

# Business Focus

## Web 3.0의 핵심 기술, 블록체인



July 2022

삼성KPMG 경제연구원

# Contacts

## 삼성KPMG 경제연구원

김규림

이사

T: +82 2 2112 4089

E: gyulimkim@kr.kpmg.com

곽호경

수석연구원

T: +82 2 2112 7962

E: hokyungkwak@kr.kpmg.com

최연경

책임연구원

T: + 82 2 2112 7769

E: yeonkyungchoi@kr.kpmg.com



본 보고서는 삼성KPMG 경제연구원과 KPMG member firm 전문가들이 수집한 자료를 바탕으로 일반적인 정보를 제공할 목적으로 작성되었으며, 보고서에 포함된 자료의 완전성, 정확성 및 신뢰성을 확인하기 위한 절차를 밟은 것은 아닙니다. 본 보고서는 특정 기업이나 개인의 개별 사안에 대한 조언을 제공할 목적으로 작성된 것이 아니므로, 구체적인 의사결정이 필요한 경우에는 당 법인의 전문가와 상의하여 주시기 바랍니다. 삼성KPMG의 사전 동의 없이 본 보고서의 전체 또는 일부를 무단 배포, 인용, 발간, 복제할 수 없습니다.

# Contents

Page

I. Web 3.0으로의 진화와 블록체인	2
II. 글로벌·국내 블록체인 시장 현황	23
III. 산업에서의 블록체인 활용 방안·동향	31
IV. 결론 및 시사점	42

# 미래를 바꿀 기술, 블록체인

가트너(Gartner), '19년과 '20년 2년 연속 10대 전략기술 트렌드로 '블록체인 선정'

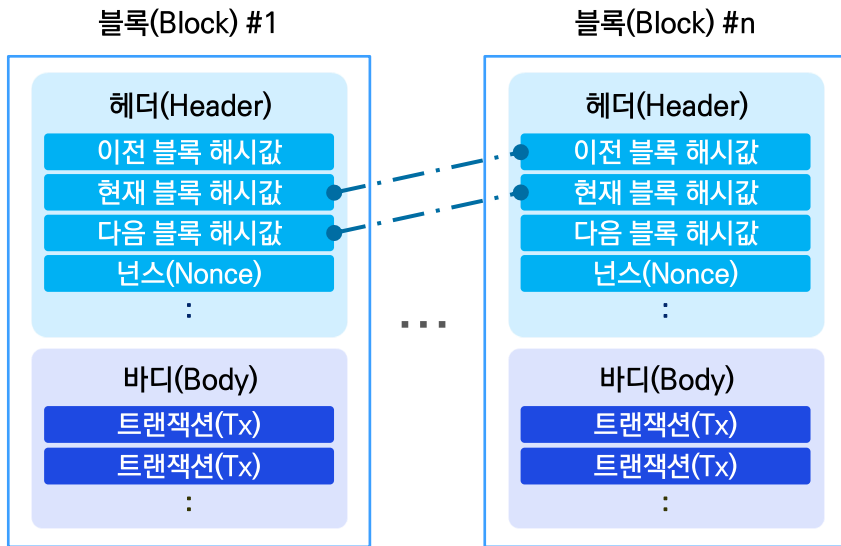
핵심 트렌드	2019년 전략 기술 트렌드	핵심 트렌드	2020년 전략 기술 트렌드
인텔리전스 (Intelligence)	▶ ① 자율 사물 (Autonomous Things)	사람 중심 (People-Centric)	▶ ① 자동화 (Hyperautomation)
	▶ ② 증강 분석 (Augmented Analytics)		▶ ② 멀티 경험 (Multiexperience)
	▶ ③ 인공지능 주도 개발 (AI-Driven Development)		▶ ③ 민주화 (Democratization)
디지털 (Digital)	▶ ④ 디지털 트윈 (Digital Twin)		▶ ④ 휴먼 증강 (Human Augmentation)
	▶ ⑤ 강화 에지 (Empowered Edge)		▶ ⑤ 투명성·추적성 (Transparency & Traceability)
	▶ ⑥ 몰입 경험 (Immersive Experience)		▶ ⑥ 강화 에지 (The Empowered Edge)
메시 (Mesh)	▶ ⑦ <b>블록체인 (Blockchain)</b>	스마트 공간 (Smart Space)	▶ ⑦ 분산 클라우드 (Distributed Cloud)
	▶ ⑧ 스마트 공간 (Smart Spaces)		▶ ⑧ 자율 사물 (Autonomous Things)
구름 (Cloud)	▶ ⑨ 디지털 윤리·개인정보보호 (Digital Ethics & Privacy)		▶ ⑨ <b>실용적 블록체인 (Practical Blockchain)</b>
	▶ ⑩ 양자 컴퓨팅 (Quantum Computing)		▶ ⑩ AI 보안 (AI Security)

전 세계는 4차 산업혁명 관련 혁신기술 중 하나로 블록체인을 주목  
가트너는 블록체인이 '23년까지 다양한 산업 분야에서 급격한 확장세를 유지할 것으로 전망

Source: Gartner

# 블록체인의 개념 및 구조

## 블록체인 구조



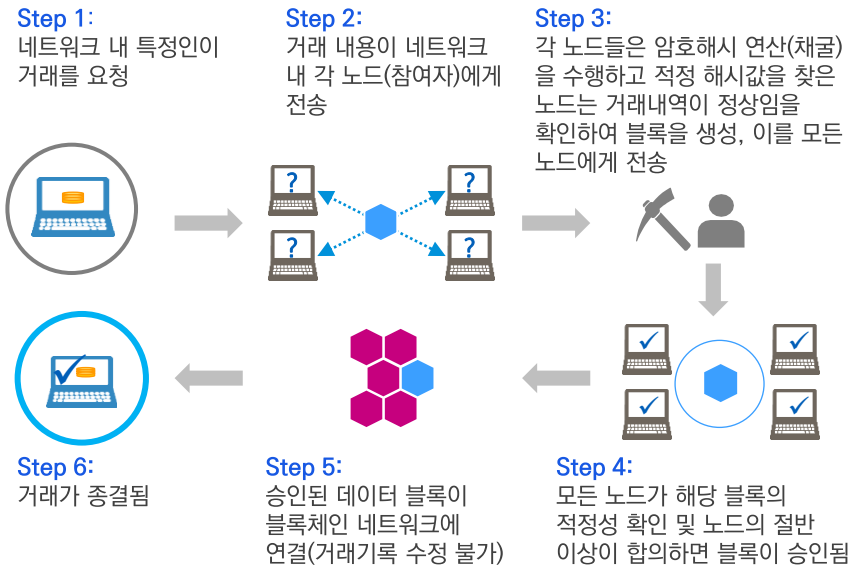
Source: 금융보안원

Note 1: 해시(Hash)함수 이용, 임의의 데이터에서 고정된 길이의 해시값 생성

Note 2: nonce(Nonce)란, 암호화된 시스템에서 한번 사용되는 임의적인 숫자

- 블록체인은 분산형 데이터베이스와 유사한 형태로 데이터를 저장하는 연결 구조체(시스템)를 뜻함
  - 블록체인 참여자들은 해시값을 통해 서로 해당 데이터의 정합성을 검증·저장함으로써 임의적인 조작이 어렵도록 설계된 저장 플랫폼
- 블록체인을 구성하는 각 블록은 헤더(Header)와 바디(Body)로 이루어짐
  - 헤더에는 현재 블록을 이전 블록과 다음 블록으로 연결하는 해시(Hash) 값과 암호화된 시스템에서 사용되는 임의의 수 nonce(Nonce) 등을 포함
  - 바디에는 거래 별 트랜잭션(Transaction)이 기록

## 블록체인 기반 거래 프로세스



Source: 한국인터넷진흥원, '비트코인 블록체인 동작원리 및 진화', 삼성KPMG 경제연구원 재구성

Note: 블록체인을 활용한 송금거래의 경우를 예시적으로 제시. 노드(Node)는 블록체인 네트워크의 참여자를 의미

- 거래발생 시 거래정보가 네트워크의 각 노드들에게 전송되고, 유효성 검증을 수행한 후 참여자들의 합의를 거쳐 해당 거래를 블록체인에 포함시키는 방식
- 블록체인을 통한 거래 프로세스 개요:
  - 거래 당사자 간 거래 발생 → 거래정보는 네트워크를 통해 블록체인상 모든 참여자에게 전송 → 거래정보를 전송 받은 블록체인 구성원들은 상호 검증을 통해 암호화된 거래정보가 타당한 거래인지 여부 결정 → 구성원 간의 유효성 검증을 통해 타당성이 입증된 거래정보가 신규 블록에 저장 → 기존 블록에 연결되어 하나의 블록체인을 구성 및 당사자 간 거래 완료

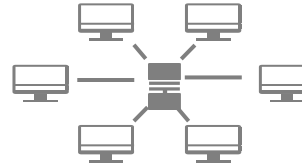
# 블록체인의 핵심 기술

## Tech 1

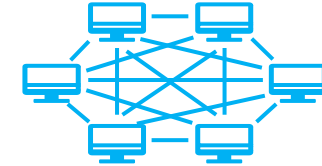
### P2P(Peer to Peer) 네트워크

- 블록을 검증·합의하는 참여자들을 연결하는 방식
- 블록체인 네트워크에 참여하는 사람들은 동등한 계층으로 연결되어 개별 서버이자 거래 당사자가 됨

#### 서버 기반 네트워크



#### P2P 기반 네트워크

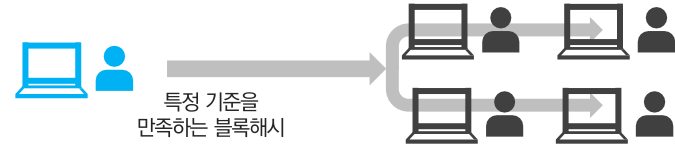


## Tech 2

### 합의 알고리즘

- 합의 알고리즘이란 다수의 참여자들이 통일된 의사결정을 하기 위해 사용하는 알고리즘(메커니즘)을 의미
- 주요 방식으로 작업증명(Proof of Work, PoW), 지분증명(Proof of Stake, PoS) 등이 있음

#### 대표적 합의 알고리즘 예시: 작업증명(PoW)



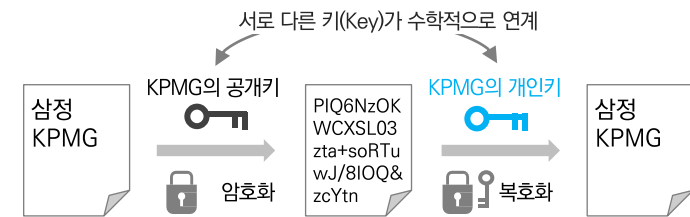
- 채굴자가 해시연산 하드웨어를 운영하여 특정 기준을 만족하는 블록해시
- 해당 작업증명(블록)을 네트워크로 전송하고 다른 채굴자들은 작업증명을 확인하고 적합성을 검증

## Tech 3

### 공개키 암호화

- 블록에 작성·저장된 데이터를 공개키 기반으로 암호화하여, 네트워크 참여자가 아니면 열람이 불가능하도록 하는 핵심기술
- 공개키를 활용한 전자서명이 함께 되어 거래 부인방지, 데이터 무결성 등을 보장

#### 공개키 암호화 작동 원리



Source: 삼성KPMG MCS1, 디지털본부, 삼성KPMG 경제연구원 재구성

# 블록체인의 기술적 특성

## 1 탈중앙화

- 제3자·중개자 개입 없이 개인·법인 등 직접 거래 및 거래비용 절감 가능
- 중앙집중형 조직이 불필요하여 중앙집중형 시스템의 구축·운영·유지보수 등 비용 절감 가능

## 2 보안성

- 거래기록 및 데이터를 모든 네트워크 참여자가 공동으로 소유
- 거래기록 및 데이터가 암호화되기 때문에 거래 조작이 어려워 무결성 확보

## 3 투명성

- 거래기록 및 데이터가 네트워크 참여자에게 모두 공유되고 누구나 접근하여 확인이 가능함

## 4 익명성

- 개인정보 없이 거래가 가능하며, 은행계좌·신용카드 등 기존 수단보다 높은 익명성 보장

## 5 안전성

- 분산형 네트워크로 구성되어 특정 네트워크가 손실되더라도 지속적으로 연결 가능하며 해킹 공격에도 안전
- 참여자 일부에서 네트워크 오류·끊김·성능 저하 등의 문제가 발생해도 전체 네트워크에 영향을 주지 않음

### 금융 혁신

- **효율성 제고·비용 절감을 통한 금융혁신 가능**
  - 금융 부문의 신용, 유동성, 운영, 법률, 시스템 등과 같은 리스크로부터 안전성을 확보하기 위해 감독기관의 법·제도적 권한이 아닌, 블록체인의 기술적 솔루션으로 해결 가능
  - 기존 중앙화된 금융 구조가 분산 기반으로 가능해져 디지털 형태로 거래되는 다양한 금융자산 등도 분산원장 기술을 통해 거래의 완결성과 효율성 제고

### 가상자산 확산

- **블록체인의 등장으로 가상화폐 생태계가 태동**
  - 비트코인을 비롯, 이더리움, 리플, 라이트코인 등 수많은 가상자산이 블록체인 기술을 기반으로 탄생
  - 대부분의 나라에서 법적 화폐로 인정받지는 못하고 있으나, 전자상거래 등에서 지급결제 기능을 갖고 실질적인 화폐로 확산되는 추세

### 산업 생태계 변화

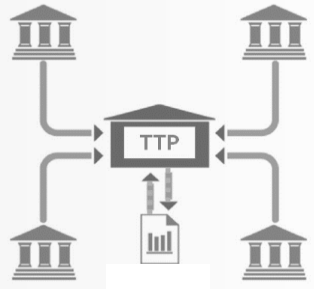
- **여러 산업군의 수직적 생태계가 수평적 생태계로 전환**
  - 블록체인 기술의 영향으로 이종·개별 산업군의 형태로 생태계 구조가 변화되는데 기여하고 있음
  - 블록체인 생태계가 확장되며 이러한 추세는 더욱 가속화되고 있음

Source: 정보통신기술진흥센터(2016), '주간기술동향', 삼정KPMG 경제연구원 재구성

# 블록체인과 기존 시스템과의 차별성

## 중앙집중형 시스템과 블록체인 기반 시스템의 비교

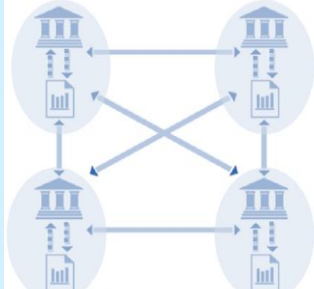
### 중앙집중형 시스템



**[기존 집중형 시스템]**  
거래 장부를 신뢰할 수 있는 제3의 기관(Trusted Third Party, TTP)을 설립하고 해당 기관에 대한 신뢰를 바탕으로 중앙집중형으로 관리

1. 기록 관리 권한과 책임이 특정 기관에 집중
2. IT인프라 및 보안 관련 대규모 인력·설비투자 필요
3. 해당 기관의 신뢰 확보를 위한 규제·감독 강화
4. 혁신적인 서비스 및 신규 사업자 진출이 제한적

### 블록체인 기반 시스템



**[새로운 분산형 시스템]**  
모든 참여자가 거래 내역이 기록된 장부 전체를 각각 보관하고 새로운 거래를 반영하여 갱신(Update)하는 작업도 공동으로 수행

1. 중앙집중적 생태계 및 서버 구축 불필요
2. 거래기록 및 증명 방식의 근본적 변화
3. 제3의 기관 없이 신뢰성 및 보안성 확보 가능
4. 거래수수료 절감 등 사회·경제적 비용 절감 가능

Source: 한국은행, 삼성KPMG 경제연구원 재구성

- 중앙집중형 시스템에서는 정보와 권한이 특정 기관에 집중
  - 조작·오류 등의 문제 등으로 인한 시스템 신뢰 훼손을 방지하기 위해 관리감독 강화 및 IT 인프라와 보안 등에 대규모 인력 및 설비투자가 이루어짐
- 반면, 블록체인 기반 시스템은 거래정보를 P2P(Peer-to-Peer) 네트워크에 분산시켜 구성원들이 공동으로 관리
  - 신뢰할 수 있는 제3의 기관을 설립·운영하기 위한 인력 및 자원 투입이 불필요하며, 거래기록이 구성원들에게 암호화되어 공개되기 때문에 거래 투명성 제고
  - 정보유출 표적이 되는 중앙서버가 존재하지 않아 블록체인 네트워크 전체 연산능력을 상회하여 해킹·조작을 시도하기가 사실상 어려워 높은 보안 안전성 확보



# P2P 네트워크의 합의 알고리즘, 블록체인 무결성을 유지

## 블록체인 합의 알고리즘

구분	‘가장 빨리 찾아내는 사람이 보상받는다’ 작업 증명 방식(Proof of Work, PoW)	‘은행 이자처럼 보상받는다’ 지분 증명 방식 (Proof of Stake, PoS)	‘시스템 기여도에 따라 보상받는다’ 중요도 증명 방식 (Proof of Importance, Pol)
코인 보상	<ul style="list-style-type: none"> <li>해시(Hash)의 크기</li> <li>해시연산을 처리하는 하드웨어(CPU, ASIC 채굴기 등)를 사용하여 거래 증명하는 방식</li> </ul>	<ul style="list-style-type: none"> <li>보유한 코인 지분(Stake)</li> <li>채굴기 없이 참여자가 소유한 코인의 지분으로 채굴되는 방식</li> </ul>	<ul style="list-style-type: none"> <li>거래량이나 거래금액 등 생태계에 대한 사용자의 기여도·중요도</li> <li>참여자의 네트워크 참여도에 따른 보상지급 방식</li> </ul>
설명	<ul style="list-style-type: none"> <li>컴퓨터가 연산을 수행해 블록 생성 및 검증(네트워크 증명)에 기여한 대가로 코인 보상</li> <li>가장 대중적으로 사용되는 방식이며, 시장이 크고, 인프라가 지속 확대되고 있는 코인들은 대부분 PoW 방식을 채택</li> </ul>	<ul style="list-style-type: none"> <li>PoS는 가지고 있는 코인양이 많을수록 더 많은 코인을 지속적으로 얻는 방식</li> <li>소유 코인의 증명 지분에 해당하는 만큼 이자를 받는 방식</li> </ul>	<ul style="list-style-type: none"> <li>PoS의 단점인 유동성 감소 등을 극복하기 위해 등장</li> <li>거래량이나 거래금액, 신용 등 생태계에 대한 기여도, 중요도가 높은 사용자에게 수수료가 배분되는 방식</li> </ul>
장점	<ul style="list-style-type: none"> <li>블록체인이 가지는 탈중앙화라는 본질을 가장 잘 살린 합의 방식</li> </ul>	<ul style="list-style-type: none"> <li>PoW의 전력 및 장비 구입비 등 채굴에 들어가는 많은 비용 해결</li> <li>지분에 비례한 공정한 보상 지급으로 PoW의 해시 독점 단점을 보완</li> </ul>	<ul style="list-style-type: none"> <li>모든 사람에게 비교적 동등한 기회 제공</li> </ul>
단점	<ul style="list-style-type: none"> <li>거래 처리 속도가 늦고, 빠른 연산 작업을 위해 고성능의 장비가 필요하여, 장비유지·전력 비용 낭비 문제</li> <li>고성능 장비 사용 및 채굴자의 단합으로 해시 캐시의 독점 구도 생성 가능성</li> </ul>	<ul style="list-style-type: none"> <li>이미 코인을 보유한 사람의 경우, 코인 유통에 대한 유인이 없기 때문에 유동성이 유입되기 어려움</li> <li>초기 코인 유포가 공평하지 못하며, 자금이 많은 사람이 쉽게 독점 가능</li> <li>채굴을 통한 이득이 PoW보다 적음</li> </ul>	-
예시	<ul style="list-style-type: none"> <li>비트코인, 라이트코인 등 채굴이 가능한 모든 코인</li> </ul>	<ul style="list-style-type: none"> <li>에이다, 퀀텀, 네오, 스트라티스</li> </ul>	<ul style="list-style-type: none"> <li>넴(NEM)</li> </ul>

블록체인은 분산화된 시스템으로, 권위 있는 중앙(Center)에 의존하지 않으므로, 분산화된 노드는 거래 유효성에 대한 합의 필요

→ 합의 알고리즘은 블록체인 네트워크에 합의를 달성하는 메커니즘이며, 합의 알고리즘은 분산화된 노드들이 어떤 버전의 블록체인이 진짜 버전인지 합의할 수 있게 해줌으로써 블록체인 네트워크의 무결성·보안을 유지 가능

Source: 해시넷, 삼정KPMG 경제연구원 재구성

# 블록체인은 활용 목적에 따라 3가지 유형으로 구분

## 블록체인 유형 및 특징

		← 좀더 중앙화된 방식(More centralized)	→ 탈중앙화(Decentralized)
구분	프라이빗 블록체인 (Private Blockchain)	컨소시엄 블록체인 (Consortium Blockchain)	퍼블릭 블록체인 (Public Blockchain)
관리자	<ul style="list-style-type: none"> <li>한 중앙기관이 모든 권한 보유</li> </ul>	<ul style="list-style-type: none"> <li>미리 선정된 컨소시엄에 소속된 소수 참여자</li> </ul>	<ul style="list-style-type: none"> <li>모든 거래 참여자</li> </ul>
거버넌스	<ul style="list-style-type: none"> <li>중앙기관의 의사결정에 따라 용이하게 규칙을 바꿀 수 있음</li> </ul>	<ul style="list-style-type: none"> <li>컨소시엄 참여자들의 합의에 따라 규칙을 바꿀 수 있음</li> </ul>	<ul style="list-style-type: none"> <li>한번 정해진 규칙을 바꾸기 매우 어려움</li> </ul>
거래속도	<ul style="list-style-type: none"> <li>네트워크 확장이 매우 쉽고 거래속도가 빠름</li> </ul>	<ul style="list-style-type: none"> <li>컨소시엄 참여자들의 합의에 따라 법칙을 바꿀 수 있음</li> </ul>	<ul style="list-style-type: none"> <li>네트워크 확장이 어렵고 거래속도가 느림</li> </ul>
데이터 접근	<ul style="list-style-type: none"> <li>허가 받은 사용자만 접근 가능</li> </ul>	<ul style="list-style-type: none"> <li>허가 받은 사용자만 접근 가능</li> </ul>	<ul style="list-style-type: none"> <li>누구나 접근 가능</li> </ul>
식별성	<ul style="list-style-type: none"> <li>식별 가능</li> </ul>	<ul style="list-style-type: none"> <li>식별 가능</li> </ul>	<ul style="list-style-type: none"> <li>익명성</li> </ul>
거래증명	<ul style="list-style-type: none"> <li>중앙기관에 의해 거래 증명이 이루어짐</li> </ul>	<ul style="list-style-type: none"> <li>거래 증명자가 인증을 거쳐 알려진 상태</li> <li>사전에 합의된 규칙에 따라 거래 검증 및 블록 생성이 이루어짐</li> </ul>	<ul style="list-style-type: none"> <li>알고리즘에 따라 거래 증명자가 결정되며, 거래 증명자가 누구인지 사전에 알 수 없음</li> <li>- PoW, PoS, Pol 등</li> </ul>
활용사례	<ul style="list-style-type: none"> <li>나스닥 비상장 주식 거래소 플랫폼 링크(Linq)</li> </ul>	<ul style="list-style-type: none"> <li>R3 CEV</li> </ul>	<ul style="list-style-type: none"> <li>비트코인</li> </ul>

Source: NICE평가정보(2021), '다양한 활용성으로 세계 경제 변화를 주도할 혁신기술', 삼성KPMG 경제연구원 재구성

# 블록체인이라는 기술이 가지는 의미

## Web 1.0: "Transferring Information"



텍스트

이미지

프로그램

영상

Web 1.0은 온라인 기반 '정보'를 일방향으로 전달하는 '온라인 시대'를 탄생시켰고...

## Web 2.0: "Interaction between Users to Exchange Information"



텍스트

이미지

프로그램

영상

플랫폼

Web 2.0은 플랫폼을 중심으로 사용자간 '정보'를 주고받는 '상호작용'을 가능하게 한 반면...

## Web 3.0: "Transferring Ownership"



돈

계약

특허

자산

플랫폼

Web 3.0은 블록체인을 기반으로 '소유권'을 전달함으로써 '디지털(가상) 자산 시대'가 열림

Source: Sam Wouters, SK증권, 삼정KPMG 경제연구원 재구성

# 지금은 블록체인 3.0 시대

	블록체인 1.0	블록체인 2.0	블록체인 3.0
	<p><b>‘디지털 통화 시대의 개막’</b> 최초 디지털 통화의 등장</p>	<p><b>‘프로세스 혁신 및 블록체인 생태계 태동’</b> 스마트 계약(Smart Contract) 플랫폼 제공</p>	<p><b>‘신규 비즈니스 모델 기반 신사업 개발’</b> 의사결정 및 적용영역 확대</p>
특징	<ul style="list-style-type: none"> <li>• 통화·화폐로서의 블록체인(블록체인이 화폐적 용도로만 제한적 사용)</li> <li>• 퍼블릭 블록체인</li> </ul>	<ul style="list-style-type: none"> <li>• 블록체인 한계점 극복 노력 및 스마트 계약 기반 다양한 응용 가능</li> <li>• 프라이빗 블록체인 출현</li> </ul>	<ul style="list-style-type: none"> <li>• 확장성·보안성 제고</li> <li>• 블록체인 간 상호운용성 지원</li> <li>• 시스템 내 자체 의사결정 기능</li> </ul>
상세	<p>▶ <b>블록체인 개념 검증</b></p> <ul style="list-style-type: none"> <li>- 공개분산원장, 합의 알고리즘</li> <li>- 탈중앙화, 분권·분산화, 거래 투명성 제공</li> <li>- 중앙화 기구에 의존하는 기존 금융체제에 대한 대안으로 제시</li> </ul>	<p>▶ <b>스마트 계약을 통한 지능화</b></p> <ul style="list-style-type: none"> <li>- 사용자 간 계약을 프로그래밍을 통해 자동 실행</li> <li>- 계약을 집행하거나 신뢰를 제공할 제3자의 개입없이 다양한 계약 구현</li> <li>- 사용자가 프로그래밍을 통해 자유롭게 계약 생성</li> <li>- 다양한 비즈니스에 활용할 수 있는 분산 애플리케이션(Decentralized Application, DApp) 개발</li> </ul>	<p>▶ <b>기술적 기능 향상</b></p> <ul style="list-style-type: none"> <li>- 지분증명방식 합의 알고리즘(전력소모 최소화)</li> <li>- 새로운 분산장부 기술(Tangle 등) 등장</li> <li>- 블록 생성주기(처리속도) 향상, 하드포크 최소화</li> <li>- 가상통화 소유자들 간 내부합의 도출 기능 탑재</li> </ul> <p>▶ <b>산업 전반에 블록체인 확대 적용</b></p> <ul style="list-style-type: none"> <li>- 공공, 의료, 운송, 스포츠·예술, 사물인터넷 등 초연결사회 구현</li> <li>- NFT, DeFi, 탈중앙화 신원증명(Decentralized ID) 등 신사업 등장 및 생태계 내 플랫폼 생성, CBDC 및 디지털 화폐</li> </ul>
한계점	<ul style="list-style-type: none"> <li>- 금융거래 등 한정적 분야에서만 활용</li> <li>- 낮은 확장성, 느린 거래속도</li> <li>- 합의도출이 어려운 의사결정 시스템</li> </ul>	<ul style="list-style-type: none"> <li>- 하드포크(Hard Fork), 증명방식(PoW)</li> <li>- 트랜잭션 용량 제한</li> <li>- 합의도출이 어려운 의사결정 시스템</li> </ul>	-
예시	- 비트코인	- 이더리움	- 솔라나, 아이오타, 네오, 이오스, 카르다노 등

Source: 한국예탁결제원, 언론보도 종합, 삼정KPMG 경제연구원 재구성

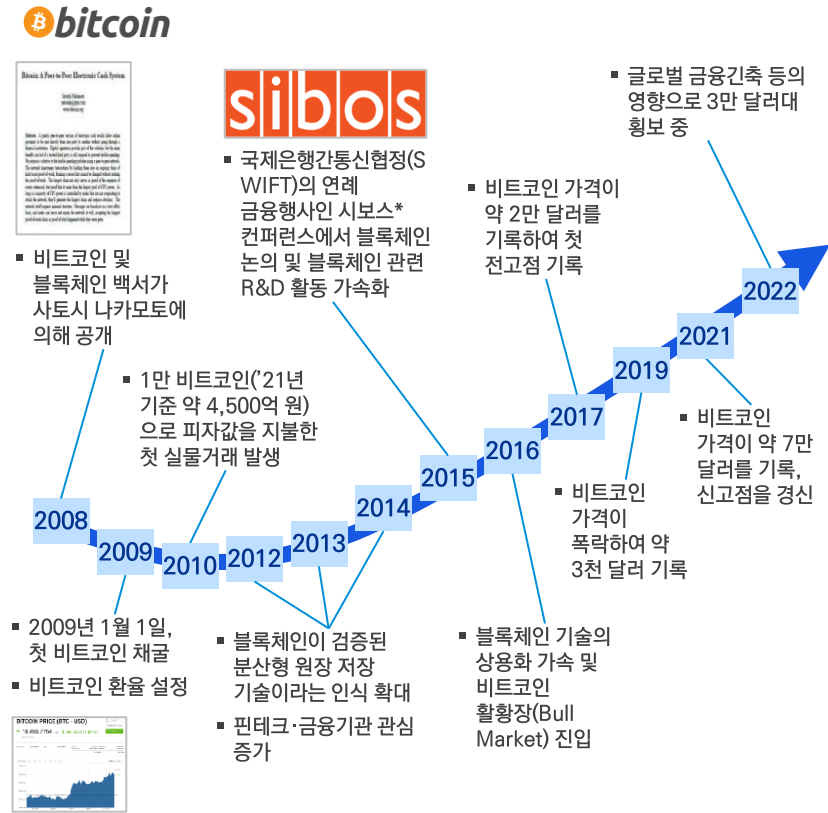
# 1세대 ‘비트코인’의 등장, ‘블록체인 시대’의 도래를 알리다

블록체인 1.0

블록체인 2.0

블록체인 3.0

## 비트코인 주요 이벤트 Timeline



## 비트코인(블록체인) 시대의 시작

- 2009년 사토시 나카모토(Nakamoto Satoshi)라는 가명을 쓰는 개발자가 비트코인을 오픈소스 소프트웨어로 공개
  - 사토시 나카모토가 제시하는 비트코인의 토대와 기본 원칙 요약
    - 1) P2P 전자거래 및 상호작용
    - 2) 금융기관의 필요성 상실
    - 3) 암호학적 증명으로 중간의 신용기관 대체
    - 4) 중앙기관 개입 없이 네트워크 자체가 신뢰·인증을 해결
- 비트코인은 P2P 네트워크·암호화 기술·합의 알고리즘(PoW)을 활용하여 가상화폐를 실현한 최초의 디지털 화폐
  - ‘노드(네트워크 참여자)’는 P2P 네트워크의 일원으로서, 거래 작업증명(PoW)에 참여하여 기존 금융기관의 역할을 대신 수행
  - 블록체인이 작동할 수 있는 전산자원은 불특정 다수(노드)가 채굴 시 발생하는 보상을 목적으로 자발적으로 제공
  - 채굴은 노드가 작업증명(PoW) 방식의 합의 알고리즘을 통해 블록에 거래내역을 확인시켜 주고 보상(비트코인+거래 수수료)을 받는 과정

## 비트코인의 단점·한계

- 비트코인이 채택한 1세대 블록체인 기술은 기술적 혁신성에도 불구하고, 낮은 거래 처리율, 채굴 시 많은 전력 소모, 튜링 완전성을 지원하지 않는 등 확장성·응용성이 낮아 기술적 파급·응용이 제한되어 주로 디지털 통화 발행 및 거래 용도로 활용

Source: 삼정KPMG 디지털/MCS1 본부, 삼정KPMG 경제연구원 재구성

Note: \*Swift international banking operations seminar, Sibos

# [참고] 작업증명(Proof of Work, PoW) 과정

## 작업증명 메커니즘

삼성KPMG 경제연구원 → 1e23fc8o1a6a7dd5ee5910...

연산

삼성KPMG 경제연구소 → F7bca63oaa9b77ofdcoo9a...

'A가 B에게 비트코인 1개를 전송했다' 거래의 암호화



목표값 이하의 해시를 찾는 과정을 반복하여 해당 작업에 참여했음을 증명  
→ 해시값이 블록 내에서 설정한 숫자보다 작으면 작업 완료

- 블록에 기록되는 모든 기록은 연산을 거쳐 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, a, b, c, d, e, f 16개로 구성된 16진수의 숫자로 암호화되는데 이를 '해싱(Hashing)'이라 하며, 한 글자라도 틀리면 해시값이 완전히 달라짐
- 해시값으로 기록 역추적이 힘들고 내용을 조금이라도 조작하는 경우 해시값이 변경되어 위·변조가 거의 불가능

- 작업증명의 과정은 컴퓨터 연산을 통해 이루어지며, 암호화를 위해 SHA-256이라는 해시함수 프로그램이 사용되고, 블록 안 년스(Nonce)라는 무작위 숫자를 SHA-256에 입력
- 년스값을 0부터 1씩 반복 입력하면 여러 해시값이 나오며, 년스는 블록이 설정한 특정 해시값보다 작은 숫자가 나올 때까지 계속 입력됨
- 'A가 B에게 비트코인 1개를 전송했다'는 'c8bd,e93eff1...'으로 암호화되어 블록에 기록되고 작업증명은 종료

'작업'이란 '채굴'에 이르기까지 연산 과정을 의미. 채굴자들은 컴퓨터로 복잡한 수식을 풀어 조건에 맞는 해시값을 찾는 과정을 반복하고, 이러한 과정을 통해 특정 노드가 해시값을 찾으면 모든 노드들이 찾아낸 해시값을 검증·승인하는 과정을 거쳐 블록에 거래 내역을 저장

→ 모든 노드들의 승인을 거쳐야 하기 때문에 거래 내역을 속이기가 어렵다는 장점이 있으나, 거래 처리 속도가 낮다는 한계도 존재

Source: 해시넷, 삼성KPMG 경제연구원 재구성

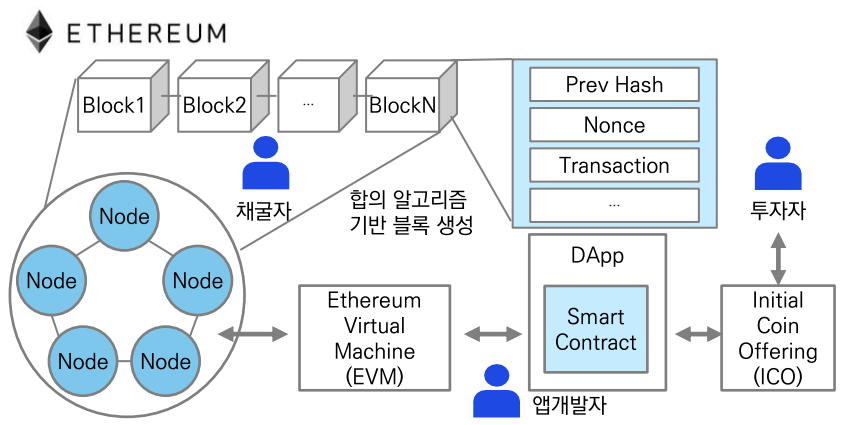
# 2세대 '이더리움', '블록체인 플랫폼'의 길을 열다

## 블록체인 1.0

## 블록체인 2.0

## 블록체인 3.0

### 이더리움 플랫폼 개요



[비트코인-이더리움 비교]

구분	비트코인	이더리움
티커	BTC	ETH
최소단위	1 Satoshi = 0.00000001 BTC	1 Wei=0.000000000000000001 ETH
목적	탈중앙화 결제 시스템	DApp을 구동하는 탈중앙화 플랫폼
최대 공급량	21,000,000	무한
블록 보상	9 BTC(210,000개 블록마다 반감기)	2 ETH
합의 알고리즘	작업증명	작업증명(지분증명으로 전환 예정)
거래 처리속도	7-8 TPS	15-20 TPS

### 탈중앙화 플랫폼의 OS 역할

- 이더리움은 비트코인과 비교하여 처리속도, 블록 용량, 합의 알고리즘 다양화 등 여러 부분에서 개선
- 특히 (1) 튜링 완전성 지원, (2) 블록체인을 활용한 모든 것을 프로그래밍할 수 있는 플랫폼 형태로 제공, (3) 스마트 계약 기능이 추가되어 블록체인 시스템이 보험·물류 등 여러 분야에서 활용 가능한 플랫폼화가 가능해졌다는 점이 가장 큰 차이점

**튜링 완전성**

- 자체 개발된 튜링 완전 언어(Solidity)를 지원하여 다양한 종류의 응용 프로그래밍도 자유롭게 개발 가능
- 블록체인 시스템에서 프로그램이 완전 구동할 수 있도록 지원·응용

**플랫폼 응용성**

- 이더리움은 탈중앙화 플랫폼의 OS와 같은 역할 수행
- 탈중앙화된 결제 네트워크만 있는 비트코인과 달리 다양한 앱을 구동할 수 있는 블록체인 기반 탈중앙화된 분산형 앱(DApp) 플랫폼

**스마트 계약**

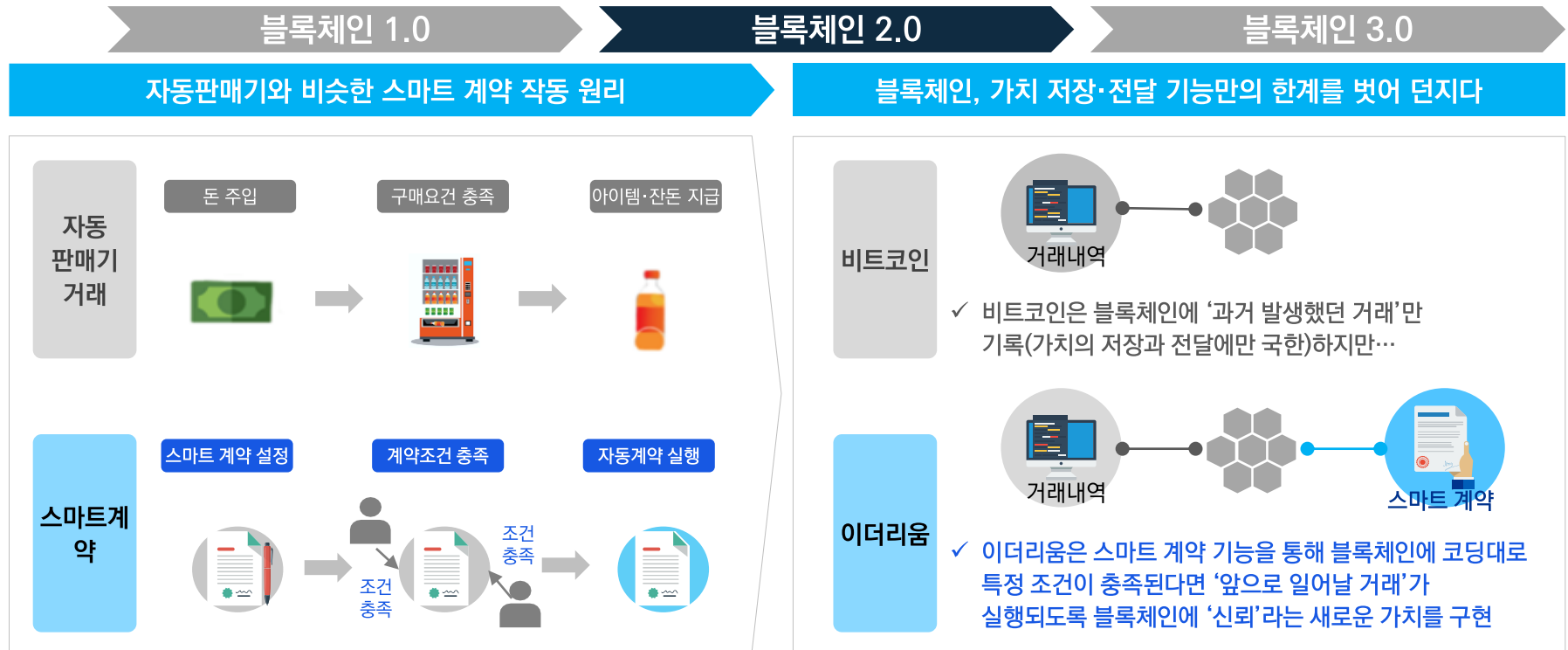
- 스마트 계약은 계약주체가 사전 협의된 내용을 미리 프로그래밍하고, 계약 조건 충족 시 자동으로 계약 내용 실행
- 계약 이행 및 검증 과정이 네트워크로 자동화, 계약실행 조건을 사람의 확인 및 추가비용 없이 직접 처리

### 이더리움의 단점과 극복 계획

- 이더리움은 높은 수수료(Gas Fees, 가스비) 및 작업증명(PoW) 기반 합의 알고리즘, 느린 속도 등이 단점으로 지적
- 이에 런던 하드포크\* 등을 통해 수수료 체계를 개선하는 등 '이더리움 2.0'을 구현 중

Source: 삼정KPMG 디지털본부, MCS1 본부, 삼정KPMG 경제연구원 재구성  
 Note: \*하드포크는 소프트웨어에 새로운 기능을 추가·개선하지만 이전 버전과 호환되지 않는 업그레이드를 뜻함

## 2세대 '이더리움', '블록체인 플랫폼'의 길을 열다 (계속)



Source: E-learning spot, 삼성KPMG 경제연구원

Source: 해시넷, 삼성KPMG 경제연구원 재구성

- 이더리움은 모든 종류의 계약을 자동 실행하는 스마트 계약 플랫폼
  - 스마트 계약은 제3의 기관 없이 계약 주체인 개인과 개인이 협의 내용을 프로그래밍하여 전자 계약서를 생성하고, 계약 조건이 충족되면 자동으로 계약 내용이 실행할 수 있도록 해주는 디지털 전자계약 기능이며, 솔리디티(Solidity)라는 프로그래밍 언어를 사용하여 계약 기간, 금액, 조건 등을 미리 코딩해두고 해당 조건이 충족되면, 어떠한 종류의 계약도 자동 실행될 수 있도록 기능
- 스마트 계약에는 프로그래밍 코드로 이루어진 알고리즘이 사전에 정해진대로 오차 없이 이행되기때문에 신뢰의 문제가 발생하지 않음
  - 다른 사람 도움이 필요 없기 때문에 리스크를 부담하거나 중개자에게 수수료를 지급할 필요가 없으며, 거래가 End-to-End로 가능



# 이더리움, 수수료·트랜잭션 이슈를 개선하며 발전 중

블록체인 1.0

블록체인 2.0

블록체인 3.0

EIP-1559 수수료 구조

런던 하드포크 결과 전망

< Before > → < After >

가스비	기본 수수료	채굴자팁(Tip)
X	X	X
사용량	사용량	사용량
=	=	=
트랜잭션 수수료 (모두 채굴자 보상으로 사용)	기본 수수료 (소각)	채굴자 보상

- 이더리움 창시자 비탈릭 부테린(Vitalik Buterin)은 '21년 7월부터 시작된 런던 하드포크가 성공적으로 완료되었다고 선언
  - 런던 하드포크는 이더리움에 EIP-1559를 도입하여 불필요하게 높은 수수료 변동성 문제를 해결하고 트랜잭션 승인이 오래 걸리는 문제를 해결하는 것을 주요 목표로 함

## 1 가스비(수수료) 예측 가능성 증대

- 네트워크가 붐비는 정도를 판단해 우선 수수료를 얼마나 지불해야 하는지 알고리즘에 따라 결정하게 되며, 수수료가 어느 정도 될지 예측 가능성 증가
- 기본료가 생겨나면서 가스비가 자동으로 계산되어 기존 이더리움의 가스비 지불 방식에서 사용자가 대략적으로 계산해야 한다는 고질적 문제 해결

## 2 이더리움 감소로 가격 상승 압력 발생

- 이더리움 생태계 확장으로 거래량이 늘어날수록 영구 소각되는 이더리움이 늘어나고, 이는 가격 상승으로 이어질 가능성 증대
- 통상 가스비는 이더리움을 Gwei(기가웨이, 1Gwei=0.000000001이더) 단위로 지불되며, EIP-1559에서 기본료로 지급되는 모든 가스비는 영구 소각됨

## 3 트랜잭션 개선 효과

- 최대 가스량이 늘어난다는 것은 트랜잭션을 담는 블록이 이전보다 커진다는 것을 의미하기 때문에 블록당 최대 가스량의 증가는 트랜잭션 개선 효과
- EIP-1559는 블록 사이즈에 탄력을 주는 방식으로 최대 가스량(Gas Limit)을 늘리는 방식을 취함. 블록에 트랜잭션이 다 차면 블록사이즈를 자동으로 키워주고, 트랜잭션이 많지 않으면 사이즈를 줄이는 식으로 변경되게끔 탄력적으로 변경

**'이더리움의 업그레이드로 높은 수수료·트랜잭션 문제를 해결된다면 이더리움 생태계는 더욱 확장될 것으로 전망'**

Source: Medium.com, 삼정KPMG 경제연구원 재구성

Source: 코인데스크(2021), '이더리움 런던 하드포크① 고질병 '수수료 문제' 해결할까', 삼정KPMG 경제연구원 재구성

# [참고] 이더리움 기능 개발 요구사항(Ethereum Request for Comments)

이더리움 표준	이더리움 기능 개발을 위한 요구사항(Ethereum Request for Comments, ERC)라 지칭되며, 다양한 서비스 플랫폼 또는 프로젝트가 이더리움의 오픈소스 프로토콜을 통해 서비스를 만들고 토큰을 발행할 수 있도록 지원
ERC-20	<b>이더리움 네트워크상에서 유통할 수 있는 토큰의 호환성을 보장하기 위한 표준 사양</b> <ul style="list-style-type: none"><li>• DApp이 발행하는 토큰이 이더리움의 통화인 이더와 호환성을 충족시키기 위해서 규정하고 있는 프로그래밍 기준임</li><li>• 토큰을 어떻게 전달하고, 토큰 관련 데이터를 어떻게 접근할 수 있는지(토큰끼리의 호환) 정의</li><li>• ERC-20은 일반적인 토큰 발행 기준이 되고 있으며, 이는 ERC-20이 대체 가능한 가상화폐를 지원하기 때문</li></ul>
ERC-223	<b>ERC-20가 지니는 문제점을 해결하기 위해 등장한 표준</b> <ul style="list-style-type: none"><li>• ERC-223은 ERC-20 토큰과 호환되어 ERC-20의 모든 기능을 지원</li><li>• ERC-20 토큰은, 호환되지 않는 주소로 토큰을 보낼 시, 토큰을 잃어버릴 수 있는 문제점이 있음</li><li>• ERC-223은 이를 해결하여 토큰 손실을 방지 기능이 추가됨</li></ul>
ERC-621	<b>토큰 공급량을 조절할 수 있는 표준</b> <ul style="list-style-type: none"><li>• 토큰의 공급량을 증가시키거나 감소시킬 수 있으며, 공급 유통량을 정할 수 없는 경우 해당 표준이 유용</li><li>• 주로 ICO 방식이 적절하지 않고, 공급 유통량을 정하기 어려운 경우에 토큰 구현 시 유용하게 활용할 수 있는 표준</li><li>• 예) 게임 내의 화폐, 골드, 퀘스트 아이템 등 수요와 공급을 예측할 수 없는 경우</li></ul>
ERC-721	<b>고유성을 가지는 수집형 토큰에 사용되는 표준</b> <ul style="list-style-type: none"><li>• 대체불가토큰(Non Fungible Token)의 표준안. ERC-721로 발행되는 토큰은 각각의 가치를 가지며, 대체 불가능(Non Fungible)하기 때문에 수집형 토큰으로 활용</li><li>• 주로 토큰 그 자체보다는 게임, 수집품 등에 주로 쓰이며, ERC-721을 활용한 대표적 사례로 크립토키티 등을 들 수 있음</li></ul>
ERC-1155	<b>대체 가능 토큰과 대체 불가 토큰 모두를 지원하는 표준</b> <ul style="list-style-type: none"><li>• ERC 토큰 표준은 각각의 모든 토큰 유형별로 별도의 스마트 계약이 필요하다는 비효율성·높은 비용이 문제점으로 지적. 이를 해결하기 위해 대체가능토큰(ERC-20)과 대체불가토큰(ERC-721)을 혼합 거래할 수 있는 ERC-1155가 등장</li><li>• 트랜잭션 당 아이템 수량도 기능에 따라 100~200개까지도 가능하며, 하나의 트랜잭션으로 한 명의 수신자에게 원하는 수량만큼의 아이템을 보낼 수 있는 멀티 전송을 구현</li></ul>

Source: 코인데스크, 해시넷, 언론보도 종합

# 3세대 코인들, 기존 세대 단점을 개선하고 특화 영역을 중심으로 발전

블록체인 1.0

블록체인 2.0

블록체인 3.0

## 카드다노(Cardano)/에이다(ADA)



- 확장성, 느린 속도 등 이더리움이 가진 문제에 대해 관심을 갖고 있던 찰스 호스킨슨은 2017년 3세대 암호화폐 에이다와 플랫폼 카드다노를 공개
- 1) 사용된 요소 기술이 사이버보안 및 암호학 분야의 최상위 학술대회 및 저널을 통해 검증되었으며, 2) 확장성 향상을 위해 지분증명(Proof of Stake, PoS) 방식의 블록체인 기술인 '우로보로스(Ouroboros)' 사용
  - 지분증명: 보유 코인수에 비례하여 블록 생성·검증 권한을 가지며 PoW와 달리 낮은 확장성 문제 및 과도한 에너지 소비, 중앙 집중화 문제 해결
- 2020년 9월 하드포코로 스마트 계약 기능이 추가, 그러나 파트너사 부족으로 아직까지 많은 DApp을 지원하고 있지 않음

## 솔라나(SOL)



- 아나톨리 야카벤코(Anatoly Yakavenko)에 의해 만들어졌으며, 2020년 3월 독자적 블록체인 생태계(메인넷)를 출시하여 빠르게 성장
- 거래 검증을 위한 역사증명(Proof of History)을 채택하여 현존하는 블록체인 중 가장 빠른 속도를 가진 것으로 평가되며, 초당 약 5만 건을 처리할 수 있는 빠른 거래속도(비트코인의 경우 초당 약 7건, 이더리움이 약 20~30건)와 건당 0.00025달러의 저렴한 수수료로 강점
  - 역사증명: 지분증명의 변형된 유형이며 검증가능지연함수(VDF; Verifiable Delay Function)를 도입, 합의를 단순화
- 뛰어난 성능으로 이더리움의 잠재적 경쟁자라는 평가를 받고 있음

## 이오스(EOS)



- 댄 라리머에 의해 개발된 DApp 플랫폼 이오스는 스마트 계약 기능을 갖췄으며, 개발사 블록원(Block.one)이 2018년 자체 메인넷 론칭
- 참가자들은 EOS 보유량에 따라 투표권을 행사해 대표자를 정하고, 21명의 선정된 대표자들에게 블록 생성 의사결정 권한을 위임하는 위임지분증명방식(DPoS)을 합의 알고리즘으로 채택
  - 위임지분방식: 대표자(21명)만 거래 검증하여 처리속도가 빠르며, 거래 수수료 무료
- '17~'18년에 진행된 EOS 암호화폐공개(ICO)는 역대 최대규모(40억 달러)로 이루어졌으나, ICO 관련 SEC 법률적 이슈로 벌금 조치, 투자자 집단 소송 등으로 주춤. 최근 대규모 투자(약 11조 원)를 유치하고 재도약 준비 중

## 클레이튼(Klaytn)/클레이(KLAY)

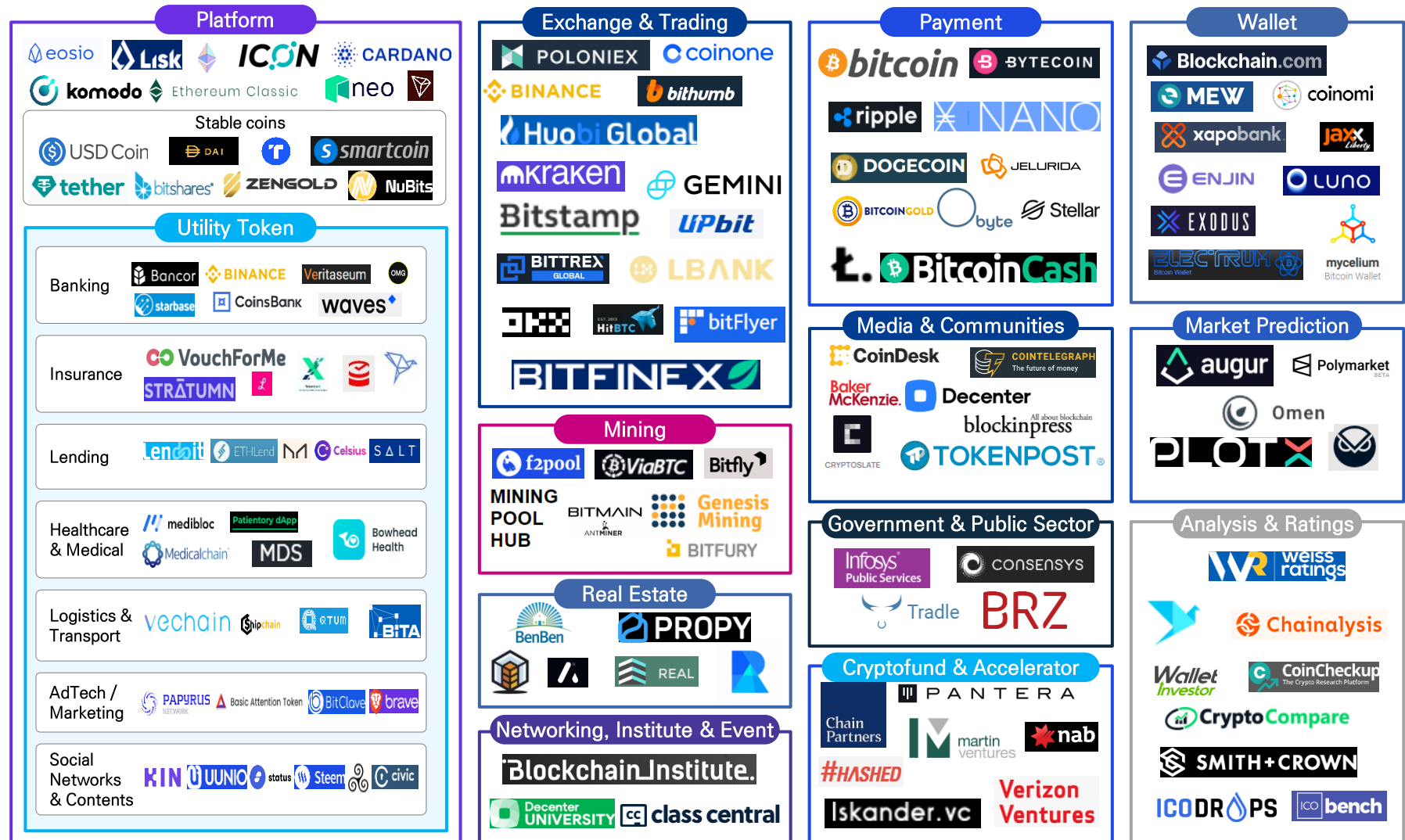


- 카카오의 블록체인 기술 관련 자회사 그라운드X가 2019년 론칭한 국산 메인넷 클레이튼은 이더리움 같은 DApp을 위한 블록체인 플랫폼
- 클레이튼은 퍼블릭·프라이빗 블록체인의 성격이 혼합된 하이브리드 블록체인으로서 플랫폼 대중화에 중점을 두고 있음
- 클레이튼 기반 블록체인 프로젝트도 최근 가시적인 성과를 보여주고 있음
  - 클레이튼 메인넷 기반 토큰 스왑 거래소인 '클레이스왑', 디지털아트 NFT거래소 '클립드록스', LandFi 메타버스 서비스 '클레이시티', 게임·SNS·메타버스 플랫폼 '클레이다이브' 등도 좋은 반응을 얻고 있음

Source: 코인데스크, 김승주 정보보호대학원 교수, 삼성KPMG 경제연구원 재구성

Source: 뱅크샐러드, 삼성KPMG 경제연구원 재구성

# 블록체인 생태계 Landscape



Source: <https://steemit.com>, 삼정KPMG 경제연구원 재구성

# 블록체인 기술의 한계 및 고려 사항

## 거래 취소 불가능

- 당초 이중지불을 방지하는 데 주안점을 두고 이미 승인된 거래가 취소되지 않도록 설계
- ✓ 블록체인 데이터나 코드를 변경하는 것은 매우 까다로우며, 한 체인이 버려지고 다른 체인이 이를 대신하는 하드포크가 종종 필요
- ✓ 이에 따라 이용자 착오나 범죄 등에 따른 우발적인 지급에 대해서도 이를 취소하거나 피해를 복구하기가 어려움

## 과도한 자원 투입

- 시스템 안전성에 대한 신뢰는 다수의 참가자가 경쟁적으로 채굴하는 과정에서 형성
- ✓ 실제 거래를 승인하는 데 필요한 수준에 비해 과도하게 많은 연산능력과 전력 등 자원이 투입
- ✓ 참가한 모든 컴퓨터가 모든 자료를 다운받거나 보관해야 하는 면에서 기존에 비해 비효율적

## 상호운용성 표준 부재

- 다양한 생태계와 블록체인 기반 시스템이 출현 중이나 블록체인 간 상호작용을 위한 표준 부재
- 블록체인 생태계가 커질수록 두 블록체인이 서로 정보를 전송할 수 있는 상호운용성에 대한 중요성 증가
- ✓ 블록체인 상호운용성을 개선을 위해 블록체인에 자산실재 여부에 대한 증명이 가능한 효율적으로 설계된 크로스체인 프로토콜 필요

## 부족한 확장성

- 블록체인 합의 메커니즘은 탈중앙화와 트랜잭션 처리량 개선이라는 두 가지 목표를 동시에 달성하기 어려움
- ✓ 블록체인의 크기가 커질수록 네트워크 참여에 요구되는 연산 성능, 스토리지 등이 증가, 일부 노드들만 트랜잭션 처리 가능하게 되어 중앙화됨
- ✓ 기술적인 오류 등 문제 발생 시 참가자들이 해결책을 채택·적용하기 위해 다수의 동의를 필요하여 의사결정이 지연될 수 있음

## 프라이빗 키 분실·탈취

- 각 블록체인 계정은 퍼블릭 키와 프라이빗 키라는 두 개의 키 보유하며, 분실·탈취 시 뚜렷한 해결책이 부재함
- ✓ 퍼블릭 키가 타인이 사용자가 자금 이체를 위한 계좌번호라면, 프라이빗 키는 계좌에 대한 통제권을 갖는 패스워드와 같음
- ✓ 사용자가 만약 프라이빗 키를 분실 또는 탈취당하게 되는 경우, 사실상 이를 해결할 마땅한 방법이 없으며, 프라이빗 키로 묶인 코인 또한 찾을 방법이 없음

## 미흡한 법·규제

- 블록체인 시장은 단 기간에 큰 성장을 이뤘으나, 관련 투자·비즈니스 등 법적 불확실성 존재
- ✓ 블록체인 산업은 빠르게 발전하고 있으나 제도가 발전 속도를 따라가고 있지 못함
- ✓ 상당수 기업이 블록체인 생태계에 높은 관심을 가지고 있으나, 높은 관심과 대조적으로 관련 규제가 미흡하여 기술 개발·사업 투자 등에 대한 불확실성이 높아 실제 사업 참여는 미비

Source: 해시넷, 언론보도 종합, 삼성KPMG 경제연구원 재구성

# [참고] 블록체인 주요 비즈니스 Player

Level 1				Level 2				Level 3											
Level 1		Level 2		Level 3		Players		Website		Level 1		Level 2		Level 3		Players		Website	
Crypto-currency	Payment		비트코인 bitcoin	https://bitcoin.org/ko/				솔트 salt	https://www.saltlending.com/										
			리플 ripple	https://ripple.com/				Lending	이더렌드 ethlend	https://ethlend.io/ko/									
			스탈라루멘 stellar	https://www.stellar.org/					메이커 maker	https://makerdao.com/									
			라이트코인 litecoin	https://litecoin.com/					셀셔스 celsius	https://celsius.network/									
			비트코인캐쉬 bitcoinCash	https://www.bitcoincash.org/				Real Estate	렌두잇 lendoit	http://lendoit.com/									
			비트코인골드 bitcoinGlod	https://bitcoingold.org/					리얼 real	https://www.real.markets/									
			바이트코인 bytecoin	https://bytecoin.org/					아틀란트 atlant	https://atlant.io/									
			나노 nano	https://nano.org/en				Insurance	프로피 propy	https://propy.com/									
			도지코인 dogecoin	http://dogecoin.com/					벤벤 benben	http://www.benben.com.gh/									
			넴 NEM	http://nem.io/					바우치포미 VouchForMe	http://vouchforme.co									
버지 verge	https://vergecurrency.com/	Utilities Token	스트라툼 stratumn	https://stratumn.com															
엔엑스티 Nxt	https://nxtplatform.org/		레모네이드 Lemonade	https://www.lemonade.com/															
바이트볼 byteball bytes	https://byteball.org/		가드타임 Guardtime	https://guardtime.com/															
대쉬 dash	https://www.dash.org/	Logistics & Transport	이더리스크 etherisc	https://etherisc.com/															
지코인 Zcash	https://z.cash/		피덴시아X fidentiaX	https://www.fidentiax.com/															
모네로 monero	https://getmonero.org/		비체인 vechai	https://www.vechain.org/															
하이퍼레저 hyperledger	https://www.hyperledger.org/	Healthcare & Medica	퀀텀 Qtum	https://qtum.org/															
이더리움 Ethererum	https://www.ethererum.org/		쉽체인 shipchain	https://shipchain.io/															
이오스 EOS	https://eos.io/		비타 BiTA	https://bita.studio/															
Platform		Platform	코모도 komodo	https://komodoplatform.com/				메디블록 medibloc	https://medibloc.org/en/										
카다노 cardano		https://www.cardano.org/en/home/	메디컬체인 medicalchain	https://medicalchain.com/en/															
아이콘 ICON		https://www.icon.foundation/?lang=en	메디쉐어 MediShares	http://www.medishares.org/															
네오 NEO		https://neo.org/	패이션토리 patientory	https://patientory.com/															
리스크 lisk		https://lisk.io/	바우헤드헬스 bowhead	https://bowheadhealth.com/															
이더리움클래식 ethererum classic		https://ethereumclassic.github.io/	Government & Public	인포시스 infosys				https://www.infosyspublicservices.com/											
보스코인 BosCoin		https://boscoin.io/		컨센시스 ConsenSys				https://consensys.net/											
TRON		https://tron.network		트레들 tradle				https://tradle.io/											
Asset-backed Stable coins				테더 tether				https://tether.to/				스팀잇 steemit	https://steem.io/						
누비츠 nubits				https://nubits.com/				Social Networks & Contents				아카샤 akasha	https://akasha.world/						
젠골드 ZenGold	http://www.zengold.org/			스테이투스 status	https://status.im/														
스마트코인 SmartCoin	http://smartcoin.cc/	ADtech / Marketing	유니오 uunio	https://uun.io/IM															
비트USD bitusd	https://bitshares.org/		키브 civic	https://www.civic.com/															
스팀달러 steemdollar	https://steem.io/		킨 kin	http://kinecosystem.org/															
Utilities Token	Banking		뱅크르 bankor	https://www.bancor.network/				베이직어텐션토큰 basic attention token	https://basicattentiontoken.org/ko										
바이낸스코인 binance coin			https://www.binance.com/	브레이브 brave				https://brave.com/											
오미세고 omiseGO			https://omisego.network/	비트클레이브 BitClave				https://www.bitclave.com/											
웨이브 waves			https://wavesplatform.com/	파피루스 papyrus				https://papyrus.global/											
코인스뱅크 coinsbank			https://coinsbank.com/																
스타베이스 starbase	https://starbase.co/																		
베리타시움 veritaseum	https://veritas.veritaseum.com/																		

Source: https://steemit.com, 삼성KPMG 경제연구원 재구성

# [참고] 블록체인 주요 비즈니스 Player (계속)

Level 1	Level 2	Level 3	Players	Website	Level 1	Level 2	Level 3	Players	Website
Mining			비트메인 앤트풀 antPool	www.antpool.com	Analysis & Ratings			Weiss 와이즈레이팅즈	https://weisscryptocurrencyratings.com/
			비트메인 비티시닷컴 bitmain	https://btc.com/				ICO벤치 ICO Bench	https://icobench.com/icos/cryptocurrency
Wallet			비아비티씨 viaBTC bitmain	https://pool.viabtc.com/	Media & Communities			ICO드랍 ICO drops	https://icodrops.com/
			비트플라이 이더풀 bitfly ethpool	https://www.ethpool.org/				크립토크컴퍼 crypto compare	https://www.cryptocompare.com/
			비트플라이 이더마인 bitfly ethermine	https://www.ethermine.org/				스미스+크라운 Smith+Crown	https://www.smithandcrown.com/
			에프투풀 f2pool	https://www.f2pool.com/				코인체크업 coincheckup	https://coincheckup.com/
			마닝풀허브 mining pool hub	https://miningpoolhub.com/				월렛인베스터 walletinvestor	https://walletinvestor.com/
			비트퓨리 Bitfury	http://bitfury.com/				체인널러시스 Chainalysis	https://www.chainalysis.com/
			제네시스마이닝 Genesis Mining	https://www.genesis-mining.com/				윙스 wings	https://www.wings.ai/#/home/discover
			마이이더월렛 myetherwallet	https://www.myetherwallet.com/				coindesk 코인데스크	https://www.coindesk.com/
			마이셀리움 mycelium	https://wallet.mycelium.com/				cointelegraph 코인텔레그래프	https://cointelegraph.com/
			엑스더스 exodus	https://www.exodus.io/				디센터 decenter	http://www.decenter.kr/
Exchange & Trading	Centralized		엔진 enjin wallet	https://enjinwallet.io/	Network & Institute & Event			크립토슬레이트닷컴 cryptoslate	https://cryptoslate.com
			블록체인월렛 blockchain	https://www.blockchain.com/				피넥터 finector	http://finector.com/
			잭스 jaxx	https://jaxx.io/				블록인프레스 blockinpress	https://blockinpress.com/
			코이노미 coinomi	https://coinomi.com/				코인판 coinpan	https://coinpan.com/
			자포 xapo	https://xapo.com/				뱅크맥킨지 bankermckenzie	http://financialinstitutions.bankermckenzie.com/
	일렉트럼 electrum		https://electrum.org/	트렌포스트 tokenpost				https://tokenpost.kr/	
	루노 luno		https://www.luno.com/	디센터 유니버시티 Decenter university				http://decenteruniv.com/	
	트레저 trezor		https://www.buypass.com/	블록체인 인스티튜트 blockchain institute				https://blockchaininstitute.io/	
	레저 ledger		https://www.ledgerwallet.com/r/81c0	블록체인 스터디 blockchain studies				http://www.blockchainstudies.org/	
	트러스트 trust		https://trustwalletapp.com/	클래스센트럴 class-central				https://www.class-central.com/tag/blockchain	
Decentralized			바이낸스 binance	https://www.binance.com/	Crypto-fund & Accelerator			체인파트너스 chainpartners	http://www.chain.partners/
			후오비 huobi	https://www.huobi.pro				이스칸더 iskander	http://iskander.vc/
			오케이엑스 OKX	https://okx.com				블록체인캐피탈 blockchain capital	http://blockchain.capital/
			비트피넥스 bitfinex	https://www.bitfinex.com				판테라 pantera	https://www.panteracapital.com/
			빗썸 bithumb	https://www.bithumb.com/				마틴벤처스 martin ventures	https://www.martinventures.com/
크라켄 kraken	https://www.kraken.com/		베리즌벤처스 verizon ventures	www.verizonventures.com/					
업비트 upbit	https://upbit.com/		NAB벤처스 NAB ventures	https://www.nab.com.au/sites/business/customer/ventures					
폴로니엑스 poloniex	https://poloniex.com/		해쉬드 hashed	https://www.hasheds.com/					
코인원 coinone	https://coinone.co.kr/								
히트비티씨 hitBTC	https://hitbtc.com								
비트스탬프 bitstamp	https://www.bitstamp.net/								
비트플라이어 BitFlyer	https://bitflyer.jp/								
비트트렉스 bittrex	https://bittrex.com/								
엘뱅크 LBank	https://www.lbank.info/								
제미니 gemini	https://gemini.com/								
제로엑스 0x	https://0xproject.com/								
비스큐 bisq	https://bisq.network/								
에어스왑 airswap	https://www.airswap.io/								

Source: https://steemit.com, 삼성KPMG 경제연구원 재구성

# Contents

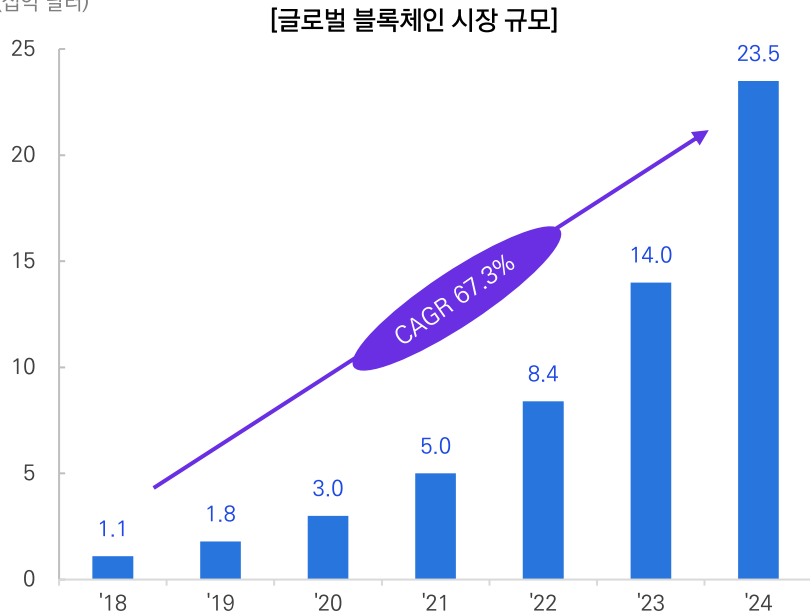
	Page
I. Web 3.0으로의 진화와 블록체인	2
<b>II. 글로벌·국내 블록체인 시장 현황</b>	<b>23</b>
III. 산업에서의 블록체인 활용 방안·동향	31
IV. 결론 및 시사점	42



# 글로벌 블록체인 시장 현황

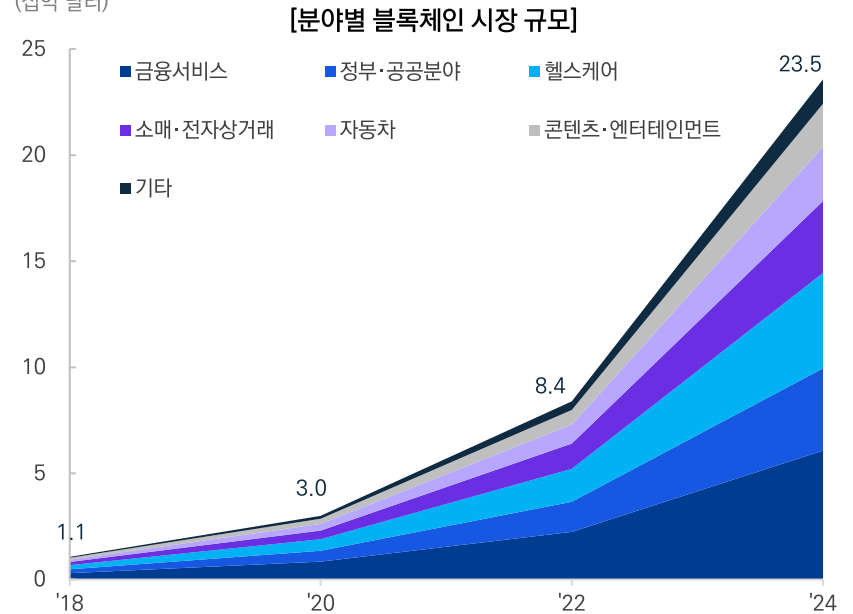
## 글로벌 블록체인 시장 전망

(십억 달러)



Source: MarketsandMarkets, 중소기업 전략기술로드맵 2021-2023, 삼정KPMG 경제연구원 재구성

(십억 달러)



Source: MarketsandMarkets, 중소기업 전략기술로드맵 2021-2023, 삼정KPMG 경제연구원 재구성

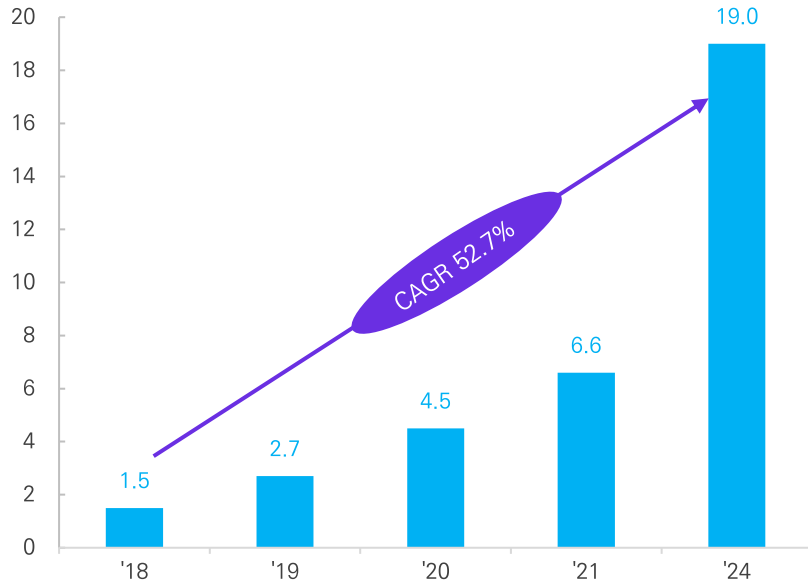
▪ 글로벌 블록체인 시장 규모는 '24년까지 235억 달러를 넘어설 것으로 전망

- '18~'24년까지 글로벌 블록체인 시장의 연평균성장률(CAGR)은 약 67.3%에 달할 것으로 전망됨
- '24년까지 7개 분야 중 금융서비스가 가장 큰 규모(60.8억 달러)로 성장하고, 다음으로 헬스케어(44.9억 달러), 정부·공공분야(38.7억 달러), 소매·전자상거래(34.0억 달러), 자동차(25.5억 달러), 콘텐츠·엔터테인먼트(20.3억 달러), 기타(11.5억 달러) 순으로 성장할 것으로 전망

# 글로벌 블록체인 시장 현황 (계속)

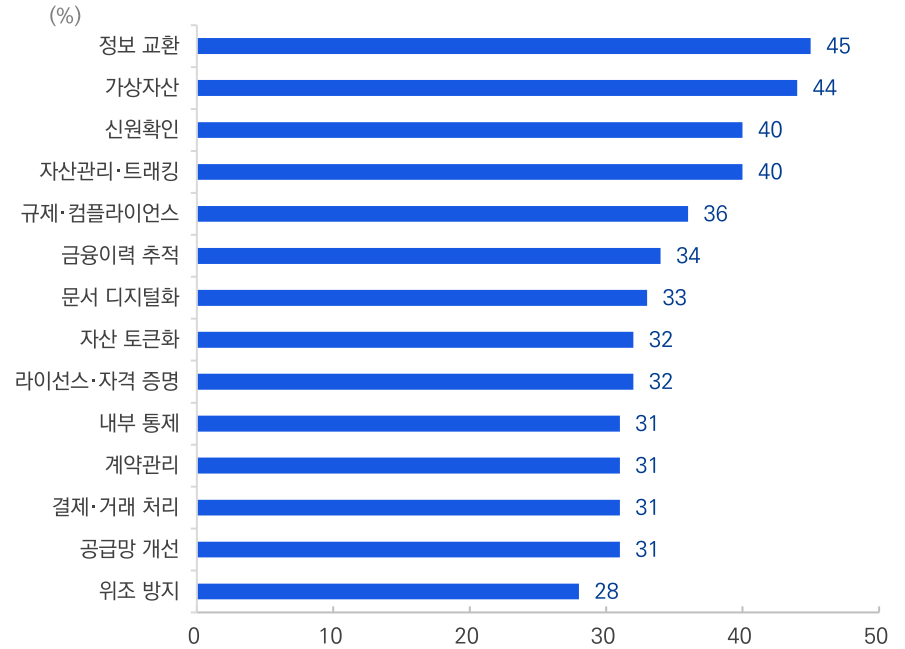
## 글로벌 블록체인 솔루션 지출 규모 전망

(십억 달러)



Source: IDC, Statista, 삼정KPMG 경제연구원 재구성

## 전 세계 블록체인 기술 적용 분야



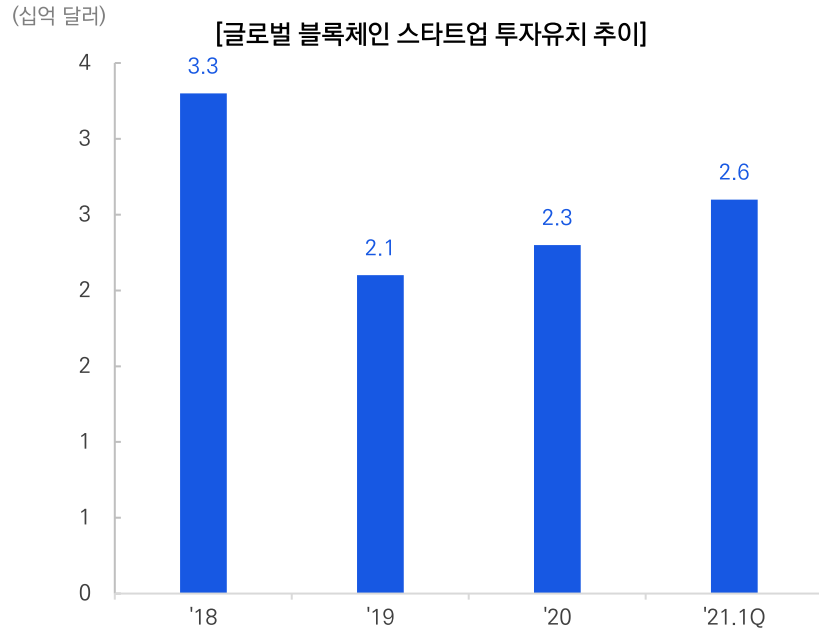
Source: Statista, 삼정KPMG 경제연구원 재구성

Note: 2021년 4월 1,280명의 고위임원 및 실무자를 대상으로 한 설문조사

- '21년 글로벌 블록체인 솔루션 지출 규모는 66억 달러에 이를 것으로 전망되며, '24년까지 약 190억 달러에 달할 것으로 전망
- 블록체인 기술 활용에 대한 설문조사 결과, 정보 교환이 블록체인 활용의 가장 큰 비중을 차지
  - '21년 4월 기준 1,280명의 고위임원 및 실무자를 대상으로 한 설문조사 결과, 응답자의 45%가 블록체인 기술을 기반으로 안전한 정보 교환을 위해 블록체인을 활용하고 있다고 답하였으며, 그 뒤를 이어 가상자산(44%), 신원확인(40%), 자산관리·이력 트래킹(40%) 등도 상위권을 차지

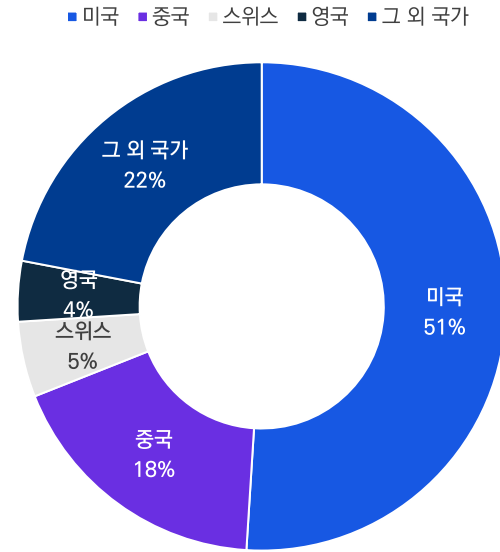
# 글로벌 블록체인 시장 현황 (계속)

## 글로벌 블록체인 투자 현황



Source: CB Insights, Bloomberg, Statista, 삼정KPMG 경제연구원 재구성

(%) [전 세계 블록체인 기업 Funding에 대한 국가별 비중]

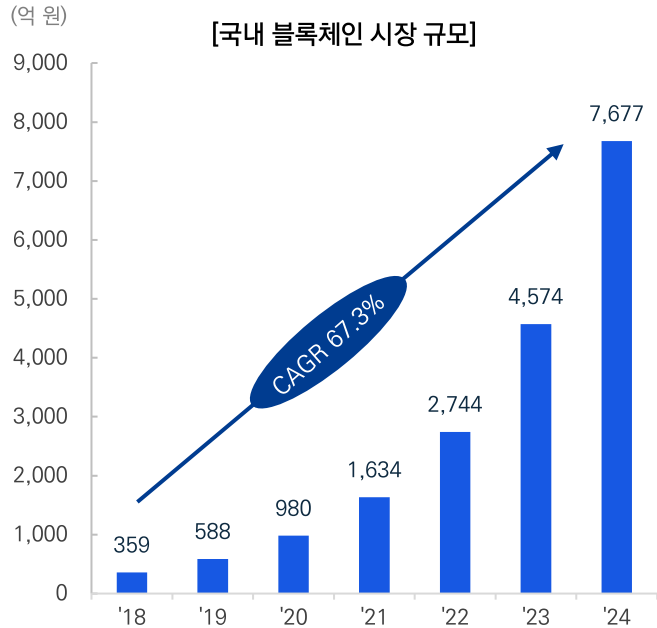


Source: CB Insights, Statista, 삼정KPMG 경제연구원 재구성  
Note: 집계기간 2015~2019년

- 전 세계 블록체인 스타트업은 '21년 1분기 26억 달러의 투자금(벤처캐피탈 펀딩)을 유치하여, '20년 전체 투자금보다 많은 금액을 기록
- '15년부터 '19년까지 전 세계 블록체인 기업의 전체 자금 조달금액 중 미국의 투자 비중이 51%에 달하여 전 세계에서 가장 큰 비중을 차지
  - 중국도 동 기간 동안 전체 조달자금의 18%의 비중을 차지하여 미국 다음으로 높았으며, 그 뒤를 이어 스위스(5%), 영국(4%) 순으로 나타남

# 국내 블록체인 시장 현황

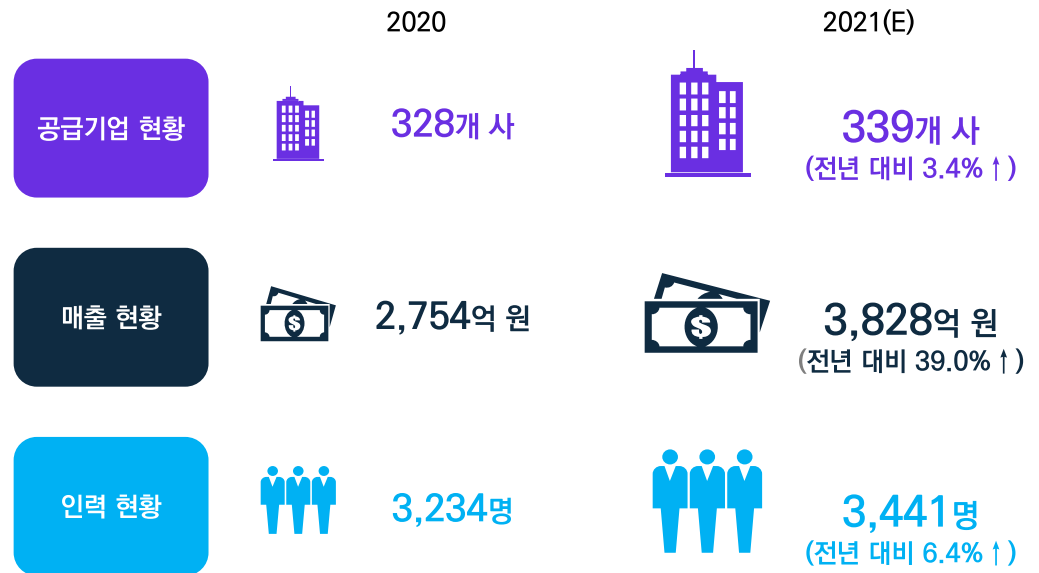
## 국내 블록체인 시장 전망



Source: MarketsandMarkets, 중소기업 전략기술로드맵 2021-2023, 삼정KPMG 경제연구원 재구성

- 국내 블록체인 시장 규모는 '24년까지 7,677억 원을 넘어설 것으로 전망
- '18~'24년까지 국내 블록체인 시장은 연평균 67.3%의 성장을 달성할 것으로 전망

## 국내 블록체인 산업 Overview

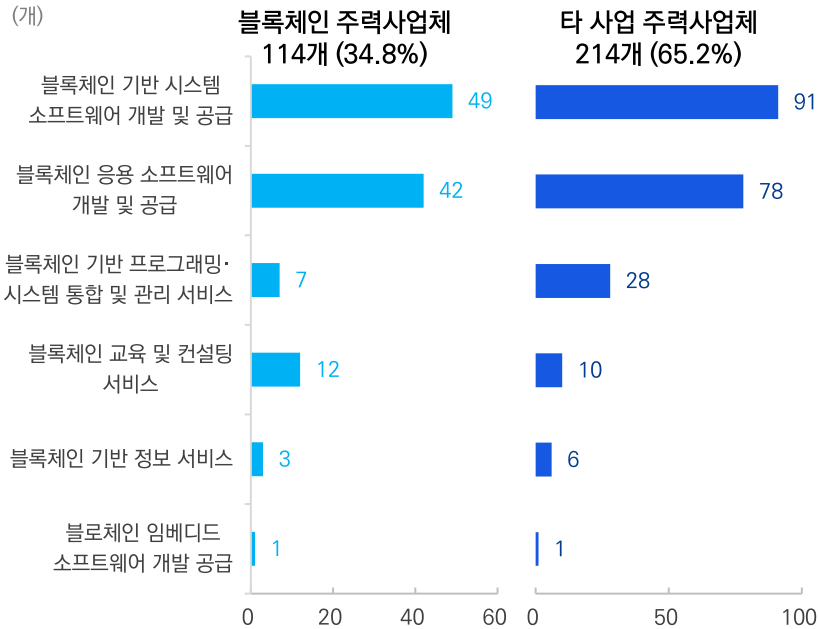


Source: 과학기술정보통신부, '2021년도 블록체인 산업 실태조사', 삼정KPMG 경제연구원 재구성

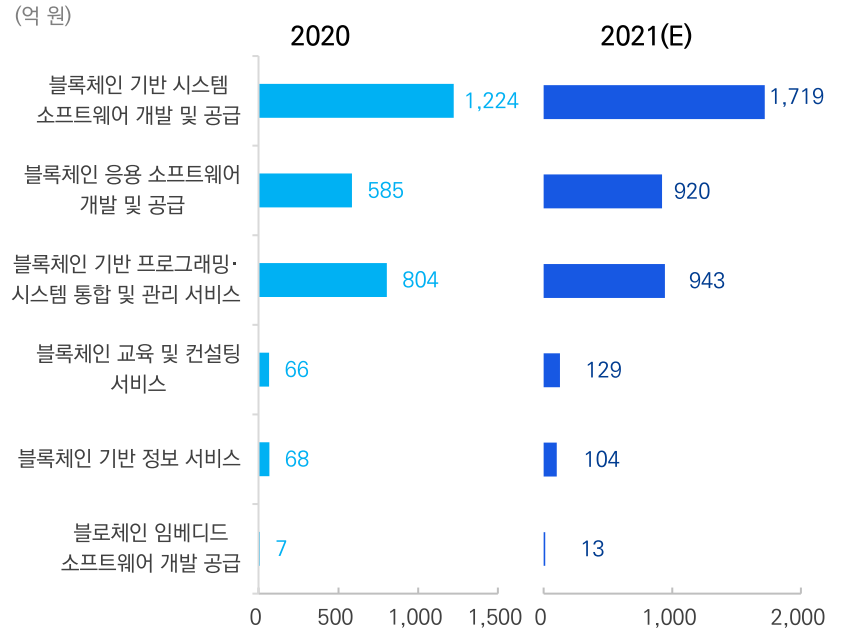
- '20년 블록체인 사업을 영위 중인 블록체인 공급기업(가상자산 기업 제외)은 328개로 조사
  - 21년 블록체인 기업은 339개로 늘어날 것으로 전망
- '20년 블록체인 부문 매출액은 약 2,754억 원(기업 평균 8.4억 원)을 기록
  - '21년 예상 매출액은 3,828억 원(평균 11.7억 원)으로 전망
- '20년 기준 블록체인 부문 종사자 수는 약 3,234명으로 집계됨
  - 블록체인 부문 종사자는 '21년 3,441명으로 증가 전망

# 국내 블록체인 시장 현황 (계속)

국내 블록체인 기업 산업 분류체계별 분포



국내 블록체인 기업 산업 분류체계별 매출액



Source: 과학기술정보통신부, '2021년도 블록체인 산업 실태조사', 삼정KPMG 경제연구원 재구성

Note1: 전체 328개 블록체인 기업 대상

Note2: 주력사업 기준은 블록체인이 주력사업인 기업, 영위사업은 타 사업이 주력사업인 기업

Source: 과학기술정보통신부, '2021년도 블록체인 산업 실태조사', 삼정KPMG 경제연구원 재구성

Note: 전체 328개 블록체인 기업 대상

- '20년 기준 산업 분류체계별 분포로 '블록체인 기반 시스템 소프트웨어 개발 및 공급업(140개, 42.7%)'에 속하는 기업이 가장 높은 비중을 차지
- 뒤를 이어 '블록체인 기반 응용 소프트웨어 개발 및 공급업(120개, 36.6%)', '블록체인 기반 프로그래밍·시스템 통합 및 관리 서비스업(35개, 10.7%)' 순으로 나타남
- '20년 기준 블록체인 기업 매출도 '블록체인 기반 시스템 소프트웨어 개발 및 공급업(1,224억 원)'이 가장 큰 비중을 차지
- 그 뒤를 이어 '블록체인 기반 프로그래밍·시스템 통합 및 관리 서비스(804억 원)', '블록체인 응용 소프트웨어 개발 및 공급(585억 원)', '블록체인 기반 정보 서비스(68억 원)', '블록체인 교육 및 컨설팅 서비스(66억 원)', '블록체인 임베디드 소프트웨어 개발 공급(7억 원)' 순으로 나타났으며, 전체 블록체인 기업 중 매출 발생 비율은 84.1%에 이르는 것으로 조사됨

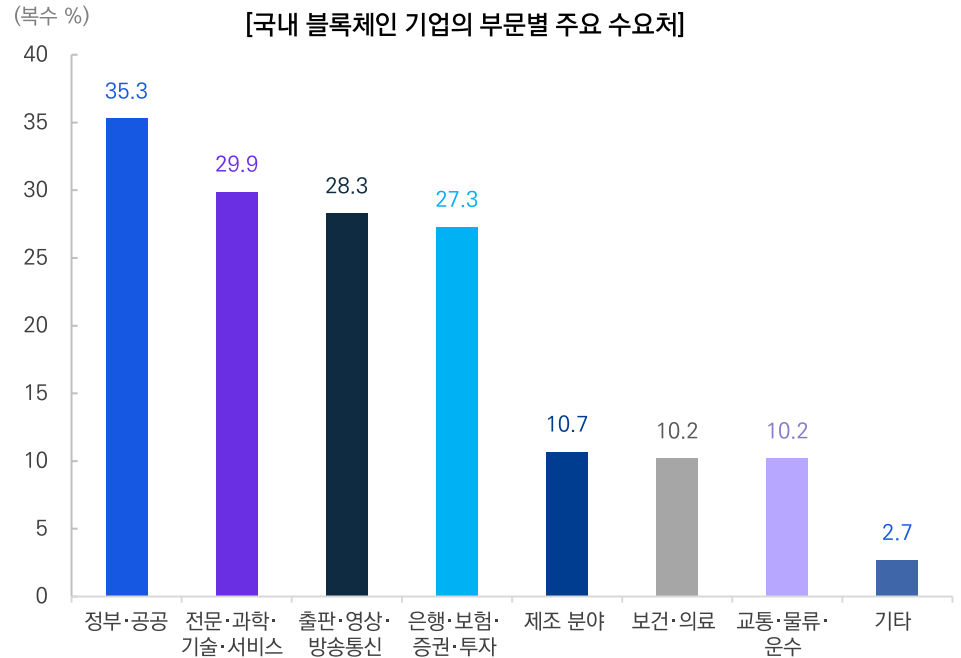
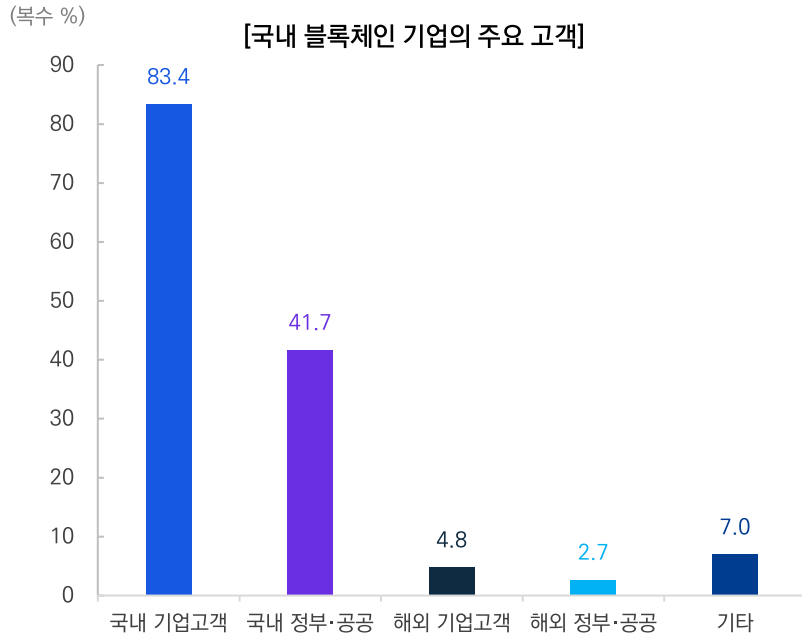
## [참고] 국내 블록체인 산업 대분류 (2021년도 블록체인 산업 실태조사 기준)

구분	개념	예시	제외
블록체인 기반 시스템 소프트웨어 개발 및 공급	<ul style="list-style-type: none"> <li>블록체인 기술 기반으로 상품 개발을 가능하게 하는 기술이나, 개발 지원 프로세스를 개발 및 공급하는 산업 활동</li> </ul>	<ul style="list-style-type: none"> <li>탈중앙화앱(DApp), 응용앱 등 다양한 블록체인 응용 소프트웨어 개발을 지원하는 소프트웨어 플랫폼 등</li> <li>- 하이퍼레저패브릭, 이더리움, 이오스</li> </ul>	<ul style="list-style-type: none"> <li>외주 개발을 통한 블록체인 소프트웨어를 이용하여 다양한 비즈니스 모델 혹은 서비스를 제시하는 산업 활동, 하드웨어 등에 탑재된 임베디드 소프트웨어</li> </ul>
블록체인 응용 소프트웨어 개발 및 공급	<ul style="list-style-type: none"> <li>블록체인 기술이 적용된 응용 소프트웨어를 개발 및 공급하는 산업 활동</li> <li>- 인터넷, 휴대폰 등 모바일용 블록체인 기반 응용앱 개발 및 공급하는 산업 활동</li> </ul>	<ul style="list-style-type: none"> <li>블록체인 플랫폼 기반 앱, 블록체인 기술이 적용된 금융·보험·저작권 관리 및 공증, 유통 추적, 의료 및 건강관리, 기타 서비스용 소프트웨어 개발 및 공급</li> </ul>	<ul style="list-style-type: none"> <li>외주 개발을 통해 공급된 블록체인 소프트웨어를 활용한 산업 활동, 하드웨어 등에 탑재된 임베디드 소프트웨어</li> </ul>
블록체인 기반 프로그래밍·시스템 통합 및 관리 서비스	<ul style="list-style-type: none"> <li>특정 고객의 요구에 의해 블록체인 기술이 적용된 주문형 소프트웨어를 자문, 개발 및 공급, 블록체인 기술 적용을 위한 컴퓨터 하드·소프트웨어 및 통신기술을 통합하는 컴퓨터 시스템을 기획·설계하는 산업 활동</li> </ul>	<ul style="list-style-type: none"> <li>블록체인 기반 주문형 응용 소프트웨어 제작, 블록체인 기반 주문형 컴퓨터 소프트웨어 분석 및 설계, 블록체인 기반 시스템 통합(SI) 구축 및 설계, 블록체인 기반 시스템 통합 설계 자문</li> </ul>	<ul style="list-style-type: none"> <li>상용 패키지 소프트웨어 개발 및 공급, 시스템 통합용 컴퓨터 프로그래밍 서비스</li> </ul>
블록체인 교육 및 컨설팅 서비스	<ul style="list-style-type: none"> <li>블록체인 기술·서비스 도입 및 서비스 모델, 구축 방식 등에 대한 컨설팅과 블록체인 인력양성 및 역량 강화를 위한 교육을 포함</li> </ul>	<ul style="list-style-type: none"> <li>블록체인 기반 시스템 통합(SI) 구축 및 설계 등에 대한 컨설팅, 블록체인 전문교육 등</li> </ul>	<ul style="list-style-type: none"> <li>블록체인을 적용하지 않는 상용 패키지 소프트웨어 개발 및 공급, 시스템 통합용 컴퓨터 프로그래밍 서비스 등에 대한 컨설팅 및 교육</li> </ul>
블록체인 기반 정보 서비스	<ul style="list-style-type: none"> <li>블록체인 기술 활용·개발 등을 위한 기반이 되는 인프라·플랫폼·소프트웨어 등을 호스팅하는 서비스 또는 블록체인 기술 적용과 관련하여 달리 분류되지 않는 각종 정보서비스 활동</li> </ul>	<ul style="list-style-type: none"> <li>블록체인용 IaaS(서버, 스토리지, 네트워크 등 인프라 제공), 블록체인용 PaaS(개발도구, 미들웨어, 운영시스템 등 플랫폼 제공), 블록체인용 SaaS(소프트웨어 제공 서비스 등)</li> </ul>	<ul style="list-style-type: none"> <li>블록체인 기술 활용 목적을 제외한 일반형 클라우드 서비스</li> </ul>
블록체인 임베디드 소프트웨어 개발 공급	<ul style="list-style-type: none"> <li>제한된 자원 여건 하 실시간·안정적으로 성능을 발휘할 수 있도록 블록체인 기술이 탑재된 하드웨어가 포함된 제품(칩셋)을 개발 및 공급하는 산업활동</li> </ul>	<ul style="list-style-type: none"> <li>블록체인 기반 투표 등을 위해 블록체인 기술이 적용된 일체형 시스템 등</li> </ul>	<ul style="list-style-type: none"> <li>블록체인 시스템의 보안 강화 및 성능을 향상시킬 수는 있으나, 블록체인 기술이 적용되지 않는 제품 혹은 칩셋</li> </ul>

Source: 과학기술정보통신부, '2021년도 블록체인 산업 실태조사', 삼성KPMG 경제연구원 재구성

# 국내 블록체인 시장 현황 (계속)

## 주요 블록체인 기업의 주요 고객 및 수요처



Source: 과학기술정보통신부, '2021년도 블록체인 산업 실태조사', 삼정KPMG 경제연구원 재구성  
 Note: 응답기업 187개 사(복수응답), 2021년 조사 시점 기준

Source: 과학기술정보통신부, '2021년도 블록체인 산업 실태조사', 삼정KPMG 경제연구원 재구성  
 Note: 응답기업 187개 사(복수응답), 2021년 조사 시점 기준

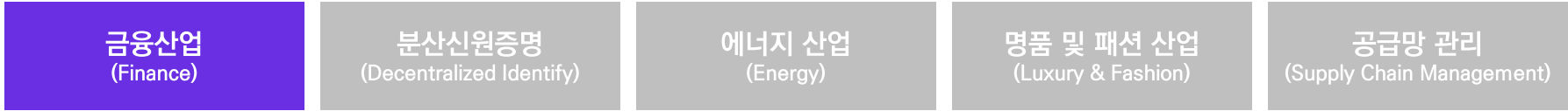
- 국내 블록체인 기업의 주요 고객은 국내 기업고객이 가장 높은 비중(83.4%)을 차지
  - 뒤를 이어 국내 정부·공공(41.7%), 기타(7.0%), 해외 기업고객(4.8%), 해외 정부·공공(2.7%) 순으로 나타남
- 국내 블록체인 기업의 주요 수요처는 정부·공공분야가 35.3%로 가장 높은 비중을 차지
  - 다음으로 전문·과학·기술·서비스(29.9%), 출판·영상·방송통신(28.3%), 은행·보험·증권·투자(27.3%), 제조 분야(10.7%) 순으로 나타남

# Contents

	Page
I. Web 3.0으로의 진화와 블록체인	2
II. 글로벌·국내 블록체인 시장 현황	23
<b>III. 산업에서의 블록체인 활용 방안·동향</b>	<b>31</b>
IV. 결론 및 시사점	42



# 산업·분야별 블록체인 활용 동향



## 금융산업 관련 블록체인의 공통 기대효과

- 1 거래, 결제, 보관 등 모든 참가자의 워크플로우를 동기화
- 2 기관 간 정산업무 관련 운영부담 감소
- 3 거래 데이터 관련 단일 Source 제공
- 4 스마트 계약 기반으로 프로세스 자동화
- 5 Compliance 및 Reporting 업무 자동화

## 업권 별 블록체인 기대효과

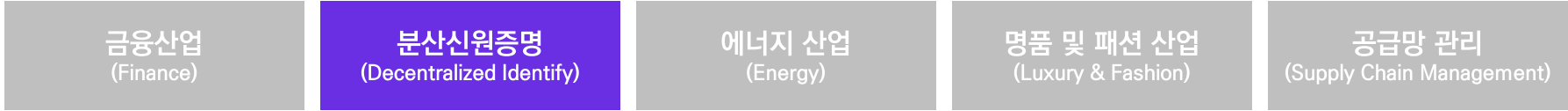
주식 시장	<ul style="list-style-type: none"> <li>자금흐름의 가시성 증가에 따라 위험 자본, 청산 자금, 결제 유동성 등에 대한 준비금 감소로 유동성 개선</li> <li>주식발행자는 중개자에 의존하지 않고 직접 상장함으로써 자본 비용 감소</li> </ul>	Repo 시장	<ul style="list-style-type: none"> <li>스마트 계약을 통해 담보물을 확보함으로써 당사자 간 담보물 실제 이전 필요성 감소</li> <li>전체 시장 유동성을 개선하고 자금 조달 비용 절감, 거래 실패 가능성 감소</li> </ul>
채권 시장	<ul style="list-style-type: none"> <li>스마트 계약을 통해 채권상품 조건, 거래 및 결제 상태, 소유권 및 이자/원금 상황에 대한 투명한 정보 공개</li> <li>스마트 계약을 통해 이자/원금지급, 정산 등 전반적 업무 자동화 및 새로운 채권상품 제조 가능</li> <li>비싼 인프라 구축 비용 절감 등</li> </ul>	자산관리 시장	<ul style="list-style-type: none"> <li>투자자 기반 확대, 접근성 및 펀드 유동성 증가에 기여</li> <li>비효율적이거나 중복된 프로세스 및 정산업무 감소로 투자자의 비용 절감</li> <li>자산 관리자와 투자자의 투명성 향상</li> </ul>
파생상품 시장	<ul style="list-style-type: none"> <li>거래조건, 가치평가 등 오류·불일치 감소로 거래 실패 발생률 감소</li> <li>정산 관련 복잡성이 개선되어 운영/거래 비용 절감</li> <li>참여자들의 파생상품 포지션 투명성 향상</li> </ul>	유동화 시장	<ul style="list-style-type: none"> <li>개별 대출에 대한 감사/검증 필요성 제거 및 투명성 증대로 투자자 리스크 이해도 증가</li> <li>대출 데이터 신뢰도 증가 및 밸류체인 전반에 걸쳐 모니터링 필요성 감소</li> <li>자금 정산을 위한 요구자본 감소</li> </ul>

Source: WEF(2021), 'Digital Assets, Distributed Ledger Technology and the Future of Capital Markets'

Source: WEF(2021), 'Digital Assets, Distributed Ledger Technology and the Future of Capital Markets'



# 산업·분야별 블록체인 활용 동향 (계속)



### 분산신원증명(Decentralized Identify, DID)

#### 분산신원증명이란?

- 온라인상에서 블록체인을 기반으로 사용자가 스스로 신원 등에 대한 증명관리, 신원정보 제출 범위 및 제출대상 등을 통제. 수행할 수 있도록 하는 신원관리 체계
- 자기 주권 신원 모델과 블록체인을 기반으로 제3인증기관 없이 사용자 신원정보의 노출 범위, 사용 목적에 따라 자신의 신원정보에 주권을 행사할 수 있음

The diagram illustrates the DID process flow: 1. Issuer (발급자) issues DID information to the Owner (소유자). 2. Owner stores DID in their Wallet. 3. Owner provides DID to Verifier (검증자). 4. Verifier checks DID against Blockchain Ledger (블록체인 보관소). 5. Blockchain Ledger returns verification results to Verifier. 6. Verifier provides service (서비스 제공) to Owner based on verification.

Source: 심사평가원

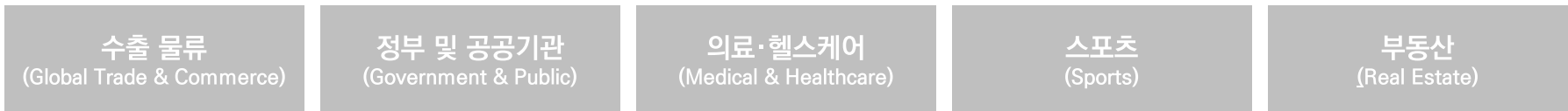
### 분산신원증명 특징

<b>지속성</b>	서비스 제공자에 의해 신원정보가 관리되지 않으므로, 외부적 환경의 변화와 관계없이 사용자가 자신의 신원정보를 지속적으로 사용가능
<b>휴대성</b>	신원증명이 필요한 경우 언제든지 사용자 스스로 스마트폰이나 ID카드 등으로 신원정보를 선택 후 제공이 가능
<b>개인정보 보호</b>	사용자가 스스로 신원정보를 관리하므로, 서비스 제공자는 서비스에 필요한 정보 이외의 사용자의 개인정보는 확인이 불가능
<b>피어(Peer)기반</b>	신원정보의 발행 검증은 특정기관에 종속적이지 않고, 피어기반으로 독립적으로 운영하며, 누구나 필요한 신원정보를 생성·이용 가능

### 분산신원증명 서비스 적용 및 연구 사례

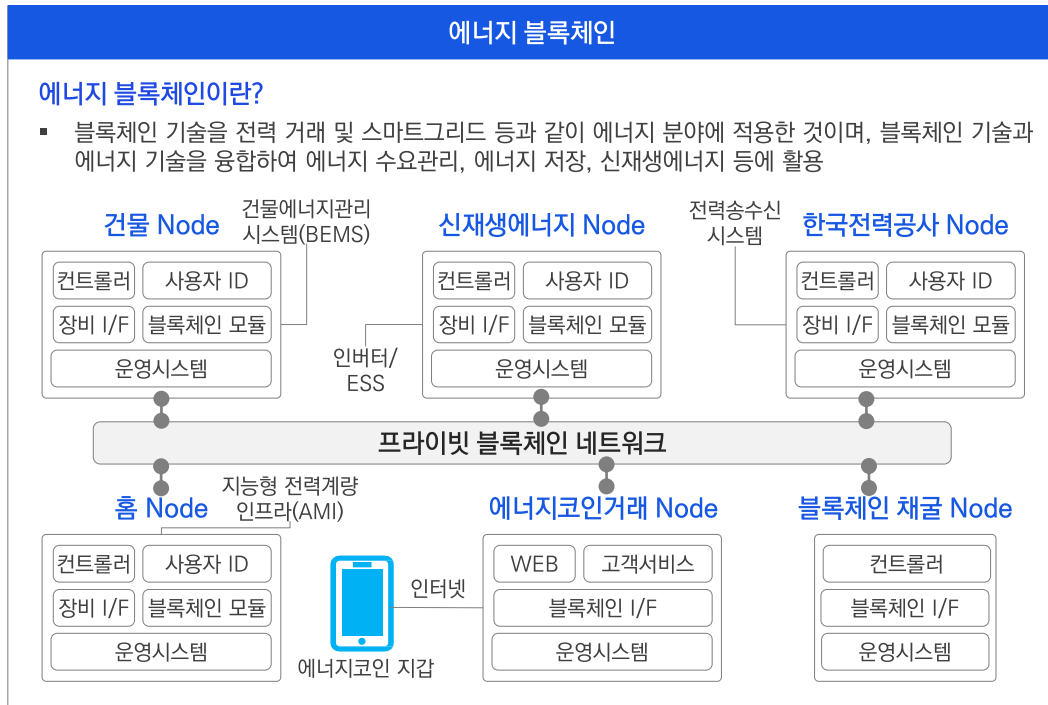
블록체인 기반 위험 구조물 안전진단 플랫폼 PID(Private ID)	시티랩스컨소시엄, SKT ReapChain	건축물 IoT디바이스
블록체인 기반 자율주행자동차 플랫폼 COOV	세종시, 라온시큐어	자율주행차량
모바일 공무원증	질병관리청, 블록체인랩스	예방접종증명서
블록체인 기반 비대면 국민연금 수급확인 시스템	행정안전부, 라온시큐어	공무원증
시큐어 키(Securekey)	드림시큐리티, 삼성SDS, 시스젠 캐나다 주요 공공기관·은행 등	국민연금 수급권 사용자 간편인증

Source: 한양대학교 권준우 교수(2021), '블록체인 기반 분산신원증명의 이해와 서비스 적용 사례'



# 산업·분야별 블록체인 활용 동향 (계속)

금융산업 (Finance)	분산신원증명 (Decentralized Identify)	에너지 산업 (Energy)	명품 및 패션 산업 (Luxury & Fashion)	공급망 관리 (Supply Chain Management)
-------------------	------------------------------------	--------------------	----------------------------------	-------------------------------------



Source: 과학기술정책연구원(2018), '에너지 블록체인 도입방안 연구'  
 Note: BEMS: Building energy management systems, AMI: Advanced Metering Infrastructure, I/F: Interface

### 에너지 블록체인 유형 및 주요 사례

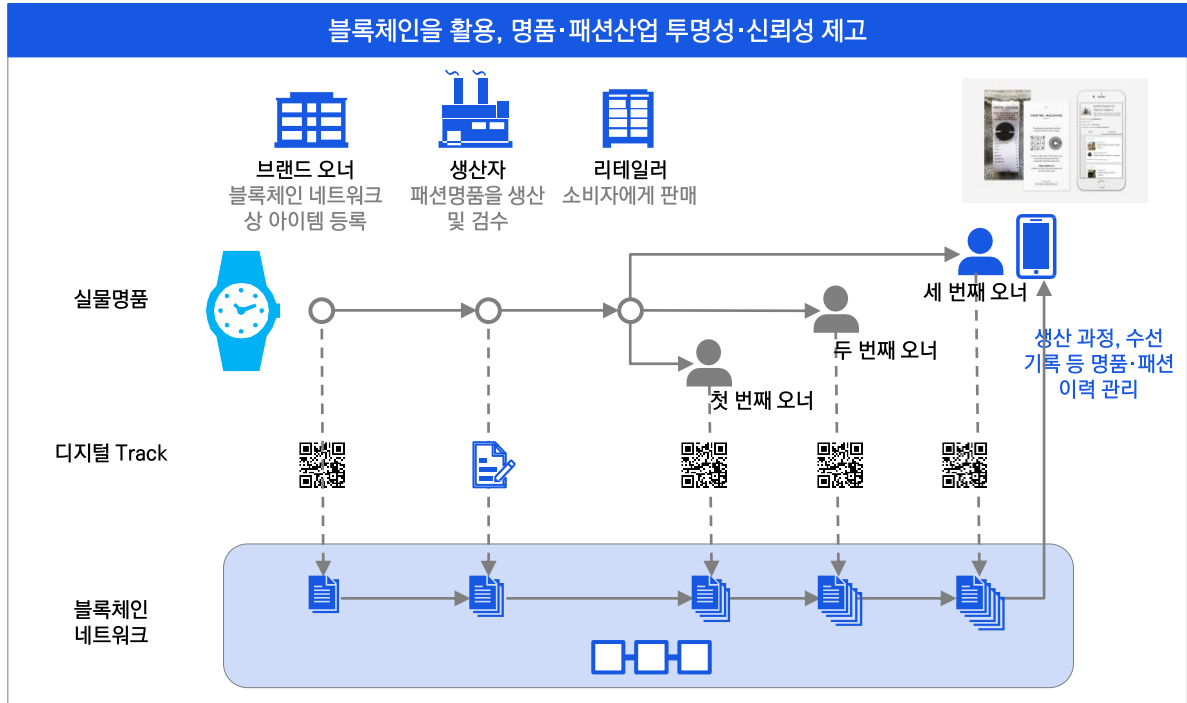
거래유형	상세	사례
개인 간(P2P) 전력거래	• 개인 간 전력거래의 비용을 줄이고 투명한, 전력거래를 위해 블록체인 기술을 활용함	• Brooklyn Microgrid Project, SolarCoin(미국) • Energo(중국) • Power Ledger(호주)
EV 충전 및 공유	• 전기차를 충전 및 결제할 때 블록체인 기술을 활용해서 신뢰성 및 비용 절감 효과를 가져올 수 있음	• Slock.it&RWE(독일) • Energo(중국)
에너지 데이터 활용	• 블록체인에 에너지 데이터를 공유함으로써 새로운 비즈니스 모델을 구축함	• Grid Singularity(오스트리아)
에너지 공유	• 에너지 공급이 필요한 개발도상국에 신재생에너지 설비를 공유할 수 있도록 블록체인을 활용함	• Bankymoon(남아공) • M-PAYG(덴마크)
탄소자산 거래	• 탄소배출권 거래제와 같은 탄소자산 거래를 활성화하기 위해 블록체인 기술을 도입함	• IBM & Smart Blockchain Lab(중국)

Source: 과학기술정책연구원(2018), '에너지 블록체인 도입방안 연구'

수출 물류 (Global Trade & Commerce)	정부 및 공공기관 (Government & Public)	의료·헬스케어 (Medical & Healthcare)	스포츠 (Sports)	부동산 (Real Estate)
------------------------------------	------------------------------------	-----------------------------------	-----------------	----------------------

# 산업·분야별 블록체인 활용 동향 (계속)

금융산업 (Finance)	분산신원증명 (Decentralized Identify)	에너지 산업 (Energy)	<b>명품 및 패션 산업 (Luxury &amp; Fashion)</b>	공급망 관리 (Supply Chain Management)
-------------------	------------------------------------	--------------------	--	-------------------------------------



Source: provenance.org, 언론보도 종합

**패션·리테일 관련 블록체인 기대효과 및 사례**

**명품·패션상품 모조·위조품 방지**

- 복잡한 유통 공급망을 가지고 있는 명품·패션업계의 공급망 특성 상 위조품으로 인한 소비자 피해가 막심
- 전 세계 위조품 총 거래량은 약 5,000억 달러에 달함(OECD 및 EU 지적재산권청 추정치)
- 블록체인 기술을 활용, 제품의 생산·유통·판매 등에서 발생(생산 단계부터 최종 소비자까지)하는 전 거래 내역을 모든 참여자에게 공정·투명하게 공개하여 제공

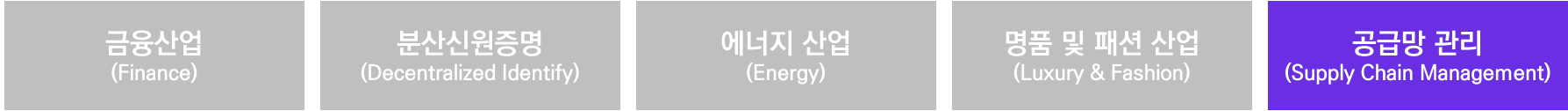
**패션·리테일 업계 블록체인 도입 움직임**

- 영국 디자이너 마틴 자를가드(Martine Jarlgaard)는 블록체인 기업 Provenance의 블록체인 기술을 활용, 패션 상품 제조 과정을 소비자에게 투명하게 공개
- 고객은 패션상품이 만들어지는 전 과정을 상세히 확인 가능하며, 이미지, 이력, 위치 데이터, 타임 스탬프 등 상품 정보를 QR코드로 확인 가능
- 루이비통 모엣 헤네시, 까르띠에 모기업 리치몬드, 프라다의 구매자가 구매 이력 확인 및 정품 인증을 할 수 있도록 '21년 블록체인 컨소시엄 '아우라(AURA)' 결성

Source: provenance.org, 언론보도 종합

수출 물류 (Global Trade & Commerce)	정부 및 공공기관 (Government & Public)	의료·헬스케어 (Medical & Healthcare)	스포츠 (Sports)	부동산 (Real Estate)
------------------------------------	------------------------------------	-----------------------------------	-----------------	----------------------

# 산업·분야별 블록체인 활용 동향 (계속)



Source: AWS, KOTRA

### 공급망 분야 블록체인

**블록체인 기반 공급망 효과**

- 각 공급망 참여자는 암호화 방식으로 기록되는 공유 원장에 접근 가능하며, 거래사항은 임의 변경 불가
- 공급망에 참여하는 기업은 블록체인 기반 단일 공유원장시스템을 통해 데이터 가시성 확보
- 거래내역 실시간 기록, 사물인터넷(IoT)과 같은 기술과 결합하여 공급망에서 생산, 운송 및 품질관리 조건 추적 자동화 및 모조품, 규제 위반, 배송지연 및 낭비 등과 같은 문제 해결 가능

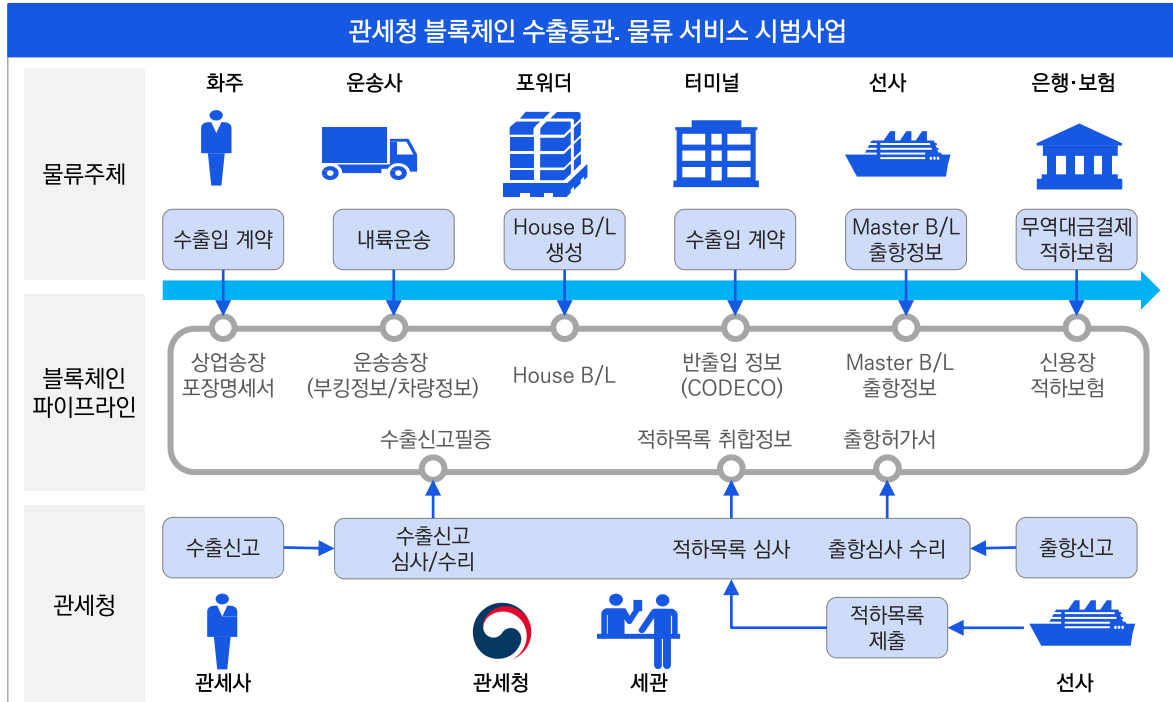
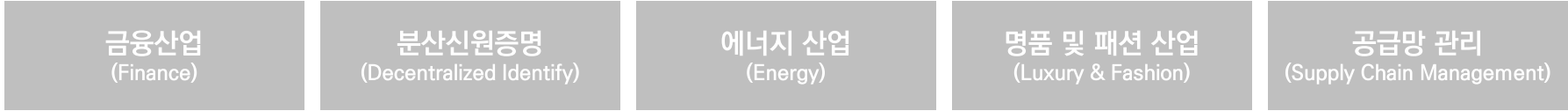
**공급망 분야 블록체인 시장 전망**

- Business Wire: 공급망 관련 블록체인 시장규모는 2020년 2억 5,300만 달러 → 2026년 30억 달러 이상으로 확대될 전망
- 블룸버그: 매출 규모가 50억 달러 이상 제조 기업의 30%가 2023년까지 블록체인 기술 기반 공급망 관리 솔루션을 이용할 것으로 전망

Source: KOTRA



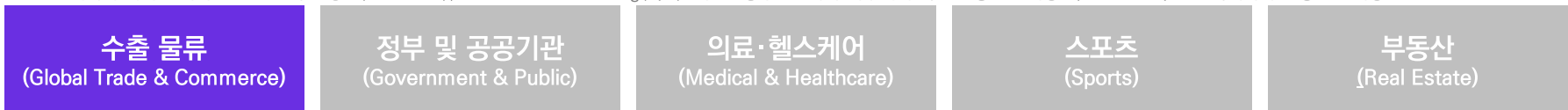
# 산업·분야별 블록체인 활용 동향 (계속)



- ### 무역거래 절차 별 블록체인 활용 사례
- 1. 물품매매계약**
    - we.trade: 유럽 내 중소기업의 무역금융과 원활한 국제 결제를 지원하고자 2018년 6월 IBM의 블록체인 플랫폼을 통해 구축. 국제송금망(SWIFT)을 거치지 않고 개별 기업간 금융 거래를 체결. 상업적 목적으로 실제 수행된 유럽 최초 실시간 거래
  - 2. 대금 결제**
    - Trade Safe: 싱가포르 정보통신개발청은 데이터 공유 블록체인 플랫폼 Trade Safe를 2016년 6월 개발. 은행의 송장 확인을 위한 단일의 정보 출처 부재 등 기존 페이퍼 기반 송장 시스템의 문제 극복
  - 3. 무역 보험**
    - 도쿄해상과 NTT 데이터: 화물해상 보험금 지급 과정의 블록체인 개념검증(PoC) 완료. 인적 비용과 서류 전달 등의 비용 절감 효과 및 보험금 신청에 필요한 정보를 빠르게 배포 및 공유 가능
  - 4. 물품 운송**
    - TradeLens: IBM과 Maersk는 2018년 8월 블록체인 기반 선적 솔루션인 TradeLens 출시. 비효율적이고 수동적인 서류 기반 업무절차를 배제하고 문서 관리 단순화
  - 5. 수출입 통관**
    - 싱가포르의 NTP: 기업과 정부 간 전자 데이터의 공유와 업무절차의 통합을 위한 원스톱 무역정보 관리 플랫폼이며, 무역 공급망 전반에 걸쳐 절차 간소화

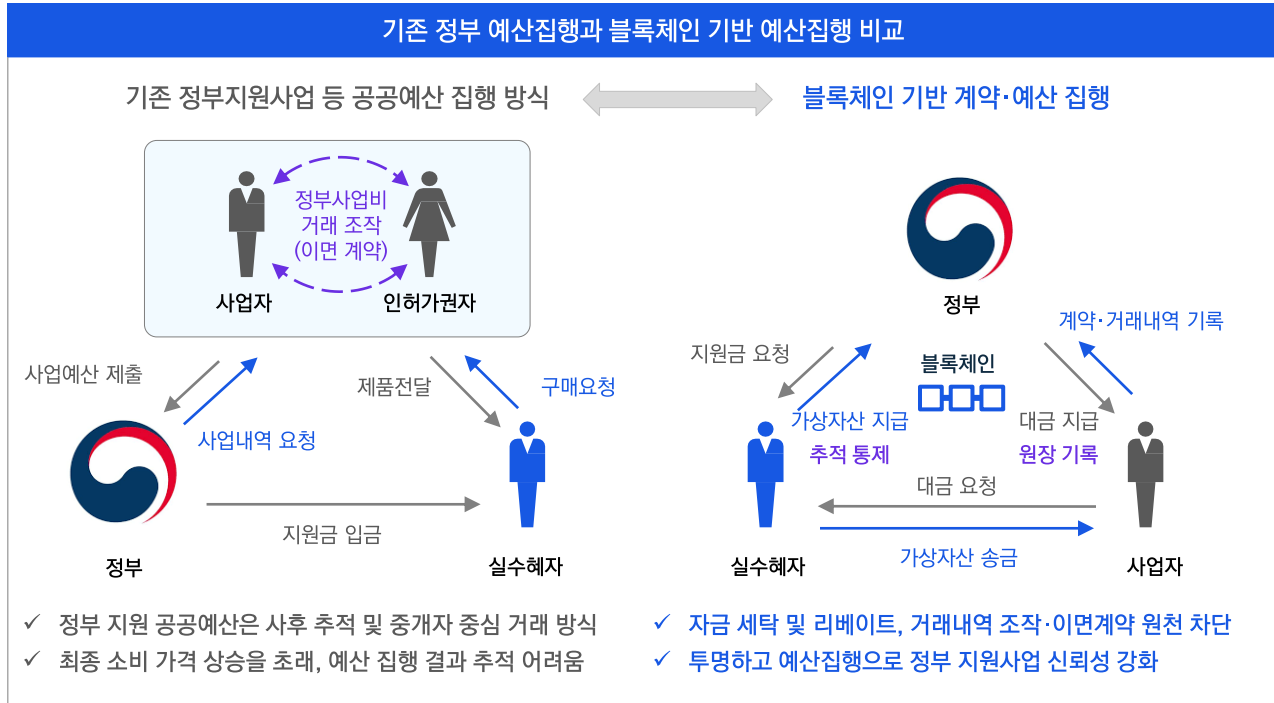
Source: 관세청, 한국조세정책연구원(2018), '블록체인 기술을 이용한 무역원활화 방안에 관한 연구'

Note: 컨테이너 터미널 게이트 반출입 확인 정보(CODECO), House Bill of Landing(B/L): 화물운송주선업자가 화주에게 직접 발행한 선하증권, Master B/L: 선박회사가 발행한 선하증권



# 산업·분야별 블록체인 활용 동향 (계속)

금융산업 (Finance)	분산신원증명 (Decentralized Identify)	에너지 산업 (Energy)	명품 및 패션 산업 (Luxury & Fashion)	공급망 관리 (Supply Chain Management)
-------------------	------------------------------------	--------------------	----------------------------------	-------------------------------------



Source: 한국산업기술진흥협회(2022), '기술과 혁신'

### 정부 및 공공기관 블록체인 활용 가능 분야

**스마트시티**

- 기술, IoT, 클라우드 컴퓨팅 등 기술을 활용, 물리적, 사회적, 비즈니스 인프라 통합 관리하며, 블록체인 기술은 스마트시티 보안 솔루션으로 주목받고 있음

**중앙은행 결제 처리**

- 블록체인이 거래량과 네트워크 복원력을 크게 높여 중앙은행이 실시간총액결제(Real Time Gross Settlement System, RTGS)\*를 빠른 속도로 처리 가능

**교육기관**

- 학교, 대학 등이 달성한 성과·작업에 대한 효과적인 검증 가능. 또한 스마트 계약을 통해 학자금 대출 등을 관리하고, 약관 준수 여부 추적 가능

**세무**

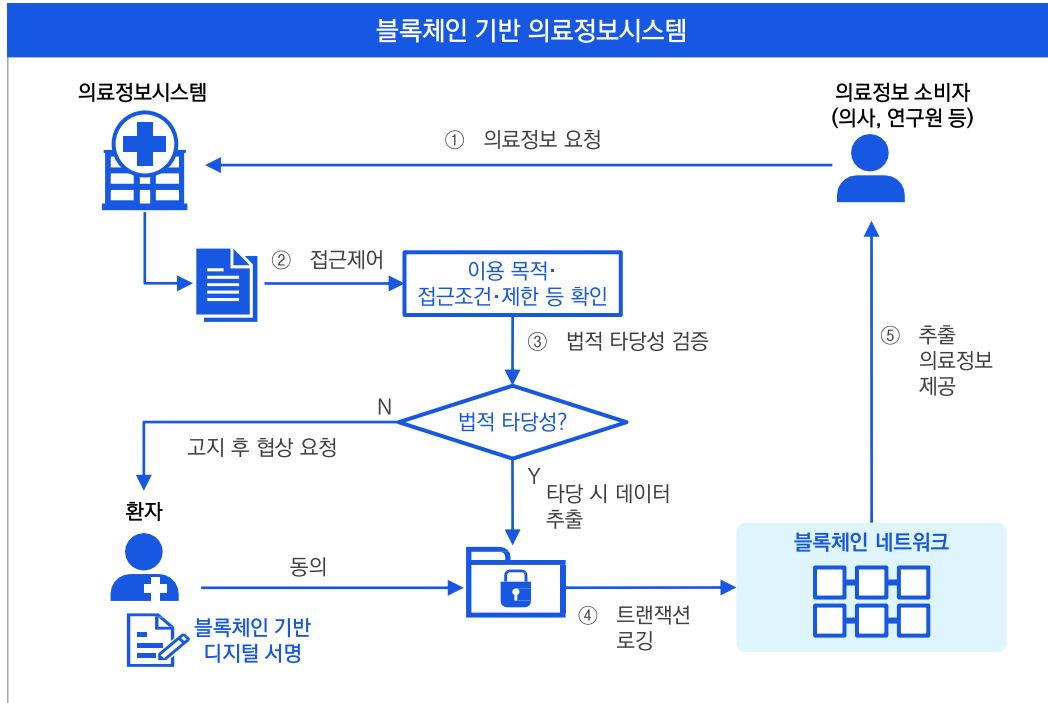
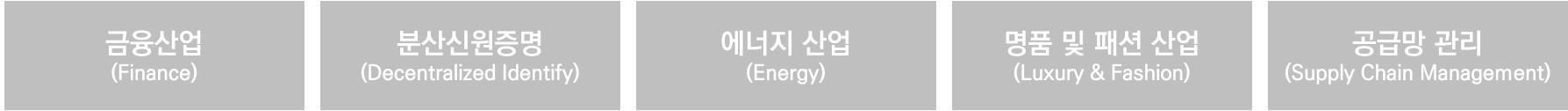
- 스마트 계약을 통해 급여와 납부세액을 각각 소득자, 징수기관에게 자동으로 이전하는 등 세금징수 효율과 속도를 개선하고 징수절차 간소화 가능

Source: consensys  
Note: \*금융기관 간 최종 자금결제가 건별 실시간 이루어짐

수출 물류 (Global Trade & Commerce)	<b>정부 및 공공기관 (Government &amp; Public)</b>	의료·헬스케어 (Medical & Healthcare)	스포츠 (Sports)	부동산 (Real Estate)
------------------------------------	--	-----------------------------------	-----------------	----------------------

III. 산업에서의 블록체인 활용 방안·동향

# 산업·분야별 블록체인 활용 동향 (계속)



Source: 한국보건산업진흥원(2018), '헬스케어 분야에서의 블록체인 기술'

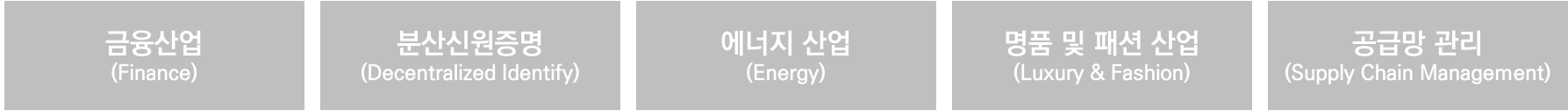
블록체인 기반 의료·헬스케어 산업 혁신방안	
병원·환자 간 의료정보 비대칭성	<ul style="list-style-type: none"> <li>환자의 개인건강기록(Personal Health Record, PHR) 관리에 블록체인 기술 기반 투명하고 보안성이 높은 통합의료정보 플랫폼 구축. 이를 통해 의료정보의 비대칭성을 해결</li> </ul>
보험청구·심사 비효율성	<ul style="list-style-type: none"> <li>블록체인 기반 자동화된 보험청구·심사 체계 구축을 통해 청구 및 심사 과정의 효율성 제고</li> <li>과다 청구, 과소 지급 등 발생 가능한 윤리적 문제 사전 예방</li> </ul>
의약품 유통 과정 모니터링 체계 미흡	<ul style="list-style-type: none"> <li>IoT를 통해 수집된 의약품 유통 전 과정을 블록체인 네트워크 상 구현</li> <li>- 의약품 원본성 보장 및 위변조 예방</li> </ul>
개인의료 정보 보안 위험	<ul style="list-style-type: none"> <li>IoT에서 수집된 개인의료정보를 블록체인 상에 저장하여 악의적인 해킹 등 보안 위험으로부터 데이터 보호</li> </ul>

Source: 한국보건산업진흥원(2018), '헬스케어 분야에서의 블록체인 기술'





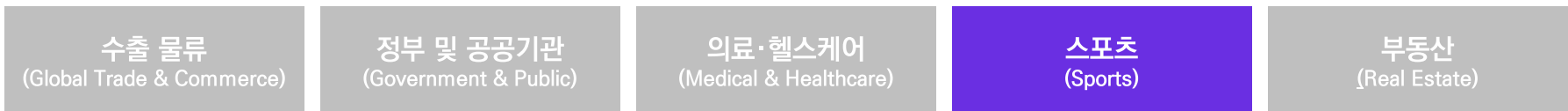
# 산업·분야별 블록체인 활용 동향 (계속)



## 스포츠 분야 블록체인 적용 가능 분야

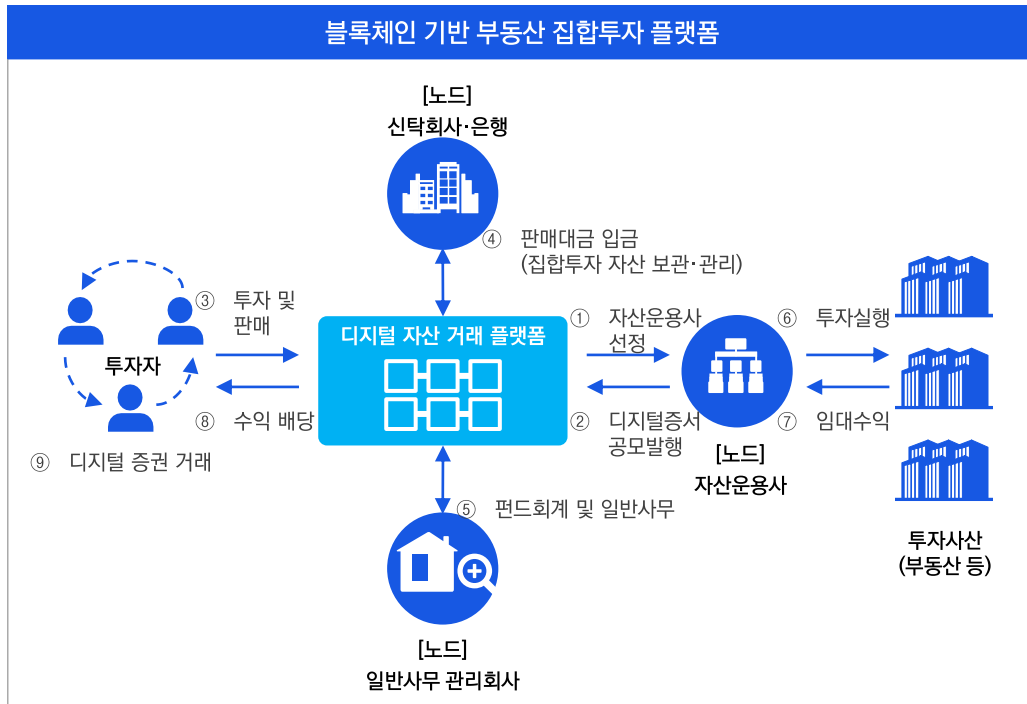
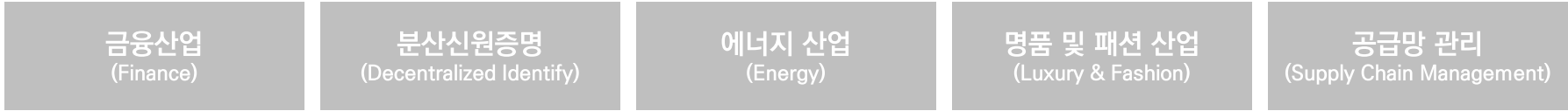
구분	블록체인 기반 혁신방안	서비스 기업	구분	블록체인 기반 혁신방안	서비스 기업
티케팅	<ul style="list-style-type: none"> <li>• 대체불가토큰(Non Fungible Token, NFT) 기반 디지털 티켓으로 압표, 티켓 위조, 티켓 허위매물 문제를 해결</li> <li>• 티켓 구매나 보관, 소유자 간 티켓 양도까지 쉽고 안전하게 할 수 있도록 있도록 지원</li> <li>• VIP 티켓에 대한 독점적인 기능 또는 권한을 자유롭게 구현</li> </ul>		베팅	<ul style="list-style-type: none"> <li>• 스마트 계약 기반 예측 시장 DApp을 통해 특정 스포츠 결과에 베팅할 수 있는 솔루션을 제공</li> <li>• 스포츠 토토와 같이 경기 결과를 예측하여 경기 결과를 맞추면 리워드를 지급하는 방식</li> </ul>	
스마트 계약	<ul style="list-style-type: none"> <li>• 스마트 계약을 통해 구단과 선수 간 계약조건 및 이행사항 등에 대한 투명성을 제고하고 선수 권리 보호에 활용</li> <li>• 인센티브 조건 만족 시 또는 선수 브랜드 상품 판매 수익 발생 시 이에 대해 스마트 계약을 기반으로 로열티를 지급하는 등 다양한 부가업무 자동화 구현 가능</li> </ul>		수집품	<ul style="list-style-type: none"> <li>• 브랜드별 수집 가능한 아이템이나 기념품, 선수 영상 등을 고유 디지털 아이덴티티를 가진 NFT 형식으로 발행하여 추가적 수익 창출 가능</li> <li>• NBA 탐샷 등 스포츠 NFT 분야는 블록체인을 스포츠 업계에 적용하여 성공한 대표적 사례</li> </ul>	
스포츠 애널리틱스	<ul style="list-style-type: none"> <li>• 성과, 건강 데이터, 이적 이력, 관리 비용 등을 포함하여 선수들의 다양한 데이터가 투명하게 관리되어 구단들의 선수 관리·스카우트 등에 활용</li> <li>• 도핑 방지 등 규정 준수에 활용될 수 있으며, 데이터 조작이 어렵고 도핑 테스트 결과가 공개적으로 투명하게 관리되어 선수들의 선수들의 부정행위 방지 등에 활용</li> </ul>		팬 토큰	<ul style="list-style-type: none"> <li>• 스포츠 구단들은 팬 참여를 늘리는 방법으로 멤버십과 비슷한 기능을 하는 팬 토큰(Fan Token) 활용</li> <li>• 팬 토큰을 통해 구단의 유니폼 선정, 경기장 배경음악 등과 같은 구단 의사결정에 참여할 수 있는 투표권 제공</li> </ul>	

Source: 삼정KPMG 경제연구원



III. 산업에서의 블록체인 활용 방안·동향

# 산업·분야별 블록체인 활용 동향 (계속)

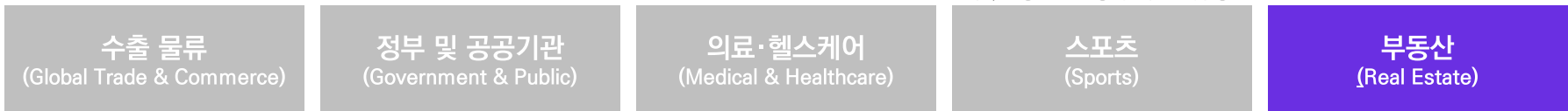


Source: 정보통신신문(2021), '조각투자서 메타버스가까지 블록체인 기반 부동산 투자 뜬다', 삼정KPMG 경제연구원 재구성

**블록체인 기반 부동산 비즈니스 모델 사례**

기업	블록체인 기반 혁신방안
ATLANT (러시아)	증권형 토큰 발행·P2P 임대차거래 중개 플랫폼 • 부동산 소유권의 지분을 나타내는 증권형 토큰 발행 - 부동산 가치상승·임대수익에 따라 일정 배당금 지급 • 토큰거래 플랫폼을 통한 부동산 자산 가치 산정 - 토큰의 가치 변화는 토큰 연동된 부동산 가치 반영 • 임대인이 등록 시 보증금 예치를 통한 보호장치 마련
BitRent (영국)	부동산 개발 자금조달 및 의사결정 지원 플랫폼 • 부동산 개발 프로젝트에 대한 기능형 토큰 발행 - 부동산 디벨로퍼 자금 조달 지원, 토큰 소유자는 개발이익 분배 권리 및 의사결정권 획득 - 투자자는 건설 단계에 대한 모든 정보를 활용·모니터링 가능하며, 프로젝트에 대한 의사결정권을 바탕으로 건설 활동 통제
Meridio (미국)	스마트 계약 부동산 거래 플랫폼 • 스마트 계약을 활용, 거래비용을 절감하고 거래의 투명성 증진, 구분소유권 거래 활성화 시도 • 부동산 개발, 기존 부동산 중개시장, 부동산 가치에 대한 실시간 자료 제공
QuantmRE (미국)	구분소유권 거래 기반 증권형 토큰 발행 플랫폼 • 주택과 주식을 조합한 포트폴리오에 기반하여 EQRE 토큰 발행, 투자자는 개별 부동산에 직접 투자하거나 EQRE 토큰을 구매 가능 • 주택소유주는 구분소유권(지분 양도) 거래로 빚을 지지 않고 현금 확보 가능

Source: 국토연구원(2020), '부동산 유통화 수단으로 블록체인 기술의 활용가능성 연구', 삼정KPMG 경제연구원 재구성



# Contents

	Page
I. Web 3.0으로의 진화와 블록체인	2
II. 글로벌·국내 블록체인 시장 현황	23
III. 산업에서의 블록체인 활용 방안·동향	31
IV. 결론 및 시사점	42

# Key Takeaways

1

## 정부:

블록체인 시장을 선점하고 해당 기술이 국가 경쟁력으로 연결되기 위해 ‘신속함’과 ‘속도’가 중요하며, 국내 블록체인 산업에 대한 정부의 적극적인 산업양성 계획 및 블록체인 관련 법·규제 체제 정비 등을 통한 체계적인 지원 방안이 요구됨

- 블록체인은 4차 산업혁명의 기반 기술로서 잠재성이 높으며, 금융뿐만 아니라 전 산업에 걸쳐 활용·부가가치가 높음
- 블록체인 분야는 2020년을 기점으로 다양한 산업적·상업적 실험이 시도되고 있으며, 생태계 확장·상용화로의 전환이 본격화되는 과정을 거치며 산업 활성화로 가는 초기 단계에 있음
- 특히 블록체인 기술이 원활히 활용되기 위해서는 가상자산산업기본법안, 전자금융거래법, 개인정보 보호법, 신용정보법 등 관련 규제 전반을 아우르는 포괄적인 고민 및 접근이 필요

2

## 기업:

글로벌 경쟁력 확보를 위해 선진국 대비 부족한 비즈니스 모델 개발과 관련하여 기업들은 기존 사업과의 시너지를 극대화하거나, 새롭게 차별화된 고부가가치 사업모델에 대한 고민이 필요

- 블록체인 기술에 대한 이해도뿐만 아니라 이를 활용한 새로운 비즈니스 모델 개발도 가능한 전문 인력을 확보·양성하는데 노력해야 함
- 블록체인의 사업 및 투자를 기획하고 있는 기업은 알고리즘의 취약성으로 인해 발생가능한 Private key 및 관리자 권한 탈취, 프로그래밍 코드 취약성을 인한 스마트 계약 정보 노출, DDoS와 같이 서비스 가용을 방해하는 사이버 공격 가능성, 블록체인 플랫폼 간 표준기술 부재 및 확장성 문제 등 블록체인의 기술적 리스크 및 관련 사업모델 관련 리스크에 대한 면밀한 검토 필요
- 더불어 파트너십, 솔루션 및 기술 확보 등 이러한 문제를 완화하기 위한 대응 방안 또한 고려 필요

# Business Contacts

## 가상자산산업 전문팀

### Consulting service

조재박  
부대표  
T: 02-2112-7514  
E: jaeparkjo@kr.kpmg.com

김민수  
전무  
T: 02-2112-7010  
E: mkim9@kr.kpmg.com

봉찬식  
전무  
T: 02-2112-7732  
E: chansikbong@kr.kpmg.com

황태영  
상무  
T: 02-2112-0490  
E: taeyoungwang@kr.kpmg.com

이지현  
상무  
T: 02-2112-3054  
E: janenelee@kr.kpmg.com

### Audit

염승훈  
부대표  
T: 02-2112-0533  
E: syeom@kr.kpmg.com

안창범  
전무  
T: 02-2112-0312  
E: cahn@kr.kpmg.com

신문철  
상무  
T: 02-2112-0356  
E: moonchulshin@kr.kpmg.com

강승미  
상무  
T: 02-2112-0061  
E: seungmikang@kr.kpmg.com

강상현  
상무  
T: 02-2112-3202  
E: sanghyunkang@kr.kpmg.com

### Tax

장지훈  
상무  
T: 02-2112-0961  
E: jihunjang@kr.kpmg.com

이상무  
상무  
T: 02-2112-7899  
E: sangmoolee@kr.kpmg.com

### Deal Advisory

손호승  
부대표  
T: 02-2112-0717  
E: hson@kr.kpmg.com

김양태  
상무  
T: 02-2112-7585  
E: ykim32@kr.kpmg.com

## home.kpmg/kr

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG Samjong Accounting Corp., a Korea Limited Liability Company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.