dollar business. The mainstream banking system has a burden now since it must decide whether to accept crypto as a means of trade.

Gadgets are proliferating, and with that, proliferation comes the potential for new security vulnerabilities. The IOT (Internet of things) markets are experiencing exponential growth and an excessive demand to save the technology. Blockchain technology is now being used to increase the online security of at least 30 billion

connected and associated devices. A better approach for using SME sectors to launch an open source plan while minimizing or zeroing out expenses while implementing the framework. The expected exponential expansion in all scenarios is a prominent characteristic of blockchain technology.

1.5 TRADITIONAL APPROACH

The traditional approach of keeping record had started since the use of paper method. However, in the digital world, the use of databases is more of fashion rather than maintenance of file. The traditional approach (Client-Server Architecture) here started with the inception of a database which was a flat file and gradually used a relational model to store data by relating information from multiple databases. It can be controlled by a single user called administrator. The administrator has the freedom to delegate certain roles to users in order to manage the database. The centralized database can be backed up, restored and prone to modification/alteration as and when required. A common place to store the data is actually a centralized database. It is a classic picture of a database and actually a single record of truth, which is stored in a single location. However, the database can be cross located and replicated.

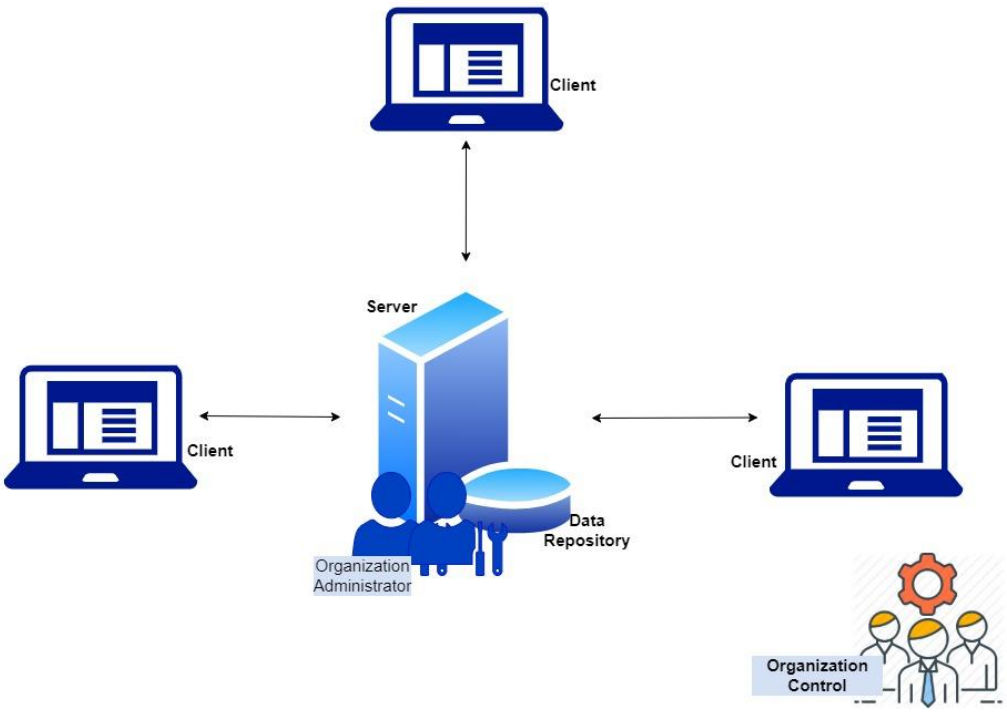

Figure 1.4 Traditional approach

Figure 1.4 shows the traditional client server approach usually small and medium enterprise sector follows. Generally, prior to implementing any kind of program or plan, companies use a more traditional method in which a transaction is done into a system, which is then kept on a centralized server. Once transaction data is sent into the network either locally or over the internet, it is stored on either a server or a central database. Now many possibilities are being investigated. For SME enterprises that have various branches in different geo locations, they are connected over MPLS (Multiprotocol Label Switching) link and transactions are fed over VPN (Virtual Private Network) or web login. However, in some cases, especially in disorganized sector, site offices, where conservative groups are not involved, transactions are usually noted in register book (hard copy) and later fed into a computer system, which eventually gets stored in the database. Other modes of capturing data like bar codes are finally stored in centralized locations. In some cases where distributed transactions are involved, the data is entered on the local database and are eventually replicated to the centralized database. In small and medium-sized businesses, affordability of only one kind of technology is critical, along with their general lack of intention to alter their business model. So therefore, the usage of a centralized database is included into the conventional approach as well. In some cases, databases are distributed and are never clubbed together. Reports are gathered from the database from branch offices. These SMEs typically focus on the product market and manpower and barely introspect towards IT security.

As an example, a famous car company introduced a driverless car as a business model, which crashed due to some extraneous factor. The root cause analysis was not possible and transparency hinges on the statement of the company given to the public. In this scenario, had the IoT logs been pushed to a blockchain network then there would have been more clarity on the series of incidents shared with the public.

A database administrator, who is in charge of the company database, can update and write information to the database. In most of the cases, databases are stored on private networks, usually behind a firewall, while some are hosted on cloud. The security and trust are retained by the company itself.

1.6 CONSTRAINTS ON TRADITIONAL APPROACH

There are potential loopholes in the traditional approach model. All nodes are accessing and saving data on a single database. However, there may be cases where this database may be replicated to some other environment but by and large uses the same data. Database using a client server architecture, gets a complete view of data, which can be updated, modified and backed up. Client server architecture platform has lots of rights to change or modify in the database especially in the small and medium enterprises where data security is minimum and have constraints on IT budget. The information, which is published from the database, is taken for granted as a genuine one. A designated authority that has full control over the database maintains database. The authority may come under influence of some entity and can do any fraud. The security of the data is violated. The database administrator or similar type of roles can destroy or corrupt the data. Traditional databases are contained within a single object regardless of their structure. Traditional application mechanisms have also fallen prey to malicious activity. Incapable and prone to various malicious attacks like SQL injections, malwares, virus and more importantly ransomwares. This also has the issue of nodes in the network when hacked or come under the influence of a virus, which writes damaged data to a common database. The affordability is a constraint when it comes to implementation of a centralized database, as software license is required including the license cost of the operating system.

Hence, in order to accumulate all points:

1. In traditional approach model in SMEs the data is stored in the form of centralized database (Alterable database)
2. The data stored in the centralized server can be edited, removed, backed up, exported, leaked, restored and corrupted too for financial gains, enmity, corruption, personal grudges etc.
3. Maintaining an IT Infrastructure cost is very high, specifically expensive hardwares, dedicated servers, power consumption, cooling systems and manpower.
4. Transparency and integrity in the centralized database is totally dependent on the backend database which cannot be trusted.

5. Traditional approach model is vulnerable to virus, malware, infectious ransomwares and other scripting attacks.
6. From the perspective of SME sector, the license and maintenance cost is high and may not be affordable.
7. Creating a fault tolerance IT infrastructure is very high.

1.7 HYBRID BLOCKCHAIN SECURED TRANSACTION SYSTEM (HBSTS) FRAMEWORK

The HBSTS framework has been developed to satisfy the constraints of the traditional approach model. It is developed keeping in mind the platform that is light, highly secured, low cost, and easy to implement both on cloud and on premise. HBSTS framework can be further developed to use with various services like smart contracts and hyperledger. Several modules can be developed on top of the HBSTS framework platform as a service. The hybrid model can be implemented in continuation of on-premise and cloud for better implementation. However, the framework can be used separately on-cloud and on-premise too. This is specially targeted for the SME sector where there are many constraints on IT budget but at the same time without compromising security. The data stored in HBSTS are secured and cannot be edited or modified and deleted. This will have a probabilistic immutability. Transactions are transparent and are over the peer-to-peer network.

The framework is easy to implement and can be used over any OS (Operating System) without any extra license cost. The framework is also not geographically dependent and does not require approval from a central body. The nodes valid the transactions over a distributed peer to peer network. The framework on cloud can be accessed without subscribing for cloud blockchain as a service. This framework can be used over various devices like iOS (iPhone Operating System)/Android/Linux and Windows. Servers and other devices maintain the continuity of the chain. Transactions can be done through handheld devices, laptops, servers, and systems, which are immutable and can be viewed by various stakeholders who are registered to the blockchain network. Each user can audit transactions. However, there are provisions for permissible transactions.

This framework has the prerogative to store space-consuming files to traditional databases as a reference to balance the performance. The transaction performance can be balanced when referred heavy files are stored in a traditional database. Hence, the framework is not only hybrid in terms of technology but also in context to implementation. The transaction may not be mandatory to store unimportant or heavy data to a traditional database, but it is an optional feature.

1.8 TRADITIONAL APPROACH VS HYBRID BLOCKCHAIN SECURED TRANSACTION SYSTEM (HBSTS) FRAMEWORK

Traditional approach, which is a client server model, has many drawbacks as compared to the developed HBSTS framework.

Data Security: HBSTS is aimed to mitigate frauds and corruptions, which has been happening over years where data is corrupted, removed, altered in view of financial benefits, personal grudges, concealing information, and corruption. Client server architecture with centralized databases employs several administrators who have full control over the database, and can be influenced in making modification to the database and eventually corruption. HBSTS, on the other hand, is a distributed ledger with no central authority or third-party control. Once input, the data is checked and updated by multiple network nodes. They are extremely powerful in situations where the integrity of the database is concerned. All transactions are hashed and encrypted and blocks are hashed.

License Cost: License cost is a factor in the case of traditional databases where an enterprise needs to purchase licenses both for the operating system and the database editions. Some are as per core license and some have the headcount limitations on the concurrent users. At the same time, HBSTS is totally free and has no limitations. As it is platform independent and can be used on any open source or licensed OS, thus giving a parameter of affordability and flexibility.

Fault Tolerance: HBSTS has an extreme degree of fault tolerance and immutability of data. To understand the algorithm, it must be looked at the completely distributed system of engineering that it is running on. In contrast to traditional client-server models, each node in the architecture displays both client and server characteristics.

All nodes perform the same function at the organizational level as they do at the network level as a continuity element. The system has fault tolerance to an exceptional degree in this manner. However, if two or more nodes are connected, the chain remains intact. It is difficult to conceive of a scenario when anything gets in the way of operating the block chain since there are external variables, such as natural catastrophe, cyber-attacks etc. It is amazingly hard to get a similar degree of expectations in a traditional approach, or if nothing else, to get such a delivery at a sensible expense.

Integrity and Transparency: A key property of HBSTS innovation, which recognizes it from traditional approach, is open certainty, which is empowered by uprightness and straightforwardness. It can be certain that the information accessed is uncorrupted and unaltered since the second it was recorded. Users have the freedom to check how the data has been recorded in the blockchain over the time. A central authority, according to the conventional method, controls data transparency. Having complete control of the data may put one's integrity at risk, since it is a controlled database.

Hacking Attacks: Blockchain with its decentralization nature eliminates the DDoS (Distributed Denial-of-Service) attack as it is distributed over a large peer. It provides a safe haven over traditional model against SQL Injection attacks. It is safe against viruses, as it cannot disturb/change the blockchain data and provides protection against ransomwares.

Interoperability: HBSTS is platform independent and can be interoperable through hybrid devices and systems. It supports almost all operating systems and can exchange information and maintain continuity of the chain established. In conventional approach architecture, majority of databases or systems has cross platform difficulties. They are not adequately integrated with one another too. Moreover, the licensed system may not connect with an open source system in the traditional approach model.

Cohesive Platform: HBSTS can be integrated with the traditional approach model can work by balancing data between classic databases and blockchain. It can be implemented in a hybrid mode.

1.9 MOTIVATION

The vast majority of the work depicted in this postulation was directed at Galgotias University, Greater Noida, in India. The reason behind leading this research work at this college where there are various incidents to be heard, that had many such fraudulent cases pertaining to defilements and proof altering in information. I generally needed to structure a framework particularly for the SME area which is exceptionally secure, incorporated, moderate in execution and simultaneously simple to actualize. The framework ideally ought not to be complex to comprehend and adequate to cater the broad requirement.

Aside this, pretty much every other day, we get to hear cases analogous to defilement, cheat, proof alter, dark cash and so forth which actually triggered me to plan and execute HBSTS (Hybrid Blockchain framework secure transaction system) where these typical threat parameters can be alleviated.

1.10 OBJECTIVE OF STUDY

- To distinguish and work-out a productive procedure for a protected innovation stage.
- To examine and test the legitimacy of the framework extending as a strength of critical inferences.
- To contemplate the relevant issues for secure transactions utilizing Blockchain innovation with explicit reference to security, transparency, and probabilistic immutability.
- To build a secured framework that has upgraded verification, integration with the conventional models.
- To distinguish the fundamental traits that contributes towards proficiency of secure transactions utilizing Blockchain innovation.
- Create a framework with improved security, which stops information robbery, information changes and exploitations, and proof altering.
- To survey and fundamentally look at the accessible hypothetical bases, research discoveries and reference prompting productive surmising.
- To create a framework which can be utilized at any technological platform, simple to implement and affordable.

- To audit, change and articulate the framework for secure transactions utilizing Blockchain innovation
- To develop a conceptual / theoretical framework for proficient secure transactions utilizing blockchain technology

1.11 THESIS OVERVIEW

Blockchain technology has many hidden innovations within itself. The transactions, which are done on small and medium sized enterprises, lack security, which ends up with information alterations, data theft, corruption, evidence tampering and lack of transparency. This results in heavy loss in terms of finance, fame, imprisonment and dishonesty towards an individual/company/public.

This thesis has developed a hybrid blockchain framework which is highly secure, can be implemented on any technological platform, integration with traditional models and more importantly affordability. The framework does not have any license cost and can be implemented over the cloud, on-premise or both. It has an enhanced authentication system and validates the data with a consensus algorithm. It does not require expensive hardware nor any software license or any cloud as a service charge. It has high fault tolerance and consumes less space. This framework can work with different OS architecture. Smart contracts can be developed in this platform and can be used with an aim to cease data tampering with no cost.

Chapter-2 describes the background study done which helped in developing the framework. Chapter-3 details about the design and development of the framework with flow charts. Chapter-4 explains the framework implementation in organization and its evaluation. Chapter-5 details the post implementation statistical analysis for supporting a conclusive answer. Chapter-6 throws light on the decision of HBSTS framework and its future study.

CHAPTER 2

LITERATURE SURVEY

This chapter defines the study carried out in background, which helped in development of the Hybrid Blockchain Secure Transaction System (HBSTS) framework. The tools used in development and various literature reviews carried out are mentioned in this chapter. This chapter throws light on the use of blockchain technology in various industries.

2.1 OVERVIEW

Blockchain technology has emerged from digital cryptocurrency to industry usage owing to its property of data security; append only database and probabilistic data immutability. The usage of blockchain technology was primarily for digital cryptocurrency for which it was invented as an underlying layer. Eventually it was realized to use the goodness of this technology on a broader scale. There are more to it from financial transactions using blockchain. New applications are built on top of the blockchain features using Ethereum. One of the important tasks that must be done to increase the use of blockchain technology is the creation of smart contracts. Work conducted without the assistance of other parties is widely applicable. The Hyperledger platform includes blockchain development tools that are well suited for a wide range of applications. HBSTS framework is not only a blockchain framework but a PaaS (Platform as a Service) which can be used in the small and medium enterprise sector where further blockchain applications can be developed for usage. The HBSTS is used to secure transactions using the underlying layer of blockchain technology with various benefits such as data security, anti-hacking, data transparency, lower license cost, lower maintenance and ease of implementation. It can be used in on-premise, cloud or both. The hybrid nature not only stands true for the implementation of technology, but also holds true for data storage, which uses the blockchain primarily and also balances the load with traditional databases of non-crucial data for performance. HBSTS challenges the existing traditional model approach, followed in industries, outlines the various vulnerabilities, and tends to address those problems. This background research throws light on various literature reviews done which helps in developing the HBSTS framework. The background

research has helped in understanding the development, execution and implementation of the HBSTS framework.

2.2 TOOLS USED IN FRAMEWORK DEVELOPMENT

Development Tools:

- Python: This is the tool which will create an application in Blockchain
- Linux/Windows: Operating system platform

Cloud Subscription:

- Azure: Azure subscription
- AWS: AWS Subscription

Network Tools:

- TCP / IP network : TCP / IP network with internet access
- Firewall: for accessing the private blockchain with required ports from internet cloud

Device Testing:

- Android
- iOS

Statistical Tools:

- Microsoft Excel: Simple user-friendly package for windows for manipulating, calculating, evaluating, functional probabilities and all types of statistical processing.

Web Tools:

- HTML 5: Verify, Correct, Monitor and Manage your Web Site and Web Based Applications
- Python Django/Flask: Retrieves an HTML page and reports on any problems that it finds.

2.3 BLOCKCHAIN TECHNOLOGY IN INDUSTRIES

Economists have been exploring people's behavior for hundreds of years. They study the way we make decisions, act individually and exchange values. There is new technological institution that will fundamentally change the way we exchange values and it is called a Blockchain. There are many people working on this since inception from financial institutions, startups and so on, and it is not just an economic evolution but this is also an evolution in computer science.

Blockchain beyond bitcoin is a revelation and it can be used in almost all industries. Blockchain rewards are extremely secured and cannot be edited and that is a radically changing way for industry adoption. Smart contracts can be introduced where it gets self-executional provided certain conditions are met, e.g. as a landlord one may not think about the rental agreement and rent for the apartments as this gets executed automatically every month with transparency from both the parties.

Another example of how individuals use a password that can be confirmed by a huge number of people at once and yet not put their security at risk. To help ensure voter eligibility, the blockchain contains checks on registered voters to determine if they are eligible to vote, and then their votes are recorded into a public, unalterable record. This concept however was implemented in Colombia as a test run, which worked.

Even companies internally have started adopting to verify that the supply lines are all working together and in total transparency. Each step in the line of process from manufacturing to distribution has been linked together by blockchain. Musicians ensure that they are paid for every stream of songs they sang and awarded for the original work. Work histories and resumes can be accessed at a glance.

Medical records can be implemented in blockchain and doctors can check and share individual's history. Blockchain cuts out the intermediary and allows faster and secure transparent use of information. Enterprises have been tapping to these technologies and are implementing nearly fifty real world used cases like finance, media, supply chain which have seen the highest among all these used cases.

Ocean industries have been gradually adopting the blockchain technology. A copy of the digital ledger passed around which is transparent and agreed upon before actually is written down to the ledger. Some of the financial sectors have already started using

blockchain with the idea of securitization of products, how other technologies and products can be integrated in the effective manner using a blockchain. Another industry, which has been seen, started with blockchain applications is big data where data needs to be stored and accessed.

Blockchain has the capability of fundamentally changing supply chain industries where it is continually updated where the goods are, thereby promising transparency and conducts trade finance in a secured way. One can ship goods around the world knowing that one would be paid for the transaction that has huge opportunists open up for global trade. Public services sector can be changed by blockchain where the government implements a blockchain based system for land registries making it easier, quicker and cheaper for registries that practice and get access to proof of ownership.

Every sector will benefit from blockchain because it has the capacity to minimize transaction friction and eliminate the mistakes associated with centralized platforms. Likewise, benefits already are seen from security industries. Trades from the stock can be recorded on blockchain; proxy votes can be made or recorded and traded on blockchain. Real Estate transactions can be put on blockchain and this technology has been tested and implemented for registering and tracking real estate properties. Protecting property rights to blockchain technologies is an important advancement in real estate.

Another area of blockchain that can be seen as advancements is putting personal details with confidence that can be used for passports, driving license, will etc. Blockchain can be gradually seen growing in changing the ecosystem with parallel economy and the property of infecting enhanced security and information sharing into financial services. Blockchain is creating footprints on messaging applications, which is still in development called “TON” abbreviated as telegram open network. Introduction to crypto exchanges by simply removing the uses of human intervention, which has an effect of reducing the risk of cyber threats and human error. Education industries are exploring blockchain technology using some universal recognized credentials. Car leasing and sales industries have started adopting this technology for leasing, buying and selling in a secured way. Music industries has been using this platform in the form of smart contracts where it offers a fairer deal avoiding

plagiarism of tunes and scripts. The medical records are on safer hands and can be used by various medical bodies to check the medical history and provide correct diagnosis of disease. Blockchain can play a great role in securing the data for innovation in energy industries like rooftop solar, electric vehicles and smart metering. Sports management can be done more efficiently using blockchain like data analysis and transparency in managing sponsorship.

Implementation of fewer manpower in the loyalty programs using blockchain technology is more cost effective and efficient. Especially in the US and some other countries where acquiring arms is legal, the possession information can be stored in blockchain which is transparent, traceable in the event of unlawful use. Retail industries are benefited by decentralized operations attaching more sellers and buyers. Transaction on charity can be embedded with blockchain to have a transparent transaction and reach the right hand. Human resources can be benefitted in storing information related to background and employment verifications. Libraries can profit by archiving material, involving more communities, and managing more digital rights. Rewarding users for completing and exchanging assets through digital currencies without involving any central authority can benefit gaming industries. Air travel industries can use blockchain technology using a smart contract to control the sale. It can also be used for preserving aircraft maintenance logs, over booking of tickets and more.

Pharmaceutical companies to establish a more effective distribution system, as well as enforce better control over manufacturing and improve medical data security are using Blockchain technology. Construction and building industries can be benefitted highly by blockchain technology where the materials are purchased from the right place without compromising the quality. Individual smart contracts can help in construction link policies where payments are automatically done when project timelines are completed. Public transportation industries can use blockchain technology for better optimizing the schedule and routes including sharing information of vehicles.

2.4 REVIEW OF LITERATURE

As discussed in Berdik et al. (2021) surveyed the potential of blockchain in maintaining security in applications used nowadays. The survey throws light on blockchain as a service used for applications in recent ages. It outlines different uses of blockchain studies in securing applications. The findings throw light on using blockchain technology in full potential for global markets.

As discussed in Jing et al. (2021) proposed a blockchain model for code copyright protection in order to avoid plagiarism. This is achieved through developing a blockchain based verification model while the nodes in the blockchain are responsible for storing and validating through the verification model. This model claims to guarantee code protection with efficiency in storage, which uses irreversible sha 256 algorithm, and betterment in speed.

As discussed in Kouhizadeh et al. (2021) carried out exploration study for the barriers in acceptance and adaptation of blockchain technology in the field of supply chain management. The extensive study has been carried out from various experts from relevant industries including academics, which is further analyzed with specialized tools. The results outline critical technology and supply chain barriers including comparisons from academics and industrial experts.

As discussed in Oham et al. (2021) proposed a blockchain framework model in the smart vehicle industry, which is resilient to malicious attacks. The proposed framework throws light in secured communication using blockchain technology with authentic smart data exchange between vehicles. The model intends to provide a new approach of security in the smart vehicle industry using the underlying blockchain technology such as trust and security.

As discussed in Ahmad et al. (2021) using blockchain technology in port logistics for data security. The transparency and security of data is a perennial challenge in this category. The traceability is scarce and integrity is at stake. The paper intends to solve challenges in introducing permissioned blockchain to improvise the operation, services and deployments. The paper outlines the issues hindering the adaptation.

As discussed in Carvalho et al. (2021) describes cases with problems and provides a relevant solution in blockchain technology. The security solutions provided are expert advice involving various security professionals from the relevant fields. The solutions drawn are the result of extensive blockchain research and includes suggestions, technical artifacts and best practices to follow while designing applications.

As discussed in Xu et al. (2021) provides a performance analytical model of permissioned blockchain. The model tends to quantify and measure the performance of fabric blockchain in a more accurate manner with its effectiveness. The insights provided are beneficial for developers with various accurate measuring parameters like size and interval of the block.

As discussed in Gupta et al. (2021) this paper explains the advantages of blockchain technology and how early adopters have embraced it. The focus of the infographic is to look at the technology's development and how it gained acceptance in many industries via step-by-step means. The ledger, smart contracts, and the excellent data security and protection capabilities of the network were described.

As discussed in Bisogni et al. (2021) prepared an encryption methodology to sign smart contracts in blockchain technology. The encryption encoding uses face as the key encoding which is combined with the RSA key using a hybrid information algorithm. The result proves authenticity of the execution without compromising the privacy including a better performance and accuracy while signing.

As discussed in Amiri et al. (2021) presents Saguaro, a permissioned blockchain, which is 5G, enabled. It is a hierarchical blockchain, which supports 5g applications, and offers better transparency, immutable data with high data security and most importantly can withstand transaction delay in mobile networks for various blockchain nodes.

As discussed in Mashatan et al. (2021) proposes a blockchain solution to avoid real estate frauds, which is a traditional challenge. The blockchain solution not only ceases fraud but also provides a high level of transparency using agent based modeling. In this way the unethical commission earned can be stopped and augment a clean way of executing real estate transactions for both the buying and selling parties.

As discussed in Hu et al. (2021) proposed a blockchain model for secure transactions in distributed energy pertaining to the internet of things (IOT). The constructed framework uses smart contracts for transparency and authenticity. This model claims to secure the transaction execution, provides higher efficiencies in IOT based on the credit value of the blockchain technology.

As discussed in Khan et al. (2021) conducted study for securing IOT transactions using blockchain technology with hyperledger fabric. The IOT transaction between devices may prove a security breach and inconsistency. The study conducted using block chain as a service proves elevated performance and better security as against the traditional approach with evaluation parameters like latency and throughput.

As discussed in Zhang et al. (2021) proposes a blockchain and smart contract methods in securing transactions pertaining to energy transactions. The various significant factors like price, consumption, flows, supply, demand and shifting are secured through contracts using blockchain technology, which uses consensus mechanisms. This method tends to improve power stability and efficiency in the market.

As discussed in Zhao et al. (2020) proposed a technique of using sidechain where it proves efficiency in multiparty transactions, which marks valid for parallel branches, and induce transactions between blockchain that solves inconsistency. The techniques also created a protocol, which is distributed within uneven blockchain, which is decentralized and implemented in an emulator.

As discussed in Pasala et al. (2020) presents an investigation of blockchain trading and technology. The paper evaluates and discusses bitcoin, its advantages, disadvantages, and the steps to safeguard. The salient features like security, assurance, trust and limitation leave an open question that can be benefited from judging the adaptation and uses of this technology in investment.

As discussed in Albayati et al. (2020) studies the usability of blockchain technology through technology acceptance model. The study unearthed some significant parameters, which are used in surveys to get a meaningful outcome. The result of the study shows the acceptance of the technology and a trust model among the users in terms of security.

As discussed in Konashevych et al. (2020) utilizes Emercoin to handle payments on the blockchain network. The payee must approve each transaction, and Emercoin itself does not charge fees. By approving it, I want to make it legally accessible. To enable a completely random lottery ticket to be used, the researchers designed a lottery ticket that does not rely on a third party to hold or print it. Extended for an empirical investigation of the impact of implementing a lottery system, the study examined a mathematical model that demonstrates the benefits of a lottery system.

As discussed in Jia et al. (2020) proposed a blockchain payment protocol, which does not have any third party intervention. It is more efficient, supports various signatures, and has better security setup as against the traditional cryptographic approach. This model is implemented in Java and is prepared enough for usage.

As discussed in Zhao et al. (2020) proposes a model, which satisfies the problem of cross blockchain transactions where there is a possibility of survival of one fork during the mining process. The paper throws light on solving this problem by creating multiple forks and spaces, which are inter-related through progressive functions. The fork topology grows with the blockchain transactions.

As discussed in Bamasag et al. (2020) studies the uses of blockchain in applications. It highlights a few important points like usage of secured smart contracts in various sectors and securing the individual property, transactions and contracts using this technology.

As discussed in Reyes-Macedo et al. (2019) presents the use of bitcoin transactions during the ransomware attack. This paper intends to analyze the transactions with the use of blockchain with transaction tracking and some measurements during the ransom payments needed to unblock the data.

As discussed in Jivanyan et al. (2019) proposes a modified and enhanced version of Zercoin known as lelantus. The study shows that the blockchain payment system shows better and smaller proof sizes and better performances than Zerocoin. Lelantus has better confidentiality and better efficiency without third party interventions.

As discussed in Gomaa et al. (2019) covers blockchain use in digital crypto transactions with the implementation of an ERP When the debate begins, it centers on

the development of a digital wallet, which then includes adding money, transacting, evaluating the transaction, and tying into an existing ERP system.

As discussed in Maksutov et al. (2019) paper proposes a detection transaction mechanism in money laundering and possibility of stopping the same. It uses an anonymization technique for detection and deanonymization technique for detection. This procedure proves to be beneficial in identifying the relationship between the users and related transactions in money laundering cases.

As discussed in Thio-ac et al. (2019) focus on the study conducted to evaluate the use of blockchain technology in procurements for organization. The study evaluates the blockchain mechanism as against the traditional method e-procurement system. The result shows that data fraud can be reduced with no third party intervention when blockchain mechanism is used.

As discussed in Saugata et al. (2020) explores the digital crypto currency and its future economic scope. The paper deals with the blockchain currency and its market standing. The replaceable financial currency scope as against traditional banking mechanisms.

As discussed in Saugata et al. (2020) explores the usage of blockchain in social media and its advantages in post privacy. The opportunity to earn rewards for up votes and an option to control the advertisement while counterfeit posts are eliminated.

As discussed in Saugata et al. (2019) chronicles the development of blockchain technology, and it covers bitcoin's early days to smart contracts and performance improvements. There are a number of different industries where blockchain technology has been used.

As discussed in Faisal et al. (2018) the research studies the capability of blockchain to store metadata in order to stop criminal use. The study uses bitcoin as an example where the metadata usage can harm and produce big security laps. Embedding the metadata with blockchain has improved security and reduced abuse.

As discussed in Tilooby et al. (2018) surveys the use of blockchain technology in financial transactions. This study shows the real insights of using the chain in financial transactions. The study has been conducted using suggestions by various

experts from finance industry. The study throws light on three approaches such as literature, perception and a theoretical interpretation.

As discussed in Kotilevets et al. (2018) proposes the usage of DAG (Directed Acyclic Graph) which has better performance in transaction speed and helps in scaling using parallel chains. This also leverages not using mining at all and affordability in terms of not paying the mining fees.

As discussed in Loebbecke et al. (2018) studies of using blockchain in the diamond industry as against the traditional approach. The study shows better trust ability in the ecosystem when blockchain technology is introduced. This has affected the transaction with better transparency and role of intermediaries.

As discussed in Loebbecke et al. (2017) proposed a framework where the GHOST protocol is used for digital transactions in blockchain. It shows a better alternative approach to bitcoin with robustness in terms of ledger transaction and uses trees instead of chains. The GHOST protocol claims to be a better approach in terms of robustness and efficiency.

As discussed in Vovchenko et al. (2017) blockchain technology is investigated to find out how it is now being utilized in the modern economy. In this study, consumers are able to execute financial transactions and reduce operational risk and cost with blockchain-enabled technologies. In order to control the digital economy, digital contracts should be used.

As discussed in Peter et al. (2017) surveyed the opportunities of using blockchain technology in sales and online payment transactions. The study shows that quite a major portion of the sector are exploring the use of this technology but less efforts are made from some european banks as they have some pending works to be completed.

As discussed in Dai et al. (2017) studies the use of blockchain in assurance and accounting. The study explores that there is a better probability of transparency and auditability including precision in accounting and assurance system.

CHAPTER 3

FRAMEWORK DESIGN & DEVELOPMENT OF HYBRID BLOCKCHAIN SECURED TRANSACTION SYSTEM (HBSTS)

This chapter explores the overview of the HBSTS (Hybrid Blockchain Secured Transaction System) and how the framework is designed with various conceptual and technological flow design. This chapter shows how the framework development has been carried out with algorithms being used. This chapter ends with the various security framework testing carried out in HBSTS and its result.

3.1 FRAMEWORK OVERVIEW

With regard to security, the framework is anticipated to provide significant safeguards. Its implementation capability is simple to develop and may be used on any platform. When compared with a client-server architecture, the framework offers superior transparency. Using the HBSTS on premise, or via the cloud, or a combination of both is known as hybrid. It has a multifactor authentication system where a client utilizing the chain needs to verify in two different ways.

The HBSTS protects every transaction with quickest hashing and encryption for superior performance and simultaneously with improved security. Transactions in HBSTS are made secure and do not fall prey to different malware, infection, ransomware, SQL infusion and other fatal attacks. It is protected as far as hacking, information variations, and erasures, proof altering and different types of misuse with data.

This hybrid framework can be incorporated with other databases to load balance the performance. The pivotal and basic piece of the data can be placed in blockchain though non-basic data can be posted on the conventional database from this structure. Hence, this system is viewed also as a hybrid regarding combination to the conventional approach model.

HBSTS works in a consensus algorithm, which does not require a third party or central authority contribution. It checks the legitimacy of the chain with itself. The transparency is not arranged and the information cannot be altered. Henceforth the transaction subtleties reflecting in the chain are unique and legitimate. HBSTS has a more noteworthy productivity in adaptation to internal failure.

The chain is very much kept up geologically and can withstand force majeure or any sort of catastrophe. HBSTS is maintenance free. The distributed ledger does not require backup and restoration, neither HBSTS require any extra labor to execute, control and maintain.

HBSTS likewise does not require any extra groundbreaking space and memory and subsequently can accommodate nodes. The continuity and coherence of the chain can be made with only two nodes.

The transactions are made secure with the idea of Merkle tree where the child and parent data are hashed eventually rehashed, which is comparatively faster for better performance. The blockchain transactions are encrypted which gives an improved security and blocks are interconnected with hashes which interfaces with the accompanying block with its past hash value.

The prime element of HBSTS is its affordability, no license or subscription cost. HBSTS is platform independent and can be utilized over any operating system and since it is a distributed ledger, hence no costly database or relevant software license is required.

HBSTS is light weighted, consumes less space. The utilization of memory is entirely less. The I/O activity is appealing fast when utilized with any system or device. As HBSTS does not require any expensive hardware, can be executed over any classic or old hardware. It can also work on any open source OS as long as library files are supported.

3.2 FRAMEWORK DESIGN AND MODEL

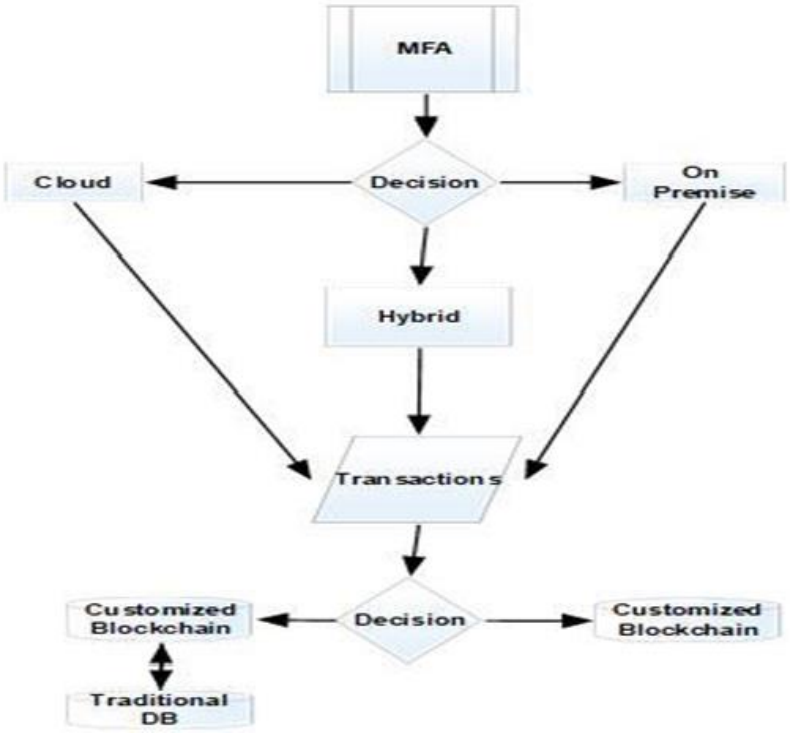

Figure 3.1 Basic flow of HBSTS framework

Figure 3.1 shows the high-level flow of HBSTS framework. The HBSTS framework can be implemented over the cloud, on premise as well as a combination of both. Once the type of implementation is selected, the next process is device registration. In device registration, the desktop, device (iOS/Android), laptop needs to be registered with a two-factor authentication system including a registered email ID and a photo. The registered devices are sent with an OTP (One Time Password) for verification, also with verification OTP to the email id. Once the device is registered with a username and password sent over SSL (Secured Socket Layer) including OTP verification, the user is registered with the device to create secure entries to the customized blockchain.

The authenticated users are allowed to create secure transactions now. The data is fed into the HBSTS and once the transaction is approved, it is saved into the blockchain-distributed ledger. The HBSTS framework will save additional data of transactions

like attachment, images, and relevant videos to the traditional model of database. The good thing about this is that it can be added with every transaction. In contrast to the data in the asset field, the metadata field allows adding new information to every transaction. This will allow us to store more additional data without putting load in the blockchain. The additional data, which is saved in the traditional model, is hashed and saved to the blockchain. In case if there is a security breach in the traditional model, the hash can be compared for, a particular transaction and fraud can be detected. **Blake 2** hashing algorithm is used in the framework, which is faster and has better performance.

Table 3.1 Hash comparisons

Algorithm	Output size	Internal Hash Sum	Block size	Message Length	Rounds	Hash Speed (MiBps)
BLAKE2b	512	512	1024	128	12	947
MD5	128	128	512	64	64	632
SHA-256	256	256	512	64	64	413
SHA3-512	512	1600	576		24	198

Table 3.1 shows the comparison of Blake2b with other hashing algorithm. Blake2 is a high performance-hashing algorithm. It is quicker than MD5, SHA-1, SHA-2, and SHA-3. It gives security better than SHA-2 and like that of SHA-3. Blake2 expels addition of constants to message words from Blake round function, changes two rotation constants, streamlines padding, adds parameter block that is XOR'ed with initialization vectors, and reduces the number of rounds from 16 to 12. Blake2 bolsters keying, salting, personalization, and hash tree modes, and can yield digests from 1 up to 64 bytes. Blake2 can accommodate more messages for hashing and the number of rounds are less as compared to others.

This framework uses **Twofish** encryption system for better performance on systems, laptops and various handheld devices. Twofish is a symmetric key block cipher of 128 bits with a key size of 256 bits. Twofish is identified as the successor of Blowfish. Twofish's unmistakable highlights are the utilization of pre-computed key-dependent

S-boxes with a complex key schedule. One portion of n-bit key is utilized as the real encryption key and the other portion is utilized to change the encryption algorithm.

Table 3.2 Encryption comparisons

Parameters	AES	DES	3DES	BLOWFISH	TWOFISH
Cipher	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric
Block size	128 bits	64 bits	64 bits	64 bits	128 bits
Round	10/12/14	16	48	16	16
Key Length	128/192/256 bits	56 bits	112 and 168 bits	32 - 448 bits	128/192/256 bits
Attacks	Side channel attack	Linear and differential cryptanalysis	Brute force attack/ Sweet32	Birthday Attacks	Secured with cryptanalytic attack
Performance	Faster	Very Slow	Very slow	Very fast	Very fast

Table 3.2 shows the comparison of Twofish with other encryption algorithm. Twofish obtains a few components from different designs like pseudo-Hadamard transform. It has a Feistel structure and utilizes a Maximum Distance Separable framework. It has 16 rounds, is viewed as one of the quickest of its sort. It is perfect for use in both IT equipment and software environments.

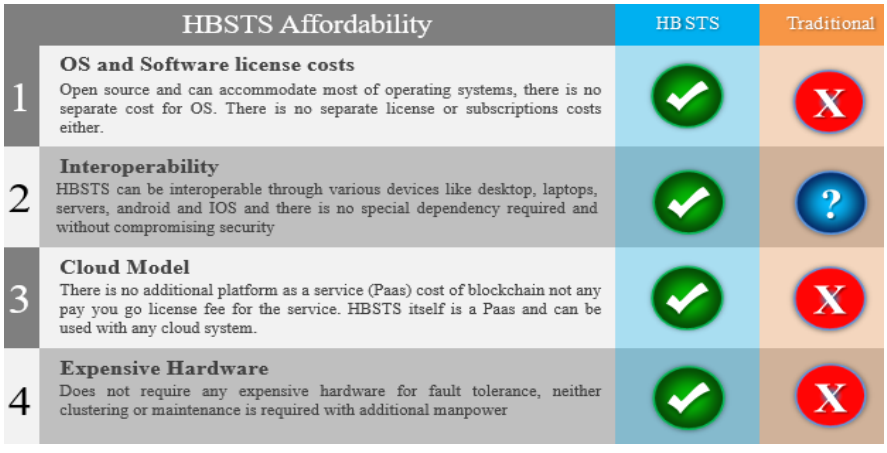

Figure 3.2 HBSTS vs Traditional affordability

Figure 3.2 shows the affordability chart of HBSTS against the traditional approach. HBSTS is open source and does not require any special hardware cost or software license. It can be used with any system, laptop, android and iOS device. As long as

the library files are supported, it can be operated on any of the operating systems. It consumes very less memory and disk space. Does not require any costly hardware to perform for fault tolerance and can withstand the chain with as small as two nodes operating. HBSTS can thus be attributed as an affordable model. In the traditional approach model, the rising cost of the database, clustering, costly hardware and maintenance are non-comparable factors

The HBSTS transaction predefined process as follows:

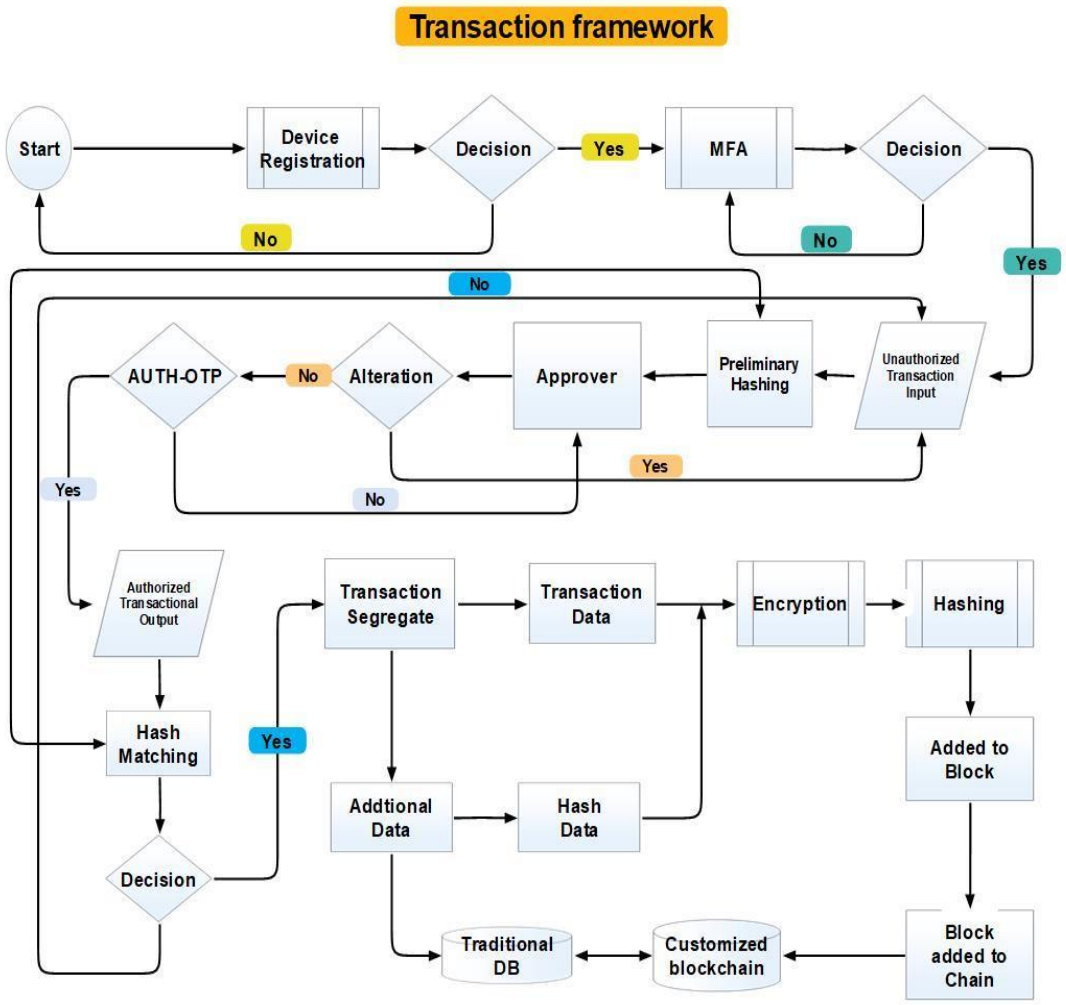

Figure 3.3 HBSTS transaction process

Figure 3.3 shows the transaction flow on HBSTS framework. The preliminary process starts with registration of devices. The registration of the device is not only associated with a username and password but also with the email id and mobile number. Once

the user is registered with a device, a multifactor authentication process runs. In this authentication process, the user ID and password are sent over SSL to authenticate and in the next cycle two different OTP is sent to the registered mobile number and email ID to authenticate further.

If this procedure fails, the user must begin the login process all over again. Transaction input can begin after the user has been authorized using the multifactor authentication technique. The entry must be made with extreme caution, as it is added solely to the distributed ledger and cannot be changed once the approver authorizes the transaction. The transaction entry not only consists of crucial data but also additional data like images, files, videos and audio, which too can be entered as a secured transaction. The transaction passes onto a preliminary hashing process where the transaction entered is hashed before passing to the approver. The approver then double-checks the transaction. If any changes to the entries are necessary, the transactions can be returned back to the user for rectification. This cycle is repeated once the approver finds the transaction valid in terms of data. Next, the approver needs to approve the transaction for which there is an OTP authentication process such that it does not fall in wrong hands. If the OTP authentication process fails, then the transaction is sent back to the approver for re-authentication. Once the transaction process is approved and authenticated by the approver, it is passed on to the hash matching process.

The hash matching procedure assures that data does not change throughout the network transaction's transmission. Once the hash matching process is successfully completed, the transaction is passed onto segregation of transactions. On fail, it signifies that there is a threat to the transaction or the transaction may have been modified. In that case the transaction becomes invalid and cancelled. The user again has to create a fresh transaction. If the hash matching process is passed, then the additional data if applicable is segregated from the transaction. The additional data is rehashed and stored to the traditional database. The hash of the additional data is then added to the original transaction and is encrypted and re-hashed. The data are then added to the block. Each blockchain node verifies the transaction using a consensus mechanism, which is a fundamental characteristic of the blockchain, and then adds the freshly produced block to the chain. As a result, the block is added to the chain, and

each subsequent block is linked to the preceding hash. All of the essential transaction data, as well as any additional data held in the conventional database, is added to the distributed ledger. The transaction in HBSTS is secured and confidential. The hash of this additional data is stored in the blockchain. If there is any change, modification, tampering with the additional data residing in the traditional model, it will be inevitably transparent. This also throws light with the performance of the blockchain where crucial data can be visible from blockchain and additional data like videos, images, audios or other related files, which consumes heavy space, can be stored and fetched from the traditional database.

The user registration model is as follows:

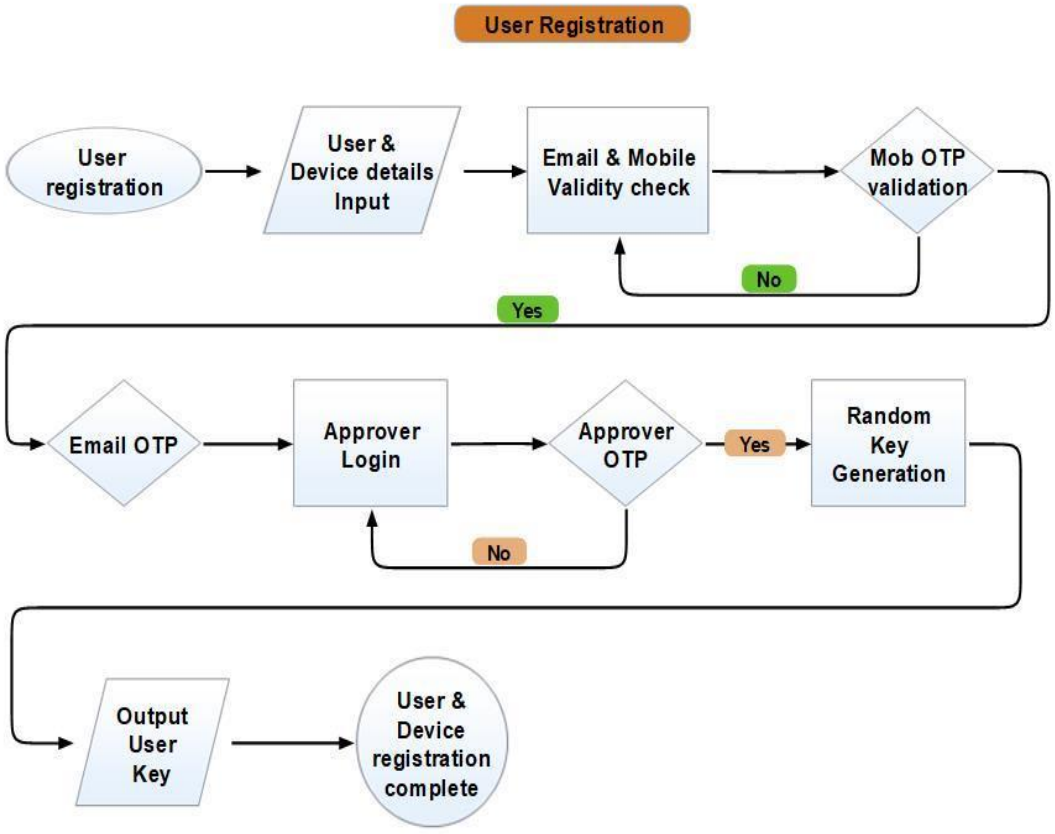

Figure 3.4 HBSTS user registration process

Figure 3.4 shows the flow of the user registration flow. The user registration starts with the details of user and device to be input. The user is presented with username, password, email, mobile and device type.

The user verification process checks the uniqueness of the username and strong password validity. The system sends verification OTP to the mentioned mobile number. Upon successful verification, an OTP is sent to the mentioned email id. Once the email verification is completed, the details are sent to the approver. Then the approver login with its own user Id and password.

The approval is presented with a validity of its own identification in the form of OTP. The approver, the user, verifies once the same and device registration is completed. A system generated random key is presented which the user has to store. This user key will be used to encrypt and decrypt the data entered in HBSTS. A copy of the key is also sent to the approver.

Multi-factor Authentication model is as follows:

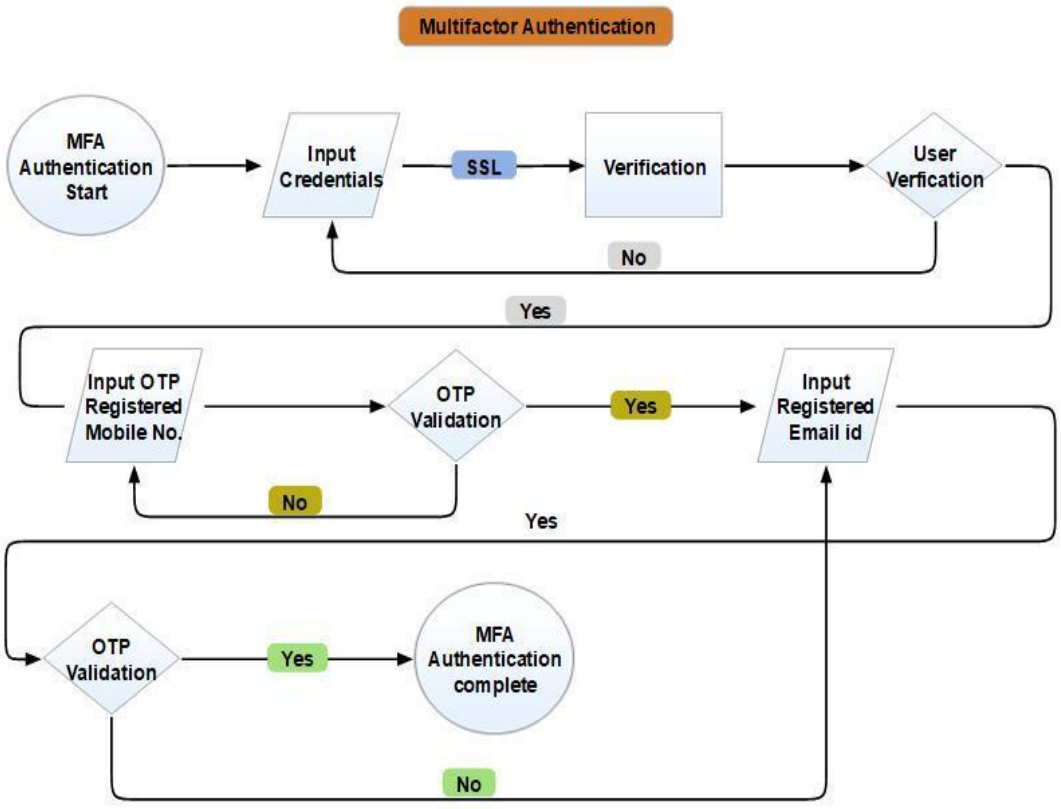

Figure 3.5 HBSTS multi factor authentication process

Figure 3.5 explains the multifactor authentication where the user inputs credentials to login to the HBSTS framework over SSL.

Once the user is verified with the username and password, the user needs to validate a second layer of authentication process. In this layer authentication is performed by sending an OTP (One Time Password) to the enrolled mobile number.

Once this OTP authentication is validated, another OTP is sent to the registered email id. Upon effective fulfilment, the email id verification is completed. This ends the process of multifactor authentication.

The encryption process is as follows:

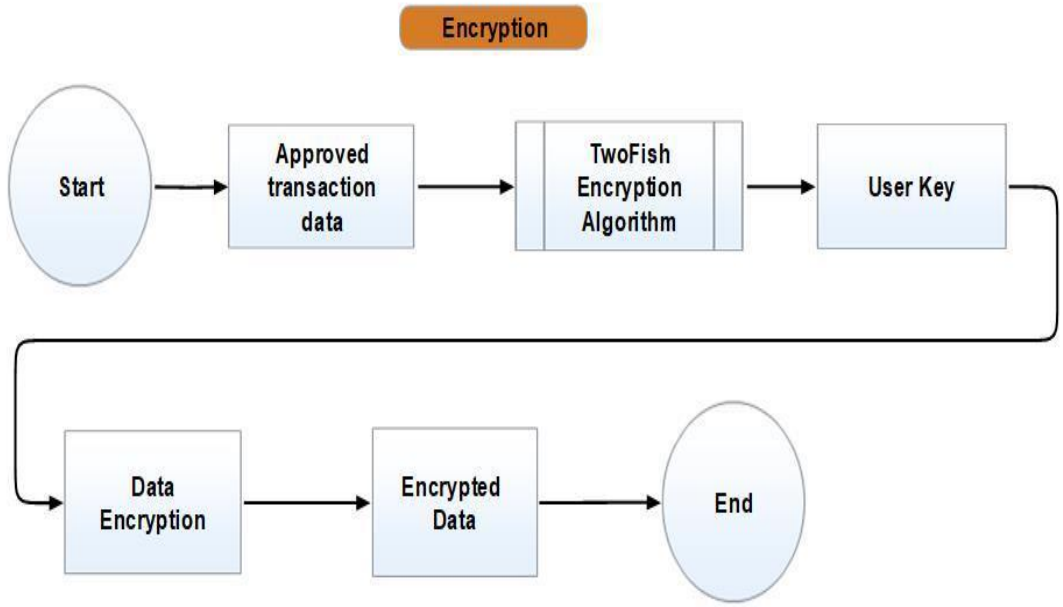

Figure 3.6 HBSTS encryption process

Figure 3.6 explains the encryption process that starts when the approver approves the transaction data.

The segregated transaction data, which means when additional data is saved into the traditional database and the crucial data along with the hash of the additional data are encrypted with Twofish encryption. First, a random key is generated and the crucial data is encrypted with the random 128-bit key and a block size of 128 bit.

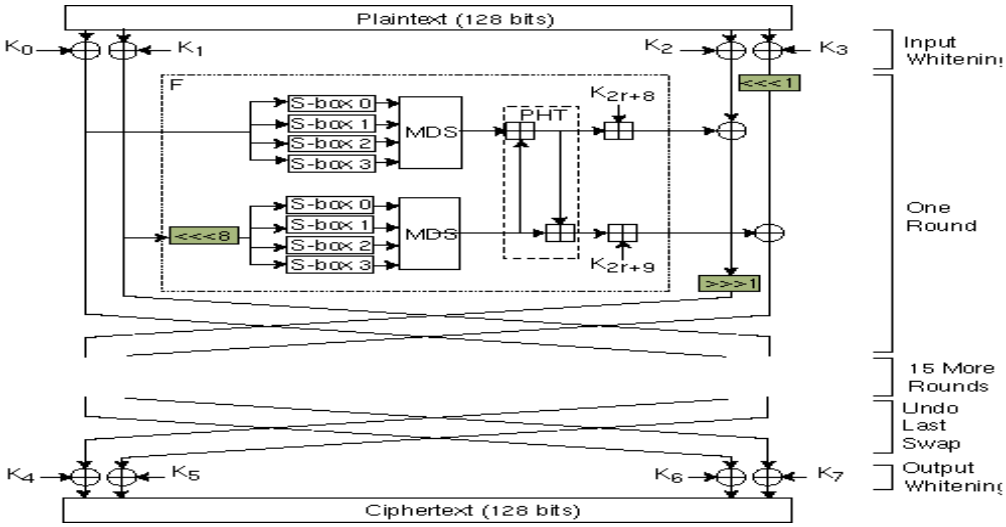

Figure 3.7 Twofish algorithm

Figure 3.7 explains Twofish, which is a symmetric encryption algorithm, uses a single key for encryption and decoding. The size of the secret key is between 256 and 512 bits, while the block size is 128 bits. Twofish's fast execution is found in many software and hardware applications. The information is very safe. The Twofish cypher is a Feistel network. When each round just half of the material is XORed, this means that half of the content is being F-ed, and then the remaining half is XORed. F function takes 32-bit words as input. The words are put into four-byte units. Each of the four bytes travels on four separate paths and enters four different key-subordinate Sboxes. This uses a Maximum Distance Separable (MDS) matrix to connect the four bytes, which is then merged into a 32-bit word. Using a Pseudo-Hadamard Transform (PHT), two 32-bit words are combined to create a 48-bit value. Then the values are XORed with the remainder of the text. In addition, two 1-bit rotation turns are occurring in front of the XOR and one after.

Twofish moreover has many allusions to "pre-whitening" and "post whitening" where before the first and last round additional sub keys are XORed. Every movement of the round capacity is injective and surjective, which implies coordinated which is a special property of Twofish. S-box substitution, GF (28) MDS matrix, GF (232) additions, XOR, and 1 bit rotations. This makes the estimation difficult to attack measurably or mathematically.

S-boxes, which are key dependent, are intended to be protected against the two significant attacks of the mid 90s, differential and linear cryptanalysis and safe against

whatever obscure attacks comes following. In Blowfish, key dependent s boxes were picked randomly but in case of Twofish, it is not chosen arbitrarily and built with improvement controls where it is tested with different stages and blend with possible 128-bit keys. The MDS network was prudently picked to give great dissemination, to hold its MDS property a lot after the 1-bit turn, with quicker execution. The key and PHT additions give dissemination between the sub blocks and the key. The round sub keys are purposely decided, using a segment like the S-box development rules, to hinder related-key attacks and to give extraordinary key mixing. The 1-bit rotation is expected to isolate the byte structure; without it, everything deals with bytes. This action benefits in cryptanalytic attack. The pre-whitening and post whitening seems to add a round to the difficulty of cryptanalytic attack.

Hashing process is as follows:

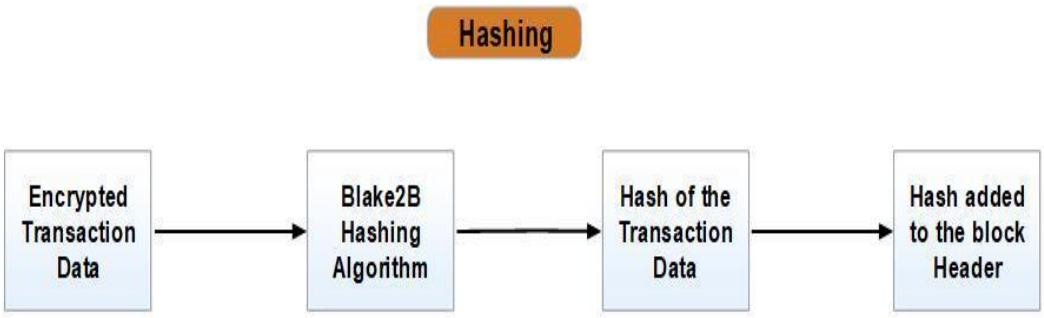

Figure 3.8 HBSTS hashing process

Figure 3.8 describes the hashing process, where the encrypted transaction data is hashed with Blake2b, which has an output size of 512 bits with internal hash sum of 512 bits and just 12 rounds yet secured. In order to improve both speed and security, the Merkle tree hash rule is used. The hash value of this transaction data is also contained in the block header. The hash of the preceding block is used to connect the blocks together in the chain of blocks. The genesis block is the first block in which no hashes from earlier blocks are present.

The data output model is as follows:

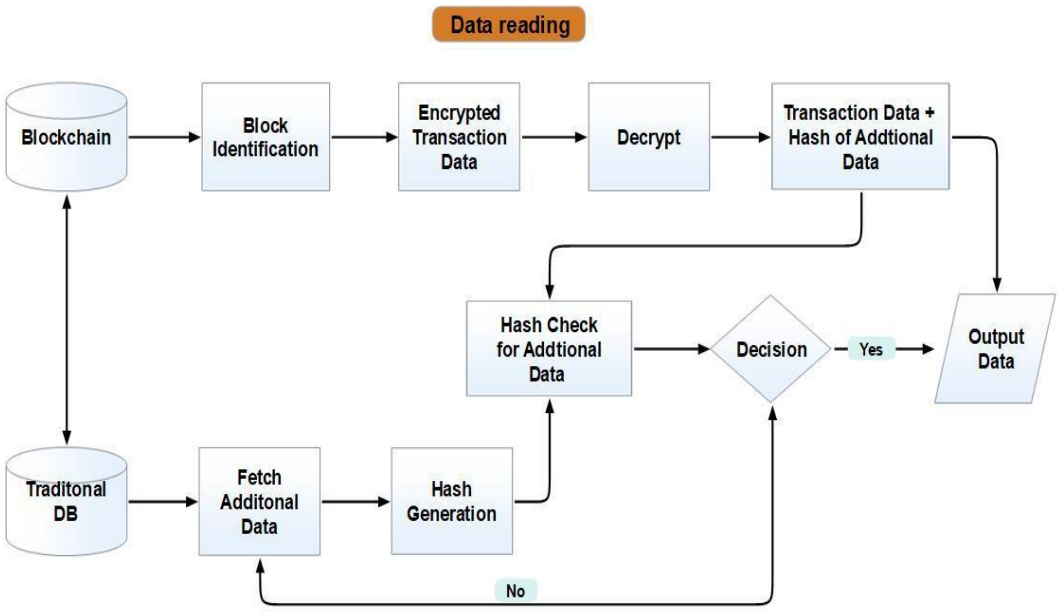

Figure 3.9 HBSTS data output process

Figure 3.9 shows when the data fetched from HBSTS framework the data is first queried or displayed in reference to a common field residing on blockchain and traditional database. The data record is queried in a blockchain distributed database and traditional database in parallel. The transaction residing in the block is identified as the first where it locates the encrypted data. The data is decrypted with the help of the user's key. The transaction data in blockchain also stores the hash of the associated record stored in the traditional database.

The record fetched from the traditional database generates a hash, which is matched with the stored hash in blockchain. If the same is matched, the data is displayed from the traditional model as output. The blockchain data, which has the crucial transaction information, is safe and displayed irrespective of the hash test result for traditional databases. In case the hash test is not passed, the additional data like images, videos, audios or other documents, which consumes more space, are tampered and returned to fetch data.

Data output for Approver model:

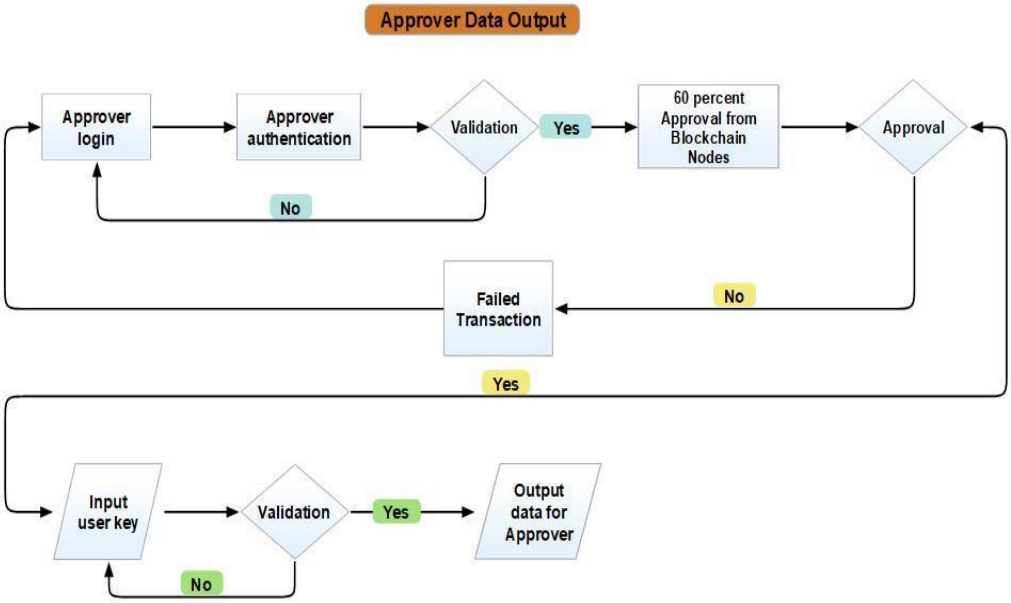

Figure 3.10 HBSTS data output process for approver

Figure 3.10 shows how approvers can view their related transactions only with the consensus model and users approval. To ensure data is transparent and only authorized individuals can view the data, it passes on to an approving process. Approver has to go through an authentication process along with an OTP validation. Once the validation is valid, a consensus of more than fifty percent of blockchain nodes is required to check if the request is valid. Once the same is valid, the related user can approve the transaction through the user key to be viewable by the user. This provides a security process such that the transaction cannot be viewed anonymously.

3.3 FRAMEWORK DEVELOPMENT

HBSTS framework is developed on Python majorly. The development of the framework starts with the creation of a block class, which has crucial components for blockchain transactions.

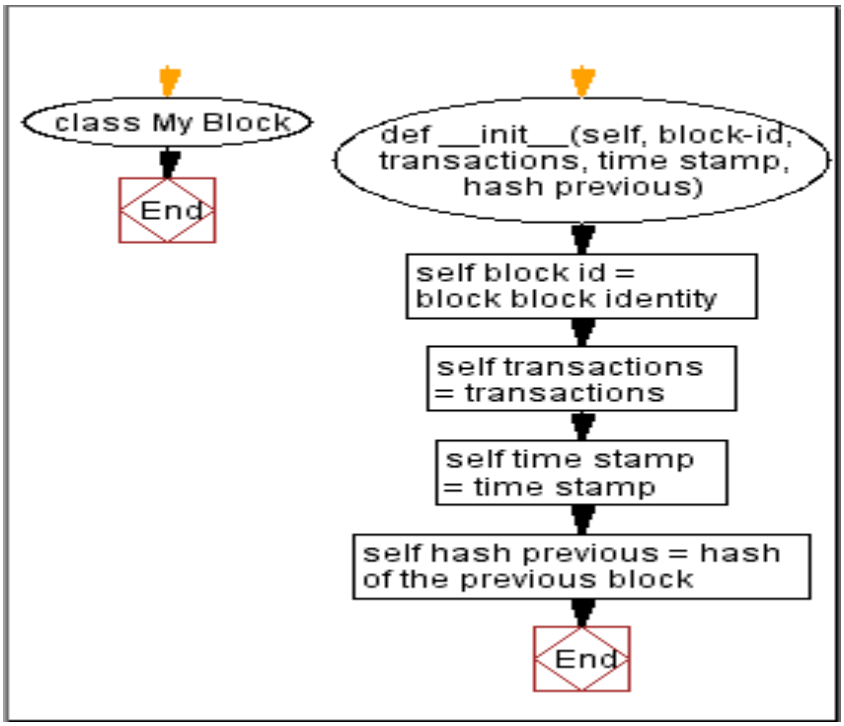

Figure 3.11 HBSTS Blockchain class algorithm

Figure 3.11 shows how the block holds the transaction data along with a timestamp and previous hash. First, the blockchain class is declared.

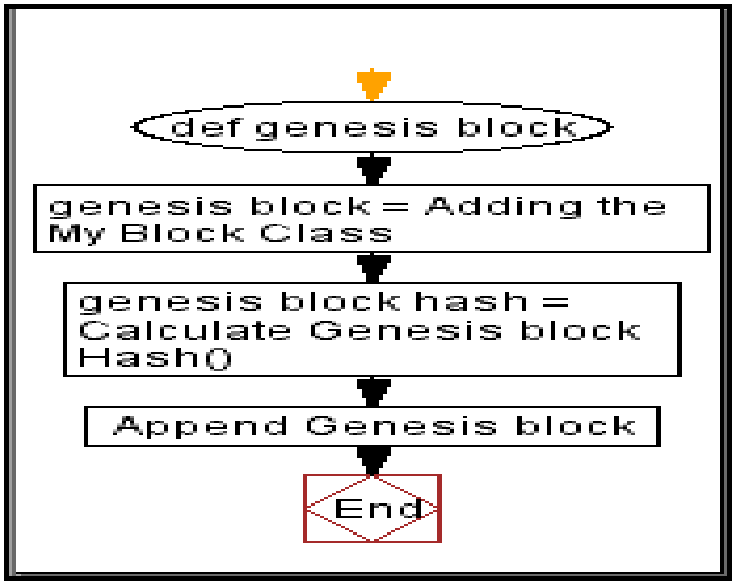

Figure 3.12 HBSTS Genesis block algorithm

Figure 3.12 defines how Genesis block serves as the starting point for the whole blockchain and devoid of previous hashes.

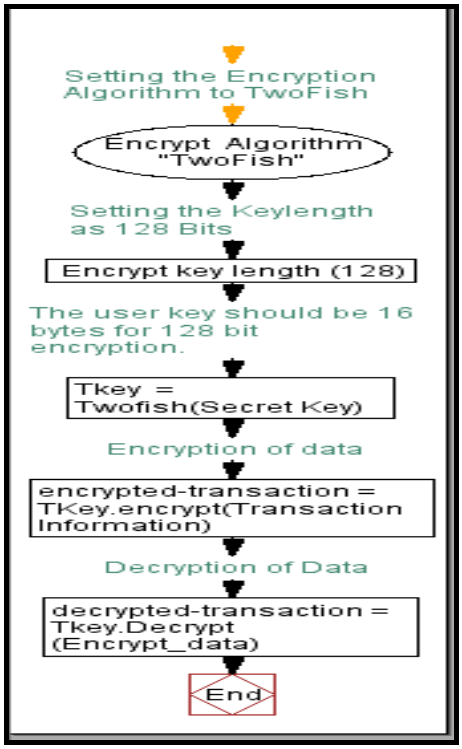

Figure 3.13 HBSTS Twofish encryption algorithm

Figure 3.13 shows how transaction data is encrypted with the user key and uses Twofish algorithm. The algorithm encrypts the transaction data and hash of the additional data. The encryption mechanism is fast and with just 16 rounds and very secured against cryptanalytic attack.

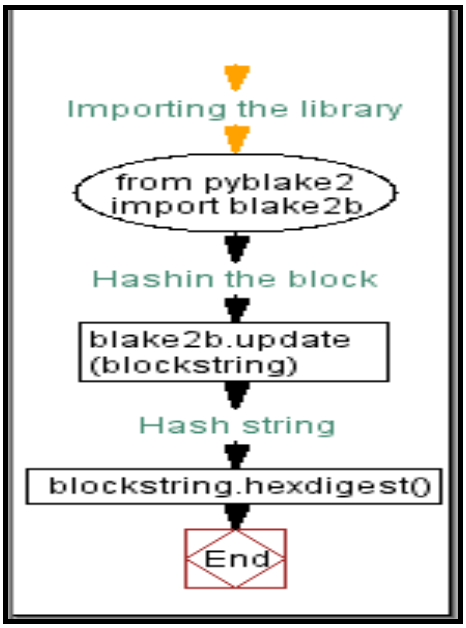

Figure 3.14 HBSTS Blake2b hashing algorithm

Figure 3.14 shows the Blake2b hashing is used to hash the data blocks for security and more importantly integrity of the block. It is hashed in such a way that if any of the blocks is tampered, all the following blocks will be invalid and the chain will not accept the data.

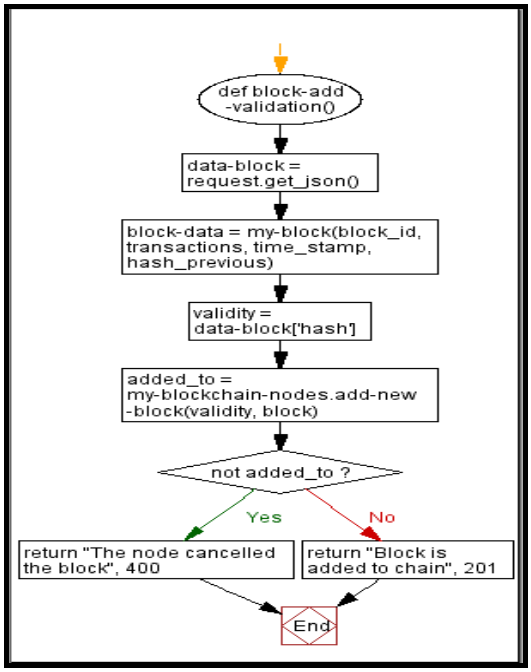

Figure 3.15 HBSTS Blake2b hashing algorithm

Figure 3.15 explains how the transaction data once approved by the approver are then added to the block. The valid encrypted and hashed data are added after checking the previous hash with the last block hash. The block will only be valid once the hash data matches and is approved. The block is then appended to the chain. On a more granular level, the acceptance and rejection of the nodes is depicted where the nodes validate the block to be added by checking the hash.

Here are two figures, which show the algorithm for the acceptance and rejection on adding a new block. Secondly nodes check by validating with the JSON (JavaScript Object Notation), validates the block data which if does not match provides 400 which means nodes cancelled the block addition to the chain whereas 201 shows the block is added to the chain.

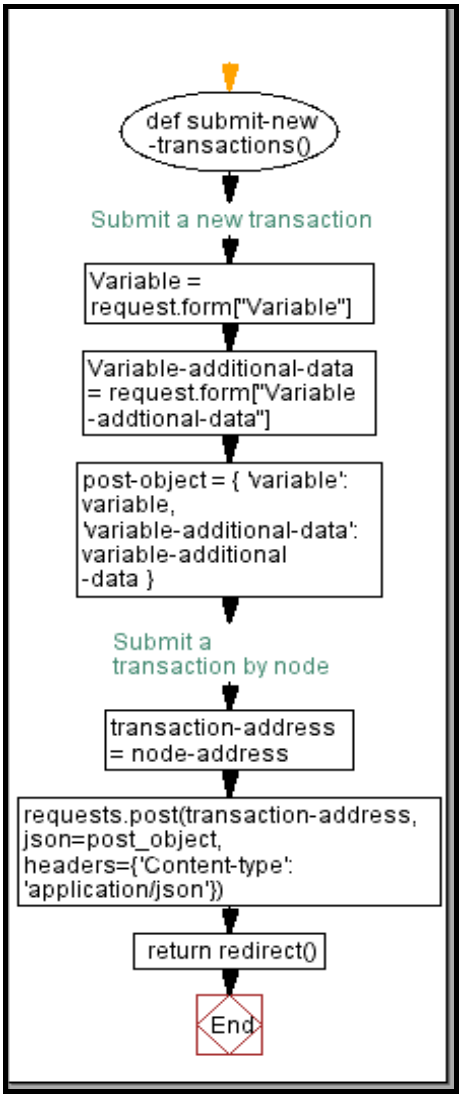

Figure 3.16 HBSTS new transaction

Figure 3.16 shows how to submit a new transaction from HBSTS framework node, it is required to enter the crucial fields which are required in the transaction as per the requirement from different lines of business or small and medium sized enterprise.

The required fields are posted where the node addresses are added. The new transactions are in the form of unsettled or unapproved transactions. These transactions require approval from the approver. The algorithm of adding new transactions is as below. The transaction data consists of crucial data to be added in the blockchain and contains the additional data to be added in the traditional model.

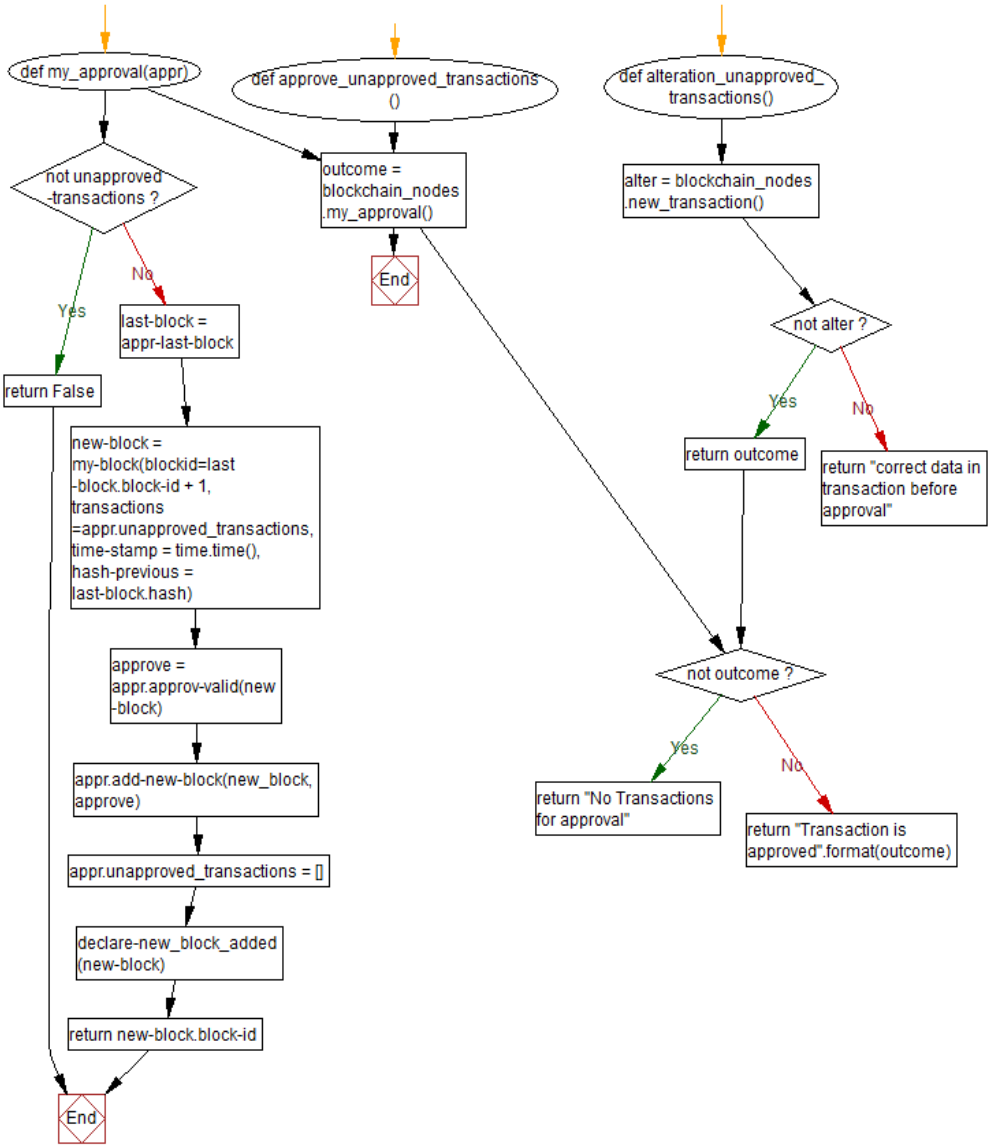

Figure 3.17 HBSTS new transaction approval algorithm

Figure 3.17 shows the way approver approves the transaction, and the issue is then handled as a confirmed transaction. If the transaction has to be changed, the data is provided to the user to make the necessary changes. The alteration cannot be made once the transaction is approved as it will be appended in append only distributed ledger. Once the transaction is finalized for approval, the algorithm returns as “Transaction is approved” else it returns as “No transaction for approval” incase if there is no transaction.

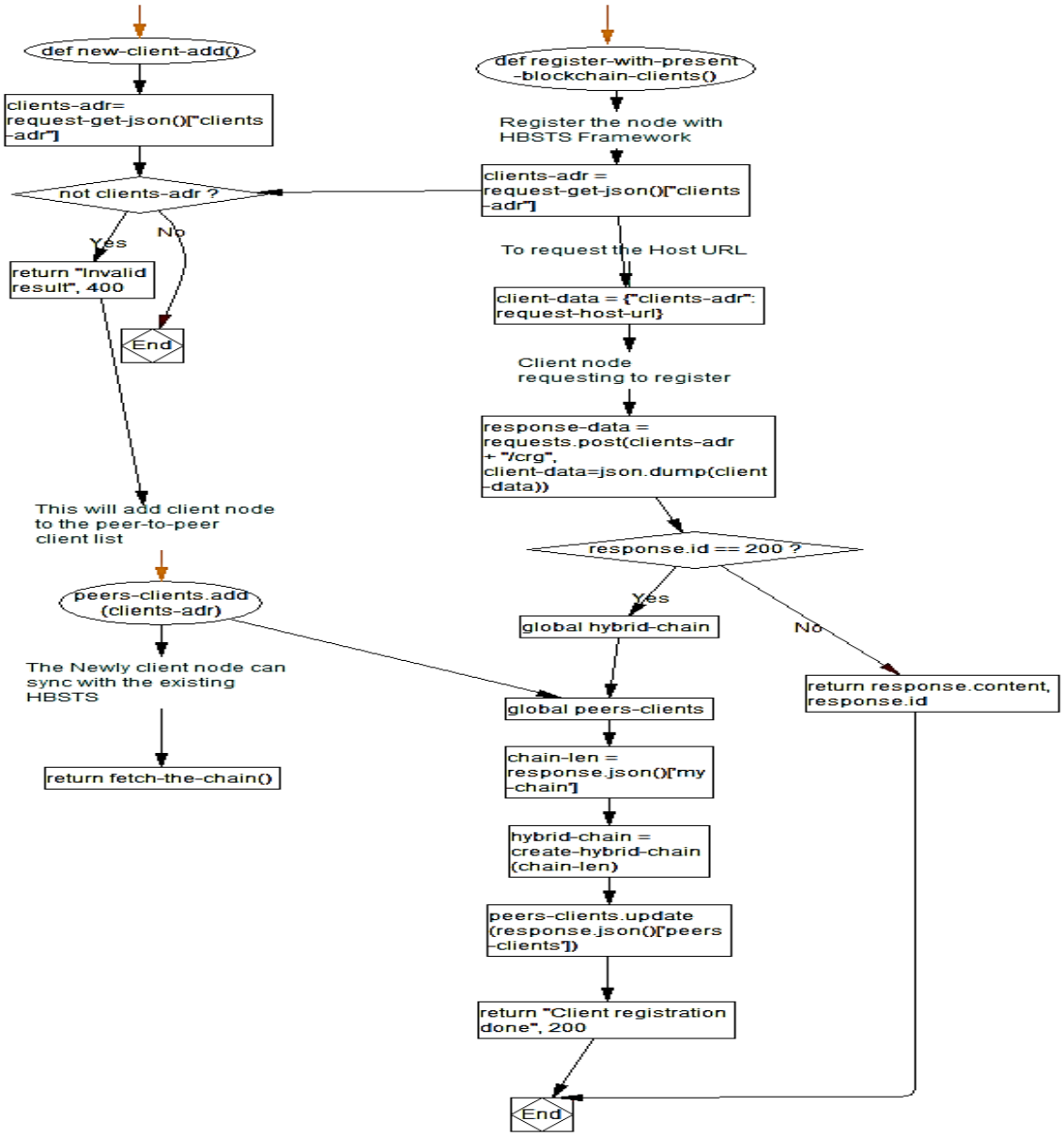

Figure 3.18 HBSTS fault tolerance

Figure 3.18 depicts how the user nodes are registered in the HBSTS peer-to-peer network. The clients are registered in the following algorithm where each new node receives a copy of the current blockchain. Here multiple client nodes will maintain a copy of the blockchain and in case any node is not reachable or not in the network, the chain is maintained creating a fault tolerance.

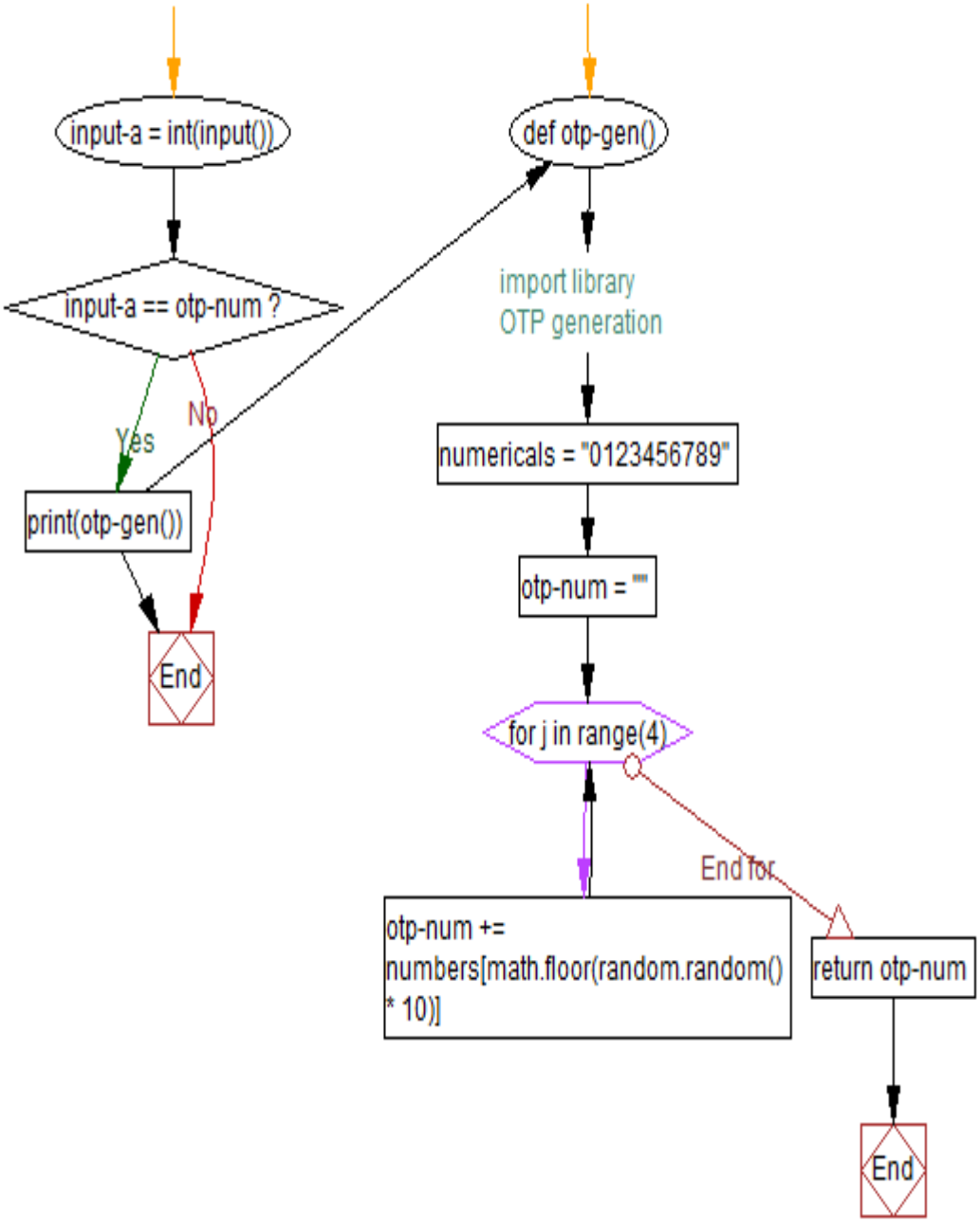

Figure 3.19 HBSTS OTP generation

Figure 3.19 explains how the OTP generation algorithm generates a random 4 digit OTP which is sent to the mobile number of the user and eventually the email ID of the user for verification. The same concept is applicable for approver as well when verification is required. The OTP generation flow shows how the algorithm is created where the OTP generation library is imported sent and matched with the OTP numbers.

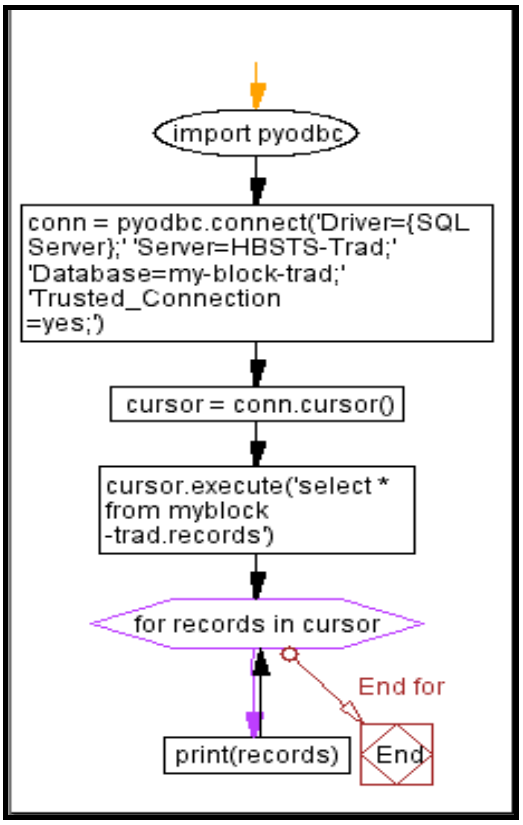

Figure 3.20 HBSTS traditional database connectivity

Figure 3.20 explains how some of the additional transactions of blockchain are stored on the traditional database. A part of the algorithm is shown here in the flow diagram with a connectivity sequence to a SQL database where records can be displayed and queried.

3.4 FRAMEWORK TESTING

Security testing is a measure to find various loopholes in the application security, which outlines the vulnerabilities and procedures that the application and data can be compromised. It is in fact a mandatory requirement for post development of any framework or application. This testing is executed from a hacker or attacker's perspective and thus examining the application, environment and networks for potential loops. Penetration testing or intrusion testing includes black-box testing, grey box and white-box testing.

Black-box Testing: In black-box testing, the tester does not have knowledge of the testing environment and has no internal permission to the application environment. This type of test is very hard to perform and time consuming. This attack is a clone attack, depicting how a hacker would try to hack the application and infrastructure environment. This type of attack truly demonstrates how an outsider might gain access to the system.

Grey-box Testing: In this type of testing, the tester has some information and knowledge of the testing environment. This simulates where an attacker penetrates to the system on perimeter level with limited information. This way a tester can impersonate a user who has lower level access to resources.

White-box Testing: In white-box testing, the tester has complete information of the application and infrastructure environment. This throws light on potential threats in source code, data and logical flow, design errors, security vulnerabilities and/or lack of security measures. This type of testing is more complete since both the internal and external threats are evaluated.

The HBSTS framework is append-only-database and stretched across various locations. It is a distributed ledger and works in a peer-to-peer environment. Although it is less vulnerable by design, there may be various threats to modify/delete records for various financial gains, corruptions, personal grudges, evidence tampering etc. Bad actors are always present targeting blockchain implementation using various exploits.

The testing is done through a professional penetration testing service, which is a combination of black-box and white-box testing. This results in a more granular level of testing from a security point of view.

Some of the common attack types are:

- Cross Site Scripting (XSS)
- Brute force
- Majority attacks
- DDOS
- Blockchain ingestion

3.4.1 Cross Site Scripting (XSS) attack

Severity: High

Issue: Cross-website scripting (otherwise called XSS) is a web security weakness that permits an attacker to bargain the communications that clients have using a weak application. Cross-site scripting weaknesses typically indulge an attacker to take on the appearance of a casualty client, to do any activities that the client can perform, and to get to any of the client's information. On the off chance that the casualty client has special access inside the application, the attacker may have the option to oversee the entirety of the application's usefulness and information. Sometimes the attackers do not have a specific objective. They infuse malicious contents into the website and transform it into a source of delivery. XSS can also be used to send user cookies to attackers.

Counter measures taken: There are few changes in the coding pattern done to put the coding framework in a more secure way.

- Removed untrusted data from scripts, div and especially in CSS and Tag
- Encoding some untrusted data
- URL encoding
- Prevented some DOM XSS
- Secured the content especially in Private network

3.4.2 Brute force attack

Severity: Low

Issue: A brute force attack to simply put, is a hit and trial method. It could be compared to trying each key from a bunch of keys, and at the end finding the correct one. A few attackers use applications and contents as brute force apparatuses. These apparatuses evaluate everything from password blends to sidestep verification forms. In different cases, attackers attempt to get to web applications via session identity. Bots perform practically all brute force attacks today. Bots methodically attack sites and attempt the arrangements of credentials, and inform the attacker when they obtain

entrance. There is less possibility that password may be compromised, even if so, it has a multifactor authentication to counteract. However, this should be addressed.

Counter measures taken: Some of the counter measures taken are

- Introducing of strong CAPTCHA in the authentication field
- Strong password mandatory
- Success header to fool automated brute force attacks

3.4.3 Secure flag in SSL

Severity: Medium

The secure flag is a significant part, which ought to be set. In the event that it is not set, the attacker could intercept the client data while the information is sent on clear text and act as a potential threat. The cookie when the secure flag is turned on, at that point it will deny accommodation on non-SSL request.

Counter measures taken:

- Secure flag set to true

3.4.4 Beast attack

Severity: Medium

The SSL protocol may introduce man-in-the-middle attack to gather http headers with which it can decrypt the SSL traffic and can visualize the sensitive information.

- App services are used in the client side
- TLS 1.2 has been introduced 1.2 as mandatory

3.4.5 Host header poisoning

Severity: Low

Browsers send a host header to educate about the URL customer needs to visit. Hackers can fiddle with the host header to control how the application functions. Hackers make a solicitation with an altered Host Header. Web server gets this Host

Header. In the event that the application is utilizing this Host Header in a connection, the vindictive site will be shown. This sort of assault can influence password reset.

Counter measures taken:

- Used Server name instead of host header
- Hostnames are whitelisted

3.4.6 Strict transport security

Severity: Low

The application neglects to keep clients from interfacing with it over unencrypted associations. A hacker ready to alter a genuine client's system traffic could sidestep the application's utilization of SSL/TLS encryption, and utilize the application as a stage for attack against its clients. If a focused client connects to the site from using HTTP, their browser never endeavors to utilize an encrypted association.

Counter measures taken:

- HSTS (Http strict transport security) enabled
- “includesubdomains” flag is set
- “preload” flag is set

3.4.7 Server headers

Severity: Low

A vulnerability, where an attacker gets the information of the server by response from the server.

Counter measures taken:

- Server token set to “off”

3.4.8 Vulnerable ports

Severity: Low

Open port alludes to a TCP or UDP port number that is arranged to acknowledge network packets. Open ports become hazardous when genuine services are abused through security weaknesses and are acquainted with a framework by means of

malware, hackers can utilize the vulnerability to increase unapproved admittance to important information.

Counter measures taken:

- All ports are blocked except the required ones
- Port scanning prevention rule is activated in Android, Windows and Linux systems

3.4.9 Orphaned blocks

Severity: Low

Orphaned block is supposed to be a block whose parent block hash field focuses on an unauthentic block that is separated from the chain. These irregularities can be presented by a hacker. Another way an orphaned block is made is the point at which a hacker endeavors to change certain old transactions in blockchain.

Counter measures taken:

- As it is no public blockchain, the creation time is permissioned
- Introduction of multifactor authentication increased the block creation time

3.4.10 Majority attacks

Severity: Medium

A majority of attack, or 51%, occur when a hacker infiltrates a system and gains control of the Blockchain network by obtaining the majority of the absolute calculation intensity of mining. Blocks will very certainly be added to the chain in this situation, since the available processing power allows for finding new blocks faster than other members of the blockchain network. Transactions are irreversible, and just a single of two indistinguishable ones can be substantial. Hence, there is a hypothetical probability of such an attack.

Counter measures taken:

- Permission by design with no mining and proof of work
- Multi authentication during block creation

- Cryptographically encrypted block

3.4.11 DDoS attacks

Severity: Medium

Here in DDOS assault, an attacker may make Sybil identities to access the blockchain and make a surge of transactions. This will trigger a slowdown in service and inevitably, service will stop working. By presenting an enormous number of transactions of little value over a brief period, the system will be clogged by making blocks containing those transactions, and service to real clients in the system will be denied.

Counter measures taken:

- Identities creation are purely permissioned
- Creation of block is permissioned with multi-factor authentication
- Increased the size of the block to accommodate more transactions

3.4.12 Blockchain ingestion

Severity: Low

Blockchain ledger, each user has access to transaction data added to the ledger. However, analyzing an open transaction ledger can provide useful information to an attacker. This process is known for processing the data of the Blockchain ledger or Blockchain ingestion, and this process can have negative consequences for the Blockchain system or its users**.**

Counter measures taken:

- All data in chain are encrypted and data is not visible

3.4.13 SQL injection attack

Severity: High

SQL (Structured Query Language) injection attack is a security weakness that permits a hacker to meddle with the questions that an application interface requests to its database store. A SQL injection attack comprises editable SQL instructions by means

of the input information from the customer to the application. These are a kind of injection attack, in which SQL instructions (Insert/Update/Delete) are infused to request to affect the execution of orchestrated SQL commands. Thus, a hacker can adjust or delete this information, making industrious changes to the application's substance or conduct.

Counter measures taken:

- Use of parameterized queries or prepared statements used in traditional database
- Created and used stored procedures wherever possible
- Updating and patching of SQL

CHAPTER 4

FRAMEWORK IMPLEMENTATION AND EVALUATION

This chapter shows how the implementation in various industries has been carried out. The participants evaluated the HBSTS system and questionnaires used in the HBSTS implementation are defined. This chapter ends with the result and analysis of the implementation.

4.1 OVERVIEW

A developed framework when used and surveyed can have a better and correct conclusive result. Similarly, the HBSTS framework is implemented and evaluated in various organizations so that the evaluation has a distinct result. The result will help us in understanding the merits and demerits of the framework. This will help in developing a better product out of the developed framework.

4.2 IMPLEMENTATION OF FRAMEWORK

HBSTS framework has been evaluated in ten organizations with ten different industries. Seven types of different departmental data have been used as input in the framework along with heavy multimedia files. The industries, which has been approached to test the framework, are:

- Business process outsourcing
- Manufacturing
- Packaging
- Software development
- Consulting
- Construction
- IT Services
- Healthcare
- ISP (Internet Service Providers)
- Education

The transactional data is divided into few categories namely

Financial transactions: The financial transactions are simply journal entries along with transactional entries like closing entries, credit notes, debit notes and adjustment entries.

Sales call transactions: Sales call entries are lead generation calls from prospective customer data. The customers had been called and the response of the customers were recorded and entered in HBSTS so that this data could not be changed or tampered with.

Support call transactions: Support calls were calls done by support call executives for various support purposes. The important support data of customers, including feedback of customers, is entered in the HBSTS. Both the conversation of executives and customers are appended to the framework in such a manner that there is no change in mutually agreed discussion.

Product data: Product data is entered in HBSTS. It consists of crucial data about the product including the product life cycle, which requires confidentiality.

Medical transaction: Medical records are of utmost importance since they have health records and cycle of patients. These records are entered in HBSTS for secured preservation and accessibility.

Service call transactions: Service call entries, which are telephonic conversations and data related to service, are entered in HBSTS.

Evaluation transactions: Evaluation entries are added in HBSTS. They comprise data related to educational result evaluation in order to ensure that the marks are stored and cannot be tampered with.

Table 4.1 HBSTS evaluation industry wise

Industries	Type of transactions
Business process outsourcing	Sales call transactions
Manufacturing	Product Data transactions
Packaging	Support call transactions
Software development	Financial transactions
Consulting	Sales call transactions
Construction	Financial transactions
IT Services	Service call transactions
Healthcare	Medical transactions
ISP	Support call transactions
Education	Evaluation transactions

Table 4.1 shows the categories of industries where HBSTS is evaluated.

The share of transactions based on industries where the drive to implement the framework is graphically depicted.

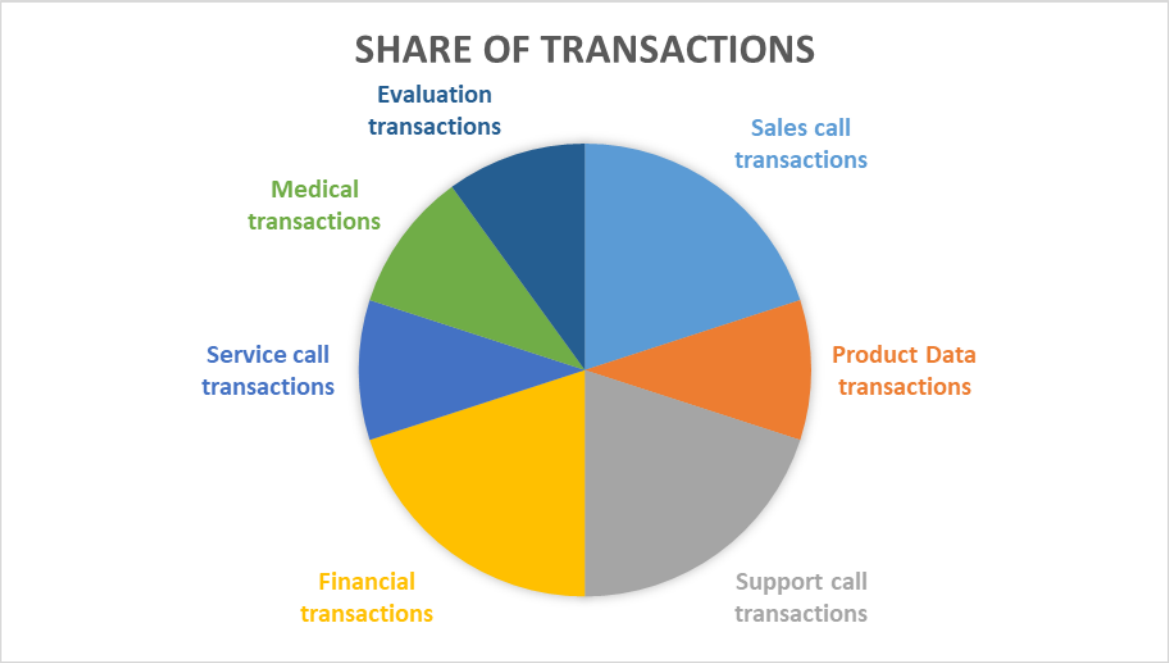

Figure 4.1 HBSTS transaction share during evaluation

Figure 4.1 provides a graphical representation of HBSTS transaction share, which are evaluated.

The implementation of HBSTS in various organizations has spanned over a period of six months where HBSTS has been tested with various transactional data. Every transaction added is tested from various systems and devices. The table below shows the period based on industries to complete the implementation and testing.

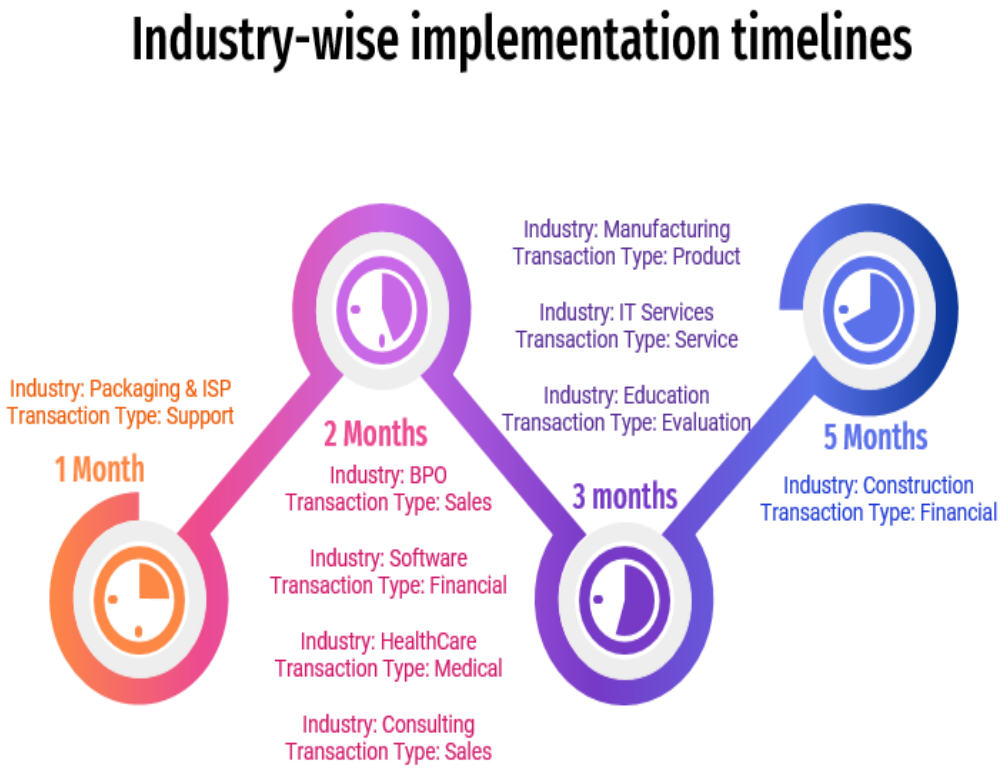

Figure 4.2. HBSTS industry wise implementation

Figure 4.2 explains the timeframe of evaluation of HBSTS in different industries. The framework has been installed and evaluated on range of industries with different categorical sensitive data. The first month of implementation of the framework started with packaging and the Internet service industry. In order to keep the customer and the organization correspondent on the same page, support call transactions are extremely important, and customer feedback is highly important, which should not be changed. The support call data along with the contract copies is entered in the framework. Call data is feeded in the blockchain where contract copies, usually heavy files, are entered in the traditional database with reference to the blockchain data. Similarly, support call data of internet service providers, which again consists of a chain of correspondence and progress tracker. This data is very sensitive and requires

no modification after the support calls end with the customer. The evaluation in these two organizations took one month. It took two months to implement and evaluate HBSTS in BPO (Business process outsourcing), software, healthcare and consulting industries. The type of transactions entered in the BPO and consulting industry are sales transactions. This is confidential data, which only pertains to certain groups of conservative employees. This data comprises of client and cost information of the business process earned by the organization.

The data from the copy of the sales contract and sales invoice along with the essential details is entered into HBSTS. Likewise, all financial transactions pertaining to the software industry have been evaluated. The financial transactions consisting of closing entries, credit and debit notes and adjustment entries were entered in HBSTS. Medical records are excessively sensitive in the healthcare industry and are prone to change or being hacked. These are medical records of the patient and details of the prescribed medicines. These also include various tests conducted for the intended patients and copies of the health checks, which were stored in the HBSTS.

The tenure for implementing and evaluating in the manufacturing, service and education industry took three months. The product information of the manufacturing unit is classified information since it contains all the ingredients of the product and its composition. There is no room for leakage or tampering with the information. These crucial product transaction details are entered in the HBSTS. In a similar fashion, service transactions consisting of service related data like service calls, service correspondence with customer, solution given to customer, engineer visit, charges applied, resolution state including cost incurred, and feedback of the customer is recorded. If this information is hacked or tampered with, then it could cause great destruction to the image of the organization. In terms of security, confidentiality, and accessibility, evaluating student data is a big complication.

The information should be easily accessible while also being secure and only available to the intended student. This evaluation transaction data was entered in the HBSTS. The construction sector data is said to be most disorganized. The financial data consists of payment to various construction vendors, and for land purchase, defaulter and fines, registry transaction and raw material procurement. This selection

of financial data and transactions is entered in HBSTS because of the sensitive nature of the information, which cannot fall under wrong hands.

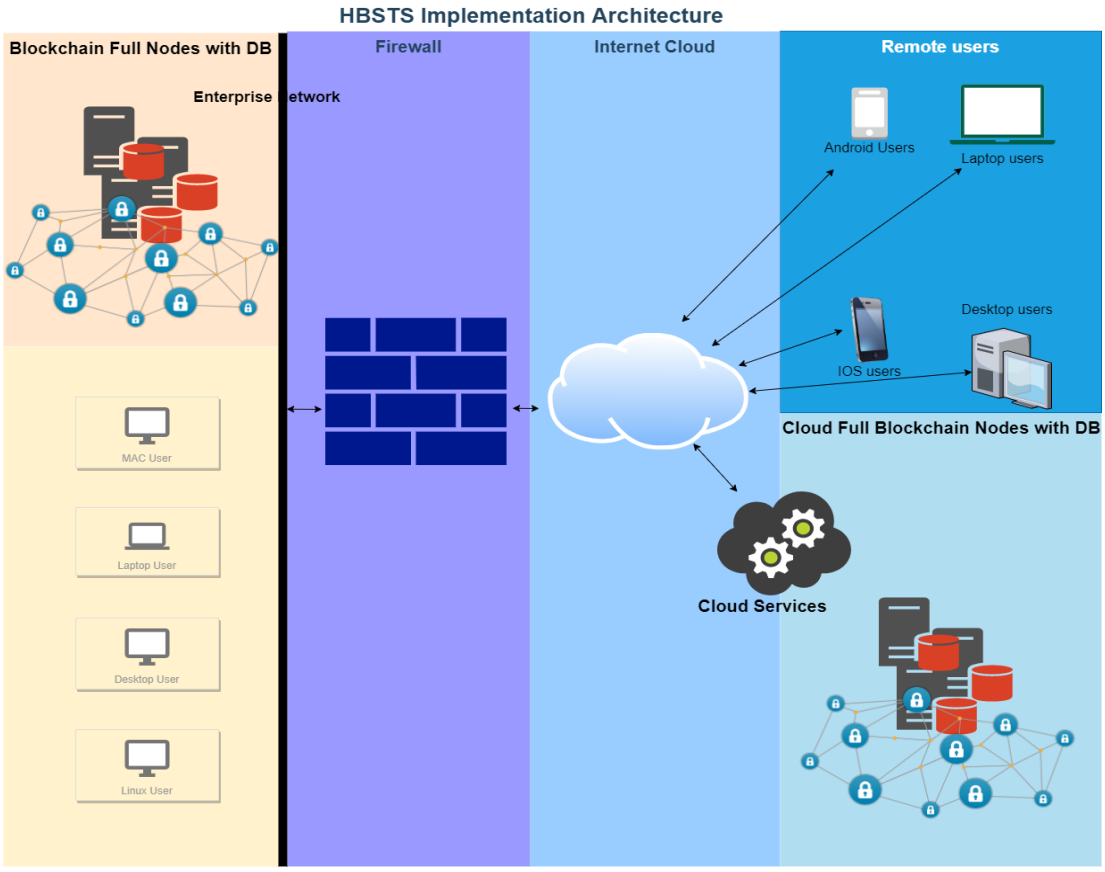

Figure 4.3 HBSTS implementation architecture

Figure 4.3 provides a graphical representation of HBSTS technological infrastructure implementation. HBSTS implementation is hybrid in nature which means not only does the architecture supports private and public cloud but the transactions are also stored in blockchain and traditional databases. HBSTS is an amalgamation of public and private cloud. Full blockchain nodes that are installed in enterprise networks and public cloud service holds the full copy of the blockchain.

The light nodes are user centric and interact with the full blockchain nodes for consensus and transaction validation. The enterprise network is connected with a firewall and internet cloud. The firewall will hold the enterprise security, nonetheless HBSTS provides seamless security to transaction data and presence of firewall hardly matters. Since this architecture is designed for implementation in enterprise, it is assumed that the presence of a firewall is inevitable. Blockchain full nodes are

installed in enterprise networks along with traditional databases like MySQL or PostgreSQL. This group of nodes holds the full copy of blockchain. Similar configuration is configured at cloud services like AWS (Amazon web service), Azure and Google cloud. Both blockchain full nodes, the one for the cloud and the one for the enterprise, are in accord with each other. The traditional database configured in both cloud and enterprise full nodes are too in accord, hence any changes in the database are replicated within. The light nodes are used from laptops, desktops and Mac machines.

Handheld devices-(Android and iOS) use very light nodes and can see only the transactions, which are applicable for a particular user. These nodes are very light; can only view the related blockchain data and do not contain any heavy media files to balance the performance. The heavy media files reside on the traditional database, hence laptops, desktops and Mac users who are using the light nodes can view the related transaction data as well as the related heavy files. The transaction can be entered in any node; the consensus and validation is done through the full blockchain nodes.

4.3 PARTICIPANTS IN THE STUDY

There were 100 participants in the study spanning across 10 different industries.

Table 4.2 Participants industry wise

Industries	Number of Participants
Business process outsourcing	10
Manufacturing	10
Packaging	10
Software development	10
Consulting	10
Construction	10
IT Services	10
Healthcare	10
ISP	10
Education	10

Table 4.2 represents the participants industry wise. For implementation of HBSTS, there were various executives and managers from different departments for transactions and evaluated the system against the traditional model approach which is being used presently.

Table 4.3 Participants roles - BPO

Industry: BPO (Business Process Outsourcing)		
Participants type	**No.**	**Role**
Sales executives	5	- Sales data transaction to HBSTS
Sales Manager	1	-Ensure correct sales transaction entered in HBSTS - Manage team of sales executive - Single point of contact for sales transactions in HBSTS
IT Executives	2	Implementation of HBSTS in the organization
IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals
IT Security Expert	1	- Testing security features of HBSTS in context for the concerned organization

Table 4.3 represents the roles and type of participants from BPO industry.

Table 4.4 Participants roles - Manufacturing

Industry: Manufacturing		
Participants type	**No.**	**Role**
Product executives	5	- Product data transaction to HBSTS
Product Manager	1	-Ensure correct product transaction entered in HBSTS - Manage team of product executives - Single point of contact for sales transactions in HBSTS
IT Executives	3	- Implementation of HBSTS in the organization

IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals - Testing security features of HBSTS in context for the concerned organization

Table 4.4 represents the roles and type of participants from manufacturing industry.

Table 4.5 Participants roles - Packaging

Industry: Packaging		
Participants type	**No.**	**Role**
Support executives	5	- Support data transaction to HBSTS
Team Lead	1	-Ensure correct support transaction entered in HBSTS - Manage team of support executives
Support Manager	1	- Single point of contact for support transactions in HBSTS - Overall Responsible for support data transaction in HBSTS
IT Executives	2	Implementation of HBSTS in the organization
IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals - Testing security features of HBSTS in context for the concerned organization

Table 4.5 represents the roles and type of participants from packaging industry.

Table 4.6 Participants roles - Software development

Industry: Software Development		
Participants type	**No.**	**Role**
Finance executives	3	- Finance data transaction to HBSTS

Finance Manager	1	-Ensure correct financial transaction entered in HBSTS - Single point of contact for all financial transactions in HBSTS - Overall Responsible for financial data transaction in HBSTS - Manage team of finance executives
IT Executives	3	- Implementation of HBSTS in the organization
IT Manager	2	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals
IT Security Expert	1	- Testing security features of HBSTS in context for the concerned organization

Table 4.6 represents the roles and type of participants from software industry.

Table 4.7 Participants roles - Consulting

Industry: Consulting		
Participants type	**No.**	**Role**
Sales executive	5	- Sales data transaction to HBSTS
Sales Manager	1	-Ensure correct sales transaction entered in HBSTS - Manage team of sales executive - Single point of contact for sales transactions in HBSTS
IT Executives	3	- Implementation of HBSTS in the organization
IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals - Testing security features of HBSTS in context for the concerned organization

Table 4.7 represents the roles and type of participants from consulting industry.

Table 4.8 Participants roles - Construction

Industry: Construction		
Participants type	**No.**	**Role**
Finance executives	5	- Finance data transaction to HBSTS
Finance Manager	2	-Ensure correct financial transaction entered in HBSTS - Single point of contact for all financial transactions in HBSTS - Overall Responsible for financial data transaction in HBSTS - Manage team of finance executives
IT Executives	2	- Implementation of HBSTS in the organization
IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals - Testing security features of HBSTS in context for the concerned organization

Table 4.8 represents the roles and type of participants from construction industry.

Table 4.9 Participants roles - IT services

Industry: IT Services		
Participants type	**No.**	**Role**
Service executives	5	- Service data transaction to HBSTS
Service Manager	1	-Ensure correct service transaction entered in HBSTS - Single point of contact for service transactions in HBSTS - Overall Responsible for service data transaction in HBSTS - Manage team of service executives
IT Executives	3	- Implementation of HBSTS in the organization

IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals - Testing security features of HBSTS in context for the concerned organization

Table 4.9 represents the roles and type of participants from IT service industry.

Table 4.10 Participants roles - HealthCare

Industry: HealthCare		
Participants type	**No.**	**Role**
Operation executives	4	- Medical data transaction to HBSTS
Operation Manager	1	-Ensure correct medical transaction entered in HBSTS - Single point of contact for medical transactions in HBSTS - Overall Responsible for medical data transaction in HBSTS - Manage team of operation executives
Doctor	1	- Ensure correctness of medical data
IT Executives	3	- Implementation of HBSTS in the organization
IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals - Testing security features of HBSTS in context for the concerned organization

Table 4.10 represents the roles and type of participants from health care industry.

Table 4.11 Participants roles - ISP

Industry: ISP (Internet Service Provider)		
Participants type	**No.**	**Role**
Support executives	3	- Support data transaction to HBSTS
Operation Manager	1	-Ensure correct support transaction entered in HBSTS - Manage team of support executives
Support Manager	1	- Single point of contact for support transactions in HBSTS - Overall Responsible for support data transaction in HBSTS
IT Executives	3	- Implementation of HBSTS in the organization
IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals
IT Security Expert	1	- Testing security features of HBSTS in context for the concerned organization

Table 4.11 represents the roles and type of participants from Internet Service Provider (ISP) industry.

Table 4.12 Participants roles - Education

Industry: Education		
Participants type	**No.**	**Role**
Teachers	6	- Evaluation data transaction to HBSTS
Operation and administration Manager	1	-Ensure correct evaluation transaction entered in HBSTS - Single point of contact for evaluation transactions in HBSTS - Overall Responsible for evaluation data transaction in HBSTS
IT Executives	2	- Implementation of HBSTS in the organization

IT Manager	1	- Overall orchestration of HBSTS in the Organization - Responsible for communication with concerned departments for implementation - Ensure testing with original data - Internal approvals - Testing security features of HBSTS in context for the concerned organization

Table 4.12 represents the roles and type of participants from education industry.

4.5 RESULT AND ANALYSIS

The experiment result of the implementation and evaluation of HBSTS has proved that it is more secure than the traditional system and has been able to address the problem statements mentioned in this research. There were a hundred participants for this real time experiment spread across ten industries. The experiment has solved the following problem statements.

- **Data tampering,** which involves editing and modification of data.
- **Data security,** which involves overall security of data like hacking, virus, ransomwares and data exportation
- **Data transparency,** which involves honest view of all important data
- **Fault tolerance**, which holds continuity of data even after various types of system and network failure.
- **Cost effective,** which can be implemented without any license cost.
- **Interoperability,** which can support various operating systems and architecture
- **Cohesive platform,** which can balance with traditional database and blockchain

During the experiment, the transactions entered in HBSTS and traditional systems are compared with respect to various quantitative and qualitative parameters. These parameters are tested with the business process team as well as the internal IT team.

The comparable parameters from the problem statements in this research are as follows:

Security features: The security characteristics of transaction data fed into the HBSTS have been tested, and the results have been compared to the current conventional method. The result took precedence over the existing traditional system. 51% of participants felt that the security features of HBSTS is good. 39% of participants felt that it is excellent and 10% of the participants felt it is fair when compared to the security features of the existing system as shown in Figure 4.4

Figure 4.4 HBSTS security features

While 94% felt that, the security features of traditional approaches are poor and only 6% of the participants felt the security features of traditional systems are fair as shown in Figure 4.5

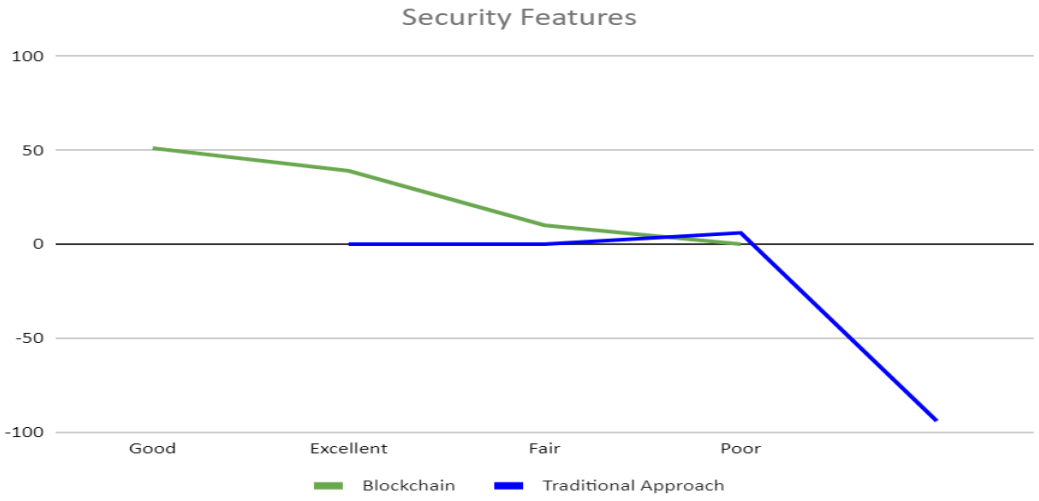

Figure 4.5 HBSTS vs Traditional approach in security features

Cost benefit features: The cost benefit features outlines the implementation and maintenance of the HBSTS in the organization. The benefits include savings in the software license cost and no maintenance cost especially manpower. This also throws light on the availability of the chain data with no extra cost. The cost benefit features in the HBSTS has been experimented and at the end of the experiment, it is compared with the existing traditional approach. The result took precedence over the existing traditional system. 89% of participants agreed on the cost benefit features of HBSTS and 11% of the participants felt probable compared with the cost benefit features of the existing system as shown in Figure 4.6

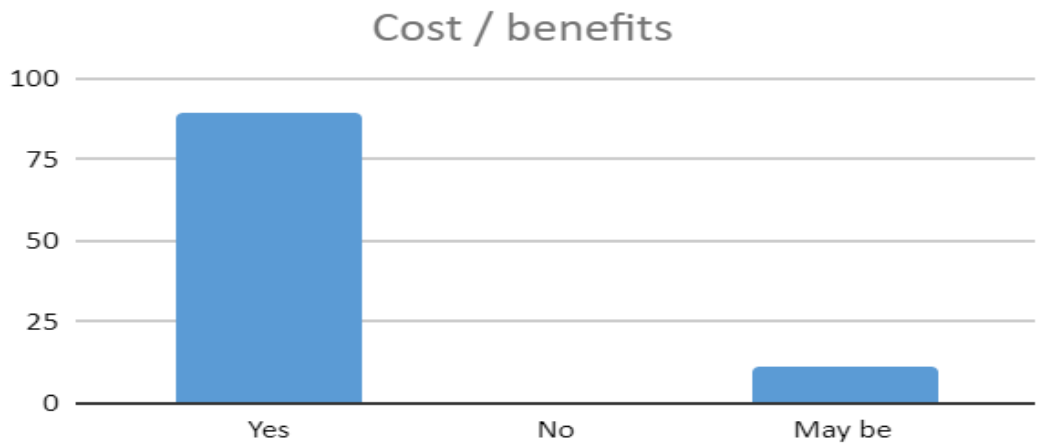

Figure 4.6 HBSTS Cost / Benefit

Only 1% agreed that the traditional approach has cost benefit features, 90% did not agree and 9% of the participants felt probable as shown in Figure 4.7

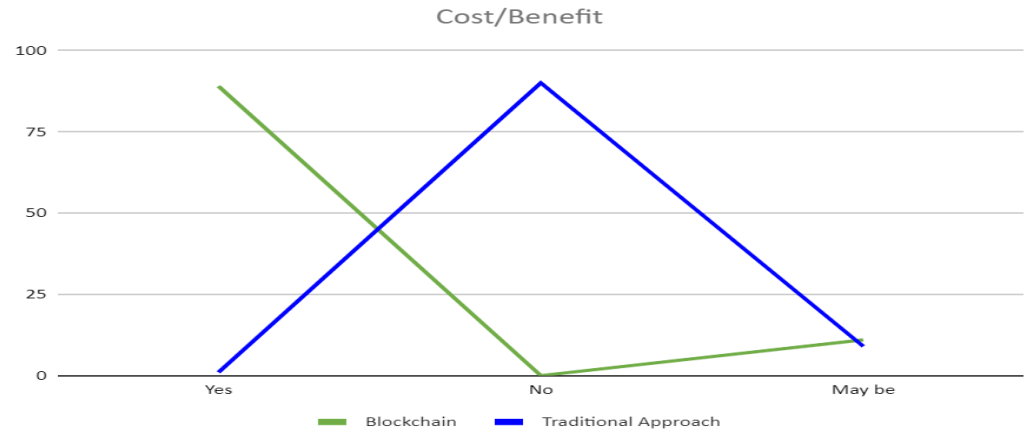

Figure 4.7 HBSTS vs Traditional approach in Cost/Benefit

Execution time: The execution time features specify the time taken to feed transactions in HBSTS, have been compared with existing traditional approach. The result states that there are no major differences between HBSTS and the traditional system in execution time. 89% of participants have marked good while 11% have marked fair for transaction execution time in HBSTS as shown in Figure 4.8

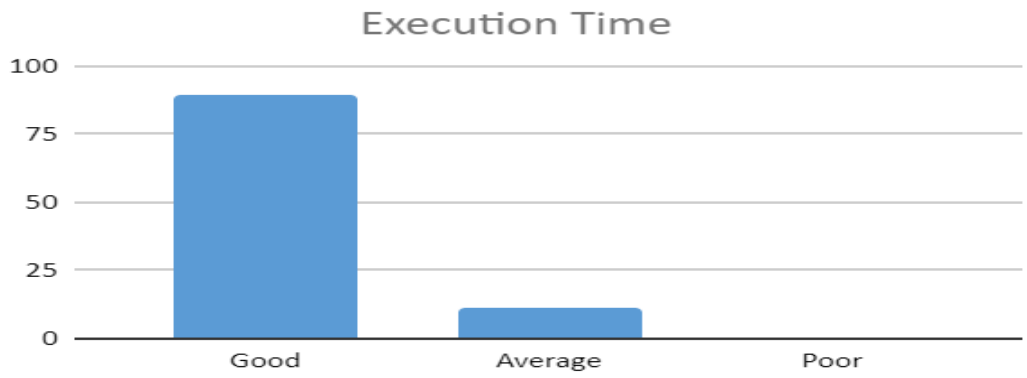

Figure 4.8 HBSTS execution time

96% of the participants marked good and 4% of the participants marked average in execution time of the existing traditional system approach as shown in Figure 4.9

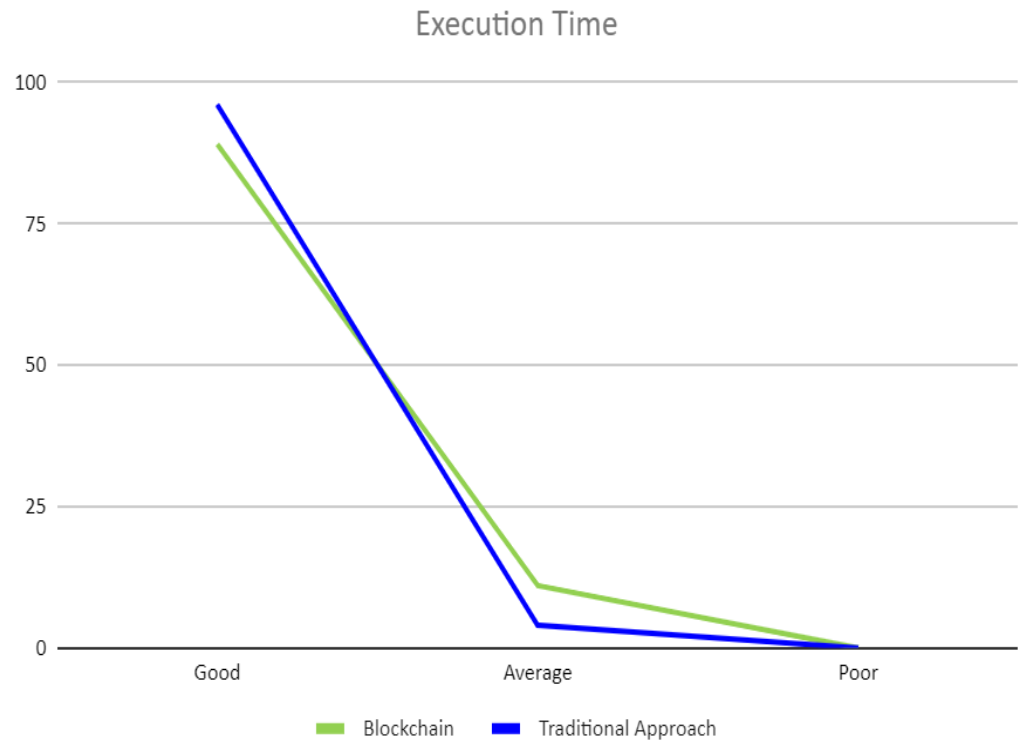

Figure 4.9 HBSTS vs Traditional approach in execution time

Foresee benefit: The Forsee benefit features defines the overall benefits of using HBSTS in the organization as compared to the existing traditional system. The result states that using HBSTS advantages over the existing system. 89% of participants have agreed on foreseeing benefits and only 2% of the participants do not foresee benefits while 9% are uncertain as shown in Figure 4.10

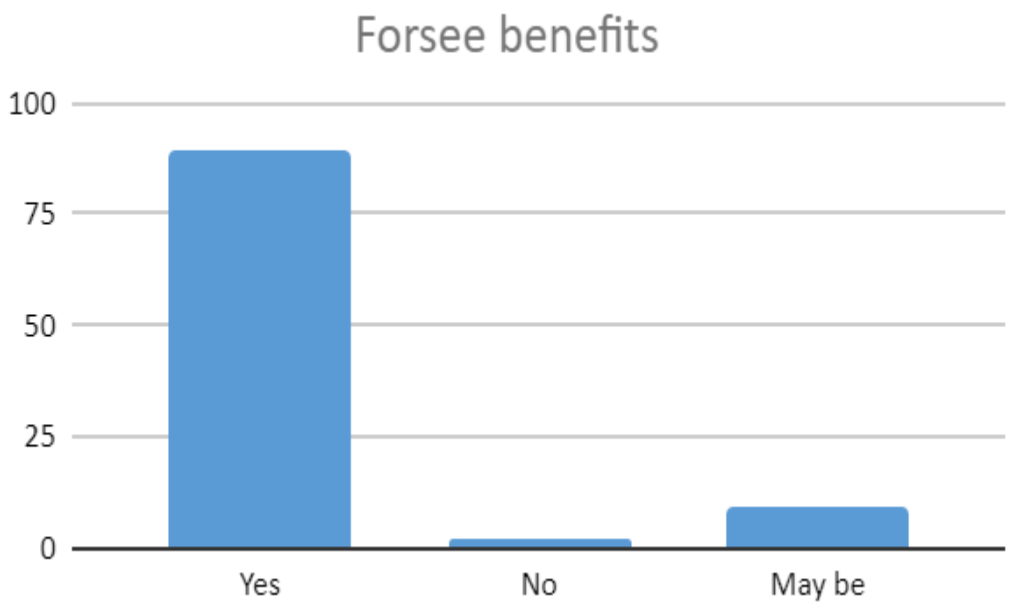

Figure 4.10 HBSTS Foresee benefit

91% of the participants don't foresee benefits of the existing system while only 2% agree to foresee benefits. 7% of the participants are uncertain to foresee benefits of the existing system as shown in Figure 4.11

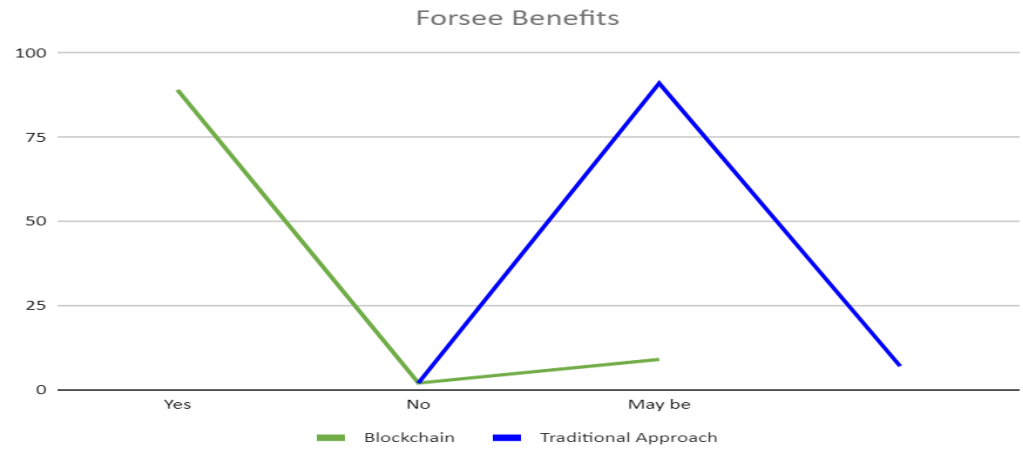

Figure 4.11 HBSTS vs Traditional approach in Foresee benefit

Transparency: The transparency features state clarity in transactions, which are immutable, unbiased, unalterable, and readable to concerned entities as compared to the existing traditional system. The result states that HBSTS has precedence over the existing approach. 100% of participants have agreed on transparency with the HBSTS transactions as shown in Figure 4.12

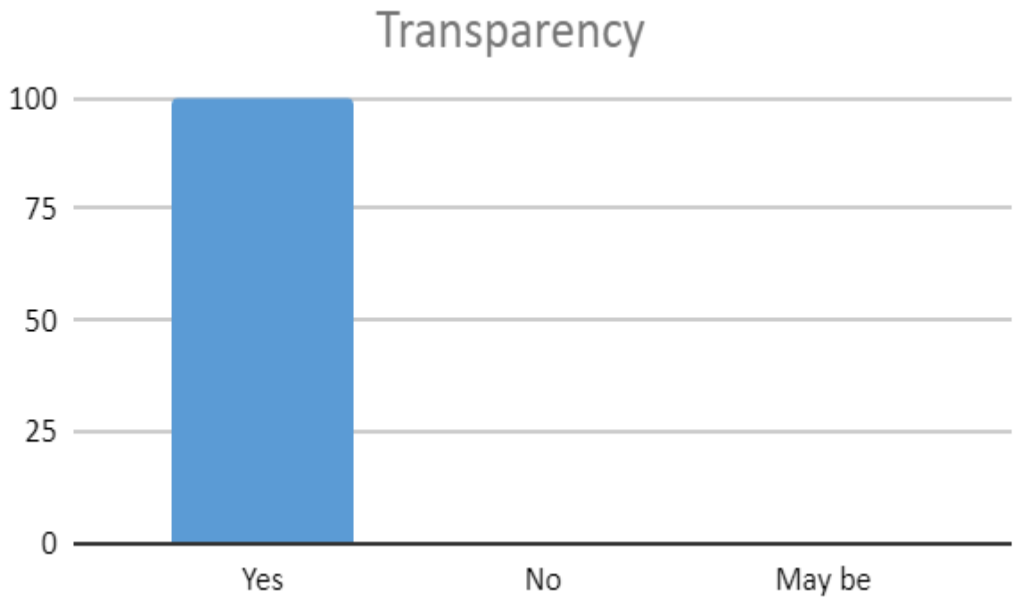

Figure 4.12 HBSTS Transparency

98% of the participants agree that there is no transparency in the existing traditional system while 2% of the participants are uncertain as shown in Figure 4.13

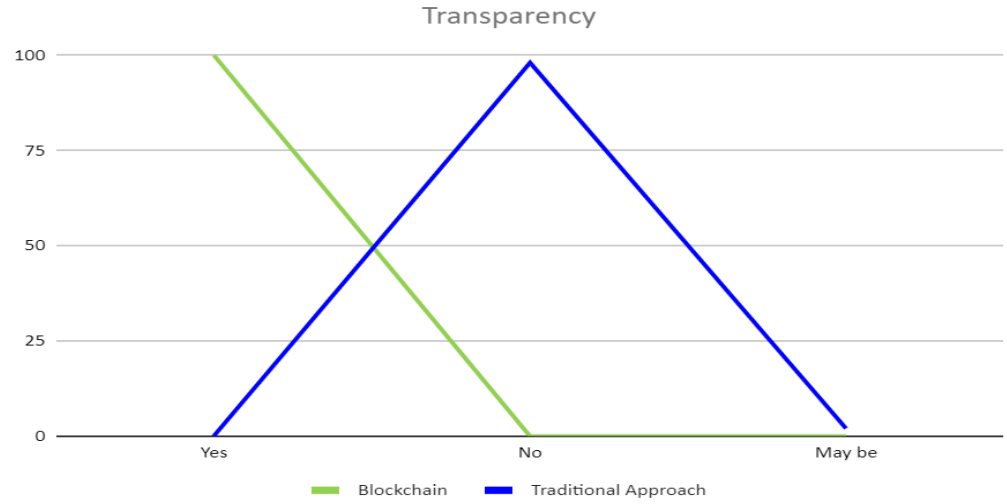

Figure 4.13 HBSTS vs Traditional approach in Transparency

Manageability: The manageability features state the governance and maintenance of HBSTS compared to the existing traditional system. The result states that HBSTS has precedence over the existing approach. 89% of participants have agreed on better manageability and marked as "Good" and 11% of participants have marked as "average" with HBSTS as shown in Figure 4.14

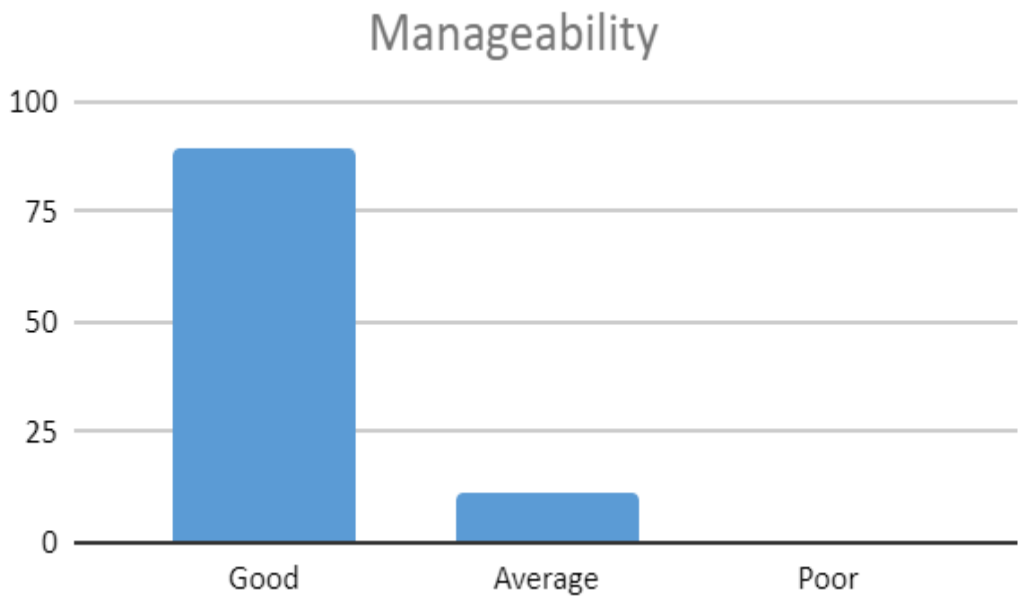

Figure 4.14 HBSTS Manageability

Only 3% of the participants felt that the existing traditional system has better manageability and 94% marked the existing system as "average" while 3% of the participants marked "poor" as compared to HBSTS shown in Figure 4.15

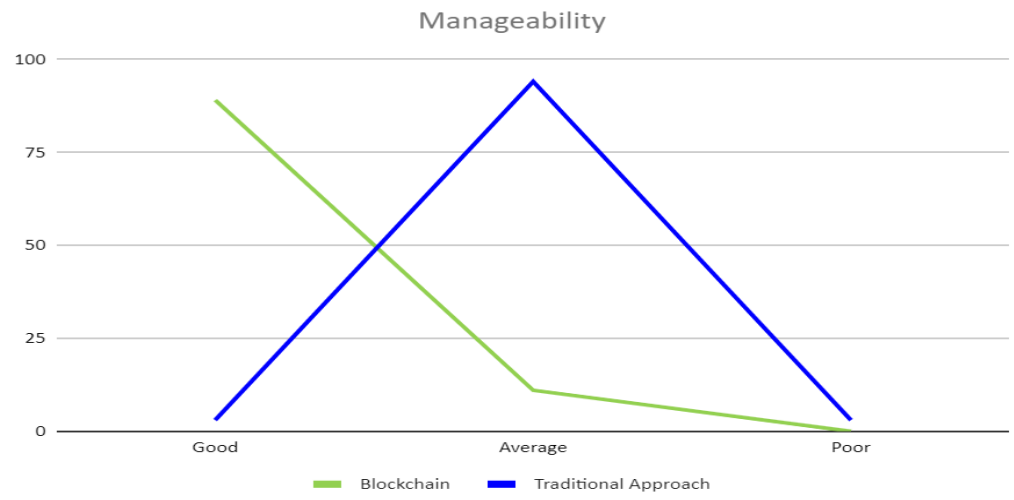

Figure 4.15 HBSTS vs Traditional approach in Manageability

Consider permanent: This features states that to consider a particular system to be acceptable and used for transactions. The experiment and evaluation states that HBSTS has been widely accepted for usage as compared to the existing traditional system. The result had taken precedence over the existing approach. 89% of participants have agreed to consider HBSTS for permanent usage while only 11% are uncertain as shown in Figure 4.16

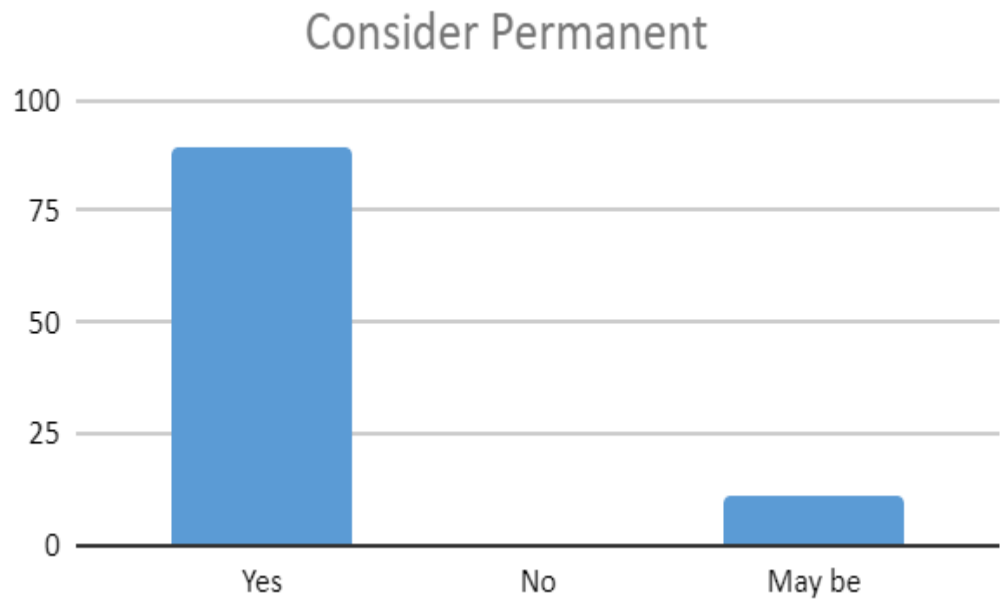

Figure 4.16 HBSTS Consider permanent

The overall experiment and evaluation has taken an exponential precedence over the existing traditional approach on various problem statement parameters. Majority of the participants are ready to welcome the changes to the existing traditional system with the HBSTS.

CHAPTER 5

STATISTICAL ANALYSIS OF HYBRID BLOCKCHAIN SECURED TRANSACTION SYSTEM (HBSTS) FRAMEWORK

This chapter provides a clear understanding of the statistical analysis being carried out on the result of the implementation. The sample size used and various measurable parameters are defined here to achieve the quantitative and qualitative result. The comparison data here is being statistically evaluated to see where the objective of the research has solved the problem statement.

5.1 OVERVIEW

The experiment and implementation of HBSTS in the organization has proved that HBSTS has precedence over the existing traditional approach model based on various parameters evaluated. There is a vast difference between the two technologies when security, acceptance, availability, manageability and cost effectiveness is concerned. The problem statements of the research have been solved with the experimentation and implementation of HBSTS. However, in order to prove the result statistically, Anova analysis is performed over the evaluated data.

5.2 SAMPLE SIZE

A sample, in study terminology, is a collection of individuals, artefacts, or items selected for measurement from a larger population. To ensure that the results from the study sample can be applied to the whole population, the sample should be representative of the population. This experimentation and evaluation has a sample size of 100 professionals from different fields. There are 10 organizations and from each organization, there are 10 professionals selected for evaluating post implementation of HBSTS.

5.3 STATISTICAL ANALYSIS USING ANOVA

The evaluation and implementation of HBSTS is further analyzed statistically for a proven conclusion on the data being evaluated. Anova analysis is conducted on the data with the purpose of collating the population means of various groups. One way ANOVA (Analysis of variance) is one of the most significant analyses in the world of statistics where populations of different groups are tested. One-way anova has a single independent variable where in our case it is, where the features of HBSTS and traditional approach is compared. Anova like any other statistical tool uses null hypothesis and alternative hypothesis. Null hypothesis states that there are no significant changes in means between the two groups or all populations are uniform. Alternative hypothesis states that there is a significant change in means between the two groups or population means are not uniform. If the null hypothesis is rejected or the anova result is significant, it shows a meaningful quantitative approach to the decision on evaluation or implemented data.

5.3.1 Security Features

Sample size total is denoted as N = 200

Calculation for Total degrees of freedom (df_{total}):

$$df_{total} = 200 - 1 = 199$$

Also, the between-groups degrees of freedom are $df_{between} = 2 - 1 = 1$ and the within-groups degrees of freedom are:

$$df_{within} = df_{total} - df_{between} = 199 - 1 = 198$$

Calculation to compute the total sum of values and the grand mean.

$$\sum_{i,j} X_{ij} = 329 + 106 = 435$$

Then, the value of square will be

$$\sum_{i,j} X_{ij}^2 = 1123 + 118 = 1241$$

The SS_{total} value is:

$$SS_{total} = \sum_{i,j} X_{ij}^2 - \frac{1}{N}\left(\sum_{i,j} X_{ij}\right)^2 = 1241 - \frac{435^2}{200} = 294.875$$

The SS_{within} value is:

$$SS_{within} = \sum SS_{withingroups} = 40.59 + 5.64 = 46.23$$

MS, which is mean sum of square, are calculated below:

$$MS_{between} = \frac{SS_{between}}{df_{between}} = \frac{248.645}{1} = 248.645$$

$$MS_{within} = \frac{SS_{within}}{df_{within}} = \frac{46.23}{198} = 0.233$$

F-statistic is calculated as follows:

$$F = \frac{MS_{between}}{MS_{within}} = \frac{248.645}{0.233} = 1064.93$$

Calculations of null and alternative hypotheses

Ho: $\mu_1 = \mu_2$

Ha: Alternative hypothesis states that all means are not equal

Hypothesis testing is based on the ANOVA analysis utilizing F ratio

Rejection region

Significance level is denoted as “α” and is α=0.05

Degrees of freedom is denoted as $df_1 = 1$ and $df_2 = 1$

Rejection region is calculated as $R = \{F : F > F_c = 3.889\}$ for F test

Statistics of the Test

$$F = \frac{MS_{between}}{MS_{within}} = \frac{248.645}{0.233} = 1064.93$$

Result of the null hypothesis

The calculation shows that *F*=1064.93>*Fc*=3.889, which shows that *null hypothesis is rejected with F value approach.* The calculation of p-value is *p*=0<0.05, which shows that *null hypothesis is rejected with P value approach*.

Conclusion:

The statistical result and conclusion states that null hypothesis Ho is rejected which provides enough proof to claim that means of two population are not equal having α=0.05 significance level

5.3.2 Cost Benefit analysis

Sample size total is denoted as N = 200

Calculation for Total degrees of freedom (df_{total}):

$$df_{total} = 200 - 1 = 199$$

Also, the between-groups degrees of freedom are $df_{between} = 2 - 1 = 1$ and the within-groups degrees of freedom are:

$$df_{within} = df_{total} - df_{between} = 199 - 1 = 198$$

Calculation to compute the total sum of values and the grand mean.

The following is obtained

$$\sum_{i,j} X_{ij} = 189 + 11 = 200$$

Then, the value of square will be

$$\sum_{i,j} X_{ij}^2 = 367 + 13 = 380$$

The SS_{total} value is:

$$SS_{total} = \sum_{i,j} X_{ij}^2 - \frac{1}{N}\left(\sum_{i,j} X_{ij}\right)^2 = 380 - \frac{200^2}{200} = 180$$

The SS_{within} value is:

$$SS_{within} = \sum SS_{withingroups} = 9.79 + 11.79 = 21.58$$

MS, which is mean sum of square, are calculated below:

$$MS_{between} = \frac{SS_{between}}{df_{between}} = \frac{158.42}{1} = 158.42$$

$$MS_{within} = \frac{SS_{within}}{df_{within}} = \frac{21.58}{198} = 0.109$$

F-statistic is calculated as follows:

$$F = \frac{MS_{between}}{MS_{within}} = \frac{158.42}{0.109} = 1453.529$$

Calculations of null and alternative hypotheses

Ho: $\mu_1 = \mu_2$

Ha: Alternative hypothesis states that all means are not equal

Hypothesis testing is based on the ANOVA analysis utilizing F ratio

Rejection region

Significance level is denoted as "α" and is α=0.05

Degrees of freedom is denoted as $df_1 = 1 \text{ and } df_2 = 1$

Rejection region is calculated as $R = \{F : F > F_c = 3.889\}$

Statistics of the Test

$$F = \frac{MS_{between}}{MS_{within}} = \frac{158.42}{0.109} = 1453.529$$

Result of the null hypothesis

The calculation shows that F = 1453.529 > Fc = 3.889 which shows that *null hypothesis is rejected with F value approach.* The calculation of p-value is *p*=0<0.05, which shows that *null hypothesis is rejected with P value approach*.

Conclusion

The statistical result and conclusion states that null hypothesis Ho is rejected which provides enough proof to claim that means of two population are not equal having α=0.05 significance level

5.3.3 Execution time

Sample size total is denoted as N = 200

Calculation for Total degrees of freedom (df_{total}):

$$df_{total} = 200 - 1 = 199$$

Also, the between-groups degrees of freedom are $df_{between} = 2 - 1 = 1$ and the within-groups degrees of freedom are:

$$df_{within} = df_{total} - df_{between} = 199 - 1 = 198$$

Calculation to compute the total sum of values and the grand mean.

The following is obtained

$$\sum_{i,j} X_{ij} = 189 + 196 = 385$$

Then, the value of square will be

$$\sum_{i,j} X_{ij}^2 = 367 + 388 = 755$$

The SS_{total} value is:

$$SS_{total} = \sum_{i,j} X_{ij}^2 - \frac{1}{N}\left(\sum_{i,j} X_{ij}\right)^2 = 755 - \frac{385^2}{200} = 13.875$$

The SS_{within} value is:

$$SS_{within} = \sum SS_{withingroups} = 9.79 + 3.84 = 13.63$$

MS, which is mean sum of square, are calculated below:

$$MS_{between} = \frac{SS_{between}}{df_{between}} = \frac{0.245}{1} = 0.245$$

$$MS_{within} = \frac{SS_{within}}{df_{within}} = \frac{13.63}{198} = 0.069$$

F-statistic is calculated as follows:

$$F = \frac{MS_{between}}{MS_{within}} = \frac{0.245}{0.069} = 3.559$$

Calculations of null and alternative hypotheses

Ho: $\mu_1 = \mu_2$

Ha: Alternative hypothesis states that all means are not equal

Hypothesis testing is based on the ANOVA analysis utilizing F ratio

Rejection region

Significance level is denoted as "α" and is α=0.05

Degrees of freedom is denoted as $df_1 = 1$ and $df_2 = 1$

Rejection region is calculated as $R = \{F : F > F_c = 3.889\}$

Statistics of the Test

$$F = \frac{MS_{between}}{MS_{within}} = \frac{0.245}{0.069} = 3.559$$

Calculations of null and alternative hypotheses

The calculation shows that F=3.559≤Fc=3.889 which shows that *null hypothesis is not rejected with F value approach.* The calculation of p-value, p=0.0607 ≥ 0.05, which shows that *null hypothesis is not rejected with P value approach*.

Conclusion:

The statistical result and conclusion states that null hypothesis Ho is not rejected which provides enough proof to claim that means of two population are equal having α=0.05 significance level

5.3.4 Foresee benefits

Sample size total is denoted as N = 200

Calculation for Total degrees of freedom (df_{total}):

$$df_{total} = 200 - 1 = 199$$

Also, the between-groups degrees of freedom are $df_{between} = 2 - 1 = 1$

and the within-groups degrees of freedom are:

$$df_{within} = df_{total} - df_{between} = 199 - 1 = 198$$

Calculation to compute the total sum of values and the grand mean.

The following is obtained

$$\sum_{i,j} X_{ij} = 187 + 11 = 198$$

Then, the value of square will be

$$\sum_{i,j} X_{ij}^2 = 365 + 15 = 380$$

The SS_{total} value is:

$$SS_{total} = \sum_{i,j} X_{ij}^2 - \frac{1}{N}\left(\sum_{i,j} X_{ij}\right)^2 = 380 - \frac{198^2}{200} = 183.98$$

The SS_{within} value is:

$$SS_{within} = \sum SS_{withingroups} = 15.31 + 13.79 = 29.1$$

MS, which is mean sum of square, are calculated below:

$$MS_{between} = \frac{SS_{between}}{df_{between}} = \frac{154.88}{1} = 154.88$$

$$MS_{within} = \frac{SS_{within}}{df_{within}} = \frac{29.1}{198} = 0.147$$

F-statistic is calculated as follows:

$$F = \frac{MS_{between}}{MS_{within}} = \frac{154.88}{0.147} = 1053.823$$

Calculations of null and alternative hypotheses

Ho: $\mu_1 = \mu_2$

Ha: Alternative hypothesis states that all means are not equal

Hypothesis testing is based on the ANOVA analysis utilizing F ratio

Rejection region

Significance level is denoted as "α" and is α=0.05

Degrees of freedom is denoted as $df_1 = 1 \text{ and } df_2 = 1$

Rejection region is calculated as $R = \{F : F > F_c = 3.889\}$

Statistics of the Test

$$F = \frac{MS_{between}}{MS_{within}} = \frac{154.88}{0.147} = 1053.823$$

Decision about the null hypothesis

The calculation shows that *F*=1053.823>*Fc*=3.889, which shows that *null hypothesis is rejected with F value approach*. The calculation of p-value since *p*=0<0.05, which shows that *null hypothesis is rejected with P value approach*.

Conclusion

The statistical result and conclusion states that null hypothesis Ho is rejected which provides enough proof to claim that means of two population are not equal having α=0.05 significance level

5.3.5 Transparency

Sample size total is denoted as N = 200

Calculation for Total degrees of freedom (df_{total}):

$$df_{total} = 200 - 1 = 199$$

Also, the between-groups degrees of freedom are $df_{between} = 2 - 1 = 1$

and the within-groups degrees of freedom are:

$$df_{within} = df_{total} - df_{between} = 199 - 1 = 198$$

Calculation to compute the total sum of values and the grand mean.
The following is obtained

$$\sum_{i,j} X_{ij} = 189 + 100 = 289$$

Then, the value of square will be

$$\sum_{i,j} X_{ij}^2 = 400 + 2 = 402$$

The SS_{total} value is:

$$SS_{total} = \sum_{i,j} X_{ij}^2 - \frac{1}{N}\left(\sum_{i,j} X_{ij}\right)^2 = 402 - \frac{202^2}{200} = 197.98$$

The SS_{within} value is:

$$SS_{within} = \sum SS_{withingroups} = 0 + 1.96 = 1.96$$

MS, which is mean sum of square, are calculated

$$MS_{between} = \frac{SS_{between}}{df_{between}} = \frac{196.02}{1} = 196.02$$

$$MS_{within} = \frac{SS_{within}}{df_{within}} = \frac{1.96}{198} = 0.01$$

below:

F-statistic is calculated as follows:

$$F = \frac{MS_{between}}{MS_{within}} = \frac{196.02}{0.01} = 19802.02$$

Calculations of null and alternative hypotheses

Ho: $\mu_1 = \mu_2$

Ha: Alternative hypothesis states that all means are not equal

Hypothesis testing is based on the ANOVA analysis utilizing F ratio

Rejection region

Significance level is denoted as "α" and is α=0.05

Degrees of freedom is denoted as $df_1 = 1$ and $df_2 = 1$

Rejection region is calculated as $R = \{F : F > F_c = 3.889\}$

Statistics of the Test

$$F = \frac{MS_{between}}{MS_{within}} = \frac{196.02}{0.01} = 19802.02$$

Decision about the null hypothesis:

The calculation shows that F = 19802.02> Fc=3.889, which shows that *null hypothesis is rejected with F value approach*. The calculation of p-value since *p*=0<0.05, which shows that *null hypothesis is rejected with P value approach*.

Conclusion:

The statistical result and conclusion states that null hypothesis Ho is rejected which provides enough proof to claim that means of two population are not equal having α=0.05 significance level

5.3.6 Manageability

Sample size total is denoted as N = 200

Calculation for Total degrees of freedom (df_{total}):

$$df_{total} = 200 - 1 = 199$$

Also, the between-groups degrees of freedom are $df_{between} = 2 - 1 = 1$

and the within-groups degrees of freedom are:

$$df_{within} = df_{total} - df_{between} = 199 - 1 = 198$$

Calculation to compute the total sum of values and the grand mean.

The following is obtained

$$\sum_{i,j} X_{ij} = 189 + 100 = 289$$

Then, the value of square will be

$$\sum_{i,j} X_{ij}^2 = 367 + 106 = 473$$

The SS_{total} value is:

$$SS_{total} = \sum_{i,j} X_{ij}^2 - \frac{1}{N}\left(\sum_{i,j} X_{ij}\right)^2 = 473 - \frac{289^2}{200} = 55.395$$

The SS_{within} value is:

$$SS_{within} = \sum SS_{withingroups} = 9.79 + 6 = 15.79$$

MS, which is mean sum of square, are calculated below

$$MS_{between} = \frac{SS_{between}}{df_{between}} = \frac{39.605}{1} = 39.605$$

$$MS_{within} = \frac{SS_{within}}{df_{within}} = \frac{15.79}{198} = 0.08$$

F-statistic is calculated as follows:

$$F = \frac{MS_{between}}{MS_{within}} = \frac{39.605}{0.08} = 496.63$$

Calculations of null and alternative hypotheses

Ho: $\mu_1 = \mu_2$

Ha: Alternative hypothesis states that all means are not equal

Hypothesis testing is based on the ANOVA analysis utilizing F ratio

Rejection region

Significance level is denoted as "α" and is α=0.05

Degrees of freedom is denoted as $df_1 = 1$ and $df_2 = 1$

Rejection region is calculated as $R = \{F : F > F_c = 3.889\}$

Statistics of the Test

$$F = \frac{MS_{between}}{MS_{within}} = \frac{39.605}{0.08} = 496.63$$

Calculations of null and alternative hypotheses

The calculation shows that *F*=496.63>*Fc*=3.889, which shows that *null hypothesis is rejected with F value approach*. The calculation of p-value since *p*=0<0.05, which shows that *null hypothesis is rejected with P value approach*.

Conclusion

The statistical result and conclusion states that null hypothesis Ho is rejected which provides enough proof to claim that means of two population are not equal having α=0.05 significance level

5.4 RESULT AND DISCUSSIONS

The development and experiment of HBSTS proves to solve the various problem statements and challenges found in client / server models. Post development and testing of the framework, HBSTS has been implemented in ten organizations for practically being verified that the problem statements are addressed matching the ground reality. After the implementation phase on various small and medium scale industries and prolonged usage, the problem statements were evaluated on the following factors:

- Security features
- Foresee benefits
- Cost benefit
- Transparency
- Execution time
- Manageability
- Consider permanent

Security Features: The security features of HBSTS has exponential acceptance as compared to the traditional approach. The evaluation results state that security features of HBSTS has superior features against data theft, data tampering, data modification, data corruption and offers full transparency of data when it comes to integrity. A majority of the sample feels that HBSTS is more efficient in countering cyber threats like hacking, cross-site scripting, injection attacks and ransomware attacks including internal threats, compared to the existing traditional client/server model approach.

Foresee Benefits: A majority of the group feels that they foresee benefits in adapting and accepting the usage of the HBSTS framework. The benefits include overall features of the HBSTS framework as compared to the existing model. The benefits in

adapting the blockchain HBSTS framework during the evaluation has been depicted by a quick rise in the graph of wide acceptance which includes data security, license cost, fault tolerance, integrity and transparency, internal and external attacks, interoperability and cohesive platform.

Cost Benefit: A majority of the group from the evaluation data exhibits higher financial benefits and affordability while using the HBSTS framework as compared to the existing traditional model. This has no license, software and operating system cost, practically no maintenance cost, open source platform and less manpower cost. This also saves direct and indirect cost in adapting this technology.

Transparency: The transparency of the data is of the utmost priority when it comes to integrity and reporting. The data should be correct and transparent to third party vendors, media, business intelligence or ad-hoc reports. A majority speaks about the transparency of the data and showed higher precedence of HBSTS over the existing model. The HBSTS framework has exhibited that the transactional data displayed is correct pertaining to users, vendors, officials and others. This practical transparency has triggered a higher precedence over the existing traditional approach by the experimental group.

Execution Time: The transaction execution time is the time taken to execute and retrieve a transaction from the HBSTS and the existing model. It, however, consists of various other factors like internet and network speed, latency, IOPS of the system and other extraneous factors. The sample group in testing the execution time for both HBSTS and the existing model has evaluated the basic execution parameters. The vast majority of the sample group feels that there is no major difference in transaction execution time of the HBSTS framework and that of the existing model. The transaction execution time in the existing traditional model is a bit better than the HBSTS framework but there is no significant difference in mean of the two sample groups.

Manageability: Manageability refers to the overall manageability of the framework as compared to the traditional approach. The manageability feature includes that the framework should have no or less management overheads. This aligns with the HBSTS framework, which has no third party intervention, and works with the

consensus mechanism and is not managed by any central authority. The overall manageability throws light on the availability feature where the technology should run on any type of failures. It also includes interoperability with which the technology communicates within hybrid devices on a shared platform. Cohesiveness is a significant factor in manageability where the technology should be integrated with the traditional approach. Majority of the population feels that HBSTS has better and higher manageability features than the existing traditional approach.

Consider Permanent: Considering all the evaluation parameters and features used during the evaluation and implementation process of the framework, HBSTS has higher precedence over the existing model. A vast majority of the population suggested considering and using the HBSTS framework as permanent as against the existing traditional model approach.

CHAPTER 6

CONCLUSION AND FUTURE STUDY

This chapter provides a conclusive note based on the research being carried out. It answers the objective of the research and problem statement. This chapter defines the achievement of the study. The future prospects and limitations of the research are given as endnotes in this chapter.

6.1 CONCLUSION

Industries have started adopting blockchain platforms in recent years for various uses in transactions and applications. The rise of the blockchain platform as a service, hyperledger, and smart contract has shifted the data security landscape and established a new paradigm in contrast to the widespread use of blockchain in digital currency. The underlying technology is more powerful and robust. Adaptation and usage of blockchain gradually has thrown light in different industries like healthcare, pharma, supply chain, logistics, finance etc. This slow and gradual adaptation is a thought-provoking factor in how the thought process is changing for various industries. Industries are realizing that security features are also a prime concern of the organization without which an organization may face various fatal business challenges and the same holds true for small and medium sized enterprises. Data theft, modification tampering, affordability, interoperability and availability challenges are addressed in HBSTS and have a greater response in adaptation.

We can conclude that HBSTS can be a secured choice of transactions in contrast to the traditional approach. A majority of the implementation data and feedback from various conservative employees feels that HBSTS can be a good alternative to traditional transaction methods. The transaction not only highlights the security feature, but it also demonstrates that the total deployment and maintenance of HBSTS is cost-effective, with no need for third-party assistance. HBSTS framework has been implemented and evaluated by ten different organizations with different lines of business. There were hundred employees from various departments and the vast majority felt that the traditional approach shortcomings can be achieved by implementing HBSTS in the organization. Thus, we can say that, the experimental

research has concluded the acceptance of HBSTS and has successfully addressed the problem statements of this research. The blockchain platform has been able to address issues aforementioned in the problem statements, usually found in small and medium scale industries wherein the information technology budget is low. In most cases, security becomes a low priority factor for various organizations and hence, are more prone to internal and external cyber-attack. Maintenance, implementation, indirect cost, manpower and various other related overheads become a burden for the SME sector and thus, a barrier for investment in information technology. Blockchain platforms become less adoptable because of unaffordability due to the various paid platforms as a service and the expertise required in this field for implementation. HBSTS proves to be a boon for data security and affordability challenges and complexity in implementing and securing data for any possible data changes, clarity and transparency in data. The development of the HBSTS framework and implementation in various organizations satisfies the problem statements related to the traditional client/server model.

6.2 ACHIEVEMENT OF THE RESEARCH

HBSTS framework has been developed keeping in mind prime challenges faced in data security like corruption, frauds, cheats, scams and cost efficiency in the implementation of a platform in the small and medium sized enterprise where transactions are feed in a technology that has no control over a central authority, no maintenance overheads and the data is transparent and secure. This also exhibits append only chains where data modification is not possible and transactions are validated through consensus mechanism. The research has opened a new lane towards a robust technology for small and medium scale sectors where the problem statements are addressed. The implementation and evaluation exhibits a wide acceptance and adaptability.

Data Security: Data security, is a major concern in the traditional approach, where the platform is prone to attacks like corruption, scams, data leak, data tampering, alteration of organization data, financial loss or data crime due to enmity, personal grudges etc. The design and implementation of HBSTS has addressed data security issues, which makes it nearly impossible to create data fraud in the consensus mechanism giving the data probabilistic immutability.

Threats and Cyber-Attacks: The threat control mechanism throws light on how the technology is vulnerable to attack and what countermeasures the technology has to prevent those threats. The existing traditional model has various vulnerabilities, which are prone to attacks like cross-site scripting, injection attacks, virus, malwares, and ransomware. HBSTS framework has addressed all these attacks, which have no or less possibility of vulnerability. The black-box and white-box testing from professional penetration services exhibits that there are no or very little chances of these attacks.

Data Transparency and Integrity: Data transparency is a very important factor for an organization. Data, especially when transparent for the intended recipient should be authentic and correct. The traditional approach, which follows the client / server model, has little or no data transparency upfront. The changed or modified data when focused on intentionally may have a reason. Regardless of this, a question on the data integrity arises and incorrect data can be focused to evade various lawful challenges. HBSTS does not have this challenge as it gives data probabilistic immutability. When both parties agree on a successful transaction, the data cannot be updated and the transaction is fed into HBSTS following various successful verification. This perennial problem is solved with HBSTS and transaction data has full transparency.

Affordability: The affordability of secured transactions refers to the cost it comes with, including maintenance. The traditional approach has a huge software license cost due to various operating systems, applications and related devices. Maintenance of technology is also a factor, which includes labor costs, power and infrastructure as is in case of the client/server model. HBSTS is highly secured with no maintenance and no control over the central authority. This has no manpower costs and gets authenticated on its own. Since this technology is open sourced, there is no license cost as such. The technology is so light weighted that it can run on very low memory devices like mobile phones too.

6.3 LIMITATIONS IN THE STUDY

Performance and stress testing with huge data and nodes is a significant limitation, which could not be carried out due to various reasons and time constraints through professional services. Nevertheless, basic performance testing has been carried out

during the development of HBSTS. The implementation and evaluation phase did not have any performance issues from any devices on hybrid network infrastructure. However, the tests were not carried out with big data. Although HBSTS framework is safe for major attacks that are considered during the time of development, there is still a chance that very recently developed attacks may leave it vulnerable.

6.4 FUTURE SCOPE

The HBSTS framework has solved the basic problems that accompanied the traditional client/server approach model. There are certain studies that need to be carried out which were not possible due to various factors including time constraints. HBSTS internal communication packets are transferred through SSL (Secured Socket Layer) encryption. Although SSL itself is a secured technology, with the advent of TLS (Transport Layer Security) which is more secure than SSL, TLS should be used for all communication. TLS V1.3 should be integrated with HBSTS network communication. There still may be a performance issue when transaction increases invariably as well as number of nodes. As performance and stress testing was not done with huge data professionally, this may be addressed with data sharding. Artificial intelligence can be introduced for security monitoring of transaction patterns in HBSTS and can create alarm or cancel a transaction according to the requirement.

REFERENCES

[1] Wu, K, Ma, Y, Huang, G, Liu, X., (2021), A first look at blockchain-based decentralized applications. Softw: Pract Exper. 51: 2033– 2050.

[2] Xuan Chen, Ryota Nakada, Kien Nguyen, Hiroo Sekiya, (2021), "A Comparison of Distributed Ledger Technologies in IoT: IOTA versus Ethereum", Communications and Information Technologies (ISCIT) 20th International Symposium on, pp. 182-187.

[3] Piera Centobelli, Roberto Cerchione, Pasquale Del Vecchio, Eugenio Oropallo, Giustina Secundo, (2021), Blockchain technology for bridging trust, traceability and transparency in circular supply chain, Information & Management, 103508.

[4] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia, (2021), A Survey on Blockchain Interoperability: Past, Present, and Future Trends. ACM Comput. Surv. 54, 8, Article 168 (November 2022), 41 pages.

[5] Irresberger, Felix and John, Kose and Mueller, Peter and Saleh, Fahad, (2021), The Public Blockchain Ecosystem: An Empirical Analysis. NYU Stern School of Business.

[6] Poonam Garg, Bhumika Gupta, Ajay Kumar Chauhan, Uthayasankar Sivarajah, Shivam Gupta, Sachin Modgil, (2021), Measuring the perceived benefits of implementing blockchain technology in the banking sector, Technological Forecasting and Social Change, Volume 163, 120407.

[7] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shahbaz Khan, Rajiv Suman, (2021), Blockchain technology applications for Industry 4.0: A literature-based review, Blockchain: Research and Applications, 100027.

[8] Auqib Hamid Lone, Roohie Naaz, (2021), Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review, Computer Science Review, Volume 39.

[9] Baozhuang Niu, Zihao Mu, Bin Cao, Jie Gao, (2021), Should multinational firms implement blockchain to provide quality verification?, Transportation Research Part E: Logistics and Transportation Review, Volume 145, 102121.

[10] Bayramova A, Edwards DJ, Roberts C, (2021), The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime. Buildings. 2021; 11(7):283.

[11] Raja Wasim Ahmad, Haya Hasan, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Mohammed Omar, (2021), Blockchain for aerospace and defense: Opportunities and open research challenges, Computers & Industrial Engineering, Volume 151, 106982.

[12] Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains unchained: Blockchain technology and its use in the public sector.

[13] Laurence, T. (2019). Introduction to blockchain technology. Van Haren.

[14] Sander, F., Semeijn, J., & Mahr, D. (2018). The acceptance of blockchain technology in meat traceability and transparency. British Food Journal.

[15] Gaggioli, A. (2018). Blockchain technology: living in a decentralized everything. Cyberpsychology, Behavior, and Social Networking, 21(1), 65-66.

[16] Alsunaidi, S. J., & Alhaidari, F. A. (2019, April). A survey of consensus algorithms for blockchain technology. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

[17] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853.

[18] Nguyen, Q. K., & Dang, Q. V. (2018, November). Blockchain Technology for the Advancement of the Future. In 2018 4th international conference on green technology and sustainable development (GTSD) (pp. 483-486). IEEE.

[19] Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: a research agenda. Australian Accounting Review, 29(2), 331-342.

[20] Dimitri, N. (2017). The blockchain technology: Some theory and applications (No. 2017/1).

[21] Ali, S., Alauldeen, R., & Ruaa, A.(2020). What is Client-Server System: Architecture, Issues and Challenge of Client-Server System. HBRP Publication, 1-6.

[22] Muller, N. J. (2020). Client/Server Architecture and Implementation. In Enterprise Operations Management (pp. 189-205). Auerbach Publications.

[23] Kim, J., & Gim, G. (2017). A study on factors affecting the intention to accept blockchain technology. Journal of Information Technology Services, 16(2), 1-20.

[24] Akgiray, V. (2019). The potential for blockchain technology in corporate governance.

[25] Yeoh, P. (2017). Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance.

[26] Mohanta, B. K., Panda, S. S., & Jena, D. (2018, July). An overview of smart contract and use cases in blockchain technology. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-4). IEEE.

[27] Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. Information & Management, 58(3), 103444.

[28] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

[29] Bayramova A, Edwards DJ, Roberts C, (2021), The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime. Buildings. 11(7):283.

[30] Arcos, L. C. (2018). The blockchain technology on the music industry. Brazilian Journal of Operations & Production Management, 15(3), 439-443.

[31] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187.

[32] Alam, T. (2021). Blockchain-based big data integrity service framework for IoT devices data processing in smart cities. Mindanao Journal of Science and Technology.

[33] Benton, M. C., & Radziwill, N. M. (2017). Quality and Innovation with Blockchain technology. arXiv preprint arXiv:1710.04130.

[34] Perera, S., Nanayakkara, S., Rodrigo, M. N. N., Senaratne, S., & Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry?. Journal of Industrial Information Integration, 17, 100125.

[35] Shang, M., & Sun, H. (2020, October). Study on the New Models of Music Industry in the Era of AI and Blockchain. In 2020 3rd International Conference on Smart BlockChain (SmartBlock) (pp. 63-68). IEEE.

[36] Ahmad, R. W., Salah, K., Jayaraman, R., Hasan, H. R., Yaqoob, I., & Omar, M. (2021). The Role of Blockchain Technology in Aviation Industry. IEEE Aerospace and Electronic Systems Magazine, 36(3), 4-15.

[37] Bilyalova, A. A., Vaslavskaya, I., & Gaifutdinova, R. (2020, May). Digitalization of the transport industry: Technology of blockchain. In 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth"(MTDE 2020) (pp. 152-156). Atlantis Press.

[38] Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y, (2021). A survey on blockchain for information systems management and security. Information Processing & Management, 58(1), 102397.

[39] Jing, N., Liu, Q., & Sugumaran, V. (2021). A blockchain-based code copyright management system. Information Processing & Management, 58(3), 102518.

[40] Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. International Journal of Production Economics, 231, 107831.

[41] Oham, C., Michelin, R. A., Jurdak, R., Kanhere, S. S., & Jha, S. (2021). B-FERL: Blockchain based framework for securing smart vehicles. Information Processing & Management, 58(1), 102426.

[42] Ahmad, R. W., Hasan, H., Jayaraman, R., Salah, K., & Omar, M. (2021). Blockchain applications and architectures for port operations and logistics management. Research in Transportation Business & Management, 100620.

[43] Carvalho, A., Merhout, J. W., Kadiyala, Y., & Bentley II, J. (2021). When good blocks go bad: Managing unwanted blockchain data. International Journal of Information Management, 57, 102263.

[44] Xu, X., Sun, G., Luo, L., Cao, H., Yu, H., & Vasilakos, A. V. (2021). Latency performance modeling and analysis for hyperledger fabric blockchain network. Information Processing & Management, 58(1), 102436.

[45] Gupta, S., Hellings, J., & Sadoghi, M. (2021). Fault-Tolerant Distributed Transactions on Blockchain. Synthesis Lectures on Data Management, 16(1), 1-268.

[46] Bisogni, C., Iovane, G., Landi, R. E., & Nappi, M. (2021). ECB2: A novel encryption scheme using face biometrics for signing blockchain transactions. Journal of Information Security and Applications, 59, 102814.

[47] Amiri, M. J., Lai, Z., Patel, L., Loo, B. T., Lo, E., & Zhou, W. (2021). Saguaro: Efficient Processing of Transactions in Wide Area Networks using a Hierarchical Permissioned Blockchain. arXiv preprint arXiv:2101.08819.

[48] Mashatan, A., Lemieux, V., Lee, S. H. M., Szufel, P., & Roberts, Z. (2021). Usurping Double-Ending Fraud in Real Estate Transactions via Blockchain Technology. Journal of Database Management (JDM), 32(1), 27-48.

[49] Hu, W., & Li, H. (2021). A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things. Alexandria Engineering Journal, 60(1), 491-500.

[50] Khan, P. W., & Byun, Y. C. (2021). Secure Transactions Management Using Blockchain as a Service Software for the Internet of Things. In Software Engineering in IoT, Big Data, Cloud and Mobile Computing (pp. 117-128). Springer, Cham.

[51] Zhang, Y., & Shi, Q. (2021). An intelligent transaction model for energy blockchain based on diversity of subjects. Alexandria Engineering Journal, 60(1), 749-756.

[52] Zhao, D. (2020). Cross-blockchain transactions. In Conference on Innovative Data Systems Research (CIDR).

[53] Pasala, S., Pavani, V., Lakshmi, G. V., & Narayana, V. L. (2020). Identification of attackers using blockchain transactions using cryptography methods. Journal of Critical Reviews, 7(6), 368-375.

[54] Albayati, H., Kim, S. K., & Rho, J. J. (2020). Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach. Technology in Society, 62, 101320.

[55] Konashevych, O., & Khovayko, O. (2020). Randpay: The technology for blockchain micropayments and transactions, which require recipient's consent. Computers & Security, 96, 101892.

[56] Jia, Y., Sun, S., Zhang, Y., Zhang, Q., Ding, N., Liu, Z., & Gu, D. (2020). PBT: A new privacy-preserving payment protocol for blockchain transactions. IEEE Transactions on Dependable and Secure Computing.

[57] Zhao, D. (2020). Topological Properties of Multi-Party Blockchain Transactions. arXiv preprint arXiv:2004.01045.

[58] Bamasag, O., Munshi, A., Alharbi, H., Aldairi, O., Altowerky, H., Alshomrani, R., & Alharbi, A. (2020). Blockchain and smart contract in future transactions—Case studies. In Decentralised Internet of Things (pp. 169-198). Springer, Cham.

[59] Reyes-Macedo, V. G., Salinas-Rosales, M., & Garcia, G. G. (2019). A method for blockchain transactions analysis. IEEE Latin America Transactions, 17(07), 1080-1087.

[60] Jivanyan, A. (2019). Lelantus: Towards Confidentiality and Anonymity of Blockchain Transactions from Standard Assumptions. IACR Cryptol. ePrint Arch., 2019, 373.

[61] Gomaa, A. A., Gomaa, M. I., & Stampone, A. (2019). A transaction on the blockchain: An AIS perspective, intro case to explain transactions on the ERP and the role of the internal and external auditor. Journal of Emerging Technologies in Accounting, 16(1), 47-64.

[62] Maksutov, A. A., Alexeev, M. S., Fedorova, N. O., & Andreev, D. A. (2019, January). Detection of blockchain transactions used in blockchain mixer of coin join type. In 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 274-277). IEEE.

[63] Thio-ac, A., Serut, A. K., Torrejos, R. L., Rivo, K. D., & Velasco, J. (2019). Blockchain-based system evaluation: The effectiveness of blockchain on E-procurements. arXiv preprint arXiv:1911.05399.

[64] [64] Dutta, S., & Saini, K. (2020). Blockchain and Ecosystem. International Journal of Advanced Science and Technology, 29(9s), 4339 – 4351.

[65] Dutta, S., & Saini, K. (2020). Blockchain and Social Media. In Blockchain Technology and Applications (pp. 101-114). CRC Press.

[66] Dutta, S., & Saini, K. (2019). Evolution of blockchain technology in business applications. Journal of Emerging Technologies and Innovative Research (JETIR), 6(9), 240-244.

[67] Faisal, T., Courtois, N., & Serguieva, A. (2018, July). The evolution of embedding metadata in blockchain transactions. In 2018 International Joint Conference on Neural Networks (IJCNN) (pp. 1-9). IEEE.

[68] Tilooby, A. (2018). The impact of blockchain technology on financial transactions.

[69] Kotilevets, I. D., Ivanova, I. A., Romanov, I. O., Magomedov, S. G., Nikonov, V. V., & Pavelev, S. A. (2018). Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions. IFAC-PapersOnLine, 51(30), 693-696.

[70] Loebbecke, C., Lueneborg, L., & Niederle, D. (2018). Blockchain technology impacting the role of trust in transactions: Reflections in the case of trading diamonds.

[71] Kiayias, A., & Panagiotakos, G. (2017, September). On trees, chains and fast transactions in the blockchain. In International Conference on Cryptology and Information Security in Latin America (pp. 327-351). Springer, Cham.

[72] Vovchenko, N. G., Andreeva, A. V., Orobinskiy, A. S., & Filippov, Y. M. (2017). Competitive advantages of financial transactions on the basis of the blockchain technology in digital economy. European Research Studies, 20(3B), 193.

[73] Peter, H., & Moser, A. (2017). Blockchain-applications in banking & payment transactions: Results of a survey. European financial systems, 141, 141.

[74] Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5-21.

[75] Atiwa, S., Dawji, Y., Refaey, A., & Magierowski, S. (2020). Accelerated Hardware Implementation of BLAKE2 Cryptographic Hash for Blockchain. In 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) (pp. 1-6). IEEE.

[76] Haq, T. U., Shah, T., Siddiqui, G. F., Iqbal, M. Z., Hameed, I. A., & Jamil, H. (2021). Improved Twofish Algorithm: A Digital Image Enciphering Application. IEEE Access, 9, 76518-76530.

[77] Siddiqui, S. T., Ahmad, R., Shuaib, M., & Alam, S. (2020). Blockchain security threats, attacks and countermeasures. Advances in Intelligent Systems and Computing, 1097, 51-62.

[78] Priyadarshini, I. (2019). Introduction to blockchain technology. Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, 91-107.

[79] Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. Computer Networks, 166, 106960.

[80] Grover, V. (2020, March). An Efficient Brute Force Attack Handling Techniques for Server Virtualization. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).

[81] Spurr, A., & Ausloos, M. (2021). Challenging practical features of Bitcoin by the main altcoins. Quality & Quantity, 55(5), 1541-1559.

[82] Guggenberger, T., Schlatt, V., Schmid, J., & Urbach, N. (2021). A structured overview of attacks on blockchain systems. In Proceedings of the Pacific Asia Conference on Information Systems (PACIS).

[83] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020). Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1977-2008.

[84] Kareem, F. Q., Ameen, S. Y., Salih, A. A., Ahmed, D. M., Kak, S. F., Yasin, H. M., & Omar, N. (2021). SQL injection attacks prevention system technology. Asian Journal of Research in Computer Science, 13, 32.

[85] Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain technology in business and information systems research.

[86] Yan, C., Zhu, J., Ouyang, Y., & Zeng, X. (2021). Marketing Method and System Optimization Based on the Financial Blockchain of the Internet of Things. Wireless Communications and Mobile Computing, 2021.

[87] Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., & Chen, S. (2020). Public and private blockchain in construction business process and information integration. Automation in construction, 118, 103276.

[88] Faccia, A., & Mosteanu, N. R. (2019). Accounting and blockchain technology: from double-entry to triple-entry. The Business & Management Review, 10(2), 108-116.

[89] Tandon, A., Dhir, A., Islam, N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, 103290.

[90] Yu, C., Jiang, X., Yu, S., & Yang, C. (2020). Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation. Robotics and Computer-Integrated Manufacturing, 64, 101931.

[91] He, P., Yu, G., Zhang, Y. F., & Bao, Y. B. (2017). Survey on blockchain technology and its application prospects. Computer Science, 44(4), 1-7.

[92] Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. Journal of Property, Planning and Environmental Law.

[93] Nandi, M., Bhattacharjee, R. K., Jha, A., & Barbhuiya, F. A. (2020). A secured land registration framework on Blockchain. In 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP) (pp. 130-138). IEEE.

[94] Valli, C., Martinus, I., Stanley, J., & Kirby, M. (2021). CyberCheck. me: A Review of a Small to Medium Enterprise Cyber Security Awareness Program. Advances in Security, Networks, and Internet of Things, 233-242.

[95] Habib, M. A., Sardar, M. B., Jabbar, S., Faisal, C. N., Mahmood, N., & Ahmad, M. (2020, February). Blockchain-based supply chain for the automation of transaction process: Case study based validation. In 2020 International Conference on Engineering and Emerging Technologies (ICEET) (pp. 1-7). IEEE.

[96] Vujičić, D., Jagodić, D., & Ranđić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th international symposium infoteh-jahorina (infoteh) (pp. 1-6). IEEE.

[97] Li, Y., Marier-Bienvenue, T., Perron-Brault, A., Wang, X., & Paré, G. (2018, January). Blockchain technology in business organizations: A scoping review. In Proceedings of the 51st Hawaii International Conference on System Sciences

[98] Guo, Y. M., Huang, Z. L., Guo, J., Guo, X. R., Li, H., Liu, M. Y., ... & Nkeli, M. J. (2021). A bibliometric analysis and visualization of blockchain. Future Generation Computer Systems, 116, 316-332.

[99] Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications, 177, 102857.

[100] Dave, D., Parikh, S., Patel, R., & Doshi, N. (2019). A Survey on Blockchain Technology and its Proposed Solutions. Procedia Computer Science, 160, 740-745.

[101] Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: a review. Ieee Access, 6, 10179-10188.

ANNEXURE-1

QUESTIONNAIRES

At the end of the implementation and evaluation of HBSTS, the participants were given google forms for feedback. The annexure were divided into three sections. The first section took the details of the participants and organizations details. The second section took the input for technical implementation details for HBSTS in the organization like type, modules evaluated and usage duration. The third section evaluates the result of HBSTS as compared to the traditional method.

Section I (General Information)

- ❑ Email address
- ❑ Name
- ❑ Designation
- ❑ Industry Type
- ❑ Number of employees in the organization
    - ❑ 1 to 100
    - ❑ 101 to 500
- ❑ Organization name

Section II (Technical Evaluation)

- ❑ Type of implementation

- ❑ Modules implemented
    - ❑ Sales call transactions
    - ❑ Product Data transactions
    - ❑ Support call transactions
    - ❑ Financial transactions
    - ❑ Service call transactions
    - ❑ Evaluation transactions
    - ❑ Medical transactions

- ❑ Usage duration
    - ❑ 1 Month
    - ❑ 2 Month
    - ❑ 3 Month
    - ❑ 4 Month
    - ❑ 5 Month
    - ❑ > 6 Months

Section III (Result section)

Security features of Blockchain	Security features of existing system as compared to blockchain
(0) Very poor---------- (4) Excellent	(0) Very poor---------- (4) Excellent

- ❑ Features liked the most
    - ❑ Enhanced security
    - ❑ Low failure rate
    - ❑ Decentralization and peer to peer
    - ❑ Zero scams
    - ❑ Transparency
    - ❑ No malicious threats
    - ❑ Other

Do you foresee the benefits of Blockchain	Do you foresee the benefits of Existing system as compared to Blockchain
(0) No---------- (2) Yes	(0) No---------- (2) Yes

Did you find blockchain cost effective	Did you find the Existing solution cost effective

(0) No---------- (2) Yes	(0) No---------- (2) Yes

Manageability of Blockchain	Manageability of Existing system
(0) Hard---------- (2) Easy	(0) Hard---------- (2) Easy

Transparency on Blockchain	Transparency on existing system
(0) Low---------- (2) High	(0) Low---------- (2) High

Execution time on Blockchain	Execution time on existing system
(0) Slow---------- (3) Very fast	(0) Slow---------- (3) Very fast

- ❑ What are the limitations of this technology faced
    - ❑ Risk of error because of human intervention
    - ❑ Blockchain uses excessive energy
    - ❑ Storage issues
    - ❑ Data modification

- ❑ Would you consider to permanently used this as an application in your organization
    - ❑ Yes
    - ❑ No
    - ❑ May be

LIST OF PUBLICATIONS FROM THE THESIS

LIST OF JOURNALS

1. Dutta, S., & Saini, K. (2021). Securing data: A study on different transform domain techniques. WSEAS Transactions on Systems and Control, 16. **(Scopus)**
2. Dutta, S., & Saini, K. (2021). Statistical assessment of hybrid blockchain for SME sector. WSEAS Transactions on Systems and Control, 16, 83-95. **(Scopus)**
3. Dutta, S., & Saini, K. (2020). Blockchain and Ecosystem. International Journal of Advanced Science and Technology, 29(9s), 4339 – 4351. **(Scopus)**

LIST OF CONFERENCE

1. Saugata Dutta, Dr. Kavita "Evolution of Blockchain Technology in Business Applications", 2nd International Conference on Future Communication & Computing Technology (ICFCCT-19), Organized by MIET and IFERP, 17 - 18 July 2019, Meerut , India

LIST OF BOOK / CHAPTERS

1. Dutta, S., & Saini, K. (2021). Blockchain Implementation Using Python. In Advancing Smarter and More Secure Industrial Applications Using AI, IoT, and Blockchain Technology (pp. 123-136). IGI Global. **(Scopus)**
2. Dutta, S., & Saini, K. (2020). Blockchain and Social Media. In Blockchain Technology and Applications (pp. 101-114). CRC Press. **(Scopus)**