Journal of Knowledge Information Technology and Systems(JKITS), Vol. 17, No. 2, pp. 193-202, April 2022
https://doi.org/10.34163/jkits.2022.17.2.002

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700 (Print), ISSN 2734-0570 (Online)

http://www.kkits.or.kr

A Study on the Application of Blockchain Technology for Data Security of Video Conferencing Systems

Taegeun Kang, Dogyung Kim, Jaeheun Han, JiHoon Jo, Hyunbean Yi*

Department of Computer Engineering, Hanbat National University

ABSTRACT

Due to COVID-19, social life has changed rapidly, and non-face-to-face classes and video conferencing services have been becoming commonplace in various fields. Information generated during the meeting should be stored and secured as necessary. Blockchain technology is widely used to enhance the security of data storage and management systems. In particular, research on the application of blockchain to various fields and application systems as a method to prevent data forgery and falsification is active. In this study, we propose a video conference data security method using blockchain technology. In the video conference system, authentication through smart contract, block chain data generation method, block chain server connection structure and implementation examples are presented, and data confidentiality, data integrity, and service practicality of the block chain network structure centered on the representative block chain server are discussed. Based on the private blockchain, the electronic signature of meeting participants obtains consent to store information and blocks the stored information. In the proposed system, data confidentiality is maintained through a permissioned blockchain structure and smart contract. Implementation and operational practicability can be improved by maintaining the the integrity of data through chaining and decentralization of the block chain, and delegating the block chain data to the block chain server instead of the user owning it. In addition, it can be a solution to prevent fraud by a server administrator in a centrally managed system.

KEYWORDS: Blockchain, Smart contract, Electronic signatures, Data distribution, Data security

ARTICLE INFO: Received 15 February 2022, Revised 27 February 2022, Accepted 8 April 2022.

*Corresponding author is with the department of Computer Engineering, Hanbat National University, 125 Dongseo-daero, Yuseong-gu, Daejeon, Korea.

E-mail address: bean@hanbat.ac.kr

1. 서 론

고속 인터넷 망과 무선 통신 인프라가 널리 보급되면서 화상 회의 시스템을 통한 사교 모임, 회의, 교육 등이 일반화 되고 있다. 비대면 안전성, 편의성, 비용 등을 고려한다면 화상 회의 서비스가 사용되는 분야는 사용량은 더욱 증가할 것이다.

화상 회의 시스템을 통한 대화 내용 또한 필요에 따라서는 정보의 재활용, 증명, 가공, 전달 등의 이유로 저장될 필요가 있다. 동시에 위의 정보들은 사용자와 시스템 관리자 모두에게 민감하므로 정보 보호를 위한 기술이 필수적이다. 대부분의 화상 회의 시스템에서는 회의 관련 정보를 시스템 서버가 보관하고 관리한다. 즉, 서버에 적용된 보안 기술과 서버 관리자에 의존하여 신뢰성을 유지한다. 그러나, 위와 같은 구조에서의 보안 방법은 시간이 흐름에 따라서 악의적인 공격에 취약해질 수 있으며 시스템 관리자에 의해 허용되지 않은 정보 탈취와 변경에 대한 위험성이 존재한다[1,2].

데이터베이스 기반이 아닌 데이터 저장과 관리의 탈중앙화와 보안성 강화를 위한 방안으로 블록체인(Blockchain) 기술이 대두되고 있다[3-5]. 블록체인은 블록체인 네트워크에 참여하는 사용자들이 데이터를 발생시킬 때마다 생성된 데이터를 일정한 단위로 블록화하고 각 블록 데이터들에 대한 해시(Hash) 연산 값들을 연쇄화하여 블록들을 이어 붙이는 기술이다. 블록들이 해시 연산으로 연결됨으로써 데이터의 부분적인 변경이 어렵고, 블록들이 네트워크 참여자들에게 공유되어 상호 비교 및 검증이 가능하다.

본 연구에서는 화상 회의 관련 정보 저장에 대한 보안성 강화 목표를 바탕으로 화상 회의에서 발생하는 데이터를 데이터베이스의 장점과 블록체인의 장점을 혼합하여 저장하는 기술을 바탕으로 저장하고 보안하는 화상 회의 데이터 보안 방법을 제안한다. 화상 회의 종료 후 주최자는 스마트 계약(Smart Contract)을 통해 참여자들의 회의 참여 여부를 인증하고 정보 저장 동의를 얻는다. 인증 후에는 회의 정보, 참여자 정보 그리고 회의 내용을 암호화하고 블록체인으로 구성하여 서버에 저장한다. 블록체인화 된 데이터는 다수의 블록체인 노드에 분산 저장된다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인에 대한 전반적인 개념을 정리하고 블록체인과 화상 통신 서비스에 관련된 기존연구에 대하여 언급한다. 3장에서는 블록체인 기술기반 화상회의 데이터 저장 방법으로 스마트 계약을 이용한 인증 과정, 블록체인에 포함되는 데이터의 종류, 데이터의 블록 체인화 과정, 그리고 전체적인 블록체인 서버 구조에 대하여 설명하고 4장에서는 그 보안성과 실용성에 대하여 분석한다. 마지막 5장에서는 제안하는 방법에 대한 가능성과 기대효과를 기술한다.

2. 관련연구

2.1 블록체인

블록체인 기술의 두 가지 주요한 아이디어는 데이터의 체인화와 분산화이다[3-5].

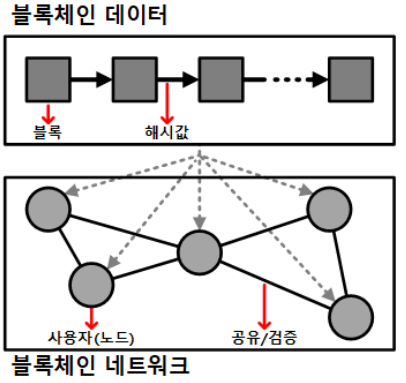


그림 1. 블록체인 데이터와 블록체인 네트워크 구조
Figure 1. Blockchain data and blockchain network structure.

<그림 1>과 같이 데이터가 발생 될 때마다 각 데이터를 일정한 단위로 블록화하고 이전 블록의 해시값을 현재 블록의 해시 연산에 참여시켜 해시값을 구하고 이 해시값을 블록에 포함시킨다. 위와 같은 과정을 통해생성된 블록을 기존 블록에 연결하여 새로운 블록체인 구성한다. 블록체인 데이터는 블록체인 네트워크에 참여하고 있는 사용자(노드, node)들에게 공유되어 분산 형태로 저장된다. 블록체인 데이터에서는 일부 데이터들이 변경이 블록들의 해시값 연관성을 와해시키기 때문에 부정을 감지하고 추적할 수 있다. 또한 노드들 간의 공유와 검증을 통해 데이터의 무결성과 신뢰성을 유지할 수 있다.

블록체인이 활용된 대표적인 사례는 비트코인(Bitcoin)이라 할 수 있다[6]. 블록체인 네트워크에 참여하는 노드들 스스로의, 그리고 노드들 간의 작업을 통해 블록을 생성하고 화폐를 거래한다. 제3의 보증기관 없이 누구나 네트워크에 참여할 수 있으며 거래명세 또한 노드들에 의해서만 데이터 공유와 검증을 수행하여 신뢰성을 유지할 수 있다. 이더리움(Etherium)은 비트코인에 이어 기능 및 성능 보완을 목표로 하는 블록체인 플랫폼이다[7]. 이더리움의 가장 큰 특징으로는 미리 프로그래밍 된 전자 계약서를 바탕으로 거래 명세 이외의 다양한 정보를 포함하여 조건이 충족될 경우 다양한 계약을 자동으로 수행할 수 있는 스마트 계약 기술이 포함되었다는 것이다[8].

블록체인의 네트워크 구조 관점에서 여러 형태의 블록체인이 고안되었다. 대표적으로는 누구나 네트워크에 참여할 수 있는 개방형(Public) 블록체인, 허가된 사람들만 참여할 수 있는 허가형(Private) 블록체인, 개방형과 허가형을 부분적으로 구성하여 연결하는 혼합형(Hybrid) 블록체인이 있다[9, 10]. 일반적으로 많은 사람이 참여하는 개방형 블록체인은 투명성이 높다는 장점이, 허가받은 소수의 사람이 참여하는 허가형 블록체인은 기밀성과 작업 속도가 높다는 장점이 있다.

제안하는 화상 회의 데이터 보안 방법에서는 허가형 블록체인 구조를 바탕으로 하여 데이터의 저장 및 관리를 화상 회의 시스템이 허가한 서버만이 가능하도록 한다. 회의 종료 후에는 스마트 계약 기능을 이용하여 사용자에게 데이터 위/변조 검증 결과를 확인시키고 회의 관련 정보 저장 여부를 묻는 인증 과정을 거쳐 회의 정보, 참여자 정보, 암호화된 회의 내용을 포함한 블록을 생성하고 블록체인을 구성한다.

2.2 기존연구

국내에서도 다양한 분야에 블록체인을 적용하려는 연구들이 진행 중이다. 화상 통신 또는 원격 지원 시스템 분야에서 블록체인 기술을 적용하기 위한 기존 연구는 다음과 같다.

[11]에서의 온라인 학습 플랫폼에서는 온라인 학습의 한계를 극복하기 위해 학습자들의 학업 상태를 분석하고 교수자에게 분석 결과를 제공하기 위해 개인의 영상정보 또는 영상 분석 결과를 저장해야 할 필요성을 이야기하고 있다. 학습자의 개인정보와 학습/평가 데이터와 함께 영상 관련 정보는 민감하기 때문에 블록체인 기술을 이용하여 학습자 관련 데이터를 보안하는 방법을 제안하고 있다.

[12]에서는, 블록체인을 이용한 원격의료 시스템에서의 환자들의 정보를 보호하는 방법을 제시하고 있다. 환자들의 개인정보와 건강정보는 민감 정보이며 정보 유출, 네트워크 장애, 의료 사고들을 방지하기 위해 블록체인 기술을 도입하여 기밀성 및 무결성을 보장한다. 또한 스마트 계약을 이용하여 블록의 생성과 네트워크 접근에 필요한 인증을 관리하여 안정성과 접근성을 유지한다.

[13]은 기존 서버-클라이언트 기반의 화상 회의 시스템에서 회의키 분배에 대한 서버의 부정과 회의 참여자에 대한 개인 정보 보호가 보장되지 않는 점을 해결하기 위해 블록체인의 스마트 계약 기술을 이용한 회의키 분배 방법을 제시하고 있다.

스마트 계약을 통한 회의키 분배 과정에서 스마트 계약 테이블에 미리 저장되어 있는 사용자만이 개인키로 회의키를 추출할 수 있기 때문에 제 3자는 회의키를 조작할 수 없다. 또한 허용된 사용자만이 회의키 생성에 참여하고 그 내용은 변경될 수 없기 때문에 내부에 의한 부정을 추적할 수 있어 보안성을 유지할 수 있다.

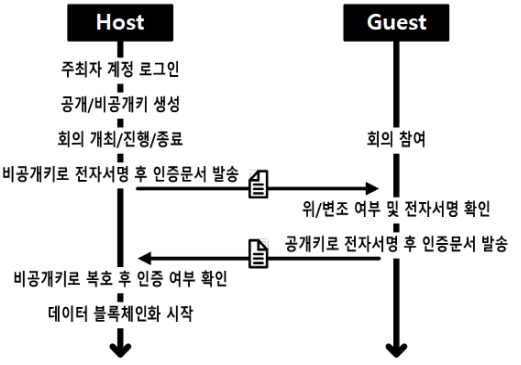
위 기존 연구와 같이 다양한 분야에서 사용자 데이터 보안을 위해 블록체인을 적용하는 노력이 진행되고 있다. 제안하는 회의 데이터 보안 방법에서는 저장되는 화상 회의 관련 정보의 보안성을 높이고자 하는 목적으로 블록체인 기술을 사용하여 회의 과정에서 발생하는 정보를 저장하고 관리한다. 허가형 블록체인과 스마트 계약을 통해 데이터의 허가되지 않은 접근을 제한하고 블록체인의 체인화와 분산화를 이용하여 데이터의 위·변조를 방지한다. 또한 블록체인 데이터를 블록체인 대표 서버에 위임하는 방식을 통해 사용자의 컴퓨팅 성능 비용을 최소화할 수 있다.

3. 블록체인 기반 화상 회의 데이터 저장 방법

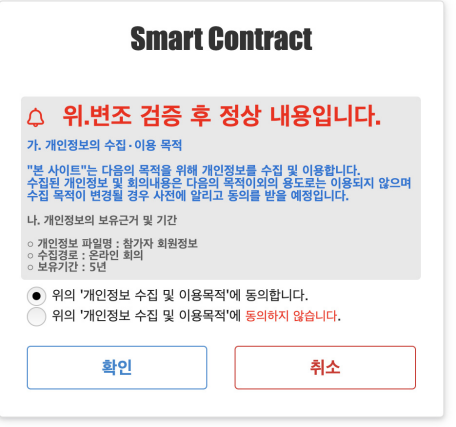
3.1 스마트 계약을 통한 인증

제안하는 방법에서는 화상 회의를 개최하기 위해서는 시스템으로부터 주최자 권한을 부여받아야 한다. 주최자는 회의 종료 후 스마트 계약을 통해 주최자와 참여자들 간에 위·변조 확인 및 저장 동의 인증 절차 그리고 회의 관련 정보를 블록 체인화 할 수 있는 권한을 갖는다.

스마트 계약을 이용한 인증 과정은 <그림 2>의 (a)와 같다. 일반적인 웹 기반 화상 회의 시스템에서는, 주최자가 지정된 또는 불특정 참여자들에게 접속 링크 또는 접속 아이디(ID)와 암호(PW)를 보내면 참여자들은 회원 가입이나 추가적인 프로그램 설치 없이 웹상에서 접속하여 참여한다. 이러한 과정은 하루에도 수없이 많이 이루어지고 참여자의 수도 매우 많을 것이다. 화상 회의 시스템의 입장에서, 매번 모든 참여자들의 개인 키를 생성하고 관리하는 일이 서버 운영에 매우 큰 부담이 될 것이다.



(a) 스마트 계약 과정



(b) 위·변조 확인과 정보 저장 동의 화면

그림 2. 스마트 계약을 통한 위·변조 확인과 동의 후 데이터 저장 과정

Figure 2. Data storage process after confirmation and consent of forgery and alteration through smart contracts

따라서, 제안하는 방법에서는 스마트 계약과 회의 관련 정보 암호화를 위해 공개키 암호 알고리즘[14]을 사용하여 주최자는 비공개키를, 참여자들은 공개키를 사용하도록 한다. 주최자는 고유의 계

정으로 시스템에 로그인 한 후 회의를 개최하기 전에 암호화된 인증문서를 주고받기 위해 공개키와 비공개키를 생성한다. 회의 종료 후 참여자들에게 비공개키와 참여자의 참여 정보를 혼합하여 서명한 인증 문서를 참여자들에게 발송한다. 참여자들은 그림 2의 (b)와 같이 인증문서에 포함된 위/변조 여부를 확인하고 데이터 저장 동의 과정을 거쳐 공개키로 암호화된 서명을 수행한다. 참여자들로부터 서명된 인증 문서는 주최자로 전송되고 주최자는 암호화 된 인증문서의 서명들을 비공개키로 복호화하여 확인한다. 최종적으로 주최자와 참여자들의 개인정보와 회의정보, 회의내용 데이터를 암호화하여 블록 체인화를 시작한다.

3.2 블록체인 데이터 생성

블록체인에 저장되는 회의 관련 정보는 크게 주최자와 참여자 정보, 회의 정보, 회의 내용으로 나눌 수 있다. <그림 3>은 블록을 구성하는 필요한 정보들을 그림으로 표현한 것으로 블록에는 개최된 회의 정보가 저장되며 주최자 정보와 함께 회의 참여자 중 스마트 계약에 동의한 참여자들의 정보가 포함된다.

각 블록에는 이전 블록과 현재 블록의 해시 값이 포함되며 현재 블록의 해시 값은 이전 블록의 해시 값과 사용자 정보 그리고 암호화된 회의 내용에 대한 해시 연산을 통해 결정된다. 회의 종료 후 스마트 계약을 통해 주고 받은 전자 서명 정보와 블록체인에서의 해당 블록의 순서번호가 블록 안에 구성된다.

블록체인은 주최자 별로 구성되어 관리되며 각 블록은 각 주최자가 회의를 개최할 때마다 생성되어 추가된다. 사용자가 회의 주최 권한을 부여받으면 해당 주최자의 정보만 포함하고 있는 제네시스(genesis) 블록이 생성된 상태로 초기 블록체인이 구성된다.

데이터 명	데이터 설명
roomname	개최된 회의 이름(주최자 계정으로만 생성 가능)
meetdata	회의 일자(시스템 정보)
partiemail	회의 참여자 이메일(로그인 정보)
partiname	회의 참여자 이름(로그인 정보)
partiphone	회의 참여자 전화번호(로그인 정보)
prehash	이전 블록의 해시값
curhash	현재 블록의 해시값(prehash와 현재 블록의 정보를 바탕으로 생성)
signature	위/변조 방지를 위한 전자 서명 정보
indexno	블록체인에서의 연결 순서
contents	회의 내용

그림 3. 블록체인의 각 블록에 포함되는 정보
Figure 3. Information included in each block of the blockchain

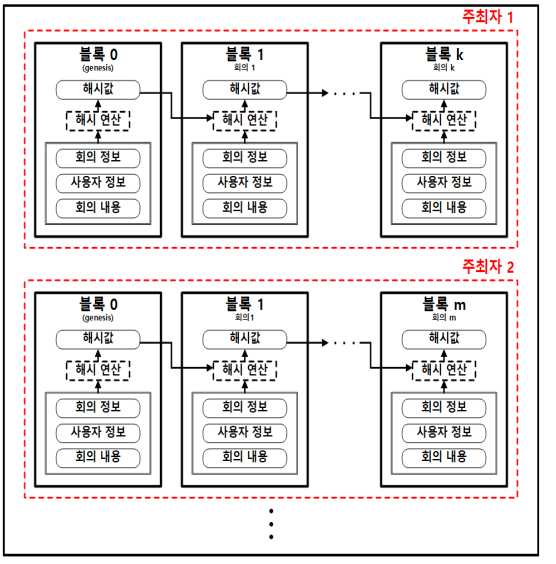


그림 4. 주최자 별 블록체인 데이터 구조
Figure 4. Blockchain data structure by organizer

<그림 4>는 회의 단위로 생성된 블록들이 주최자 별로 연결된 블록체인 구조를 나타낸다. 하나의 블록은 <그림 4>와 같이 구성되며 회의 정보, 사용자 정보, 회의 내용은 암호화되어 저장된다. 각 항목은 해당 회의에 참여한 수에 따라 다수의 정보를 포함할 수 있다. 블록은 이전 블록의 해시값과 해당 블록의 해시값을 포함하며 해시값은 해당

블록의 회의 관련 정보들과 이전 블록의 해시값에 대한 해시 연산 결과이다. 따라서 하나의 주최자에 대한 블록체인 데이터의 각 블록들은 해시 연산으로 연결되어 있으며 해시 연산 검증을 통해 데이터 위·변조에 대한 검증과 추적이 가능하다. 블록체인 데이터는 다른 블록체인 노드들에 동일한 형태로 저장되면 화상회의 시스템의 중재로 다른 블록체인 노드로 공유된다.

3.3 화상 회의 시스템과 블록체인 서버 구조

블록체인의 데이터 분산화 구조에서는 블록체인 네트워크에 참여하는 모든 노드들이 블록체인 데이터를 소유하여야 한다. 그러나 참여자 수에 따른 사용자 정보와 회의 과정에서 발생하는 정보의 양은 일반적인 컴퓨터에서 관리하기 어려울 수 있기 때문에 대표되는 블록체인 서버에 양도하여 저장한다. 제안하는 방법에서는 시스템에서 허용된 서버만이 블록체인 데이터를 저장하고 공유할 수 있는 허가형 블록체인 네트워크 구조이다. 회의 종료 후 생성된 블록체인 데이터는 대표 블록체인 서버에 저장되고 다른 블록체인 서버와 공유하여 상호 검증할 수 있다.

<그림 5>는 제안하는 블록체인 네트워크 구조를 나타내고 있다. 화상 회의 서비스를 이용하는 사용자 즉, 주최자와 참여자들의 회의 관련 정보는 주최자에 의해 블록 체인화 되고 연결된 대표 블록체인 서버에 저장한다. 블록체인 서버와 사용자는 기관 또는 지역에 따라서 그룹화 될 수 있다. 즉, 사용자의 소속 또는 거주 지역에 따라 대표되는 서버에 블록체인 데이터가 저장되고 각 블록체인 서버는 다른 관리자에 의해 운용된다. 화상 회의 시스템 제어부의 중재에 따라 다른 서버로 분산 공유되고 분산된 블록체인은 블록의 생성 주기 또는 일정한 시간 단위로 서버들 간의 검증에 의하여 보호된다. 시스템 제어부는 블록 및 블록체인 생성에 중재 역할만 수행하고 블록체인 데이터를 소유하거나 접근할 수 있는 권한이 없다. 따라서 제어부에 의한 블록체인 생성 및 변경에 대한 부정을 방지할 수 있다.

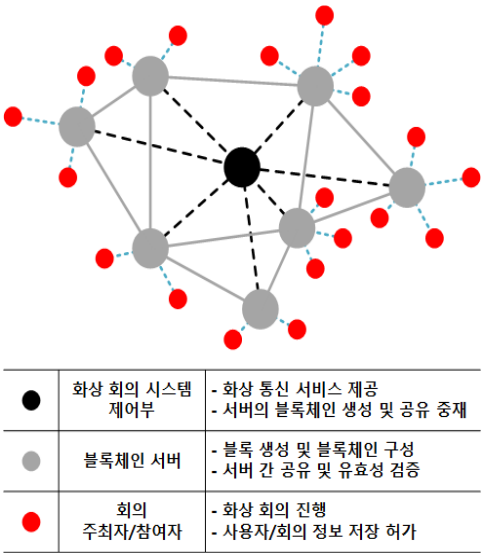


그림 5. 제안하는 블록체인 네트워크 구조
Figure 5. The proposed blockchain network structure

4. 보안성 및 실용성 분석

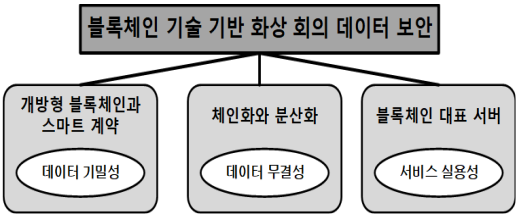


그림 6. 제안하는 데이터 보안 방법의 특징과 장점
Figure 6. Features and advantages of the proposed data security method

제안하는 블록체인 기술 기반 화상 회의 시스템에서는 <그림 6>과 같이 허가형 블록체인 구조와 스마트 계약을 통해 데이터의 기밀성을 유지한다. 블록체인의 체인화와 분산화를 통해 데이터의 무결성을 유지하고 사용자가 블록체인 데이터를 소

유하는 대신 블록체인 서버에 위임하는 방식을 통해 구현과 운용 실용성을 높인다.

4.1 데이터 기밀성

블록체인에 포함되는 데이터는 민감 데이터이기 때문에 제한된 접근과 이에 대한 인증 과정이 필요하다. 제안하는 방법에서는 공개키 암호기술인 타원곡선 알고리즘 기반 스마트 계약을 통해 데이터 저장 동의 과정을 거친다. 즉, 스마트 계약에 동의한 사용자만이 블록 생성에 참여할 수 있다. 이후 블록체인 데이터에 저장된 회의 내용에 접근할 경우에도 비공개키를 가지고 있는 주최자만이 가능하다. 참여자가 회의 내용을 열람하기 위해서는 주최자를 통해서만 가능하며 주최자는 해당 블록의 참여자 정보와 전자 서명 정보를 확인하여 정보 제공 여부를 결정할 수 있다. 정리하면 허가되지 않은 사용자의 블록 생성 및 블록체인 데이터의 접근을 제한하여 기밀성을 유지한다.

사용자들이 생성한 블록 그리고 블록체인 데이터를 위임하는 블록체인 서버 또한 화상 회의 시스템의 허용에 의해서만 블록체인 네트워크에 참여할 수 있다. 그 대상은 기관 또는 지역을 대표하는 서버가 될 수 있으며 인증된 서버만이 블록체인 데이터를 저장하고 관리할 수 있다. 결과적으로 스마트 계약과 허가형 블록체인 구조를 통해 허가된 사용자와 서버만이 블록체인 데이터의 생성과 관리에 관여할 수 있다.

4.2 데이터 무결성

블록체인 데이터는 회의 단위로 구성되며 각 블록은 하나의 회의에 대한 사용자 정보와 회의 내용을 포함한다. 각 사용자의 정보와 회의 내용은 해시 연산으로 연결되어 있기 때문에 사용자 정보, 회의 정보, 회의 내용 또는 해시값 자체를 검증할 수 있으며, 따라서, 사고 또는 부정에 의한 손실 또는 위·변조에 대한 감지 및 추적이 가능하다.

생성된 블록체인 데이터는 대표되는 블록체인 서버에 저장되고 다른 블록체인 서버로 공유된다. 그리고 각 블록체인 서버는 각기 다른 관리자에 의해 관리된다. 블록체인 데이터에 대한 사고 또는 고의에 의한 부정이 발생할 경우 블록체인 네트워크에 참여하는 서버들 간의 비교 및 검증을 통해 블록체인 데이터에 대한 부정 여부 확인과 복구가 가능하다. 블록체인 네트워크에 참여하는 서버의 수가 많아질수록 동시의 데이터 접근과 조작이 어려워지기 때문에 부정에 의한 데이터 손실 또는 위·변조가 사실상 불가능해진다. 정리하면 각 블록체인 데이터는 해시 연산으로 체인화된 블록들 간의, 그리고 여러 서버로 분산된 블록체인 데이터 간의 검증을 통해 무결성을 유지할 수 있다.

4.3 서비스 실용성

참여자 정보와 회의 내용에 대한 데이터의 크기는 회의 진행 시간에 따라서, 그리고 참여한 사용자의 수에 따라서 방대해질 수 있다. 또한 주최자 권한을 가진 사용자가 증가하고 각 주최자에 의한 회의가 반복될수록 블록체인 데이터가 누적되기 때문에 블록체인 데이터의 저장과 관리를 위해 요구되는 저장장치의 성능이 높아질 수밖에 없다. 일반 사용자들 모두가 이와 같은 데이터를 관리하기에는 현실적으로 불가능하기 때문에 제안하는 방법에서는 대표되는 서버들을 두어 사용자를 대신하여 블록체인 데이터를 저장하고 관리한다. 따라서 사용자는 데이터 저장과 관리에 필요한 저장공간에 관련된 컴퓨터 성능을 부담하지 않을 수 있다.

블록체인 네트워크에서는 다수의 사용자에 의한 블록 생성의 유효성 검증과 경쟁 중재, 그리고 효율적인 공유를 위해 합의 알고리즘이 필요하다[15]. 기존의 비트코인과 이더리움 같은 가상 화폐를 다루는 네트워크에서는 작업증명, 지분증명 등의 고

도의 컴퓨팅 성능과 시간을 필요로 하는 합의 알고리즘이 적용되었다. 그러나 누구나 참여할 수 있는 공개형 블록체인 네트워크와는 달리 시스템으로부터 허용된, 그리고 비교적 소수의 블록체인 서버들이 블록체인 네트워크에 참여하는 허가형 블록체인 구조이기 때문에 블록 생성을 위한 경쟁은 불필요하므로 기존의 복잡한 합의 알고리즘을 적용하는 것은 비효율적이다. 제안하는 방법에서는 화상 회의 시스템 제어부의 중재 아래 경량화된 합의 알고리즘을 적용할 수 있다. 정리하면 데이터를 위임하는 블록체인 서버 운용과 비교적 소수의 서버가 참여하는 허가형 블록체인 네트워크 구조를 통해 사용자의 블록체인 데이터 관리에 필요한 컴퓨팅 성능 부하를 최소화할 수 있다.

5. 결 론

본 논문에서는 블록체인 기술을 이용하여 화상 회의 데이터를 보안하는 방법과 구현 예를 제안하였다. 블록체인의 데이터 체인화와 분산화를 통한 데이터의 무결성과 비공개 블록체인 네트워크 구조와 스마트 계약을 통한 기밀성을 높일 수 있다. 또한, 대표하는 블록체인 서버들에게 데이터를 위임하는 구조로써 사용자가 부담하는 컴퓨팅 부하를 줄여 실용성을 높였다. 제안하는 방법은 기존의 보안 기술의 한계와 중앙 관리형 시스템에서의 관리자에 의한 부정에 대한 우려에 대한 해결책이 될 수 있다. 현재 구현된 시스템에서는 소수의 블록체인 서버를 두어 블록체인 데이터를 공유하고 검증하는 구조이지만 기관별 또는 지역별 협의를 통해 다수의 블록체인 서버를 탄력적으로 운용하는 구조가 가능하며 보안성과 실용성 면에서 가치가 있을 것으로 기대한다. 향후 연구는 블록체인을 활용한 원격진료 서비스를 진행하고 민감한 환자 정보 보호에 대한 연구를 수행하고자 한다.

References

[1] M. G. Jeon, H. W. Byeon, H. G. Lee, and H. S. Na, *Applications of blockchain in business,* Journal of Knowledge Information Technology and Systems, Vol. 16, No. 2, pp. 297-311, 2021.

[2] S. Aldossary, and W. Allen, *Data security, privacy, availability and integrity in cloud computing: issues and current solutions*, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[3] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, *A survey on the security of blockchain systems*, Future Generation Computer Systems, 2017.

[4] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, *Untangling blockchain: A data processing view of blockchain systems,* IEEE Trans. Knowledge Data Engineering, Vol. 30, pp. 1366-1385, 2018.

[5] D. Y. Lee, J. W. Park, J. H. Lee, S. R. Lee, and S. Y. Park, *Blockchain core technology and domestic and foreign trends*, Communications of the Korean Institute of Information Scientists and Engineers, Vol. 35, No. 6, pp. 22-28, 2017.

[6] R. Böhme, N. Christin, B. Edelman, and T. Moore, *Bitcoin: economics, technology, governance* Journal of Economic Perspectives, Vol. 29, No. 2, pp. 213-38, 2015.

[7] C. Y. Hwang, M. G. Jeon, Y. J. Kim, and H. S. Na, *Comparative study on blockchain platforms,* Journal of Knowledge Information Technology and Systems, Vol. 16, No. 2, pp. 241-253, 2021.

[8] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F-Y. Wang, *An overview of smart contract: Architecture applications and future trends*,

Proc. IEEE Intelligent Vehicles Symposium (IV), pp. 108-113, 2018.

[9] R. Yang, R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, X. Yang, G, Amarasinghe, and S. Chen, *Public and private blockchain in construction business process and information integration*, Automation in Construction, Vol. 118, 2020.

[10] S. Pahlajani, A. Kshirsagar, and V. Pachghare, *Survey on private blockchain consensus algorithms*, Proc. 1st Conference on Innovations in Information and Communication Technology, pp. 1-6, 2019.

[11] D. H. Lee, S. C. Kim, and N. J. Park, T*he blockchain-based online learning platform for the untact education environment in the post-COVID-19 era*, The Journal of Korean Institute of Information Technology, Vol. 18, No. 11, pp. 109-121, 2020.

[12] Y. B. Cho, J. B. Seo, and S. H. Woo, *Research on tele-medicine system using blockchain*, Korea Institute of Information and Communication Engineering, Vol. 24, No. 2, pp. 209-212, 2020.

[13] S. H. Yun, *The smart contract based conference key distribution scheme*, Journal of The Korea Internet of Things Society, Vol. 6, No. 4, pp. 1-6, 2020.

[14] J. Lopez, and R. Dahab, *An overview of elliptic curve cryptography*, Technical report, Institute of Computing, State University of Campinas, Brazil, 2000.

[15] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, *A review on consensus algorithm of blockchain*, Proc. IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 2567-2572, 2017.

화상 회의 시스템의 데이터 보안을 위한 블록체인 기술 적용 연구

강태근[1], 김도경[1], 한재훈[2], 조지훈[2], 이현빈[3]

[1]*국립한밭대학교 컴퓨터공학과 연구원*

[2]*국립한밭대학교 컴퓨터공학과 석사과정*

[3]*국립한밭대학교 컴퓨터공학과 교수*

요 약

COVID-19 인하여 사회생활이 급변하여 비대면 수업, 화상 회의 서비스가 다양한 분야에서 일상화되고 있다. 회의 진행 중 발생하는 정보는 경우에 따라서는 저장 및 보안 될 필요가 있다. 데이터 저장 및 관리 시스템의 보안성 강화를 위하여 블록체인 기술이 많이 활용되고 있다. 특히, 데이터 위·변조를 방지하기 위한 방법으로써 다양한 분야와 응용 시스템에 블록체인 적용에 관한 연구가 활발하다. 본 연구에서는 블록체인 기술을 이용한 화상 회의 데이터 보안 방법을 제안한다. 회상 회의 시스템 상에서 스마트 계약을 통한 인증, 블록체인 데이터 생성 방법, 블록체인 서버 연결 구조와 구현 예시를 제시하고 대표 블록체인 서버를 중심으로 한 블록체인 네트워크 구조의 데이터 기밀성, 데이터 무결성, 서비스 실용성에 대해서 기술한다. Private 블록체인을 기반으로 회의 참여자의 전자 서명으로 정보 저장의 동의를 구하고, 저장된 정보를 블록화한다. 제안하는 시스템에서는 허가형 블록체인 구조와 스마트 계약을 통해 데이터의 기밀성을 유지한다. 블록체인의 체인화와 분산화를 통해 데이터의 무결성을 유지하고 사용자가 블록체인 데이터를 소유하는 대신 블록체인 서버에 위임하는 방식을 통해 구현과 운용 실용성을 높일 수 있다. 뿐만 아니라 중앙 관리형 시스템에서의 서버 관리자에 의한 부정을 방지하는 해결책이 될 수 있다.

감사의 글

이 논문은 2020학년도 한밭대학교 교내학술연구비의 지원을 받았음.

Taegeun Kang received the B.S., M.S., and Ph.D. degrees in the Department of Computer Engineering from Hanbat National University, Daejeon, Korea, in 2013, 2015, and 2020, respectively. He is currently a Researcher at Hanbat National University. His research interests include Database Structure and Blockchain.
E-mail address: taegnism@naver.com

Dogyung Kim received the M.S. and Ph.D. degrees in the Department of Computer Engineering from Hanbat National University, Daejeon, Korea, in 2013 and 2020, respectively. He is currently working as a researcher at Hanbat National University. The field of interest is WebRTC and Blockchain.
E-mail address: dgkim1007@naver.com

Jaeheun Han received the B.S. in the Department of Computer Engineering from Hanbat National University, Daejeon, Korea, in 2020. He is currently M.S student in Hanbat National University. He is interested in Blockchain and Internet privacy.
E-mail address: dev@o365.hanbat.ac.kr

JiHoon Jo received the B.S. in the Department of Computer Engineering from Hanbat National University, Daejeon, Korea, in 2021. He is currently M.S student in Hanbat National University. His research interests are NFT and WebRTC.
E-mail address: cjh010203@naver.com

Hyunbean Yi received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Hanyang University, Korea, in 2001, 2003, and 2007, respectively. He had been a Researcher at University of Massachusetts (UMass), USA from 2007 to 2009 and at Nara Institute of Science and Technology (NAIST), Japan from 2009 to 2011. He is currently a professor in the Department of Computer Engineering at Hanbat National University. He is interested in Blockchain and video conference system.
E-mail address: bean@hanbat.ac.kr

KOREA KNOWLEDGE INFORMATION TECHNOLOGY SOCIETY

논문게재증명서

논 문 제 목 : 화상 회의 시스템의 데이터 보안을 위한 블록체인 기술 적용 연구

저자 및 소속 : 강태근, 김도경, 한재흔, 조지훈, 이현빈(한발대학교)

상기 논문은 분야별 전문가의 엄격한 심사과정을 거쳐 본 학회 편집위원회에서 게재하기로 최종 결정하였으며, 한국지식정보기술학회 논문지 2022년 4월호(제17권 제2호, 4월 30일 발행)에 게재된 논문임을 증명합니다.

2022年 5月 6日

KKITS 韓國知識情報技術學會
논문편집위원장 전병찬

※ 위 증명서는 온라인으로 발급된 것입니다.

한국지식정보기술학회 논문지

관심저널 알림

자료유형	학술저널	발행주기	없음
발행기관명	한국지식정보기술학회	저널 발행기간	2009 ~ 2021
주제분류	복합학 > 학제간연구	ISSN	
등재정보	KCI등재		

권호수 72 논문수 1,050 이용수 11,112 피인용수 84

이 저널에서 논문 검색

검색어 입력

동일 발행기관의 다른 저널

권호 리스트

조회하기

많이 이용된 Top10 논문 | 최근 발간된 논문

이 저널에서 가장 많이 이용된 논문 10편을 둘러보세요.

최근1년

1 코로나 팬더믹 사태(COVID-19)에서 원격의료 활성화 방안에 관한 연구
이종식 이용수 118

2 스마트폰 과의존 실태 분석
오송석, 정현용 이용수 74

3 선형회귀분석 기법을 이용한 고교야구투수의 투구속도 예측
오영환 이용수 68

4 기업의 빅데이터 활용성 연구
김광현, 김유중 이용수 66

5 조류 울음소리를 이용한 조류 분류 딥러닝 시스템 개발
강민정, 김영선, 신화영 외 1명 이용수 53

6 소비자행동분석을 통한 마케팅전략과 전자상거래의 문제점 및 해결방안
김광현, 임근우 이용수 47

7 노인 만성질환자의 건강관리를 위한 원격의료모니터링의 효용성 연구
이종식 이용수 46

8 코로나 팬더믹(COVID-19)에서 비대면 수업의 사용자 경험에 관한 연구
이종식 이용수 33

9 반려동물형 로봇을 이용한 고령자 심리 안정의 향상 방안
이종식, 이강년 이용수 33

10 E-commerce의 시장 지배 전략에 대한 연구
김광현, 강승희 이용수 31

논문이 많이 이용된 Top9 저자

논문을 많이 발행한Top9저자

이 저널에서 가장 많이 이용된 저자 9명을 확인하세요.

최근1년

1 김광현
한국교통대학교
저널 내 논문 이용 수 426
저자 논문 누적 이용 수 0

2 이종식
안양대학교
저널 내 논문 이용 수 360
저자 논문 누적 이용 수 0

3 박장우
-
저널 내 논문 이용 수 197
저자 논문 누적 이용 수 0

4 오영환
나사렛대학교
저널 내 논문 이용 수 183
저자 논문 누적 이용 수 0

5 김유중
한국지식정보기술학회
저널 내 논문 이용 수 175
저자 논문 누적 이용 수 0

6 김철진
인하공업전문대학
저널 내 논문 이용 수 127
저자 논문 누적 이용 수 0

7 오송석
대전보건대학교
저널 내 논문 이용 수 116
저자 논문 누적 이용 수 0

8 정현용
대전대학교
저널 내 논문 이용 수 116
저자 논문 누적 이용 수 47

9 서상혁
한국지식정보기술학회
저널 내 논문 이용 수 102
저자 논문 누적 이용 수 0

논문을 많이 이용한 기관

저널 인용정보

이 저널을 가장 많이 이용한 기관 20개입니다.

최근1년

NO.	이용기관명	이용수
1	경희대학교	54
2	서울대학교	50
3	동국대학교	42

4	한국방송통신대학교	42
5	이화여자대학교	39
6	가천대학교	38
7	공주대학교	35
8	인하대학교	34
9	국민대학교	34
10	고려대학교	33
11	한국외국어대학교	33
12	서울여자대학교	33
13	연세대학교	32
14	홍익대학교	32
15	한양대학교	29
16	단국대학교 죽전캠퍼스	29
17	숭실대학교	27
18	성신여자대학교	25
19	경상국립대학교	25
20	경북대학교	24