

# Preservation of Smart Home System Based on Blockchain



**MCS**

By

**Amara Riaz**

**(Registration No: 00000431930)**

A thesis submitted to the National University of Science and Technology, Islamabad,

in partial fulfilment of the requirements for the degree of

Master of Science in

Information Security

Supervisor: **Dr. Faiz Ul Islam**

Military College of Signals

National University of Sciences and Technology (NUST) Islamabad, Pakistan

(May 2024)


# THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by Amara Riaz, Registration No. 00000431930, of Military College of Signals has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

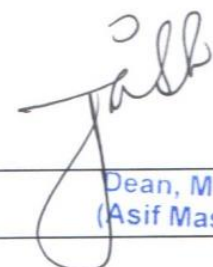
Signature: 

Name of Supervisor Dr Faiz ul Islam

Date: 29/04/2024

Signature (HOD):  **HoD**  
**Information Security**  
**Military College of Signals**

Date: 29/4/24

Signature (Dean/Principal)  **Brig**  
**Dean, MCS (NUST)**  
**(Asif Masood, Phd)**

Date: 13/6/24

**NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY**

**MASTER THESIS WORK**

We hereby recommend that the dissertation prepared under our supervision by **Amara Riaz, MSIS-21 Course** Regn No **00000431930** Titled: **“Preservation of Smart Home System Based on Blockchain”** be accepted in partial fulfillment of the requirements for the award of **MS Information Security** degree.

**Examination Committee Members**

1. Name: **Dr. Muhammad Faisal Amjad**

Signature: \_\_\_\_\_

2. Name: **Maj Sarmad Idrees**

Signature: \_\_\_\_\_

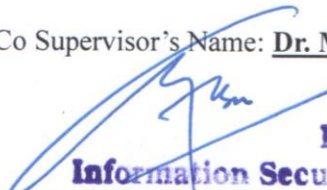
Supervisor's Name: **Dr. Faiz Ul Islam**

Signature: \_\_\_\_\_

Co Supervisor's Name: **Dr. M.M Waseem Iqbal**

Signature: \_\_\_\_\_


Date: \_\_\_\_\_

  
**HoD**  
**Information Security**  
**Military College of Sigs**  
**Head of Department**

11/6/24  
Date

**COUNTERSIGNED**


Date: 12/6/24

  
**Brig**  
**Dean, MCS (NUST)**  
**Asif Masood, PhD**  
Dean

## CERTIFICATE OF APPROVAL

This is to certify that the research work presented in this thesis, entitled “Preservation of Smart Home Systems Based on Blockchain.” was conducted by Amara Riaz under the supervision of Dr. Faiz Ul Islam. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Military College of Signals, National University of Science & Technology Information Security Department in partial fulfillment of the requirements for the degree of Master of Science in Field of Information Security Department of information security National University of Sciences and Technology, Islamabad.

**Student Name:** Maj Amara Riaz


Signature: 

Examination Committee:


a) Co-supervisor: Dr. M.M Waseem Iqbal(MCS)

Signature: 

b) External Examiner 1: Dr. Muhammad Faisal Amjad. (MCS).

Signature: 

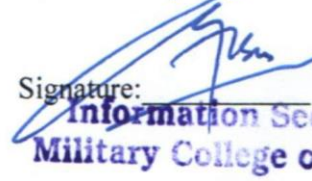
c) External Examiner 2: Maj Sarmad Idrees. (MCS).

Signature: 

Name of Supervisor: Dr. Faiz Ul Islam

Signature: 

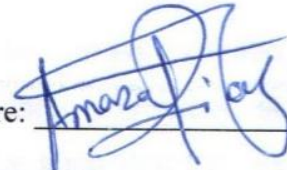
Name of Dean/HOD: Dr Muhammad Faisal Amjad

Signature:  HoD  
**Information Security**  
**Military College of Sig**

## **AUTHOR'S DECLARATION**

I **Maj Amara Riaz** hereby state that my MS thesis titled **Preservation of Smart Home Systems Based on Blockchain** is my own work and has not been submitted previously by me for taking any degree from National University of Sciences and Technology, Islamabad or anywhere else in the country/ world. At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Student Signature: \_\_\_\_\_



Name: **Maj Amara Riaz**

Date: \_\_\_\_\_

11/6/24

## **PLAGIARISM UNDERTAKING**

I solemnly declare that research work presented in the thesis titled **Preservation of Smart Home Systems Based on Blockchain** is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and National University of Sciences and Technology (NUST), Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the University reserves the rights to withdraw/revoke my MS degree and that HEC and NUST, Islamabad has the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized thesis.

Student Signature: \_\_\_\_\_



Name: **Maj Amara Riaz** \_\_\_\_\_

Date: \_\_\_\_\_

11/6/24

## **DEDICATION**

To my parents, whose love, support, encouragement, and sacrifices have made everything I have achieved possible. Their faith in me has been a constant source of inspiration throughout my life.

To my husband and beloved children, for their understanding, patience, and endless support. Their love and encouragement have been my anchor during the tough and challenging times of this journey. This thesis is dedicated to my family who have been my encouragement and lights throughout my academic pursuit.

To my mentors and advisors, Dr. M. Faisal Amjad, Dr. Mian Muhammad Waseem Iqbal, Dr. Faiz Ul Islam and committee members, for their experience, wisdom, guidance, and faith in my abilities. Their mentor-ship has shaped me into a better researcher.

To my friends, who have been my pillars of strength and a source of joy throughout this academic endeavor. Your comradeship has made this journey memorable.

## **ACKNOWLEDGEMENT**

First and foremost I am very grateful to ALMIGHTY ALLAH, The most gracious and the most merciful, who bestowed upon me health, wisdom, knowledge, and the power of communication. I owe a great deal to my supervisor and co-supervisor for valuable guidance, encouragement, and supervision, which made it possible for me to undertake this project and complete my training in this area. I am deeply obliged for the support of my colleagues, Major Sarmad Idrees, Madiha Hassan and Rabiya Tariq, whose cooperation proved very helpful in the compilation of my thesis. I am also gratified to put words of special thanks to my dear husband and my beloved kids for their patience, motivation, sacrifices, cooperation, love, and affection helping me tide over my difficulties and enable me to complete this research work.



## **ABSTRACT**

Smart home systems are becoming more prevalent and popular in modern society, as they can provide convenience, comfort, and efficiency to the users. The proliferation of the Internet of Things (IoT) creates a network of interconnected devices generating vast amounts of data in real-world applications like smart cities, connected appliances, and supply chain management. This growth necessitates addressing challenges related to data security, integrity, and regulatory frameworks for emerging applications and integrations. Blockchain technology offers a potential solution for securing and preserving user and data integrity in a decentralized manner. Hyperledger Fabric, a permissioned blockchain platform, stands out for its open-source nature, modular architecture, and high performance, making it a versatile tool for addressing these concerns within the smart home IoT domain. In this thesis, a blockchain enabled architecture based on Hyperledger Fabric is presented to address the data security and integrity challenges associated with the smart home IoT. A new architecture is introduced to enable this integration, and is developed and deployed, and its performance is analyzed in various scenarios. The evaluation results demonstrate that the proposed solutions outperform over the existing solutions and is feasible and effective over the existing solutions.

# Table of Contents

<b>CHAPTER 1</b>	<b>1</b>
<b>INTRODUCTION</b>	<b>1</b>
<b>1.1 Background</b>	<b>1</b>
<b>1.2 The Evolving Landscape of the Internet of Things</b>	<b>2</b>
<b>1.3 Limitations of IoT Devices</b>	<b>4</b>
1.3.1 Privacy and security concerns	4
1.3.2 Limited power resource	5
1.3.3 Interoperability issue	5
1.3.4 High costs	5
1.3.5 Analytics and data management	5
1.3.6 Data integrity issue	5
1.3.7 Connectivity and reliability	6
1.3.8 Latency issue	6
<b>1.4 Transforming Smart Homes</b>	<b>8</b>
<b>1.5 Security Challenges in Smart Homes</b>	<b>10</b>
1.5.1 Compromised devices	10
1.5.2 Unfettered access to personal information	10
1.5.3 Limited control over information sharing	10
1.5.4 Heterogeneous landscape	11
1.5.5 Data throughout its lifecycle	11
1.5.6 Exponential growth, exponential threats	11
<b>1.6 Importance of Data Integrity</b>	<b>11</b>
1.6.1 Data validation	11
1.6.2 Access controls	12
1.6.3 Data encryption	12
1.6.4 Data audit	12
<b>1.7 Use of Blockchain for enhancing Security and Integrity of Smart Home Systems</b>	<b>12</b>
<b>1.8 Problem Statement</b>	<b>15</b>
<b>1.9 Research Objectives</b>	<b>16</b>
<b>1.10 Research Contributions</b>	<b>16</b>
<b>1.11 Research Questions</b>	<b>17</b>
<b>1.12 Research Significance</b>	<b>17</b>
<b>1.13 Thesis Outline</b>	<b>17</b>
<b>CHAPTER 2</b>	<b>19</b>
<b>RELATED WORK AND LITERATURE REVIEW</b>	<b>19</b>
<b>2.1 Introduction</b>	<b>19</b>
<b>2.2 Smart Homes</b>	<b>20</b>
<b>2.3 Data Integrity</b>	<b>20</b>
<b>2.4 Blockchain Technology</b>	<b>21</b>
<b>2.5 Blockchain for Data Integrity and Security</b>	<b>22</b>

<b>2.6</b>	<b>Trends and Challenges in Cyber-Security for Smart Home IoT Devices</b>	<b>22</b>
<b>2.7</b>	<b>Limitations of Traditional Data Integrity Mechanisms</b>	<b>23</b>
<b>2.8</b>	<b>Possible Attacks</b>	<b>24</b>
<b>2.9</b>	<b>General Approaches for Security in IOT Environments</b>	<b>26</b>
2.9.1	Cryptographic Measures in IoT Environments	26
2.9.2	Access control-based approach	27
2.9.3	Blockchain based approach for IoT security	29
2.9.4	Emergence of DLTs for IoT security	30
<b>2.10</b>	<b>Literature Analysis</b>	<b>31</b>
<b>CHAPTER 3</b>		<b>37</b>
<b>EXPLORING BLOCKCHAIN PLATFORMS</b>		<b>37</b>
<b>3.1</b>	<b>Overview</b>	<b>37</b>
3.1.1	Decentralized	37
3.1.2	Consensus Mechanism	37
3.1.3	Cryptographic Hash	37
3.1.4	Smart Contracts	38
3.1.5	Security and Transparency	38
<b>3.2</b>	<b>Distributed Ledger Technology</b>	<b>38</b>
<b>3.3</b>	<b>Benefits of Blockchain</b>	<b>39</b>
<b>3.4</b>	<b>Types of Blockchain</b>	<b>40</b>
3.4.1	Permissioned vs permissionless blockchain	40
<b>3.5</b>	<b>Public vs Private Blockchain</b>	<b>42</b>
<b>3.6</b>	<b>Challenges Associated with Public Blockchain</b>	<b>45</b>
<b>3.7</b>	<b>Blockchain Platforms</b>	<b>45</b>
3.7.1	Bitcoin	46
3.7.2	Ethereum	46
3.7.3	Hyperledger fabric	46
3.7.4	IBM blockchain	46
3.7.5	OpenChain	47
3.7.6	Stellar	47
3.7.7	EOS	47
3.7.8	Ripple	47
3.7.9	Corda	48
3.7.10	Hedera hashgraph	48
<b>3.8</b>	<b>Comparison of Consensus Mechanisms</b>	<b>49</b>
3.8.1	Proof of work (PoW)	49
3.8.2	Proof of Stake (PoS)	49
3.8.3	Delegated Proof of Stake (DPoS)	49
3.8.4	Byzantine Fault Tolerance (BFT)	50
3.8.5	Practical Byzantine Fault Tolerance (PBFT)	50
3.8.6	Proof of Authority (PoA)	50
3.8.7	Proof of Space (PoSpace)	50
3.8.8	Proof of Burn (PoB)	51
3.8.9	Proof of Elapsed Time (PoET)	51
3.8.10	Proof of Identity (PoI)	51

3.8.11 Proof of Weight (PoWeight)	51
3.8.12 Proof of Activity (PoA)	51
3.8.13 Proof of Reputation (PoR)	52
3.8.14 Tangle	52
3.8.15 Tendermint BFT	52
3.8.16 Honeybadger BFT	52
<b>3.9 Requirements for IoT Systems</b>	<b>52</b>
<b>3.10 General Terminologies</b>	<b>54</b>
3.10.1 Smart contract	55
3.10.2 Decentralized applications (DApp)	56
3.10.3 Blockchain node	57
3.10.4 Token	57
3.10.5 Mining	57
3.10.6 Bitcoin minting	58
3.10.7 Interoperability	58
3.10.8 Oracles	58
<b>CHAPTER 4</b>	<b>59</b>
<b>PROPOSED METHODOLOGY</b>	<b>59</b>
<b>4.1 Selection of Blockchain</b>	<b>60</b>
<b>4.2 Why Hyperledger Fabric (HLF)?</b>	<b>60</b>
<b>4.3 Comparison of HLF with other blockchains</b>	<b>61</b>
4.3.1 Installation steps	62
<b>4.4 Proposed Framework</b>	<b>65</b>
<b>4.5 Participating Entities</b>	<b>66</b>
4.5.1 Home admin (Owner)	66
4.5.2 Home users	67
4.5.3 Smart home	67
4.5.4 Blockchain	68
4.5.5 IPFS	69
4.5.6 Service provider	69
4.5.7 Service requester	69
4.5.8 Evaluation Parameters	70
<b>4.6 Proposed HLF Architecture</b>	<b>70</b>
4.6.2 Channels	71
4.6.3 Committing peers	71
4.6.4 Endorsing peers	71
4.6.5 Ordering service (ODS) peers	72
4.6.6 Membership service provider	72
4.6.7 CC	72
4.6.8 RCA and CA	72
<b>CHAPTER 5</b>	<b>73</b>
<b>ANALYSIS AND RESULTS</b>	<b>73</b>
<b>5.1 PerformanceEvaluation and Comparative Analysis</b>	<b>73</b>

<b>5.2</b>	<b>Limitations of Experimental Setup</b>	<b>74</b>
<b>5.3</b>	<b>Environment Setup</b>	<b>74</b>
<b>5.4</b>	<b>For Efficiency</b>	<b>75</b>
<b>5.5</b>	<b>For Effectiveness</b>	<b>76</b>
<b>5.6</b>	<b>Performance comparison with other schemes</b>	<b>77</b>
<b>5.7</b>	<b>Workflow of the Proposed Architecture</b>	<b>79</b>
5.7.1	Application workflow	79
5.7.2	Service provider workflow	81
<b>CHAPTER 6</b>		<b>84</b>
<b>CONCLUSION AND FUTURE WORK</b>		<b>84</b>
<b>6.1</b>	<b>Conclusion</b>	<b>84</b>
<b>6.2</b>	<b>FutureWork</b>	<b>85</b>
6.2.1	Sharding	85
6.2.2	Real World Testing and Deployment	85
6.2.3	Larger Data Set	86
6.2.4	Use of HLF in Other Domains	86
6.2.5	Other Blockchain Platform	86

## **LIST OF FIGURES**

Figure 1. 1: Different aspects of IoT	4
Figure 1. 2: Overview of a traditional smart home system	10
Figure 1. 3: Overview of blockckchain	14
Figure 2. 1: Smart home devices communications	23
Figure 2. 2: Attacks on Smart Home Systems	26
Figure 2. 3: Different Approaches in IoT Smart Security Environments	31
Figure 3. 1: Basic blockchain concept	38
Figure 3. 2: Types of blockchain	43
Figure 4. 1: Proposed system model	66
Figure 4. 2: HLF architecture	70
Figure 5. 1: Latency of proposed framework	76
Figure 5. 2: CPU usage of proposed framework	77
Figure 5. 3: Comparison of proposed framework with centralized storage	78
Figure 5. 4: Application Workflow	80
Figure 5. 5: Service provider Workflow	82

## **LIST OF TABLES**

Table 1. 1: Limitations of IoT devices and their suggested mitigations .....	6
Table 2. 1: Summary of literature .....	32
Table 3. 1: Permissionless vs Permissioned blockchain.....	40
Table 3. 2: Comparison of Private and Public blockchain .....	44
Table 3. 3: Blockchain platforms and consensus Protocols .....	48
Table 3. 4: Features of Consensus Mechanisms .....	53
Table 3. 5: DApplications vs Centralized Applications.....	56
Table 4. 1: Comparison of blockchains .....	61
Table 5. 1: Specifications of the system .....	74

## **ACRONYMS**

Internet of Things	IoT
Hyperledger Fabric	HLF
Service Provider	SP
Service Requester	SR
Internet of Things Application	IOTA
Distributed Ledger Technology	DLT
Denial of Service	DOS
Information and Communication Technology	ICT
Industrial Internet of Things	IIoT
Electro-Optical System	EOS
Decentralized Application	DApp
Proof of Work	PoW
Proof of Stake	PoS
Byzantine Fault Tolerance	BFT
Practical Byzantine Fault Tolerance	PBFT
Channel Controller	CC
Root Certificate Authority	RCA
Certificate Authority	CA
Inter Planetary File System	IPFS



# CHAPTER 1

## INTRODUCTION

### 1.1 Background

The Internet of Things (IoT) is a concept that removes its initial uncertainty and offers exciting prospects for the future, thanks to the rapid advancements in computer technology [1]. IoT fundamentally builds a network by tying common appliances and electronics devices to the internet, enabling remote control and communication [1]. This opens the door to the intelligent home, where technology integrates every aspect of our living spaces to improve our quality of life at home and convenience. To fully appreciate the smart home revolution, it is imperative to comprehend IoT. Imagine a network where your toaster notifies you when breakfast is ready or your lights adjust automatically based on the time of day.

This is the core idea of a smart home system, which leverages the IoT to turn everyday things into intelligent assistants who can anticipate our needs and streamline daily tasks [2]. Smart homes provide a lot of advantages. Convenience is one of the major benefits. Imagine using your smartphone to prepare the oven while you're on your way home, or using voice control to adjust the lighting or thermostat. Smart homes provide a simplified and easier user experience by doing away with the need for several remote controls and manual changes [2].

Another important consideration is security. Security systems and smart houses can work together to provide real-time monitoring and possible intrusion alarms. This gives homeowners peace of mind, particularly those who wish to monitor their property from a distance or who travel regularly [3]. There can also be a financial benefit: research indicates that smart homes can maximize appliance utilization, which could result in lower energy costs and even cheaper electricity bills [1].

A network of connected electronic devices and sensors is necessary for a smart home's operation. By collecting information and initiating automated reactions, these devices function as a digital nervous system, resulting in a responsive and effective home

environment. A few examples of the parts that function well together are smoke detectors, cameras, thermostats, and motion sensors.

Wireless connectivity is essential part of such systems because it makes installation easier and eliminates the need for heavy wiring, which is a big advantage over traditional systems. This improves aesthetics and makes it easier for the smart home network to grow in the future.

## **1.2 The Evolving Landscape of the Internet of Things**

Evolution of the Internet of Things (IoT) is a paradigm shift, which encourages the networking of common objects (referred to as "things") that are outfitted with sensors, software, and communication technologies. These "things" have the ability to establish connections with other intelligent devices and the internet, creating a constant network. IoT has grown rapidly in the last several years, disrupting many facets of our life and drastically changing the way we engage with technology. A variety of sectors, including industry, energy, transportation, housing, agriculture, and healthcare, are among those in which it finds employment [4]. In the upcoming years, it is anticipated that the IoT environment will grow explosively. Statista estimates that by 2030, astonishingly 29.42 billion smart devices to be connected [5]. The International Data Corporation predicts that by 2025, IoT devices will produce an unbelievable 80 Zeta Bytes of data, which emphasizes this exponential rise even more [3].

The IoT, or IoT, has come a long way since Ashton and Gamble first envisioned it as a network model back in 1999. The wide range network of connected nodes, communication protocols, and devices that provide increased convenience and efficiency across a variety of industries are responsible for its rapid acceptance [6]. But there are also serious security issues that have been raised by the IoT ecosystem's rapidly expanding size and complexity [6, 7].

The fundamental idea behind the IoT is to allow physical items to exchange data with one other in an easy-to-use manner for further analysis. Usually, information gathered by sensors built into these devices is analyzed and saved in the cloud for later review. A number of possibilities are presented by this data-driven strategy, including increased

automation and better decision-making in a variety of fields. But it also presents a lot of difficulties, especially when it comes to extracting data from devices with low computing power [8].

Furthermore, the IoT ecosystem's rapidly expanding network of connected devices has raised privacy concerns, which has prompted industry leaders and researchers to work together to build strong solutions [8]. It is expected that in the upcoming years, there will be an exponential number of connected devices [9], making it more important than ever to address the security risks that come with them.

Sensors for data collection, computational nodes for processing, receivers for data aggregation, actuators for physical manipulation, and the connected devices themselves are the core components that form the basis of the IoT ecosystem. A generic IoT framework is usually constructed with distinct layers, each performing a specialized role, to enable efficient operation. The application layer, which manages user interaction and certain functionalities, the middle layer, which handles data management and processing, the network layer, which facilitates communication between devices and the cloud, the physical/sensor layer, which gathers data from the environment, and the business layer, which concentrates on value creation and service delivery, are examples of common layers [10]. Figure 1.1 shows different prominent aspects of IoTs being used in this era.

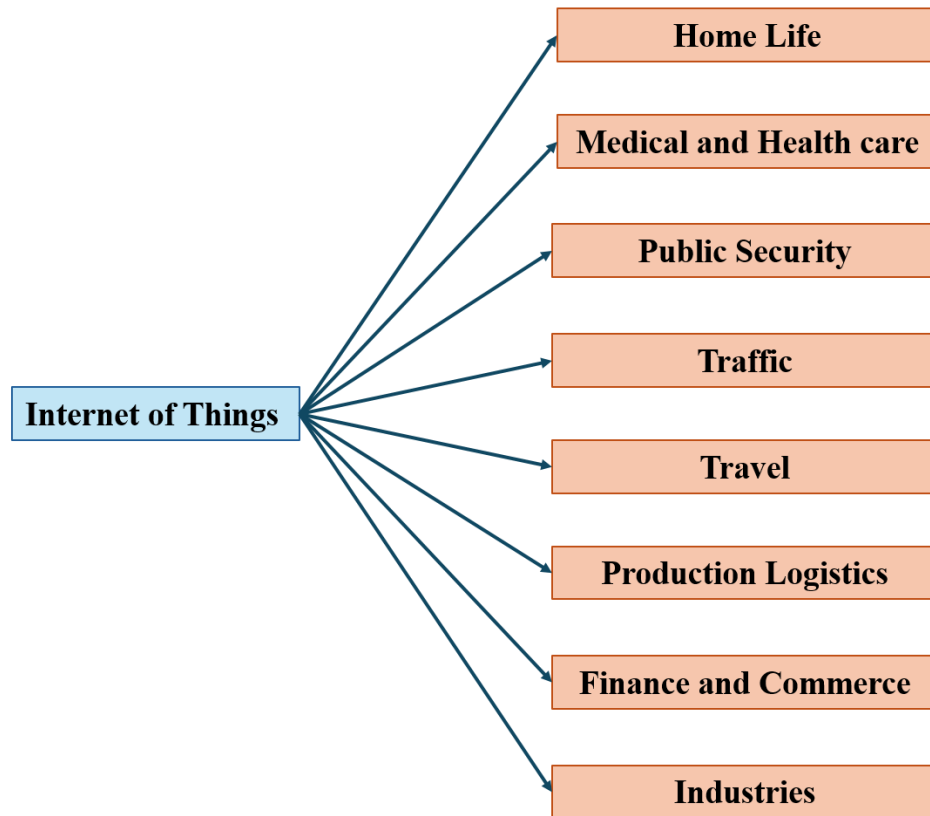


Figure 1. 1: Different aspects of IoT

### 1.3 Limitations of IoT Devices

The IoT has grown quickly and has many advantages, but it also has downsides and limitations of its own. Some of the limitations of IoT device are as below:

#### 1.3.1 Privacy and security concerns

Sensitive data is regularly collected and transmitted by IoT devices. Personal information may be exposed due to data breaches caused by insufficient security measures. IoT is prone to cyberattacks that could jeopardize the confidentiality and security of the data being gathered and shared. If the systems being controlled are vital infrastructure, like power plants or transportation systems, this could result in financial losses, harm to one's reputation/ image, or even physical losses. IoT devices' constant monitoring of users creates privacy concerns because these devices can be collecting private data without the users' knowledge. Getting informed consent of consumers to collect data might be

difficult since they might not realize how much information is collected by connected gadgets.

### **1.3.2 Limited power resource**

Since many IoT devices run on batteries, it's critical to optimize energy consumption. It can be difficult to balance functionality with longer battery life, particularly for devices that need to transmit data often. Maintaining power for large-scale IoT deployments might be logistically difficult and expensive to replace or recharge batteries.

### **1.3.3 Interoperability issue**

IoT systems usually depend on proprietary protocols and technologies, which makes it challenging for various systems to exchange data and connect with one another. This may raise the cost of installing and maintaining IoT systems and restrict their scalability and adaptability. Interoperability issues arise because of the IoT's lack of industry-wide standards. Incompatible communication protocols between devices made by various manufacturers can prevent devices from integrating and communicating seamlessly.

### **1.3.4 High costs**

IoT system implementation can come with significant upfront expenditures, particularly if new sensors, actuators, and communication infrastructure need to be installed. Moreover, IoT system support and maintenance cost is also high, particularly if they need specialist expertise.

### **1.3.5 Analytics and data management**

A huge amount of data are produced by IoT devices. Efficiently managing and evaluating this data presents difficulties, particularly given that certain applications require real-time processing.

### **1.3.6 Data integrity issue**

It is crucial to guarantee the accuracy and correctness of the data generated by IoT devices. Inaccurate information may cause poor decision-making. Ensuring the accuracy and Integrity of IoT-generated data is crucial for informed decision-making, requiring special mechanisms to address potential manipulations.

### 1.3.7 Connectivity and reliability

IoT devices depend largely on network access. Inconsistent or unstable connectivity has the potential to impair communication between devices and centralized systems. IoT applications' reliance on network connectivity exposes them to disruptions, which affects linked devices' ability to respond in real time.

### 1.3.8 Latency issue

There should be as minimum delay as possible in the time-sensitive processes. For certain use cases, however, the latency caused by network connectivity in IoT installations can be troublesome. For example some applications require low-latency communication and network delays may reduce these applications' efficacy.

*Table 1. 1: Limitations of IoT devices and suggested mitigations*

<b>Limitation</b>	<b>Description</b>	<b>Mitigations</b>
<b>Security Concerns</b>	Data Privacy and Security: Inadequate encryption and protection mechanisms may expose sensitive user data. Device Vulnerabilities: Limited computational capabilities make devices susceptible to cyberattacks.	Implement robust encryption, regular security audits, and timely software updates. Prioritize security in device design and address vulnerabilities promptly.
<b>Interoperability Issues</b>	Diverse Standards: Lack of universal communication standards hinders interoperability. Fragmentation: Proprietary ecosystems create silos, limiting collaboration among devices.	Establish and adopt universal communication standards. Encourage industry collaboration to create open ecosystems and interoperable solutions.
<b>Scalability Challenges</b>	Network Congestion: Growing numbers of connected devices can lead to network congestion. Management Complexity: Scaling up deployments requires efficient device management.	Optimize network architecture for scalability. Implement effective device management solutions and update mechanisms.

<b>Limited Power Resources</b>	Battery Life: Energy-efficient design is crucial for prolonged operational life. Maintenance Issues: Managing battery-powered devices at scale presents logistical challenges.	Implement energy-efficient design practices. Explore alternative power sources and improve battery technology. Develop efficient maintenance strategies.
<b>Data Management and Analytics</b>	Data Overload: Large volumes of data require sophisticated management. Data Quality: Ensuring accuracy and reliability of IoT-generated data is crucial.	Employ advanced data management and analytics solutions. Implement data quality checks and validation mechanisms.
<b>Privacy Concerns</b>	Invasive Data Collection: Constant monitoring raises privacy concerns. Inadequate Consent: Users may not fully understand the extent of data collection.	Enhance transparency in data collection practices. Implement robust consent mechanisms and privacy policies.
<b>Regulatory and Legal Issues</b>	Compliance Challenges: Rapid technology evolution outpaces regulations. Liability Concerns: Determining liability for malfunctions or breaches is complex.	Stay informed about evolving regulations. Advocate for clear legal frameworks. Implement comprehensive liability policies.
<b>Reliability and Connectivity</b>	Network Reliability: Dependence on networks makes applications vulnerable. Latency Issues: Some applications demand low-latency communication.	Implement redundancy and failover mechanisms. Optimize network infrastructure. Prioritize low-latency communication for critical applications.
<b>Cost of Implementation</b>	High Initial Costs: Implementation involves significant upfront expenses.	Explore cost-effective IoT solutions. Plan for long-

<b>and Maintenance</b>	Upkeep Expenses: Ongoing maintenance and updates contribute to the total cost.	term sustainability and factor in maintenance costs during budgeting.
<b>Environmental Impact</b>	E-Waste: Rapid device turnover contributes to electronic waste. Resource Consumption: Production and disposal impact resources and the environment.	Encourage recycling programs and responsible disposal. Adopt sustainable manufacturing practices and explore eco-friendly materials.

#### 1.4 Transforming Smart Homes

Recent developments in the IoT and information and communication technology (ICT) have drastically changed the purposes and features of smart homes [11].

Defined as a residence capable of real-time data exchange, a smart home utilizes various connected devices, such as televisions, lighting systems, security system, and refrigerators, to deliver automated and intelligent services [11]. With the help of these interconnected devices, a home-based communication network is created, allowing for smooth communication between the devices and the outside world without the constant need for human interaction [12]. Users can handle and control these different household appliances by configuring user settings and making use of the home network configuration [12]. Notably, two major elements impacting the operation of smart homes are the network environment and the IoT [13].

Multiple IoT devices are being connected wirelessly to the network architecture of smart homes, which previously mainly made up of embedded computers [13]. Users no longer need to monitor individual devices separately because they can now manage their smart home environment both inside and outside of their homes by using the centralized mechanisms via smart phone or tablets. The next generation of mobile communication technology, or 5G, is now being made available commercially. This, together with



industry convergence and hardware development breakthroughs, might lead to even more organized and efficient smart home network designs and architectures.

While initially envisioned as a convenience-driven technology, the evolving capabilities of smart homes have revealed their potential to enhance efficiency, security, and assisted living functionalities. Studies have demonstrated the ability of smart homes to reduce overall electricity consumption, contributing significantly to improved efficiency [14, 15]. Although individual smart home devices may yield modest energy savings, the cumulative impact is substantial.

Smart homes also hold immense potential in the realm of home security. By leveraging various built-in sensors, a smart home system can create a safer living environment [16, 17]. Beyond these core functionalities, smart homes cater to the growing market of ambient luxury living. However, the true transformative power of this technology lies in its potential to assist people with disabilities, the elderly, and patients recovering from illness [18].

Applications-specific systems, such as those that use motion and image recognition, are useful assistive technologies for those with age- or condition-related limitations [19]. Similar to this, virtual reality platforms have started to show up as another possible way to help in such scenarios [20].

A traditional smart house, as seen in Figure 1.2, is usually set up using a centralized architecture. The home gateway serves as the platform using which service providers (SPs) offer residents services. It is connected to the home appliances through the home network. These systems, which prioritize convenience of use and energy efficiency, may have some basic automation and remote control features.

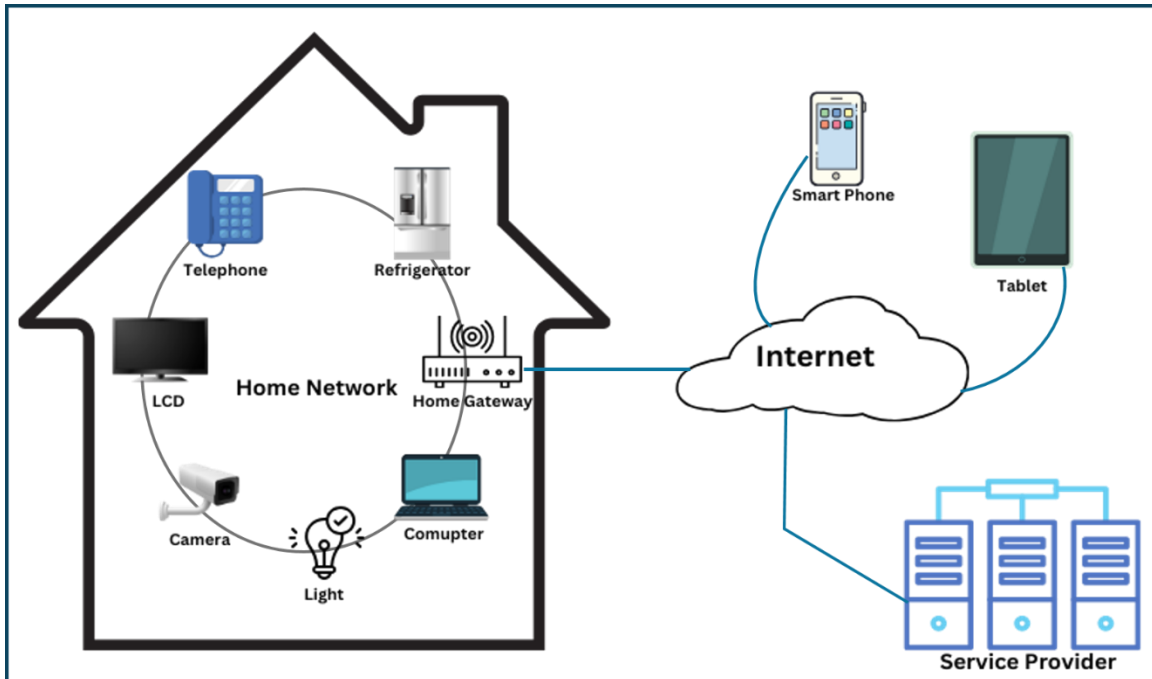


Figure 1. 2: Overview of a traditional smart home system

## 1.5 Security Challenges in Smart Homes

Although there are many advantages to smart homes, security and integrity issues continue to be a major obstacle. Below is a summary of the major issues:

### 1.5.1 Compromised devices

Because connected devices are the foundation of smart homes, a single device's flaw might expose the entire system to risk. These weaknesses can be used by hackers to obtain unauthorized access and possibly take control of household equipment [21].

### 1.5.2 Unfettered access to personal information

Large amount of information about our everyday activities, energy usage, and even behaviors are gathered by smart homes. For attackers, this Personally Identifiable Information (PII) can be a goldmine, possibly resulting in identity theft or specifically targeted scams [21].

### 1.5.3 Limited control over information sharing

Additionally, there are tends to have limited control over data sharing in current smart home systems. As homeowners may have to choose between full disclosure and limited

functionality, this raised the concerns about the indiscriminate exposure of sensitive information [21].

#### **1.5.4 Heterogeneous landscape**

The wide variety of smart devices and systems connected in smart homes results in a disorganized and complex environment. This diversity and heterogeneity raises the possibility of vulnerabilities and makes it challenging to create uniform security procedures and protocols [21].

#### **1.5.5 Data throughout its lifecycle**

The lifecycle of data collected by smart homes includes collecting, processing, storing, and using it. Any stage can be a potential target for attackers attempting to steal or alter data [21].

#### **1.5.6 Exponential growth, exponential threats**

Malicious actors have a wider attack surface in smart homes due to the large number of internet-connected devices. This means that there is a higher chance of privacy violations and cyberattacks that take advantage of vulnerabilities in these electronic devices [22].

These above mentioned challenges show that there is a dire need of stronger security protocols and more stringent data privacy laws in smart home sector/ systems. We can only guarantee that privacy and security threats do not outweigh the comfort and convenience of smart homes by addressing these concerns.

### **1.6 Importance of Data Integrity**

Ensuring data integrity involves making sure that no unauthorized individuals have altered or tampered with the data. Data integrity is critical to the dependability and security of smart home systems. Here are a few methods of maintaining data integrity:

#### **1.6.1 Data validation**

Perform data validation checks at the time data is being entered to ensure that it conforms to already established standards and limitations. Cross-referencing the data with other data sets or dependable sources will help you confirm the accuracy of the data. Verifying

that data is accurate, consistent, and follows specified guidelines or formats is known as data validation. Range checks, format checks, and cross-field validations are a few examples of how to make sure data integrity at the time of entry.

### **1.6.2 Access controls**

Access control systems restrict authorized personnel's ability to access data according to their roles, duties and positions within the company/ organization. By implementing role-based access controls (RBAC), you may lower the risk of unauthorized access and data modification by ensuring that users can only access the data they need to complete their specific jobs.

### **1.6.3 Data encryption**

Encrypt critical and sensitive information while it's being transmitted (with SSL/TLS) and while it's being stored (with disk encryption). To safeguard data in files, databases, and backups, use encryption. Using cryptographic techniques, data encryption converts data into an unintelligible format that can only be unlocked with the right encryption key. Encrypting data offers data security and protection from unlawful interception when it is stored or being transported over networks.

### **1.6.4 Data audit**

For forensic analysis and monitoring purposes, keep thorough logs of all system events, access activities, and data modifications. Audit trails helps to identify suspicious activity and guarantee data accountability by recording user actions, data access, and updates. Examine and review audit trails reports on a regular basis to find any odd or unlawful activity.

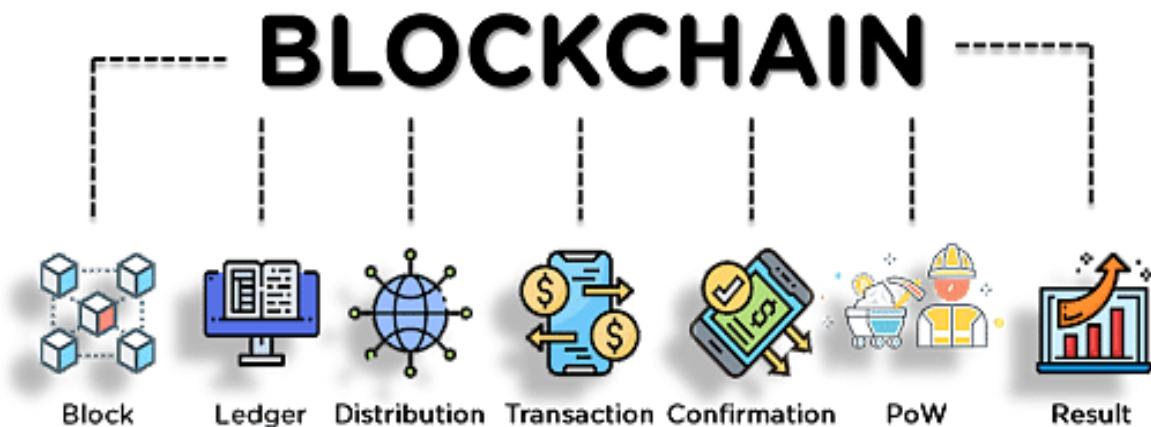
## **1.7 Use of Blockchain for enhancing Security and Integrity of Smart Home Systems**

Smart homes, despite their undeniable convenience, face significant security and privacy challenges. Blockchain technology, known for its secure data management, offers a potential solution.

Blockchain functions as a Distributed Ledger Technology (DLT), distributing data across a network rather than storing it centrally. This makes tampering nearly impossible and enhances security with cryptographic mechanisms like Public Key Infrastructure (PKI).

These characteristics show promise for smart homes: they allow for the sharing of ethical data in home environments by utilizing smart contracts to regulate access, and they provide a more secure environment because of the blockchain's fault tolerance and immutability. Still, there are issues to be resolved, such as security threats and scalability issues with managing the large amounts of data that smart homes generate. Future studies will probably concentrate on reducing these hazards and creating suitable consensus algorithms to fully utilize blockchain technology for safe and private smart homes [22].

Security concerns related to IoT can be addressed with the help of Blockchain technology. It may provide a transparent and safe means of exchanging and storing data. Blockchain technology's decentralized approach to data storage and administration reduces the likelihood of centralized data breaches, which is a major risk in traditional IoT setups. This decentralized approach not only increases security but also allows people more control over their data in accordance with modern privacy regulations. In smart homes, blockchain clearly outperforms centralized systems, especially in terms of data redundancy, reliability, and integrity. Because centralized systems frequently susceptible to single point of failures, they are more subject to data loss and manipulation. However, the decentralized structure of blockchain automatically increases data reliability and adds redundancy. Throughput, processing overhead, and packet delivery ratio (PDR) are examples of factors that show how well blockchain-based systems outperform centralized ones. Blockchain-based systems, for instance, provide significant enhancements in overall system dependability and the reduction of corrupted or missing data instances. Enhancing data redundancy and reliability is a major benefit of blockchain technology in smart homes. An overview of the blockchain workflow is shown in Figure 1.3.



*Figure 1. 3: Overview of blockckchain*

- **Block:** As the name suggests a blockchain is a chain made up of specific data and information blocks. These blocks serve as basic storage units for the blockchain's transaction log. The block header and the block body are the essential parts of a block on a blockchain. A block cannot be removed from the blockchain once it is added.
- **Ledger:** Ledger is a kind of record keeping, where financial transactions are documented. Blockchain is a type of digital ledger that validates and records every transaction that occurs within its network. For instance, the Bitcoin blockchain uses cryptography-secured blocks to record every transaction involving bitcoins.
- **Distribution:** Blockchain is one of the well-known application of distributed ledger technology. The key difference between DLT and conventional centralized ledgers is that each node in the network receives a copy of the ledger, which allows any node to read, edit, and verify the ledger— it is a feature that provides transparency and trust.
- **Transaction:** Any activity undertaken on a blockchain network is represented by a transaction. A contract, agreement, transfer, or asset exchange involving two or more parties is referred to as a transaction. A piece of information kept on the blockchain is called a transaction. Various types of data may be present in it, based upon the intended usage of the blockchain. For example, it occurs when someone gives another person access to a digital asset they own. The transaction itself will always contain

the following information: the amount, the funds' destination, and a signature attestation for validity.

- **Confirmation:** A confirmation shows that the blockchain network has accepted a new block with several transactions in it. A 'confirmation' takes place when a miner successfully adds a new block to the network.
- **PoW:** It is one of blockchain consensus mechanisms in which the computing power is used to verify transactions and add them in blocks which further added to blockchain.
- **Result:** As a result blockchain technology can be used to create an immutable ledger for securing orders, payments, accounts, data, information and other transactions. Blockchain system has a default mechanism to prevent unauthorized transactions and make them consistent.

Enhancing data redundancy and reliability is a major advantage of blockchain technology in smart homes. Blockchain technology is suggested by Siqi He et al.'s study [23] as a decentralized third-party auditor to guarantee the immutability and dependability of data stored in smart homes. By utilizing game theory to improve the effectiveness of verification processes, this method shows how reliable blockchain is at preserving data availability and integrity.

Chunliang Chen et al. in [24] proposed a blockchain-based data integrity verification mechanism for smart homes by using a home gateway to compile and store tag data and information. This system tracks interactions on the blockchain and use homomorphic verifiable tags for verification and has shown to be efficient and reasonably cost effective. The method shows how blockchain technology can be applied to smart home situations to guarantee data integrity and accuracy.

## **1.8 Problem Statement**

Security and privacy issues with smart home systems include data availability, authentication, and integrity. Data integrity refers to the guarantee that the data has not been modified or tampered with by unauthorized parties. The purpose of this research is to address security and data integrity concerns in smart home devices by implementing a blockchain-based architecture. Through the use of a decentralized ledger, this system

seeks to securely store and manage data, improve data processing to reduce latency, and withstand security risks such as fake block injection and DDoS attacks. By using these components, the research presents a potentially significant progression in safeguarding the huge quantity of data produced by smart home appliances. A new architecture is proposed, built, and implemented in order to facilitate this integration. Its performance and efficiency are assessed in various contexts. The results of the evaluation show that the suggested solutions perform better than the ones that are already in place and are more workable and efficient.

### **1.9 Research Objectives**

The main objectives of the thesis are:

- To review the existing literature on smart home systems, blockchain technology, and data integrity challenges and solutions.
- To design and implement a blockchain-based smart home architecture that prevents data forgery and enhance data integrity and security.
- To discuss the advantages and limitations of blockchain technology for smart home systems.

### **1.10 Research Contributions**

The key contributions of this thesis are:

- To provide an architecture that provide data integrity and security in the context of smart homes with blockchain system while maintaining efficiency and effectiveness of the system.
- To close the research gap that exists because there is insufficient research on the architectures that ensures data integrity and security with maintained performance and strength while also taking into consideration the presence of cyberthreats.



### **1.11 Research Questions**

RQ1: How important data integrity and security is for Smart home IoT architectures that uses blockchain?

RQ2: What would be the average latency of transactions on Hyperledger fabric on the smart home architecture that utilizes blockchain?

RQ3: How efficiently and effectively the proposed architecture manages the allocated resources during a transactional activity?

RQ4: What are the open perspectives and future research directions for protecting smart home systems?

### **1.12 Research Significance**

The relevance of this thesis is to contribute to the development and improvement of smart home systems, which are part of the national vision and strategy for digital transformation and innovation. Smart home systems can enhance the quality of life, well-being, and sustainability of the citizens and the society. However, smart home systems also require high security and privacy standards to protect the data and devices from unauthorized access and manipulation. For smart home systems, blockchain technology can offer a decentralized, safe solution that guarantees data availability, integrity, and authenticity. In addition to providing cooperation and better interaction between users and smart home devices, blockchain can also benefit other parties like service providers, regulators, and researchers. Consequently, the thesis can help the country's requirements for improving the security and privacy of smart home systems as well as encouraging the use and integration of blockchain technology in the smart home environment.

### **1.13 Thesis Outline**

The research contributes to address the security and privacy issues related to smart home devices, which are growing more common and prevalent contemporary societies. Although smart home systems can offer users comfort, efficiency, and convenience, there

is a chance that they can be compromised by cyberattacks, manipulations and data breaches.

Data integrity is one of the most important security and privacy requirements for smart home systems, as it affects the quality and functionality of the devices and services. Blockchain is a promising technology that can provide data integrity for smart home systems by using its distributed, transparent, and immutable features. Blockchain can also securely enable peer-to-peer resource sharing and collaboration among smart home devices and users. Using private blockchain for smart home privacy and integrity is relevant, timely, and significant for both academic and practical purposes. The research is organized in following chapter:

- **Chapter 1:** This chapter briefly describes the background of the thesis topic, address the limitations of IoT devices, and introduces the basics of smart home systems and traditional architecture, importance of security and integrity and then possible use of blockchain for ensuring security of smart home systems. At the end some research objectives and contributions are listed along with thesis outline.
- **Chapter 2:** Outlines the current research being done to provide solutions for various smart systems with focused on Smart home Systems.
- **Chapter 3:** Describes the blockchain technology in detail and which all platforms are available and their basic features.
- **Chapter 4:** Outlines the details of approach taken, the recommended solution, and the suggested architecture.
- **Chapter 5:** This chapter describes the effectiveness of proposed solution and analysis of suggested methodology.
- **Chapter 6:** This chapter wraps up the thesis by highlighting the contributions, discussing the shortcomings, and suggesting directions for further investigation to improve the system.

## CHAPTER 2

### RELATED WORK AND LITERATURE REVIEW

#### 2.1 Introduction

In this chapter, some of the most significant challenges that the smart home systems are discussed. A detailed analysis of what has previously been done and what has to be taken into consideration, along with the various current mitigations and processes/methods, their applicability, and functions, are all described in detail. At the end, a comparison table listing already done work, challenges identified and mitigation strategies are provided.

Research in smart home security has extensively explored the challenges faced by different stakeholders, including vendors, installers, and homeowners, when integrating IoT devices into their homes. These studies have also investigated solutions to mitigate these challenges. Some recent research proposes individual architectures and frameworks to secure smart home IoT devices, while others advocate for combining various technologies to strengthen device security and ensure data privacy. Notably, current research identifies four key areas where security and privacy vulnerabilities are most prevalent in smart homes: the devices themselves, communication channels, the services used, and the applications connected to these devices. Furthermore, researchers have identified several key security concerns in IoT-enabled smart homes. These include protecting user privacy, ensuring compatibility between different devices, verifying user identities, and establishing secure connections throughout the entire data flow, especially when malicious actors might try to disrupt the system. In response to these challenges, some studies propose secure end-to-end cryptographic frameworks as a potential solution that could comprehensively address these security vulnerabilities [23].

## **2.2 Smart Homes**

Smart homes are setups that connect several home equipment and gadget in a house over the IoT allowing to monitor and control remotely. With intelligent home devices, as an instance, you can use your voice assistant or cellphone to manipulate/ control your home's lighting, entertainment, protection, and temperature remotely. Because of latest advancements in ICT and IoT, smart home functions and roles are constantly evolving [24].

Global marketplace studies firm Gartner predicts that by the 2025, there can be 75 billion smart home devices in use. Stratecast research indicates that by 2025, the worldwide smart home industry is expected to develop at a rate exceeding \$7 billion [25].

A private home that has instant data transmission and reception is called a "smart home." It provides automated and intelligent services via a range of home appliances such as refrigerators, TVs, and lighting. These appliances, gadgets and devices connect to external settings as part of the automated home communication system [26].

Because unencrypted passwords are frequently used on these smart home gadgets' wireless networks, hackers target them primarily as a means of launching distributed denial-of-service (DDOS) attacks [27].

## **2.3 Data Integrity**

An essential component of smart home systems is data integrity, which includes data correctness and preservation during data processing, transmission, and storage in these contexts [28].

In traditional systems, encryption and secure protocols for data transfer and storage are commonly used to protect data integrity. For data transit and storage, this may involve encrypting the data and utilizing (TLS) transport layer security or secure socket layer (SSL). In order to protect data from unwanted access, cloud providers may also use security tools including intrusion detection systems, firewalls, and access controls [29].

Some of the reasons that why data integrity is important are as following:

- **Accuracy and reliability:** By assuring that the data being utilized is accurate and consistent, data integrity helps to ensure the correctness and dependability of information.
- **Trustworthiness:** Maintaining data integrity contributes to increased trust in the information and the systems that produce and use it.
- **Compliance with regulations:** Most of industries and fields follow strict standards, rules and regulations that must be met with regards to data management, comprising data integrity. Considering data integrity enables firms to comply by these rules and guidelines.
- **Avoiding inherent consequences:** Data that is faulty or compromised can have harmful effects, including poor decision-making, reputational damage, legal liability, and economic/ financial losses.
- **Efficient processes management:** The maintenance of data integrity facilitates the efficient and effective operation of systems and processes.
- **Securing/ protecting sensitive information:** In most of the cases, sensitive information that needs to be protected may be found in data. By preserving data integrity, you may help make sure that this information is safe and shielded from unwanted access or change.

## 2.4 Blockchain Technology

Blockchain technology, identified for its decentralized and tamper-evidence nature, offers giant blessings in improving the safety, confidentiality, integrity and privateness of smart houses. In the contemporary age of the IoT, clever houses are being increasingly related, but they face vital demanding situations in records integrity and privateness protection. Blockchain's software on this area promises to transform how information is stored, shared, and secured.

Eghmazi et al. (2024) discover the integration of blockchain with IoT, based totally on Hyperledger Fabric offering a solution blockchain as a provider (BaaS) utility. This software introduces a new architecture and facts along with public and personal key

encryption, addressing the essential protection and privacy concerns in IoT applications [30].

Similarly, Yao and Liu (2023) recommend a blockchain-based public audit scheme for newer and better home structures, using blockchain and IPFS to make sure data integrity and safety, supplying an extra efficient answer than centralized servers [31].

## **2.5 Blockchain for Data Integrity and Security**

Blockchain technology's potential in making sure information integrity and safety in clever homes is widespread. Maintaining and ensuring the correctness, completeness and statistics consistency at some stage in its complete lifecycle is known as records integrity. Data integrity is provided by means of blockchain's immutable ledger, which makes sure that once facts is recorded, it cannot be modified without the community's approval.

Kumar et al. (2023) introduce a blockchain-based totally new solution for facts provenance, integrity, and protection in decentralized sharing ecosystems, advocating for using high-overall performance structures like Solana for facts provenance monitoring [32].

## **2.6 Trends and Challenges in Cyber-Security for Smart Home IoT Devices**

Aaasha Aldahmani et al. (2023) provide a detailed analysis of the challenges, requirements, and trends in cyber security for IoT devices used in smart homes in [33]. They focus on the vulnerabilities and security concerns of smart home technology, highlighting the need for robust solutions to protect these increasingly interconnected environments. The paper emphasizes the evolving nature of cyber-threats and the necessity for adaptive security measures to ensure the safety and privacy of smart home users.

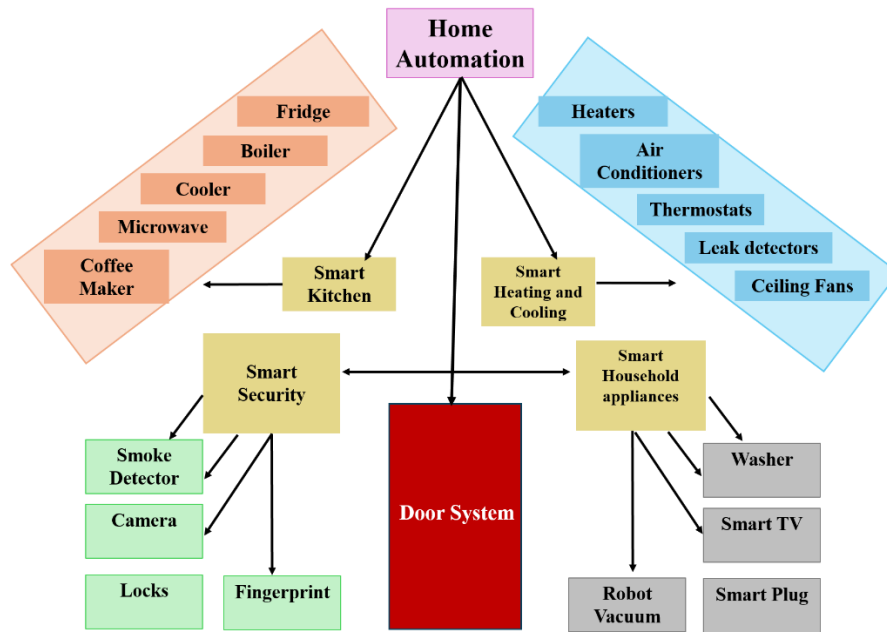


Figure 2. 1: Smart home devices communications

## 2.7 Limitations of Traditional Data Integrity Mechanisms

Following are the reasons, in smart home systems, conventional data integrity techniques including hashing, checksums, cryptographic algorithms, error-detecting codes, data redundancy, and backups might not be suitable.

- **Latency and bandwidth:** Usually, data processing and storing takes place at the network's edge near the data source. This method may result in higher latency and limited capacity, which could pose problems for data integrity systems that depend on large-scale data processing or transmission.
- **Resource limitations:** There may be limitations on the processing power, memory, and storage of the edge devices, which include gateways and IoT devices. These limitations can make it difficult to execute data integrity procedures that need a lot of processing power or storage.
- **Centralized architecture:** Conventional Smart Home Systems and Technologies process and store data via centralized servers or cloud-based systems. These systems, which prioritize convenience and energy efficiency, may have some basic automation and remote control features.

- **Scalability issue:**It might be difficult to scale data integrity procedures to manage the enormous quantity of data produced and processed by several edge devices in smart home networks.
- **Privacy issue:** Through sensors and networked apps, smart devices frequently gather enormous volumes of personal data. Concerns over data privacy arise from the possibility of sharing this information, which includes our daily schedules, preferences, and even biometric data, with outside parties due to centralized data storage.

Considering the challenges posed resource-constrained nature of IoT devices and centralized architecture, alternative data integrity techniques might need to be developed. These mechanisms should be made to function well in highly dynamic and resource-constrained contexts, with an emphasis on latency, bandwidth, and compute efficiency. This paper is assuming the importance of smart home security and privacy aims to address complex problem of data integrity and security in smart homes.

## 2.8 Possible Attacks

- **Unauthorized access**  
Attackers may obtain illegal access to the central control system or smart home appliances.
- **Device exploitation**  
Device exploitation means taking advantage of software or firmware flaws in smart home devices.
- **Phishing and social engineering**  
Deceiving people and users into revealing personal information, such as their login credentials and personal information
- **Denial of service (DoS) attacks**  
An attempt to prevent a computer or other device from operating normally so that the intended users cannot use it is known as a denial-of-service (DoS) attack. 96% of devices involved in DOS/ DDOS are IoT devices.



- **Message modification attacks**

Unauthorized changes made to messages during transmission or storage with the goal of altering or jeopardizing the integrity of the data are referred to as message modification attacks. Major consequences may include sensitive data being compromised, unauthorized access, or false information being spread.

- **Eavesdrop**

Attackers use network communication and intercepts it to observe or take data without altering it. Eavesdropping is quite simple as smart homes' servers and devices interact with one another over the internet.

- **Masquerading**

Masquerade attacks are cyberattacks that use a digital signature, network address, certificate, or fake, spoof, or stolen user identity of a device to trick digital infrastructure and gain access to systems or authorization to perform specified privileged operations.

- **Passwordattacks**

By guesswork, social engineering, sniffing the network connection, or getting access to a password database, a hacker can obtain a user's password information.

- **Replay attacks**

One type of cyberattack known as a replay attack occurs when an attacker intercepts data that has already been collected and retransmits it. Replay attacks try to fool a system by playing back legitimate data as though it were a fresh, authentic message.

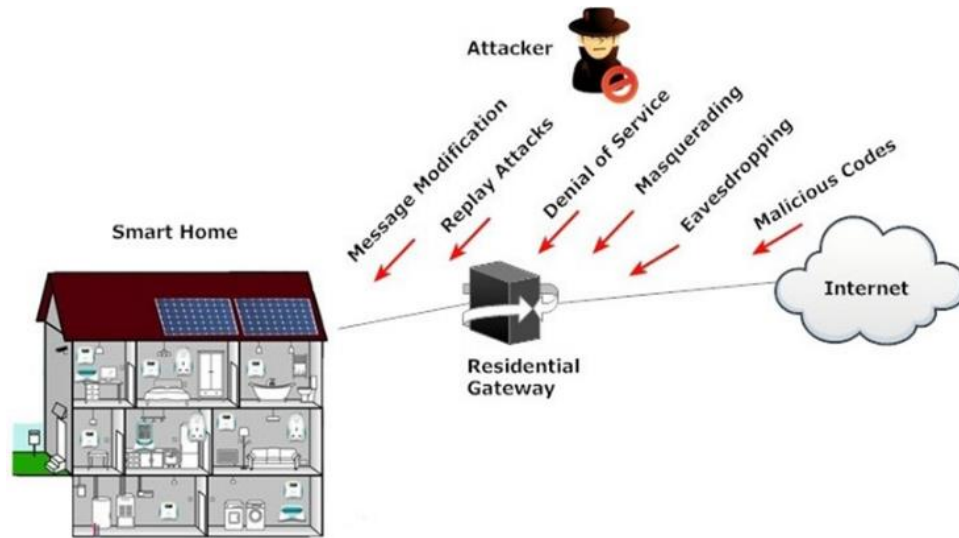


Figure 2. 2: Attacks on Smart Home Systems

## 2.9 General Approaches for Security in IOT Environments

Some of the prominent approaches for ensuring security of IOT environments are given below:

### 2.9.1 Cryptographic Measures in IoT Environments

Traditional cryptographic techniques have proven essential for safeguarding the confidentiality and integrity. Building on established cryptographic techniques like AES and ECC, in [34] author explores lightweight cryptography (LWC) primitives that are particularly well-suited for resource-constrained systems.

A number of studies [35–37] have looked into using hybrid cryptography in blockchain applications. These methods combine asymmetric cryptography based on Elliptic Curve Cryptography (ECC) with lightweight symmetric techniques like variations of AES and DES. Because ECC requires a smaller key size for the same security levels as RSA, it is a more effective solution for situations with limited resources. Features like identity-based encryption, searchable encryption, privacy by design, and distinct data-dependent keys are made possible by this hybrid method. These methods thereby uphold the least

privilege principle, confidentiality, shared transparency, improved computer efficiency for secure communication, and personal data sovereignty. They also preserve privacy when querying data. While public-key cryptography has benefits, there are some limitations also. Although it safeguards the privacy of messages encrypted with your public key, as highlighted in [38], there are situations in which it can be subject to impersonation attacks.

These attacks use weak Public Key Infrastructure (PKI) to spoof digital certificates and take the identity of trustworthy users. Simpler and more effective secret-key cryptography may be adequate in certain situations. It's crucial to keep in mind that while public-key cryptography safeguards the data it is intended to encrypt, breaches cannot be avoided if your private key is compromised. All of your messages can be decrypted by an attacker if they manage to obtain your private key.

### **2.9.2 Access control-based approach**

Researchers have suggested a number of methods for managing access control in smart homes, taking into account the varying degrees of trust that many IoT devices have in these environments. A viable approach that is gaining popularity is using a private local blockchain to manage access to these devices. With the help of this technology, permissions can be managed securely and dispersed, guaranteeing that only authorized parties can communicate with particular smart home devices [39].

Private local blockchains offer a promising approach for access control in smart homes. They can establish distributed trust and privacy for device interactions. However, this approach introduces trade-offs. The additional "overlay tier" responsible for blockchain operations can introduce latency (delays) in communication. Additionally, storing public keys off-chain might create vulnerabilities if attackers exploit transactions involving these keys. Another approach, explored in [39], repurposes blockchain as a trustless automated access control moderator. As a result, a central authority has been eliminated (TTP). It uses a Distributed Hash Table (DHT), an off-chain key-value store, to store user data, including location data. However, there are disadvantages to this strategy as well. The Proof of Work (PoW) consensus method, which can be expensive and time-consuming to perform computationally, is used by certain blockchains. As a result, it is

less appropriate for smart home setups with limited resources. In order to solve access control issues in cloud environments, the profile-based access control model (PrBAC) was established in [40]. Data owners (DOs) used to have to be online all the time to control user access permissions to data stored in the cloud. By providing authorized users with a secret key or password just once during the initial decryption key request, PrBAC simplifies this process. As a result, DOs are no longer required to be online constantly. Although, PrBAC also provides advantages such as decreased data redundancy and access times and costs. But there are drawbacks to this strategy. There is still room for improvement in the system's overall security and secrecy. Furthermore, because of issues with permitted frameworks for ethical disclosure, keeping sensitive data in the cloud is not optimal for scenarios involving the ethical disclosure of private data in remote management within smart home ecosystems. Inter Planetary File System (IPFS) shows itself as a better option in certain situations. IPFS provides a decentralized storage option with possible links to blockchain technology, yet it has certain characteristics (ACID features) in common with conventional databases. This dispersed strategy more closely matches the application's privacy-related needs.

This research looks into how resource-constrained IoT devices in smart homes can safely manage data sharing through the use of blockchain technology and a lightweight Proof-of-Authority (PoA) consensus mechanism [41]. The benefit of PoA is that it can process transactions more quickly because it does not require the computationally demanding mining phase that is included in other consensus mechanisms. PoA generates blocks using a pre-defined set of validators, which allows for high scalability. Compared to alternative consensus processes, this predictable approach enables faster transaction processing.

A privacy-preserving method for location sharing is provided via attribute-based access control using smart contracts [42]. However, because of the intricate data storage structure, it is inefficient for queries. However, the permissioned blockchain method described in [43] achieves traceability with privacy protection for access policies and uses Practical Byzantine Fault Tolerance (PBFT) for consensus. This method uses Message Authentication Codes (MAC) for effective home gateway authentication and

integrates blockchain with group signatures for anonymous group member authentication. Although it provides traceability and certain privacy capabilities, fine-grained access control is absent. Furthermore, as network size increases and transmission cost rises, PBFT becomes inefficient due to its dependence on computations akin to Proof-of-Work (PoW). Furthermore, certain effective authorization techniques rely on centralized servers, which exposes them to single point of failure (SPOF) attacks like Denial-of-Service (DoS) attacks. Additionally, the use of ECDSA for verification and anonymity in smart contracts provides limited identification assurance.

### **2.9.3 Blockchain based approach for IoT security**

Blockchain technology is acting as a catalyst for Industry 4.0, transforming how businesses operate. It offers a secure and transparent platform for data exchange, authentication, asset tracking, and access control through smart contracts [44, 45]. These self-executing contracts eliminate the need for intermediaries and reduce human error, streamlining processes. Additionally, the rise of permissioned blockchains, like Ethereum, enables seamless integration between different blockchain systems, fostering greater efficiency and trust within Industry 4.0 ecosystems [46-48]. This decentralized approach revolutionizes the traditional, centralized systems across various sectors, including healthcare, finance, supply chain, and manufacturing [49-50].

VeChain [51] exemplifies how blockchain technology can be harnessed for Industry 4.0 applications. Particularly in supply chain management, manufacturing, and transportation, VeChain offers a value-driven approach. By monitoring ownership and authorization along the entire value chain, it guarantees the origin of the product and, in the end, makes value exchange safe and transparent. Proof-of-Authority (PoA) is a good consensus method for permissioned blockchain applications in smart homes, according to [52], which makes a similar suggestion. Because PoA is lightweight, it can be used in contexts with limited resources. PoA further provides a safe value chain for tracing authorization, ownership, and provenance. Through this value exchange, unwanted access (Sybil assaults) that can jeopardize confidentiality in a smart home authorization system can be lessened. PoA-based blockchains are not immune to censorship, despite the fact that they have advantages over Proof-of-Work (PoW) systems like faster transaction

speeds and less energy usage. In contrast to anonymous users on permissionless PoW blockchains, PoA is dependent on pre-selected, reliable validators. This concept aligns well with permissioned blockchains like Hyperledger, where trusted nodes are assigned validation rights.

#### **2.9.4 Emergence of DLTs for IoT security**

The limitations of blockchain technology, particularly its scalability and data privacy constraints, have prompted exploration of alternative distributed ledger technologies (DLTs) for data security. Holochain, a new DLT approach, is gaining traction. Unlike blockchain, Holochain utilizes an agent-centric model where each participant maintains their own chain. This design offers potential benefits for scalability, data sovereignty, and efficiency compared to traditional blockchain systems [53, 54].

Beyond healthcare, Holochains unique capabilities can address security and privacy concerns in the smart home sector [55]. While blockchain offers undeniable value in data integrity and transparency, Holochain presents a viable alternative or complementary solution for optimizing data privacy and security in healthcare and smart home ecosystems [56, 57].

While Holochain offers promising features for smart home data security, it's crucial to acknowledge that every technology has its pros and cons [58]. Permissioned blockchain with Proof-of-Authority (PoA) can be beneficial in specific scenarios. For instance, established infrastructure, easier integration with existing systems, and specific security guarantees might favor PoA-based approaches. Ultimately, the choice between Holochain and PoA depends on the specific requirements of a use case.

Similarly figure 2.3 summarizes different approaches of IoT smart security Environments.

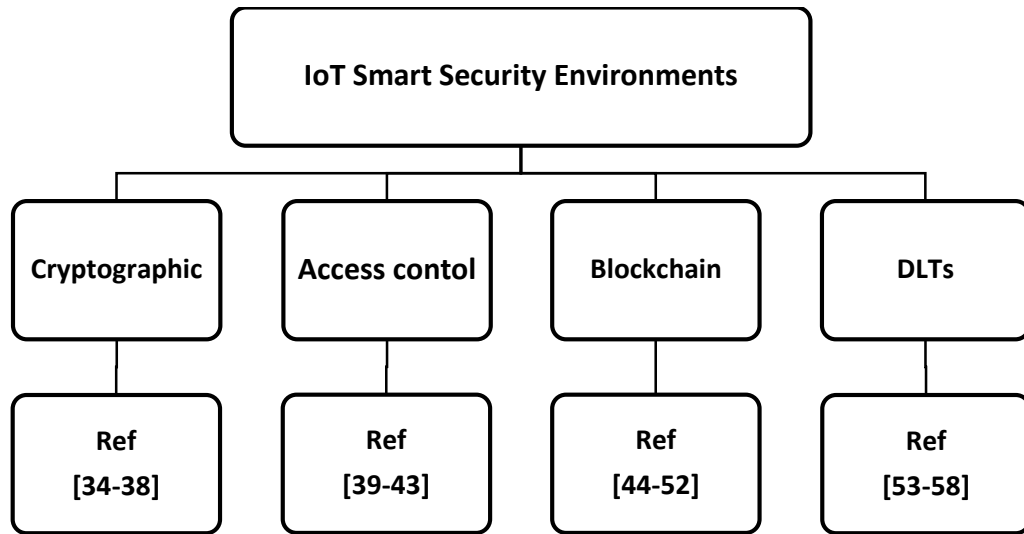


Figure 2. 3: Different Approaches in IoT Smart Security Environments

## 2.10 Literature Analysis

Data integrity is the property of data being accurate, consistent, and reliable over its entire lifecycle. Data integrity is essential for smart home systems, as it ensures that the data collected and processed by IoT devices are not tampered with, corrupted, or lost. Several things may impact data integrity, including hardware malfunctions, network outages, hostile assaults, and human mistake. Data integrity must therefore be safeguarded by applying the proper methods and procedures. Blockchain technology has been suggested as one method of maintaining data integrity in smart home systems. Using agreement protocols and cryptographic techniques, blockchain is a kind of shared database that securely and transparently records transactions. By preventing data modification, ensuring data accessibility, and tracking data provenance, blockchain can guarantee data integrity. Through the use of smart contracts, authentication, and encryption, blockchain can also enhance data security and privacy. Numerous scholarly articles have examined the integration of blockchain technology into smart home systems, utilizing diverse approaches and designs. These studies show the viability and effectiveness of blockchain technology for data security in smart home systems, along with the difficulties and possibilities for further investigation. Eghmazi et al. (2024) discover the integration of blockchain with IoT, based totally on Hyperledger Fabric

offering a solution blockchain as a provider (BaaS) utility. This software introduces a new architecture and facts along with public and personal key encryption, addressing the essential protection and privacy concerns in IoT applications [59]. Zhicheng et al. in 2023 proposed a practical method based on blockchain and employing situation-aware access management to enhance the security of smart homes [60]. The author in [63] addresses the security vulnerabilities by developing a blockchain based smart home gateway network to reduce gateway based attacks by using the ethereum blockchain. Table number 2.1 contains the detailed literature study.

*Table 2. 1:Summary of literature*

<b>Ref</b>	<b>Year</b>	<b>Purpose</b>	<b>Findings</b>	<b>Technology</b>	<b>Blockchain Stores</b>	<b>Language Used</b>	<b>Limitations</b>
[59]	2024	Blockcha in-as-a Service for challenge s in smart devices	Evaluated in actual scenarios for enhanced security and privacy.	HLF	Credentials, Public/private key	Hyperledg er Caliper	Implementat ion is extensively complex.
[60]	2023	Access Control Mechanis m	Blockchai n used for situation aware access manageme nt	Private Blockchain	User and device interactions	N/A	Limited details for addressing system complexitie s



[61]	2022	Securing data within an IoT architecture using a blockchain approach	Concept of a smart home using blockchain is proposed	EOS	Information is gathered and stored within EOS	N/A	Resource intensive architecture
[62]	2021	A novel approach to securing smart home networks	For monitoring IoT-based smart home devices using private blockchain	HLF	Monitoring logs or transitional information.	N/A	No discussion on cyber threats
[63]	2020	Blockchain with Machine learning for smart home security	Enhanced Anomaly Detections and data security	Ethereum	Device Status and Security data	Solidity, Java	Limited details of proposed approach
[64]	2020	Smart home security using	Addresses security concerns for	Ethereum	Environmental and monitoring data	Java, Kotlin	No discussions on data privacy.

		Blockcha in	security in IoTs				
[65]	2020	Secure Smart Home Gateways and prevent Data forgery	Blockchai n is utilized in smarthome gateways	Ethereum	Device status and Preferences	GO	Highlights only a specific area in smart homes
[66]	2020	Blockcha in for smartho me security	Enhancing Secure communic ation and temper proof logs	HLF	Energy Consumptio n Data	Java	Limited Technical details
[67]	2020	HomeCh ain, blockchai n-based system for secure mutual authentic ation.	Smart home environme nts, architectur e with enhanced authenticat ion	Ethereum	Device control and security data	N/A	Scalability, for resource constraints environmen ts.
[68]	2020	Securing the overall smart	shows feasibility and effectivene	HLF	Environmen tal and monitoring data	N/A	Proposed framework is technically

		home network using Blockchain	ss of blockchain to enhance security				complex
[69]	2020	Blockchain and consensus mechanisms to manage smart applications	Enhanced security and decentralized management	HLF	Security Event data	N/A	Security challenges in implementing
[70]	2019	Privacy scheme for smart homes.	Provides differential privacy especially in Smart homes.	Ethereum	Device and User data	GO	No discussions on Cyber Attacks
[71]	2019	Limitations and challenges related to the integration of	Discusses benefits of combining blockchain with edge computing .	Ethereum	Device control and automation	N/A	No discussions on potential cyber threats.

		blockchain					
[72]	2019	Aspects of IoTs in context of smart environments.	Highlights challenges and solutions to IoT deployments in smart environments.	Ethereum	Device status and preferences	N/A	May have interoperability issues.

## CHAPTER 3

### EXPLORING BLOCKCHAIN PLATFORMS

#### 3.1 Overview

Blockchain technology is a distributed ledger system that securely records transactions on a decentralized computer network. Basically, a blockchain is merely a collection of blocks, each containing a list of transactions. These transactions are received collectively, timestamped, and encrypted. The word "blockchain" emerges because blocks are added to the existing chain in the order that they are completed, creating a linear sequence of blocks. Important blockchain components are:

##### 3.1.1 Decentralized

Traditional databases are centralized, meaning that all of the data is managed and kept on a single server by one person. In contrast, a decentralized network of computers, or nodes, is used by blockchain. The entire blockchain is replicated on each node, eliminating the possibility of a single point of failure. This decentralization improves security and eliminates the need for middlemen.

##### 3.1.2 Consensus Mechanism

Consensus mechanisms are employed to validate transactions and preserve the blockchain's integrity. By using these protocols, all nodes are able to agree on the blockchain's present state. Several well-known examples of consensus algorithms are Practical Byzantine Fault Tolerance (PBFT), Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Proof of Stake (DPoS).

##### 3.1.3 Cryptographic Hash

A blockchain is made up of a series of linked blocks, each of which has a distinct cryptographic hash of the one before it. This hash guarantees the blockchain's immutability and functions as a digital fingerprint. A block's hash would change with even a small modification in its data, indicating that the block has been tampered with right away.

### 3.1.4 Smart Contracts

Smart contracts, which are self-executing, contain clear contract requirements embedded into their code. These contracts automatically take effect and enforce their terms when certain requirements/ conditions are met. The use of smart contracts on blockchain platforms like Ethereum or any other platform enables to develop decentralized apps (dApps) and use cases including supply chain management, voting systems, and decentralized finance (DeFi).

### 3.1.5 Security and Transparency

Blockchain makes transactions transparent by enabling anybody to see the complete history of transactions. Transactions are transparent, but they are also pseudonymous, which means that cryptographic addresses—rather than user names—are used to identify users. Furthermore, security is maintained by blockchain's cryptographic protocols, which make it very impossible for bad actors to modify or falsify transactions.

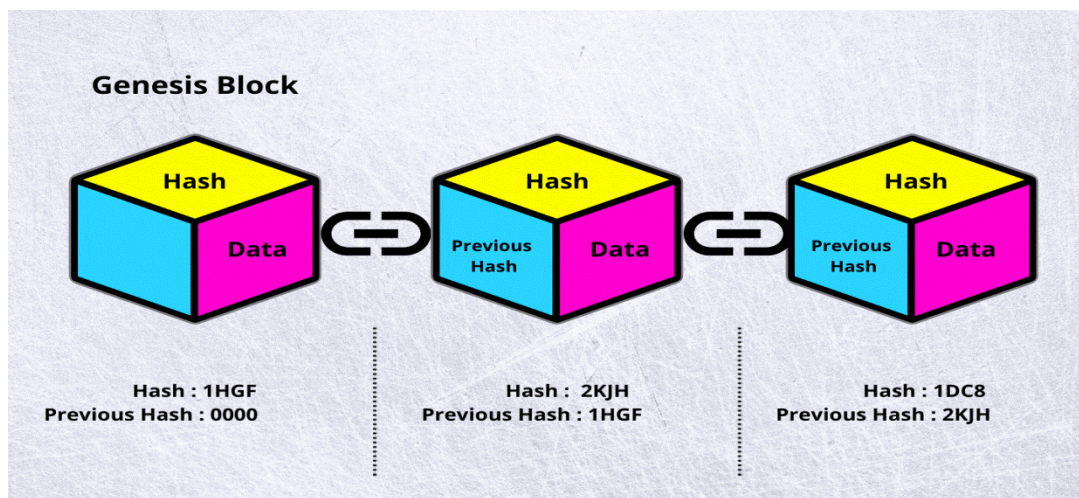


Figure 3. 1: Basic blockchain concept

## 3.2 Distributed Ledger Technology

DLT is an umbrella term for different types of technologies and blockchain is one of them. Other types of DLT include directed acyclic graph (DAG), hashgraph, and holochain. In other words, not all distributed ledgers are blockchains, but all

blockchains are distributed ledgers. A distributed ledger is an electronic log or database that is shared voluntarily and synchronized across multiple locations, organizations, or regions, and that is accessible to a large number of individuals.

### 3.3 Benefits of Blockchain

Some significant benefits of blockchain technology are as under:

- **Security:** Blockchain protects data using cryptographic procedures and techniques, which makes it extremely resistant to fraud and hacking.
- **Transparency:** Because all network users can see transactions on the Blockchain, accountability and transparency are increased.
- **Decentralization:** Blockchain functions on a decentralized network, as opposed to conventional centralized systems, minimizing the possibility of a single point of failure.
- **Immutability:** The Blockchain ensures the integrity of historical records by making data nearly impossible to modify once data is recorded.
- **Smart Contracts:** Smart contracts automate procedures and eliminate the need for intermediaries by executing agreements based on predetermined rules. These are self-executing programs that run on predefined conditions.
- **Cost-Efficiency:** Blockchain eliminates the need of intermediate parties/ entities, which lowers transaction costs and expedites procedures. It saves time and money.
- **Global Accessibility:** Due to its worldwide business processes, blockchain is available to everybody with an internet connection.
- **Data Integrity:** Data validity can be verified using blockchain, which makes it incredibly useful for supply chain management and traceability.
- **Innovation:** Blockchain's ability to provide novel solutions to persistent issues has encouraged innovation in a number of sectors, including banking, private, smart homes and healthcare.
- **Tokenization:** Blockchain makes it possible to create digital assets and tokens, creating new avenues for investment and fundraising.

### 3.4 Types of Blockchain

Permissioned and permissionless blockchains are the two primary types of blockchains. Blockchains without permission, such as Ethereum and Bitcoin, allow everyone to validate transactions and to take participation. On the other hand, permissioned blockchains limit access to specific participants, which makes them appropriate for enterprise applications where control and privacy are crucial.

#### 3.4.1 Permissioned vs permissionless blockchain

Following table shows the detailed comparison of both techniques:

*Table 3. 1: Permissionless vs Permissioned blockchain*

Ser		Permissionless	Permissioned
1.	Overview	Anyone can communicate on this open network and take part in consensus validation. Entirely decentralized among unknown individuals and parties.	Closed and restricted network. Known parties participate in consensus validation and designated parties interact with communication. Partially distributed among known parties, or partially decentralized.
2.	Key Features	<ul style="list-style-type: none"> <li>• Complete transparency of transactions as it is based on open source protocol.</li> <li>• Development is open source</li> <li>• Generally anonymous (But may have exceptions)</li> </ul>	<ul style="list-style-type: none"> <li>• Transparency is controlled, based on different organizations' goal.</li> <li>• Development is done by private entities</li> </ul>



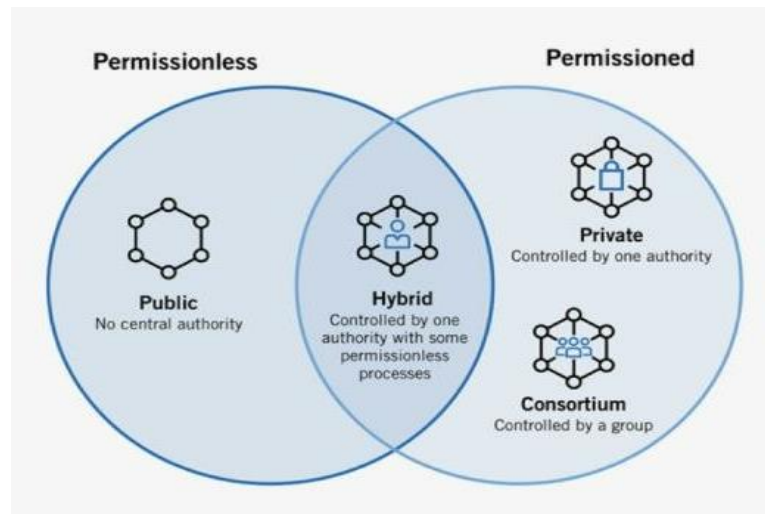
		<ul style="list-style-type: none"> <li>• Technological limitations or innovations affect privacy.</li> <li>• There is no central authority</li> <li>• Often incentives with digital assets or tokens.</li> </ul>	<ul style="list-style-type: none"> <li>• It is not anonymous</li> <li>• Privacy is determined by governance decision.</li> <li>• A private group authorizes decisions rather than a single authority.</li> <li>• Can or cannot use digital assets or tokens</li> </ul>
3.	Benefits	<ul style="list-style-type: none"> <li>• <b>Increased decentralization</b>, which increases network access of users.</li> <li>• <b>Extremely Transparent</b>, which helps with speed and reconsolidation between different regions and nationalities</li> <li>• <b>Resistance to censorship</b> because of accessibility and involvement from anonymous parties</li> <li>• <b>Security resilience</b>, as it is expensive and difficult to compromise 51% of the network and attackers cannot target a single</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Gradual decentralization</b>, but the participation of several businesses reduces the dangers associated with more centralized structures.</li> <li>• <b>Stronger information privacy</b> due to permission-based access to transaction data.</li> <li>• <b>Highly configurable</b> to individual use cases via a variety of configurations, modular components, and hybrid integrations</li> <li>• <b>Faster and more scalable</b> since transaction verification and consensus are managed</li> </ul>

		repository.	by fewer nodes.
4.	Pitfalls	<ul style="list-style-type: none"> <li>• <b>Reduced energy efficiency</b> due to the resource incentive provided by network-wide transaction verification.</li> <li>• <b>More difficult to scale</b> and slower because large volumes can cause problems with network-wide transaction verification.</li> <li>• <b>Less control</b> over user privacy and information.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Limited decentralization</b> due to the higher possibility of corruption and collision in networks with fewer participants.</li> <li>• <b>Override risk:</b> owners and operators have the power to override or alter the mining, consensus, or immutability rules.</li> <li>• <b>Less transparent</b> to outside scrutiny since operators set privacy restrictions and there are fewer players.</li> </ul>
5.	Market Traction	<ul style="list-style-type: none"> <li>• Peer to peer</li> <li>• Business to consumer</li> <li>• Government to citizens</li> </ul>	<ul style="list-style-type: none"> <li>• Business to business</li> <li>• Business to consumer</li> <li>• Governments to organizations</li> </ul>

### 3.5 Public vs Private Blockchain

Blockchains can be public and private and have different level of control, transparency, and accessibility features. Because public blockchain networks are transparent and open to all, anybody can join, validate transactions, and take part in the consensus mechanism.

However, because private blockchains are only available to authorized users, they offer more privacy and control. Moreover, private blockchains are more popular among businesses that need stringent security measures, public blockchains are more popular with cryptocurrency users and promote decentralization.



*Figure 3. 2: Types of blockchain*

**Consortium blockchains:** These blockchains are semi-decentralized networks in which transactions are validated by a pre-selected set of participants. These networks are appropriate for sectors that need to strike a compromise between openness and privacy since they are more scalable than public blockchains and retain some degree of control.

**Hybrid blockchain:** A hybrid blockchain combines the two unique characteristics of public and private (permissioned) blockchains in a unique way. It seeks to combine the advantages of both while resolving some of their particular limitations. A hybrid blockchain design has sections of the network that are private and run by certain corporations, and sections that are decentralized and accessible to the general public.

Table 3. 2: Comparison of Private and Public blockchain

Ser.	Features	Private Blockchain	Public Blockchain
1.	Permissioned Access	Yes	Yes
2.	Participation	Limited	Open
3.	Decentralized	Yes (For part of Organization)	Yes
4.	Same Ledger	No	Yes
5.	Anonymous	No	Yes
6.	All Node Verification	No (Endorsing Nodes only)	Yes
7.	Consensus Mechanism	Centralized	Decentralized
8.	Governance	Centralized	Decentralized
9.	Transaction Speed	Faster	Slower
10.	Transparent	No	Yes
11.	Scalability	Higher	Lower
12.	Privacy	Higher	Lower
13.	Smart Contract	Yes	Yes
14.	Immutability	High	High
15.	Native Token	Not necessary	Yes
16.	Energy consumption	Less	More
17.	Attacks	No possibility or risk of a minor collision. Every validator is identified and known.	greater possibility or risk of a collision or a 51% attack
18.	Examples	Hyperledger Fabric, Corda, R3 (Banks), EWF (Energy), B3i (Insurance)	Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar, Steemit etc.

### 3.6 Challenges Associated with Public Blockchain

Major challenges faced with public blockchain are as described below:

- **Scalability issues:** Scalability is one of the main issues public blockchains face because of their limited capacity to handle transactions. This limitation may result in increased fees and delayed transaction times, particularly on networks like Ethereum and Bitcoin.
- **Energy consumption:** Some networks, like Bitcoin, that use PoW need a lot of energy, which is major concern for the such environments. The community is debating and becoming increasingly concerned about this matter as blockchain mining is energy-intensive PoW.
- **Regulatory and compliance hurdles:** Public blockchains' decentralized and open architecture presents difficulties for legal and regulatory framework compliance. The legal frameworks of various nations regarding cryptocurrencies and blockchain technology can pose challenges to the widespread acceptance and utilization of these networks.
- **Confidentiality:** Every complete node has access to and shares the same data. It is inappropriate for a private company that every transaction is visible to every participating node.
- **Slow speed:** Each node participates in the publication and mining process, which verifies transactions before they are made available to the general public. In Bitcoin, it takes ten minutes or more for a block to be published. The blockchain lags as a result of the Proof of Work protocol since it takes time to solve the hash puzzle. However, the private sector need a blockchain that operates really quickly.

### 3.7 Blockchain Platforms

Some of the popular blockchain platforms are discussed below with quick review of their properties:

### **3.7.1 Bitcoin**

Using a proof-of-work consensus process, Bitcoin is acknowledged as the first and most widely used digital currency. It is also recognized by many as the first blockchain network. The first decentralized cryptocurrency is called Bitcoin (abbreviation: BTC). Peer-to-peer nodes in the bitcoin network encrypt and publicly record all transactions in a distributed ledger known as a blockchain, decentralized from a central authority. To ensure the security of the bitcoin blockchain, consensus can be achieved among nodes through mining, a computationally demanding process based on proof of work. Mining has been criticized for its effects on the environment and for using an increasing amount of electricity.

### **3.7.2 Ethereum**

Smart contracts are executed on the customized blockchain network by Ethereum, an open-source blockchain platform. Additionally, it is the greatest platform on which developers may create decentralized autonomous organizations (DAOs) and decentralized applications. Ethereum, in contrast to the Bitcoin protocol, makes it easier to trade cryptocurrencies and smart contracts securely. Ethereum has been recognized as the premier blockchain platform for organizations in the sector. It is therefore among the greatest platforms for creating enterprise-level applications.

### **3.7.3 Hyperledger fabric**

It is one of the top blockchain platforms. It is an open-source blockchain platform that allows developers to create modular applications based on blockchain technology. The platform provides numerous technological advancements that are critical for the creation of intelligent applications for the manufacturing, supply chain, finance, healthcare smart homes and technology sectors. In addition, the platform provides decentralized hosting and decentralized application storage that supports smart contracts. Hyperledger Fabric blockchain architecture mainly focus on permissioned, which allows network members to participate in the blockchain.

### **3.7.4 IBM blockchain**

The IBM blockchain platform offers all the necessary components for developing commercial applications. With the addition of Kubernetes-based architecture and the

ability to create blockchain applications in cloud environments more quickly, it offers you a centralized user interface, deployment flexibility, support for IoT, Hyperledger Fabric SDK, AI data analytics, and an updated suite of developer tools. The blockchain is permissioned.

### **3.7.5 OpenChain**

It is currently one of the most popular blockchain platforms as well. Developed by Coinprism, it is an open-source distributed ledger technology platform that is secure and ideal for managing digital assets for enterprises. It is built on a peer-to-peer network and features a single point of control for online asset exchanges and payment transaction validation. Additionally, because OpenChain uses partitioned consensus, all transactions occur without a fee, and each transaction on the ledger is verified by the owner of the asset or by means of a digital signature.

### **3.7.6 Stellar**

It is a distributed ledger network built on blockchain technology that provides both individuals and commercial organizations with an efficient and affordable international payment solution. Developers can create smart banking tools and mobile wallets similar to Paypal's online payment system using the Stellar blockchain platform. Setting consensus without utilizing a closed system to record financial transactions is made possible by the Stellar blockchain.

### **3.7.7 EOS**

It is another approach for enabling and securing the purchase, sale, and exchange of datasets via smart contracts. Block.one, a private corporation, introduced the open-source EOS network in June 2018. Its foundation is the idea of decentralized technology, which gives users the capacity to carry out a variety of functions on the EOS platform. Additionally, it does away with the requirement for payments for its customers, so using an EOS-based dApp does not require payment.

### **3.7.8 Ripple**

This blockchain technology is most well-known in the banking, corporate, and payment provider communities. The platform is appropriate for solutions involving international

payments. It makes cross-border banking transactions possible. For huge business entities as opposed to SMEs or individual consumers, Ripple is the ideal blockchain platform. With "XRP or Ripple," a well-liked digital asset for cryptocurrencies like Bitcoin and Ether, users can make international payments.

### 3.7.9 Corda

Distributed ledger technology (DLT) and permissioned Blockchain platform corda is made to function with the modern financial services sector. Regulated institutions rely on Corda to facilitate speedier settlement, tokenization of digital assets and currencies, and automation of intricate business procedures. The Corda blockchain technology only permits authorized users to access payment data (not the network as a whole) and does not support cryptocurrencies or token-based payments.

### 3.7.10 Hedera hashgraph

Based on a directed acyclic graph (DAG) data structure, Hedera Hashgraph is a distributed ledger technology (DLT) platform that uses the Hashgraph consensus method. The platform's architecture prioritizes fairness, security, and speed.

*Table 3. 3: Blockchain platforms and consensus Protocols*

<b>Blockchain Platforms</b>	<b>Consensus Mechanism</b>
Bitcoin	Proof of Work
Ethereum	Proof of Work , Proof of Stake
Hyperledger Fabric	Practical Byzantine Fault Tolerance (PBFT)
IBM	Consensus byzantine fault tolerance (CFTBFT)
OpenChain	Proof of Authority



Stellar	Federated Byzantine Agreement (FBA)
EOS	Delegated Proof of Stake (DPoS)
Ripple	Ripple Protocol Consensus Algorithm (RPCA)
Corda	Notary Service
Hedera Hashgraph	Hashgraph

### 3.8 Comparison of Consensus Mechanisms

#### 3.8.1 Proof of work (PoW)

PoW is the original and primary consensus algorithm that Bitcoin first introduced. Miners compete to validate transactions and add new blocks to the blockchain by working through challenging mathematical challenges. It requires a large amount of energy and processing power. When miners solve riddles, they are rewarded with freshly created cryptocurrency. PoW is used by Ethereum and Bitcoin at the moment [73].

#### 3.8.2 Proof of Stake (PoS)

Block validators are chosen by PoS according to the quantity of cryptocurrency they own and are prepared to "stake" as collateral. King and Nadal presented the benefits of PoS in 2012 [74]. Depending on their stake, validators are selected to add new blocks and approve transactions. lowers energy usage in comparison to PoW. In addition to transaction fees, validators receive extra cryptocurrency benefits. With Ethereum 2.0, Ethereum is making the switch to Proof-of-Stake.

#### 3.8.3 Delegated Proof of Stake (DPoS)

In DPoS, token owners cast votes for a select group of delegates to approve transactions. Block producers, also known as delegates, alternately build blocks and verify transactions. Provides quicker times for processing transactions than PoW and PoS.

utilized by blockchain networks such as Tron and EOS. Larimer's research on Delegated Proof of Stake (DPoS) demonstrates how DPoS is a variation of PoS that offers an additional technique for block building and transaction validation [75].

#### **3.8.4 Byzantine Fault Tolerance (BFT)**

A consensus technique called BFT was created expressly to deal with malfunctioning nodes in dispersed networks. The network is more resilient to malicious actors and system failures when a sizable number of nodes concur on the legitimacy of transactions [76].

#### **3.8.5 Practical Byzantine Fault Tolerance (PBFT)**

For permissioned blockchains with a known group of participants PBFT is designed. It involves three stages in the process: pre-prepare, prepare, and commit. It requires the approval of two thirds of the participants in order for a transaction to be valid. Low latency and high throughput are provided. Utilized in systems such as Ripple and Hyperledger Fabric. To reach a consensus, it follows a preset voting process and allows for the acceptance of up to one-third of the network's nodes being compromised or broken [76].

#### **3.8.6 Proof of Authority (PoA)**

PoA relies on a set of approved validators (authorities) to validate transactions. Validators are identified and trusted entities within the network. Offers high throughput and low energy consumption. Suitable for private and consortium blockchains. Used in networks like Ethereum's Clique consensus and VeChain. Its reliance on trusted authority contributes to the network's integrity, and its suitability for private or permissioned blockchains stems from its decreased dependency on processing power and resource-intensive operations [77].

#### **3.8.7 Proof of Space (PoSpace)**

PoSpace leverages unused hard drive space as a resource for mining and validating blocks. Miners allocate disk space to store cryptographic proofs rather than performing computational work. Encourages participants to contribute storage space to the network. Chia Network is a prominent example of a blockchain utilizing PoSpace.

### **3.8.8 Proof of Burn (PoB)**

In order to gain a chance or right to validate blocks, participants in Proof of Work (PoW) must burn (destroy) a predetermined quantity of cryptocurrency. By burning tokens, participants demonstrate a commitment to the network's security. Provides an alternative to traditional mining or staking. Used in projects like Counterparty and Slimcoin.

### **3.8.9 Proof of Elapsed Time (PoET)**

PoET is an Intel-developed consensus mechanism that is a part of Hyperledger Sawtooth. The network's participants construct a random wait time, and the first person to complete the wait period has the opportunity to build the following block. It relies on trusted execution environments (TEEs) to ensure fairness and randomness. It was proposed in 2017 by Ren et al [78].

### **3.8.10 Proof of Identity (PoI)**

PoI ties the validation of transactions to the identity of participants. Validators are required to provide proof of their real-world identity before they can validate transactions. Helps enhance trust and accountability within the network. Still a relatively experimental consensus mechanism with limited adoption.

### **3.8.11 Proof of Weight (PoWeight)**

PoWeight assigns different weights to validators based on factors such as reputation, stake, or past performance. Validators with higher weights have a greater influence on the consensus process. Promotes the participation of trustworthy and reliable validators. Provides a more nuanced approach to stake-based consensus.

### **3.8.12 Proof of Activity (PoA)**

PoA combines PoW and PoS mechanisms to validate transactions. Miners first compete to solve cryptographic puzzles (PoW), and then validators (chosen based on stake) confirm the validity of the block (PoS). Provides a balance between security and energy efficiency. Used in projects like Decred. This approach is safer and uses less energy than one that uses conventional PoW algorithms [79].

### **3.8.13 Proof of Reputation (PoR)**

PoR relies on the reputation of network participants to determine their role in the consensus process. Participants with a positive reputation have a greater influence on decision-making.

Reputation is typically assessed based on past behavior, contributions to the network, and adherence to rules. Enhances network security by incentivizing good behavior and penalizing malicious actors.

### **3.8.14 Tangle**

The IOTA blockchain network uses a consensus algorithm called Tangle. To validate transactions, this novel technique makes use of a directed acyclic graph (DAG) structure. A transaction needs to validate two other transactions in order to be accepted as legitimate. By comparison, the Tangle algorithm produces a network that is both scalable and quick compared to previous consensus algorithms [80].

### **3.8.15 Tendermint BFT**

A consensus method called Tendermint BFT was created especially to handle high-throughput blockchain networks. In order to reach consensus, it uses a voting system. It can process thousands of transactions per second [81].

### **3.8.16 Honeybadger BFT**

Another variant of BFT, HoneyBadgerBFT, the first practical asynchronous BFT protocol, which guarantees liveness without making any timing assumptions.

## **3.9 Requirements for IoT Systems**

Some the basic requirements for IOT Systems are as follows:-

- **State Machine Replication:** A common method for creating fault-tolerant systems in distributed computing is called state machine replication, or SMR. This is accomplished by setting up client exchanges with server replicas and replicating servers, also known as state machines. By distributing copies of a web service over several servers as opposed to just one, SMR does this. Because the replicas give the service access to more resources, this method may improve a system's performance

and capacity while establishing operational fault tolerance by removing the single point of failure.

- Transaction Integrity and authentication
- Block and transaction validation
- Identity management (private/ consortium chain)
- Avoid or Protect against Sybil attack
- Consensus finality
- No Forks
- Tolerate maximum nodes
- Integrity checks
- Asynchronous network
- Low Latency
- Low computation complexity
- Low Communication Complexity
- Low Energy Cost

*Table 3. 4: Features of Census Mechanisms*

<b>Ser.</b>	<b>Feature</b>	<b>Existing Protocols (If implemented)</b>
1.	State Machine Replications	BFT, PBFT, DBFT, Honeyledger BFT, IOTA
2.	Permissioned Ledger	BFT
3.	Identity Management	BFT
4.	Un-Forgeability	All
5.	IoT Devices' Transaction Validation	None
6.	Tx Integrity Check	ALL
7.	Device Integrity Check	None
8.	<ul style="list-style-type: none"> <li>• Consensus finality</li> </ul>	All BFT Based Protocols

	<ul style="list-style-type: none"> <li>• No forks</li> <li>• Low Latency in tx confirmation</li> </ul>	
9.	Asynchronous Network (No weak timing assumptions)	Honeybadger PBFT
10.	Avoid DoS stacks (weak time assumptions)	Honeybadger PBFT
11.	Maximum Faulty Nodes tolerance	$>(n-1)/3$
12.	Protection against Sybil attack	POW, PoS
13.	Detect faulty nodes	Only tendermint and Bitcoin-NG, that flags a double spending node
14.	Penalty for faulty node or replicator (Sometimes at stake)	In Tendermint, bonded coins are confiscated, and in Bitcoin-NG loss of block reward & fee
15.	Sybil Attack	<ul style="list-style-type: none"> <li>• In PoW and PoS, a sybil node has to invest in energy and coinbase to make an impact</li> <li>• In voting based consensus, a randomize selection of consensus quorum in each epoch</li> </ul>
16.	Fault detection in BFT	Based on request and response message only

### 3.10 General Terminologies

Some of the basic important terminologies related to blockchain technology are as following:

### 3.10.1 Smart contract

A smart contract is a self-executing program that performs the actions specified in a contract or agreement. The transactions are traceable and irreversible once they are completed. Smart contracts eliminate the need for a central authority, legal framework, or external enforcement mechanism by enabling trusted agreements and transactions to be conducted amongst anonymous, dispersed individuals

- Smart contracts are computer programs designed to automate interactions between two parties.
- Smart contracts are just pieces of code that, when certain conditions are fulfilled, take action. They don't contain any legal language, terms, agreements or commitments.
- In 1998, American computer scientist Nick Szabo developed the concept of a virtual currency known as "Bit Gold" [82]. He described smart contracts as computerized transaction protocols that carry out a contract's conditions.

#### Pros and cons of smart contract

Main advantage of smart contracts is comparable to that of blockchain technology in that they eliminate the necessity for intermediaries and third parties. Added advantages of this technique include:

- **Efficiency:** They expedite contract execution
- **Accuracy:** No human error can be introduced
- **Immutability:** The code cannot be changed

A few disadvantages of smart contracts include:

- **Permanent:** If they are incorrect, they cannot be altered.
- **The human factor:** People depend on programmers to make sure the code is written correctly so that the expected activities are carried out.
- **Loopholes:** There can be coding errors that let contracts to be carried out dishonestly

### 3.10.2 Decentralized applications (DApp)

Decentralized applications, or dApps, are software programs that run on blockchains or peer-to-peer (P2P) networks of computers instead of just one computer. Distributed application programs (dApps) are managed by their users collectively on the network, as opposed to being governed by a single entity. These are a new kind of applications that are not controlled by a single entity and, more crucially, cannot be shut down and never experience downtime. These are open-source programs that conduct blockchain transactions via smart contracts.

#### Pros

- Supports user privacy
- Are resistant to censorship
- Provides a flexible framework for dApp development

#### Cons

- Experimental, might not be able to scale
- Difficult to develop a user-friendly interface
- Difficulties in implementing necessary code changes
- Security risks resulting from careless programming

*Table 3. 5: DApplications vs Centralized Applications*

<b>Ser</b>	<b>DAPP</b>	<b>Centralized Applications</b>
1.	Decentralized Control	Centralized Control
2.	Trustless	Trusted
3.	Data immutability	Prone to data censorship/ modification
4.	App cannot be changed	Change anytime
5.	Rigorous testing required	Updates can follow



	(as once deployed, it cannot be modified)	
	Being distributed secure against hacking and ransomware attacks	Vulnerable to hacking and ransomware attacks

### 3.10.3 Blockchain node

A blockchain node is any device that participates in a blockchain network; these are often computers. It helps with network security and transaction validation by putting the blockchain protocol's software into action. Blockchain nodes communicate with one another via messages. The more nodes in the network, the more decentralized it is. The two main functions of a blockchain node are broadcasting and transaction validation. A transaction that a user submits is received by a node, which then broadcasts it to the whole network. Each node in the network checks the transaction to make sure the sender is authorized to send the money and has the required amount of currency on hand.

### 3.10.4 Token

Tokens are digital assets in the blockchain ecosystem that facilitate the efficient and safe transmission, storing, and verification of value and information. A token is an asset that is digitally represented and can be kept on a distributed ledger technology (DLT) network. It can act as a store of value, a medium of trade, or a sign of ownership for both digital and physical assets.

### 3.10.5 Mining

An act of adding transactions to the blockchain based on PoW. Bitcoins are initially produced and distributed through mining and transactions are also verified through mining. Network nodes perform computational effort known as "blockchain mining" to verify and arrange data in blocks. Thus, miners are also compensated for performing their tasks. In addition to creating a new block and verifying the initial transaction, they are also getting paid for their efforts.

### **3.10.6 Bitcoin minting**

The block reward is given by minting new bitcoins (bring new coins into circulation).

### **3.10.7 Interoperability**

The capacity of several DLT platforms to communicate and work together efficiently is known as interoperability. This makes it possible for assets and data to move between different DLT platforms and blockchains seamlessly.

### **3.10.8 Oracles**

Blockchain oracles are entities that establish connections between blockchains and external systems, allowing smart contracts to operate based on real-world inputs and outputs. A third-party smart contract service is known as a blockchain oracle. Oracles provide trusted information based on the outside-world sources to the on-blockchain smart contracts. An oracle typically encapsulates the real-world complexity outside of the blockchain, since the on-chain critical errors are hard to fix. Oracles are organizations or systems that provide smart contracts with external data. They serve the purpose of confirming and validating data obtained from outside sources before a smart contract processes it.

## **CHAPTER 4**

### **PROPOSED METHODOLOGY**

This chapter offers a comprehensive overview of a proposed framework that incorporates blockchain technology into the smart home market. It begins with providing a synopsis of the framework, highlighting its key components and their interrelationships. The proposed framework makes use of blockchain, a decentralized and secure technology, to enhance the security, confidentiality, and integrity of data related to smart homes. The framework aims to leverage blockchain technology to tackle many concerns within the smart home industry, such as data integrity.

The chapter also explores the assessment measures that are used to assess the usefulness of the frameworks. It looks at a number of measurements and standards to assess problems like latency and system efficiency. The foundation for an unbiased analysis and comparison of the suggested framework with current smart home systems is provided by these assessment measures. The chapter also highlights the research that went into developing and suggesting the blockchain architecture for smart homes. It outlines the framework's unique attributes, advantages, and potential uses in the smart home industry.

The importance of data integrity continues to increase as the emergence of usefulness of modern technologies and IOT in smart homes increases. Blockchain technology improves data security and interoperability in smart homes, but it also increases processing and storage requirements. Data or generated logs of IoT devices calculated centrally or decentrally are under continuous threat and are vulnerable to integrity attacks as they are not saved on the blockchain. To avoid, intrusions, Blockchain technology can play a significant role in enhancing the security and ensuring the data integrity of IoT devices. Blockchain technology can enhance the security and preservation of generated information in IoT devices by providing data integrity, security, automation, consensus, traceability, and identity management. These features can collectively contribute to a

more reliable and secure IoT ecosystem, fostering greater confidence among both users and service providers.

Resultantly, we are motivated to apply blockchain to play its role to enhance security and data integrity of nodes to avoid cyberattacks. Hence, device data hashes will be calculated and will be stored on the blockchain.

#### **4.1 Selection of Blockchain**

What is the best and most advantageous type of blockchain for preserving smart home systems? It is the following question on our way towards developing a better solution. There are various kinds of blockchain, as was covered in the previous chapter. Which kind of blockchain will be more beneficial in our situation? By considering the needs of smart home systems and requirements of IoT devices as discussed, a permissioned/private blockchain is appropriate to implement for solution.

#### **4.2 Why Hyperledger Fabric (HLF)?**

HLF is believed to be more efficient in our scenario than any public blockchain. Because HLF is a private ledger, it works better for nodes that interact with one another and have less resources. To function, HLF needs a network of nodes that are committing, endorsing, and ordering service peers. All nodes are committed peers in the HLF, but only endorsing peers and ODS are needed for continuous operation. It is possible to assign the tasks of endorsing peers and ordering service peers to a small number of Nodes that have greater processing power, memory, and backup time. The remaining nodes can function as regular clients and cancel a smart contract whenever they require blockchain services. Moreover following factors are the reason to choose HLF for suitability of our solution:

- Personal data be processed only on consent of the data owner.
- Any system that relies on user information needs to protect user privacy by design. By design, HLF offers privacy because of channels.

- The collection, handling, processing, or application of personal data must adhere to guidelines established by a mutual contract between the user and third parties.
- The data owner must be able to get information on how his data is being processed, including which third parties can access what data and how they can use it.
- Once no longer needed, data should be deleted. The history of transactions will be preserved.
- The system has to be transparent so that people are aware of how their data is collected and used.

### 4.3 Comparison of HLF with other blockchains

Comparison of selected blockchain HLF with some other renowned blockchains is given in table 4.1 below:

*Table 4. 1: Comparison of blockchains*

<b>Feature</b>	<b>Bitcoin</b>	<b>Ethereum</b>	<b>HLF</b>	<b>IOTA</b>
Data confidentiality	No	No	Yes	No
ID management	No	No	Yes	No
Key management	No	No	Yes (CA)	No
User authentication	Yes	Yes	Yes	Yes
Device Authentication	No	No	No	No
Attacks	51%	51%	>1/3 faulty nodes	34%
Transaction throughput	7 TPS	8-10 TPS	In Thousands	7-12 TPS
Latency	60 mins	15-20 sec	Less than ethereum and bitcoin	Mins to hours

Scalable (Tx)	No	No	Yes	Yes (In term of pending Tx)
Fully developed	Yes	Yes	Yes	Yes
Miner participation	Public	Public, Private	Private	Public, Private
Trustless operation	Yes	Yes	Trusted Validator Nodes	Yes
Multiple Applications	Financial	Yes	Yes	Yes
Consensus	PoW	PoW, PoS	Pluggable (PBFT, SIEVE)	Tangle (Coordinator approves Tx)
Consensus Finality	No	No	Yes	No
Forks	Yes	Yes	No	Yes tangle can be faded out
Fee Less	No	No	Optional	Yes
Smart Contract	No (Yes)	Yes	Yes	Yes
Transaction Integrity	Yes	Yes	Yes	Yes

#### 4.3.1 Installation steps

Detailed information about building a test network is available on link “<https://www.ibm.com/docs/en/hlf-support/1.0.0?topic=started-build-network>”.

However, followings steps are performed for Installation of Test network HLF:

- **Prerequisites**

1. Install Git in the system if not already installed.

```
$ sudo apt-get install git
```

2. Install Git in the system if not already installed

```
$ sudo apt-get install curl
```

3. Install the latest version of Docker if it is not already installed.

```
$ sudo apt-get -y install docker-compose
```

- Once installed, confirm that the latest versions of both Docker and Docker Compose executables were installed by fol command

```
$ docker --version
```

```
docker version 19.03.12, build 48a66213fe
```

```
$ docker-compose --version
```

```
docker-compose version 1.27.2, build 18f557f9
```

4. Make sure the Docker daemon is running.

```
$ sudo systemctl start docker
```

5. Optional: If you want the Docker daemon to start when the system starts, use the following:

```
$ sudo systemctl enable docker
```

6. Add your user to the Docker group.

```
$ sudo usermod -a -G docker <username>
```

- Download Fabric samples, Docker images, and binaries.

1. \$ cd (/to go to home directory)

2. \$ mkdir hlf

3. \$ cd /hlf

4. `$ curl -sSLO https://raw.githubusercontent.com/hyperledger/fabric/main/scripts/install-fabric.sh&& chmod +x install-fabric.sh`
  5. To pull the Docker containers and clone the samples repo, run one of these commands in the same folder  
  
`$ ./install-fabric.sh docker samples binary`  
  
or  
  
`$ ./install-fabric.sh d s b`  
  
`$ cd (go back to home directory)`  
  
`$ cd smartHome (Folder created during initial work contains code of website)`
  6. To install all dependencies of web application  
  
`$ npm install`
- Steps to Run System  
  
Run HLF blockchain
    1. Go to home directory  
  
`$ cd`
    2. Go to Hlf Directory  
  
`$ cd hlf/fabric-samples/test-network/`
    3. To make down the previous network (if any)  
  
`$ sudo ./network.sh down`
    4. Start all docker container that will act as nodes of the HLF  
  
`$ sudo ./network.sh up -ca`
    5. Create Channel



```
$ sudo ./network.sh createChannel -c identitymanagement
```

6. Save chaincode file in specific folder (Manually)

7. Deploy chaincode on the network

```
$ sudo ./network.sh deployCC -ccn identity -ccp PATH TO Chaincode -ccl  
javascript -c identitymangement
```

- Running Application Website

1. \$ cd (go back to home directory)

2. \$ cd smartHome (Folder created during initial work contains code of website)

3. Run website in development mode

```
$ npm run dev
```

//Note: Before this HLF must be running

#### **4.4 Proposed Framework**

The suggested framework focuses on integrating smart home architecture with blockchain technology. The major purpose is to give Smart service providers and users a better knowledge of the system usefulness while also assuring its effectiveness, efficiency, and security. The framework intends to shed light on the necessity of data integrity for smart home implementations that use blockchain by studying the relevant element. As user expectations increase, data integrity with security becomes increasingly important in the success of smart home systems. Our proposed methodology is divided into three sections. These sections are graphically depicted in Figure 4.1:

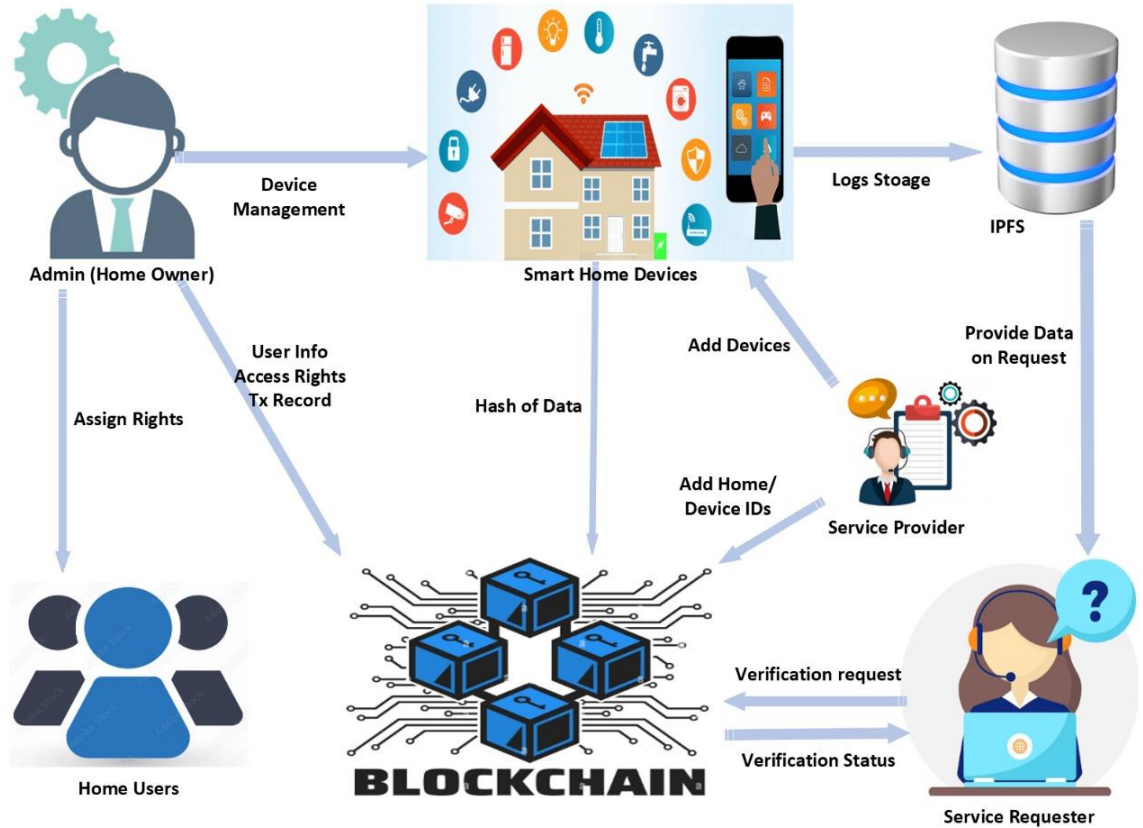


Figure 4. 1: Proposed system model

## 4.5 Participating Entities

There are several participating entities in the proposed framework which are described below:

### 4.5.1 Home admin (Owner)

The Home Admin (Owner) in this system refers to the homeowner or the person in charge of managing the smart home devices. The home admin interacts with the blockchain-enabled smart home system and as under:

- Device management:** The home admin can add new devices to the network and assign them specific rights. This allows them to control which devices can access and share data on the blockchain network.

- **User information & access rights:** The Home Admin can also manage user information within the system. This includes assigning users specific access rights to devices and data.
- **Transaction record:** All actions performed by the Home Admin are recorded on the blockchain as a transaction. This creates a permanent and immutable record of changes made to the system.
- **Verification requests:** The Home Admin can also use the system to initiate verification requests. This could be to verify the integrity of logs data based on hash stored on the blockchain or to confirm the validity of a transaction.

#### 4.5.2 Home users

It refers to individuals who have been granted access to the smart home system by the Home Admin (owner). There can be different types of home users with varying levels of access depending on the setup. Some of them are:

- **Family members:** This includes spouses, children, or other close relatives living in the home. They can have full access to control lights, thermostats, entertainment systems, and view sensor data (motion, temperature etc.).
- **Guests:** The Home Admin can create temporary guest accounts with limited access. This could be for functionalities like controlling guest room temperature or turning on lights in designated areas.
- **Caregivers:** In some cases, the Home Admin may provide access to caregivers who can monitor the home environment or receive alerts for emergencies.

#### 4.5.3 Smart home

It's a prominent entity in the entire framework, main functions performed is as follows:

- **Connecting to the network:** Smart home devices establish a connection to the blockchain network through a central hub or gateway. This connection allows them to securely send and receive data.
- **Data sharing:** The data collected from the devices, such as temperature readings from a smart thermostat or motion detection from a security camera or device logs, is recorded on the database and hash of data is saved on blockchain ledger. Blocks in the ledger contain hashed data, which was gathered from smart devices, that acts like a

fingerprint and ensures data integrity. If any tampering were to occur, the hash would change, alerting homeowners to a potential security breach.

#### **4.5.4 Blockchain**

It acts as a secure and transparent method for recording and managing data from smart home devices. It works like a backbone within this system and perform the following key functionalities:

- **Distributed ledger:** Transaction Information from Home admin, hash of Data from smart homes is recorded on a shared, distributed ledger. This ledger is not stored on a single server but replicated across multiple devices on the network. This makes it tamper-proof because altering data on one device would require altering it on all devices, which is highly improbable.
- **Immutable records:** Once data hashes and transaction information is added to a blockchain, it cannot be changed or deleted without detection. Each block of data is cryptographically linked to the one before it, creating a chain-like structure. Any modification to a block would change its unique code, alerting the system to a potential security breach.
- **Security:** Blockchain uses cryptographic hashing to secure data. Each block contains a unique hash code derived from the data in the previous block. This creates a tamper-evident chain, where any data alteration would invalidate the hash codes, signaling a security issue.

This entity benefits an entire smart home system architecture by:

- **Enhancing security:** The decentralized nature of blockchain makes it resistant to hacking attempts, and reduces the risk of exploiting single point of failure by attackers. This strengthens the security of data communication between smart home devices.
- **Data integrity:** Blockchain ensures that the data collected from smart home devices remains unchanged and verifiable. This is crucial for maintaining trust in the system, especially for sensitive data like security sensor readings.
- **Transparency:** Homeowners can view a complete history of transactions on the blockchain ledger. This provides transparency regarding device activity and data changes within the smart home system.

#### 4.5.5 IPFS

IPFS is basically a distributed file system to store and access data which stores data in P2P network. It also has an incentive system layer called “Filecoin”. Nodes from all around the world are incentivized to store and retrieve this data. Different providers can be used to provide IPFS node like infura and pinata etc. In our case we used “Pinata” which is considered an easy to use service where we can pin our files to IPFS and store the IPFS hash in blockchain. It provides secure storage for the logs generated from various smart home appliances and provides the following key functionalities within the framework:

- **Data storage:** Stores data and logs generated from smart home devices, data and other information is available on request.
- **Data on demand:** Provide useful data insights and information to “Service Requester” upon admin approvals.

#### 4.5.6 Service provider

It refers to a third-party company that offers various services to establish a smart home system focused on data integrity and security. Some of the prominent features include:

- **Add devices:** As depicted in the figure, a service provider can add devices to smart home. This indicates that a service provider can install or deploy a new device or update an existing one for the smooth operations.
- **Add home to blockchain:** The service provider can add a new home of the same owner, this eliminates the use of separate blockchain for each smart home.

#### 4.5.7 Service requester

It refers to the company or entity who is responsible for providing specific service to home for which purpose it may need limited access to some devices. Some other services can be granted restricted access for specific purposes. For instance, a smart grid user might be allowed to remotely access a smart meter for billing purpose, some of the prominent features of this entity is:

- **Getting data from database:** It gathers data from database to perform several operations related to their services.

- **Verification requests:** Service requester can request verification from blockchain network in order to verify the overall integrity of the framework, this ensure the overall integrity and provide audit and compliance to local authorities where required.

#### 4.5.8 Evaluation Parameters

In the proposed framework, the main concern is to provide data integrity and security to the entire smart home architecture. Out of so many parameters, the following proposed parameters will be taken out to calculate the efficiency of the architecture:

- **Latency:** It is the time required for a packet to traverse among two different nodes. Less the latency, the more responsive the framework is.
- **CPU usage:** It is the percentage of the resource utilized for the transactions processed to blockchain. The less the CPU usage the more resource friendly the framework is.

#### 4.6 Proposed HLF Architecture

In a private home Hyper Ledger Fabric will be best-suited blockchain type for storing and sharing of data. The basic proposed architecture is described in Figure 4.2 below.

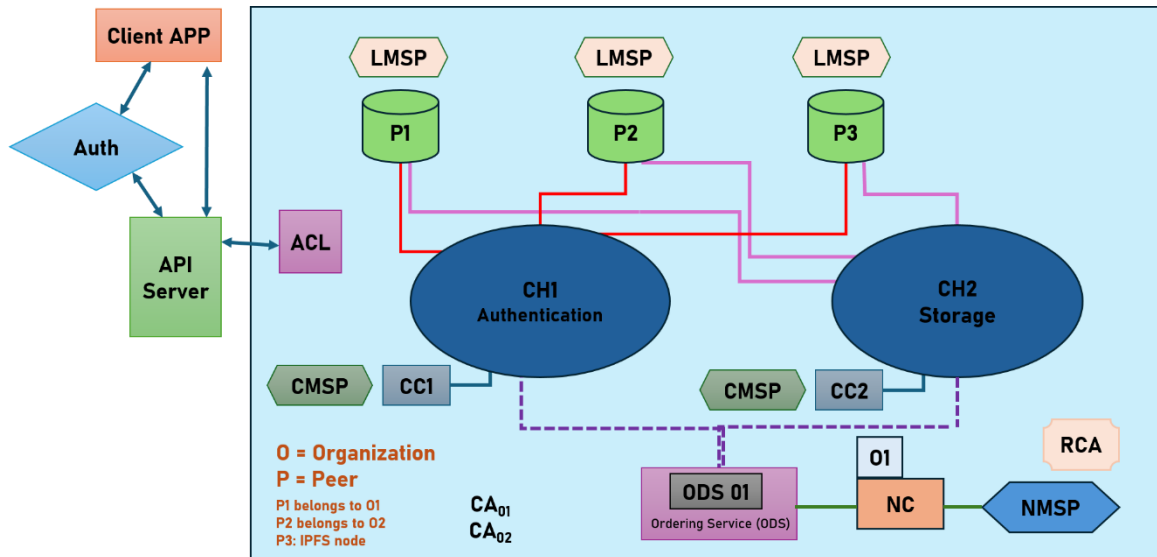


Figure 4. 2: HLF architecture

#### 4.6.1 Chaincode

An application that operates on top of the underlying architecture to preserve state and enforce business rules is called a chaincode, also sometimes referred to as a "smart contract." This program may use the services provided by other chain codes that are operating concurrently on the same peer node, or it can construct its own data structures. A chaincode is basically a container that contains multiple smart contracts for installations and instantiations. When a chaincode is deployed, all the smart contracts within that chaincode are also deployed and made available to applications.

#### **4.6.2 Channels**

A Hyperledger Fabric channel is a private "subnet" of communication used for private and confidential transactions between two or more members of a certain network. Members (organizations), shared ledger, ordering service node(s), chaincode application(s), and anchor peers for each member comprise a channel. All transactions on the network are executed across a channel, and in order to transact on that channel, a party needs to be authenticated, verified and granted authorization. A membership services provider (MSP), which authenticates each peer to its channel peers and services, provides each peer that joins a channel with a unique identity. A channel provides completely separate communication mechanism between set of organizations that are part of channel.

#### **4.6.3 Committing peers**

All the peer nodes participating in HLF blockchain are committing peers. However, smart contracts are not installed on committing peers. These nodes just validates and commits the new blocks having transaction into its copy of ledger, sent by ordering service peers.

#### **4.6.4 Endorsing peers**

These are also committing peers that have special ability to run smart contracts. The chaincode is executed by an endorsing peer, and if successful, it results in an actual transaction for the ledger. The transaction is subsequently signed by the endorsing peer and given back to the proposer. The transaction proposals sent by the client is prepared, signed and endorsed by these peers in line with endorsement policy of specific channel.

#### **4.6.5 Ordering service (ODS) peers**

These are the collection of peer nodes from various channels that will arrange the transactions in the block and broadcast the new block to all the peers of particular channel. The transaction blocks are created by the ordering service and are eventually sent to all peers on the channel for committing to the ledger and validation.

#### **4.6.6 Membership service provider**

Certificates Authorities (CAs) issue X.509 certificates to all the network entities whereas, membership service provider tells that which CAs will be accepted by the blockchain network and determines which node is membership of which organization. Membership service providers can be defines at channel, network and peer or local level.

- **NMSP:** Network MSP outlines who all are the members of network and out of them who will have admin rights. It also tells that which RCAs and CAs will be trusted.
- **CMSP:** Channel MSP defines admin and participatory at channel level.
- **LMSP:** Local MSP is defined for all peers/ nodes. It is used to associates a peer with its organization.

#### **4.6.7 CC**

A channel is governed by policies contained by “Channel Controller” that which organization is responsible to regulate channel and add new members in the channel whereas, CMSP will defines the roles the node can play within a channel and establish a link between nodes/ peers and their organizations. For example, which node can instantiate a smart contract on channel.

#### **4.6.8 RCA and CA**

Root Certificate Authority issues X.509 certificates to network entities which serve to authenticate these entities and used to sign digitally client application transaction proposal and smart contract transaction response. CA is certificate authority at organization level.



## CHAPTER 5

### ANALYSIS AND RESULTS

#### 5.1 Performance Evaluation and Comparative Analysis

This section includes a simulation study intended to offer insightful information to service providers and smart home customers alike, in order to thoroughly assess the efficacy and efficiency of the suggested system. Here, the effectiveness of the suggested framework in solving the identified issue is the main concern. We carry out thorough analyses taking effectiveness and efficiency measures into account. Furthermore, possible threats to cyber security related to deployment are recognized.

In order to evaluate how well the recommended system works, the simulation parameters are carefully chosen, and the settings are painstakingly created. This entails contrasting the outcomes of several simulated situations. Moreover, a comparison study is carried out, examining substitute methods and contrasting them with the advantages of the suggested framework. This comparison technique finally confirms the importance and viability of our suggested methodology by enabling a detailed assessment of the benefits and drawbacks of various solutions.

When implementing a system, it is crucial to carefully evaluate potential cyber dangers, especially in the sector of smart homes where data security and privacy are critical. A useful method for determining a framework's vulnerability to online attacks and identifying latent flaws is simulations. We can ensure that sensitive user data is protected and increase system resilience by putting strong security measures in place and thoroughly evaluating the system against a variety of cyberattack scenarios. This proactive approach not only mitigates potential risks but also fosters user confidence in the system's security posture.

## 5.2 Limitations of Experimental Setup

In a real system, IoT devices are required to provide storage data and logs to store in database and hash values to the blockchain for data integrity and security. IoT devices in our scenario are not real but are simulated. Some random hash values are used to evaluate the results parameters i.e. Latency, CPU Usage just like the actual IoT devices. These random hash values are fed to the proposed framework and result parameters are calculated.

## 5.3 Environment Setup

For simulating the Blockchain network, we employed a nextjs based web application. Visual Studio Code served as the integrated development environment (IDE), and smart contract written in java script facilitated the interaction with the simulated blockchain. A computer system with adequate storage capacity was used to run the simulation.

Our designed blockchain network incorporates two attributes for data storage. These attributes are then used by the verification mechanism to ascertain the legitimacy and authenticity of the stored data within the network. To evaluate the efficiency and effectiveness of the proposed framework, we conducted simulations by varying the number of transactions processed and monitoring the corresponding central processing unit (CPU) usage.

The Simulation experiments were conducted on a computer system and other technical details are described in Table 5.1.

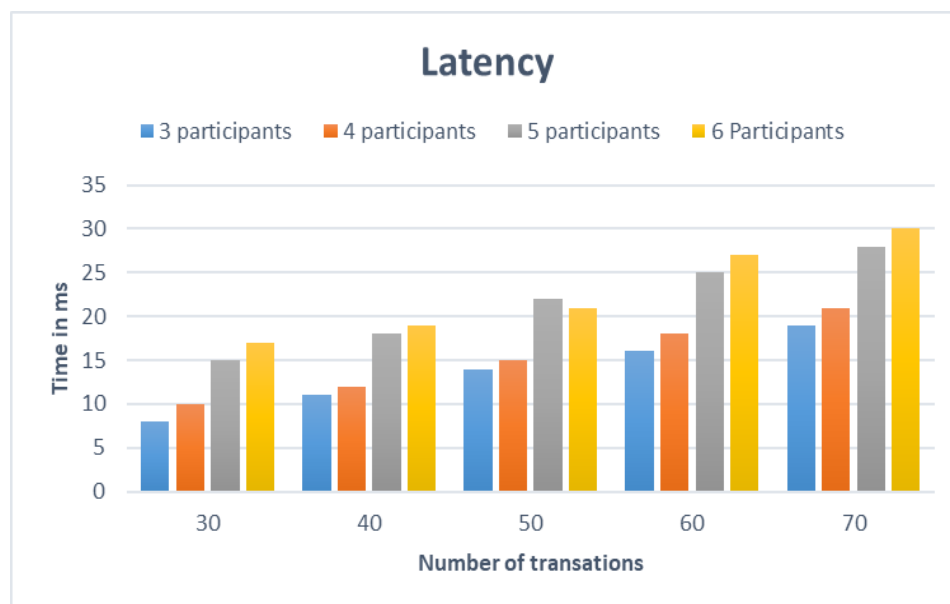
*Table 5. 1: Specifications of the system*

<b>Processor</b>	Core i5 6300U
<b>Storage</b>	256 GB SSD
<b>RAM</b>	16 GB
<b>Operating System</b>	Windows 10 64 bit

<b>Compiler</b>	Visual studio code
<b>Blockchain</b>	Hyperledger Fabric
<b>Fron/Back End</b>	Nextjs
<b>Smart contract</b>	Java script

### 5.4 For Efficiency

Building upon our established problem statement, this study prioritizes the integrity of data while concurrently striving to maintain system efficiency. To address this challenge, we have specifically considered the scenario of a high volume of transactions originating from smart devices. Figure 5.1 depicts the relationship between transaction volume and processing delay. By analyzing this, we evaluate the system performance under varying transaction loads and identify strategies to optimize the proposed framework efficiency. Understanding the involved link between transaction volume and processing time allows to design tactics that maximize efficiency while accommodating an ever-growing number of transactions. Ultimately, our objective is to achieve a well-balanced system that prioritizes both data integrity and efficient operation, ensuring a seamless user experience.

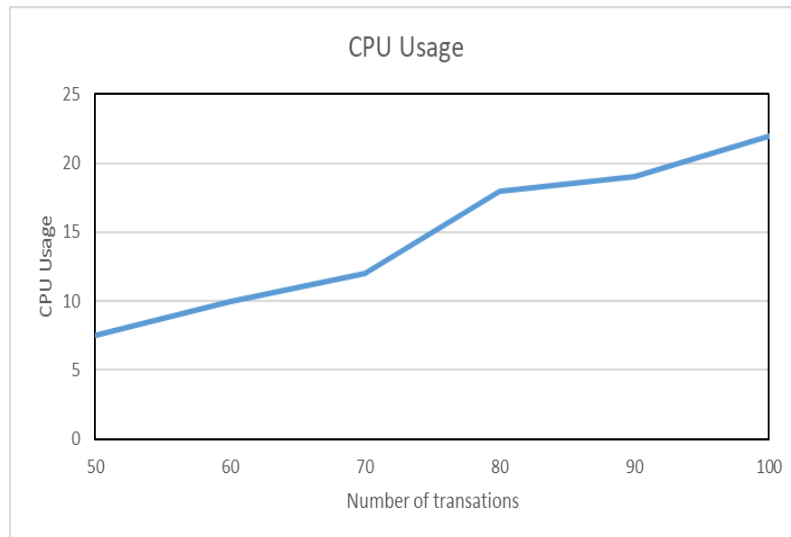


*Figure 5. 1: Latency of proposed framework*

The figure depicts the relationship between the number of transactions processed within a smart home blockchain system and latency. This plays a critical role in evaluating the system efficacy in maintaining data integrity and security under varying operational loads. It shows the significance of evaluating a smart home framework security posture under varying transaction loads. By understanding this, we can achieve an optimal balance between vigorous and efficient system operation, ultimately fostering a secure and seamless user experience within smart homes.

### **5.5 For Effectiveness**

As per problem statement outlined earlier, our key objective revolves around achieving a harmonious balance between data integrity, security, and system effectiveness within the smart home context using blockchain technology. To address this complicated task, we have devised a specific simulation scenario. This scenario explores the impact of varying transaction volumes on central processing unit (CPU) utilization. By examining this data, we can explain the integrity implications associated with our proposed system. This investigation focuses on how transaction volume influences CPU usage, particularly as the number of transactions progressively increases. By investigating deeper into this, we can gain valuable insights into the system functionality under varying workloads.



*Figure 5. 2: CPU usage of proposed framework*

The figure 5.2 depicts the relationship between the number of transactions processed within a smart home blockchain system and its corresponding central processing unit (CPU) utilization. The axis represents CPU usage as a percentage of total capacity, while the other dimension shows the varying number of transactions processed during the simulation (50 to 100 transactions).

This simulation also emphasizes the significance of evaluating the trade-offs between security and efficiency in smart home systems that uses blockchain technology. By understanding this relationship between transaction and CPU usage, we can achieve an optimal balance between robust security ensured by blockchain and efficient system operation, ultimately fostering a secure and seamless user experience within smart homes, it can be observed that as number of transactions increases, so does CPU utilization. This graph is useful for analyzing system scalability, detecting possible performance bottlenecks, and optimizing resource allocation to ensure the system transaction processing is efficient and effective.

## **5.6 Performance comparison with other schemes**

This simulation stresses on evaluating the performance of a proposed smart home architecture that leverages a decentralized storage system, as compared to a traditional centralized approach. The corresponding graph shows the findings of this evaluation.

An important evaluation matrix for assessing the responsiveness and overall performance of a smart home system is access time i.e. the time it takes to retrieve the desired data. This simulation delves into data retrieval times within a decentralized architecture that utilizes blockchain technology. By examining these access times, we aim to demonstrate the effectiveness of data retrieval in such a distributed smart home environment. Also, this investigation highlights the advantages that decentralization highlights, when coupled with blockchain, can offer in terms of data security and integrity within smart homes.

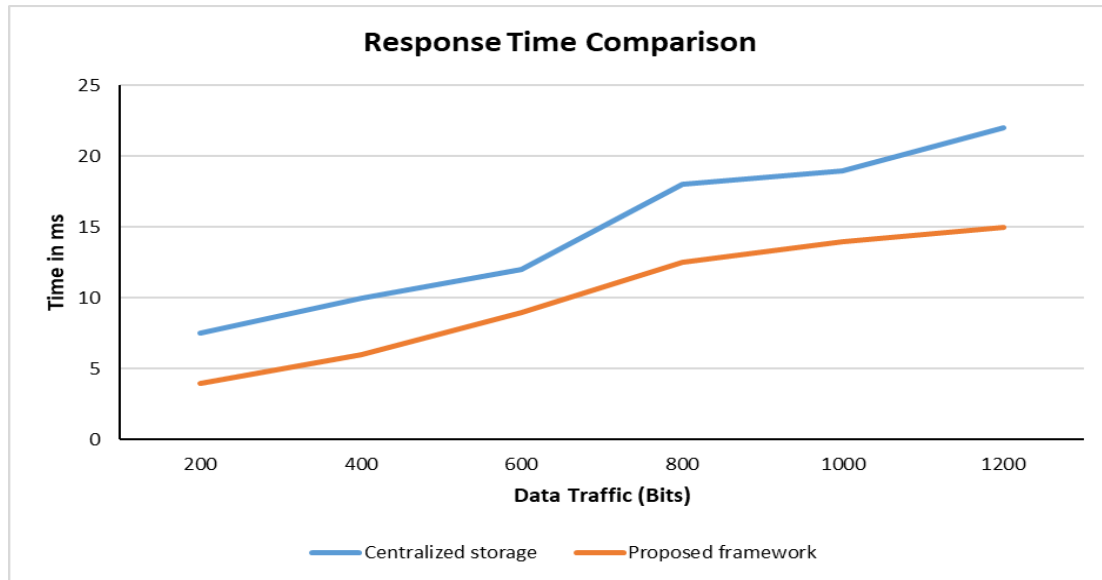


Figure 5. 3: Comparison of proposed framework with centralized storage

Figure 5.3 depicts the response time, measured in milliseconds (ms), required to access data stored in a centralized storage system or a blockchain-based system. One axis represents the volume of data traffic, and another axis represents the response time. A lower response time signifies a more responsive and efficient system. A detailed comparison is described below:

- Centralized Storage vs. Blockchain:** The graph shows that as the data traffic volume increases, the response time for the centralized storage system rise more significantly compared to the blockchain-based system. This specifies that a centralized architecture become less efficient under heavy workloads, leading to delays in retrieving data from smart home devices.
- Security and Integrity:** A prominent aspect of blockchain technology is its ability to guarantee data integrity and security. Every transaction hash, containing sensor data (temperature readings), security system status updates, and lighting configurations, is immutably stored on blockchain. This distributed ledger ensures that any attempt to tamper with the data would be easily detectable.

- **Decentralization and Performance:** While blockchain offers prominent security advantages for data integrity, it is important to acknowledge that it introduces some trade-offs in terms of processing speed, especially when dealing with huge data volumes. However, the potential advantages of decentralization for data security and integrity in smart homes are highly convincing.

## **5.7 Workflow of the Proposed Architecture**

As we are concerned with the integrity and security of the proposed framework, so we design the workflows for service provider and a general application workflow.

### **5.7.1 Application workflow**

It ensures data integrity by implementing a multi-layered approach. It validates user existence, ensures role-based access control, checks unauthorized alterations through read-only modes, and verifies data integrity before saving. This is depicted in Figure 5.4

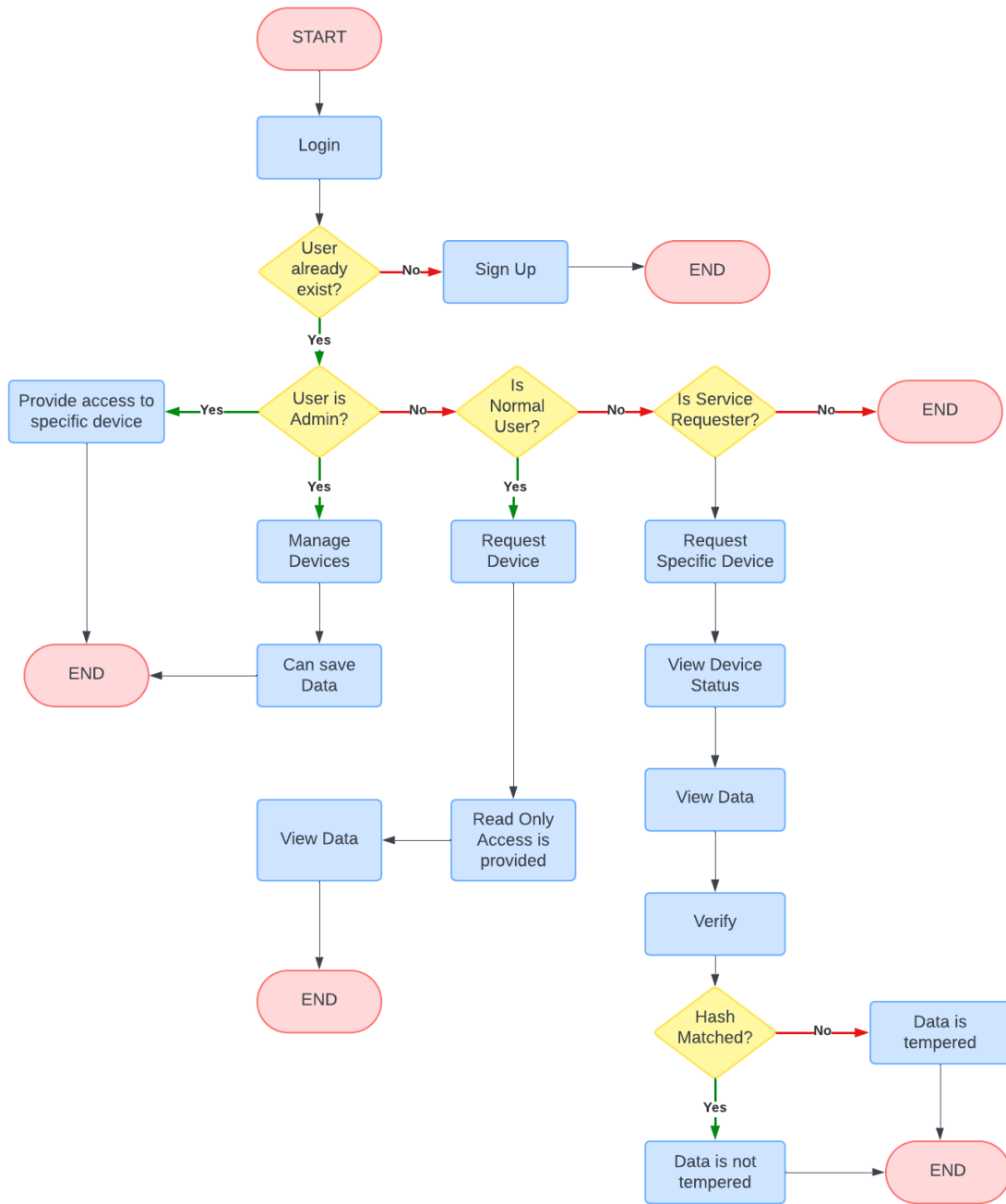


Figure 5. 4: Application Workflow

As seen in the figure 5.4 the work flow ensures data integrity by ensuring access controls for the specific users. Some of the prominent features of this includes:

**Login Prompt:** The user interaction instigates by prompting for credentials, originating the authentication process.



**User Existence Check:** The framework verifies if provided credentials match to a registered account within the system. This initial check confirms only authorized users can continue.

**New User Registration (Sign up):** If the user is not found, the system initiates a separate process for new user registration. This segregation helps maintain data integrity by mitigating unauthorized access over unregistered accounts.

**Admin User Check:** After verifying the user credentials, the framework determines if the user has administrative privileges. Admins are typically assigned with managing system configurations and potentially sensitive data, so the distinction is crucial.

**Admin Access Granted (Manage Devices):** If the user is recognized as an admin, the framework permits access to a dedicated section for managing devices and providing access to specific device. This restricted access compartmentalizes sensitive administrative tasks.

**Normal User Check:** If the user is not an admin, the framework categorizes them as a standard user or a service requester.

**Service Requester Check:** The framework categorizes normal users into service requesters, who have precise device request privileges.

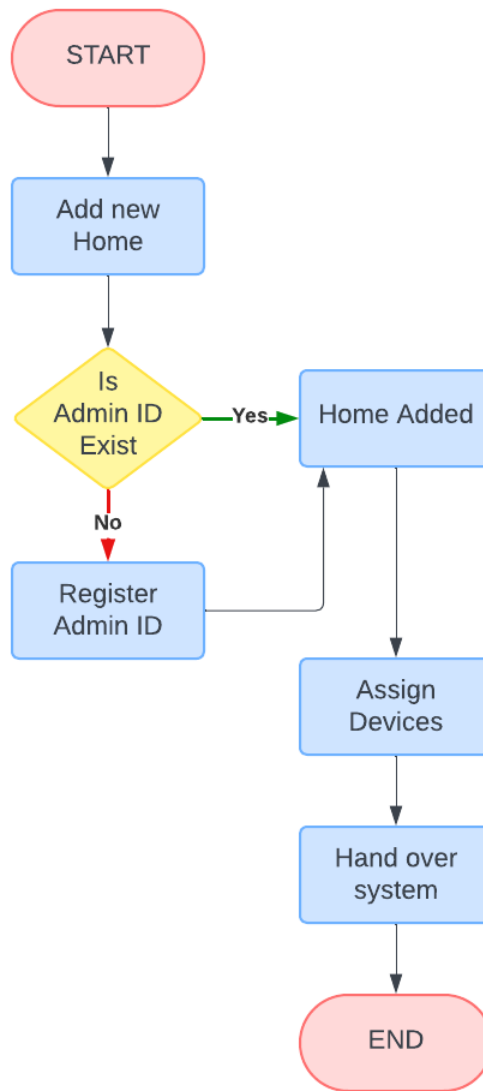
**Device Request Access:** If the user is a service requester, the framework grants permission to request access to particular devices within the system. This access control ensures users can only use authorized devices.

**Data Save Check:** The framework has a data save function, before saving data, it executes a verification step to make ensure the data integrity is preserved.

**Process Termination:** Upon completion of data viewing and saving, the framework ends the user session, following to security best practices.

### **5.7.2 Service provider workflow**

It refers to a third-party company that offers various services to establish a smart home system focused on data integrity and security. The workflow is depicted in the figure 5.5



*Figure 5. 5: Service provider Workflow*

Figure 5.5 enhances data integrity by ensuring home is registered with the system, relating devices with matching homes, and assigning appropriate administrative control. The workflow has several parts which includes:

**Start:** The process initiates with the process to add a new home.

**User Existence Check:** The framework makes sure if the user already exists within the system. This check makes sure duplicate entries are avoided, preventing data inconsistencies and duplication.

**New Home Creation:** If the user does not exist in the system, the framework allows user to create a new password record for that user and creates a home for that particular user. This ensures all homes are properly registered with the system.

**Device Creation:** The framework also allow user to create a new device record, to associate specific devices with the new home. This enhances data organization and device management within a home. New devices will be added to already exiting Device List.

**Assign Device:** The framework authorizes the user to assign devices to newly added home. This step is crucial for assigning appropriate access privileges to manage the home within the system.

**System Handover:** The workflow concludes by a system handover, signifying the completion of the home adding process and granting the admin user access to the system with the newly added home. After that service provider will not have any access to devices of particular home.

## CHAPTER 6

### CONCLUSION AND FUTURE WORK

#### 6.1 Conclusion

The emerging field of smart homes presents a unique challenge in balancing functionality with robust security and data integrity. Many current systems struggle to adequately protect sensitive user information from unauthorized access, falling short of the security and integrity requirements demanded by users.

The emergence of Blockchain technology offers a promising solution to address these critical security and data integrity challenges within smart home environments. This technology, coupled with the increasing popularity of big data, the IoT, and cloud computing, has the potential to revolutionize smart home security.

While traditional centralized cryptographic solutions have been implemented to safeguard smart home data, they often fall short in providing a comprehensive and future-proof solution. This document proposes a novel framework that leverages blockchain technology to address the growing security concerns surrounding smart home data. The authors aim to demonstrate the adaptability, efficiency, and effectiveness of their proposed framework, particularly in the face of evolving cyber threats.

The rapidly increasing realm of smart homes introduces a multitude of security and privacy concerns. Traditional centralized storage systems for smart home data, where information is collected from various sensors (temperature, security systems, lighting), create a single point of vulnerability. If a cybercriminal gains access to this central server, they could potentially tamper with data or compromise the entire system. Blockchain technology offers a promising solution to these challenges. It functions as a distributed ledger technology that securely stores data across a network of computers. Data added to the blockchain is encrypted and chronologically linked to preceding entries, forming an immutable chain. This distributed architecture makes it highly

difficult to tamper with data, as any modifications would require altering all subsequent blocks on the chain.

We highlight the adaptability of the suggested system, which utilize blockchain technologies. Utilizing the advantages of technologies, this solution gets around some of the drawbacks of conventional smart home systems. The framework promises to provide an effective and efficient solution for managing smart home data by using the security and transparency of blockchain technology. This thesis also explains how the problems of data integrity and security in smart home can be solved using the provided architecture. The framework provides a reliable and secure platform for storing, maintaining, and transferring smart home information by integrating blockchain technology. With a flexible and effective system that can handle the rising needs of the smart home business, it guarantees that user and device information is safe from unauthorized access.

## **6.2 FutureWork**

The development to improve the design from a smart city perspective should be the main emphasis of the probable future roadmap. The problem of effective keyword search in smart home can be addressed by the integrated structure of quantum aware blockchain. The methods for search requests, commitments, decryptions, and other operations were created utilizing cutting-edge post-quantum cryptography algorithms. Moreover, benefits of other blockchain platforms may be explored for the same solutions to increase effectiveness of the system.

### **6.2.1 Sharding**

It is a method for dividing the blockchain into more manageable chunks called shards that can execute transactions simultaneously. Smart home providers can boost the smart system's processing of transactions capacity and scalability by implementing sharding. Additionally, sidechains may be used to offload certain tasks off the primary blockchain, such as storing information or complicated computations, further improving scalability.

### **6.2.2 Real World Testing and Deployment**

Real world deployment and testing of this system in an actual IoT environment can be conducted to check the effectiveness of the given system.

### **6.2.3 Larger Data Set**

Further studies can be conducted to evaluate the performance of HLF in smart home systems with larger and more complex data sets.

### **6.2.4 Use of HLF in Other Domains**

Research can be done to investigate the use of HLF in different domains, such as Smart hospitals, Industry, and smart cities, to determine its potential impact in these areas.

### **6.2.5 Other Blockchain Platform**

Benefits of other blockchain platforms may be explored for the same solutions to increase effectiveness of the system.

Data security and privacy must be uncompromised. Through methods like hashing with cryptography, data encryption, and de centralized access control, blockchain offer prospects for improved privacy and security. Future research should concentrate on creating strong privacy-preserving systems that provide scalability with access control while maintaining data security.

## References:

- [1] Yue, S. Du, Y. & Zhang, X. (2021). Research and application of agricultural internet of things technology in intelligent agriculture. *Journal of Physics Conference Series*, 1769(1), 012020.
- [2] Pang, L. , Yang, W. , Xia, B. , & Cheng, Z. . (2020). Development of intelligent warehouse management system based on internet of things technology. *IOP Conference Series: Materials Science and Engineering*, 750(1), 012107 (4pp).
- [3] “Future of industry ecosystems: Shared data and insights,” Available at <https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/> (2022/08/22).
- [4] Alam, Hasibul, and Emmett Tomai. "Security Attacks And Countermeasures In Smart Homes." *International Journal on Cybernetics & Informatics (IJCI)* 12.12 (2023): 109.
- [5] “Number of internet of things (iot) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030,” Available at <https://www.statista.com/statistics/1183457/iot-connected-devicesworldwide/> (2022/08/22).
- [6] Verma, G.; Prakash, S. Emerging Security Threats, Countermeasures, Issues, and Future Aspects on the Internet of Things (IoT): A Systematic Literature Review. In *Advances in Interdisciplinary Engineering*; Kumar, N., Tibor, S., Sindhvani, R., Lee, J., Srivastava, P., Eds.; Lecture Notes in Mechanical Engineering; Springer: Singapore, 2021; pp. 59–66.
- [7] Patnaik, R.; Padhy, N.; Raju, K.S. A Systematic Survey on IoT Security Issues, Vulnerability and Open Challenges. In *Intelligent System Design*; Satapathy, S.C., Bhateja, V., Janakiramaiah, B., Chen, Y.-W., Eds.; *Advances in Intelligent Systems and Computing*; Springer: Singapore, 2021; pp. 723–730.
- [8] Roy, R.; Dheebea, J. Survey on Methodological Model of IoT in Digital Forensic. In *Proceedings of the 2023 International Conference on Intelligent Systems, Advanced*

Computing and Communication (ISACC), Silchar, India, 3–4 February 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6.

[9] Suny, M.F.I.; Fahim, M.M.R.; Rahman, M.; Newaz, N.T.; Akhund, T.M.N.U. IoT Past, Present, and Future a Literary Survey. In Proceedings of the Information and Communication Technology for Competitive Strategies (ICTCS 2020); Jaipur, India, 11–12 December 2020, Kaiser, M.S., Xie, J., Rathore, V.S., Eds.; Lecture Notes in Networks and Systems; Springer Nature: Singapore, 2021; pp. 393–402.

[10] Zhonghua, C.; Goyal, S.B. Blockchain-Based Framework to Handle Security and Privacy for IoT System. In Proceedings of the Third Doctoral Symposium on Computational Intelligence, Lucknow, India, 5 March 2022; Khanna, A., Gupta, D., Kansal, V., Fortino, G., Hassanien, A.E., Eds.; Lecture Notes in Networks and Systems. Springer Nature: Singapore, 2023; pp. 71–82.

[11]. Sun, R., Xi, J., Yin, C., Wang, J., Kim, G. J. (2018). Location privacy protection research based on querying anonymous region construction for smart campus. *Mobile information systems*, 2018.

[12]. Park JH, Salim MM, Jo JH, Sicato JCS, Rathore S, Park JH (2019) CIoT-Net: a scalable cognitive IoT based smart city network architecture. *Human Compu Inf Sci* 9(1):1–29

[13]. Wang J, Gao Y, Liu W, Sangaiah AK, Kim HJ (2019) Energy efficient routing algorithm with mobile sink support for wireless sensor networks. *Sensors* 19(7):1468–1494

[14] I. Zengin, J. Vardakas, N. E. Koltsaklis, and C. Verikoukis, “Smart home’s energy management through a clustering based reinforcement learning approach,” *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 16363–16371, 2022.

[15] F. Shahriyar, M. Islam, A. Chakraborty, M. Hasan, H. U. Zaman, and A. H. Siddique, “Fault and system analysis model of voltage source control based HVDC transmission system,” in Proceedings of the 2021 12th International Conference on Computing



Communication and Networking Technologies (ICCCNT), pp. 1–6, Kharagpur, India, July 2021.

[16] I. V. Paputungan, M. R. Al Fitri, and U. Y. Oktawati, “Motion and Movement Detection for DIY Home Security System,” in Proceedings of the 2019 IEEE Conference on Sustainable Utilization and Development in Engineering and Technologies (CSUDET), pp. 122–125, Penang, Malaysia, November 2019.

[17] M. N. Hassan, M. R. Islam, F. Faisal, F. H. Semantha, A. H. Siddique, and M. Hasan, “An IoT based environment monitoring system,” in Proceedings of the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 1119–1124, Toothukudi, India, December 2020.

[18] P. Mtshali and F. Khubisa, “A smart home appliance control system for physically disabled people,” in Proceedings of the 2019 Conference on Information Communications Technology and Society (ICTAS), pp. 1–5, Durban, South Africa, March 2019.

[19] T. Vaiyapuri, E. L. Lydia, M. Y. Sikkandar, V. G. D’iaz, I. V. Pustokhina, and D. A. Pustokhin, “Internet of things and deep learning enabled elderly fall detection model for smart homecare,” *IEEE Access*, vol. 9, pp. 113879–113888, 2021.

[20] K. Viard, M. P. Fanti, G. Faraut, and J.-J. Lesage, “Human activity discovery and recognition using probabilistic finite state automata,” *IEEE Transactions on Automation Science and Engineering*, vol. 17, no. 4, pp. 2085–2096, 2020.

[21] Popoola, Olusogo, et al. "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions." *Blockchain: Research and Applications* (2023): 100178.

[22] I. Butun, A. Sari and P. Österberg, "Security implications of fog computing on the internet of things," In 2019 IEEE International Conference on Consumer Electronics (ICCE) IEEE., pp. 1 - 6, 2019.

[23] Siqi He; Xiaofei Xing; Guojun Wang; Zeyu Sun “A Data Integrity Verification Scheme for Centralized Database Using Smart Contract and Game Theory”, 2023

- [24] Chunliang Chen a, Liangliang Wang a b, Yu Long c, Yiyuan Luo d, Kefei Chen “A blockchain-based dynamic and traceable data integrity verification scheme for smart homes”, 2022.
- [23] N. Lefkovitz and K. Boeckl, "NIST Privacy Framework: An Overview.," 2020. [Online]. Available: [https://tsapps.nist.gov/publication/getpdf.cfm?pub\\_id=930470](https://tsapps.nist.gov/publication/getpdf.cfm?pub_id=930470). [Accessed 28 February 2021]
- [24] Sun, R., Xi, J., Yin, C., Wang, J., Kim, G. J. (2018). Location privacy protection research based on querying anonymous region construction for smart campus. *Mobile information systems*, 2018
- [25] Robles RJ, Kim TH, Cook D, Das S (2010) A review on security in smart home development. *Int J Adv Sci Technol* 15:13–22
- [26] Park JH, Salim MM, Jo JH, Sicato JCS, Rathore S, Park JH (2019) CIoT-Net: a scalable cognitive IoT based smart city network architecture. *Human Compu Inf Sci* 9(1):1–29.
- [27] Wang J, Gao Y, Liu W, Sangaiah AK, Kim HJ (2019) Energy efficient routing algorithm with mobile sink support for wireless sensor networks. *Sensors* 19(7):1468–1494.
- [28] Abdulwahab Alazeb and Brajendra Panda. “Ensuring data integrity in fog computing based health-care systems”. In: *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 12th International Conference, SpaCCS 2019, Atlanta, GA, USA, July 14–17, 2019, Proceedings 12*. Springer. 2019, pp. 63– 77.
- [29] Wenjun Luo and Guojing Bai. “Ensuring the data integrity in cloud data storage”. In: *2011 IEEE International Conference on Cloud Computing and Intelligence Systems*. IEEE. 2011, pp. 240–243.
- [30] M. A. Ali Eghmazi, "Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy," vol. 1, no. Security, p. 15, 2024.
- [31] B. L. Xueyan Yao, "Blockchain-based public audit scheme for smart home data integrity," vol. 3, no. smart home security, p. 16, 2023.

- [32] S. Kumar, "A BLOCKCHAIN-BASED SOLUTION FOR ENSURING PROVENANCE TO OUT," vol. 1, p. 18, 2023.
- [33] Aaasha Aldahmani, Bassem Ouni, Thierry Lestable, And Merouane Debbah "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends", p. 12, 20222
- [34] S. S. Dhanda, B. Singh and P. Jindal, "Lightweight cryptography: A solution to secure IoT.," *Wireless Personal Communications* , vol. 112 , no. 3, pp. 1947-1980, 2020
- [35] C. Wirth and M. Kolain, "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data.," In *Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET).*, 2018.
- [36] G. S. Poh, P. Gope and J. Ning, "PrivHome: Privacy-preserving authenticated communication in smart home environment.," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1095 -1107, 2019.
- [37] S. Lee, J. Choi, J. Kim, B. Cho, S. Lee, H. Kim and J. Kim, "FACT: Functionality-centric access control system for IoT programming frameworks.," In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies.*, pp. 43-54, 2017.
- [38] Muthumanikandan, V., Valliyammai, C., Swarna Deepa, B. (2019). Switch Failure Detection in Software-Defined Networks. In: Peter, J., Alavi, A., Javadi, B. (eds) *Advances in Big Data and Cloud Computing. Advances in Intelligent Systems and Computing*, vol 750. Springer, Singapore
- [39] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home.," In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* , pp. 618-623, 2017.

- [40] S. Namasudra, S. Nath and A. Majumder, " Profile based access control model in cloud computing environment.," In 2014 International Conference on Green Computing Communication and Electrical Engineering, pp. 1-5, 2014.
- [41] Alpa, "Proof-of-Authority consensus," 2018. [Online]. Available: <https://apla.readthedocs.io/en/latest/concepts/consensus.html>. [Accessed 10 October 2021].
- [42] Q. Wang, T. Xia, Y. Ren, L. Yuan and G. Miao, " A New Blockchain-Based Multi-Level Location Secure Sharing Scheme.," Applied Sciences., vol. 11, no. 5, p. 2260, 2021.
- [43] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. K. R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart homes.," IEEE Internet of Things Journal, vol. 7, no. 2, pp. 818-829, 2019.
- [44] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai and D. Trentesaux, "A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0.," Sustainability, vol. 12, no. 21, p. 9179, 2020.
- [45] K. Hameed, M. Barika, S. Garg, M. B. Amin and B. Kang, " A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues.," Journal of Industrial Information Integration, vol. 26, no. 1, p. 100312., 2022.
- [46] M. Alwabe and Y. Kwon, "Blockchain Consistency Check Protocol for Improved Reliability.," Computer Systems Science & Engineering., vol. 36, no. 2, 2021.
- [47] D. Cocîrlea, C. Dobre, L. A. Hîrţan and R. Purnichescu-Purtan, "Blockchain in intelligent transportation systems," Electronics, vol. 9, no. 10, p. 1682, 2020.
- [48] A. S. Bale, T. P. Purohit, M. F. Hashim and S. Navale, "Blockchain and Its Applications in Industry 4.0.," A Roadmap for Enabling Industry 4.0 by Artificial Intelligence, pp. 295-313, 2022.

- [49] A. O. Almagrabi, R. Ali, D. Alghazzawi, A. AlBarakati and T. Khurshaid, "Blockchain-as-a-Utility for Next-Generation Healthcare Internet of Things.," *Computers, Materials & Continua*, vol. 68, no. 1, 2021.
- [50] Q. Wang, R. Li and L. Zhan, "Blockchain technology in the energy sector: From basic research to real world applications," *Computer Science Review*, vol. 39, p. 100362, 2021.
- [51] VeChain, "VeChain Whitepaper 2.0," VeChain Foundation, [http://www.vechain.org/qfy-content/uploads/2020/01/VeChainWhitepaper\\_2.0\\_en.pdf](http://www.vechain.org/qfy-content/uploads/2020/01/VeChainWhitepaper_2.0_en.pdf), 2019.
- [52] VeChain, "VeChain Whitepaper 2.0 - Creating Valuable TXs on The VeChainThor Blockchain," VeChain Foundation, 12 2019. [Online]. Available: [https://www.vechain.org/whitepaper/#bit\\_65sv8](https://www.vechain.org/whitepaper/#bit_65sv8). [Accessed 2 December 2021].
- [53] S. Gaba, H. Khan, K. J. Almalki, A. Jabbari, I. Budhiraja, V. Kumar, A. Singh, K. Singh, S. Askar and M. Abouhawwash, "HoloChain: An Agent-Centric Distributed Hash Table Security in Smart IoT Applications.," *IEEE Access.*, 2023.
- [54] A. A. Kamran, I. U. Din, A. Almogren, A. K. Hasan and J. P. C. R. Joel, "EdgeTrust: A lightweight data-centric trust management approach for IoT-based healthcare 4.0.," *Electronics*, vol. 12, no. 1, p. 140, 2023.
- [55] A. Aftab, C. Chrysostomou, H. K. Qureshi and S. Rehman, "Holo-Block Chain: A Hybrid Approach for Secured IoT Healthcare Ecosystem.," In *2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, pp. 243-250, 2022.
- [56] S. Zaman, M. R. Khandaker, R. T. Khan, F. Tariq and K. K. Wong, "Thinking out of the blocks: HoloChain for distributed security in IoT healthcare," *IEEE Access.*, vol. 10, pp. 37064-37081, 2022.
- [57] K. Janjua, M. A. Shah, A. Almogren, H. A. Khattak, C. Maple and I. U. Din, "Proactive forensics in IoT: Privacy-aware log-preservation architecture in fog-enabled-

cloud using holochain and containerization technologies.," *Electronics*, vol. 9, no. 7, p. 1172, 2020.

[58] H. D. Zubaydi, P. Varga and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review.," *Sensors.*, vol. 232, p. 788, 2023.

[59]Eghmazi, Ali, et al. "Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy." *IoT 5.1* (2024): 20-34.

[60] Zhicheng Lin and and Stephen S. Yau. "A Blockchain-Based Approach to Improving Smart Home Security With Situation-Aware Access Control", *IEEE International Conference on Blockchain*, pp. 1-8, 2023.

[61] Aurelle Tchagna Kouanou, Christian Tchito Tchapgga, Michael Sone Ekonde, Valery Monthe, Brice Anicet Mezatio, Josépha Manga, Gael R. Simo & Yves Muhozam, "Securing Data in an Internet of Things Network Using Blockchain Technology: Smart Home Case", *SN Computer Scieince*, pp. 1-12, Feb. 2022.

[62] Baucas, Marc Jayson, Stephen Andrew Gadsden, and Petros Spachos. "IoT-based smart home device monitor using private blockchain technology and localization." *IEEE Networking Letters* 3.2 (2021): 52-55.

[63]Khan, Muhammad Adnan, et al. "A machine learning approach for blockchain-based smart home networks security." *IEEE Network* 35.3 (2020): 223-229.

[64] Y. Nakamura, Y. Zhang, M. Sasabe and S. Kasahara, "Capability-based access control for the Internet of Things: An Ethereum blockchain-based scheme", *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pp. 1-6, Dec. 2020.

[65] Lee, Y., Rathore, S., Park, J.H. et al. "A blockchain-based smart home gateway architecture for preventing data forgery". *Hum. Cent. Comput. Inf. Sci.* 10, 9 (2020). <https://doi.org/10.1186/s13673-020-0214-5>.

[66] M. Moniruzzaman, S. Khezr, A. Yassine and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges", *Comput. Electr. Eng.*, vol. 83, May 2020.

- [67] Lin, Chao, et al. "HomeChain: A blockchain-based secure mutual authentication system for smart homes." *IEEE Internet of Things Journal* 7.2 (2019): 818-829.
- [68] Saxena, Utkarsh, J. S. Sodhi, and Rajneesh Tanwar. "Augmenting smart home network security using blockchain technology." *International Journal of Electronic Security and Digital Forensics* 12.1 (2020): 99-117.
- [69] Singh, Pranav Kumar, et al. "Managing smart home appliances with proof of authority and blockchain." *Innovations for Community Services: 19th International Conference, I4CS 2019, Wolfsburg, Germany, June 24-26, 2019, Proceedings* 19. Springer International Publishing, 2019.
- [70] I. C. Vidal, F. Rousseau and J. C. Machado, "Achieving differential privacy in smart home scenarios", *Proc. 34th Anais Principais do Simpósio Brasileiro de Banco de Dados*, pp. 211-216, 2019.
- [71] R. Yang, F. R. Yu, P. Si, Z. Yang and Y. Zhang, "Integrated blockchain and edge computing systems: A survey of some research issues and challenges", *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508-1532, Feb. 2019.
- [72] W. Ejaz and A. Anpalagan, "Internet of Things for Smart Cities: Technologies Big Data and Security", Cham, Switzerland: Springer, 2019.
- [73] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: *Bitcoin.org* (2008).
- [74] Sunny King and Scott Nadal. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake". In: (2012).
- [75] Dan Larimer. "Delegated Proof-of-Stake (DPoS)". In: (2014).
- [76] Miguel Castro and Barbara Liskov. "Practical Byzantine fault tolerance". In: *ACM Transactions on Computer Systems (TOCS)* 20.4 (1999), pp. 398–461.
- [77] Kyle Croman et al. "Scalable Byzantine fault tolerance". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2016, pp. 716–727.

[78] Yael Ren, Shouling Liu, and Hector Garcia-Molina. “PoET: Practical Byzantine fault tolerance via Proof of Elapsed Time”. In: Proceedings of the 26th Symposium on Operating Systems Principles. ACM. 2017, pp. 87–102.

[79] Aggelos Kiayias et al. “Ouroboros: A provably secure proof-of-stake blockchain protocol”. In: Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part I. Springer. 2017, pp. 357–388.

[80] Serguei Popov. “The tangle”. In: IEEE European Symposium on Security and Privacy Workshops. IEEE. 2017, pp. 31–36.

[81] Jae Buchman et al. “Tendermint: Byzantine Fault Tolerance in the Age of Blockchains”. In: International Conference on Financial Cryptography and Data Security. Springer. 2014, pp. 447–462.

[82]<https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>