

Implementation of Quality Management System for Wild-Simulated Ginseng Using Blockchain

Youngjun Sung and Yoojae Won*

Abstract

A special government agency has been charged with implementing quality management to guarantee the quality of wild-simulated ginseng. However, these processes are carried out by use of documents, and this has resulted in information omission and high document management costs. To solve this problem, this study analyzed the existing quality management process by using a smart contract for the existing offline form and proposed a new quality management system for storing and managing all log data in the blockchain. This system reduced documentation management costs about quality management and recorded information in the previous step through the quality management steps, thus forming a step-by-step record chain. Experiments were conducted by implementing this system, which improved data integrity and reliability. Additionally, sensitive information, such as personal information, was included in the system by use of the off-chain technology.

Keywords

Blockchain, Smart Contract, Off-Chain, Quality Management System

1. Introduction

There is a growing interest in food safety worldwide and an increase in the production of organic foods. Since consumers may find it difficult to distinguish these organic foods from regular foods, every country certifies food quality through the establishment of certain laws or standards [1]. South Korea has established a food quality certification system, which has passed several quality management laws (e.g., laws related to pesticide-free and organic foods). Wild-simulated ginseng, a forest product, has been designated as a domestic quality management food. Wild-simulated ginseng is grown in an environment similar to that of ginseng in the wild, and no pesticides are used during its cultivation process. This differs from the cultivation process for general ginseng, and consumers often find it difficult to identify this difference; therefore, a special law requires government agencies to manage all ginseng production processes and certify their quality [2] (Table 1, Fig. 1).

The quality management process for wild-simulated ginseng manages all processes in a step-by-step manner from the start of cultivation to sale to the consumers. Wild-simulated ginseng that has passed all the steps can be distributed and sold with a certificate of acceptance provided by government agencies. However, quality management is an inefficient process for documenting and managing all processes for

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Manuscript received September 10, 2021; first revision December 2, 2021; accepted December 19, 2021.

*Corresponding Author: Yoojae Won (yjwon@cnu.ac.kr)

Dept. of Computer Science and Engineering, Chungnam National University, Daejeon, Korea (tjd428@o.cnu.ac.kr, yjwon@cnu.ac.kr)

at least seven years. The process of sales requires more than 20 documents which must be maintained separately. This method is inefficient because it incurs significant document management costs. Even in the production record process, which is one of the quality management stages, producers who grow wild-simulated ginseng maintain handwritten records [3].

Table 1. World organic agricultural land by region: 10 years growth [1]

Region	Organic agricultural land 2019 (ha)	10 years growth (ha)	10 years growth (%)
Africa	2,030,830	958,706	89.4
Asia	5,911,622	3,453,707	140.5
Europe	16,528,677	6,499,896	64.8
Latin America	8,292,139	752,496	10.0
North America	3,647,623	1,174,944	47.5
Oceania	35,881,053	23,735,998	195.4
Total	72,285,656	36,571,729	102.4

The period of inspection by the management agency is very long (3 years). Inspection cycles can cause information omission during the production process. Consequently, a transparent production process is not provided to consumers, and consumers have to trust and purchase the wild-simulated ginseng using only a single authentication method, a pass certificate. To solve this problem, we intend to provide a transparent quality management system using blockchain technology, which has been recently used in various fields such as supply chain management (SCM) and digital certificates [4,5].

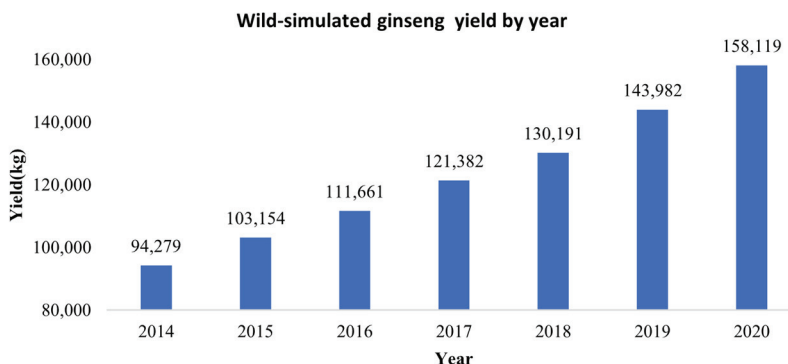


Fig. 1. Wild-simulated ginseng yield by year.

In this study, we propose a quality management system that satisfies all legal requirements for the quality management of wild-simulated ginseng. The system utilizes a private blockchain to form a blockchain network for the quality management stakeholders. After network configuration, the existing quality management process is analyzed, and smart contracts are introduced into the step-by-step process to automate the offline process online and record step-by-step information on the blockchain. Lastly, due to the nature of the blockchain, the information recorded therein is also disclosed to third parties, so it is not suitable to record information in the same format as personal information. To this end, the personal information included in the form uses off-chain technology to prevent sensitive data from being recorded and exposed on the blockchain.

2. Related Work

2.1 Blockchain-based Data Management

2.1.1 Supply chain management

SCM technology manages flows so that the entire process from raw material procurement to product delivery can proceed smoothly. The technology tracks and manages information regarding products (e.g., supply, manufacturing, wholesale, and logistics) from a single value chain perspective. As supply chains develop, their management and control may become complex. However, as SCM is an important factor in increasing company competitiveness, it is important to strengthen it, for example, using models that evaluate the degree of trust between supply chain partners [6]. It is also important to increase reliability within SCM, for example, using blockchain technology (a distributed ledger technology). Blockchain technology provides transparency, traceability, and security and can mitigate several SCM problems. Thus, it is important to increase the number of cases in which blockchain technology is applied to SCM [7].

2.1.2 Digital certificates

Certificates, a type of official document used for fact-checking, can be used in various ways (e.g., certificate of completion, confirmation, certificate, and diploma). Offline certificates pose the risk of being lost and have several other disadvantages that users must manage separately. Conversely, digital certificates have several advantages, such as a lower risk of loss and convenient management. However, digital certificates also pose certain risks, such as forgery and falsification; hence, a separate management process is required to verify their authenticity [4]. Blockchain technology can provide a solution to this problem. In addition to the distributed storage and management of existing digital certificates in a blockchain, blockchains and smart contracts can be used to automatically issue and manage digital certificates when certain conditions are met. A digital certificate solution utilizing blockchain technology is proposed in this paper [8].

2.1.3 Internet of Things management

The Internet of Things (IoT), an interconnected smart device, shares sensed data through a network and enables the monitoring, sharing, and adjustment of interactions between things that are connected through the Internet. Several methods have been proposed to utilize IoT management by applying blockchain technology [9].

Consider an example of a smart car that records and manages all state data and errors that occur in the vehicle (e.g., information regarding tires, oil, and temperature) in a blockchain [10]. Recent research has focused on the use of blockchains to manage the operational integrity of black box data inside cars, and cases of blockchains being used to maintain data integrity are growing [11].

2.2 System Configuration

2.2.1 Blockchain

Blockchain technology distributes and manages data in blocks to multiple nodes in a P2P network [12].

The nodes can select other nodes for distributing blocks using a consensus algorithm before distribution [13]. The selected node creates a new block by writing the hash value of the previously created block in the block header. After this block generation process, all blocks (except the genesis block) form a hash chain that stores the hash value of the previous block. The hash chain maintains data integrity and prevents malicious users from forging and manipulating data. The hash chain is formed through the process shown in Fig. 2.

A given blockchain can be broadly divided into a public blockchain and a private blockchain based on its configuration, and the relevant differences are listed in Table 2. A public blockchain is an open network where anyone can participate; although free participation is possible, it has the disadvantage of slow block generation. In a private blockchain, each participant receives a different type of permission, and only a small number of nodes with consensus authority can proceed with consensus formation, which allows faster block generation but forfeits the benefit of decentralization.

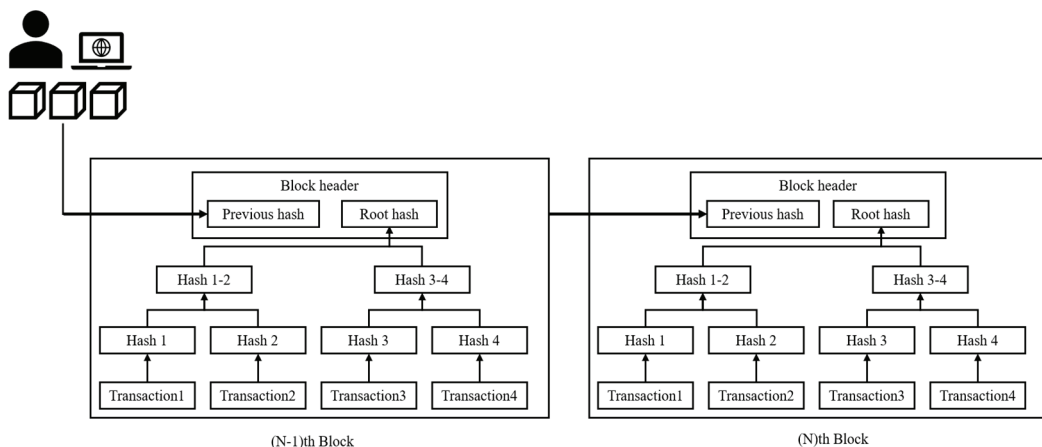


Fig. 2. Hash data recorded in the block header.

Table 2. Comparison of public and private blockchains

	Public blockchain	Private blockchain
Consensus	All miners	Selected set of nodes
Read	Public	Public or restricted
Write	Public	Restricted
Speed	Slow	Fast
Member	Anonymous	Known identity

2.2.2 Smart contract

The smart contract concept was first proposed by Nick Szabo [14], where contracts between contracting parties are written in code and automatically executed when the conditions are met. Buterin [15] implemented the smart contract concept using the Solidity language provided by Ethereum, which allows for the use of various blockchains for various purposes (e.g., electronic voting and real estate transactions) [16].

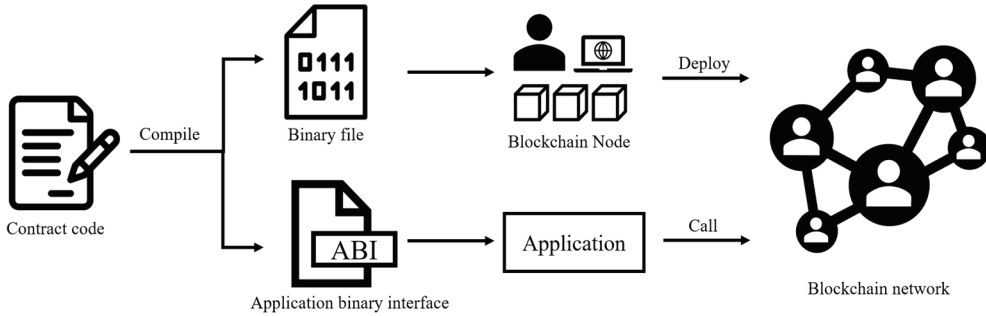


Fig. 3. Hash data recorded in the block header.

Fig. 3 depicts the smart contract deployment of Ethereum. The contract code is compiled into a binary file, which is recorded in the blockchain, and an application binary interface (ABI), which provides an interface for the deployed contract. The distributed code can be used as an interface for recording specific log data in the blockchain and for providing automated contracts.

2.3 Off-Chain

The nature of blockchain allows for the opening of the data stored in the block to the network participants, so this system is unsuitable for storing sensitive information or large files with extensions such as img, mp3, and mp4 in the block.

The off-chain mechanism provides functions for managing private data and large-capacity data in the blockchain. Once data are stored outside the block, metadata referring to the corresponding raw data can be recorded and managed in the blockchain. The storage methods for the on-chain and off-chain mechanisms are shown in Fig. 4.

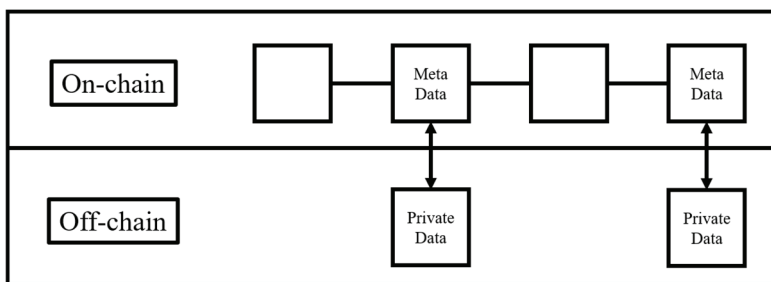


Fig. 4. Off-chain use in the blockchain.

3. Proposed Quality Management System

3.1 Existing Quality Management Process

From cultivation to the market, wild-simulated ginseng production quality management is executed by two agencies (Agency1 and Agency2). The applications for each course and the issuance of the results are all completed through offline documents. A certificate attesting the previous step has been passed

must be attached when applying for permission to conduct the next step.

Before commencing wild-simulated ginseng production, the ginseng must be inspected by Agency2 to determine its suitability for production. Production commences only after Agency2 has obtained inspection results and filed a favorable report. The production lasts at least seven years, and every three years, Agency2 inspects production progress and records its findings. To be allowed into the market produced wild-simulated ginseng must be inspected for quality. During this process, all the aforementioned records are investigated. Only wild-simulated ginseng that has passed all these inspections may be awarded a certificate of acceptance and thereby allowed into the market. Even after distribution, the two agencies inspect whether it is the accredited ginseng that was distributed. Figs. 5 and 6 present brief flowcharts depicting this process.

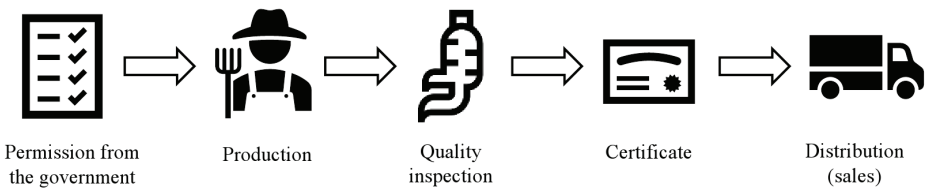


Fig. 5. Quality management process steps.

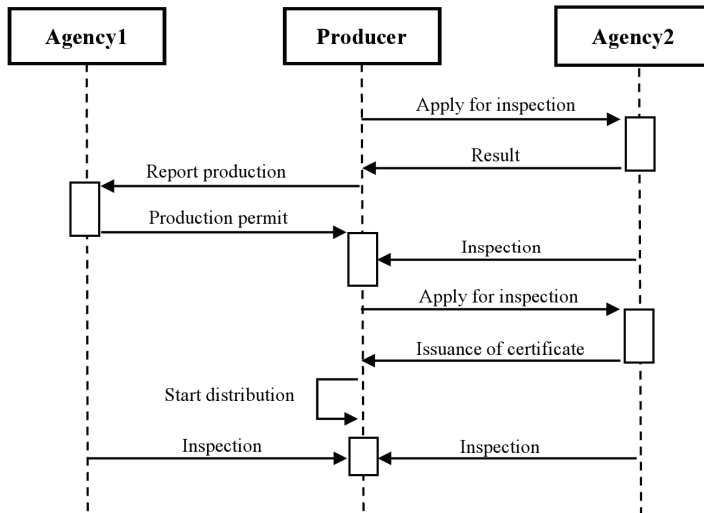


Fig. 6. Existing quality management process.

3.2 Quality Management using Blockchain

To apply blockchain to the existing quality management process, we analyzed the existing process and proposed the use of smart contracts. In the proposed system, the smart contract is used as an interface for processing existing offline documents online and recording log data onto the blockchain.

The smart contract is primarily divided into five stages, where all stages (except the first) record the address of the previous stage so that the results can be referred to in the previous management process. In the first step, we allowed the recording of commonly required personal information on the form.

However, because personal information is unsuitable for recording on a blockchain that is disclosed to network participants, we recorded the personal information off-chain, and any metadata that could be referred to in the record was recorded on the blockchain. In the subsequent steps, an automated contract is generated in the section where the producer requests from the institution and the section records the production process in the existing process, and the result is recorded after satisfying the pass conditions such as pass in the previous step. Fig. 7 depicts the flow of the proposed system.

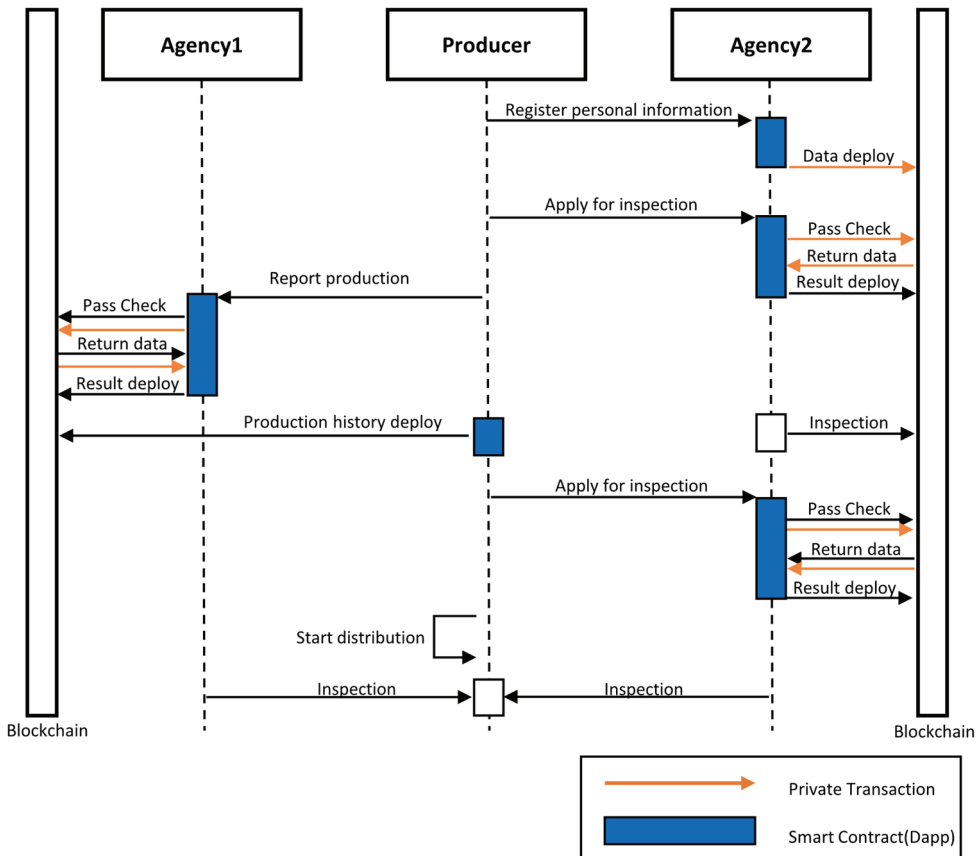


Fig. 7. Existing quality management process.

3.3 Network Design

Blockchain for the quality management system consists of a private blockchain, not a public blockchain. In the proposed system, the network is opened up and composed of permitted participants rather than free participation to speed up to block generation and restrict some privileges. In the proposed system, only authorized nodes to operate nodes in the network, and participating participants have read, write, and consensus rights on blocks by establishing a consortium of producers and two agencies. Other participants can only read the information on the blockchain. The detailed node configuration is as follows.

First, each network participant constitutes an off-chain node (in addition to the blockchain node.) When storing information using on-chain metadata, metadata that can identify only the node to share information with is stored. For this purpose, an off-chain group is selected. For example, if there are n

nodes in the blockchain network, at least three of them will constitute one private group. The group will have the same off-chain so that the producer can inquire about the personal information recorded. Private data are managed with an off-chain mechanism so that the other nodes within the same blockchain network cannot be inquired about unless they are in the same group. Fig. 8 shows the blockchain network.

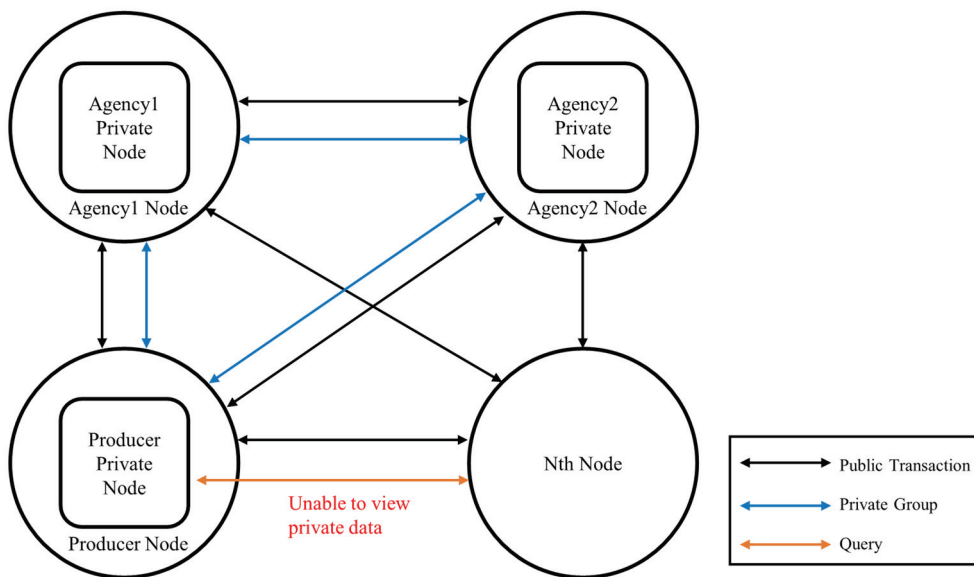


Fig. 8. Blockchain network with private groups.

4. Implementation and Experiments

4.1 Implementation Environment

We established a blockchain network environment to test whether the proposed quality management system could solve problems in the existing process. The detailed implementation of the environment of this study is presented in Table 3.

Table 3. Implementation environment

	Environment
OS	Ubuntu 20.04.2 LTS
CPU	Intel Core i7-7700 CPU @ 3.60 GHz
RAM	16 G
Ethereum client	Hyperledger Besu v21.7.2
Off-chain	Tessera v21.7.2
Web sever	Nodejs v14.17.5
Smart contract	Solidity v0.7.0

Four experimental nodes were built in the same VMware-based virtual environment. We used a blockchain platform provided by Hyperledger Besu, an open-source Ethereum client, and Tessera, an off-


```

"result" : {
  "blockHash" :
  "0x933c8c8f2b9dcd7b46cd22918957d86734f2d9832cd55b8490481ce25270d43a",
  "blockNumber" : "0x2053a",
  "from" : "0x3cfa51d06456fc025f2aea38871bc685aeedaeca",
  "gas" : "0x2dc6c0",
  "gasPrice" : "0x0",
  "hash" : "0x8ee41ff7bd517e9fb77fa440fe743f2da09d312717d460fc564dd2d51c5b553d",
  "input" : "0xa99c52940bf8a9e5e710c9b0906520c6e0840dled368a9e9b39262647bcb9ae1",
  "nonce" : "0x0",
  "publicKey" :
  "0xe307c3eb1b33105d9812c2c5b410b5298bfea7739b9fa73e31d4alfbee4e94d8d7a39868936
  ba22516e2 885eb785b5185e7a69e06f8bbb89ebe9f87f11edd3f8",
  "raw" :
  "0xf88080832dc6c0940000000000000000000000000000000000000000000000007e80a0a99c52940bf8
  a9e5e710c9b0906520c6e0840dled368a9e9b39262647bcb9aellca0e3658b1df3ad407f764ad7
  85428722eac84d1c8f27d20442ee90a72bc765aee2a03896c41c570759c93352be3adifc23fe03
  e9560a6538fce718d1a41bbeac5002",
  "to" : "0x0000000000000000000000000000000000000000000000000000000000000007e",
  "transactionIndex" : "0x0",
  "value" : "0x0",
  "v" : "0x1c",
  "r" : "0xe3658bldf3ad407f764ad785428722eac84d1c8f27d20442ee90a72bc765aee2",
  "s" : "0x3896c41c570759c93352be3adifc23fee3e9560a6538fce718d1a41bbeac5002"
}
    
```

Fig. 10. Lookup not using off-chain.

If a private transaction is searched inside the blockchain without using a node or an off-chain that is not in the same group, a general transaction receipt is returned. The transaction is written for the Ethereum environment, and its contents and receipt are the same. However, this information alone cannot reveal what was recorded. Even if a third party checks its contents, they will not find personal information unless they have an off-chain that has the same configurations as the owner’s private group.

Conversely, if an off-chain that can identify metadata is configured in the transaction, information can be retrieved easily. The transaction recorded in the off-chain is returned by referring to the metadata recorded in the on-chain. The recorded data are stored in the information recorded in the off-chain, and the recorded personal information can be queried in the system.

Register

Register	Application	Record	Result
Besu PrivKey	<input type="text" value="0x04dd868d1a9880ad7056bba493cec48efffe69b41"/>		
Name	<input type="text" value="Young jun"/>		
Address	<input type="text" value="test address"/>		
Phone Number	<input type="text" value="01012345678"/>		
Brithday	<input type="text" value="01/08/1996"/> <input type="checkbox"/>		
<input type="button" value="regist"/>			

Register

Register	Application	Record	Result
Registration Success Log			
Private data address : 0xfe9690ad2f1027e4ec80a5b177cda71b2af96b40			
Name : Young jun			
Brithday : 1996-01-08			
Address : test address			
Phone Number : 01012345678			
My Address : 0x355152aB610Cb71E40510351866f4F93A8aD224c			

Fig. 11. Personal information registration UI.

Fig. 11 depicts a web application for recording personal information. When personal information is recorded (e.g., producer's name, home address, and phone number), it is stored separately in the off-chain, and only institutions and personal information subjects involved in the quality management process can inquire about this information.

4.3 Application and Record

In the subsequent steps, an automated contract is generated when the production process has passed the current step to pave way for the next step. This is done to proceed with the specific legal quality management process that is used as a means of authentication. Fig. 12 shows the log in which the pass and time were recorded in the previous step.

```
Result {
  '0': true,
  '1': '1631042159',
  '2': '0xc362654f1ae7C0829EF1340DAF386C1FbFea8e3a',
  '3': '0x5F51bb7aB30ba7a8F5B842010706B032aa47275f',
  __length : 4,
  pass: true,
  time: '1631042159',
  preCA: '0xc362654f1ae7C0829EF1340DAF386C1FbFea8e3a',
  admin: '0x5F51bb7aB30ba7a8F5B842010706B032aa47275f'
}
```

Fig. 12. Check whether you passed the previous step.

To search the log in the previous step, the contract address must be known in the previous step. Except for the first personal information registration where the previous step does not exist, all other steps must record the address in the previous step. The abstracted code is shown in Fig. 13.

```
pragma solidity ^0.7.0;
contract abstractCode{

  address admin;
  address previousCA;

  constructor(address _previousCA){
    admin=msg.sender;
    previousCA=_previousCA;
  }

  event successLog(
    uint time,
    address whoami,
    address preCA,
  );

  event result(
    bool pass,
    uint time,
    address preCA,
    address admin
  );
}
```

Fig. 13. Abstract solidity code that writes the previous address.

Essentially, smart contracts, except for the first step, require the admin address to be hosted in the contract and the previous contract address (previous CA) to refer to the results of the previous step. When deploying the initial contract, admin and previous CA are initialized using the constructor provided by

Solidity.

Subsequently, the detailed data to be recorded in the blockchain and the functions that the smart contract should show are different, but the two things need to be recorded in common. First, when the producer succeeds in reporting or application, the relevant information should be recorded. The time of the transaction, the address of the wallet that sent the transaction, and the contract address are recorded in the blockchain before quality management. The second is the information that the management organization needs to record in the blockchain and records whether it has passed the relevant step. Similar to the previous step, the records should be executed only by the governing body.

4.4 Pass Confirmation

In the existing quality management process, when all certification processes are completed, a pass certificate is issued, thus allowing distribution and sales. As the proposed system can inquire about data recorded in the blockchain (e.g., whether the application has been passed) by referring to the address of each step, if the contract address that was passed in the final step is used, then the log data recorded in the blockchain can be used for the previous steps. Therefore, the results can be searched continuously. This function makes it more difficult to falsify accurate management records and logs during each process. Fig. 14 shows the results of the final pass inquiry.

Result

Register	Application	Record	Result
Quality certification completed			
	Private Contract Address :	0xfE9690ad2F1027e4EC80a5b177cda71B2AF96b40	
	inspection1 Contract Address :	0x26AbD4eaaf13683948A6291e9535FC98001d11b2	
	Report Contract Address :	0xc362654f1ae7C0829EF1340DAF386C1FbFea8e3a	
	Record Contract Address :	0x5519f4f46d77a47466B6f5DDeFb753B11aAbbf81	
	inspection2 Contract Address :	0x94e95300569c3269a89fd0510bd5618c92cb96d6	

Fig. 14. Overall quality management record.

Through the certificate, the processing results can be checked when inquiring about the link to each account address. However, the address in which personal information is stored cannot be viewed by a third party. To inquire about this information, a blockchain node with an off-chain that maintains the same group must be used. By accessing from outside the node, we secured an authentication method using the characteristics of the blockchain. The personal information subject transmits a transaction signed with the private key for self-authentication and compares it with the information in the log recorded when creating personal information. The log recorded when registering personal information is shown in Fig. 15.

If the address recorded in the log where personal information was first recorded and the address that signed the transaction were the same, authentication was complete, and the log was recorded, and personal information was inquired. Conversely, if the recorded address and the transaction address were different, it was considered that authentication failed and the corresponding personal information could

not be viewed, so a failure log was recorded. The authentication success and failure logs are shown in Figs. 16 and 17, respectively.

```
Result {
  '0': '1631011925',
  '1': 'jun',
  '2': '2021-09-01',
  '3': 'address test',
  '4': '01012345678',
  '5': '0x355152aB610Cb71E40510351866f4F93A8aD224c',
  __length__: 6,
  time: '1631011925',
  name: 'jun',
  birthday: '2021-09-01',
  addr: 'address test',
  phone: '01012345678',
  from: '0x355152aB610Cb71E40510351866f4F93A8aD224c'
}
```

Fig. 15. Information recorded on the blockchain when registering personal information.

```
From address : 0x355152ab610cb71e40510351866f4f93a8ad224c
Log address : 0x355152aB610Cb71E40510351866f4F93A8a0224c
Success
```

Fig. 16. Personal information authentication success log.

```
From address : 0xd4b7cdfc9217b653621bf776817f05bc6309cb34
Log address : 0x355152aB610Cb71E40510351866f4F93A8a0224c
Fail
```

Fig. 17. Authentication failure log.

5. Conclusion

In this paper, we propose a quality management system for wild-simulated ginseng using blockchain that satisfies legal procedures by analyzing the quality management process for wild-simulated ginseng. The system is based on private blockchain, and institutions and producers related to wild-simulated ginseng production participate in the network and record information. In addition, this study automates the existing process by introducing a smart contract to the existing offline document process and converts it online to reduce document management costs and facilitate convenient quality management procedures. This system increases the integrity of information and provides transparent information to increase the reliability of the quality of wild-simulated ginseng from consumers, and at the same time, it can protect the personal information written in the document by using off-chain technology.

In the future, we plan to actually operate the proposed system for quality management of wild-simulated ginseng to measure the performance of the system and identify additional requirements for the system. Therefore, we try to find a way to supplement the shortcomings of this paper and develop the proposed model into a practical system.

Acknowledgement

This work was supported by an Institute for Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No. 2019-0-01343, Training Key Talents in Industrial Convergence Security).

This study was carried out with the support of the R&D Program for Forest Science Technology (Project No. 2020184C10-2122-AA02) under the Korea Forest Service (Korea Forestry Promotion Institute).

References

- [1] H. Willer, J. Travnicek, C. Meier, and B. Schlatter, *The World of Organic Agriculture 2021: Statistics and Emerging Trends*. Frick, Switzerland: Research Institute of Organic Agriculture (FiBL); 2021.
- [2] Korea Forestry Promotion Institute, "Wood cultivated ginseng information service system," 2015 [Online]. Available: <https://sam.kofpi.or.kr/front/guid/qualCtrlMngSys.do>.
- [3] S. Yu, J. Lee, J. Jeong, and Y. Won, "Design of quality management system for special forest product using blockchain," *Proceedings of the Korea Information Processing Society Conference*, vol. 27, no. 2, pp. 625-628, 2020.
- [4] J. C. Cheng, N. Y. Lee, C. Chi, and Y. H. Chen, "Blockchain and smart contract for digital certificate," in *Proceedings of 2018 IEEE International Conference on Applied System Invention (ICASI)*, Chiba, Japan, 2018, pp. 1046-1051.
- [5] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117-2135, 2019.
- [6] H. Jiao, W. Ding, and X. Wang, "Supply chain trust evaluation model based on improved chain iteration method," *Journal of Information Processing Systems*, vol. 17, no. 1, pp. 136-150, 2021.
- [7] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Computers & Industrial Engineering*, vol. 135, pp. 582-592, 2019.
- [8] W. Y. Jeong and M. Choi, "Design of recruitment management platform using digital certificate on blockchain," *Journal of Information Processing Systems*, vol. 15, no. 3, pp. 707-716, 2019.
- [9] M. Kim, K. Kim, and J. H. Kim, "Cost modeling for analyzing network performance of IoT protocols in blockchain-based IoT," *Human-centric Computing and Information Sciences*, vol. 11, article no. 7, 2021. <https://doi.org/10.22967/HGIS.2021.11.007>
- [10] M. M. Salim, V. Shanmuganathan, V. Loia, and J. H. Park, "Deep learning enabled secure IoT handover authentication for blockchain networks," *Human-centric Computing and Information Sciences*, vol. 11, article no. 21, 2021. <https://doi.org/10.22967/HGIS.2021.11.021>
- [11] T. Kim, I. Y. Jung, and Y. C. Hu, "Automatic, location-privacy preserving dashcam video sharing using blockchain and deep learning," *Human-centric Computing and Information Sciences*, vol. 10, article no. 36, 2020. <https://doi.org/10.1186/s13673-020-00244-8>
- [12] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008 [Online]. Available: <https://bitcoin.org/bitcoin.pdf>.
- [13] M. Du, X. Ma, Z. Zhang, X. Wang, and Q. Chen, "A review on consensus algorithm of blockchain," in *Proceedings of 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Banff, Canada, 2017, pp. 2567-2572.

- [14] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997. <https://doi.org/10.5210/fm.v2i9.548>
- [15] V. Buterin, "A next-generation smart contract and decentralized application platform," 2014 [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
- [16] C. H. Roh and I. Y. Lee, "A study on electronic voting system using private blockchain," *Journal of Information Processing Systems*, vol. 16, no. 2, pp. 421-434, 2020.
- [17] Tesseract private transaction manager [Online]. Available: docs.tesseract.consensys.net/en/stable.
- [18] Hyperledger Besu [Online]. Available: <https://besu.hyperledger.org/en/stable>.



Youngjun Sung <https://orcid.org/0000-0003-4204-870X>

He is pursuing a master's in computer science at Chungnam National University. His main research interests are blockchain and malicious code analyses.



Yoojae Won <https://orcid.org/0000-0002-7706-5983>

He received his B.S. and M.S. degrees from the Department of Computational Statistics at Chungnam National University, South Korea, in 1985 and 1987, respectively. He received his Ph.D. from the Department of Computer Science Engineering at Chungnam National University, South Korea, in 1998. He worked on wireless Internet information security at the Electronics and Telecommunications Research Institute from February 1987 to February 2001 and mobile security at AhnLab from March 2001 to August 2004. His work included incident handling, and he was in charge of management planning at the Korea Internet & Security Agency from September 2004 to February 2014. He is currently a professor in the Department of Computer Science Engineering at Chungnam National University.