블록체인을 활용한 디지털 증거의 무결성 강화 방안 연구

A Study on Ways to Reinforce Integrity of Digital Evidence Using Blockchain

최 복 용* · 함 영 욱**

차 례

● 국 문 요 약 ●

오늘날 인터넷 산업의 발달로 디지털 기기의 활용이 급증하고 있으며, 범죄 현장에서 확보한 디지털 기기가 중요 증거로 채택되는 경우가 늘어나고 있다. 특히 이메일 및 컴퓨터 파일 등 디지털 증거도 증거 능력을 인정하는 형사소송법 개정안이 2016년 5월 19일 국회 본회의를 통과하였다. 앞으로는 사이버범죄 뿐만 아니라 모든 범죄의 혐의 유무를 판단하는데 디지털 증거가 중요한 비중을 차지할 것으로 예상된다. 그러므로 압수수색 등을 통해 확보한 디지털 증거의 수집, 분석 및 제출 등 과정을 거치면서 변경되지 않았다는 무결성입증이 매우 중요하게 될 것이다. 그러나 디지털 증거의 위·변조 차단 등 무결성을 보장을 위한 선행 연구들은 아직 미흡한 상태이다. 이에 본고에서는 블록체인을 활용한 디지털 증거의 무결성을 강화시키는 방안에 대해 제시하였다. 블록체인 기법을 활용하면 디지털 증거의 위·변조 가능성, 시스템 해킹 위험성 및 운영비용 측면에서 선행 연구에 비해 비교적 높은 수준의 성능 유지를 기대 할 수 있는 등 본 제안 기법으로 디지털 증거의 무결성 보장을 더욱 강화시킬 수 있을 것이다.

◈ 주제어 : 블록체인, 디지털 증거, 무결성, 해시값

* 경찰청 사이버안전국 사이버수사과 사이버수사전략팀(제1저자)
** 경찰청 사이버안전국 사이버수사과 사이버수사전략팀장(교신저자)

Ⅰ. 서 론

현대사회는 인터넷 및 디지털기기의 발달로 디지털 정보의 활용이 급증하고 있으며, 스마트 TV·냉장고 등 일반 생활가전에도 인터넷이 연결되는 사물인터넷(IoT)[1] 시대가 도래함에 따라 범죄 현장에서 확보한 디지털기기가 증거로 채택되는 경우가 점점 더 많아지고 있다.

디지털 증거란 "디지털(이진수) 방식으로 저장 또는 전송되는 증거가치가 있는 정보"를 말하며, 범행 자체나 범죄와 관련 있는 것으로 판단되어 형사소송법 제106조 및 제215조부터 제218조까지의 규정에 따라 압수한 '디지털 데이터'[2] 또는 '디지털 저장매체'[3] 중 범죄사실의 증명에 필요한 디지털 데이터를 말한다.[4]

디지털 증거는 모든 범죄의 혐의 유무를 확인하는데 매우 중요한 역할을 하고 있으며, 앞으로 그 중요성은 더욱 증가될 것이다. 특히 2016년 5월 19일 형사소송법 제313조 제1항이 개정되어 진술이 담긴 종이서류뿐만 아니라 피고인 등이 작성했거나 진술한 내용이 포함된 문자·사진·영상 등의 정보가 컴퓨터용 디스크 등 정보저장매체에 저장된 디지털 증거까지 전문증거 대상에 포함되었다. 또한 같은 법 제313조 제2

1) 인터넷을 기반으로 모든 사물을 연결하여 사람과 사물, 사물과 사물간의 정보를 상호 소통하는 지능형 기술 및 서비스.

2) 전자적 방법으로 저장되어 있거나 네트워크 및 유·무선 통신 등을 통해 전송중인 정보를 말함(디지털 증거 수집 및 처리 등에 관한 규칙 제2조 제1호).

3) 컴퓨터 디스크, 그 밖에 이와 비슷한 정보 저장매체를 말함(디지털 증거 수집 및 처리 등에 관한 규칙 제2조 제2호).

4) 양근원, "형사절차상 디지털 증거의 수집과 증거능력에 관한 연구", 경희대 박사학위논문, 2006, 20쪽.

항을 보면 디지털 증거 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에도 과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명될 때에는 증거능력을 인정하도록 개정되었다.

따라서 앞으로는 피고인이 법정에서 이메일이나 컴퓨터 파일 등 디지털 증거의 작성을 부인하더라도 디지털 포렌식 조사관 등의 증언을 통해 증거능력이 인정될 전망이다. 그러므로 압수수색 등을 통해 확보한 디지털 증거가 수집, 분석 및 제출 등의 과정을 거치면서 변경 또는 훼손되지 않았다는 무결성 입증은 더욱 중요하게 되었다.

이에 본고에서는 블록체인 기법을 활용하여 디지털 증거의 무결성을 강화시키는 방안에 대해 제시하고자 한다.

Ⅱ. 무결성 보장을 위한 선행 연구

법정에 제출된 디지털 증거가 증거능력을 인정받기 위해서는 수집, 분석 및 제출과정에서 변경·훼손되지 않았다는 무결성이 보장되어야 하며, 이러한 무결성 보장을 위해 선행 연구된 기법에 대해 먼저 알아본다.

1. 변조 탐지 코드(MDC) 공개 방식

변조 탐지 코드(Manipulation Detection Code) 공개 방식은 저장매체의 디지털 증거 수집 절차에서 획득한 MDC(해시값, CRC[5]) 값을 디지

5) CRC(Cyclical Redundancy Check)은 순환오류검사로 파일이 전송되는 도중에 손상되지 않았는가를 검사해주는 것을 말하며, CRC가 에러가 났다는 것은 파일의 일부 내용이 손상되었다는 것을 말함.

털 증거 수집 직후부터 누구나 접근 및 열람할 수 있는 공간에 게시하는 방식이다.

〈그림 1〉 변조 탐지 코드(MDC) 방식 개요도

출처 : 탁희성·이상진, 디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안, 형사정책연구원, 2006, 161쪽

이 방식은 기존에 증거 수집자 또는 증거 관리 담당자만이 알고 있었던 MDC 값을 디지털 증거 수집 초기에 변호사(피고), 검사, 판사 등에게 공개하여, 사후 위조 가능성을 차단할 수 있다. 이를 위해 MDC 값은 획득과 동시에 게시되어야 하며, 게시 후 수정 및 삭제가 불가능해야 한다. 또한 신뢰성 확보를 위해 게시된 공간은 공신력 있는 기관 및 단체에서 운영하여야 한다.

기존 디지털 증거 수집 방식에 큰 변화가 없어, 구현 및 현장 적용이 용이한 장점이 있다. 그러나 위조된 상태에서 MDC 값이 게시되었을 경우 이를 탐지할 방법이 없으며, MDC 값 게시 이후 공격자의 해킹 등으로 인해 MDC 값이 위·변조 될 가능성이 남아 있는 문제점이 있다.[6][7]

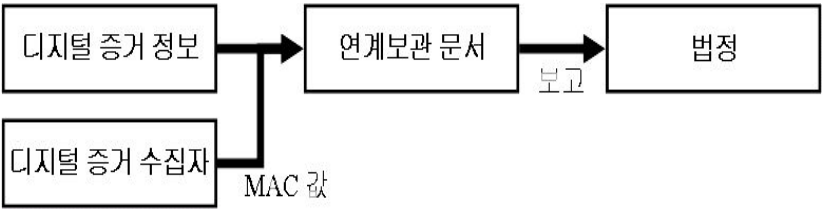
6) 탁희성·이상진, "디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안", 형사정책연구원, 2006, 161쪽.

7) 조상수·신용태, "디지털 증거의 무결성 보장 절차에 대한 개선", 정보과학논문지(정보통신 제39권 제2호), 2012, 185쪽.

2. 메시지 인증 코드(MAC) 사용 방식

메시지 인증 코드(Message Authentication Code) 사용 방식은 디지털 증거 수집자 비밀키(secret key)를 사용한 해시값을 저장매체 원본과 이미지에 각각 적용하여 MAC 값을 획득한 후 이를 디지털 증거 관리 담당자에게 인계 하는 방식이다.

〈그림 2〉 메시지 인증 코드(MAC) 방식 개요도



출처 : 탁희성・이상진, 디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안, 형사정책연구원, 2006, 162쪽

이 방식은 공격자가 증거 수집자의 비밀키를 모르는 경우 정당한 MAC 값을 생성할 수 없으므로, MAC 값을 이용하여 증거의 위・변조 여부를 탐지할 수 있다. 이를 위해 증거 수집자는 공신력이 있어야 하며, 비밀키의 생성・보관・갱신 등의 키 관리가 철저해야 한다.

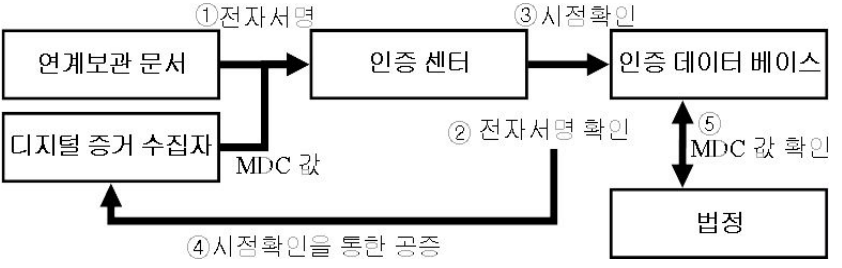
위와 같이 비밀키를 알지 못하는 경우 디지털 증거물에 대한 MAC 값의 위조가 불가능하며, 절차가 단순하여 비교적 현장 적용이 쉽다는 장점이 있다. 하지만 디지털 증거물이 대용량인 경우 비밀키를 사용하여 MAC 값을 획득하는데 상당한 시간비용이 발생한다. 또한 디지털 증거 수집자와 증거 관리 담당자를 따로 분리하여 운영하기 때문에 추가 인력 운영비용이 발생하고, 비밀키의 관리가 철저하지 않을 경우 디지털

증거의 위·변조 가능성은 여전히 남아 있는 문제점이 있다[8)9)].

3. 공개키 기반 구조(PKI) 공증 방식

공개키 기반구조(Public Key Infrastructure)를 이용한 공증 방식은 디지털 증거 수집자가 디지털 증거의 MDC(해시값, CRC) 값이 포함된 정보에 자신의 전자서명을 첨부해 온라인 인증시스템(인증 센터)에 원격으로 공개키 기반의 공증을 요청한다. 공증을 요청받은 인증시스템은 전자서명을 확인하고, 공증시점과 함께 데이터베이스에 저장하는 방식이다.

〈그림 3〉 공개키 기반 구조(PKI) 공증 방식 개요도



출처 : 탁희성·이상진, 디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보 방안, 형사정책연구원, 2006, 163쪽

이 방식은 공격자가 디지털 증거 수집자의 전자서명 값을 작성할 수 없고, 전자서명, 공증시점 확인, 인증시스템 데이터베이스 저장이 순차적으로 이루어지므로, 디지털 증거에 대한 위·변조가 불가능하다.

디지털 증거 수집 과정에서 온라인 인증시스템을 통해 자동화된 방법

8) 탁희성 외 1명, 앞의 논문, 162쪽.
9) 조상수 외 1명, 앞의 논문, 186쪽.

으로 공증이 이루어지므로, 신속하고 효율적으로 디지털 증거의 무결성을 확보할 수 있는 장점이 있다. 하지만, 새로운 절차와 시스템이 요구되므로 초기 도입 비용이 상대적으로 많이 요구 되는 문제점이 있다.[10][11] 또한 온라인 인증시스템의 오류로 인해 전체 네트워크가 마비될 수 있으며, 디지털 증거의 MDC 값이 포함된 전자서명 등 중요 정보가 인증시스템에 집중되어 있기 때문에 해킹과 같은 공격자의 표적이 될 수 있다.[12]

4. 선행 연구 방식의 장·단점 분석

변조 탐지 코드(MDC) 공개 방식은 초기 구축비용이나 운영비용이 비교적 낮고, 증거 수집 절차가 복잡하지 않아 현장 적용이 용이하여 실무상 도입이 큰 어려움이 없다. 그러나 디지털 증거가 위조된 상태에서 MDC 값이 게시되었을 경우 이를 탐지할 방법이 없고, 공개 게시판이 운영 중인 서버의 해킹으로 인한 위·변조 가능성이 남아 있는 문제점이 있다.

메시지 인증 코드(MAC) 사용 방식은 증거 수집 담당자의 비밀키를 알지 못하면 위·변조가 불가능하며, 변조 탐지 코드 공개 방식과 마찬가지로 증거 수집 절차가 복잡하지 않아 현장 적용이 용이하다. 그러나 비밀키가 노출될 경우 위·변조의 위험성이 높으며, 대용량 디지털 증거의 경우 MAC 값을 계산하는데 시간 비용이 발생하는 문제점이 있다.

공개키(PKI)를 이용한 공증 방식은 디지털 증거 수집자가 MDC 값에

10) 탁희성 외 1명, 앞의 논문, 163-164쪽.

11) 조상수 외 1명, 앞의 논문, 186쪽.

12) 김예구, "블록체인 기술과 금융의 변화", KB금융지주 경영연구소, 2015, 1쪽.

전자서명을 한 후 인증시스템 데이터베이스에 저장하고, 온라인상에서 자동으로 공증처리가 되므로 운영 효율성 및 보안성이 뛰어나다. 그러나 인증 시스템 구축 등 초기 도입 비용이 많이 들며, 중앙 집중 방식의 인증시스템에 대한 해킹의 위험성이 높은 문제점이 있다.

Ⅲ. 블록체인의 이해

블록체인은 P2P 네트워크[13]를 통해서 관리되는 분산 데이터베이스의 한 형태로, 거래 정보를 담은 장부를 중앙 서버 한 곳에 저장하는 것이 아니라 블록체인 네트워크에 연결된 여러 컴퓨터에 저장·보관하는 기술이다. 따라서 모든 거래 정보가 담긴 블록체인이 네트워크를 통해 연결되어 있기 때문에 중앙 서버 운영에 따른 해킹의 위험성이 없으며, 관리자가 임의로 거래 정보를 위·변조하는 것이 원천적으로 불가능하다. 대표적인 적용 사례는 가상화폐인 비트코인[14]을 들 수 있다.

1. 블록체인 기본 원리

블록체인은 일정시간(비트코인 경우 약 10분)동안 발생한 모든 거래 정보가 기록된 '블록(Block)'을 생성, 블록체인에 연결된 모든 컴퓨터로 전송하고, 전송된 블록의 유효성이 확인될 경우 기존 블록체인에 연결하

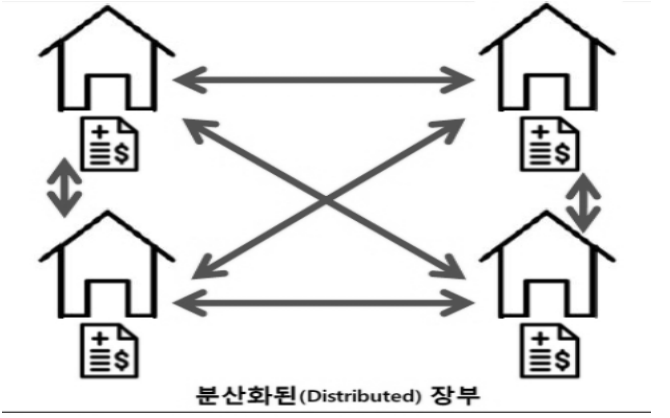
13) Peer-To-Peer Network, 컴퓨터와 컴퓨터를 직접 연결해 서버 없이도 인터넷 등을 통해 네트워크내의 컴퓨터를 공유하게 할 수 있는 기술.

14) 비트코인(Bitcoin)은 2009년 1월, 나카모토 사토시라는 가명의 컴퓨터 프로그래머가 만든 디지털 통화로, 지폐나 동전과 달리 물리적인 형태가 없는 온라인 가상화폐.

는 방식으로 동작한다.

또한 네트워크에 참여하는 각 이용자(컴퓨터)를 노드로 삼아 데이터의 보관, 공유, 관리 부담을 나누는 기술로, 중앙의 관리서버 없이 이용자(컴퓨터) 간의 교차 검증을 통해 보안성과 무결성을 보장한다. 즉, 거래정보를 기록한 원장을 블록체인에 연결된 컴퓨터가 각자 보관하고, 새로운 거래가 발생할 때마다 장부를 똑같이 업데이트 하는 방식으로, 보안성이 강력한 디지털 공공장부 또는 분산원장이라 말한다.

〈그림 4〉 블록체인 P2P 네트워크 개념도



출처 : 스페인 산탄데르은행, 국제금융센터

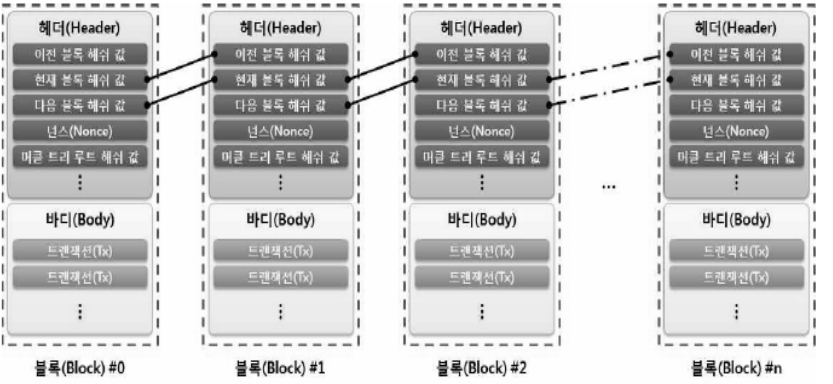
블록체인 방식의 분산원장 기술은 공개키 기반(PKI)[15]의 암호구조로 설계되어 해킹 및 조작 시도로부터 매우 안전한 것으로 평가된다.

15) Public Key Infrastructure, 공개키 알고리즘을 토한 암호화 및 전자서명을 제공하기 위한 복합적인 보안 시스템 환경.

2. 블록체인 구조

블록체인은 P2P 네트워크에서 새로운 거래내역을 담은 신규 블록(block)이 형성되어 기존 블록에 계속 연결(chain)되는 데이터베이스 구조를 가진다. 각 블록은 헤더(Header)와 바디(Body)로 구성된 구조체로, 헤더에는 이전·현재 블록의 해시값(Hash value),[16] 난수(Nonce) 등을 포함하고 있다.[17]

〈그림 5〉 블록체인 연결 구조



출처 : 보안연구부, 블록체인 및 비트코인 보안 기술, 금융보안원, 2015, 1쪽

새로 형성된 블록의 거래정보는 직전 블록의 해시 값을 포함하고 있으며, 직전 블록은 다시 그 이전 블록의 해시 값을 포함하고 있다. 만약 특정 블록의 데이터(거래기록)를 위조 또는 변조하려면 이미 분산 저장

16) 해시 함수를 이용해 임의의 데이터로부터 고정된 길이의 난수를 만들어 내며, 입력값에서 출력값의 계산은 가능하나, 역으로 출력값으로부터 입력값을 계산하는 것은 불가능함 ex) MD5, SHA-1, HAS-160.

17) 보안연구부, "블록체인 및 비트코인 보안 기술", 금융보안원, 2015, 1쪽.

된 모든 사용자 컴퓨터를 해킹하여 블록을 수정해야 하며, 이어진 모든 블록을 수정해야 가능 하는 등 실질적으로 데이터의 위·변조가 거의 불가능하다고 볼 수 있다.

3. 블록체인 종류

블록체인 네트워크 참가자의 성격, 범위 등에 따라 여러 가지 형태가 존재하고 사용용도에 맞게 응용이 가능하다. 특히 네트워크 참가자의 성격에 따라 구분하면, 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain) 및 하이브리드 또는 컨소시엄 블록체인(Hybrid or Consortium Blockchain)으로 나뉜다.[18)19)]

〈표 1〉 블록체인 종류별 특징

구 분	개념 및 특징	예시
퍼블릭 블록체인 (Public Blockchain)	– 최초의 블록체인 활용사례 – 인터넷을 통해 모두에게 공개, 운용 가능한 거래 장부 – 컴퓨팅파워를 네트워크에 제공함으로서 누구든 공증 참여 – 네트워크 확장 어렵고 거래 속도 느림	비트코인, 이더리움[20)]
프라이빗 블록체인 (Private Blockchain)	– 개인형 볼록체인 – 1개의 주체가 내부 전산망을 블록체인으로 관리권한 행사 – Private Blockchain 개발을 위한 플랫폼 서비스도 등장	나스닥[21)]
컨소시엄 블록체인 (Consortium Blockchain)	– 반중앙형 블록체인 – 미리 선정된 N개의 주체들만 참여 가능 – N개의 주체들 간의 합의된 Rule을 통해 공증 참여 – 네트워크 확장이 용이하고 거래속도가 빠름	CITI bank,[22)] HSBC bank

출처 : 보안연구부, 국내외 금융분야 블록체인 활용 동향, 금융보안원, 2015, 2-3쪽

18) Amit, "Public and Private Blockchain Concepts and Examples", https://letstalkpayment.com/public-and-private-blockchain-concepts-and-examples/, 2016. 9. 5. 검색.

19) 보안연구부, "국내외 금융분야 블록체인 활용 동향", 금융보안원, 2015, 2-3쪽.

퍼블릭 블록체인은 공개성, 분산성과 같이 흔히 블록체인에 대해 언급하는 특성들을 모두 가지고 있으며, 가상화폐, 스마트 금융플랫폼인 비트코인, 이더리움 등이 이에 해당된다. 반면 프라이빗 블록체인은 특정한 기관, 업체들이 자신들의 목적과 특성에 맞게 설계한 블록체인으로, 퍼블릭 블록체인과 달리 데이터를 분산 관리하는데 더 적합할 것으로 예상하고 있다.[23]

4. 블록체인 활용분야

블록체인 기술에 대한 금융권 활용분야는 전자화폐, 해외송금, 장외거래, 데이터 저장 및 보호, 메시지 보호 및 전달 등의 형태로 활용되고 있다. 또한 네트워크 및 암호분야 응용과 플랫폼 기능에 따라 암호화폐(Crypto currency),[24] 공공・보안(Public & Security), 산업응용(Industrial Applications), 거래・결제(Transaction & Payments) 등으로 활용범위가 더욱 확대되고 있다.[25]

---

20) 블록체인 기술에 기반한 클라우드 컴퓨팅 플랫폼 또는 프로그래밍 언어로 이 플랫폼을 이용하여 SNS, 이메일, 전자투표 등다양한 정보를 기록하는 시스템을 창안함.

21) 나스탁 프라이빗 마켓에 블록체인 기술을 적용(변호사에게 의뢰하던 거래 승인 절차를 자동으로 검증하는데 블록체인 기술 이용) 계획, 2015. 5.

22) 블록체인 기술을 활용한 자체 사이드체인 생태계인 시티코인(citicoin) 시스템을 금융권 최초로 개발(2015. 7), 사이드 체인은 기존 비트코인 블록체인의 메인 체인에서 분기하여 별도의 원장을 구축한 시스템.

23) 김진화 외 3명, 블록체인의 기술적 이해 및 도입을 위한 첫 걸음, 코빗, 2016, 5-6쪽.

24) 블록체인 기술을 활용한 대표적 분야로, 디지털통화(Digital currency) 또는 가상화폐(Virtual currency) 등의 용어와 혼용 사용.

25) 임명환, 블록체인 기술의 활용과 전망, 한국전자통신연구원, 2016, 4쪽.

〈표 2〉 블록체인 활용분야

분야	적용 사례
암호화폐(가상화폐)	– 비트코인(Bitcoin), 라이트코인(Litecoin), 도기코인(Dogecoin)
공공보안	– 디지털 계약, 공공기록, 전자시민증, 전자투표
산업응용	– 사물인터넷, 소셜 네트워크, 전자상거래, 콘텐츠저작권
거래·결제	– 핀테크, 소액거래, 지불결제, 인증

출처 : 임명환, 블록체인 기술의 활용과 전망, 한국전자통신연구원, 2016, 4쪽

지금까지 블록체인의 기본원리, 구조, 종류 및 활용분야 등 블록체인 기술에 대한 전반적인 개념을 살펴보았다. 이처럼 블록체인은 중앙의 관리서버 없이 네트워크에 연결된 컴퓨터가 모든 거래 내역을 공유 및 교차 검증함으로써 무결성을 보장하고, 해킹을 차단하는 기술로 금융, 의료, 부동산, 지적재산권 등 다양한 분야에 활용 될 수 있다.

하지만, 블록체인은 별도의 중앙 관리시스템이 없기 때문에 네트워크에 문제가 발생할 경우 책임소재가 모호해질 수 있으며, 불법 거래대금 결제, 마약, 탈세 등의 불법적인 용도에 블록체인 기술이 악용될 수 있다. 또한 블록체인 거래내역을 검증 및 확정하기 위해서는 네트워크 구성원 다수의 확인과정을 거쳐야하기 때문에 시간이 다소 필요 하는 등 아직 해결해야 할 문제점들이 남아 있다.[26][27]

26) 홍승필 외 9명, "블록체인기술 금융분야 도입방안을 위한 연구", 금융위원회, 2016, 7쪽.

27) 안랩, "비트코인과 블록체인, 미래를 지배할까", http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24715(2016. 12. 8. 검색)

Ⅳ. 새로 제안하는 블록체인 활용 기법

2장에서와 같이 무결성 보장을 위한 선행 연구된 각 방식은 나름대로 장단점을 갖고 있다. 특히 디지털 증거의 무결성 보장 측면에서는 위·변조 가능성이 낮은 공개키 기반 구조(PKI) 방식이 가장 적합하다고 볼 수 있다. 하지만 모든 데이터를 인증 서버에 저장·보관하는 중앙 집중 방식은 서버 해킹 등으로 인해 문제가 발생할 경우 디지털 증거의 MDC 값이 포함된 전자서명 등 중요 정보가 유출 또는 위·변조 될 수 있으며, 인증 서버의 오류로 인해 전체 시스템 운영이 마비 될 수 있는 등 공개키 기반 구조(PKI) 방식도 여러 문제점을 가지고 있다.

따라서 본 제안에서는 공개키 기반 구조(PKI) 방식의 취약점인 별도의 중앙 인증 시스템 운영 없이 디지털 증거의 위·변조를 차단할 수 있는 블록체인 활용 기법을 제시하고자 한다.

1. 기본 개념

블록체인은 일정 시간동안 발생한 모든 거래 정보가 저장된 블록을 생성하고, 생성된 블록은 중앙 서버가 아닌 네트워크에 연결된 구성원 컴퓨터에 전파하여 저장·보관한다. 만약 특정 블록에 저장된 데이터를 변경하려면 이미 블록이 전파된 모든 컴퓨터를 해킹하여 데이터를 수정해야 하는 등 실질적으로 데이터의 위·변조가 불가능하다. 이와 같이 블록체인은 데이터의 위·변조를 차단할 수 있는 기술로, 중요 문서의 원본 입증 및 콘텐츠에 대한 저작권 인증에 이미 응용서비스 되고 있다.

따라서 확보한 디지털 증거의 데이터 원본에서 추출한 해시값, 등록

번호, 등록자 ID, 등록 시간, 증거 정보 등 등록 데이터를 블록체인 네트워크에 연결된 모든 컴퓨터(노드)에 전파하는 방법으로 위·변조를 차단함으로써 디지털 증거의 무결성을 보장할 수 있다.

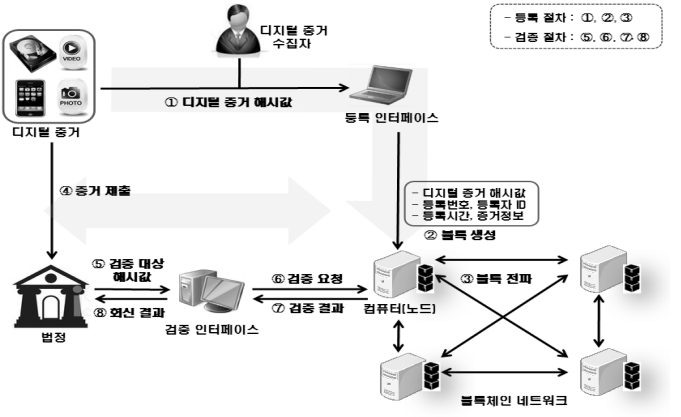
〈표 3〉 등록데이터 상세 내역

등록데이터	내 용
디지털 증거 해시값	– 하드디스크 이미지, 스마트폰, 음성, 사진, 동영상, 문서 파일 등
등록 번호	– 블록체인에 기록할 당시 부여한 순차 번호
등록자 ID	– 디지털 증거 수집자에게 부여한 고유 정보
등록 시간	– 블록체인에 기록할 당시 날짜 및 시간 정보
증거 정보	– 하드디스크 시리얼 번호 or 파일명, 파일 크기 등

※ 등록자 ID, 증거 정보는 암호화 대상

또한 제안 기법은 등록 데이터(디지털 증거 해시값, 등록 번호, 등록자 ID, 등록 시간, 증거 정보)를 기록한 블록을 생성하여 블록체인 네트워크에 전파 및 저장하기 위한 '등록 절차'와 법정에 증거로 제출된 디지털 증거의 위·변조 유무를 확인하기 위한 '검증 절차'로 구분할 수 있다.

〈그림 6〉 블록체인(Block-chain) 활용 기법 개요도

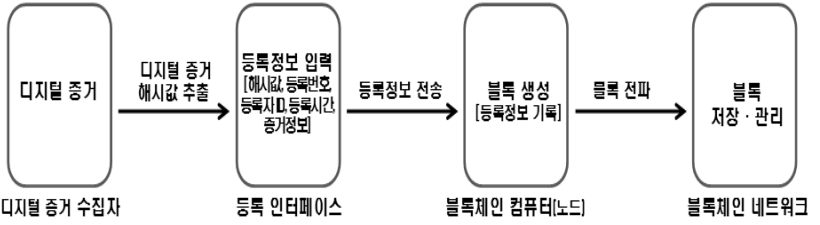


이러한 블록체인 활용 방식은 공개키 기반 구조(PKI) 방식의 가장 큰 취약점인 중앙 인증 시스템의 해킹 위험성 및 시스템 장애로 발생되는 문제점을 보완할 수 있다.

2. 등록 절차

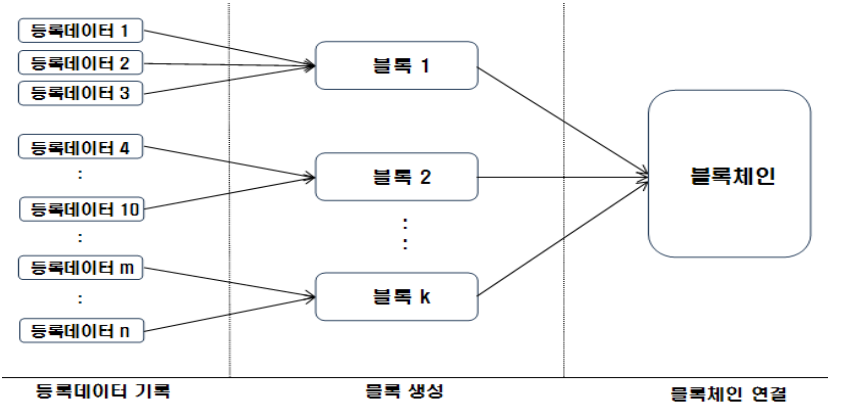
먼저 디지털 증거 수집자가 디지털 증거에서 추출한 해시값을 비롯한 데이터를 등록 인터페이스에 입력한다. 입력된 데이터는 블록체인 네트워크에 연결된 컴퓨터(노드)로 전송되고, 데이터를 전송 받은 컴퓨터(노드)는 새로 생성된 블록에 등록데이터를 기록한다. 이후 생성블록은 블록체인 네트워크에 연결된 모든 컴퓨터(노드)에 전파되고, 블록을 전달받은 각 컴퓨터(노드)는 블록의 이상 유무를 확인한 후 보관중인 블록체인에 연결하여 저장 및 관리한다.

〈그림 7〉 등록 프로세스



특히 새로 생성된 블록에는 일정시간(비트코인 경우 약 10분) 동안 수집된 등록 데이터(디지털 증거 해시값, 등록 번호, 등록자 ID, 등록 시간, 증거 정보)가 포함되어 있으며, 이러한 등록 데이터가 포함된 블록들이 연결되어 블록체인을 구성한다.

〈그림 8〉 등록데이터 저장 구조

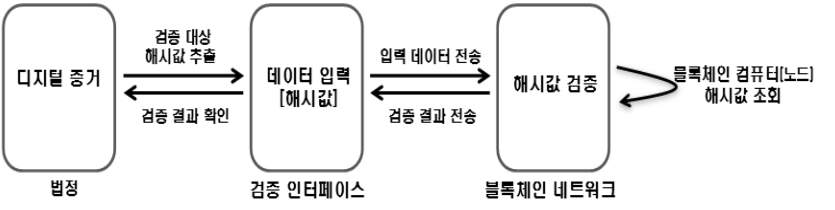


출처 : 이성복, 비트코인 개인간 전자화폐시스템 요약 설명, HP, 2014, 10쪽, 참조 작성

3. 검증 절차

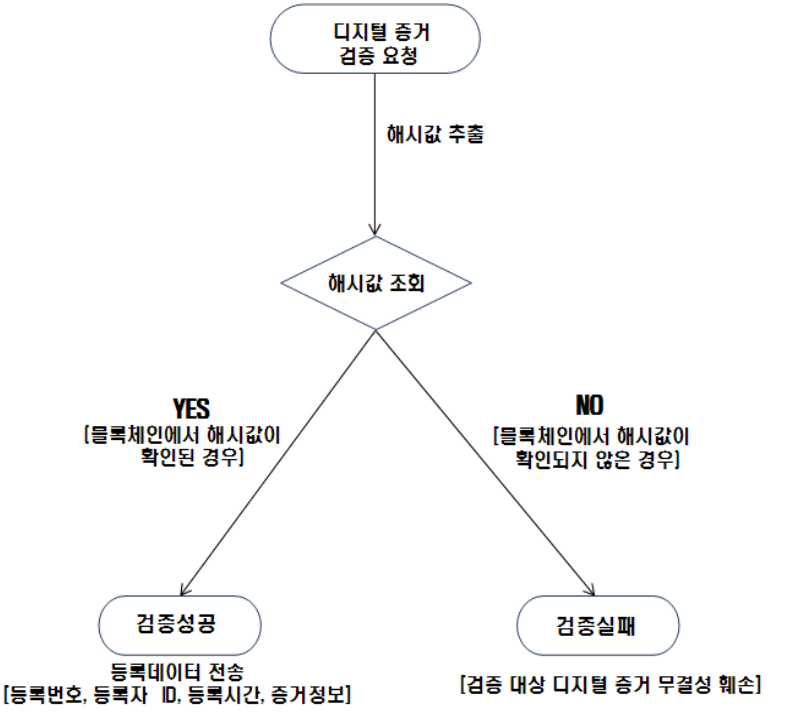
법정에 제출된 디지털 증거에서 추출한 해시값을 검증 인터페이스에 입력한다. 입력된 해시값은 검증 인터페이스를 통해 블록체인 네트워크에 검증을 요청한다. 검증을 요청받은 블록체인 컴퓨터(노드)는 보관중인 블록체인에서 해시값 조회를 통해 검증하고, 검증 결과를 검증 인터페이스로 전송하여 제출된 디지털 증거의 위·변조 유무를 확인한다.

〈그림 9〉 검증 프로세스



검증 대상 디지털 증거의 해시값 조회 결과는 블록체인에서 해시값이 확인되는 '검증 성공'과 해시값이 확인되지 않은 '검증 실패'로 구분된다. 만약 검증에 성공된 경우에는 등록 당시 입력한 "등록 번호, 등록자 ID, 등록 시간, 증거 정보" 등 등록 데이터를 검증 결과값으로 전송하고, 검증에 실패한 경우에는 검증 대상 디지털 증거의 무결성이 훼손된 것으로 볼 수 있다.

〈그림 10〉 디지털 증거 해시값 조회 결과 내역



4. 블록체인 활용 제안 기법과 선행 기법의 특성 비교

디지털 증거의 무결성 보장을 위한 새로 제안하는 블록체인 활용 기법과 선행 연구된 MDC 공개방식, MAC 사용방식 및 PKI 공증 방식의 특성을 비교하였다.

〈표 4〉 블록체인 활용 제안 기법과 선행 기법의 특성 비교

구 분	제안 기법	MDC 공개방식	MAC 사용방식	PKI 공증방식
디지털 증거 해시값 위변조 가능성	낮음	높음	보통	낮음
시스템 해킹 위험성	낮음	높음	낮음	높음
운영 비용	낮음	낮음	보통	높음
등록 소요 시간	보통	낮음	높음	낮음
공신력	높음	낮음	높음	높음

블록체인을 활용한 제안 기법은 블록체인 네트워크에 연결된 모든 컴퓨터(노드)에 디지털 증거의 해시값 등 데이터를 전파하여 저장·공유하는 특성상 선행 제안 방식에 비해 공격자 및 관리자에 의한 데이터의 위·변조가 불가능하므로, 제안 기법에 대한 공신력은 매우 높다. 또한 제안 기법은 모든 데이터를 인증 시스템에 보관하는 PKI 공증 방식과 달리 별도의 중앙 서버가 없기 때문에 시스템 해킹의 위험성 및 서버 운영에 따른 비용을 줄일 수 있다.

그러나 제안 기법은 디지털 증거의 해시값 등 데이터를 블록체인 네트워크에 연결된 모든 컴퓨터(노드)에 전파하여 공유하는 과정이 필요하므로, 공개 게시판 게재(MDC 공개 방식) 및 중앙 서버에 저장(PKI

공증 방식)하는 선행 기법에 비해 데이터를 등록하는데 약간의 추가 시간이 필요하다.

V. 결 론

다가오는 사물인터넷 시대에는 스마트 가전 등 디지털 기기의 활용은 더욱 증가될 것이며, 이에 따라 범죄 현장에서 발견된 디지털 증거는 범죄 혐의를 입증하는데 매우 중요한 열쇠가 될 것이다. 이처럼 디지털 증거의 중요성은 계속 증가하고 있는데도 불구하고, 확보한 디지털 증거의 위·변조 차단 등 무결성을 보장하는 기술과 절차에 대한 선행 연구는 아직 미흡한 상태이다.

따라서 본고에서는 디지털 증거의 무결성 보장을 위한 블록체인 활용 기법을 제시하였다. 블록체인은 일정 시간동안 발생한 모든 거래 정보를 기록한 블록을 생성하고, 생성한 블록을 중앙 서버가 아닌 블록체인 네트워크에 연결된 모든 컴퓨터로 전파하여 공유하는 방식으로 데이터의 위·변조를 차단 할 수 있는 기술로 평가된다.

이처럼 블록체인을 활용한 제안 기법은 디지털 증거의 해시값 위·변조 가능성, 시스템 해킹 위험성, 운영비용 및 공신력 측면에서 선행 연구된 기법에 비해 비교적 높은 수준의 성능이 보장되는 등 본 제안 기법의 활용으로 디지털 증거의 무결성을 더욱 강화시킬 수 있을 것으로 예상된다.

〈논문 접수 : 2016. 10. 24, 심사 개시 : 2016. 11. 17, 게재 확정 : 2016. 12. 20〉

참 고 문 헌

Ⅰ. 국내문헌

1. 단행본

김진화 외 3명, 블록체인의 기술적 이해 및 도입을 위한 첫 걸음, 코빗, 2016

임명환, 블록체인 기술의 활용과 전망, 한국전자통신연구원, 2016

2. 논문

양근원, “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 경희대 박사학위논문, 2006

조상수·신용태, “디지털 증거의 무결성 보장 절차에 대한 개선”, 정보과학논 문지(정보통신 제39권 제2호), 2012

탁희성·이상진, “디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확 보 방안”, 형사정책연구원, 2006

홍승필 외 9명, “블록체인기술 금융분야 도입방안을 위한 연구”, 금융위원회, 2016

3. 기타

김예구, “블록체인 기술과 금융의 변화”, KB금융지주 경영연구소, 2015

보안연구부, “블록체인 및 비트코인 보안 기술”, 금융보안원, 2015

_____, “국내외 금융분야 블록체인 활용 동향”, 금융보안원, 2015

이성복, “비트코인 개인간 전자화폐시스템 요약 설명”, HP, 2014

안랩, “비트코인과 블록체인, 미래를 지배할까”, http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24715 (2016. 12. 8. 검색)

Ⅱ. 외국 문헌

Amit, “Public and Private Blockchain Concepts and Examples”, https://letstalkpayment.com/public-and-private-blockchain-concepts-and-examples/(2016. 9. 5. 검색)

< ABSTRACT >

A Study on Ways to Reinforce Integrity of Digital Evidence Using Blockchain

Choi, Bok-Yong·Ham, Yeong-Ug

Today, development of Internet industry is resulting in rapid increase in utilization of digital devices and the ones secured from crime scenes are increasingly chosen as important evidences. In particular, amendments of criminal procedure act acknowledging admissibility of digital evidences such as emails and computer files passed the assembly plenary session on May 19, 2016. In the future, digital evidences are expected to play important roles in judging suspicions of not only cyber crimes but also all crimes. That is why proving integrity of the digital evidences secured through search and confiscation, that they have not been tampered with in the process of collection, analysis and submission, is expected to become very important. However, advanced research to ensure integrity of digital evidences by blocking them from tampering has been inadequate so far. Thus, this study suggests ways to reinforce integrity of digital evidences using blockchain. Utilizing suggested blockchain technique will enable us to ensure integrity of digital evidences more strongly while maintaining relatively higher performance than that provided by advanced research in terms of potential tampering of digital evidences, system hacking risk and operation cost.

◈ Key Words : Blockchain, Digital Evidence, Integrity, Hash Value