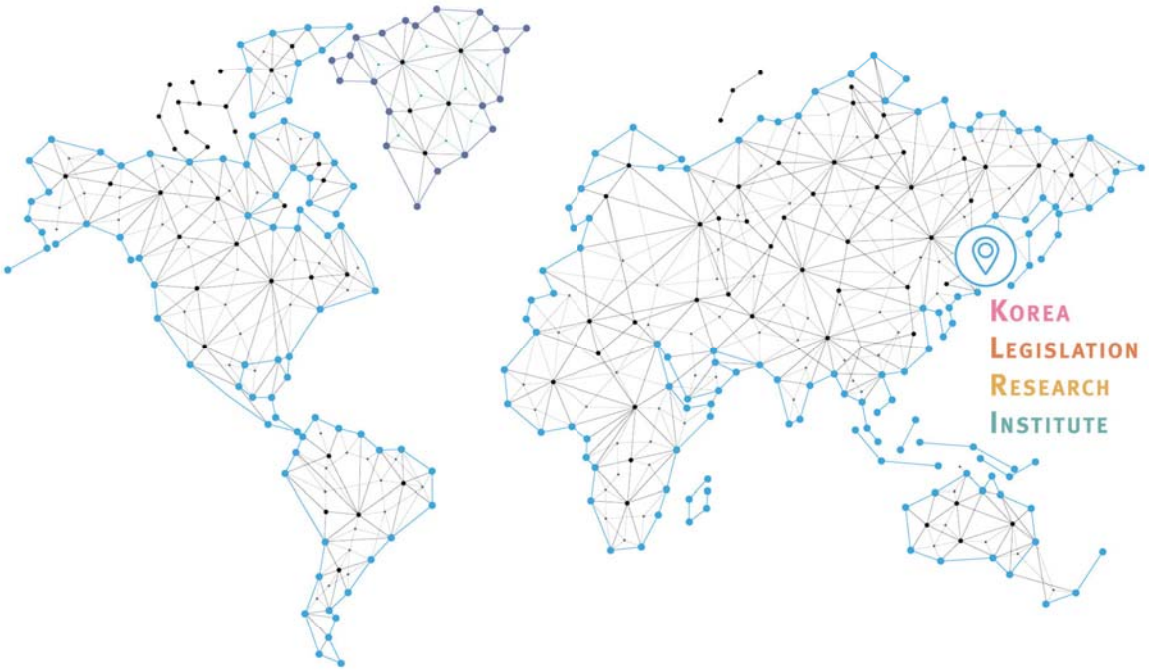
Global Issue Paper 16-20-②



블록체인 분산원장 도입을 위한 법적 과제

정 승 화 (한국예탁결제원 부장, 법학박사)

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

블록체인 분산원장 도입을 위한 법적 과제

정 승 화 (한국예탁결제원 부장, 법학박사)

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

KOREA LEGISLATION RESEARCH INSTITUTE

CONTENTS

Ⅰ. 서 론

- 2009년 사토시 나카모토(Satoshi Nakamoto)에 의해 처음 실제적으로 구현된 탈중앙화된 화폐는 공개키(public key) 암호방식과 소유권 관리를 위한 작업증명(proof-of-work)이라고 알려진 합의 알고리즘이 결합되어 가능하게 되었는데, 그것이 바로 블록체인(Blockchain) 기술을 활용한 비트코인(Bitcoin)임

- 블록체인 기술은 상호분산원장(mutual distributed ledger)을 통하여 기존 중앙집중형 네트워크 기반의 인프라를 뛰어넘는 높은 보안성, 확장성, 투명성 등을 보장하는 것으로 알려져 큰 관심을 받고 있음

  - 블록체인은 네트워크 접근권한 및 작업증명 참가권한에 따라 별도의 권한이 필요 없는 공공형 블록체인(public blockchain), 네트워크 접근은 자유로우나 작업증명에는 권한이 필요한 컨소시엄형 블록체인(consortium blockchain), 네트워크 접근 및 증명 작업에 권한이 필요한 사적 블록체인(private blockchain)이 있음

- 블록체인은 우선적으로 은행과 증권과 같은 금융 분야에서 그 적용이 시도되고 있는데, 이외에도 정부분야와 사물인터넷 부분에서 그 적용이 시도되고 있는 등 그 잠재적 적용 분야가 매우 다양하여 인터넷과 같은 혁신적 기술로 평가되고 있음

  - 은행분야의 경우 지급결제, 해외송금 분야에서, 증권분야의 경우 증권발행, 증권거래, 증권결제, 자산관리서비스, 파생거래 등의 분야에서, 비금융 분야의 경우 자산등록부, 신원등록부, 지적재산, 음악 및 엔터테인먼트, 전자장치 및 사물인터넷, 정부 및 대리인 사용, 전자공증, 공인인증서 발급 등의 분야에서 그 적용이 시도되고 있음

- 세계적인 금융기관들은 플랫폼 생태계를 선도하기 위하여 서비스와 표준화를 위하여 글로벌 블록체인 컨소시엄(R3 CEV), 하이퍼레저(Hyperledger) 프로젝트 등의 진행하고 있으며, 국내에서도 은행들은 블록체인 기술을 통하여 해외송금서비스를 개발 중이며, 증권회사의 경우 금융투자협회를 중심으로 공동으로 블록체인 기술을 활용하여 공인인증서를 대체하는 개인 인증서비스를 개발 중에 있음

  - 블록체인 기술의 활용은 기술의 완성도 미흡, 활용에 대한 규제 장애, 대규모 적용사례 부재 등으로 기술개발 및 도입이 지연되고 있으나, 장차 기술의 발달, 규제 장벽 철폐, 적용사례 확대 등으로 안정적인 블록체인 네트워크 생태계가 마련될 것으로 예상

- 본 자료에서는 먼저, 블록체인에 대한 이해, 블록체인의 국내외 동향, 금융 분야와 비금융 분야에서의 활용, 블록체인 기술의 도입방향과 방법 등에 대하여 살펴본 후 블록체인 기술의 활용을 위한 주요 법적과제에 대하여 살펴보고자 함

Ⅱ. 블록체인의 이해

1. 블록체인의 개요

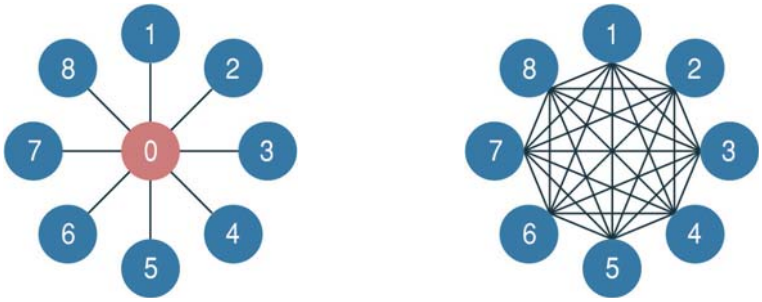
≡ 블록체인의 개념

- 블록체인(blockchain)은 디지털 가상화폐의 대명사인 비트코인에 적용된 기술로서 거래정보를 기록한 원장(ledger)을 모든 참가자가 분산(distributed) 보관하고 신규거래가 발생하거나 기존 거래에 편집이 실행되면 암호인증으로 새로운 블록이 체인처럼 연결되는 방식으로서 특정의 제3기관(trusted third party)의 중앙 서버가 아닌 온라인 P2P(Peer-to-Peer) 네트워크* 에 분산하여 참가자가 공동으로 거래정보를 기록·관리하고, 주기적으로 갱신되는 디지털 공동분산원장(mutual distributed ledger)을 의미[1]

  * 클라이언트나 서버의 개념 없이 동등한 참가자(peer nodes)들이 클라이언트와 서버의 역할을 동시에 수행하며 데이터나 주변 장치 등을 공유하는 방식

1_ Andres Guadamuz and Chris Marsden, "Blockchain and Bitcoin : Regulatory response to cryptocurrencies," (First Monday – Peer Reviewed Journal On The Internet, Volume 20, Number 12 ~ 7 December 2015), p.57; Andreas M. Antonopoulos LLC, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 2015, p.163; McKinsey & Company, "Beyond the Hype: Blockchain in Capital Markets," (McKinsey Working Papers on Corporate & Investment Banking/No.12, December 2015), p.4; CoinDesk, "Banks and the Blockchain Report," 2015, p.6; Michael Mainelli/Alistair Milne, "The Impact and Potential of Blockchain on the Securities Transaction Lifecycle," (SWIFT Institute, SWIFT Institute Working Paper No.2015-007, 09 May 2016), p.3; 김동섭, 「분산원장 기술과 디지털통화의 현황과 시사점」, (한국은행, 금융결제국 결제연구팀), 2016.01, 4면.

그림_ 01 클라이언트·서버와 P2P 네트워크 모델 비교



클라이언트 · 서버 모델　　P2P 네트워크 모델

- 블록체인 기술을 통한 분산원장에서는 모든 참가자가 거래내역이 기록된 원장 전체를 각각 보관하고 새로운 거래를 반영하여 갱신(update)하는 작업도 공동으로 수행

■ 블록체인은 블록(block)을 잇달아 연결한 모음[2]으로 유효화된 블록의 집합으로서 블록에 일정시간 동안 확정된 거래내역을 담는 공개분산원장 금융장부로서, 각 블록은 이전에 생성된 블록과 연결되어 최초블록(genesis block)까지 이어짐

- 블록체인은 공개분산장부인 블록에 거래들을 포함시키기 위해 한데 합쳐 놓은 긴 컨테이너 데이터 구조로서, 블록은 메타데이터를 담고 있는 헤더와 그 뒤에 블록 크기를 결정하는 거래 목록이 길게 나열되어 있음

  * 블록(block)은 거래의 집합으로 타임스탬프와 이전 블록의 지문이 표시되어 있는데, 블록헤더를 요약해서 작업증명**을 만들고 이를 통해 거래가 유효화 되며, 유효화된 블록들은 네트워크의 동의를 얻은 후 블록체인에 추가되며, 작업증명은 블록을 찾기 위해 다량의 계산을 요구하는 데이터임

- 각 블록은 분장원장(distributed ledger)으로서 기능하며 이 분산원장에는 지금까지 처리된 거래정보가 포함되어 있어서 참가자의 컴퓨터에서 거래의 유효성을 검사할 수 있음

2_ 과반수의 사용자가 동의한 거래내역만 보관할 블록으로 묶고, 새로 만든 블록은 이전 블록체인 뒤에 덧붙이는 과정을 반복함

- 이러한 블록체인은 분산 데이터베이스의 한 형태로 지속적으로 성장하는 데이터 기록 리스트로서 분산 노드(Node)의 운영자에 의한 임의 조작이 불가능하도록 고안됨
  - 블록체인의 대표적 응용사례는 암호화폐의 거래과정을 기록하는 탈중앙화된 전자장부로서 비트코인이며, 이 거래기록은 의무적으로 암호화되고 블록체인 소프트웨어를 실행하는 컴퓨터상에서 운영

블록체인의 구조

- 블록체인은 이전블록의 정보, 현재의 거래정보 및 해쉬 값 등을 포함하여 블록을 생성하므로 블록의 내용을 조작할 수 없으며, 거래정보가 공유되어 있기 때문에 투명하게 관리가 가능함[3]

그림_ 02 금리 블록체인의 기본 구조

자료 : BITCOINIST.NET, Thoughts on Bitcoin Block Size Economics 그림 재구성

- 각 블록은 헤더와 바디로 구성된 구조체로 헤더에는 이전, 현재 블록의 해쉬 값, 넌스(Nonce) 등을 포함하고 있으며, 블록 검색 시 데이터베이스 인덱스 방식으로 데이터 값을 찾음[4]
  - 블록헤더에는 다음 블록의 해쉬 값을 포함하지 않으나, 편의상 값을 추가하여 이용

3_ 금융보안원, "블록체인(Blockchain) 개요 및 활용사례," 2015.6.24, 1면.
4_ 금융보안원, "블록체인 및 비트코인 보안기술," 2015.11.23, 1면.

- 블록헤더는 다음과 같은 블록 메타데이터(metadata)의 3가지 집합으로 구성되어 있음[5]
  - 첫째 부분은 현재의 블록이 블록체인에 있는 이전 블록과 연결되었음을 나타내는 이전 블록 해쉬 값이 있음
  - 둘째 부분은 난이도(difficulty)*, 타임스탬프(time stamp), 난스(nonce)로 구성

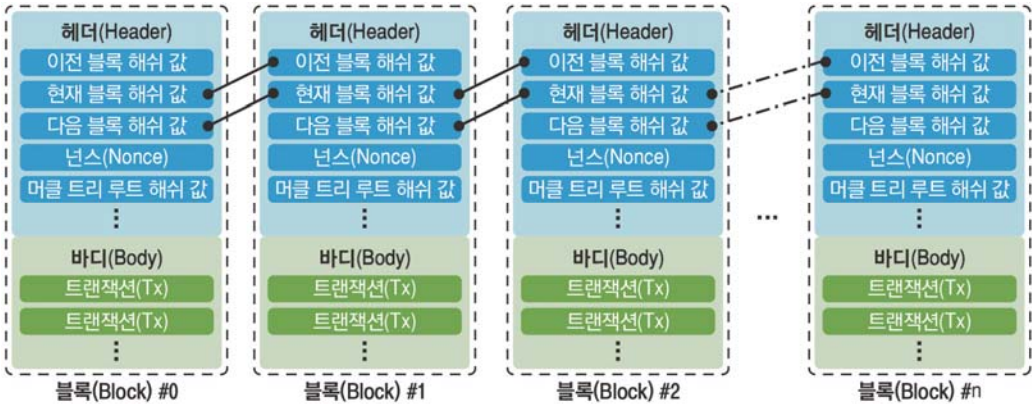
    * 난이도는 작업증명을 하기 위해서 얼마나 많은 계산이 필요한지를 제어하는, 전 네트워크의 설정값임
  - 셋째 부분은 머클트리루트(Merkle trees root)로서, 머클트리루트는 블록 내에서 거래 전부를 효율적으로 요약하는데 사용되는 데이터 구조

표_01 블록 헤더의 구조

크 기	필 드	설 명
4바이트	버 전	소프트웨어/프로토콜 업그레이드 추적을 위한 버전번호
32바이트	이전 블록 해쉬	체인 내 이전(부모)블록의 해쉬에 대한 참조 값
32바이트	머클 루트	해당 블록에 포함된 거래로부터 생성된 머클 트리의 루트에 대한 해쉬
4바이트	타임 스탬프	블록의 대략적인 생성시간(유닉스 기준일로부터 초단위로 계산)
4바이트	난이도 목표	블록의 작업증명 알고리즘에 대한 난이도 목표
4바이트	난 스	작업증명 알고리즘에 사용되는 카운터

5_ 최은실, 김도훈, 송주한(역저), 「비트코인, 블록체인과 금융의 혁신」, (고려대학교 출판문화원, 2015.10), 233면.

그림_ 03 블록체인의 연결구조 [6]



- 블록체인 데이터 구조는 거래가 담겨있는 블록이 그 이전블록과 연결되어 있는 형태의 정돈된 목록으로서, 블록체인은 플랫 파일의 형태로 저장되거나 단순한 데이터베이스 내에 저장될 수 있음
  - 블록체인 내에 있는 블록 각각은 해쉬를 이용해 식별되며, 해쉬는 2진수 입력에 대한 디지털 지문으로서 블록의 헤더에서 SHA256 암호화 해쉬 알고리즘을 이용해 생성됨
  - 해쉬는 주어진 문자열을 특정 알고리즘에 적용하여 축약시켰을 때 유일하게 생성되는 난수와 유사하여 원본데이터가 바뀌지 않는 한 해쉬값은 항상 동일

- 각 블록은 블록헤더에 있는 '이전블록해쉬' 필드를 통해 부모블록이라고 알려진 이전블록을 참조하는데, 이는 각 블록이 자신의 블록 헤더 내에 있는 부모블록의 해쉬를 포함하고 있음을 의미
  - 각 블록과 그 부모블록을 연결해 주는 해쉬의 배열은 최초블록인 첫 생성 블록까지 이어지는 체인을 만듦

6_ Andreas M. Antonopoulos LLC, op. cit., p.165.

- 블록은 단 한 개의 부모블록을 가지며, 자식블록 각각은 동일한 부모블록을 참조하며 '이전블록해쉬' 필드에 있는 동일한 (부모)해쉬를 담고 있음[7]

- '이전블록해쉬' 필드는 블록헤더 내에 들어 있으며, 이러한 특성 때문에 블록의 해쉬에 영향을 미치며, 부모블록의 정체성 이 변경되면 자식블록 자체의 정체성도 변경됨
  - 부모노드가 어떤 방법으로든지 수정되는 경우 부모노드의 해쉬도 변하여 부모노드의 해쉬가 변경되면 자식노드의 '이전블록해쉬' 포인터도 변경되어야 함
  - 그 결과 자식노드의 해쉬도 변해야 하고, 손자노드의 포인터도 변해야 하고, 증손자의 노드도 계속해서 변해야 함
  - 이러한 연쇄효과 덕분에 블록 하나가 그 아래에 여러 세대를 두는 경우 나중에 생성된 블록 전부를 재계산해야만 해당 블록의 내용을 변경시킬 수 있음
  - 이러한 재계산을 위해서는 엄청난 규모의 계산을 실행해야 하기 때문에 체인으로 연결된 블록들은 블록체인의 누적된 기록을 변경시킬 수 없으며, 이러한 특성 덕분에 블록체인 기술의 보안성이 유지됨[8]

- 블록의 주요식별자는 디지털지문역할을 하는 암호화 해쉬로 SHA256알고리즘을 통해 블록헤더를 해싱해서 얻어진 결과값으로 나온 32바이트 크기의 해쉬를 블록해쉬라 함[9]
  - 블록헤쉬는 유일하고 확실한 방법으로 해당 블록을 식별하며, 모든 노드는 블록헤더를 간단히 해싱함으로써 독립적으로 블록 해쉬값을 얻을 수 있음
  - 대신 블록해쉬는 해당 블록을 네트워크에서 전송받으면서 각 노드에 의해 계산되며, 블록의 메타데이타의 일부로 별도의 데이터베이스 테이블 내에 저장될 수도 있는데, 이를 통해 디스크로부터 블록에 대한 색인을 용이하게 하고 검색 속도를 향상시킴

7_ Andreas M. Antonopoulos LLC, Ibid., p.165.
8_ 최은실, 김도훈, 송주한(역저), 앞의 책, 232면.
9_ 최은실, 김도훈, 송주한(역저), 앞의 책, 233면.

- 블록체인 내의 첫번째 블록을 최초블록이라 하며, 블록체인 내에 있는 모든 블록의 공통된 선조로서 고정적으로 인코딩되어 있기 때문에 모든 노드는 적어도 하나의 블록으로 구성된 블록체인으로 시작하며, 이러한 이유로 최초블록은 변경이 불가능[10]
  - 모든 노드는 최초블록의 해쉬와 구조, 생성시간, 최초블록 내에 있는 단일 거래까지도 항상 '알고' 있음
  - 따라서 모든 노드는 블록체인 생성의 시작점을 가지고 있으며, 최초블록은 신뢰받는 블록체인을 만드는데 기반이 되는 안전한 '루트'인 것임
- 블록체인은 고도의 보안전략 및 기술적 요소들이 내포된 금융거래 기술의 하나로서 4가지의 과정을 통해서 블록체인이 완성됨[11]

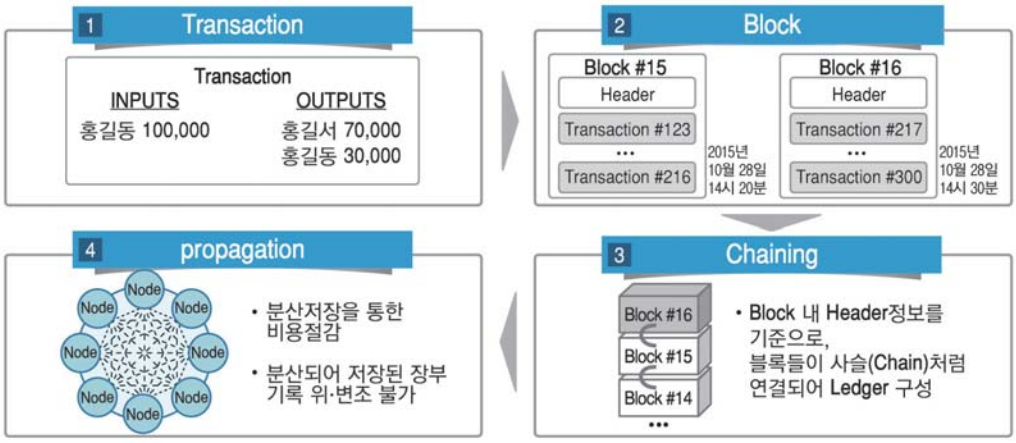
표_ 02 블록체인의 금융거래단계

거래단계	내 용
1단계 (거래단계)	A 라는 소유자가 B 라는 사람에게 특정금액을 거래하는 단계
2단계 (암호화단계)	거래 내용들이 블록에 저장되며, 거래에 암호화가 적용되어 거래 자체를 위변조 등 불가
3단계 (상호연결단계)	블록들이 순서대로 서로 묶이게 되며, 거래들이 모여서 블록을 생성하게 되고, 이 블록들은 일련의 순서대로 이전의 블록 B, C와 연결되어 하나의 거대한 관리 대장이 됨
4단계 (분산저장단계)	서로 사슬처럼 연결된 블록들을 거래에 참가한 여러 대의 컴퓨터들이 모두 장부를 똑같이 가지고 있게 되며, 분산저장된 장부는 블록으로 연결되어 있어 모든 컴퓨터를 해킹하지 않는 이상 조작될 수 없음

* 블록체인을 해킹하려면 6만 4천대의 슈퍼컴퓨터(일반컴퓨터 1,500억대)가 필요하며, 이들 6만 4천대의 슈퍼컴퓨터 운영에 드는 전기비용을 내야 할 정도로 해킹에 천문학적 비용 발생

10_ 위의 책, 236면.
11_ 박소영, "Blockchain," (PayGate, 2015.12), 18면.

그림_ 04 블록체인 개념도 [12]



2. 기존 중앙집중형과 분산원장형의 비교 [13]

- 현재까지 자산에 대한 소유권은 실물보관 여부와 무관하게 특정한 기관에서 관리하는 원장(ledger)에 기록(record)된 바에 따라 결정되었음
  - 예금의 경우 은행이 고객별로 잔고를 관리하면서 입출금을 승인하고 기록
  - 주식 등과 같은 증권의 발행은 발행회사, 명의개서대리인 또는 등록기관이 관리하는 주주명부, 사채원부, 채권등록부 등의 장부를 통하여 발행되고 관리되고 있음
  - 예탁된 주식, 채권 등 증권은 예탁결제원의 예탁자계좌부상 계좌대체의 방법으로 매매에 따른 결제를 처리
  - 토지, 건물 등 부동산은 등기소에서 소유권 및 담보권 등을 보존등기, 변경등기, 경정

12_ 박소영, 앞의 글, 17면; 정유신, "블록체인의 금융산업에 대한 영향과 정책과제," 2016. 5, 2면.

13_ 박정국, "블록체인 기술의 동향과 금융권의 대응,"「블록체인 : 금융산업의 파괴자인가 아니면 새로운 기회인가?」(한국지급결제학회 2016년 춘계세미나, 2016.6.1.), 44면.

등기, 말소등기, 회복등기 등을 통하여 기록관리

- 이 같은 중앙집중방식은 자산을 직접 보관하는 방식에 비해 비용을 절감하고 소유권을 명확히 할 수 있는 장점을 가지는 반면, 기록을 관리하는 권한과 책임이 특정기관에 집중되어 중앙집중기관에 대한 신뢰*에 크게 의존하는 한계도 있음

  * 특정기관이 원장을 조작 또는 개인정보를 유출하지 않을 뿐 아니라 시스템 오류 및 처리속도 저하를 예방하고, 해킹 등 외부로부터의 악의적인 공격 및 조작 시도를 방지할 수 있다는 신뢰가 필요[14]

- 장부를 중앙집중형으로 관리하는 기존 시스템은 신뢰할 수 있는 제3의 기관(trusted third party)을 설립하고 해당 기관에 대한 신뢰를 확보하는 방식으로 발전해 왔음

  - 이에 따라 특정기관에서 조작 등 문제가 발생하여 시스템에 대한 신뢰가 훼손되는 것을 예방하기 위해 감독과 감시 등 규제를 제도화

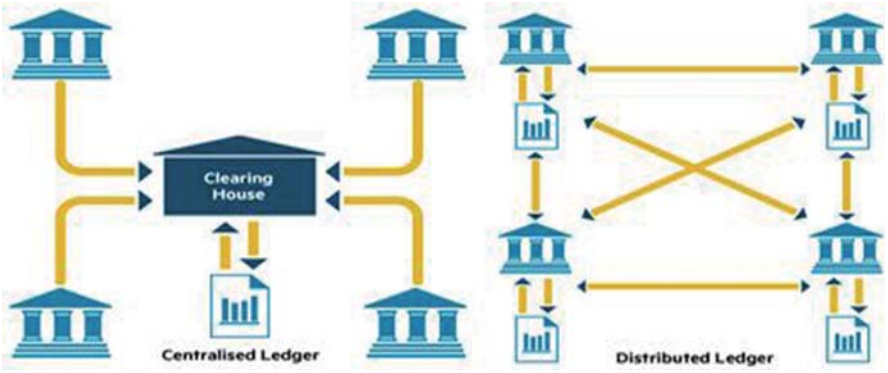
  - 또한 전산시스템의 오류 및 해킹 등이 발생하여 시스템이 마비되거나 이용자 피해가 발생하지 않도록 IT 인프라와 보안 등에 대해 대규모 인력 및 설비를 투자

- 그러나 신뢰할 수 있는 제3의 기관을 설립하여 운영하는 데 소요되는 높은 사회적 비용은 금융산업 발전의 제약 요인으로 작용할 수 있음

  - 대규모 조직을 설립 · 운영하기 위한 비용은 이용자의 높은 수수료 부담으로 이어지며, 규제 및 감독은 진입장벽으로 작용하여 혁신적 신규 서비스 및 사업자의 진출을 제한[15]

14_ 김동섭, 앞의 책, 3면.
15_ 김동섭, 앞의 책, 5면.

그림_ 05 기존방식 및 블록체인 방식 구조 비교



기존 방식(중앙집중원장) 블록체인 방식(분산원장)

자료 : FT, Santander InnoVentures

표_ 03 기존과 블록체인 기반 전자금융거래 비교[16]

기존 전자금융거래	구분	블록체인 기반 전자금융거래
• 중앙집중형 • 개인과 제3자 신뢰기관(은행, 중앙예탁기관, 정부 등) 간 거래	개념	• 분산형 구조 • 거래내역을 모든 네트워크 참가자 공유 및 보관 • 모든 거래참가자가 거래내역을 확인하는 공증 및 관리
• 빠른 거래 속도	장점	• 거래 정보의 투명성 • 적은 시스템 구축 및 유지보수 비용 • 해킹 공격 불가능
• 해킹에 취약 • 중앙시스템 보안 위험 및 관리비용 높음	단점	• 상대적으로 느린 거래 속도 • 제어의 복잡성

16_ 금융보안원, "국내외 금융분야 블록체인(Blockchain) 활용동향," (보안연구부 – 2015 – 028, 2015.11.23), 4면.

3. 블록체인의 종류[17]

- 블록체인 네트워크 참가자의 성격과 범위, 작업증명 참가권한에 따라 공공형 블록체인(public blockchain), 사적 블록체인(private blockchain), 컨소시엄 블록체인(consortium blockchain)으로 구분할 수 있음

≡ 공공형 블록체인

- 공공형 블록체인(public blockchain)은 비트코인에서 적용된 블록체인 기술로서 노드에 제한이 없고, 공개성과 분산성 형태로서 합의에 의해 거래가 승인되는 특징을 가지고 있으며, 공개형 블록체인이라고도 함
  - 공공형 블록체인은 현재 가장 일반적으로 이용되는 유형으로 개인 또는 중앙관리기관 등 어떠한 제약사항 없이 블록체인 네트워크에 참가하여 이용할 수 있으며, 네트워크 참가자들은 컴퓨팅 파워를 이용하여 거래의 정당성을 입증할 수 있음
  - 비트코인이나 이더리움(Ethereum)[18]에서 작동하는 블록체인은 모두 공공형 블록체인을 활용한 가상화폐이자 스마트금융 플랫폼임
  - 공공형 블록체인은 불특정 다수의 참가를 통해서 운용되기 때문에 참가와 충성도를 유도하기 위해 채굴자(miner)들에게 비트코인과 이더리움과 같은 블록체인 상에서 발행된 코인의 지불과 같은 경제적 인센티브 필요

17_ 한승우, "블록체인 활용사례로 알아보는 금융권 적용고려사항," 「전자금융과 금융보안」(금융보안원, 2016.1), 26면 참조; 김태우, "블록체인이 자본시장에 미치는 영향," 「예탁결제」(한국예탁결제원, 제97호 2016－1분기, 2016), 31~33면 참조.

18_ 이더리움(Ethereum)은 2013년 비탈릭 뷰테린(Vitalik Buterin)에 의해 고안되었으며, 프로그래밍이 가능한 블록체인(programmable Blockchain)을 구현한 웹 프레임워크로서 확장된 분산어플리케이션을 만들 수 있는 플랫폼을 제공하는 것임. 이더리움은 비트코인이 화폐로서의 신뢰성을 보장하기 위한 체계를 구축하였지만, 시스템을 확장하고 개선하기 위한 협의가 이루어지지 않아 지속적으로 실패론이 대두됨에 따라 비트코인을 이용한 서비스 개발에는 한계가 있으며 추가 기능을 개발하기 위해서는 상당량의 코드 수정이 필요하므로 매우 비효율적이라는 문제점을 개선하기 위해서 등장(금융보안원, "이더리움(Ethereum) 소개 및 특징 분석," 보안연구부－2016－0098, 2016.3.4), 1면.

≡ 사적 블록체인

- 사적 블록체인(private blockchain)은 개인화된 블록체인으로써 한 중앙기관이 규칙변경, 기록 되돌리기 등 모든 권한을 가지며, 네트워크에 참가하기 위해서는 이 기관의 허가가 필요하며, 인프라 구축을 위한 비용 절감과 효율성 향상 등의 특징이 존재하는데, 비공개형 블록체인이라고도 함
  - 사적 블록체인은 자신들의 목적과 특성에 맞게 설계한 블록체인이기 때문에 블록체인의 공개성과 분산성과 같은 특성을 모두 다 구현하지 않아도 되며, 기존의 인프라와 유사하며 암호감사(cryptographic auditability)의 기능이 추가된 기존의 중앙집중식 데이터베이스라고 볼 수 있음
  - 사적 블록체인 상에서는 네트워크상의 운용 노드가 제한되어 있기 때문에 굳이 코인 발행과 같은 경제적 인센티브 불필요
  - 사적 블록체인은 고유 화폐를 통한 네트워크 유지나 지불 · 결제와 같은 용도로 사용되기보다는 데이터를 분산 관리하는데 더욱 적합한 방식의 블록체인이라 할 수 있음

≡ 컨소시엄 블록체인

- 컨소시엄 블록체인(consortium blockchain)은 공공형 블록체인과 사적 블록체인이 결합된 형태로서, 네트워크에 참가하는 것은 자유로우나 미리 선정된 참가자에 의해서 제어되며, N개의 참가자에게 권한을 부여하여 각 참가자의 동의에 의해서 거래를 기록하도록 함
  - 컨소시엄 블록체인은 이용자들에게는 기록을 열람할 수 있도록 권한을 부여할 수 있지만, API를 통해 특정 대상에게만 공개할 수도 있으며, 일부기업이나 기관 등의 협업을 위해 컨소시움을 구성하는 모델이 이에 해당될 수 있는데, 반공개형 블록체인이라고도 함
  - 컨소시엄 블록체인은 미리 선정된 여러 기관이 컨소시엄을 이루고 기관들이 블록체인 데이터베이스를 복사하여 보관하는 방식으로서 각 기관이 한 개의 노드씩 담당하고, 이 노드들이 동의를 이루어야 승인이 되는 방식

- 승인권자인 노드들이 시장유지 등 자신의 이익을 위해 채굴의 역할을 수행함으로 비트코인 채굴시 발생하는 비트코인과 같은 경제적 유인책 불필요

소 결

- 공공형 블록체인은 금융기관의 블록체인 응용목적인 법적 정당성, 효율성, 거래속도와 같은 문제를 해결해 주지 못하기 때문에 금융기관은 컨소시엄이나 사적 블록체인을 선택할 것임
  - 금융거래의 경우 거래오류 발생과 이에 대한 정정 등이 필요한 경우 공적인 권위에 의한 수정이 필요하기 때문에 완전히 탈중앙화된 형태의 공공형 블록체인을 도입하기에는 한계 존재
  - 공공형 블록체인은 참가자에게 동등한 지위와 권한을 부여하는 특성 때문에 금융기관, 증권발행자, 투자자, 금융규제기관 등 각각의 역할이 상이한 금융시장의 금융거래에는 적용하기가 쉽지 않음
  - 또한 공공형 블록체인에서 나타나는 합의제도의 특성상 실시간 금융거래의 니즈를 충족시키는데도 한계 존재

- 블록체인은 기반기술이기 때문에 이를 활용한 다양한 형태의 블록체인이 나타날 수 있는데, 이러한 점이 블록체인을 통한 거래시스템을 구축하는 것에 장애가 될 수 있음[19]
  - 컨소시엄 블록체인 개발 연합인 R3 CEV의 목표가 '표준화된 블록체인 기술의 공통적용'인 것도 이러한 맥락에서 출발한 것임

19_ 예를 들어 모건스탠리와 골드만삭스는 A라는 블록체인 거래 시스템을 사용하고, BOA와 베어스턴즈는 B라는 블록체인 거래 시스템을 사용한다고 하면, 만약 A와 B사이의 상이한 기술적 요인들이 있을 경우 모건스탠리와 베어스턴즈 사이에는 블록체인 기반의 거래를 할 수 없는 한계점이 존재

표_ 04 종류별 블록체인의 특성 요약[20]

구 분	개념 및 특징	주요니즈 / 선결 요건	예시
공공형 블록체인 (Public Blockchain)	• 최초의 블록체인 활용사례 • 인터넷을 통해 모두에게 공개, 운용 가능한 거래 장부 • 컴퓨팅파워를 네트워크에 제공함으로써 누구든지 공증에 참가 • 한번 정해진 법칙을 바꾸기 굉장히 어려움 • 네트워크를 유지(채굴)하는데 드는 비용이 큼 • 네트워크 확장이 어렵고 거래 속도가 느림	• 네트워크 효과 • 위험(Risk)관리	비트코인 등
사적 블록체인 (Private Blockchain)	• 개인형 블록체인 • 1개의 주체가 내부 전산망을 블록체인으로 관리 • Private Blockchain 개발을 위한 플랫폼 서비스도 등장 • 시스템 구축 후 규제변경 가능	• 시스템 변경 감수/안정성확보 • 1개의 주체 내 글로벌 브랜치	나스닥 Linq
컨소시엄 블록체인 (Consortium Blockchain)	• 반중앙형 블록체인으로서 미리 선정된 N개의 주체 (상호신뢰관계에 있는 주체들만 참가가능 • N개의 주체들 간의 합의된 규칙을 통해 공증에 참가 • 네트워크 확장이 용이하고 거래 속도가 빠름 • 거래증명자가 인증을 거쳐 알려진 상태(known)이기 때문에 51% 공격이나 이중송금(double spending)과 같은 문제는 없음 • 블록체인 소유자에게 알맞게 규칙을 바꿀 수 있음 • 네트워크 유지비용이 거의 없음 • 참가자간의 선택에 따라 규제 변경가능	• 참가주체들 간의 비즈니스적인 동의 / 합의 • 시스템 안정성 확보	R3 CEV

20_ 금융보안원, "국내외 금융분야 블록체인(Blockchain) 활용동향," (보안연구부 – 2015 – 028, 2015.11.23.), 2~3면.

4. 블록체인의 특징과 금융산업에 미치는 영향

≡ 특징과 장점[21]

- 블록체인 기술은 모든 기록이 집중된 제3의 기관이 없기 때문에 기존 중앙집중형 시스템에 비해 다음과 같은 특징과 장점을 가질 수 있으나, 이러한 특징과 장점이 단점이 되는 양면성도 일부 존재

① 탈중앙성 / 탈중개성[22]

- 탈중앙성과 탈중개성(decentralized web) 서비스와 분산파일시스템(distributed hash table)기술을 이용하여 웹으로 이용 가능한 서비스의 탈중앙화와 탈중개성으로 공인된 제3자의 공증 없이 개인거래 가능

② 효율성(Efficiency)

- 중앙집중식 전산시스템은 복잡하여 개별 서비스 도입 때마다 최소한의 표준화 등 관리비용이 과다하여 신규 전산시스템 도입 시 엄청난 비용 소요(예 JP모건 : 9조원)
- 블록체인 기술을 이용하는 경우 제3자에 대하여 지불하는 수수료가 불필요하고, 시스템의 안정성이 높아 시스템 오류 등을 예방하고, 해킹 등 보안사고를 방지하기 위한 인프라 투자비용도 절감 가능

③ 확장성(Scalable)

- 기존의 중앙집중식 폐쇄형 전산시스템으론 확장성과 수용성이 부족하여, 최신의 전산시스템은 인터넷, 구글, 리눅스와 같은 개방형이 추세
- 블록체인은 쉽게 블록을 구축하여 연결할 수 있어 강력한 확장과 새로운 아이디어의 수용이 가능하여 확장성이 우수한 것으로 평가

21_ McKinsey & Company, op.cit., pp.5~6; CoinDesk, "Banks and the Blockchain Report," 2015, pp.12~13; 정유신, 앞의 글, 43~45면 참조.

22_ http://bolckchainos.org/(2016.4.11 방문)

④ 보안성(Security)

- 기존의 전산시스템은 해커들의 연구가 축적되어 최신 사이버 공격에 취약하며, 심지어 중앙은행, 거래소, 중앙예탁기관 등도 해커공격에 노출 우려
- 블록체인은 블록체인 시스템 상에서는 거래정보가 분산 기록되기 때문에 장부를 해킹하려면 고비용이 발생하고, 중앙집중관리가 불필요하여 내부자조작, 정보유출 위험도 감소하여 보안성이 우수
- 블록체인은 블록 간 연결을 통해 암호의 해킹과 해독이 사실상 불가능하여 암호안정성(cryptographic secure)이 매우 우수[23]

⑤ 안정성(Resilience)

- 블록체인의 강력한 보안능력으로 개인정보 보호 및 유출방지 등으로 금융거래의 신뢰성 제고로 금융거래의 활성화에 기여
- 블록체인은 모든 사용자가 거래 장부를 갖고 있어 단일실패점(single point of failure)*이 존재하지 않으므로 네트워크 일부에 문제가 생겨도 전체 블록체인에는 영향이 없음

  * 제품이나 서비스의 구성요소 중 일부가 정상적으로 작동하지 않으면 전체 제품 또는 서비스를 중단시키는 부분을 의미

⑥ 투명성(Transparency)

- 블록체인 참가자가 장부를 공유하고 모든 거래기록을 공개하기 때문에 거래기록에 대한 투명성이 높아 투명성이 중요한 금융거래와 회계관리에 적용 가능성이 높음
- 한번 컨퍼메이션*된 데이터는 영구적으로 보관되고 누구나 추적 가능한 불변성(immutable)과 블록체인의 개방성과 분산성을 통해 망중립성(net neutrality) 확보가 가능하여 투명성이 높음

  * 컨포메이션은 데이터 기록행위를 이웃이 컨펌해 주는 상황 가치가 높은 데이터일수록 많은 컨포메이션을 받음

23_ 김동섭, 앞의 책, 5면.

≡ 금융산업에 미치는 영향[24]

① 금융의 IT화

- 블록체인은 공인된 제3자가 불필요하여 금융회사를 P2P대출, 크라우드펀딩과 같이 수요자와 공급자가 직접 만나는 P2P네트워크 플랫폼을 운영하는 IT 회사화
- 금융산업과 IT 산업의 정체성 구분이 어려워지는 시대가 도래하고, IT 경쟁력이 금융산업의 핵심경쟁력으로 변화하여 안정성과 효율성을 갖춘 블록체인시스템이 이를 가속화할 전망

② 금융의 제조산업화

- 블록체인 기술을 활용한 전산시스템은 개방형이면서 안정성이 높아 금융소비자 요구에 맞는 맞춤형 상품설계가 가능하여 장외파생상품 등 다양한 금융상품개발이 활성화될 전망
- 블록체인 기술을 활용하여 금융상품, 서비스 개발내용, 시점 등을 명확히 할 수 있어, 특허·지적소유권 등에도 긍정적 효과가 발생하여 금융상품도 제조 상품처럼 실체가 있는 상품으로 변화될 가능성
- 금융산업의 제조산업화를 시작하여 금융기능을 금융상품제조, 유통, 운용으로 전환하여 4차 산업혁명의 물결이 2차 제조산업에서 3차 서비스산업으로 확산 중
- 향후 금융산업은 제조산업처럼 금융상품 제조·유통판매로 구분되고, 금융산업 특성상 운용이 추가되는 형태로 발전

③ O2O 비즈니스의 확대

- 금융의 IT화는 금융 인력의 표준화된 업무를 IT / 인터넷이 대체할 가능성이 높아 금융 인력들이 IT / 인터넷을 하나의 수단으로 사용하여 금융상품개발, 개선에 나선다면 금융 인력(Off-Line)과 IT(On-Line)의 시너지가 더욱 커질 수 있음

24_ 정유신, 앞의 글, 18~22면 참조.

- 금융 인력은 O2O 상품개발, O2O 상품판매 두 그룹으로 구분되고, 금융규제, 관리감독도 점차 은행·증권·보험의 권역별로가 아닌 제조·유통판매·운용으로 변화할 가능성도 대두

표_ 05 금융거래 단계별 블록체인 기술 도입 효과 [25]

거래 전	거래 시	거래 후	증권서비스
• 보유지분에 대한 정확한 검증 가능 • 신용 익스포져 (exposures) 감소 • 고정 데이터 (static data) 공유 • 보유지분 명확화에 따른 고객확인의무(KYC)* 단순화	• 안전하고 실시간적인 거래 매칭, 즉시 철회 불가능한 결제 시스템 • 현금장부에서 자동 동시결제(DVP) • 감독 당국의 정확한 감시 및 자동 리포팅 • 엄격한 자금세탁방지 (AML)** 기준 적용	• 실시간 현금거래에 대한 집중청산 생략 • 마진·담보 요건 완화 • 신속한 경개(更改) 거래 및 거래 후 업무처리의 절차적 효율성 제고 • 블록체인 내 자산을 담보로 대체사용 가능 • 스마트계약 (smart contract)의 자동 체결	• 블록체인 기술을 이용하여 직접 발행 • 서비스 자동화 및 중복 방지 • 평면적 계좌 구조에 의한 데이터의 집중화 • 참조 데이터의 공유 • 블록체인 기술을 이용하여 펀드 청약·설정 환매 자동처리 • 펀드서비스, 회계 등의 단순화

* KYC : Know Your Customer

** AML : Anti-Money Laundering

5. 블록체인의 문제점과 한계

≡ 문제점

- 블록체인 기술을 통한 분산원장의 신뢰를 담보해 줄 외부기관 등이 존재하지 않기 때문에 시스템 자체에서 신뢰를 형성하는 메커니즘으로 설계할 필요가 있음 [26]

25_ Euroc－lear/Oliver Wyman, "Blockchain in Capital Markets(The Prize and the Journey, 2016.2)" p.12.

26_ 김동섭, 앞의 책, 7면.

- 분산원장에서는 모든 참가자가 새로운 거래를 반영하여 원장을 갱신하는 권한과 책임을 갖고 있기 때문에 특정 내부 참가자가 악의적으로 원장을 조작하여 배포하는 것을 방지할 필요*가 있음

  * 분산원장 기술에서는 제3의 기관이 존재하지 않고 모든 참가자가 동등한 지위를 갖기 때문에 내부의 조작과 외부의 침입을 구분할 필요가 없음

- 최근(비트코인 개발 이전)까지 동 기술을 지급결제 시스템 및 여타 금융서비스 등에 실제로 적용하지 못했던 것은 조작 가능성을 차단하면서 원장을 갱신할 수 있는 합의(consensus) 절차*를 마련하지 못했기 때문

  * 비잔틴 장군들의 딜레마(Byzantine generals problem)의 일종으로 컴퓨터 공학의 난제로 알려짐[27]

❑ 블록체인 기술은 현재 빠르게 발전하고 있으나 아직까지는 기술적으로 POC(Proof of concept) 단계이며 금융시장에 도입되는 부분은 틈새시장(niche market)을 중심으로 제한적임

- 블록체인과 같은 기술의 상용화과 과정은 프로토타입 개발단계(prototyping), 개념증명 단계(proof of concept), 파일럿 테스트단계(pilot test), 알파단계(Alpha), 베타단계(Beta), 상용화단계(product)와 같은 흐름을 거침

- 통상 금융서비스의 신규 시작 시 알파와 베타 기간 동안 같은 정보를 기존 레거시시스템과 신규시스템에서 동시에 운영한 후 상용화 시 레거시시스템 중단함

27_ 비잔틴 장군 문제(Byzantine Generals Problem)는 1982년 Leslie Lamport 등 3명의 컴퓨터공학자가 마이크로소프트의 의뢰를 받아 연구를 수행하여 발표한 논문에서 최초로 정식화한 문제임. 해당 논문에서 중앙통제 시스템이 없는 상황에서 네트워크 참가자간 통일된 의사결정을 위한 합의(consensus)를 도출해야 하는 문제를 다음과 같이 가상의 상황으로 설명하였음. "비잔틴 군대의 여러 부대가 적군의 도시 외곽에 진을 치고 있다. 각 부대를 대표하는 장군이 부대를 통솔한다. 장군들은 오로지 연락병을 통해서만 서로 연락할 수 있다. 적군의 동태를 살핀 후 장군들은 합동작전 계획을 결정해야 한다. 그렇지만, 장군들 가운데에는 배신자가 섞여 있을 수도 있고, 그들은 다른 장군들이 합의에 이르지 못하게 하려 한다." 각 부대의 장군들이 한자리에 모여서 의사 결정을 할 수 없는 상황에서 어떻게 하면 합동 공격시간을 '합의' 하여 출격할 수 있을지 문제화 하였다. 비트코인은 분산 컴퓨팅 분야에서 발생할 수 있는 이 문제를 작업증명과 블록체인을 도입하여 해결하였다. 즉, 여러 명의 장군들이 다음과 같은 제약 조건 하에서 각자 병력을 통솔하여 함께 요새를 공격할 시간에 합의하기 위한 절차를 찾는 문제임. (i) 과반수 이상의 장군이 참가할 때만 공격에 성공할 수 있음, (ii) 각 장군들은 전령을 통해서만 서로 교신할 수 있음, (iii) 일부 장군은 악의적으로 거짓 공격시점을 전달하여 다른 장군에게 피해를 입히고자 함(한승우, 앞의 논문, 27면)

≡ 블록체인의 한계[28]

① 규제환경의 미흡

- 아직 블록체인 기술을 활용할 수 있는 법적근거가 마련되어 있지 아니하며, 또한 블록체인 기술과 그 활용과 관련된 법적분쟁에 대한 법상 해결방안도 부재

② 기술적 공감대 형성 미흡

- 블록체인 기술을 금융시장에 적용에 있어서 노드선정, 실시간거래 한계, 대용량 데이터 처리 한계·감시감독·과세 등 다양한 문제들에 대한 해결책과 공감대 형성 미흡

③ 분산성의 한계

- 블록체인의 탈중앙적 속성은 정보의 검색을 곤란하게 하는 측면이 존재하고, 금융실명제와 익명성추구 간의 딜레마도 존재

④ 우발적 거래에 대한 취소 불가능

- 블록체인 기술은 당초 비트코인의 이중지불을 방지하는 데 주안점을 두고 이미 승인된 거래가 취소되지 않도록 설계되었기 때문에 이용자 착오나 범죄 등에 따른 우발적인 지급에 대해서도 이를 취소하거나 피해를 복구하기가 불가능

- 블록체인 기술의 고유한 보안 특성상 기록이 기재되면 수정이 불가능하고 그에 대한 수정을 위해서는 그 후의 모든 블록을 변경해야 하는 문제 발생

⑤ 과도한 자원 투입

- 블록체인 시스템의 안전성은 다수의 참가자가 경쟁적으로 채굴하는 과정에서 형성되기 때문에 실제거래를 승인하는데 필요한 수준에 비해 과도하게 많은 연산능력과 전력 등 **자원이 투입**(특히 비트코인 블록체인의 경우가 이에 해당)

28_ 김동섭, 앞의 책, 11면; 김태우, 앞의 글, 40면; DTCC, "EMBRACIING DISRUPTION–TAPPING THE POTENTIAL OF DISTRIBUTED LEDGERS TO IMPROVE THE POST–TRADE LANDSCAPE," JANUARY 2016, p.5, 8; Euroclear/Oliver Wyman, op. cit., pp.14~15.; McKinsey & Company, op.cit., pp.11~14.

⑥ 과도한 도입비용

- 블록체인 기술을 활용하여 금융시장인프라를 구축하는 것에는 개발자와 참가자 모두에게 상당한 투자비용이 발생
- 블록체인 기술을 금융시장에 도입하는 경우 상당한 규모의 비용이 발생할 것으로 추정되며 시장운영 지연과 비효율성으로 인한 자본 및 유동성 비용도 발생 예상
- 컨소시엄 또는 사적형태의 블록체인 기술을 도입하기 위해서는 상당한 규모의 인적·물적 투자가 이루어져야 하는 만큼 도입비용, 효율성 등에 대한 면밀한 검토 필요

⑦ 확장성 제약

- 비트코인의 경우 현재 처리할 수 있는 거래건수가 매우 제한적(초당 7건[29])임에도 불구하고 과거의 모든 거래내역을 포함하는 블록체인이 과도하게 많은 저장 공간(현재 약 45GB)을 차지하여 확장성의 제약요인으로 작용 가능
- 현재의 기술표준은 자본시장에서 도입될 수 있는 수준에 못 미치나, 블록체인 기술의 확장성과 처리능력의 문제는 기존 비트코인 플랫폼의 개선에 따라 해소될 수 있는 것임

⑧ 이견조정 지연

- 블록체인 기술을 활용한 시스템 상 기술적 오류 등 문제 발생 시 참가자들이 해결책을 채택하기 위해 다수의 동의를 얻는 과정에서 의사결정이 지연되어 신속한 대응이 어려움

29_ 비자카드의 네트워크는 미국에서 초당 1,700여건의 거래를 처리한다고 함

Ⅲ. 블록체인의 국내외 동향

1. 해외동향

≡ 해외 금융기관 동향

- 주로 글로벌 금융기관과 스타트업 기업 간 협업의 형태로 블록체인 기술에 의한 분산원장을 활용하기 위한 방안을 활발히 논의하고 개발 중
  - 아직까지는 대부분 적용 가능성을 시험하는 초기 개발단계에 머물고 있으며 디지털통화를 이용한 송금시스템(Ripple 등) 등 일부를 제외하면 실제 상용 서비스 출시까지는 이르지 못하는 상황

- 골드만삭스, 바클레이즈, JP모건, UBS 등 42개 글로벌 대형은행은 컨소시엄을 결성하고 미국 핀테크 업체인 R3 CEV*와 제휴하여 블록체인을 금융서비스에 활용하기 위한 플랫폼을 공동 개발 중임[30]

  * 2014년 설립된 미국 뉴욕 소재 금융기술 벤처기업으로 블록체인을 이용하여 저비용으로 해외송금 및 자산 관리 등에 활용할 수 있는 플랫폼을 개발 중[31]

30_ Morrison & Foerster LLP, “Client Alert,” 2016, p.3.
31_ 김동섭, 앞의 책, 31면.

표_ 06 R3 CEV 컨소시엄 참가 금융기관(44개)

구 분	참가 금융기관
북미(14개)	Bank of America, BNY Mellon, Citi, the Canadian Imperial Bank of Commerce, Goldman Sachs, J.P. Morgan, State Street, Morgan Stanley, Royal Bank of Canada, Toronto-Dominion Bank, US Bancorp, Wells Fargo, Northern Trust, BMO Financial Group,
유럽(19개)	Barclays, BBVA, Commerzbank, Deutsche Bank, HSBC, Credit Suisse, Skandinaviska Enskilda Banken, SociéétGééale, Nordea, BNP Paribas, ING, Banco Santander, Scotiabank, Danske Bank, Natixis, OP Financial Group, UniCredit, Intesa Sanpaolo,
호주(4개)	Commonwealth Bank of Australia, National Australia Bank, MacQuarie, Westpac Banking Corporation
일본(5개)	Mitsubishi UFJ Financial Group, Mizuho Bank, Sumitomo Mitsui Banking Corporation, Nomura,
한국(2개)	하나금융그룹, 신한은행

* R3 CEV 컨소시엄 참가금융기관은 계속 증가하고 있으며, 현재 51개 전세계 금융기관이 참가 중 (2016.6월 기준)

- 각국 은행들은 R3와 협업을 통해 블록체인 시스템을 표준화하고 이를 통해 글로벌 금융 시장에 더 빠르고 효율적인 시스템을 도입할 계획[32]
- 은행들은 공동으로 R3에 담당직원을 파견해 설계, 기술, 규제 등 분야 연구에 공동으로 참가해 향후 1~2년 내 시스템을 개발하고 실험에 나설 계획
- R3 CEV에 합류하며 은행 간의 모든 거래정보가 완전히 공개되는데, 사용자의 익명성이 확보되는 비트코인 거래보다는 폐쇄적이고 사적인 성격을 띠게 될 것으로 전망

32_ 심윤보, "블록체인 기술 공동 개발에 나선 글로벌 은행들," 하나금융경영연구소 Weekly Hana Financial Focus(제5권39호 2015.10.12.~10.18), 12면; "Blockchain initiative pulls in another 13 banks," FT, 2015.9.29)

표_ 07 외국 금융기관의 블록체인 활용 및 추진 현황[33]

구 분	활 용 현 황
비자 (Visa)	• 2015. 8월, 블록체인 기술을 새로운 지급수단을 개발하는 데 활용할 계획을 발표 • 2015. 9월, 비자, 시티, 나스닥 등은 블록체인 기술을 활용한 분산원장 개발 플랫폼 업체인 Chain.com에 3천만 달러를 투자
Factom사 (미국 IT업체)	• 2015. 5월, 온두라스 정부로부터 투자를 받고, 온두라스 토지등기부를 분산원장 기술을 이용하여 기록, 관리하는 시스템 개발을 수탁 • 온두라스는 남미에서 두 번째로 큰 국가로서 군벌 귀족들이 토지대장을 조작해 농민들의 토지를 수탈하는 것을 방지하기 위해 조작이 불가능한 디지털부동산 등기소 추진 중
리눅스 재단 (Linux Foundation)	• 리눅스 재단(Linux Foundation) 주도로 2015.12월에는 글로벌 금융기관 뿐 아니라 다양한 IT 관련 기업이 함께 참가하여 상용 수준(Enterprise grade)의 오픈소스 분산원장 프레임워크를 공동 개발하는 프로젝트가 추진 중임 * Accenture, ANZ Bank, Cisco, CLS, Credits, Deutsche Böse, Digital Asset Holdings, DTCC, Eris Industries, Fujitsu, IC3, IBM, Intel, J.P. Morgan, London Stock Exchange Group, Mitsubishi UFJ Financial Group, R3, State Street, SWIFT, VMware, Wells Fargo 등 * 이를 통해 각 기업들은 공동 플랫폼을 기반으로 개별 산업에 특화된 응용 프로그램 및 하드웨어 개발 등에 집중할 수 있을 것으로 기대[34]
나스닥	• 2015년 말, 장외주식거래 확대차원에서 장외거래에서의 실시간 거래, 명확한 소유권이전 확인, 즉시결제(T+0) 등의 효과를 증명하기 위해 Pre IPO 플랫폼 LINQ 파일럿시스템을 운영 중이며, 2016년 9월에 공개 예정
디지털 홀딩스	• 2015. 10월, 호주 증권거래소와 블록체인시스템 개발을 계약하고, 호주 증권거래소는 디지털홀딩스에 1,200만$ 투자
Overstock	• 2015. 5월, 자사의 주식을 발행하여 장외시장에 유통시키고 있으며, 당일결제(T+0) 플랫폼으로 관심 제고하였으며, 2015. 6월에는 자사 플랫폼에서 2,500만달러 규모의 회사채를 발행하였으며, 2015. 12월에는 증권거래위원회(SEC)로부터 분산원장 플랫폼을 통한 공모주식(public securities) 발행 인가를 획득

33_ 정유선, 앞의 글, 14~16면 참조.

34_ 김동섭, 앞의 책, 33면.

2. 국내동향

- 국내 은행들도 핀테크 기업과 제휴 등의 형태로 블록체인 기술을 해외송금 서비스, 인증 체계 개발 등에 활용하는 방안을 검토 중

표_ 08 은행권의 블록체인 기술 분산원장 활용현황[35]

구 분	활 용 현 황
KB 금융그룹	• 국민은행은 2015. 9월 코인플러그에 15억 원을 투자하여 동사와 블록체인을 기술을 기반으로 한 외환송금서비스 및 개인인증서, 문서보안서비스 등 관련 제휴 ▸'16년 초 블록체인 기술을 활용하여 국제금융결제망(SWIFT)을 거치지 않고 해외로 외환송금 가능 기술검증 완료
신한은행	• 신한은행은 2015년 '신한퓨처스랩'(신한금융그룹 핀테크 스타트업 육성 프로그램) 1기 업체로 선정된 스타트업 스트리밍에 5억 원의 지분을 투자하여 동사와 해외로 외환송금시스템을 공동 개발 중
우리은행	• 핀테크 사업부를 중심으로 블록체인 기술의 도입 타당성을 검토 중
NH 농협은행	• 국내 최초의 비트코인 거래소인 코빗과 제휴를 맺고 자사 업무에 블록체인 기술을 접목하는 방안에 대해 검토 중
KEB 하나은행	• KEB하나은행은 센트비(핀테크 기업)와 업무협약을 체결하고 블록체인 기술을 활용한 해외송금서비스를 구축 중 • 2015년 스타트업 육성을 위한 핀테크 '1Q랩'을 개소하고 블록체인 플랫폼을 구축하는 방안을 검토
BNK 부산은행	• BNK금융그룹은 코인플러그와 공동으로 블록체인 기반의 금융서비스 개발을 위한 업무협약을 체결

35 김태우, 앞의 글, 36면 참조.

- 공동시스템 개발 참가 대형은행들은 동시에 각각 자체적으로 블록체인 시스템 개발에도 참가하는 등 다양한 대응전략을 마련

- 국내 대형은행들은 블록체인 스타트업에 투자자·이사회 멤버 등의 형태로 참가하고 있으며, 벤처유닛을 통해 블록체인 시스템 개발 및 실험에도 참가 중

❑ 국내 증권업계의 경우에도 금융투자협회와 함께 2016. 10월 블록체인 기반의 개인인증 서비스 개시 예정

- 현재 6개 증권사가 기술개발 중이며, 2016. 10월부터는 20여개 증권사가 참가한 시범 서비스를 시작 예정으로 인증서비스가 안착되면, 2017년 1분기에는 장외시장, 채권거래 등으로 기술을 확대할 계획

Ⅳ. 블록체인의 활용과 변화

1. 금융분야

- 블록체인은 주식, 채권, 파생 등과 같은 금융분야에 잠재적 적용가능성이 높은 것으로 전망되나 구체성과 대규모 실질적 적용가능성에 대해서는 더 많은 연구와 기술적 진보가 필요[36]

(1) 지급결제

- 블록체인 기술이 금융거래의 전반으로 확산되는 경우 소액결제시스템뿐 아니라 거액결제시스템 등 지급결제제도 및 금융시스템 전반에서 활용 가능성이 큰 것으로 분석되고 있음(BIS, 2015)
- 업계에서는 분산원장 기술을 역외거래, 증권거래 등에 적용하는 경우 2022년까지 매년 약 150～200억 달러 규모의 IT 인프라 투자비용을 절감할 수 있을 것으로 전망(Santander, 2015)
- 은행권의 경우 비트코인의 경우와 달리 블록체인 공동시스템은 승인을 받은 참가자만 접근이 가능한 컨소시엄 또는 사적 블록체인 형태로 설계될 계획

(2) 증권발행

- 블록체인 기술을 통하여 증권발행 시 증권은 증권장부에서 직접 발행되며, 증권의 발행과 투자자간 거래에 대해서 스마트계약(smart contract)과 동시결제 기능이 제공됨

36_ Andres Guadamuz and Chris Marsden, op. cit., p.58.

(3) 증권거래[37]

- 증권거래는 거래가 체결된 곳에서 매매확인이 이루어지고(matching) 자동적으로 승인이 완료됨
- 거래당사자는 개인키(private key)로 증권 또는 현금의 잠금을 해제하는 방식으로 거래에 서명을 하고 공개키(public key)로 수령인에게 소유권을 이전함
- 완료된 거래내역은 분산장부(증권)에 통보되어 해당 장부가 업데이트 되는 경우 검증·기록되고 이와 동시에 현금장부도 업데이트 됨
- 그러나 블록체인 기반에 통용되는 신용화폐가 없으므로 현시점에서 블록체인 기반 증권거래에 사용될 호환 가능한 견고한 현금장부가 필요한데, 이를 위하여 특정한 암호화폐*의 생성이나 은행의 기존계좌를 활용**하는 방안을 마련할 필요가 있음

  * 영구적 액면가가 있고, 리스크를 최소화하여 현금을 에스크로 방식으로 보유할 수 있게 하는 화폐

  ** 참가자들이 은행의 기존계좌를 활용하여 별도계정의 거래를 위한 유동성을 예치하면, 현금장부의 변동사항이 거래계정의 잔고에 반영됨

(4) 증권결제

- 현재 블록체인 기술을 활용하는 경우 'T+2~3'일 결제를 'T+0'일 결제로도 가능하다는 의견도 존재하나, 현행 결제주기는 증권의 종류(주식, 채권 등), 거래의 방식(장내거래, 장외거래 등), 거래자의 종류(내국인, 외국인 등), 결제방식(증권과 대금의 동시결제, 분리결제 등) 등에 따라 다양
- 국내 장외채권거래는 실시간결제(real time gross settlement), 장내주식거래는 T+2, 미국의 장내주식거래는 T+3일 결제 등으로 다양하며, 특히 증권거래는 결제완결성 확보를 위하여 증권과 대금의 동시결제(DVP : delivery versus payment)가 중요

37_ Euroclear/Oliver Wyman, op. cit., p.10.

- 이렇게 증권의 매매거래 후 결제일이 다양한 이유는 거래증권, 거래방식, 거래장소, 국제간 시차, 환전 문제 등으로 그 배경이 다양하며, IT 기술적인 이유로만 인하여 당일 동시결제가 미흡한 것은 아님

(5) 자산관리 서비스[38]

- 펀드매니저는 증권에 대한 투자현황을 명확히 볼 수 있으며, 펀드장부에서 펀드 내 투자자 지분을 관리함

- 평면적 계좌 구조(flat accounting)를 통해 다층적인 보관구조가 단층으로 축소되는데, 현재는 단일 증권이 5~6개층(증권사, 매도측 은행, 로컬 보관기관, 글로벌 보관기관, 중앙예탁기관 등)으로 보관되고 있으며, 각각 별도의 계좌 관리방식을 가지고 있으며, 증권은 최종 실질소유자를 기록하는 'wallet provider' 형식으로 보관됨

(6) 파생상품거래[39]

- 파생상품 거래의 경우 두 당사자의 채무(마진계약 또는 스왑조건 등)를 확정하는 프로그램화된 스마트계약을 이용함으로써 거래가 체결될 수 있음

- 딜러들은 청산기관(CCP: central counterparty)를 통한 거래로 거래상대방에 대한 신용위험을 낮출 수 있으며, CCP에 담보를 제공하는 것은 현금장부에 현금을 에스크로(escrow)*하는 방법 또는 다른 자산장부에 보관된 자산을 담보장부에 배정하는 방법으로 가능

  * 에스크로는 구매자와 판매자 간에 신용관계가 불확실한 경우 제3자가 상거래가 원활히 이루어질 수 있도록 중계하여 매매를 보호하는 것

38_ Euroclear/Oliver Wyman, ibid., p.10.
39_ ibid.

2. 비금융분야

- 블록체인은 금융분야뿐만 아니라 자동계약, 저작권, 계약체결, 기타 법적 거래 등에 많은 적용가능성이 있음[40]

(1) 자산등록부(asset registers)

- 분산원장은 자산의 내역, 거래내역 그리고 유효성을 관리하는 안정성과 신뢰성이 요구되는 장부에 이용될 수 있으며, 이 기술은 분명한 방법(indisputable way)으로 소유권과 출처를 증명하는데 이용될 수 있음
- 영국의 스타업인 Everledger사는 다이아몬드 업계의 사기와 도난문제를 해결하기 위해 이 기술을 사용 중
- 이외에도 토지소유권, 선하증권, 자동차 리스, 금 거래, 순수미술(fine art), 에너지, 주식, 기타 자산의 등록부의 존재 여부 또는 유지 및 관리의 비용과 관련 없이 전자적으로 대표될 수 있고, 저장될 수 있고, 거래될 수 있는 모든 자산에 분산원장 적용 가능

(2) 신원등록부(identity registers)

- 분산원장은 신원과 사기적 청구(claim fraud)를 줄이는데 도움을 주고 개인이 그들의 개인적 데이터의 통제를 잘 할 수 있도록 하여 디지털 인증을 간소화 할 수 있음

(3) 지적재산(intellectual property)[41]

- 분산원장 기술은 지적재산의 등록과 라이선스 등 다양한 잠재적 사용을 가지며, 이 기술은 저작권과 관련하여 다른 토큰(token)으로서 저작권과 관련된 권리에 이용될 수 있음

40_ Andres Guadamuz and Chris Marsden, op. cit., p.58.
41_ DTCC, op. cit., p.11.

(4) 음악 및 엔터테인먼트(music and entertainment)

- 많은 예술가들은 그들의 콘텐츠가 이용되고 지불되는 방법과 지적재산권의 침해와 불법적 파일 공유를 방지하는 것과 관련하여 유용할 것이라는 점에서 분산원장에 관심을 가지고 있음
- 이 분야는 분산원장이 로열티를 음반사 및 기타 유통 및 라이선스 기관에 어떻게 수집, 배분하는데 지원하는지를 알 수 있는 방법을 제공

(5) 전자장치 및 사물인터넷(electronics and internet of things)[42]

- 블록체인 기반의 IoT 플랫폼을 통하여 모든 사물들을 인터넷을 통해 연결하여 서로 정보를 공유할 수 있는 환경을 구성하여 중앙장치에 의한 통제를 블록체인 기술을 통하여 기기 스스로 통제할 수 있는 기술적 환경 조성
- IBM의 ADEPT(Autonomous Decentralized Peer-To-Peer Telemetry)는 자동 분산 P2P 원격 측정으로 분산된 접근 방식을 택함으로써 IoT의 보안성과 규모를 확장시킨다는 계획을 가지고 있음
- 사물인터넷과 스마트 계약을 서로 연계시켜 제품 스스로가 소모성 품목을 재주문하거나, 기기의 이상이 있을 경우 셀프 서비스 요청 등을 수행 가능

(6) 정부 및 대리인 사용(government and agency use)

- 에스토니아의 디지털 신원시스템인 이-레지던스(e-Residency)[43]은 에스토니아 국내 온라인 정부 서비스에 접근을 인증하는 용도로 이용
- 에스토니아 정부는 '키 없는 전자서명 인프라스트럭처(KSI)'를 통해 전자시민권을 개발 중인데, KSI는 시민들이 정부가 관리하는 DB에서 자신들의 정보에 대한 정확여부를 확인할 수 있으며,

42_ 한승우, 앞의 글, 33면.
43_ http://www.idgconnect.com/abstract/9207/who-wants-to-be-an-estonian

- 또한 내부 관리자가 불법적으로 네트워크에 침입할 수 없게 하여 시민들이 전자상거래 등록이나 전자세금계산서와 같은 디지털 서비스를 활용할 수 있도록 기여

- 에스토니아 이외에도 미국은 의료정보의 기록 및 공유, 우크라이나는 투표관리운영, 영국은 모든 공공서비스 분야 등에 블록체인 기술을 적용시키기 위해 연구 및 개발 중

(7) 전자공증[44]

- 블록체인 기술의 타임스탬프(시점확인)와 해쉬 함수를 이용하여 인증서, 계약서 등 공적 증명이 필요한 문서 또는 각종 파일들을 증명할 수 있는 전자공증 가능

- 기업들은 전자공증시스템을 자체 구축하기 보다는 위탁하여 운영하는 경우가 대부분인데, 집중관리기관인 위탁운영기관이 해킹 등으로 데이터가 위·변조될 위험 존재

- 그러나 블록체인을 이용할 경우 저장된 데이터의 불변성을 이용하여 전자공증시스템 구축 가능

(8) 공인인증서 발급

- 인터넷뱅킹에 사용되는 공인인증서를 별도의 인증기관을 거치지 않고, 블록체인 기술을 통하여 '공개키기반구조(PKI)'[45]라는 표준 암호화 기술을 통하여 사용자와 은행 간에 사용할 수 있는 방법 가능

- 개인키와 공개키 생성 작업을 스마트폰 앱을 통하여 인증기관 없이도 공인인증서 로그인과 자금이체 등에 활용 가능

- 은행뿐 아니라 정부의 민원서류 발급, 조달청 입찰 등에서도 공인인증서가 활용되고 있기에 블록체인 기술은 개인정보유출 또는 해킹 등으로부터 보다 안전하고 저렴한 수단으로 재조명[46]

44_ 한승우, 앞의 글, 31면

45_ PKI는 국제전기통신연합(ITU-T)이 정한 표준기술인 X.509를 따른 것으로, 공개키(public key)와 개인키(private key)를 생성하고, 이를 통해 상대방과 통신이 안전하다는 사실을 확인하는 것

3. 스마트 계약

- 스마트 계약(smart contract)은 블록체인을 통해 일정 조건을 만족시키면 거래가 자동으로 실행되도록 프로그래밍한 자동화된 계약시스템으로[47], 소유권 이전, 상속, 증여, 물품구매 등에 폭넓게 활용되고 있으며 최근에는 사물인터넷과 연계되어 이용되고 있음

  - 조건에 의해 거래가 자동적으로 성립되므로 중간관리자에 의한 사기 피해를 막을 수 있으며, 거래정보 기록이 보존되기 때문에 계약서 위조, 사고기록 조작 등과 같은 악의적 행위를 방지 가능하여 신용 리스크(credit risk)와 상대방 리스크(counterparty risk)를 감소시킬 수 있음[48]

  - 독일의 스타트업인 '슬록(Slock)'은 부동산 보증금과 임대료를 지불하면, 스마트폰을 이용해 건물에 부착된 스마트 자물쇠를 계약기간 동안 중간관리자 없이 입주자가 자유로이 열 수 있도록 하는 블록체인을 활용한 스마트계약 부동산임대서비스를 제공 중

    [예시 1] 3등급 이상의 신용등급, 5천만원 이하의 부채를 지닌 개인에게 투자하고 싶은 사람과 조건에 부합하는 개인이 대출을 신청하였을 때 이를 자동으로 연결 가능

  - 스마트계약은 블록체인을 활용해 기존 중앙방식 보안에서 탈 중앙방식 보안으로 나아갈 수 있는 매개체로서, 비대면 거래에서 가장 중요한 부분인 금융거래 정보의 암호화와 인증 문제를 해결

  - 고객의 국민연금, 건강보험, SNS 활용정보 등 고객의 신용도 등을 판단할 수 있는 스크래핑 기술로 비대면 거래에 있어 간편성을 확보하고, 블록체인을 통해 보안성을 높일 수 있어 블록체인과 스크래핑 기술을 활용한 스마트계약의 대중성과 신뢰성을 확보할 수 있음

46_ http://www.seri.org/ic/icDBRV.html?s_menu=0608&pubkey=ic20160308001&menu_gbn=6&pgsj=&pgno=1&pgor=&menucd=0602&tabGbn=SBJT&kw=(2016.4.11.방문)

47_ CoinDesk, "Smart Contracts," 2016, p.8.

48_ 한승우, 앞의 글, 32면.

4. 금융시장구조의 변화 - 증권시장을 중심으로

일선업무(front-office) [49]

- 고객(client)
  - 대부분의 고객(특히 매수 측)들은 거래비용과 증권서비스 비용의 절감으로 인해 큰 수혜를 받을 것으로 예상됨
  - 거래정보를 투명하게 공개하여 다수의 참가자가 검증을 수행하므로 도 · 소매 투자자 상호 간의 거래도 가능할 것임
- 딜러(dealer)
  - 딜러는 시장 유동성이 약한 경우 유동성 공급 또는 원본리스크 인수 등을 통해 계속적으로 시장 내에서 중요한 역할을 수행할 것임
  - 딜러는 시장에 대한 접근 경로를 제공하는 것이 아니라 가격결정, 거래자문 및 이행관리 측면에서 핵심적인 역할을 할 것임
- 사설거래회사(private trading companies)
  - 실시간 결제절차는 시장조성자(market – makers)와 초단타매매자(high frequency trader) 등 사설거래회사에 큰 영향을 미칠 수 있음
  - 매매거래 전에 소유권을 사전검증하는 경우 초단타매매자는 거래를 하기 위해 각 결제 사이클 동안 기다려야 하는데, 이때 이들의 활동률이 크게 저하되고 블록체인 기술의 도입 범위가 제한될 수 있음

49_ Euroclear/Oliver Wyman, op. cit., pp.10–13; McKinsey&Company, op.cit., pp.16–17.

- 초단타매매자가 의미가 없는 시장 또는 하이브리드 모델(CCP를 사용하기로 합의한 방식)로 운영되는 시장 내에만 블록체인 기술이 도입될 수 있음

❑ 거래장소(venues)

- 거래장소는 대체로 현재와 동일하게 유지될 것이며, 가격형성과 거래상대방 매칭을 촉진할 것임
- 거래 시 생성되는 암호화된 서명데이터는 결제에 필요한 데이터로 기능하여 거래장소의 역할 가치를 증대시킬 것임
- 초단타매매가 거래량의 상당부분을 차지한다는 점에서 시장구조의 중대한 변화는 거래소 및 기타 거래장소에도 영향을 줄 수 있음

≡ 후선업무(back-office)[50]

❑ 청산기관(CCP : central counterparty)

- 현금으로 결제되는 실시간 자산거래의 경우 양 당사자가 거래 전에 각 상대방에 대한 투명성(transparency)을 확보하여 결제가 즉시 이루어지기 때문에 집중청산의 필요성이 사라짐
- 그러나, 파생상품과 같이 만기가 있는 거래의 경우 만기 시에 발생하는 이익을 보장하고 신용리스크를 감소시키기 위하여 계속적으로 CCP를 이용할 필요가 있음

❑ 보관기관(custodian)

- 평면적 계좌구조를 가진 분산 증권장부로 인하여 현재 보관기관이 수행하는 역할 중 일부가 사라질 수 있음

50_ Euroclear/Oliver Wyman, op. cit., pp.10~13; McKinsey&Company, op. cit., pp.16~17.

- 보관기관은 보유지분 정보를 관리하고 자동화된 증권서비스 운영의 올바른 이행을 보장하는 'keeper of the keys'로서 그 역할이 변화될 것임
- 이에 따라 다른 서비스로부터 계좌가 분리되는 결과가 발생할 수 있고, 예탁된 증권을 기반으로 하는 담보관리 등의 서비스가 약화될 수 있음

중앙예탁기관(CSD : central securities depository)

- CSD는 증권을 예탁받아 관리하고 시장의 질서유지기능을 보장하는 역할을 계속 수행할 필요가 있음
- 전통적인 CSD 기능과 같이 장부를 관리하는 프로토콜(protocol)의 조정, 장부상 토큰(token)[51]의 관리 및 규제기관과의 업무연계 등의 역할(operational governance)을 수행하는 것 외에도 증권발행에 있어 분산장부 관리가 가장 중요한 임무가 될 것임

51_ 블록체인 기술 기반에서 거래를 위하여 발행된 거래수단을 말함(비트코인도 토큰의 일종임)

Ⅴ. 블록체인 도입방향과 방법

1. 도입방향

- 블록체인 기술은 이론적으로 다양한 특징과 장점을 가지고 있으나 기술적으로 완벽히 검증되거나 실증적으로 검증되지 아니한 기술임에도 불구하고 계속 발전하고 틈새시장(niche market)을 중심으로 적용분야가 확대되고 있는 중
  - 블록체인 기술은 틈새시장에서의 안정성을 기초로 더 복잡하고 다양한 금융거래 등으로 그 적용이 확대될 것으로 예상

- 블록체인은 아직 기술적으로도, 규제적으로도 성숙하지 않아 이 새로운 산업을 가속화(accelerate)하려면 결국 분산자원을 모아 협력(collaborate)할 필요
  - 블록체인이 인터넷 탄생만큼이나 파급력을 가진 기술이라면, 정부·금융기관·규제기관·기술 스타트업들 모두 한 방향을 향해 긴밀한 협력과 지원이 필요

2. 도입방법

- 금융시장에서 블록체인 기술은 단계적 도입이 예상되며, 도입방식에 따라 경쟁적, 협력적, 강제적 도입 등 세 가지 유형으로 분류할 수 있음

단계적 도입[52]

- 1단계 도입에서는 블록체인 기술의 독립적 도입과 운영을 하고, 2단계 도입에서는 블록체인 기술을 주요자산에 도입하는 것을 고려할 수 있음
  - 한편, 신기술을 도입하는 경우 시스템 인프라의 병행 운영 또는 시스템의 실질적인 교체로 인하여 운영상의 리스크가 발생하므로 이를 최소화 할 수 있는 대책이 필요함
  - 시스템 이행 과정에서의 기술적 실패에 대한 리스크 해소를 위하여 참가자의 신속한 복구 능력 또는 신기술 도입 전 시스템으로의 전환 능력이 요구됨

표_09 단계적 도입 예상모델[53]

유형	이용사례	자본시장 예시	도입 사유
〈1단계도입〉 블록체인 기술의 독립적 도입 · 운영	• 기존 공통장부에 미기재된 자산의 토큰화 (신규 블록체인 기술 또는 비트코인 토큰)	• IPO 전 주식 • 신디케이트론 • 예탁증서(DR)	• 소유권 및 출처 증명 능력 제고 • 결제효율성 제고
	• 참가자간 데이터 공유를 위한 신규 블록체인 기술 이용	• 고객확인의무(KYC) 데이터 • 효율적인 마진관리를 위한 담보장부 • 참조 데이터 및 시장 데이터	• 정보수집 효율화
	• 거래절차에 신규 블록체인 기술 이용	• 기업금융 장부관리 • 펀드 포트폴리오 관리	• 탈(脫) 금융중개화 • 데이터 및 인프라 단순화
〈2단계도입〉 블록체인 기술을 주요자산에 도입	• 더 많은 데이터 셋 감시	• 집중 감시 • 시장 감시 • 가격 데이터	• 데이터 이해도 향상
	• 블록체인 기술을 이용한 업무처리	• 증권 서비스 • 규제 보고	• 업무처리 효율화

52_ Euroclear/Oliver Wyman, op. cit., p.16.

53_ Euroclear/Oliver Wyman, ibid., p.16.

도입방법

- 경쟁에 의한 도입[54]
  - 경쟁에 의한 블록체인 기술의 도입은 기술이용을 촉진할 것이며, 틈새시장에의 경쟁적 기술 도입과 새로운 솔루션의 개발은 금융시장에서 신속하고 성공적인 블록체인 기술 적용을 가능하게 할 것임
  - 수익이 실현되기 전에 네트워크가 형성되어야 하므로 수익성 있는 비즈니스 모델 마련이 어려움
  - 수년간 개발로 인한 현금자원의 고갈, 이용자 확보의 어려움, 목표수익 달성의 어려움 등으로 인해 다수의 신규기업들이 시장에서 이탈할 것임
  - 실패율은 보통의 신규기술과 마찬가지로 90% 이상일 것으로 예상되므로 기술 도입 시 비용 축소, 리스크 감축 등을 위한 적극적인 노력이 필요함

- 블록체인 기술이 성공적으로 도입되면 현재의 이용자 또는 전혀 새로운 이용자를 기반으로 하는 새로운 생태계(ecosystem)가 기존 생태계와 동시에 조성될 것임
  - 기술 도입은 기존 메커니즘의 비용을 부담하기 어려운 발행자를 중심으로 하는 틈새시장에서부터 시작할 수 있음
  - 시간이 지날수록 블록체인 기술을 적용하는 것이 비용이 낮고 효율적이라는 점이 증명되는 경우, 이 기술을 이용하는 분야는 확대되고 보편화될 것으로 예상

54_ ibid., p.17.

협력에 의한 도입 : 기존 참가자의 채택 [55]

- 다수의 공감대 형성은 행위자의 선호도, 기술적인 견해의 차이 등에 의해 그 형성에 많은 시간과 노력이 필요함
  - 금융시장에서 협력에 의한 비기술적 혁신 사례로는 국제스왑 및 파생상품협회(ISDA) 계약을 들 수 있음
  - 이미 기존 참가자들이 내부적 목적뿐만 아니라 다른 참가자와의 컨소시엄 활동을 위해 블록체인 기술 이용을 준비를 하고 있으며, 이에 대한 투자는 계속될 것임
  - 컨소시엄들도 기술 표준 및 기술 프로토콜 선택, 법적·규제적 문제 등의 조정을 위해 협력할 것임

- 초기의 도입 사례로는 기업(예 : R3 CEV)과 함께 협력하여 블록체인 기술을 도입한 사례나 Post Trade Distributed Ledger initiative* 등이 있음

  * 런던증권거래소, 유로클리어, 美 CME그룹 등이 블록체인 기술 솔루션 개발을 위해 함께 구성

강제적 도입 [56]

- 강제적 도입은 정책결정자가 소비자의 비용 절감 또는 시스템 리스크 감축을 위해 블록체인의 기술 이용·도입에 개입하는 것임
  - 최근 호주 증권거래소가 블록체인 기술을 이용한 차세대 청산결제시스템 구축을 추진하고 있음

55_ Euroclear/Oliver Wyman, ibid., p.18.
56_ ibid.

- 그러나 강제적 도입 방식은 의견수렴 과정에서 시장참가자들의 저항에 부딪힐 것으로 예상되며, 블록체인 기술의 강제적 도입은 이 기술이 입증되고 여러 시장에서 사용되는 경우에만 실현 가능할 것임

표_ 10 유형별 블록체인 도입과정[57]

유형	주요 혁신자	시스템 구성	도입 경로
경쟁	• 핀테크(Fintech) • 밸류체인 중 다른 부분에서 나오는 경쟁자	• 기존 시스템과 경쟁	• 고객별 도입
협력	• 참가자, 시장인프라 • 컨소시엄	• 기존 시스템과 병존	• 경제적 이해관계에 따른 회사별 도입
강제 (정책)	• 정책결정자	• 기존 시스템의 교체	• 시스템 전반(또는 업종별) 도입 • 정책결정자 또는 규제기관의 강제

3. 블록체인 도입시기 및 도입비용

도입시기[58]

- [최초 도입] 블록체인 기술은 소수의 참가자만으로 최초 도입이 가능할 것이며, 이러한 도입이 성공적으로 이루어진다면 다수의 주요 참가자도 이 기술을 활용할 수 있으므로 신중하고 실행 가능한 초기 도입이 중요함
  - 변화의 영역 및 규모가 작은 시장에서 과감한 변혁을 시도하는 것이 성공가능성이 가장 크므로 최초의 도입은 틈새시장에서 시작될 것임
  - 향후 12개월 내지 18개월 이내에 통제할 수 있는 비핵심적인 영역에서 도입될 것으로 예상

57_ Euroclear/Oliver Wyman, ibid., p.19.
58_ ibid.

- [도입 확장] 3~5년 후에는 주요시장에서 대다수의 주요 참가자들이 블록체인 기술을 도입함으로써 실질적인 기술 적용이 시작될 것임
  - 이러한 도입 확장은 최초 틈새시장에서의 블록체인 기술 도입 후 시장의 성장 또는 도입의 실패로부터 얻은 시행착오를 바탕으로 가능할 것임
  - 블록체인 기술이 복수의 시장 · 절차 · 자산종류에 대하여 광범위하고도 장기적으로 도입되기 위해서는 다음의 요건이 반드시 필요함
  - 견고한 기술, 기술 솔루션에 대한 강한 친숙도 및 신뢰성, 기존 시스템으로의 전환 능력 등에 대한 다수 시장참가자의 전폭적인 시간 · 자원 투자, 모든 참가자가 사용할 공통 표준 마련 필요

- [시장변화 가능성] 기술은 예상보다 빠르게 진보할 수 있으며 그 파괴력은 다른 시장을 획기적으로 변화시켰으나, 금융시장의 근본 역할과 규제감독 수준을 고려해 볼 때 금융시장이 혁명적으로 변화할 가능성은 낮음
  - 블록체인 기술의 도입과정에서 많은 노력이 필요하므로 2020년 이전에는 블록체인 기술 도입은 기획되지 않을 것이고, 향후 수 년간 블록체인 기술의 대규모 도입은 진행되지 않을 것임

도입비용[59]

- 블록체인 기술을 활용하여 시장 인프라를 구축하는 것은 대규모 작업이므로 성공적인 기술 도입을 위해서는 인프라 · 프레임 개발자측과 네트워크 참가자측 모두 상당한 투자가 필요함
- 시장운영 지연과 비효율성으로 인한 유동성 비용도 발생할 것으로 예상되며, 이 밖에도 블록체인 기술 도입 시 소요되는 비용의 절감을 위해 중복적 시스템의 철폐, 기업에 대한 재정적 요구사항의 축소, 기관 간 비용분담 등이 필요함

59_ Euroclear/Oliver Wyman, ibid., p.20.

Ⅵ. 블록체인의 주요 법적과제

1. 기본방향

- 블록체인 기술을 통한 분산원장을 활용하기 위해서는 누가, 누구에게 규제를 받아야 하는지, 기존규제의 변경 또는 새로운 규제의 제정 필요 등에 대한 검토가 필요[60]

- 블록체인의 분산저장방식을 수용할 수 있는 법적 근거 마련
  - 현행 금융시장은 특정금융기관의 중앙관리를 통하여 전산시스템을 관리하며 처리속도, 해킹 방지, 위변조 방지 등을 위하여 전용선과 폐쇄망을 통하여 보안성을 확보하고 있으며, 중앙관리기관에 의한 전산시스템 운용에 따른 책임소재도 분명히 하고 있음
  - 그러나 블록체인의 경우 특정기관에 의한 중앙관리가 아닌 각 참가자의 분산원장을 통하여 정보의 공유 및 관리가 이루어지기 때문에 현행의 중앙관리중심의 전산시스템 운영체계뿐만 아니라 분산관리시스템인 블록체인 기술의 분산원장을 수용할 수 있는 법상 근거 마련과 책임에 관한 사항을 규제할 필요

- 규제기관의 적법한 개입근거 마련 필요
  - 현행 금융시장에서 중앙관리기관은 하나의 규제수단으로서 매개체 역할을 수행하나, 블록체인 기술을 활용하는 경우 중앙관리기관이 존재하지 않아 규제수단의 매개체가 사라져 정부는 자금흐름, 세금징수, 불법거래, 자금세탁 등의 관리에 애로 예상

60_ 박정국, 앞의 글, 44~45면.

- 특히 2008년 금융위기 이후 세계 각국은 금융거래내역을 집중 관리하기 위하여 규제를 강화하고 있으며[61], 우리나라의 금융정보분석원에서도 금융거래내역의 모니터링을 통하여 불법적 금융거래와 세금탈루거래 등을 발견하고 억제하는 역할을 수행하고 있음

- 이와 같이 블록체인 기술을 이용한 금융거래의 경우 탈중개화와 탈중앙화로 인하여 불법적 거래나 조세회피 등에 악용될 우려가 있는데 블록체인 하에서 이루어지는 거래에 대하여 모니터링 할 수 있는 근거 마련 필요

- 또한 블록체인 기술의 고유한 특성상 한번 기록되면 원칙적으로 수정이 불가능하며, 만일 특정거래의 기록을 수정하기 위해서는 해당 거래가 있는 블록 이후에 생성된 모든 블록을 변경할 필요

- 이를 위하여 거래당사자의 동의가 필요하며, 분쟁 또는 법적 소송의 경우에는 사법적 개입을 위한 규제기관의 적법한 개입과 증거 수집을 위한 원칙과 절차의 마련이 필요

블록체인 기술의 공통표준 및 관리체계[62]

- 블록체인 기술을 통한 분산원장 시스템의 개방 여부, 네트워크 간의 호환성 문제 등 일정한 설계사항에 대하여 공통표준을 마련할 필요가 있으며, 공통규약(protocol) 및 코딩 에러에 대한 보호방법, 다른 네트워크 간의 호환성 확보 등에 대한 표준과 그 관리체계도 마련할 필요가 있음

- 블록체인 기술이 시장 인프라의 중요 부분이 되고 국제 네트워크를 통하여 공통 프로토콜(consensus protocols)[63]로 운영되는 경우 시스템 무결성(integrity)에 대한 보장을 위한 공통표준을 제정할 필요가 있음

61_ 거래정보저장소(TR: rade repository)의 경우 장외파생상품거래 거래내역의 중앙집중적 모니터링을 통하여 장외파생상품거래의 위험을 관리하고 위험에 대하여 사전에 대처하고자 하는 국제적 노력의 대표적 사례라 할 수 있음

62_ Euroclear/Oliver Wyman, op. cit., p.15.

63_ 블록체인 기술 하에서는 모든 참가자가 새로운 거래를 반영하여 원장을 갱신할 수 있는 권한과 책임을 갖고 있기 때문에 특정 내부 참가자가 악의적으로 원장을 조작하여 배포하는 것을 방지할 합치된 규약(consensus protocols) 필요함

2. 블록체인 기술과 관련한 주요 법적이슈와 정비방향

- 이하에서는 블록체인 기술의 완성도와 효율성 여부에 대한 논의는 별론으로 하고, 1개 기관이 독자적으로 운영하는 사적 블록체인 아닌 컨소시엄형 또는 공공형 블록체인을 전자문서, 전자거래 등에 도입하기 위하여 정비가 필요한 규제내용과 관련법에 대하여 살펴보고자 함

(1) 전자문서 및 전자거래의 작성과 송수신 장소

- 관련법 : 전자문서 및 전자거래기본법

- 「전자문서 및 전자거래기본법」상 주요용어(전자문서 및 전자거래기본법 제2조)

  * "전자문서"란 정보처리시스템에 의하여 전자적 형태로 작성, 송신·수신 또는 저장된 정보를 말함

  * "정보처리시스템"이란 전자문서의 작성·변환, 송신·수신 또는 저장을 위하여 이용되는 정보처리능력을 가진 전자적 장치 또는 체계를 말함

  * "작성자"란 전자문서를 작성하여 송신하는 자를 말하며, "수신자"란 작성자가 전자문서를 송신하는 상대방을 말함

  * "전자거래"란 재화나 용역을 거래할 때 그 전부 또는 일부가 전자문서에 의하여 처리되는 거래를 말함

  * "전자거래사업자"란 전자거래를 업(業)으로 하는 자를 말하며, "전자거래이용자"란 전자거래를 이용하는 자로서 전자거래사업자 외의 자를 말함

- 전자문서 및 전자거래의 송신 및 수신의 시기 및 장소와 관련하여 전자문서는 수신자 또는 그 대리인이 해당 전자문서를 수신할 수 있는 정보처리시스템에 입력한 때에 송신된 것으로 보며(전자문서 및 전자거래기본법 제6조 제1항),

- 전자문서는 작성자 또는 수신자의 영업소 소재지에서 각각 송신 또는 수신된 것으로 보며, 영업소가 둘 이상일 때에는 해당 전자문서를 주로 관리하는 영업소 소재지에서 송신·수신된 것으로 보고 있음(전자문서 및 전자거래기본법 제6조 제2항)

- 한편, 「전자문서 및 전자거래기본법」은 전자문서와 전자거래의 송신자와 수신자의 영업소 소재지에서 각각 송신과 수신이 있는 것으로 보고 있으며, 송신자와 수신자의 관계를 1 : 1, 또는 1 : 多의 관계로 파악하고 있어 송신과 수신에 있어서 분산 또는 공유의 관계를 포함하고 있는지 여부가 불분명

- 따라서 현행 「전자문서 및 전자거래 기본법」 상으로 컨소시엄형 또는 공공형 블록체인 기술을 도입하는데 한계가 있어 분산원장 상에서 전자문서가 작성되고 수용할 수 있도록 하는 근거 마련이 필요

- 이를 통하여 블록체인 기술로 작성된 전자문서 및 전자거래도 「전자거래 및 전자문서 기본법」 상 동일한 효력을 인정받을 수 있도록 하여 블록체인 기술을 통한 분산원장의 법적 안정성 확보

(2) 금융회사 및 전자금융업자의 범위

- 관련법 : 전자금융거래법

- 「전자금융거래법」 상 주요용어(전자금융거래법 제2조)

  * "전자금융거래"라 함은 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말함(전자금융거래법 제2조 제1호)

  * "전자금융업자"라 함은 제28조의 규정에 따라 허가를 받거나 등록을 한 자를 말함

  * "전자금융보조업자"라 함은 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 「금융위원회의 설치 등에 관한 법률」 제3조에 따른 금융위원회가 정하는 자를 말함

  * "결제중계시스템"이라 함은 금융회사와 전자금융업자 사이에 전자금융거래정보를 전달하여 자금정산 및 결제에 관한 업무를 수행하는 금융정보처리운영체계를 말함

- 그리고 전자자금이체업무, 직불전자지급수단의 발행 및 관리, 선불전자지급수단의 발행 및 관리, 전자지급결제대행에 관한 업무 등과 같은 전자금융업무를 영위하고자 하는 자는

금융위원회에 등록하도록 하고 있음(전자금융거래법 제28조 제2항)

- 한편 금융회사 또는 전자금융업자는 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고, 전자금융거래를 위한 전자적 장치 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고 등에 대하여 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을 부담(전자금융거래법 제9조 제1항)

- 따라서 금융회사 및 전자금융업자의 범위는 전자금융거래 과정 중에 발생하는 사고 등에 대한 책임을 부담하는 자의 범위에 관한 문제로서, 컨소시엄형 또는 공공형 블록체인 기술을 통하여 전자금융거래를 하고 거래자료를 공유하고 보관하는 자의 경우에도 모두 전자금융업자로 등록되어야 하는지 아니면 전자금융보조자 등으로 취급해야 하는지에 대한 검토와 정비 필요

(3) 규제기관으로의 자료제출

- 한국은행은 금융통화위원회가 전자지급거래와 관련하여 통화신용정책의 수행 및 지급결제제도의 원활한 운영을 위하여 필요하다고 인정하는 때에는 금융회사 및 전자금융업자에 대하여 자료제출을 요구하거나 금융감독원에 검사를 요구하거나 한국은행과의 공동검사를 요구할 수 있음(전자금융거래법 제41조 제1항 및 제2항)

- 그러나, 전자지급거래와 관련한 자료를 블록체인 기술을 통하여 분산원장으로 보관하는 경우 누구에게 자료를 요구하고 누구를 대상으로 검사를 해야 하는지가 문제

- 이와 관련하여, 컨소시엄형 또는 공공형 블록체인의 경우 해당 블록체인의 규약을 관리하는 자 등에 대하여 자료제출 의무를 부여하는 방법을 고려해 볼 수 있으며, 검사대상의 경우에는 규약관리자만을 대상으로 할 것인지 아니면 해당 블록체인의 모든 참가자를 대상으로 해야 하는지는 블록체인 기술구조와 운영구조를 고려하여 정할 필요가 있음

(4) 개인정보보호 및 데이터 보안

- 관련법 : 개인정보보호법
- 「개인정보보호법」상 주요용어(개인정보보호법 제2조)
  - * "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말하며,
  - * "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말함
  - * "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말함.
- 이와 같이 현행 「개인정보보호법」은 개인정보를 중앙집중적 또는 위탁을 통하여 개인정보관리주체가 있는 경우를 가정하여 관련내용을 규정하고 있음(개인정보보호법 제3조)
- 한편, 블록체인 기술을 통하여 분산원장으로 개인정보를 보유하고 있는 경우에 모든 분산원장 보관자가 개인정보처리자 또는 위탁관리자에 해당하는지가 문제
- 이와 관련하여 개인정보처리자 또는 위탁자의 범위에 일정한 요건하의 분산원장 보관자도 포함될 수 있도록 정비할 필요
- 또한 신원확인 등 개인정보 확인 시에 발생할 수 있는 해킹, 바이러스, 메일폭탄, 서비스 거부 등과 같은 데이터 침해사고(breach)[64]를 방지할 수 있는 대책 마련의 주체도 정할 필요

64_ 해킹, 컴퓨터바이러스, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망이나 이와 관련된 정보시스템을 공격하는 행위를 하여 발생하는 사고를 의미함

(5) 공인전자서명

- 관련법 : 전자서명법
- 「전자서명법」 상 주요용어(전자서명법 제2조)
  - "전자서명"이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말함
  - "공인전자서명"이라 함은 다음의 요건을 갖추고 공인인증서에 기초한 전자서명을 말함
    - 전자서명생성정보가 가입자에게 유일하게 속할 것
    - 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것
    - 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것
    - 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것
  - "인증"이라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말함
  - "인증서"라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고, 이를 증명하는 전자적 정보를 말하며, "공인인증서"라 함은 공인인증기관이 발급하는 인증서를 말함
  - "공인인증기관"이라 함은 공인인증업무를 제공하기 위하여 미래창조과학부장관이 공인인증업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정하여 지정한 자를 말함
- 전자서명법 상 전자서명의 효력은 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 보며(전자서명법 제3조 제1항),
- 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정하며 (전자서명법 제3조 제2항),
- 공인전자서명외의 전자서명은 당사자 간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가지는 것으로 규정하고 있음(전자서명법 제3조 제3항)
- 이와 관련하여 현행 「전자서명법」상 블록체인 기술을 통한 전자서명이 공인전자서명으로 인정받기 위해서는 "서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것"이라는 요건이 필요한데,

- 블록체인 기술의 분산원장으로 전자서명을 관리하는 경우에 서명자가 전자서명 생성정보를 지배하고 관리하고 있다고 볼 수 있는지가 의문

- 이와 관련하여 일정조건 하의 블록체인 기술의 분산원장으로 '전자서명 생성정보를 지배관리'하는 경우에는 이를 서명당시 가입자가 지배하고 관리하는 것으로 인정하는 방법을 고려할 수 있음

- 또한 일정한 요건하에서 블록체인 기술의 분산원장시스템을 통하여 서명한 경우에는 이를 공인전자서명과 같은 효력을 가지는 것으로 인정하는 방안도 검토 가능

(6) 상법상 전자등록증권 및 전자선하증권의 발행

- 관련법 : 상법

- 「상법」은 유가증권을 전자등록기관의 전자등록부를 통하여 발행할 수 있도록 규정하면서(상법 제65조 제2항), 주식, 신주인수권증서, 채권 등의 전자등록(상법 제356조의2 제1항, 제420조의4, 제478조 제3항, 제516조의2)은 모두 별도의 전자등록기관을 통하여 전자적으로 발행하도록 하고 있음

- 이에 따라 블록체인 기술을 통하여 발행회사가 직접 주식을 전자적으로 발행하는 것은 상법의 규정에 반하는 것으로서 주식이나 채권 등의 발행의 효력이 없는 것으로 보아야 할 것임

- 따라서 발행회사가 직접 블록체인 기술을 통하여 주식이나 채권 등을 발행할 수 있도록 하기 위하여 발행회사가 블록체인 기술을 통하여 분산원장방식으로 전자등록기관에 의하지 아니하고 주식이나 채권 등의 증권을 발행할 수 있는 근거규정이 필요

- 이외에도 운송인이 전자선하증권을 발행하는 경우에는 법무부장관이 지정하는 등록기관에 등록하는 방식으로 전자선하증권을 발행할 수 있도록 규정하고 있는데(상법 제862조 제1항),

- 운송인이 블록체인 기술을 통하여 직접 전자선하증권을 발행할 수 있도록 하기 위해서는 역시 등록기관을 통하지 아니하고 블록체인 기술의 분산원장 방식으로 운송인이 직접 전자선하증권을 발행할 수 있도록 하는 규정 정비가 필요

- 한편, 회사는 정관이 정하는 바에 의하여 명의개서대리인을 둘 수 있으며, 명의개서대리인의 자격은 「자본시장과 금융투자업에 관한 법률」(이하 "자본시장법"이라 함)에 따라 설립된 한국예탁결제원 및 전국적 점포망을 둔 은행으로서 규정(상법 제337조 제2항, 동법 시행령 제8조),

- 또한 한국거래소에 주권상장의 요건과 한국예탁결제원에 주식의 예탁대상지정 요건으로 명의개서대리인 선임이 의무화되어 있음

- 이렇게 명의개서대리인의 자격을 엄격히 제한하고 주권의 상장요건과 예탁대상지정요건으로 명의개서대리인 선임의무를 부여하고 있는 것은 발행회사에 의한 주금의 납입 없이 허위로 주식을 발행하는 것을 방지하고 주식발행 및 주주명부관리업무의 안정성과 효율성을 도모하기 위한 것임

- 따라서 블록체인 기술을 통한 분산원장 방식으로 발행회사가 직접 주식 등 증권을 발행하기 위해서는 발행의 효율성뿐만 아니라 주금 납입없는 주식발행이나 채권의 대금납입 없는 채권의 허위발행과 유통과 같은 위험을 차단할 수 있는 제도적 장치의 마련도 동시에 필요

(7) 전자적 의결권 행사

- 관련법 : 상법

- 회사는 이사회의 결의로 주주가 총회에 출석하지 아니하고 전자적 방법으로 의결권을 행사할 수 있으며, 전자적 방법에 의한 의결권 행사시 주주 확인 및 전자투표는 전자서명법 상 공인전자서명의 방법으로 하도록 규정하고 있음(상법 제368조의4 제4항 및 동법 시행령 제13조)

- 따라서 블록체인 기술을 통하여 주주 확인과 전자투표를 위해서 공인인증서 사용의무에 관한 제한이 해소될 필요가 있음

(8) 특별법상 전자등록증권의 발행

- 관련법 : 주식 및 사채 등의 전자등록에 관한 법률
- 상법은 유가증권을 전자등록기관의 전자등록부를 통하여 발행할 수 있도록 규정하면 전자등록기관에 관한 사항 등 세부사항은 상법시행령에서 규정하도록 하고 있으나 상법시행령에서 이에 관한 사항이 규정되어 있지 아니하여 전자증권제도가 사실상 운영되지 아니하고 있었음
- 한편, 「주식 및 사채 등의 전자등록에 관한 법률」(이하 "전자증권법" 이라 함)에서는 주식 등의 전자등록업을 영위하고자는 하는 자는 전자등록업 허가단위별로 허가를 받도록 규정하고 있음(전자증권법 제5조 제1항)
- 따라서 블록체인 기술을 통하여 분산원장 방식으로 허가받은 전자등록기관 이외의 자가 주식 등을 발행하는 것은 현행법으로는 불가능하여 이에 대한 정비가 필요
- 한편 집단·대량·정형적으로 발행·유통·결제되고 복잡하고 다양한 권리가 존재하는 하는 증권의 속성상 전자등록기관 업무를 영위하기 위해서는 증권에 관한 전문성과 업무에 대한 신뢰성이 필요
- 따라서 블록체인 기술을 통하여 분산원장 방식으로 전자등록기관과 같이 중앙관리기관이 없이 증권을 발행하고 관리하게 하기 위해서는 엄격한 발행 및 관리 절차가 필요

(9) 블록체인 기술을 이용한 금융투자상품 거래

- 증권 등 금융투자상품을 정규시장에서 거래하기 위해서는 상장, 공시, 시장감시, 분쟁조정 등 시장관리와 투자자 보호 장치를 마련하는 것이 중요

- 이에 따라 현행 자본시장법은 거래소허가를 받지 아니하고는 금융투자상품시장을 개설하거나 운영할 수 없도록 규정(자본시장법 제373조 본문),
- 다만, 다자간매매체결회사(alternative trading system)의 다자간매매체결업무, 금융투자협회가 비상장주권에 대해 장외매매거래를 하는 경우 및 기타 금융투자상품의 공정한 가격 형성, 매매거래의 안정성 및 효율성 도모, 투자자보호에 우려가 없는 경우에 한하여 거래소 허가 없이 시장을 개설하거나 운영 가능(자본시장법 제373조 단서)
- 한편, 외국인투자자의 경우 증권대차거래와 같은 경우 이외에는 외국인투자자의 투자내역과 투자동향을 효율적으로 관리하기 위하여 원칙적으로 장내시장을 통해서만 매매를 하도록 하고 있음
- 따라서 금융투자상품의 거래를 컨소시엄형 또는 공공형 블록체인 기술을 이용하여 분장원장으로 이용하기 위해서는 매매거래의 안정성과 효율성을 도모하고 투자자 보호를 할 수 있도록 금융투자상품거래 프로세스의 재정비와 더불어 관련법규의 정비도 필요

(10) 블록체인 기술을 이용한 증권결제

- 증권시장에서의 증권의 매매거래에 따른 증권인도 및 대금지급업무는 결제기관으로서 예탁결제원이 수행하도록 규정하고 있으며(자본시장법 제297조),
- 증권거래에 따른 결제를 위해서는 원칙적으로 증권 거래시에 매도자가 증권을 보유하고 있는지, 매수자가 결제대금을 보유하고 있는지에 대하여 사전적으로 확인할 필요가 있음
- 특히 매도자와 매수자가 각각 1인인 상대매매와 상대결제의 경우가 아닌 장내거래와 같이 다자간 매매거래와 다자간(차감)결제의 경우에는 현행 중앙예탁결제기관과 같은 제3자 관리기관의 개입이 결제의 효율성을 높이고 결제의 완결성 확보에 더 안정적일 수 있음

- 따라서 블록체인 기술을 통한 국내외에서의 동시적인 대규모 증권거래와 이에 따른 결제의 완결성을 확보할 수 있는 블록체인 기술을 적용하기 위해서는 우선적으로 결제의 효율성과 안정성 및 결제완결성을 확보할 수 있도록 프로세스의 재정비와 더불어 관련 법규의 정비도 필요

- 그러나 개인 간 상대거래와 이에 따른 상대결제가 이루어지는 순수한 장외거래의 경우에는 민법과 상법 등 관련법에 따라 분산저장 기술을 이용하는데 법적 제약 요인은 없을 것으로 보임

Ⅶ. 결 론

- 블록체인 기술은 탈중앙성, 탈중개성, 효율성, 확장성, 보안성, 안정성, 신뢰성, 투명성 등에 있어서 많은 장점을 보유한 기술로 평가되고 있으며, 동 기술이 계속 발전하고 적용대상이 확대되는 경우 금융의 IT화, 금융의 제조산업화, O2O 비즈니스의 확대 등 금융시장에 미치는 영향은 매우 높을 것을 예상

- 그러나 블록체인은 아직 규제환경의 미흡, 기술적 공감대 형성 미흡, 분산성의 한계, 우발적 거래의 취소 불가능, 과도한 자원 투입, 상당한 도입비용소요, 확장성 제약, 이견조정 지연 등 여전히 해결해야 하고 실증적으로 검증해야 할 과제도 산적해 있음

  - 금융인프라기관은 금융산업을 구성하는 모든 주체가 공동으로 소유하고 이용하는 인프라로서 기술의 진보와 발전에 편견이나 이해관계가 없기 때문에 블록체인 기술이 발달하여 그 유용성이 입증된다면 블록체인 생태계(ecosystem)를 현재의 금융시장 인프라와 통합하는 역할을 수행할 것으로 예상

- 따라서 많은 장점을 가진 블록체인 기술이지만 이를 금융기관과 공공영역 서비스에 바로 도입하기 위해서는 금융기관, 스타트업 기업, 규제기관 등 상호간 커뮤니케이션이 중요하며, 기술에 대한 완벽한 이해가 우선되고, 정부와 민간 영역, 개방과 중앙통제 사이에 균형을 이루면서 데이터를 공유한다면 보다 많은 분야에 적용가능

  - 그러나 블록체인이 오픈소스로서 효율성과 확장성에 대한 기술적 불확실성, 익명성을 이용해 가상화폐 일부가 불법 거래대금 결제, 비자금 조성, 탈세로 이어지는 문제점이 존재하며

- 블록체인 기술에 대한 모호한 이용사례 및 막대한 비용절감에 대한 비현실적인 약속 등으로 인하여 금융기관은 아직 블록체인 기술의 도입에 관망적인 태도를 취하고 있음

- 그러나 블록체인 기술이 널리 도입되면 블록체인과 관련한 현재의 기술적 제도적 문제들은 개선될 것이며, 여러 금융기관들의 역할이 근본적으로 변화하게 될 것이고, 금융시장의 가치사슬(value chain)의 각 부분을 흔들어 놓을 수 있기 때문에 이러한 태도는 바람직하지 못함

- 현재, 국내외 금융기관 등은 블록체인 기술의 한계와 문제점에도 불구하고 그 기술의 우수성과 잠재력이 상당할 것으로 예상하고, 관련 스타트업 기업과 협업하면서 적용가능 대상 분야에 대해 POC 등을 통해 기술검증과 적용가능성을 높이고 있음

  - 블록체인 기술의 적용가능 금융분야로는 지급결제·증권발행·증권거래·증권결제·자산관리 서비스·파생상품거래 등이 있으며, 비금융분야로는 자산등록부·신원등록부·지적재산권등록·음악 및 엔터테인먼트·전자장치 및 사물인터넷·정부 및 대리인 사용·전자공증·공인인증서발급 등 그 적용분야가 매우 다양

- 그러나 블록체인 기술은 다양한 장점에도 불구하고 금융기관에 공공형 블록체인을 도입하기에는 한계가 있어, 컨소시엄 또는 사적 블록체인 현태로 도입될 가능성이 더 높아 보이고 있으며,

- 도입방법도 일시적이고 강제적으로 도입되기 보다는 충분한 기술검증을 통해 적용대상 분야를 점점 확대해 나가는 방식으로 단계적으로 도입될 것으로 예상되며, 또한 정부 주도의 강제적 방식보다는 민간주도의 경쟁적, 협력적 방식으로 도입될 것으로 예상됨

- 블록체인 기술의 도입을 위한 연구와 투자를 위해서는 우선적으로 업무프로세스의 재정비와 중앙집중식 전산시스템을 가상한 현행의 규제체계를 분산원장 방식도 수용할 수 있도록 정비할 필요

- 이외에도 블록체인 기술을 통해 결제의 최종성과 데이터의 물리적 보관 장소에 관한 규정, 규제기관의 적법한 개입근거 마련에 관한 사항, 블록체인 기술의 공통표준 관리체계(governance)에 관한 사항 등 정비해야 할 프로세스와 법적 과제가 상당할 것으로 예상됨

- 이와 관련하여 IT 관련법으로는 「전자문서 및 전자거래기본법」, 「전자금융거래법」, 「전자서명법」, 「개인정보보호법」 등의 정비가 필요하며, 금융관련법으로는 「상법」 등의 정비가 필요

- 한편, 블록체인 기술 이용사례를 명확히 설명하여야 하고, 왜 블록체인 기술이 필요한지 왜 이 기술이 업계 · 고객에게 이득이 되는지를 명확히 제시하여야 하며, 규제기관은 금융시장이 블록체인 기술을 도입하는 데에 있어 중요한 이해관계를 가지고 있으므로 모든 쟁점에 대하여 철저히 분석하고 혁신적인 기술이 금융시장에 도입되는 것에 대한 프로세스적, 제도적, 규제적 장애를 제거하는데 대한 적극적인 자세 필요

참고문헌

김동섭, 「분산원장 기술과 디지털통화의 현황과 시사점」, (한국은행, 금융결제국 결제연구팀), 2016.

금융보안원, “블록체인(Blockchain) 개요 및 활용사례,” 2015.6.24.

, “블록체인 및 비트코인 보안기술,” 2015.11.23.

, “국내외 금융분야 블록체인(Blockchain) 활용동향,” (보안연구부－2015－028), 2015.11.23.

, “국내외 금융분야 블록체인(Blockchain) 활용동향,” (보안연구부－2015－028), 2015.11.23.

, “이더리움(Ethereum) 소개 및 특징 분석,” 보안연구부－2016－0098), 2016.3.4.

김태우, “블록체인이 자본시장에 미치는 영향,” 「예탁결제」 (한국예탁결제원, 2016. 제97호 2016－1분기).

박정국, “블록체인 기술의 동향과 금융권의 대응,” 「블록체인 : 금융산업의 파괴자인가 아니면 새로운 기회인가?,」 (한국지급결제학회 2016년 춘계세미나, 2016.6.1.).

박소영, “Blockchain,” (PayGate, 2015.12).

심윤보, “블록체인 기술 공동 개발에 나선 글로벌 은행들,” 하나금융경영연구소 Weekly Hana Financial Focus (제5권39호 2015.10.12.∽10.18).

정유신, “블록체인의 금융산업에 대한 영향과 정책과제,” 2016.5.

최은실, 김도훈, 송주한(역저), 「비트코인, 블록체인과 금융의 혁신」, (고려대학교 출판문화원), 2015.10.

한승우, "블록체인 활용사례로 알아보는 금융권 적용고려사항," 「전자금융과 금융보안」 (금융보안원), 2016.

Andres Guadamuz and Chris Marsden, "Blockchain and Bitcoin : Regulatory response to cryptocurrencies," (First Monday–Peer Reviewed Journal On The Internet, Volume 20, Number 12–7), December 2015.

Andreas M. Antonopoulos LLC, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 2015.

CoinDesk, "Banks and the Blockchain Report," 2015.

CoinDesk, "Smart Contracts," 2016.

DTCC, "EMBRACIING DISRUPTION–TAPPING THE POTENTIAL OF DISTRIBUTED LEDGERS TO IMPROVE THE POST–TRADE LANDSCAPE," JANUARY 2016.

McKinsey & Company, "Beyond the Hype: Blockchain in Capital Markets," (McKinsey Working Papers on Corporate & Investment Banking / No.12) December 2015.

Morrison & Foerster LLP, "Client Alert," 2016.

Michael Mainelli / Alistair Milne, "The Impact and Potential of Blockchain on the Securities Transaction Lifecycle," (SWIFT Institute, SWIFT Institute Working Paper No.2015－007, 09 May 2016).

블록체인 분산원장 도입을 위한 법적 과제

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE