Biometric Authentication Service on Smart Contract

No author given

***Abstract*—As transactions of monetary value on the public blockchain become more widespread, there is a growing demand that the transactions be verified as legitimate. As a result, it has become mandatory for crypto asset exchanges to perform identity verification. On the other hand, Bitcoin and other public blockchains are easy to start transactions with, and the anonymity of the transactions is a significant value for users. To achieve these conflicting requirements at a certain level, we developed a method to manage information generated from a user's biometric information with Smart Contract and link transactions on the blockchain to real people. This mechanism makes it relatively easy for the user to claim their identity while the operator can control the degree of identity verification.**

***Index Terms*—Blockchain, KYC, Biometrics, Authentication**

I. Introduction

Although specific prerequisite knowledge is required to participate in public blockchains, unlike most financial institutions, anyone can easily join at any time. In addition, many blockchains use addresses linked to private keys managed by the user for transactions with others. There is practically no upper limit to the number of addresses that can be used, and users can have multiple addresses. While this feature is good from the perspective of protecting users' privacy, it also poses a problem because it is difficult for service providers on the blockchain to grasp the direct relationship between addresses and users. To deal with this issue, we introduce a method to link addresses used on the blockchain to real people. Specifically, we will provide a service that connects the biometric information of a real person to a blockchain address, which other services can then reference to confirm the identity of the transaction.

This demo describes a sample implementation of an event that only NFT holders are allowed to attend, where biometric information is used to prove the identity of the NFT holder at the venue. The scenario envisioned in this demonstration is as follows:

1) Users purchase NFTs with their Crypto Wallet.
2) Users register their biometric information before the event.
3) Users provide their biometric information at the event to prove that they are an NFT holder.

The purchase of NFTs and biometric registration can be done in reverse order.

II. System Overview

Figure 1 shows an overview of the systems architecture to realize our scenario. Users in each process will use different systems. The upper left of figure 1 is the NFT purchase process, the lower left is the following biometric registration process, and the lower right is the NFT holder confirmation process. Figure 2 shows the process flow for the NFT purchase and biometric registration processes, and figure 3 shows the process flow for the NFT holder confirmation process. The table in figure 1 shows the information managed by each Smart Contract.

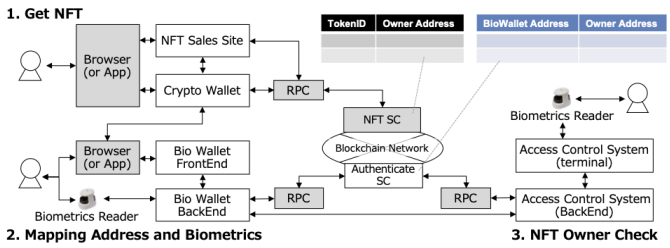

Fig. 1. Demo System Overview

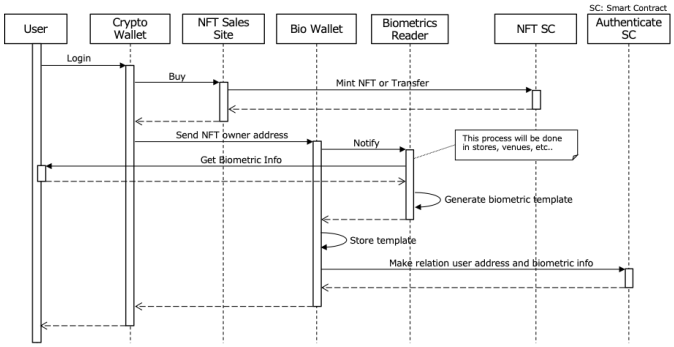

Fig. 2. NFT Purchase and Address Registration Process

A. Purchase NFT

In this demonstration, the user purchases NFTs first. This purchase process is assumed to be performed using a crypto wallet such as MetaMask, which the user uses. As shown in the upper left of figure 1, the user accesses NFT sales sites via a browser or an application and purchases the desired NFTs. This process is the same as the normal NFT purchase process.

B. Register Biometric Infomation

Next, the NFT purchaser's blockchain address is linked to the purchaser's biometric information. This is the part shown in the lower left of figure 1, which manages the information linked by Authenticate Smart Contract. In this demonstration, we call the application that manages the user's biometric information Bio Wallet.

To link that information, a user goes to a specific store or other location that provides a service that connects their biometric information with a blockchain address managed by

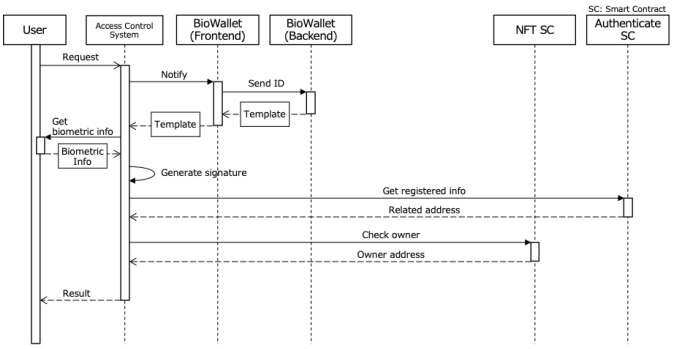

Fig. 3. NFT Owner Check Process

the user's crypto wallet. At that location, there are devices that read the biometric information, and those devices communicate with the Bio Wallet. When the user requests a linkage, the Bio Wallet works with the crypto wallet to obtain the user's address. It sends the user's address and user's biometric information to the Authenticate Smart Contract to maintain that relationship. Other applications and smart contracts can then reference this information to see which biometric information is associated with the blockchain address.

Figure 2 summarizes the process flow of NFT purchases and ties.

C. NFT Owner Check by Biometric Information

By referring to the information managed by the NFT smart contract and Authenticate Smart Contract, it is possible to quickly confirm the identity of the NFT owner at events such as stadiums. There are several possible confirmation methods, but in this demonstration, the user's biometric information is used as the starting point to confirm that the user is an NFT holder. This process is shown in figure 3. The user accesses the admission control system at the event venue. The admission control system obtains the user's biometric information from the event venue's biometric readers. This information matches the relationship information in the Authenticate Smart Contract to get the corresponding address on the blockchain, and the blockchain address is queried to the NFT smart contract to determine if the user is an NFT owner. If the user is the owner, the system will provide benefits based on the event.

III. Implementation

To efficiently implement the demonstration scenario, we use hardhat [1] as the blockchain environment. Because it is EVM compatible with many public blockchains, is widely used and mature as a development environment, and is easy to test by starting the blockchain network in a local environment. For biometric data acquisition, we used a device that implements a fuzzy extractor [2]. This device can generate a unique secret key from the user's finger vein and a corresponding public key from the secret key. The Authenticate Smart Contract manages a relationship table that connects the public key corresponding to the user's biometric information and the user's blockchain address. Connecting the blockchain address with the real person is possible by referring to the Authenticate Smart Contract.

The specific procedure for registering the generated public key to the Authenticate Smart Contract depends on the requirements for the degree of identity verification in the actual usage scenario. If strict identification is not required, the user can read the biometric information with a device, such as a smartphone, to generate the binding information; if rigorous identification is required, the confirmation process should follow the formal procedures of banks and government agencies.

IV. Conclusion

In this paper, we introduce and implement an authentication service that manages the user's blockchain address and the user's biometric information to identify the person on the blockchain. By utilizing this mechanism, it is possible to prove that a transaction is being conducted by someone who exists at that time. Those proved transactions have the clear intent that a real person requested them. This will provide different values to the transactions and services that refer to those.

On the other hand, the extent to which the person's identity is strictly required depends on the system's and service's operation, and the method of operation is an issue. This mechanism can be used to achieve step-by-step identification.

References

[1] Nomic Foundation, "Hardhat," https://hardhat.org/.

[2] K. Naganuma, T. Suzuki, M. Yoshino, K. Takahashi, Y. Kaga, and N. Kunihiro, "New secret key management technology for blockchains from biometrics fuzzy signature," in *15th Asia Joint Conference on Information Security, AsiaJCIS 2020, Taipei, Taiwan, August 20-21, 2020*. IEEE, 2020, pp. 54–58. [Online]. Available: https://doi.org/10.1109/AsiaJCIS50894.2020.00020