논문

기록관리시스템 블록체인 기술 적용 방안 연구*

A Study on Application of Record Management System Block Chain Technology

이기영(Lee, Gi-yeong)** · 김익한(Kim, Ik-han)***

* 본 연구는 명지대학교 기록정보과학전문대학원 석사학위논문을 수정 · 보완한 것임.
** 명지대학교 기록정보과학전문대학원 기록관리전공 석사 (mj65170012@gmail.com) (제1저자).
*** 명지대학교 기록정보과학전문대학원 교수 (ikhan@mju.ac.kr) (교신저자).
■투고일: 2019년 03월 29일 ■최초심사일: 2019년 04월 02일 ■게재확정일: 2018년 04월 26일.
■기록학연구 60, 317-358, 2019, https://doi.org/10.20923/kjas.2019.60.317

〈초록〉

블록체인 기술은 4차 산업혁명의 핵심기술 중 하나로 등장했다. 블록체인 기술은 블록 내 저장된 정보의 진위 여부와 위·변조 여부의 검증이 가능하고, 특정 기록을 임의로 조작하거나 삭제하는 행위가 불가능하며, 투명한 감사추적이 가능하다는 특징을 가지고 있다.

본 연구는 기록관리에 블록체인 기술 적용방안을 모색한다. 이를 위해 블록체인 기술의 물리적인 영역인 코드영역으로 접근하여 핵심적인 물리적 구조를 일부 살펴보고, 블록체인 기술의 응용가능성을 도출하고자 한다. 미래의 기록관리 모델이자 현재 단계적으로 전환 추진 중인 '클라우드 기록관리시스템'의 일부 기능을 모듈 방식의 블록체인으로 구현하여 현행 기록관리 프로세스의 여러 기능을 간소화 하거나 대체할 수 있는 블록체인 네트워크 모델을 제시하고자 하였다.

주제어 : 기록관리 프로세스, 클라우드 기록관리시스템, 블록체인, 모듈 방식, 블록체인 네트워크 모델

〈Abstract〉

Blockchain technology has emerged as one of the key technologies of the fourth industrial revolution. Blockchain technology is characterized by being able to verify the authenticity of stored information in a block and whether it is false or falsified, cannot arbitrarily manipulate or delete a particular record, and is capable of transparent audit trail.

This study is designed to explore how to apply blockchain technology to record management. For this purpose, we want to approach the code area, the physical area of the blockchain technology, to explore some of the key physical structures, and to derive the applicability of the blockchain technology. By implementing the part of'Cloud-Record Management System', future record management system model and currently in the process of phasing out step by step, as a modular block

chain, I suggest a blockchain network model that can simplify or replace various functions of the current record management process.

Keywords : Record management process, Cloud-Record management system, Blockchain, modular, Blockchain network model

1. 서론

1) 연구의 배경과 목적

블록체인 기술은 4차 산업혁명의 핵심기술 중 하나로 등장했다. 비트코인의 기반기술로서 처음 알려지기 시작하면서, 현재는 다양한 분야에서 활용방안을 모색하는 미래핵심기술로 평가받고 있다. 블록체인 기술은 블록 내 저장된 정보의 진위 여부와 위·변조 여부의 검증이 가능하고, 특정 기록을 임의로 조작하거나 삭제하는 행위가 불가능하며, 투명한 감사추적이 가능하다는 특징을 가지고 있다. 이러한 관점에서 보면 블록체인 기술은 전자기록관리 환경에서 활용하기에 적합한 기술이라 판단할 수 있다. 그렇기 때문에 기록학계에서도 블록체인 기술에 큰 관심을 두고 있다. 그러나 필자는 초기 블록체인 기술의 활용성에 대한 논의가 활발하게 이루어지던 시점에서 당시 이해하고 있던 블록체인 기술을 바탕으로 고민하였을 때, 블록체인 기술을 기록관리에 적용하는 것에 대해 조금의 우려를 가지고 있었다. 그 이유는 크게 두 가지인데, 하나는 블록체인 기술 자체의 기능적 특성 때문이고, 다른 하나는 아직 심층연구가 진행되지 않은 기술이기 때문에 발생할 수 있는 위험요소에 대한 경계심이었다.

블록체인 기술에 대해 구체적으로 연구를 시작하기 이전 시점에서 필자가 생각했던 블록체인 기술 자체의 기능적 특성으로 인한 우려는 크게 세 가지 이슈였다. 첫째, 블록체인 기술은 분산원장의 기술로 익명의 참여자들이 같은

정보를 공유하고 있기 때문에, 기록에 대한 접근권한을 부여하거나 접근을 통제하는 것이 불가능하다. 둘째, 블록체인 내 블록에 컴포넌트로 전자기록 원문을 저장할 경우, 볼륨이 매우 커져 스토리지를 감당할 수 없다. 셋째, 블록체인의 특성상 한번 입력된 트랜잭션은 삭제할 수 없는데, 만약 이 트랜잭션을 활용하여 기록을 관리한다고 하면, 기록 폐기와 같은 처분절차를 수행할 수 없다는 문제를 발생시킨다. 이러한 우려를 해소하기 위해, 블록체인 기술을 기록관리에 적용시키기 위해 우려되는 사항들을 해결할 수 있는 방안을 모색하였고, 그 결과 다음과 같은 방향에서 문제의 해결방안을 확인했다.

첫 번째 이슈와 관련해서는 블록체인 유형별 특성을 분석하여 보다 적합한 유형을 선택함으로써 문제를 해결하는 방안을 확인했다. 분산원장 기술의 특성으로 인한 문제는 블록체인의 세 가지 유형 중 퍼블릭 블록체인에 해당하는 내용이다. 해결방안을 모색하는 과정에서 프라이빗 블록체인 유형과 컨소시움 블록체인 유형이라는 다른 유형의 블록체인이 연구되었으며, 각 유형을 분석하여 적합한 유형을 선택하면 문제를 해결할 수 있을 것임을 확인했다. 두 번째 이슈와 관련해서는 블록체인의 블록 컴포넌트에 기록의 원문을 담지 않고 원문을 대체할 수 있는 정보를 담아내어 관리하는 방향으로 문제의 해결방안을 확인했다. 기록의 원문을 저장하는 스토리지와 블록체인 네트워크를 분리하고, 기록원문의 해시값 혹은 기록원문에서 추출한 일부 메타데이터의 해시값 등을 활용하면 스토리지 문제를 해결할 수 있을 것임을 확인했다. 마지막으로 세 번째 이슈와 관련해서는 두 번째 이슈의 문제 해결방안을 확장하여 해결방안을 확인했다. 우선 블록체인에 기록 원문을 저장하는 것이 아닌 해시값 형태를 저장하는 것이기 때문에, 이는 트랜잭션에 이력으로 남게 되어도 해시값을 역 추적하여 원문을 확인할 수 있는 방법이 없으므로 문제가 되지 않는다.

블록체인 기술에 대한 연구를 통해 블록체인 기술의 특성으로 인한 위험요소로 생각했던 부분들은 해결방안이 있다는 점은 확인했지만, 여전히 심층연구가 진행되지 않은 기술이기 때문에 발생할 수 있는 위험요소에 대한

경계심이 남아있었다. 현 시점까지도 블록체인 기술에 관한 연구는 대부분 개념적 영역과 논리적 영역으로 접근하고 있기 때문에 선행연구를 통해서도 이는 해소할 수 없었다.

이러한 배경에서 본 연구는 기록 관리에 블록체인 기술 적용방안을 모색하는 과정에서 기술의 위험요소를 파악하기 위해 기존 연구들의 블록체인 기술 접근 범위에서 확장하여 물리적 영역인 코드 영역을 살펴보는 것을 목표로 설정하였다. 블록체인 기술의 물리적 영역인 코드영역으로 접근하여 핵심적인 기능들을 구현하는 물리적 구조의 일부를 살펴보고 블록체인 기술의 응용가능성을 도출하고자 한다. 도출한 결과를 기반으로 기록관리에서 블록체인 기술을 활용할 수 있는 방향을 제시하고, 이에 적합한 블록체인 모델을 제시할 것이다.

국가기록원은 중앙부처 기록물을 범정부 차원에서 공동·활용하는 클라우드 기록관리시스템(CRMS)을 지난 2016년 개발해 2019년 1월까지 총 43개 중앙부처의 전환을 마치고, 범정부 차원의 단일 시스템을 운영할 계획을 가지고 있다. 이에 따라 현행 기록관리시스템의 프로세스의 많은 부분이 변화될 것이 예측되며, 기록관리시스템 재설계에 관한 연구도 활발하게 이루어지고 있다. 최근 연구에서는 기록관리 신기술로 '마이크로서비스 아키텍처'를 소개하면서, 모듈형 시스템으로 시스템을 운영할 때의 장점에 대해 소개한 바 있다(오진관, 임진희, 2018).

클라우드 기록관리시스템과 모듈형 시스템이라는 두 가지 이슈에서 착안하여, 본 연구는 미래 기록관리 모델인 '클라우드 기록관리시스템'의 환경을 염두에 두고, 커스터마이징과 시스템 적용에 용이한 모듈 방식으로 구현하여 현행 기록관리 프로세스의 여러 기능을 간소화 하거나 대체할 수 있는 블록체인 네트워크 모델을 제시하고자 한다.

2) 연구의 범위와 방법

본 연구는 클라우드 기록관리시스템 환경에 모듈방식으로 구현해 적용시

킬 블록체인 네트워크 모델을 제시하는 것을 목적으로 한다. 이를 위해 블록체인 기술의 개념을 검토하고, 나아가 구체적으로 탐구하여 그 구조적 특성을 파악한다. 또한 클라우드 기록관리시스템 환경을 가정하였을 때, 현행 프로세스 기능 중에서 개선이 필요한 기능들을 추출해내고, 이를 블록체인 기술을 활용하여 대체하거나 간소화 할 수 있는 방안을 살펴본다.

우선 블록체인 기술에 대한 문헌 및 선행연구, 기사정보들을 살펴보고 핵심 기능요소를 추출한다. 추출한 기능요소를 구체적으로 탐구하기 위해 '비트코인 코어'의 소스코드를 분석한다. 비트코인 코어는 대표적인 가상화폐 중 하나인 비트코인의 클라이언트 소프트웨어를 유지관리하고 공개하는 오픈소스 프로젝트로, C++ 언어를 기반으로 개발되어 사토시 나카모토에 의해 배급되었다(Bitcoin-core 2018). 사토시 나카모토가 개발 배포한 버전의 여러 갈래 중 직계로 내려오는 오픈소스이며, 현재까지도 활발하게 버전 업데이트가 이루어지고 있다. 전체 블록 사이즈는 65GB 이상으로, 클라이언트 소프트웨어를 설치할 경우 비트코인 네트워크에 익명의 참여자로서 참여할 수 있게 된다. 비트코인 코어는 가상화폐를 사용하기 위해 개발된 1세대 블록체인 플랫폼으로 이를 기록관리에 직접 적용시킬 수 없지만, 핵심 구조의 코드(소스코드)를 살펴봄으로써 블록체인의 물리적 구조를 이해할 수 있기 때문에 비트코인 클라이언트 소프트웨어를 구성하는 소스코드 분석을 통해 응용가능성을 모색할 것이다.

비트코인 코어를 구성하는 소스파일(.h, .cpp)에는 비트코인 블록체인 네트워크를 구성하는 코드들이 분산되어 구조화 되어있다. 분산된 코드 중에서 블록체인의 핵심인 블록을 구성하는 헤더와 트랜잭션에 관련된 소스를 추출하여 어떻게 구성되어 있는지를 살펴보았다. 블록의 헤더와 트랜잭션을 구성하는 물리적 코드를 분석하면, 각각에 어떠한 코드를 더해서 무엇을 구현할 수 있는지를 가늠할 수 있게 된다. 예를 들어, 헤더 파일에 기존에 입력되는 내용을 일부 수정하거나 추가할 수 있다면, 헤더에 입력되는 정보를 더블린코어에 입각하여 구성해 블록헤더 자체에 메타데이터 정보가 입

력될 수 있도록 커스터마이징 할 수 있다. 이와 같이 코드구성 안에서 커스터마이징이 가능한 부분이 어느 부분인지를 분석하여, 해당 부분을 어떤 방식으로 커스터마이징 하여 기록관리에 어떻게 적용시키고 활용할 수 있을지를 구체적으로 살펴보았다.

국가기록원은 2016년 기록보존기술 연구개발사업으로 클라우드 서비스 기반 전자기록 관리모델 및 거버넌스 개발 연구를 수행한 바 있다. 이 연구에서는 클라우드 기반 전자기록 관리 모델을 제시하면서 그 기능요건을 정의하였다. 클라우드 기반 기록관리시스템 환경에서는 하나의 클라우드 스토리지에 전자기록을 보관하고, 각급 기관이 이에 연동하여 접근한다. 이러한 구조는 이관절차, 생산현황통보 등 현행 기록관리 프로세스의 기능의 일부가 재편되거나 대체되는 등 크고 작은 변화를 가져올 것으로 예상된다. 현행 기록물관리 법령에서 제시하고 있는 기록관리 프로세스를 바탕으로 이와 같이 프로세스의 변화지점들을 추출하여 향후 방향성을 제시하고, 블록체인 기술을 활용하였을 때 어떤 방식으로 적용될 수 있을지를 제안한다. 또한 클라우드 기반 기록관리시스템 환경에서는 통상적으로 클라우드의 특성상 보안성이 낮다고 평가된다. 특히 기록은 위·변조 방지를 위한 보안이 매우 중요한 요소이기 때문에 보안과 관련한 이슈가 상당히 중요해지고 항상 우려사항으로 지적될 수밖에 없다. 이러한 측면에서도 차세대 보안기술로도 논의되고 있는 블록체인 기술을 적용할 방안을 모색하였다.

3) 선행연구

블록체인 기술은 현재 다양한 분야에서 연구되고 있으며, 초기 금융 분야에서 집중적으로 연구되었으나, 최근에는 다양한 분야에서 활용하고 있다.

국가의 단위로는 에스토니아가 블록체인 기술을 가장 빠르고 성공적으로 도입하여 활용하고 있다. 현재 에스토니아는 블록체인 기술을 기반으로 데이터플랫폼을 구축해 투표, 의료처방, 세금납부 등 공공서비스를 전자적으

로 제공하고 있으며, 국민의 98%가 전자신분증을 보유하고 있고, 전자신분증 인증을 통해 은행업무와 개인정보 관련 업무가 가능하다(경기연구원 2018). 에스토니아에서 구축한 블록체인 기술 기반의 데이터플랫폼으로 제공되는 공공서비스는 모두 개인정보 보호의 측면에서 보안성이 매우 중요한 서비스들이다. 국민의 98%가 전자신분증을 보유하면서 이를 이용해 개인정보를 활용해야 하는 각종 업무들을 문제없이 수행하고 있다는 점에서 블록체인 기술이 전자기록의 보안성을 매우 높은 수준으로 보장하고 있음을 확인할 수 있다.

2016년도부터 기록관리 분야에서도 국내외로 블록체인 기술에 대한 연구 및 표준화 동향을 보이고 있다. 캐나다의 University of British Columbia(UBC)는 블록체인 기술의 기록관리 분야에 대한 적용가능성에 대한 연구를 진행하고 있다. UBC는 기록관리의 관점에서 볼 때 블록체인의 리스크를 조직의 통제, 기록 신뢰성 보장, 장기 디지털 보존 등으로 보고 있으며, 이러한 리스크를 해결하기 위해 다양한 매체의 정보를 조사하는 것을 목표로 하고 있다(Victoria Lemieux 2016). 또한 영국 국립보존기록소(The National Archives)는 블록체인의 핵심기술인 분산원장기술을 기록관리에 적용하여, 제도적 신뢰에서 벗어나 기술적 신뢰를 확보하는 분산원장기술 적용 플랫폼 개발을 실험하는 'ARCHANGEL' 프로젝트를 수행중이다(왕호성 2018). ARCHANGEL 프로젝트는 약 7억 원의 연구기금, 24개월의 기한으로 진행되고 있으며, ARCHANGEL의 프로토타입 플랫폼은 블록체인 기술 중 하나인 이더리움을 기반으로 개발되었다. ARCHANGEL은 전자서명, 수작업으로 생산하던 메타데이터 관리 등 기존의 실무에 분산원장기술을 적용하여 혁신할 것을 제안하고 있으며, 현재 프라이빗 블록체인 모형과 퍼블릭 블록체인 모형의 합의모형을 실험중이다. ARCHANGEL 플랫폼에는 전자문서 공개여부의 자동분류를 위해 메타데이터와 파일형식을 구분하는 파일포맷 식별도구가 포함될 예정이며, 해시 알고리즘을 특정 포맷에만 적용 가능한 맞춤형 해시 기능, 비공개 기록에 대한 각종 보안기법의 자동화도 시도된다(왕호성 2018).

국내의 경우, 전자문서의 진위 확인 및 시점확인과 관련해서 이미 2015

년에 블록체인 기반의 기술이 발표되었으며, 2016년 이와 관련된 보안 기술서가 발표된 바 있다(블로코 2016). 하지만 이는 기록관리적 측면에서 진행된 연구가 아닌 전자문서의 데이터에 초점을 두고 수행된 연구이다.

2017년 국가기록원의 연구과제 “차세대 기록관리모델 재설계 연구”에서 불록체인 기술에 대해 논한 바 있다. 이 연구에서는 2017년 2월 행정자치부는 지능형 전자정부를 위한 기술로 블록체인 기술 도입을 검토한 바 있음을 소개하며, 블록체인 기술을 기록 품질요건 개념을 확장시키는 수단으로 보았으며, 기록관리에 블록체인 기술을 적용할 경우 중앙집중형 방식에서 퍼블릭 또는 프라이빗 블록체인 네트워크 구축을 통한 분산 방식의 진본인증 체계로 개념이 전환됨을 시사하였다(명지대학교 산학협력단 디지털아카이빙연구소 2017).

기록관리 분야에서 블록체인 기술의 활용방안을 진본인증 체계로 보는 또 다른 연구가 최근 발표되었다. 이 연구에서는 기록의 진본인증 수단으로 블록체인 기술을 활용하는 방안으로 기록관리를 위한 블록체인 모형 세 가지를 제시하였다(이경남 2018). 각 모형은 일부 프로세스를 대체하거나, 아카이브 시스템과 연계되거나, 프로세스 이벤트를 저장하는 역할을 하며, 이 중 아카이브 시스템과의 연계 모델은 클라우드 기록관리시스템 환경에서의 블록체인 모형을 가정하고 제안하였다. 이는 본 연구에서 제안하고자 하는 모형과 그 틀은 같지만, 논리적 구조를 가정에 두고 모형을 제안하였기 때문에 진본인증 수단으로서의 활용방안에서 확장되지는 않았다는 점에서 본 연구와 차이가 있다.

본 연구는 이를 확장하여, 클라우드 기록관리시스템 환경에서 블록체인 기술을 활용할 수 있는 부분들을 물리적 구조 분석을 통해 진본인증의 수단 외에 활용될 수 있는 지점들을 도출하고, 새로운 기록관리 블록체인 모델을 제시할 것이다. 소스코드 분석을 통해 물리적 구조를 파악하고 접근하는 연구이기 때문에 본 연구에서 제시하는 기능 프로세스들은 향후 실제로 구현될 가능성이 매우 높을 것이라 전망한다.

2. 블록체인 기술

1) 블록체인 기술의 개념

블록체인 기술은 2008년 나카모토 사토시라는 익명의 개발자가 2008년 10월 31일 공개한 〈Bitcoin : A Peer-to-Peer Electronic Cash System〉이라는 논문에서, 가상화폐의 일종인 비트코인의 기반기술로 소개하면서 대중들에게 알려지기 시작하였다(이동영 외 2017). 블록체인 기술은 사토시의 논문에서 소개하고 있는 것처럼 Peer-to-Peer(P2P) 구조를 가지고 있으며, 중앙관리자나 중앙 데이터 저장소가 없으며, P2P 망 내 모든 참여자가 모든 거래 목록을 서로 공유하고 감시·관리하는 '분산원장'기술이다. 블록체인의 핵심은 분산원장 기술로, 트랜잭션(거래정보)을 참여자들이 분산저장 하여 신뢰성을 확보하는 것이다.

블록체인 기술은 화폐시장을 중심으로 연구 및 개발 되고 있으며, 다양한 분야에서 블록체인 기술을 활용하기 위한 연구를 수행하고 있다. 블록체인 기술이 적용된 블록체인 네트워크의 소스들은 대부분 퍼블릭 블록체인 유형의 오픈소스로, 가장 대표적이라 할 수 있는 가상화폐인 비트코인의 블록체인 소스 역시 앞서 언급한 비트코인 코어라는 명칭의 오픈소스로 깃허브(github)에 업로드 되어있다. 블록체인은 C++, JAVA, Python, WebAssembly, Go 등 다양한 프로그래밍 언어로 구현된다. 가상화폐 블록체인 네트워크인 비트코인이나 EOS의 경우는 C++로 주요 기능들을 개발했으며, 비트코인의 양대 산맥으로 칭해지는 가상화폐 네트워크인 이더리움의 경우에는 Go 언어를 기반으로 주요기능이 개발되었다. 비트코인의 기반기술로 활용되는 퍼블릭 블록체인 유형 외에 대표적인 유형으로는, 중앙집중형의 구조를 갖는 프라이빗 블록체인 유형과, 퍼블릭 블록체인과 프라이빗 블록체인의 특성을 일부 결합한 구조를 갖는 반 중앙 집중형 구조의 컨소시엄 블록체인 유형이 있다.

블록체인 기술 및 분산원장 기술은 2016년 9월 신설된 국제 표준 제정기

구 ISO/TC 307에서 표준화 하고 있다. 설립 당시 블록체인 전문용어 표준화를 위한 워킹그룹(WG)을 수립하고, 5개의 연구그룹(SG)을 결성하였다(이경남 2018). 이후 ISC/TC 307은 주요 블록체인 이슈를 분야별로 나눠서 집중적으로 다루기 위해 3개의 워킹그룹과 3개의 연구그룹으로 재편하였으며, 제3차 정례회의에서는 ISO/IEC JTC 1/SC 27(IT Security techniques)과 공동 워킹그룹(JWG 1)을 설립하기로 결의한 바 있다(정보통신기술진흥센터 2018).

워킹그룹과 연구그룹은 필요에 의하여 재편되며, 회원국의 합의에 의하여 설립·폐지되거나, 연구그룹을 통합하여 워킹그룹으로 전환한다. 현재 ISO/TC 307의 구조는 〈표 1〉와 같다.

〈표 1〉 ISO/TC 307의 워킹그룹 (2018.11. 기준)

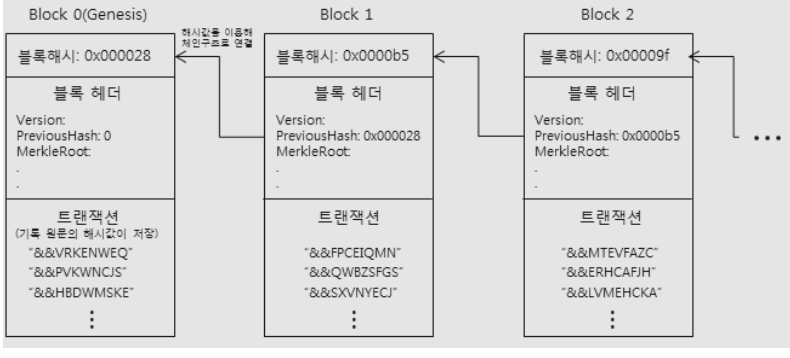
· CAG 1	컨퍼런스 조정 그룹
· JWG 4	ISO/IEC JTC 1/ SC 27 공동 WG : 블록체인, 분산원장기술 및 IT 보안기술
· SG 2	활용 사례 연구
· SG 6	블록체인 및 분산원장기술 시스템의 거버넌스
· SG 7	블록체인 및 분산원장기술 시스템의 상호 운용성
· WG 1	토대
· WG 2	보안, 정보 보호 및 식별
· WG 3	스마트 계약과 어플리케이션
· WG 5	거버넌스

워킹그룹들은 현재 총 11개의 표준을 개발 중이며, ISO/CD 22739(용어), ISO/CD TR 23455(블록체인 및 분산원장 기술 시스템의 스마트계약 개요 및 상호작용) 두 개의 표준은 현재 위원회 초안(CD) 등록단계이고, 이외의 9개 표준은 개발 시작단계 혹은 초기단계로, 전체 보고서 배포 단계까지 개발되어 게시되어 있는 표준은 아직 없다. 현재 개발 중인 표준 중에서 본 연구와 직접적인 연관이 있는 부분은 보안 이슈와 관련된 표준인 보안위험 및 취약점(ISO/NP TR 23245), 블록체인 시스템 개발과 관련된 표준인 참조 아키텍처(ISO/NP AWI 23257) 정도로 파악된다.

2) 블록체인의 구조

블록체인은 명칭에서 알 수 있듯이, 연결된 블록(chained-block)의 형태로 구성된다. 〈그림 1〉은 블록체인의 구성도를 개념적으로 나타낸 것이다. 블록은 크게 블록헤더와 트랜잭션 두 부분으로 구성되어 있다. 블록헤더는 여러 정보가 담겨있는데, 통상적으로 이전 블록헤더의 해시값을 포함한 6가지 정보를 핵심으로 본다. 트랜잭션은 해당 블록에 저장되는 주요 정보를 담고 있으며, 하나의 블록에는 여러 개의 개별 트랜잭션이 존재할 수 있다. 블록체인 네트워크상에서 첫 번째 블록은 이전 블록이 존재하지 않기 때문에 이전 블록 헤더의 해시값이 없으며, 이를 제네시스 블록(Genesis Block)이라 한다. 이후 생성되는 블록은 블록헤더에서 이전 블록의 해시값을 받아와 포함시킴으로써 앞의 블록을 가리키게 되고, 이 작업이 반복되면서 체인구조가 형성된다. 블록체인의 구조를 자세히 살펴보면 각각은 다음과 같은 구성을 가지고 있다.

〈그림 1〉 블록체인의 구조



(1) 블록헤더

앞서 언급한 바와 같이, 블록헤더 필드는 통상적으로 버전, 이전 블록 해

시, 머클 루트 해시, 타임스탬프, 난이도, 결과값(nonce) 총 6개의 정보로 구성된다. 버전은 해당 블록헤더의 버전 정보를 담고 있으며, 소프트웨어나 프로토콜 등의 업그레이드를 이력을 추적하기 위해 사용된다. 이전 블록 해시는 블록체인 내에서 바로 이전 블록의 해시값을 담고 있다. 머클 루트의 해시는 해당 블록의 머클트리[1](Merkle Tree) 구조에서 루트(Root)의 위치에 해당하는 해시값을 담고 있다. 머클트리에는 블록의 개별 트랜잭션들의 해시값이 담겨 있으며, 이 해시값들을 다시 해시하는 작업을 반복해 최종적으로 나오는 해시값이 루트 해시값이다. 타임스탬프는 해당 블록이 생성된 시점의 정보를 담고 있으며, 난이도는 블록의 채굴과정에서 필요한 작업 증명(PoW)의 목표 난이도 정보를 담고 있다. 결과값(nonce)은 채굴과정의 작업 증명에서 사용되는 값으로, 해당 블록을 채굴하기 위한 값을 담고 있다.

〈그림 2〉 Bitcoin-Core 소스코드 중 블록헤더 관련 코드

```
UniValue blockheaderToJSON(const CBlockIndex* blockindex)
{
AssertLockHeld(cs_main);
UniValue result(UniValue::VOBJ);
result.pushKV("hash", blockindex->GetBlockHash().GetHex());
int confirmations = -1;

// Only report confirmations if the block is on the main chain
if (chainActive.Contains(blockindex))
confirmations = chainActive.Height() - blockindex->nHeight + 1;

result.pushKV("confirmations", confirmations);
result.pushKV("height", blockindex->nHeight);
result.pushKV("version", blockindex->nVersion);
result.pushKV("versionHex", strprintf("%08x", blockindex->nVersion));
result.pushKV("merkleroot", blockindex->hashMerkleRoot.GetHex());
result.pushKV("time", (int64_t)blockindex->nTime);
result.pushKV("mediantime", (int64_t)blockindex-
>GetMedianTimePast());
result.pushKV("nonce", (uint64_t)blockindex->nNonce);
result.pushKV("bits", strprintf("%08x", blockindex->nBits));
result.pushKV("difficulty", GetDifficulty(blockindex));
result.pushKV("chainwork", blockindex->nChainWork.GetHex());
result.pushKV("nTx", (uint64_t)blockindex->nTx);
if (blockindex->pprev)
result.pushKV("previousblockhash", blockindex->pprev-
>GetBlockHash().GetHex());
CBlockIndex *pnext = chainActive.Next(blockindex);
if (pnext)
result.pushKV("nextblockhash", pnext->GetBlockHash().GetHex());
return result;
}
```

```
CBlockHeader GetBlockHeader() const
{
CBlockHeader block;
block.nVersion = nVersion;
if (pprev)
    block.hashPrevBlock = pprev->GetBlockHash();
block.hashMerkleRoot = hashMerkleRoot;
block.nTime = nTime;
block.nBits = nBits;
block.nNonce = nNonce;
return block;
}
-----------------------------------------------------------------
uint256 CBlockHeader::GetHash() const
{
return SerializeHash(*this);
}

std::string CBlock::ToString() const
{
std::stringstream s;
s << strprintf("CBlock(hash=%s, ver=0x%08x, hashPrevBlock=%s,
hashMerkleRoot=%s, nTime=%u, nBits=%08x, nNonce=%u,
vtx=%u)₩n",
GetHash().ToString(),
nVersion,
hashPrevBlock.ToString(),
hashMerkleRoot.ToString(),
nTime, nBits, nNonce,
vtx.size());
for (const auto& tx : vtx) {
s << "  " << tx->ToString() << "₩n";
}
return s.str();
}
```

1) 머클트리(Merkle Tree)는 해시트리(Hash Tree)라고도 불리며, 1979년 Ralph Merkle이 고안한 개념이다. 빠른 검색을 목적으로 하는 다른 트리 알고리즘과 다르게, 머클트리는 데이터의 간편하고 확실한 인증을 목적으로 한다. (머클트리(merkle tree)란?(2018). Retrieved September 5, 2018 from https://steemit.com/kr/@brownbears/merkle-tree)

〈그림 2〉는 비트코인 코어의 소스코드 중 블록 헤더와 연관된 코드들이다. 좌측의 코드는 블록체인 네트워크에서 블록헤더를 생성할 때 값을 불러와 입력하는 코드로, 여러 코드 사이에 핵심정보로 언급한 버전(version), 머클루트(merkleroot), 타임스탬프(time), 결과값(nonce), 난이도(difficulty), 이전블록해시(previous block hash)를 불러오는 코드가 있음을 확인할 수 있다. 우측 위의 그림은 블록헤더를 생성하는 소스코드로, 핵심정보 다섯 가지가 포함된 것을 확인할 수 있으며, 'Bits'는 증명의 난이도를 조정하는 값으로 'difficulty'와 같은 역할을 한다. 우측 아래의 코드에서는 각 정보의 출력값의 유형을 통해 어떤 유형으로 정보가 입력되는지를 확인할 수 있다. 버전과 Bits는 부호가 없는 16진수 정수 유형(%x)이고, 타임스탬프와 값은 부호가 없는 10진수 정수 유형(%u)이다. 해시값이 들어가는 항목은 전부 문자열 유형(%s)으로 선언되어 있음을 알 수 있다.

블록헤더의 정보에는 블록에 포함된 트랜잭션 머클루트 해시값이 포함되어 있기 때문에, 만약 해당 블록 내 트랜잭션이 추가되거나 수정되는 등 변화가 생기면 이에 따라 머클루트 해시값도 변경되고, 결과적으로 블록헤더에 입력된 해시값 정보가 변형된다. 블록체인은 이전 블록의 헤더에 입력된 해시값을 이용해 연결하는 구조이기 때문에, 이 경우 다음 블록이 가리키는 이전 블록의 해시값과 현재 블록의 해시값이 달라져 체인 구조가 붕괴된다. 이러한 구조적 특성으로 인해 블록체인은 현재상태가 문제없이 유지되고 있다는 사실 자체만으로도 블록 내 트랜잭션에 아무런 위변조가 가해지지 않았음을 증명할 수 있다.

(2) 트랜잭션

트랜잭션은 정보를 담아내어 저장하는 것으로, 블록체인의 구성요소 중 핵심이다. 블록체인은 트랜잭션을 안전하게, 그리고 신뢰할 수 있는 방식으로 저장하는 것을 목적으로 만들어진 구조로, 트랜잭션은 한 번 생성되면

수정할 수 없도록 만들어진다. 트랜잭션은 기본적으로 입출력의 구조를 가지고 있으며, 비트코인에서는 거래정보를 입력하여 주고받는 용도로 활용된다. 하나의 트랜잭션은 여러 개의 입력값과 출력값을 가질 수 있으며, 하나의 트랜잭션 내의 입력값은 출력값에 반드시 연결되지 않아도 되지만, 출력값은 반드시 입력값과 연결되어 있어야 한다. 출력값은 반드시 목표지점인 트랜잭션의 입력값을 가지고 있어야 생성되기 때문이다.

〈그림 3〉은 비트코인 코어의 코드 중 트랜잭션의 입출력 구조와 관련된 코드와 트랜잭션에 입력되는 정보와 관련된 코드이다. 트랜잭션의 입력(좌 상단)에서는 연결된 이전 트랜잭션의 출력값 prevout과, 트랜잭션 출력(좌 하단) 시 퍼블릭 키의 값으로 사용되는 scriptSig를 확인할 수 있고, 트랜잭션의 출력에서는 트랜잭션이 가지고 있는 정보값이 입력되어 있는 Value와, scriptSig에서 입력받아 저장되어있는 암호로 값을 잠그는 scriptPubKey를 확인할 수 있다. Value에 입력되는 값(우 하단)을 확인해보면 정수형(%d) 값을 입력받고 있음을 알 수 있다. 트랜잭션의 정보를 출력부에 담아 출력할 때에는, 입력부에서 저장한 암호를 사용해 그 값을 잠근다. 비트코인 트랜잭션은 담고 있는 정보값(Value) 외에도 여러 값을 담고 있는데(우 상단), 받는 이의 주소값(addrTo), 보낸 이의 주소값(addrFrom), 결과값(nNonce) 등이 해당된다.

〈그림 3〉 Bitcoin-Core 소스코드 중 트랜잭션 관련 코드

```
CTxIn::CTxIn(COutPoint prevoutIn, CScript
scriptSigIn, uint32_t nSequenceIn)
{
prevout = prevoutIn;
scriptSig = scriptSigIn;
nSequence = nSequenceIn;
}
```

```
CTxOut::CTxOut(const CAmount& nValueIn,
CScript scriptPubKeyIn)
{
nValue = nValueIn;
scriptPubKey = scriptPubKeyIn;
}
```

```
class msg_version:
self.nVersion = MY_VERSION
self.nServices = NODE_NETWORK | NODE_WITNESS
self.nTime = int(time.time())
self.addrTo = CAddress()
self.addrFrom = CAddress()
self.nNonce = random.getrandbits(64)
self.strSubVer = MY_SUBVERSION
self.nStartingHeight = -1
self.nRelay = MY_RELAY
```

```
std::string CTxOut::ToString() const
{
return strprintf("CTxOut(nValue=%d.%08d,
scriptPubKey=%s)", nValue / COIN, nValue % COIN,
HexStr(scriptPubKey).substr(0, 30));
}
```

블록체인 구조의 소스코드 분석을 통해 도출되는 시사점은 다음과 같다. 첫째, 블록체인 구조는 새롭게 만들어진 구조가 아니다. 블록체인의 구조는 '링크드 리스트'의 구조와 비슷하다. 그렇기 때문에 새롭게 등장한 기술임에도 불구하고 그 구조는 기존의 기술에 대한 분석을 통해 더 쉽게 접근할 수 있다. 둘째, 블록체인의 구조를 용도에 맞게 사용하기 위해 코드를 추가하거나 변화시켜야 하는 부분을 유추해낼 수 있다. 예를 들어 트랜잭션의 아웃풋 부분의 코드에 정보가 입력되는 Value에 문자열 유형을 입력할 수 있도록 설정해, 비트코인의 화폐를 저장하는 부분을 중요한 기록정보를 저장하는 공간으로 활용할 수 있을 것이다. 또한 블록의 헤더에 여러 추가적인 정보를 저장할 수도 있을 것이다. 이러한 시사점은 거래정보의 관리가 아닌 기록관리를 목적으로 블록체인 기술을 커스터마이징 할 때, 기록관리에 필요한 요소에 맞도록 블록을 설계할 수 있음을 보여준다.

3) 블록체인의 유형

블록체인의 유형은 블록체인의 구조와 형태를 기준으로 나눌 수 있다. 가장 대표적인 구조적 선형적 구조이다. 최초의 블록인 제네시스 블록에서 시작하여 블록이 생성되는 순서대로 이어지는 구조이다. 블록체인 기반의 전자문서를 생산하는 환경을 구축하는 데에 관심이 모이면서 선형구조에서 파생되어 등장한 개념인 다차원 구조[2] 역시 꾸준히 연구되었다. 선형구조를 기본으로 하지만, 기존의 1차원적 선형구조의 개념에서 탈피해 2차원의 선형구조로 메인 체인과 서브 체인의 개념으로 구분해내고, 이를 3차원의 병렬형 구조로 확장해 낸 것이 다차원 구조이다, 구조의 특성상 폴더 혹은 철의 개념을 적용할 수 있다는 장점이 있지만, 그와 동시에 동기화 시간의 지연, 방대한 크기의 스토리지 요구 등의 문제점 역시 존재한다. 그 외에도 27개의 블록으로 큐브 구조를 만들고, 그 큐브를 체인으로 연결시키는 구조의 큐브체인[3] 등, 다양한

2) 문서를 위한 다차원 블록체인 만들겠다. https://www.bloter.net/archives/305153 (원문 확인 2018.09.05 17:34)

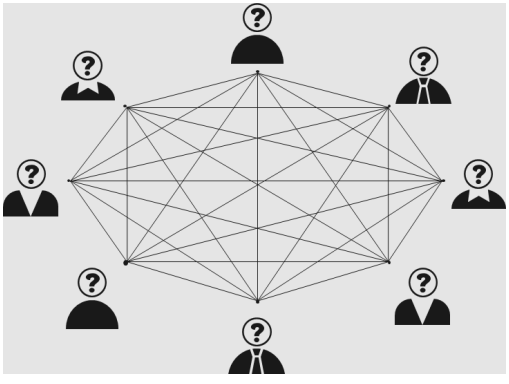
시도들을 통해 새로운 구조의 블록체인이 개발되고 있다.

큰 틀에서 블록체인의 형태는 퍼블릭 블록체인(Public BlockChain) 유형, 프라이빗 블록체인(Private BlockChain) 유형, 컨소시엄 블록체인(Consortium BlockChain) 유형 세 종류로 구분할 수 있다. 각 유형은 고유의 특징을 가지고 있으며, 유형마다 기능 및 구조가 조금씩 다르다.

(1) 퍼블릭 블록체인(Public BlockChain)

퍼블릭 블록체인 유형은 흔히 알려진 비트코인의 기반기술이 되는 유형으로, 지금까지 연구되고 있는 블록체인에 관한 연구의 상당수가 퍼블릭 블록체인 유형을 활용하기 위한 연구이다. 퍼블릭 블록체인은 탈중앙화 된 분산 시스템으로, 불특정 다수의 참여자들이 시스템 상에서 발생하는 트랜잭션을 공유하고 상호 검증하는 구조이다. 공개형 블록체인으로 별도의 관리주체가 존재하지 않으며, 누구나 익명으로 참여할 수 있고, 권한에 제한이 없다. 또한 전체 트랜잭션 정보를 참여자 모두가 공유한다.

〈그림 4〉 퍼블릭 블록체인의 구조



3) 큐브체인, 4세대 블록체인. https://www.cubechain.io/cubechain/ (원문확인 2018.11.15 14:22)

퍼블릭 블록체인은 금융 분야에서 활발히 연구되고 있는 유형으로 분산원장기술이 핵심이며, 제3의 신뢰기관을 두지 않고도 인증절차를 수행할 수 있다는 점에서 금융거래분야 뿐만 아니라, 운송 등의 분야에서도 효과적으로 활용될 가능성을 보이고 있다.

기록관리의 측면에서 퍼블릭 블록체인 유형을 살펴보면, 기록은 그 생산자가 식별되고 권한이 부여되어야 하지만, 퍼블릭 블록체인은 특별한 자격 없이 누구나 익명으로 참여할 수 있기 때문에 기록의 출처나 신뢰성의 측면에서 취약성을 가질 수 있다. 또한 별도의 접근권한이 존재하지 않아 누구나 트랜잭션의 정보를 읽을 수 있기 때문에, 누가 누구에게 무엇을 전송했다는 사실이 공개된다는 점에서 정보 프라이버시와 기밀유지 또한 낮을 수 있다. 하지만 보안의 측면에서는 다수의 참여자가 공동으로 원장을 거치는 구조이기 때문에, 내부 관계자가 임의로 특정 기록을 조작하는 것은 불가능하다는 점에서 높은 무결성을 가질 수 있다. 퍼블릭 블록체인은 기록관리에 적용 시 여러 측면에서 장단점이 각각 있지만, 구조적 특성상 기록관리에 적용하여 활용하기에는 쉽지 않은 유형임을 알 수 있다. 만약 높은 보안성을 염두에 두고 기술을 활용한다면, 공공저작물 관련 기록과 같은 특수한 유형의 기록관리에 한해 효과적으로 활용할 수 있을 것이다.

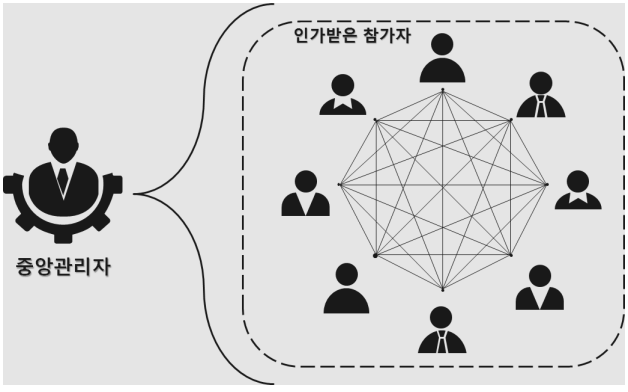
(2) 프라이빗 블록체인(Private BlockChain)

프라이빗 블록체인 유형은 중앙형 블록체인으로, 중앙집중형 구조에 보안성을 강화하기 위한 방안으로 블록체인 기술을 접목 도입한 유형이다. 퍼블릭 블록체인과 달리 관리주체가 존재하며, 하나의 관리주체가 독자적으로 운영하는 구조이다. 네트워크상에서 만든 인증방식을 통해서 검증된 대상만이 참여할 수 있는 구조이며,[4] 트랜잭션에 접근하기 위해 참여자들

4) 출처 : 퍼블릭 블록체인(Public Blockchain) vs 프라이빗 블록체인(Private Blockchain) https://tokenpost.kr/terms/5822 (원문확인 2018.09.05. 17:44).

은 각각 적절한 권한을 부여받아야 한다. 또한 트랜잭션 유형 및 상호간 합의에 따라 트랜잭션 인장의 공개대상을 결정한다. 주로 기업에서 보안성 강화를 목적으로 개발하여 사용하는 유형이다.

〈그림 5〉 프라이빗 블록체인의 구조

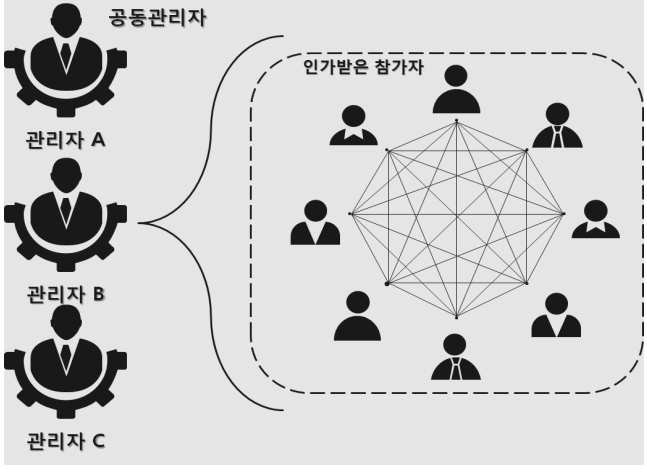


기록관리 측면에서 프라이빗 블록체인 유형을 살펴보면, 단일주체에 의해서 관리가 이루어지기 때문에 기록의 출처와 신뢰성이 높고, 트랜잭션별로 권한설정 및 부여가 가능하므로, 관계자들에게만 트랜잭션 내역을 공개할 수 있어 정보 프라이버시도 높다. 그러나 중앙관리자에 의해 운영되는 블록체인이기 때문에 투명성이 낮을 수 있다는 단점을 갖고 있다. 프라이빗 블록체인 유형은 기록관리에 충분히 활용할 가능성이 있음을 파악할 수 있다. 특히 트랜잭션 별로 권한설정 및 부여가 가능하다는 점에 주목하면, 클라우드 기록관리시스템 환경에서 권한설정의 변경을 통해 특정 기록에 대한 접근권한을 조정하는 방식을 이용하여 이관 프로세스를 대신할 가능성이 있다. 하지만 중앙관리에 의해 투명성이 낮을 수 있다는 단점이 있기 때문에, 이를 보완할 수 있는 방안을 마련해야 한다.

(3) 컨소시엄 블록체인(Consortium BlockCahin)

컨소시엄 블록체인은 어떤 사용자에게는 블록체인의 전체 또는 일부를 보는 것만 허용하나, 어떤 사용자에게는 새 블록을 추가할 수 있는 권한까지 부여하는 등 블록체인에서 사용자에게 할당되는 허가수준을 달리하는 블록체인이다(국회도서관 2018). 여러 기관들이 공동주체가 되어 구성하는 반 중앙형 블록체인으로 프라이빗 블록체인과 같이 인가 받은 대상만 참여할 수 있으며, 각각에 대한 권한이 존재하며, 트랜잭션 유형 및 상호간의 합의에 따라 트랜잭션 인장 공개대상을 결정한다. 컨소시엄 블록체인에서는 공동주체 기관이 합의한 규칙에 따라 원장이 이루어진다.

〈그림 6〉 컨소시엄 블록체인의 구조



기록관리 측면에서 컨소시엄 블록체인 유형을 살펴보면, 프라이빗 블록체인과 동일하게 관리주체가 존재해 기록의 출처와 신뢰성이 높으며, 마찬가지로 권한설정 및 부여가 가능해 트랜잭션 내역에 대한 프라이버시가 높

다. 그리고 프라이빗 블록체인과 다르게 한 조직의 관리자가 임의로 특정 기록을 조작하기가 매우 어렵다는 점에서도 기록의 신뢰성이 높다고 볼 수 있다.

하지만 공동주체가 동일한 권한을 갖고 합의과정이 필요하다는 점에서 운영주체가 조직 위계상 동일선상에 위치하는 기관들로 구성되어야 하므로, 전체 기록관리 프로세스에 적용시키기는 어렵다. 그렇기 때문에 다른 유형의 블록체인과 적절하게 융합하거나 병행하여 활용하는 방안으로 모색해 볼 필요성이 있다.

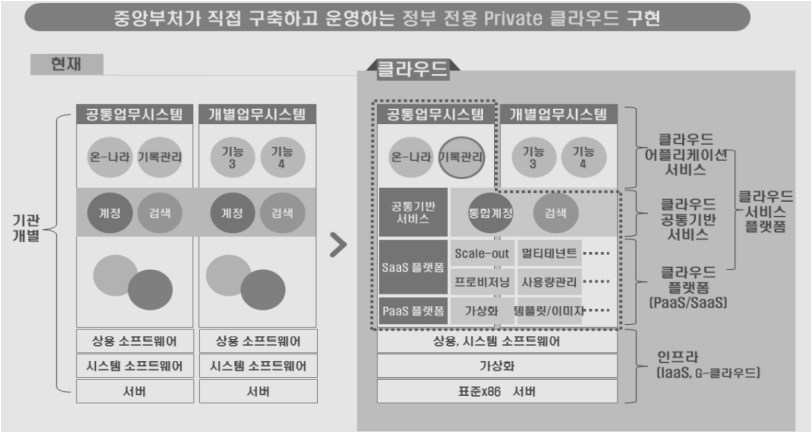
컨소시엄 블록체인 유형은 앞서 언급한 프라이빗 블록체인 유형의 활용 방안과 같은 맥락에서의 가능성을 가지고 있으며, 프라이빗 블록체인과 컨소시엄 블록체인 두 유형을 적절히 융합하여 활용한다면 향후 다가올 전자기록관리 환경의 변화에 맞춰 커스터마이징 된 구조의 블록체인을 구상해 볼 수 있다.

3. 기록관리 프로세스 및 시스템 분석

1) 기록관리 프로세스

앞서 블록체인 기술을 구체적으로 살펴본 것에 이어서, 이 장에서는 국가기록원에서 올해 발행하여 배포한 2018년도 기록물관리지침(국가기록원 2018)에 명시된 기록물관리 프로세스를 분석한다. 분석을 통해 클라우드 기반 기록관리시스템으로의 변화에 맞게 개선되어야 하는 핵심 프로세스를 도출하고, 각 프로세스에서의 블록체인 기술 활용 가능성을 파악한다. 또한 표준 기록관리시스템의 기능을 통해 앞서 도출한 핵심 프로세스가 실제로 어떻게 활용되고 있는지를 살펴본다.

〈그림 7〉 클라우드 RMS 개념도



※출처 : 중앙부처 기록물, 범정부 공동활용 길 열린다. 행정안전부 보도자료, 2018.8.

국가기록원은 중앙부처 기록물을 범정부 차원에서 공동·활용하는 클라우드 기록관리시스템(CRMS)을 지난 2016년 개발한 데 이어, 지난해 15개 부처를 전환하였고, 올해 27개의 중앙부처를 추가해 내년 1월까지 총 43개 부처의 전환을 마치고 범정부 단일 시스템을 운영한다고 밝혔다(국가기록원 2018). CRMS는 현재 각 부처별로 구축하여 운영하고 있는 기록관리시스템(RMS)을 클라우드 기반으로 통합한 것이다.

〈그림 7〉은 행정안전부 보도자료 내에 소개된 클라우드 RMS의 개념도이다. CRMS의 소프트웨어는 중앙부처가 공동으로 사용하며, 현재 기관별로 구축 및 운영중인 하드웨어와 소프트웨어를 클라우드 서버로 통합하여 구축, 관리 및 운영한다. 2016년 행정안전부를 시작으로, 2017년에는 고용노동부, 국토교통부, 공정거래위원회 등을 포함한 15개 기관이 전환하였으며, 2018년에는 국무총리비서실, 국무조정실, 기획재정부, 감사원 등을 포함한 27개 기관이 전환하는 것을 목표로 하고 있다(행정안전부 2018). 클라우드 기록관리시스템 환경에서는 중앙부처가 스토리지를 공유한다. 스토리지를

공유하게 되면 가장 문제가 되는 것은 보안이다. 클라우드 기술 자체만으로도 보안과 관련된 이슈들을 심심치 않게 볼 수 있다. 그렇기 때문에 보안은 클라우드 기록관리시스템에 있어서 필수적인 기능요건에 해당한다. 블록체인 기술은 기술 자체가 신뢰성, 무결성, 진본성을 기반으로 하는 구조를 갖추고 있기 때문에 그 자체적으로도 뛰어난 보안성을 갖고 있으며, 블록체인 네트워크를 구축함으로써 네트워크 참여기관 간의 상호 감시통제를 가능하게 하고, 이를 통해 보안성의 향상을 기대할 수 있다.

국가기록원에서 발행 및 배포한 2018년도 기록물 관리지침에서는 크게 처리과의 기록물관리와 기록관의 기록물관리로 구분하여 생산, 관리 과정의 프로세스와 각 프로세스별 지침을 설명하고 있다.

처리과의 기록물관리 장에서는 기록물의 생산, 등록, 분류, 정리 프로세스와 유형별 관리, 개인정보가 포함된 기록물 관리, 기록물 생산현황 통보 및 이관 프로세스에 대해 설명하고 있다. 이 중 클라우드 기록관리시스템으로 전환하였을 경우 개선이 필요한 프로세스는 기록물 생산 이후의 과정인 생산현황통보 및 이관 프로세스이다. 두 프로세스 모두 하나의 스토리지를 공유하는 구조에서는 그 기능의 효용성을 검증해야 한다. 블록체인 기술을 활용하면 앞서 언급한 것처럼 두 프로세스를 대체할 수 있다.

기록관의 기록물관리 장에서는 기록물의 인수, 전자기록물의 보존포맷 변환·관리, 영구기록물관리기관으로의 이관, 특수기록관 비공개기록물 이관 연장, 공개재분류, 기록물의 평가 및 폐기 프로세스에 대해 설명하고 있다. 기록관의 기록물관리 프로세스는 대부분 연계를 필요로 하는 프로세스이다.

기록물의 인수는 처리과와 연계가 필요한 프로세스이며, 영구기록물관리기관으로의 이관 역시 영구기록물관리기관과 연계가 필요하다. 비공개기록물 이관 연장, 기록물의 평가 및 폐기 프로세스는 유관기관이나 심의회와 연계가 필요한 프로세스이며, 공개재분류 프로세스도 필수사항은 아니지만 심의회를 구성할 수 있기 때문에 연계가 필요한 프로세스라 볼 수 있다. 클라우드 기록관리시스템은 연계시스템이 통합된 구조이기 때문에, 이러한

연계절차는 간소화 되거나 다른 적절한 프로세스로 대체되어야 한다.

또 하나 눈여겨 볼 프로세스는 보존포맷 변환·관리 프로세스이다. 보존포맷 변환은 전자기록을 장기적으로 보관하기 위해 수행하는 프로세스로, 문서보존포맷 변환과 장기보존포맷 변환이 이에 해당된다. 하나의 스토리지를 통합하여 사용하는 클라우드 기록관리시스템 환경에서 보존을 위한 포맷변환이 어떤 의미를 갖는지에 대한 고민이 필요하다. 또한 블록체인 기술을 도입하여 포맷변환을 간소화하거나 대체할 수 있는 방법이 있는지를 고민해야 한다.

2) 블록체인 기술의 구조적 특성 활용

(1) 보안

현행 기록관리시스템은 기관마다 개별적으로 하드웨어 및 소프트웨어 환경을 구축하여 사용한다. 기관 간의 정보소통은 수동적으로 이루어지기 때문에 각 기관이 관리하고 있는 스토리지의 보안에 대한 문제는 개별기관 단위에서 대응하고 해결하는 수준의 문제이다. 그러나 클라우드 기록관리시스템 환경에서는 이러한 시스템이 통합운영 되면서, 여러 부처의 협업사업인 경우 공동결재 기록으로 공동관리가 가능하고, 타 부처가 생산 및 관리하고 있는 기록물도 공개기록물인 경우는 검색과 공동 활용이 가능한 구조가 될 것임을 기대하고 있다(행정안전부 2018). 이러한 환경에서 보안은 매우 중요한 문제가 된다.

클라우드 환경에서는 스토리지가 물리적으로 구분되지 않기 때문에, 특정 기록에 대한 접근권한을 시스템적으로 통제하고 관리한다 하더라도 접근권한이 없는 기록이 접근할 수 있는 기록과 같은 스토리지에 존재한다는 사실은 변함이 없다. 만약 스토리지의 보안에 문제가 발생한다면, 단순히 하나의 기관의 문제가 아닌 클라우드 스토리지를 공유하는 43개 기관 전체

의 문제가 된다. 문제의 규모가 커짐에 따라 피해의 규모도 확대되며, 이는 단일기관에서 해결할 수 없는 문제이기에 장기화 될 가능성도 있다. 그렇기 때문에 클라우드 환경의 스토리지에서는 개별 기록에 대해 접근권한을 부여하는 것에 각별히 신경 써야하며, 완전한 보안에 대해 끊임없이 고민해야 한다.

클라우드 스토리지에서 보안이슈를 해결하는 방법도 있지만, 블록체인 기술의 특성을 활용하여 보안이슈를 해결하는 방법도 있다. 블록체인 유형 중 프라이빗 블록체인 유형은 참여자들이 각각 정보에 대한 접근권한을 중앙 관리자로부터 부여받는다. 프라이빗 블록체인 기술은 기업형 블록체인이라고도 불리우며, 기존 중앙관리 방식에 보안성을 개선하기 위한 목적으로 도입된다(고윤승, 최홍섭, 2017). 이런 특징을 기반으로 프라이빗 블록체인을 활용하여 스토리지 접근권한을 원격으로 통제하는 방식을 구상해볼 수 있다.

(2) 보존포맷 변환 · 관리

기록물관리기관이 처리과로부터 인수한 기록물 중 보존기간이 10년 이상인 기록물은 문서보존포맷으로 변환해야 한다. 문서보존포맷 변환대상은 전자기록물 건에 포함된 본문문서 및 첨부파일이다. 문서형식이 아닌 시청각 유형이나 압축파일, PDF 파일 등은 변환 대상에서 제외되며, 암호화 파일, 손상파일 등 가독이 불가능한 파일도 변환 대상에서 제외된다. 장기보존포맷 변환 대상은 모든 기록물의 철과 건이다.

장기보존 포맷은 문서자체의 보존뿐만 아니라 설명정보 등을 포함하고 기록물과 관련된 정보들을 영구적으로 보존하고 유지하기 위해 XML 형식으로 인캡슐레이션 하는 것으로, 전자문서의 경우 문서보존포맷으로 마이그레이션한 뒤 이를 원본 및 설명정보와 함께 다시 인캡슐레이션 하므로 양파모델이라고도 불린다. 두 번의 포맷변환 과정에서 XML 파일은 원본파

일에 비해 약 3배 정도 큰 용량을 가지게 되며, 이는 스토리지의 낭비를 초래한다.

최근에는 XML 형식의 장기보존포맷을 대체하기 위한 포맷으로 BagIt 포맷을 사용하는 방법을 검토한 사례가 있다(서울시 2016). BagIt은 해시 알고리즘을 활용한 무결성 검증기술을 활용한 포맷으로, 자체적인 압축기술을 활용한다. Base64 기반의 인코딩 기술을 활용하기 때문에 자체 뷰어를 별도로 개발할 필요가 없고, 기존의 XML 변환 포맷인 NEO에 비해 기술종속성 이슈에서 자유롭다(서울시 2016). 여기서 주목할 점은, Bagit이 해시알고리즘을 활용한 무결성 검증기술을 활용한 포맷이라는 점이다. 블록체인은 해시알고리즘을 활용해 체인으로 연결되는 구조를 가지고 있으며, 트랜잭션의 무결성을 머클루트 해시알고리즘을 통해 검증한다. 이러한 부분에서 접점을 찾아볼 수 있으며, BagIt 포맷을 사용하기 위한 기술을 블록체인 모듈로 구현하는 방법을 구상해볼 수 있다.

3) 프로세스 통합 및 간소화

(1) 생산현황통보

전자문서의 생산현황통보는 매년 5월31일 실시되며, 전년도에 생산된 기록물 생산현황을 '기록물 생산현황 통보 서식'에 따라 작성하여 각급 기록관에 통보하도록 되어있으며, 비밀기록물의 경우 전년도에 생산한 비밀기록물 원본의 통계를 기록물 유형별 비밀등급별, 보존기간별, 보호기간별로 구분하여 작성하도록 되어있다.

국가기록원에서 개정 배포한 2018년도 기록물 생산현황 통보 지침에 따르면, 기존 15개 서식에서 감소된 12개의 서식을 사용하여야 하며, 일반기록물, 조사 · 연구 · 검토보고서, 회의록, 시청각기록물, 비밀기록물, 간행물 생산현황과 행정박물 보유목록을 통보하도록 지침하고 있다(국가기록원

2018). 대부분의 서식은 앞서 나열한 유형들에 대한 생산현황과 보유목록이며, 2018년 개정을 통해 전년도 보유기록물 현황 총괄표 서식은 삭제되었다.

서식의 수가 12개로 감소되었지만, 문서류를 제외한 나머지 유형은 모두 사람이 직접 입력하는 수기 방식으로 통보되고 있어, 생산현황 통보를 위해 법정시한인 8월까지 제출서식을 수기로 채우는 데 대다수의 기록관이 업무역량을 집중하고 있다는 문제점을 가지고 있다(왕호성, 설문원, 2018). 차세대 전자기록관리 프로세스 재설계 연구에서는 생산현황통보 제도 자체를 불필요한 제도로 보며, 기록생산시스템 및 기록관리시스템의 통계정보와 중앙기록물관리시스템의 연계를 통해 생산현황 파악이 가능하고, 기술적으로 충분히 가능하다고 보고 있다(주현미, 임진희, 2017). 그러나 클라우드 기록관리 환경에서는 앞서 언급한 것처럼 생산현황통보 프로세스 자체의 효용성을 검증해야 한다.

기록을 관리하는 스토리지가 하나로 통합되어있기 때문에, 따로 생산현황을 통보하거나 요청할 필요 없이 현재 스토리지 내에 존재하는 기록 중에서 생산현황통보 제도상 명시된 기간범위에 생산된 기록물을 확인할 수 있도록 기능을 구현하는 것만으로 대체할 수 있다. 이러한 기능요건은 여러 방법으로 개발할 수 있겠지만, 블록체인 모듈을 통해서도 구현할 수 있다. 기록이 생산되어 스토리지에 저장되는 과정에서 일부 정보를 블록체인 네트워크로 송신하는 정도의 코드 구현으로 블록체인 네트워크 참여기관들이 실시간으로 생산현황을 모니터링하며 그 이력을 추적할 수 있다.

⑵ 이관

현행 기록물 관리지침에 따르면, 이관매체를 이용하여 전자기록물을 온·오프라인으로 이관하도록 되어있다. 이관을 위한 절차로는 '이관전용 PC 확보, 스토리지 용량 확보, RMS-CAMS 연계, RMS-전자서명인증센터 연

계, RMS-전자서명장기검증센터 연계, 인증서 현행화, WAS 교체' 를 제시하고 있다.

온라인 이관의 경우 기록물 이관이 완료되면 이관 완료된 전자기록물을 기록관리시스템에서 삭제처리 하도록 지침 되어있으며, 오프라인 인관의 경우 전자기록물 오프라인 인계 · 인수서를 발급하도록 지침 되어있다(국가기록원 2018).

처리과에서 기록물관리기관으로 이관하는 유형은 업무관리시스템(온-나라 시스템)에서 기록관리시스템으로 이관하는 유형과 기타 전자문서시스템에서 기록관리시스템으로 이관하는 유형 두 가지로 크게 구분할 수 있다. 업무관리시스템에서 이관을 하는 경우 기록관리시스템과 연계되어있기 때문에 시스템 내에서 이관절차를 수행할 수 있다. 이관요청과 이관승인처리 등 비교적 간단한 절차를 통해 이관이 완료된다. 전자문서시스템에서 이관을 하는 경우, 기록관리시스템에 이관을 위해 별도의 송수신 모듈이 필요하며, 이관파일을 접수한 뒤 이관파일의 규격 누락여부 확인, 이관파일 내 정보오류 확인, 이관파일의 정수 · 검수 및 인수 절차를 통해 이관이 완료된다. 업무관리시스템의 경우 기록관리시스템과 연계되어있지만 전자문서시스템의 경우 이관을 위해 별도의 송수신 모듈과 기타 문서검증절차가 필요하다.

하지만 이러한 복잡한 과정은 클라우드 기록관리시스템에서는 필수적인 프로세스가 아니게 된다. 통합 스토리지 내에서 이관 프로세스를 수행한다는 것은 하나의 큰 창고에 들어있는 상자를 창고 내 다른 칸으로 옮기는 것과 다르지 않다. 기록의 위치정보의 개념이 중요하지 않은 클라우드 스토리지 환경에서 이러한 프로세스는 반드시 필요하지 않다. 그렇기 때문에 클라우드 기록관리 환경에서는 이관 프로세스를 대체할 수 있는 기능이 마련되어야 한다. 이런 관점에서 블록체인 기술을 적용해보면, 블록체인 네트워크 참여자의 권한설정을 응용하여 기능을 구현해볼 수 있다. 블록체인 네트워크 참여기관의 블록에 대한 접근권한을 설정하면서 동시에 스토리지 기록물의 접근권한에 영향을 주는 구조로 구현을 시도해볼 수 있다.

4) 프로세스 효율화

〈그림 8〉 표준기록관리시스템 기능구성 일부

검색활용	검색	통합검색, 조건별검색, 분류체계검색, 기관간인수대상검색, 정부간행물검색, 행정박물검색	
	열람	열람신청, 기록물열람, 열람승인(기록관), 열람승인(처리과), 열람통계	
	통계	생산현황, 보유현황, 폐기현황, 이관현황, 공개구분현황, 이용현황	
기준관리	기록관리기준표	보존기간관리, 기록관리기준표고시	• 기능분류시스템 (중앙/지방/지방교육)
	기록물분류기준표	분류체계관리	
	기준정보	준칙기준관리,단위과제별기준작성	
접근 감사추적	접근관리	기록물철, 기록물건, 생산부서	
	감사추적	사용자별 추적, 기록물별 추적, 위치추적, 감사추적데이터문서화	
	검증현황	장기보존포맷검증현황	
시스템관리	시스템관리	사용자관리, 불법사용자차단, 메뉴관리, 메뉴권한그룹관리, 다운로드용PC관리	• 전자기록생산시스템 또는 업무포털 (사용자 정보 연계)
	환경설정	코드반영, 기록관환경설정	
	기록물관리	공개관리, 접근범위관리, 처리부서관리, 조직이력관리	
공개관리	공개관리	원문정보공개시스템 (기록물통합검색시스템: 미사용)	• 원문정보공개시스템
기록관현황	기록관현황	일반현황, 시설·장비현황, 기록물보유현황	

※출처 : 유영문(2018), 표준기록관리시스템(RMS)의 기능 현황 및 발전방향 p241 표 일부 인용.

〈그림 8〉은 표준기록관리시스템의 기능을 대·중·소 기능으로 구분하여 나열한 표의 일부이다. 기능현황에서 눈에 띄는 기능은 접근감사추적 기능과 기록관현황 기능이다. 접근 감사추적 기능은 처음 개발된 이후 개선이 거의 이루어지지 않은 상태로 활성화되어있지 않으며, 문서보안솔루션 등이 보완재로서 활용되고 있다(유영문 2018).

클라우드 기록관리 환경에서 접근감사추적은 기능을 별도로 두지 않고 하나의 모듈에서 해당 기능을 수행하도록 구현할 수 있다. 다시 말해, 하나

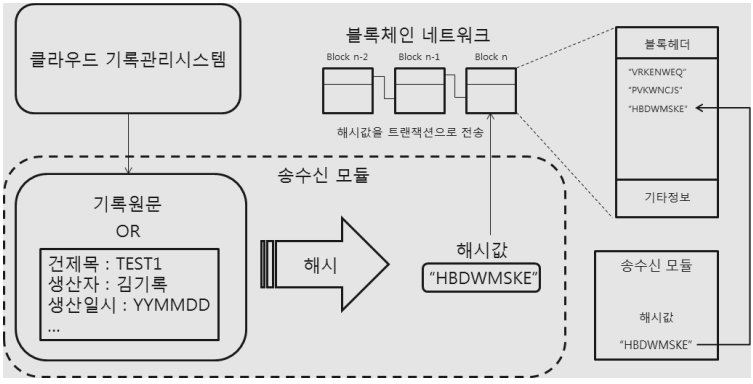
의 모듈이 작동하는 프로세스를 활용하여 여러 기능들을 구현할 수 있다. 클라우드 스토리지 내의 기록을 모니터링 할 수 있는 기능을 가진 모듈에 모니터링 된 기록에 대한 접근이력을 일정 간격으로 지정된 경로에 모아두는 기능을 추가 구현하면 모니터링과 접근, 감사추적을 하나의 모듈로 해결할 수 있을 것이다. 이는 앞서 제시한 생산현황통보의 변형 프로세스와 비슷한 기능을 갖는 기록관현황 기능에도 해당하는 사항이다. 이처럼 클라우드 기록관리 환경에서는 하나의 모듈이 여러 비슷한 기능을 수행하도록 구현하여 효율적인 프로세스를 구성할 수 있다.

4. 기록관리시스템 적용 블록체인 모델

1) 블록체인 기술 활용방안

앞에서는 클라우드 기록관리시스템 환경으로의 변화에 따라 개선되어야 할 현행 기록관리 프로세스들을 살펴보고, 각 프로세스의 개선에 블록체인 기술을 활용할 수 있는 방향에 대해 제시하였다. 서론에서 언급한 것처럼, 본고의 핵심은 모듈 방식으로 구현하여 현행 기록관리 프로세스의 여러 기능을 간소화 하거나 대체할 수 있는 블록체인 네트워크 모델을 제시하는 것이다. 모듈 형태의 블록체인 네트워크와 기록관리시스템이 연계되려면 한 가지 기능모듈의 구현이 전제되어야 한다. 바로 기록관리시스템과의 송수신 기능이다. 기록관리시스템에서 기록이 생성될 때, 기록의 원문 혹은 필요한 값을 추출하여 해시값으로 변환한다. 변환한 값을 블록체인 네트워크 모듈로 송신하면 블록체인 네트워크에서는 그 값을 수신 받아 트랜잭션으로 입력한다. 이러한 기능을 전제로 이번에는 앞서 살펴본 네 가지 프로세스의 개선에 구체적으로 어떤 부분에 블록체인 기술을 적용시켜 구현할지 살펴본다.

〈그림 9〉 송수신 모듈



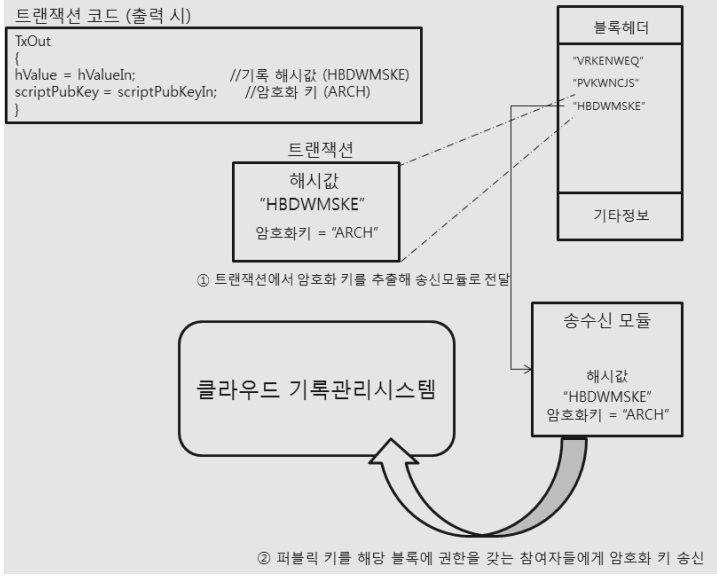
(1) 보안

블록체인 기술은 그 자체로 보안성이 상당히 뛰어나다. 하지만 블록 내에 기록원문을 트랜잭션으로 입력하여 관리하는 구조가 아니라면 기술 자체의 보안성을 활용할 수는 없다. 기본적인 보안은 클라우드 기록관리시스템이 구현된 G-클라우드 자체에서 그 이슈를 해결하고 있다. 하지만 추가적인 기능모듈구현을 통해 블록체인 네트워크를 활용하여 추가로 보안성을 향상시킬 수 있다.

블록체인 기술로 보안성을 높이기 위해 구현되어야 할 기능모듈은 '접근키'이다. 이는 2장에서 살펴본 트랜잭션의 '퍼블릭 키'개념에서 파생한다. 우선 송수신 기능을 활용해 기록의 해시값을 수신 받아 블록체인 네트워크의 트랜잭션에 입력한다. 이후, 트랜잭션에 입력된 값을 퍼블릭 키로 설정되어있는 암호로 잠근다. 트랜잭션의 값을 잠그는 데 사용된 퍼블릭 키를 해당 블록에 권한을 갖는 참여자들에게 송신한다. 네트워크 참여자가 클라우드 스토리지에 등록되어 있는 기록으로 접근을 시도할 때, 해당 블록의 해시값을 블록체인 네트워크로부터 수신 받은 퍼블릭 키 암호로 잠가 암호

화 된 트랜잭션의 형태로 블록체인 네트워크로 송신한다. 블록체인 네트워크는 참여자가 접근하려는 트랜잭션의 값을 수신 받은 암호값과 비교하여 일치할 경우 접근을 허용한다. 만약 해당 기록에 대한 접근권한이 없는 참여자가 접근을 시도했다면 두 값은 일치하지 않고, 해당 기록으로의 접근도 제한된다. 이와 같은 구조를 통해 기록에 대한 권한을 갖지 못하는 기관은 접근할 수 없도록 기록관리시스템과 블록체인 네트워크가 이중으로 통제하여 보안성을 높일 수 있다.

〈그림 10〉 접근키 모듈 이미지 및 코드



(2) 보존포맷 관리

보존포맷의 관리는 앞서 BagIt 기술의 구조가 블록체인 기술과 비슷한 형태를 띠고 있음을 확인하며 그 가능성을 파악하였으나, 현 시점에서 구현

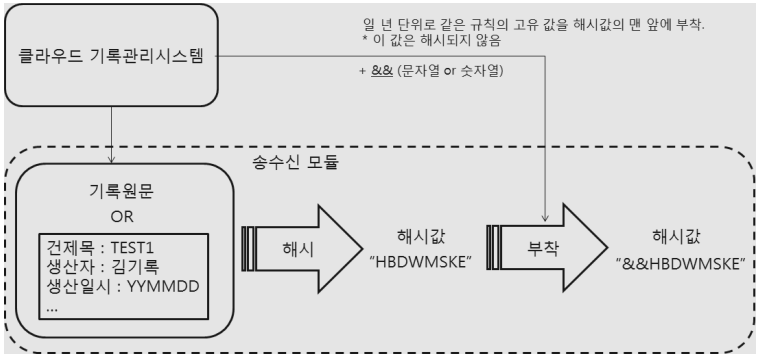
이 어려운 모형이다. BagIt 기술은 보존포맷을 대체할 방안으로 연구되고 있는 단계이며, 이를 포함한 여러 기술들이 제시되고 있지만, 완전한 대체 기술로서 채택된 기술은 등장하지 않았다. 또한 BagIt 기술을 블록체인 구조를 활용하여 기능을 구현했을 때의 이점이 무엇인가에 대한 확신을 현재로서는 도출하기 어렵다. 그렇지만 해시값을 사용하는 구조라는 점에서 충분한 연구를 통해 블록체인 기술과의 접점을 적절히 융합하여 활용할 여지가 있을 것으로 생각된다. 연구가 발전되고 구체화되어 기술적 접점을 찾아내면 기존의 블록체인 구조에 위에서 제시한 내용들과 같이 모듈을 구현하여 부착하는 형식으로 구현해 볼 수 있을 것이다.

(3) 생산현황통보

클라우드 기록관리 환경에서 생산현황통보는 모니터링으로 대체할 수 있다. 앞서 언급한 것처럼 스토리지를 공유하는 환경에서 생산현황통보는 대체 가능한 프로세스이기 때문에 생산현황을 모니터링할 수 있는 기능 정도로 대체할 수 있을 것이다. 생산현황 모니터링 기능을 구현하기 위해서는 문자열 부착 기능이 추가되어야 한다. 기록을 생산해서 해시값을 전송할 때, 1년을 기준단위로 삼아 동일한 규칙을 갖는 문자열을 생성하여 해시값에 부착해 함께 전송한다. 이후 과정은 접근키 모듈의 과정과 동일하며, 이런 과정을 통해 시스템 내에서는 자동적으로 생산현황 정보가 관리된다.

육안검수가 필요한 경우, 모니터링 권한을 가진 검수자가 기록관리시스템에서 모니터링 버튼을 누르면, 조회하려는 시기에 해당되는 문자열이 부착된 트랜잭션을 블록체인 네트워크에서 검색하여, 해당 트랜잭션과 매칭되는 기록들을 기록관리시스템의 결과화면에 보여주게 된다. 이와 같은 구조를 통해 권한을 가진 참여자는 모니터링을 시행하는 당시의 기록물 생산현황만을 모니터링 하여 확인할 수 있다.

〈그림 11〉 문자열 부착 프로세스



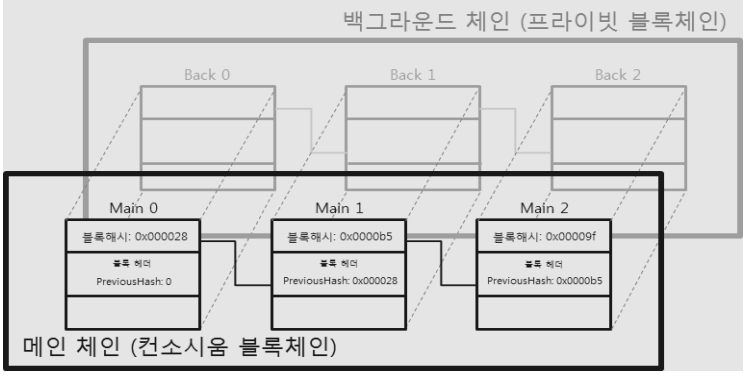
(4) 이관

생산현황통보와 마찬가지로, 클라우드 기록관리 환경에서 이관 절차는 개선이 필요한 프로세스이다. 앞서 설명한 것처럼, 동일한 스토리지 내에서 위치를 옮기는 행위는 큰 의미를 갖지 못한다. 하지만 이관의 개념은 기록의 생애주기에 있어 중요한 의미를 갖는 프로세스이다. 이관을 대체할 수 있는 프로세스는 '접근권한 설정'이다. 기록을 이관한 후 삭제하는 등의 번거로운 절차는 접근권한 설정이라는 하나의 프로세스로 충분히 대체할 수 있다. 블록체인 네트워크를 활용하여 기록에 대한 접근권한 설정을 구현하려면 블록체인 네트워크 자체를 하나 더 설계하는 것이 가장 편하다. 즉, 병렬구조의 블록체인 네트워크 모듈을 구성한다.

두 개의 블록체인 모듈은 각각 메인체인과 백그라운드 체인의 역할을 한다. 메인체인은 컨소시엄 블록체인의 형태를 띠며, 이 체인은 앞서 제시한 클라우드 기록관리시스템과 연동되는 핵심 블록체인 네트워크의 역할을 한다. 메인체인에 병렬구조로 만들어지는 백그라운드 체인은 프라이빗 블록체인의 형태를 띠며, 메인체인과 연동되며 관리자는 영구기록물관리기관으로 설정한다. 그 외의 메인체인 참여자는 일반 참여자의 권한으로 백그라

운드 체인에 참여한다. 기록관리시스템과 메인체인 간의 정보소통은 앞서 제시한 바와 같이 '송수신 모듈'을 통해서 이루어진다. 기록이 생성되면 기록관리시스템이 그 기록의 해시값을 메인체인의 트랜잭션으로 전달한다. 이때 또 하나의 송수신 모듈이 사용된다. 이번에는 메인체인이 수신한 트랜잭션의 값을 메인체인의 퍼블릭 키로 암호화하여 백그라운드 체인으로 송신한다. 값을 수신한 백그라운드 체인은 트랜잭션에 수신한 값을 백그라운드 체인의 퍼블릭 키로 다시 암호화 하고, 백그라운드 체인의 퍼블릭 키를 메인체인으로 송신한다. 즉, 앞의 보안에서 퍼블릭 키를 주고받던 작업을 이중으로 수행한다.

〈그림 12〉 메인체인과 백그라운드체인 이중구조의 블록체인 네트워크



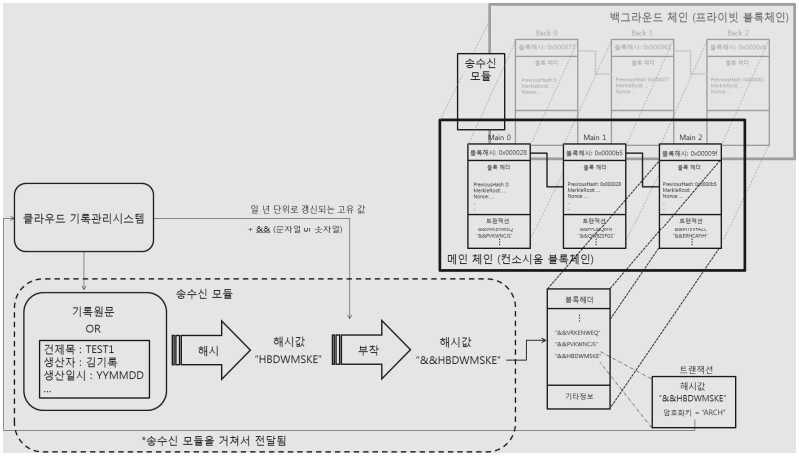
이러한 구조에서 기록에 대한 접근은 다음과 같이 이루어진다. 네트워크 참여자 A는 기록에 접근하기 위해 메인체인과 접근키 검증을 먼저 수행한다. 검증을 통해 매칭된 메인체인의 트랜잭션은, 백그라운드 체인과 접근키 검증을 수행한다. 이때 A가 백그라운드 체인 내에서 해당 트랜잭션에 접근권한을 가지고 있지 않다면 해당 기록에 대한 접근 승인이 이루어지지 않고, 접근권한을 가지고 있다면 해당 기록에 대한 접근이 승인된다. 정리하

면, 프라이빗 블록체인으로 구성된 백그라운드 블록체인이 각 트랜잭션에 대한 접근권한을 조정함으로써 기록관리시스템에서 기록에 접근이 가능한지의 여부를 결정하고, 이러한 기능을 이용하면 권한설정으로 이관절차를 대체할 수 있다.

2) 기록관리시스템 연계형 블록체인 네트워크 모델

〈그림 13〉은 앞서 제시한 블록체인 기술 적용방안을 하나로 통합하여 구축한 클라우드 기록관리시스템 연계형 블록체인 네트워크 모델이다. 기록관리시스템–메인체인, 메인체인–백그라운드 체인 사이에 각각 송수신 모듈이 하나씩 연계되어 있으며, 메인체인은 컨소시엄 블록체인으로, 백그라운드 체인은 프라이빗 블록체인으로 구축된다. 송수신 모듈에는 문자열 부착 기능과 접근키 모듈이 통합되어 구현되어 있으며, 단방향 송수신 모듈이 아닌 양방향 송수신 모듈로서의 역할을 한다.

〈그림 13〉 기록관리시스템 연계형 블록체인 네트워크 모델



메인체인인 컨소시엄 블록체인에서 관리권한을 갖는 합의주체는 기록관과 영구기록물관리기관 단위의 참여자이다. 메인체인의 참여자는 병렬구조를 취하고 있는 백그라운드 체인에도 참여하게 되며, 백그라운드 체인에서 관리권한을 갖는 주체는 영구기록물관리기관 단위이다. 백그라운드 체인에서는 영구기록물관리기관이 이하 단위 기관의 트랜잭션에 대한 접근권한을 조정하는 구조가 구현된다. 하지만 영구기록물관리기관이 접근권한을 임의로 조정하였을 때의 위험성이 존재하기 때문에, 기본적으로는 접근권한 조정을 정해진 시기에 시스템으로 처리되도록 자동화 구현을 해야 하며, 특수상황이 발생하여 직접 권한조정이 필요할 경우, 메인체인의 유관기관과 합의를 통해 권한을 조정하는 구조로 구현해야 한다. 보존포맷관리를 제외한 세 기능은 위의 모델을 기반으로 다음과 같이 구현된다.

보안에는 앞서 제시했던 보안성 향상을 위한 기술 적용방안에서는 하나의 '접근키' 기능을 사용하였다. 하지만 제시한 네트워크 모델에서는 블록체인 네트워크가 병렬구조로 이루어진 두 개의 네트워크로 구성되면서 기록관리시스템과 블록체인 네트워크 간의 접근키 기능에 프라이빗 블록체인 네트워크와 컨소시엄 블록체인 네트워크 사이에 접근키 기능 하나를 추가해 총 두 개의 접근키 기능을 사용한다. 두 접근키는 같은 프로세스로 작동되며, 두 네트워크를 연결하는 접근키에 시스템과 네트워크를 연결하는 접근키가 종속된다. 결과적으로 두 개의 접근키를 활용해 이중 통제의 기능이 구현됨으로써 보안성을 더욱 향상시키는 효과를 얻을 수 있다.

생산현황 모니터링 프로세스에는 백그라운드 체인은 관여하지 않는다. 현행 시스템의 생산현황통보는 처리과에서 통보한 내용을 기록관에서 모아 최종적으로는 영구기록물관리기관으로 통보하게 되는데, 이를 생산현황 모니터링의 방식으로 바꾸면 기록관과 영구기록물기관 단위에서 모니터링이 가능하도록 프로세스를 구현하면 된다. 그렇기 때문에 기록관리시스템과 메인체인 사이의 송수신 모듈만을 이용해도 모니터링에 필요한 프로세스 과정을 모두 소화할 수 있으며, 백그라운드 체인이 프로세스에 관여할 경우

시스템 간 통신횟수가 늘어나 오히려 시스템 속도가 느려지고 프로세스 처리과정이 복잡해진다.

접근권한 설정 프로세스에는 필수적으로 백그라운드 체인이 참여한다. 현재 제시하고 있는 블록체인 네트워크 모델은 접근권한 설정을 영구기록물관리기관에서 수동으로 처리할지 자동화 할지에 대해서는 나타내고 있지 않다. 만약 접근권한 설정 프로세스를 자동화 한다면 업무의 편의성과 효율성은 높아지겠지만 비치기록물 요청, 이관연장 요청 등 특수상황이 발생할 경우에 대응하기 쉽지 않다. 만약 접근권한 설정 프로세스를 자동화 한다면 이러한 특수상황을 모두 고려하여 적합한 모듈을 추가로 구현해야 할 것이다.

5. 결론

본 연구에서는 클라우드 기록관리시스템이 적용될 환경을 가정하고, 현행 기록관리시스템의 프로세스 중에서 환경에 맞게 변화가 필요한 프로세스를 도출하고, 이에 해당하는 프로세스들을 하나의 블록체인 네트워크 모델을 구현함으로써 대체할 수 있는 방안을 제시하였다. 블록체인 네트워크 모델은 클라우드 스토리지의 보안성을 높일 수 있고, 모니터링 기능으로 생산현황 통보나 기록물 현황 등의 프로세스를 대체할 수 있으며, 접근권한 설정 기능을 활용해 이관 프로세스를 대체할 수 있다는 점에서 클라우드 기록관리시스템 환경에 효과적으로 적용시킬 수 있다. 또한 본 연구에서 제시하는 블록체인 네트워크 모델은 하나의 모듈 구현으로 여러 프로세스를 대체할 수 있다는 점에서도 의미가 있다.

다수의 프로세스를 하나의 기능으로 통합하고, 통합한 기능들을 하나의 블록체인 네트워크 모듈로 구현함으로써 효율성 측면에서 큰 이점을 갖는다. 또한 제시한 모델을 기본으로 간단한 추가 기능모듈을 구현함으로서, 현재는 예측할 수 없지만 잠재적으로 변화의 필요성을 내포하고 있는 기록

관리 프로세스에 유연하게 대응할 수도 있다.

연구에서 제시한 방향으로 블록체인 네트워크를 설계할 경우 대부분의 시스템 동작은 기록관리시스템에서 이루어지지만, 불가피하게 블록체인 네트워크에 참여자가 직접 접근을 하여 이용해야 하는 경우가 생길 수도 있다. 이때 블록체인 네트워크 자체에 접속해서 활용하는 것은 매우 복잡하여 활용효율이 낮으므로, 만일의 상황에 대비하여 블록체인 네트워크 자체도 활용할 수 있도록 적절한 블록체인 서비스 UI를 개발하여 적용해야 한다.

본 연구의 한계점은 클라우드 기록관리시스템 환경을 가정하고 블록체인 네트워크를 구상하였기 때문에, 실제로 이를 구현하여 적용해보지 못했다. 그렇기 때문에 발견하지 못한 구조적 문제점이 있을 가능성이 있으며, 다가오는 클라우드 기록관리시스템의 사양에 따라 일부는 구현이 어려울 가능성이 있다. 향후 클라우드 기록관리시스템으로 전환이 되어 본 연구에서 제시한 모형을 적용하려 한다면, 제시한 블록체인 네트워크 모형을 실제 시스템에 연계했을 때 충돌점이 없는지를 검증하면서 수정작업을 해 나가야 하며, 블록체인 네트워크 모듈을 기록관리시스템에 어떻게 연계할 것인지 그 방법이 구체적으로 연구되어야 한다.

본 연구는 공공기록관리의 영역을 중심으로 수행되었으나, 블록체인 기술은 민간분야에서도 충분히 활용될 가능성이 있다. 특히 민간분야에서는 저작권 관리 방안으로 가장 효과적으로 활용할 수 있다. 마을공동체 혹은 민간 영역에서 다수의 참여자가 함께 생산한 기록이 저작권의 문제로 인해 법적공방에 휘말리는 경우가 종종 있다. 하지만 민간의 경우 법적공방에 대한 막연함과 두려움 등의 이유로 제대로 대처하지 못하는 경우가 대부분이다. 만약 블록체인 네트워크를 구축해 기록생산에 참여한 이들이 공동주체가 되어 저작권을 상호 검증해줄 수 있는 구조를 구현한다면, 민간분야 기록의 저작권 보호 및 검증 측면에서 큰 도움을 줄 수 있을 것이다.

블록체인 기술은 새로 개발된 기술이라기보다는 기존에 존재하던 링크드 리스트와 같은 개념을 좀 더 깔끔하게 정리한 기술이다. 하지만 블록체인 기술은 그 구조의 특성이 명확하기 때문에 환경에 맞춰 유연하게 기술을 적용시키는 것이 쉽지는 않다. 이는 기록관리에서도 마찬가지이다. 이상의 연구를 기반으로 볼 때 다음 사항들에 대한 학문적 논의가 요구된다.

첫째, 클라우드 기록관리 환경에서 구현될 기록관리시스템에 대한 학문적 논의가 지속되어야 한다. 현재도 CRMS와 연관된 논의들은 끊임없이 이루어지고 있고, 다방면에서 접근하는 연구들도 꾸준히 나오고 있다. CRMS의 도입완료 시기가 다가오는 만큼 지속적인 논의와 연구를 통해 상을 구체화해야 할 필요가 있다.

둘째, 블록체인 네트워크 모듈 구현을 위한 심층적 코드연구가 필요하다. 본 연구에서는 블록체인 기술의 코드를 분석하여 활용할 수 있는 방안을 거시적으로 제시하였다. 때문에 실제 시스템을 구현하기 위해서는 보다 심층적으로 코드를 연구해야 한다.

셋째, 블록체인 기술을 적용시킬 수 있는 프로세스에 대한 논의가 이루어져야 한다. 본 연구에서 블록체인 기술을 활용하여 블록체인 기술을 적용시킬 프로세스를 제시하였지만 제시한 프로세스가 적용 가능성을 가지고 있는 프로세스의 전부는 아니며, 향후 블록체인 기술이 발전하면서 적용시킬 수 있는 프로세스의 범위가 확장될 가능성이 있다. 현 시점에서 파악했을 때, 블록체인 기술로 간소화 하거나 대체할 수 있는 기록관리시스템의 프로세스는 그리 많지 않다. 그러나 블록체인 기술이 세대를 거쳐 가며 점점 유연한 형태로 변화해가고, 기록관리시스템의 환경 또한 끊임없이 변화하고 발전해 나가고 있다. 블록체인 기술이 기록관리시스템의 더 많은 프로세스에 적용하고 활용하기 위해 블록체인 기술과 기록관리시스템 각각의 변화와 발전에 항상 관심을 두고 연구해야 한다.

〈참고문헌〉

고윤승, 최홍섭. 2017. 비즈니스 패러다임 변화와 그 활용방안－블록체인 기술을 중심으로.『한국과학예술포럼』. 27. 13-29.

과학기술정보통신부. 2018.『블록체인 기술 발전전략』: 과학기술정보통신부.

국가기록원. 2018.『2018년도 기록물관리지침』. 국가기록원.

국가기록원. 2018.『2018년도 정부산하공공기관 기록물관리 지침』. 국가기록원.

국가기록원. 2018.『클라우드 RMS 개념도 및 전환 기관』. 국가기록원.

명지대학교 산학협력단 디지털아카이빙연구소. 2017.『차세대 기록관리 모델 재설계 연구 개발』. 명지대학교 산학협력단 디지털아카이빙연구소.

배영임, 최준규. 2018.『블록체인 기반 공공 플랫폼 구축을 위한 제언.』경기연구원.

백영태, 민연아. 2018.『블록체인을 활용한 디지털 콘텐츠 저작권 보호 및 거래활성화 방법 연구. 한국컴퓨터정보학회 학술발표논문집』. 26(2), 73-75.

블로코. 2016.『블록체인 기반 전자문서 진위 확인 솔루션 보안 기술서』. 블로코.

서울시. 2016.『서울기록원 정보화전략계획(ISP) 수립 용역 완료보고회 결과보고』. 서울시 정보공개정책과.

왕호성. 2018. 블록체인과 기록관리의 미래 : 영국 TNA ARCHANGEL 프로젝트를 중심으로.『기록인(IN)』. 44호, 64-73.

왕호성. 2018.『블록체인과 기록관리의 미래』. 2018년도 제10회 전국기록인대회 세션 발표, 한남대학교, 대전.

왕호성, 설문원. 2018. 기록물 생산현황 통보제도 운영 실태와 개선방안.『한국기록관리학회지』. 18(1). 79-99

유영문. 2018. 표준기록관리시스템(RMS)의 기능 현황 및 발전방향.『기록학연구』. (57), 235-279.

이경남. 2018.「기록의 진본인증을 위한 블록체인 기술 적용방안 연구」. 박사학위논문. 한국외국어대학교 대학원, 정보기록학과.

이동영, 박지우, 이준하, 이상록, 박수용. 2017. 블록체인 핵심 기술과 국내외 동향.『정보과학회지』. 35(6), 22-28.

주현미, 임진희. 2017. 차세대 전자기록관리 프로세스 재설계 연구.『한국기록관리학회지』. 17(4). 201-223.

차홍기, 이원석, 최영환, 이주철, 이강찬. 2018.『블록체인 국제표준화 동향』. 정보통신기술진흥센터.

Victoria L. Lemieux. 2016.『Blockchain technology for record keeping : Help or Hype?』. University of British Columbia.

〈참고 사이트〉

국가기록원, 내년 1월까지 클라우드 기록관리 전 부처 확산. 정부24, Retrieved November 15 from https://www.gov.kr/portal/ntnadmNews/1572240

머클트리(merkle tree)란?(2018). Retrieved September 5, 2018 from https://steemit.com/kr/@brownbears/merkle-tree

퍼블릭 블록체인(Public Blockchain) vs 프라이빗 블록체인(Private Blockchain). 2018. Retrieved September 5, 2018 from https://tokenpost.kr/terms/5822

BitcoinCore 홈페이지의 About. 2018. Retrieved November 13, 2018 from https://bitcoincore.org/en/about