블록체인 기술의 효용성과 문제점 분석

지도교수 : 이 강 호
연 구 자 : 임 경 빈

< 목 차 >

요 약

2020년 전세계적인 전염병 COVID-19의 피해로 각국의 경제적 피해와 사회적 위기로 가상화폐(디지털화폐)의 특수성과 필요성이 대두되고 있으며 즉, 가상화폐 시장은 '인플레이션'으로 인한 물가 상승에 따라 곧 비트코인의 상승으로 이어질 것이라는 분석이 화두에 오르고 있다.

비트코인이란, 첫 번째로 만들어진 디지털화폐이다. 비트코인은 디지털 코인이며 인터넷을 통해 보낼 수 있다. 기존의 다른 통화들과 비교해서 비트코인은 많은 장점들이 있다.

비트코인은 은행이나 다른 대행업체를 거치지 않고 직접적으로 인터넷을 통해 개인 대 개인으로 거래를 할 수 있다. 그래서 수수료가 은행이나 다른 대행업체에 비해 아주 저렴하다. 어느 나라에서나 사용이 가능하며 구좌가 동절 되거나 독점적인 제한이 없다. 비트코인은 누구든지 비트코인마이너(Bitcoin Miner)라고 부르는 매체를 사용하여 인터넷을 통하여 발행할 수 있다. 비트코인 네트웍스 '코인생성' 옵션을 선택한 소프트웨어를 작동하는 누군가에게 한 묶음의 새로운 비트코인을 시간당 6번 정도씩 무작위로 생성해 배분한다. 소프트웨어를 작동하는 사람은 누구나 비트코인 묶음을 받을 수 있으며 발행금액은 네트웍에 의해 자동적으로 조정되어 예측과 조정이 가능하다.

이러한 비트코인의 핵심 기술인 블록체인 이란, 네트워크상의 기록 데이터들이 하나의 블록 단위로 집합하여 저장되며 이러한 블록들이 서로 연결되어 저장되는데, 이 형태가 블록들이 연결되어 있는 모습과 비슷하여 블록체인이라 불리게 되었다. 오늘날 국내외의 기업과 정부는 블록체인 기술을 활용하여 디지털화폐 유통뿐만 아니라, 정부의 각종 증명서와 계약, 표결과 같은 기록과 금융, 의료, 공공 인프라, 부동산 거래 등 데이터의 신뢰성이 중요한 영역 등 실제로 이루어지는 사건과 사물을 기록하고자 한다. 본 연구에서는 이러한 블록체인 기술의 효용성과 해당 기술을 이용하였을 때 부각되는 문제점에 대해 모색하고자 한다.

주요어: 블록체인 (Block Chain), 효용성, 문제점

1. 서론

1.1 연구 배경 및 목적

제4차 산업혁명이 도래하면서 빅데이터(Big Data), 가상현실(AR/VR), 사물인터넷(IoT), 인공지능(AI), 클라우드 컴퓨팅(Cloud Computing) 등 첨단 정보통신기술이 경제·사회·문화 전반에 걸쳐 융합되어 혁신적인 변화가 나타나고 있다. 제4차 산업혁명은 초지능(superintelligence)과 초연결(hyperconnectivity)을 특징으로 하여서 기존 산업혁명에 비하여 더 넓은 범위에 더 빠른 속도로 큰 영향을 끼치고 있다.

세계 경제 포럼(WEF: World Economic Forum) 보고서에 따르면 떠오르는 10대 기술 중 하나로 블록체인을 선정했고, 향후 10년간 1조 달러에 이르는 새로운 무역 거래를 창출할 수 있다고 발표했다. 보고서는 분산 원장 기술이 무역의 장벽을 허물면서 1조 1,000억 달러에 이르는 새로운 교역량이 발생하고, 전통적인 거래량의 9,000억 달러가 더 나은 서비스와 낮은 수수료로 인해 분산 원장 기술로 옮겨갈 것이라고 전망했다. 업종별로는 금융업, 유통 및 서비스 분야, 제조 및 자원 분야 순으로 비중을 차지할 것으로 예상했다. 또한, 전체 응답자의 50%를 넘는 비율이 2025년까지 글로벌 GDP의 최소 10%가 블록체인 플랫폼에서 일어날 것이라고 전망했다. 국제연합(UN)은 유엔미래 보고서 2015에 따르면, 2050년경엔 지금까지 정부가 관리하고 보관해 오던 각종 증명서뿐만 아니라 표결, 계약과 같이 디지털화된 모든 기록에 블록체인 기술이 적용되면서 이전과는 다른 새로운 국가관리 구조가 등장할 것이라고 예측했다.

최근 가상화폐인 비트코인 거래가 활발히 진행되고 있다. 비트코인에 적용되어 있는 기술은 블록체인 기술로 다양한 분야에 접목되고 있으며, 블록체인은 암호화 보안, 분산된 합의 및 적절하게 통제되고 권한을 가진 공유 된 공공 원장 덕분에 우리가 정치적, 경제적, 사회적 및 과학적 활동을 체계화하는 방식을 근본적으로 바꿀 수 있다.

블록체인 기반의 기술은 사토시 나카모토(Satoshi Nakamoto)가 2007년 글로벌 금융위기 이후 중앙집권화된 금융 시스템의 위험성을 인지하고, 개인 간 거래가 가능한 블록체인 기술을 고안하였다. 이후 2009년 사토시 나카모토는 블록체인 기술을 적용하여 암호화폐인 비트코인을 개발하였다. 비트코인을 지탱하는 기술인 블록체인 기술에 의해 이론적으로 비트코인은 거의 조작이 불가능하고 거의 영구적으로 기록에 남는다. 이러한 기술로 인해 약 2,000개가 넘는 암호화폐가 생겨났다.

이에 본 논문에서는 블록체인 기술의 다양한 시나리오를 제언(提言)하고 그에 대한 효용성과 한계점에 대해 연구 기술하고자 한다.

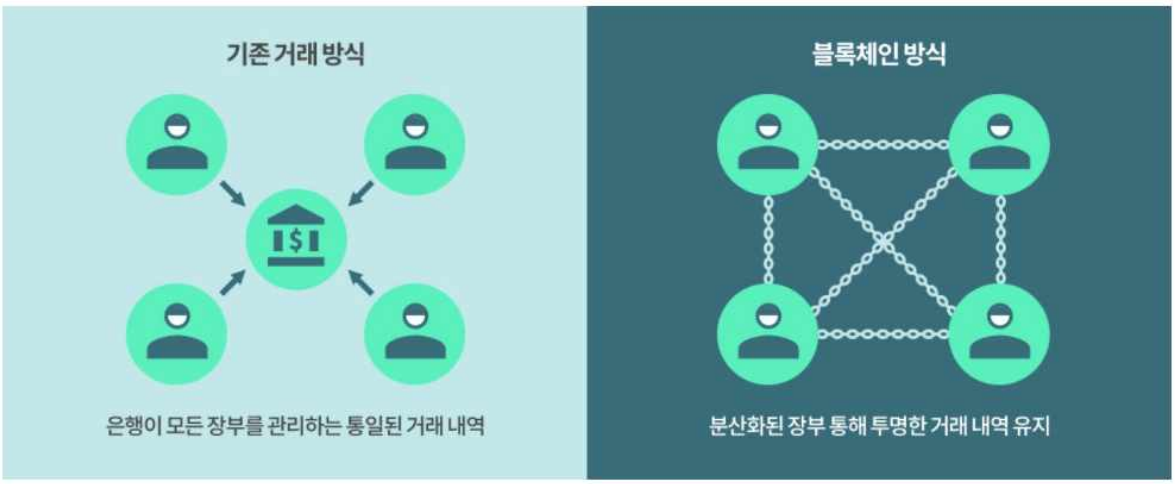
1.2 연구 방법

본 논문은 연구 배경을 기술하고 국내외의 다양한 논문과 보고서 및 학술지를 참고하였으며, 서론 본론 결론을 구성하였으며, 서론에서는 블록체인의 개념을 정의하고, 핵심요소와 블록체인 네트워크의 분류를 나열하고, 블록체인 기술의 효용성과 다양한 영역에서의 실제 활용 및 운용사례를 연구하였으며, 또한 블록체인 기술의 장점과 문제점을 알아보고, 마지막 결론으로 연구 결과 및 의논점을 기술하였다.

2. 본론

2.1 블록체인의 정의

블록체인은 관리 대상 데이터를 “블록”이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 데이터 분산 처리 기술이다. 이는 근본적으로 분산 데이터 저장기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안되었다. 블록체인 기술은 비트코인을 비롯한 대부분의 암호 화폐 거래에 사용된다. 암호화폐의 거래 과정은 탈중앙화된 전자 장부에 쓰이기 때문에 블록체인 소프트웨어를 실행하는 많은 사용자들의 각 컴퓨터에서 서버가 운영되어, 중앙에 존재하는 은행 없이 개인 간의 자유로운 거래가 가능하다.



[사진 1] 기존 거래와 블록체인 기술이 적용된 거래의 차이점

2.1.1 블록체인 기술의 동작 방식

1) 각 트랜잭션[1]이 발생하면 데이터의 블록으로서 기록되고 이는 유형과 무형의 자산 이동을 나타낸다.

2) 이러한 데이터 블록은 자산이 한 장소에서 다른 곳으로 이동하거나 소유권이 이전될 때 데이터의 체인을 형성한다. 블록이 트랜잭션의 정확한 시간과 순서를 확인하고 블록이 안전하게 서로 링크되면서 블록이 변경되거나 순서가 바뀌지 않도록 방지한다.

3) 각각의 추가 블록들은 이전 블록과 전체 블록의 검증을 강화한다. 이는 블록체인 변경 증거를 렌더링하여, 불변성을 제공하고, 악성 침입자의 조작 가능성을 차단한다. 자신과 기타 네트워크의 멤버가 신뢰할 수 있는 트랜잭션의 원장을 구현한다.

---

1) 트랜잭션(Transaction)이란, 데이터베이스의 상태를 변화시켜서 수행하는 작업의 단위를 뜻한다.

[사진 2] 블록체인 기술기반의 거래 동작 순서

블록체인에 기반을 둔 거래 과정의 순서는 다음 [사진 2]와 같다. 먼저, A 송금자가 B 수신자에게 송금하려고 한다고 가정했을 때, 해당 거래정보는 온라인상에서 '블록'에 저장된다. 그리고 해당 블록은 네트워크 구성원들 모두에게 전파되며, 구성원들은 해당 거래의 유효성을 승인한다. 이후에 승인된 거래 블록은 새로운 블록으로 기존의 블록체인에 연결된다. 마지막으로 A가 보낸 실제 자금이 B에게 이동된다.

2.1.2 블록체인 기술의 핵심 3요소

블록체인의 핵심 요소로서 첫 번째는 분산 원장 기술이다. 분산 원장 기술은 복제, 공유 또는 동기화된 디지털 데이터에 대한 합의 기술이며, 데이터들은 지리적으로 여러 사이트나 국가 혹은 여러 기관에 분산되어 있게 된다. 즉 중앙 집중화된 데이터 저장소가 존재하지 않고 기능이 동작하게 되어 해당 네트워크의 모든 참여자는 분산 원장과 트랜잭션의 불변 레코드에 액세스할 수 있다. 이 공유 원장에서 트랜잭션은 한 번만 기록되며, 기존 네트워크에서 중복 작업이 사라지게 된다.

두 번째 요소는 불변 레코드이며, 이러한 불변 레코드는 데이터의 무결성이 보장됨을 의미한다.

공유 원장에 정보가 기록되면 어떠한 참가자도 트랜잭션을 변경하거나 위조가 불가하다. 이러한 트랜잭션 레코드에 오류가 포함되면 해당 오류를 되돌리기 위해 새 트랜잭션을 추가하고 이때 추가된 트랜잭션과 오류가 포함된 트랜잭션을 모두 볼 수 있다.

마지막 요소로서 스마트 계약은 계약 당사자, 즉 네트워크 참여자가 사전에 협의한 내용을 미리 프로그래밍하여 전자 계약서 문서 안에 넣어두고, 이 계약 조건이 충족되면 자동화된 계약 내용이 실행되도록 하는 시스템이다. 이러한 스마트 계약은 트랜잭션의 속도를 증진시키고, 일련의 규칙들이 블록체인에 저장되고 자동으로 실행된다. 기존의 블록체인 기술이 과거에 일어났던 일을 기록하여 데이터를 저장한다면, 스마트 계약 기능을 구현한 블록체인 기술은 미래에 일어날 계약 조건을 미리 기록해 둘 수 있다.

2.1.3 블록체인 네트워크의 분류

블록체인 네트워크는 여러 가지의 분류로 나뉠 수 있는데 이를 나누는 기준은 해당 블록체인 네트워크에 인가된 구성원이 얼마나 참여할 수 있는가에 의해 나뉜다.

우선 첫 번째로 퍼블릭 블록체인 네트워크는 누구든지 참여할 수 있는 공공 블록체인 혹은 개방형 블록체인이라고 한다. 해당 블록체인은 인터넷이 연결되는 환경이라면 누구든지 신청하여 참여가 가능하다. 하지만 모든 거래자가 한 네트워크에 참가하는 특성 때문에 상당한 컴퓨팅 파워가 필요하고 이에 거래 속도가 느려진다. 알고리즘에 의해 거래 증명자가 결정되어 거래 증명자가 누구인지 사전에 판단할 수 없는 것 그리고 이에 대한 보안이 취약하다는 것, 그리고 한 번 정해져 설정된 법칙을 변경하기 매우 어렵다는 문제점을 가지고 있다. 그래서 블록체인 기술을 기업에서 채용함에 있어서 중요한 고려사항이 된다.

프라이빗 블록체인 네트워크는 퍼블릭 블록체인 네트워크와 유사한 분산형 P2P(peer-to-peer)의 네트워크이다. 하지만 퍼블릭 블록체인의 상대적인 개념으로서 폐쇄적인 네트워크로 네트워크의 주체(관리자)가 네트워크를 관리하고 참여가 허용되는 자를 통제하여 합의 프로토콜을 실행하고, 공유 원장을 유지 보수한다. 이에 해당 네트워크는 네트워크의 확장이 쉽고 참여한 참가자들 간의 신뢰성과 안정성을 상당히 높아 거래 속도가 빠르고 원활하다. 허가형 블록체인 네트워크는 프라이빗 블록체인 네트워크의 연장선으로서 위 블록체인 네트워크를 채용하는 주체들은 일반적으로 허가형 블록체인 네트워크를 설정한다. 블록체인 네트워크를 운용하는 주체가 네트워크 및 특정 트랜잭션에 참여할 수 있는 사용자를 제한하고, 인가된 사용자임을 파악하기 위한 권한이 꼭 필요하다.

마지막으로 컨소시엄 블록체인 네트워크는 컨소시엄에 소속된 참여들이 권한을 소유한다. 즉 해당 네트워크는 여러 네트워크상에서 참여자들이 해당 컨소시엄 블록체인을 유지 보수하는 책임을 공유할 수 있다. 사전에 설정되어진 법칙들은 컨소시엄 참여자들의 의사 결정에 의해 법칙을 바꿀 수 있다. 해당 네트워크 참여자들은 트랜잭션을 제출하거나 데이터에 액세스 할 수 있는 참여자들을 중앙 기관이 판별한다. 컨소시엄 블록체인 네트워크는 모든 참여자가 인가를 받아야 하고 블록체인에 대한 공유 책임을 보유하는 상황에 적합하다.

2.2 블록체인 기술의 효용성

2.2.1 다양한 분야에서의 활용 예시

- 암호 화폐 영역

블록체인 응용 기술 중 가장 많이 활용되는 분야로서, 암호 화폐는 블록체인 기반 네트워크의 참여자로서 진정성을 보여주기 위해 특정한 형태의 작업 증명을 제시하고, 이에 따라 새로운 코인을 생성해 보상받으며 상호 거래 내역을 검증하는 화폐이다. 2009년 1월 3일에 출시된 비트코인을 선두로 라이트코인, 리플, 이더리움, 에이다와 같은 다양한 형태의 암호 화폐들이 만들어졌다.

- 스마트 계약

블록체인 기술의 응용 서비스는 기존의 금융 상품 혹은, 파생상품 등에 적용된 스마트 계약 기반 서비스에도 활용된다. 주가지수 연동 상품부터 결혼과 이혼의 과정, 주택

매매 과정 등 일상에서 발생할 수 있는 다양한 사건을 스마트 계약을 통해 검증받고 분산하여 기록할 수 있기 때문에 블록체인 기술이 적용되면 법적 논쟁, 문서 작성에 필요한 작업, 비용, 인력 등 상당 부분이 절감될 것으로 예상된다.

- 스마트 자산 관리

소유권 이전이나 매매, 거래 등 모든 재산에 대한 등록 및 관리를 블록체인에 올려 운용하는 스마트 자산 관리 체계에 블록체인 기술을 활용할 수 있다. 블록체인 기술이 적용된 스마트 자산 관리 서비스는 동사무소에서 인감증명서나 부동산 등기부등본을 요구하는 일 등의 번거로운 과정을 생략시킬 수 있을 것이다.

- 병원 시스템

병원에서는 진료과목별 다양한 플랫폼에 환자에 대한 정보를 저장한다. 이러한 환자의 정보를 잘 활용하여 정확한 진단을 내리고 치료비용 등을 절감할 수 있는데, 블록체인 기술의 활용으로 개인정보 보호와 자료의 일관성 측면에 도움을 줄 수 있다. 또한 환자의 데이터 연결 과정에서 발생하는 개인정보의 노출 등 기존 문제점을 해결하면서 환자의 데이터를 직접 연결하는 구조가 가능하기 때문에 이에 대한 가능성이 주목받고 있다.

2.2.2 실제 블록체인 기술 운용 사례

- Bitcoin

비트코인(Bitcoin)은 블록체인 기술 응용의 첫 시작점으로 금융기관을 중심으로 하는 중앙집중형 거래의 취약한 구조 대신 중앙의 금융기관 없이 개인과 개인 간의 온라인 지불을 가능하게 하는 Peer to peer (P2P)네트워크를 활용한다. 비트코인은 암호화폐가 거래될 때마다 송금자의 소유여부와 중복사용 여부를 모든 네트워크 참여자들이 함께 검증하게 되며, 검증이 완료된 송금들을 묶어서 블록에 저장한다. 네트워크상에서 새로운 비트코인 거래를 기록하여 공식화하는 과정을 채굴(mining)이라고 하며, 작업증명(proof of work)은 네트워크 구성원들이 해시값을 통해 새로운 거래 데이터를 검증하는 것을 뜻한다. 비트코인은 전자서명의 연속으로, 인터넷을 통해 온라인 거래를 할 때 두 명의 거래 당사자들이 제 3자 신뢰 메커니즘이 아닌 암호화 증명을 사용한다. 각 거래는 거래를 원하는 소유자의 공개키를 포함하여 발신자의 개인키를 사용하여 디지털 서명을 진행하여 거래를 마친다.

- Everledger

다이아몬드 유통 추적을 위해 블록체인 기술을 활용한 사례이며, 다이아몬드의 모든 유통 경로에 대한 정보를 블록체인에 기록한다. 이 Everledger는 블록체인을 이용한 귀금속 공급망 관리 스타트업이며, 블록체인을 활용해 유통 정보가 기록되었을 때 잘못된 정보가 기록되면 수정할 수 없기에 정보 훼손을 막기 위해 자동으로 정보가 기록되는 방식을 활용한다. 예를 들면, 거래되는 귀금속을 현미경에 부착된 센서로 측정하여 블록체인에 기록되는 형식을 사용함으로써 잘못된 정보가 저장되는 것을 방지한다.

- Steemit

블록체인 기술과 트래킹 기술을 결합한 사례로서, 블로그 정보를 블록체인에 기록한다. 기존의 블로그를 사용할 경우 서비스가 중단되면 블로그에 업로드된 컨텐츠 및 기록 자료들을 소실하게 되는 경우가 있으며, 플랫폼에서 이러한 것들을 삭제하는 경우가 있다. 이에 Steemit은 블록체인에 콘텐츠들이 업로드되어 영구 보존이 가능하며 콘텐츠의 검열로 삭제되는 것이 불가능해진다. 또한, 양질의 콘텐츠가 생산되었을 때 다른 사용자들이 암호화폐를 제공하여 많은 콘텐츠 제작자들이 Steemit으로 이동하게 되어 이로 인해 수익 창출이 가능하게 된다. 콘텐츠를 생산하기 위한 동기부여가 되는 셈이다. 하지만 블로그 정보를 블록체인에 등재 하게 되면 암호 화폐의 보상성 때문에 선정적, 비인륜적 콘텐츠가 성행할 수 있고, 이를 파기할 수 없다는 단점이 있다.

- Civic

블록체인의 분산된 원장의 특징은 해커가 대상으로 할 중앙 집중식 거래의 약점이 없다는 것을 의미한다. 이는 디지털 신원 관리의 좋은 사용 사례로 적합할 수 있다. 개인 디지털 ID는 신원 확인이 필요할 때마다 개인이 수많은 문서와 서류를 작성하지 않아도 신원을 확인하는 데 사용할 수 있다. 이것은 변하지 않는 원장과 일치하는 단일키로 수행할 수 있고, 디지털 ID는 사회 보장 정보, 의료 기록 및 소셜 미디어 자격 증명과 같은 사용자의 신원에 대한 다른 온라인 정보를 수집하여 블록체인에 안전하게 저장한다. 은행 계좌를 가지고 있지 않은 수십억의 사람들에게 디지털 신원을 갖도록 하여 금융 서비스를 이용할 수 있게 할 수도 있다.

Civic은 신원 확인 기술을 개발하여 개인정보 전송을 보호하고자 하였으며, 블록체인 기반의 신원 확인 서비스를 identity.com에 구축하였다. 모든 사용자들은 디지털식별 플랫폼을 사용하여 자신의 가상 신원을 생성하여 개인정보와 함께 장치에 저장할 수 있다. Civic은 주문형 액세스, 서비스에 대한 안전하고 저렴한 액세스를 쉽게 하기 위해 설계된 에코 시스템을 구축하여 블록체인을 통해 개인의 신원을 확인하므로 더 이상 배경 및 개인정보를 기반으로 한 테스트 확인이 더 이상 필요하지 않다. 예를 들어 A회사는 미국 시민에게만 적합한 무료 제품 판매를 제공한다고 했을 때, A회사는 Civic과 협력하여 공짜 참가자가 미국 시민인지 여부를 확인하는 QR 코드 (또는 이와 유사한 것)를 제공한다. 계정이 있는 시민들은 자신이 미국 시민임을 증명하는 문서를 제공하지 않고 Civic의 시민 계정을 사용하여 정보를 확인할 수 있다.

2.3 블록체인 기술의 문제점

탈중앙화 및 분산 장부 시스템 기반의 블록체인은 현재의 코로나-19 시국의 경제 상황에서 전 분야에 영향을 미치고 있다. 블록체인은 이머징 시장에서 양질의 금융 서비스 증가, 새로운 거래 서비스로서 금융 기관의 직거래 생성, 모든 종류의 가치 교환이 가능한 디지털 거래자산의 폭발적 증가, 스마트 계약의 거래 및 법적 서비스 증가 등의 긍정적인 영향을 볼 수 있다. 이에 퍼블릭 블록체인 네트워크의 문제점을 살펴보고 이에 대한 해결방안을 가진 프라이빗 블록체인에 대해 기술하도록 하겠다.

2.3.1 퍼블릭 블록체인 네트워크의 문제점

우선 첫째로 퍼블릭 블록체인 네트워크의 문제점을 살펴보도록 한다. 퍼블릭 블록체인 네트워크는 누구에게나 공개되어 있으므로, 악의를 가진 참여자가 블록체인 네트워크에 대한 공격을 가할 경우를 대비하여 설계될 필요가 있다. 가장 먼저 쉽게 생각해 볼 수 있는 위험은 해커가 이미 저장된 데이터를 위조 또는 변조하는 것이다. 그런데, 단순화하여 보자면 같은 정보가 수백, 수천 개의 노드에 중복되어 저장되므로, 해커가 이미 저장된 데이터를 함부로 위조하거나 변조하는 것은 극히 어렵게 된다. 블록체인 기술은 단순히 여러 노드에 저장되어 있는 것에 그치지 않고, 암호학적인 기법을 이용하여 이미 저장된 데이터를 해킹하여 조작하는 것이 불가능하도록 구성되어 있다.

이러한 방식에 문제점으로서 언급되는 51% 공격은 블록체인의 단점 중 가장 크게 논의되고 있다. 이러한 공격은 단일 혹은 의견이 통합된 단체의 주체(악의를 가진 해킹 공격자)가 네트워크 해싱 파워의 50% 이상을 통제할 수 있게 됐을 때 발생할 수 있으며, 고의적으로 트랜잭션의 순서를 변경하거나 제외하여 마지막에는 블록체인 네트워크를 방해할 수 있다.

분산원장 된 블록 데이터의 51%의 손상은 즉 모든 데이터 블록에 영향을 끼치게 되는 공격이지만 이론적으로 가능한 일임에도 불구하고, 51%의 공격이 비트코인 블록체인에 성공했던 적은 한 번도 없었다. 그러한 이유는 네트워크가 더 크게 성장함에 따라 보안이 증대되고, 이러한 내부 데이터들이 훼손되는 것보다 안전한 상태로 유지되는 것이 더 많은 이익을 얻을 수 있기에, 공격자가 비트코인을 공격하기 위해 많은 돈과 자원을 투자하지 않았기 때문이다.

이러한 퍼블릭 네트워크의 데이터 중복성과 새로운 정보가 추가될 때마다 그 정보가 앞서 저장된 데이터들과 충돌하는지 여부를 확인함으로써 이미 저장된 정보가 변조되거나, 위조된 정보가 데이터베이스에 추가되는 것을 효과적으로 막을 수 있다.

그러나 이러한 공개성 요건은 퍼블릭 블록체인의 활용에 현실적으로 큰 걸림돌이 된다. 예를 들어 많은 기업들은 자신의 거래 정보가 제3자에게 공개되는 것을 원하지 않는다. 혹은 반대로 거래 정보가 경쟁사들 사이에 교환될 경우 공정거래법에 따른 담합으로 판단될 소지도 있다. 따라서 기업의 상거래 정보나 개인정보를 저장하는 수단으로서 전통적 데이터베이스 시스템 또는 최소한의 프라이빗한 블록체인을 고려하게 될 것이다.

또한, 퍼블릭 블록체인은 모든 노드에게 동등한 권한이 부여된다는 특성이 있다. 만약 각 노드별로 읽기, 쓰기 권한을 달리하기 위해서 노드들에게 차별적인 권한을 부여하기 위해 권한의 범위에 대한 판단을 내릴 수 있는 관리자를 지정하거나 또는 의사 결정을 내릴 수 있는 투표 시스템이 필요하게 된다. 하지만 퍼블릭 블록체인에서는 불특정 다수가 동등한 권한을 가지고 참여하기 때문에 이것이 구현되기 어렵다.

마지막으로 퍼블릭 블록체인의 잘 알려진 취약점은 기존 데이터베이스에 비하여 단위 시간 내에 처리할 수 있는 거래의 수가 적고, 거래의 처리 속도가 느리다는 점이다. 비트코인 블록체인은 이중 지출 문제를 작업증명(Proof-of-Work) 개념을 도입하여 해결하였는데, 이는 데이터베이스에 정보가 저장되기 위해서는 상당한 연산을 수행하였다는 점에 대한 증거를 요구함으로써, 특정 정보의 저장 여부를 확정하는 시점을 의도적으로 지연시키는 구조이다. 이러한 퍼블릭 블록체인의 처리 성능은 전통적인 데이터베이스 시스템을 이용한 VISA의 결제 서비스의 경우 초당 평균 약 1,700건을 처리할 수 있음에 비하면 초당 3~20건을 처리하는 현저히 느린 처리 속도를 보유하고 있다.

2.3.2 프라이빗 블록체인을 통한 퍼블릭 블록체인의 문제점 개선

프라이빗 블록체인은 이상에서 설명한 퍼블릭 블록체인의 한계를 극복하는 대안으로 개발된 것으로, 네트워크 자체에 참여할 수 있는 권한을 제한하는 동시에/또는 네트워크에 참여한 각 노드들의 정보에 대한 접근 권한을 각 노드마다 차별적으로 부여할 수 있는 블록체인 방식이다. 전술한 바와 같이 프라이빗 블록체인은 네트워크를 완전한 탈집중화하는 방식을 버리고, 그 대신 부분적인 권한을 가진 관리자(authority)를 도입함으로써, 퍼블릭 블록체인의 현실적 제약들을 해결한다.

프라이빗 블록체인은 그 운영 주체를 기준으로 하여 컨소시엄 블록체인(consortium blockchain)과 단일 주체 블록체인(single entity blockchain)으로 나뉜다. 컨소시엄 블록체인은 여러 기관이나 기업들이 공동으로 블록체인을 운영하는 것으로, 컨소시엄에 가입한 단체로 참여자가 제한된다. 컨소시엄 블록체인을 활용하면 여러 단체가 상위 차원 네트워크를 구축하여 상호 간 정보를 효율적으로 교환하는 것이 가능하게 될 수 있다. 가령 여러 대학들이 공동으로 졸업 정보의 진위 여부를 확인하는 컨소시엄 블록체인을 구축할 수 있다. 요즘 금융권에서 고려중인 대부분의 블록체인 프로젝트도 컨소시엄 블록체인을 도입하는 것으로 보인다.

단일 주체 블록체인은 프라이빗 블록체인 그 자체로 표현할 수 있으며 하나의 운영 기관(기업)이 여러 대의 서버를 두고 그 복수개의 서버상에 데이터를 저장・관리하고, 그 운영 기관의 허락에 따라 제3자가 그 정보에 대해 읽기 권한을 가질 수 있는 구조이다. 이는 정보가 다수의 주체에게 분산되지 않는다는 점에서 전통적인 데이터베이스와 본질적인 차이가 없으나, 기존 기술에 비하여 내부 직원에 의한 데이터의 위조나 변조가 어렵다는 장점이 있다. 하나의 회사 또는 회사 그룹 내의 회계 정보를 블록체인을 통해서 저장하는 방안에 대한 논의는 대부분 위와 같은 단일 주체 블록체인을 도입하는 방향으로 검토가 이루어지고 있는 것으로 보인다. 이러한 프라이빗 블록체인은 참여하는 모든 노드들이 일정한 권한에 복속되어 각 노드들이 규칙에 따라 동작할 것이라는 높은 기대치를 가지고, 그 결과 퍼블릭 블록체인에 비해 훨씬 더 나은 처리 속도와 확정성을 갖는다. 따라서, 성능상 제약 문제로부터 상당히 자유롭게 된다.

또한 프라이빗 블록체인이 제공하는 주요한 기능 중 하나는 블록체인에 저장된 데이터에 대한 접근 권한을 세밀하게 정할 수 있다는 것이다. 즉, 프라이빗 블록체인은 접근 권한에 대해 유연하게 통제할 권한을 부여함으로써 기업 간 비밀정보나 개인정보도 블록체인을 통해 저장할 수 있도록 한다.

이로써 프라이빗 블록체인은 앞 장에서 설명한 퍼블릭 블록체인의 현실적 제약 사항들인 데이터의 공개성, 동등한 권한 부여, 제한된 공간 확장성 문제를 해결한다.

2.3.3 블록체인 기술의 공통적 문제점

앞서 분류된 퍼블릭 블록체인과 프라이빗 블록체인의 장점과 문제점을 대조하여 서술했다면 이번에는 블록체인 기술 자체의 공통적인 문제점에 대해 서술해보고자 한다. 비트코인에 적용되어 시작된 블록체인 기술은 2009년 등장 이래 빠른 속도로 진화하여 여러 분야에 도입되고 있는 반면, 연구 개발 및 시험 적용 단계에서의 블록체인 기술은 적용과 활용 자체에 문제점도 내포하고 있다. 이러한 공통적인 문제점을 나열해보고자 한다.

- 거래검증의 주체가 전 세계에 분포된 노드(컴퓨터)이며 익명의 검증인(사용자)은 방대한 양의 컴퓨팅파워를 이용해 거래를 증명해야 한다. 또 한, 참가한 모든 컴퓨터가 모든 자료를 다운 및 보관해야 하므로 기존 방법에 비해 비효율적이고 이에 투자되는 비용이 낭비된다.

- 블록체인 시스템의 또 다른 단점은 블록체인에 데이터가 기록되면 이를 수정하기가 무척 까다롭다는 것이다. 안정적인 측면에서 볼 때 블록체인의 장점이긴 하지만, 블록체인 사용자가 거래 기록의 일부로 이미지를 첨부할 때 데이터 용량은 급증하게 되고, 시간이 흐름에 따라 일방적인 추가만 가능한 블록체인 방식으로 인해 데이터 용량이 지속적으로 커지게 되면 이는 네트워크 오버헤드로 이어지게 된다. 따라서 일부 거래에 대해서는 통제가 어려운 블록체인 방식보다는 별개의 네트워크 보관소로 운용되는 관계형 데이터베이스의 효율성이 더 높다는 것이다.

- 프라이빗 키

블록체인은 공개 키(혹은 비대칭 키) 암호학을 사용해 사용자가 자신의 암호 화폐 자산(혹은 다른 블록체인 데이터)에 소유권을 주장할 수 있게 구성된다. 각 블록체인 계정(혹은 주소)은 상응하는 두 개의 키를 갖고 있는데, 공유될 수 있는 퍼블릭 키와 개인 검증에 필요한 안전하게 보관되어야 하는 프라이빗 키이다. 사용자는 자신들의 자금에 접근하기 위해 프라이빗 키가 필요하며, 이는 스스로가 자신의 은행 역할을 한다는 것을 의미한다. 사용자가 만약 프라이빗 키를 분실하게 된다면, 사실상 자금을 잃게 되는 것과 같으며, 이를 어찌할 수 있는 방법이 없다.

구분	블록체인 기술의 문제점
불법 거래	- 도박, 마약, 무기 등의 암시장 거래, 불법 상속과 증여 탈세, 비자금, 범죄자금으로 악용 - 불법 거래한 가상화폐 자체의 전자지갑 주소에 대한 익명성은 보장되지만 거래내역은 분산원장에 기록되므로 현금화할 때 사용자 추적 가능
화폐 위상	- 비트코인 등 가상화폐가 실물경제에 영향을 줄만큼 확대되었으나 가치산정과 거래기준에 대한 국제적 규범은 미비 - 금융과 자산의 거래를 관리하기 위해 반허가 및 허가형 블록체인 프로토콜이 공존
인증 거래	- 이더리움 등 스마트계약에 타임스탬프가 포함된 블록체인 기술이 응용되어 소유권 증명, 자동차/주택/부동산 계약, 저작권 인증 등에 활용 - 사적 디지털 인증의 법적 효력과 종이로 된 권리증서의 공존으로 실제 소유에 대한 혼란
용량 확장	- 거래가 폭발적으로 증가하면서 이로 인한 거래지연 등 문제가 봉착하여 현재 1MB 를 향후 2MB, 8MB, 36MB 로 확장시켜야 한다고 주장 - 용량을 확장하면 거래수수료 감소 및 거래경쟁 격화와 채굴의 중앙화 현상 초래

[사진 3] 블록체인 기술의 문제점 4가지

[사진 3]의 사례에서 볼 수 있듯이 블록체인은 불법 거래적인 측면에서, 가상 디지털 화폐가 도박, 마약, 무기 등의 암시장 거래, 불법 상속과 증여 탈세, 비자금이나 범죄 자금 돈세탁의 용도로서 사용되어 부작용이 나타나고 있다. 그러나 불법 거래한 가상 화폐 자체의 전자 지갑 주소는 익명성이 보장되더라도 거래 내역은 분산원장에 기록되어 나중에 현금화를 하게 되면 사용자를 추적할 수 있다.

인터넷 도박, 마약, 무기 등의 불법 거래에 비트코인 등 가상 화폐를 이용하게 되면 자금 추적을 당하더라도 익명성이 존재하여 누가 사용했는지 파악할 수 없기에 문제점으로 지적되며, 과거 핵 개발 관련 미국이 금융제재를 할 때 이란 측 신발 업체가 비트코인으로 대금을 결제하여 감시망을 벗어난 사례도 있었다. 탈세와 관련된 사례로는 부동산의 상속, 증여의 경우에 가상 화폐를 사용하여 익명성으로 인해 탈세가 가능하며, 송수금 기록 등 일체의 기록은 모두 공개되지만 누구에게 얼마를 주었는지, 준 사람과 받은 사람 이외에 제 3자는 관여할 수 없어 탈세의 수단으로 사용되기도 한다. 또 한, 기업의 불법 비자금, 정치인의 뇌물 또는 정치자금, 마피아의 범죄 자금 등을 가상 화폐로 전달하거나 이를 가상화폐로 전환하여, 그 결과 불법 경제 규모를 확대시켜 실물 경제를 교란시킬 수 있다. 최근에는 COVID-19 사태로 인한 가상 화폐의 가치 상승으로 인해 이에 따른 채굴 경쟁으로 일부 해커들이 좀비 컴퓨터를 양산한 뒤 인증서를 조작하여 가상화폐를 불법 채굴하거나, 가상화폐 거래소의 사이트를 해킹하여 고객의 코인을 유출하는 사례가 나타났다.

인증 관리 측면에서 이더리움 등 스마트 계약에 타임스탬프가 포함된 블록체인 기술이 응용되어 소유권 증명, 자동차/주택/부동산 계약, 디지털 저작권 인증 등에 유용하게 활용되고 있으나, 사적 디지털 인증의 법적 효력과 종이로 된 권리증의 공존으로 실제 소유 권리에 대한 혼란이 초래될 수 있다. 즉, 디지털 데이터 기반의 사진, 그림, 서류, 인증서 등에 타임스탬프를 적용하여 소유권을 인증하고 있으며, 다수의 사적 인증 사업자에 의한 소유권 증명이 유사한 디지털 자산으로 중복 인증이 가능할 수 있으며, 이로 인해 소유권의 법적 효력 문제가 발생될 수 있다.

마지막으로 용량의 확장 측면에서 블록체인 원장은 시간이 지나며 데이터가 계속 축적되어 그 데이터의 양들이 너무 방대해 질 수 있다. 이에 해당 원장에서 발생하는 거래의 지연 등 문제가 생길 수 있다. 비트코인 블록체인은 현재 200GB의 저장 공간을 필요로 한다. 이러한 블록체인 규모의 성장 속도는 하드 드라이브(저장 공간)의 성장 속도를 앞지를 것으로 보이며, 원장이 너무 커져 개인이 이를 다운로드하거나 저장할 수 없게 되면 노드를 잃게 될 위험이 있다. 그렇다고 지속적으로 용량을 확장시키게 된다면 거래 수수료가 감소하고 거래 경쟁의 격화로 해당 암호 화폐 채굴자들은 수수료를 줄일 수밖에 없고, 이에 따라 대규모 코인 채굴자만이 이익을 얻는 채굴의 중앙화 현상이 초래할 수 있다.

3. 결론

블록체인 기술은 2009년 비트코인 출시 후 급속도로 변화하는 이 시대에서 고유한 장점들을 제공하며 성장하여 대중화 되고 있는 반면, 첫째, 거래검증 시 방대한 자료의 기록 및 보관에 대한 투자 비용의 비효율성과 둘째, 블록체인 네트워크에 대해 수행할 수 있는 몇 가지 잠재적인 공격에 대한 손상으로 블록체인 시스템의 또 다른 단점은 블록체인에 데이터가 기록되면 이를 수정하기가 무척 까다롭다는 점, 셋째, 퍼블릭 키와 프라이빗 키 분실 시 사실상 정보에 접근이 불가하여 다수의 소유권의 법적 효력 문제 발생 가능성, 마지막으로 량의 확장 측면에서 블록체인 원장은 시간이 지나며 데이터가 계속 축적되어 그 데이터의 양들이 너무 방대 해질 수 있는 등의 문제점을 내포하고 있다.

따라서 암호 화폐의 구현에서 시작된 블록체인 기술이 향후 여러 요소의 기술 및 융합 기술의 형태로 다양한 분야에 활용될 것이므로 블록체인 기술의 이해를 바탕으로 단점을 보완하는 연구가 필요할 것이다.

각 나라마다 블록체인 기술을 다양한 분야에 활용하고자 하는 시도를 하고 있고, 암호화폐뿐만 아니라 금융서비스, 전자상거래 및 물류 공급망, 국제무역, IOT 그리고 의료와 헬스케어, 공공기록관리 등 다양한 영역에서 블록체인 기술을 적용하려는 노력이 이루어지고 있으며 향후 무궁무진한 기술의 발전 가능성을 내포하고 있다. 그러나 최근 가상화폐 시장이 빠른 속도로 성장하면서, 강력한 규제 조치가 없을 경우 제2의 서브프라임 모기지 사태[3]를 촉발 시킬 수 있을 것이라는 우려에 각별한 주의를 기울여야 한다는 목소리 또한 높다.

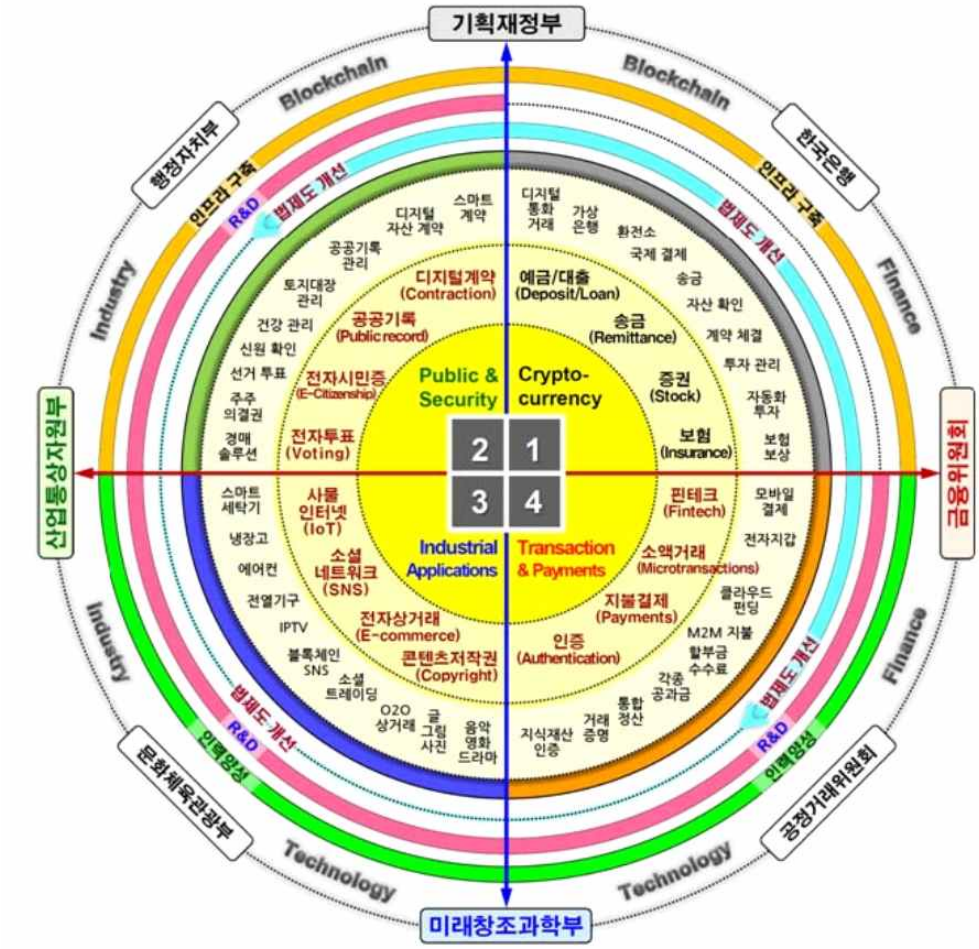
국내에서도 그동안 정부가 '블록체인 기술은 육성하되 암호화폐는 금지한다'는 정책 기조 하에 암호화폐 산업을 사실상 방치해 왔던 방향에서 벗어나 '특정 금융거래정보의 보고 및 이용 등에 관한 법률(이하 특금법)[4] '에 특금법 개정안(2021.3.5)은 통해 암호화폐 거래소 신고제를 비롯해 암호화폐 거래소에 자금세탁방지 의무를 부과하고 '실명계좌 및 정보보호인증(ISMS)'을 골자로 한 법안이 최종 통과되고 국내에서 암호화폐 관련 법안이 처음으로 공식 제정된 만큼 그동안 외면받았던 암호화폐 관련 사업이 제도권으로 진입할 근거가 마련됐다고 볼 수 있다.

그러나 개별적인 법률 및 제도에 대한 논의가 부족한 만큼 향후 새로운 시장에 대한 규제당국과 감독체제 설립 및 개별적인 법제(예를 들어 전자금융거래법, 전자상거래법, 증권법 등)에 대한 법률적 제도와 디지털 산업에 특화된 규제체계 및 사기 방지 및 정보 공개 상호 운용에 개선방안에 대한 자세한 연구를 통해 제도권적 규제기관이 만들어져 정책을 통해 블록체인 활용 생태계와 연계하여 발전시켜 나가야 할 것으로 사료된다.

---

3) 서브프라임 모기지 사태(subprime mortgage crisis): 2007년 미국의 초대형 모기지론 대부업체들이 파산하면서 시작된, 미국만이 아닌 국제금융시장에 신용경색을 불러온 연쇄적인 경제 위기를 말한다.

4) 외국환거래 등 금융거래를 이용한 자금세탁 행위를 규제하는 데 필요한 특정 금융거래정보의 보고 및 이용 등에 관한 사항을 규정함으로써 범죄행위를 예방하고, 건전하고 투명한 금융거래 질서를 확립하기 위하여 제정한 법(2001. 9. 27, 법률 제6516호). [네이버 지식백과]



[사진 4] 블록체인 기술의 활용 및 정책 방향

그동안 블록체인은 암호 기술이 주도하고 혁신가 중심으로 비즈니스 모델이 개발되어 왔지만, 점차 산업이 확장되고 전반에 활용됨으로써 글로벌 ICT 기업들도 적극적으로 블록체인 기술 개발에 참여하고 있다. 우리나라도 IoT 연계 생활 가전 장치, 디지털 자산/콘텐츠 시스템 등의 분야에 연구 개발을 강화한다. 점차 발전해 나가는 블록체인 기술을 활성화하고 글로벌 시장을 선도하기 위해 우리나라는 [사진 4]와 같이 연구 개발과 인력 양성을 추진하고, 기타 정부 조직은 법제도 개선과 인프라 구축 등을 공공 기반 사업으로 추진하는 국가 차원의 정책 방안을 마련해야 한다.

많은 문제점을 가지고 있음에도 불구하고, 블록체인 기술을 활용함으로써 정보의 중복성 및 부정확성 등의 문제를 해결하기 위한 비용을 절감하고, 정보의 보안성 및 투명성을 제공함으로써 특정 이해관계자들이 불이익 혹은 기회주의적 행동을 차단하는 역할을 한다. 또 이러한 서비스를 통해 모든 이해 관계자들은 어우러 혜택을 받을 수 있는 비즈니스 모델 설계가 가능하여 블록체인 기반의 서비스 및 활용 모델을 기존의 서비스를 대체할 가능성을 보여주고 있다. 이러한 블록체인 기술만의 고유한 장점은 대중화되어 사람들에게 제공되고 있다. 주류에 채택되기까지는 아직 발전해야 하는 기술이지만, 향후 몇 년 동안 블록체인 기술의 가치를 최대한 더할 수 있는지 알아내기 위해 기업과 정부는 해결 방안에 대해 고민하며 새로이 실험해나가야 할 것이다.

참고문헌

[사진 1] 출처 : SW 중심사회

[사진 2] 출처 : https://m.blog.naver.com/dhl_korea/221249443137

[사진 3] 임명환, 블록체인 기술의 활용과 전망, ETRI, 2016, 5, 31 p.6

[사진 4] 임명환, 블록체인 기술의 활용과 전망, ETRI, 2016, 5, 31 p.12

[1] https://www.weusecoins.com/

[2] 한수연(2016), “블록체인 비트코인을 넘어 세상을 넘본다”

[3] 고윤승, 최흥섭(2017), “비즈니스 패러다임 변화와 그 활용 방안 – 블록체인기술을 중심으로-

[4] 이종기(2017), “블록체인에 의한 분산형 원장 처리 기법의 탐색적 사례연구: IMB Bluemix 블록체인을 이용하여”

[5] 나무 위키
https://namu.wiki/w/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8
– 암호화폐

[6] DBpia 한국컴퓨터정보학회논문지 26(2), 2021.2, 89-97 (9 page)(통권 제203호) 이새봄(Kyung Hee University), 박아름(Kyung Hee University), 송재민(Kyung Hee University) – 블록 체인 기술과 활용 연구

[7] 블록 체인의 장단점 (기술 활용 방법)
https://wing-health.tistory.com/entry/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8Block-Chain%EC%9D%B4%EB%9E%80-%EB%9C%BB%EA%B3%BC-%EC%9E%A5%EC%A0%90-%EB%8B%A8%EC%A0%90-%EC%A0%95%EB%A6%AC

[8] Everledger, https://everledger.io/

[9] Steemit, https://steemit.com/kr/@mechuriya/4-steem-token-economy

[10] Civic, https://www.civic.com/company/

[11] 블록체인 기술의 활용 범위에 관한 비판적 고찰
(A Critical Analysis on Application of Blockchain Technology) 김광필, 전정현

[12] 더루프, “퍼블릭 블록체인의 한계와 프라이빗 블록체인
https://www.bloter.net/newsView/blt201703070002

[13] 임명환, 블록체인 기술의 활용과 전망, ETRI, 2016