Wood traceability system using blockchain and zero-knowledge proof

K. Shibano 1, T. Nakajima 2 and G. Mogi 1

1 Department of Technology Management for Innovation, The University of Tokyo, Tokyo, Japan
2 Department of Forest Science, The University of Tokyo, Tokyo, Japan
E-mail: shibano@tmi.t.u-tokyo.ac.jp

Summary: The system proposed in this study uses zero-knowledge proof (ZKP) to verify the traceability of wood recorded in a public blockchain. Wood is a byproduct of several states, ranging from standing trees to logs, lumber, and wood products (hereinafter “wood objects”). The advantage of using the blockchain for record keeping is that participants can freely record the information at their discretion, without any restrictions. However, the openness of the blockchain may allow a malicious third party to introduce disinformation. In this study, we employ ZKP and near-field communication (NFC) chips to eliminate the possibility of disinformation introduction. ZKP is used to prove/validate changes in the state of wood objects, and the unique nonce associated with that state is encrypted and recorded on an NFC chip. The nonce is concealed and its id of the wood object is defined as hash value of this nonce. We developed a prototype system based on an Android application and an Ethereum smart contract. We confirm that wood traceability and verification can be performed using the prototype system.

Keywords: blockchain, traceability, supply chain management, zero-knowledge proof, NFC, wood, logs, lumber.

1. Introduction

In this study, we propose a traceability system for trees, logs, lumber, and final wooden products based on a public blockchain and zero-knowledge proof (ZKP). The blockchain has the advantage of allowing any user to keep records on it without restrictions. Furthermore, because records can be kept semi-permanently, it is possible to avoid the loss of existing tree records. However, because anyone can input a record on the blockchain, there is a possibility that third parties will record malicious disinformation. For example, if there is a very expensive tree, a person may wish to mislead others by claiming that his log was generated by that tree. ZKP can be used to verify which trees are used to make wood and which wood products are made from which wood, eliminating the possibility of disinformation. This can be done by using only the records on the blockchain. We have developed a prototype system using an Android application and an Ethereum smart contract to verify its operation.

End users will be able to confirm the origin of wood products using the proposed system. This may provide high added value that could not be realized until now. For example, a good-luck charm for academic success in school made from a tree on the campus of the same university may have a high added value. It would also help to reduce illegal timber.

2. Related studies

Several wood traceability systems that use blockchain have been proposed. Figorilli et al. (2018) use RFID, the blockchain, and a client-server application to implement a wood traceability system [1]. Cueva-Sánchez et al. (2020) propose a system that uses Hyperledger Fabric to eliminate illegal wood in the wood supply chain. They developed web and mobile applications [2]. There exists wood traceability system using not only blockchain but also ZKP. Xue et al. (2022) propose ZKP for a public blockchain-based system to prove transactions while ensuring privacy protection [3]. Baliyanet et al. (2021) propose a highly transparent system that utilizes blockchain and RFID for general supply chain management systems. It prevents fraud by having the Law Enforcing Agency assess transactions. They mention wood traceability as an area of application [4]. Further details on blockchain-based wood traceability systems can be found in He and Turner (2022) [5]. The novelty of this study is that it uses ZKP to prove traceability. Traceability can be verified by the information in the blockchain only.

3. Zero-knowledge proof

ZKP is a protocol that allows a prover to tell a verifier that a proposition is true without conveying any knowledge other than that the proposition is true. We use zkSNARKs, a noninteractive zero-knowledge proof protocol used in many blockchain applications. The process to be proven has inputs and outputs and is converted into a circuit. Then, a trusted setup ceremony is performed to generate proving and verification keys. The prover generates a witness using the circuit, the proving key, and input. The verifier can confirm that the prover used the correct value for the private input using the verification key for the proof and public output. The public output is the output of the process and the value of the public input.

4. System overview

In this system, historical state records of wood supply chains, such as trees, logs, lumber, and wood products (hereinafter “wood objects”) can be verified by referring to only blockchain records. A supply chain record has a tree structure and the state changes in one direction. We assume there are two users of the
proposed system: a prover and a verifier. The prover is a wood object producer or processor, and the verifier is a consumer. The prover uses an Android application to record unique information of the wood object on a near-field communication (NFC) chip and generate a proof of ZKP. The NFC chip is attached to the corresponding wood object, and a proof of ZKP is simultaneously recorded to the blockchain when information is recorded on the NFC chip. The verifier can verify the wood object’s traceability by verifying the proof. When writing to the blockchain, the signature is also recorded, allowing verification of who wrote the record. The key pair of the private and public keys of elliptic curve cryptography is stored in the Android application and can be used for signing and encryption/decryption. The Elliptic Curve Digital Signature Algorithm (ECDSA) is used for signatures, and the Elliptic Curve Integrated Encryption Scheme (ECIES) is used for public key cryptography.

5. Design of Android application and developing environment
The prototype system comprises an Android application, an Ethereum blockchain, and an NFC chip.

In this system, we use circom and snarkjs [6] for ZKP as libraries to implement. snarkjs [6] is used in the Android application to generate proof. The circuit and proving key data loaded in snarkjs are generated previously in the PC using circom, whose ZKP scheme is Plonk. Since it is a JavaScript library, it cannot be run directly in the application. A web server is set up within the application and accessed via WebView. web3j [7] connects to the Ethereum blockchain.

Key pairs associated with Ethereum’s externally owned accounts are used for keys related to ECDSA and ECIES. The private key is stored in the application’s storage area, bouncycastle [8] is used as the ECIES library, and web3j is used for the ECDSA library.

The Ethereum smart contract only records data for which the ECDSA signature and the proof of ZKP have been verified, and the ZKP verification contract is the snarkjs output.

The development environment is Ryzen 3600, 16 GB RAM (Windows 10), the Android device is Pixel3a (Android 12), the Ethereum blockchain is built locally using Ganache [9], and the NFC chip is MIFARE Classic 1k. Fig. 1 shows the Android device and NFC chip used in the development.

6. Proof of traceability by zero-knowledge proof
A random number called “nonce” is encrypted and recorded on the NFC chip with its id. Each wood object w has a unique id created, as expressed in (1).

\[ id_w = \text{hash}(\text{nonce}_w). \]  

Ids are used to identify wood objects and are related to other metadata in or outside the blockchain. When running a proof/verification process, an error occurs if the id and nonce of the previous wood object state p is not available. In this process, the public input is the id of p, the private input is p-nonce and w-nonce, the main process is the calculation of the hash value, and the output is the id of w. The flow of the process is shown in (2). If w is a tree, p-nonce is assigned to 0, and p-id is assigned to a hash value of 0. Process (2) is converted into a circuit using circom [6]. Proving and verification keys are generated based on the circuit. The circuit data and the verification key are built into the Android application. The verification process using the verification key can be performed using an Ethereum smart contract.

function CalculateID (  
  public input p_id,  
  private input p_nonce,  
  private input w_nonce) {  
  p_hash = hash(p_nonce);  
  p_eq = p_hash == p_id;  
  w_hash = hash(w_nonce);  
  return w_hash * p_eq;  
}

After a nonce is generated using the prover's Android device, it is recorded on an NFC chip and
then discarded. ECIES encryption is performed using the public key in the device, and the encrypted nonce is recorded on the NFC chip with the id. Therefore, once a nonce is written on the NFC chip, only the prover can decrypt it by reading the NFC chip. To generate an id of wood objects without trees, the parent’s nonce is required. The device that recorded the previous id in the NFC chip can read and decrypt nonce on that NFC chip. That nonce is received separately from that device, and along with its generated nonce, the public output and proof are generated in the process (2) and recorded in the blockchain. A QR code is used for transmitting the previous id and nonce between Android devices.

The sequence of all process is shown in Fig. 2. This shows an example that a log is generated from a tree. The first row shows initial setup procedure on PC. Output results are a circuit file and proving and verification keys. The circuit file and proving key are built-in Android application. The verification key is used for smart contract in the blockchain. The second and third rows show how to record the information of the wood objects in the blockchain using Android application.

7. Prototype experiment
We confirmed that the developed prototype system works correctly. We have simulated a scenario where we cut down a tree and generated a log from it. We conducted two tests: (A) whether the NFC chip can be attached to an actual tree and remain without peeling off over a long period of time and (B) whether verification using the application worked properly.

(A) To check whether it is safe to leave the NFC chip on the tree, it was taped to a tree in a forest managed by the University of Tokyo. We confirmed that it remained there for 6 months without incident (Fig. 3).

(B) Next, we confirmed that only records verified by ECDSA signature and ZKP are recorded in the Ethereum blockchain. There are two Android devices: one for the tree and another for the log. The device for the tree read data from the NFC chip, decrypts nonce, and transmitted the tree nonce to the device for the log by a QR code on the app. The log device generated a new nonce and id of the log. Then, this device generates an id and an encrypted value of the new nonce to a new NFC chip. The proof and public output were recorded in the blockchain.

| w-id | p-id | Proof of ZKP | Signature | Registerant |
|------|------|--------------|-----------|-------------|
|      |      |              |           |             |
We should also confirm whether this system can be used without problems for actual lumber processors. We plan to assess this with Japanese companies.

Although this system is applied to the traceability of wood in this study, it can be applied to the traceability of all products with the same relationships. We study what products and goods the system can be applied to and what value it might generate.

9. Conclusions

In this study, we proposed a method for verifying wood traceability using blockchain, NFC chips, and zero-knowledge proof. We constructed a prototype system and confirmed that wood traceability verification can be performed accurately. This system is a sample application of ZKP using an Android application and the Ethereum blockchain, and we hope this study’s results will help develop applications using ZKP.

Acknowledgments

This work has been supported by Endowed Chair for Blockchain Innovation and the Mohammed bin Salman Center for Future Science and Technology for Saudi-Japan Vision 2030 (MbSC2030) at The University of Tokyo.

References

[1] S. Figorilli, et al. A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain. Sensors 18 (9), 3133, 2018.

[2] J. J. Cueva-Sánchez, A. J. Coyco-Ordemar, and W. Ugarte. A blockchain-based technological solution to ensure data transparency of the wood supply chain. 2020 IEEE ANDESICON, 2020.

[3] Y. Xue, and J. Wang. Design of a blockchain-based traceability system with a privacy-preserving scheme of zero-knowledge proof. Security and Communication Networks 2022, 2022.

[4] A. Baliyan, K. S. Kaswan, Akansha, and N. Mittal. Blockchain assembled supply chains to foster secure trading using distributed ledger. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), 2021.

[5] Z. He, and P. Turner. Blockchain Applications in forestry: a systematic literature review. Applied Sciences 12 (8), 3723, 2022.

[6] Iden3 docs, (https://docs.iden3.io/).

[7] Web3j: Web3 Java Ethereum Dapp API, (https://github.com/web3j/web3j).

[8] Bouncycastle, (https://www.bouncycastle.org/java.html).

[9] Ganache, (https://trufflesuite.com/ganache/).

[10] Etherscan Ethereum Gas Tracker (https://etherscan.io/gastacker).

[11] Coinmarketcap Ethereum (https://coinmarketcap.com/currencies/ethereum/).