POSRI 이슈리포트

2019.1.10.

기업용 블록체인, 무엇이 다른가?

권보경 수석연구원, 신성장/그룹사업연구센터(bkkwon@posri.re.kr)

목차

posco
포스코경영연구원

Executive Summary

○ **비트코인과 함께 세상에 소개되어 각광을 받고 있으며 우리가 잘 알고 있는 블록체인은 개방형 블록체인**

- 개방형 블록체인은 누구든지 허가 없이 블록체인에 저장된 데이터를 읽고, 쓰고 검증할 수 있는 무허가형 블록체인
- 개방형 블록체인은 분산형 DB 구조를 기반으로 한번 기록된 정보의 변경 불가능성, 익명성 기반의 투명성을 통해 정보의 위조와 변조를 방지

○ **개방형 블록체인은 개인정보보호 관련 국내·외 법적 규제로 기업 비즈니스에 그대로 활용하는 것은 곤란**

- 2018년 5월 25일부로 시행된 유럽연합의 GDPR(General Data Protection Regulation)은 기업이 개인 프라이버시를 보호하도록 광범위한 규정 준수를 강제
- 국내법의 경우 일정기간이 지나면 개인정보의 파기를 명시적으로 규정하므로 기업 입장에서는 실명 기반 거래정보의 중앙통제권 확보가 선결 조건

○ **기업은 개인정보보호를 위해 실명 기반 거래 정보 관리가 가능한 허가형 블록체인을 활용하여 기존 비즈모델 강화 및 신사업 기회 발굴**

- 소수의 컴퓨터를 연결해서 직접 구축하거나 아마존과 MS가 제공하는 클라우드 컴퓨팅 기반의 블록체인 플랫폼 서비스를 대여하여 허가형 블록체인 구축 가능
- 기업의 비즈니스 특성을 고려하여 접근 권한을 맞춤형으로 설계 가능하고 비트코인처럼 해시경쟁 없이도 혁신적인 업무처리 기회 제공
- 허가형 블록체인을 활용하여 글로벌기업은 공급망 관리, 제조혁신, 판매 및 고객 채널 관리, 새로운 Biz. 생태계 구축 등 다양한 성공사례 제시

○ **반면, 실명 거래에 따른 개인 프라이버시 노출 등 허가형 블록체인의 한계를 파악하고 기업별 사업 특성에 맞는 블록체인 기술의 채택과 운영 필요**

- 허가형 블록체인은 개방형 블록체인 대비 기술 혁신 성과의 활용과 보안성 일부 제한 가능
- 개인의 프라이버시 침해 문제를 해결하기 위해서 영지식 증명이라는 암호화 기술, 허가형과 개방형 블록체인을 연계하는 앵커링 기술 등 신기술 개발 진행
- 미래 변화 시나리오를 기반으로 초기 대규모 투자보다는 외부 블록체인 서비스를 활용하여 새로운 비즈니스 모델 시험 및 신사업 창출 전략 추진 필요

1. 분산형 컴퓨팅과 블록체인

□ 블록체인은 인터넷 거래의 이중지불 문제 해결이 가능한 신뢰생성 시스템

○ **Peer-to-Peer 형태의 분산형 컴퓨팅에서 개인 간 가치의 전달과 결재가 어려운 이유는 손쉬운 정보의 복제와 공유 때문**

- 디지털 정보의 최대 장점은 손쉬운 복제성과 인터넷 네트워크를 통한 전달 및 거래 가능성
- 기존 인터넷은 개인과 개인 간 정보 공유는 가능하지만 중개업체를 거치지 않고는 디지털 화폐를 활용한 개인과 개인 간 가치 지불은 곤란
- 디지털 형태의 화폐를 개인이 복사해서 재활용할 경우 진본을 구분할 수 없다는 이중지불 문제가 Peer to Peer 형태의 가치지불에서 최대의 장애

○ **비트코인과 함께 출현한 개방형 블록체인 기술은 분산처리 환경에서 해킹 및 거래 정보의 위·변조 방지를 통해 Peer-to-Peer 거래의 이중지불 방지 역할 담당**

- 블록체인은 인간이 생산하는 정보를 하나의 블록으로 묶고 그 블록이 꼬리에 꼬리를 물고 연결되는 구조
- 블록체인은 전 세계에 분산되어 있는 수많은 컴퓨터에 분산 저장
- 블록체인에 저장된 정보를 해킹하기 위해서는 전 세계에 분산되어 저장된 정보를 제한된 시간에 모두 변경해야 하므로 현재의 컴퓨터 기술로는 해킹 어려움

○ **비트코인 이후 블록체인을 활용하여 다양한 분야에서 1,000여종의 암호화폐가 세계 시장에서 거래**

2. 개방형 블록체인의 기술적 특징과 활용

□ 개방형 블록체인은 누구든지 허가 없이 참여 가능한 분산형 정보 저장 및 관리시스템

○ **개방형 블록체인은 누구든지 허가 없이 블록체인에 저장된 데이터를 읽고, 쓰고, 검증 가능한 무허가형 블록체인**

- 개인용 컴퓨터에 블록체인 클라이언트 프로그램만 설치하면 누구든지 허가 없이 블록체인에 데이터를 읽고, 쓰고, 검증 가능
- 개방형 블록체인에 참여한 개인의 선택에 따라 어떤 데이터가 입력될 지 투표로 결정하는 역할도 수행
- 참여자는 자신의 컴퓨터 저장공간을 블록체인의 거래정보 저장을 위해 공유하고 사전에 설정된 블록체인 운영 원칙 준수

○ **개방형 블록체인은 분산형 DB구조를 기반으로 기록변경 불가능성, 익명성 기반의 투명성을 통해 정보의 위·변조 방지**

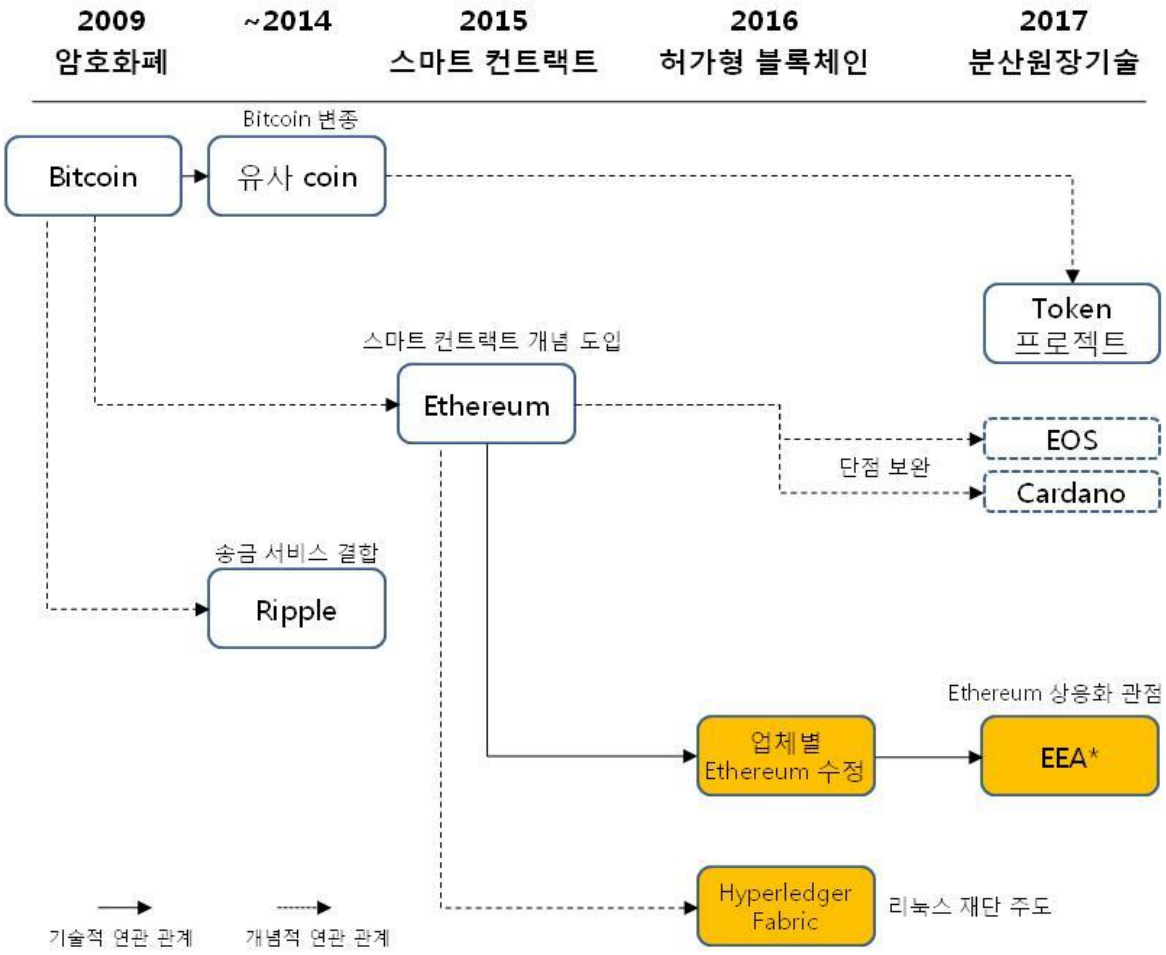
- 블록체인은 각각의 당사자가 모든 이력에 접근 가능하며, 일단 DB에 정보가 입력되면 그 기록은 변경 불가
- 익명성 기반 투명성으로 인해 블록체인에 기록된 모든 거래 정보는 시스템에 접근할 수 있는 모든 사용자가 확인 가능
- 비트코인의 경우 투명하게 공개된 변경 불가능한 속성을 지닌 블록체인 DB의 정보를 현재의 컴퓨터 성능으로 해커가 10분 만에 해킹하는 것은 거의 불가능 수준

□ 비트코인 출현 후 개방형 블록체인은 현재 기술적 발전과 함께 활용 영역 지속 확대

○ **1세대 블록체인은 암호화폐 기능 중심의 비트코인을 시작으로 다양한 알트코인으로 확장**

- 이중지불 방지 기능을 기반으로 비트코인 출현 이후 다양한 종류의 유사 코인 발행 확산
- 초기 블록체인 기술은 송금 서비스와 결합 Ripple과 같은 은행 간 청산과 통신 및 가치의 거래와 이동에 활용
- 최근에는 비트코인 블록체인 기술을 기반으로 디지털 자산의 표현과 거래 등 토큰 형태의 프로젝트로 활용영역 확대

〈그림 1〉 블록체인의 진화 과정



자료: LGCNS, 블록체인 기술동향 및 적용방향, 2018

○ **2세대 블록체인 이더리움은 스마트계약 기능을 강화**

- 2세대 이더리움 블록체인은 비즈니스 환경에서도 활용 가능한 수준의 스마트계약 기능과 가상머신 개념을 도입
- 이론적으로 이더리움 블록체인은 가상머신과 스마트계약 기술을 활용하여 인터넷 공간을 거대한 단일의 분산형 컴퓨터로 운영하는 것이 목표
- 이더리움의 상용화 관점에서 EEA(Enterprise Ethereum Alliance)를 통하여 솔루션 간 호환성을 높이고 프라이버시 보호와 접근성 제어가 가능한 이더리움 호환 프로토콜 구축

○ **2세대 블록체인의 기술적 한계를 극복한 3세대 블록체인도 출현**

3. 개인정보보호와 기업의 블록체인 활용

□ 개인정보보호 관련 국내·외 법적 규제가 기업의 개방형 블록체인 활용에 최대 걸림돌

○ **유럽연합의 GDPR은 온라인에 저장된 개인정보에 대한 정정권과 삭제권을 명시**

- EU의 GDPR(General Data Protection Regulation)은 2016년 5월에 공표되었고, 2018년 5월 25일부로 시행
- GDPR은 EU 거주자의 개인정보를 다루는 기업이나 단체가 개인 프라이버시 보호와 관련된 광범위한 규정들을 준수하도록 강제

[참고] GDPR 개인정보보호 조항

- GDPR 17조 삭제권 관련 내용
  - 개인정보 수집 목적 등과 관련하여 더 이상 불필요한 경우
  - 정보 주체가 동의를 철회하고, 그 처리에 법적 근거가 없는 경우
  - 정보주체가 처리를 반대하고 그 처리에 우선적인 정당한 근거가 없는 경우
  - 개인정보가 불법적으로 처리된 경우
  - 컨트롤러가 EU 또는 회원국 법을 준수하기 위해 삭제하는 경우
  - 정보사회서비스 제공과 관련하여 개인정보가 수집된 경우
- GDPR 16조 정정권 관련 내용
  - 개인정보가 부정확하거나 불완전할 경우 실행

○ **국내법의 경우 일정기간이 지나면 개인정보의 파기를 명시적으로 규정**

[참고] 우리나라 개인정보보호법 개인정보보호 관련 조항

- 개인정보보호법 제21조 1항 개인정보파기 관련 내용
  - 개인정보관리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 됐을 때는 지체 없이 그 개인정보를 파기해야 한다.(파기는 복구 또는 재생되지 않도록 하는 조치)
  - 개인정보의 정정, 삭제에 대해서는 제36조 1항에서 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다.

□ 기업에는 실명 기반 거래정보 관리가 가능한 허가형 블록체인이 적합

○ 탈중앙화된 개방형 블록체인은 기업의 거래정보 기록 및 관리에 부적합

- 금융거래를 실명으로 법제화하는 금융산업의 경우 블록체인의 익명 기반 거래 정보 공개를 실제 금융업무에 적용하기는 곤란
- 기업 입장에서 고객들의 자산과 거래 정보는 비밀관리 대상이므로 개방형 블록체인의 장점인 자유로운 접근성과 투명성을 오히려 단점으로 인식
- 해킹을 방어하기 위한 기록정보의 변경 불가능성은 개인정보보호법에 의거한 고객정보와 거래정보의 삭제 또는 수정을 어렵게 하는 장애 요인

○ 기업의 경우 실명 거래 환경에서 블록체인 운영 주체가 사용자들에게 데이터 읽기, 쓰기 권한을 부여하고 직접 관리 가능한 개인화된 허가형 블록체인 구축 필요

- 허가형 블록체인은 블록체인을 구축하고 운영하는 기업이 주체가 되어 블록체인 생태계 참여자들이 무엇을 할 수 있고 없는지에 대한 결정권 행사 가능
- 개방형 블록체인도 사용자 권한 설정이 가능하지만 합의된 규칙에 의거하여 결정되며 특정 주체가 결정하는 것은 불가능
- 블록체인에 참여하는 모든 컴퓨터가 장부를 분산 저장하고, 장부를 검증해서 동기화하는 등 기본적인 원리는 개방형 블록체인과 동일

○ 개인용 허가형 블록체인은 소수의 컴퓨터를 연결해서 직접 구축 또는 아마존과 같은 블록체인 플랫폼 활용 가능

- 개인용 허가형 블록체인은 개별 기업에서 소수의 컴퓨터 네트워크를 활용해서 구축 및 운영 가능
- MS, IBM 등이 클라우드 컴퓨팅 인프라와 블록체인 기술을 결합하여 제공하는 BPaas(Blockchain Platform as a Service)형 허가형 블록체인 서비스도 고려 가능한 대안

4. 허가형 블록체인과 기업 비즈니스

□ 허가형 블록체인은 기업의 Biz. 특성을 고려하여 맞춤형으로 구축 가능

○ 허가형 블록체인은 접근 권한 설정을 맞춤형으로 설계 가능

- 허가형 블록체인의 경우 읽기, 쓰기, 합의 과정에 참여할 수 있는 참여자가 미리 정해져 있으며, 필요에 따라 특정 주체가 새로 추가되거나 제거 가능
- 따라서 모두가 자료를 조회할 수 있으나 자료의 기록은 특정 주체만 할 수 있는 경우, 또는 읽기와 쓰기 모두 특정 주체만 가능한 경우 등 다양하게 적용 가능
- 활용 목적에 따라 여러 가지 버전으로 허가형 블록체인을 설계 가능

○ 허가형 블록체인은 비트코인처럼 해시경쟁 없이도 혁신적인 업무처리 기회 제공

- 허가형 블록체인은 POW를 통한 해시파워 경쟁모델이 아니라 POS 또는 FBA 등 해시경쟁이 없는 알고리즘 사용을 통해 에너지 소모 절약 등 비용 절감 가능
- 기업의 입장에서 블록체인을 통한 정보의 분산 저장 및 공유를 통해 보안성의 증가를 기대할 수 있으며 처리시간과 비용 절감을 위한 솔루션으로도 사용
- 중개기관을 거치지 않고 서로 다른 노드가 자신의 데이터를 온전하게 신뢰할 수 있게 된다면 데이터 오차수정, 불일치 내역조정, 커뮤니케이션을 위한 메세징 시간 절감 등 다양한 혁신적 변화 기대 가능

□ 허가형 블록체인을 활용한 기업들의 새로운 Biz. 모델 개발 노력 지속

○ 블록체인의 이중지불 방지 기능과 스마트계약 기능을 활용하여 기업은 다양한 비즈니스 모델 개발 및 기존 사업의 경쟁력 강화 시도 중

- 분산된 상호 인증 기능을 활용하여 보안비용을 절감하고 이중지불 위험과 해킹 위험을 제거할 수 있으며, 중개기능의 제거 통해 수수료 절감 가능
- 확장성 측면에서 블록체인을 활용하면 IT 구축 비용을 절감하고 신사업 서비스 확장 가능
- 자동화 측면에서 신속한 거래처리와 에러 발생을 줄이는 효과 달성 가능

○ 허가형 블록체인을 활용하여 기업은 공급망 관리, 제조혁신,

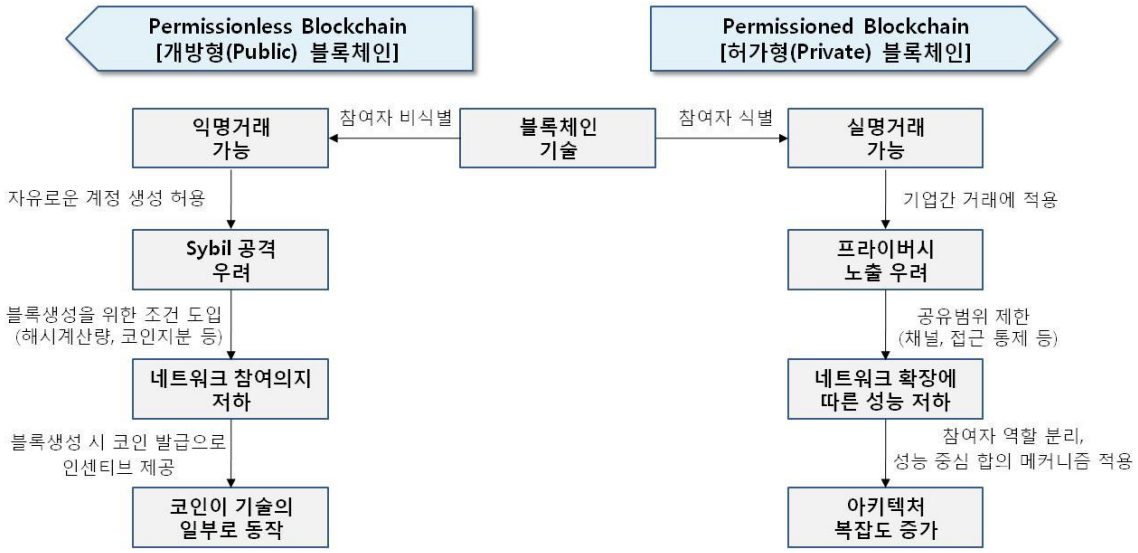
판매채널/고객관리 및 새로운 Biz. 생태계 구축 등 다양한 기회 창출 가능

□ 허가형 블록체인은 개방형 블록체인 대비 기술 혁신성과 활용과 보안성에서 일부 제한

○ 허가형 블록체인은 실명기반 거래이므로 개방형 블록체인 대비 개인의 프라이버시 보호 측면이 취약

- 개방형 블록체인은 51% 공격 방어가 주요 이슈지만 허가형 블록체인도 실명 거래에 따른 정보보호 기능의 취약성 내포
- 허가형 블록체인은 실명으로 거래가 이루어지므로 익명성이 무너지고 거래의 투명성만 강조되어 개인 프라이버시 침해 발생 가능

〈그림 2〉 개방형과 허가형 블록체인 보안성 비교



자료: LGCNS, 블록체인 기술동향 및 적용방향, 2018

○ 소수의 컴퓨터 네트워크로 허가형 블록체인 구축 시 내부자의 담합에 따른 51% 공격에 대한 취약성 보유

- 비트코인의 경우 네트워크 참여자가 많기 때문에 51% 공격은 어려울 수 있지만 참여자가 적은 허가형 블록체인 네트워크는 해커의 공격에 취약
- 기업의 소규모 컴퓨터 네트워크 기반 허가형 블록체인의 경우 한 노드에서 발견된 취약점이 다른 모든 노드를 공격하는 데 사용 가능
- 외부의 공격뿐만 아니라, 폐쇄적인 시스템 내부 참여자들이 악의적으로 담합을

해서 블록체인 내용을 위·변조할 가능성도 존재

□ 허가형 블록체인은 자체 취약성 극복을 위해 기술개발과 운영 방식 측면에서 개방형 블록체인의 장점을 활용하는 하이브리드형으로 발전

○ **개인의 프라이버시 침해 문제를 해결하기 위해 기술적 영지식 증명이라는 암호화 기술을 활용, 개인의 프라이버시 강화 시도**

○ **블록체인 내부 참여자의 담합을 방지하고 대외 투명성을 확보하기 위해서 참여자 접근제어를 강화하고 앵커링 기술 등 특화기술 개발**

〈표 1〉 허가형 블록체인의 보안성 강화 대책

구 분	내 용	비고
영지식 증명	• 암호학에서 누군가가 상대방에게 어떤 것에 대한 설명문이 참이라는 것을 증명할 때 해당 문장의 참/거짓 여부를 제외하면 어떤 것도 노출되지 않는 상호절차 • 어떤 추가 내용도 노출하지 않고 해당 정보를 알고 있다는 것을 증명하는 방법 • 실제 내용을 공개하지 않고도 그 진위를 확인함으로써 프라이버시 강화 가능	암호화폐 Zerocash 적용
앵커링 기술	• 프라이빗 블록체인과 퍼블릭 블록체인을 연계하는 기술 • 보안 대상인 개인용 허가형 블록체인의 대표 해시값을 주기적으로 비트코인 등의 개방형 블록체인에 기록 • 내부 담합이 의심되면 개방형 블록체인에 기록한 내용과 허가형 블록체인 정보를 비교해서 검증을 수행해 내부 담합으로 개인용 블록체인 내용을 변경하려는 시도를 방지 가능	
스마트계약 기반 접근 제어	• 참여자 권한에 대해 설정된 정책 자체가 스마트계약의 형태로 배포되며, 요청에 대한 접근제어도 스마트계약 시행을 기반으로 동작	

5. 시사점

○ **앞으로 블록체인은 기술적 이슈보다는 사업모델 개발과 사회적 솔루션 제공 관점에서 접근 필요**

- 현재 블록체인의 거래 처리 효율성과 정보보안 측면의 한계는 기술발전을 통해 해결 가능할 것으로 전망
- 개방형 블록체인과 허가형 블록체인의 구분 또한 무의미하며, 앞으로 기업의 사업적 활용을 위해 두 유형의 장점을 결합한 하이브리드 방식으로 진화
- 기업 입장에서는 분산원장 기능을 활용하여 기존 사업 모델의 효율성을 높이고 암호화폐나 토큰 기반 Biz. 생태계의 선제적 구축 방안 모색
- 블록체인의 스마트계약 활용도 제고와 스마트계약 활용 과정에서 발생하는 분쟁 해결을 위한 사회적 지원 인프라 구축이 중요 이슈로 부각 가능

○ **미래 변화 시나리오를 기반으로 초기 대규모 투자보다는 외부 블록체인 서비스를 활용한 소규모 투자를 시작으로 단계적 확대 전략 추진**

- 소규모의 자체 허가형 블록체인 구축 또는 가격 대비 효과적인 글로벌기업의 블록체인 서비스를 활용하는 방안 검토
- 사내 소규모 분산 컴퓨팅 환경 기반 업무 효율성 제고 프로젝트 수행을 통해 기술의 사업적 활용성 평가
- 아마존이나 구글 같은 클라우드 기반의 블록체인 기술과 인프라를 활용하여 비즈니스 모델 구현 및 경험 축적
- 시장환경 변화와 블록체인을 기반으로 한 인터넷 거래환경의 진화 단계에 따라 비즈니스 모델을 개선하고 규모를 확장해 가는 사업전략 추진

○ **미래를 준비하는 차원에서 기업형 하이브리드 블록체인 기반 비즈니스 생태계를 구축하고 지속성장이 가능한 신사업 아이템 육성 기회 모색**

[참고자료]

[보고서]

블록체인 기술의 발전과정과 이해, 피넥터보고서, 2016

블록체인 산업실태/기술혁신 및 적용전략과 응용·실증사례 세미나, 산업교육연구소, 2018

블록체인 이상과 현실 어디쯤 와 있나, 한화투자증권, 2018

지능형 정부 추진을 위한 블록체인 동향분석 및 시사점, 한국정보화진흥원, 2018

블록체인 기술동향 및 적용방향, LGCNS, 2018

[서적]

김용태, 블록체인으로 무엇을 할 수 있는가, 연암사, 2018

김응수 외, 블록체인의 충격, 북스타, 2017

나라얀 프루스티, 이더리움을 활용한 블록체인 프로젝트 구축, 에이콘, 2017

NEC·컨센서스베이스주식회사, 이더리움을 활용한 블록체인 개발 입문서, 국일증권경제연구소, 2018

박재현 외, 코어 이더리움 프로그래밍, 제이펍, 2018

임정빈, 돈의 미래 비트코인은 혁명인가 반란인가, 시사매거진, 2018

조수현 외, 이더리움 베이직, 북스타, 2017

안드레아스 M. 안토노풀로스, 비트코인 블록체인과 금융의 혁신, 고려대학교 출판문화원, 2015

최윤일, 암호화폐 혁명, 이더리움 블록체인, 두리미디어 라꽁떼, 2018