Security for Blockchain-based DID Key Generation

Seong-Kyu Kim[*]

*Assistant Professor (Tenure Track) of Department of Information Security, Joongbu University, Gyeonggi-do Goyang-Si 10279, Republic of Korea.(e-mail : skkim@joongbu.ac.kr or guitara77@gmail.com)

Jun-Ho Huh[**]

** Assistant Professor (Tenure Track) of Department of Data Informatics, (National) Korea Maritime and Ocean University, 727, Taejong-ro, Yeongdo-gu, Busan, Republic of Korea (e-mail : 72networks@pukyong.ac.kr or 72networks@kmou.ac.kr)

Abstract

This study has recently been actively researched on blockchain-based identity authentication systems. In addition, DID, which refers to a digital identity verification system that allows users to select only the information needed for proof purposes and provide it to verification institutions to strengthen privacy protection, has been studied a lot. In addition, as the non-face-to-face economy is expected to accelerate after Corona19, the proliferation of DID services, an online identity verification technology, is in full swing, and in this study, we study major architectures for DID key generation and mobile-based privacy certification.

I. Introduction

Blockchain-based distributed IDs (DIDs) will enable digital financial transactions anytime, anywhere by embedding digital IDs and identification cards in smartphones. In addition to resident registration cards and passports and driver's licenses, these digital identification cards will be developed into self-sustaining identification using biometric distributed IDs. Domestic and foreign mobile carriers also use biometric information such as fingerprint authentication and face recognition of smartphones [1].

It uses an app for authentication and financial account number by biometric authentication ID(Identification) and electronic signature. In this paper, we would like to propose a plan to utilize a blockchain DID-based biometric key generation device. Specifically, we design DID(Decentralized Identifier) generation and authentication modules for the storage of distributed IDs. As such a user-certified node, the USB(Universal Serial Bus) module intends to propose a virtual currency recommendation in the key-store through online real-time authentication by DID-based FIDO(Fast IDentity Online). In addition, we propose a digital identity verification system that allows users to manage and control their own identity information online, just as they manage identity verification in real life as a distributed identity management system [2].

II. Related Research

2.1 Blockchain Security

Blockchain technology includes concepts

beyond distributed ledger technology, and blockchain definitions can be considered as 'global trust computers'. Figure 1 summarizes five ways to define blockchain, and the most appropriate definitions can be seen as the third "smart contract execution platform" and the fourth "global trust computer." Here, smart contracts can be considered software running on blockchain computers. In addition, blockchain/blockchain-based security technologies are classified in various ways depending on the source core technologies, platform technologies [3], and security service technologies. Along with the development of blockchain technology, it is a technology field that is gradually expanding its application to all industrial areas.

In existing centralized transaction systems, each transaction must be validated through a trusted central server (e.g., a central bank), resulting in a cost and performance bottleneck on the central server. Unlike centralized systems, blockchain does not require a third trust organization. In blockchain, consensus techniques are used to maintain consistency of data in distributed networks.

2.2. Characteristics of blockchain (invariant)

Transactions on the chain can be quickly validated and invalid transactions are not accepted by nodes in the blockchain [4]. Once a transaction is recorded in the blockchain, it is almost impossible to delete or revert the content. Blocks on nodes containing invalid transactions can be found immediately.

2.3. Characteristics of blockchain (anonymous)

Each user interacts with the blockchain with their similar anonymous address. This address does not include user entity identification information [5]. Thus, user anonymity can be preserved. However, transaction anonymity cannot be guaranteed because blockchain discloses all transaction content [6].

2.4. Characteristics of Blockchain (Traceability)

All transactions are referenced to previous unused transactions assigned to nodes on the block [7]. When the current transaction is written to the blockchain, the state of the referenced unused transaction transitions from unused to used. Therefore, all transactions can be easily identified and tracked.

III. Research method

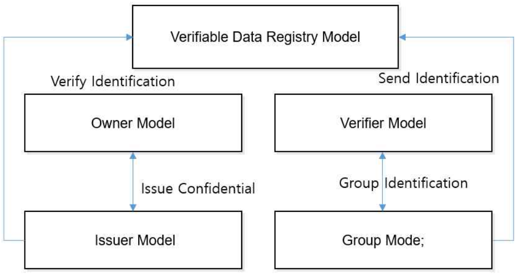
3.1. Study Design

With the advent of distributed ledger technology, a completely new identity management system is being developed. Entities that exist in distributed identity management systems are free to use shared trust roots. Globally distributed ledger (or distributed P2P(Peer to Peer) networks that provide similar functions) provides a means of managing IDs without using centralized privileges. The combination of distributed ledger technology and distributed identifiers allows all entities to be distributed to create and manage unique identifiers in independent and reliable roots. In addition, entities in distributed ID management systems are identified as distributed identifiers and can be authenticated through proofs. Distributed identifiers are a new type of identifier for verifiable autosovereignty IDs, and provide a standard way to create globally unique and cryptographically provable permanent identifiers. Distributed identifiers are managed under the control of DID subjects, independent of centralized based identity providers. The distributed identifier refers to

DID Documents, which briefly describes how to use them, and each DID Document provides at least proof points, verification methods, and service endpoints information. Include, DID Document describing sample information and distributed identifiers that represent distributed identifiers.The proof purpose, combined with the verification method, provides a mechanism for proving things. DID Document can specifically specify that proofs generated for authentication purposes can be validated using specific verification methods, such as public keys or anonymous biometric protocols. Service endpoints enable reliable interaction with DID controllers.

3.2. Research Architecture

This research architecture works with the Verifiable Credentials Data Model 1.0 standard in W3C's Verifiable Climes Working Group, which provides cryptographically secure, privacy-preserving, and machine-verifiable ways to represent a wide variety of Credentials on the web. This allows verifiable Credentials to represent all the same information as physical Credentials, and by adding techniques such as digital signatures, information can be tampered with, making it more reliable than physical Credentials. We also describe the role of ecosystems and key actors for verifiable CREDITALs and their relationships [Fig. 1]



[Fig. 1] Architecture for verifiable DIDs

3.2.1 Issuer Model

Produces verifiable credentials for a particular object and verifies them by serving to deliver them to Holder.

3.2.2 Owner Model

Owns one or more verifiable certificates and is responsible for generating and delivering them in the form of Presentation when submitting them to Verifier.

3.2.3 Verifier Model

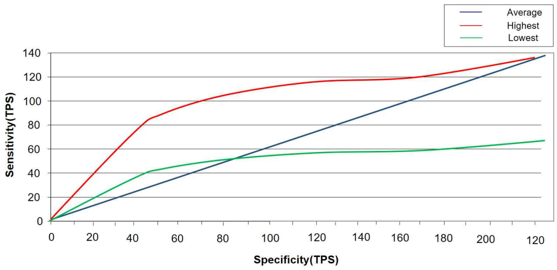
Holder has a role in verifying that it has adequate verifiable credentials.

3.2.4 Verifiable Data Registry Model

Distinguish distributed DB(Database), government ID DB, distributed ledger, etc. from the role of mediating the generation and verification of identifiers, keys, and other relevant data.

3.3 Experimental Results

The demonstration objective of the experiments in the study, combined with the verification method, provides a mechanism for proving things. For example, DID Document can specifically specify that proofs generated for authentication purposes can be verified using certain verification methods, such as public keys or anonymous biometric protocols. Service endpoints enable reliable interaction with DID controllers. The DID performance test was also performed as shown in Figure 2. The average value was 80 for TPS(Transaction per Second), 120 for the best and 60 for the lowest.



[Fig. 2] DID PerformanceSpecific Results

IV. Future research and conclusions

In this paper, we describe ID management techniques using blockchain technology and distributed identifiers and verifiable credentials for self-sovereign ID management. Blockchain-based ID management technology emphasizes self-sovereignty to manage and control one's own information. Distributed identifiers and verifiable credentials that are essential to constructing a self-sustaining ID system are now actively standardized through W3C, but have so far either been a group report or a draft statement.

It is a stage that is being announced in the form of a book.Currently, the study of blockchain-based ID management techniques is focused on aspects of sharing and utilizing information. Given its application in various fields in the future, research on analysis of constraints for information sharing between heterogeneous domains and update and deletion processing of shared information should also be carried out. It is also necessary to focus on future research on identity management and new forms of authentication technology for a wide variety of entities, such as the ID of groups such as corporations and organizations, and the ID of smart devices, beyond identity management technology for individuals.

In addition, standards that are required for key technologies on DID's technology roadmap in advance or that require simultaneous development need to be derived as a key standardization item in the standardization strategy map.

[Reference]

[1] Manohar, Arthi, Jo Briggs, "Identity Management in the Age of Blockchain 3.0," HCI for Blockchain – CHI2018 workshop, 22nd, April 2018.

[2] Rohan Pinto, "How Blockchain Can Solve Identity Management Problems", Forbes, July 2018.

[3] Microsoft Blog, "Decentralized digital identities and blockchain: The future as we see it," February 2018.

[4] Huh , J.-H.; Kim, S.-K. The blockchain consensus algorithm for viable management of new and renewable energies. Sustainability 2019, 11, 3184.

[5] Paul Dunphy, and Fabian A. P. Petitcolas. "A First Look at Identity Management Schemes on the Blockchain," IEEE Security and Privacy Magazine special issue on "Blockchain Security and Privacy", August 2018.

[6] Mingoo, Kang et al, "Blockchain system for authorized recommendation of cryptocurrency based on context-aware smart kisok ,“ Korea patent(10-2019-0137060), 2019.10.31.

[7] Nakhoon Choi, Heeyoul Kim, "A Blockchain-based User Authentication Model Using MetaMask,“ Vol. 20, No. 6, pp. 119-127,Dec.2019.