블록체인 기술의 디지털포렌식 및 수사 과정에서의 활용 방안

김 태 룡*

논 문 요 약

분산 컴퓨팅 기반 데이터 위/변조 방지 기술인 블록체인의 등장은 데이터 무결성 검증의 새로운 패러다임으로 다양한 분야에 영향을 끼쳤으며, 이로 인해 디지털포렌식 학계 및 수사기관에서도 블록체인을 활용한 데이터 무결성 검증용 플랫폼 및 수사망을 구축하고자 노력하고 있다.

하지만 채증 및 이미징 이후의 데이터에 대한 무결성과 연계보관성에 대한 검증 플랫폼 및 서비스에 대한 비중이 채증 및 이미징 이전 작업에 대한 서비스보다 훨씬 많으며, 여전히 수사 및 디지털포렌식 과정에서의 애로사항을 시원하게 긁어주지 못하고 있다.

이에 본 논문에서는 디지털포렌식 및 수사 과정에서의 애로사항에 대하여 알아보고, 블록체인 기술을 활용하여 애로사항을 타개할 수 있는 몇 가지 방안을 제시하고자 한다.

[주제어] 블록체인, 디지털포렌식, 수사, 위/변조 방지

■ 과제접수 : 2021. 02. 13. ■ 심사개시 : 2021. 02. 10. ■ 제출확정 : 2021. 02. 13.

목 차

[블록체인]

* KITRI Best of Best 9기 디지털포렌식 트랙 교육생.

1. 블록체인 개념

블록체인(Blockchain)은 상호연결(P2P) 방식으로 생성된 소규모 데이터블록이 서로 연결된 형태이다. 데이터의 분산 저장방식으로 인해 임의로 수정하기 힘들고, 수정하더라도 수정된 데이터조차 모든 참여 노드에 기록되기 때문에 누구나 변경 결과를 알 수 있으므로 조작이 거의 불가능하다.

더하여 블록체인에 사용되는 알고리즘에 따라 탈중앙화를 통한 조직 없는 조직화가 가능하며, 대부분의 블록체인 알고리즘에는 위/변조 방지 방안이 내재되어있다.

구분	주요내용
작업 증명 (Proof of Work: PoW)	비트코인의 창시자인 나카모토 사토시가 제안한 가장 기본적인 합의 알고리즘으로, P2P 네트워크에서 시간 및 비용을 들여 실행된 컴퓨터 수행 작업을 신뢰하기 위해 참여 당사자 간에 검증하는 방식
지분 증명 (Proof of Stake: PoS)	작업 증명 방식(PoW)의 단점인 과도한 에너지 소비문제를 해결한 것으로, 블록 생성권 지분에 참여자가 보유한 지분이 반영되도록 하는 방식
위임지분증명 (Delegate Proof of Stake: DPoS)	반 중앙화된 방식으로, 지분을 보유하고 있는 사람이 자기 권한을 대표자에게 위임하여 대표자들이 블록 생성 및 검증에 대한 권한을 행사하는 방식
PoI (Proof of Importance)	NEM(New Economy Movement)과 같은 가상화폐에서 사용하는 알고리즘으로, 네트워크 참여도에 따라 지급 보상이 달라짐

[표 1] 블록체인과 합의 알고리즘[2)]

2. 서비스

블록체인은 분산 컴퓨팅 기반 데이터 위/변조 방지 기술인만큼 개인정보 혹은 민감 정보를 다루는 서비스군 뿐만 아니라 금융, 데이터 산업, 게임, 의료, 유통 서비스 등 다양한 곳에서 사용되고 있다.

분야	주요내용
금융	연방준비은행&IBM - 지급 결제 시스템 개발 SK C&C - 리플 기반 암호화폐 지급결제 시스템을 갖춘 '체인Z' 출시
물류 및 유통	알리바바 - 블록체인 QR코드 및 위조방지 지문서명 기능이 추가된 블록체인 추적 시스템 현대오토에버&블로코 - 중고차 이력관리 서비스
의료	메디블록 - 의료관광 모바일 결제 플랫폼 '메디토' 개발 KBIDC - DNA와 RNA에 있는 핵염기 순서를 규명/저장하는 '시퀀스 마이닝플래폼' 기술 특허
인증	SK텔레콤&LG유플러스&코인플러그&해치랩스 - 전화번호 바탕 모바일 신분증 기술 개발 파수닷컴 - 증명서 확인검증 플랫폼 '파스블록' 개발
치안	경찰청 - 디지털 증거 관리 플랫폼 구축

[표 2] 블록체인 추진 현황[3)]

2) 이재규, "블록체인을 활용한 해외직구 프로세스 개선방안 연구", 숭실대학교, 2018. 12.

또한 단일 서비스 외에도 블록체인 산업의 대표적인 산출물인 암호화폐와 함께 엮여 서비스되는 경우가 많으며, 그 예로 암호화폐를 사용하는 인터넷 마켓, 거래 내역 추적, 거래 내역 세탁 등의 2차 서비스가 성행하고 있다.

Ⅰ. 들어가며

암호화폐의 등장이후 블록체인의 분산 컴퓨팅 기반 데이터 위/변조 방지 기술이 화제 되면서, 데이터에 대한 무결성(Integrity)을 중시하는 금융, 전자 문서, 데이터 산업 분야뿐만 아니라 연계보관성(Chain of Custody)까지 중시하는 디지털포렌식계와 수사 방면에서도 그 사용처를 탐구하는 중이며, 실제로 암호화폐 추적, 디지털 증거 관리, 데이터 전송/인증에 대한 플랫폼이 형성되어있다.

때문에 본 논문에서는 현재 디지털포렌식 및 수사 과정에서의 애로사항에 대해 찾아보고, 블록체인 기술 적용을 통해 해결 가능한 부분과, 디지털포렌식과 관련한 부가적인 블록체인 플랫폼에 대하여 탐구 해 나갈 것이다.

Ⅱ. 디지털포렌식 및 수사 과정에서의 애로사항

디지털포렌식과 수사 방면에서의 블록체인 기반 서비스 및 플랫폼은 이미징 작업 이후 단계에서 발생하는 데이터 보존, 관리 및 운반에 치중되어있다. 하지만 디지털포렌식 및 수사 과정에서 발생하는 애로사항은 대부분 안티포렌식 기법과 조사관의 실수로 인해 발생하는 경우가 많다. 때문에 본 논문에서는 이미징 이전 단계에서, 즉 사건이 발생하기 전 혹은 발생 직후의 애로사항을 알아 볼 것이다.

1. 주요 로그파일 삭제

안티포렌식 기법의 대표적인 예로, 디지털포렌식에 대한 전문 지식을 가진 크래커가 피해 PC의 주요 로그파일(이벤트로그, $MFT, 기타 로그파일 등)까지 삭제 및

3) 국경완, “블록체인 핵심기술 및 국내외 산업 분야별 적용 사례”, 정보통신기획평가원, 2020. 06.

변조하였을 경우 파일 시스템 관련 증거자료 수집과 분석이 까다로워진다.

2. 선별압수

선별압수 시 대상 기기 속 일부 데이터만 채증 해야 할 경우가 생긴다. 때문에 어쩔 수 없이 각종 문서 및 디렉터리를 옮겨 다니며 선별작업을 진행하게 되는데, 이 때 '수사관에 의해 변조되는 데이터'가 필연적으로 생기게 된다.

하지만 선별압수 이후 해당 데이터에 대하여 수사관에 의한 조작이 발생하였다는 주장이 나오거나, 수사관이 다녀간 후 서비스가 정상작동하지 않는다는 민원이 들어올 경우, 해당 주장에 대한 검증절차가 이루어지는데, 선별압수를 위해 열람했던 문서에 악성 스크립트가 존재하여 선별압수 이후 백그라운드에서 추가 작업이 진행되었을 경우, 현장 캠코더 동영상과 참여인의 증인만으로는 쉽게 끝나지 않는다.

3. 가상환경 및 클라우드 환경

현재 많은 서비스가 클라우드로 넘어가는 추세이다. 이로 인해 채증 대상은 더 커졌으며, 선별수집도 더욱 힘들어졌다. 더하여 도커와 같이 가상환경 기술이 발달함에 따라 불법 도박사이트나 마약거래 사이트 등 범죄목적의 서비스 구축 또한 이미지 배포만으로도 뚝딱 만들 수 있기 때문에 박멸이 힘들어졌다.

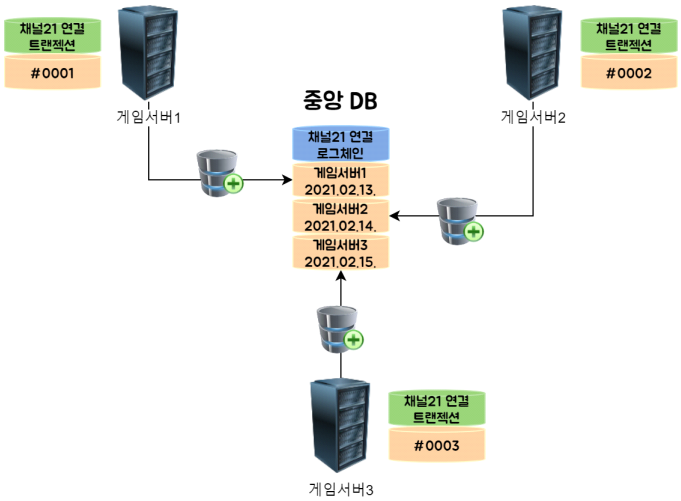
Ⅲ. 블록체인 기술을 통한 해결방안

1. 로그체인 (암호화 : X, 반 중앙화)

주요 로그파일을 삭제하는 행위를 막기 위해 동일 로그를 다른 PC에 저장하는 미러링도 나쁘지 않은 방법이나, 금융, 국제 기업 등 동일 서비스를 제공하는 PC가 수 백 수 천대일 경우, 한 시간에 생성되는 '동일' 로그만도 어마어마할 것이다.

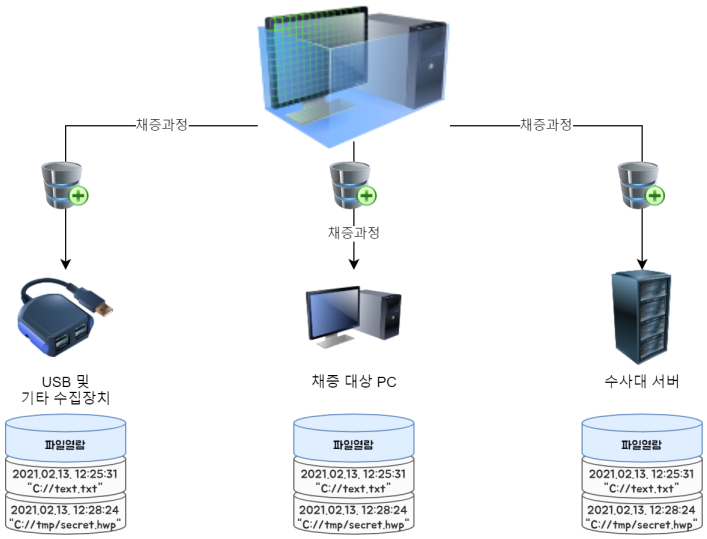
때문에 동일한 이벤트 발생 시 동일한 내용의 로그가 시간 순으로 쌓이기만 할 뿐, 삭제되거나 변조되지 않는 특성을 이용하여, 동일 혹은 유사 이벤트를 묶어 저

장하는 로그체인 방안을 제시한다.



[그림 1] 로그체인 동작 구상도

2. 채증활동 로그체인 (암호화 : X, 탈 중앙화)



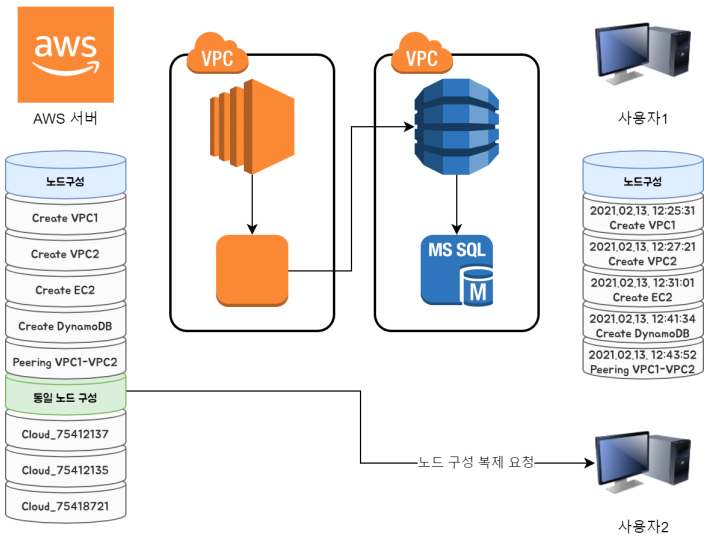
[그림 2] 채증활동 로그체인 동작 구상도

USB 혹은 기타 저장장치에 기기에 삽입 된 이후의 활동내역을 저장장치와 연결된 디바이스, 수사 네트워크망 세 곳에 블록체인 기반 데이터로 기록하는 방안이다.

활동 내역이 세 곳 모두 동일하게 기록되므로 선별압수 이후 현장 캠코더 영상 및 피압수자의 날인만으로 검증하기 힘든 데이터 오차가 발생하였을 경우, 자동화된 본래증거로써 채증활동 로그체인이 도움 될 것이다.

3. 동일 노드구성 체인 (암호화 : X, 반 중앙화)

클라우드 구성 및 가상환경 빌드 이미지의 설치 또는 구성 요소에 대한 정보를 블록체인 형태로 저장하여 사용자에게는 서비스 구성 스냅샷 기능 제공을, 서비스 제공 업체는 사용자 패턴 데이터 획득을, 수사기관은 범죄가 발생한 연관 이미지/클라우드에 대한 구성 정보와 사용자 수 등을 얻을 수 있다. 다만 클라우드 서비스와 가상화 서비스의 협조가 필요하며, 본인의 노드 구성을 수사기관 이외 타인에게 공개할지 여부를 활성화/비활성화 할 수 있는 메뉴가 필요하다.



[그림 3] 동일 노드구성 체인 동작 구상도

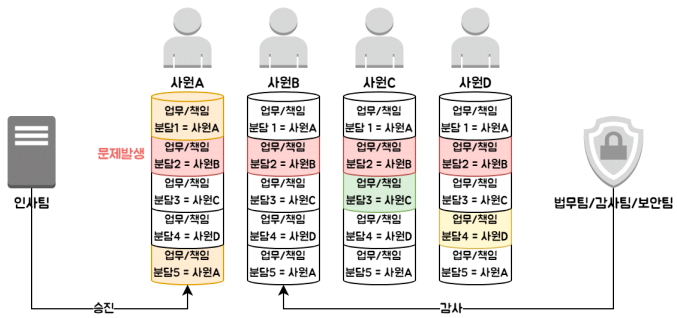
IV. 기타 블록체인 기술 활용방안

애로사항을 제외한 이외의 방향에서 블록체인 기술의 활용방안을 찾기 위해서는 우선 디지털포렌식과 수사가 이루어지는 곳을 알아 볼 필요가 있다.

분야	사용 처
일반 기업	법무팀, 감사팀, 보안팀
개발 회사	포렌식 도구 개발, 세일즈 엔지니어
보안 회사	침해사고 대응, 악성코드 분석
법무법인	소송관련 디지털 증거 분석, eDiscovery
회계법인, 컨설팅 회사	회계부정조사, eDiscovery
수사/조사 기관	범죄수사, 위법 행위 조사
연구/대응 기관	기술 연구, 이상 대응

[표 3] 디지털포렌식 기술이 사용되는 분야와 사용처

일반 기업에서는 사원들에 대한 업무 관리 시 블록체인 기술이 사용될 수 있을 것이다. 각 사원마다 프로젝트 진척도나 맡은 업무 및 사용기기에 대한 정보를 각자 공유함으로 써 PC 및 전자기기를 이용한 사고 발생 시, 책임소재를 분명하게 가리거나, 기술 유출 사건이 일어났을 때 빠른 대처가 가능해 질 것이다.



[그림 4] 일반 기업에서의 블록체인 기술 사용 방안

개발회사는 포렌식 도구 개발 시 버전 관리 및 소스코드 증명 시 개발팀 전체에게 해당 정보를 공유하여 패치서버 탈취에 대응할 수 있을 것이며, 세일즈 엔지니어는 동일 판매상품을 구매한 고객들과 판매 제품 정보를 공유함으로 써 제품과 고객관리를 수월하게 진행할 수 있을 것이다.

보안회사의 경우 보안점검 수행 내역을 체인 데이터로 엮어 고객사와 공유함으로 써 보안점검 이후 이행내역 확인 시 사용할 수 있을 것이다.

법무법인의 경우 E-Discovery 시, 상대측에서 공개한 증거자료와 본인이 제출한

증거자료를 체인 데이터로 엮어 공유함으로 써 서로의 데이터가 추가/제거/변조되지 않는지 확인하는데 사용할 수 있을 것이다.

V. 마치면서

분산 컴퓨팅 기반 데이터 위/변조 방지 기술인 블록체인의 등장 이후 다양한 데이터 무결성 검증 플랫폼 및 서비스가 생겨났으며, 디지털포렌식 학계 및 수사기관에서 이를 어떻게 활용할 것인가를 두고 많은 연구가 이루어지고 있다. 기본이 위/변조 방지 기술인만큼 앞으로 수사 및 디지털포렌식 과정에서의 애로사항을 긁어주는 다양한 기술이 파생될 것을 기대하며, 본 논문에서 제시한 활용 방안이 도움 될 수 있기를 바란다.

참 고 문 헌

1. 국내문헌

논문

이재규, “블록체인을 활용한 해외직구 프로세스 개선방안 연구”, 숭실대학교, (2018.12.)

국경완, “블록체인 핵심기술 및 국내외 산업 분야별 적용 사례”, 정보통신기획평가원, (2020.06.)