Proof of Origin: Creating Data Authenticity by Biometric Information

No author given

***Abstract*—Non-Fungible Token(NFT) issued on the blockchain made adding scarcity to digital data possible. However, as NFT transactions soared, illegal use of other people's content increased. To solve this situation, this paper proposes the Proof of Origin concept, which adds authenticity to NFTs by utilizing a technology that generates the cryptographic keys required for digital signatures directly from biometric information and describes the system architecture, data structure, and implementation of this concept. Using biometric information to link NFTs to actual persons makes it possible to provide trustworthiness and high-added value to data. At the same time, the creator does not need to manage secret keys and can safely and efficiently claim the originality of the data.**

***Index Terms*—Blockchain, NFT, Biometrics signature, Authenticity**

I. Introduction

NFTs began to spread around 2017, and some will be traded at high prices around 2021, attracting much attention. Against this backdrop, services that can easily issue NFTs have also begun to spread. However, there have also been rampant cases of rights theft and fraudulent activities, such as using images created by others without permission or making NFTs look like famous NFTs, and both creators and users are now demanding reliability in NFTs.

This paper proposes a ”Proof of Origin” concept using biometrics-based fuzzy signatures to generate NFTs by secret keys created from the creator's biometric information. First, we explain Biometrics-based fuzzy signatures and the technical background of NFT. We introduce the Proof of Origin concept in section III. Next, we describe the software architecture, basic processing flow, and data structure for realizing this concept, followed by a prototype system we have developed. Finally, we introduce related services and compare them with this concept.

In this paper, our system for digital signature is constructed using the fuzzy extractor proposed by Hitachi, Ltd [1].

II. Preliminary

A. Biometrics-based fuzzy signature

Biometrics based fuzzy signature [2] [3] is a digital signature technology based on biological information. This signature scheme corrects ”fluctuations” in biological information obtained from fingerprint or biological sensors and extracts the unique user's secret keys. Of course, when the fluctuations are significant, when coming from another person, a different key is output. This process is called a fuzzy extractor [4]. Also, the extracted secret key can generate a digital signature based on a conventional public-key cryptosystem. A feature of this signature method is that a secret key is generated from a user's biometric information each time, so there is no need to store the secret key on a server or key management device. As a result, the user does not risk losing the key management devices and can prevent attacks from malware that steals the secret key. The user registration and signature generation processing are as follows.

- User registration:
  At the time of registration, the user inputs biometric information to the sensor and extracts a feature value from the biometric information. Next, the one-way conversion is performed using the PKI secret key and the feature value as input to generate template data, including a public key and system parameters. Finally, the user template data is stored in the authentication device. This user's template data is public information; even if it is leaked to an attacker, it is difficult to reconstruct the user's secret key or biometric information.
- Generating a digital signature:
  When generating a digital signature, the user inputs biometric information to the authentication sensor device and extracts a feature value. Next, the PKI secret key is reconstructed from the template and the feature value. The correct secret key is reconstructed only when the feature value at the time of registration and the feature value at the time of authentication are sufficiently close. After generating the secret key, the user generates the digital signature for the transaction and immediately removes the secret key from the memory. The generated signature can be verified with the ordinary PKI public key.

B. Brief of NFT from the Technical View

NFT is information managed by a smart contract implemented on the blockchain, which often holds information about ID numbers and the data to which that ID refers. In addition, storing data on the blockchain incurs a cost that depends on the amount of data. For this reason, content data like images and video are stored outside the blockchain (called off-chain). If the off-chain data is rewritten, the data displayed when the NFT is referenced will be changed. This is a problem. To address this issue, external storage that links content and URL one-to-one, such as IPFS(InterPlanetary File System) [5], is often used.

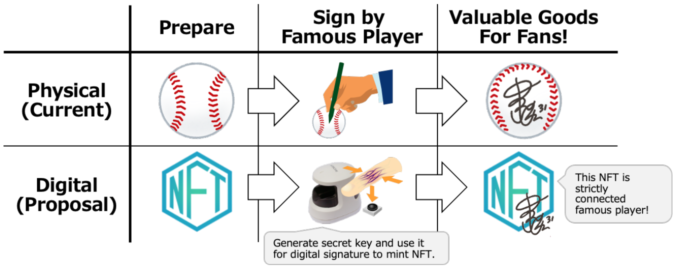

Prepare
Sign by Famous Player
Valuable Goods For Fans!
Physical (Current)
Digital (Proposal)
NFT
This NFT is strictly connected famous player!
Generate secret key and use it for digital signature to mint NFT.

Fig. 1. Concept of ”Proof of Origin”

C. NFT Related Issues

The fact that the content referenced by NFTs is outside the blockchain, as described in section II-B, is a well-known and technically difficult problem to solve. In addition, because anyone can easily issue NFTs, there are problems such as illegal use of contents, not knowing the issuer of NFTs and room for NFT issuers to manipulate prices through wash trade and other means. Besides these issues, other issues must be addressed when using blockchain. In particular, the issue of ”difficulty in private key management” remains a problem that is difficult to solve even now.

III. Concept

A. ”Proof of Origin” Concept

In the real world, objects signed by famous people create high value as memorabilia. Using biometric information, Proof of Origin brings this concept to the digital world. Figure 1 shows this concept.

In addition, by issuing NFTs using biometric information, the problem described in II-C can be solved or mitigated. A similar mechanism can be applied to business processing in a company. For example, information on who invented and owns the rights is essential when considering the digitization and distribution of patents and other rights. It must be maintained without tampering, just as with the signature on a ball. We named this concept ”Proof of Origin” because the generated digital signature is stored in the NFT so that anyone can always check the information on the creator of the NFT at any time and the information on whom the issuer is retained without being tampered with.

IV. System Design

Proof of Origin is realized by linking the blockchain to the biometric signature(BS) system. The overall structure of this system is shown in Figure 2 The following sections describe signature creation/assignment and verification aspects. The left-hand side of the NFT (smart contract) in Figure 2 is related to the creation and assignment of signatures, and the right-hand side is associated with the verification.

A. Generate and Attach Signature to NFT

When writing data on the blockchain, a crypto wallet generates a signed transaction, which maintains the sender’s private key. Proof of Origin utilizes biometric information in the signature process in the wallet to provide the creator’s signature to either or both the transaction and contents referenced by the NFT. In addition, the generated signature and the corresponding public key must be stored somewhere. There are many possible storage locations, but keeping them on the blockchain is preferable. This is because the blockchain is tamper-resistant, and anyone can check and verify them if they are on the public blockchain. For this reason, the basic pattern is to store that information in the smart contract that manages the NFT.

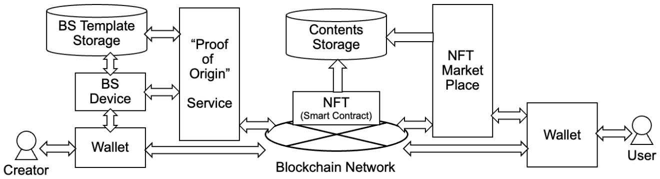


Fig. 2. ”Proof of Origin” System Architecture

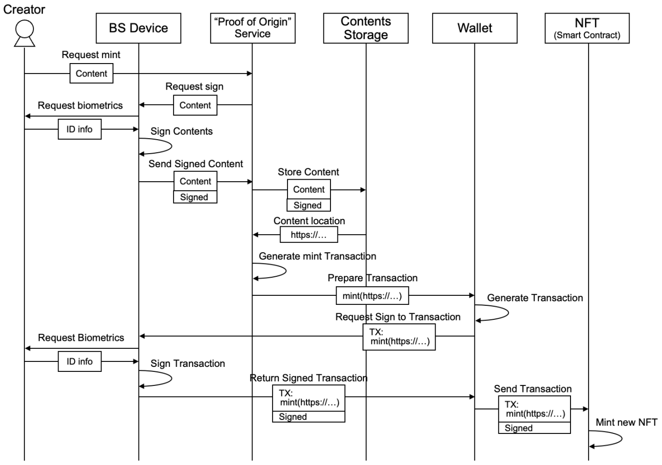
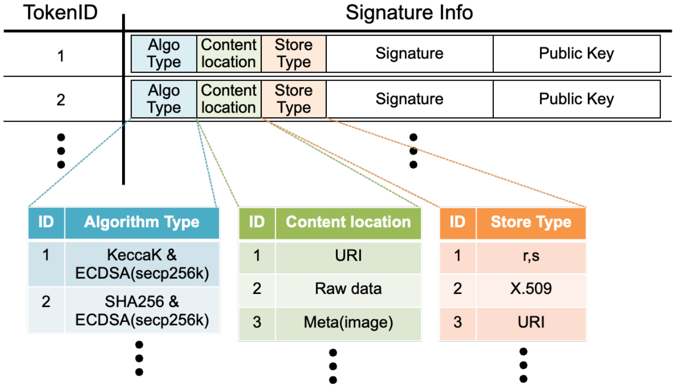


Fig. 3. Mint flow with BS

1) *NFT Mint Process:* Since smart contracts manage NFTs, a transaction requesting a new NFT is sent to the smart contract. Usually, the NFT smart contract has a ”mint” API. A new NFT is issued by setting the necessary parameters and calling this. Our system adds the creator’s signature by combining BS with the NFT issuance process. Figure 3 shows the processing flow of the NFT issuance process when using the BS system. This shows the NFT issuance process, but the same processing flow can be used when updating NFTs’ content-related data.

2) *Target data for signature and auxiliary information for signature verification:* There are two possible signature targets for the BS system: contents and transactions. For signing a transaction, the blockchain specifies the protocol. Therefore, the BS system follows this, and signed transactions are stored on the blockchain. On the other hand, no clear rules exist for signing content. Therefore, we need to make rules for how to refer to the data during signature verification. There are three content storage patterns: (1) content itself is stored on-



TokenID	Signature Info				
1	Algo Type	Content location	Store Type	Signature	Public Key
2	Algo Type	Content location	Store Type	Signature	Public Key
⋮			⋮		

ID	Algorithm Type
1	KeccaK & ECDSA(secp256k)
2	SHA256 & ECDSA(secp256k)
	⋮

ID	Content location
1	URI
2	Raw data
3	Meta(image)
	⋮

ID	Store Type
1	r,s
2	X.509
3	URI
	⋮

Fig. 4. Signature Info in NFT

chain, (2) content generation information is stored on-chain, and (3) content is stored off-chain. Of these, (2) and (3) are issues.In the case of (2), if it stores generation parameters, it is sufficient to create a signature for those. But if only the generation process is stored, creating a signature for the process is meaningless. Therefore, it is necessary to generate a signature for the information, such as images generated by the stored generation process. It isn't easy to handle in (3) case because of many possible patterns. However, in most cases, a JSON file is placed as metadata, and the URL of the content storage destination is described in the "image" element [6]. Since major NFT marketplaces support this method, most contents are believed to be stored this way.

In addition, NFT creators should be free to use any signature algorithms for their content. Therefore, signature-related information must be stored for verification.

3) Signature Information Management in Smart Contract: Figure 4 shows the considered data structure that holds necessary information. It is stored in the NFT smart contract to achieve high tamper resistance and viewability. Since token IDs manage NFTs, this token ID and its corresponding signature are in a table. The following information is stored: which algorithm is used, which data is the signature target, in which format the signature is stored, the signature, and the signer's public key. As shown in the table at the bottom of Figure 4, this format stores only ID in the type and location column to suppress volume. Those IDs are defined separately.

B. Signature Verification

The signature verification method is the same as standard digital signature verification. Still, the difference is that it is determined from the information stored in the NFT smart contract like figure 4, such as where the data is obtained from and which of the received data is used. Service providers, such as NFT Market Place, use this information to provide users with values such as trustworthiness.

While users can perform the verification themselves, however, it's hard for many users. Therefore, the Proof of Origin service provides a verification function. In this way, the authenticity of the NFT can be presented to the user in an easy-to-understand manner.

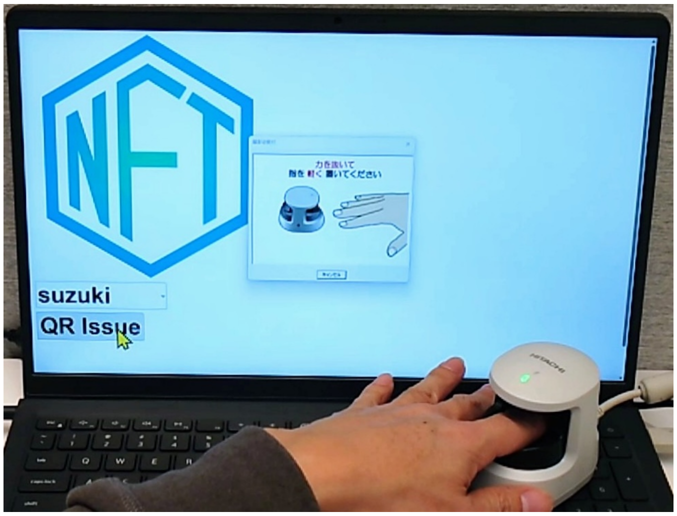


Fig. 5. Prototype System

V. Implementation

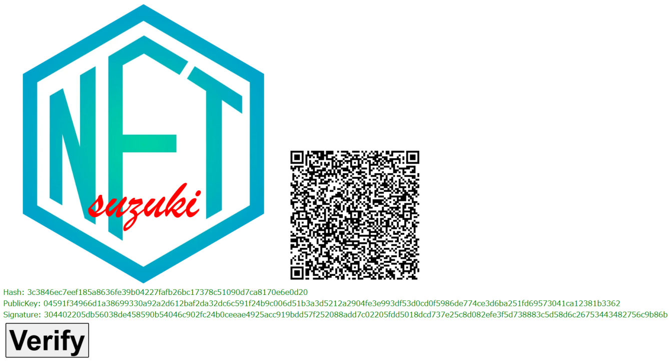
We made a prototype based on the design. Figure 5 shows the NFT minting process in our prototype. In this prototype, we implemented each module other than Wallet, BS Device, and NFT marketplace in figure 2. We use Node.js for frontend and backend implementation, run the local blockchain network by hardhat [7], and use Hitachi's H-1 finger vein scanner as a BS device. This device and that management software work as a wallet. We confirmed the operation of each process of signing contents using biometric information, creating NFT, and verifying signatures assigned to NFT. This prototype was built on a local laptop machine and operated independently from the external environment. We used RSA signature and SHA256 and confirmed that signatures are generated less than 1200 ms in the prototype environment (Windows11 Home, CPU: Intel Core i5-1135G7/2.4GHz, Memory: 8GB, and H-1(PC-KCA110)), which was confirmed to be fast enough for practical use.

About the smart contract implementation, we extended the ERC-721 implementation of OpenZeppelin [8] to store necessary information in figure 3 and made additional APIs and those implementations to receive related information for minting NFT and verification.

Figure 6 shows the signature verification screen of the generated NFT. The signer's name is shown on original NFT images just for demonstration. We don't change NFT's original image and generate a signature from the original data. This QR code is generated from the creator's public key and signature information in the NFT smart contract.

VI. Related Work

Many prior studies use biometrics for authentication or how to keep templates secure [9] [10]. Some use it for signature generation [11] [12], but those are unrelated to NFT. For this



```
Hash: 3c3846ec7eef185a8636fe39b04227fafb26bc17378c51090d7ca8170e6e0d20
PublicKey: 04591f34966d1a38699330a92a2d612baf2da32dc6c591f24b9c006d51b3a3d5212a2904fe3e993df53d0cd0f5986de774ce3d6ba251fd69573041ca12381b3362
Signature: 304402205db56038de458590b54046c902fc24b0ceeae4925acc919bdd57f252088add7c02205fdd5018dcd737e25c8d082efe3f5d738883c5d58d6c26753443482756c9b86b
```

Fig. 6. Minted NFT

reason, we will investigate and compare services similar to the Proof of Origin concept.

A. Brief Description of Similar Services

1) Autograph [13]: Autograph is a service launched by Tom Brady, a famous American football player, that sells NFT autographs of prominent sports players. The signature is image data; no digital signature seems to be attached. Autograph checks whether the signature is the original by using personal identification documents.

2) AutographNFT [14]: AutographNFT is a service that requests others to sign NFTs. Requests can be made easily via SNSs for signatures on NFTs held by the user. The signature is only displayed on the NFT content as an X(Twitter) account. The image information, including the X(Twitter) account and information on who signed the autograph, appears to be implemented off-chain to check their services.

3) ArtistCert [15]: This service provides artists with legally valid digital signatures for NFTs and related rights. The link to the PDF is realized by writing the URL in the NFT metadata. A QR code authenticated by Skriblle [16] is stored in the PDF.

4) AllCertified [17]: A service that provides NFT content with a sticker verified by the creator and other relevant parties. Identity verification is done by AllCertified through online meetings and other means.

5) Physical Backed Token [18] [19]: A technology proposed by Azuki to link real-world objects to NFT. It's called SCAN to OWN. When a smartphone first reads this, the corresponding NFT is issued, and the NFT holder information is changed according to when the transfer occurs in the physical world.

6) Startrail [20], Starttrail PORT [21]: Authenticity assurance service provided by StartBurn for physical artworks. This service attaches NFC tags to physical artwork. The tag is linked to NFT, which contains artwork analysis information to ensure authenticity.

7) Content Authenticity Initiative [22]: An association to define industry-standard metadata to manage the provenance of content reliably. While blockchain is not mandatory, it has introduced initiatives that have utilized NFT in the past [23].

8) Numbers Protocol [24]: Their service provides digital media provenance by using blockchain. Their ”Blockchain Camera App” and ”Capture App” applications work with smart contracts on the blockchain. This service assigns ”Numbers ID” to distinguish other contents in the network and manages the contents' history.

B. Comparison of Services

Although obtaining detailed information on any services is impossible, they all store signatures off-chain, raising concerns about their future use. Similarly, all companies perform their identity verification. This is why the service provider is a Single Point of Trust (SPOT). The SPOTs in a decentralized blockchain environment raise concerns about the trustworthiness of the data. Proof of Origin is significantly superior in this regard. Our concept matches the contents' provenance, too.

VII. Conclusion

In this paper, we proposed the concept of ”Proof of Origin,” which is to give authenticity to NFTs by combining them with biometrics information. We have designed a system architecture to realize this concept and implemented a prototype. By realizing this concept, we can provide the following advantages.

1) Assign authenticity to NFT: ”Who created this NFT?”
2) Add more value to NFTs by authenticity
3) Increase the historical value of NFT transactions, etc.
4) Free from secret key management when creating transactions such as NFT creation.
5) Provide a sense of security to NFT users.

References

[1] 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

[2] K. Takahashi, T. Matsuda, T. Murakami, G. Hanaoka, and M. Nishigaki, “Signature schemes with a fuzzy private key,” *International Journal of Information Security*, vol. 18, no. 5, pp. 581–617, 2019.

[3] T. Matsuda, K. Takahashi, T. Murakami, and G. Hanaoka, “Fuzzy signatures: relaxing requirements and a new construction,” in *International Conference on Applied Cryptography and Network Security.* Springer, 2016, pp. 97–116.

[4] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” *SIAM journal on computing*, vol. 38, no. 1, pp. 97–139, 2008.

[5] J. Benet, “Ipfs - content addressed, versioned, p2p file system,” 2014.

[6] OpenSea, “Metadata standards,” https://docs.opensea.io/docs/metadata-standards.

[7] Nomic Foundation, “Hardhat,” https://hardhat.org/.

[8] OpenZeppelin, https://docs.openzeppelin.com/contracts/4.x/erc721/.

[9] O. Delgado-Mohatar, J. Fierrez, R. Tolosana, and R. Vera-Rodriguez, “Biometric template storage with blockchain: A first look into cost and performance tradeoffs,” in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2019, pp. 2829–2837.

[10] F. Toutara and G. Spathoulas, “A distributed biometric authentication scheme based on blockchain,” in *2020 IEEE International Conference on Blockchain (Blockchain)*, 2020, pp. 470–475.

[11] Y. Kaga, M. Fujio, K. Naganuma, K. Takahashi, T. Murakami, T. Ohki, and M. Nishigaki, “A secure and practical signature scheme for blockchain based on biometrics,” in *Information Security Practice and Experience*. Springer International Publishing, 2017, pp. 877–891.

[12] Y. A. Lotfy and S. M. Darwish, “A secure signature scheme for iot blockchain framework based on multimodal biometrics,” in *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2020*, A. E. Hassanien, A. Slowik, V. Snášel, H. El-Deeb, and F. M. Tolba, Eds. Cham: Springer International Publishing, 2021, pp. 261–270.

[13] Autograph, https://autograph.io/.

[14] AutographNFT, https://autographnft.io/.

[15] ArtistCert, https://www.artistcert.art/.

[16] Skriblle, https://www.skribble.com/en-eu/legal-validity/.

[17] AllCertified, https://www.allcertified.ai/.

[18] 2pmflow, locationtba, C. Robertson, and cygaar, “Erc-5791: Physical backed tokens /minimal interface for linking ownership of eip-721 nfts to a physical chip,” https://eips.ethereum.org/EIPS/eip-5791, 10 2022.

[19] Azuki, “Introducing the physical backed token (pbt),” https://www.azuki.com/updates/pbt, 10 2022.

[20] Startrail, https://startrail.io/.

[21] StarttrailPORT, https://startbahn.io/startrail-port.

[22] Content Authenticity Initiative, https://contentauthenticity.org/.

[23] W. Allen and A. Parsons, “Nfts & provenance: How cai protects creators and collectors alike,” https://contentauthenticity.org/blog/protecting-creators-in-the-nft-world-with-cai-code, March 2021.

[24] Numbers Protocol, https://www.numbersprotocol.io/.