Decentralized Identifiers and NFT-Driven Blockchain Solution for Personal Data Trading

DaeGeun Yoon
Decentralized Network Research Section
Electronics and Telecommunications Research Institute (ETRI)
DaeJeon, South Korea
dayoon@etri.re.kr

KiSung Park
Decentralized Network Research Section
Electronics and Telecommunications Research Institute (ETRI)
DaeJeon, South Korea
ks.park@etri.re.kr

SungJin Mun
Decentralized Network Research Section
Electronics and Telecommunications Research Institute (ETRI)
DaeJeon, South Korea
sjmoon @etri.re.kr

SungKee Noh
Decentralized Network Research Section
Electronics and Telecommunications Research Institute (ETRI)
DaeJeon, South Korea
sknoh @etri.re.kr

Abstract— **With the onset of the AI era, the demand for personal data is on the rise. Numerous companies are gathering user data to enhance their services. As the utilization of this personal data surges, its intrinsic value also escalates. Despite individuals being the source of this valuable personal data, it's the centralized service providers that reap the profits. This research introduces a blockchain-based trading framework for personal data utilizing Decentralized Identifiers (DID) Non-Fungible Token (NFT). The proposed system empowers users to amass personal data within their designated storage space provided by the system. DID and NFT serve the roles of verifying user identity and establishing data ownership, respectively, all without relying on centralized systems. To guarantee data integrity and transaction history, Ethereum is employed, which constitutes a decentralized blockchain nodes. The operational demonstration of our system is showcased through a monitoring setup that offers real-time insights into user data and trading activities. The research validates that our proposed system enables seamless personal data transactions between two parties - a seller and a buyer - eliminating the need for centralized service providers.**

Keywords—Blockchain, Decentralized Identifiers, Non-Fungible Token, Personal Data Trading System

I. Introduction

In the IoT era, individual data has surged, becoming "digital oil" with transformative value. As its worth rises, a marketplace for data exchange is crucial. For instance, selling health data from smart devices benefits both earners and data-hungry businesses.

To invigorate the data sharing economy, a trusted platform for trading personal data is imperative, addressing the limitations of the current Trusted Third Party (TTP) structure while reinstating users' control over their data. Several initiatives are underway to tackle the aforementioned challenges. Some blockchain communities are exploring the extension of their scope beyond cryptocurrency data to encompass diverse data types through interoperability with external data storage. This approach aids in mitigating storage constraints [3] [4]. Nevertheless, these efforts are still nascent, lacking mature product development for commercial use. Concurrently, certain projects [5] [6] [7] are in progress to establish a trading platform for personal data, although their focus has predominantly been on trading IoT sensor data.

In this paper, we present an innovative proposition: a blockchain-driven system for trading personal data. This system harnesses the potential of Decentralized Identifiers (DID) [1] and Non-Fungible Token (NFT) [2]. Our proposal establishes a decentralized infrastructure, enhancing the reliability of personal data management for users. This infrastructure negates the necessity of solely relying on TTP for data storage. Instead, users gain the flexibility to manage their personal data either within the proposed system, on the TTP side, or in both domains. Prior to engaging in personal data transactions, user authentication and data ownership claims are paramount. To achieve this, DID is leveraged for user identity authentication, while NFT empowers users to assert ownership of their data.

II. PERSONAL DATA TRADING SYSTEM

The proposed system encompasses two main components as shown in Fig. 1: the personal data trading and the monitoring system. Within this system, the personal data trading system is composed of Mobile Apps, User Connectors, Trade Connectors, and Ethereum. The Mobile Apps are installed on users' mobile devices, serving various functions such as authentication, personal data management, data trading, and the collection of users' health data. These Mobile Apps generate users' DID and RSA keys, which in turn are used to create the DID documents essential for user identity authentication. Subsequent to this, a request for DID document registration is transmitted to the User Connectors.

Furthermore, a module for acquiring users' health data is implemented within the Mobile App, primarily to show the process of trading personal data among users. Users are granted permission to gather health-related data like pulse rate and distance covered during walking and running. These accumulated data points find storage within their corresponding User Connectors. Lastly, Mobile Apps receive metadata concerning users' personal data, trading history, and account details. This information is presented to users through the graphical user interface (GUI) of the Mobile Apps.

User Connectors provide APIs responsible for overseeing users' DID and their corresponding personal data. These Connectors receive requests from the Mobile Apps to process DIDs and DID documents, subsequently furnishing the outcomes of these requests. Furthermore, User Connectors undertake the task of regulating the lifecycle of users' personal data, encompassing functions for data creation, retrieval, updating, and deletion (CRUD operations). When Mobile Apps send requests to store user data, these requests include metadata indicating the data's categorical classification. As a

This work was supported by Electronics and Telecommunications Research Institute(ETRI) grant funded by the Korean government. [23ZR1330, Core Technology Research on Trust Data Connectome]

979-8-3503-1327-7/23/$31.00 ©2023 IEEE

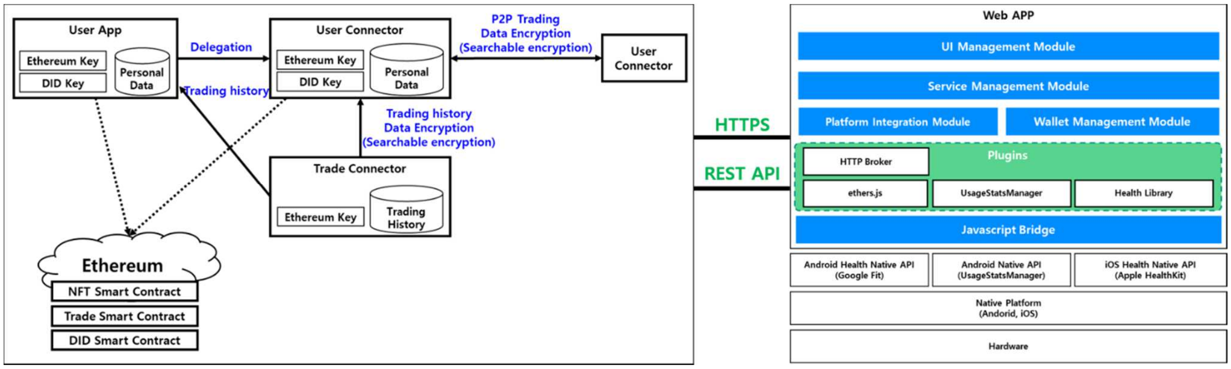

Fig. 1. Overall architecture of the proposed system.

result, User Connectors manage data categorized by type, providing essential metadata to the monitoring system. This metadata enhances the graphical user interface (GUI) of the monitoring system, ultimately offering a more user-friendly experience.

Trading Connectors are responsible for overseeing all metadata pertaining to the exchange of personal data among users. As such, these Connectors handle user-related aspects like account details, current balances, profiles, and trade histories. Moreover, Trading Connectors function as intermediaries between buyers and sellers. They propose an estimated price—calculated through an algorithm—to both parties and subsequently confirm the transaction upon receiving agreement.

Ethereum functions as a decentralized infrastructure, utilizing distributed peer nodes to establish an immutable storage mechanism. We've chosen Ethereum as the immutable storage solution for our proposed system due to its open nature, enabling participation from anyone interested in providing services to users and benefiting from the ecosystem. Our implementation involves the development and deployment of three distinct smart contracts: the Trade Smart Contract, the DID Smart Contract, and the NFT Smart Contract.

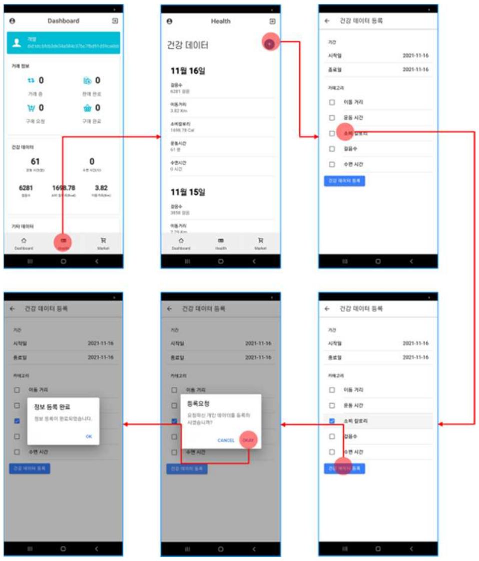

Fig. 2. The mobile app UI example.

The Trade Smart Contract serves as the hub for trading-related data, encompassing aspects like personal data prices, projected pricing calculations, and the history of personal data state transitions. Handling authentication information, the DID Smart Contract preserves users' DID documents containing their DID and corresponding public key. This contract facilitates the retrieval of a DID document linked to a specific DID. For ownership management of personal data, the NFT Smart Contract mints a non-fungible token (NFT) inclusive of the owner's data. When a user sells their personal data to a buyer, the user transfers the NFT to the buyer. This NFT serves as proof of ownership for the traded data, reinforcing the transaction's legitimacy.

III. IMPLEMENTATION

We have implemented a proof of concept (PoC) system to test the functionality of the personal data trading system. Within this PoC system, two Mobile Apps are designated as the seller and buyer respectively. Each Mobile App is accompanied by a User Connector, responsible for managing both personal and authentication data. Fig. 2 illustrates an example of the user interface (UI).

The PoC also encompasses a monitoring system accessible through a web browser, providing users with valuable insights. On the left side of Fig. 3, the user's trading history is displayed, including trading dates, categories of sold data, the quantity of sales per category, and the data transaction history. The right side of Fig. 3 presents details about the user's personal data registered in both the User Connector and the Trade Connector. By parsing metadata received from the personal data trading system, the monitoring server presents user data in categorized format.

Through this PoC system, we demonstrate that users within our personal data trading system can undergo identity authentication via DID without dependence on a centralized system. Additionally, we establish the feasibility of secure personal data trading using NFTs, effectively guaranteeing ownership of user data.

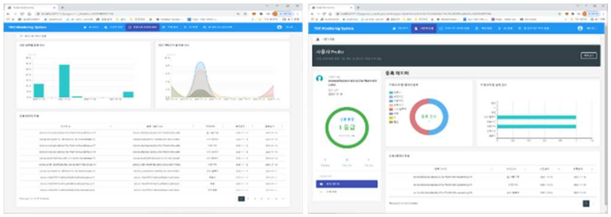

Fig. 3. The monitoring system UI example.

IV. CONCLUSION

This paper presents a data trading system rooted in blockchain technology, utilizing Decentralized Identifiers (DID) and Non-Fungible Token (NFT). The proposed system empowers users to accumulate their personal data via the system's provided storage. Subsequently, users can validate their identity and establish data ownership, all facilitated by DID and NFT without reliance on centralized mechanisms. To ensure data integrity, Ethereum is employed to manage and secure traded data and transaction history. Additionally, the implementation of a monitoring system with a well-structured graphical user interface (GUI) showcases the system's functionality. Through this setup, we demonstrate the successful completion of data trading between sellers and buyers within our system, circumventing the need for centralized service providers.

REFERENCES

[1] Dddd D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt, “Decentralized identifiers (DIDs) v1.0,” W3C, https://www.w3.org/TR/did-core, July 2022.

[2] W. Entriken, D. Shirley, J. Evans, and N. Sachs. EIP721: ERC-721 Non-Fungible Token Standard. [Online]. Available: https://eips.ethereum.org/EIPS/eip-721.

[3] Wilkinson, Shawn, et al. "Storj a peer-to-peer cloud storage network." (2014).

[4] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." arXiv preprint arXiv:1407.3561 (2014).

[5] BitClave, “BitClave homepage”, https://www.bitclave.com, June 2021

[6] G. Drosatos, “Personal sensor data aggregator architecture”, ddd https://www.carre-project.eu/personal-sensor-data-aggregator-architecture, Jan 2015.

[7] Silvano, Wellington Fernandes, and Roderval Marcelino. "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data." Future Generation Computer Systems 112 (2020): 307-319.