Journal of Convergence for Information Technology
Vol. 9. No. 11, pp. 15-21, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.11.015

# 인터넷 허위통신 신고의 증거물 보존을 위한 프라이빗 블록체인 시스템 제안

배석민[1], 양성열[2], 정재진[3*]
[1,2]단국대학교 일반대학원 미래ICT융합학과 학생, [3]단국대학교 일반대학원 응용컴퓨터공학과 교수

# A Proposed Private Blockchain System for Preserving Evidence of False Internet Communications

Suk-Min Bae[1], Seong-Ryul Yang[2], Jai-Jin Jung[3*]
[1,2]Student, Dept. of Future ICT Convergence Engineering, Graduate School, Dankook University
[3]Professor, Dept. of Applied Computer Engineering, Dankook University

**요 약** 프라이빗 블록체인 기술은 허가된 사용자만이 원장에 기록하거나 조회할 수 있어 기관이나 기업에서 주목을 받고 있으며, 분산원장기술에 기초하고 있어 저장된 트랜잭션은 위변조 할 수 없는 시스템이다. 인터넷을 통한 뉴스는 손쉽게 변경이 가능하므로 그만큼 조작의 가능성도 높아졌다. 이러한 폐해를 방지하기 위해 허위통신 신고 제도를 운영한다. 하지만, 허위통신 신고와 검증시점 사이에 웹사이트의 콘텐츠가 변경되거나, 조작된 증거물로 허위 신고를 할 수 있다. 본 논문에서는 증거물을 일반 파일 서버에서 저장하여 위변조 방지에 취약한 문제가 있다. 보다 정확한 허위통신 관리를 위한 헤드리스 브라우저를 이용한 증거물 수집과 프라이빗 블록체인을 통한 증거물을 안전하게 보존하고 훼손될 가능성을 차단하는 시스템을 제안한다. 제안기법은 원본 HTML을 다운로드 받고 웹사이트를 이미지로 캡처한 후 신고내용과 함께 트랜잭션에 담아 프라이빗 블록체인에 저장하여 증거물의 획득부터 보존까지 무결성을 보장한다.

**주제어 :** 블록체인 시스템, 허위통신, 신고, 증거물, 프라이빗 블록체인

**Abstract** Allowing only authorized users to record and inquire in the ledger, private blockchain technology is attracting attention from institutions and companies. Based on distributed ledger technology, records are immutable. Because news via the Internet can be easily modified, the possibility of manipulation is high. Some false communication report systems are designed to prevent such harm. However, during the gap between the false communication report and verification time, contents on the website can be modified, or false evidence can be submitted intentionally. We propose a system that collects evidence using a headless browser for more accurate false communication management, and securely preserves evidence through a private blockchain and prevents possibilities of manipulation. The proposed system downloads original HTML, captures the website as an image, stores it in a transaction along with the report, and stores it in a private blockchain to ensure the integrity from acquisition to preservation of evidence.

**Key Words :** Blockchain system, False communication, Report, Evidence, Private blockchain

*Corresponding Author : Jai-Jin Jung(dothan@dankook.ac.kr)
Received October 7, 2019
Revised October 28, 2019
Accepted November 20, 2019
Published November 28, 2019

## 1. 서론

인터넷의 발달로 인해 다양한 미디어가 인터넷에서 제공되고 있다. 뉴스는 미디어의 본령이라고 할 수 있다. 뉴스의 공익적인 측면을 생각한다면 의도적이지 않은 오보도 있지만, 정확하지 않거나 의도적으로 조작된 뉴스가 끼치는 사회적 해악은 매우 심각하다. 과거 신문, TV 방송과는 달리 인터넷을 통한 뉴스는 웹사이트 운영자가 매우 용이한 변경이 가능하므로 그만큼 조작의 가능성도 높아졌다. 이러한 폐해를 방지하기 위해 공공기관에서는 허위통신 신고 센터도 운영 중이다.

하지만, 허위통신 신고와 검증시점까지의 시간 사이에 해당 웹사이트의 콘텐츠가 변경되어 있거나, 신고자가 조작된 증거물로 허위 신고를 할 수 있으며, 증거물을 일반 파일 서버에서 저장하여 위변조 방지에 대책이 없는 문제가 있다.

블록체인은 기본적으로 거래정보가 중앙시스템이 아닌 분산장부에 기록, 보관된다[1]. 블록체인 기술은 사이버 상에 있는 모든 참여자가 공동으로 거래정보를 검증, 기록, 보관할 수 있는 일종의 분산원장 기술로서 투명성(Transparent)과 보안성(Secure), 신속성(Instantaneous), 탈중개성(P2P- based) 등의 장점을 갖추고 있다. 분산된 거래장부 기술에 기반을 둔 블록체인 기술은 시스템의 유지비용이 적게 들 뿐만 아니라 해킹에 대한 위험성이 낮다는 장점이 있으며, 해커가 수많은 네트워크 참여자의 모든 블록체인을 동시에 해킹하는 것이 사실상 어렵기 때문에 이에 대한 위변조가 불가능하다는 특징이 있다[2]. 프라이빗 블록체인은 블록체인과 마찬가지로 분산원장 기술에 기반을 하고 있지만 시스템을 운영하는 주최가 있어 권한을 받은 사용자만이 원장에 읽고 쓰기가 가능하다.

본 논문에서는 보다 정확한 허위통신 신고를 위한 서버 사이드 헤드리스 브라우저를 이용하여 정확한 증거물 수집과 프라이빗 블록체인을 이용하여 증거물을 안전하게 보존하여 훼손될 가능성을 차단하는 시스템을 제안한다.

본 논문은 아래와 같이 구성된다. 2장에서는 관련연구로 블록체인, 프라이빗 블록체인, 헤드리스 브라우저와 타임스탬프에 대해 기술하고 선행연구를 알아본다. 3장에서는 현재 운영되고 있는 허위통신 신고 시스템의 문제점을 알아본 후 프라이빗 블록체인을 이용한 본 논문의 제안 기법을 소개한다. 4장에서는 제안기법과 선행연구의 비교분석 및 평가를 하고 5장에서 결론을 기술한다.

## 2. 관련연구

### 2.1 블록체인

블록체인은 여러 레코드를 블록 단위로 묶어서 각 블럭의 해시값을 다음 블록에 넣는 방식으로 사고 혹은 임의적 기록 변경의 가능성을 차단하는 기술이다. 이를 통해 블록체인을 원장처럼 사용할 수 있으며, 권한을 확보한 사용자는 새로운 기록을 공유하고 입증 할 수 있다. 원장의 정확성을 입증하는 방법에는 합의방식이 따라 블록체인의 세부 기술들을 분류할 수 있다. 이 입증된 블록들은 블록체인 네트워크의 서버에 동일하게 분산되어 기록이 되기 때문에 일부 서버가 정상적으로 작동하지 않거나 해킹을 당하는 경우에도 다수의 서버에 분산 기록된 원장들에 의해 원본 훼손을 방지할 수 있다. 채굴이라는 용어는 암호화폐 Bitcoin에서 이 사용되기 시작하였다[3-5].

블록체인 기술의 참신한 점은 단순한 데이터베이스가 아니라 트랜잭션 자체에 연결된 트랜잭션 또는 비즈니스 로직에 대한 규칙을 설정할 수 있다는 것이다. 이는 전체 데이터베이스 수준이나 응용 프로그램에서 규칙이 설정되지만 트랜잭션 단위에서는 설정되지 않는 기존 데이터베이스와 대조된다. 이 규칙은 개인 혹은 기업 간의 거래 규칙으로도 사용될 수 있는데 이를 스마트 컨트랙트라고 부른다.

### 2.2 프라이빗 블록체인

프라이빗 블록체인은 허가형 블록체인(Permissioned Blockchain)이라고도 한다. 상대되는 개념의 퍼블릭 블록체인은 허가없이 누구나 자유롭게 원장에 작성, 조회가 가능하지만 프라이빗 블록체인에서는 사전에 허가된 사용자나 조직만 원장을 작성하거나 조회할 수 있다.

Table 1은 프라이빗 블록체인과 퍼블릭 블록체인을 비교 정리한 표이다.

프라이빗 블록체인 네트워크에는 초대가 필요하며 네트워크 스타터 또는 네트워크 스타터가 설정한 규칙 세트에 의해 검증되어야 한다. 프라이빗 블록체인을 설정 한 관리자는 일반적으로 허가된 네트워크를 설정한다. 이로 인해 누가 네트워크에 참여할 수 있고 특정 거래에만 참여할 수 있는 사람이 제한된다. 참가자는

초대를 받거나 참여 허가를 받아야 한다. 접근 제어 장치 다양 할 수 있으며, 기존 참가자는 향후 참가자를 결정할 수 있다. 규제 당국은 참여 라이센스를 발급 할 수 있으며, 컨소시엄이 대신 결정을 내릴 수 있습니다. 참여자가 네트워크에 가입하면 분산 방식으로 블록체인을 유지 관리하는 역할을 한다[6-8].

**Table 1. Comparison of Private Blockchains and Public Blockchains**

| Features | Private Blockchain | Public Blockchain |
|---|---|---|
| Access | Permissioned read & write access to database | Open read & write access to database |
| Speed | Faster | Slower |
| Security | Pre-approved participants | Proof of Work |
| Identity | Known identities | Anonymous |
| Asset | Any asset | Native assets |
| Cost | The Operator covers | Shared by all Participants |
| Example | Hyperledger Fabric, R3 Corda | Bitcoin, Ethereum |

### 2.3 헤드리스 브라우저

헤드리스 브라우저(Headless browser)는 그래픽 사용자 인터페이스가 없는 웹 브라우저이다. 명령 줄 인터페이스로 웹 페이지에 접속하지만 사용자에게는 웹 페이지의 내용을 표시하지 않는 브라우저이다.

일반 웹브라우저와 달리 주로 서버에서 사용되며, 웹 페이지의 내용을 타 프로그램에 제공하거나, 웹페이지의 자동화 테스트를 하는데 이용된다. 최근 들어 웹페이지 내의 데이터 수집이나 캡처를 하는데 사용되고 있다.

가장 많이 쓰이는 헤드리스 브라우저로는 구글에서 제공하는 헤드리스 크롬과 javascript 기반으로 만들어진 PhamtomJS 등이 있다.

### 2.4 타임스탬프

타임스탬프는 컴퓨터에 의해 기록된 로그 또는 메타데이터로 저장되는 이벤트와 관련된 시간 정보이다. 사용자의 요구 또는 타임스탬프를 생성하는 프로세스의 기능에 따라 모든 이벤트에 타임스탬프가 기록 될 수 있다. 타임 스탬프는 대부분의 컴퓨터 관련 프로세스, 특히 동기화 목적에 필수적인 기능이다. 예를 들어, 날짜 수정 타임스탬프에서 참조한대로 변경되었는지 여부를 확인하여 백업 중인 파일과 현재 파일의 차이를 알 수 있으려면 백업이 필요한 파일의 타임스탬프가 필수적이다. 운영체제에서 자동으로 기록되는 타임스탬프의 일반적인 이벤트는 파일 생성 및 파일 수정이며 파일 속성을 확인하여 확인할 수 있다. 서버가 생성하거나 프로그램을 디버깅 할 때 생성된 디버그 로그에서 발생하는 각 이벤트는 타임스탬프와 함께 기록되므로 관리자나 디버거는 발생한 상황과 시기를 즉시 알 수 있다. 타임스탬프는 여러 프로세스의 동기화에 필수적이다. 발신 측에서 보내는 모든 패킷은 타임스탬프가 필수적으로 포함되어 있어야 수신 측에서 데이터를 모두 정리하기 전에 데이터를 구성하는 방법을 알 수 있다. 이것은 일부 미디어 스트리밍 프로토콜에서도 동일하게 이루어진다[9].

사토시 나카모토라는 익명의 개인 또는 단체가 작성한 'Bitcoin: A peer-to-peer electronic cash system.' 논문에서 블록체인이라는 용어를 사용하지 않고 그에 해당되는 개념을 타임스탬프 서버(Timestamp Server)로 설명했다[10,11].

### 2.5 선행연구

Aravind Ramachandran(2017)은 논문[12]에서 안전한 데이터 출처 관리를 위해 블록체인 및 스마트 계약을 사용하는 연구를 아래와 같이 진행하였다.

중요한 과학 연구에서 연구 목표와 일치하도록 데이터 제작, 결과보고 부족 및 결과 위조와 같은 데이터 사기를 피하려면 데이터의 출처를 유지해야 한다. 데이터 출처는 다양한 출처의 과학 데이터를 통합하고 출처를 확인할 수 있게 한다. 또한 실험 결과가 연구의 실제 목표를 얼마나 지원하는지 측정하고 투명성과 신뢰성을 높이는 척도 역할을 한다. 출처 시스템의 주요 과제는 출처 데이터의 수집 및 변경 불가능한 저장소, 검증 가능성 및 수집된 출처 데이터의 개인 정보 보호이다. 데이터 출처 추적은 중요하지만 수집된 출처 데이터의 보안 및 개인 정보를 유지하는 것도 중요하다. 모든 형태의 데이터 출처 관리 시스템은 데이터가 무단으로 액세스 되지 않도록 보호해야 한다. 기존의 많은 출처 시스템은 중앙 집중식 저장소 모델을 기반으로 한다. 중앙 집중식 시스템 아키텍처의 단점은 중앙 서버가 손상되면 전체 데이터 출처 추적이 손상 될 수 있다. 또한, 현재 출처 시스템은 변경 사항을 저장하기 전에 유효성을 검사하지 않는다. 이 연구에서 제안한 시스템은 블록체인을 출처 정보를 저장하는 매체로 사용하고 스마트 계

약을 사용하여 변경 사항을 기록하기 전에 각 변경 사항에 대한 유효성 검사를 제공하여 이러한 문제를 해결한다. 변경 불가능한 블록체인의 특성인 인해 승인된 출처 변경 사항을 저장한 사용자는 임의로 수정할 수 없다. 또한, 블록체인의 분산 특성으로 인해 데이터 출처 추적이 블록체인의 모든 노드에 복제되어 높은 가용성과 내결함성을 보장한다[12].

## 3. 시스템 운영사례 및 제안기법

### 3.1 시스템 운영사례

Table 2. Submission Items of false communication reporting system

| | Website A[13] | Website B[14] |
|---|---|---|
| reported items | Type,<br>Name,<br>E-mail address,<br>URL,<br>reason for reporting,<br>File Attachment | Channel,<br>Type,<br>Name,<br>Phone number,<br>E-mail address,<br>URL,<br>reason for reporting,<br>File Attachment |

Table 2는 현재 국내에서 운영 중인 허위통신 신고 시스템의 신고 수집 항목이다. 해당 시스템은 전기통신기본법에 의거하여 허위 콘텐츠 증거물을 수집하는데 목적이 있다. 하지만, 위 두 시스템은 허위통신을 신고하는데 있어 다음과 같은 문제점을 갖는다.

첫 번째, URL로 신고할 경우 인터넷 상의 정보는 해당 웹사이트 운영자가 수정할 수 있는 권한이 있기 때문에 URL로 신고할 경우 신고한 시각의 정보 내용과 신고 내용을 확인하는 시각의 정보 내용이 상이 할 수 있다.

두 번째, 캡처한 이미지로 신고할 경우 신고자는 웹사이트의 내용을 웹브라우저의 개발자 도구로 편집하여 수정하거나 캡처 이후 그래픽 툴로 수정할 수 있다.

세 번째, 증거물을 일반적인 파일 서버에 저장할 경우 서버에 접근 권한이 있는 관리자는 언제든지 증거물을 임의적으로 수정할 수 있다.

### 3.2 제안기법

서버 사이드 헤드리스 브라우저로 원본 HTML을 다운로드 받고 웹사이트를 캡처한 후 프라이빗 블록체인에 저장함으로써 신고한 증거물을 위변조 할 수 없는 프라이빗 블록체인 시스템을 제안한다.

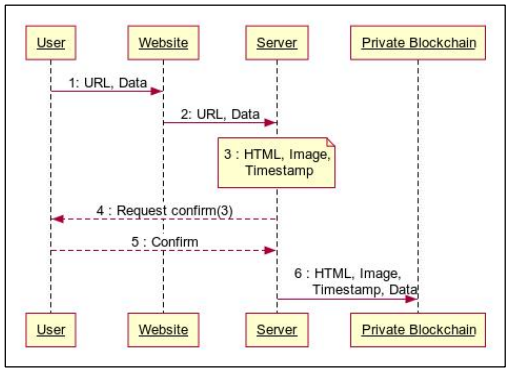


Fig. 1. Private Blockchain System for Preserving Evidence of False Internet Communications

Fig. 1은 본 논문에서 제안하는 시스템에서 사용자가 시스템에 허위통신을 신고하는 프로세스 시퀀스 다이어그램이다.

단계 1 : 사용자는 허위통신 신고 시스템에 접속하여 신고할 웹사이트의 URL과 함께 이름, 전화번호, 이메일, 신고할 내용을 작성한다.

단계 2, 3 : 서버는 URL을 받아 헤드리스 브라우저를 가동하여 원본 HTML을 다운로드 받고 웹사이트의 이미지를 캡처한 후 타임스탬프와 함께 저장한다.

단계 4 : 단계 3에서 캡처한 이미지를 사용자에게 출력한 후 신고할 웹사이트가 맞는지 확인을 받는다.

단계 5, 6 : 사용자의 허가가 완료되면, 서버는 원본 HTML, 캡처한 이미지, 타임스탬프와 사용자가 입력한 정보를 프라이빗 블록체인에 저장한다.

```
'use strict';
const{Contract}= require('fabric-contract-api');
class Evidence extends Contract {
    async createEvidence(ctx, evidenceID,
userName, userPhone, userEmail, reason, userIP,
tiemstamp, URL, captureImage, originHTML) {
        const evidenceData = {
            userName,
            userPhone,
            userEmail,
            reason,
            userIP,
            tiemstamp,
            URL,
            captureImage,
            originHTML
        };
        await ctx.stub.putState(evidenceID,
Buffer.from(JSON.stringify(evidenceData)));
    }
}
module.exports = Evidence;
```

Fig. 2. Smart contract - Invoke

Fig. 2는 Fig. 1의 단계 6에서 사용하는 Invoke 스마트 컨트랙트 소스코드이다. 하이퍼래저 패브릭의 node.js 체인코드로 작성하였으며, 증거물 ID와 데이터를 입력받아 프라이빗 블록체인에 저장한다.

```
// Transaction Data
{"userName" : "Hong Kil Dong",
"userPhone" : "010-1234-5678",
"userEmail" : "user@mail.com",
"reason" : "reason",
"userIP" : "1.234.56.78",
"tiemstamp" : "1234567890",
"URL" : "http://www.website.com/q?page=123",
"captureImage" : "imageFile",
"originHTML" : "htmlFile"}
```

**Fig. 3. Transaction Data**

Fig. 3는 제안하는 시스템에서 프라이빗 블록체인에 저장한 트랜잭션이다. 사용자가 허위통신 신고 시스템에 입력한 이름, 전화번호, 이메일주소, 신고할 웹사이트의 URL, 신고내용과 함께 사용자의 IP, 타임스탬프를 저장한다. 웹사이트를 캡처한 이미지는 binary 파일이며 원본 HTML은 JSON 형태로 저장하기 적합하지 않으므로 base64로 인코딩 한 이후 위의 정보와 함께 트랜잭션에 저장한다. 트랜잭션 쿼리 시에는 이와 반대로 이미지와 원본 HTML을 base64로 디코딩하여 출력한다. 각 트랜잭션은 Fig. 2의 스마트 컨트랙트에서 실행되어 블록에 저장된 후 네트워크에 참여한 피어에 분산 저장된다.

## 4. 비교분석 및 평가

선행연구에서는 퍼블릭 블록체인 이더리움을 사용하여 안전한 데이터 출처 관리 시스템을 제안하였다. Table 3은 선행연구와 제안하는 시스템을 비교분석하여 정리한 표이다.

**Table 3. Comparison of Precedent research and Proposal system**

| | Precedent research | Proposal system |
|---|---|---|
| Blockchain type | Public Blockchain | Private Blockchain |
| Data type | Research data | Evidence data |
| Access | Approved | Approved |
| Peer | Over 5 | 4 |
| Maintenance cost | Low | High |
| Speed | Faster | Slower |
| Registration | Required | Optional |

제안하는 시스템은 선행연구 시스템과 같이 저장된 데이터에 접근 권한을 인증하여 통제한다. 제안하는 시스템과 선행연구와의 차이점으로는 선행연구는 퍼블릭 블록체인을 이용하고 데이터 갱신 시 투표를 필요로 하여 피어가 최소 5대 이상 운영되어야 하는 반면, 제안하는 시스템은 프라이빗 블록체인을 이용하여 피어가 4대로 구성할 수 있다. 프라이빗 블록체인 플랫폼 중 가장 많이 쓰이는 하이퍼레저 패브릭의 경우 오더링 서비스 네트워크가 Kafka 클러스트를 사용한다. Kafka는 피어 4대에 설정하여 4개의 브로커를 사용할 경우 1개의 브로커가 중단되어도 3개의 브로커로 안전하게 시스템을 가동할 수 있다. 그리고 추가적인 Geth 사용이 없으므로 시스템 유지비용을 크게 절감할 수 있다. 또한 퍼블릭 블록체인의 복잡한 합의과정을 거치지 않으므로 트랜잭션 저장 속도가 매우 빠르다. 마지막으로 사용자는 데이터를 저장하기 위해 블록체인 네트워크에 가입할 필요 없이 웹사이트에서 직접 데이터 저장이 가능하므로 시스템 이용이 편리한 이점이 있다.

```
'use strict';
const{Contract}= require('fabric-contract-api');
class Evidence extends Contract {
    async queryEvidence(ctx, evidenceID) {
        const docAsBytes = await ctx.stub.
getState(evidenceID);
        if (!docAsBytes || docAsBytes.length ===
 0) {
            throw new Error(`${evidenceID}
 does not exist`);
        }
        return docAsBytes.toString();
    }
}
module.exports = Evidence;
```

**Fig. 4. Smart contract - Query**

제안기법은 원본 HTML을 다운로드 받고 웹사이트를 이미지로 캡처한 후 신고내용과 함께 트랜잭션에 담아 프라이빗 블록체인에 저장을 수행한다.

Fig. 4는 제안하는 시스템의 Query 스마트 컨트랙트 소스코드이다. CLI(Command Line Interface, 명령 줄 인터페이스)나 SDK(Software Development Kit, 소프트웨어 개발 도구 모음)를 통해 웹사이트에서 증거물 ID를 입력받아 프라이빗 블록체인에서 조회한 후 해당 트랜잭션을 리턴 해준다.

Fig. 5는 허위통신 신고 시스템 관리자 화면이다.

Fig. 1의 과정을 거쳐 프라이빗 블록체인의 트랜잭션 저장된 데이터를 기반으로 관리자 화면 상단 좌측에 신고내용을 출력하고 우측에 원본 HTML을 출력한다. 화면 하단에 신고할 당시 웹페이지를 캡처한 이미지를 출력하여 관리자는 신고자가 신고한 시각의 웹사이트의 콘텐츠를 명확하게 파악할 수 있다.

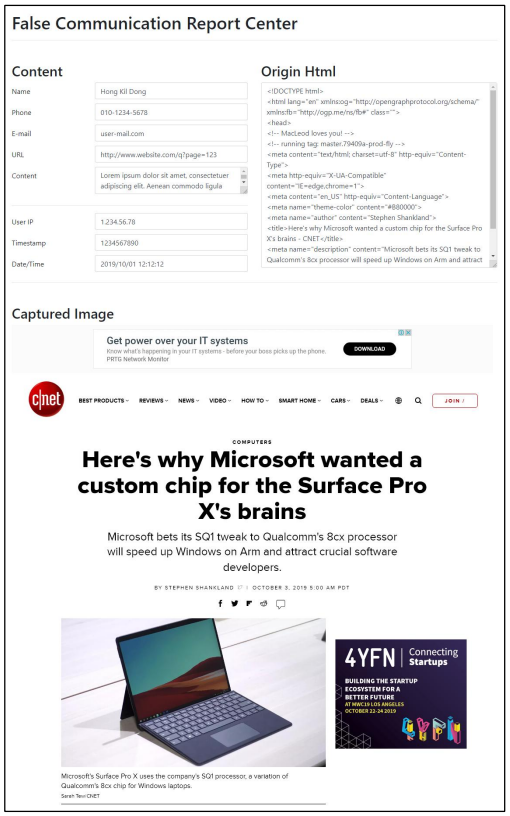


Fig. 5. False Communication Report Administrator Page

제안기법은 증거물을 보존하는데 있어 3가지 측면에서 장점을 가진다.

첫 번째, 신고자가 화면을 캡처한 것이 아닌 서버에서 헤드리스 브라우저를 사용하여 원본 HTML 파일과 웹사이트의 이미지를 캡처함으로써 사용자의 고의적인 증거물 편집을 방지하였고,

두 번째, 신고 데이터와 함께 타임스탬프를 저장함으로써 신고한 시각의 정확한 증거물을 확보하였으며,

세 번째, 증거물에 해당하는 모든 데이터를 프라이빗 블록체인에 저장하여 신고 이후에 신고자와 검증자의 증거물 위변조를 원천적으로 차단하였다.

## 5. 결론

최근 블록체인 기술 중에서 프라이빗 블록체인 기술이 급성장하고 있다. 주로 암호화폐에 사용되는 퍼블릭 블록체인 기술과 다르게 허가된 사용자만이 원장에 기록하거나 조회할 수 있어 기관이나 기업에서 주목을 받고 있다. 또한, 프라이빗 블록체인은 퍼블릭 블록체인과 마찬가지로 분산원장기술에 기초하고 있으므로 블록에 저장된 트랜잭션은 사용자나 운영자 모두 위변조 할 수 없는 시스템이다.

현재 허위통신 신고 시스템은 인터넷 상에서 초기 수준으로 운영되고 있다. 대부분 신고자의 신원정보, 신고내용과 함께 URL이나 웹사이트를 캡처한 이미지를 업로드 하는 형식이다. 이는 신고자가 신고하는 시점부터 신고받은 자가 검증할 때까지의 시간 사이에 웹사이트의 콘텐츠가 변경될 수 있어 증거물로써의 한계가 있다. 이러한 취약점을 보완하기 위해 서버 사이드 헤드리스 브라우저와 프라이빗 블록체인을 이용한 허위통신 신고 시스템을 제안하여 현재 운영되는 시스템의 문제점을 해결하였다.

본 논문에서 제안하는 시스템은 허위통신 뿐만이 아닌 인터넷에서 이루어지는 모든 거래의 증거물 보존을 위한 시스템으로 확대될 수 있다. 향후 연구로는 데이터 압축과 프라이빗 블록체인의 데이터 저장 용량을 줄여줄 필요성에 따라 외부 스토리지를 이용하는 방식에 관한 것이다. 또한, 이미지 캡처로 저장할 수 없는 미디어의 증거물 보존을 위한 연구가 필요하다.

## REFERENCES

[1] M. An. and Y. Park. (2019). Domastic Blockchain Legislation and Policy Analysis and the Limitations Deriving and Present Improvement Points. *Journal of Convergence for Information Technology, 9(9),* 44-51.
DOI : 10.22156/CS4SMB.2019.9.9.044

[2] H. Lee & J. H. Kim. (2019). The Effects of Technostress from using Blockchain on the Technology Acceptance Model(TAM). *Journal of Convergence for Information Technology, 9(8),* 27-34.
DOI : 10.22156/CS4SMB.2019.9.8.027

[3] R. Li & H. Asaeda. (2019). A Blockchain-Based Data Life Cycle Protection Framework for

Information-Centric Networks. *IEEE Communications Magazine, 57(6),* 20-25. DOI : 10.1109/MCOM.2019.1800718

[4] Government Office for Science. (2016). *Distributed Ledger Technology: beyond block chain(A report by the UK Government Chief Scientific Adviser).* London : Government Office for Science.

[5] H. J. Mun. (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain. *Journal of Convergence for Information Technology, 8(3),* 85-90. DOI : 10.22156/CS4SMB.2018.8.3.085

[6] A. Dorri, F. Luo, S. S. Kanhere, R. Jurdak & Z. Y. Dong. (2019). SPB: A Secure Private Blockchain-Based Solution for Distributed Energy Trading. *IEEE Communications Magazine, 57(7),* 120-126. DOI : 10.1109/MCOM.2019.1800577

[7] P. Jayachandran. (2017). *IBM. Blockchain explained: The difference between public and private blockchain.* https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[8] N. Gaur, L. Desrosiers, P. Novotny, V. Ramakrishna, A. O'Dowd & S. A. Baset. (2018). *Hands-On Blockchain with Hyperledger.* Birmingham : Packt Publishing.

[9] Techopedia. (2019). *Timestamp.* Techopedia. https://www.techopedia.com/definition/16285/timestamp

[10] S. Nakamoto. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Bitcoin. https://bitcoin.org/bitcoin.pdf

[11] Hashnet. (2019). *Hashnet.* Coinwiki: Timestamp http://wiki.hash.kr/index.php/%ED%83%80%EC%9E%84%EC%8A%A4%ED%83%AC%ED%94%84

[12] A. Ramachandran & M. Kantarcioglu. (2017). *Using Blockchain and smart contracts for secure data provenance management.* arXiv:1709.10000. https://arxiv.org/abs/1709.10000

[13] Korea Internet Self-governance Organization. (2018). *Fake News Report Center. KISO.* https://report.kiso.or.kr/fakenews/

[14] Theminjoo. (2015). *False operation information report center.* Theminjoo. http://theminjoo.kr/fakenews.do/

**배 석 민(Suk-Min Bae)** [정회원]

- 2016년 ~ 현재 : 단국대학교 일반대학원 ICT융합공학 박사 수료
- 2017년 ~ 2019년 : Graph Blockchain Limited 부사장
- 관심분야 : 그래프 이론, 프라이빗 블록체인, 머신러닝 등
- E-Mail : 72160340@dankook.ac.kr

**양 성 열(Seong-Ryul Yang)** [정회원]

- 2016년 ~ 현재 : 단국대학교 미래ICT융합학과 박사과정
- 2006년 ~ 현재 : (주)디엠씨시스 대표이사
- 2019년 ~ 현재 : (주)유니트론텍 상무이사
- 관심분야 : 자율주행. IOT 보안, 블록체인
- E-Mail : 72171408@dankook.ac.kr

**정 재 진(Jai-Jin Jung)** [정회원]

- 2005년 : 동신대학교 디지털콘텐츠학과 교수
- 2005년 ~ 2009년 : 동의대학교 디지털문화콘텐츠공학과 교수
- 2009년 ~ 현재 : 단국대학교 SW융합대학 응용컴퓨터공학과 교수
- 2015년 ~ 현재 : 단국대 일반대학원 미래ICT융합학과 교수
- 관심분야 : 블록체인 플랫폼, ICT융합서비스, 바이오융합
- E-Mail : dothan@dankook.ac.kr