Matter Tunnel

Dongwook Kim
College of Engineering
Hanyang University
Dept.of Information Systems
Seoul, Korea
dongwook1214@gmail.com

Jisu Shin
College of Engineering
Hanyang University
Dept.of Information Systems
Seoul, Korea
sjsz0811@hanyang.ac.kr

Giram Park
College of Engineering
Hanyang University
Dept.of Information Systems
Seoul, Korea
kirammida@hanyang.ac.kr

Seoyoon Jung
College of Engineering
Hanyang University
Dept.of Information Systems
Seoul, Korea
yoooonnn@naver.com

***Abstract*—Our team introduces "Matter Tunnel," which enables the Matter protocol to operate on a blockchain basis. Matter is a protocol that provides interoperability between IoT devices from various manufacturers, allowing control of multiple brands of IoT devices from a single application. However, due to current network constraints such as NAT and firewalls, a dedicated Matter hub is required when using Matter devices. Matter Tunnel resolves the current limitations of Matter by utilizing blockchain technology, operating as if creating a virtual private network between applications and IoT devices. Primarily, it eliminates the mandatory use of Matter hubs, significantly enhancing user experience and flexibility. This innovation also extends the operational range of Matter devices, allowing them to be placed and controlled beyond the confines of a home. Users can easily manage devices in various environments such as home, workspaces, and vehicles through a single application. From an enterprise perspective, All device interactions and transactions are permanently recorded on the blockchain, providing businesses with reliable, immutable data for tracking device usage patterns and extracting valuable operational insights. Furthermore, Matter Tunnel ensures platform independence, freeing users from being locked into specific ecosystems. It strengthens security by enabling complete end-to-end encryption (E2EE) and enhances user privacy. Additionally, by lowering entry barriers, Matter Tunnel opens up opportunities for small development teams to participate in the Matter ecosystem. With these improvements, users can enjoy a more secure, versatile, and unrestricted IoT experience.**

***Index Terms*—Matter Tunnel, Matter, Blockchain, Matter hub, user experience, E2EE**

TABLE I
ROLE ASSIGNMENTS

Roles	Name	Task description and etc.
Development manager Blockchain Developer	Dongwook Kim	The role involves designing and implementing solutions utilizing blockchain technology. This position sets the technical direction for projects and applies the latest blockchain trends and technologies. Responsibilities include developing smart contracts, optimizing blockchain protocols, managing team members' work, and developing their skills.
User, Customer, Front-end Developer	Jisu Shin	From user and customer perspective, considers what features would enhance the IoT experience and how to improve user interaction. From a development perspective, designs and implements user interfaces for IoT applications, focusing on intuitive and responsive front-end solutions that integrate with Matter protocol and blockchain technology.
User, Customer, Embedded Developer	Giram Park	From a user standpoint, evaluates how IoT devices can better serve everyday needs. As an Embedded developer, works on firmware and software for IoT devices compatible with the Matter protocol and proposed blockchain solution. Focuses on implementing user-centric features that enhance device functionality, improve reliability, and simplify setup processes.
User, Customer, Front-end Developer	Seoyoon Jung	From user and customer perspective, considers what features would enhance the IoT experience and how to improve user interaction. From a development perspective, designs and implements user interfaces for IoT applications, focusing on intuitive and responsive front-end solutions that integrate with Matter protocol and blockchain technology. Aims to create user-friendly interfaces that simplify device control and management.

I. INTRODUCTION

A. Motivation

The rapid advancement of Internet of Things (IoT) technology has led to significant growth in the smart home market. However, compatibility issues among IoT devices from various manufacturers have been a persistent challenge. To address this problem, the Matter protocol was developed, offering an approach that enables control of IoT devices from multiple brands through a single application.

Despite the introduction of the Matter protocol, the current implementation still harbors several crucial issues. These problems prevent the full realization of Matter's original goals: true interoperability, security, and protection of user privacy.

Therefore, we believe a new approach is necessary to overcome these limitations and maximize the potential of the Matter protocol.

B. Problem Statement

The current implementation of the Matter protocol presents the following key issues:

Mandatory use of Matter hubs: Network limitations such as NAT and firewalls make direct P2P communication between IoT devices and applications challenging in typical households. This necessitates the use of dedicated Matter hubs.

Limited Operational Range: As a consequence of the mandatory use of Matter hubs, the operational range of Matter is confined to the home. This limitation restricts the potential for broader IoT applications and remote device management beyond the immediate household environment.

Platform Dependency: The need for platform-specific solutions, such as Apple's "HomeKit" and "HomePod" or Google's "Google Home" and "Nest Hub," results in consumers being locked into particular platforms.

Limited End-to-End Encryption (E2EE): The advantage of E2EE in the Matter protocol is confined to operation within private networks, failing to ensure complete security throughout the entire communication process.

Threats to User Privacy: The communication structure that routes through cloud services potentially threatens user privacy.

Centralized Authentication System: Matter devices must be certified by a centralized root certificate authority (CA), which makes it difficult for small development teams to participate and limits consumer choices.

These issues hinder the original purposes of the Matter protocol: interoperability, security, and openness.

Moreover, the existing centralized server-based IoT architecture presents significant challenges for businesses:

Data Reliability and Trust Issues: The centralized server architecture creates vulnerability in data integrity, making it challenging for businesses to maintain reliable records. Without an immutable ledger system, businesses cannot ensure the authenticity and accuracy of device interaction data, which is crucial for operation analysis and service improvement.

Data Analysis and Tracking Problems: Traditional centralized IoT systems lack comprehensive data tracking mechanisms. This limitation makes it difficult for businesses to effectively analyze device usage patterns, maintain accurate maintenance histories, and extract valuable insights for business optimization. The fragmented nature of data across different platforms and environments further complicates the analysis process.

Therefore, we have determined that a new approach is necessary to overcome these limitations and fully realize the potential of the Matter protocol. We propose a solution utilizing blockchain technology to address these challenges.

C. Research on related technical elements

1) Matter

We use a variety of IoT devices, and several manufacturers develop and sell IoT devices with different names and appearances. It is Matter that enables these various smart home devices to be connected and managed at once.

Matter is an IP-based smart home interworking standard that is compatible with all devices, designed to overcome the manufacturer-dependent limitations of smart home devices. It was launched in 2019 by four IoT giants Apple, Amazon, Google, Samsung SmartThings, and the global association CSA, formerly the Zigbee Alliance, and renamed Matter in 2021.

Matter has the following technical features:

Unlike existing ZigBee and Z-Wave, Matter operates based on IP protocols. Since Matter is based on IP, which is a network layer protocol, the communication protocol below it does not matter, and eventually all processing is done at the application layer. In other words, the transmission method varies depending on what the application is, but as long as IP is used, the method is not important. Therefore, devices with the Matter logo can work together regardless of brands or supported transmission protocols. In addition, the reason why it is important to use IP is that IP protocols are already proven in the market in terms of interoperability and security.

Matter is interoperable between devices. Matter allows each device to interact using the same protocol, even if it is from a different manufacturer. For example, Samsung Electronics' products have been linked to SmartThings, and LG Electronics only to the ThinQ platform, but now Samsung Electronics' products can be connected to ThinQ. Matter is a very desirable standard from a user's point of view because most homes use a mixture of products from multiple brands.

Matter supports both Wi-Fi and Thread, a low-power mesh network protocol, and supports various network protocols, such as using BLE in the device setting process.

In addition, Matter has the characteristics of Multi-Admin, which uses the same device in conjunction with multiple platforms, AES authentication prescribed by NIST in the United States regarding data encryption, and PKI and certificates for device authentication.

An open ecosystem is being created with the introduction of Matter with these characteristics, and the trend of automation and intelligence of residential environments is spreading through integration with Generative AI technology. Korea is also promoting active efforts to build and expand a smart home ecosystem by preparing support

plans in line with global trends. The Korean government is expanding policy support by promoting 'AI@Home', a project centered on Matter and Generative AI, to support the creation of a smart home ecosystem.

However, privacy protection, application of smart home technology of existing houses, and high installation costs are challenges that limit the growth of the market, so it is necessary to proactively prepare countermeasures.

2) Network Constraints in P2P Communication

In a Peer-to-Peer (P2P) structure, there is minimal reliance on always-on infrastructure servers. Instead, the application allows pairs of intermittently connected hosts, called peers, to communicate directly with each other. Peers are desktops and laptops controlled by users rather than owned by service providers, and most peers are located in homes, universities, and offices. Since communication occurs directly between peers without passing through a specific server, this structure is referred to as Peer-to-Peer.

Network constraints in P2P communication negatively impact user experience by assigning additional complex tasks to users.

NAT (Network Address Translation) and Firewalls: When many peers are behind NAT, NAT converts the private network's IP addresses into public IP addresses, allowing communication with external networks. However, NAT can block incoming connections, making it difficult for peers behind NAT to be accessed directly from the outside. Firewalls also block incoming connections from external networks, hindering communication between peers. To address these constraints, NAT traversal technologies like STUN, TURN, and ICE are required, or users may need to manually configure complicated network settings, such as port forwarding, to facilitate incoming connections. These manual configurations can bypass NAT and firewall restrictions, enabling direct access to specific services within the internal network from external sources.

3) Matter hub

Matter Hub is a central component of the Matter ecosystem, designed to facilitate seamless communication and interoperability between smart home devices from various manufacturers. Matter aims to unify different smart home technologies, allowing devices to work together regardless of brand.

Smart Home Hubs serve as central controllers for smart home devices, enabling communication between Matter-compatible devices from different manufacturers. Samsung SmartThings and Amazon Echo are representative examples.

Matter Hubs connect Matter devices to the internet and other networks, allowing for remote access and control. Notable examples include Google Nest Hub, which integrates with Google services, and Apple HomePod, which utilizes Siri for voice commands.

While Matter Hubs play a crucial role in enhancing interoperability within the smart home ecosystem, it's important to note that using Matter devices typically requires a home hub. Each application may dictate the specific Matter hub that must be used, which can strictly lock users into particular platforms. This limitation highlights the need for greater flexibility and broader compatibility in the Matter ecosystem to ensure a truly open and user-friendly IoT environment.

4) Blockchain

To effectively integrate blockchain technology into the IoT industry, it is crucial to consider blockchains with high transaction processing speeds (TPS) and enterprise-friendly features.

Several blockchain platforms stand out for their high TPS capabilities, including:

Solana: Solana is an innovative platform designed for mainstream adoption. The core development team, including co-founder Anatoly Yakovenko, focused on scalability and efficiency based on their experience in building telecommunications networks. By implementing Proof of Stake (PoS) and Proof of History (PoH), they achieved a throughput of up to 65,000 TPS and realized very low transaction fees ($0.00025). It's also highly energy efficient, consuming less power than a typical household refrigerator.essing up to 65,000 transactions per second

XRP: XRP (Ripple) uses the RPCA consensus algorithm and provides approximately 1,500 TPS throughput. Specialized in international remittance, it has established partnerships with many banks and financial institutions, featuring fast transaction completion times of 3-5 seconds.

Hyperledger Fabric: Hyperledger Fabric is an enterprise blockchain platform that provides 2,000-20,000 TPS throughput. Through various network configurations, organizations can adjust the throughput and degree of centralization according to their needs. For example, by modifying parameters such as the number of organizations, ordering service nodes, peer nodes, and channels, administrators can find the optimal balance between performance and decentralization.

Among enterprise-friendly blockchain platforms, the following are noteworthy:

Hyperledger Fabric: Hyperledger Fabric features a modular architecture and permissioned blockchain characteristics, supporting channel-based data partitioning. It has various enterprise use cases including supply chain

management, asset tracking, identity management, and healthcare data management.

Quorum: Quorum, developed by JP Morgan, is an enterprise blockchain based on Ethereum, featuring enhanced privacy features and high throughput. It supports private transactions, voting-based consensus mechanisms, role-based access control, and multi-signature contracts.

Hyperledger Besu: Hyperledger Besu is a Java-based blockchain platform compatible with Ethereum. It supports both public and private networks and provides enterprise-grade governance. It is being utilized in various fields including financial services, supply chain management, digital asset management, and inter-enterprise collaboration platforms.

After careful consideration of these options, Hyperledger Fabric is judged as the most suitable blockchain platform for the IoT industry. It offers a combination of high TPS and enterprise-grade features that are essential for large-scale IoT implementations. Furthermore, Hyperledger Fabric is compatibility with Monachain, a blockchain platform developed by LG CNS based on Hyperledger Fabric. This compatibility allows for seamless integration and immediate application in existing systems, potentially accelerating adoption and reducing implementation barriers.

5) Arduino

Arduino is an open-source electronics platform based on easy-to-use hardware and software. In the context of Matter IoT, Arduino plays a significant role due to its flexibility, ease of use, and strong community support. When considering Arduino for Matter IoT applications, the following aspects are crucial:

Processing power: Matter protocol requires sufficient computational resources to handle encryption and network communication.

Connectivity options: Wi-Fi or Ethernet capability is essential for Matter, as it's IP-based.

Memory capacity: Adequate RAM and flash memory to run Matter stack and application code.

Power efficiency: For battery-operated IoT devices, low power consumption is critical.

Compatibility with Matter SDK: The board should be capable of running the Matter SDK.

Some Arduino boards suitable for Matter IoT projects include:

Arduino Nano 33 IoT: This compact board features Wi-Fi connectivity and a powerful SAMD21 microcontroller, making it suitable for small Matter devices.

Arduino MKR WiFi 1010: With its low power consumption and robust Wi-Fi capabilities, it's excellent for battery-operated Matter devices.

Arduino Portenta H7: This high-performance board with dual-core processor and multiple connectivity options is ideal for more complex Matter applications.

ESP32-S3: While not an official Arduino board, the ESP32-S3 is widely used in the Arduino ecosystem and offers powerful processing capabilities, Wi-Fi and Bluetooth connectivity, and ample memory.

These boards offer various combinations of processing power, connectivity, and memory, allowing developers to choose the most suitable option for their specific Matter IoT application

6) Web Assembly

Web Assembly (Wasm) is a binary instruction format designed for efficient execution in web browsers. It serves as a portable target for compilation of high-level languages like C, C++, and Rust, enabling deployment on the web for client and server applications.

Key features and benefits of Web Assembly in the context of IoT and Matter include:

Language Versatility: Web Assembly allows developers to use languages like C, C++, or Rust in web environments. This is particularly beneficial for IoT applications, as these languages are commonly used in embedded systems development.

Performance: Wasm provides near-native performance, making it suitable for computationally intensive tasks often required in IoT applications.

Code Reusability: It enables the use of the same codebase across different platforms - from embedded devices to web interfaces. This is especially valuable for functions like encryption and decryption, where consistent implementation across platforms is crucial.

Frontend Capabilities: Web Assembly empowers frontend applications to perform complex operations typically associated with backend or embedded environments. This can include data processing, encryption, and other intensive computations directly in the browser.

In the context of Matter, Web Assembly can play a significant role in creating consistent, high-performance interfaces for controlling and managing IoT devices across different platforms. It allows developers to implement complex Matter protocol operations in web applications, maintaining consistency with the implementations on the devices themselves. This consistency across platforms is particularly valuable for ensuring that security measures, device interactions, and data handling are uniform across the entire Matter ecosystem.

D. Research on related study

1) Benefits of Blockchain for Data Mining

The synergy of blockchain technology and data mining techniques for anomaly detection introduces effective methods for detecting anomalies through the interaction of blockchain and data mining. Data stored on the blockchain can be considered big data, and data mining techniques are useful for extracting hidden patterns or knowledge from blockchain. This paper presents analytical approaches to blockchain data and practical application examples, explaining how these technologies can contribute to anomaly detection and fraud prevention.

Using blockchain allows for transparent recording of all data, making data tracking and monitoring easier. It can serve as a valuable tool for data analysis when companies process information, and one of its significant advantages is the ability to quickly detect changes in system operations or the occurrence of fraud.

Specific application examples of this in the literature are as follows :

Analysis of Bitcoin Transaction Networks : Zola et al. analyzed changes in Bitcoin transaction patterns by utilizing the time-series data of the blockchain. They used data from WalletExplorer and the Bitcoin mainnet over the past three years, calculating F1 scores through k-fold cross-testing. By analyzing the transaction data linked in chronological order on the blockchain, it is possible to detect cybersecurity threats and identify changes in behavioral patterns.

Blockchain Data Collection and Analysis : Brinckman et al. presented techniques for crawling, collecting, and analyzing blockchain data. They demonstrated a method for clustering transactions and extracting account characteristics to identify fraudulent accounts, which serves as a good example of understanding the data structure of the blockchain and effectively analyzing it.

Time-Series Transaction Data Analysis : Zhao et al. analyzed the entire dataset of the Ethereum blockchain from a temporal perspective. They utilized the ethereum blockchain dataset from the Bigquery Public Data Repository to examine changes in transaction patterns over time, comparing the accuracy of Random Forest and Logistic Regression, and visualizing the temporal evaluation of the collected data.

These application examples demonstrate that effective analysis is possible by leveraging the connected data structure and temporal characteristics of the blockchain. In particular, the data structure of the blockchain can be effectively utilized to identify patterns in large-scale transaction data and detect anomalous behaviors, which can be considered a significant advantage of blockchain-based data analysis.

2) Benefits of Blockchain for Data Integrity and Accessibility

A representative project to use blockchain in the health care field is MedRec, which enables overall management of medical data, such as providing medical data by medical institutions, licensing by patients, and using medical data by research institutes, using blockchain. MedRec 2.0 is conducted using Go-hereum and Solidity languages, and uses smart contracts on the Ethereum blockchain to enable data exchange without intermediaries. MedRec, like other blockchains, secures security and safety as a blockchain. Due to the decentralized nature of the blockchain, data is maintained on all nodes on the network and stored in the nodes of patients and their service providers. The consensus mechanism of the blockchain can avoid security problems caused by vulnerabilities in any one place. In addition, if one node is modified, such as when modifying a specific transaction in a specific block, the modified node becomes inconsistent with the other and is excluded from the agreement, thereby maintaining the integrity of records on the blockchain.

Estopia is secured with KSI blockchain by combining KSI blockchain, and data of data. The company Estonian eHe Health Foundation and Guide has strengthened security and monitoring function of patients by combining KSI blockchain by combining KSI blockchain. The Ministry of Health and Medical System was able to integrate data related to medical services related to X-Road, a data exchange platform, and enables data analysis of medical services related to medical services. This system provides personal, family, family, medical services providers, family, medical services providers transmit the integrity of medical data to the KSI server and permanently record blockchain and offline. In particular, the doctor through ”e-first-first service,” the doctor and pharmacies and pharmacies were able to check the integrity of prescription of prescription of prescription. In addition, maintain data as ”electronic health registration service” and doctors, doctors were able to check the medical image, such as X-ray Kids ID code alone in the patient ID code alone. These systems have enabled the secure storage, efficient sharing, and integrity verification of medical data.

Mediblock is a blockchain-based integrated management platform for personal medical data that aims for a platform that can integrate distributed patient medical data. Mediblock secures security by granting patients access to medical data and allowing only them to decrypt the entire data, and records the hash value of the data on the blockchain to ensure integrity. It improves the reliability of data by allowing only certified medical personnel to write medical records of others, and provides high transparency by recording data access information and access rights on the blockchain. In addition, it is possible to safely share data through services that act as data relay and secondary backup storage, and data transactions are made in an encrypted state through the data trading

market within the platform, allowing data to be used without the risk of leakage.

As such, many studies are being conducted to utilize blockchain technology, and as shown in the above three cases, blockchain technology provides important advantages such as enhancing data integrity and security, improving accessibility and transparency, and efficient data integration and utilization. These advantages can also be applied to the implementation of blockchain-based Matter tunnels that replace Matter hubs, which in turn can greatly improve the reliability and efficiency of Matter.

II. Requirements

A. Core Requirements

The solution proposed in this study must meet the following key requirements

1) Eliminate the mandatory use of Matter hubs

   it must eliminate the mandatory use of Matter hubs, enabling direct and secure device-to-application communication without relying on intermediary hardware. This removal of hub dependency not only reduces system complexity and cost but also enhances system reliability by eliminating single points of failure.

2) Extended Operational Range

   The solution should overcome the limitation of traditional Matter hub-based systems, which confine device operation to a home network. It must enable secure and efficient management and control of IoT devices from remote locations, expanding the utility of Matter-compatible devices beyond the immediate household environment. This extended range should not compromise security or user privacy.

3) Enhanced data tracking mechanisms

   The solution must incorporate enhanced data tracking mechanisms that provide comprehensive visibility into device operations, interactions. This tracking system should maintain tamper-proof records of all device activities, enabling businesses to analyze usage patterns, monitor performance metrics, and optimize their operations effectively. The implementation should support both real-time monitoring and historical data analysis while maintaining user privacy and data security.

4) Improved system reliability

   To ensure system reliability and trust, all data interactions and transactions must be recorded on an immutable ledger, creating a verifiable and transparent history of device operations. This trustworthy data foundation is crucial for both operational intelligence and regulatory compliance, allowing businesses to make data-driven decisions with confidence. The system should provide mechanisms for data verification and validation while maintaining appropriate access controls and privacy measures.

5) decentralization

   The solution should embrace decentralization by removing dependencies on centralized certificate authorities (CAs) and platform-specific ecosystems. This decentralization should establish a more democratic and open IoT ecosystem where small developers and manufacturers can participate freely, fostering innovation and competition. Furthermore, the solution allow IoT devices from various manufacturers to interact seamlessly.

6) Enhanced End-to-End Encryption (E2EE)

   E2EE should be guaranteed even outside private networks, maintaining data confidentiality throughout the entire communication process.

7) User Privacy Protection

   It should reduce reliance on centralized cloud services for communication and minimize the collection and use of user data while managing it transparently.

8) Interoperability

   The solution must maintain full compatibility with the existing Matter protocol while concurrently supporting Matter Tunnel. It should provide backward compatibility for legacy devices and forward compatibility for future Matter protocol updates, ensuring a cohesive ecosystem that evolves without disrupting existing setups.

9) Real-time Performance

   The solution must support real-time communication and responsiveness, even when utilizing blockchain technology. It should ensure that blockchain integration does not introduce significant latency or delays in device interactions. The system should maintain quick response times for user commands and device state updates, while leveraging the benefits of blockchain for enhanced security and decentralization.

10) Development Convenience

    It should support Matter Tunnel with minimal code changes to existing Matter devices and provide a simple API that developers can easily understand and implement.

    By meeting these requirements, the proposed solution is expected to overcome the limitations of the current Matter hub-based Matter protocol and provide a better user experience, security, and privacy.

B. Development Requirements

1) User Authentication

The login system should prioritize security, simplicity, and compatibility with the Matter protocol. To achieve this, we propose implementing a login mechanism based on asymmetric cryptography, specifically using the secp256k1 elliptic curve algorithm, which is also employed by Matter. Users can easily log in by entering their secp256k1 private key instead of using social login methods.

a) Sign Up

Users can initiate the registration process by clicking the Sign Up button on the login page of the application. During the sign-up process, users will create their private key, which will serve as their unique identifier for logging in. Generated private key will be securely stored in local storage. If desired, users can retrieve their private key at any time from the application's account management section. This feature allows users to back up or transfer their private key to another device if needed.

b) Login

Users can log in by entering their private key. Upon successful login, a public key is derived from the private key, and users are directed to a page where they can register Matter devices. If the entered key doesn't match the required format, an error message starting "Your key is incorrectly formatted" will be displayed.

2) Add Device

To register a Matter-compatible device, the user clicks the '+' button to add a new device. User can scan the QR code or enter the setup code provided by the device to proceed with the registration. The device information will be stored in the local storage. Once the device is successfully registered, the user gets registration confirmation message and will be directed to a screen displaying the device status and features.

3) Remove Device

To remove an unnecessary device, the user select the device and click the 'Remove' button. The user will be prompted to confirm choice before the device is removed from the system. Upon confirming the removal, the system will delete the device from the local storage and the user will receive a message confirming the successful deregistration. If an error occurs during the process, an error message will be provided.

4) Device Control

A user-friendly interface will be designed for controlling each device, focusing on intuitive navigation and clear functionality. The interface will display available control options. When the user issues a command to control a device, the command will be executed through communication with the blockchain and the device. Feedback will be provided to the user upon successsful command execution. User can set devices to operate automatically based on specific time or conditions. The application will allow users to configure and manage their automations.

5) Data Display

Matter devices transmit a variety of signals to the application through the Matter Tunnel. These signals are structured in various formats to accommodate diverse data types and use cases. The formats include, but are not limited to, JSON, binary data. Each format serves a specific purpose, allowing for flexible and efficient data transmission.

The application is responsible for processing these diverse signals and presenting them to users in a manner that aligns with their respective data formats. Upon receiving the signals, the application will parse and interpret the data to ensure it is accurately represented. The transformed data will then be displayed in a user-friendly and intuitive interface that enhances the overall user experience.

The application will be designed to automatically update the user interface in real-time, reflecting any changes in the device status or incoming data. This ensures that users have access to the most current information available, allowing for informed decision-making and timely responses.

By supporting various signal formats and providing a clear, interactive display, the application aims to enhance the usability and effectiveness of Matter devices within the connected ecosystem.

III. Development environment

A. software development platform

1) JavaScript

JavaScript is a programming language used to make web pages dynamic, allowing for content changes in response to user interactions. It evolved from historically static web pages and is now utilized in both client-side and server-side development, with various libraries and frameworks expanding its functionality. JavaScript is interpreted by the browser, modifying the DOM in response to user events on the client side and generating dynamic content by interacting with databases on the server side. Additionally, when combined with HTML and CSS, it enhances the UI of web applications and allows for efficient task execution. As a client-side scripting language, JavaScript is one of the core technologies of the World Wide Web. Its features can improve the user experience of websites, from refreshing social media feeds to animations and interactive map displays. For example, when browsing

the internet, if you encounter an image slideshow, a drop-down menu that appears upon clicking, or dynamic color changes of objects on a webpage, you are witnessing the effects of JavaScript in action. Its selection for this project is driven by the team's familiarity with it, which enhances efficiency and productivity.

2) React

React is a JavaScript library developed by Facebook, primarily used for building user interfaces (UI). It has a component-based structure, allowing developers to create reusable components for UI construction. React uses a Virtual DOM to efficiently handle updates and optimize performance, making it widely used in the front-end development of web applications. The decision to use React for this project was influenced by the fact that the team conducted a study on React together during their vacation, enhancing their familiarity and readiness to implement it effectively.

3) Electron

Electron is a framework for building desktop applications using JavaScript, HTML, and CSS. By embedding Chromium and Node.js into its binary, Electron enables developers to maintain a single JavaScript codebase and create cross-platform applications that work on Windows, macOS, and Linux. Popular desktop applications like Slack and Visual Studio Code are developed using Electron. Implementing the dashboard as a desktop application is advantageous for local use, particularly when want to use AI function in local, which makes Electron a suitable choice for this project. This decision reflects the need for a robust and efficient local application to meet the project's requirements.

4) Go

Go (or Golang) is an open-source programming language developed by Google, designed to be fast and concise while supporting concurrency, making it ideal for network applications and server-side programming. Its straightforward syntax and ease of error handling contribute to its popularity in projects that require high performance and efficiency. Additionally, Go boasts a large ecosystem of partners, communities, and tools, making it easy to learn and fostering effective team collaboration. The decision to use Go for this project is influenced by the requirement that Hyperledger Fabric must be developed using Go, ensuring compatibility and optimal performance within the blockchain framework.

5) gRPC

gRPC is a high-performance, open-source Remote Procedure Call (RPC) framework initially developed by Google. It uses HTTP/2 for transport and Protocol Buffers as the interface description language, enabling efficient communication between distributed systems across different languages and platforms. gRPC excels in scenarios requiring high-throughput and low-latency communication, making it particularly suitable for microservices architectures. The framework's strong typing system, bidirectional streaming capabilities, and built-in support for authentication enhance the reliability and security of service-to-service communication. The decision to use gRPC for this project was influenced by its essential role in communicating with the Hyperledger Fabric gateway. Since the Electron-based frontend needs to interact with the Hyperledger Fabric network through its gateway, gRPC provides the necessary protocol and tools to establish this communication efficiently and securely.

6) C++

C++ is a high-performance, object-oriented programming language developed by Bjarne Stroustrup as an extension of the C language. It is widely used in various applications, including game engines, system software, IoT, embedded systems, and graphics processing. C++ provides a clear program structure and enables code reuse, which helps reduce development costs, while also offering portability for creating applications that can adapt to multiple platforms. Furthermore, C++ offers a high level of control over system resources and memory. This project leverages C++ for building Arduino and WebAssembly applications, capitalizing on its efficiency and versatility in these domains.

7) Arduino

Arduino is an open-source electronics platform based on easy-to-use hardware and software, primarily used in IoT and embedded systems projects. Arduino boards can read inputs—such as light from a sensor, a finger press on a button, or a Twitter message—and turn them into outputs, like activating a motor, lighting an LED, or publishing data online. Programmed using C/C++, Arduino enables rapid prototyping by connecting various sensors and actuators, and is also popular for educational and DIY projects. Users can control their boards by sending instructions to the microcontroller, allowing for flexible and dynamic applications. Arduino was chosen for this project because it offers a simple way to develop embedded systems, streamlining the development process and enhancing efficiency.

8) Python

Python is a high-level programming language with concise and easy-to-read syntax. It is used in various fields, including data science, artificial intelligence, web development, automation, and scripting. Thanks to its rich libraries and community support, Python enables rapid

prototyping and highly productive development. In this project, Python is chosen specifically for AI development, leveraging its capabilities to create efficient and effective AI solutions.

9) Visual Studio Code

Visual Studio Code is a code editor redefined and optimized for building and debugging modern web and cloud applications. Developed by Microsoft, it is a free and open-source editor that supports a wide range of programming languages, including JavaScript, Python, and C++. With features like extensive extensibility through a marketplace of plugins, built-in debugging tools, and seamless integration with version control systems like Git, VS Code provides a user-friendly interface that enhances productivity. Additionally, it is available on multiple platforms, including Windows, macOS, and Linux, making it accessible to developers regardless of their operating system. Visual Studio Code was chosen for this project because it is the most commonly used code editor, offering familiarity and reliability for efficient developmen

10) GoLand

GoLand is an integrated development environment (IDE) specifically designed for the Go programming language, developed by JetBrains. It offers smart code assistance with advanced code completion, navigation, and refactoring tools, making it easier to write clean and efficient code. GoLand features a powerful integrated debugger for setting breakpoints and inspecting variables, as well as built-in support for unit testing and code coverage analysis. Additionally, it integrates seamlessly with version control systems like Git, allowing developers to manage their repositories directly within the IDE. With a customizable interface and cross-platform compatibility for Windows, macOS, and Linux, GoLand enhances the development experience, enabling developers to write, test, and deploy Go applications more effectively. GoLand was chosen for this project to facilitate the use of the Go programming language, providing the necessary tools and environment for optimal development.

11) LaTeX

LaTeX is a high-quality typesetting system. It includes features designed for the production of technical and scientific documentation. LaTex is the de facto standard for the communication and publication of scientific documents.

12) GitHub

GitHub is a web-based platform that uses Git version control for managing and sharing code repositories. It enables developers to collaborate on projects by allowing them to track changes, manage branches, and resolve conflicts seamlessly. With features like pull requests, code reviews, and issue tracking, GitHub facilitates efficient team collaboration and project management. Additionally, it hosts a vast repository of open-source projects, providing developers with resources to learn from and contribute to. GitHub's integration with various CI/CD tools and support for GitHub Actions enhances its capabilities, making it an essential tool for modern software development.

13) Notion

Notion is an all-in-one workspace that combines note-taking, task management, databases, and collaboration tools, allowing teams to organize and share information effectively. With its flexible structure, users can create custom templates and pages tailored to their specific needs, promoting productivity and collaboration. Notion's rich formatting options, including tables, kanban boards, and calendars, enable users to visualize and manage their work dynamically. Additionally, its real-time collaboration features allow multiple users to edit and comment simultaneously, making it a powerful tool for project management and team communication.

14) macOS

macOS is a widely used operating system for software development, known for its user-friendly interface and exceptional versatility. It equips developers with essential tools and integrated development environments (IDEs) for creating a variety of applications, including web, desktop, mobile, and gaming software. The platform supports multiple programming languages and frameworks, offering the flexibility to adapt to specific project requirements. Its intuitive design simplifies the setup of development environments and project management. Additionally, an active macOS developer community fosters collaboration and knowledge sharing. With continuous updates, developers have access to the latest technologies and tools, enabling them to modernize their applications effectively. Overall, macOS is recognized as a crucial platform for software development, playing a significant role in turning innovative ideas into reality.

B. Computer resources

TABLE II
COMPUTER RESOURCES

Name	Computer Resource	Version of OS, SW
Dongwook Kim	Apple M3 Pro Chip 18GB RAM memory	macOS Sequoia 15.0.1
Jisu Shin	Apple M1 Chip 16GB RAM memory	macOS Sequoia 15.0.1
Giram park	Apple M2 Chip 16GB RAM memory	macOS Sequoia 15.0.1
Seoyoon Jung	Apple M2 Chip 8GB RAM memory	macOS Sequoia 15.0.1

C. Cost Estimation

Although it is different from the actual application in the industry, we envision a test network operating two Hyperledger Fabric peers and one orderer on a single computer. For this configuration, we plan to use an AWS EC2 t2.medium instance (2vCPU, 4GB RAM). This t2.medium instance is deemed suitable for a test network of this scale, as it meets the minimum specifications required for running peers and orderer while providing a cost-effective option for development and testing purposes. According to the AWS pricing calculator, operating a t2.medium instance in the Seoul region with a long-term commitment would cost approximately $18.47 per month. Adding the cost of a required 50GB EBS volume at approximately $4.56, the total estimated monthly cost would be $23.03. This represents the minimum cost for establishing a test environment, and an actual production environment would likely require higher-specification instances and additional infrastructure configuration. However, if we can utilize the company's existing underutilized server resources, we expect to significantly reduce these cloud cost.

D. Software in use

1) ADEPT

ADEPT, which stands for Autonomous Decentralized Peer-to-Peer Telemetry, is a blockchain platform designed for IoT devices that operates on a peer-to-peer basis. The idea behind ADEPT was introduced in 2015 as a result of collaboration between Samsung and IBM. It incorporates technologies like BitTorrent, Telehash, and Ethereum. ADEPT organizes IoT devices based on their capacities, allowing them to independently manage, analyze, and share their data. This platform is being implemented in wearable technology and household appliances. For instance, Samsung's smart washing machine employs ADEPT technology to automatically order essential supplies, such as detergent, when they are running low.

2) IoT Chain

IoT Chain operates on blockchain technology and incorporates various mechanisms like PBFT (Practical Byzantine Fault Tolerance), DAG (Directed Acyclic Graph), SPV (Simple Payment Verification), and CPS (Cyber Physical System). Its primary goal is to improve security within the IoT ecosystem while utilizing ICT (IoT Chain Token) for accessing IoT products. By leveraging the decentralized security of conventional blockchains, IoT Chain overcomes challenges related to transaction speed and scalability through PBFT and DAG. The architecture consists of a main chain and a side chain; the side chain executes smart contracts using coins generated from the main chain. The main chain employs PBFT for rapid transaction validation, while the side chain utilizes DAG for efficient transaction processing. SPV allows payment verification by checking only the headers of blocks, rather than all their components, which reduces verification fees and decreases user overhead. IoT Chain finds applications in shared economies and smart home technologies. In November 2018, initiatives were launched to create a developer ecosystem, with plans to publicly release IoT Chain in December.

3) SLOCK.IT

SLOCK.IT, a startup based in Germany, focuses on creating a sharing economy infrastructure utilizing Ethereum technology. They are in the process of developing the Universal Sharing Network, which integrates an automated payment system with Ethereum. This platform allows individuals to share and trade unused resources like homes or cars via blockchain technology, ensuring trust between parties. SLOCK.IT provides a smart lock feature, allowing users to unlock their assets for others by paying with tokens to execute Ethereum smart contracts. Additionally, users can control the keys required for transactions through a mobile application.

4) JD.COM

JD.com offers blockchain gateway services, blockchain node services, and blockchain consensus network services. The platform utilizes a BFT-like consensus algorithm and employs an authentication protocol to manage the number of accesses to the blockchain network. The system consists of three types of peers: consensus peers, gateway peers, and IoT devices. Gateway peers operate within the middleware layer to integrate inputs and protocols from the lower layers.

E. Task distribution

TABLE III
TASK DISTRIBUTION

Name	Task
Dongwook Kim	Blockchain Development
Jisu Shin	Front-end Development
Giram Park	Embedded Development
Seoyoon Jung	Front-end Development

IV. SPECIFICATIONS

A. Core Requirements Specifications

1) Hub Elimination and Range Extension

To eliminate the mandatory use of Matter hubs and extend operational range, we propose replacing traditional Matter hubs with Hyperledger Fabric's chaincode functionality. This transformation fundamentally changes how Matter devices communicate and operate, freeing them from the physical constraints of home networks.

The core of this solution lies in implementing a message queue system within the blockchain. Instead of relying on a physical hub for communication, each Matter device interacts with a dedicated queue in the blockchain. This queue serves as a virtual communication channel, enabling devices to operate beyond the traditional home network boundaries.

However, implementing a traditional queue structure in Hyperledger Fabric would be inefficient due to the complexity of transaction operations. Reading and writing to an array-based queue would require reading the entire array for each push operation, creating unnecessary overhead. To optimize this process, we propose using a Key-Value Store structure where the key is formatted as *devicePK-mCTR* (device public key combined with a message counter) and the value contains the message payload.

This architecture provides several advantages:

a) Eliminates the need for physical Matter hubs by virtualizing their functionality through blockchain

b) Enables device operation from any location with internet connectivity

c) Maintains secure and reliable communication through blockchain's inherent security features

d) Optimizes performance through efficient key-value based message handling

2) Data Analytics and System Reliability

For enhanced data tracking and improved system reliability, we propose a revolutionary approach to data analytics and visualization that leverages blockchain's inherent advantages in data integrity and accessibility. Traditional IoT data analysis systems typically involve multiple intermediaries - data analysts processing raw data and relay servers transmitting processed information to decision-makers. This multi-step process introduces potential points of data corruption and creates opportunities for malicious administrators to compromise data integrity.

Our solution implements a direct data access approach through a desktop application built with Electron, which connects directly to Hyperledger Fabric via gRPC. Additionally, the solution incorporates generative AI to transform natural language inputs into executable queries, enabling administrators without programming expertise to interact with and analyze raw data directly. This AI-powered query generation system allows non-technical users to extract meaningful insights from the blockchain data through intuitive language-based interactions.

This approach significantly improves system reliability by ensuring that decision-makers work with authentic, unaltered data. The combination of blockchain's immutable data storage, direct access through gRPC, and AI-assisted query generation creates a powerful platform for data-driven decision making that maintains data integrity while being accessible to users regardless of their technical expertise.

3) Decentralization

Our approach to decentralization fundamentally reimagines the Matter protocol's architecture while maintaining its core benefits. Unlike the traditional Matter protocol that relies on a centralized Certificate Authority (CA) for device certification, Matter Tunnel eliminates this requirement while preserving protocol compatibility. By removing the centralized authentication system, we lower barriers to entry for device manufacturers and smaller development teams, fostering innovation and competition in the IoT ecosystem.

This decentralized approach maintains the Matter protocol's ability to control multiple vendors' devices through a single application, ensuring that the key benefit of interoperability remains intact. The elimination of platform dependencies further enhances true decentralization, freeing users from vendor lock-in and creating a more open IoT environment.

4) Enhanced Security and Privacy Protection

Our solution significantly enhances End-to-End Encryption (E2EE) and user privacy protection by fundamentally restructuring the communication architecture of Matter

devices. Traditional Matter implementations rely on a cloud-based communication model where applications communicate with cloud services, and Matter hubs poll these services for updates. This structure inherently compromises both E2EE and privacy. Matter Tunnel addresses these limitations through a blockchain-based approach.

Key Security and Privacy Enhancements:

a) Direct Blockchain Communication

By eliminating cloud service intermediaries, this system enables direct and encrypted communication between applications and devices. The removal of vulnerable points in the communication chain enhances security, while ensuring true end-to-end encryption throughout the entire process.

b) Enhanced Privacy Protection

This system maintains privacy by only exposing device public keys on the blockchain, while keeping sensitive information like IP addresses and location data completely private. This approach enables anonymous device operation, significantly reducing the attack surface for potential privacy breaches.

c) Secure Message Counter Implementation

The system leverages Matter devices' built-in message counter (mCTR) to effectively prevent message replay attacks. By maintaining synchronized encryption states across devices and broadcasting mCTR values through the blockchain for coordination, it ensures secure and synchronized communication between devices.

By leveraging blockchain technology and existing Matter security features, our solution creates a more robust and private IoT ecosystem. The combination of anonymous operation, secure message counting, and direct blockchain communication ensures that both E2EE and user privacy are maintained at the highest possible level.

5) Interoperability and Development Convenience

Matter Tunnel is designed with a strong focus on interoperability and development convenience, offering a seamless path for integrating blockchain capabilities into existing Matter implementations. Our approach minimizes development overhead while maximizing compatibility and flexibility in implementation.

The core strength of our solution lies in its simplicity of integration. Developers can enable blockchain support by adding just a few lines of code to their existing Matter applications. This minimal modification approach significantly reduces the barrier to entry for blockchain adoption while maintaining the integrity of current implementations. The system provides a straightforward API that abstracts the complexities of blockchain interaction, allowing developers to focus on their application logic rather than blockchain implementation details.

A key architectural feature is the ability to separate blockchain polling threads from Matter processes. This separation enables applications to simultaneously support both traditional Matter communication and blockchain-based operations. Developers can implement and validate blockchain features while maintaining their current Matter communication channels, ensuring continuous service availability and reducing implementation risks.

6) Real-Time Performance with Hyperledger Fabric

To ensure real-time performance in Matter Tunnel, we carefully selected Hyperledger Fabric as our blockchain platform after extensive evaluation of various options. This choice was driven by Hyperledger Fabric's unique characteristics that align with the real-time requirements of IoT device communication.

Hyperledger Fabric's high transaction processing capability stands out as a crucial feature for our implementation, supporting 2,000-20,000 transactions per second (TPS). This throughput is achieved through multiple channels that enable parallel transaction processing, effectively handling concurrent device communications while providing near-instantaneous transaction finality. The platform's configurable architecture can enhance performance by allowing optimization of network parameters, enabling adjustment of block creation time, supporting custom channel configurations for different device groups, and permitting fine-tuning of consensus mechanisms to match specific use case requirements.

By leveraging Hyperledger Fabric's comprehensive capabilities, Matter Tunnel achieves the real-time performance necessary for effective IoT device control and monitoring. The platform's ability to handle high transaction volumes while maintaining low latency ensures that device interactions remain responsive and reliable, meeting the demanding requirements of modern IoT applications.