



**KCMI**

Korea Capital  
Market Institute

# 자본시장에서의 블록체인 기술의 활용 전망 및 시사점

조성훈

## 조성훈 (Sung Hoon Cho)

선임연구위원 / 경영학 박사

### 연구분야

- Securities Industry
- Investment Banking
- Corporate Finance
- Corporate Governance

# 자본시장에서의 블록체인의 기술의 활용 전망 및 시사점

2016. 11.

선 임 연구 위원      조 성 훈





## 序 言

블록체인은 최근 등장하고 있는 다양한 핀테크(fintech) 중에서도 특히 많은 관심의 대상이 되고 있는 기술이다. 디지털화된 공개 분산원장을 의미하기도 하는 블록체인은 거래를 보다 신속하게 처리하고, 시장 운영 비용을 획기적으로 절감하며, 강력한 보안성을 바탕으로 원장에 대한 신뢰성을 높일 수 있다는 등의 강점을 보유한 기술로 알려지면서 다양한 분야에서의 활용 가능성이 논의되고 있다. 그리고 그 중에서도 금융, 특히 자본시장은 블록체인의 강점들이 가장 잘 발휘되고 활용될 수 있는 영역으로 여겨지고 있으며, 따라서 전 세계적으로 도입·활용을 위한 활발한 논의와 시도가 이루어지고 있다. 새로운 기술의 출현 초기에 흔히 수반되는 흥분과 과장(hype)은 블록체인에서도 나타났으나, 현재는 보다 냉정하고 치밀하게 블록체인 기술의 현주소와 가능성을 평가하고, 도입을 위한 구체적인 로드맵을 논의하는 양상을 보이고 있다.

이와 같은 시장과 업계에서의 높은 관심과 활발한 움직임에 따라, 외국에서는 정책·규제기관, 금융회사 및 시장운영기관, 컨설팅회사 등으로부터 다양한 자료가 등장하고 있다. 국내에서도 금융 및 자본시장 관련 기관들이 블록체인에 관한 검토 혹은 조사 자료들을 내놓고 있다. 그러나 현재 블록체인 기술의 도입과 활용에 대하여 국제적으로 어떠한 논의가 어느 정도 수준에서 이루어지고 있는지, 그리고 향후 전망은 어떠한지 등을 포괄적으로 정리한 자료는 그리 많지 않다. 본 보고서는 이러한 배경에서 자본시장을 중심으로 한 금융에서의 블록체인 기술의 도입·활용 현황 및 관련 이슈들을 정리한다는 목적으로 작성되었다.

본 보고서는 블록체인의 작동 원리와 특징을 설명하고, 현재 진행되고 있는 자본시장에서의 논의 및 대표적인 도입 시도 사례들을 소개한다. 그리고 이를 토대로 자본시장 업계 및 정책·규제당국에 대한 시사점을 제시해 보고자 하였다. 아무쪼록 본 보고서가 우리나라 자본시장에서의 블록체인 기술의 도입 및 활용에 있어서 도움이 될 수 있기를 기대한다.

본 보고서는 자본시장연구원의 조성훈 선임연구위원에 의하여 작성되었다. 저자의 노고에 감사의 뜻을 표한다. 또한 보고서의 개선을 위한 귀중한 조언을 아끼지 않은 지정논평자 최순영 연구위원 및 원내 세미나에 참석한 본원의 연구위원들께도 감사의 말씀을 전한다. 자료 수집 및 정리를 위하여 수고한 여밀림 연구원, 원고 정리와 편집을 담당한 이수련 연구조원의 수고에도 감사드린다.

마지막으로 본 보고서의 내용은 전적으로 저자의 개인적 견해이며 자본시장연구원의 공식적 입장이 아님을 밝혀둔다.

2016년 11월  
자본시장연구원  
원장 안 동 현

# 목 차

---

---

Executive Summary .....	vii
Abstract .....	xi
I. 서론 .....	3
II. 블록체인 소개 .....	11
1. 블록체인의 개념 및 역사 .....	11
2. 블록체인의 작동 메커니즘 .....	15
3. 블록체인의 특성 .....	24
4. 비트코인 외 블록체인 기반 플랫폼의 등장 .....	31
III. 블록체인 기술의 활용 논의 및 도입 시도 동향 .....	37
1. 블록체인 기술의 활용에 대한 평가와 기대 .....	37
2. 해외의 블록체인 기술 도입 동향 .....	48
3. 국내 기관의 블록체인 기술 도입 동향 .....	59
IV. 종합 및 시사점 .....	63
1. 자본시장 업계에의 시사점 .....	64
2. 정책·규제당국에의 시사점 .....	65
참고문헌 .....	71

## 표 목 차

---

---

<표 III-1> R3CEV 참여 기관 현황 (2016년 6월 기준) .....	49
<표 III-2> Hyperledger 프로젝트 참여 기관 현황 (2016년 6월 기준) ·	52
<표 III-3> 국내 금융회사의 블록체인 도입 사례 .....	60

## 그림 목 차

---

---

<그림 I-1> 블록체인과 비트코인 관심도 추이 (Google Trends) .....	4
<그림 II-1> ‘제3자’를 통한 집중형 원장 시스템과 블록체인의 분산원장 시스템 비교 .....	13
<그림 II-2> 블록의 구성 및 연결 구조 .....	20
<그림 III-1> 자본시장 후선업무 구조 .....	40

## 약어 표

---

ASIC	Application Specific Integrated Circuit
ASX	Australian Securities Exchange
CCP	Central Counterparty
CFTC	(US) Commodity Futures Trading Commission
CSD	Central Securities Depository
DAO	Decentralized Autonomous Organization
DTCC	Depository Trust and Clearing Corporation
EMIR	European Market Infrastructure Regulation
ESMA	European Securities and Markets Authority
EU	European Union
FCA	Financial Conduct Authority
HLP	Hyperledger Project
JPX	Japan Exchange Group
KPM	KRX Private Market
KRX	Korea Exchange
LSE	London Stock Exchange
NSA	National Security Agency
P2P	Peer-to-Peer
SAC	Securities Association of China
SEC	Securities and Exchange Commission
SFD	Settlement Finality Directive

## 《 Executive Summary 》

블록체인(blockchain)은 ‘디지털화된 공개 분산원장(public distributed ledger)에 의하여 거래 기록의 무결성(integrity)과 신뢰성(trust)을 확보하는 컴퓨터 네트워크 기반 기술’이라고 정의할 수 있으며, 동시에 분산원장(distributed ledger) 자체를 의미하기도 한다. 블록체인은 비트코인(Bitcoin)의 기반 기술로 처음 등장하였으며, 시간이 경과함에 따라 이 기술이 갖는 독창적인 특성들, 그리고 다양한 측면에서의 활용 가능성에 대한 인식이 확산되면서 블록체인에 대한 관심이 폭발적으로 증가하였다. 금융산업에서 먼저 블록체인의 가능성에 주목하기 시작했고, 이후 금융 뿐 아니라 실물경제와 행정 등에서 다양한 활용 가능성이 논의되고 있다. 일각에서는 블록체인을 가리켜 인터넷 이후 가장 혁신적이며, 파괴적인(disruptive) 기술이라고까지 평가하기도 한다. 그러나 아직까지 블록체인의 실제 응용 및 도입은 초기 단계이며, 블록체인을 활용한 서비스가 본격적으로 제공되고 있지는 않은 바, 블록체인이 실제로 금융 및 인간 사회에 얼마나 큰 영향을 미칠 것인지에 대한 판단은 시기상조이다.

블록체인 기술의 핵심적인 특징은 첫째로 ‘제3자 기관’이나 중개 기관 없이, 시장의 모든 거래 참여자가 P2P(peer-to-peer)로 직접 연결된다는 점, 둘째로 거래 내역을 기록한 원장(ledger)이 모든 시장 참여자들에 의하여 분산 보관되며, 원장의 업데이트 및 기록의 정확성에 대한 검증과 승인이 비트코인에서의 작업증명(proof of work)과 같은 사전에 프로그래밍 된 규칙에 따라 시장 참여자들의 합의 메커니즘에 의하여 이루어진다는 점, 셋째로 이 모든 과정은 고도의 암호화(cryptographic) 기법에 의하여 보안이 유지된다는 점으로 요약할 수 있다. 이러한 특징들은 블록체인 기술이 기존의 거래 및 원장의 관리 방식, 즉 중개기관을 경유하는 거래, 그리고 신뢰할 수 있는 ‘제3자 기관’에 의한 원장의 관리라는 방식과는 전혀

다른 새로운 거래 및 원장 관리 방식이라는 것을 의미한다.

블록체인 중에서도 비트코인 시스템에서 사용되고 있는 것은 사전 허락이나 동의 없이 누구나 네트워크에 참여할 수 있는 개방형(permissionless) 블록체인이다. 그런데 최근 금융을 비롯하여 블록체인의 도입·활용을 검토 또는 시도하고 있는 산업계에서는 대부분 개방형이 아닌 폐쇄형(permissioned) 또는 완전한 사적(private) 블록체인의 채택을 검토하고 있다. 폐쇄형 블록체인은 정해진 구성원들만으로 네트워크의 노드가 구성된 블록체인을 의미하며, 사적 블록체인은 완전한 개인형 블록체인으로 단일의 주체가 내부 전산망을 블록체인 네트워크로 구성하여 관리·운영하는 것을 의미한다.

블록체인은 몇 가지의 독특한 기술적, 경제적 특성을 가진다. 우선 '제3자'로의 집중 없이, 모든 네트워크 참여자들이 P2P로 연결되며, 원장이 모든 네트워크 참여자들에게 공개되어 있다는 점에서 분산·분권·개방형 구조를 갖는다. 또한 블록체인 기술이 주목을 받는 가장 핵심적인 요인은 강력한 보안성과 안전성이다. 그리고 이러한 강력한 보안성과 안전성은 바로 분산·분권형 네트워크 구조, 그리고 블록체인 내에서의 블록의 연결 구조에 그 바탕을 두고 있다. 그리고 블록체인에서 발생하는 거래는 각각의 거래 발생 시점에 거래 대상 상품의 인도와 대금의 결제가 이루어지며, 일단 블록에 기록되어 블록체인에 연결된 거래는 취소나 정정이 불가능하다는 특성을 갖는다. 또한 '제3자 기관'을 따로 설치할 필요가 없고, 거래에 있어서 중개기관을 배제할 수 있다는 점에 기인하는 경제성, 원장의 기록을 변경할 수 없고, 원장이 네트워크 참여자들에게 공개된다는 점에 기인하는 투명성 등이 블록체인이 갖는 특성으로 거론된다. 추가적으로 개방형 블록체인의 경우에는 네트워크 참여자들 사이의 신뢰를 필요로 하지 않는다는 점도 중요한 특성이다.

블록체인 기술의 도입과 활용이 기대되는 경제와 사회의 많은

영역과 기능 중에서도 현재 도입을 위한 구체적인 논의와 노력들이 가장 활발하게 이루어지고 있는 부문은 금융, 그 중에서도 자본시장이다. 자본시장은 다수의 시장참가자들 사이에서 자산의 거래가 지속적으로 발생하고 있고, 거래에 따른 자산 소유권의 이전에 대한 정확한 기록을 담은 원장의 안전한 보관이 매우 중요하다는 점에서 블록체인 시스템이 가지고 있는 본질과 특성이 장점으로 발휘될 수 있는 부문으로 여겨지고 있다.

현재 자본시장을 비롯한 금융에서 블록체인 기술의 도입은 시작 단계이다. 은행을 중심으로 한 일부 금융회사에서 외화송금과 같은 일부 서비스에 블록체인 기술을 도입하는 것을 개발·시험 중이다. 그리고 전 세계 유수의 금융회사들로 구성된 R3CEV와 같은 블록체인 컨소시엄 역시 현재 블록체인 네트워크의 설계, 지배구조(governance), 기술표준 등에 관한 논의를 진행하면서, 구현하려는 서비스에 대한 개념증명(proof of concept)을 시도하는 단계로 본격적인 서비스가 가동되고 있지는 않다.

현재 자본시장에서 블록체인 기술의 도입에 관하여 이루어지고 있는 논의는 두 개의 흐름으로 압축되고 있다. 첫째로 매매거래의 체결과 같은 전선업무(front office)에서는 상대적으로 거래 빈도가 낮고, 거래 참가자의 자격과 수가 제한적인 비공개기업의 주식 발행 및 거래 플랫폼을 블록체인 기반으로 구축하는 것이다. 둘째로 청산·결제·예탁과 같은 후선업무(back office)를 블록체인 기반으로 구축하는 것이다. 그리고 다수의 논의는 후자에 집중되고 있다. 여러 기관들이 이와 관련된 자료들을 내놓고 있으며, 이러한 자료들에서 제시된 논의들을 종합하면 대체로 자본시장에 도입되는 블록체인은 폐쇄형이 될 것이며, 실제 블록체인 기반의 후선업무 플랫폼이 등장하는 것은 대략 2~3년 후가 될 것이라는 데에 의견이 일치하고 있다.

블록체인 기술을 자본시장에 도입하여 활용하는 데 있어서는 산업

전체 차원에서의 공동의 노력과 협력이 반드시 필요하다. 따라서 개별 회사 차원이 아닌 산업 전체 차원에서의 논의·조정·합의를 위한 기구가 구성되는 것이 필요하다. 이 기구에는 거래소, 예탁결제원과 같은 자본시장 인프라기관, 증권회사·자산운용회사와 같은 주요 참여자들, 블록체인 기술기업들이 핵심적으로 포함될 것이며, 정책·규제당국 역시 함께 참여하는 것이 필요하다. 이 기구에서 논의되고 합의가 도출되어야 하는 핵심적인 의제로는 자본시장의 일련의 프로세스 중 블록체인 기술을 도입할 부분 혹은 기능, 요구되는 기술표준, 만들어질 블록체인 네트워크의 지배구조, 참여기관들의 유인 및 이해 조정, 블록체인 네트워크 구축 소요비용 분담을 들 수 있다.

자본시장에서의 블록체인 기술의 도입과 관련하여 정책·규제당국이 해야 할 가장 핵심적인 역할은 규제적 불확실성을 최소화하여 블록체인의 도입 논의, 그리고 도입을 위한 혁신이 방해받지 않도록 하는 것이다. 우선 블록체인 기술의 도입과 관련하여 법적·제도적 기반이나 근거가 필요한 경우, 이를 마련해 주는 것이 필요하다. 또한 현행 제도 및 규제 중에서 블록체인 기반의 새로운 시스템과 충돌할 가능성이 있는 부분에 대한 검토 및 수정·보완을 통하여 제도와 블록체인 시스템과의 정합성을 높이도록 해야 할 것이다. 그리고 이러한 역할을 효과적으로 수행하기 위해서 정책·규제당국은 블록체인 기술의 본질 및 특성, 현재 진행되고 있는 논의의 내용, 기술 개발 등 동향을 실시간으로 파악하고 있어야 하며, 이를 위해서는 업계와의 긴밀한 소통이 필수적이다. 또한 새로운 블록체인 기반 플랫폼 혹은 시스템이 자본시장에서 사용될 경우 안전성, 투자자 보호 등에서 기존 시스템과 최소한 동일한 수준을 달성하도록 담보하는 것 역시 중요한 역할이다.

« Abstract »

**Blockchain in Capital Markets: A Brief Review**

Blockchain is defined as a computer network technology which ensures the integrity and trust of a ledger (record of transactions) with digitalized public distributed ledger. It first emerged as an operation mechanism of Bitcoin, and is recognized as one of the most important and disruptive innovations since the internet.

Blockchain has some unique features. Blockchain has the P2P (peer-to-peer) network structure without a ‘trusted third party.’ All participants (nodes) in a blockchain network store and update the ledger. Verification of the validity of transactions, and confirmation of a block are conducted by network participants with a programmed ‘consensus algorithm.’ And the whole process in blockchain is strongly secured by highly sophisticated cryptographic technologies. Due to some strengths of blockchain such as strong security, fast processing of transactions and the potential of huge cost reduction, blockchain draws explosive attention from various industries and governments around the world.

Blockchain used in Bitcoin or Ethereum is ‘permissionless’ one in the sense that anyone can participate in the network as a node without permission or approval. But the consensus is that ‘permissioned’ blockchain in which a new member can be added to the network only with the permission of incumbent members will be adopted for industry or business

purpose.

Capital markets are widely believed to be an area in which strengths of blockchain can be made the best use of because trading of assets took place incessantly among a number of market participants, and also because accurate updating and secure storage of ownership transfer records are important. Currently, most capital market players concentrate their efforts for adopting blockchain technology on the ‘post-trade processing’ among the whole capital markets value chain. Also exchanges, Nasdaq and KRX for example, are developing the blockchain-based trading platforms for private companies.

Industry-wide collaboration is essential for successful adoption of blockchain technology in capital markets. Therefore, an industry-wide blockchain consortium composed of exchanges, depositories, CCPs, broker-dealers, tech companies and regulatory authorities should be organized. Key agendas to be discussed will include the area or function where blockchain technology to be adopted, required technology standard, governance, coordination of interests of participating organizations and sharing of development costs.

The most important role of regulatory authorities is to minimize legal/regulatory uncertainties so as for the adoption of blockchain technology not to be hindered. For instance, legal foundation for issuing and trading of crypto-securities needs to be provided. Close communication with industry is crucial for playing this role effectively.

## I. 서론

---



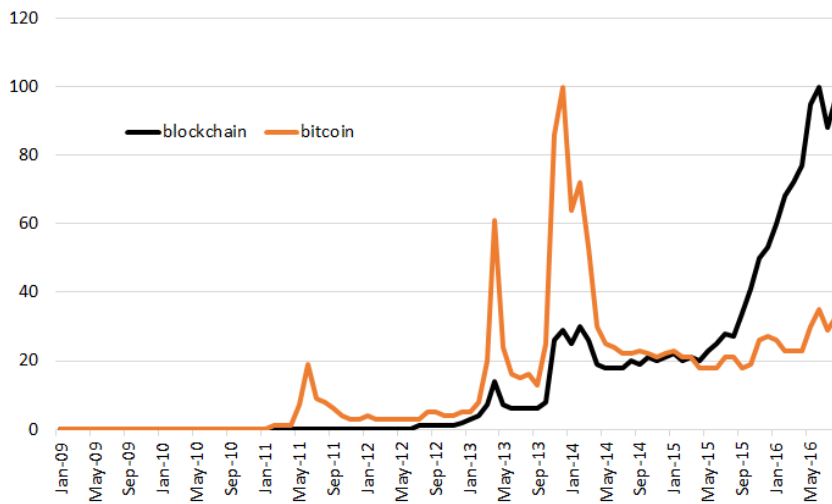
## I. 서론

2009년 1월 비트코인(Bitcoin)이 등장하여 거래되기 시작한 이후, 비트코인은 많은 화제와 주목의 대상이 되어 왔으며 비트코인에 관한 다수의 조사와 연구가 이루어졌다. 비트코인에 관한 초기의 연구 혹은 논의는 최초의 성공적인 디지털통화(digital currency) 혹은 암호화통화(cryptocurrency)로서 비트코인에 대해서 중앙은행의 통화정책상의 함의, 지급결제 시스템에 미치는 영향, 나아가 법화(fiat currency)의 대체 가능성 등 주로 화폐경제학적 측면에서 이루어진 것이 다수를 차지하였으며, 인터넷 상에서 비트코인의 유통이 가능하도록 만든 기반 기술에 대해서는 상대적으로 많은 관심이 기울여지지 않았다. 그러나 시간이 경과하면서 블록체인(blockchain)이라고 불리는, 비트코인의 기반 기술이 갖는 독창적인 특성들, 그리고 블록체인이 갖는 다양한 측면에서의 활용 가능성에 대한 인식이 확산되면서 블록체인에 대한 관심이 크게 증가하였다. 이러한 관심은 2014년 이후에 폭발적으로 증가하였고, 특히 2015~2016년 초의 기간에 걸쳐서 다양한 기업(주로 금융회사)들에서의 도입 시도 사례들이 발표되었으며, 자본시장을 비롯한 여러 영역에서의 활용 가능성과 관련 이슈에 대한 많은 논의가 진행되었다. 또한 블록체인 기술을 자신의 비즈니스로 삼는 다수의 스타트업들이 생겨났다. 현재는 비트코인 관련 스타트업보다 블록체인 관련 스타트업이 더 많아졌고, 벤처캐피탈 역시 비트코인 관련 스타트업보다 블록체인 관련 스타트업에 더 많은 자본을 투자하고 있다(Economist, 2016a). 다음 쪽의 <그림 I-1>은 구글에서의 검색 빈도를 통해 나타난 비트코인과 블록체인에 대한 상대적인 관심의 추세 변화를 잘 보여준다.

#### 4 자본시장에서의 블록체인 기술의 활용 전망 및 시사점

블록체인은 ‘디지털화된 공개 분산원장(public distributed ledger)에 의하여 거래 기록의 무결성(integrity)과 신뢰성(trust)을 확보하는 컴퓨터 네트워크 기반 기술’이라고 정의할 수 있으며, 문헌에 따라서는 분산원장(distributed ledger) 자체를 의미하는 것으로 쓰이기도 한다.

<그림 1-1> 블록체인과 비트코인 관심도 추이 (Google Trends)



주 : 구글 검색 빈도를 이용한 상대적 관심도(100=최고 관심도, 0=최저 관심도)를 나타냄

자료: <https://www.google.com/trends>

블록체인 기술의 핵심적인 특징은 첫째로, 어떤 ‘제3자 기관’이나 중개기관이 없이, 시장의 모든 거래 참여자가 P2P(peer-to-peer)로 직접 연결된다는 점, 둘째로 거래 내역을 기록한 원장(ledger)이 모든 시장 참여자들에 의하여 분산 보관되며, 원장의 업데이트 및 기록의 정확성에 대한 검증과 승인이 사전에 프로그래밍 된 규칙에 따라

시장 참여자들의 합의 메커니즘에 의하여 이루어진다는 점, 셋째로 이 모든 과정은 고도의 암호화(cryptographic) 기법에 의하여 보안이 유지된다는 점으로 요약할 수 있다. 이러한 특징들은 블록체인 기술이 지금까지 오랜 세월을 걸쳐 인류가 사용해 온 기존의 거래 및 원장의 관리 방식, 즉 중개기관을 경유하는 거래, 그리고 신뢰할 수 있는 ‘제3자 기관’에 의한 원장의 관리라는 방식과는 전혀 다른 새로운 거래 및 원장 관리 방식이라는 것을 의미한다.

블록체인 기술에 대한 초기의 논의들의 상당수는 블록체인 기술이 갖는 이러한 혁신적인 특성에 주목하면서, 이 블록체인 기술이 기존의 시스템을 어느 부문에서 어느 정도까지 대체하면서 활용될 수 있을 것인지에 대한 가능성에 초점을 맞추었다. 예를 들면 비트코인과 같은 암호화통화를 통한 지급결제, 자금이체 등에서 시작하여, 보다 광범위한 금융거래에서 사용될 가능성이 거론되었다. 자본시장의 경우 가장 극단적으로는 전자적으로 발행된 암호화증권(cryptosecurities)을 역시 암호화통화를 이용하여 모든 거래자들이 P2P로 거래하고, 그 모든 거래 내역과 거래로 인한 증권 소유권의 이전 기록을 분산원장에 의하여 유지·관리하는 암호화증권시장(cryptosecurities market)의 가능성까지도 거론되었다(Lee, 2016). 그리고 시장 거래 다음 단계에서는 사회의 각 부문, 기업 및 정부의 비금융적 기능 - 건강보험, 공적연금, 신분증 관리, 자동차 등록 등 - 에서의 활용 가능성이 언급되었다(Swan, 2015; UK Government, 2015). 여기에서 한발 더 나아가 물리적 실체 없이 블록체인 위에서 오직 프로그래밍 된 규칙에 의하여 가상적으로 존재하고 작동하는 조직이 등장하고<sup>1)</sup>, 심지어는 국가의 정치과정까지도 블록체인 기반으로 옮겨올 수 있다는 데까지 논의가 나아가기도 하였다.

1) Ethereum이 시도한 Decentralized Autonomous Organization(이하 DAO)이 이러한 블록체인상의 가상조직의 예이다. 이에 관해서는 II장에서 다시 언급한다.

그러나 이와 같은 논의의 상당 부분은 어떤 새로운 혁신적인 기술이 등장하는 초기에 흔히 관찰되는 흥분과 과장(hype)이 어느 정도 반영된 측면이 있는 것도 사실이다. 2016년 1/4분기 정도부터는 이러한 초기의 흥분과 과장이 어느 정도 가라앉기 시작하면서, 보다 치밀하고 단계적으로 현재 시점에서의 블록체인 기술의 현주소를 진단하고, 어느 영역, 어느 서비스 혹은 기능에 이 기술을 도입하는 것이 가장 큰 효과와 편익을 얻을 수 있으며, 그러기 위해서는 무엇이 필요하고 무엇을 해야 하는지를 논의하는 분위기로 바뀌고 있다.

블록체인은 이제 시작 단계의 기술이다. 은행을 중심으로 한 일부 금융회사에서 외화송금과 같은 일부 서비스에 블록체인 기술을 도입하는 것을 개발·시험 중이다. 그리고 전 세계 유수의 금융회사들로 구성된 R3CEV와 같은 블록체인 컨소시엄 역시 현재 블록체인 네트워크의 설계, 지배구조(governance), 기술표준 등에 관한 논의를 진행하면서, 구현하려는 서비스에 대한 개념증명(proof of concept)을 시도하는 단계로 본격적인 서비스가 가동되고 있지는 않다. 자본시장의 경우에는 시장에서의 매매거래 체결과 같은 거래(trade) 혹은 전선업무(front office) 단계에서보다는 거래 체결 후에 이어지는 일련의 ‘거래후 처리과정(post-trade processing)’ 혹은 후선업무(back office)에서 블록체인 기술이 먼저 도입될 가능성이 높다는 것, 그리고 이 블록체인 기반으로 거래후 과정을 처리하는 것이 최초 등장하는 것은 대략 2~3년 후가 될 것이라는 데에 해외 다수의 전문가 및 기관들의 의견이 일치하고 있다.<sup>2)</sup>

즉, 블록체인은 현재진행형인 기술이며, 현재진행형인 이슈이다. 따라서

2) 자본시장에서의 블록체인 기술의 도입을 다룬 다수의 외국 문헌들은 ‘post-trade processing’이라는 용어를 사용하고 있으나, 본 보고서에서는 이것을 번역하는 대신 ‘후선업무’라는 용어로 대체하여 사용한다. 한국예탁결제원(2014)은 “청산, 결제, 예탁을 매매 이후의 업무, 즉 후선업무라 한다.”라고 서술하고 있다.

블록체인 기술의 자본시장에의 도입과 관련된 논의를 담은 자료들도 매우 다양하게 등장하고 있다. 외국에서는 정부의 정책 및 규제기관, 금융회사 및 시장운영기관, 컨설팅회사 등으로부터 블록체인이 자본시장 및 관련 산업에 미치는 영향, 도입과 관련된 제반 이슈, 업계 및 당국의 대응 방향 등을 다룬 자료들이 산발적으로 나오고 있다. 국내에서도 금융 및 자본시장 관련 기관들이 블록체인에 관한 검토·조사 자료들을 내놓고 있다. 그러나 아직까지 블록체인의 자본시장 도입과 관련된 제반 이슈들을 포괄적으로 정리한 자료는 그리 많지 않다.

본 보고서는 이러한 배경에서 자본시장을 중심으로 한 금융에서의 블록체인 기술의 도입·활용 현황 및 관련 이슈들을 정리한다는 목적으로 작성되었다. 또한 블록체인의 개념, 작동 원리, 종류를 설명하고, 블록체인이 갖는 기술적, 경제적 특성을 정리해보고자 하였다. 따라서 본 보고서는 블록체인에 관한 것이며, 비트코인에 관한 것은 아니다. 제Ⅱ장에서 블록체인의 작동 원리를 불가피하게 비트코인을 예로 들어 설명하기는 하지만, 본 보고서는 비트코인을 소개하고 관련 이슈를 설명하려는 것이 아니라, 그 기반에 깔려 있는 기술인 블록체인을 소개하고 관련 이슈를 정리하려는 것이다. 따라서 비트코인과 관련된 제반 이슈들, 예를 들면 화폐경제학적 논의들이나 불법적 자금 이동과 같은 것들은 본 보고서에서 다루지 않는다.

본 보고서는 다음과 같이 구성되어 있다. 제Ⅱ장에서는 블록체인의 작동 원리와 특징을 비트코인을 예로 들어 설명한다. 그리고 블록체인의 종류 및 비트코인 이후 등장한 대표적인 블록체인 플랫폼을 소개한다. 제Ⅲ장에서는 자본시장을 비롯한 금융산업에서의 블록체인 기술 도입과 관련하여 진행되고 있는 논의들을 정리하고, 대표적인 도입 시도 사례들을 소개한다. 제Ⅳ장에서는 이상의 논의들을 종합하고, 이를 토대로 자본시장 업계 및 정책·규제당국에 대한 시사점을 제시한다.



## II. 블록체인 소개

---

1. 블록체인의 개념 및 역사
2. 블록체인의 작동 메커니즘
3. 블록체인의 특성
4. 비트코인 외 블록체인 기반 플랫폼의 등장



## II. 블록체인 소개

본장에서는 블록체인의 개념과 특징, 기본적인 작동 원리를 설명하고, 블록체인에 내포되어 있는 경제적·기술적 특성을 서술한 다음, 도입 및 활용 가능성에 대한 논의를 정리한다.

### 1. 블록체인의 개념 및 역사

#### 가. 블록체인의 개념

블록체인(blockchain)이 무엇인가에 대하여 일반적으로 가장 널리 알려진 정의는 ‘디지털화된 공개 분산원장(public distributed ledger)에 의하여 거래 기록의 무결성(integrity)과 신뢰성(trust)을 확보하는 컴퓨터 네트워크 기반 기술’이라는 것이다(금융보안원, 2015a; 김동섭, 2015; 김석원, 2016; 김예구, 2015). 또한 좁은 의미의 블록체인은 분산원장(distributed ledger) 자체를 지칭하기도 하며, 상당수 문헌에서는 ‘블록체인 기술’과 ‘분산원장 기술’을 같은 의미로 사용하고 있다.<sup>3)4)</sup> 블록체인은 ‘블록’과 ‘체인’이 결합된 단어로서, 블록은 일정 시간 동안 발생한 모든 거래가 기록되어 있는 원장이다. 이 블록들을 블록의 생성 순서에 따라 사슬(체인)과 같이 연결해 놓은 것이 곧 블록체인인 것이다.

경제활동에 있어서 금융거래를 포함한 거의 대부분의 거래는 지급결제, 거래기록의 관리 등에 있어서 ‘신뢰할 수 있는 제3자(trusted third party)’의 존재를 필요로 한다. 예를 들어, 신용카드로 어떤 재화를 구매할 경우, 신용카드 유효성의 검증에서부터 거래의 완결에 이르기까지

3) 예를 들면 DTCC(2016), UK Government Office for Science(2015)

4) ESMA(2016)는 분산원장이 보다 일반적인 표현이며, 블록체인은 분산원장 중에서 비트코인의 기반으로 만들어진 특정 분산원장의 명칭이라는 입장을 취하고 있다.

신용카드회사와 은행이 개입되어 거래의 유효성을 검증하고, 지급결제가 이루어지게 하며, 이 모든 거래를 원장(ledger)에 기록하고 관리한다. 부동산의 경우, 거래의 결과를 정리하여 현재 누가 어떤 부동산을 소유하고 있는지를 기록하고 인증하는 ‘부동산 등기부’는 정부기관이 작성하고 관리한다.

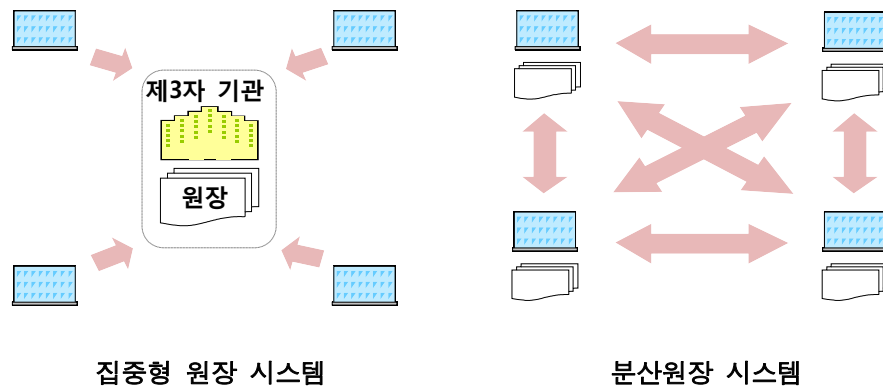
그런데 거래에 있어서 소위 ‘이중 지출의 문제(double spending problem)’ - 소유하고 있지 않은 돈으로 구매 대금을 지불하거나 소유하고 있지 않은 재화를 파는 행위의 가능성 - 가 발생하지 않도록 하려면 이 원장이 정확하게 작성되어야 하고, 변조되지 않도록 안전하게 보관되어야 한다. 즉, 임의의 시점에서 ‘누가 무엇을 소유하고 있는가(who owns what)’에 대한 정확한 기록이 유지되어야 한다. 그리고 대부분의 경우 이러한 원장의 기록과 보존은 은행이나 정부기관과 같은 신뢰할 수 있는 제3자가 담당한다.

이러한 시스템에서는 은행이나 정부기관과 같은 ‘제3자’가 작성·보관하고 있는 원장의 정확성을 신뢰할 수 있는지의 여부, 그리고 이와 관련하여 이 제3자 자신이 신뢰할 만한 존재인지의 여부가 결정적인 중요성을 갖게 된다. 거래 참여자들이 제3자, 그리고 제3자에 의하여 작성·보관되는 원장을 믿지 못하게 되면 그 거래 시스템은 붕괴될 것이다.

이와는 달리, 블록체인은 거래 네트워크의 모든 참여자에게 공개된(public) 원장을 모든 참여자가 자신의 컴퓨터에 각자 저장할 수 있도록(distributed) 하고, 네트워크 참여자들의 합의(consensus)에 의하여 원장의 기록이 관리·보존될 수 있도록 하는 시스템이라는 점에서 기존의 ‘제3자 집중형 시스템’과는 근본적인 차이가 있다. 블록체인에서 네트워크 참여자는 누구든지 블록체인(즉 원장)을 조회하여, 누가 그 블록체인 네트워크에서 유통되는 자산, 혹은 디지털통화(예: 비트코인, 토큰(token)이라고 부르기도 한다.)를 얼마나 보유하고 있는지를 파악할 수 있다. 동시에 블록체인은 고도의 암호화(cryptographic) 기술에 의하여 기록의 변조가 사실상 불가능하도록 보호된다.

따라서 블록체인 시스템에서는 은행과 같은 제3자의 존재가 불필요하다. 네트워크 참여자 사이에서 발생한 거래의 유효성에 대한 검증, 거래 내역의 원장 기록, 원장 기록의 정확성에 대한 승인이 다른 네트워크 참여자들에 의하여 이루어진다. 그리고 새롭게 발생한 거래가 기록되어 업데이트된 원장 역시 모든 네트워크 참여자들에 의하여 공유된다. 즉, 블록체인을 기반으로 하는 거래 네트워크는 <그림 II-1>과 같이 제3자를 중심으로 집중된 host-client 형태가 아닌, 모든 네트워크 참여자가 P2P(peer-to-peer)로 연결된 그물 형태를 갖게 된다.<sup>5)</sup>

<그림 II-1> '제3자'를 통한 집중형 원장 시스템과 블록체인의 분산원장 시스템 비교



나. 블록체인의 역사 및 종류

블록체인은 비트코인(Bitcoin) 시스템의 운영 기반으로 처음 만들어진 것으로 알려져 있다. 비트코인은 2008년 Satoshi Nakamoto<sup>6)</sup>에 의하여 만들어

5) 과거 'Napster'와 같은 파일공유 시스템과 네트워크 구성이 유사하다.

6) Satoshi Nakamoto의 정체는 아직까지 정확하게 알려져 있지 않다. 2016년 5월 2일

졌으며, 2009년 1월 3일 최초의 비트코인 거래 기록을 담은 블록(genesis block), 즉 디지털 원장이 만들어지면서 작동되기 시작하였다(Nakamoto, 2008). 초기에는 대부분의 관심이 디지털통화(digital currency) 혹은 암호화통화(cryptocurrency)로서 비트코인에 집중되었으나, 2013~2014년경부터 비트코인 보다는 그 운영 기반인 블록체인의 잠재력이 주목을 받기 시작하였다.

금융산업에서 먼저 블록체인의 가능성에 주목하기 시작했고, 이후 금융 뿐 아니라 실물경제와 행정 등에서 다양한 활용 가능성이 논의되고 있다. 일각에서는 블록체인을 가리켜 인터넷 이후 가장 혁신적이며, 파괴적인(disruptive) 기술이라고까지 평가하기도 한다. 그러나 아직까지 블록체인의 실제 응용 및 도입은 매우 초기 단계이며, 블록체인을 활용한 서비스가 본격적으로 제공되고 있지는 않은 바, 블록체인이 실제로 금융 및 인간 사회에 얼마나 큰 영향을 미칠 것인지에 대한 판단은 시기상조이다.

블록체인 중에서도 비트코인 시스템에서 사용되고 있는 것은 사전 허락이나 동의 없이 누구나 네트워크에 참여할 수 있는 개방형(public 혹은 permissionless) 블록체인이다. 비트코인을 이용한 거래에 참여하고 싶은 자는 누구나 비트코인 관련 웹사이트(bitcoin.org)에서 필요한 애플리케이션을 받아 설치함으로써 참여할 수 있고, 블록체인을 조회할 수 있으며, 채굴(2절에서 설명)에 참여할 수도 있다. 그런데 최근 금융을 비롯하여 블록체인의 도입·활용을 검토 또는 시도하고 있는 산업계에서는 대부분 개방형 블록체인이 아닌 폐쇄형(permissioned) 블록체인 혹은 완전한 사적(private) 블록체인의 채택을 검토하고 있다. 폐쇄형 블록체인은 정해진 구성원들만으로 네트워크의 노드가 구성된 블록체인을 의미하며, 컨소시엄(consortium) 블록체인이라고도 한다. 그리고 폐쇄형 블록체인에 추가적인 구성원으로 참여하기 위해서는 기존 구성원들의 동의와 허락이 필요하다. 사적 블록체인은 완전한 개인형 블록체인으로 단일의 주체가 내부 전산망을 블록체인 네트워크를 구성하여 관리·운영하는 것으로 이 경우

---

영국 BBC를 비롯한 일부 언론에서 Craig Wright라는 호주인이 자신이 Satoshi Nakamoto임을 밝혔다는 보도를 한 바 있으나 입증된 것은 없다(Economist, 2016b 참조).

블록체인 네트워크에서의 노드는 정해진 검증 및 승인 알고리즘에 따라 작동하는 컴퓨터들로 구성되는 것이 일반적이다.<sup>7)</sup>

개방형 블록체인 시스템의 중요한 특징이기도 하며 동시에 갖추어야 할 핵심적 요구사항은 네트워크 참여자 간의 신뢰를 필요로 하지 않는다는 점이다. Satoshi Nakamoto는 비트코인 시스템을 설계하면서 네트워크 참여자 간에 ‘분산된 합의(distributed consensus)’의 도출 메커니즘을 설계하여 집어넣음으로써 소위 ‘비잔틴 장군 문제(Byzantine Generals Problem)’를 해결하였다고 주장하고 있다(Nakamoto, 2008).<sup>8)</sup> 이에 관해서는 2절에서 상세하게 설명한다. 반면 폐쇄형 블록체인 시스템에서는 사전에 서로 알고, 따라서 이미 신뢰관계가 존재하는 구성원들로 네트워크가 구성되기 때문에 분산된 합의 도출 메커니즘의 중요성이 개방형 블록체인에 비해서 크지 않고, 이것은 블록체인 메커니즘의 설계에도 영향을 미치게 된다.

## 2. 블록체인의 작동 메커니즘<sup>9)</sup>

본절에서는 블록체인의 작동 메커니즘을 비트코인 시스템을 예로 들어 설명한다. 현재 블록체인을 기반으로 하는 서비스, 혹은 애플리케이션 중에서

7) 블록체인의 구분에 대해서는 문헌들 간에 차이가 존재한다. 일반적으로 ‘public’과 ‘permissionless’는 동일한 의미로 사용되지만, ‘permissioned’ 블록체인은 문헌에 따라 컨소시엄 블록체인과 동일한 의미로 사용되기도 하고, 컨소시엄과 사적 블록체인을 모두 포괄하는 의미로 사용되기도 한다. 본 보고서는 컨소시엄 블록체인과 사적 블록체인을 구분하여 블록체인을 3가지 종류로 나누는 구분법을 따르며, ‘폐쇄형(permissioned)’ 블록체인이란 컨소시엄 블록체인을 의미하는 것으로 한다.

8) ‘비잔틴 장군 문제’란 상호간에 알지도 못하고 신뢰도 없고, 따라서 악의적으로 행동할 가능성이 있는 네트워크 참여자들 사이에서 어떻게 합의를 이끌어내어 네트워크가 추구하는 목적을 달성하도록 할 것인가에 관한 컴퓨터 네트워크 설계상의 문제로 Lamport et al.(1982)에 의하여 처음으로 정리되었다.

9) 본절의 내용은 주로 Antonopoulos(2014)와 Harvey(2016)를 참고하여 작성되었다.

실질적으로 완전한 형태로 구동되면서 실제 사용되고 있는 것으로는 비트코인이 가장 대표적이다. 또한 블록체인은 비트코인 시스템의 운영 기반으로 최초로 등장한 것인 만큼, 비트코인에서 사용되고 있는 블록체인은 이후 등장하고 있는 모든 블록체인의 원형(prototype)이 되고 있을 뿐 아니라, 세부적 작동 메커니즘이 공개되어 있기 때문에 블록체인의 작동 메커니즘은 비트코인 시스템을 예로 사용하여 설명하는 것이 편리하고 어느 정도 불가피한 측면도 있다.

## 가. 비트코인 거래 발생 단계

본절의 목적은 블록체인의 작동 메커니즘을 설명하는 것이기 때문에, 거래에 사용되는 비트코인의 획득 과정에 대한 설명은 생략하고, 이미 비트코인을 보유하고 있는 ‘갑’이라는 주체가 ‘을’로부터 어떤 재화를 구입하고 그 대금을 비트코인으로 지불하는 거래를 가정하여 거래의 최초 시작 시점부터 설명한다.

### 1) 거래의 발생

‘갑’이 ‘을’로부터 어떤 재화를 구입하고 그 대금을 비트코인으로 지불하려고 하는 경우, 우선 ‘을’은 자신의 디지털 비트코인 지갑(wallet)의 주소(address)를 ‘갑’에게 알려주게 된다. 주소는 비트코인 지갑의 공개키(public key)로부터 자동적으로 생성되며 이메일 주소와 유사하나, 매 거래마다 각각 다른 주소를 생성, 사용한다는 점에서 차이가 있다.<sup>10)</sup> 공개키는

10) 비트코인에서는 지갑의 개인키(private key)로부터 일방(one-way) 암호화함수인 타원곡선곱셈(elliptic curve multiplication)함수를 이용하여 공개키를 생성하고, 다시 공개키로부터 역시 일방 암호화함수인 해시함수(hash function)를 이용하여 매 거래마다 주소를 생성한다. 이러한 암호화 기법들은 모두 일방(one-way)이기 때문에 공개키, 혹은 주소로부터 개인키를 알아내는 것은 거의 불가능한 것으로 알려져 있다(Antonopoulos, 2014).

해당 지갑의 식별자(id)로서의 역할을 하며 은행거래에서의 계좌번호와 유사하다. 그리고 이 공개키는 비트코인 거래에서 비트코인 수취자(‘을’)가 거래를 위하여 ‘갑’에게 제공하는 유일한 정보이다.

이어서 ‘갑’은 ‘을’의 주소(즉 지갑)로 필요한 금액의 비트코인을 전송하고, 개인키(private key)를 이용하여 서명(signature)한다. 개인키는 지갑 하나 당 하나가 생성되어 보관된다. ‘개인키를 이용하여 서명’한다는 것은 서명된 거래(즉 ‘갑’의 지갑에 있는 비트코인의 소비)가 비트코인 네트워크의 전체 참여자(‘노드(node)’라고 부른다.)에게 전송되고, 그 중 누군가 이 거래의 유효성(즉 ‘갑’이 정말로 가격 지불에 충분한 비트코인을 지갑 속에 보유하고 있음)을 확인하고 검증할 수 있도록 허용한다는 의미이다. 개인키는 인터넷뱅킹에서 사용하는 ‘인증서 비밀번호’ 혹은 ‘이체비밀번호’와 유사하다고 볼 수 있다. 개인키는 유출되지 않도록 주의해야 하며, 개인키 보관의 보안성은 블록체인의 보안성과는 별개의 문제로 각 개인의 책임이다.

이 과정에서 ‘갑’의 지갑에서는 ‘을’에게 지불된 재화 대금 외에 소액의 거래수수료(transaction fee)가 차감된다. 거래수수료는 이 거래를 블록(원장)에 기록함으로써 최종적으로 거래를 승인하고, 그 전까지의 블록의 집합(블록체인)에 연결하는 수고를 제공하는 채굴자(miner, 후술)에 대한 보상의 재원으로 사용된다.

## 2) 거래 유효성(Validity) 검증

‘갑’이 자신의 개인키를 이용하여 서명한 거래는 수초 이내에 비트코인 네트워크 대부분의 노드들에게 전송, 도달된다. 전송되는 거래 정보에는 개인키를 포함한 개인정보나 인증서 등이 포함되어 있지 않기 때문에 보안의 필요성이 크지 않다. 따라서 네트워크 자체의 보안성이 크게 요구되지 않기 때문에 공개된 인터넷을 이용할 수 있으며, 와이파이(wi-fi)에 의한 전송도 크게 문제되지 않는다고 한다. 또한 전송한 바와 같이 각 노드들이 서로 알아야 할 필요가 없으며, 상호간에 신뢰도 필요하지 않다.

각 노드들은 그 시점까지의 원장(블록체인)을 조회하여 해당 거래의 유효성, 즉 ‘갑’이 정말로 거래대금 지불을 위하여 충분한 비트코인을 자신의 지갑에 보유하고 있는지의 여부를 검증한다. 원장 조회 결과 거래의 유효성이 검증되면, 이 거래는 해당 노드와 연결된 다른 노드로 다시 전송되고, ‘갑’에게는 성공 메시지가 전송된다. 원장 조회 결과 거래의 유효성이 부인되면 해당 노드는 이 거래에 대한 유효성 검증을 거부하고, ‘갑’에게는 거부 메시지가 전송되며, 이와 같이 유효성이 부인된 거래는 더 이상 다른 노드들로 전송되지 않는다.

‘을’은 자신의 지갑을 조회하여 ‘갑’이 지불한 비트코인이 입금되었다는 것을 확인할 수 있다. 그러나 ‘을’이 이 비트코인을 다른 거래에서 다시 사용하기 위해서는 본 거래에 대한 최종적인 승인(confirmation)이 이루어져야 한다.

## 나. 거래의 승인 및 확정 단계: 블록의 생성

발생한 거래를 블록에 기록하고 블록체인에 연결하여 고칠 수 없는 영구적인 기록으로 남기는 과정이 거래의 승인 및 확정 단계에서 이루어지며, 이 단계의 핵심은 ‘채굴(mining)’이라고 일컬어지는 블록의 생성이다. 이 단계가 블록체인 메커니즘의 가장 핵심적인 부분이다.

### 1) 거래의 수집

유효성이 검증된 거래들은 전 세계로 전송되면서, 동시에 ‘채굴자(miner)’라고 불리는 노드의 메모리풀(memory pool)에 수집·저장된다. 메모리풀에 저장되어 있는 거래들은 아직까지는 미승인 상태이다. 즉, 전술한 거래의 예에서 ‘을’은 ‘갑’으로부터 받아 자신의 지갑에 입금된 비트코인을 아직 다른 거래에서 사용할 수 없다.

## 2) 블록의 구성 및 보안

채굴자는 자신의 메모리풀에 저장되어 있는 거래들을 모아 하나의 블록을 만드는데, 이 블록은 일종의 ‘후보 블록(candidate block)’이라고 볼 수 있다. 블록은 그 블록에 기록되는 거래 내역과 블록헤더(block header)로 구성되며, 현재 비트코인 시스템에서 한 개의 블록에는 400~3,000개 정도의 거래가 포함·기록되고 있다.<sup>11)</sup>

채굴자는 ‘SHA256’<sup>12)</sup>이라는 암호화 함수를 이용하여 블록헤더에 대한 해시(hash)값을 구한다. 따라서 각각의 블록에 대하여 고유한 해시값이 부여되며, 해시값은 블록의 ‘높이(height)’와 함께 해당 블록의 식별자(id) 기능을 수행한다.<sup>13)</sup> 각 블록의 블록헤더에는 바로 이전 블록의 해시값이 포함되어, 그 전까지의 모든 블록들과의 연결고리를 형성하게 된다. 따라서 만일 어떤 이유로 이전 어떤 블록의 거래기록이 변경되면 그 블록의 해시값이 달라지고, 그에 따라 그 이후 모든 블록의 해시값이 모두 달라지게 된다. SHA256 암호화 함수는 미국 국가안보국(NSA)에 의하여 개발된 것으로 알려져 있으며(Harvey, 2016), 입력값의 크기에 관계없이 64자리의 숫자와 문자의 조합으로 구성된 해시값을 출력하는 일방향(one-way) 함수이다. 즉, 입력값을 이용하여 해시값을 산출하는 것은 매우 용이하나, 반대로 해시값을 이용하여 원래의 입력값을 알아내는 것은 사실상 불가능하다. 또한 SHA256 암호화 함수는 입력값이 미세하게 달라져도 전혀 다른 해시값을 출력하게 되어 있다.

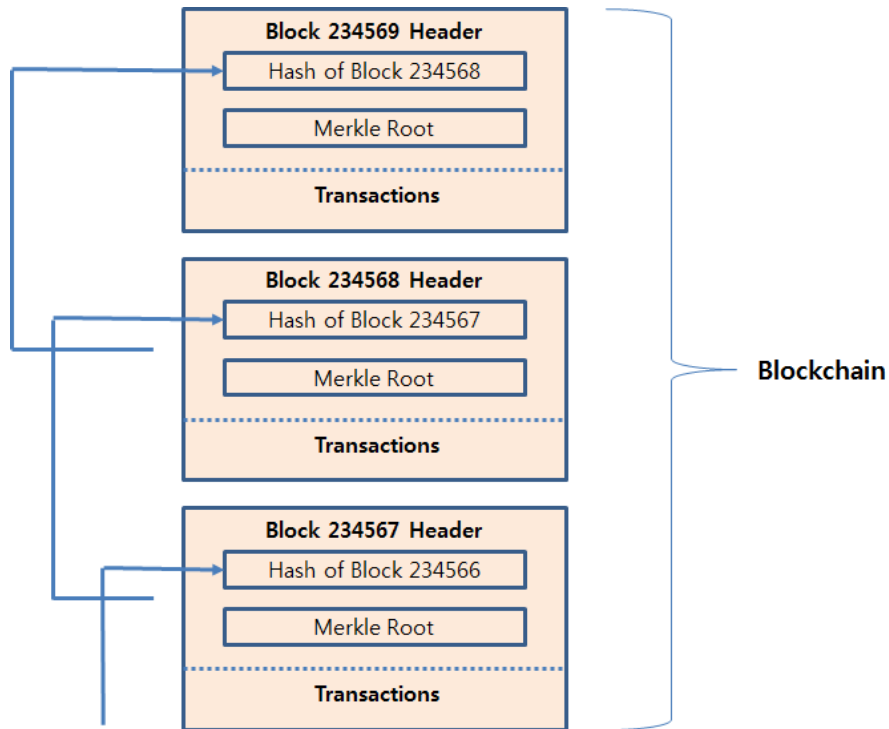
이와 같은 블록의 구성 내용 및 블록체인의 연결 구조를 그림으로 나타내면 <그림 II-2>와 같다.

11) <https://blockchain.info>

12) SHA는 Secure Hash Algorithm의 약자이다.

13) 블록의 높이는 블록의 생성순서에 따른 일련번호이다.

<그림 11-2> 블록의 구성 및 연결 구조



### 3) 블록의 검증 및 확정: 채굴과 작업증명

한 채굴자가 만든 후보 블록이 정식 블록으로 인정받아 블록체인에 연결되기 위해서는 이 후보 블록이 정확한 거래기록을 담고 있으며, 채굴자가 정직한 노력을 기울여 이 후보 블록을 만들었음을 네트워크의 다른 노드들이 검증하고 승인해야 한다. 채굴자는 이 승인을 얻기 위하여 자신이 정직한 노력을 기울였음을 입증해야 하는데, 이를 위하여 필요한 것이 작업증명(Proof of Work)이다.

현재 비트코인 시스템에서 작업증명은 SHA256 암호화 함수를 이용하여 '특정한 요구조건을 만족시키는 해시값을 산출하는 어떤 정수값'을 찾는 것으로

이루어져 있다. 구체적으로, 해당 블록의 헤더 마지막에 임의의 정수를 덧붙인 입력값의 해시값이 정해진 개수의 0으로 시작하도록 산출되도록 하는 임의의 정수값을 찾는 것이다. 예를 들어, 블록헤더가 ‘자본시장연구원’이라면 ‘자본시장연구원n’과 같이 맨 뒤에 정수를 붙여 입력했을 때 SHA256함수가 산출하는 해시값이 정해진 개수의 0으로 시작하도록 하는 n 값을 찾는 것이다. n 값을 찾는 것은 방정식을 푸는 것과 같은 연산적(algorithmic) 방법으로는 불가능하며, 오직 시행착오에 의한 반복에 의해서만 가능하다. 즉 비트코인 시스템에 의하여 0의 개수가 13개로 정해져 있다면, 13개의 0으로 시작하는 해시값이 산출될 때까지 ‘자본시장연구원 0’, ‘자본시장연구원1’, ... 과 같이 입력과 출력을 반복하는 것이다.

현재 비트코인 시스템에서는 평균적으로 10분에 한건의 작업증명이 성공할 수 있도록, 즉 해당 정수값을 찾는 데 소요되는 시간이 평균적으로 10분이 되도록 작업증명의 난이도가 설정되어 있다. 또한 작업증명의 답이 되는 해당 정수값을 ‘논스(nonce)’라고 하며, 논스 역시 블록헤더에 포함된다.

채굴자가 작업증명을 해결하면 이 블록은 즉시 전 세계 비트코인 네트워크의 노드들로 전송된다. 그리고 각 노드들은 전송받은 블록의 작업증명이 참인지를 검증한다. 작업증명의 해결과는 달리 작업증명의 검증은 대단히 간단하다. 즉, 블록에 포함된 논스값을 이용하여 정말로 요구되는 해시값이 산출되는지를 검증하면 된다. 작업증명을 검증한 노드는 해당 블록을 승인(confirm)하며, 승인된 블록은 바로 직전까지의 블록체인에 연결되어 블록체인을 업데이트한다. 그리고 업데이트된 블록체인은 다시 전 세계의 노드들로 전송되어 분산 저장된다.

블록이 승인되어 블록체인에 연결되면 그 블록에 포함된 거래들 역시 승인상태가 되어, 앞의 예에서 ‘을’은 ‘갑’으로부터 입금된 비트코인을 다른 거래에서 사용할 수 있게 된다. 블록이 승인되었다는 것은 그 블록에 포함된 거래가 모두 유효하며, 정확하게 기록되었고, 앞으로 변경되지 않을 것이라는 것에 전 네트워크가 동의한 것이라고 볼 수 있다.

채굴자는 블록을 만들고 그에 대한 작업증명을 네트워크에 제공하여 승인을 받음으로써 블록에 대한 승인과정을 완료하고 블록체인을 업데이트하는 노력을 제공한 데 대하여 보상(대가)을 수취한다. 채굴자의 노력은 구체적으로 거래들을 모아 블록을 만들고, 자신의 컴퓨터 연산능력(computing power)을 이용하여 논스값을 찾아 작업증명을 해결함으로써 블록에 대한 승인을 받아 블록체인을 업데이트하는 것이다. 그리고 이것은 비트코인 네트워크가 항상 정확하고 신뢰성 있는 원장(즉 블록체인)을 업데이트하고 유지하도록 하는 것이라는 점에서 채굴자의 노력 제공은 비트코인 네트워크가 지속적으로 작동할 수 있도록 동력을 제공하는, 블록체인에서의 핵심 요소이다.

채굴자에 대한 보상은 비트코인으로 주어지며, 여기에는 신규로 발행되는 비트코인과 매 거래마다 소액의 수수료로 징수된 비트코인이 사용된다. 비트코인 시스템은 2009년 1월 3일 최초의 블록(genesis block)이 생성되면서 작동되기 시작했으며, 1 블록당 50 비트코인을 신규로 발행하여 해당 채굴자에게 지급하였다. 채굴자에게 보상으로 지급되는 비트코인 금액은 21만 블록(약 4년)마다 1/2로 줄어들도록 설계되어 있다. 따라서 채굴자에 대한 보상은 2012년 11월에 현재의 1 블록당 25 비트코인으로 감소하였으며, 2016년 7월에 다시 12.5 비트코인으로 감소하였다.

신규 비트코인의 발행은 오직 채굴자에 의하여 새로운 블록이 만들어질 경우에만 이루어지며, 블록당 보상액이 감소함에 따라 신규 발행량 역시 감소하게 되어 있다. 즉 현재는 매 10분마다 12.5 비트코인이 새롭게 발행(채굴)되고 있는 것이다. 또한 비트코인 시스템에서 비트코인의 발행 총량은 2,100만 비트코인으로 사전에 프로그램되어 있으며, 따라서 2,100만 비트코인의 채굴이 모두 끝나는 2140년부터는 비트코인은 더 이상 신규발행되지 않는다. 그리고 채굴자에 대한 보상은 매 거래에서 수수료로 징수된 비트코인으로 지급하게 될 것이다.

이러한 일련의 과정을 ‘채굴(mining)’이라고 부르는 이유는 전체 매장량이 정해져 있는 광물을 채굴해 내듯이, 비트코인 역시 새로운 블록을 만들어냄으로써 새롭게 “캐내어져서” 발행되는 데에서 유래한 것으로 보인다.

#### 4) 채굴 경쟁

전술한 바와 같이 채굴, 즉 블록을 생성하여 승인을 받아 블록체인에 연결하는 작업에 대해서는 현재 12.5 비트코인이 보상으로 주어지고 있다. 현재 1 비트코인은 약 400~600달러 선에서 거래되고 있으며<sup>14)</sup>, 따라서 12.5 비트코인은 약 5,000~7,500달러에 해당한다. 따라서 전 세계의 비트코인 네트워크에서는 채굴자(채굴 노드) 간에 채굴 경쟁이 치열하게 벌어지고 있으며, ‘채굴 산업’이라고 일컬어질 정도로 채굴자의 규모가 커지고 있다.

채굴에서의 경쟁력은 컴퓨터 연산능력에 달려 있는 바, 2009년 1월 3일 최초의 블록이 만들어진 이후 현재까지 컴퓨터 연산능력은 채굴 전용의 ASIC(application specific integrated circuit)칩의 사용 등을 통하여 비약적으로 증가해 왔다. 2009년도 1년 동안에 전체 비트코인 네트워크상의 ‘hashing power’는 0.5 MH/sec (1초에 50만개의 해시 산출)에서 8 MH/sec로, 2014년말에는 150 PH/sec (1초에  $150 \times 10^{15}$ 개의 해시 산출)로, 다시 2016년 6월말에는 1,500 PH/sec 수준으로 시작 당시보다 3조배 증가하였다.<sup>15)</sup>

채굴 경쟁에 뛰어들기 위해서는 상당한 규모의 하드웨어 투자가 필요할 뿐 아니라, 논스값을 찾기 위한 반복연산(즉 해싱) 과정에서 소비되는 막대한 전력비용을 감당해야 한다. 따라서 개인이 채굴 경쟁에 뛰어들기는 매우 어려우며, 많은 채굴자들이 채굴 풀(mining pool)을 형성하여 각자 보유한 컴퓨터 연산능력을 합쳐서 채굴 경쟁에 나서고 있다.

각 채굴자들의 메모리풀에 수집·저장되어 있는 거래들의 목록은 서로 다를 수 있으며, 각 채굴자들은 자신의 메모리풀을 기반으로 블록을 만드는 채굴 경쟁을 전개한다. 이 중에서 어느 한 채굴자가 작업증명을 해결하면 이것은 전체 노드들에게 전달되고, 이어서 이 작업증명에 대한 검증 및 해당 블록에 대한 승인이 다시 전체 노드들에게 전달된다. 그리고 채굴자들은

14) <http://bravenewcoin.com/>

15) <https://blockchain.info/>

그 즉시 새로운 블록을 만들기 위한 다음 라운드의 경쟁에 돌입하게 된다. 이 때 자신의 메모리풀에서 새 블록에 포함된 거래들은 삭제되고, 그 동안에 새롭게 저장된 거래들을 묶어서 다시 채굴작업을 시작하는 것이다.

#### 다. 블록 생성 이후 단계

치열한 채굴 경쟁의 결과로 2개 이상의 노드가 거의 동시에 작업증명의 해결에 성공하는 경우가 발생한다. 2개의 채굴 노드가 거의 동시에 N 번째 블록의 작업증명을 해결하면 일시적으로 2개의 '정당한' 블록체인이 존재하게 된다. 비트코인 시스템은 이러한 경우에 2개의 블록체인 중에서 N+1 번째 블록이 먼저 연결된, 즉 '더 긴(longer)' 블록체인을 최종적으로 정당한 블록체인으로 인정하는 방식을 채택하고 있다. 각 채굴노드들은 서로 다른 블록체인을 받는 경우 그 중에서 길이가 긴 것을 선택하게 되고, 시간이 경과함에 따라 짧은 블록체인은 사라지게 된다.

### 3. 블록체인의 특성

이상에서 서술한 바와 같은 메커니즘에 의하여 작동되는 블록체인은 그에 따른 기술적, 경제적 특성을 가진다. 본 절에서는 이 특성들을 살펴본다. 비트코인 시스템을 이용하여 작동 메커니즘을 설명하였기 때문에, 본 절에서 서술하는 특성들 역시 비트코인과 같은 개방형 블록체인이 갖는 특성이다.

### 가. 구조상의 특성: 분산·분권·개방형 구조

본 장의 1절에서 서술한 바와 같이 블록체인 네트워크는 ‘신뢰할 수 있는 제3자’의 존재를 필요로 하지 않고, 원장의 기록, 보존 및 관리가 네트워크의 모든 참여자들에게 맡겨져 있는 분산형 구조를 갖는다.

그리고 이 참여자들, 즉 노드들은 네트워크에서 동일한 위상을 가지며, 노드들 간에 어떤 계위(hierarchy)가 존재하지 않는다는 점에서 블록체인 네트워크는 분권형 네트워크이다. 즉 다른 노드를 지배하거나 통제하는 ‘상위’ 노드라는 개념이 없다. 풀노드, 단순지불검증노드 등이 존재하나, 이는 계위에 따른 차이가 아니라, 블록체인 전체를 보관하느냐 헤더만 보관하느냐에 따른 기능의 차이이며, 각 노드가 선택할 수 있다. 채굴노드 역시 상위계층의 노드가 아니며, 자발적으로 채굴이라는 추가적 기능을 수행하고 보상을 얻고자 하는 노드이다. 따라서 네트워크 전체를 통할하는 단일의 의사결정 주체가 존재하지 않으며, 프로그래밍 되어 있는 규칙에 따라 네트워크의 노드 전체적으로 합의가 도출되는 분산화된 합의(distributed consensus) 메커니즘에 의하여 운영된다.

또한 원장이 모든 네트워크 참여자들에게 공개되어 어떤 노드든지 블록체인 조회를 통하여 모든 비트코인 거래의 역사를 비트코인의 발행(즉 채굴) 시점까지 추적할 수 있다는 점에서 블록체인 네트워크는 개방형 네트워크이다. 그러나 블록체인에 기록되는 개인정보는 거래 당사자의 공개 키(public key) 혹은 지갑의 주소(address)가 유일하며, 따라서 블록체인의 조회를 통해서 거래 당사자가 구체적으로 누구인지를 알아낼 수는 없다. 또한 비트코인 시스템의 경우, 소스코드가 모두 공개되어 있는 오픈소스 시스템이다.

## 나. 보안성 및 안전성

흔히 블록체인의 최대 강점으로 일컬어지고 있는 것이 보안성 및 안전성이다. 그리고 이와 같은 강력한 보안성과 안전성은 바로 전술한 분산형·분권형 네트워크 구조, 그리고 블록체인 내의 블록의 연결 구조에 그 바탕을 두고 있다.

우선 ‘신뢰할 수 있는 제3자’가 원장의 관리 및 보관을 책임지고 있는 기존의 시스템에서는 바로 이 ‘제3자’가 해커 등으로부터 공격을 받아 원장의 기록이 변조되거나 원장이 삭제되는 경우 시스템 전체가 마비된다. 반면, 블록체인 네트워크에서는 동일한 원장이 네트워크의 수많은 노드들에 의하여 저장·보관되고 있기 때문에, 이 중 어느 노드가 공격을 받아 원장이 훼손되더라도 네트워크 전체에는 거의 영향을 미치지 않는다. 다른 노드들에 저장되어 있는 원장을 가져오면 되기 때문이다(no single point of attack).

<그림 II-2>에서 묘사한 바와 같이 블록체인의 각 블록의 헤더에는 전 블록헤더의 해시값이 포함되는 방식으로 연결되어 있다. 따라서 블록체인 중 어느 한 블록의 거래기록이 변조되면 그 블록의 헤더가 바뀌고 그에 따라 블록헤더의 해시값이 바뀌고, 이후 모든 블록의 블록헤더 해시값이 바뀌게 된다. 따라서 특정 거래 기록을 변조하기 위해서는 그 거래기록이 담겨 있는 블록 뿐 아니라 그 이후 모든 블록의 블록헤더 해시값을 새로 찾아 변조해야 하며, 동시에 이 모든 작업을 새로운 블록이 생성되어 블록체인이 업데이트되기 전에 완료해야 한다. 이로부터 블록에 담겨 있는 거래기록은 그 블록 뒤에 붙어 있는 블록의 수가 많을수록, 즉 거래기록이 오래되었을수록 변조가 더욱 어려워짐을 알 수 있다.

이론적으로 전체 네트워크 hashing power의 과반수가 ‘선의’의 노드 - 정확한 거래기록을 담은 블록을 만들고, 그에 대한 작업증명을 수행하며, 타 노드의 작업증명에 대하여 정확하게 검증하여 승인을 해주는 -, 즉 부여된 기능을 그대로 수행하는 노드에 의하여 제공되고 있다면 외부로부터의

공격에 의한 원장의 변조는 불가능하다고 알려져 있다(Nakamoto, 2008). 그리고 선의의 노드의 hashing power가 과반에 미치지 못하더라도 나머지 노드들의 ‘악의’가 의도하는 바가 모두 일치할 가능성은 극히 낮다. ‘선의’는 하나이지만, ‘악의’는 다양하다는 것이다. 따라서 어떤 단일의 외부자가 네트워크 전체 hashing power의 과반을 완전히 장악하는 경우에 블록체인의 기록 변조가 가능한데(이를 ‘51% attack’이라고 한다.), 비트코인의 경우 네트워크의 규모 및 투입되고 있는 컴퓨터 연산능력의 크기를 고려할 때 그럴 가능성은 매우 낮다는 것이 일반적인 견해이다.<sup>16)</sup>

이상에서 논의한 블록체인의 보안성이라 함은 원장의 기록과 보존에 있어서의 보안성을 의미하며, 개별 노드의 지갑에 대한 보안성을 의미하는 것이 아니라는 점을 유의할 필요가 있다. 즉, 개별 노드의 지갑이 외부로부터 공격을 받아 개인키가 유출되어 지갑에 보관 중이던 비트코인을 도난당하거나 비트코인 거래소의 컴퓨터가 공격을 받아 비트코인을 도난당하는 경우는 얼마든지 발생 가능하며, 이는 개별 노드의 보안은 노드 자신의 책임이라는 것을 의미한다.<sup>17)</sup> 또한 블록체인 네트워크 프로그램(코드) 상의 실수나 오류로 인하여 보안상 취약점이 존재할 가능성이 전혀 없다고 말할 수는 없다.<sup>18)</sup>

16) 그러나 채굴 풀들이 점차 대형화하면서, 단일의 채굴 풀이 51% 이상의 hashing power를 가질 가능성은 충분히 존재한다. 실제로 2014년 1월 당시 세계 최대의 채굴 풀이었던 GHash.IO는 자신의 hashing power가 전체의 40%를 초과함에 따라, 비트코인 네트워크의 신뢰성 유지를 위하여 자발적으로 더 이상의 신규가입을 막은 사례가 있다(ghash.io/ghashio-press-release.pdf, 2014. 1. 9).

17) 대표적 사례로 2014년에 발생한 비트코인 거래소 Mt Gox에 대한 해킹 및 그로 인한 파산을 들 수 있다.

18) Economist(2016c), CoinDesk(2016f)는 블록체인 네트워크의 하나인 Ethereum을 기반으로 하는 DAO가 공격을 받아 5,500만~6,000만달러 가치에 해당하는 ether(Ethereum의 암호화화폐)를 도난당한 사건을 보도하면서, 코드상의 오류 가능성을 언급하였다. 이 사건으로 인하여 Ethereum은 결국 DAO 프로젝트를 중단하였다(Economist, 2016d).

## 다. 거래 관련 특성

비트코인을 이용하는 거래는 비트코인을 지불수단으로 사용하려는 측이 실제로 자신의 지갑에 사용 가능한 비트코인을 보유하고 있는지의 여부가 확인되는 경우에만 네트워크상에서 유효한 거래로 인정된다. 또한 거래의 대가로 타인으로부터 자신의 지갑에 입금된 비트코인은 그 거래가 기록된 블록이 네트워크상에서 승인되어 블록체인에 연결되어야만 다른 거래에 사용할 수 있다. 비트코인 시스템은 이러한 방식에 의하여 ‘이중지불’이 발생하는 것을 방지하고 있다. 또한 비트코인 거래는 각각의 거래마다 거래 발생 시점에 거래 대상 상품의 인도와 비트코인에 의한 대금의 결제가 이루어지고, 차감(netting) 및 청산(clearing)의 절차가 없으며, 따라서 거래상대방위험(counterparty risk)이나 결제불이행의 위험은 존재하지 않는다.<sup>19)</sup>

또한 비트코인 거래는 비가역적(irreversible)이다. 즉, 일단 블록에 기록되어 블록체인에 연결된 거래는 취소가 불가능하며, 거래를 취소하기 위해서는 거래 당사자간의 합의에 의하여 반대 방향의 거래를 다시 발생시켜야 한다. 이 비가역성이라는 특성은 거래의 안정성과 확실성을 담보한다는 점에서 장점이기도 하지만, 거래에 착오 혹은 실수가 있는 경우 이를 바로잡을 기회가 없다는 점에서 블록체인을 비트코인 이외의 일반적 금융거래에 도입함에 있어서 해결되어야 할 과제이기도 하다.

## 라. 기타 특성

보안성·안전성과 더불어 블록체인이 갖는 강점으로 내세워지고 있는 것이 경제성이다. 즉 원장의 기록과 보존을 담당할 신뢰할 수 있는 ‘제3자

19) 거래상대방위험이 존재하지 않는다는 것은 거래의 형태가 비트코인 시스템에서와 같이 모두 현물(cash)거래로만 이루어질 경우에만 확보되며, 파생상품 거래와 같이 거래시점과 인도 및 결제시점이 상이한 경우에는 확보되지 않는다(ESMA, 2016).

기관'을 따로 설치할 필요가 없기 때문에 이에 따른 제반 비용을 절감할 수 있다는 것이다. 그러나 현재 비트코인 시스템의 경우 전 세계적으로 막대한 컴퓨터 연산용량이 오직 채굴을 위한 반복연산, 즉 해싱에 투입되고 있으며, 이 과정에서 막대한 전력을 소모하고 있다는 점에서 시스템 전체적으로 볼 때 과연 얼마나 경제적인지는 쉽게 판단하기 어렵다. 또한 블록체인, 즉 거래기록을 담은 원장 역시 최초의 블록(비트코인의 경우 2009년 1월 3일에 생성)부터 시작하여 이후 생성된 모든 블록들이 계속 추가되기 때문에 그 파일 크기는 무한정 증가하도록 되어 있다. 2016년 6월말 현재 비트코인 블록체인의 파일 크기는 약 70기가바이트에 달한다.<sup>20)</sup>

블록체인은 네트워크, 즉 참여자 간의 연결에 의하여 시스템이 구성되고 운영되기 때문에 당연히 네트워크 외부성(network externality)을 갖는다. 블록체인 네트워크가 클수록, 즉 네트워크 참여자(노드)가 많을수록 이 네트워크에 참여함으로써 얻는 편익이 커진다. 예를 들면 거래 상대방을 찾기가 쉬워지며, 따라서 해당 시장의 유동성 역시 높아진다. 또한 네트워크 참여자가 많을수록 더 많은 노드가 거래를 검증하고 블록을 승인하기 때문에 검증 및 승인 속도가 빨라질 것이다.<sup>21)</sup> 특히 이러한 네트워크 효과는 블록체인 네트워크의 보안성과 관련하여 매우 중요하다. 참여자가 많을수록 외부로부터의 공격자 혹은 어떤 특정 노드가 51% 이상의 hashing power를 확보하기는 어려워진다. 동시에 상호간에 사전적 신뢰 관계가 없는 참여자가 많을수록 어떤 악의적인 목적에 노드들이 동의하여 hashing power를 합칠 가능성 역시 낮아진다. 즉, 블록체인 네트워크의 보안성은 그 네트워크의 크기(참여 노드 수)와 직접적인 관계에 있다고 할 수 있다.

모든 거래 내역이 블록체인에 기록, 저장되고, 그 내용을 변경할 수 없으며, 또한 모든 네트워크 참여자들에게 원장이 공개된다는 것은 블록체인이 갖는 투명성의 원천이 된다. 정부의 규제당국이 특정 부분에 대한

20) <https://blockchain.info/>

21) 블록체인 네트워크에는 단일의 'host'가 존재하지 않기 때문에, 참여자의 수가 증가하면서 host에 걸리는 부하가 커지고 그에 따라 처리속도가 떨어지는 현상이 나타나지 않는다.

거래 내역을 필요로 할 때, 해당 블록체인에서는 어렵지 않게 그 부분을 조회하여 규제당국에 제출할 수 있다.

#### 마. 폐쇄형 블록체인 관련 특성

이상에서 논의한 블록체인의 특성은 비트코인과 같은 개방형(permissionless) 블록체인이 갖는 특성이다. 그리고 이러한 특성들은 현재 금융을 중심으로 하는 산업계에서 주로 도입될 가능성이 높은 폐쇄형(permissioned) 블록체인에서는 동일하게 나타날 수도 있고, 다른 양상을 보일 수도 있다.

먼저 분산형 구조라는 특성은 블록체인의 정체성 혹은 본질과 관련된 특성으로 개방형, 폐쇄형 모두가 갖는 특성이다. 그러나 모든 네트워크 참여자가 위계가 없이 동등한 위상을 갖는다는 분권형이라는 특성은 폐쇄형 블록체인의 경우에는 네트워크 설계에 따라 그렇게 될 수도 있고, 어느 정도의 위계를 갖는 형태가 될 수도 있다. 즉, 노드별 위계에 따라 블록체인 네트워크의 기능에 참여하는 정도, 분산원장への 접근 정도에 차등을 두는 설계가 가능할 것이다. 그리고 ‘host’는 아니라고 하더라도, 블록체인 네트워크에서 어느 정도 리더의 역할을 하는 노드가 존재할 수도 있을 것이다.

개방형 블록체인에서는 보안성과 관련하여 네트워크 외부성이 매우 중요하다. 즉, 어느 정도 이상의 충분한 수의 노드가 확보되지 않으면 그 블록체인은 외부로부터의 공격에 취약할 수 있다. 51% 이상의 hashing power를 확보하기도 쉽고, 노드의 수가 적은 만큼 노드들 간의 담합 가능성도 높다. 그러나 폐쇄형 블록체인은 블록체인을 구성하는 참여자들의 필요성과 합의에 의하여 네트워크 외부성에 기반한 보안성의 확보를 어느 정도 포기한 것이라고 볼 수 있다. 따라서 폐쇄형 블록체인은 이를 보완할 수 있는 추가적인 보안성 제고 장치가 필요할 것이다. 우선 참여자 간의 신뢰관계를 전제하지 않는 개방형 블록체인과는 달리, 폐쇄형 블록체인은 참여자들 간에 신뢰관계가 이미 검증되었음을 전제로 하기 때문에

노드들 간의 담합 가능성은 사전적으로 제거할 수 있다. 그러나 폐쇄형 블록체인에서는 개별 노드의 컴퓨터 보안이 개방형에서보다 훨씬 더 중요하다. 만일 어느 한 노드가 외부의 공격에 의하여 뚫리게 되면 블록체인 참여자(즉 노드)들 간에만 공유되도록 되어 있는 분산원장 기록의 변조는 방지할 수 있다고 하더라도, 분산원장 자체가 블록체인 네트워크 외부로 유출될 수 있다. 그리고 이러한 경우 ‘폐쇄형’의 가치를 잃게 된다.

또한 참여자 간의 신뢰관계를 전제로 하는 폐쇄형 블록체인에서는 그렇지 않은 개방형에 비하여 보다 간단하고 단순화된 블록 승인 메커니즘을 가질 수 있다. 전술한 바와 같이 비트코인의 경우 참여 노드들 간에 신뢰관계를 필요로 하지 않는 대신, 분산된 합의 도출을 위하여 작업증명(proof of work)이라는 블록 승인 메커니즘을 채택하고 있는데, 이 작업증명은 대단히 많은 노력과 컴퓨터 연산 능력, 그리고 전기에너지를 소모하는 메커니즘이다. 이와는 달리 폐쇄형 블록체인에서는 노력과 자원 투입이 적고, 보다 단순하고 신속하게 블록에 대한 승인이 이루어지는 블록 승인 메커니즘을 개발·채택하고 있다.<sup>22)</sup>

#### 4. 비트코인 외 블록체인 기반 플랫폼의 등장

비트코인 이후 블록체인 기술에 내재되어 있는 다양한 가능성이 주목을 받으면서, 블록체인을 기반으로 하는 다양한 플랫폼들이 등장하였다. 그리고 사회의 다양한 기능을 수행하는 데 있어서 블록체인의 활용 가능성들이 논의되고 있고, 금융산업을 중심으로 다수의 구체적인 도입이 시도되고 있다. 본절에서는 블록체인 기반 플랫폼 중에서 대표적인 것 2개를 간략하게 소개하고, 도입 사례는 제III장에서 소개한다.

22) 작업증명 외에 블록 승인을 위한 대안적 메커니즘으로 제안된 것에는 Proof of Stake(PoS), Proof of Importance(PoI), Consensus by Bet, Practical Byzantine Fault Tolerance(PBFT) 등이 있다(김진화 외, 2016; Nomura Research Institute, 2016).

### 가. Ethereum<sup>23)</sup>

Ethereum은 비트코인을 제외하고, 현재 가장 널리 알려져 있는 블록체인 기반 플랫폼이다. Ethereum은 2013년 12월에 Vitalik Buterin에 의하여 최초 고안되었으며(Buterin, 2014, 2016), 플랫폼 설계에 관한 이론적 세부사항은 Wood에 의하여 정리되었다(Wood, 2014). 그리고 2014년 8월 크라우드펀딩을 통하여 1,843만달러를 조달하였고, 2015년 7월 30일 정식으로 네트워크의 작동이 개시되었다.

Ethereum은 비트코인과 마찬가지로 인터넷 상에서 작동되는 개방형 블록체인 기반 플랫폼이다. 비트코인에서처럼 누구나 네트워크에 참여할 수 있으며, 특정 국가나 정부의 통제나 규제를 받지 않는다. 자체적인 암호화통화로 ‘ether’를 만들어 유통하고 있다. 또한 참여자들 간의 신뢰를 필요로 하지 않는다는 점, 참여 노드들이 채굴이라는 작업을 수행하고, 그 대가로 ether를 받는다는 점, 소스코드가 공개되어 있다는 점도 비트코인과 유사하다.

Ethereum을 비트코인과 구별짓는 가장 중요한 차이는 오직 암호화통화를 사용한 거래 플랫폼으로서 그 기능이 제한되어 있는 비트코인과는 달리, Ethereum은 암호화통화 거래 이외의 보다 다양한 기능을 프로그래밍화하여 탑재할 수 있는 ‘programmable blockchain’을 구현하려고 한 것이며, 그 중에서도 소위 ‘스마트계약(smart contract)’을 탑재하여 구동시킬 수 있는 플랫폼으로 설계되었다는 점이다. 스마트계약이란 계약의 내용과 실행 조건을 컴퓨터 프로그램으로 코딩하여, 정해진 조건이 충족되면 자동적으로 계약의 내용이 실행되도록 만든 디지털 계약을 의미한다. 스마트계약을 블록체인에 탑재하면 블록체인의 보안성에 힘입어 누구도 계약의 내용을 임의로 변경할 수 없으며, 계약 내용의 실행에 따른 자산의 이동이 블록체인 네트워크를 통해 이루어지도록 할 수 있다. 개방형 블록

23) 본 소절은 다음 문헌들을 참고하여 작성되었다. 금융보안원(2016), 류한석(2015), Buterin(2014, 2016), Wood(2014), CoinDesk(2016a, 2016b, 2016c, 2016d, 2016e, 2016f)

체인으로서 Ethereum에는 누구나 스마트계약 코드를 만들어 올려서 구동시킬 수 있다. Ethereum은 홈페이지([www.ethereum.org](http://www.ethereum.org))에서 자신을 “스마트계약 - 즉 작동중단, 검열, 사기 혹은 제3자에 의한 간섭의 가능성을 완전히 차단하여, 프로그램된 대로 정확하게 작동하는 애플리케이션 - 을 구동하는 분산화된 플랫폼”으로 소개하고 있다.

2016년 4월에는 Ethereum 상에 올려진 스마트계약들에 의하여 조직의 운영이 이루어지는 것을 지향하는 일종이 가상조직인 Decentralized Autonomous Organization(이하 DAO) 프로젝트를 시작하였고, 이를 위한 크라우드펀딩을 진행하였으나, 해킹 사건으로 인하여 모집 자금을 투자자들에게 반환하고 DAO 프로젝트를 중단하였다.<sup>24)</sup>

#### 나. Ripple<sup>25)</sup>

Ripple은 글로벌 은행간 실시간 결제(global interbank real-time settlement), 환전(currency exchange) 및 송금(remittance) 서비스를 제공하는, 인터넷 상에서 구동되는 블록체인 기술 기반의 오픈소스 시스템이다. 미국 샌프란시스코에 위치한 Ripple Labs 사에 의하여 개발되어 운영되고 있다. 즉 Ripple은 Ethereum과 같이 암호화통화를 이용한 거래나 스마트계약과 같은 애플리케이션을 구동하기 위한 플랫폼이라기보다는, 제공하는 기능 혹은 서비스가 명확하게 정의되어 있는 애플리케이션에 가까운 성격을 갖고 있다고 볼 수 있다.

Ripple은 비트코인이나 Ethereum과 같이, XRP라는 자체의 암호화통화를 갖고 있으며, XRP 외에도 달러와 같은 일반 법정통화, 비트코인 등에 의한 거래를 지원한다.

2016년에 Ripple은 일본의 SBI Holdings와 함께 아시아의 금융기관이

24) 해킹 사건은 18번 주석 참조. Economist(2016d)

25) 본 소절은 다음 문헌들을 참고하여 작성되었다. Thomas and Schwartz(2015), Ripple(2015, 2016), CoinDesk(2013, 2015a, 2016g), Business Wire(2016), Financial Times(2016), Finextra(2016), The Finanser(2016)

국제 송금 시스템에 블록체인 기술을 보급하는 것을 목적으로 하는 ‘SBI Ripple Asia’의 설립을 발표하였고, 스페인의 Santander를 비롯한 7개 금융기관과 내부 시스템에 블록체인을 도입·적용하는 프로젝트를 시작하였으며, 이 외에도 금융기관들을 위한 결제 프로그램들을 지속적으로 개발, 소개하고 있다.

### Ⅲ. 블록체인 기술의 활용 논의 및 도입 시도 동향

---

1. 블록체인 기술의 활용에 대한 평가와 기대
2. 해외의 블록체인 기술 도입 동향
3. 국내 기관의 블록체인 기술 도입 동향



### Ⅲ. 블록체인 기술의 활용 논의 및 도입 시도 동향

본장에서는 비트코인과 같은 암호화통화를 이용한 거래를 넘어선 블록체인 기술의 활용 가능성에 관한 논의를 자본시장에서의 블록체인 기술의 도입·활용을 중심으로 정리한다. 먼저 1절에서는 블록체인 기술의 활용 가능성에 대한 평가와 기대를 정리한다. 그리고 2절에서는 해외의 블록체인 기술 도입을 위한 시도들의 동향을 소개하고, 이어서 3절에서는 국내의 동향을 소개한다.

#### 1. 블록체인 기술의 활용에 대한 평가와 기대

##### 가. 블록체인 기술의 활용 가능성에 대한 일반적 논의

블록체인 기술과 관련된 전문가들, 블록체인을 기반으로 하는 사업을 시도하고 있는 스타트업들, 블록체인 기술의 도입과 관련된 정책과 규제를 담당하는 정부기관들로부터 블록체인 기술의 향후 활용 가능성에 대한 다양한 논의를 담은 자료들이 나오고 있다. 이러한 자료들에서 제시된 논의들을 종합하면 블록체인 기술은 현재의 암호화통화를 이용한 거래를 넘어, 자본시장을 포함한 다양한 금융 거래에서, 그리고 이어서 금융 이외 경제 전반에서, 궁극적으로는 사회 전반의 다양한 부문과 기능에서 활용될 수 있다는 것이다.

금융 부문에서는 금융회사간 거래, 송금 서비스, P2P 대출 등, 그리고 그 중에서도 자본시장에서는 주식, 채권, 파생상품 등과 같은 금융투자상품의 거래, 클라우드펀딩 등이 블록체인 기술이 효과적으로 활용될 수 있는 서비스로 꼽히고 있다.

금융 외의 영역에서는 기업의 주주명부 관리 및 의결권 행사, 부동산

등기부, 차량 등록, 출생·사망 증명, 신분증(운전면허증, 여권 등) 발급 및 관리, 공적연금·건강보험 등의 징수 및 지급, 지적재산권·특허 출원 및 소유 증명 등과 같은 기록의 정확하고도 신속한 업데이트 및 안전한 보관이 요구되는 다양한 사적·공적 기능들에서 블록체인이 효과적으로 도입·활용될 수 있을 것으로 기대된다(UK Government, 2015; Swan, 2015; Nomura Research Institute, 2016 등).

이와 같은 경제 및 사회의 제반 기능 혹은 서비스에서의 블록체인 기술의 활용과 관련하여 많은 주목을 받고 있는 것이 ‘스마트계약(smart contract)’이다. 스마트계약은 II장의 Ethereum 소개에서 설명한 바와 같이 계약의 실행 조건을 포함한 모든 내용을 컴퓨터 코드로 만든 디지털 계약이다. 블록체인 기술이 갖는 특성을 활용하여 실행 조건이 충족되면 자동적으로 계약 내용이 실행되도록 하고, 동시에 계약의 내용을 그 누구도 변조할 수 없도록 만들 수 있다는 점에서 금융 뿐 아니라 공공 및 민간 부문의 다양한 영역에서 활용 가능성이 논의되고 있다.

#### 나. 블록체인 기술의 자본시장에의 도입·활용 논의

블록체인 기술의 도입과 활용이 기대되는 경제와 사회의 많은 영역과 기능 중에서도 현재 가장 활발하게 논의가 일어나고 있고, 또한 도입을 위한 구체적인 노력들이 가장 많이 이루어지고 있는 부문은 금융, 그 중에서도 자본시장이다. 자본시장은 다수의 시장참가자들 사이에서 자산의 거래가 지속적으로 발생하고 있고, 거래에 따른 자산 소유권의 이전에 대한 정확한 기록을 담은 원장의 안전한 보관이 매우 중요하다는 점에서 블록체인 시스템이 가지고 있는 본질과 특성이 장점으로 가장 잘 발휘될 수 있고, 따라서 블록체인 기술의 활용에 의하여 가장 많은 편익을 누릴 수 있는 부문으로 여겨지고 있다. 미국의 Nasdaq, 호주의 ASX 등의 거래소들은 실제로 주식거래에 있어서 블록체인 기술의 도입을 위하여 가장 적극적인 움직임을 보이고 있으며, 거래소 외에도 미국의 DTCC와 같은 자본

시장 후선업무(back-office) 기관들도 많은 관심을 갖고 블록체인 논의와 도입 노력에 참여하고 있다.

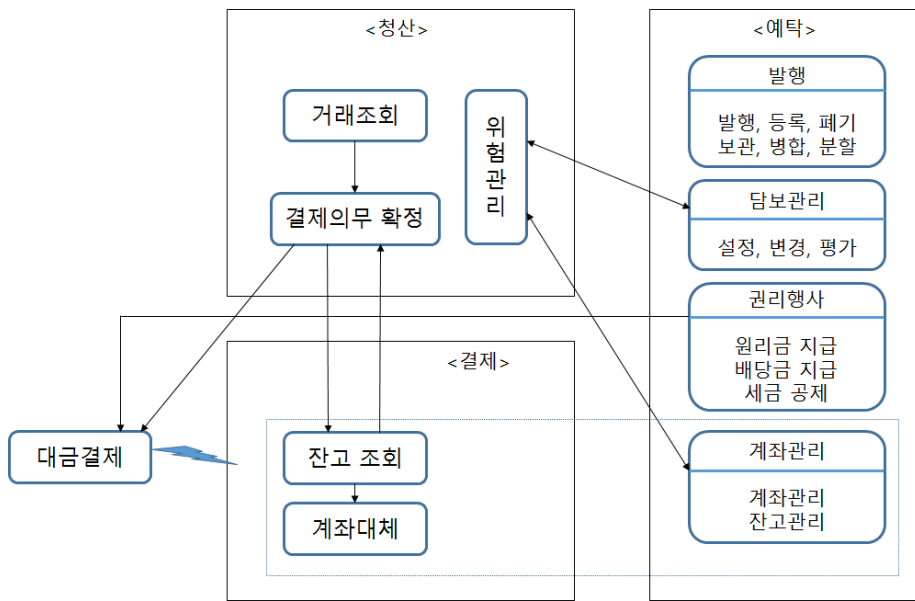
자본시장을 블록체인 기반으로 운영할 경우, 생각할 수 있는 가장 극단적인 형태는 완전히 디지털화되어 발행, 유통되는 디지털증권(digital securities) 혹은 암호화증권(cryptosecurities)을 모든 거래 참가자가 P2P로 연결되어 암호화통화를 이용하여 거래하는 시장일 것이다(Lee, 2016). 비트코인에서와 마찬가지로 이러한 시장에서는 거래소 및 청산소(clearinghouse)라는 집중화된 기관이 없을 것이고, 차감이나 청산 절차 없이 모든 거래에서 증권의 인도와 대금의 결제가 실시간으로 이루어지게 될 것이다. 중앙예탁기관(CSD)도 존재하지 않게 될 것이다. 그러나 현실적으로 이러한 형태의 시장이 등장하기에는 기술적, 제도적으로 해결해야 할 과제들이 매우 많다. 예를 들어, 현재의 블록체인 기술 수준에서는 서술한 바와 같은 개방형 블록체인의 암호화증권시장에서 발생하는 거래를 감당할 수 없다. 현존하는 가장 대규모의 개방형 블록체인인 비트코인에서 10분마다 생성되는 블록에 기록되는 거래 수가 수천개 수준임에 비하여, 현재 세계 유수의 주식시장에서는 1초당 수만건이 훨씬 넘는 거래가 이루어지고 있다. 그리고 이 모든 거래들을 기록하는 원장 역시 비트코인과는 비교할 수 없을 정도의 크기를 갖게 되는데, 이러한 원장을 모든 거래 참가자들에게 분산시켜 저장하는 것이 과연 효율적이며, 현재 기술 수준에서 가능한 것인지도 불확실하다. 또한 블록체인 기반의 일종의 ‘가상’ 시장에서 거래될 수 있는 암호화증권의 발행 및 유통을 위한 법적·제도적 기반 역시 우리나라를 비롯하여 많은 국가에서 마련되어 있지 않거나 시행되고 있지 않다.<sup>26)</sup> 더욱이 증권의 거래가 이와 같이 P2P로 이루어지는 것이 현재의 방식보다 과연 바람직한 것인지에 대한 판단 역시 불확실하다.

따라서 현재의 논의는 보다 실현 가능한 수준에서 매매거래의 체결과 같은 전선업무(front office) 단계에서는 상대적으로 거래 빈도가 낮고, 거래 참가자의 자격과 수가 제한적인 비공개기업의 주식 발행 및 거래 플랫폼을

26) 우리나라에서는 2016년 3월 22일, 「주식·사채 등의 전자등록에 관한 법률」이 제정되었으나, 시행일은 아직 미정이다.

블록체인 기반으로 구축하는 것, 그리고 ‘거래후 처리과정(post-trade processing)’, 즉 후선업무를 블록체인 기반으로 구축하는 두 개의 흐름으로 압축되고 있으며, 그 중에서도 다수의 논의는 후선업무에 블록체인 기술을 도입하는 것으로 집중되고 있다. 자본시장 후선업무는 <그림 III-1>과 같은 구조를 갖고 있으며, 계좌를 조회하고 변경사항을 기록하는 것, 대금의 결제, 발행·담보관리·권리행사와 같은 제반 예탁 관련 기능들을 블록체인 기술을 활용하여 수행하도록 하는 것에 대한 모색이 이루어지고 있다.

<그림 III-1> 자본시장 후선업무 구조



자료: 한국예탁결제원(2014)

또한 자본시장에서 활용되는 블록체인은 자본시장이 갖는 특성 및 자본시장 거래 플랫폼과 후선 인프라가 갖추어야 할 필수적인 요구사항을 반영하여 설계되어야 하고, 특정한 상품이나 특정한 고객을 위한 맞춤형

설계가 가능해야 하며, 참여자들 간의 사전적 신뢰가 확보될 필요가 있다는 점에서 개방형이 아니라 폐쇄형(permissioned)이 될 것이라는 데에 거의 모든 자본시장 관련 기관들과 전문가들의 의견이 일치하고 있다(DTCC, 2016b; SWIFT, 2016; Morgan Stanley, 2016).

미국의 대표적인 자본시장 후선업무 서비스 기관인 DTCC는 2016년 1월에 발표한 블록체인에 관한 ‘White Paper’(DTCC, 2016a)에서 비교적 보수적인 평가를 내리고 있다. DTCC(2016a)는 블록체인 기술이 자본시장에서 후선업무를 전혀 다른 모습으로 혁신할 수 있는 충분한 가능성을 갖고 있다고 평가하면서, 동시에 그러한 가능성에 대한 기대가 과장될 수 있다는 견해를 피력하였다. DTCC(2016a)는 DTCC가 운영하고 있는 현재의 시스템은 오랜 기간에 걸쳐 안정성, 경제성, 효율성, 규제정합성 등에서 이미 입증된 우수한 시스템임에 비하여, 블록체인은 DTCC에 대한 신뢰를 기반으로 한 집중화된 형태인 현재 시스템과는 모든 면에서 반대되는 시스템으로서 아직까지 초기 단계의 검증되지 않은 기술이며, 현재의 자본시장 환경에 깔끔하게 통합될 수 있을지는 불분명하다는 평가를 내리고 있다. 그러나 블록체인 기술에 의하여 가장 직접적으로 영향을 받게 될 기관인 DTCC는 보수적인 평가와는 별도로 2016년 3월에 대규모의 블록체인 컨퍼런스를 개최하고(DTCC, 2016b), Hyperledger 프로젝트에 프리미어 회원으로 참여하는 등<sup>27)</sup> 블록체인 기술을 파악하고, 시장참여자들 및 블록체인 기술기업들과의 광범위한 협력에도 매우 적극적인 태도를 보이고 있다. 일례로, DTCC는 2016년 4월, Axoni라는 블록체인 기술기업과 J.P. Morgan을 비롯한 4개의 글로벌 금융회사들과 함께 신용부도스왑(CDS) 거래의 블록체인 기반 후선업무 테스트의 성공적인 실시를 발표하기도 하였다(DTCC, 2016d). DTCC(2016a)는 블록체인 기술의 도입을 위한 노력이 개별 기업 차원에서 별개로 이루어지는 것 보다는 자본시장 산업 전체적인 차원에서의 협력을 통하여 산업 전체의 기술표준을 수립하는 방향으로 나갈 필요가 있다는 입장을 견지하고 있다.

DTCC가 개최한 블록체인 컨퍼런스(DTCC, 2016b)에서 참가자들은

27) Hyperledger 프로젝트에 관해서는 III장 2절에서 설명한다.

DTCC와 같은 중앙집중형 ‘제3자 기관’은 금융위기와 같은 상황에서 매우 중요한 역할을 담당하며, 따라서 블록체인 기술이 도입되더라도 유사한 역할을 담당하는 어떤 운영주체가 있어야 하고, 대사(reconciliation)의 필요성이 완전히 사라지는 않을 것이라는 데에 의견을 같이 하였다. 또한 블록체인의 장점으로 일컬어지는 결제기간의 단축, 예를 들면 T+0 결제는 현재의 시스템에서도 충분히 가능하며, 블록체인 역시 다양한 결제주기를 지원하도록 발전되어야 한다는 점을 지적하고 있다. 그리고 블록체인 기술이 도입되어 안정적으로 운영되기까지는 앞으로도 수년의 시간이 더 필요할 것이며, 현재의 시스템을 완전히 대체하려는 시도보다는 후선업무의 어느 부분에 블록체인 기술을 적용하는 것이 가장 효과적인지를 찾아내는 것이 현 시점에서 가장 중요한 도전이라고 말하고 있다.

SWIFT(2016)는 자본시장 후선업무 전문가들과의 인터뷰 및 토론을 통하여 도출된 의견을 정리하여 발표하였는데, 블록체인 기술의 도입은 데이터 처리에 소요되는 비용 및 수반되는 위험을 상당한 정도로 감소시킬 수 있는 잠재력을 갖고 있다고 평가하였다. 그러나 동시에 시장과 업계에서 블록체인 기술의 가능성과 도입 효과에 대하여 비현실적인 기대를 갖는 것은 위험하다고 주의를 환기하였다. 또한 블록체인 기술의 도입이 자본시장에서 제3자 기관의 필요성을 완전히 제거하지는 못할 것이며, 현재 자본시장에의 도입과 관련된 가장 중요한 도전은 기술적 실행가능성(technological feasibility)을 보여주는 것이 아니라, 도입으로 인한 자본시장에서의 비즈니스 프로세스 리엔지니어링을 위한 산업 전체 차원에서의 조정과 합의를 이끌어내는 것이라고 언급하였다.

한편 유럽의 European Securities and Markets Authority(ESMA, 2016)는 블록체인 기술의 자본시장 도입에 따른 여러 잠재적 편익들을 인정하면서, 동시에 다음과 같은 몇 가지 견해를 표명하였다. 즉, 현물(cash) 거래와 달리 파생상품 거래에서는 블록체인을 도입한다고 해서 거래상대방위험이 없어지는 것은 아니며, 따라서 중앙청산기관(central counterparty: CCP)과 같은 ‘제3자 기관’ 및 담보는 여전히 필요할 것이다. 그리고 담보 관리, 증거금(margin) 관리 등을 스마트계약으로 만들어

블록체인에 올림으로써 계약 내용의 변조의 위험으로부터 안전하게 보관하고 자동적 계약 실행을 효율적으로 관리할 수 있을 것이라는 점이다.

#### 다. 블록체인 기술의 도입·활용에 따른 기대 편익

자본시장에 블록체인 기술을 도입, 활용함으로써 누리게 될 것으로 기대되는 편익으로 공통적으로 언급되는 것들은 다음과 같다(Accenture, 2016; ESMA, 2016; Morgan Stanley, 2016; Oliver Wyman and J.P. Morgan, 2016). 첫째로 블록체인의 본질과 관련된 것으로서, 자본시장 거래와 관련하여 ‘제3자 기관’을 설치할 필요가 없음으로써 후선업무의 관리비용(back-office administration cost)을 절감할 수 있다는 것이다. SWIFT(2016)는 다양한 분석과 자료를 인용하여 현재 전 세계적으로 자본시장의 거래 데이터 관리(데이터의 획득, 기록의 확인, 대사 등)에 소요되는 비용이 약 170억~240억달러, 준법감시(compliance) 관련 업무에 소요되는 비용이 최대 120억달러에 달하는 것으로 추정되며, 블록체인 기술의 도입·활용에 의하여 청산, 결제, 담보관리, 예탁 부문에서 현재의 기존 시스템과 비교할 때 전세계적으로 매년 400억~450억달러 정도의 비용 절감을 기대할 수 있다고 분석하였다. 또한 Goldman Sachs는 주식, repo, leveraged loan 시장의 청산·결제 부문에서만 전세계적으로 매년 60억달러의 비용절감을 기대할 수 있으며, 여기에 외환, 실물상품, 파생상품까지 포함하면 절감 규모는 더욱 커질 것이라는 예측을 발표하였다(CoinDesk, 2016r). 미국의 대표적인 후선업무 ‘제3자 기관’이라고 할 수 있는 DTCC의 2015년도 수익이 약 16억달러, 영업비용이 약 15억달러이며(DTCC, 2016c), 유럽의 LCH.Clearnet Group의 2015년도 수익이 4억 1,660만달러, 영업비용이 3억 5,520만달러(LCH.Clearnet, 2016)임을 고려하면 이러한 절감 규모는 매우 크다고 볼 수 있다. 그러나 II장 3절에서 언급한 바와 같이, 블록체인 네트워크를 작동시키기 위하여 전 세계에 퍼져 있는 수많은 노드들로부터 투입되는 컴퓨터 연산용량, 적지 않은

크기의 블록체인 파일을 또한 이들 노드들이 동시에 보관하는 데서 발생하는 비효율 등을 고려하면 경제 전체적으로 볼 때 과연 얼마나 비용 절감이 이루어지는지를 판단하기는 쉽지 않다. 한 기관으로부터 발생하는 비용을 네트워크의 노드들에게로 분산시킨 것과 비슷하다는 것이다.

둘째로 중개기관의 수를 극단적으로는 0으로 줄임으로써 청산·결제에 소요되는 시간을 크게 줄일 수 있다. 결제기간을 수초 정도로 단축할 수 있을 뿐 아니라 시장의 특성과 시장참여자의 필요에 맞추어 결제기간을 조정할 수도 있다. 또한 거래의 완결을 위하여 개입되는 중개기관의 수가 줄어든다는 것은 특히 국가간의 거래가 보다 효율적으로 이루어질 수 있다는 가능성을 의미하기도 한다.

셋째로 블록체인이 갖는 강력한 보안성과 안정성으로 인하여 후선업무에서의 운영리스크(operational risk)를 줄일 수 있고, 결제기간 단축에 따라 담보의 필요성이 낮아지고 거래상대방위험 역시 줄어든다. 그에 따라 시장에서의 거래와 관련된 계약불이행의 위험도 감소한다.

넷째로 원장이 블록체인 참여자들에게 공개되고 분산 저장되기 때문에 원장 관리의 투명성이 제고되고, 대사의 필요성이 줄어든다. 또한 전체 원장에서 규제당국이 요구하는 부분을 신속하게 압축하여 제공함으로써 준법감시(compliance) 관련 비용을 줄이고 효율성을 높일 수 있다.

그러나 블록체인 기술의 도입에 의하여 이와 같은 편익들이 실제로 실현될 것인지, 그리고 DTCC(2016b)에서 언급된 바와 같이 이러한 편익들이 기존의 시스템은 제공할 수 없고 블록체인만이 제공할 수 있는 것인지에 대해서는 다른 견해 역시 존재한다.

## 라. 블록체인 기술의 도입 관련 과제

블록체인 기술이 실제로 자본시장에서 도입·활용되기 위해서는 먼저 해결되어야 할 몇 가지 도전 혹은 과제들이 있다. 다수의 문헌들은 거의

공통적인 과제들을 제시하고 있으며(Accenture, 2016; McKinsey, 2015, Morgan Stanley, 2016; UK Government, 2016), 본 소절에서는 이를 기술적 과제와 경제적·규제적 과제로 나누어 서술한다.

### 1) 기술적 과제

블록체인 기술을 자본시장에 도입하여 활용하는 데 있어서 현 시점에서 가장 많이 지적되고 있는 기술적 과제는 처리 속도 및 용량(scalability)의 문제이다. 전술한 바와 같이 현재 비트코인에서 거래의 처리 - 거래의 유효성을 검증하고, 거래기록을 모아 블록을 만들고 작업증명을 해결하며, 작업증명을 검증하여 블록을 승인하고 기존의 블록체인에 연결하여 업데이트하는 것 - 속도로는 일반적인 자본시장, 특히 거래소시장과 같은 공개시장(public market)의 거래 속도 및 빈도를 감당할 수 없다. 그리고 P2P 네트워크라는 블록체인의 본질적 속성상 네트워크가 커짐에 따라, 즉 참여 노드 수가 많아짐에 따라 더 많은 노드가 거래를 검증하고 블록을 승인하기 때문에 처리 속도는 어느 정도 빨라질 수 있으나, 기존의 '제3자 기관'으로의 중앙집중형 시스템에서 이 '제3자 기관' host 컴퓨터의 처리 능력을 증대시키는 것이 거래 증가에 대응하는 데에는 보다 효율적일 가능성이 높다. 또한 원장의 저장 용량은 노드 수가 많아진다고 해서 증가하지 않는다. 개별 노드의 저장장치를 합쳐서 사용하는 것이 아니기 때문이다. 이 처리 속도 및 용량의 문제는 자본시장 중에서도 공개시장이 아닌 비공개기업 주식과 같은 사모 혹은 장외시장에서 블록체인의 도입이 먼저 추진되고 있는 핵심적 이유이다.

두 번째 기술적 과제는 보안성 및 안정성에 대한 확신을 시장참여자들에게 주어야 한다는 것이다. II장에서 서술한 바와 같이 블록체인의 가장 큰 특징이며 강점으로 여겨지고 있는 것이 보안성인데, 이 보안성이 비트코인 외의 다른 블록체인 네트워크에서도 동일한, 혹은 그 이상의 수준으로 보장될 수 있는 것인지에 대해서는 아직까지 확실하게 검증되지 않았다. 블록체인이 이론적·개념적으로는 매우 강력한 보안성을 가진다는 데에는

거의 동의가 이루어지고 있으나, 실제 새로운 블록체인 기반의 어떤 시스템을 만들어 내는 데 있어서는 인간의 오류, 예를 들면 코드상의 실수와 같은 가능성이 언제나 존재한다. 전술한 Ethereum의 DAO는 그 하나의 사례이다. 그리고 보안성 혹은 시스템의 안정성에 어떤 문제가 발생할 경우, 그 확산과 영향은 기존 시스템에서보다 심각할 수 있으며, 수습하기도 어려울 가능성이 있다(ESMA, 2016).

비트코인 거래에서 볼 수 있듯이, 블록체인 기반 네트워크에서 발생하는 거래의 중요한 특징의 하나는 일단 승인되어 블록에 기록된 거래는 취소나 정정이 불가능하다는 것이다. 착오로 인하여 비트코인이 잘못 이전된 경우에는 반대 방향의 거래를 또 한 번 발생시켜 비트코인을 돌려보내야 한다. 그러나 자본시장에서는 거래상의 착오나 실수의 가능성이 언제나 존재하며, 반대 방향의 거래에 의하여 해결되지 않고 취소 혹은 정정이 반드시 필요한 경우가 존재한다. 따라서 블록체인 기술이 자본시장에서 활용되기 위해서는 거래의 취소·정정 기능이 포함되어야 한다.

다음으로 필요한 기술적 과제는 기존의 시스템 및 동일한 기능을 수행하는 다른 블록체인 시스템과의 연동성(interoperability)을 확보하는 것이다. 연동성의 확보에 의하여 네트워크 효과가 더 크게 나타날 수 있으며, 그럴수록 그 시스템 혹은 플랫폼에 참여함으로써 얻을 수 있는 효용이 더욱 커질 것이다.

또한 블록체인 기술을 도입하려고 하는 자본시장 비즈니스 프로세스상의 특정 영역이나 서비스 혹은 업무의 특성에 맞춘 맞춤형 설계가 가능해야 한다. 예를 들어 거래되는 상품의 성격과 특성, 거래자의 필요에 따라 결제 주기를 신축적으로 설정할 수 있어야 한다.

## 2) 경제적·규제적 과제

블록체인을 기반으로 한 시스템 혹은 플랫폼을 구성함에 있어서 시스템의 지배구조(governance) 및 유인체계(incentive scheme)에 대하여 참여자,

혹은 참여기관 간의 조정을 거쳐 합의가 도출되어야 한다. 자본시장에서 도입이 논의되는 블록체인은 비트코인과 같이 네트워크 전체를 관리하거나 의견을 조정하는 리더십이 없는 개방형 블록체인이 아닌 폐쇄형 블록체인이다. 그리고 이러한 폐쇄형 블록체인 네트워크를 구성하는 경우 네트워크 관리 및 의견 조정에 있어서 리더십과 권한은 누구에게 어떻게 부여할 것인지, 신규 참여자(노드)의 가입 승인은 어떠한 기준에 의하여 어떻게 결정할 것인지 등 네트워크의 지배구조는 매우 중요하며, 블록체인 네트워크의 성패를 결정하는 중요한 요소가 된다.

또한 개방형 블록체인에서는 블록의 검증과 승인을 담당하는 각 노드에 대한 보상과 유인을 적절하게 설계하는 것이 매우 중요하다. 그러나 폐쇄형 블록체인에서는 각 노드가 채굴에 따른 보상이 아닌, 자신의 사업상의 필요에 의하여 네트워크에 참여하는 것이기 때문에 이미 내재적인 유인을 갖고 있다고 볼 수 있고, 따라서 블록의 검증과 승인에 대한 별도의 유인을 제공할 필요성은 크지 않다고 볼 수 있다.

블록체인 기반의 자본시장 플랫폼이 실제로 사용되기 위해서는 법적·규제적 측면에서도 해결되어야 할 과제들이 있다. 우선 블록체인 기반의 증권거래 플랫폼이 작동하기 위해서는 디지털증권, 혹은 암호화증권의 발행, 유통, 권리 및 소유 이전 등에 관한 법적 근거가 마련되어야 한다. 또한 금융보안 등과 같은 전자금융과 관련된 기존의 규제 중에서 블록체인의 성격과 충돌하는 부분이 없도록 정리해놓을 필요가 있다. 각국 규제기관 간의 공조 역시 매우 중요하다. 글로벌 블록체인의 경우 수많은 노드들이 각각 다른 나라들에 흩어져 존재하기 때문에 이 경우 일관된 규제를 집행하기 위해서는 사전적 조정과 협력이 필수적이다.

## 2. 해외의 블록체인 기술 도입 동향

### 가. 블록체인 도입을 위한 글로벌 협력 및 컨소시엄

#### 1) R3CEV<sup>28)</sup>

R3CEV는 블록체인 스타트업 R3와 세계 각국의 50여개 금융회사로 구성된 블록체인 컨소시엄으로, 2015년 9월에 9개의 글로벌 대형 금융회사들의 참여로 시작되었다. R3의 창업자인 David Rutter는 R3CEV의 결성 목적은 은행 등 금융회사의 업무 프로세스를 블록체인 기술을 도입하여 구축하고, 이들 금융회사들을 위한 블록체인 기반 상용 애플리케이션을 개발하는 데 있다고 밝히고 있다. 이는 현재의 은행 업무, 금융투자업무 시스템에 블록체인 기술을 적용하여 보안성을 높이고 비용을 절감하기 위한 시도라고 평가되고 있다.

R3CEV가 금융회사 업무에 도입하고자 시도하는 블록체인은 비트코인과 같은 개방형이 아니라 컨소시엄에 참여하고 있는 기관들만이 노드가 되고, 전체 블록체인 네트워크를 관리하는 관리자가 존재하는 폐쇄형(permissioned)을 지향하고 있다. 그리고 컨소시엄에 참여하는 금융회사들을 블록체인 네트워크로 연결하여 일차적으로는 이들 금융회사 간 거래에서 블록체인 기술을 도입, 활용하는 것을 시도할 것으로 보인다.

최초 J.P. Morgan, Goldman Sachs, UBS 등 9개의 글로벌 대형 금융회사들로 시작된 R3CEV는 이후 컨소시엄 참여 기관을 꾸준히 늘려 나가, 현재는 전 세계에 걸쳐 거의 50개의 기관이 참여하는 대형 프로젝트로 성장하였다. 한국에서는 2016년 4월 15일 하나금융그룹이 최초로 R3CEV에 참여한다고 발표하였다. 2016년 6월말 현재 R3CEV 참여 기관의 현황은 <표 III-1>에 정리되어 있다.

28) 본 소절은 다음 문헌들을 참고하여 작성되었다. CoinDesk(2016h, 2016i, 2016j, 2016k, 2016l), Coinspeaker(2016), Cryptocoinsnews(2016), Econotimes(2016), Financial Times(2015a, 2015b), R3(2015, 2016a, 2016b, 2016c), Reuters(2015)

**<표 III-1> R3CEV 참여 기관 현황 (2016년 6월 기준)**

가입일자	참여 기관명
2015. 9. 15 (9개 기관)	Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, State Street, UBS
2015. 9. 29 (13개 기관)	Bank of America, BNY Mellon, Citi, Commerzbank, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, National Australia Bank, Royal Bank of Canada, Skandinaviska Enskilda Banken, Société Générale, Toronto-Dominion Bank
2015. 10. 28 (3개 기관)	Mizuho Bank, Nordea, UniCredit
2015. 11. 19 (5개 기관)	BNP Paribas, Wells Fargo, ING, Macquarie Group, Canadian Imperial Bank of Commerce
2015. 12. 17 (12개 기관)	BMO Financial Group, Danske Bank, Intesa Sanpaolo, Natixis, Nomura, Northern Trust, OP Financial Group, Banco Santander, Scotiabank, Sumitomo Mitsui Banking Corporation, U.S. Bancorp, Westpac Banking Corporation
2016. 3. 14 (1개 기관)	SBI Holdings
2016. 4. 15 (1개 기관)	하나금융그룹
2016. 4. 25 (1개 기관)	Itaú Unibanco
2016. 5. 24 (1개 기관)	Ping An Insurance Group
2016. 6. 2 (1개 기관)	AIA
2016. 6. 23 (1개 기관)	Toyota Financial Services
2016. 6. 29 (1개 기관)	Banco Bradesco

자료: <https://r3cev.com>

현재 R3CEV는 참여 기관들과의 지속적인 협의 및 블록체인 네트워크에 대한 테스트를 통하여 블록체인 네트워크의 플랫폼, 기술표준 등을 정하고, 금융 서비스에 특화된 블록체인 기술을 개발하고, 블록체인 기술이 활용될 수 있는 금융 서비스 부문을 정하여 여기서의 기술 활용을 위한 개념 증명(proof of concept) 계획을 수립하여 추진하는 활동을 벌이고 있다. 2016년 1월에는 11개 은행들이 참여하여 Ethereum 네트워크를 통하여 암호화통화인 ether<sup>29)</sup>를 은행 간에 이전하는 테스트를 실시하여, 제3자 기관 없이 ether와 같은 '토큰화'된 자산 이전의 은행 간 정산이 거의 실시간으로 이루어질 수 있음을 확인하였고, 향후 개인의 금융거래까지 확장할 수 있는 기술적 가능성을 검증할 수 있었음을 발표하였다.

2016년 4월에는 R3사에서 'Corda'라고 명명된, 금융회사 간 계약의 기록, 관리 및 동기화(synchronise)에 특화된 블록체인 플랫폼의 개발을 발표하였다. R3의 발표에 의하면, Corda는 기존의 공개형 블록체인과는 구별되는 다음과 같은 특징들을 가진다.

- ① 상호간 합의에 의하여 원장 기록을 보아야 할 적절한 필요가 있는 참여자(노드)만이 원장을 공유, 보관한다.
- ② 중앙 통제기관(central controller) 없이 금융회사 간의 직접적 작업 흐름(workflow)을 가능하게 한다.
- ③ 거래 유효성 검증은 시스템 전체 차원이 아닌, 각 개별 거래 차원에서 당사자 간의 합의로 이루어진다.
- ④ 규제 및 감독 목적의 노드 참여가 가능하다.
- ⑤ 다양한 합의 도출 메커니즘을 지원한다.
- ⑥ 자체적인 암호화통화는 없다.

또한 같은 4월에는 금융거래에서의 블록체인 기술의 활용을 위한 8가지 개념증명 계획을 발표하였다. 이 8가지에는 시스템 연동성(interoperability), 지급, 결제, 무역금융, 회사채, repo, 스왑, 보험이 포함된다.

29) II장 4절의 Ethereum 설명 참조

R3CEV는 금융 부문에서 가장 큰 규모로 진행되고 있는 블록체인 컨소시엄이다. 그러나 블록체인 기술 도입의 초기 단계에서 아직까지는 금융업계 공동의 연구개발 프로젝트로서의 성격이 강하다고 볼 수 있을 것이다.

## 2) Hyperledger 프로젝트<sup>30)</sup>

Hyperledger 프로젝트(이하 HLP)는 Linux Foundation이 중심이 되어 60여개의 기업이 참여하고 있는 글로벌 블록체인 프로젝트로서 2015년 12월에 시작되었다. 처음에는 20개 기업의 참여로 시작되었으며, 이후 지속적으로 참여 기업의 수를 늘려 나가 2016년 6월 현재 참여기업 수는 60여개에 달하고 있다. HLP에는 R3, ConsenSys와 같은 블록체인 전문기업, Cisco, Digital Asset Holdings, IBM과 같은 IT 기업들과 더불어 ABN-AMRO, BNY Mellon, J.P. Morgan과 같은 금융회사, 한국예탁결제원, DTCC, SWIFT와 같은 금융인프라 및 후선서비스 기관, 독일거래소, CME Group 등의 시장운영기관 등이 폭넓게 참여하고 있다.<sup>31)</sup> 2016년 6월말 현재 HLP 참여 기관의 현황은 <표 III-2>에 정리되어 있다.

참여기관(회원)은 프리미어, 일반, 준(associate)회원으로 구분되며, 모든 회원은 등급에 관계없이 HLP의 총회를 비롯한 제반 활동에 참여할 수 있고, 기술적 측면에 관한 제안을 할 수 있다. 다만, 프리미어 회원은 HLP의 이사회(governing board), 마케팅위원회 및 기타 위원회의 대표를 지명할 수 있는 자격이 주어진다라는 점에서 차이가 있다.

HLP는 모든 산업에서 발생하는 상업적 거래에 범용적으로 사용될 수 있는 블록체인 플랫폼을 만들기 위한 개방형 표준을 구축하기 위하여 결성되었다. 구체적으로 HLP는 다음을 목표로 한다(Linux Foundation, 2016b).

30) 본 소절은 다음 문헌들을 참고하여 작성되었다. 한국예탁결제원(2016), Bitcoin Magazine(2016a), Linux Foundation(2015, 2016a, 2016b, 2016c)

31) 한국에서는 한국예탁결제원이 처음으로 2016년 7월에 HLP에 참여하였다.

<표 III-2> Hyperledger 프로젝트 참여 기관 현황 (2016년 6월 기준)

구분		참여 기관명
프리미어 (Premier)	금융, 자본시장	CME Group, 독일거래소, DTCC, J.P. Morgan
	기술, 기타	Digital Asset, Fujitsu, Hitachi, IBM, Intel, R3, Accenture
일반 (General)	금융, 자본시장	한국예탁결제원, ABN-AMRO, ANZ Bank, BNP Paribas, BNY Mellon, Broadridge Financial Solutions, Calastone, CLS, Cuscal, IntellectEU, INVeSHARE, Montran, Moscow Exchange, State Street, SWIFT, TMX Group, Wells Fargo
	기술, 기타	Belink Technologies, BitSE, Blockchain, Blockstream, Bloq, Bubi, Cisco, Cloudsoft, Coinplug, Colu, ConsenSys, Credits, Eurostep Digital, eVue Digital Labs, Gem, Guardtime, itBit, Libra, Milligan Partners, MonetaGo, NEC, Norbloc, NTT Data, Onchain, Red Hat, Rabbit.me, Skry, Soramitsu, Symbiont, Tequa Creek, Thomson Reuters, VMware

자료: <https://www.hyperledger.org>

- ① 상업적 거래를 지원할 수 있는 강력한 산업별 애플리케이션, 플랫폼, 하드웨어 시스템을 구축하고 실행할 수 있는 오픈소스 분산원장 프레임워크 및 코드베이스(code base)의 개발
- ② HLP 솔루션 제공자와 사용자들의 생태계를 돕기 위한 오픈소스 기술 공동체(open source, technical community)의 형성
- ③ 개발자, 솔루션 제공자, 최종 사용자들을 포함하는 생태계 리더들의 참여 촉진
- ④ 회의, 각종 행사, 토론회 주관 등 블록체인 공동체를 위한 인프라 기관으로서의 역할 수행

현재 HLP에서는 IBM이 작성한 ‘Hyperledger Whitepaper’에 대한 내부 검토를 진행하고 있으며, 또한 IBM, Blockstream, Digital Asset

Holdings 등이 각각 개발한 블록체인 네트워크의 레이어 별 코드를 융합하는 작업을 진행 중인 것으로 알려져 있다. 실제 금융산업과 자본시장에서 활용될 수 있는 가시적인 성과가 나오기까지는 어느 정도 시간이 필요할 것으로 보인다.

## 나. 해외 기관별 동향

본절에서는 전술한 글로벌 컨소시엄 외에 세계 각국의 기관별로 이루어지고 있는 블록체인 기술의 도입을 위한 움직임들을 소개한다. 먼저 자본시장 운영기관, 금융회사 등 업계의 추진 현황을 정리한다. 현재 각국의 수많은 기관들로부터 블록체인 기술의 도입 추진과 관련된 발표들이 계속 이어지고 있고, 또한 이를 위한 논의와 협력을 위한 기구들이 만들어지고 있는데, 본 보고서에서는 그 중에서 대표적인 사례를 추려서 소개한다. 또한 주요 자본시장 규제기관들 역시 블록체인 기술의 도입과 관련하여 관심을 갖고 추이를 주시하면서 입장을 표명하고 있는데, 그러한 견해 및 대응 동향을 소개한다.

### 1) 업계의 추진 현황

#### 가) Nasdaq Linq<sup>32)</sup>

Nasdaq Linq는 Nasdaq이 운영하는 비공개기업 주식시장인 ‘Nasdaq Private Market’에 만들어진 블록체인 기반의 비공개기업 주식 거래 플랫폼이다. Nasdaq은 2015년 5월, 블록체인 기술을 기반으로 하는 비공개기업 주식의 거래를 위한 장외 플랫폼을 개발할 계획을 수립하고, Chain.com 등 블록체인 기술 스타트업들과 개발에 착수하여, 2015년 10월 27일 Nasdaq Linq를 발표하였다.

32) 본 소절은 다음 문헌들을 참고하여 작성되었다.

Bloomberg(2015), Forbes(2015), Nasdaq(2015a, 2015b, 2016a, 2016b)

Nasdaq의 발표에 의하면, Nasdaq Linq는 비공개기업 주식의 발행, 분류(cataloging), 주식소유권의 이전에 이르는 과정을 블록체인 기반으로 처리하는 최초의 플랫폼이다. Nasdaq은 Nasdaq Linq의 고객기업들이 블록체인 기술의 적용으로 주식 발행과 소유권 이전에 대한 완전한 역사적 기록에 대한 관리·유지 서비스를 제공받게 될 것이라고 언급하였다. Nasdaq Linq에서 주식이 거래되는 최초의 고객 기업은 Chain.com, ChangeTip, PeerNova, Synack, Tango, Vera 등 6개 기업이다. Nasdaq Linq는 당분간 비공개로 이들 6개 기업의 주식에 대한 발행 및 매매거래를 시험운영한다. Nasdaq은 Nasdaq Linq의 운영 개시를 발표하면서 블록체인 기술이 향후 금융서비스의 인프라를 영구적으로 바꿔놓을 수 있는 기술이라고 평가하였다.

Nasdaq Linq는 Nasdaq이 추진하고 있는 ‘전사적 블록체인 기술 이니셔티브(enterprise-wide blockchain technology initiative)’의 일환으로, 그 중 첫번째로 선보인 플랫폼이다. Nasdaq Linq는 Nasdaq 자체의 기술진들과 Chain.com, IDEO 등의 기업들과의 협력을 통하여 개발되었다.

Nasdaq은 이어서 2015년 12월 30일, Nasdaq Linq 시험운영의 일부 결과를 발표하였다. 이 발표에서 Nasdaq은 Chain.com사가 Nasdaq Linq의 블록체인 원장 기술을 이용하여 비공개 주식의 거래와 그 기록을 성공적으로 완결지을 수 있었으며, 이 성공은 주식시장에서의 블록체인 기술의 적용을 위한 중요한 개념증명(proof of concept)을 제공하는 것이라고 언급하였다. 또한 이것은 블록체인 기술이 주식시장에서 결제에 소요되는 시간, 그리고 그에 따른 위험 노출을 99%까지 줄일 수 있는 잠재력을 갖고 있음을 보여주는 것이라고 언급하였다.

이와는 별도로 Nasdaq은 주주의 의결권 행사에 있어서 전자투표 서비스를 블록체인 기반으로 제공하는 방안을 개발하고 있으며, 그 일환으로 2016년 2월, 에스토니아 정부와 함께 에스토니아의 탈린거래소(Tallinn Stock Exchange) 상장기업을 대상으로 시험운영(pilot)을 시작한다고 발표하였다.<sup>33)</sup> 에스토니아는 이미 국가적으로 ‘e-Residency’라는 전자 신원인증 시스템을 운영하고 있기 때문에 시험운영에 적합한 국가로 판단되었다.

본 프로젝트에서는 e-Residency 시스템을 이용하여 주주 명부를 파악하고, 주주명부를 블록체인을 이용하여 관리할 예정인 것으로 알려져 있다.

또한 2016년 5월에는 ‘Nasdaq Financial Framework’ 계획을 발표하였다. 이것은 시장운영기관들에게 거래의 전 과정에 걸쳐 ‘일관되게 연결된 기술적 기능(seamless tech functionality)’을 제공한다는 것을 비전으로 내세운 계획이다. Nasdaq은 블록체인 기술이 이 프레임워크의 전 과정에 걸친 모든 애플리케이션에 통합될 것이라고 언급하였다. Nasdaq은 이 프레임워크를 전 세계에 걸쳐 100개 이상의 시장운영기관 - 전통적 거래소, 인터딜러브로커, 대체거래시스템, 청산소, 중앙예탁기관(CSD) - 들이 이용 가능하도록 할 계획임을 밝혔다.

나) 호주증권거래소(ASX)<sup>34)</sup>

Nasdaq 외에 블록체인 기술의 도입에 대하여 적극적인 움직임을 보이고 있는 곳은 호주증권거래소(Australian Securities Exchange: ASX)이다. ASX는 2015년 2월에 자사의 주요 거래 시스템 및 후선업무 인프라를 대체하거나 업그레이드할 계획임을 발표하였고, 이어 11월의 사내 사업위원회(Business Committee)에서 자사의 청산, 결제를 포함한 후선업무 인프라의 업그레이드 혹은 대체에 있어서 블록체인의 도입을 포함한 모든 가능성을 검토하고 있음을 처음으로 언급하였다.

이어서 ASX는 2016년 1월, 블록체인의 도입을 위한 솔루션 개발을 담당할 파트너로 미국의 Digital Asset Holdings를 선정하였다.<sup>35)</sup> Digital Asset은 향후 6~12개월에 걸쳐 블록체인 기술에 기반한 새로운 청산결제 솔루션을 개발하고, 이후 모든 이해관계자들을 대상으로 한 시연을 통하여 현재 ASX가 사용하고 있는 청산결제 시스템인 CHESS를 새로운 블록체인

33) 탈린거래소는 Nasdaq Nordic이 지분의 100%를 소유하고 있다.

34) 본 소절은 다음 문헌들을 참고하여 작성되었다.  
ASX(2015, 2016a, 2016b, 2016c)

35) ASX는 Digital Asset Holdings의 소수지분을 보유한 주주이기도 하다.

기반 시스템으로 대체할 것인지에 대한 의견을 수렴하도록 되어 있다. 이를 위하여 ASX는 시드니 소재 ASX 본사 건물 내에 ‘acceler8’이라고 명명된 블록체인 플랫폼 시연을 위한 전시장을 설치하였다. ASX는 2017년에 후선업무 인프라에 대한 최종적인 결정을 내릴 예정이다.

#### 다) 일본거래소그룹(JPX)

일본거래소그룹(Japan Exchange Group: JPX)은 2016년 2월, 블록체인 기술의 자본시장 도입 가능성을 검토하기 위한 개념증명 테스트를 IBM Japan과 공동으로 시작한다고 발표하였다(JPX, 2016a). 본 테스트는 비공개주식과 같이 거래가 많지 않은 유통시장에서 블록체인을 도입할 경우의 기술적 한계와 가능성에 대한 평가를 실시하는 것이 목적이다. JPX는 이어서 4월에 또 하나의 개념증명 테스트를 노무라연구소(Nomura Research Institute)와 공동으로 시작한다고 발표하였다(JPX, 2016b).

#### 라) 기타

유럽의 7개 금융회사는 중소기업들을 위한 저비용의 거래후 결제(post-trade settlement) 서비스를 블록체인 기반으로 제공하는 것을 목표로 공동의 노력을 기울이기로 합의하는 양해각서(MOU)를 체결하였다(CoinDesk, 2016o).<sup>36)</sup>

영국의 런던거래소(London Stock Exchange: LSE), 미국의 CME 등의 기관들은 ‘Post Trade Distributed Ledger Working Group’이라는 명칭의 블록체인 기술의 자본시장 도입을 논의하기 위한 워킹그룹을 형성하였다(CoinDesk, 2015b).<sup>37)</sup>

36) 7개의 참여 금융기관은 다음과 같다. BNP Paribas Securities Services, Caisse des Dépôts, Euroclear, Euronext, S2iEM, Société Générale, Paris EUROPLACE

37) 참여 기관은 다음과 같다. CME Group, Euroclear, LCJ.Clearnet, London Stock Exchange, Société Générale, UBS

러시아에서도 은행을 비롯한 금융회사들이 블록체인 기술의 도입에 초점을 맞춘 민간 컨소시엄을 발족시켰다(CoinDesk, 2016p). 이 컨소시엄은 블록체인 기술의 도입을 위한 개념증명, 공동연구 및 정책홍보, 기술표준의 정립을 위하여 공동의 노력을 해 나갈 것이라고 발표하였다.

중국에서는 2016년 4월, Wanxiang Blockchain Labs의 주도로 ChinaLedger라는 명칭의 중국의 독자적인 오픈소스 블록체인 플랫폼 개발을 위한 연합인 ChinaLedger Alliance가 발족되었다(Bitcoin Magazine, 2016b). 이 연합에는 11개 중국 지역상품거래소 및 증권거래소들이 참여하고 있으며, 중국증권업협회(Securities Association of China: SAC)의 인터넷보안위원회(Internet Securities Commission)가 자문역할로 참여한다. 또한 2016년 5월에는 31개의 금융 및 IT 회사들의 블록체인 연합체인 'Financial Blockchain Shenzhen Consortium'이 발족하였다(CoinDesk, 2016q).

개별 금융회사 차원에서 미국의 BoA는 은행으로서 블록체인 중에서도 특히 암호화통화와 관련된 부분에서의 기술 개발에 집중하고 있으며, 그 결과 블록체인 관련 특허를 다수 보유하고 있다. 2015년 12월에 10개의 특허를 출원한 데 이어서, 2016년 1월에는 다시 15개의 특허를 출원하면서, 향후 20개의 추가적 특허출원을 준비하고 있다고 발표하였다. BoA는 R3CEV의 초기 참여기관으로서(<표 III-1> 참조), 블록체인 기술에 많은 관심을 갖고 집중하고 있다.<sup>38)</sup>

## 2) 자본시장 규제당국의 대응 동향

주요국의 자본시장 규제당국 중에서 아직까지 자본시장에서의 블록체인

38) BoA가 보유하고 있는 블록체인 및 암호화통화 관련 특허 중 몇 가지를 소개하면 다음과 같다.

- Cryptocurrency Offline/Online Vault Storage System
- Cryptocurrency Transaction Validation/Payment System
- Cryptocurrency Electronic Payment System
- Cryptocurrency Suspicious User Alert System
- Cryptocurrency Real-Time Conversion System

기술의 도입과 관련하여 구체적인 규제상의 변화를 실행했거나 계획하고 있는 곳은 없다. 아직 자본시장의 어느 부분에 어떤 모습으로 도입될 것인지가 불확실하고 모색 중인 상황이기 때문에 각국의 규제당국들은 블록체인 기술의 내용 및 잠재력·가능성을 평가하고, 현재 진행 중인 자본시장에의 도입 논의를 지켜보면서 진행 동향을 파악하고, 여기에서 얻어진 정보와 지식을 기반으로 향후 규제당국이 취해야 할 방향에 대한 큰 원칙에 대한 언급 정도만 하고 있는 상황이다.

미국의 SEC는 2015년 12월, Overstock.com사가 자신의 주식을 자신이 개발한 블록체인 플랫폼인 TØ를 통하여 발행하겠다는 계획을 승인하는 등, 블록체인 기술에 대해서는 전향적인 입장을 취하고 있다. 최근 SEC의 장 Mary Jo White는 SEC의 현행 규제체제 하에서 일반사무관리회사(transfer agent)나 결제기관(clearing agent)과 같이 블록체인 기반의 자본시장 애플리케이션을 등록(registration)하도록 하는 것이 필요한 것인지의 여부를 판단하는 것이 현재의 핵심 이슈라고 언급한 바 있다(SEC, 2016).

US Commodity Futures Trading Commission (CFTC)의 J. Christopher Giancarlo 의장(CFTC, 2016a, 2016b)은 블록체인과 같은 새로운 기술이 잘 활용될 수 있도록 하기 위해서는 규제 때문에 혁신이 제약받지 않도록 소위 'Do No Harm'이라는 규제접근방식을 취해야 한다고 언급하였다. 즉, 혁신은 민간부문이 선도하고, 규제당국은 혁신에 걸림돌이 되지 않도록 하면서 예측가능하고, 일관성이 있으며, 명확한 법적 환경을 제공해야 하며, 이를 위해서 세계 각국의 규제당국은 긴밀한 조정을 통해 원칙중심(principle-based)의 규제가 이루어지도록 협력해야 한다는 것이다.

유럽의 ESMA(2016)는 후선업무에 블록체인 기술이 도입, 사용될 경우 현행 EU의 규제상 어떤 부분에서 어떤 규제를 받게 되는지를 시나리오별로 검토하였다. 즉, 청산, 결제, 기록관리 등의 부분이 블록체인 기반으로 이루어질 경우 어떤 규제가 적용되는지를 검토한 것으로, 구체적인 기술적 내용이 정해지지 않은 현 시점에서 블록체인 기반이 갖는 차별성을 규제에 어떻게 반영할 것인지에 관한 것은 아니다. 다만 현행 규제의 대상이 되는

‘현행 시스템’의 자리에 ‘블록체인 기반’을 대입하여 검토한 내용이다. 첫째로 장외파생상품 거래 청산의 경우, 유럽시장인프라규제(European Market Infrastructure Regulation: EMIR)의 규정에 따라 CCP를 통하여 청산하여야 하는 장외파생상품은 블록체인 기반에서도 여전히 CCP를 통하여야 한다. 그렇지 않은 장외파생상품은 거래상대방 상호간의 자료 교환 의무를 적용한다. 둘째로 장내파생상품의 청산은 CCP를 통하는 것이 의무이기 때문에, 블록체인 기반에서도 여전히 CCP가 필요하다. 셋째로 결제의 경우, 회원국 자국의 증권결제시스템으로 지정되지 않은 블록체인 네트워크에 의한 증권거래의 결제에는 SFD(Settlement Finality Directive)가 적용되지 않을 것이며, 동시에 이 블록체인 네트워크는 중앙예탁기관(CSD)이 될 수 없다. 이와 같은 ESMA(2016)의 보고서 내용은 블록체인 기반의 플랫폼이 자본시장에 도입되는 데 있어서 규제상 검토와 보완 혹은 수정이 필요한 부분이 어디인지를 보여준다고 할 수 있다.

### 3. 국내 기관의 블록체인 기술 도입 동향

자본시장에의 블록체인 기술의 도입과 가장 직접적으로 관련되고, 따라서 가장 가시적인 움직임을 보이고 있는 기관은 한국거래소(KRX)이다. 한국거래소는 2016년 3월, 창업지원센터를 통하여 스타트업을 비롯한 비공개 기업 주식의 장외거래플랫폼인 KPM(KRX Private Market) 사업 추진을 밝혔다. 그리고 이 KPM을 블록체인 기술 기반으로 설계하여 만들겠다는 것이 한국거래소의 계획이다. 이를 위하여 한국거래소는 2016년 4월, IT 부서에 블록체인의 도입을 위한 기술적 방향을 결정하기 위한 전담 TF를 구성하여 사업을 추진하고 있다(신재룡, 2016; 매일경제, 2016; 디지털타임스, 2016).

한편 이보다 앞서 LG CNS는 2015년 11월 국내에서는 최초로 블록체인 기반의 ‘비상장주식 유통 플랫폼’을 개발하였다고 발표하였다. 이 개발

프로젝트에는 바이터그룹, 블로코, 슈퍼스트링, 스마트포캐스트, 오메카 등 5개의 스타트업이 참여하였으며, 본 플랫폼을 통하여 이들 5개 스타트업의 예탁결제원 미등록 주식을 전자증권으로 발행하는 데 성공하였다고 발표하였다(LG CNS, 2015).

한국거래소나 LG CNS의 거래 플랫폼이 정상적으로 작동하기 위해서는 디지털증권, 즉 전자증권의 발행과 유통에 관한 법적 근거가 확보되어야 하는 바, 2016년 3월에 제정된 「주식·사채 등의 전자등록에 관한 법률」이 시행되면 본격적으로 활성화될 것으로 기대하고 있다.

이 외에 국내에서는 주로 은행들을 중심으로 자사 서비스에 블록체인을 도입하려는 시도가 활발하게 일어나고 있으며, 주요한 사례들은 <표 III-3>에 정리되어 있다.

**<표 III-3> 국내 금융회사의 블록체인 도입 사례**

회사명	주요 내용
한국예탁결제원	Hyperledger 프로젝트 가입
코스콤	장외채권거래 시스템 개념증명
KB국민은행	해외송금서비스 개발: 개념증명 성공 비대면 실명확인 증빙자료 보관시스템
신한은행	외환송금 시스템 개발
KEB하나은행	해외송금서비스 시스템 개발
NH농협은행	블록체인 기술의 사내업무 적용방안 검토
IBK기업은행	금융서비스 개발을 위한 업무협약 체결
전북은행	간편로그인 서비스에 블록체인 기술 탑재
대신증권	블록체인 분야 업무협약 체결

자료: 언론보도 및 각사 보도자료

## IV. 종합 및 시사점

---

1. 자본시장 업계에의 시사점
2. 정책·규제당국에의 시사점



## IV. 종합 및 시사점

이상에서 살펴본 바와 같이 블록체인에 대해서는 혁신적이며 높은 가능성을 지니고 있는 기술이고, 자본시장과 금융 그리고 이를 넘어서 사회 각 분야의 다양한 서비스에서 활용 가능성이 매우 높으며, 획기적인 변화를 가져올 수 있는 기술이라는 평가에는 거의 의견이 일치하는 것으로 보인다. 그렇지만 현재 블록체인 기술이 와 있는 지점은 이러한 기대가 실현되기까지는 아직 해결되어야 할 과제들이 많다는 데에도 역시 대부분의 의견이 일치하고 있다. 블록체인 기술의 자본시장 도입·활용이라는 측면에서의 현재 상황은 자본시장 비즈니스 프로세스 중의 어느 부분에 어떤 형태로 도입되는 것이 가장 효과적인지를 모색 중이고, 블록체인 기술의 적용을 위한 다양한 개념증명 시도가 진행 중인 단계라고 정리할 수 있다. R3CEV, Hyperledger 프로젝트 등도 아직까지는 어디에 어떻게 도입할 것인지를 모색하고, 기술적 실현 가능성을 테스트하며, 개념증명을 만들어내고 있는 단계이다. 개념증명 단계를 넘어 블록체인 기술을 적용한 자본시장 플랫폼 혹은 애플리케이션이 본격적으로 등장하기까지는 향후 2~3년이 소요될 것이라는 것이 다수 전문가 그리고 관련 기관들의 공통된 견해이다(DTCC, 2016b; McKinsey, 2016; Morgan Stanley, 2016; Oliver Wyman and J.P. Morgan, 2016). 우리나라에서도 많은 금융회사, 자본시장 유관기관들과 블록체인 스타트업들이 노력을 경주하고 있으며, 정책·규제당국 역시 관심을 갖고 동향을 주시하고 있다. 본장에서는 이러한 상황에서 블록체인 기술의 자본시장에의 도입과 관련하여 고려하여야 할 시사점들을 정리하여 제시한다. 먼저 자본시장 업계에 주는 시사점을 설명하고, 다음으로 정책·규제당국에 주는 시사점을 정리한다.

## 1. 자본시장 연계에의 시사점

블록체인 기술을 자본시장에 도입하여 활용하는 데 있어서는, 그 기술이 거래 부분에 도입되든 후선업무에 도입되든, 어느 하나의 회사가 홀로 노력한다고 되는 일은 아니며 산업 전체 차원에서의 공동의 노력과 협력이 반드시 필요하다. 왜냐하면 블록체인 기술은 자본시장 인프라에 도입되며, 이 인프라는 증권회사 등 거의 대부분의 자본시장 참여기관이 이용하게 될 것이기 때문이다. III장에서 소개한 R3CEV도 이러한 이유에서 조직된 컨소시엄이다. 우리나라에서도 개별 회사 차원이 아닌 산업 전체 차원에서의 논의·조정·합의를 위한 기구가 구성되는 것이 필요하다.

이 기구에는 거래소, 예탁결제원과 같은 자본시장 인프라기관, 증권회사, 자산운용회사와 같은 자본시장의 주요 참여자들, 그리고 블록체인 기술기업(주로 스타트업)들이 핵심적으로 포함될 것이며, 정책·규제당국 역시 함께 참여하는 것이 필요하다.

이 기구에서 논의되고 합의가 도출되어야 하는 핵심적인 의제로는 다음과 같은 것들이 있다.

- ① 자본시장의 일련의 프로세스 중 블록체인 기술을 도입할 부분 혹은 기능
- ② 요구되는 기술표준
- ③ 만들어질 블록체인 네트워크의 지배구조
- ④ 참여기관(블록체인의 노드)들의 서로 다른 유인 및 이해 조정
- ⑤ 블록체인 네트워크 구축 소요비용 분담

개별 회사 차원에서 자사의 어떤 서비스를 사적(private) 블록체인 기반으로 구축하려고 하는 경우에는, 블록체인 기술을 사용하는 것이 기존의 기술을 사용하는 것보다 유리하다는 확고한 근거가 있어야 한다. Accenture(2016)는 다음과 같은 경우에 블록체인 기술을 사용하는 것이 유용할 수 있다고 제안하고 있다. 첫째로, 다수의 참여자와 다수의 데이터

저장소(data storage)가 존재하며, 원장의 대사(reconciliation)가 필요한 서비스 혹은 기능이다. 둘째로, 감사 및 규제당국에의 보고 목적상 변조 불가능(immutable)하고 신뢰성 있는 재무회계의 역사적 자료의 필요성이 높은 경우이다. 셋째로 데이터 보안성과 데이터 접근에 대한 통제가 중요한 경우이다.

블록체인 기술을 적용한 어떤 새로운 플랫폼 혹은 애플리케이션이 등장한다고 해서 그것이 기존의 것을 대체할 가능성은 높지 않다. DTCC(2016a)의 견해에서도 나타난 바와 같이, 기존의 ‘제3자 기관’ 시스템이 갖는 강점이 있고, 또 기존의 시스템에서 제3자 기관이 관리하던 원장을 블록체인 네트워크상에 공개·분산시키는 데에도 많은 난점이 존재하기 때문이다. 블록체인 기반의 새로운 플랫폼 혹은 애플리케이션은 어떤 새로운 거래 플랫폼 혹은 서비스를 설계할 때 채택, 적용되는 방식으로 등장할 가능성이 높다.

## 2. 정책·규제당국에의 시사점

자본시장에서의 블록체인 기술의 도입과 관련하여 정책·규제당국이 해야 할 가장 핵심적인 역할은 규제적 불확실성을 최소화하여 블록체인의 도입 논의, 그리고 도입을 통한 혁신이 방해받지 않도록 하는 것이다.

우선 블록체인 기술의 도입과 관련하여 법적·제도적 기반이나 근거가 필요한 경우, 이를 마련해 주는 것이 필요하다. 여기에는 예를 들면 디지털증권, 혹은 암호화증권의 발행과 유통, 결제수단이 되는 암호화통화(혹은 토큰)의 발행과 유통을 위한 법적 근거의 마련이 포함될 것이다. 또한 블록체인 기반 거래 플랫폼이 등장할 경우 이 플랫폼의 법적 지위를 어떻게 규정할 것인지에 대해서도 도입의 진행에 맞추어 입장을 명확하게 정립해 놓는 것이 필요하다.

현행의 법령이나 규제들은 대부분 기존의 ‘제3자 기관’ 시스템을 암묵적으로

전제하고 만들어진 것이기 때문에 블록체인 기반의 새로운 시스템의 성격과는 맞지 않는 부분이 다수 나타날 가능성이 높다. 예를 들면 「전자금융거래법」 및 「전자금융감독규정」에서 정하고 있는 금융보안에 관한 세부조항들이 블록체인 기반의 시스템이 등장할 경우에 어떻게 적용될 것이며, 어떤 영향을 미칠 것인지를 면밀하게 검토하여 제도 및 규제와 블록체인 시스템 간의 정합성을 높이도록 해야 할 것이다.

법적·규제적 불확실성을 효과적으로 제거하기 위해서, 정책·규제당국은 블록체인 기술의 본질 및 특성, 현재 진행되고 있는 자본시장에의 도입 논의의 내용, 기술 개발이 어느 정도까지 진행되었는지 등 현재의 동향을 실시간으로 파악하고 있어야 한다. 이를 위해서는 블록체인 기술의 도입을 진행하고 있는 업계와의 상시적인 긴밀한 소통이 필수적이며, 민간 업계의 협의체가 구성될 경우 함께 참여하는 것이 바람직하다. 대다수의 해외 기관들 역시 민간 업계와 정책·규제당국 간의 긴밀한 의사소통의 중요성을 강조하고 있다.

자본시장에의 블록체인 기술의 도입을 선도하거나 장려하는 것은 정책·규제당국의 역할이 아니며, 민간 업계의 역할이다. 정책·규제당국의 역할은 이미 언급한 바와 같이 규제적 불확실성을 제거하여 도입에 장애가 되지 않도록 하는 것, 그리고 동시에 새로운 블록체인 기반 플랫폼 혹은 시스템이 자본시장에서 사용될 경우 안정성, 투자자 보호 등에서 기존 시스템과 최소한 동일한 수준을 달성하도록 담보하는 것이다. 현재 도입 방식, 기술 표준 등에 대한 논의가 진행 중이고, 개념증명을 위한 테스트가 진행되고 있는 초기 단계라는 점을 고려하면 특히 첫번째 역할이 중요하다고 생각된다. 이 역할과 관련해서 III장에서 간단하게 언급한 CFTC의 J. Christopher Giancarlo 의장(CFTC, 2016b)의 ‘Do No Harm’ 접근방식의 제언은 좋은 참고가 된다. 보다 구체적으로 Giancarlo 의장은 다음과 같은 다섯 가지 규제 단계(regulatory step)를 제안하고 있다.

- ① 블록체인 핀테크기업들과 협력하며 의사소통할 수 있는 전담 기술 전문가팀 구성

- ② 블록체인 핀테크기업들이 실패할 경우의 책임에 대한 우려 없이 혁신적 솔루션을 자유롭게 개발하여 테스트할 수 있는 규제당국과의 협력의 장 마련<sup>39)</sup>
- ③ 규제당국은 기술혁신에 대한 이해를 높이고, 이 혁신이 효과적이고 효율적인 규제집행에 도움이 되는지를 판단하기 위하여 핀테크 기업의 개념증명 단계부터 직접적으로 참여
- ④ 핀테크기업을 비롯한 업계의 의견 경청
- ⑤ 글로벌 협력

---

39) 영국 금융 감독청(Financial Conduct Authority: FCA)의 ‘Sandbox’를 예로 들고 있다.



## 참 고 문 헌

---



## 참 고 문 헌

- 금융보안원, 2015a, 블록체인 개요 및 활용사례, 2015. 6. 24.
- 금융보안원, 2015b, 국내외 금융분야 블록체인 활용 동향, 2015. 11. 23.
- 금융보안원, 2015c, 블록체인 및 비트코인 보안 기술, 2015. 11. 23.
- 금융보안원, 2016, 이더리움(Ethereum) 소개 및 특징 분석, 2016. 3. 4.
- 김동섭, 2016, 분산원장 기술과 디지털통화의 현황 및 시사점, 『지급결제 조사자료』 2016-2, 한국은행.
- 김석원, 2016, 비트코인의 기반 기술 블록체인의 원리, 소프트웨어기술연구소.
- 김예구, 2015, 블록체인 기술과 금융의 변화, 『KB 지식 비타민』 15-91호, KB금융지주 경영연구소.
- 김자봉, 2014, 비트코인 거래 메커니즘의 분석과 시사점, 『KIF VIP 시리즈』 2014-11, 한국금융연구원.
- 김진화, 2015, 모든 거래 기록된 장부 블록체인, 진정한 P2P 시대 여는 인터넷의 미래, 『동아비즈니스리뷰』 No.187.
- 김진화·정명호·김재모·유영석, 2016, 블록체인의 기술적 이해 및 도입을 위한 첫걸음, (주)코빗.
- 김태우, 2016, 블록체인이 자본시장에 미치는 영향, 『예탁결제』 제97호, 한국예탁결제원.
- 디지털타임스, 2016. 3. 15, 사적시장에 블록체인 기술 도입.
- 류한석, 2015, 플랫폼의 플랫폼, 이더리움의 시사점, 디지에코 보고서 2015. 9. 16.
- 매일경제, 2016. 2. 28, 장외주식 ‘블록체인’ 사흘 걸리던 대금결제 하루만에 OK.

신재룡, 2016, 자본시장에서의 블록체인 동향 및 거래소 대응방안, 블록체인 현황과 자본시장에의 활용 세미나 발표자료.

한국예탁결제원, 2014, 『증권예탁결제제도』, 박영사.

한국예탁결제원, 2016. 7. 28, 한국예탁결제원 하이퍼렛저 블록체인 프로젝트 참여, 보도자료.

LG CNS, 2015, LG CNS, 블록체인 기반 국내 최초 전자증권 발행. <http://blog.lgcns.com/962>, 2015. 11. 23

Accenture, 2015, Blockchain in the Investment Bank.

Accenture, 2016, Blockchain-Enabled Distributed Ledgers: Are Investment Banks Ready?

Antonopoulos, A.M., 2014, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media.

Australian Securities Exchange (ASX), 2015, Minutes of the Business Committee, November 26.

Australian Securities Exchange (ASX), 2016a, ASX Selects Digital Asset Holdings LLC, Media Release, January 22.

Australian Securities Exchange (ASX), 2016b, Business Committee Agenda, February 17.

Australian Securities Exchange (ASX), 2016c, Adopting Blockchain in Our Financial Markets: ASX Plans and the Benefits for the Market, Speech by ASX Deputy CEO at the Annual Stockbrokers Conference, June 1.

Bank for International Settlements - Committee on Payments and Market Infrastructures (BIS), 2015, Digital Currencies.

- Bitcoin Magazine, 2016a, Blockstream, Bloq, Gem, ItBit, Thomson Reuters and Others Join the Linux Foundation's Hyperledger Project, Mar 31.
- Bitcoin Magazine, 2016b, China Joins the Blockchain Race with ChinaLedger Alliance, May 2.
- Bloomberg, 2015, Nasdaq Seeks to Show Progress Using Much-Hyped Blockchain, December 30.
- Business Wire, 2016, MIT Adopts Ripple Validator to Advance Consensus and Blockchain Research, April 12.
- Buterin, V., 2014, Ethereum: A Next Generation Cryptocurrency and Decentralized Application Platform.  
<https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211>
- Buterin, V., 2016, White Paper: A Next Generation Smart Contract and Decentralized Application Platform.  
<https://github.com/ethereum/wiki/wiki/White-Paper>
- CoinDesk, 2013, 10 Things You Need to Know about Ripple, May 17.
- CoinDesk, 2015a, Ripple Labs Joins Cross-Border Payments Association, March 5.
- CoinDesk, 2015b, CME, London Stock Exchange Form Blockchain Settlement Group, November 17.
- CoinDesk, 2016a, State of Bitcoin and Blockchain 2016.  
<http://www.coin-desk.com/research/stte-bitcoin-blockchain-2016>
- CoinDesk, 2016b, Microsoft Certifies Ethereum Offering in Blockchain Service First, March 1.

CoinDesk, 2016c, Microsoft Adds Ethereum to Windows Platform for over 3 Million Developers, March 30.

CoinDesk, 2016d, The DAO: Or How a Leaderless Ethereum Project Raised \$50 Million, May 12.

CoinDesk, 2016e, Public Opinion Split as the DAO Rakes in Ethereum Funding, May 18.

CoinDesk, 2016f, The DAO Attacked: Code Issue Leads to \$60 Million Ether Theft, June 17.

CoinDesk, 2016g, Ripple Adds 7 New Financial Institutions as Tech Partners, June 22.

CoinDesk, 2016h, R3 Announces New Distributed Ledger Technology Corda, April 5.

CoinDesk, 2016i, Brazil's Bank Itaú Joins R3 Blockchain Consortium, April, 25.

CoinDesk, 2016j, R3 Bank Partner Northern Trust Details Four Internal Blockchain Tests, May 16.

CoinDesk, 2016k, Chinese Finance Giant Joins R3 Blockchain Consortium, May 24.

CoinDesk, 2016l, R3 Adds Life Insurance Firm AIA to Blockchain Consortium, June 2.

CoinDesk, 2016m, CFTC Commissioner: Agency Should Revisit Rules for Distributed Ledgers, March 29.

CoinDesk, 2016n, SEC Chair: Agency 'Actively Exploring' Blockchain Regulation, April 1.

CoinDesk, 2016o, 7 Financial Firms to Build Post-Trade Blockchain for Small Businesses, June 22.

- CoinDesk, 2016p, Russian Finance Firms Form Blockchain Consortium, July 1.
- CoinDesk, 2016q, 31 Chinese Firms Form Financial Blockchain Consortium, June 24.
- CoinDesk, 2016r, Goldman Sachs: Blockchain Tech Could Save Capital Markets \$6 Billion a Year, May 25.
- Coinspeaker, 2016a, R3CEV Develops Eight Proofs-of-Concept for Blockchain Trials, April 14.
- Coinspeaker, 2016b, Bank of America Files for 20 New Blockchain-Related Patents, January 28.
- Cryptocoinsnews, 2016, R3 Consortium's Blockchain Initiative: What Makes 'Corda' Different?, June 4.
- Deloitte, 2016, Blockchain: Enigma, Paradox, Opportunity.
- DTCC, 2016a, *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape, A White Paper to the Industry.*
- DTCC, 2016b, 2016 Blockchain Symposium.  
<http://www.dtcc.com/>
- DTCC, 2016c, Consolidated Financial Statements as of and for the Years Ended December 31, 2015 and 2014.
- DTCC, 2016d, Successful Blockchain Test Completed by Axoni, DTCC, Markit, and Multi-Bank Working Group, Press Release, April 7.
- Economist, 2015a, The Trust Machine, Oct 31.
- Economist, 2015b, The Great Chain of Being Sure about Things, Oct 31.

Economist, 2016a, Hype Springs Eternal, Mar 19.

Economist, 2016b, Craig Wright's Claims to Be Satoshi Nakamoto Come under Fire, May 2.

Economist, 2016c, Theft Is Property, June 25.

Economist, 2016d, Not-so-clever Contracts, July 30.

Econotimes, 2016, SBI Holdings First to Join R3 Blockchain Consortium's Second Round of Partnerships, March 16.

Euroclear, 2016, Blockchain: How the Capital Markets Industry Should Respond.

Euroclear and Oliver Wyman, 2016, Blockchain in Capital Markets: The Prize and the Journey, February 26.

European Securities and Markets Authority (ESMA), 2015, Call for Evidence; Investment Using Virtual Currency or Distributed Ledger Technology, April 24.

European Securities and Markets Authority (ESMA), 2016, The Distributed Ledger Technology Applied to Securities Markets, ESMA Discussion Paper ESMA/2016/773.

Evans, D.S., 2014, Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms, University of Chicago Coase-Sander Institute for Law and Economics Working Paper No. 685.

Financial Times, 2015a, Blockchain Initiative Backed by 9 Large Investment Banks, September 15.

Financial Times, 2015b, Blockchain Initiative Pulls in Another 13 Banks, September 30.

- Financial Times, 2016, Banks Claim Blockchain Breakthrough in Money Transfer, June 22.
- Finextra, 2016, Ripple and Expertus Team up for Blockchain Testing Service, June 6.
- Forbes, 2015, Nasdaq Unveils Blockchain-Enabled Platform Linq, Announces 6 Inaugural Clients, October 27.
- Goldman Sachs, 2015, What if I Told You ..., Emerging Theme Radar, December 2.
- Harvey, C.R., 2014, Bitcoin Myths and Facts.  
<http://ssrn.com/abstract=2479670>
- Harvey, C.R., 2016, Cryptofinance.  
<http://ssrn.com/abstract=2438299>
- ITNOW, 2016, Blockchain: Double Bubble or Double Trouble?, March 2016.
- Japan Exchange Group (JPX), 2016a, Commencement of Proof of Concept Testing for Blockchain Technology, February 16.
- Japan Exchange Group (JPX), 2016b, Commencement of Proof of Concept Testing for Blockchain Technology, April 7.
- Lamport, L., Shostak, R., Pease, M., 1982, The Byzantine Generals Problem, *ACM Transactions on Programming Language and Systems* 4, 382-401.
- LCH.Clearnet, 2016, Consolidated Financial Statements for the Year Ended 31 December 2015.
- Lee, L., 2016, New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, University of Utah S.J. Quinney College of Law Research Paper No.138.

Linux Foundation, 2015, Linux Foundation Unites Industry Leaders to Advance Blockchain Technology, December 17.

Linux Foundation, 2016a, Hyperledger Whitepaper.

[https://docs.google.com/document/d/Z4M\\_qwILLRehPbVRUsJ3OF8lir-gqS-ZYe7W-LE9gnE/edit?pref=2&pli=1#heading=h.m6iml6hqrnm2](https://docs.google.com/document/d/Z4M_qwILLRehPbVRUsJ3OF8lir-gqS-ZYe7W-LE9gnE/edit?pref=2&pli=1#heading=h.m6iml6hqrnm2)

Linux Foundation, 2016b, Hyperledger Project Charter.

<https://www.hyperledger.org/about/charter>

Linux Foundation, 2016c, Hyperledger Projects Maintains Strong Momentum with New Members, June 22.

London Stock Exchange Group, 2016, The Process of Trading.

<http://www.lseg.com/investor-relations/group-glance/process-trading>

McKinsey&Company, 2015, Beyond the Hype: Blockchains in Capital Markets, McKinsey Working Papers on Corporate & Investment Banking No. 12, December.

Morgan Stanley Research, 2016, Blockchain in Banking: Disruptive Threat or Tool?, Global Insight April 20.

Nakamoto, S., 2008, Bitcoin: A Peer-to-Peer Electronic Cash System.

<https://bitcoin.org/bitcoin.pdf>

Nasdaq, 2015a, Nasdaq Announces Inaugural Clients for Initial Blockchain-Enabled Platform 'Nasdaq Linq,' October 27.

Nasdaq, 2015b, Nasdaq Linq Enables First-Ever Private Securities Issuance Documented with Blockchain Technology, Press Release, December 30.

- Nasdaq, 2016a, Nasdaq's Blockchain Technology to Transform the Republic of Estonia's e-Residency Shareholder Participation, Press Release, February 12.
- Nasdaq, 2016b, Nasdaq Debuts Groundbreaking Nasdaq Financial Framework, Enhancing Operations for Over 100 Market Operators Globally, Press Release, May 26.
- Nomura Research Institute, 2016, Survey on Blockchain Technologies and Related Services, FY2015 Report.
- Oliver Wyman, J.P. Morgan, 2016, Unlocking Economic Advantage with Blockchain: A Guide for Asset Managers.
- PwC, 2016, What's Next for Blockchain in 2016?, PwCFinTech, January.
- R3, 2015, R3's Distributed Ledger Initiative Grows to 42 Bank Members and Looks to Extend Reach to the Broader Financial Services Community, Press Release, December 17.
- R3, 2016a, R3 Brings Eleven Major Global Financial Institutions Together on a Cloud Based Distributed Ledger, Press Release, January 20.
- R3, 2016b, Microsoft and R3 Partnership to Accelerate Adoption of Distributed Ledger Technology by Global Banks, Press Release, April 4.
- R3, 2016c, Introducing R3 Corda: A Distributed Ledger Designed for Financial Services, April 5.
- Ream, J., Chu, Y., Schatsky, D., 2016, Upgrading Blockchains: Smart Contract Use Cases in Industry, Deloitte University Press.
- Reuters, 2015, Nine of World's Biggest Banks Join to Form Blockchain Partnership, September 15.

- Ripple, 2015, Implementing the Interledger Protocol in Ripple, October 6.
- Ripple, 2016, Ripple Strikes Multi-National Deal with SBI Holdings to Meet Growing Demand for Ripple Solutions across Area, January 29.
- Securities and Exchange Commission (SEC), 2016, Keynote Address at the SEC-Rock Center on Corporate Governance Silicon Valley Initiative by Chair Mary Jo White, March 31. <https://www.sec.gov/news/speech/chair-white-silicon-valley-initiative-3-31-16.html>
- Swan, M., 2015, *Blockchain: Blueprint for a New Economy*, O'Reilly Media.
- SWIFT Institute, 2016, The Impact and Potential of Blockchain on the Securities Transaction Lifecycle, SWIFT Institute Working Paper No. 2015-007.
- TATA Consultancy Services, 2015, Blockchain Technology- Transforming Transaction Processing in Capital Markets.
- The Finanser, 2016, The Finanser Interviews: Chris Larsen, CEO and Cofounder, Ripple Labs, July 6.
- Thomas, S., Schwartz, E., 2015, A Protocol for Interledger Payments. <https://interledger.org/interledger.pdf>
- UK Government Office for Science, 2015, *Distributed Ledger Technology: beyond Block Chain*.
- US Commodity Futures Trading Commission (CFTC), 2016a, Regulators and the Blockchain: First, Do No Harm, Special Address of CFTC Commissioner J. Christopher Giancarlo before the DTCC 2016 Blockchain Symposium, March 29.

US Commodity Futures Trading Commission (CFTC), 2016b, Blockchain: A Regulatory Use Case, Keynote Address of Commissioner J. Christopher Giancarlo before the Markit Group 2016 Annual Customer Conference, May 10.

Wood, G., 2014, Ethereum: A Secure Decentralised Generalised Transaction Ledger.

<http://gavwood.com/paper.pdf>

비트코인 소개, 가입	<a href="http://bitcoin.org">bitcoin.org</a>
비트코인 통계	<a href="http://bravenewcoin.com">bravenewcoin.com</a>
비트코인 블록체인 통계	<a href="http://blockchain.info">blockchain.info</a>
CoinDesk	<a href="http://www.coindesk.com">www.coindesk.com</a>
Ethereum	<a href="http://www.ethereum.org">www.ethereum.org</a>
Hyperledger	<a href="http://www.hyperledger.org">www.hyperledger.org</a>
R3CEV	<a href="http://r3cev.com">r3cev.com</a>
Ripple	<a href="http://ripple.com">ripple.com</a>

자  
본  
시  
장  
연  
구  
원



**자본시장연구원**  
Korea Capital Market Institute

서울시 영등포구 의사당대로 143  
T 02.3771.0600 [www.kcmi.re.kr](http://www.kcmi.re.kr)

값 10,000원



9 788960 891517 93320  
ISBN 978-89-6089-151-7