

전략분야 현황분석

블록체인



블록체인

1. 개요

가. 일반적 정의

(1) 정의

- ☐ 블록체인은 트랜잭션을 보관하는 단위인 블록들을 체인 형태로 연관시킨 데이터 저장 구조를 의미
 - 거래내역의 예를 들어 쉽게 블록체인을 정의하면 블록(block)에 거래내역이 담긴 데이터를 담아 체인(chain) 형태로 연결하는 것을 의미(아래 그림)
- ☐ 블록체인은 혁신적 기술로 독특한 특징 보유
 - 기술적 관점에서, 블록체인은 공개적으로 열람 가능한 분산원장(Distributed ledger)를 유지하는 백엔드 데이터베이스를 포함
 - 블록체인 기술은 중앙화된 공인 주체 없이 정보의 무결성 및 신뢰성을 확보하는 P2P 기반 분산원장 기술
 - 블록체인 네트워크 참여자가 공동으로 거래 정보를 검증하고 해시(Hash) 기반으로 거래 정보를 블록에 기록 보관함으로써, 정보의 완결성 및 무결성을 보장

[기존 거래방식과 블록체인 거래방식 비교]

기존 거래방식



블록체인 거래방식



* 출처: 세상을 바꿀 매력적 기술, LG-CNS 공식블로그

(2) 필요성

- ☐ 블록체인은 향후 인공지능(AI)이나 사물인터넷(IoT) 등 4차 산업혁명을 이끄는 핵심기술들과도 융·복합될 가능성 확대
 - 4차 산업혁명 시대에 블록체인은 데이터 보안은 물론 개별 데이터에 대한 개인의 통제권을 강화
 - 글로벌 사물인터넷 시장의 경우 서비스 확장성과 보안 강화를 위해 블록체인을 활용하려는 시도 증가
 - 공급망 관리(SCM, Supply Chain Management) 분야에서 제품 공급 및 소비와 관련된 일련의 과정(생산, 마케팅, 매매 등)에서의 투명하고 신뢰성 높은 정보를 제공
 - 지능형 교통 시스템과 같이 인공지능 기술과 결합되어 운행 중인 차량, ITS 서비스 공급자 및 관리자 간의 데이터 전송 및 분석
- ☐ 블록체인 기술의 현실 적용을 위한 다양한 연구가 진행되고 실용화도 추진 중
 - P2P 시스템의 효율성, 저비용의 특성과 투명성, 불변성 등의 장점은 인증, 저작권 등록 분야에서 활발히 연구가 진행되고 있으며 상업화도 확대
 - 블록체인의 투명성, 비가역성, 신뢰성은 이용료의 정산, 배분에서 고질적인 문제에 대한 해결책으로, 사전에 정해진 바에 따라 집행이 보장되는 스마트 계약을 활용하여 이용료의 징수와 배분의 미이행에 따른 다툼을 원칙적으로 방지 가능
 - 결제, 거래내역 분야에 활용하기 위한 노력이 증대되고 있으며, 앞으로 블록체인 기술은 지금까지 한계로 여겨졌던 확장성, 상호운용성, IoT 지원 등의 한계를 뛰어넘어 사회 전반을 혁신하는 기반 기술로 자리 잡을 것으로 예상
- ☐ 블록체인 기술이 안정화되고 시장에서 구매가 이루어지는 2030년까지 블록체인이 가져올 디지털 파괴의 직접 효과와 간접효과를 살펴보면 제품, 시장 및 산업변동과 블록체인 관련 지출액 부분이 매우 큰 것으로 확인
 - 이러한 파급효과는 2023년까지의 직·간접효과를 보면, 단계적으로 진행될 것으로 예상

[블록체인이 미치는 분야별/연도별 효과 예측]

파괴적 혁신의 분야	직접효과(~2030년)	간접효과(~2030년)	직접효과(~2023년)	간접효과(~2023년)
제품, 시장 및 산업변동	높음	높음	중간높음	중간
비즈니스 방법론의 개선	낮음	중간	낮음	낮음
인력강화 및 인력변동	중간	중간	중간낮음	중간낮음
업무활동의 개선	중간	중간	중간낮음	중간낮음
고객 구매행동	중간	높음	중간낮음	중간
지출액	높음	높음	중간높음	중간
거시경제	낮음	중간	낮음	중간

* 출처: Digital Disruption Profile: Blockchain's Radical Promise Spans Business and Society, 2018, Gartner

나. 구축 범위

(1) 가치사슬

- ☐ 블록체인 산업의 가치사슬은, 마이닝 전용 하드웨어 기술, 암호화 알고리즘 기술 및 P2P 통신 기술과 같은 블록체인 근간 기술을 포함하는 후방산업과 블록체인 기반 응용 서비스 기술을 포함하는 전방 산업을 포함
- ☐ 2019년 기술로드맵에서는 중소기업의 기술개발 가능성 및 시장성을 고려하여, 블록체인 가치사슬의 전방산업에서의 활용과 프로토콜 개발에 초점을 맞추어 기술

[블록체인 가치사슬]

후방산업	블록체인	전방산업
컴퓨팅, 네트워크, 스마트 기기, 반도체, 플랫폼	블록체인 프로토콜 개발 (블록체인 네트워크 구조 / 블록 구조 / 토큰 이코노미 구조 / 합의 알고리즘)	의료, 금융, 거래, 물류, 보안, 서비스, 문화 및 콘텐츠

(2) 대표적 분류 방법

◎ 기술요소에 따른 분류

- ☐ 블록체인 기술을 크게 분산저장기술, 프라이버시 및 암호화, 합의 알고리즘, 블록체인 기반 어플리케이션 요소기술로 분류 가능

[블록체인의 기술 분류 및 구성요소 별 비교]

분산 저장 기술	프라이버시 및 암호화	합의 알고리즘	블록체인 기반 어플리케이션
퍼블릭&프라이빗 네트워크	해시 함수	PoW, PoS, DPoS, PoET, PBFT, PoI, PoA	증권형 토큰 플랫폼
분산 원장	공개 키 및 개인 키 알고리즘	거래 검증	게임 DApp
블록 구조	보안 알고리즘	블록 채굴	De-Fi (Decentralized Finance, 탈중앙화 금융서비스)
노드 결합	디지털 서명	이중 지불 문제 해결 방법	분산형 이커머스
사이드 체인	유저 인증	결제 검증	분산형 투표 시스템
온 체인/오프 체인	전자 지갑	하드/소프트 포크 관련	분산형 DRM 관리

* 출처: 블록체인 세미나, 2018, 파이특허법률사무소

◎ 네트워크 구조에 따른 분류

□ 블록체인 네트워크 구조는 공개형과 비공개형으로 나뉨

- 블록체인 네트워크 구조에 따라 퍼블릭, 프라이빗, 컨소시엄으로 크게 구분
- 아래 표는 퍼블릭과 프라이빗을 중심으로 블록체인 네트워크의 특징을 비교 분석

[퍼블릭과 프라이빗 블록체인 네트워크의 비교]

분류 기준	퍼블릭 블록체인 네트워크	프라이빗 블록체인 네트워크
누가 거래 기록을 열람하였는가	누구나 익명으로 이체잔고와 거래기록을 열람	거래당사자와 규제기관만 열람
누가 거래에 참여하였는가	누구나 쉽게 사용자 인증과정 없이 계좌를 개설하고 거래에 참여	법적 책임을 지는 승인된 기관만 참여
누가 거래를 검증/승인하는가	누구나 컴퓨터를 통해 거래 검증에 참여	법적 책임을 지는 승인된 기관만 참여
누가 거래기록을 보관하는가	누구나 전체 거래내역을 보관할 수 있음	거래 당사자끼리 같은 거래내역을 보관
어떻게 합의의 도출하는가	작업증명 또는 지분증명 알고리즘을 통해 합의 도출	BFT계열 알고리즘을 통해 합의 도출
자체 암호화폐가 필요한가	필요함	필요없음
충분히 확장할 수 있는가	제한적 확장	금융 후선업무에 적합한 확장성
예시	비트코인, 대시, 이더리움	R3CEV, DAH, Clearmatics

* 출처: 퍼블릭과 프라이빗 블록체인 네트워크의 비교, 2019, 해시넷

(3) 기술로드맵 전략분야의 범위

- 블록체인 분야는 가치사슬에 따라, 블록체인 근간 기술, 블록체인 프로토콜 및 블록체인 기반 응용 서비스로 나누어질 수 있으며, 본 로드맵에서는 중소기업의 기술개발 가능성 및 시장성을 고려하여 블록체인 기반 응용 서비스에 관하여 중점적으로 다룰 예정

[블록체인 기술로드맵 전략분야의 범위]

*: 본 전략분야의 범위

분류	세부기술	주요 제품 및 기술
블록체인 프로토콜	블록체인 구조	프라이빗 체인, 퍼블릭 체인, 인터체인 기술, 사이드 체인 기술, DAG 체인 기술
	암호화폐	비트코인, 라이트코인, 리플, 이더리움 등
	운영 구조(프라이빗 체인)	하이퍼레저 등의 프라이빗 체인
	합의 알고리즘	PoW, PoS, DPoS, PBFT 등
블록체인 기반 응용서비스	신원/보안*	암호화폐 거래소 보안성 강화, 분산 신원 인증(DIDs), Self-Sovereign Identity(SSI), 전자지갑, 암호키 관리, 불법 거래 탐지
	소셜 미디어*	Steemit, Line, 에이콘, 메신저 서비스, 소액 기부/후원
	에너지*	블록체인을 이용한 에너지 관련 거래 기록 관리, 에너지 체인
	게임*	블록체인 기반 게임, 블록체인 기반 게임 아이템 거래소, 확률형 아이템 플랫폼, 유저들의 게임 운영 참가
	공급망 관리*	블록체인 이용 공급망 관리, 기업형 블록체인 시스템
	데이터 관리*	전자 지갑 기술, 의료 기록 관리 기술, 저작권 관리, 전자 투표 시스템, 기업형 블록체인 시스템, 물류 이력 관리, 온라인 쇼핑몰
	금융 서비스*	암호화폐 운용, 암호화폐 기반 Banking, 암호화폐 P2P 대출
블록체인 근간 기술	마이닝 전용 하드웨어*	FPGA 기반 ASIC 반도체, GPU
	암호화 알고리즘*	SHA 및 PBKDF2 등의 해시 암호화 알고리즘, RSA 및 ECC 등의 공개키 암호화 알고리즘, 및 전자 서명
	P2P 통신*	P2P 통신 프로토콜, 하이브리드 P2P 통신 프로토콜, DAG 기반 통신 프로토콜, Bittorrent, Napster, Skype, eMule, Shareaza

2. 시장 분석

가. 세계 시장 분석

(1) 세계시장 동향 및 전망

◎ 블록체인 세계시장 전망

- MARKETSANDMARKETS 2020년 보고서에 따르면 블록체인 시장규모는 2020년 30억 달러에서 2025년도까지 연평균 67.3% 성장하여 397억 달러 규모로 성장 전망
- 성장동인으로 코로나-19에 따른 고강도 사회적 거리두기로 인한 경제사회 전반의 디지털화(Digital Transformation)·비대면화(Untact) 촉진
 - 블록체인 기술이 재조명되고 각국의 주도권 경쟁이 치열하며 초기 시장 장악 중요성 대두
 - 시장 초기 과열되었던 가상자산에 대한 관심이 잦아들고, 블록체인 기술과 활용 자체의 가능성에 주목

[블록체인 세계시장 전망]

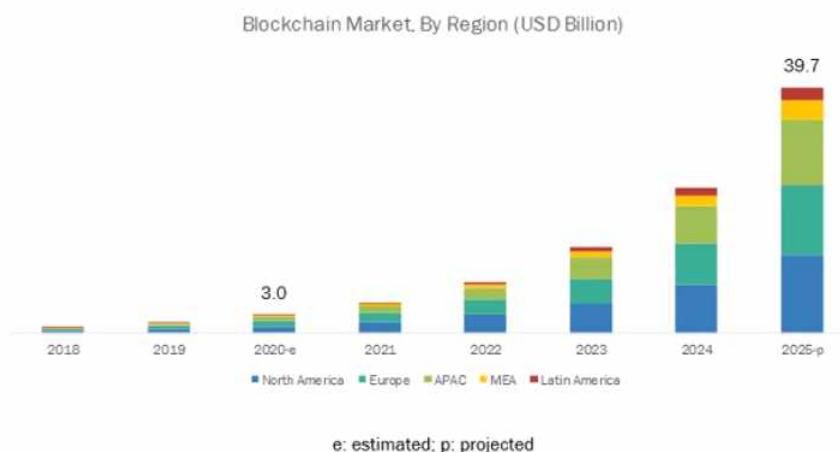
(단위: 십억 달러, %)

구분	`18	`19	`20	`21	`22	`23	`24	CAGR
블록체인	1.1	1.8	3.0	5.0	8.4	14.0	23.5	67.3

* 출처: Blockchain Market by Component - Global Forecast to 2025, marketsandmarkets(2020)을 근거로 네모아이씨지 재가공

[블록체인 세계시장 전망]

(단위: 십억 달러)



* 출처: Blockchain Market by Component - Global Forecast to 2025, marketsandmarkets(2020)

- 블록체인 시장은 급격히 성장하는 중이기 때문에, 시장조사업체마다 예측연도 추정치의 차이가 발생
- 시장조사기관 가트너에 따르면 '20년에는 사업적 부가가치의 연간성장률이 120%에 이르고, 2030년에는 사업적 부가가치가 약 3조 달러를 초과할 것으로 전망¹⁾
 - '18년 기준 한국과학기술정보원에 의하면 블록체인의 글로벌 시장 규모는 5억 5,000만 달러, 국내 시장 규모는 5천만 달러로 산출

[글로벌 블록체인 시장 전망 요약]

(단위: 백만달러, %)

조사기관	기준 연도	시장규모	예측연도	추정치	연간성장률
Market and Markets	2020	3,000	2025	39,700	79.6
IDC	2017	735	2022	10,860	71.3
Accuray Research	2016	210	2025	16,300	62.1
Statista	2016	210	2021	2,312	61.5
Market Research Future	2016	168	2022	2,000	51.0
Netscribes	2018	3,351	2023	19,900	42.8
Grand View Research	2016	604	2024	7,589	37.2
평균	2017	813	2023	9,521	58.4

* 출처: 블록체인 산업의 고용 파급효과 분석 연구, 2018, KAIST

- (투자지출) IDC에 따르면, 기업들의 글로벌 블록체인 투자지출이 '22년까지 연평균 73.2%의 증가율을 기록해 117억 달러에 달할 전망
- '19년 블록체인 시장 지출금액은 약 2억9,000만 달러(약 3,364억)를 기록하고 있으며, 이는 전년 대비 약 55% 가까이 증가한 수치
 - 국가별로는 미국이 글로벌 지출의 36%에 해당하는 가장 많은 지출을 할 것으로 예상. 다음으로는 서유럽, 중국, 아시아 태평양(중국과 일본 제외) 지역 순으로 투자를 전망
 - 중국 기업들의 블록체인 관련 지출액은 '19년에 총 3억 달러(약 3,657억 9,000만 원)에 육박해 지난해보다 대략 2배 정도 성장

◎ 산업별 전망

- ☐ MarketsandMarkets에 따르면 7개 분야의 블록체인 시장 중에서 금융서비스 분야가 가장 큰 규모로 성장하고, 콘텐츠 엔터테인먼트 분야가 가장 큰 성장률을 보일 것이라고 전망

[블록체인 산업별 규모 전망]

(단위: 백만 달러, %)

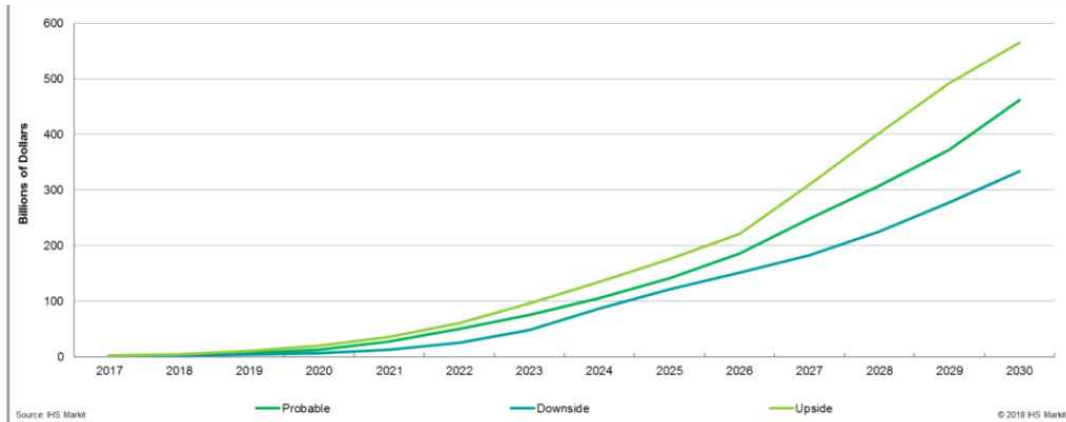
분야	`18	`20	`22	`24	CAGR
금융 서비스	300	839	2,251	6,083	65
정부, 공공분야	184	516	1,413	3,874	66
헬스케어	193	539	1,555	4,488	69
소매, 전자상거래	147	413	1,185	3,399	69
자동차	113	316	898	2,553	68
콘텐츠, 엔터테인먼트	85	237	692	2,025	70
기타	50	141	402	1,146	68
전체	1,072	3,000	8,397	23,502	67

* 출처 : Global Blockchain Technology Market 2016-2021, MarketsandMarkets(2016)과 Blockchain Market by Component, MarketsandMarkets(2020)을 근거로 네모아이씨지 재가공

☐ 금융 분야

- IHS Markit에 따르면 금융산업과 관련된 블록체인 시장은 2030년까지 전세계적으로 4,620억 달러에 이를 것으로 예상
- 금융 업계는 2017년에 블록체인이나 분산원장 기술(DLT : Distributed Ledger Technology)에 17억 달러를 투자한 것으로 집계
- 금융 부문 중 국가 간 결제와 계약이 4억 5,300만 달러로 가장 크고, 무역 금융과 PTS(post-trade transaction settlements)가 2억 8,500만 달러로 두 번째로 큰 시장
- 은행의 경우 핀테크 기술과 융합되어 기존 금융권에서 블록체인 기술 전문 기업과의 제휴를 통해 다양한 분야에 활용
- 증권거래소들은 후선관리(backoffice) 등 운영비용 절감, 거래기록의 신뢰향상을 목표로 증권거래 시스템에 블록체인 기술을 도입 및 적용

[금융업에서 블록체인의 사업적 가치]



* 출처: Blockchain in Finance Report, 2019, IHS Markit

□ 서비스 분야

- 서비스로서 블록체인(Blockchain-As-A-Service)의 활용 증가
- Mordor Intelligence에 따르면 세계 BaaS 시장은 2019년 420억 달러에서 2025년까지 연평균 15.2% 성장하여 982.9억 달러 규모로 전망
- 최근 BaaS로 변화를 가장 유리하게 활용할 수 있는 회사로 아마존, 마이크로소프트, 오라클 같은 BaaS의 기반이 될 서비스를 공급하는 업체와 함께 IBM, 세일즈포스닷컴, VM웨어, 또한 레드핀(Redfin), 질로우(Zillow), 렌딩트리(LendingTree) 등 블록체인 기반의 다양한 온라인 서비스를 제공하는 회사가 수혜를 입을 것으로 전망

□ 의료 분야

- ARC(Acumen Research and Consulting), 헬스케어 블록체인 시장이 매년 48%의 성장률로, 2026년까지 17억 달러로 성장할 것을 예상²⁾
- 미국과 유럽 및 중국이 시장을 선도하고, 일본 등의 아시아 태평양 지역이 세 번째로 큰 시장을 형성할 것으로 예상
- 바이오산업은 민감한 DNA 정보를 중간 거래기관 없이 병원이나 연구소로 전달
- 제약산업의 경우 제약 공급사슬 관리에서 각 제약품의 제조 단계를 추적

□ 물류·유통 분야

- 유통 산업은 프로세스마다 발생하는 수수료로 인한 고비용 구조와 복잡한 프로세스로 극복위한 블록체인 기술 도입
- 블록체인을 이용한 공급망 관리(SCM) 전체의 최적화를 지원
- 농수산물유통은 블록체인 기술을 활용하여 식품 원사지를 추적하고 질병·리콜에 대한 대응시간 최소화

2) Acumen Research and Consulting (ARC) Forecast: Blockchain Healthcare Use at \$1.7 Billion by 2026('19.7.16)

- 광고 및 콘텐츠유통의 경우 수익 구조의 단순화를 통해 기존 복잡한 유통 구조를 변화시키고 다양한 기업들은 암호통화 보상시스템을 활용하여 소비자 개입 촉진

☐ 보안 분야

- 블록체인 기술의 가장 큰 위협인 개인키 분실 및 해킹을 보안하기 위해 개인키 분실에 대한 대책과 보안성이 강화된 거래소 서버 운영 및 전자지갑 기술 개발에 대한 관심이 증가할 것으로 전망

[보안·컨텐츠분야 블록체인 적용 현황]

문화 및 콘텐츠 분야 블록체인	주요 내용
코닥원(KODAKONE)	• 사진, 인쇄기업 코닥이 개발한 블록체인 기반 플랫폼으로서, 코닥코인(KODAKCoin)을 활용하여 사진거래 및 저작권 지급이 이루어짐
스팀잇(Steemit)	• 암호화폐 중 하나인 Steem에 기반하여 운영되는 소셜 네트워크 서비스(SNS)로서 게시된 글에 대한 추천에 기반하여 보상이 지급되는 시스템. 기존 SNS 시스템에서의 힘의 균형을 SNS 서버로부터 사용자로 이전시켰다는 점에서 주목받고 있음
우조뮤직(Ujo Music)	• 이더리움 블록체인 기반의 아티스트 중심의 음악 플랫폼으로, 아티스트는 자신이 정한 스마트계약과 함께 음원을 업로드하며 사용자는 이더리움 기반 디지털 지갑을 통해 결제할 수 있음. 우조뮤직 또한 음악 제작자들에게 공정한 가치의 분배를 실현하고자 하는 목적으로 뮤직코인을 발행
시빌(Civil)	• 블록체인 기술과 가상화폐 보상을 통해 뉴스를 생산하고 배포하는 탈중앙화 뉴스 플랫폼으로서, 기자와 독자가 직접 뉴스 콘텐츠를 거래할 수 있게 하는 오픈 마켓

* 출처: “블록체인 기술을 활용한 콘텐츠 유통 사례”, 2019, 한국저작권보호원

☐ IoT 블록체인 분야

- Zion Market Research에 따르면 IoT 블록체인 세계시장은 2018년 3천만 달러에서 2025까지 연평균 91.4% 성장하여 30.3억 달러 규모 전망
- IoT와 블록체인 기술이 결합하여 건설, 헬스케어 등에 활용되어 새로운 산업으로 도약
- 블록체인 기반 IoT 네트워크 센서(Xensor)의 경우 센서를 활용하여 건물 내 관리 포인트를 자동화하고 고성능 게이트웨이를 사용해 저렴한 비용으로 IoT 통신망을 구축

☐ 거버넌스 분야

- 블록체인을 활용하여 신뢰있는 데이터 공유로 시민들의 참여에 의한 의사결정 구조를 구축
- 정책금융의 투명화를 위한 블록체인 바우처 도입과 지방자치단체 차원의 블록체인 투표 도입 등의 사례 급증
- 영국은 시민복지 바우처 관리에 블록체인 기술을 적용하여 불필요한 행정절차 및 서류 위변조로 누수되는 복지예산 2.5%~5.4% 절감을 예상
- 블록체인이 가진 높은 수준의 불변성은 투표가 조작될 수 없도록 하는 훌륭한 해결책으로 선거 과정에서 도입 상용화 추세

◎ 활용별 전망³⁾

- PwC는 2020년 발표한 ‘The trillion-dollar reasons to rethink blockchain’ 보고서에서 블록체인이 GDP에 미치는 기여 효과가 2021년 660억 달러에서 2025년 4,220억 달러, 2030년 1.76조 달러 규모로 폭발적인 성장을 할 것으로 전망

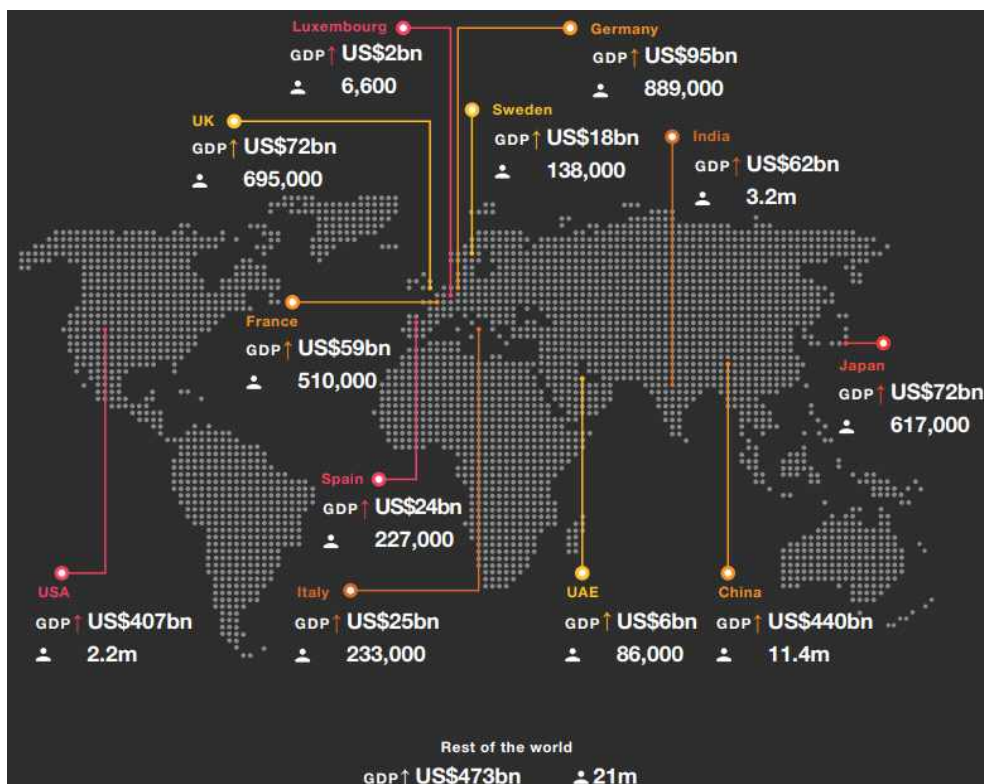
[활용별 블록체인 기여효과 전망]

(단위: 십억 달러, %)

분야	'21	'25	'30	CAGR
출처(Provenance)	34	231	962	52
결제 및 금융 상품	17	105	433	50
신원증명	9	54	224	49
계약 및 분쟁 해결	3	18	73	49
고객 참여(Customer Engagement)	2	13	54	51
기타	1	1	14	39
전체	66	422	1,760	51

* 출처 : The trillion-dollar reasons to rethink blockchain, PwC(2020)

[지역별 블록체인 기여효과 전망]



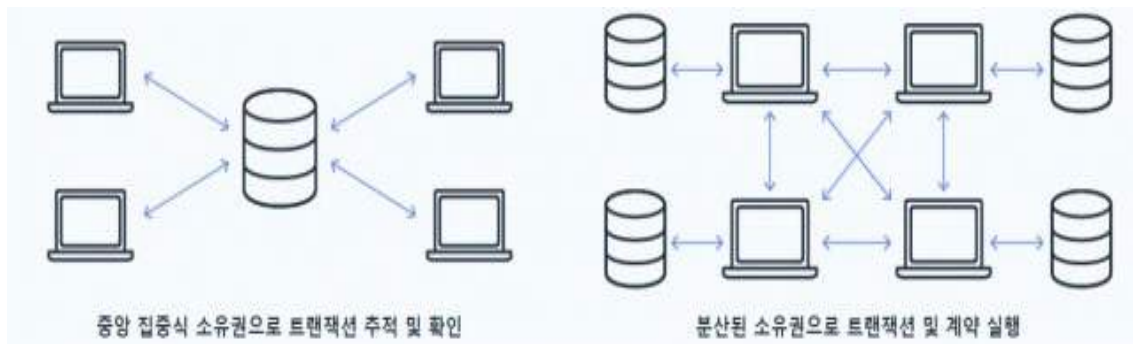
* 출처 : The trillion-dollar reasons to rethink blockchain, PwC(2020)

(2) 세계시장 핵심플레이어 동향

◎ 해외 주요기업 동향

- (Amazon) 아마존웹서비스(AWS)는 클라우드 기반 분산원장 데이터베이스인 아마존 QLDB(Amazon QLDB)와 아마존 매지니드 블록체인 서비스를 공개
 - 아마존 QLDB는 거래를 완전하고 영구적으로 기록하기 위해 투명하고 변경이 불가능한 환경을 제공하는 원장(ledger) 데이터베이스 서비스
 - 아마존 매니지드 블록체인은 널리 사용되는 블록체인 오픈소스 프레임워크인 이더리움과 하이퍼렛저 패브릭(Hyperledger Fabric)을 사용해 확장가능한 블록체인 네트워크를 쉽게 구축하고 관리할 수 있게 해주는 솔루션

[아마존 AWS의 매니지드 블록체인]



* 출처: 'AWS로 기업 블록체인 도입을 앞당긴다', 2019, 동아일보

- 또한 아마존은 취득유통구조의 투명성, 일관성, 보안성 문제 해결하기 위한 블록체인 기반 제품 인증 및 상품 추적에 관한 특허 취득
- (Alibaba) 중국의 대형 글로벌 터미널 운영사인 초상국항만(CMP)와 블록체인 플랫폼 계약 체결
 - 비대면 무역을 실시할 수 있도록 지원하는 블록체인 플랫폼 공동 개발 및 구축 예정
- (Baidu) 자체 블록체인플랫폼 슈퍼체인(XuperChain) 테스트 베타버전 출시
 - 블록체인이 필요한 기업에 맞는 앱을 배치할 수 있도록 앱 제작 환경, 스마트 컨트랙트 템플릿 지원
- (Axoni) 블록 체인 기반 스마트 계약을 사용하여 세계 최대 파생 시장의 백 오피스를 점검
 - 분산 원장은 거래 당사자가 지불, 계산 및 기타 중요한 거래 정보를 실시간으로 볼 수 있도록하여 효율성을 개선하고 위험을 줄임. Axoni는 Goldman Sachs, JP Morgan 등으로부터 5천9백만 달러를 투자받는 등 세계 최대 은행 및 금융 중개업자와 이미 파트너 관계를 맺음

- ☐ (Coinbase) 비트 코인 지갑 및 소매 거래소를 넘어 현재 암호 화폐 관리, 전문 및 기관 거래 플랫폼 및 기관 거래 플랫폼을 제공
 - Coinbase는 2018년에 사용자가 이메일을 통해 전문가에게 연락하기 위해 비트 코인으로 지불하는 서비스인 Earn.com을 1억 달러에 구매
- ☐ (Ripple) 그들의 블록 체인 기반 글로벌 결제 네트워크를 통해 전세계 거의 모든 은행과 오랫동안 연결된 은행 간 메시징 플랫폼인 SWIFT를 대체하는 것이 목표
 - Ripple은 또한 회사가 창립자가 만든 암호화폐인 XRP에서 최근에 비트 코인 가치에 이어 두 번째로 국경 간 지불을 할 수 있는 서비스를 시작
- ☐ (IBM) ADEPT(Autonomous Decentralized P2P Telemetry) 프로젝트를 통해 IoT 환경의 신뢰성과 확장성 문제를 블록체인 기술로 극복하기 위한 계획 중
 - IBM, 금융기관을 위한 실시간 글로벌 금융결제 네트워크 'IBM 블록체인 월드 와이어(IBM Blockchain World Wire)'의 확대를 공식 발표
 - 태국 세관 당국이 IBM과 해운회사 머스크가 구축한 블록체인 비즈니스 플랫폼 '트레이드렌즈(TradeLens)' 도입
 - 기업 오라클(Oracle)과 블록체인 플랫폼 호환성 높이기 위해 협업, 패브릭 기반 크로스 네트워크 테스트 진행
- ☐ (MS) 자사 클라우드 애저(Azure)에서 블록체인 기술을 활용할 수 있는 'BaaS(Blockchain as a Service)'를 구축하고, 애저 플랫폼을 블록체인 생태계로 유치하려는 전략을 추진. 또한, 분산 신원 인증(DIDs)과 관련한 백서를 출간
 - 세계은행과 호주 연방 은행은 글로벌 개발 프로젝트에 자금을 지원하기 위해 마이크로소프트 애저 클라우드 플랫폼의 블록체인 이용해 50~60억 달러의 채권을 이더리움 플랫폼에 출시
 - MS가 공개한 '블록체인 데이터 매니저'는 애저 블록체인 내 데이터를 외부 데이터저장소에 연결하는 기능 제공
- ☐ (Google) 018년 블록체인 앱 개발 툴 제공 업체 Digital Asset, Blckapps 등과 파트너십을 체결하는 등 블록체인 스타트업과의 협력을 강화하고 있음. 이를 통해, 자체 클라우드 서비스로 블록체인을 제공
 - 구글이 미국 의료 서비스 업체 어센션(Ascension)과 파트너십을 체결하여 환자 진료 데이터를 수집해 블록체인 기반 의료 검색 엔진 개발 추진
- ☐ (UBS) 유틸리티 결제 코인 출시 계획
 - 바클레이 및 HSBC가 공동 참여하여 중앙은행에서 현금으로 전환할 수 있는 블록체인 기반 새로운 코인 지불 시스템 출시 계획. 중앙은행들의 자국 통화 발행 지연에 따른 대체 수단으로 결제 상태를 최신으로 유지하고 중앙은행의 자금을 지원

나. 국내 시장 분석

(1) 국내 시장 동향 및 전망

- (국내시장 동향 및 전망) 2018년 국내 블록체인 시장 규모는 359억 원에서 연평균 67.3% 성장하여 2024년까지 7,677억 원 규모까지 성장 전망

[블록체인 국내시장 규모]

(단위: 억 원, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
블록체인	359	588	980	1,634	2,744	4,574	7,677	67.3

* 출처: Blockchain Market by Component, MarketsandMarkets(2020)의 데이터를 기준으로 비트코인 화폐별 거래량 중 원화 점유율 2.97%⁴⁾(코인힐스 2020.12.30.)을 근거로 네모아이씨지 재가공(환율:1100원/달러)

- 국내 블록체인 분야는 중소기업이 많이 진출했지만 인공지능이나 빅데이터 등 신소프트웨어에 비해 매출 발생이 현저히 낮음⁵⁾
- 국내 블록체인 기업은 2018년 198개에서 2019년 237개로 증가한 것으로 조사
 - 신소프트웨어 분야 진출 기업 중 신소프트웨어 매출이 발생한다고 응답한 기업 비중은 클라우드(72.1%), 빅데이터(67.8%), IoT(65.7%)가 상대적으로 높은 반면, 블록체인은 실제 매출이 발생하는 기업의 비중이 30.5%에 그침(2018년은 22% 수준에서 다소 상승)
 - 2020년 신규로 총원 예정인 인력 중 현 인원 대비 신규 총원 인력의 비중이 가장 높은 분야는 블록체인으로 현재 인력의 58.3%에 해당되는 인원을 총원할 계획이 있는 것으로 나타남
- 블록체인 분야의 참여기업은 여러 그룹으로 나눌 수 있음
- 암호화폐 및 블록체인 관련 지원 및 사업을 하는 투자 및 엑셀러레이터 그룹으로 거래소, ICO 플랫폼, 미디어 및 커뮤니티 등
 - 블록체인 기술을 이용하여 플랫폼과 서비스를 만드는 그룹으로 유틸리티 및 서비스, 블록체인 교육 플랫폼, 마케팅 및 컨설팅 등

4) 미국달러:72.7%, 일본엔화:18.66%, 유로화:3.06%, 한국원화:2.97%

5) 2019 소프트웨어 산업 실태조사(소프트웨어정책연구소)

(2) 국내 생태계 현황

[블록체인 소분야별 생태계 이슈]

소분야	생태계 주요이슈
신원/보안	<ul style="list-style-type: none"> 금융보안원은 2020년 3월 31일 금융보안표준화협의회를 통해, 「분산ID를 활용한 금융권 신원관리 프레임워크」를 금융보안 표준으로 제정 블록체인을 이용하여 자기 주권 신원(Self-sovereign identity) 또는 분산형 신원 인증(DIDs)를 구현하려는 시도가 있으며, MS 및 W3C를 중심으로 이러한 연구가 수행 중 병무청 '인증서 없는 민원 서비스 제공을 위한 블록체인 플랫폼 구축' 경상남도 스마트 도민증을 DID로 발급하여 관광지 등에서 지역주민 요금할인 등을 위해 제출하던 실물 신분증을 경남분산신원서버에 연결된 매표서 QR코드 스캔으로 안전하고 간편하게 확인
탈중앙화 금융 서비스 (De-Fi)	<ul style="list-style-type: none"> 탈중앙화 금융 서비스(De-Fi)는 중앙화된 주체 없이 실행될 수 있는 모든 금융 서비스를 아우르는 것 블록체인 기반의 금융 서비스는 ICO/MEO, STO, 게임 DApp을 통해 현재의 탈중앙화 금융 서비스에 이르게 됨. 탈중앙화 금융 서비스에서 담보 대출을 제공하는 서비스는 메이커다오(MakerDAO), 컴파운드 파이낸스(Compound.Finance), 달마(Dharma), DY/DX 등이 존재
표준화 동향	<ul style="list-style-type: none"> 블록체인 관련 공적 표준은 ISO 및 ITU-T가, 사실 표준은 W3C 및 IEEE가 담당 중 (ISO) TC307(블록체인과 DLT)에서 DLT 기반 기술, 블록체인 보안 및 식별체계, 스마트 계약, 거버넌스, 블록체인 유스케이스와 블록체인 상호운용성을 표준화 중 (ITU-T) SG17(정보보호 연구그룹)에서 DLT 관련 정보보호 표준권고 작업을, FG-DLT에서 DLT 응용과 서비스의 식별·분석·구현을 위한 모범 사례 및 지침을 도출 중 (W3C 및 IEEE) 2016년부터 블록체인 기술표준 개발 활동을 시작하였으나, 미흡한 수준
블록체인 프로토콜	<ul style="list-style-type: none"> 기존의 블록체인은 트랜잭션 또는 스마트 컨트랙트들이 포함된 블록이 순차적으로 연결되는 구조 이러한 방식은 제한된 트랜잭션 처리속도를 가짐. 따라서 짧은 시간에 많은 트랜잭션이 발생 시 경우에는, 트랜잭션이 확정되기 위하여 긴 시간을 기다려야 하는 문제점이 있음 이를 해결하기 위해, 세그윗(Segwit), 샤딩(Sharding) 등의 기법에 대한 연구가 진행 중 확장성 문제에 대한 다른 관점의 해결책으로서, 블록 구조가 없이 블록체인을 구현하려는 시도(예컨대, DAG 구조 기반 트랜잭션 체인)가 존재
데이터 관리	<ul style="list-style-type: none"> 블록체인 기술은 분산화되어 있음에도, 단일한 기록을 제공할 수 있음. 이를 통해 많은 산업과 조직들(예를 들면, 자선 단체, 공급망, 의료 서비스 등)이 성능과 보안을 향상 블록체인 기술은 재능있는 이들이 누가 자신들의 콘텐츠를 대여하고, 구매하고, 사용하는지에 대한 불변하는 공개적 기록을 제공하는 플랫폼을 만드는데 사용될 수 있음. 이러한 플랫폼은 디지털 컨트랙트 위에서 자동으로 실행되는 스마트 컨트랙트를 통한 결제도 가능 블록체인 기술은 공급망 네트워크 내의 생산과 유통 과정을 추적하는데 사용할 수 있음. 분산화된 데이터베이스는 관련 데이터를 안전하게 기록하고 제품의 진위성을 보장하며, 결제와 운송의 투명성을 보장하는데 적합
증권형 토큰(STO)	<ul style="list-style-type: none"> STO는 underlying asset이나 사업에 대한 지분을 암호화폐를 통해 디지털 자산화하려는 것으로서 전통 자산의 디지털 자산화를 통한 분산화 과정으로 정의 STO의 경우 실제 자산과 매칭된 토큰으로 기존 토큰의 실질 가치가 있는지에 대한 의문을 해소하여 암호화 화폐 시장의 질적 성장이 촉진될 수 있는 역할을 하지만, 기존의 증권 시장에서 발생할 수 있는 문제에 대한 각국의 관리 감독 규제에 똑같이 노출되기 때문에 기대만큼 STO 시장의 유동성을 확대하기 어려움

(3) 생태계 핵심플레이어 동향

◎ 대기업의 시장 동향

- ☐ (삼성그룹) 블록체인 기술 진출을 선언하고 스타트업들을 인수
 - 삼성전자는 2020년 암호화폐 지갑 '삼성 블록체인 월렛' 출시
 - 한국정보인증과 블록체인 기술 활용하여 정보의 위·변조 불가능한 모바일 운전면허 확인 서비스 2020년 말까지 출시 목표
 - 위메이드의 블록체인 전문 계열사 위메이드트리와 손잡고 블록체인 플랫폼 '위믹스'를 탑재한 스마트폰 '위믹스 폰'은 토큰 보관 및 거래와 트랜잭션 확인 가능
- ☐ (삼성SDS) 삼성SDS의 넥스레저(Nexledger)는 블록체인 플랫폼에 기반하여 물류 이력관리 서비스를 제공
 - 세계 최대 가전·정보기술(IT) 전시회인 CES 2020을 통해 미국에 자사 블록체인 플랫폼인 '넥스레저' 수출에 성공
 - 아이티센과의 컨소시엄을 통해 행정안전부의 모바일 공무원증 구축사업의 우선협상대상자로 선정
- ☐ (한화투자증권) 2019년 태국 블록체인 핀테크 업체 라이트넷(Lightnet)에 싱가포르 UOB 벤처 매니지먼트와 DU 캐피탈, 호페신 벤처, 시그넘 캐피탈, 중국 유니 프레지던트 에셋 홀딩스, 일본 세븐뱅크, 홍콩 해쉬케이 캐피탈 등이 함께 투자
 - 라이트넷은 해외 송금 서비스를 제공하는 업체로 제3의 신용기관을 거치지 않고 바로 해외에 송금하도록 해 수수료 비용과 시간을 절약하는 블록체인 기반 송금 서비스 VELO를 출시
- ☐ (KB국민은행) 비트코인, 이더리움 등 암호화폐 관리 서비스인 'KBDAC'에 대한 상표 2020년 1월 31일에 출원
 - 특허는 비트코인, 이더리움 등 암호화폐에 대한 거래, 정보제공, 관리, 자문, 상담, 투자, 운용 등의 내용으로 구성
 - 특금법(특정 금융거래정보의 보고 및 이용 등에 관한 법률) 이후 금융권도 암호화폐 산업 적극적 개입
- ☐ (카카오) 자회사 그라운드X를 통해 블록체인 기반의 토큰 '클레이(Klay)'와 블록체인 지갑 '클립' 출시
 - 카카오톡 사용자 수는 1억 이상으로 잠재 수요층 다수, 업계에서는 단숨에 주요 암호화폐로 급부상 예상
 - 클레이튼 블록체인 네트워크에는 LG전자, SK네트웍스, 셀트리온 등 국내외 약 29개 기업이 참여 중

[클레이튼 블록체인 네트워크 현황]



* 출처: 클레이튼 공식 홈페이지

- ☐ (아이콘루프) 2020년 6월 60억원 규모의 브릿지 라운드 투자 유치하여 총 누적 투자금 160억원 기록
 - 금융권에서 유일하게 즉시 도입 가능한 DID 솔루션 보유한 기업으로 핀테크혁신펀드의 조성 지원
 - 향후 다양한 페이먼트 사업으로 확장할 경우 다날의 통합결제 플랫폼과 협업하면 강력한 시너지를 낼 수 있을 것으로 판단
- ☐ (롯데그룹) 대표 서비스로 하이퍼레저 패브릭 기반 자체 블록체인 플랫폼인 랄프(LALP, LOTTE Agile Ledger Platform)를 2020년 3월 출시
 - 랄프는 기업이 기존 및 신규 서비스에 블록체인을 손쉽게 적용할 수 있도록 돕는 통합 플랫폼으로 현재 온프레미스(On-premise)와 클라우드(L.Cloud) 환경을 모두 지원
- ☐ (기업연합) DID(Decentralized Identity)를 활용한 탈중앙화 신원확인 서비스를 제공하기 위한 기업연합이 경쟁 중
 - 공인인증서 등 기존의 신원 또는 자격증명 확인 방식은 중앙시스템(특정업체나 기업)이 가졌다면 DID는 개인(정보주체)이 직접 정보를 관리하고 증명
 - 신원증명에 필요한 개인 정보(성명, 생년월일, 주소, 각종 증명서)를 스마트폰 내 지갑에 저장했다가 제출하는 방식

[3대 DID⁶⁾연합 현황 비교]

블록체인개발사	아이콘루프	sk 텔레콤	라온시큐어
참여자 특징	금융권	통신사, 대기업	글로벌 IT
주요참여기관	코스콤	코스콤	금융결제원, 한국전자서명포럼, 한국 FIDO포럼
관련 정부부처	금융위원회	과학기술정보통신부, 한국인터넷진흥원 주관'2019 블록체인 민간주도 국민 프로젝트'	과학기술정보통신부, 한국인터넷진흥원, 공공선도 시범사업자
참여기관 및 기업수	44개	11개	56개
출범일	2019년 11월	2019년 7월	2019년 11월
주요 구성원	이현재 위원장(현 여시재 이사장, 전 경제부총리겸 재정경제부 장관)	추진체 결성 中	김영린 회장(현 EY한영 부회장, 전 금융보안원장)
상용화 예상 시기 및 목표	1분기 마이아이디서비스 출시	연초 이니셜앱 출시	상반기 병적증명발급 처리 서비스 출시

* 출처: 3대 DID연합, 단기 승부처 '서비스 상용화', 2020, 팩스넷뉴스,

◎ 중소기업의 시장 동향

□ (두나무) 두나무의 블록체인 기술 자회사 람다256이 공유형 블록체인 서비스 출시

- 프라이빗 블록체인도 하나의 블록체인을 공유해서 쓸 수 있어 기업형 블록체인 서비스의 발전에 기여

□ (GMR 머티리얼즈) 블록체인 전문기업 글로스퍼의 지분 74.5%를 265억 원에 양수하기로 결정

- 글로스퍼는 자체 기술력을 보유한 국내 1세대 블록체인 전문기업으로 퍼블릭 블록체인과 프라이빗 블록체인 등의 영역에서 시장을 선도하는 기업으로 다수의 블록체인 상용화 이력이 있으며, 정부·지자체·민간 등 다양한 분야 진출
- 업비트의 신뢰 제고를 위해 두나무는 AML(자금세탁방지) 시스템 구축과 KYC(고객 알기 제도) 정책 강화를 진행 중이며, 2019년 12월 인도네시아에서 정식으로 암호화폐 거래소 사업자 등록

□ (테라) 블록체인 기반 핀테크 기업 테라는 2019년 간편결제 애플리케이션(앱) '차이(CHAI)'로 전국 CU편의점과 제휴

- 기존에 '티몬'과 '야놀자' 등 온라인 간편결제에 주력했던 '차이'가 오프라인 시장에 진출

□ (무비블록) 블록체인 기반 영화배급 플랫폼 무비블록이 영화 제작자가 자신의 작품을 공유할 수 있는 정식 서비스 2019년 출시

- 영화 제작자 및 배급사는 영상 콘텐츠를 서비스 플랫폼에 업로드하고 전 세계에 홍보가 가능하고 서비스 사용자는 플랫폼을 통해 영화제 수상작과 같은 평소 접하기 어려운 영화를 시청

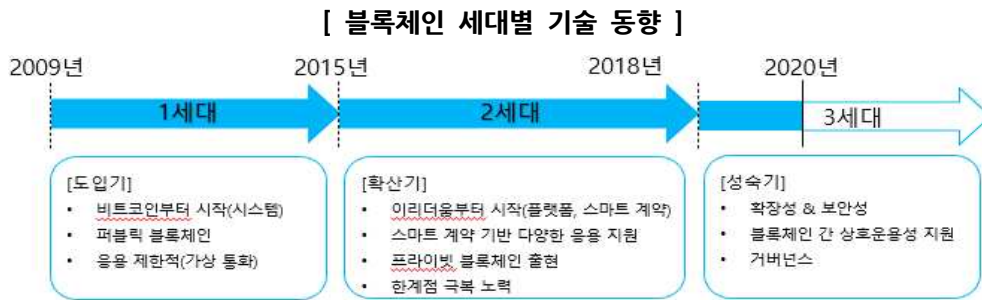
6) 탈중앙화 신원확인(Decentralized Identity)

3. 기술 분석

가. 해외 기술 동향

(1) 주요 기술 동향

◎ 블록체인 프로토콜(세대)별 기술 동향



* 출처: “블록체인 세대별 기술 동향”, 2018, 한국전자통신연구원,

- 분산장부 공유기술을 처음 도입 및 적용한 비트코인이 발표된 2009년부터, 이더리움이 발표되는 2015년 전까지의 시기를 1세대, 스마트 계약 기술을 활용한 이더리움을 시작으로 다양한 분야에 확산 가능성을 타진하는 응용기술이 등장하는 현재까지의 시기를 2세대로 크게 구분 가능함. 최근 IOTA, Hashgraph 등 DAG(Directed Acyclic Graph) 형태를 갖는 블록체인을 3세대 블록체인으로 구분

[2020년 10대 전략 기술 동향]

2019년		2020년	
핵심트렌드		전략기술	
지능	<ul style="list-style-type: none"> 자율 사물 증강 분석 인공지능 주도 개발 디지털 트윈 	인간중심	<ul style="list-style-type: none"> 초자동화 다중 경험 전문성의 민주화 인간 증강 투명성 및 추적성
디지털	<ul style="list-style-type: none"> 자율권을 가진 에이지 몰입 경험 		
메시(Mesh)	<ul style="list-style-type: none"> 블록체인 스마트 공간 	스마트 공간	<ul style="list-style-type: none"> 자율권을 가진 엣지 분산형 클라우드 자율 사물 실용적 블록체인 인공지능 보안
공동영역	<ul style="list-style-type: none"> 디지털윤리와 개인정보보호 양자 컴퓨팅 		

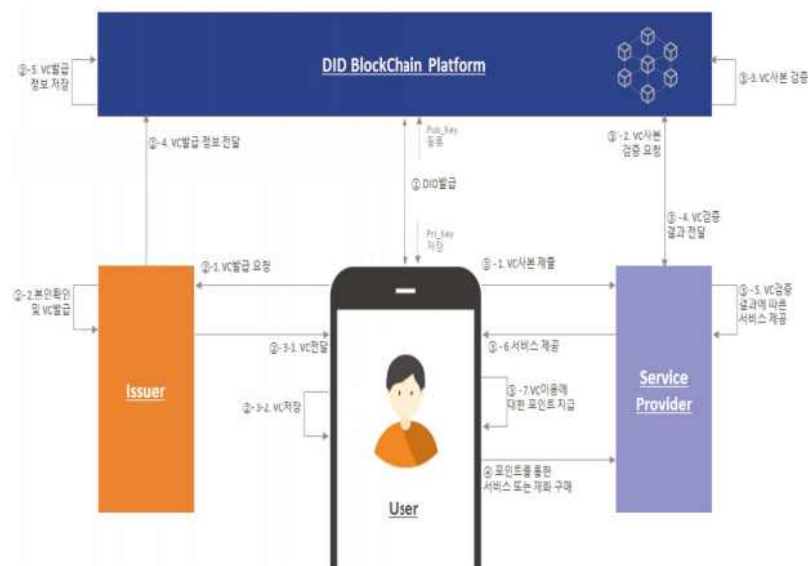
* 출처: Top 10 Strategic Technology Trends for 2020, 2019, Gartner

- 1세대 및 2세대 블록체인 기술은 거래 속도, 처리 용량, 상호 운용성, 거버넌스, 확장성 등의 문제를 내포하고 있음. 이하 다양한 각도에서 현존하는 블록체인 프로토콜들에 대한 분석을 수행

◎ 분산 ID(DID)의 활용 증대

- 미래사회에서 ICT의 발전에 따라 다양한 행위, 다양한 전자상거래가 온라인에서 수행될 것으로 예상되어 온라인 활동을 더욱 편리하게 해줄 인증 방법이 연구되고, 동시에 프라이버시권 문제가 대두됨에 따라 자기정보를 통제할 수 있는 방법이 필요
 - 블록체인이 별도의 기관 없이도 저장된 데이터의 신뢰성을 담보할 수 있는 수단을 제공함으로써 전자서명이나 생체 정보 등과 접목될 수 있도록 연구, 설계되고 있으며 실제 서비스로 구현 중
- 분산 ID(DID) 구성요소
 - 발행인(Issuer): 검증 가능한 자격증명을 생성하는 개체로 특정 주체와 검증 가능한 자격증명을 연결하고 이를 유저에게 전달하는 역할
 - 서비스제공자(Service Provider): 유저의 자격증명을 활용하며 서비스를 제공
 - 유저(User): 검증 가능한 자격증명을 소유하고 있는 개체로 검증 가능한 자격증명에서 제공하는 ID 데이터 집합을 생성
 - 검증인(Verifier): 유저에게 검증 가능한 제공 ID데이터 집합인 Verifiable Presentations을 전달받아 소유자가 검증 가능한 자격증명에 특정한 특성이 포함되어 있는지 확인하는 개체
 - 검증 가능한 데이터 저장소(Verifiable data registry): 식별자, 키 그리고 관련 데이터를 생성하고 검증하는 중재 시스템

[DID FLOW]



* 출처: “블록체인 전문위원회 블록체인 기술 동향 보고서”, 2020, KISIA한국정보보호산업협회

□ DID FLOW 과정

- DID 발급 후, Public Key는 블록체인 플랫폼에, Privacy Key는 개인 모바일 단말기에 저장
- 유저는 자격증명이 가능한 Issuer에게 VC(Verifiable Credentials) 발급을 요청
 - Issuer는 휴대폰인증 등 대면인증을 통해 본인임을 확인하고 VC 발급
 - 발급된 VC는 User의 휴대폰으로 전달하여 저장
 - 발급된 VC의 정보를 블록체인 플랫폼에 저장
- VC의 정보 추출이 불가하도록 Service Provider에게 사본을 제출
 - 제출된 VC사본을 블록체인 플랫폼을 통해서 검증을 진행
 - Service Provider는 VC검증 결과를 전달받아 이에 맞는 서비스 제공
 - VC이용에 대한 혜택으로 포인트 지급
- 유저는 포인트를 통해 서비스나 물건 구매

◎ 블록체인 프로토콜 현황

□ 비트코인

- (운영구조) 비트코인은 퍼블릭 블록체인으로, 블록체인을 이루는 블록을 생성하는 데 참여하는 노드들에게 연산 능력에 따라 경제적 보상을 부여하여, 시스템을 지속적으로 운영
- (합의 알고리즘 및 거버넌스 문제) 작업증명(Proof of Work) 방식의 합의 알고리즘을 차용. 자체 의사 결정 기능이 없어 하드 포크가 발생 가능
- (확장성) 비트코인은 블록 생성 시간을 평균 10분으로, 블록의 크기를 1MB로 제한하여 트랜잭션 처리 속도가 느림. 따라서 낮은 확장성을 가짐. 이를 해결하기 위하여 SegWit(Segregated Witness), 라이트닝 네트워크(Lightning Network) 등의 개선 방식이 연구 중
- (기타) 라이트 코인(Litecoin), 리플 등 응용사례들이 존재하나 비트코인에 비해 획기적인 개선 특징 없음

[블록체인 프로세스 분류]

구분	주요내용
작업 증명 (Proof of Work: PoW)	• 비트코인의 창시자인 나카모토 시토시가 제안한 가장 기본적인 합의 알고리즘으로, P2P 네트워크에서 시간 및 비용을 들여 실행된 컴퓨터 수행작업을 신뢰하기 위해 참여 당사자 간에 검증하는 방식
지분 증명 (Proof of Stake: PoS)	• 작업 증명 방식(PoW)의 단점인 과도한 에너지 소비문제를 해결한 것으로, 블록 생성된 지분에 참여자가 보유한 지분이 반영되도록 하는 방식
위임지분증명 (Delegate Proof of Stake: DPoS)	• 반 중앙화도니 방식으로, 지분을 보유하고 있는 사람이 자기 권한을 대표자에게 위임하여 대표자들이 블록 생성 및 검증에 대한 권한을 행사하는 방식
Pol (Proof of Importance)	• NEM(New Economy Movement)과 같은 가상화폐에서 사용하는 알고리즘으로, 네트워크 참여도에 따라 지급 보상이 달라짐
PBFT (Practical byzantine Fault Tolerance)	• PoW, PoS 단점을 해결한 방식으로, 블록체인 시스템에서 약속된 행동을 하지 않고 일부러 잘못된 정보를 전달하는 비잔틴 노드가 있을 수 있는 비동기 시스템일 때, 노드 전부가 성공적인 합의를 할 수 있도록 개발된 증명방식
Tendermint (PBFT+DPoS)	• PBFT 알고리즘을 보완, 공개 및 비공개 블록체인에 맞도록 개량한 증명방식으로, 추가로 DPoS가 포함되어 지분 기반 투표를 진행하는 방식
Consensus-by-bet	• 기존의 알고리즘과는 달리 참여자의 동의 및 베팅을 통해서 블록체인의 거래를 승인하는 방식

* 출처: 이재규, “블록체인을 활용한 해외직구 프로세스 개선방안 연구”, 2018, 숭실대학교

□ 이더리움(Ethereum)

- (운영구조) 비트코인과 유사한 운영구조를 가짐. 다만, 플랫폼 형태로 제공되며 스마트 컨트랙트 기능을 제공
- (합의 알고리즘 및 거버넌스 문제) Ethash라고 불리는 비트코인과 유사한 작업 증명 방식의 합의 알고리즘을 가짐. Casper를 거쳐 궁극적으로는 PoS 방식으로 전환하고자 함. 이더리움은 비트코인과 마찬가지로 거버넌스 문제를 가지며, DAO(Decentralized Autonomous Organization) 해킹 사건으로 인해 하드포크가 발생
- (확장성) 이더리움의 초당 트랜잭션 처리 능력은 15TPS 정도임. 따라서 확장성 문제를 해결하기 위해 Sharding 등의 기술을 도입하고자 연구가 이루어지는 중

□ EOS

- (합의 알고리즘) EOS는 DPoS(Delegated PoS)와 PBFT를 기반으로 하는 합의 알고리즘을 사용함. DPoS 방식으로 21명의 블록 생성자를 선출하며, PBFT 방식으로 투표를 통해 0.5초마다 블록을 생성. 소수의 합의 주체만이 참여하고 빠른 처리가 가능
- (거버넌스 문제) EOS는 지분 소지자들이 투표를 통하여 분리된 블록 생성자에게는 표를 주지 않을 것이므로 하드 포크의 문제가 발생하지 않는다고 주장
- (확장성) 분산 합의 알고리즘의 특성 상 높은 처리속도를 자랑하여 확장성 이슈가 상대적으로 적음

(2) 해외기업 기술동향

- Amazon, Google, Apple과 같은 거대 인터넷 기업들은 4차 산업혁명의 핵심 ICT 기술인 클라우드 컴퓨터를 이용하여 P2P 생산의 결과물을 자신들의 데이터센터에 저장하는 구상 중
- 데이터의 축적, 관리, 접근, 이용 등을 본인들의 통제 하에 두려는 의도로 해석
 - 클라우드는 정보나 서비스를 개인 PC나 기업 서버가 아닌 대형 플랫폼을 활용해 처리하면 이용자가 갑자기 몰려도 용량 증설이 용이

[글로벌 IT 기업의 서비스로서 블록체인 활용 사례 요약]

기업명	플랫폼	세부내용
IBM	블록체인 플랫폼	<ul style="list-style-type: none"> • 클라우드 기반 플랫폼에서 블록체인 생태계를 신속하고 경제적으로 개발, 관리 및 운영 가능 • 베타 기간 Starter Membership Plan 무료 가입 및 Enterprise Membership Plan으로 프리미엄 기능 지원
MS	애저 플랫폼	<ul style="list-style-type: none"> • 코다(Corda), 이더리움(Ethereum), 하이퍼레저 패브릭(Hyperledger Fabric)을 포함하여 적합한 블록체인 원장을 고객이 선택할 수 있도록 사전 구성된 모듈형 옵션으로 애플리케이션 개발 소요시간이 단축 • 블록체인 솔루션 자체에 대해 요금을 부과하지 않으며 컴퓨팅, 스토리지 및 네트워킹 등 리소스만 구매하는 방식
Amazon	블록체인 템플릿	<ul style="list-style-type: none"> • 이더리움이나 하이퍼레저 패브릭 원장 기술을 기반으로 구축 • 이더리움은 공개 애플리케이션을 대상으로 하며, 하이퍼레저 패브릭은 프라이빗 클라우드 애플리케이션에 적합
Oracle	블록체인 클라우드 서비스	<ul style="list-style-type: none"> • PaaS(Platform-as-a-Service) 서비스의 일환으로 블록체인 클라우드 서비스를 선제적으로 시작 • 오픈소스 하이퍼레저 패브릭 프로젝트 위에 구축되어 기업 고객이 관리하는 방식으로 블록체인 제공
Baidu	블록체인 오픈 플랫폼	<ul style="list-style-type: none"> • 2018년 초 자체 개발한 기술로 BaaS 플랫폼을 출시 • 거래의 빠른 작성 및 추적을 목표로 디지털 통화, 보험 관리, 디지털 청구, 은행 신용 관리 등 서비스 분야에 활용 계획
Huawei	블록체인 서비스	<ul style="list-style-type: none"> • 기업들이 스마트 계약을 체결할 수 있도록 지원하는 블록형 플랫폼을 출시 • 오픈소스 하이퍼레저 패브릭 위에 구축되어 공급망과 관련된 솔루션 개발, ID 확인, 재무 감사, 토큰화된 증권 자산 등 공공서비스 개발에 활용할 계획

* 출처: 해외주요국 블록체인 시장전망 및 기업 동향, 2018, SPRi

[물류/유통 분야에서의 블록체인 기술 활용 사례]

구분	주요내용
에버레저	• 2015년 설립된 영국 런던 스타트업으로, 다이아몬드 특성 정보, 감정서, 소유권 상태 등의 정보를 블록체인에 저장 및 관리하는 서비스 제공
루이비통	• 명품 패션 브랜드 업체 루이비통모에헤네시(LVMH) 그룹이 블록체인 기술 개발업체 컨센시스, 마이크로소프트의 애저 클라우드 서비스 개발팀과 함께 블록체인 기반 상품 이력 관리 및 추적 플랫폼을 개발하고 있으며, 개발이 완료되면 진품 여부를 가리기 위해 제품 원산지부터 판매 시점까지 전 유통 과정의 추적이 가능하고, 지적 재산권 관리, 고객 맞춤형 상품제안, 고객 이벤트 관리, 허위 광고 방지 등의 부가 서비스도 제공할 예정
징동닷컴	• 중국의 2위 전자상거래 업체로, 5만 종류의 제품 추적을 위해 블록체인 기술을 활용
엘버트슨	• 미국 전역에 2,300여개의 지점을 가지고 있는 세계 2위 슈퍼마켓 체인으로, 로메인 상추를 대상으로 “푸드 트러스트”를 시범 적용할 예정
코다 커피	• 최근 고객들이 커피 공급망의 모든 기점을 따라가면서 그 경로를 추적할 수 있는 클라우드 기반 원장에 접속하게 함으로써, ‘세계 최초의 블록체인 추적 커피’를 제공
토큰리	• 블록체인 기반 음원판매 서비스 ‘토큰.FM’은 기존 음원사이트의 유통구조인 음악인과 음원 유통업체, 제작사, 소속사 등과 계약을 맺고 수익을 정산한 뒤 배분 받았던 구조중개 없이 음악인과 소비자 간 직접 거래함으로써 음악인 수익 증가 및 거래 정보를 블록체인에 기록하여 정확한 정보 제공 가능

* 출처: 블록체인허브 2018.09, 헤럴드 경제 2019.04, 이코노믹 2018.04

[금융/보험 분야에서의 블록체인 기술 활용 사례]

구분	주요내용
지브롤터 증권거래소	• 지브롤터 증권거래소는 2016년 비트코인ETI라는 암호 해독 기능을 공개한 유럽 최초의 비트코인 제품을 출시. 블록체인을 사용하는 핀테크 기업의 맞춤형 라이선스 도입
마스터 카드	• 분산 원장 기술을 도입해 기록된 보증을 사용해 즉석 지불을 위한 방법 및 시스템을 개발하는 ‘블록체인으로 지불카드 검증을 위한 방법과 시스템’에 대한 특허 출원. 계정 프로필 저장, 계정 번호 및 잔액 포함, 인수 금융기관으로부터 결제 네트워크를 통한 거래 메시지 수신 등의 전자거래 처리 과정을 거치는 블록체인 송금서비스 특허 출원
IBM	• Northern Trust와 파트너십을 맺고 하이퍼레저 패브릭 기반 플랫폼 제작. 관료주의가 팽배한 사모펀드 거래시스템의 검증 속도를 높이고 거래 전반에서 투명성을 높임 리눅스재단에서 추진한 오픈소스 블록체인 프로젝트인 ‘오픈소스 하이퍼레저 패브릭(Hyperledger Fabric)’ 플랫폼에서 금융 기관이 블록체인을 사용하여 국경 간 결제를 처리할 수 있도록 돕는 बैं킹 솔루션을 개발
R3	• 100개 이상의 회원사가 참여하는 그룹으로 오픈소스 블록체인 플랫폼인 코타(Corda)와 비즈니스 사용자를 위해 최적화된 블록체인 플랫폼인 코다 엔터프라이즈(Corda Enterprise)를 개발함. RBS은행과 영국 금융감독청(Financial Conduct Authority, FCA)은코다 플랫폼을 사용하여 은행에 대한 모기지 납부 영수증 및 데이터 전송 자동화

* 출처: 블록체인허브 2018.09, 헤럴드 경제 2019.04, 이코노믹 2018.04

□ (중국) 2016년부터 본격적으로 블록체인 연구와 지원

- 2015년 13차 5개년계획(2016~2020년)에서 블록체인을 “전략적 최첨단기술”로 규정하여 진흥을 추진
- 2019년 10월 시진핑 국가주석은 “블록체인 핵심 기술을 인공지능, 빅데이터, 사물인터넷 등 첨단정보 기술과 융합하고 각종 산업부분에 적용”하라고 함

[중국 주요기업 블록체인 추진 현황]

분야	대표기업	주요내용
물류 및 유통	알리바바	• 2019년 말 20억 달러의 자금으로 인수한 수입 e-커머스 플랫폼 코알라(Koala)가 블록체인 QR코드와 위조방지 지문서명 기능이 추가된 블록체인 추적 시스템을 도입
	테슬라	• 2020년 4월 중국 해운 기업 코스코(COSCO), 항구 운영 기업 SIPG(SHANGHAI INTERNATIONAL PORT GROUP)와 함께 “화물 통과(방출) 공정”에 블록체인 기술을 적용하는 시범 프로젝트를 완수
게임	바이두	• 2018년 2월 ‘라이츠거우(Letsdog)’라는 블록체인 기반 강아지 육성게임 분산형 앱(DAPP)을 출시
	텐센트	• 텐센트의 자체 블록체인 플랫폼인 트러스트SQL을 기반으로 제작된 블록체인 게임 “렛츠헌트몬스터(Let's Hunt Monster)”가 2019년 4월 중국 아이폰(iOS) 앱스토어에서 무료게임 분야 다운로드 순위 1위를 기록
부동산	이취치예지탄	• 부동산 기업 이취치예지탄은 2019년 1월 부동산거래, 정보서비스, 자산운용 등 네 가지 기능을 갖춘 ‘중국자산정보컨설팅서비스(CIAC)’ 플랫폼 운영을 시작
	형다디찬	• 2020년 4월 블록체인 플랫폼에서 중국 최초로 부동산 전자증빙 발급을 시작
	중국은행	• 2019년 4월 홍콩 ASRT와 NWD가 공동 개발 중인 부동산 서류 공유 블록체인 플랫폼의 PropTech 활용, 거래서비스 개시
	상하이체육국	• 블록체인 기반 위챗 애플릿을 출시하여 온라인으로 일대일 헬스 수업을 받을 수 있는 ‘홈 헬스’ 서비스 제공
금융/보험	핑안(平安)	• 중국 대형 보험금융 기업인 핑안의 핀테크 부분 자회사 등이 공유 데이터베이스 기반 단일 시스템을 통해 중국 세관과 항만, 물류 기업 등 수출입 기업들로부터의 정보를 포괄하여 관리할 수 있는 블록체인 기반 정보공유 플랫폼 개발
	인민은행	• 2020년 2월 블록체인 보안 표준 규정인 “금융 분산식 원장 기술 보안 규범(JR/T 0184-2020)”을 발표, 인프라, SW, 원장데이터, 합의 프로토콜 등 보안 시스템을 규정/적용

* 출처: 국방통합데이터센터 작성

□ (미국) 블록체인을 산업 전반에 적용하기 위해 다양한 법률 제정을 추진하고, 다수의 부처가 적극적으로 시범사업과 연구를 추진 중

- 서비스를 위한 규제 연구를 강화
- 주정부 및 지방정부는 지방 경제 활성화, 투표, 의료 서비스, 공공 서비스 향상을 위해 블록체인 기술을 도입하여 산업경쟁력을 강화

[미국 주요기업 블록체인 추진 현황]

분야	대표기업	주요내용
콘텐츠저작권	코닥	• 블록체인 기반 저작권 보호 플랫폼 코닥원(KodakONE)을 활용, 플랫폼 내에서 거래 시 코닥코인으로 체결
	툰토큰 (TuneToken)	• 블록체인에 음원 저작권을 기록해 데이터베이스화하고 해당 음원을 활용 가능
물류/유통	월마트	• 2016년부터 IBM과 블록체인 기반 시스템 개발을 협업, 2017년 징동닷컴, IBM, 칭화대, 전자상거래기술연구소와 함께 세이프티 얼라이언스 설립
부동산	프로피 (Propy)	• 이더리움을 기반으로 부동산 거래를 획기적으로 줄이고 안전한 거래가 가능
	유비트커티 (Ubitquity)	• 블록체인 기반의 부동산 계약 보관 플랫폼으로 부동산 거래의 고질적인 문제를 해결할 것으로 기대
의료	IBM	• 미국 FDA와 블록체인 기술을 활용하여 환자 데이터를 안전하게 공유하기 위해 공동개발 계약을 체결하고 개발 중이며, 임상시험, 게놈데이터, 사물인터넷(IoT)의 보건데이터 등을 포함한 환자 데이터를 연구
	인텔	• DNA와 RNA에 있는 핵염기 순서를 규명하고 저장하는 플랫폼인 시퀀스마이닝플랫폼(SMP) 기술 특허를 등록
금융/보험	나스닥	• 비트코인 및 암호화폐를 도입하였으며, 엔터프라이즈 블록체인 솔루션을 개발하는 벤처 스타트업에 상당한 금액을 투자
	연방준비은행	• IBM과 함께 블록체인을 응용한 지급 결제 시스템을 개발

* 출처: 국방통합데이터센터 작성

◎ 해외 DID 적용 사례

- ☐ (캐나다) 2017년부터 캐나다 은행 및 정부기관을 중심으로 블록체인 기반의 신원인증 시스템인 ‘베리파이드미(Verified.Me)’ 시범사업을 운영하고 있음
- ☐ (스위스) 유럽 블록체인 산업의 중심지로서, 2017년부터 스위스 Zug(Zug)시에 ‘크립토 밸리’를 조성하였으며 블록체인 기반의 신원인증 사업을 운영 중
 - 주크 시민 대상으로 블록체인 기반 신분증을 발급하는 파일럿을 운영 중이며 해당 신분증을 이용해 주크시에서 제공하는 공공 서비스를 ID와 패스워드 없이 사용 가능
- ☐ (스페인) 2019년 6월 스페인 카탈루냐 정부는 탈중앙화 신원확인 플랫폼인 ‘이덴티캣(IdentCAT)’ 프로젝트를 수행하겠다고 밝힘
 - 2016년 7월 1일 시행된 전자본인확인인증서명(eIDAS: Electronic identification and trust services for electronic transaction)은 유럽연합 회원국 간 국경을 추월한 전자적 환인과 거래에 대한 프레임워크 마련을 위해 제정
- ☐ (영국) 에스토니아의 블록체인을 활용한 의료정보관리 사례를 영국의 Reform이라는 씽크탱크에서 공공서비스 신원관리 전체로 확대 적용하는 모델을 제안

나. 국내 기술 동향

- 블록체인 분야의 기술경쟁력 평가 결과, 최고기술국은 미국으로 나타났으며 우리나라의 경우는 최고기술국 대비 87% 수준으로 나타났고 중소기업은 80% 수준으로 평가되었음
- 최고기술국 대비 우리나라의 기술격차는 1.3년으로 평가되었으며 중소기업의 경우는 1.8년으로 평가되었음

(1) 기술 동향

- 블록체인 기술분야는 해외 선진국들에 비해 기술수준에 있어서 2017년 기준 2.4년의 기술 격차가 존재하는 것으로 분석
- 블록체인 기술경쟁력('17) : 미국 > 유럽(96%) > 일본(84.8%) > 중국(78.9%) > 한국(76.4%)

[블록체인 분야별 최고기술국 대비 기술 수준 및 격차]

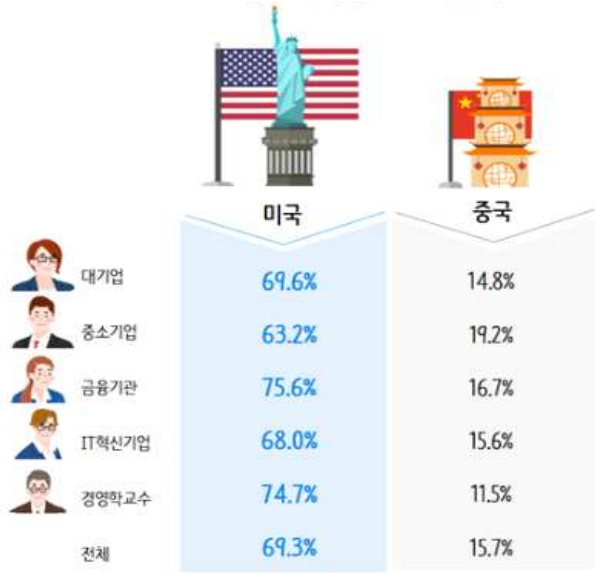


* 출처: "ICDT 기술수준조사보고서", 2017, 보통신기술진흥센터

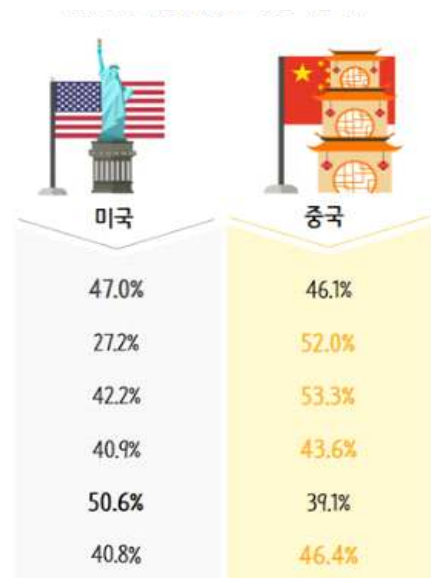
- 현재 블록체인 주도국은 미국이나, 향후 5년 내 중국이 주도 예측
- 블록체인 전문가 대상으로 실시한 설문조사의 응답자 대부분이 현재는 미국이 블록체인 기술을 주도하고 있다고 평가했지만, 향후 5년 내에는 미국과 함께 중국이 블록체인의 주도권을 가질 것으로 전망

[블록체인 도입실태 및 향후 전망에 대한 의견조사]

블록체인 기술을 주도하고 있는 국가



5년내에 블록체인 주도권을 가질 국가



* 출처: KDI경제정보센터

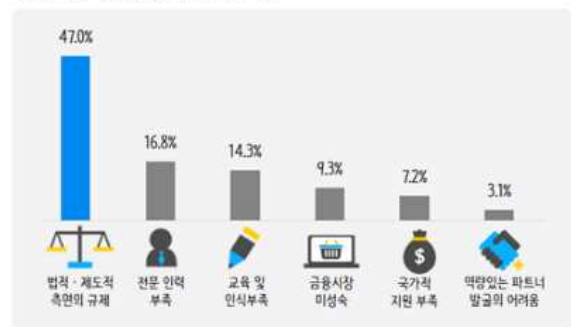
□ 우리나라 블록체인 경쟁력은 주도국의 절반 수준으로 현재 평가

- 우리나라의 블록체인 기술과 경쟁력이 뒤쳐진 이유가 '법적·제도적 측면의 규제'에 있다고 지적
- '블록체인의 잠재력에 비해 과소평가되고 있다'며 사회적 인식 부족 지적

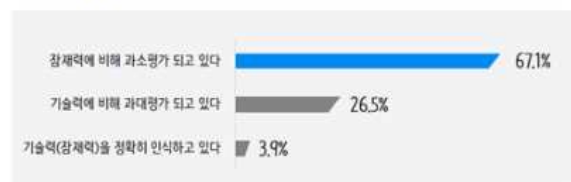
[블록체인 도입실태 및 향후 전망에 대한 의견조사]



블록체인 기술과 경쟁력이 뒤쳐진 이유



블록체인에 대한 우리사회 평가



* 출처: KDI경제정보센터

- ☐ 전 세계적으로 블록체인 기술에 대한 기술개발이 가속화되고 있는 가운데 기술 활용을 위한 국제적 협업 사례도 증가하는 추세이며, 특히 글로벌 다국적 기업들이 블록체인에 대한 관심을 견인하고 있으며, 개념증명 및 시험 프로그램 등이 가동되면서 분산형 원장 기술에 대한 신뢰 상승
- ☐ 금융 분야에서 시작되었던 블록체인 기술 개발의 흐름이 물류, 유통, 정부 공공행정 서비스 등 다양한 분야로 확대되는 추세
- ☐ 기존 분산 DB 기술로 구현이 충분히 가능한 영역에 대한 블록체인 기술 적용은 무의미하다고 판단되며, 특히 탈중앙화에 대한 명확한 니즈가 존재하는 비즈니스 영역에 대한 블록체인 기술 적용이 이루어지는 추세 (특히, 투명성, 효율성, 비용 등 글로벌 공급사슬에 만연한 문제 해결의 방법으로 블록체인 기술을 적용)
- ☐ 블록체인의 역기능은 최소화하고 순기능은 최대화
 - 블록체인의 단점을 보완하는 프로젝트, 블록체인의 응용 및 확산 기술, 블록체인 프레임워크 그리고 제도 보완 등을 고려한 기술 개발 시나리오가 요구
 - 블록체인 기술은 사회 변혁 또는 사회 진보의 보폭이 넓어 아날로그 사업자의 저항 또는 기존 기득권과의 갈등 요소가 발생할 수 있어 기술 개발 시나리오에는 해당 기술이 파급시키는 문제에 대한 제도 보완을 함께 숙의하는 방향으로 진행

(2) 국내기업 기술동향

- ☐ 블록체인을 사회 전반적으로 혁신을 이루는 기반기술로서 4차 산업혁명의 핵심 산업으로 판단하고, “블록체인 기술 발전전략”을 통해 초기시장 형성기술, 경쟁력 확보, 산업 활성화 기반 조성의 3대 전략을 제시, 국가 혁신 동력을 발굴하고, 다양한 응용분야에서 부처 간 협업에 의한 시범사업을 활발하게 추진 중

[2020년 블록체인 공공선도 시범사업 선정과제]

분야	대표기업	주요내용
치안	경찰청	블록체인 기반 디지털 증거 관리 플랫폼 구축
농업	농촌진흥청	블록체인 기반 노지작물 생산·유통 관리 플랫폼 구축
사회안전망	보건복지부	블록체인 기반 복지급여 중복수급 관리 플랫폼 구축
식품안전	식품의약품안전처	블록체인 기반 식품안전 데이터플랫폼 구축
의료	강원도	블록체인 기반 강원도형 만성질환 통합 관리 플랫폼 구축
인증	경상남도	분산신원증명(DID) 기반 지역공공 서비스 플랫폼 구축
교통	세종특별자치시	블록체인 기반 자율주행자동차 신뢰 플랫폼 구축
	한국도로공사	블록체인 기반 상호신뢰 통행료 정산 플랫폼 구축
환경	부산광역시	블록체인 기반 상수도 스마트 수질 관리시스템 구축
	제주특별자치도	블록체인 기반 전기차 배터리 Life Cycle 관리시스템 구축

* 출처: 20년 블록체인 사업 통합 사업설명회, 2020, 과기정통부

[국내 주요기업 블록체인 추진 현황]

분야	대표기업	주요내용
보안/인증	SK텔레콤	LG유플러스, 코인플러그, 해치랩스 등과 협력해 전화번호를 바탕으로 신원을 간편히 증명할 수 있는 모바일 신분증 기술 개발
	파수닷컴	블록체인 기반의 증명서 확인검증 플랫폼인 파스블록 개발
물류/유통	삼성SDS	‘넥스레저(Nexledger)’ 블록체인 플랫폼을 활용하여 관세청 “블록체인 기반 수출통관 물류서비스” 시범운용
	현대글로벌비스	정보기술(IT) 전문기업 현대오토에버는 블록코와 손잡고 중고차 이력관리 서비스 개발
의료	메디블록	블록체인 기반으로 의료, 관광, 금융을 통합해 체계적인 의료 환경과 양질의 의료 서비스를 제공해 주는 의료관광 모바일 결제 플랫폼 ‘메디토’ 개발
	KBIDC	블록체인을 활용하여 DNA와 RNA에 있는 핵염기 순서를 규명하고 저장하는 플랫폼인 시퀀스 마이닝플랫폼(SMP) 기술 특허를 등록
금융/보험	삼성	갤럭시 S10에 전자지갑(월렛)을 탑재하여 암호화폐를 저장 및 송금할 수 있도록 하였으며, 디앱(DApp) 등 블록체인 서비스를 출시하고, 현재 블록체인 기반 신원확인 플랫폼을 개발 중에 있음
	SK C&C	하이퍼레저 패브릭 기반 프라이빗 블록체인에 리플 기반 가상화폐(암호화폐) 지급결제 시스템을 갖춘 블록체인 플랫폼 ‘체인Z’ 출시

* 출처: 국방통합데이터센터 작성

◎ 국내 DID 적용 사례

- ☐ (고용노동부) 학력증명서, 자격증, 경력 증명서 등 취업을 위해 필요한 증명서를 블록체인 시스템으로 제공·검증되는 방안이 추진 중이며, 해당 증명서를 디지털 지갑에 발급받아 온라인으로 제출하는 사업을 진행할 것이라고 발표
- ☐ (행정안전부) 2019년에 전자증명서 발급, 유통하는 플랫폼을 구축한 뒤 시범 서비스를 거쳐 2020년부터 전자증명서를 발급 및 유통
 - 블록체인 기반의 전자증명서 발급, 유통센터, 전자문서 지갑, 전자증명서의 진본 여부 확인 및 사용자 인증 시스템 등을 구축하여 국민의 편의성과 행정서비스의 신뢰성을 높일 전망
- ☐ (라온시큐어 - 옴니원(OmniOne) 이용자 스스로 개인의 정보를 통제할 수 있도록 구축한 신원인증 플랫폼으로 증명 가능한 기관(Issuer)으로 발급된 정보(자격정보)를 스마트폰의 보관하며, 정보가 필요한 서비스 업체에게 이용자가 직접 자격정보를 제출하여 검증받고 이에 대한 보상을 받는 서비스 제공
- ☐ (SK텔레콤 - 스톤(STON)) ‘자기주권 신원지갑’에 모바일 운전면허증을 넣어놓고 차량공유와 렌터카 계약 등 필요한 순간에 실명인증 및 운전자격을 증명할 수 있도록 하는 개념

◎ 대기업 동향

- ☐ (삼성SDS) 현재 국내에서 가장 블록체인 관련 사업을 활발히 하는 기업으로 자체 블록체인 플랫폼 '넥스레저'를 자체 개발하고 2019년 8월 세계적인 시장조사업체 가트너(Gartner)로부터 글로벌 블록체인 주요 기업으로 선정
 - 관세청과 하이퍼레저 기반 물류서비스를 제공함. 또한, 서로 다른 블록체인 플랫폼을 연결하는 '딜리버' 플랫폼을 출시
 - 은행연합회 بانک사인(BankSign) 서비스가 '넥스레저'의 블록체인 생태계 확장의 대표적 사례로 분산합의와 위·변조가 불가능한 블록체인 특성을 적용해 더 안전하고 편리한 전자금융거래 서비스를 가능케 하는 블록체인 기반의 은행권 공동 인증 서비스
 - 넥스레저, 하이퍼레저 패브릭, 이더리움 등 이기종 블록체인 네트워크간 연결을 위해 네덜란드 3대 은행 중 하나인 ABN AMRO, 유럽 최대 물동량의 로테르담 항만청과 '딜리버(DELIVER)'를 공동 개발
 - 의료기관, 보험사, 디지털 헬스케어 전문기업 등과 컨소시엄을 구성해 환자가 복잡한 신청 과정 없이 보험금 청구에 필요한 진료 데이터를 제출할 수 있는 보험금 자동청구 서비스를 선보일 예정
- ☐ (삼성전자) 2019년 스마트폰 갤럭시 S10에 블록체인 키스토어(모바일 암호화폐 지갑)를 탑재했고, 카카오와 협업으로 '클레이튼폰(KlaytnPhone)'을 출시하며 블록체인 기술과 암호화폐를 대중에게 알리는 계기를 마련
- ☐ (LG CNS) 2018년 5월 기업용 블록체인 플랫폼 '모나체인(Monachain)'을 출시
 - LG CNS는 올초 한국조폐공사의 지역화폐 결제 플랫폼 착(chak)을 구축했고 이는 공공영역에서 블록체인이 적용된 최초사례로 평가되고 2019년 2월 경기도 시흥시를 시작으로 성남시, 군산시, 영주시, 제천시 등 지자체에서 이 플랫폼을 활용 중
 - 2019년 7월 LG CNS는 업계 최초로 LG유플러스가 모나체인을 기반으로 분실되거나 파손된 휴대폰의 보험금을 지급하는 시스템을 블록체인 기반으로 마련
- ☐ (카카오) 카카오의 계열사 그라운드X는 블록체인 플랫폼 '클레이튼(Klaytn)'을 자체 개발
 - 클레이튼과 관련된 메인넷 사이프러스는 퍼블릭 블록체인으로, 합의 노드, 레인저 노드, 고객의 세 개의 노드 계층을 가지며, PBFT 알고리즘을 기반으로 한 합의 알고리즘을 가짐
 - 2020년 6월 카카오톡에서 클레이튼 기반 암호화폐를 관리할 수 있는 지갑 서비스 '클립' 출시
 - 특히 LG전자, LG상사, SK네트웍스, GS홈쇼핑, 한화시스템 등 국내 주요 대기업 대표 계열사 절반이 카카오의 블록체인 플랫폼 '클레이튼'을 공동 운영하는 '거버넌스 카운슬(Governance Council)'에 참여

- (KT) 블록체인 기술 ‘스마트 컨트랙트’를 활용한 실시간 로밍 자동정산 시스템 ‘B.Link’를 중국 차이나모바일과 함께 베타 상용화
 - ‘B.Link’는 통신사간의 상호 로밍 데이터를 자동으로 검증하고, 오류가 없다면 실시간 정산까지 진행할 수 있도록 지원
 - KT는 기존 KT 네트워크에 블록체인 기술을 적용한 통합 인증 시스템을 구축. 이 시스템은 자체 블록체인 시스템과 관련된 지갑에 의해 IP가 암호화된 ID 형태로 인증을 수행하여 사용자 인증에 ID 및 패스워드가 더 이상 필요하지 않음

◎ 중소기업 동향

- (한컴위드) 블록체인 기반의 쿼서비스 플랫폼인 ‘말랑말랑 아니벌써’를 출시
 - ‘말랑말랑 아니벌써’는 블록체인 기반의 ‘스마트 컨트랙트’ 기능이 탑재돼 사용자와 쿼서비스 기사간의 모든 거래들이 실시간으로 자계약이 체결되는 시스템으로 체결된 계약정보를 분산저장해 해킹이나 정보의 위·변조를 방지함으로써 쿼서비스 이용 시 발생할 수 있는 배송 분쟁도 차단
- (AHAM) 인공지능망(RNN) 또는 강화학습(RL) 기반의 AI를 활용한 블록체인 네트워크 최적화 기술을 발표
 - 블록체인 합의 과정 중 가장 널리 쓰이는 비잔틴 내성(Byzantine Fault Tolerance, BFT) 기반의 알고리즘을 하드웨어로 가속하는 방법에 대한 특허 출원
- (와이즈엠글로벌) 분산ID 전용 블록체인을 제공하는 심버스(SymVerse) 프로젝트를 개발 중
 - SymID라는 분산ID는 인증서비스를 제공하는 CA서버와 연동해 생성하며, 이를 이용해 복수의 계정 신청이 가능, 계정은 부가정보를 블록체인에 저장함으로써 개인키 분실이나 유출에 대응이 가능
- (펜타시큐리티) 암호화폐 전용지갑 ‘Pallet’ 및 블록체인 KMS(Key Management System) ‘디아모(D'Amo)’를 개발
 - ‘Pallet’은 다양한 암호화폐를 한 곳에 보관 및 관리하는 암호화폐 전용지갑으로 모바일, 개인 사용자 디바이스 및 카드, 거래소 및 엔터프라이즈 제품으로 구성
 - ‘디아모’는 양자난수 생성기와 하드웨어 보안모듈(HSM)을 추가한 보안성 강화 패키지가 포함
- (수호) 블록체인의 핵심 기술인 스마트컨트랙트의 취약점을 분석하는 솔루션을 개발하는 업체로, 블록체인상에 존재하는 거래 내역인 ‘온체인 데이터’를 분석하는 방식의 KYT를 발표
 - 암호화폐 거래소 바이낸스가 개최한 글로벌 해커톤 행사에서 거래소, 암호화폐 지갑, 디앱(DApp)과 같은 서비스 관점에서 필요로 하는 이상 거래 탐지 서비스를 발표하여 최고 기술상을 수상
 - 발표한 자금세탁방지(AML)는 기존 암호화폐 거래소나 블록체인 회사는 블록체인 밖 정보인 신원 등 ‘오프체인 데이터’를 분석하는 방식에서 차이가 존재하며, 이를 통해 이상거래 탐지 및 실제 활용 가능성에서 높은 평가를 받음
 - 수호는 자체 기술로 6만 건 이상의 확인된 악성 주소를 수집하고, 이를 기반으로 해킹에 활용된 암호화폐 계정들은 바로 확인이 가능하여 이상 거래를 발견 즉시 동결 조치가 가능

- (열매컴퍼니) 블록체인 프로젝트인 아이콘(ICON)의 기술기업 아이콘루프와 협업을 통해 공동 소유권 증명서를 발급하여 미술품의 공동소유와 거래를 내용을 기록해 투명한 거래를 보장하는 '아트앤가이드'를 운영 및 국내 최초로 미술품의 토큰화를 개발 중
 - 아이콘루프의 블록체인 증명서 발급 서비스인 '브루프'는 아이콘 퍼블릭 블록체인 네트워크를 활용해 위변조되지 않는 증명서 발급과 영구 보관을 지원
- (왓차, 블로터앤미디어) 국내에서는 왓차가 블록체인 기반 '콘텐츠 프로토콜' 프로젝트를, IT 블로터앤미디어가 블록체인 기반의 탈중앙화 미디어 네트워크 'LEVEL'을 시작
 - 왓차가 선보인 '콘텐츠 프로토콜(Contents protocol, CPT)'은 콘텐츠 생산자뿐 아니라 콘텐츠를 공유하는 사용자의 자발적 활동, 리뷰나 평점 행위에 보상을 제공

◎ 공공 기관 동향

- 공공 부문에서는 블록체인이 금융업계뿐 아니라 정부 공공 서비스 및 기업 비즈니스 환경에 영향을 미칠 것으로 판단하여 정부 차원의 기반 플랫폼 개발 및 시범사업 실시, 성공사례 발굴 등에 집중
 - 미래창조과학부와 한국정보화진흥원(NIA)은 '17년 4월, 블록체인 활용기반조성 및 다양한 산업 분야에 적용될 수 있는 우수 사례 발굴을 위해 '17년 시범사업 과제를 선정 (아주경제, "미래부, 교보생명·SKT 등 14억 원 규모 블록체인 시범과제 선정", 2017.4.19.)
- 미래부에서는 인공지능(AI), 블록체인 등을 융합보안 시범사업 4대 과제로 선정하여 '17년 말까지 기술 및 서비스 개발, 시범적용 추진
 - 블록체인 분야의 경우, 블록코(Blockco)가 사물인터넷(IoT) 기기 인증에 블록체인 기술 활용 서비스를 개발하는 과제 선정
 - 이를 통해 스마트 팩토리와 스마트 그리드 등의 IoT 기기 인증 서비스 보안성 강화 및 블록체인 서비스의 활성화에 기여할 것으로 예상
- 한국인터넷진흥원(KISA)은 '18년까지 도입 단계로 블록체인 기술개발 및 산업 활성화를 위해 환경 조성에 중점, 향후 '19년부터는 블록체인 기반기술 공급을 통해 산업 성장의 토대를 마련할 계획
 - 도입 단계에서는 블록체인 협력체계 구축 및 적용 가능한 산업 생태계 연구에 초점을 맞추고 오픈 포럼 운영, 산업별 시장 분석, 법제도 개선 등 기업들의 블록체인 기반 비즈니스 환경 구축을 위한 다양한 지원을 계획
 - 성장·확산 단계에서는 블록체인 기반 비즈니스 지원센터 관리 및 시범사업 실증 테스트 환경 고도화, 산업별 전문인력 육성구축 등 기업의 비즈니스 관련 전문적인 지원 및 블록체인 가이드라인 수립/거버넌스 확산에 집중할 예정

4. 정책 분석

가. 해외 정책 동향

- ☐ 해외 각 국 정부는 산업별 활용, 국가 차원의 신뢰 확보 기반으로 블록체인을 공공분야에 선도적 도입 중
- (미국) 공공서비스에 블록체인 접목 실증과제를 통해 블록체인 상용화 적극 지원
 - (영국) 규제샌드박스 적용을 통해 공공서비스 제공에 필요한 사항 등을 통합적 관리
 - (독일) 암호통화와 거래소에 관한 규제 정립 및 국가 차원의 블록체인 개발전략 수립
 - (일본) 국가성장전략 차원에서 블록체인 기술을 금융 인프라 고도화에 적용
 - (중국) 정부주도 인프라 구축에 투자 및 지방정부 차원의 스마트시티 사업 접목

[국외 블록체인 정책 시사점]

	데이터 규제	데이터 집중화	암호통화 규제
미국	비식별화 정보 활용성 높음	거대플랫폼 기업 중심 데이터의 집중과 유통	(미국)디지털자산으로 인정 (중국) 암호통화 전면규제
중국			
유럽	비식별화 정보 활용성을 인정하나 규제 존재	데이터의 이동권 강화 (유럽) 데이터 이동권 (일본) 데이터 독점금지	암호통화에 대한 규제가 존재하긴 하나 활용은 인정
일본			

* 출처: 블록체인 산업 활성화를 위한 정책 지원방안 연구, 2019 KCERN

- ☐ 해외 각 국 정부는 산업별 활용, 국가 차원의 신뢰 확보 기반으로 블록체인을 공공분야에 선도적 도입 중
- (영국) 'Beyond Blockchain 전략'을 발표하여 정보 보안, 정부 문서의 위·변조 방지, 사회보장 부정수급 방지 등 다양한 분야에서 블록체인 활용을 촉진 중
 - (독일, 일본) 블록체인 기술뿐만 아니라 가상통화 거래에 대해서도 개방적인 정책을 마련
 - (미국, 중국) 가상통화에 대한 규제는 강화하면서 블록체인의 산업적 활용을 촉진하는 방향으로 정책을 수립
 - (에스토니아) 국가 차원의 블록체인망을 구축하여 주민관리, 건강기록, 금융기록, 전자 선거서비스 등을 제공 중

◎ 미국

- ☐ 스타트업, 대기업, 투자기관 등 민간기관을 중심으로 적극적으로 블록체인 생태계 구축
 - 다양한 글로벌 블록체인 컨소시엄 구성 및 기업간 협력·제휴를 통해 생태계 활발
- ☐ 주 정부마다 다른 입장을 취하고 있으나, 정부 차원에서 블록체인 서비스 활용을 위해 공공서비스에 블록체인 기술을 접목하는 실증과제를 적극적으로 추진 및 지원
- ☐ 우정청(USPS)은 포스트코인이라는 금융 플랫폼 만들어 금융서비스에 블록체인 기술 접목
 - 비용 효율성 개선 및 배송 시간 단축하며 분쟁 해결에 도움
- ☐ 총무청(General Services Administration)은 기존 인프라 위에 블록체인 기반 소프트웨어 적용 프로젝트 추진
 - 조달 프로세스 자동화 및 고정 비용 절감 목표
- ☐ 나스닥은 블록체인 기반 시스템 나스닥 링크(Nasdaq Linq)를 도입하여 비상장주식시장의 거래기록을 Linq 블록체인에 기록
- ☐ 보건정보기술국은 블록체인 활용하여 건강데이터를 저장 및 관리하는 사업 추진 중
 - 병원·정부 등은 전자기록 관리비용을 절감할 수 있을 것으로 기대
- ☐ 유타(Utah)주는 블록체인 기반 Voatz 투표 앱을 통해 표 조작 가능성 낮춤
- ☐ 정부서비스에 블록체인을 활용하기 위해 연방정부 및 주정부가 법률제정 등을 추진하는 등 블록체인에 대한 관심이 증가 중. 버몬트주(2016.6), 애리조나주(2017.3), 네바다주(2017.6)는 블록체인 상 기록 및 서명의 법적 효력을 인정하거나 블록체인 거래에 대해 면세하는 법안을 통과시켰으며, 델라웨어주(2017.7)는 주식 거래 명부에 블록체인의 사용을 허용 중. 또한, 나스닥 주식거래 시스템에 블록체인 기술 도입을 추진하고 있으며 연방준비은행(FRB) 주도의 블록체인 기반 지급결제 시스템 개발과 금융거래에 적용할 수 있는 플랫폼을 개발 중
- ☐ 미국 뉴욕주, 미국 최초로 디지털 화폐 TF 출범⁷⁾
 - Andrew Cuomo 뉴욕 주지사, 디지털 화폐 연구법안 'A8783B/S9013'에 서명
- ☐ 미국 FDA는 IBM 왓슨 헬스와 2년간의 개발협약을 체결하여 환자 데이터를 안전하게 공유하고자 블록체인을 사용
- ☐ 미국 국토안보부는 국경수비대 카메라 및 센서에서 수집한 데이터 보호 목적으로 블록체인 기능을 테스트하기 위해 신생 업체 Factom에 약 20만 달러의 보조금 지원

7) 뉴욕 주, 美 최초로 디지털 화폐 TF 출범(블록체인투데이, '19.01.24)

◎ 중국

- ☐ 국가 주도의 적극적인 지원을 블록체인 산업 응용 분야에서 급속한 성장세
 - 디지털화폐 발행 계획 중
- ☐ 암호통화에 대해서는 엄격히 규제하고 블록체인 산업 활용은 촉진하는 정부 주도로 블록체인 인프라 구축 및 투자 지원 시작
- ☐ 중국 7대 도시 모두 블록체인 진흥을 위한 지원 정책 발표
 - 22개의 대규모 블록체인 산업단지 조성
- ☐ 국가외환관리국은 국가 간 무역금융에서 발생하는 각종 비효율성 문제를 해결하기 위한 블록체인 시스템 개발, 전국으로 확대 및 도입 예정
- ☐ 중국은 4차 산업혁명시대의 핵심기술로 블록체인을 선정(2016. 12.)하여 기술개발 및 시범사업을 추진
 - 항저우에 블록체인 산업파크를 조성
 - 제13차 5개년 국가 정보화 계획에 블록체인을 포함시키는 등 블록체인 활성화 정책을 추진 중이며 정부-민간 형태의 블록체인 단지 건설(33조 원 투입 예정) 및 블록체인 기반의 중국 전자화폐 개발을 추진 중
- ☐ 중국은 블록체인과 블록체인 기반 디지털 위안화의 법적 근거를 위한 암호화법을 2020년부터 시행 개시
 - 암호화법은 암호화 기술이 블록체인 기술과 분리할 수 없다고 판단해 제정되었고 데이터를 암호화해 보호하고 조작할 수 없는 블록체인의 특성을 효율적으로 활용한다는 방침
 - 암호화법은 지난해 10월 26일 중국 제13차 전국인민대표대회 상무위원회에서 통과된 법률로 5장 44조로 구성되었으며 핵심암호와 보통암호는 엄격하게 규제하고 상용암호 산업을 육성한다는 계획

◎ 일본

☐ 블록체인 암호통화에 대한 개방정책 및 금융 분야 활용 촉진

- 특히, 경제산업성을 중심으로 블록체인 분석을 통해 국가 차원에서 도입 검토를 활발하게 추진

☐ 지역사회에서도 다양한 산업 연계 블록체인 모델 등장

- 구마모토현은 부속병원과 함께 블록체인을 접목한 웨어러블 기기 제작하여 데이터 축적비용 절감
- 오이타현은 공문서 관리에 블록체인 활용하여 문서 위·변조 유무 확인

◎ 영국

☐ 'Beyond Blockchain' 정책을 기반으로 블록체인 도입 가능성 검토 및 확대하며 8가지 권고사항 발표

- 정부는 블록체인 로드맵 구상 권고
- 연구 단체는 블록체인의 효용성을 평가
- 실증을 위해 지방정부가 추진할 수 있게 지원
- 블록체인에 대한 규제 사항을 명확히 고려
- 보안성과 통합성을 위해 산학협력을 이룸
- 효과적이고 실용적인 보안 프로토콜 사용을 위해 산학협력을 구성
- 정부는 블록체인이 연구수준이 아닌 실제 적용될 수 있게 지원
- 탑-다운 방식 뿐만 아니라 협력으로 정부가 블록체인 역량을 쌓음

◎ 독일

☐ 베를린을 중심으로 암호통화 강국으로 진화 중

- 정부 내 전문가 부재이기에 협회를 중심으로 정부, 기업들이 협업을 통해 정책 및 규제 조율
- 블록체인 기반 디지털 신원 시범사업 추진 및 도입 계획
- 2019년도 9월에 에너지, 금융, 물류·유통, 자동차 등 산업에 블록체인을 도입한다는 국가비전·전략 발표

◎ 유럽

☐ 스위스

- 스위스는 유럽 블록체인 산업의 중심. 중부의 소도시 주크는 크립토밸리(Crypto Valley)가 조성되어 블록체인 분야의 실리콘밸리로 각광받는 중. 주크 정부는 주민등록과 각종 결제에 비트코인을 허용하고 있으며, 민간단체인 크립토밸리협회(Crypto Valley Association)가 자율규제안을 마련

☐ 에스토니아

- 에스토니아는 세계에서 블록체인을 정부시스템에 가장 먼저 도입하였고 2014년 주민등록에 블록체인을 도입한 e-레지던시(e-Residency) 서비스를 세계 최초로 선보임. 이를 통해 전세계 누구나 에스토니아나 EU 회원국에서 법인을 설립할 수 있는 전자신분증을 발급받을 수 있음. 에스토니아는 1997년 전자정부를 구축한 이후, 세금, 교통, 주민등록, 투표 등을 전산화해옴. 2008년에는 세계 최초로 정부 기록에 블록체인을 도입하는 것을 검토하여 마침내 2012년 보건, 형사, 법제, 사업자 등록 등에 블록체인을 적용하는 데 성공
- 블록체인을 통해 정부 서비스를 단일 디지털 플랫폼에 연결하는 e-에스토니아 프로그램을 구현, 건강관리, 사법부, 입법부, 보안 등 데이터를 통합해 부패 및 오용으로부터 보호하고자 블록체인에 저장

☐ 네덜란드

- 건강관리공단은 블록체인 기반 개인 치료기록 관리 프로젝트 '메인 조그 로그(Mijn Zorg Log, 나의 치료기록)' 추진

☐ 덴마크

- 덴마크의 자유당은 2014년 블록체인 기술을 사용하여 투표한 세계 최초의 주요 정당임. 3자 연립정부 구성 및 자유당 내부 선거자료의 보안 목적으로 블록체인 기반의 전자투표시스템을 지속적으로 사용 중

☐ 조지아

- 조지아 정부는 Bitfury Group과 함께 개발한 토지 레지스트리 프로젝트 NAPR(National Agency of Public Registry) 블록체인을 도입하였고, 공공등기청의 디지털 기록 시스템에 통합 맞춤 설계된 블록체인 시스템을 구현

나. 국내 정책 동향

◎ 정부 정책 동향

□ 우리 정부는 다양한 분야에서 블록체인을 적용하고 활용하는 방안을 모색 중

- 국토교통부, 외교부, 관세청은 부동산 거래플랫폼, 공문서 시스템, 물류 시스템에 블록체인을 적용

[공공부문 블록체인 동향]

공공부문	주요동향
국토교통부	<ul style="list-style-type: none"> • 블록체인 기반 부동산 거래 플랫폼 - 부동산 담보 대출 요청 시 서류 처리를 위해 여러 기관을 방문해야 하는 번거로움을 덜기 위해 관계 기관이 함께 참여할 예정
외교부	<ul style="list-style-type: none"> • 블록체인 기반의 공문서 시스템 - 외교부 관련 공문서 저장 및 실시간 관리 가능
관세청	<ul style="list-style-type: none"> • 물류 시스템을 블록체인으로 관리 - 물류 과정을 블록체인에 기록 - 실시간 수입 신고로 통관시간 단축, 물류비용 절감 - (해양수산부) 블록체인 기반 유통문서 관리 및 공유하여 프로세스 개선 계획

□ 과학기술정보통신부는 2020년도 6월에 '블록체인 기술 확산 전략' 발표

- 7대 분야*전면 도입으로 블록체인 효과성에 대한 사회적 인식 제고

- *온라인 투표, 기부, 사회복지, 신재생에너지, 금융, 부동산 거래, 우정
- (온라인 투표) 투표 이해관계자가 투·개표 결과를 직접 접근하여 확인할 수 있는 블록체인 기반 온라인 투표시스템 구축(21~22)
- (기부) 기부 전 과정을 블록체인에 기록하고 모바일로 기부자가 확인
- (사회복지) 자산형성 지원사업을 대상으로 블록체인을 활용하여 중복수급 방지체계 마련
- (신재생에너지) 블록체인 기반 공급인증서(REC: Renewable Energy Certification) 종합관리시스템 구축하여 REC 거래서비스 확산
- (금융) 규제자유특구 연계하여 디지털 화폐 도입
- (부동산 거래) 블록체인 기반 실시간 연계·공유체계 구축하여 스마트 컨트랙트 기반 부동산 거래 서비스 활성화
- (우정) 분산신원확인 플랫폼 구축하여 우정사업 통합 고객 관리체계 구축

- 비대면 경제의 인프라로서 분산신원증명 서비스 활성화
 - 공공부문 DID* 서비스의 통합적 운영을 공공플랫폼 구축·지원체계 마련
 - *Decentralized Identifier: 사용자가 증명 목적에 필요한 정보만을 선택하여 개인정보 보호를 강화할 수 있는 디지털 신원확인 체계
 - 개인이 데이터를 관리 통제할 수 있는 국민체감형 사업 추진
 - 정부·민간이 참여하여 공통요구사항 등의 마련을 위한 DID 거버넌스 체계 구축
 - 해외에서도 통할 수 있는 기업 육성을 위한 지원체계 마련
 - 아이디어 쉽게 구현 위한 BaaS* 활용 지원 및 검증받을 수 있도록 ‘기술혁신지원센터’ 구축
 - *Blockchain as a Service: 블록체인 응용서비스 개발과 관리, 나아가 SW 사용을 클라우드 기반으로 편리하게 지원하는 서비스
 - 수요발굴 -> 컨설팅 -> 기술검증으로 이어지는 체계적 지원
 - 해외진출 지원 체계 운영 및 네트워크 구축을 통한 신남방 국가 진출의 가시적 성과도출
 - 기술 로드맵에 따른 핵심·융합 기술개발 및 글로벌 표준대응 강화
 - 블록체인 기술 생태계를 강화하는 차세대 원천기술·산업화 융합기술 확보
 - 블록체인 기술분류 체계 개선 및 중장기 기술로드맵 재정립
 - 차세대 핵심 원천기술 위한 산업화 융합기술 확보의 개발 전략 추진
 - 체감할 수 있는 법제도 개선, 시장수요에 맞는 인력양성 추진 등
 - 규제 샌드박스과 연계하여 블록체인 신산업 활성화
 - 기술이해 및 사업 추진의 편의를 도모하기 위한 가이드북 제작 및 배포
- 대통령 직속 국가균형발전위원회는 2019년 9월부터 2020년 1월까지 ‘국가균형발전을 위한 디지털 뉴딜 전략수립’ 연구를 진행
- 국가균형발전위원회는 지역의 중소기업 성장을 촉진시키고 국가균형 발전을 이루기 위해서는 지역혁신이 필수적이라고 보고 지역혁신을 촉진하기 위해 디지털 뉴딜 전략 수립 계획
 - 디지털 뉴딜에 블록체인 인재 육성도 포함될 예정이며 제안요청서는 ‘인공지능(AI), 블록체인, 빅데이터 등 지능정보화 10대 핵심 기술 영역별 산업맞춤형 혁신인재 육성 전략을 도출한다’는 내용이 포함된 것으로 알려짐
- 과기정통부는 2020년에 블록체인 핵심기술개발 및 전문기업 육성을 통해 블록체인 산업의 기초체력을 강화하는 한편 공공, 민간 부문 확산을 통한 초기시장 형성을 지원
- 2019년 117억 원이었던 블록체인 융합기술개발 예산을 2020년 161억 원으로 증액
 - 과기정통부는 2020년 1월 17일 ‘2020년 블록체인 사업 통합설명회’를 개최할 예정







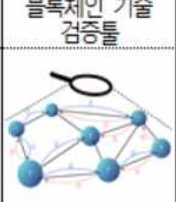


[블록체인 분야 과제 제안 기관 및 과제]

분야	제안기관	과제명
관광	전라북도	• 블록체인 기반 전라북도 인공지능 맞춤형 관광 설계시스템
계약	방위사업청	• 블록체인 기반 제안서 접수 및 평가 시스템 구축
식품안전	식품의약품안전처	• 국민향(向) 해썹(HACCP) 서비스 플랫폼 구축 시범사업
의료	서울의료원	• 블록체인 기반 맞춤형 의료 서비스 시스템 구축
인증	병무청	• 인증서 없는 민원서비스 제공을 위한 블록체인 플랫폼 구축 사업
재난	부산광역시	• 블록체인 기반 재난재해 대응 서비스 구축 시범사업
전자문서	우정사업본부	• 블록체인 기반 전자우편사서함 시범사업
	국가기록원	• 블록체인을 적용한 신뢰기반 기록관리 플랫폼 구축 시범사업
	서울특별시	• 시간제 노동자 권익보호(근로계약서)
친환경	환경부	• 블록체인 기반 탄소배출권(외부감축사업) 이력관리 시스템 구축
	제주도	• 블록체인 기반 폐배터리 유통이력 관리시스템 구축 시범사업
	한국남부발전	• 블록체인 기반 신재생에너지 공급의무화제도(RPS) 통합관리 서비스 시범사업

□ 2018년 11월 발표한 ‘ICT R&D 기술로드맵 2023’에 블록체인 기술이 포함

- 블록체인의 기술범위는 분산장부 자체 작동에 필요한 기반기술, 블록체인 내외 데이터와 연동해 활용하는 확장기술, 블록체인을 여러 가지 산업에 활용하는 서비스 기술 3가지로 구성

[ICT R&D 기술로드맵 2023]

구분	2018	2019	2020	2021	2022	2023
블록체인	서비스		대용량 데이터 처리 서비스 	전자문서 사용이력 관리서비스 	농축수산물 이력관리 서비스 	전자투표 관리서비스 
	제품	블록체인 기반의 IoT 플랫폼 	대용량 데이터 유통 블록체인 플랫폼 	블록체인 기술 검증틀 	블록체인 서비스별 특화 컨포넌트 	공공 블록체인 플랫폼 

□ 정부는 2019년 다음과 같은 R&D 과제를 발주

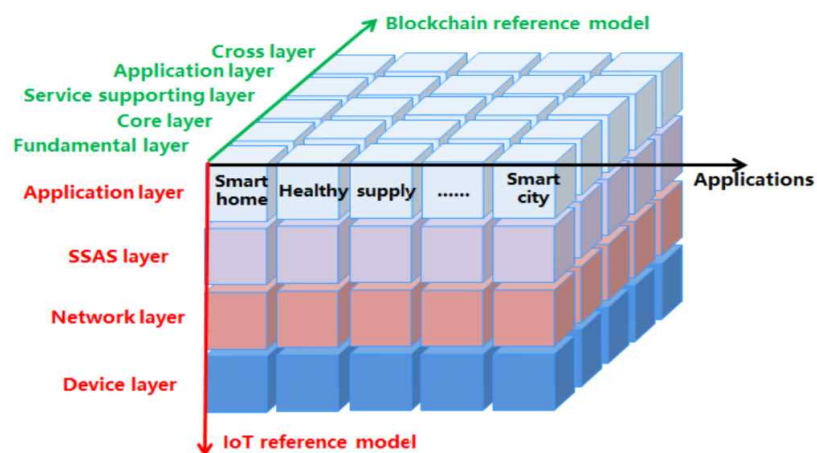
[분야별 블록체인 R&D 과제]

(단위 : 백만원)

기술분야	과제명	수행기간/예산
블록체인	• 블록체인을 활용한 분산형 자기주권 신원정보관리 기술 개발	2년/2400
	• 블록체인 외부 정보 접근을 위한 스마트 컨트랙트 오라클 기술 개발	2년/1200
	• 블록체인 간 트랜잭션 및 블록 전파 지연 문제 해결	2년/1600
	• 블록체인 트랜잭션에 따른 최적 합의 알고리즘 문제 해결	2년/1600
	• 블록체인의 개인 콘텐츠 추적과 완전소멸수정을 위한 잊힐 권리 문제 해결	2년/1600
	• 스마트 컨트랙트 정형명세	2년/1200
	• 블록체인 핵심 기술	2년/1200
	• 부정거래/수급 특화 블록체인 응용 플랫폼	2년/1000
	• 학술논문 특화 블록체인 응용 플랫폼	2년/1000
	• 전자문서 특화 블록체인 응용 플랫폼	2년/1000
	• 콘텐츠 특화 블록체인 응용 플랫폼	2년/1000
	• 공유경제 특화 블록체인 응용 플랫폼	2년/1000
	• 물류 특화 블록체인 응용 플랫폼	2년/1000

□ 정부의 블록체인 핵심 기술 중심으로의 융복합 방향은 다음과 같음

[블록체인 융복합 방향]



◎ 정부 규제 현황

- ☐ 국내에는 암호화폐를 통한 자금 모집이나 암호화폐 거래소의 운영에 관한 법률 규정이 제정되어있지 않으므로, 사업자의 행위가 기존 법령에 위배 시 그에 따른 규제
- ☐ 블록체인 산업 진흥 기본법(안)
 - 블록체인에 저장된 기록물을 '전자문서'로 인정
 - 개인정보를 지울 수 없는 블록체인 특성상 개인정보보호법에 따라 개인정보는 비식별화하는 기술적 조치를 요구
 - 블록체인을 활용한 스마트 계약은 소스코드를 활용해 조건이 갖추어지면 자동으로 거래가 성사될 수 있도록 문서 공개, 제공 등의 조건을 포함
- ☐ 특정금융거래정보 보고 및 이용 등에 관한 법

[특정금융거래정보 보고 및 이용 등에 관한 법 개정안]

개정안 주요 내용	해석
금융 거래를 금융 거래 등으로 수정	암호통화 거래까지 범위가 확장되었으나 금융 거래로 인정한 것은 아님
가상자산 취급 업소를 정의	가상자산 매도, 매수, 교환, 보관 관리, 이전, 중개, 알선 업무까지 포괄
가상자산 취급업소, 금융정보분석원에 신고	현재 은행을 통한 정부의 간접규제에서 직접규제로 전환되는 것으로 해석
실명확인 입출금 계정 서비스 요건	현재 은행의 실명가상계좌를 사용하고 있는 국내 대형 거래소만이 지속될 것으로 보임

* 출처: 블록체인 산업 활성화를 위한 정책 지원방안 연구, KCERN(2019)

☐ KYC, AML 규제

- 대표적인 국내 암호화폐 규제 조치로서 '가상통화 관련 자금 세탁방지 가이드라인'이 존재. 위 가이드라인은 가상통화 취급업소(암호화폐 거래소)와 거래하는 금융회사(은행 등)의 역할과 책임을 명시. 또한 금융회사가 FIU에 금융거래 보고할 때, 대상이 된 금융거래 자료, 합당한 근거자료 등을 함께 보고해야 한다고 명시해, 암호화폐 거래소에 대한 간접적인 규제 역할
- 업비트, 빗썸, 코빗, 코인원 등은 가이드라인 시행 전 발급받은 '실명확인 가상계좌'를 유지. 하지만 은행은 가이드라인을 근거로 추가로 신규 실명확인 가상계좌를 발급해주지 않는 중. 또한 가이드라인은 '은행은 가상화폐 취급업소가 고객확인을 위한 정보제공을 거부하거나 제공한 정보를 신뢰할 수 없는 경우 바로 거래를 거절하거나 종료해야 한다'고 명시
- 금융위원회는 2018년 7월 10일 가이드라인을 개정. 1년간 시행되는 이 가이드라인은 '특정금융거래정보의 보고 및 이용 등에 관한 법률(특금법)'의 개정안으로 대체될 예정이었으나, 특금법 개정이 늦어지면서 금융위는 최근 가이드라인의 기간을 연장

□ ICO, STO 규제

- 가상통화 관계기관 합동TF는 2017년 9월 29일 “지분증권·채무증권 등 증권발행 형식으로 가상통화를 이용하여 자금조달(ICO)하는 행위는 자본시장법 위반으로 처벌한다”고 밝힘. ICO를 금지한다는 것은 가이드라인 형태의 행정지도에 불과했지만, 정부의 방침을 거스르고 국내에서 ICO를 할 기업은 없음
- 금융감독원은 2018년 9월 22개 기업을 대상으로 ICO 실태 조사를 시작했고, 국무조정실이 주도하는 ‘범정부 가상통화TF’는 2019년 1월 31일 결과를 발표. 정부는 투자 위험성이 매우 높은 상태라며 ICO 투자에 신중을 기해주실 것을 당부한다고 밝힘. 하지만 아직 국내에서 ICO에 대해서 명시적으로 규제하는 법률은 제정되지 않음
- 따라서 ICO, IEO는 현재상태에서 사실상 가능. 다만 현재 존재하는 법률에 위배되지 않게 진행되어야 함. 판매 과정에서 방문판매법이나 유사수신행위에 관한 법률에 위배되지 않아야 하며, 특히 사업 내용에 허위 사실을 포함해서는 안됨
- 허위사실이 있다면 형법상 사기죄가 문제 될 수 있고, 모금된 자금을 함부로 유용한다면 형법상 횡령죄가 문제 될 수 있음. 또한 발행되는 암호화폐가 선불전자지급수단과 유사한 성격을 갖는다면, 전자금융거래법상 등록이나 인가 의무가 있는지도 확인 필요
- 증권형 토큰 발행(STO)은 자본시장법의 엄격한 규제에 따라야 하므로 여러 한계가 존재

□ 외국환 규제

- 국외에서 ICO를 했다면 외국환거래법상 규제가 문제 될 수 있음. 국내 프로젝트들이 일반적으로 시스템 개발을 하기 때문에 외국의 발행 법인이 국내에 자금을 송금하면서 외국환거래법상 신고의무를 부담하게 되는 경우도 있음. 하지만 현실적으로 암호화폐로 자금을 전달할 경우에는 외국환거래법상 신고를 하더라도 수리가 될 것인지에 대해서 의문인 상황

□ 세금 규제

- 부가가치세, 소득세, 법인세, 상속세 및 증여세 납부 의무를 생각해볼 수 있음. 우선 암호화폐가 부가가치세 과세 대상인지 여부에 대해 아직 명확한 결론은 나지 않았음. 국세청은 암호화폐가 화폐로서 통용되는 경우 부가가치세 과세 대상에 포함되지 않지만, 재산적 가치가 있는 재화로서 거래되는 경우 부가가치세 과세 대상이 될 수 있다는 해석을 내놓은 바 있음. 따라서 그 법적 성격이 규명되기 전까지는 부가가치세 납부대상에 해당한다고 보기는 어려움
- 소득세는 소득세법에서 열거하고 있는 과세대상 항목에 해당해야 과세가 가능하고, 사업소득의 경우 암호화폐와 관련된 항목이 명시되어 있지 않지만 사업에 준하는 활동을 통해 얻은 소득이라면 소득 신고를 하는 것이 바람직. 그리고 급여를 현금이 아닌 암호화폐로 받은 경우 근로소득에 산입돼 과세 대상이 될 수도 있음
- 다만 양도소득세는 법률에 규정되어 있는 경우에만 부과될 수 있는데 현재까지 암호화폐 양도에 따른 소득에 대해서는 과세 규정이 없으므로 양도소득세는 문제 되지 않음. 법인세의 경우 포괄적 과세주의를 채택하고 있어 암호화폐로 인해 법인의 순자산이 증가한 경우 법인세 과세가 가능

□ 거래소 규제

- 금융거래정보의 보고 및 이용 등에 관한 법률(특금법) 개정안이 2020년 3월 5일 국회 본회의에서 통과됨에 따라, 암호화폐 관련 산업이 제도권으로 편입될 수 있는 기반이 마련
- 개정안은 암호화폐를 '가상자산'으로 암호화폐 거래소를 '가상자산 사업자(VASP)'로 정의하고 가상자산 거래소의. 조건부 신고제를 주요 내용으로 포함
 - 개정안은 가상자산 사업자에 대해 자금세탁행위 방지를 위한 의무를 부과하고 금융회사가 가상자산 사업자와 금융거래를 수행할 때 준수해야 하는 사항을 규정
 - 특금법 개정안은 공포 후 1년이 경과된 시점에서 시행될 예정이며, 기존 사업자의 경우 개정안 시행일로부터 6개월 내 의무적으로 신고
- 국제자금세탁방지기구(FATF)가 2019년 6월 암호화폐에 대한 권고안을 발표하면서 국내에서도 이를 반영해 시행령에 반영한 하위 법규를 마련할 것으로 예상. 권고안에 따르면 암호화폐 거래소도 고객신원확인(KYC), 자금세탁방지(AML)의 주체이므로 향후 암호화폐 거래소에서도 KYC와 AML을 의무적으로 수행해야 할 것으로 전망⁸⁾

□ 금융규제 샌드박스와 관련하여(규제 샌드박스란, 신산업, 신기술 분야에서 새로운 제품과 서비스를 내놓을 때 일정 기간 기존 규제를 면제하거나 유예시켜주는 제도를 말함), 블록체인 관련 서비스 신청이 가장 많은 것으로 파악

- 금융위의 입장에 따르면, 기존 혁신 금융서비스와 같거나 비슷한 서비스 중 규제 개선 계획이 있는 경우엔 우선 심사되어 처리되고, 법 개정이 추진 중인 사항에 관한 서비스 역시 신속하게 심사될 예정이며, 향후 아이디어의 독창성 등 서비스의 혁신성, 금융소비자의 편익 증대 등에 중점을 두고 심사가 진행될 것으로 판단⁹⁾

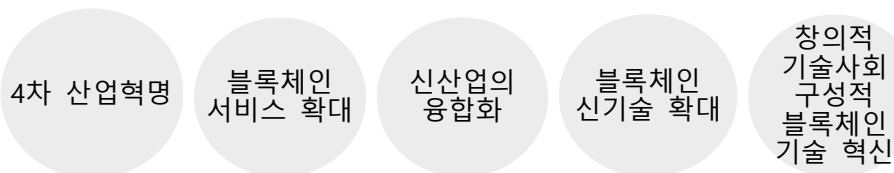
8) “한국(엔 없는...) ‘암호화폐 규제’의 모든 것”, 코인데스크 코리아, 2019.7.4.

9) ‘금융규제 샌드박스, 142개社, 219개 서비스 신청.. 블록체인 가장 많아’, 토큰 포스트, 2019.8.6.

5. 중소기업 전략제품

가. R&D 추진전략

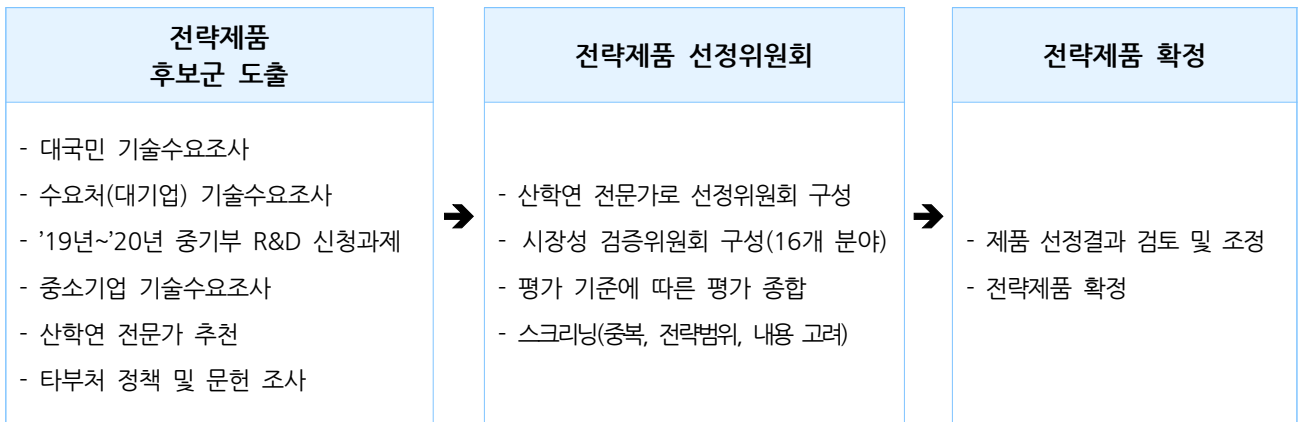
Factor	기회요인	위협요인
정책	<ul style="list-style-type: none"> 4차 산업혁명에서 핵심 기술로 블록체인 서비스를 확산할 수 있는 주도적 역할 아날로그 산업의 정체기에 새로운 성장 동력으로서의 블록체인 신산업 형성 	<ul style="list-style-type: none"> 단기적 미시적 R&D 지원 및 개발 정책으로 장기적인 기회 요인이 소멸 선진국 및 선진 글로벌 기업의 조기 산업화 정책으로 후발 주자들의 극복 정책이 부족
산업	<ul style="list-style-type: none"> 세계최고 수준의 블록체인 생태계와 산업 환경 구축 인공지능 사회의 도래에 따른 융/복합형 블록체인 신규산업 도래 	<ul style="list-style-type: none"> 글로벌 기업들의 공격적인 투자 및 환경 구축으로 산업기술 선점 및 신시장 조기 진입 글로벌 기업들의 제도/환경을 구비한 국가로 이전하여 서로 상생하며 신산업 전략 확보
시장	<ul style="list-style-type: none"> 4차 산업 관련 시장 변화와 블록체인 기반의 새로운 서비스 시장이 확대 진행 사물인터넷과 인공지능 시장의 확대에 따른 블록체인 시장 확산 	<ul style="list-style-type: none"> 글로벌 기업들의 공격적인 투자 및 새로운 시장의 선점 글로벌 기업의 신시장 선점 및 블록체인 시스템 시장의 선점
기술	<ul style="list-style-type: none"> 블록체인 기술을 이용한 서비스 확산 및 새로운 응용 서비스와 기술 발전이 기회 블록체인 기술로 운용되는 데이터 소사이어티의 투명성과 민주성 등 다양한 신기술 분야로 확대 	<ul style="list-style-type: none"> 글로벌 업체와의 기술격차 및 기술경쟁력이 선진국 대비 취약함 국내 블록체인 전문가와 정책입안가 부족



중소기업의 시장대응전략

- 4차 산업 혁명의 블록체인 전파할 수 있는 공유형 서비스 중심의 블록체인 기술과 소액 기부 및 후원에 대한 블록체인 플랫폼 시장 선점
- 블록체인의 다양한 기술 분야에 대해 기술 경쟁력 확보 및 새로운 밸류체인 확보
- 국내 기업 간 기술 M&A를 통한 상호 보조로 글로벌 기업의 기술 대응

나. 전략제품 선정 절차



□ 전략제품 후보군 도출

- (최근 신청 과제) 중소벤처기업부 R&D 지원 사업 '19년~'20년 상반기 신청과제
- (기술수요조사) 중소기업기술정보진흥원 주관 SMTECH(중소기업 기술개발사업 종합관리시스템) 성과분석 대상 중소기업으로부터 기술수요 수신
- (대기업 의견) 전략분야 관련 대기업의 중소기업 유망 제품 관련 인터뷰
- (산학연 전문가 추천) 분야별 전문가 대상 후보 추천 의뢰 의견수렴
- (타부처 정책 및 문헌조사) 타 부처 정책사항 및 문헌조사를 통한 품목 발굴

※ (재밍, Jamming) 데이터 기반의 전략제품 발굴을 위하여 인공지능 전략분야에 시범적으로 도입

□ 전략제품 선정위원회

- (선정방식) 중소기업 적합형 기술로드맵 수립 및 전략 강화를 위해 전략제품 선정위원회의 평가와 시장성 검증위원회의 평가를 종합하고, 전략분야에 따라 평가항목의 가중치를 조절하여 반영
- (전략제품 선정평가위원회) 분야별 산·학·연 전문가 위원회를 구성하여 전략제품에 대해서 각 5개 항목을 평가 및 검토 진행
- (시장성 검증위원회) 시장성 검증이 필요한 분야에 대해서 해당 전략분야에 관련성이 높은 전문가와 VC(투자심사역)으로 구성된 위원회가 전략제품 평가 진행
- (평가항목) 시장성, 기술난이도, 개발기간, 수입의존성 및 중소기업 적합성을 기준으로 평가
- (평가기준) 전략분야의 대구분(한국판 뉴딜 및 소부장·뿌리산업)에 따라 평가항목의 가중치를 조절

□ 전략제품 확정

- (검토 및 조정) 선정된 전략제품들에 대해 최종적인 타당성 검증 및 분야 간 전략제품 검토 및 조정을 통해 전략분야별 전략제품 확정

다. 전략제품 선정결과

◎ 블록체인 기반 디지털 콘텐츠 관리 플랫폼

- 음원, 영상, 게임 등 디지털 콘텐츠를 블록체인 네트워크에 저장함으로써 디지털 콘텐츠 및 그에 관한 권리들의 발생 시점을 투명하고 명확하게 관리하여 고수수료를 청구하는 별도의 중개기관 없이 디지털 콘텐츠에 대한 효율적인 관리를 달성하기 위한 플랫폼

- 복잡한 중간유통으로 인해 콘텐츠 크리에이터들의 권익이 제대로 보호받지 못하고 있으며, 전통적인 문화산업계에서 이러한 관행을 개선할 의지 부족
- 블록체인 기술은 콘텐츠 생태계 유통 구조를 개선하고 저작권 보호를 강화할 수 있는 새로운 기술

◎ 블록체인 기반 분산 ID 및 인증 시스템

- 기존 중앙에서 관리되던 개인정보를 각 개인이 주체가 되어 관리할 수 있도록 하고, 블록체인에 개인정보가 담겨 분산형 방식의 관리 방법으로, 해킹의 위험으로부터 자기 정보를 보호할 수 있는 기술

- 전세계적으로 개인의 프라이버시를 보호하고자 하는 움직임과 더불어 각 서비스 제공기관마다 사용자 인증정보 및 개인정보를 관리함에 따른 위험성 및 불편함 인지
- 실생활에서 사용자가 신원증명을 관리하듯, 온라인상에서도 새로운 인증체계 필요

◎ 블록체인 기반 불법거래탐지

- 블록체인 상에서 거래 데이터를 수집하여 해당 거래가 정상적인지 아닌지 판단하고, 탐지된 데이터와 연계된 블록을 블록체인에 등록하는 기술

- 산업 전반에 블록체인 인프라 사용 증가하며 불법거래 탐지 기술에 대한 필요성 대두
- 기존에 존재하는 데이터를 분석하는 것은 사용자의 몫이었던 블록체인 데이터 분석 서비스의 한계

◎ 블록체인 기반 소유자 이력 관리 시스템

- 디지털 자산의 투명성, 신뢰성 및 제고를 위한 공적 가시성 확보를 위해 디지털 자산이 블록체인 네트워크에서 이동할 때 소유권의 전부 혹은 일부가 변경된 이력을 탐지, 추적 및 관리할 수 있는 시스템

- 중개자가 필요 없이 참여자 모두가 동등한 권한을 갖고 여러 가지 다양한 인센티브에 따라 자발적으로 네트워크 참여함으로써 민주적인 의사결정에 의한 운영 가능
- 블록체인 관련 범죄나 오남용 등 부정적 측면에 대한 예방 및 조치를 위한 연구 개발 필요

◎ 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템

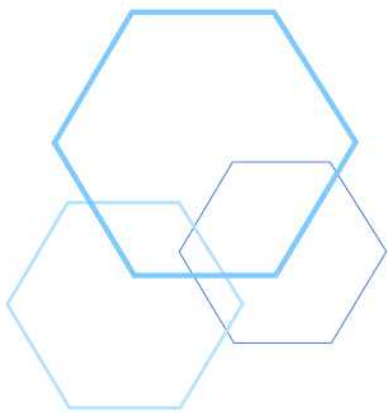
- 블록체인 운영 설정 및 블록체인 참여자의 블록체인 활동 시작 시 블록체인 암호키 수명 주기 관리 정책에 따른 키 관리 프로세스를 통해 블록체인 암호키 관리(생성, 발급, 저장, 백업, 폐기 등)를 실시할 수 있게 해주는 시스템

- 암호자산 기반 서비스를 위한 블록체인 시스템에서 ‘암호키 관리’는 핵심적인 필수 보안요소
- 특히, 은행과 같이 개인 데이터 교환을 관할하는 중앙 기관이 없다는 점 때문에 블록체인 네트워크를 통해 전 세계적 개인 식별정보 교환 실현을 위해 암호키관리가 매우 중요

◎ 블록체인 기반 공유 경제 서비스

- 중앙화된 플랫폼에서 탈중앙화된 플랫폼으로의 이동과 동시에 공유거래 메커니즘에서 발생하는 가치들이 온전히 공유경제 거래 참여자들에게 돌아가며 참여자 네트워크를 확보

- 공유경제는 참여자 간에 형성되는 시장인 반면, 현재 공유경제 서비스 시장에서는 ‘플랫폼 사업자’가 대부분의 이윤을 가져가는 구조로 인해 진정한 공유경제의 실현 어려움 존재
- 수익형 공유기업들이 제공하는 중앙집권화된 플랫폼의 공유거래 메커니즘 실현을 위한 필요성 확대



전략제품 현황분석

블록체인 기반 분산 ID 및 인증 시스템



블록체인 기반 분산 ID 및 인증 시스템

정의 및 범위

- 기존 중앙에서 관리되던 개인정보를 각 개인이 주체가 되어 관리할 수 있도록 하고, 블록체인에 개인정보가 담겨 분산형 방식의 관리방법으로, 해킹의 위험으로부터 자기 정보를 보호할 수 있는 기술
- 분산 ID 및 인증 시스템을 구축하기 위한 기술은 DID Document 표준화 및 API 연동기술, 블록체인 기반 신원인증 서비스, 블록체인 암호키 관리 기술, 대용량 신원정보 저장, 검증 기술 등으로 분류

전략 제품 관련 동향

시장 현황 및 전망	제품 산업 특징
<ul style="list-style-type: none"> • (세계) 블록체인 ID 세계시장 규모는 '18년 1.7억 달러에서 연평균 약 79.2%씩 성장하여 '24년에는 56억 3,000만 달러의 규모로 성장할 것으로 전망 • (국내) 2018년 국내 블록체인 ID 시장규모는 2018년 56억 원에서 연평균 약 79.2%로 성장하여 2024년 시장규모는 약 1,839억 원으로 추산됨 	<ul style="list-style-type: none"> • 기존 ID 체계로 식별, 인증 시 정보가 네트워크를 통해 전송되는 과정에서 발생하는 보안 문제 해결을 위한 블록체인 기반 분산 ID 및 인증 시스템 필요성 증가 • 정보통신산업진흥원은 가맹점의 프로모션 이용 고객 응대와 결제관리가 가능한 블록체인 DID 기반 통합인증결제 플랫폼 개발 지원
정책 동향	기술 동향
<ul style="list-style-type: none"> • '한국판 뉴딜' 정책 발표와 '지능형 정부' 구축하여 개인 맞춤형 공공서비스 신속 처리, 5G 업무망 및 클라우드 기반 업무환경 구현 예정 • 분산 ID 기반의 금융서비스에 대한 기술적 명확성을 제공하고 상호 운용성과 보안성 확보위해 '분산 ID 금융보안표준' 제정 • 공인전자서명의 우월한 법적 효력을 폐지하는 내용의 전자서명법 전부개정안 국회 통과 • 금융결제원, 분산 ID로 금융거래가 가능하도록 하는 모바일 신분증 시스템 상용화 	<ul style="list-style-type: none"> • 분산 ID(DID) 기술은 사용자가 신원 관리 서비스를 선택하여, 발행받은 신원정보로 여러 서비스를 이용할 수 있도록 하는 기술로 신원정보는 분산원장 기반으로 공유되고, 신원정보는 사용자가 관리 • 분산 ID는 지갑보유자가 신뢰기관에게 자신을 증명해 블록체인에 기록해달라고 요청해야 하며 분산 ID가 분산원장에 저장되면 지갑보유자는 자신의 지갑에 개인정보를 저장하고 이를 외부에 제공 가능
핵심 플레이어	핵심기술
<ul style="list-style-type: none"> • (해외) IBM, Evernym, CISCO, Microsoft, Amazon • (대기업) 교보생명, KB국민카드, LG CNS, SK 텔레콤 • (중소기업) DID 얼라이언스, 라온시큐어, 블로코 	<ul style="list-style-type: none"> • DID Document 표준화 및 API 연동 기술 • 대용량 신원정보 저장 및 검증 기술 • 블록체인 기반 신원 인증 서비스 기술 • 블록체인 암호키 관리 기술 • 선택적 신원 정보 기술

중소기업 기술개발 전략

- DID 특허 활성화를 위한 중소기업 산업 표준 아이템 도출 전략 제시 필요
- 자주적 신원관리 표준을 위한 '증명 가능 주장'에 대한 기술개발 진행 독려
- DID는 블록체인 표준화 중에서도 선결과제로 주목되고 있는 관계로 중소기업이 대기업, 정부, DID 협회 관련 프로젝트에 참여할 수 있도록 지원하는 전략 필요

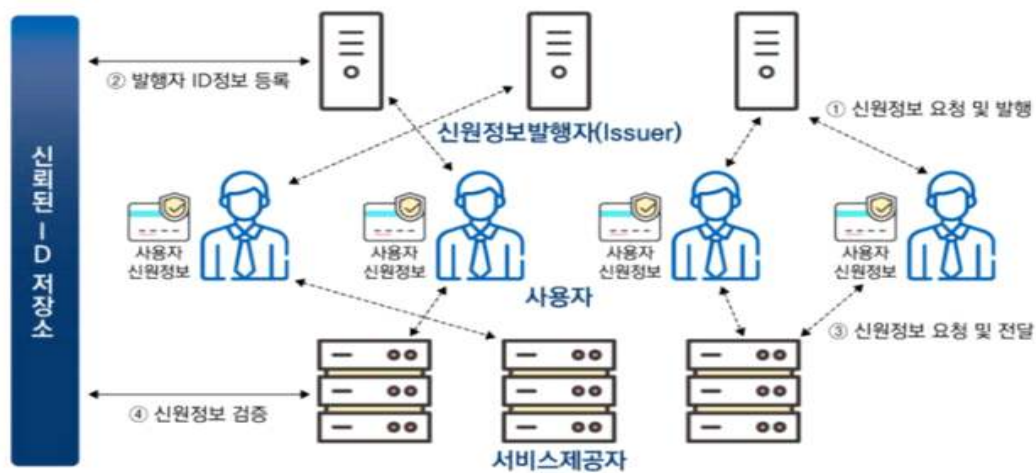
1. 개요

가. 정의 및 필요성

(1) 정의

- 분산 아이디 또는 분산 신원 확인(DID, Decentralized Identity)은 기존 신원확인 방식과 달리 중앙 시스템에 의해 통제되지 않으며 개개인이 자신의 정보에 완전한 통제권을 가질 수 있게 하는 기술
- 온라인상에서 사용자가 스스로 신원 등에 대한 증명 관리, 신원정보 제출 범위 및 제출 대상 통제 등을 수행하는 체계
 - 유럽 연합 개인정보 보호법(GDPR) 및 미국 소비자 프라이버시 권리장전 등 개인 데이터의 자기 주권을 강화하는 현 상황에서, 사용자가 자신의 신원정보에 자기 주권¹⁰⁾ 행사가 가능한 분산 ID 체계가 각광받고 있음
 - 전통적인 서버-클라이언트 모델 신원 관리체계와는 달리, 사용자가 자신의 신원정보에 주권 행사 가능
 - 특히, 분산원장의 암호학적 특성(일단 분산원장에 올라간 데이터는 위조 및 변조가 불가능)을 기반으로 한 신뢰성이 있는 ID 저장소를 이용하여, 제3 기관의 통제 없이 분산원장에 참여 가능한 누구나 신원정보의 위조 및 변조 여부를 검증 가능

[블록체인에서의 분산 ID(Decentralized ID의 개념도]



<분산ID 개념도 자료:금융보안원>

* 출처 :금융보안원

10) 주권(Self-Sovereignty) : 사용자가 스스로 신원정보의 사용방법 및 목적을 결정할 수 있는 권리

(2) 필요성

☐ 인터넷 ID 시스템의 문제점

- 인터넷 ID 시스템은 전문 공격자의 공격에 취약한 면이 있으므로 보안 문제가 심화되면 인터넷 기반의 경제 거래시스템은 신뢰를 잃어갈 수 있는 문제가 존재
- 인터넷 공격자는 개별 소비자 자신이 상대방을 알 수 있는 능력이 없다는 점을 이용하여 ‘피싱(Phishing)’을 통해 은행 및 기타 정보를 탈취하거나 컴퓨터에 있는 ‘스파이웨어’를 실수로 설치하게 하여 장기간 ‘파밍(Pharming)’ 공격하여 정보를 수집하도록 유도
- 방대한 ID를 보유한 기업, 정부 등의 데이터베이스에서 수십만 개의 신원을 한 번에 해킹 가능
- 피싱 및 파밍은 현재 컴퓨터 업계에서 가장 빠르게 성장하는 인터넷의 신뢰를 저하시키는 기술 중 하나로 연간 복합 성장률이 1,000%

☐ 전 세계적으로 개인의 프라이버시를 보호하고자 하는 움직임과 더불어 각 서비스 제공기관마다 사용자 인증정보 및 개인정보를 관리함에 따른 위험성 및 불편함을 인지

- 유럽 연합, 미국 등은 개인의 데이터 주권을 강화하기 위한 정책을 수립 및 시행 중
- 특히, 사용자의 신원정보가 글로벌 서비스제공자에게 집중됨으로써 발생하는 프라이버시 침해 가능성에 우려

☐ 기존 ID 관리 시스템에서는 단일 서버 중앙화 및 믿을 수 있는 제3의 신뢰기관에 대한 신뢰 구조 문제가 존재

- 서비스 제공기관마다 사용자의 신원정보 관리 시, 해킹 등 전자적 침해에 따른 대량의 개인정보 유출, 노출 사고가 발생 가능
- 기존의 시스템은 ID 관리를 각 서버별로 구축하고 관리해야 한다는 불편함 및 비용 문제가 존재

☐ 사용자 입장에서 개별 서비스마다 인증정보를 다르게 설정 및 관리하기에 한계가 있어, 사용자가 여러 서비스에 동일한 인증정보를 설정하는 것을 이용하는 ‘크리덴셜 스템핑(Credential stuffing)’ 공격이 가능

☐ 실생활에서 사용자가 주민등록증 등 신원증명을 관리하는 것처럼, 온라인에서도 개별 서비스 제공기관이 아닌 사용자 스스로 자신의 신원정보를 관리 및 통제할 수 있도록 하는 새로운 인증체계가 필요

나. 범위 및 분류

(1) 가치사슬

- ☐ 다양한 DID 플랫폼 간의 호환이 가능해지는 표준화 및 인터체인 간 연결 기반이 구축될 경우 분산 ID 기술의 산업 융합이 가속화되어 전 산업 분야에서 추가적 부가가치 창출이 가능
- ☐ 거래 및 계약 과정 중 본인확인이 필요한 모든 분야에 큰 영향을 미칠 것으로 전망되며 통신, 금융, 보안 등의 영역에서 직·간접적인 새로운 부가가치 창출이 가능할 것으로 예상

[분산 ID 및 인증 시스템 분야 산업구조]

후방산업	분산 ID 및 인증 시스템	전방산업
DID Document 표준화 및 API 연동기술, 대용량 신원정보 저장 및 검증 기술	블록체인 기반 신원 인증 서비스 기술, 블록체인 암호키 관리 기술 등	분산 ID 기반 통신, 금융, 보안 서비스 산업

(2) 기술별 분류

- ☐ 분산 아이디 또는 분산 신원확인인 현재 금융권을 중심으로 그 활용이 시작되고 있는 단계
 - 기술의 초기 생태계는 금융거래 위주로 조성되었으나, 산업, 서비스 간 경계를 넘어 의료, 유통, 부동산 등으로 적용 분야가 확대되는 추세
 - 금융권은 블록체인 기반의 분산원장기술 등을 활용하여 외환, 소매·상업 은행, 거래 신용카드 발급, 송금, 청산, 투자, 대출 등 다양한 서비스에 적용하는 것을 고려 중
- ☐ 디지털 아이덴티티에는 중앙집중형 아이덴티티, 제3자 아이덴티티 제공자 기반의 아이덴티티, 분산원장 혹은 블록체인기반의 자기 주권 아이덴티티 모델이 있으며 전략제품으로 다룰 분산원장, 또는 블록체인 기반의 자기 주권을 보장하는 블록체인 기반 아이덴티티는 두 당사자의 신뢰를 블록체인 기반으로 인증하는 모델
 - 공개 표준으로는 World Wide Web Consortium(W3C)의 검증할 수 있는 자격 증명(Variable Credentials), Decentralized Identifiers(DIDs), OASIS의 탈중앙화된 키 관리 시스템, InternetEngineering Task Force(IETF), Digital Identity Foundation(DIF)의 DID Auth, 그리고 SOVRIN 재단의 제 3자의 인증기관이 필요 없는 영구적인 아이덴티티가 존재
 - 중앙집중형 아이덴티티는 사용자가 외부 사이트에 이름과 비밀번호로 계정을 만들고 두 당사자가 기밀성과 데이터 무결성이 보장된 상태로 서로 식별 및 인증하여 통신할 수 있는 암호화 프로토콜
 - 제3자 아이덴티티 제공자 기반의 아이덴티티는 두 당사자 중간에 아이덴티티의 신뢰를 보장하는 아이덴티티 제공자가 존재하는 모델

- 분산 ID 서비스 기술은 DID Document 표준화 및 API 연동 기술, 대용량 신원정보 저장 및 검증 기술, 블록체인 기반 신원인증 서비스 기술, 블록체인 암호키 관리 기술로 분류

[기술별 분류]

분류	상세 내용
DID Document 표준화 및 API 연동기술	<ul style="list-style-type: none"> • DID Document란 DID Subject(대상)이 자신을 인증하고, DID와의 연관성을 증명하는데 필요한 데이터 집합으로, 공개키 및 익명 처리되어있는 생체 인식등의 메커니즘을 포함 • DID 시스템의 확대를 위해서는 DID 체계의 표준화가 요구 • API 연동 기술은 사용자가 분산 ID를 사용할 수 있게 해주는 응용 프로그램 • W3C Decentralized Identifiers, Omnione
대용량 신원정보 저장 및 검증 기술	<ul style="list-style-type: none"> • 분산된 시스템에서 DID에 대한 조회 및 해결의 표준 방법을 제공하고, DID와 연결된 DPKI 메타데이터를 캡슐화하는 DID Document Object(DDO)를 반환하는 서버 기술을 포함 • DID는 DPKI에 필요한 메커니즘과 기능을 제공하는 분산 시스템을 기반으로 하며, 신원 데이터 저장 및 신원 상호 작용을 용이하게 하는 클라우드 및 엣지 인스턴스로 구성된 암호화된 개인 데이터의 복제된 mesh • DID의 서명 인증을 위해 그 기반이 되는 표준 형식 및 프로토콜이 필요 • Decentralized systems, DIF Universal resolver, DIF Identity Hubs, DID Attestations
블록체인 기반 신원 인증 서비스 기술	<ul style="list-style-type: none"> • 신원확인 허브 개인 데이터 스토어와 쌍을 이루는 DID에 기반한 새로운 종류의 앱 및 서비스 • 사용자의 ID 허브를 사용하여 데이터를 저장하고 부여된 사용 권한의 범위 내에서 작동 • DID User agents, Decentralized apps and services
블록체인 암호키 관리기술	<ul style="list-style-type: none"> • 암호 키 생성부터 폐기까지의 라이프 사이클 관리, 키 접근 시 보안 정책에 따른 접근 통제, 관리자 및 사용자의 키 접근 이력 감사 및 암호화/복호화 기능 등을 제공하는 기술 • DID User agents, Decentralized apps and services

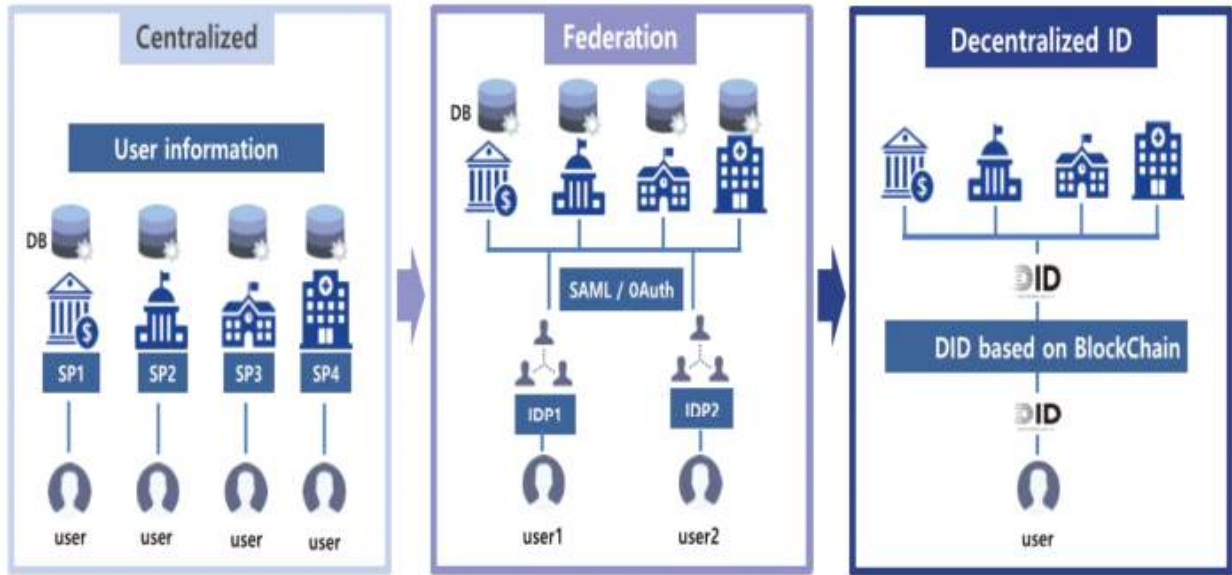
2. 산업 및 시장 분석

가. 산업 분석

◎ 기존 ID 체계의 문제점과 신원인증의 변화

- 기존 ID 체계로 식별, 인증 시 정보가 네트워크를 통해 전송되는 과정에서 보안 문제가 발생
 - 기존 ID 체계로 식별, 인증을 추진하던 온라인 시스템에서는 해킹의 75%가 ID를 서버 데이터베이스에 저장할 때와 다시 로그인할 때 발생
 - 각 서비스의 제공기관이 개별적으로 사용자 인증정보와 개인정보를 관리하여 각 서비스 제공기관이 해킹의 대상이 되면 이용자의 과실 여부와는 관계없이 이용자의 개인정보가 해킹될 수 있음
 - 이러한 문제점으로 인해 온라인 환경에서 사용자가 스스로 신원정보를 관리, 통제할 수 있도록 하는 새로운 인증체계인 블록체인 기반의 분산형 ID(Decentralized ID)의 필요성 대두
- 신원인증은 중앙집중형에서 연합형을 거쳐 이용자 중심형으로 변화하고 있음
 - 중앙집중형 ID는 인터넷 사이트마다 각각 다른 ID와 Password를 발급받아 사용하는 ID 체계
 - 현재 네트워크상의 신원 관리는 대부분 중앙집중형으로 사용자가 ID를 생성한 후 직접 관리할 필요가 없음
 - 많은 온라인 인터넷 사이트에 가입할 경우 모든 사이트에서 각각 ID와 Password를 발급받아야 함
 - 관리하는 중앙 기관에 문제가 발생하거나 모든 사이트에 같은 ID와 Password를 사용했을 경우 개인정보 유출의 피해가 커짐
 - 연합형 ID는 OpenID 또는 OAuth 등을 기반으로 한 연합 서비스제공자 중 한 곳에서 신원인증을 완료하면 타 연합 서비스도 이용 가능한 ID 체계
 - OpenID는 웹 사이트에서 사용자를 개별 인증하는 대신 사용자 인증을 독립된 OpenID Provider를 통해 통합 관리하는 인증방식
 - OAuth는 매쉬업 서비스로 만들어진 어플리케이션이 다른 어플리케이션의 사용자 정보와 리소스에 접근할 수 있게 해주는 표준적 인증방식
 - 대표적인 연합형 ID의 예시는 페이스북 로그인, 네이버 인증, 카카오 인증을 통한 로그인 등이 있음
 - 연합 서비스를 제공하는 곳에서 개인정보를 관리하기 때문에 여러 사이트에 가입할 필요가 없지만, 개인정보 유출이 발생하게 되면 연합 서비스를 제공하는 곳 전체에 상당한 위험 존재
 - 이용자 중심형 ID는 사용자가 신원 관리 서비스를 선택하여 발행받은 신원정보로 여러 서비스를 이용할 수 있으며 신원정보는 신원 관리 서비스제공자가 관리
 - 대표적인 이용자 중심형 ID에는 분산형 ID가 있음

[신원인증환경의 변화]



* 출처 : 신원인증환경의 변화, 2019.10, DID Alliance Korea

◎ 블록체인 기반 분산 ID(DID) 및 인증 시스템이 블록체인 게이트웨이로 부각

- ☐ 분산 ID(DID)는 정보 위변조 가능성 차단뿐만 아니라 기존 중앙집중화 방식의 ID 한계인 정보 유출 문제 해결 가능
 - 한 번만 인증받아 스마트폰 등 개인 단말기에 저장하면 금융권 비대면 계좌 개설, 여러 홈페이지에 흩어져 있는 ID와 비밀번호의 관리 문제 해결 가능
- ☐ 블록체인 관련 플랫폼은 개인정보 관리, 사용자 인증, 전자계약 등 여러 방면에서 두각을 드러내고 있음
 - 경찰청은 블록체인 기반 디지털 증거 관리 플랫폼을 구축하였고 보건복지부는 복지급여 중복수급 관리 플랫폼을 구축
 - 식품의약품안전처는 수입식품 위생증명서 진위여부를 실시간으로 확인하기 위한 블록체인 식품안전 데이터 플랫폼 출범
 - 세종시는 블록체인 기반 자율주행차 신뢰 플랫폼을, 한국도로공사는 상호신뢰 통행료 정산 플랫폼을 구축
- ☐ 코로나-19 사태로 인해, 비대면 시대로 경제 및 산업구조가 재편되는 과정에서 블록체인이 핵심기술로 재조명받고 있음
 - 코로나-19의 확산으로 비접촉, 비대면 서비스 수요가 늘어나면서 이러한 추세가 한층 강화됨
 - 온·오프라인에서 금융, 이커머스, 게임, 결제 등 다양한 서비스를 이용하기 위해서 매번 ID 인증받아야 하는 번거로움 해결

- 전자서명법 개정안 통과로 21년간 국내 전자인증 시장을 주도했던 공인인증서 제도가 사라지면서 블록체인 기반 분산신원인증 기술(DID) 시장이 주목받고 있음
 - 중앙시스템 통제 없이 분산화된 체계를 이용해 이용자가 개인의 정보를 직접 보관하고 관리할 수 있으며, 블록체인 자체가 위변조 방지 기능이 있는 만큼 실물 발급 신분증을 디지털화시키는 기술로 부상하고 있음
 - 공인인증서도 개인이 관리하지만, 공인인증서 소유자가 본인이 맞는지 확인하려면 이를 발급한 공인인증기관이 관리하는 서버를 거쳐야 함
- ID 관리의 독점과 개인정보 유출에 대한 해결책으로 블록체인 기반 인증 시스템 활용이 증가
 - 캐나다에서는 2017년부터 금융기관을 중심으로 '사이버 인증 리뉴얼 프로젝트'의 일환으로 후원하고 있는 디지털 신원확인 플랫폼을 제공하는 스타트업 시큐어키(SecureKey)가 IBM의 하이퍼레저 패브릭 기반으로 시장을 주도
 - 에스토니아는 2013년부터 정부 주도로 블록체인을 이용한 '전자거주권(e-Residency)' 프로그램으로 국적에 관계없이 디지털 ID 형태의 신원증명서를 발급 중. 법인설립에 필요한 절차를 간소화하고, 외국인도 인터넷을 통해 손쉽게 법인을 설립이 가능
 - 스위스의 도시 주크(Zug)에서는 2017년부터 지방정부 주도로 시민을 대상으로 블록체인 기반 신분증을 발급하는 파일럿 프로젝트를 운영 중. 분산 ID 플랫폼 업체인 유포트(uPort)와 협업해 신분증 발급과 증명을 위해 공개형 블록체인인 이더리움에 기반한 분산 ID 플랫폼을 구축
 - 일본은 2017년부터 일본 거래소 그룹과 증권사를 중심으로 블록체인 기반의 KYC 업무를 실증 실험함으로써 개념검증을 완료하고, 계좌개설 시 필요한 신원정보를 공유함으로써 고객의 불편함을 해소
 - 민간의 경우 자기주권ID(Self-sovereign identifier) 관리를 위해 IBM, Sovrin, Ockam, Aversafe, Trustedkey 등 다양한 스타트업과 비영리 단체를 중심으로 새로운 구조의 서비스 개발이 진행되고 있다. 이들은 대부분 하이퍼레저를 분산원장 기반으로 활용
- 세계 유수의 거대 기업들이 분산 ID 기술에 주목하고 있는 이유는 고객의 확보와 유지에 대한 주도권 때문
 - 여태까지 모든 인터넷 플랫폼은 플랫폼 가입 시 로그인 ID와 패스워드를 확보하고 이를 기반으로 중앙집중적인 방식을 통해 고객의 플랫폼 접근을 통제. 또한 좀 더 강력한 보안이 요구되는 금융권이나 공공기관의 경우, 공인인증서(PKI)를 이용해 플랫폼 접근을 관리
 - 블록체인 기반의 분산 ID가 확산되면 플랫폼에 대한 접근방법도 달라질 것.
 - 지갑보유자가 플랫폼에게 자신의 분산 ID만 알려주면, 플랫폼은 분산 ID의 존재 여부를 블록체인에서 확인하고 지갑보유자에게 분산 ID의 실제 보유자 여부를 증명하라고 요구
 - 지갑보유자는 분산 ID의 소유를 증명하고 플랫폼에 전달함으로써 플랫폼에 접근할 수 있음
 - 플랫폼 사업자들은 플랫폼 이용자들의 분산 ID는 알 수는 있지만, 과거처럼 이메일 등 개인의 정보는 알 수 없음

◎ 블록체인 DID 기반 통합인증결제 플랫폼 구현

- 정보통신산업진흥원(NIPA)이 지원하는 '2020년 블록체인 기술검증(PoC) 지원사업'의 지원과제로 선정되어 '블록체인 DID 기반 통합인증결제 플랫폼' 기술 구현 및 검증 수행 중
 - 기술검증(PoC) 지원사업은 초기 단계에 머물러 있는 블록체인 기반의 새로운 비즈니스 모델에 대해 기술 구현 가능성과 성능 평가 등을 지원하는 사업
 - 본격 사업 상용화에 앞서 '블록체인 DID 기반 통합인증결제 플랫폼'의 테스트베드 구축 및 오프라인 가맹점, 대학생 사용자 대상으로 실증 테스트를 통해 사업의 상용화 가능성에 대한 사전 검증 수행
- 간편한 타겟 마케팅 서비스를 갖춘 '블록체인 DID 기반 통합인증결제 플랫폼'은 기존 가맹점주들이 특정 고객을 타겟팅하여 홍보할 수 있는 마땅한 수단이 없어 겪던 어려움 해결
 - 가맹점에서 대상 고객의 자격 조건과 상품 금액만 설정하면 되기 때문에 타겟 마케팅 방법이 간편함
 - 프로모션 등록이 완료되면 사용자의 단말기는 해당 조건의 일치 여부 판단 후 프로모션 알림 제공하며 사용자 조건과 일치하지 않는다면 알림이 발생하지 않음
 - 가맹점주는 불특정 다수를 향한 과도한 홍보비를 지출하는 부담이 줄어들고 사용자는 관계없는 프로모션 안내를 받지 않아 기존에 광고 문자에 느껴왔던 피로감을 해소할 수 있음
- '블록체인 DID 기반 통합인증결제 플랫폼'을 통해 가맹점의 프로모션 이용 고객 응대와 결제관리 또한 쉽게 할 수 있음
 - 고객이 본인의 스마트폰을 제시하여 QR코드를 인식하면 프로모션에 적합한 자격 소지자인지 증명하고 할인 결제까지 한 번에 처리
 - 신분증이나 증명서를 직접 확인하거나 별도의 결제 프로세스를 진행하지 않고 인증과 결제가 한 번에 이루어져 간편함
 - 블록체인에 기록되는 모든 인증과 결제 내역은 향후 감사 로그 등으로 활용가능하고 블록체인 원장에 기록된 정보는 위변조할 수 없어 고신뢰 검증 가능

[블록체인 DID 기반 통합인증결제 플랫폼 구현]



* 출처 : 블록체인 DID 기반 통합인증결제 플랫폼 구현, 2020, 디지털존

나. 시장 분석

(1) 세계시장

- AlliedMarketResearch의 2020년 보고서에 따르면 2018년 블록체인 ID 세계시장 규모는 2018년 1억 7,000만 달러에서 연평균 성장률 약 79.2%로 성장하여 2024년에는 56억 3,000만 달러의 규모로 성장할 것으로 전망

[글로벌 블록체인 ID 관리 시장 규모 및 전망]

(단위 : 백만 달러, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
합계	170	305	546	978	1,753	3,142	5,630	79.2

* 출처 : 글로벌 블록체인 ID 관리 시장 규모, 2020, AlliedMarketResearch

(2) 국내시장¹¹⁾

- 2018년 국내 블록체인 ID 시장규모는 2018년 56억 원에서 연평균 약 79.2%로 성장하여 2024년 시장규모는 약 1,839억 원으로 추산됨
- 공인인증서 의무 사용이 폐지된 시점에서도 대다수 금융거래와 정부 민원 처리가 공인인증서를 통해 처리 중
 - 따라서 분산 ID 및 인증 시스템또한 전자 인증 서비스 시장의 상당 부분을 대체할 수 있을 것으로 판단

[블록체인 암호 Key 관리 시스템 국내 시장규모 및 전망]

(단위 : 억 원, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
합계	56	100	178	320	573	1,026	1,839	79.2

* 출처 : 글로벌 블록체인 ID 관리 시장 규모, 2020, AlliedMarketResearch를 기반으로 비트코인 화폐별 거래량 중 원화 점유율 2.97%¹²⁾(코인힐스 2020.12.30.)을 근거로 환율은 1100원/달러를 적용하여 추산

11) 블록체인 기반 ID 관리 시장은 대부분 북미에서 주도하고 있으며 국내시장은 매우 작아 자료가 존재하지 않아 세계시장 대비 국내시장 비율로 추산

12) 미국달러:72.7%, 일본엔화:18.66%, 유로화:3.06%, 한국원화:2.97%

3. 기술개발 동향

□ 기술경쟁력

- 블록체인 기반 분산 ID 및 인증 시스템은 미국이 최고기술국으로 평가되었으며, 우리나라는 최고기술국 대비 87.1%의 기술수준을 보유하고 있으며, 최고기술국과의 기술격차는 1.3년으로 분석
- 중소기업의 기술경쟁력은 최고기술국 대비 82.3%, 기술격차는 1.5년으로 평가
- 한국(87.1%)>EU(86%)>중국(75.6%)>일본(67.1%)의 순으로 평가

□ 기술수명주기(TCT)¹³⁾

- 블록체인 기반 분산 ID 및 인증 시스템은 3.42의 기술수명주기를 지닌 것으로 파악

가. 기술개발 이슈

◎ 블록체인 기반 분산형 ID(Decentralized ID) 기술

- 분산형 ID(DID)란 사용자 스스로 필요에 따라 신원정보를 발급, 증명, 관리, 통제하는 형태의 신원 관리체계로 개인정보를 관리할 수 있는 시작점을 제공하는 것을 의미

- 블록체인을 기반으로 하며 분산형 데이터베이스(장부)를 이용해 분산형 장부를 관리하는 Node¹⁴⁾의 연결을 근거로 기능
- 데이터가 분산됨으로써 동등한 권리를 가진 사용자들 사이에서의 상호작용을 통해 장부상 데이터가 지속적으로 갱신되므로 Node 한쪽에서 일방적으로 데이터를 삭제하거나 편집하는 것이 불가능
- DID 문서는 DID 대상이 자신을 인증하고, DID와의 연관성을 증명하는데 필요한 데이터의 집합으로 공개키 암호화 기술, 익명 처리되어있는 생체인식 등의 메커니즘을 포함

- DID가 동작하는 방법은 DID와 연관되어있는 DID 문서가 특정 분산원장이나 네트워크에서 생성되고 읽어지고 업데이트되면서 비활성화되는 메커니즘

- 특정 DID가 DID 문서와 관련된 전체 기능들을 사용할 수 있도록 하기 위해선 DID 방법 중 DID의 생성, 읽기, 업데이트 및 비활성화 등의 작업을 수행해야 함

[스키마, DID 방법의 상세를 나타내는 문자열]



* 출처 : DID 방법의 상세를 나타내는 문자열, W3C

13) 기술수명주기(TCT, Technical Cycle Time): 특허 출원연도와 인용한 특허들의 출원연도 차이의 중앙값을 통해 기술 변화속도 및 기술의 경제적 수명을 예측

14) 통신망 가운데도 시간을 잇는 기간 회선과 단말에 연결되는 지회선의 접속 부분으로 노드 지점에 설치한 통신제어장치에 의해 통신망 전체를 제어

☐ DID와 DID 문서는 분산 ID의 기반이지만 이는 전체 시스템을 설명하는 일부분에 불과함

- 개인정보의 관리와 활용의 패러다임이 '자기 주권 신원'의 개념으로 옮겨감에 따라 이 패러다임을 현실화하는데 기존 신원인증의 개념보다 더 많은 개념이 필요
- 정보 주체가 제공한 특정 정보가 신뢰할만한 정보인지 증명하는 '증명 가능한 자격증명'의 개념

☐ DID는 지속성, 피어(PEER) 기반, 휴대 용이성, 개인정보 활용 및 보호의 특성을 가짐

- DID는 외부 환경의 변화와 관계없이 자신의 신원정보를 지속적으로 사용 가능
- 자신의 신원정보를 직접 관리하므로 신원인증 서비스제공자의 서비스 운영 중지 등 외부적 요인이 발생하더라도 신원정보의 유효성이 유지됨
- 신용정보의 발행, 검증은 특정 기관(TTP)에 종속적이지 않고 피어 기반으로 독립적으로 운영되며 누구나 신원정보 생성, 이용 가능
- 단, 사용자의 신원을 최초로 검증할 수 있는 최소한의 신뢰된 기관이 필요
- 신원증명이 필요한 경우 언제든지 스스로 신원정보를 선택 후 제공 가능
- 휴대성을 위해 사용자의 스마트폰을 이용한 모바일 ID, 칩이 내장된 실물카드 형태의 ID 카드 등으로 이용 가능
- 개인의 명시적 동의 없이는 서비스제공자의 개인정보 활용이 제한됨
- 사용자가 신원정보를 스스로 관리하므로 서비스제공자는 서비스에 필요한 정보 이외의 정보를 확인하거나 활용할 수 없음
- 분산원장 기반의 ID 저장소 내에서 개인정보가 포함된 신원정보는 암호화 등의 조치를 수행하거나 분산원장 밖(Off-Chain)에 저장함으로써 보안 확보 가능

◎ DID 표준화 활동의 본격화

☐ 분산 ID 기술은 사용자가 신원 관리 서비스를 선택하여, 발행받은 신원정보로 여러 서비스를 이용할 수 있도록 하는 기술로 신원정보는 분산원장 기반으로 공유되고, 신원정보는 사용자가 관리

- 사용자는 외부 환경의 변화와 무관하게 자신의 신원 정보를 지속적으로 사용 가능
- 서비스제공자에 의해 신원정보가 관리되지 않으므로, 서비스제공자의 서비스 운영 중지 등 외부적 요인이 발생하더라도 신원정보의 유효성은 유지

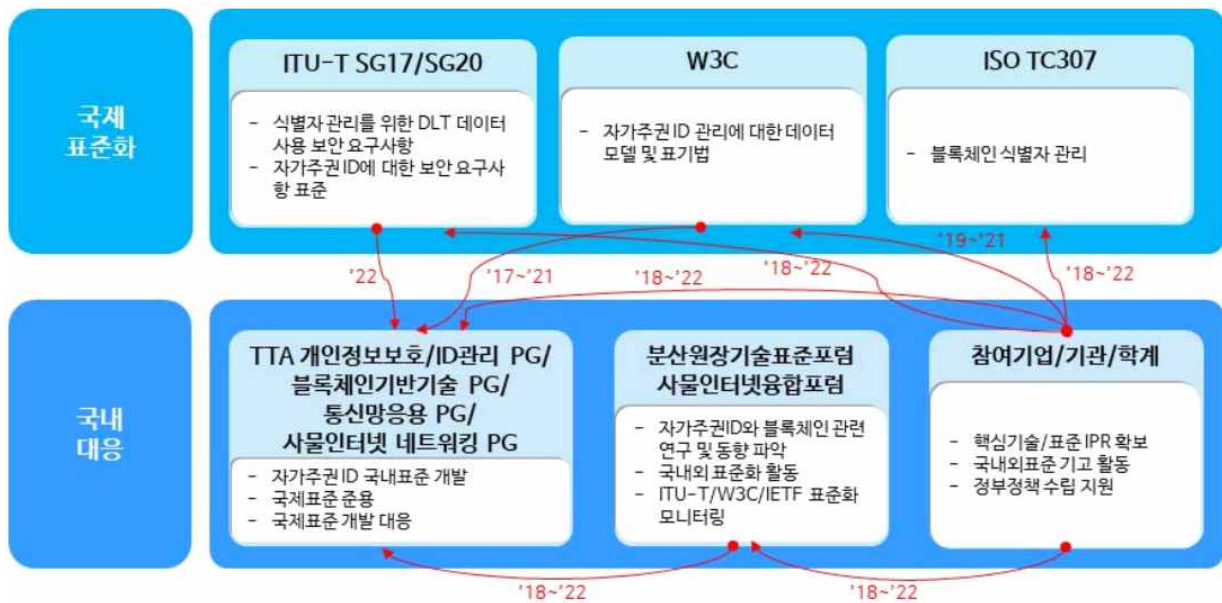
☐ 디지털 신원증명의 진본성과 신뢰성을 확고히 하는 탈중앙화된 신원 증명(DID, Decentralized Identity) 서비스를 위해 설립된 오픈 산업 협회인 DID Alliance가 설립

- 표준화되고 상호호환 가능한 프레임워크의 개발이 목표
- 국내에서는 병무청, 신한은행 등의 금융계, LG CNS, 삼성 SDS 등의 SI 업체 등이 다양하게 참여

□ 국내 TTA 표준화 계획

- TTA 통신망 응용 PG(PG224)에서 블록체인 환경에서 DNS 시스템(기술보고서)을 개발 추진
- TTA 사물인터넷/스마트시티 플랫폼 PG(PG1001)에서 블록체인서 활용할 수 있는 식별자 체계 표준을 개발 추진
- TTA 블록체인 기반기술 PG (PG1006)에서 블록체인과 식별자를 연계한 테스트넷 지침서 표준 개발 추진

[블록체인 기반의 자가주권 ID (DID) 국제 표준화 대응체계]



* 출처: ICT 표준화 전략맵, 2020, 과학기술정보통신부

◎ 분산 ID의 생성, 유통 과정

□ 분산 ID의 생성과 저장방식

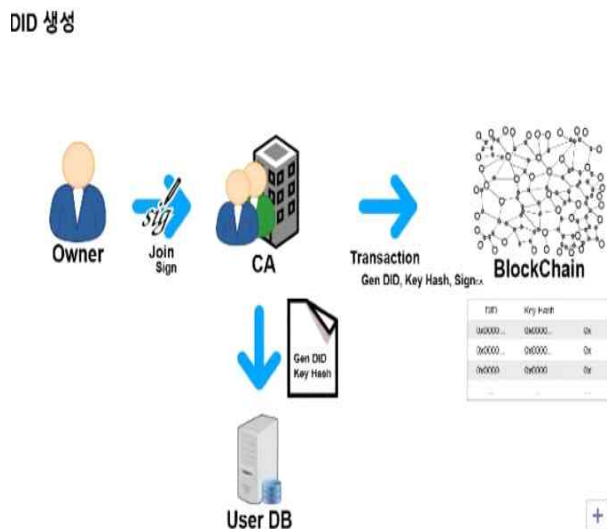
- 분산 ID는 지갑보유자가 신뢰기관에게 자신을 증명해 블록체인에 기록해달라고 요청
- 신뢰기관은 지갑보유자의 신원을 확인한 후 이를 분산원장에 기록하고 분산 ID를 발급. 분산원장 기반의 신뢰된 분산 ID 저장소 내에는 개인정보를 평문으로 저장하지 않으며, 개인정보가 포함된 신원정보는 암호화 등의 조치를 수행하거나, Off-Chain에 저장이 가능
- 분산 ID 생성 방식은 신원정보 저장위치에 따라 세가지로 분류
 - 분산원장 내에서 암호화해 저장하는 방식으로 분산원장 내에 신원정보가 암호화돼 저장되며, 사용자는 복호화에 필요한 키를 관리하는 방식(더키(thekey), vip 등이 채택)
 - 사용자 모바일 내 신원정보가 저장되며, 사용자는 서비스 제공자에게는 필요한 신원정보만 선택해 제공하는 방식(소브린, 유포트 등이 채택)
 - 발급기관 내에 저장하는 방식으로 신원정보를 발급하는 기관에서 신원정보를 저장하며, 사용자가 동의한 경우에만 서비스 제공자에게 신원정보를 제공(시큐어키 등이 채택)

□ 분산 ID의 유통 과정

- 분산 ID가 분산원장에 저장되면 지갑보유자는 자신의 지갑에 개인정보를 저장하고 이를 외부에 제공할 수 있음
- 예시) 새로운 직장에 취직하기 위해 입사원서를 제출하는 지갑보유자
 - 지갑보유자는 자신의 최종 학교 졸업증명서와 경력증명서를 새로운 직장에 제출해야 함
 - 그는 지갑을 통해 해당학교에 자신의 분산 ID로 졸업증명서를 새로운 직장에 보내 달라고 요구할 수 있음
 - 해당 학교는 분산 ID를 확인하기 위해 지갑보유자에게 신원증명을 요구하게 되고 지갑보유자는 필요한 신원정보를 보내면, 학교는 확인한 후 새로운 직장에 졸업증명서를 보냄
 - 경력 증명서를 발행하는 이전 직장도 동일한 방식으로 경력증명서를 발급
- 여기서 이용자들의 편의성을 높이기 위해 이런 신원증명이나 신원증명 요청에 대한 표준 양식인 신원증명이 필요
- 향후 분산 ID를 기반으로 이런 과정을 중계하는 신원증명 중계기관도 등장 가능

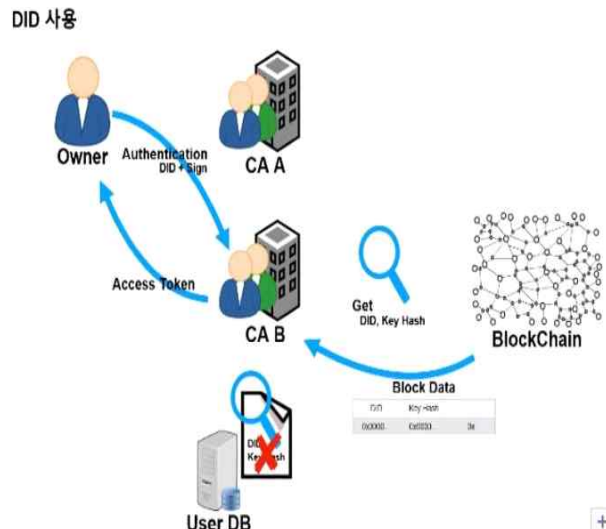
[분산 ID의 생성 과정]

DID 생성



[분산 ID의 유통 과정]

DID 사용



* 출처 : 분산 ID의 생성, 유통 과정, 2019.2, 심버스 분산 ID와 이용자 자기주권시대

나. 생태계 기술 동향

(1) 해외 플레이어 동향

◎ DID 기술기업 연합체 Sovrin 재단

☐ (IBM) Visa의 'B2B Connect' 솔루션을 위해 하이퍼레저의 패브릭 프레임 워크를 적용

- 하이퍼레저 패브릭은 허가형 프라이빗 블록체인(Permissioned Private Blockchain)의 형태를 가짐
 - 하이퍼레저 패브릭에서는 인증관리 시스템에 의해 허가된 사용자만 블록체인 네트워크에 참여할 수 있음
- 하이퍼레저 패브릭의 구성요소에는 분산원장, 체인코드, Peer, Orderer가 있음
- 사용자의 권한 및 인증을 위해 MSP(Membership Service Provider)를 사용
 - MSP를 발급하고 관리하기 위해 Fabric-CA 노드를 사용하여 1차적으로 사용자의 서명과 권한 등을 확인하고 Peer를 통해 원장에 기록되기 전에 보증정책을 준수하는지 확인

☐ (Evernym) DID 기술의 글로벌 표준 수립에 있어 가장 선도적인 역할을 하는 기업

- W3C에서 DID 표준 정립 및 DID의 근간인 자기 주권 신원(Self-sovereign Identity, SSI) 개념을 최초로 제시
 - SSI란 개인 스스로가 발급하고 관리(통제)하는 자기 주권 신원을 말함
- Linux Foundation과 공동으로 DID 솔루션을 개발
- ATP Financial, Barclaycard, Mastercard, British Columbia 등 글로벌 기관들과 협력을 통해 DID 글로벌 표준안 수립을 선도

☐ (CISCO) 보안을 강화한 엔터프라이즈 블록체인 서비스 출시 및 공동 사업 추진

- 국내 블록체인 자회사 람다256이 자체 개발한 서비스형 블록체인 플랫폼(BaaS)인 '루니버스'와 시스코가 운영하는 클라우드 기반 보안 서비스 '스텔스워치 클라우드'를 결합하는 형태로 보안을 강화한 서비스를 출시
- 머신러닝과 행동모델링으로 엔터프라이즈 고객이 새로운 위협에 대응할 수 있도록 보안 강화형 블록체인 서비스 개발 중
 - 기업이 블록체인 네트워크에서 누가 무엇을 하고 있는지 이해하고, 네트워크 세분화로 중요한 데이터를 보호할 수 있는 기능을 제공할 예정

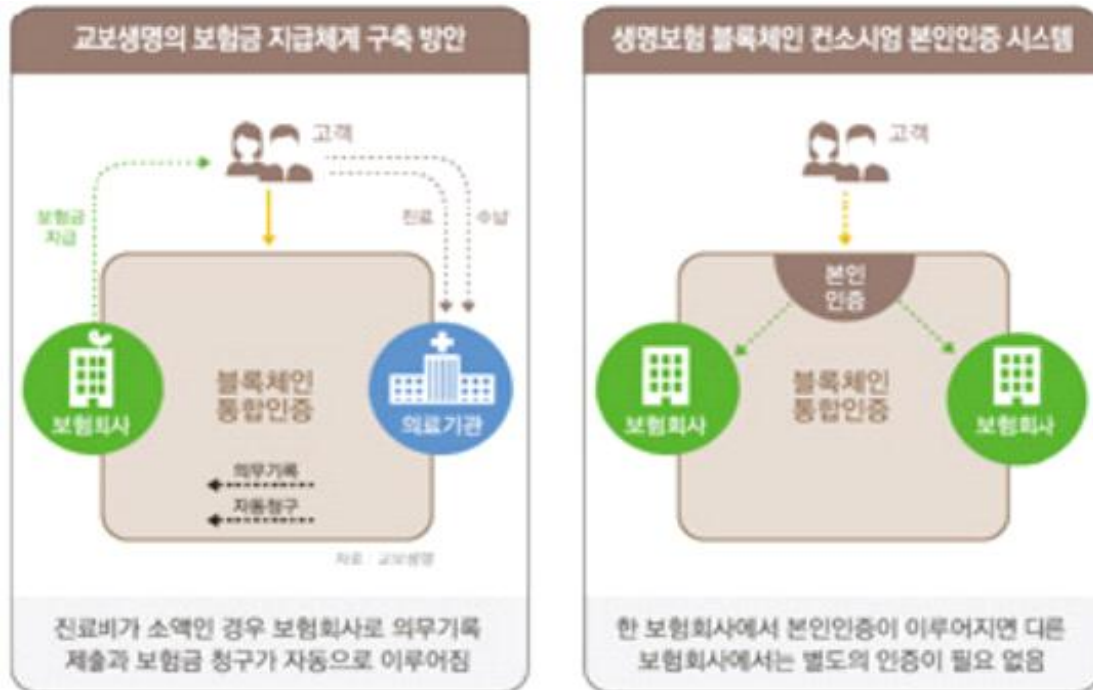
◎ 그 외 블록체인 기반 인증 시스템을 활용한 해외 플레이어

- ☐ (Microsoft) DIF(Distributed Identity Foundation), W3C 자격증명 커뮤니티 그룹들과 적극적으로 협업 중
 - 효율성과 확장성 문제를 해결함과 동시에 보안을 확보하기 위한 공용 신규 블록체인 네트워크인 child chain 및 side chain 등을 통해 기존 공용 체인 위에서 실행되는 오픈 소스 DID 구현을 개발
 - 기업이 사용자가 제어할 수 있는 새로운 제품, 응용 프로그램 및 서비스를 구축하기 위해 의존할 수 있는 통합된 상호 운용 가능한 생태계 구축이 목표
 - 2019년 5월, 오픈소스 프로젝트인 아이온(ION) 공개
 - 아이온은 퍼블릭 인프라스트럭처 프로토콜인 사이드 트리 기반으로 개발된 레이어 2 프로젝트로, 비트코인을 메인 네트워크로 활용
- ☐ (Amazon) 제품 공급망에 디지털 신뢰를 제공하기 위한 분산 원장 기술 특허 취득
 - 아마존이 판매한 제품의 진위를 보장하기 위한 상품 추적 솔루션으로 분산원장인증 시스템을 활용하여 공급망에 가시성을 더해 신뢰도 증가
 - 공급망 참여자들에게 특정한 인증절차를 요구하고, 관리규정을 제시하는 인증기관을 두어 해당 기관에 등록된 제조업체, 운송업체, 유통업체 최종 사용자는 분산원장에 변경사항 추가 가능
 - 분산원장 기반 시스템을 통해 제조업체, 유통업체 운송업체가 보유한 데이터를 개방형 프레임워크에 종합해 투명성, 일관성, 참조 무결성, 보안성이 결여된 시스템과 데이터베이스가 급속히 증가하면서 생긴 공급망 문제를 해결
 - 분산원장 기반 시스템을 통해 데이터 조작을 방지하고 단일 장애 지점을 제거할 수 있음
- ☐ (uPort) 세계 최대 이더리움 소프트웨어 개발 회사인 ConsenSys에서 개발한 플랫폼으로, 블록체인 기반의 신원증명 기술 구현
 - 신원 및 개인 데이터를 제어할 수 있는 안전한 자기 주권 신원 지갑 제공
 - 이용자가 이더리움(Ethereum) 블록체인 네트워크에서 ID를 생성하여 비밀번호 없이 애플리케이션 내에서 안전하게 로그인하여 개인정보 및 검증
 - 이를 통해 메시지 수신자는 중앙 집중식으로 서버 없이 메시지 송신자를 신뢰할 수 있도록 하며, 스마트계약의 특성을 이용하여 영구 ID를 생성하여 개인키 분실로 인한 신원인증의 문제점 보완

(2) 국내 플레이어 동향

- (교보생명) 국내 최초로 보험금 지급 체계에 블록체인 기반 인증 기술을 활용

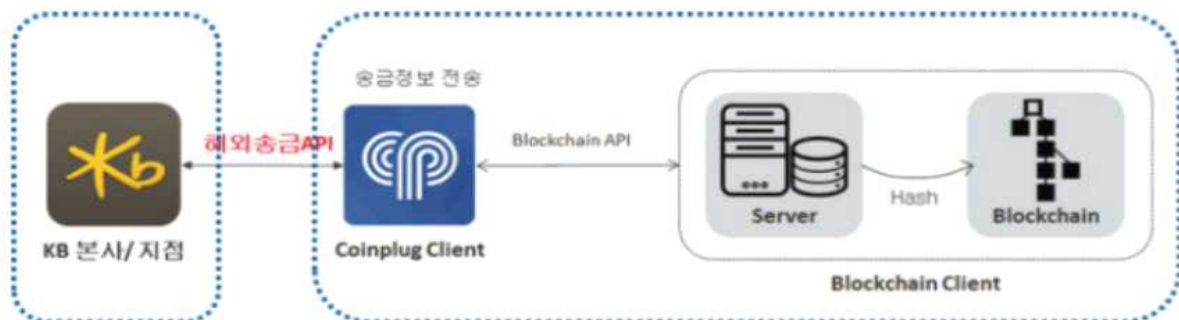
[교보생명 블록체인 기반 인증 시스템]



* 출처 : 보험연구원 - 블록체인 적용 사례

- (KB국민카드) 국내 금융사 중 최초로 블록체인 기술을 활용한 개인인증 시스템 도입
- 2018년 8월 기존의 공인인증서를 대체할 수 있는 블록체인 기반 모바일버전 '뱅크사인' 출시

[KB국민은행 블록체인 기반 인증 시스템]

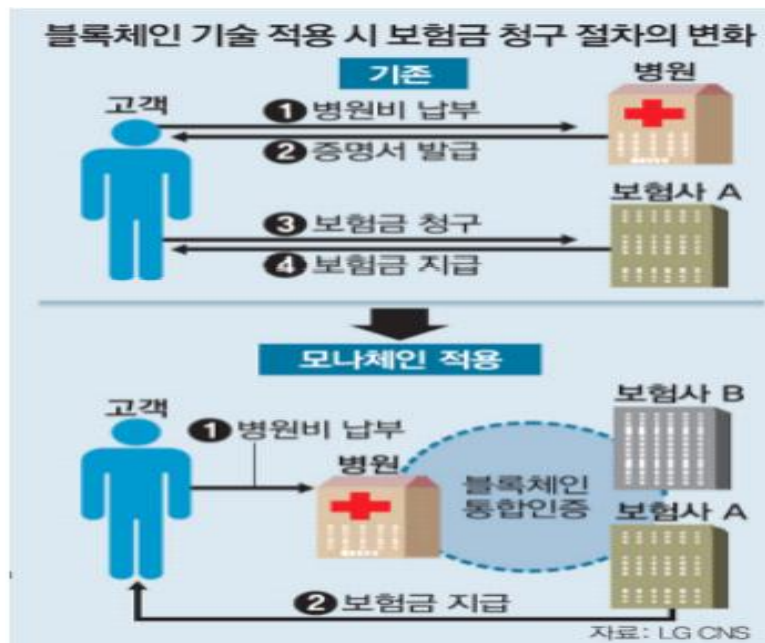


* 출처 : (주)코인플러스

□ (LG CNS) 사채 블록체인 플랫폼 ‘모나체인’을 출시

- 금융, 공공, 통신, 제조와 같은 모든 산업영역에서 적용 가능한 기업용 블록체인 플랫폼
- 차별화된 디지털 인증 서비스를 위해 분산 신원 확인 기술 채택
- 블록체인 기술을 통해 보험금 청구 관련 정보가 보험사와 병원사이 쉽게 공유함으로써 기존 병원에서 증명서를 받고 보험사에 청구한 후에 보험금 지급받던 방식에서 사용자가 병원에서 의료비 결제함과 동시에 보험금 자동 수령 가능

[LG CNS의 모나체인을 이용한 보험금 청구 프로세스]



* 출처 : 보험연구원 - 블록체인 적용 사례

□ (금융보안원) 금융보안원은 금융 보안 표준화 협의회를 개최하여, 금융권 분산 ID 프레임워크를 금융보안 표준화 신규 과제로 채택

- 암호키 저장·관리·복구 방법, 정보보호 거버넌스 요구사항 등을 포함하고 분산 ID 기술 표준을 통해 금융권 분산 ID 기반 신원확인서비스 간 상호 연동 및 보안성을 확보, 혁신적 금융서비스 창출 및 금융소비자의 신원정보 보호 강화를 기대 중
- 구체적으로, 표준 개발 내용 및 범위는 자기통제 기반 분산형 신원관리 프레임워크 구성 및 기능, 자기통제 기반 분산형 신원관리 방법, 자기통제 기반 분산형 신원관리 생태계 요구사항 등을 포함
- 이를 위해 금융소비자의 신원확인 편의성 제고 및 자기정보결정권 보장을 강화하고, 금융회사의 신원확인 업무 효율성 제고 및 혁신적인 금융서비스 창출 기반을 제공할 계획
- 금융보안원은 2019년에 표준개발그룹을 통해 표준안 개발을 완료하고, 2020년 상반기에 표준 제정·공고할 예정

- (SK텔레콤) LG 유플러스, KT, 삼성전자, KEB하나은행, 우리은행, 코스콤 등 7개사와 사업 협약을 맺고, DID를 기반으로 한 '자기주권 증명서 지갑 서비스'를 준비 중
 - '비들 아시아 2019'에서 기업용 블록체인 플랫폼인 '스톤(STON)'을 공개. 스톤은 하이퍼레저를 기반으로 하는 블록체인 플랫폼으로 별도의 암호화폐는 발행하지 않음
 - 스톤 프로젝트에는 탈중앙화 신원증명 서비스가 포함되어 있으며, 신원증명 시 개인의 핸드폰 번호를 활용할 수 있을 것이라 밝힘
 - '블록체인 기반 모바일 전자 증명 서비스 공동 사업 협약'. 탈중앙화 신원증명 기술을 기반으로 사용자가 자신의 개인정보를 직접 관리할 수 있는 '자기 주권 신원 지갑(Self-Sovereign Identity)'을 출시할 계획
- (DID 얼라이언스) 분산 ID 기술 표준화 방향으로 국제표준과 연계한 DID 얼라이언스 중심의 기술 표준 개발 금융 분산 ID 통합 컨소시엄 기반의 서비스 표준 개발 기술 표준 및 서비스 표준을 통합한 새로운 표준 제정 등을 언급
- (병무청) EOS 블록체인을 기반으로, '블록체인 기반 DID를 활용한 병무 행정 서비스'를 제공하기 위한 DID 플랫폼을 85% 구현(2019. 10 기준). 테스트를 거쳐 2020.1 오픈할 계획
- (금융결제원) DID 플랫폼의 개발을 완료하여 테스트를 진행하여 비대면 상황에서 분산 ID로 계좌를 개설하는 실증 모델을 개발, 비대면 실명확인에 대한 실증작업 진행
- (라운시큐어) 생체인증에 강점을 가진 기업으로 FIDO 생체인증과 블록체인 기술이 적용된 '옴니원(OmniOne)' 서비스를 출시.
 - 라운시큐어는 '2019년 블록체인 공공선도 시범사업자'로 선정되어 병무청과 함께 '블록체인 기반 인증서 없는 민원서비스'를 구축
 - 라운시큐어는 탈중앙화 신원증명을 이용해 병무청 민원 포털 서비스의 전자서명 및 부인방지에 적용 예상
- (블로코) 롯데카드 블록체인 기반 생체인증 간편 로그인, 블록체인 기반 전자서명 간편 로그인, 삼성카드 블록체인 기반 바우처 등을 허가형 기반의 코인스택을 이용해 개발
- (와이즈엠글로벌) 분산 ID 전용 블록체인을 제공하는 심버스(SymVerse) 프로젝트를 개발 중
 - SymID라는 분산 ID는 인증서비스를 제공하는 CA서버와 연동해 생성하며, 이를 이용해 복수의 계정 신청이 가능, 계정은 부가정보를 블록체인에 저장함으로써 개인키 분실이나 유출에 대응이 가능

다. 국내 연구개발 기관 및 동향

(1) 연구개발 기관

[블록체인 기반 분산 ID 및 인증 시스템 분야 주요 기술개발 기관]

기관	소속	연구분야
백석대학교	정보통신학부	<ul style="list-style-type: none"> • 공통 보안기술 • 네트워크 시스템 보안 • 서비스/응용보안
한국전자통신연구원	정보보호연구본부	<ul style="list-style-type: none"> • 현대 암호 알고리즘 및 차세대 암호 후보군에 대한 부채널 분석 • 디바이스 DNA 기반 안전한 암호키 생성/사용/은닉 기술 • 글로벌 표준(KMIP) 키관리 기술 및 이의 드론 보안 적용 기술
	블록체인연구실	<ul style="list-style-type: none"> • 신뢰 인프라 제어/관리 기술 • 스마트 사이니지 플랫폼 기술

(2) 기관 기술개발 동향

□ (아이콘루프)

- 블록체인 기반 분산 ID를 이용한 출입통제 인증 시스템 (2020-06-01~2021-11-30)
 - W3C 표준을(W3C DID) 따르는 DID Document 개발
 - 분산 ID 생성/조회/업데이트/폐기 Smart Contract 개발
 - 발행인, 검증인 제공 연동 인터페이스 개발
 - 분산 ID 관리 모듈 개발 (DID Manager)
 - 신원증명 발행/폐기 기록 관리 및 유효성 검증용 Smart Contract 개발
 - 분산 ID Tx생성 및 Smart contract 실행을 위한 SDK 개발

□ (백석대학교)

- 블록체인 기반 탈중앙화 신원 증명(DID) 플랫폼 연구 (2020-06-01~2022-02-28)
 - 모바일 신분증으로 신분 · 자격 · 소유 권한에 기반한 거래 및 이용 행위를 통합 관리하는 서비스 플랫폼 연구
 - Self-Sovereign ID 체계 구축: 개인이 스스로 정보 보관 및 공유에 대한 소유권을 가진 자기주권 개인정보 관리체계 연구
 - 비대면 실명인증을 위한 KYC 및 자격인증, 블록체인으로 공유되는 정보를 기반으로 신분/자격/소유 증명 서비스 연구

□ (한국전자통신연구원)

- O2O 서비스를 위한 무자각 증강인증 및 프라이버시가 보장되는 블록체인 ID 관리 기술 개발 (2018-05-01~2020-12-31)
 - 블록체인 저장 바이오 템플릿 누출 방지 기술, 상황인지 기반 증강 인증 기술, 무자각 증강 인증 프레임워크 실용화 기술 개발
 - 블록체인 ID 관리 프라이버시 모니터링 서버, 실증 서비스를 위한 레거시 시스템 연동 기술 개발, 블록체인 ID 관리 실증 서비스 구축
 - 프라이버시 침해방지 스마트계약 동적 생성 기술, 블록체인 ID 관리 UMA 정책 서버, 블록체인 ID 정보 은닉 실용화 기술 개발
- 블록체인을 활용한 분산형 자기주권 신원정보관리 기술 개발 (2019-04-01~2020-12-31)
 - 선택적 신원정보 교환 프로토콜 개발
 - 선택적 신원정보 발급·관리·검증 기능 개발
 - 식별자 기반 전자인증 서비스 개발
 - 분산형 자기주권 신원정보관리를 위한 블록체인 레퍼런스 모델 구축
 - 분산형 자기주권 신원정보관리 아키텍처 표준화

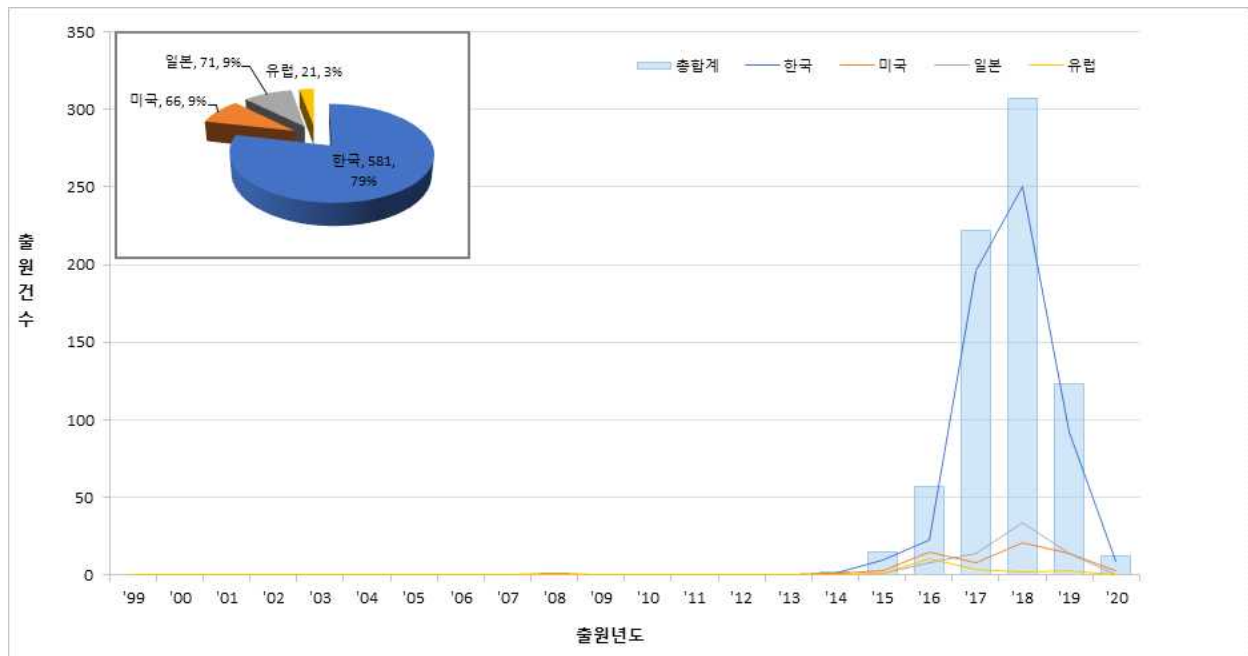
4. 특허 동향

가. 특허동향 분석

(1) 연도별 출원동향

- ☐ 블록체인 기반 분산 ID 및 인증 시스템은 '16년부터 급격한 성장을 보임
 - 각 국가별로 살펴보면 한국이 가장 활발한 출원활동을 보이고 있음
- ☐ 국가별 출원비중을 살펴보면 한국이 전체의 79%의 출원 비중을 차지하고 있어, 최대 출원국으로 블록체인 기반 분산 ID 및 인증 시스템 분야를 리드하고 있는 것으로 나타났으며, 일본은 10%, 미국은 9%, 유럽은 3% 순으로 나타남

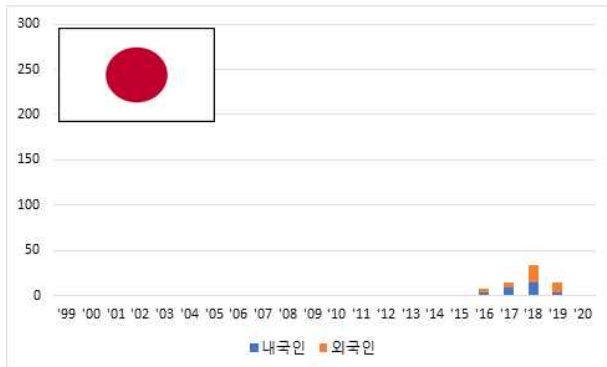
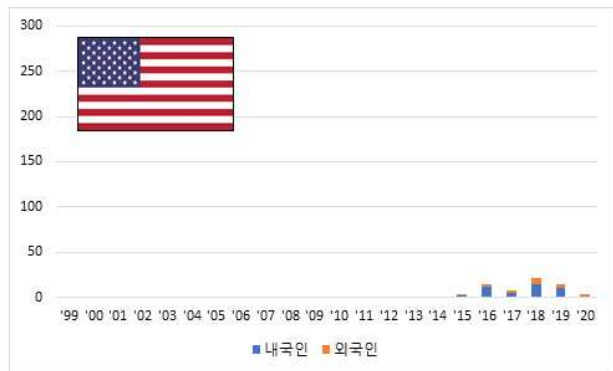
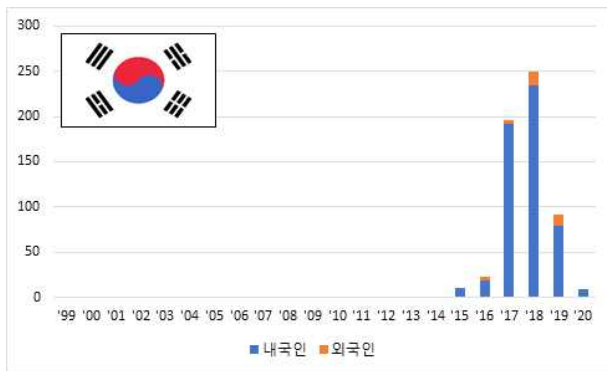
[블록체인 기반 분산 ID 및 인증 시스템 연도별 출원동향]



(2) 국가별 출원현황

- ☐ 한국의 출원현황을 살펴보면, '17년부터 해당 기술의 출원이 급격히 증가하는 추세
 - 내국인 위주의 출원이 진행되고 있음
 - 한국 기술의 양적 흐름은 '18년에 가장 많은 특허를 출원
 - 한국의 출원 수는 미국, 유럽, 일본에 비해 가장 많은 특허를 출원
- ☐ 미국의 출원현황은 출원수가 매년 20건 이하로, 뚜렷한 증감 동향이 나타나지 않음
- ☐ 유럽의 출원현황은 출원수가 매년 10건 이하로, 뚜렷한 증감 동향이 나타나지 않음
- ☐ 일본의 출원현황을 살펴보면, 한국과 유사한 동향을 보임

[국가별 출원현황]

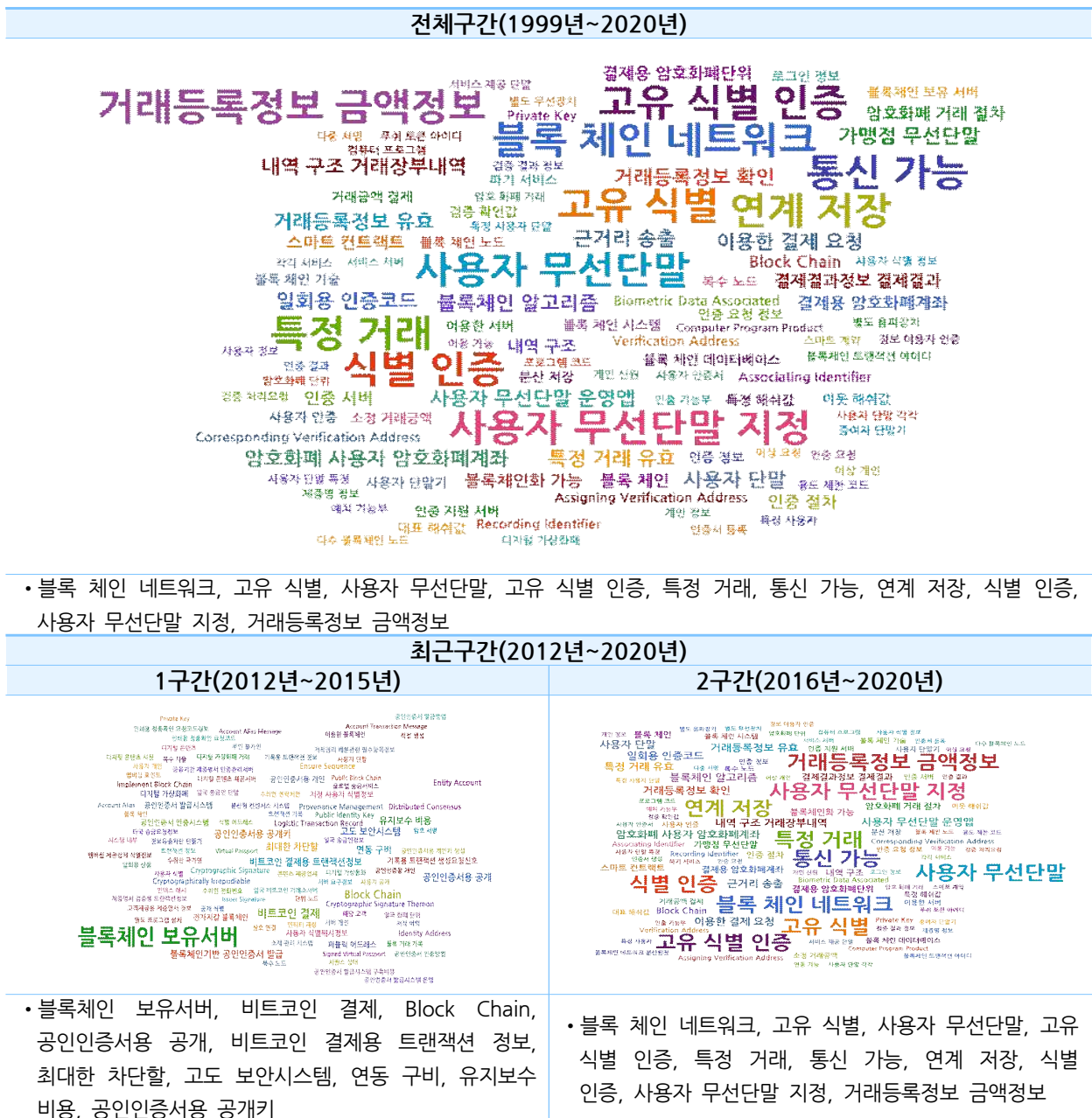


(3) 기술 집중도 분석

□ 전략제품에 대한 최근 기술 집중도 분석을 위한 구간별 기술 키워드 분석 진행

- 전체 구간(1999년~2020년)에서 블록 체인 네트워크, 고유 식별, 사용자 무선단말 등 키워드가 다수 도출
- 최근 구간 분석 결과, 최근 1구간(2012년~2015년)과 비교할 때 2구간(2016년~2020년)에서 블록체인 네트워크, 고유 식별, 사용자 무선단말, 고유 식별 인증 키워드가 많이 등장하는 것으로 보아 블록체인 기반 분산 ID 및 인증 시스템 분야에는 블록체인 기반 신원인증서비스 기술, 선택적 신원 정보 기술 관련 연구개발이 활발한 것으로 추정

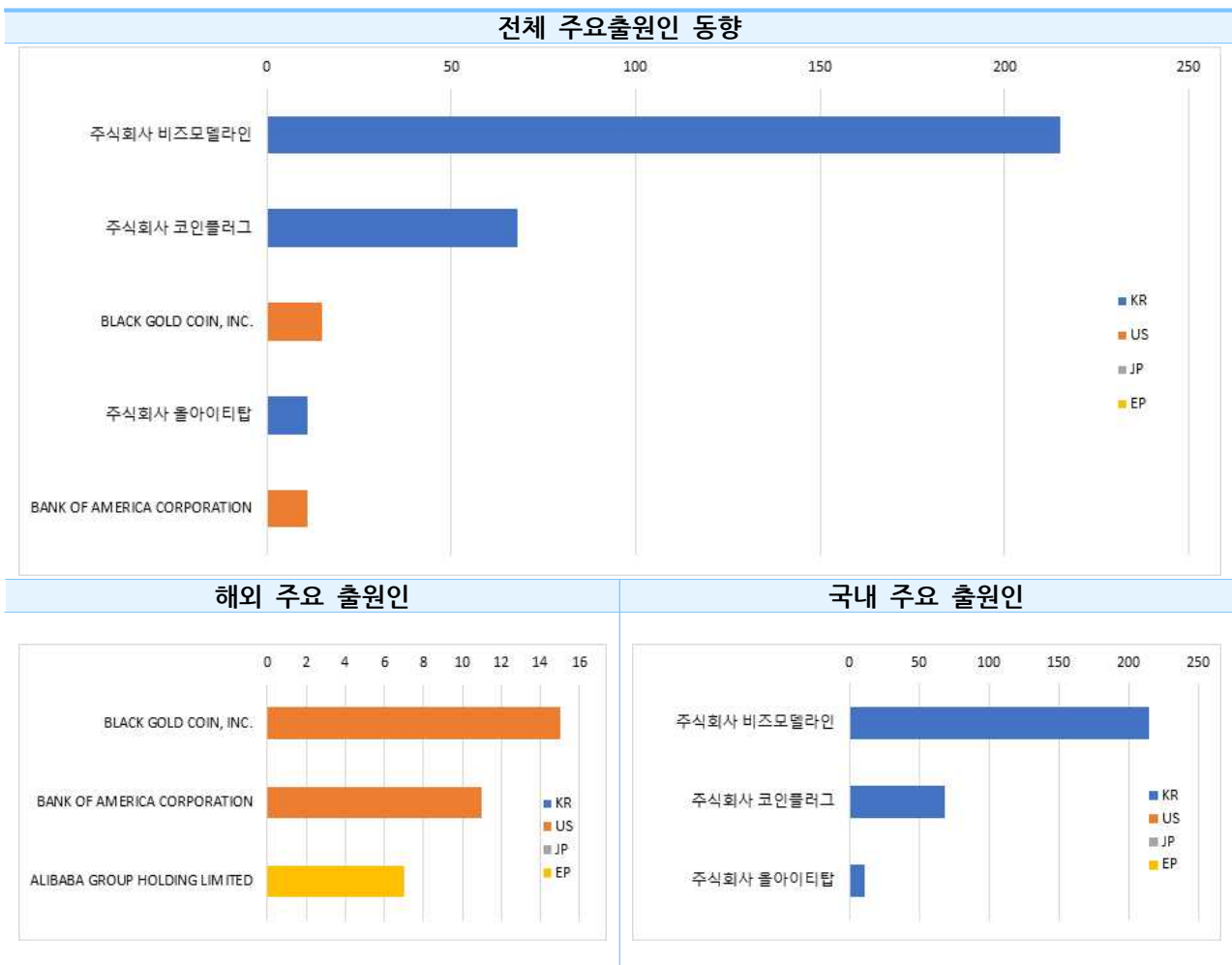
[특허 키워드 변화로 본 기술개발 동향 변화]



나. 주요 출원인 분석

- ☐ 블록체인 기반 분산 ID 및 인증 시스템의 전체 주요출원인을 살펴보면, 주로 한국 국적의 출원인이 다수 포함되어 있는 것으로 나타났으며, 제 1 출원인으로는 한국의 주식회사 비즈모델라인인 것으로 나타남
 - 제 1 출원인인 주식회사 비즈모델라인의 출원은 한국에 집중된 경향을 보임
- ☐ 블록체인 기반 분산 ID 및 인증 시스템 관련 기술로 블록체인을 다루는 대기업에 의한 출원이 대다수를 차지
 - 국내에서는 중소기업(개인)의 활발한 출원이 이루어짐

[블록체인 기반 분산 ID 및 인증 시스템 주요출원인]

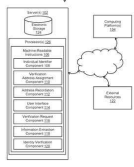
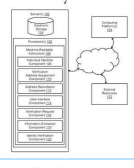
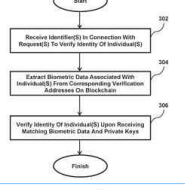
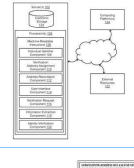



(1) 해외 주요출원인 주요 특허 분석

◎ BLACK GOLD COIN, INC.

- BLACK GOLD COIN, INC.는 미국 기업으로 다수의 블록체인 관련 특허를 보유하고 있으며, 블록체인 기반 분산 ID 및 인증 시스템 기술과 관련한 특허를 미국, 유럽, 일본에 출원
- 블록체인 기반 분산 ID 및 인증 시스템과 관련하여 20건의 출원을 진행하였으며, 그 중 등록된 특허는 7건으로 파악

[BLACK GOLD COIN, INC. 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
US10389713 (2018.09.21)	Systems and methods for providing block chain-based multifactor personal identity verification	개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록함으로써, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공	
US10298572 (2018.09.21)	Systems and methods for providing block chain-based multifactor personal identity verification	개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록함으로써, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공	
US10298571 (2018.08.21)	Systems and methods for providing block chain-based multifactor personal identity verification	하나 이상의 개인들과 연관된 생체인증 데이터를 대응하는 확인 주소들로부터 추출하고, 매칭하는 생체인증 데이터 및 개인 키들을 수신할 때 하나 이상의 개인들의 신원을 확인	
US10182051 (2018.08.14)	Systems and methods for providing block chain-based multifactor personal identity verification	개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록함으로써, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공	
US10749865 (2018.05.11)	Systems and methods for providing block chain or distributed ledger-based entity identity and relationship verification	개체 식별에 대한 블록체인/분산원장기반 검증 또는 둘 이상의 개체 간의 관계에 대한 검증이 제공	

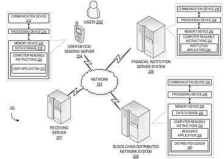

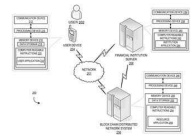
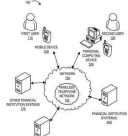
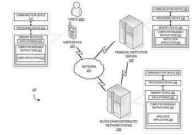
* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ BANK OF AMERICA CORPORATION

□ BANK OF AMERICA CORPORATION은 미국의 상업 은행으로 블록체인 기반 소유자 이력 관리 시스템과 관련하여, 블록 체인 분산 네트워크를 활용한 기술에 특화된 특허를 다수 출원. 그 중 등록된 특허는 6건 보유

- 주요 특허들은 시간에 따른 사용자 식별 모핑(morphing)을 추적하고 검증하기 위해 블록 체인 분산 네트워크 관련 특허를 다수 출원하는 것으로 파악

[BANK OF AMERICA CORPORATION 주요특허 리스트]

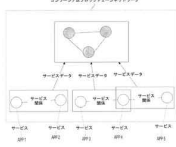
등록번호 (출원일)	명칭	기술적용분야	도면
US10735199 (2018.01.02)	File based transmission validation and failure location identification system	전송되는 파일의 각 블록에 대한 고유 해시를 생성하기 위한 암호화 해싱 함수(cryptographic hashing function)를 제공	
US9825931 (2016.02.22)	System for tracking and validation of an entity in a process data network	시간에 따른 사용자 식별 모핑(morphing)을 추적하고 검증하기 위해 블록 체인 분산 네트워크(block chain distributed network)를 생성	
US10116667 (2016.02.22)	System for conversion of an instrument from a non-secured instrument to a secured instrument in a process data network	검증된 보안 기기로서의 기기의 변환을 용이하게 하기 위한 블록 체인 분산 네트워크(block chain distributed network)를 생성	
US10679215 (2016.02.22)	System for control of device identity and usage in a process data network	데이터 네트워크에서 장치 아이덴티티(device identity) 및 사용(usage)의 제어를 위한 시스템	
US10440101 (2016.02.22)	System for external validation of private-to-public transition protocols	개인-보유 구조(private-held structure)로 배열되는 것으로부터 추적 및 검증하기 위해 블록 체인 분산 네트워크를 생성	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ ALIBABA GROUP HOLDING LIMITED

- ☐ ALIBABA GROUP HOLDING LIMITED은 중국 온라인 쇼핑물을 운영하는 기업으로, 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템과 관련하여, 블록체인을 통한 서비스 요청 기술에 특화된 특허를 다수 출원

[ALIBABA GROUP HOLDING LIMITED 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
JP6705064 (2018.07.26)	블록 체인 노드 통신 방법 및 장치	인증국(CA)에 의해서 송신된 증명서를 기억함과 동시에 CA신뢰 리스트가 사전 설정 된 서비스 노드를 포함한 블록 체인 네트워크	

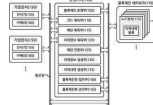
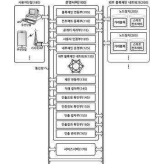
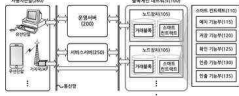
* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

(2) 국내 주요출원인 주요 특허 분석

◎ 주식회사 비즈모델라인

- 주식회사 비즈모델라인은 블록체인 기반 분산 ID 및 인증 시스템 기술에 있어서, '17년도 12월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- 주식회사 비즈모델라인은 블록체인 기반 분산 ID 및 인증 시스템에 있어서, 블록체인 기술 관련된 특허를 국내에만 특허를 215건 출원

[주식회사 비즈모델라인 주요특허 리스트]

공개번호 (출원일)	명칭	기술적용분야	도면
KR2020-0042093 (2018.10.12)	블록체인 기반 명품 유통 관리 방법	거점장치와 통신하는 운영서버 중 적어도 하나 포함하여 구현되는 시스템을 통해 블록체인 기반 명품 유통 관리 방법	
KR2019-0132159 (2018.05.18)	스마트 컨트랙트를 이용한 블록체인 기반 암호화폐 거래 플랫폼 제공 방법	스마트 컨트랙트(Smart Contract)를 지원하는 외부 블록체인 네트워크와 연동 가능한 운영서버를 통해 실행되는 방법	
KR2019-0132052 (2018.05.18)	암호화폐 거래 플랫폼을 위한 블록체인 기반 스마트 컨트랙트	스마트 컨트랙트(Smart Contract)를 지원하는 지정된 블록체인 네트워크 상에 구비된 노드장치를 통해 탈중앙화 실행 가능한 프로그램 코드	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 주식회사 코인플러그

- 주식회사 코인플러그는 한국의 블록체인을 중점으로 하는 핀테크 기업으로, 블록체인 기반 분산 ID 및 인증 시스템과 관련된 특허를 68건 출원하였으며, 68건의 특허 중 등록된 특허는 43건을 보유

[주식회사 코인플러그 주요특허 리스트]

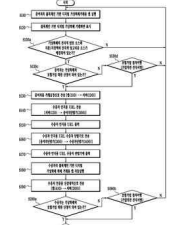
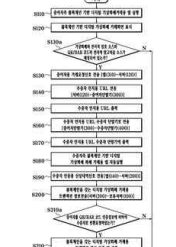
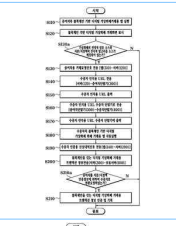
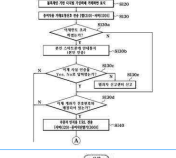
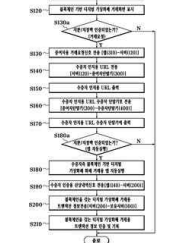
등록번호 (출원일)	명칭	기술적용분야	도면
KR2116235 (2019.03.15)	블록체인 네트워크를 이용하여 사용자의 아이디엔티티를 관리하는 방법 및 서버, 그리고, 블록체인 네트워크 기반의 사용자 아이디엔티티를 이용하여 사용자를 인증하는 방법 및 단말	블록체인 네트워크를 이용하여 사용자의 아이디엔티티를 관리하는 방법	
KR2118962 (2019.03.15)	블록체인 네트워크를 이용하여 사용자의 아이디엔티티를 관리하는 방법 및 서버, 그리고, 블록체인 네트워크 기반의 사용자 아이디엔티티를 이용하여 사용자를 인증하는 방법 및 단말	사용자 인증을 위한 각각의 사용자 아이디엔티티들에 대한 권한을 사용자 자신이 소유하여 관리하는 방법	
KR2118935 (2018.12.31)	블록체인 네트워크를 이용하여 사용자의 아이디엔티티를 관리하는 방법 및 서버, 그리고, 블록체인 네트워크 기반의 사용자 아이디엔티티를 이용하여 사용자를 인증하는 방법 및 단말	블록체인 네트워크를 이용하여 사용자 인증을 위한 각각의 사용자 아이디엔티티들에 대한 관리하는 기술	
KR2118947 (2018.12.31)	블록체인 네트워크를 이용하여 사용자의 아이디엔티티를 관리하는 방법 및 서버, 그리고, 블록체인 네트워크 기반의 사용자 아이디엔티티를 이용하여 사용자를 인증하는 방법 및 단말	블록체인 네트워크를 이용하여 사용자의 아이디엔티티를 관리하는 방법	
KR1936417 (2017.07.04)	블록체인 기반의 전자상품권을 서비스하는 방법, 이를 이용한 전자상품권 자동판매기 및 서비스 지원 서버	전자상품권 자동판매기로 하여금 발급 전자상품권을 사용자의 저장 매체에 전송하도록 지원하는 블록체인 기반의 전자상품권을 서비스하는 방법	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 주식회사 올아이티탑

- 주식회사 올아이티탑은 한국의 생체 인증을 전문으로 하는 기업으로, 블록체인 기반 분산 ID 및 인증 시스템과 관련된 특허를 11건 출원하였으며, 출원을 진행한 11건의 특허 중 8건 등록

[주식회사 올아이티탑 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
KR2112682 (2019.08.21)	보상보험에 의한 디지털 가상화폐를 생체인증신호와 연동시켜 전송하는 디지털 가상화폐의 거래방법	가상화폐 거래시의 하자에 대한 보상보험을 지급할 수 있도록 생체수단을 이용한 디지털 가상화폐를 생체인증신호와 연동시켜 전송하는 디지털 가상화폐의 거래방법	
KR2060976 (2019.02.01)	디지털 가상화폐를 qr(또는 bar)코드와 매칭시켜 전송하는 디지털 가상화폐의 전송 방법	디지털 가상화폐를 생체인증신호와 연동시켜 전송하는 디지털 가상화폐의 거래방법	
KR2024372 (2018.12.07)	디지털 가상화폐를 생체인증신호와 연동시켜 전송하는 디지털 가상화폐의 거래방법	네트워크에서 이루어진 전송기록들을 모아서 암호화시킨 블록체인(Blockchain) 구조로 화폐의 발행 주체가 없는 암호화폐(Crypto-Currency)인 비트코인(가상화폐와 동일 개념)의 거래 방법	
KR1935817 (2018.04.30)	해킹방지용 이체 사실확인 및 전화번호와 매칭된 블록체인을 갖는 디지털 가상화폐의 거래방법	당사자간 블록체인을 갖는 디지털 가상화폐의 거래시스템을 이용하여 지문 및 지정액 정보를 이용하여 당사자간에 블록체인을 갖는 디지털 가상화폐의 거래 방법	
KR1973592 (2017.12.20)	인체정보를 이용한 보안 및 해킹 방지기능을 구비하는 디지털 가상화폐의 거래방법	네트워크에서 이루어진 전송기록들을 모아서 암호화시킨 블록체인(Blockchain) 구조로 화폐의 발행 주체가 없는 암호화폐(Crypto-Currency)의 거래 방법	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

다. 기술진입장벽 분석

(1) 기술 집중력 분석

- ☐ 블록체인 기반 분산 ID 및 인증 시스템관련 기술에 대한 시장관점의 기술독점 현황분석을 위해 집중률 지수(CRn: Concentration Ratio n, 상위 n개사 특허점유율의 합) 분석 진행
- 상위 4개 기업의 시장점유율이 0.42로 블록체인 기반 분산 ID 및 인증 시스템 분야에 있어서 독과점 정도는 높은 수준으로 판단
 - 국내 시장에서 중소기업의 점유율 분석결과 0.87로 해당 기술에 대하여 중소기업이 진입하여 활동하고 있는 것으로 파악

[주요출원인의 집중력 및 국내시장 중소기업 집중력 분석]

주요출원인 집중력	주요출원인	출원건수	특허점유율	CRn	n
	주식회사 비즈모델라인(한국)	215	29.1%	0.29	1
	주식회사 코인플러그(한국)	68	9.2%	0.38	2
	BLACK GOLD COIN, INC.(미국)	15	2.0%	0.40	3
	주식회사 올아이티탑(한국)	11	1.5%	0.42	4
	BANK OF AMERICA CORPORATION(미국)	11	1.5%	0.43	5
	인포뱅크 주식회사(한국)	8	1.1%	0.44	6
	ALIBABA GROUP HOLDING LIMITED(중국)	7	0.9%	0.45	7
	주식회사 바스랩(한국)	6	0.8%	0.46	8
	한국전자통신연구원(한국)	6	0.8%	0.47	9
	삼성전자주식회사(한국)	6	0.8%	0.48	10
	전체	739	100%	CR4=0.42	
국내시장 중소기업 집중력	출원인 구분	출원건수	특허점유율	CRn	n
	중소기업(개인)	488	87.3%	0.87	
	대기업	32	5.7%		
	연구기관/대학	39	7.0%		
	전체	559	100%	CR중소기업=0.87	

(2) 특허소송 현황 분석

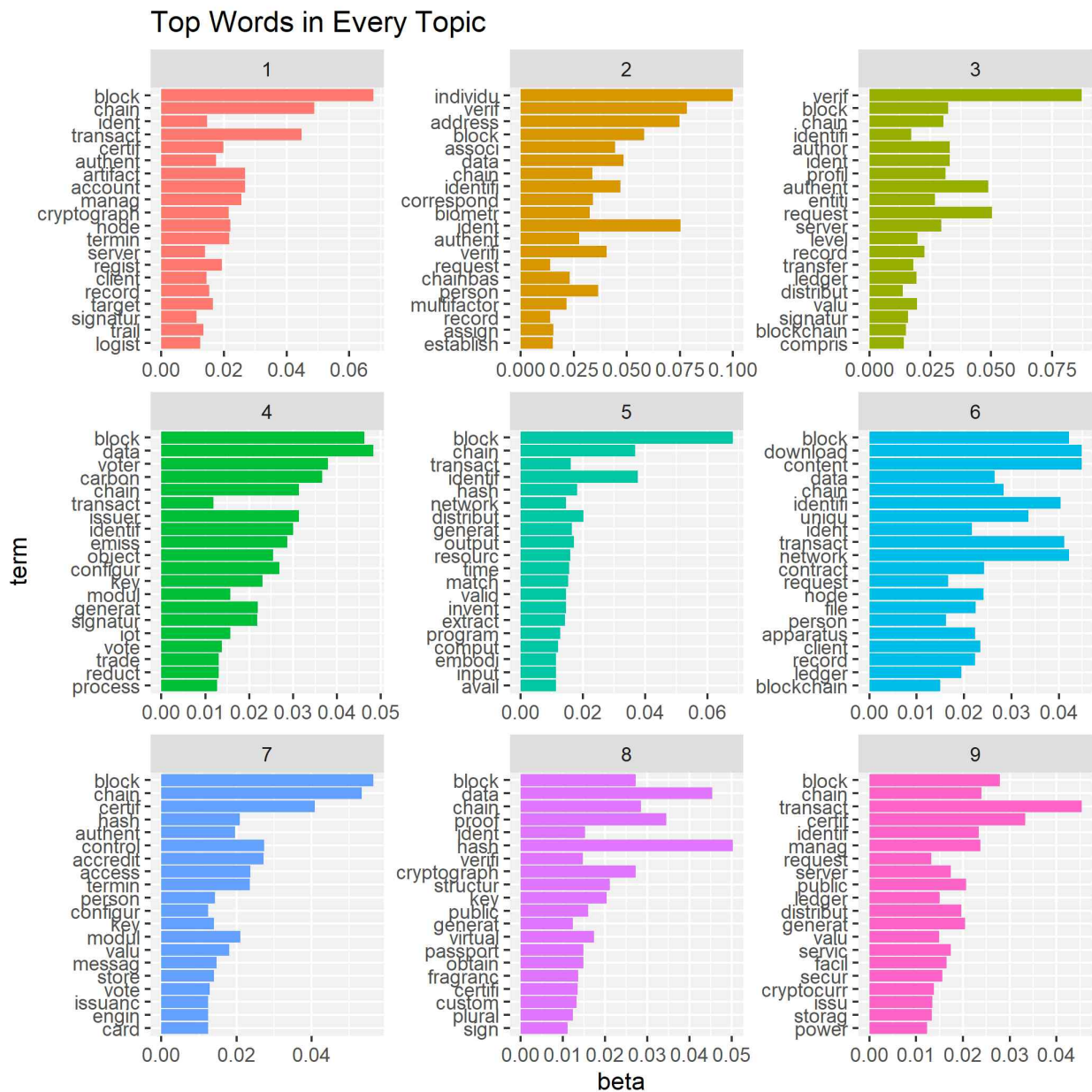
- ☐ 블록체인 기반 분산 ID 및 인증 시스템 분야 관련 특허소송 이력은 검색되지 않음
 - 따라서 국내기업이 미국시장에 진입하는 경우, 해당 분야를 선점할 수 있을 것으로 판단
 - 다만, 블록체인과 관련해서는 4개의 소송이 검색

5. 요소기술 도출

가. 특허 기반 토픽 도출

- 113개의 특허의 내용을 분석하여 구성 성분이 유사한 것끼리 클러스터링을 시도하여 대표성이 있는 토픽을 도출

[블록체인 기반 분산 ID 및 인증 시스템에 대한 토픽 클러스터링 결과]



나. LDA¹⁵⁾ 클러스터링 기반 요소기술 도출

[LDA 클러스터링 기반 요소기술 키워드 도출]

No.	상위 키워드	대표적 관련 특허	요소기술 후보
클러스터 01	block, chain, transact, artifact, account, manage, node, terminal, cryptograph, certify	<ul style="list-style-type: none"> • Server, vehicle, distributed transaction certification system, and distributed transaction certification method • Article information management apparatus, system, method and program 	블록체인 기반 신원인증 서비스 기술
클러스터 02	individual, verify, identify, address, block, data, identification, association, verification, personal	<ul style="list-style-type: none"> • Systems and methods for realizing block chain-based multifactor personal identity verification • Secure processing of an authorization verification request 	블록체인 기반 신원인증 서비스 기술
클러스터 03	verify, request, authentication, authority, identify, block, profile, chain, server, entity	<ul style="list-style-type: none"> • A distributed user profile identity verification system for e-commerce transaction security • Authority authentication method for block chain infrastructure, terminal, and server using the same 	블록체인 인프라 기술
클러스터 04	carbon, download, emission, verify, vote, block, artifact, content, transact, account	<ul style="list-style-type: none"> • Blockchain-based carbon trading system • Blockchain electronic voting system and method 	블록체인 암호키 관리 서비스 기술
클러스터 05	block, identify, chain, distribute, hash, output, generate, transact, resource, time	<ul style="list-style-type: none"> • History management method, history management device, and history management system • Cryptographic asic for derivative key hierarchy 	블록체인 기반 신원인증 서비스 기술 블록체인 암호키 관리 서비스 기술
클러스터 06	download, content, block, network, transact, identification, unique, chain, data, contract	<ul style="list-style-type: none"> • Method and system for distributing digital content in peer-to-peer network • Blockchain smart contract verification method and apparatus, and storage medium 	네트워크 기술 사용자 데이터 관리 기술
클러스터 07	block, chain, certify, control, accredit, access, terminal, module, hash, authentication	<ul style="list-style-type: none"> • Accredited certificate issuance system based on block chain and accredited certificate issuance method based on block chain using same, and accredited certificate authentication system based on block chain and accredited certificate authentication method based on block chain using same • Cryptographic asic for derivative key hierarchy 	대용량 신원정보 저장 및 검증 기술 블록체인 암호키 관리 서비스 기술
클러스터 08	hash, data, proof, chain, block, cryptograph, structure, key, virtual, public	<ul style="list-style-type: none"> • Method for establishing, securing and transferring computer readable information using peer-to-peer public and private key cryptography 	블록체인 암호키 관리 서비스 기술
클러스터 09	transact, certify, block, chain, manage, identification, public, generate, distribute, server	<ul style="list-style-type: none"> • Certificate management device and certificate management method • Custody support system and custody support method 	블록체인 기반 신원인증 서비스 기술

15) Latent Dirichlet Allocation

다. 특허 분류체계 기반 요소기술 도출

- 블록체인 기반 분산 ID 및 인증 시스템 관련 특허에서 총 10개의 주요 IPC코드(메인그룹)를 산출하였으며, 각 그룹의 정의를 기반으로 요소기술 키워드를 아래와 같이 도출

[IPC 분류체계에 기반한 요소기술 도출]

IPC 기술트리		
(서브클래스) 내용	(메인그룹) 내용	요소기술 후보
(G06F) 전기에 의한 디지털 데이터처리	• (G06F-021) 부정행위로부터 프로그램 또는 데이터, 그 컴퓨터 부품을 보호하기 위한 보안 장치	-
(G06Q) 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 데이터 처리 시스템 또는 방법; 그 밖에 분류되지 않는 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 시스템 또는 방법	• (G06Q-030) 거래, 예. 쇼핑 또는 전자상거래	-
	• (G06Q-050) 특정 사업 부문에 특히 적합한 시스템 또는 방법, 예. 공익사업 또는 관광	-
	• (G06Q-040) 금융; 보험; 세무 전략; 법인세 또는 소득세의 처리	-
	• (G06Q-020) 지불 체계, 방식 또는 프로토콜	-
	• (G06Q-010) 경영; 관리	-
(G07C) 시간이나 출석자의 등록; 기계가동의 등록이나 표시; 난수의 발생; 투표 또는 추첨장치; 다른 개소에 속하지 않는 검사를 위한 배열, 방식 또는 장치	• (G07C-009) 개개의 출입을 등록하는 것	대용량 신원정보 저장 및 검증 기술, 블록체인 기반 신원인증 서비스 기술
(H04L) 디지털 정보의 전송, 예. 전신통신	• (H04L-009) 비밀 또는 보안통신을 위한 배치	-
	• (H04L-029) 그룹 1/00에서 H04L 27/00의 하나에도 포함되지 않는 배치, 장치회로 또는 시스템	-
(H04W) 무선통신네트워크	• (H04W-012) 보안 장치, 예. 접속 보안 또는 부정 검출; 인증, 예. 사용자 신원 또는 권한 검증; 프라이버시 또는 익명성 보호	사용자 데이터 관리 기술

라. 최종 요소기술 도출

- ☐ 산업·시장 분석, 기술(특허)분석, 전문가 의견, 타부처 로드맵, 중소기업 기술수요를 바탕으로 로드맵 기획을 위하여 요소기술 도출
- ☐ 요소기술을 대상으로 전문가를 통해 기술의 범위, 요소기술 간 중복성 등을 조정·검토하여 최종 요소기술명 확정

[블록체인 기반 분산 ID 및 인증 시스템 분야 요소기술 도출]

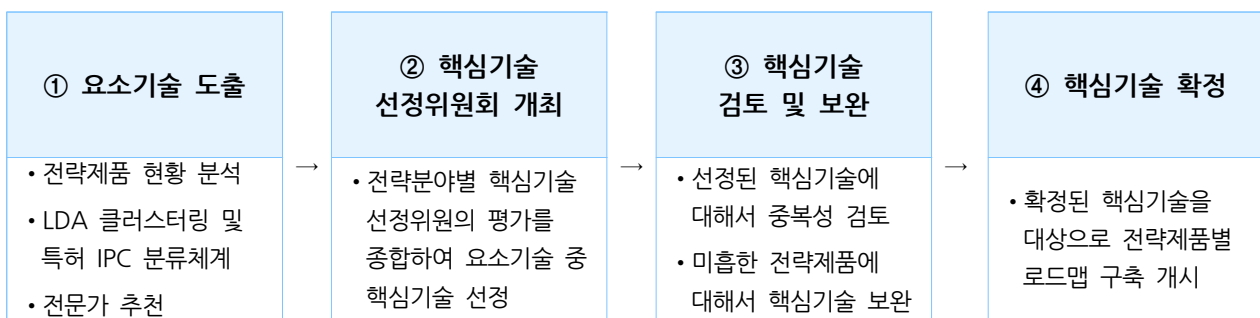
요소기술	출처
DID Document 표준화 및 API 연동기술	전문가추천
대용량 신원정보 저장 및 검증 기술	특허 클러스터링, IPC 기술체계, 전문가추천
블록체인 기반 신원인증 서비스 기술	특허 클러스터링, IPC 기술체계, 전문가추천
블록체인 암호키 관리 기술	전문가추천
선택적 신원 정보 기술	전문가추천
블록체인 암호키 관리 서비스 기술	특허 클러스터링, 전문가추천
고속화된 블록체인 데이터 처리 기술	전문가추천
블록체인 합의 알고리즘 고도화 기술	전문가추천
사용자 데이터 관리 기술	IPC 기술체계, 전문가추천
블록체인 인프라 기술	특허 클러스터링, 전문가추천
네트워크 기술	전문가추천

6. 전략제품 기술로드맵

가. 핵심기술 선정 절차

- ☐ 특허 분석을 통한 요소기술과 기술수요와 각종 문헌을 기반으로 한 요소기술, 전문가 추천 요소기술을 종합하여 요소기술을 도출한 후, 핵심기술 선정위원회의 평가과정 및 검토/보완을 거쳐 핵심기술 확정
- ☐ 핵심기술 선정 지표: 기술개발 시급성, 기술개발 파급성, 기술의 중요성 및 중소기업 적합성
 - 장기로드맵 전략제품의 경우, 기술개발 파급성 지표를 중장기 기술개발 파급성으로 대체

[핵심기술 선정 프로세스]



나. 핵심기술 리스트

[블록체인 기반 분산 ID 및 인증 시스템 분야 핵심기술]

핵심기술	개요
DID Document 표준화 및 API 연동기술	• 중앙 신뢰기관 없이도 신뢰할 수 있는 개체 식별 정보를 제공하는 분산 식별자의 데이터 포맷 및 구조, 검색(discovery) 등에 대한 표준화 연동 기술
대용량 신원정보 저장 및 검증 기술	• 블록체인 기반 ID 시스템을 통해 관리되는 대용량 신원정보의 안전한 저장 및 신원정보의 유효성/무결성에 대한 고속 검증 기술
블록체인 기반 신원 인증 서비스 기술	• 블록체인 기반 ID 시스템을 통해 관리되는 사용자 신원정보(ID)를 통해 사용자의 신원을 확인하는 서비스 기술
블록체인 암호키 관리 기술	• 블록체인 서비스 및 사용자 인증에 필요한 암호키를 안전하게 생성/분배 및 관리하는 기술
선택적 신원 정보 기술	• 사용자가 서비스에 제공되는 신원정보를 선택적으로 제공하는 기술






다. 중소기업 기술개발 전략

- ☐ DID 특허 활성화를 위한 중소기업 산업 표준 아이템 도출 전략 제시 필요
- ☐ 자주적 신원관리 표준을 위한 '증명 가능 주장'에 대한 기술개발 진행 독려
- ☐ DID는 블록체인 표준화 중에서도 선결과제로 주목되고 있는 관계로 중소기업이 대기업, 정부, DID 협회 관련 프로젝트에 참여할 수 있도록 지원하는 전략 필요

라. 기술개발 로드맵

(1) 중기 기술개발 로드맵

[블록체인 기반 분산 ID 및 인증 시스템 분야 중기 기술개발 로드맵]

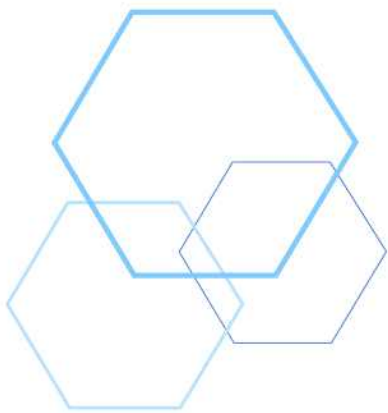
블록체인 기반 분산 ID 및 인증 시스템	사용자 스스로 자신의 신원 정보를 관리 및 통제할 수 있는 새로운 인증체계 개발			
	2021년	2022년	2023년	최종 목표
DID Document 표준화 및 API 연동기술				글로벌 연동 DID 문서 생성/등록 검색 서비스 제공
대용량 신원정보 저장 및 검증 기술				실시간 대용량 신원정보 관리 및 검증 서비스 상용화
블록체인 기반 신원 인증 서비스 기술				멀티 패턴 기반 사용자 신원 인증 Prototype 개발
블록체인 암호키 관리 기술				암호키 유출 방지 및 손망실 대비 백업/복구 지원
선택적 신원 정보 기술				암호학적으로 안전성이 검증된 신원정보 노출 최소화

(2) 기술개발 목표

- ☐ 최종 중소기업 기술로드맵은 기술/시장 니즈, 연차별 개발계획, 최종목표 등을 제시함으로써 중소기업의 기술개발 방향성을 제시

[블록체인 기반 분산 ID 및 인증 시스템 분야 핵심요소기술 연구목표]

핵심기술	기술요구사항	연차별 개발목표			최종목표	연계R&D 유형
		1차년도	2차년도	3차년도		
DID Document 표준화 및 API 연동기술	SSO Framework	Framework 기획	설계	PoC	이종 블록체인 간 연동	산학연
	표준준용 DID 연동기술 확보	DID문서 생성 및 등록	DID 문서 검색	DID 연동 API	글로벌 연동 DID 문서 생성/등록 검색 서비스 제공	상용화
대용량 신원정보 저장 및 검증 기술	DHT	설계 및 구현	테스트	상용화	분산환경에서의 상용화	산학연
	대용량 신원정보의 빠른 검색/검증	100만명 수준 신원정보 저장 및 검증 기술 설계	10만 명 대상 (1초 이내)	100만명 대상(1초 이내)	실시간 서비스가 가능한 대용량 신원정보 관리 및 검증	기술혁신
블록체인 기반 신원 인증 서비스 기술	FIDO/PUFF/Digital Signature	설계	구현	PoC	Prototype 개발	산학연
	보안성 강화를 위한 다양한 인증수단 확보	공개키 기반 신원 인증	바이오 기반 신원 인증	행위 패턴 기반 신원 인증	멀티 패턴 기반 사용자 신원 인증	상용화
블록체인 암호키 관리 기술	Multisig	설계	구현	상용화	DID 활용 상용화	산학연
	암호키의 안전한 사용 및 백업	HW기반 안전한 암호키 저장/사용	손망실 대비 백업/복구 기능 설계	손망실 대비 백업/복구 기능 개발	암호키 유출 방지 및 손망실 대비 백업/복구 지원	산학연
선택적 신원 정보 기술	ZKP	설계	구현	PoC	Prototype 개발	산학연
	사용자 프라이버시 강화	사용자 정책 기반 신원정보 노출	영지식 증명 기반 자격 증명	영지식 증명 기반 자격 증명 실용화 (1초 이내)	암호학적으로 안전성이 검증된 신원정보 노출 최소화	산학연



전략제품 현황분석

블록체인 기반 소유자 이력 관리 시스템



블록체인 기반 소유자 이력 관리 시스템

정의 및 범위

- 디지털 자산의 투명성, 신뢰성 및 제고를 위한 공적 가시성 확보를 위해 디지털 자산이 블록체인 네트워크에서 이동할 때 그 소유권의 전부 혹은 일부가 변경된 이력을 탐지, 추적 및 관리할 수 있는 시스템
- 블록체인 기반 소유자 이력관리 시스템은 신원의 부여 및 인증, 개인키 관리를 포함하는 사용자 지갑, 그리고 자산의 이동이나 거래 이벤트의 탐지 및 추적, 그리고 이를 위한 정책을 수행하기 위한 관리 시스템을 포함, 한 걸음 더 나아가 자산 이동경로를 예상할 수 있는 예측 기술까지 포함

전략 제품 관련 동향

시장 현황 및 전망	제품 산업 특징
<ul style="list-style-type: none"> • (세계) 블록체인 기반 소매 및 전자상거래 세계 시장규모는 '18년 1.5억 달러에서 연평균 성장률 69% 성장하여 '24년 34억 달러 규모에 이를 것으로 전망 • (국내) 블록체인 기반 자동차 거래 국내 시장규모는 '18년 48억 원에서 연평균 성장률 64% 성장하여 '24년 1,110억 원 규모에 이를 것으로 전망 	<ul style="list-style-type: none"> • 각국에서 토자주택차량관리, 선거투표관리, 의료정보관리 등 다양한 공공서비스 영역 블록체인 기술 적용 작업 진행 • 블록체인 인증서비스를 통한 작품출처 정확성과 거래의 투명성 확보 가능한 문화 콘텐츠 산업으로의 확산 • 블록체인 기반 건강 데이터 저장 방식을 통한 의료산업의 확장 • 자동차 업계의 산업적 특성상 많은 이해관계자들에게 공유할 수 있는 데이터 제공을 위한 블록체인 기술 응용
정책 동향	기술 동향
<ul style="list-style-type: none"> • 과기 정통부는 '블록체인 기술발전전략'을 발표(2018.6), 이에 따라 시범사업 12건 선정 하였으며(2018.12), 이중 가능성이 높은 3개 컨소시엄을 선정, 민간 주도 국민프로젝트로 추진(2019. 3) • 환경부 및 농림축산부 등에서 관련 사업 발주 	<ul style="list-style-type: none"> • 금융, 부동산, 법인, 의료 등 소유권과 관련있는 기록들의 블록체인 기술 이용한 분산 원장 기술 개발 • 블록체인의 기술 수준. 시장은 아직은 초기 단계, 국가 간 기술 격차가 크지 않고, 아직 주목할 만한 성공사례가 없는 신기술 분야 • 전 세계 물류 · 유통 · 의료를 담당하고 있는 글로벌 해운회사들도 블록체인 기술의 활용에 참여
핵심 플레이어	핵심기술
<ul style="list-style-type: none"> • (해외) ,Blockai, Lamborghini, MicroSoft, SelKey, IBM, Walmart, Nestle • (대기업) 삼성전자, 삼성 SDS, LG, 카카오, 네이버 • (중소기업) 비주얼넷, 페이지트, 스마트코어, 열매컴퍼니, ARTBLOC, 위메이드트리 	<ul style="list-style-type: none"> • 실물/디지털 자산에 대한 소유권자 등록 기술 • 공적 가시성을 위한 거래내역 추적 기술 • 실물-디지털 정보 매핑 기술 • 불법 취득 자산 탐지 기술 • 부정 거래 탐지 기술

중소기업 기술개발 전략

- 정부의 블록체인 기술 개발을 위한 R&D 지원 및 투자 정책을 활용
- 대기업 및 금융회사들의 블록체인 기술 수요에 따라 협업이나 컨소시엄 구성
- 해외 스타트업들과의 협업을 통해 지속적이고 선제적인 기술 개발 수행

1. 개요

가. 정의 및 필요성

(1) 정의

- ☐ 디지털 자산의 투명성, 신뢰성 및 제고를 위한 공적 가시성 확보를 위해 디지털 자산이 블록체인 네트워크에서 이동할 때 그 소유권의 전부 혹은 일부가 변경된 이력을 탐지, 추적 및 관리할 수 있는 시스템
 - 디지털 자산이란, 개인, 기업 또는 공공기관에서 생산·수집한 문서, 그림, 사진, 동영상, 사운드 및 신호나 상품 등을 비롯하여 자산화의 가치가 있는 디지털 자료
 - 블록체인 네트워크는 암호화에 기초한 개인키(Private key)와 공개키(Public key) 및 이 키에서 생성된 지갑의 주소를 사용하여 디지털 자산의 거래 및 이동이 이루어짐
 - 주소의 소유자와 디지털 자산의 관계는 블록체인 특징의 하나인 주소의 익명성에 의해 보호되나, 불법 및 탈법 사례의 증가로 익명성을 최대한 보장하면서 디지털 자산에 대한 소유권을 인증할 수 있는 기술들이 출현하여 구현되고 있으나 아직은 일반화되어 있지는 않음
- ☐ 블록체인 기반 소유자 이력관리 시스템은 신원의 부여 및 인증, 개인키 관리를 포함하는 사용자 지갑, 그리고 자산의 이동이나 거래 이벤트의 탐지 및 추적, 그리고 이를 뒷받침하는 정책의 수립 및 수행을 지원하는 관리 시스템을 포함
 - 블록체인 상에서 주소에 기반한 소유자 이력관리는 이 업무 프로세스의 시작점인 신원의 부여 및 인증, 자산의 이동이나 거래 이벤트의 탐지, 그리고 이러한 정보들에 대한 저장, 처리, 공유 등의 관리 시스템을 포함하며 이러한 것들이 정책적으로 수립되어 수행되어야 함
 - 자산의 다양성 및 익명성으로 인해 소유권의 이동을 탐지하고 추적하기 위한 신원의 부여 및 인증 기술, 실제 이벤트 발생 시 이를 탐지하는 기술과 추적하여 계량화 및 시각화하는 기술, 그리고 이력을 추적하는 목적, 범위 및 결과물의 제공 방안 등을 정책으로 수립하고 반영할 수 있는 기술 필요

(2) 필요성

- 중개자가 필요 없이 참여자 모두가 동등한 권한을 가지고 여러 가지 다양한 인센티브에 따라 자발적으로 네트워크에 참여함으로써 민주적인 의사결정에 의한 운영이 가능
 - 중개자들은 장부를 소유한 기관이나 개인으로서 네트워크 운영을 독점하게 되고, 문지기의 역할을 하게 됨으로써 참여자의 자유로운 참가 및 탈퇴를 제한하게 되어 결국 다양한 비즈니스 창출과 아이디어의 사업화를 위한 구현에 장애물로 작용
 - 블록체인은 참여자 모두가 동등한 권한을 가지고 의사결정 과정에 참여할 수 있고 다양한 인센티브에 따라 자발적으로 참여함으로써 중개자에 대한 수수료 지불이나 권한에 지배 받지 않고 자유로운 사업 운영 및 영위 가능
- 2017년 하반기부터 전 세계적으로 일어났던 암호화폐 시장의 급격한 팽창을 필두로 가상세계에서 블록체인을 기반으로 한 탈중앙화된 경제생태계 구축이 2018년 말부터 안정세에 접어들었으나, 각종 보안 위협으로 인한 손실이 급증
 - 이후 암호화폐시장은 급락과 반등을 거듭하면서 2018년 말부터 안정세에 접어들었고 각국 정부와 기관들을 중심으로 블록체인의 장점을 현실세계에 활용하고자 하는 노력들이 나타나기 시작
 - 금융 분야에서는 은행 및 기존 금융회사들의 계좌를 암호화폐 거래소의 계좌와 연동시키는 방법으로 블록체인 기반 시스템과 현실세계를 매핑 시킴으로 거래내역 및 소유자 이력을 관리
 - 하지만, 3년(2015년~2018년) 간 해킹으로 인한 암호화폐 피해가 1,121억 원에 달하는 등 블록체인 생태계를 위협하는 사건들이 지속적으로 발생
- 블록체인의 익명성은 매우 긍정적인 효과가 있는 반면, 범죄나 오남용과 같은 부정적인 측면에 대한 예방이나 조치를 위해서는 신원의 부여 및 인증을 포함하여 소유자 및 거래 이력 관리를 위한 대한 심도 있는 연구 개발 필요
 - 비트코인 등 암호화폐와 연관된 블록체인 네트워크에서 해마다 다수의 해킹 및 범죄와 연관된 행위들이 적발되었고, 이에 따른 피해자들의 발생뿐 아니라, 사회적으로 물의를 일으킴으로써 산업 발전에 저해요소로 작용
 - 신원이 익명성에 의해 보호되면서도 범죄와 같은 공공에 대한 해악에 대해서는 조치가 가능한 신원체계가 요구
- 유통 및 물류 분야에서의 필요성
 - 현재 SCM은 근본적으로 국가 간에 무역거래에서 발생하는 복잡성에 기인한 문제를 안고 있음
 - 수많은 단계별로 다양하고 제 각기 역할을 하는 공급자가 있고 공급자끼리 수많은 문서를 주고받아야 하며 국가 간에 각 공급자끼리도 서로 다른 양식과 다른 의미의 같은 용어를 사용하기도 함
 - 이 같은 복잡성으로 인해 SCM은 지금까지도 비용절감, 제품 품질, 신속성에 관한 이슈가 늘 존재. 블록체인 기술의 도입으로 기존의 SCM에서 야기되어왔던 문제점 해결이 가능

나. 범위 및 분류

(1) 가치사슬

- ☐ 제4차 산업혁명을 위한 ‘초연결 사회’ 및 ‘초지능 사회’는 기존의 진입 위한 기반기술로서 각종 기술들이 각각의 역할에 따라 전반적인 산업구조의 개편을 초래할 것으로 예상
 - 향후 제4차 산업혁명의 전개과정에서 나타날 산업구조의 변화는 명확하게 예측하기 쉽지 않으나, 혁신적 선도기업들이 추진하고 있는 가치사슬 상의 혁신과 생산방식의 변화, 더 나아가 비즈니스모델의 혁신 예상
 - 센서와 초고속통신 기반의 사물인터넷과 빅데이터, 클라우드 컴퓨팅과 인공지능 등 지능정보기술의 적용과 확산으로 사람과 사람, 제품과 서비스, 기계와 기계의 상호연결성이 강화됨으로써 초연결성과 초지능화의 확산에 따른 제품과 서비스의 스마트와 및 시스템화
 - 제4차 산업혁명의 전개과정에서 지능정보기술 기반의 디지털화가 급속히 진전되면서 일상의 모든 영역이 끊임없이 상호 연결되며, 네트워크화된 자원들의 의존도가 점차 심화될 것으로 예상
- ☐ 블록체인은 일반적인 산업의 구조 관점에서 보면 전형적인 기반기술인 후방산업으로서의 성격이 짙으나, ‘고객의 접점 장악’과 ‘고객 점유율 극대화’라는 목표가 중요한 디지털 산업의 특성상 전방산업의 역할도 수행 가능

[블록체인 소유자 이력관리 시스템 분야 산업구조]

후방산업	블록체인 소유자 이력관리 시스템 기술 분야	전방산업
암호화기술, 디지털 신원 기술, 자기주관 신원기술, 디지털 서명, 개방형 자산 프로토콜, 권한/인증 부여 기술	실물/디지털 자산에 대한 소유권자 등록 기술 실물/디지털 정보 매핑 기술 소유권 이전 이벤트 처리 기술 불법 취득 자산 탐지 기술 부정거래 탐지 기술 참여자 권한 설정 기술	금융거래 및 서비스, 디지털 자산관리, 공공 기록관리, 헬스케어, 생산/물류정보 공유 및 관리, 암호화폐

(2) 용도별 분류

- 블록체인 소유자 이력관리 시스템은 농축산물 등의 유통 이력 관리에 사용 중. 블록체인을 이용한 소유자 이력관리 시스템은 축산물뿐 아니라 사회 전반에 있어 소유 여부에 관한 등록이 요구되는 모든 사물에 적용 가능
 - 일례로, 차량의 소유권 이전에 블록체인이 접목 가능. 차량의 소유권을 판매자에서 구매자로 넘기는 작업은 절차가 복잡
- 공급망 관리/SCM/유통 이력 관리/중고 거래/부동산 소유 이력 관리/전력, 탄소 배출권 등 무형 권리에 대한 소유 이력 관리
 - 공급망 관리 관점에서도 블록체인이 접목되면 효과적일 수 있음
 - 예를 들어, 자동차 업계의 경우 자동차 제조사 입장에서는 단순히 차량 생산과 판매뿐만이 아니라 차량 제조부터 폐차까지 전 주기를 관리하고 싶어함. 경쟁이 치열해짐에 따라 고객의 구매 주기에 맞춰 적재적소에 차량을 공급해야 하는 상황이 벌어지고 있기 때문. 따라서, 아래와 같이 블록체인이 활용 가능
 - 차량 부품 추적과 비교: 엄청나게 많은 자동차 부품을 추적하고 비교하는 작업을 블록체인을 사용해 공유 원장에 기록할 경우 많은 부분이 개선 가능
 - 공급망과 비즈니스 프로세스 간소화: 1, 2, 3차로 구분되는 여러 협력업체 사이의 정보 교환 과정에서 블록체인을 활용할 경우 프로세스 간소화가 가능
 - 차량 인도부터 폐차에 이르는 전 주기 이력 관리(공장에서 차량 출고 → 선적 → 수출 세관 통과 → 목적지 국가 도착 → 수입 세관 통과 → 분배 센터 입고 → 대리점 인도 → 고객에게 인도 → (점검을 위해) 서비스 센터 입고): 각 단계마다 블록체인을 활용해 거래 이력을 만들면 한 곳에서 차량의 상태를 일목요연하게 확인이 가능

2. 산업 및 시장 분석

가. 산업 분석

◎ 블록체인을 활용한 문화 콘텐츠 및 의료산업

□ 블록체인 기반의 콘텐츠 인증서비스 통해 작품출처 정확성과 거래의 투명성 확보 가능

- 블록체인 기술을 통해 소유자들의 이력을 포함한 모든 거래 내역을 기록할 수 있기 때문에 소유권에 대한 추적을 가능
- 미술, 음악 등 예술작품의 인증에 블록체인 기술을 이용하면 작품의 출처파악이 쉽고 사용이 투명하게 이루어지게 되므로 불법적인 복제와 유통 미연 방지 가능

□ 미국 보건복지부(HHS) 산하 기관인 ONC HIT(The Office of the National Coordinator for Health Information Technology)는 블록체인을 이용해 의료 정보를 보호, 관리, 교환할 수 있는 방법에 대한 아이디어를 공모하는 'Blockchain Challenge' 진행

- 건강 데이터가 암호화되어 사용자의 고유 식별표식과 함께 데이터 호수(Data Lake)에 저장되어 자신의 데이터에 대한 접근 권한을 가진 사용자가 블록체인 기술을 통해 데이터를 공유
- ONC HIT에서는 오픈소스 분산원장 기술과 건강 관련 표준을 활용하여 3가지 트랙 중 하나를 해결하는 'Blockchain in Healthcare Code-A-Thon' 진행

[건강 데이터의 저장 방식]



* 출처 : 소프트웨어 정책연구소(2017), p.25

◎ 블록체인을 결합한 스마트 물류 산업

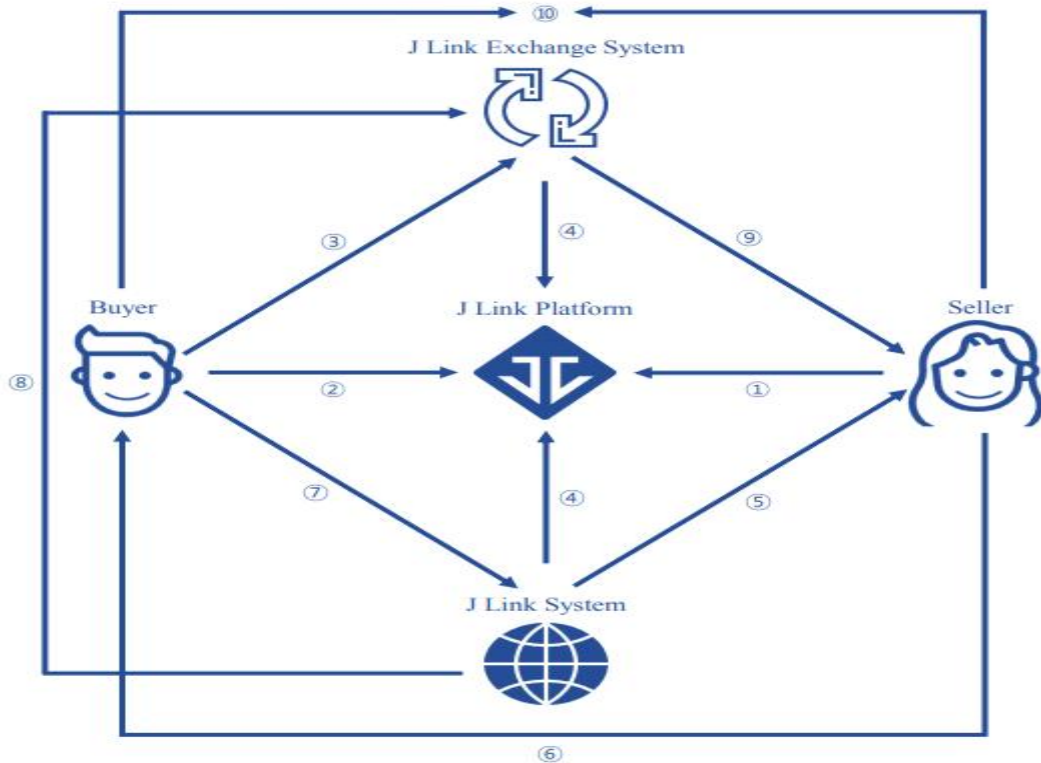
- ☐ SCM(공급사슬관리)와 ERP(전사적자원관리)는 블록체인 플랫폼 위에서 구동될 것으로 예상
 - 물류산업에서 시스템으로 관리되지 못하는 부분이 많았으나, 클라우드의 경우 단일 기업이 클라우드 소유하게 되면 종속에 대한 우려 때문에 다른 기업과 연동이 어려움
 - 세계 최대 특송 회사인 UPS에 이어 FedEx가 블록체인운송연맹(BiTA)에 가입하며 본격적으로 블록체인 기술을 개발
 - 블록체인 도입을 통하여 향상되는 점은 신뢰성과 필수 서류에 대한 상호 공유. 대부분의 기업들은 전사적으로 SCM을 운영하고 있으며 SCM 데이터는 다수 있지만 활용하지 못하는 경우가 대부분
 - 블록체인 기술을 도입하면 사람이 직접 데이터를 저장하는 것이 아니라 블록체인 내 프로토콜을 통하여 저장되므로 끊임없이 신뢰성 있는 데이터가 생성. 블록체인 기술은 중앙이 아니라 다수가 저장하므로 허위 조작이 거의 불가능하여 신뢰성 또한 확보
- ☐ 해운 및 물류 분야에서는 실시간 물류 추적 및 관리 자동화를 통한 혁신이 가능할 것으로 예상
 - 다양한 이해관계들이 함께 참여하는 블록체인을 통해 실시간 추적성 확보, 재고 관리 최적화, 진품 확인 등 유통 선진화
 - 관세청은 ‘더 빠른 직구’, 신속하게 처리하고 허위 신고도 예방하는 개인 통관 시스템을 개발 중(2018)
 - 전자상거래 통관은 쇼핑몰→특송업체→관세청 순으로 진행되며, 3,300만개(’17)에 이르는 수입 물품 신고(특송업체) · 확인(관세청) 과정에 건당 12시간 이상 소요됨. 블록체인 기술을 접목하여, 통관 관련 정보를 쇼핑몰, 특송업체, 관세청이 공유하면 실시간 수입 신고가 가능하고 저가 신고도 방지
- ☐ 식품안전이력관리 사업은 식품 유통분야에 블록체인을 적용함으로써 농축산물 및 식자재, 가공식품 유통 관리의 투명성을 확보할 수 있어 주목받고 있는 사업분야로, 블록체인을 접목한 시도가 늘어나는 추세

◎ 블록체인을 활용한 거래산업

- ☐ 의류, 차량 분야 등의 명품 브랜드에서 자사 관련 제품의 중고거래 등을 관리하기 위한 기술로써도 활용되는 추세
 - 람보르기니는 중고차 시장에서 매매되는 자사 차량의 정품 여부를 확인하기 위해 세일즈 포스(Salesforce)의 기업형 블록체인 플랫폼을 활용해 차량 이력을 추적·관리할 계획
 - 마스터카드(MasterCard)는 여성 명품 디자이너들의 한정판 의류 제품들에 대한 이력 추적 서비스를 선보임
 - 마스터카드의 제품 이력 추적 플랫폼의 이름은 프루브넌스(Provenance)이며, 이는 고객에게 제품이 매장에 진열되기까지의 생산, 유통 과정을 모두 보여줌

- ☐ J-Link를 통한 중고거래는 중고거래를 원하는 사람들을 국적과 지역에 상관없이 이어줄 수 있으며, 비용 지불을 J-Link를 통해서 결제 가능

[J-Link 중고거래 구조]



* 출처 : Steemit, 제어링크(J-Link, JLC) - 블록체인 중고거래 시장

- ☐ 미술품 수집 및 거래 시장에서도 블록체인을 이용한 공동소유 및 거래 플랫폼 시도 중

- 블록체인은 분절화된 예술 소유권을 가능하게 하고, 제 3자 중개자의 필요성을 줄이고, 지적 재산권을 보호하고 위조 방지에 도움
- 블록체인 기반의 미술품 소유권 관리를 통해 예술 작품의 신뢰성(출품 및 진품성)을 보장하고, 위조 여부에 관한 정보를 수요자에게 제공할 수 있음
- 미술품 수집-거래시장이 일반인들이 참여할 수 있는 투명한 시장이 되도록 하려면 공동소유와 소유권 거래가 필수적이라는 주장이 제기
- 미술품의 공동소유권을 가진 사람이 이 소유권을 처분하려면 지인들에게 판매하는 방법밖에 없음. 미술품 공동구매가 더 활성화되려면 이 소유권을 거래할 수 있는 신뢰도 있는 플랫폼이 요구

◎ 블록체인 기반 무형적 권리의 소유 이력 관리

- 실물 자산에 대한 소유 이력 관리에 그치지 않고, 무형적 권리에 관한 소유 이력 관리에도 블록체인 기술이 접목 가능
 - 환경부 온실가스 종합정보센터는 ‘블록체인 기반 탄소배출권 이력 관리 시스템 구축 사업’을 진행. 해당 시스템은 온실가스 감축 외부 사업 및 탄소배출권 거래 내역 등을 블록체인으로 기록하고 추적할 수 있도록 하여, 탄소배출권 관리 및 거래 투명성을 확보
 - 투명한 에너지 거래, 수요관리 최적화 등 에너지 신산업 창출, 에너지 블록체인을 통해 에너지 거래시스템 구축, 신재생에너지 거래 확산, 미래 에너지 산업 발육을 촉진할 것으로 전망
 - 네덜란드 꺼블(de Ceudel) 마을은 이에 관한 실증 사례. 블록체인을 도입하여 이웃 간 실시간 전력 거래 시스템을 구축. 지붕 위에 150여개의 태양광 패널을 설치하여 연간 3만6,000kWh의 전력을 생산하고, 여유 전력을 주고받으며 마을 공동체 내에서 함께 활용
 - 전력이 남는 집과 부족한 집을 실시간으로 연결하고 전력 거래 내역은 블록체인에 기록, 효과적인 전력 배분을 통해 이상적인 마이크로 그리드 구현 가능
 - 전력 거래에 줄리에뜨라는 코인이 사용되며, 이 코인을 이용해 마을 내 카페에서 음식·음료 구매 가능
 - 음원이나 드라마, 영화 판권과 같은 무형 자산에 대한 거래 플랫폼을 블록체인을 통해 구현 가능할 것으로 전망
 - 게임 아이템 등에 대한 소유권 관리도 가능
 - 그 동안 게임 내 아이템은 유저가 ‘사용권’에 대한 구매를 하는 시스템. 즉 소유권이 없기 때문에 게임 서비스가 종료되면 아이템도 사라지는 형태. 하지만 블록체인 기술을 활용하면 아이템이 자유롭게 이동할 수 있기 때문에 유저가 소유하는 개념으로 자리 잡힐 수 있음
 - 블록체인 게임은 블록체인화 한 아이템을 다양한 게임으로 옮길 수 있으며, 해당 아이템에 대한 소유가 게임회사가 아닌 이용자가 갖는 것이 강점

나. 시장 분석

(1) 세계시장

- 블록체인 기반 소매 및 전자상거래 세계 시장규모는 2018년 1.5억 달러에서 연평균 성장률 69% 성장하여 2024년 34억 달러 규모에 이를 것으로 전망

[블록체인 기반 소매 및 전자상거래 세계 시장규모 및 전망]

(단위 : 백만 달러, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
합계	147	280	413	799	1,185	2292	3,399	69

* 출처 : Global Blockchain Technology Market 2016-2021, MarketsandMarkets(2016)과 Blockchain Market by Component, MarketsandMarkets(2020)을 근거로 네모아이씨지 재가공

(2) 국내시장

- 블록체인 기반 자동차 거래 국내 시장규모는 2018년 48억 원에서 연평균 성장률 64% 성장하여 2024년 1,110억 원 규모에 이를 것으로 전망

[블록체인 기반 소매 및 전자상거래 국내 시장규모 및 전망]

(단위 : 억 원, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
합계	48	91	135	261	387	749	1,110	69

* 출처: Blockchain Market by Component, MarketsandMarkets(2020)의 데이터를 기준으로 비트코인 화폐별 거래량 중 원화 점유율 2.97%¹⁶⁾(코인힐스 2020.12.30.)을 근거로 네모아이씨지 재가공(환율:1100원/달러)

16) 미국달러:72.7%, 일본엔화:18.66%, 유로화:3.06%, 한국원화:2.97%

3. 기술개발 동향

☐ 기술경쟁력

- 블록체인 기반 소유자 이력 관리 시스템은 미국이 최고기술국으로 평가되었으며, 우리나라는 최고기술국 대비 77.8%의 기술수준을 보유하고 있으며, 최고기술국과의 기술격차는 1.6년으로 분석
- 중소기업의 기술경쟁력은 최고기술국 대비 72.4%, 기술격차는 2.0년으로 평가
- 한국(77.8%)>EU, 중국(75.6%)>일본(68%)의 순으로 평가

☐ 기술수명주기(TCT)¹⁷⁾

- 블록체인 기반 소유자 이력 관리 시스템은 3.35의 기술수명주기를 지닌 것으로 파악

가. 기술개발 이슈

☐ 블록체인을 이용한 소유권과 분산원장기술 개발

- 금융, 부동산, 가족 관계기록, 법인, 특허, 의료 기록은 모두 소유권과 관련 있으며, 소유권 이전이 발생할 때마다 새로운 변경 내역이 기존 변경 내역 다음에 이어져 최신 상태 유지
- 블록체인은 소유권을 증명하고 소유권을 사용하기 위한 두 가지 상반된 기능 제공
- 블록체인은 단일 원장이 아닌 분산원장에 다수의 노드가 동의하는 진실을 기록함으로써 소유권 유지
- 소유권을 증명하고 사용하기 위해서는 식별이라는 개념이, 소유권을 사용하기 위해서는 인증과 승인이라는 개념이 필요
 - 식별은 자신이 누구라고 주장하는 행위이며, 인증은 실제 식별을 증명하는 행위이며, 승인은 사전에 인증된 대상에 대해 자원의 접근을 허가하는 행위

[소유권 권리를 위한 블록체인의 기술과 소유권 관계]

블록체인 기술	소유권
블록과 거래 데이터	소유권 관련 데이터
데이터 변경에 대한 내재적인 저항력	소유권에 대한 진실을 판단하고 유지
검증과 합의 알고리즘	개별 노드들이 일관된 소유권 상태에 도달
암호화 기법	식별, 인증, 승인

17) 기술수명주기(TCT, Technical Cycle Time): 특허 출원연도와 인용한 특허들의 출원연도 차이의 중앙값을 통해 기술 변화속도 및 기술의 경제적 수명을 예측

□ 오라클 문제의 해결 필요성 대두

- 블록체인은 데이터의 위변조가 거의 불가능한 분산 저장 기술이지만, 데이터가 블록체인 안으로 들어와야 블록체인으로 관리할 수 있어서 데이터가 블록체인 안으로 들어오지 않거나, 혹은 블록체인 안으로 들어오는 과정에서 위변조가 발생한다면, 설령 그 데이터가 블록체인으로 관리된다고 할지라도 신뢰하기 어려움
- 오프체인 데이터가 온체인 데이터로 바뀌기 위해서는, 현실 세계와 블록체인의 중간에서 데이터를 블록체인 안에 넣어주는 사람이나 장치가 요구되며, 이러한 사람 또는 장치를 오라클이라고 정의
 - 오라클 문제는 이러한 중간자 역할을 하는 사람이나 장치를 어떻게 신뢰할 수 있을 것인가 하는 문제. 블록체인은 탈중앙 분산화를 추구하므로 권위를 가진 중앙이 존재하지 않음
 - 따라서 블록체인에 데이터를 입력하는 중간자를 신뢰할 수 있는 특별한 방법이 필요
- 신뢰할 수 있는 오라클 없다면 디앱의 핵심이라 할 수 있는 스마트 컨트랙트의 사용성은 제한적일 수밖에 없어서 토큰을 주고받는 것 말고는 블록체인에서 할 수 있는 것이 많지 않게 됨
 - 따라서 오라클 문제에 대한 해결 없이는 블록체인 기반의 소유권 관리 시스템을 구현하기 위한 스마트 컨트랙트의 신뢰성에 근본적인 문제가 발생할 수밖에 없음
- 예를 들어, 이러한 오라클 문제는 블록체인 기반의 물류관리 시스템에서도 발생할 수 있음
 - 물류관리에 블록체인 기술을 적용하면, 제품생산에서부터 최종 소비자까지 생산·가공·보관·운송 이력을 투명하게 관리할 수 있다는 장점이 있으나, 제품 생산 및 가공 내역을 입력하는 사람이 정직하게 데이터를 입력했는지, 해당 제품을 보관·운송하는 업체가 중간에 제품을 '바꿔치기'하지 않고 제대로 전달했는지 등을 확인하기는 쉽지 않음
 - 블록체인에 기록된 물류관리 이력 데이터는 위변조가 불가능하여 신뢰할 수 있지만, 최종적으로 소비자에게 전달된 제품이 해당 블록체인에 기록된 제품이 맞는지 확인하기는 어려움
- 오라클 패러독스
 - 오라클은 중앙화된 오라클, 탈 중앙화된 오라클, 연방 형태의 오라클의 유형으로 분류 가능
 - 중앙화된 오라클 - 연방 형태의 오라클 - 탈 중앙화된 오라클 순으로 정보가 데이터 소스에서부터 블록체인으로 도달하기 위해 거치는 과정이 더 복잡해지고, 대신 그 순서대로 우리가 오라클에 걸어야 하는 리스크는 줄어드는데 이를 오라클 패러독스라고 정의
 - 어느 정도의 효율성을 지님과 동시에 리스크가 적은 오라클을 구축해 내야만 그와 연결된 스마트 컨트랙트와 블록체인의 신뢰성을 유지할 수 있을 것으로 예상
- 오라클 문제를 해결하기 위해 다양한 방법이 도입되고 있으나 확실한 해결책은 나타나지 않은 상태
 - 암호화폐 소유자들의 투표를 통해 결정하거나, 다양한 데이터의 중앙값(median)을 선택하거나, 현실 세계와 블록체인 사이에서 신뢰할 수 있는 데이터를 제공해 주는 중간자(middleware)를 두는 방법 등 블록체인 오라클 문제를 해결하기 위한 다양한 방안이 제시되는 중
- Oraclize, ChainLink, Augur 등이 블록체인의 오라클 문제를 해결하기 위한 프로젝트

- ☐ 소유권 관리에 이용되는 스마트 컨트랙트 코드에 존재할 수 있는 보안 취약점에 대한 대비가 필요
- 스마트 컨트랙트 배포 이전에 코드 검토를 통해 보안 취약점 존재 여부와 악성코드 감염 여부를 확인

[스마트 컨트랙트 악성코드 탐지 도구]

도구명	분석 방법	취약점 유형	세부 작동 방식
Oyente	정적 분석	RE, ME, TD	<ul style="list-style-type: none"> • 제어 흐름 그래프 모듈은 컨트랙트의 바이트 코드를 입력 받아 프로그램의 실행 흐름을 나타내는 제어 흐름 그래프(CFG)를 생성하고 이를 바탕으로 기호 실행을 수행 • 코어 분석 모듈은 기호 실행의 결과를 통해 취약점을 탐지 • 유효성 검증 모듈은 최종적으로 탐지된 결과물에 대한 거짓 양성케이스를 걸러내어 사용자에게 보고
Maian	정적 분석	RE, ME, SC	<ul style="list-style-type: none"> • 스마트 컨트랙트 바이트 코드를 구동시킬 수 있는 커스텀 이더리움 가상 머신을 직접 개발하여 바이트 코드에 대한 기호 실행 수행 • 기호 실행의 결과인 실행 흔적들을 분석해 특정 보안 속성을 만족하지 않는 실행 흔적을 도출 • 실행 흔적이 보안 취약점을 유발하는 실제 입력 값을 예시로 반환하여 이를 이용해 거짓 양성 케이스 필터링을 수행
Zeus	정형 검증	RE, IO, ME, TD, SC	<ul style="list-style-type: none"> • 바이트 코드가 아닌, 스마트 컨트랙트의 상위 레벨 소스 코드(Solidity)와, XML 형태의 보안 정책을 입력 받아 각 보안 정책들을 assert 함수의 형태로 소스 코드 상에 삽입 • 소스 코드 변환 모듈이 assert 함수가 추가된 소스 코드를 LLVM(Low Level Virtual Machine) 비트 코드로 변환 • 변환된 비트 코드에 대한 수학적 검증들을 통해 스마트 컨트랙트가 보안 속성을 만족하는지를 정형 검증

나. 생태계 기술 동향

(1) 해외 플레이어 동향

□ (B)lockai) 블록체인 기술을 활용한 예술작품 저작권 보호 서비스 출시

- 예술가들이 자신의 사진에 대한 저작권을 저비용으로 보호받을 수 있도록 블록체인 기술을 이용해 저작권 데이터 수집 및 활용
- 기존 고가의 저작권 보호 방식에서 벗어나 합리적인 가격과 안전한 보안방식으로 서비스를 제공하며 블록체인 기반의 새로운 저작권 보호 방식 제시

[블록아이의 예술작품 저작권보호 서비스]



블록체인활용 디지털저작권 보호증서

블록아이를 활용한 예술가 및 작품

*출처 : 한국지식재산연구원 - 블록체인(BlockChain)기술의 산업동향 및 특허동향

□ (Lamborghini) 블록체인 기술로 차량 이력 추적·관리

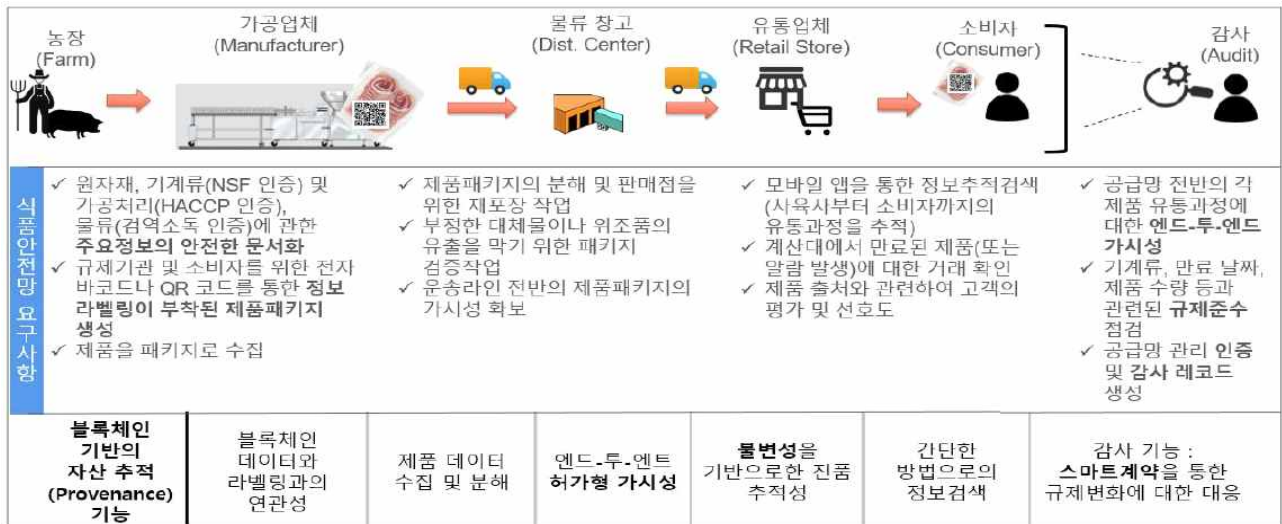
- 람보르기니가 중고차 시장에서 매매되는 자사 차량의 정품 여부 확인을 위해 세일즈포스(Salesforce)의 기업형 블록체인 플랫폼 활용, 차량 이력을 추적·관리할 계획
- 대리점, 경매회사, 수리센터, 사진기사 등 다양한 업체와 전문 인력을 활용해 모든 차량의 이력을 일일이 기록, 블록체인 기술을 통해 협력 기업체들을 하나의 분산 네트워크에 모아 편리하고 효율적으로 차량 이력 관리할 것으로 기대

- (Microsoft) 블록체인 기반 소유자 이력관리 시스템은 신원에서부터 인증, 접근통제, 불법/부정 거래 탐지에 이르는 과정의 일부로써 신원관리를 위한 Digital ID에 관련하여 MicroSoft의 Self-Sovereign Digital Identity Platform을 테스트
 - ID2020 Alliance와 자체 연구를 통해 블록체인 기반 신원관리시스템 개발하였으며, 법적인 신원확인 문제로 기본권을 보장 받지 못하고 선거, 의료보험, 주거, 교육 같은 서비스를 누리지 못하는 사람을 대상
 - MS Cloud를 기반으로 한 Microsoft Authenticator 어플리케이션을 활용하여, 이 어플리케이션에 ‘분산된 신원(Decentralized Identities)’을 추가하여 테스트 예정
 - 사용자의 해시 ID만을 블록체인에 기록하며, 실제 신원 데이터는 암호화돼 오픈 블록체인 ID 허브에 저장. 승인을 받으면 MA는 사용자의 User Agent로서 신원 데이터와 암호화 키를 관리
- (SelfKey) SelfKey는 이더리움에 기반하여 자신의 ID 특성을 공유
 - 이더리움 기반의 개인 검색ID에코 시스템으로 사용자가 안전하고 개인적이며 분산되어 신뢰할 수 있는 방식으로 자신의 ID특성을 공유
 - 사용자가 특정 서비스에 로그인할 때 사용자 본인이 소유한 정보가 아니라 각 서비스 사이트마다 보관/유지되는 정보에 기인하여 확인되므로 사용자 본인이 본인 정보를 소유하고 있지 못함. SelfKey는 SSI 개념을 적용하여 사용자가 디지털 설치 공간과 ID를 실제로 소유
 - 이는 사용자가 블록체인에서 분산된 응용 프로그램의 잠금을 해제하는 다른 앱을 통해 정보를 본인이 소유하고 활용할 수 있도록 지원해 주기 위한 프로젝트
- (CarFix) CarFix는 자동차 라이프사이클 블록체인 토큰(Vehicle Lifecycle Blockchain: VLB)의 ICO를 실시
 - 기존 중고차 구매시 차량 관리 내역이 불완전하거나 의도적으로 세탁된 경우가 있어 온전하지 않은 차량을 높은 가격을 지불하고 구매하는 경우가 있음
 - CarFix 플랫폼에 블록체인 기술이 도입되면 플랫폼제조사, 정비사, 전 주인에 걸쳐 기록된 차량에 관한 정보를 분산 저장하여 조작이 불가능하게 만들어 중고차 구매시 발생하는 리스크로부터 안전한 거래가 가능
 - 특히 CarFix는 차량이 공장에서 출고되어 폐차장에서 재활용되기 전까지의 전 과정에 걸쳐 일어나는 모든 거래를 투명하게 만들고, 관련 계약이 임의로 변경되는 일이 없도록 하는 블록체인 플랫폼을 개발하고 도입할 계획
 - 여러 기관이 보안의 위협 걱정없이 디지털 공간에서 연결되도록 하여 자동차 분야의 전자상거래를 변화시킬 것으로 기대

- (IBM, Walmart) IBM, Walmart, 블록체인 기술 활용 돼지고기 이력 추적시스템 개발 및 '19년 9월까지 Walmart에 납품하는 공급업체들이 식품에 관한 상세한 정보 제공을 의무화 실시

- 식품 유통과정에서 생길 수 있는 안전 등의 문제점들을 최소화, 문제가 생겼을 때 원인 파악에 드는 시간과 비용을 절감

[블록체인 기술을 이용한 식품 정보 추적]



*출처 :블록체인 기술을 이용한 식품 정보 추적, 2018.6, GS&J Institute

- 유통업체와 Walmart는 제품 출처 정보의 실시간 확인은 물론 고객의 평가 및 선호도를 파악 가능. 감독기관은 공급망 전반의 규제 준수를 점검하고, 공급망 관리 인증 및 감사 레코드를 생성. 이 과정에서 농장주인과 도축·가공업체, 물류창고, 유통업체, Walmart 및 감독기관 모두는 유통과정의 참여자가 되고 소비자는 모바일 어플리케이션 서버의 블록체인 네트워크에 접속해 필요한 정보 확인 가능




[상품의 원산지 추적과 블록체인 네트워크]



*출처 :상품의 원산지 추적과 블록체인 네트워크, 2018.6, GS&J Institute

- ☐ (Nestle) 블록체인 기술을 통해 고객이 직접 유아식품의 원산지와 유통경로를 추적할 수 있도록 함으로써 반품요청 수를 줄이고, 고객의 신뢰도를 높이는데 주력
- ☐ (DFA) 푸드테크 스타트업 Ripe와 협업 하에 블록체인 기술을 통해 식품 공급망의 투명성을 높이고, 농가와 유통업자, 고객의 연결고리를 강화하는데 주력
- ☐ (덴츠국제정보서비스(ISID)), 미야자키현 아야마을 블록체인 활용 유기 농산물 품질 보증
 - 각각의 야채 포장에 QR 코드를 부여하고 소비자는 스마트폰으로 QR 코드를 통해 야채가 자란 토양이나 작물이 언제 심어졌는지 등 생산 프로세스를 포장 단위로 확인 가능

[국외 블록체인 기반 서비스 사례]

회사명	서비스 개요	시기	국가
 Microsoft	MS-엑센츄어, 블록체인 기술 활용한 디지털 ID 인증 서비스 개발	'17.6	 미국
 IBM Watson	환자정보 공유를 위해 블록체인 기술 적용, FDA와 공동연구	'17.1	
 JPMorganChase	금융 관련 IT기술에 90억 달러 투자, EEA 주축 멤버로 참여	'17.2	
 Google	환자정보 추적에 블록체인 적용 추진	'17.3	
 Walmart	드론 배송 시스템에 블록체인 적용 특허 신청	'17.5	
 Risk Cooperative	68조원의 보험중개 시장에서 블록체인 적용 결정	'17.6	
 EUROPEAN CENTRAL BANK EUROSYSTEM	일본은행(BOJ)과 함께 결제시스템 적용에 대한 연구 착수	'16.12	 유럽
 Deutsche Bank	유럽 7개 은행과 함께 Hyperledger 기반의 무역금융 플랫폼 구축 진행	'17.6	
 fidor bank	출금계좌이체 서비스를 제공하는 리플 연구소와 제휴	'15.4	
 MAERSK	해운화물 추적에 블록체인 기술 적용 추진	'17.3	
 中国人民银行 THE PEOPLE'S BANK OF CHINA	블록체인 기반 자체 암호통화 발행준비	'16.1	 아시아
 阿里巴巴 Alibaba.com	블록체인 기반 푸드 트러스트 프레임워크 개발	'17.3	
 SoftBank	스프린트와 함께 통신사업자를 위한 블록체인 기술 공동 개발 착수	'17.2	
 DBS BANK	스탠다드 차타드 은행과 파트너십 블록체인 기반 전자송장 플랫폼 개발	'15.12	

*출처: 과학기술정보통신부, '블록체인 기술 발전전략', 2018.6

(2) 국내 플레이어 동향

- (KT) 농심데이터시스템(NDS)과 블록체인 기반 식품안전이력관리 사업 협력을 통해 식품 유통분야에서 농축산물 등 식재료를 안심하고 소비할 수 있는 서비스를 개발
 - 마트에서 쇠고기를 구매한 소비자가 쇠고기 포장재의 바코드나 QR코드를 활용해 축산업자 및 가공업자, 중간 유통업자 등의 정보와 모든 유통경로를 확인할 수 있으며, 이러한 정보는 모두 블록체인으로 관리
 - 식품 유통 데이터를 체계적으로 관리함으로써 수요·공급 예측을 통한 생산량 조절 등 생산성 향상이 가능. 기존 유통과정에서 수기로 관리하던 계약, 정산 등의 프로세스도 신속하게 처리할 수 있어 효율 및 비용 측면에서도 장점
 - NDS는 농축산물 이력관리 시범사업을 통해 쇠고기 유통 가정의 사육, 도축, 포장, 판매에 이르는 모든 트랜잭션을 블록체인으로 실시간 기록하고 검증했을 때 유통 이력 추적 시간이 기존 최대 6일에서 10분 이내로 단축되는 것을 확인
 - 양사는 이러한 축산물 이력관리 시범사업의 성공적인 사례를 민간 업체가 활용할 수 있도록 2019년 하반기 중에 블록체인 기반의 식품안전이력관리 플랫폼을 구축할 예정
 - KT의 블록체인 개발 플랫폼 기가 체인 기업용 BasS(블록체인 서비스, Blockchain-as-a-Service)에 NDS의 식품 이력관리 솔루션을 결합하는 형태
- (LG CNS) 세이정보기술과 협력하여 블록체인 기반의 농산물 유통 플랫폼 개발을 발표
 - LG CNS가 2018년 5월 출시한 기업용 블록체인 ‘모나체인’을 기반으로 한국조폐공사의 블록체인 오픈 플랫폼 구축 사업을 수주. 2019년 2월 모바일 고향사랑 상품권 플랫폼 ‘착(Chak)’을 개발
 - 이번 협력에서는 LG CNS가 모나체인과 기반 기술을 지원하고 세이정보기술은 구체적인 서비스를 개발하는 방식으로 구성
- (SK C&C) SK C&C는 선주와 육상 운송업자 등 물류 관계자 모두가 개인 간(P2P) 네트워크로 물류 정보를 전달받아 블록체인으로 관리하는 서비스를 개발
 - 컨테이너 화물의 위치 및 관리 정보가 자동으로 수집되어 물류 관계자 모두에게 실시간 공유를 통해 선하증권(B/L)과 신용장(L/C) 등 각종 거래원장을 블록체인에 등록시켜 원본임을 보장한 후 유통되도록 함
- (페이게이트) 페이게이트가 개발한 클라우드 기반 핀테크 플랫폼인 ‘세이퍼트’ 블록체인 지갑을 이용하여 신분 위조 등으로 P2P 거래를 할 수 있는 위험을 낮춤
 - '19년 초 EOS와 비트코인, 이더리움 등 다양한 가상화폐 기반의 지갑 서비스를 세이퍼트에 추가하며 가상통화 영역으로 플랫폼 지원 범위를 넓힘

- (스마트코어) 스마트코어는 블록체인 플랫폼 Gbrick 서비스를 상용화해서 가동 중으로 자체 합의 알고리즘으로 특허출원 중임. 이 플랫폼은 ECDSA(타원곡선 알고리즘) 암호를 적용하여 키를 생성/검증하고, 노드 간 합의를 통해 거래 진행 시 정상 거래인지 검증 가능
 - 계정 간 거래 시에는 계정에 특정 값을 부여하여 중복 거래를 검증하며, 중복된 조건의 블록생성에 대한 문제점 해결을 위해 임의의 Nonce 적용
 - 정족수 합의를 유지하기 위해 참여한 대표 노드들 간의 합의를 진행하며 특정 리더가 없는 LLFC 알고리즘을 활용
 - 말레이시아 LeadCo Resource와 블록체인 투표시스템 개발 MOU를 체결하였으며, 고려대와는 블록체인 보안 관련 산학 MOU 체결
- (열매컴퍼니) 열매컴퍼니는 미술품의 공동소유와 거래를 내용을 기록해 투명한 거래를 보장하는 '아트앤가이드'를 운영 및 국내 최초로 미술품의 토큰화를 개발 중
 - 또한, 국내 대표 블록체인 프로젝트인 아이콘(ICON)의 기술기업 아이콘루프와의 협업을 통해 공동 소유권 증명서를 발급. 아이콘루프의 블록체인 증명서 발급 서비스인 '브루프'는 아이콘 퍼블릭 블록체인 네트워크를 활용해 위변조되지 않는 증명서 발급과 영구 보관을 지원
- (ARTBLOC) ARTBLOC은 국내에서는 블록체인 기반 미술품 투자 플랫폼 아트블록(ARTBLOC)이 데이비드 호크니(David Hockney)의 '거울과 함께 모인 그림(Pictured Gathering with Mirror, 2018)'과 '초점 이동(Focus Moving, 2018)' 2점에 대한 소유권 분할 판매를 시작
 - 이 블록체인의 소유주들은 미술 작품의 실물 소유는 불가능. 아트블록 측이 작품을 보관하고 전시에 활용. 발행 수가 정해져 있어서 작품 수요가 증가하면 토큰 가격이 상승하고 작품의 가치도 상승
- (위메이드트리) 위메이드트리는 블록체인 플랫폼 '위믹스 네트워크(Wemix Network)'를 발표
 - 하나의 게임이 서비스가 종료되더라도 그 게임에서 파생된 다른 게임으로 아이템을 이동시킬 수 있음
 - 많은 서비스 체인들 간의 자산과 데이터 이동을 지원하기 위해 인터체인 역할을 하는 브릿지 체인을 구현했으며, 이를 통해 체인의 수와 종류에 관계없이 통합적 자산과 데이터 관리가 가능
 - 위메이드트리는 블록체인 게임을 직접 개발한 RPG인 '크립토테이도 for WEMIX'를 시작으로, '원드러너 for WEMIX', '캔디팡 for WEMIX', '에브리타운 for WEMIX', '두근두근 레스토랑 for WEMIX', '터치파이터 for WEMIX', '전기 모바일 for WEMIX' 등을 순차적으로 출시할 계획

다. 국내 연구개발 기관 및 동향

(1) 연구개발 기관

[블록체인 기반 소유자 이력관리 시스템 분야 기술개발 기관]

기관	소속	연구분야
동국대학교	블록체인연구센터	• PoW 및 PoS 등 기존 합의 알고리즘의 문제점을 해결한 deb 합의 알고리즘 개발
한양대학교	블록체인연구원	• 블록체인 및 토큰 경제 관련 연구 수행
한국전자통신연구원	IDX+연구단	• 분산 트러스트 데이터 거래 기술 • 분산형 자기주권신원 정보관리 기술 • 블록체인 네트워크 지연 문제 해결 기술

(2) 기관 기술개발 동향

☐ (티맥스비아이)

- 유통이력 관리 및 제품 인증 서비스를 위한 블록체인 플랫폼 개발 (2019-05-01~2021-12-31)
 - 채널 관리를 통한 블록체인 네트워크 관리 기술 개발
 - 채널 구성 구조 개발
 - 블록체인 합의 알고리즘의 다양화 및 개발
 - 블록체인 채널 및 관리자 모니터링 지원 개발
 - 스마트계약 개발을 위한 API 구현
 - Hyperdata를 기반으로 한 IoT 데이터 관리 및 모니터링 모듈 개발

☐ (비주얼넷)

- 블록체인 네트워크와 정품인증 태그의 융합 기술을 활용한 제품(귀중품 등) 진위성 검증 및 소유권 변경이력관리 시스템 개발 (2019-06-26~2020-06-25)
 - 초미세 반도체 제조공정을 통한 제품(정품인증 태그) 설계
 - 블록체인 기반의 진위성 검증 및 소유권 변경이력 관리 솔루션 적용
 - 인증 편리성 확대 및 정품인증 태그 복제 방지

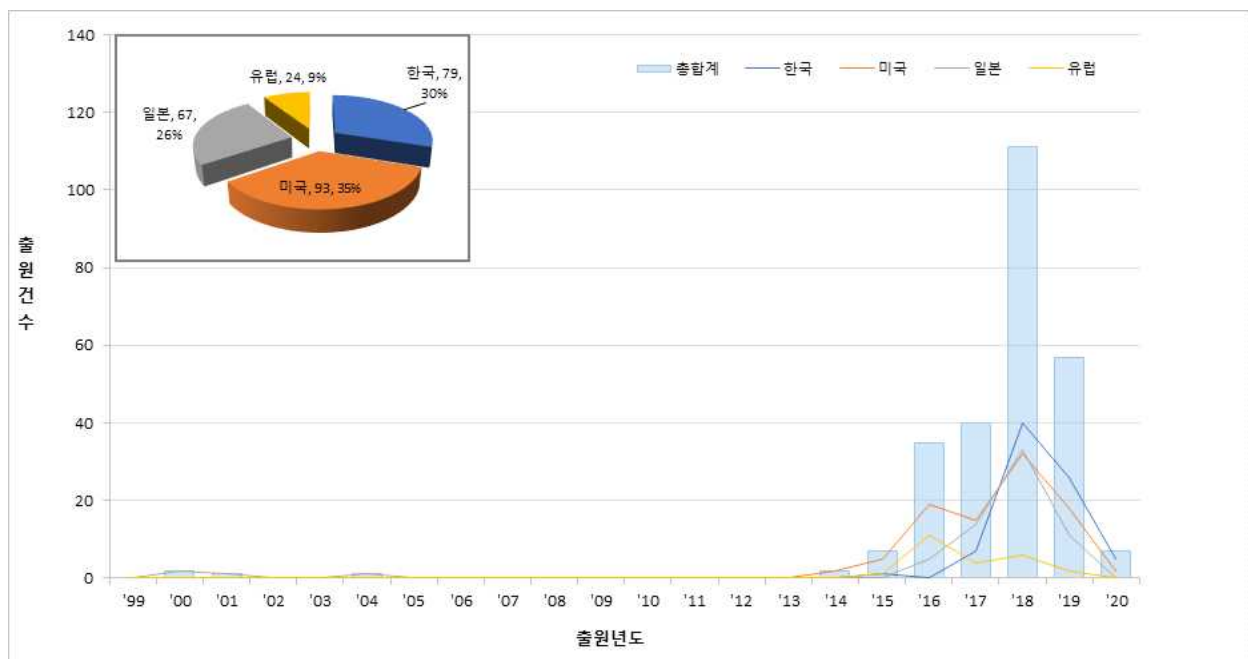
4. 특허 동향

가. 특허동향 분석

(1) 연도별 출원동향

- 블록체인 기반 소유자 이력 관리 시스템은 '16년부터 급격한 성장을 보임
 - 각 국가별로 살펴보면 미국이 가장 활발한 출원활동을 보이고 있음
- 국가별 출원비중을 살펴보면 미국이 전체의 35%의 출원 비중을 차지하고 있어, 최대 출원국으로 블록체인 기반 소유자 이력 관리 시스템 분야를 리드하고 있는 것으로 나타났으며, 한국은 30%, 일본은 26%, 유럽은 9% 순으로 나타남

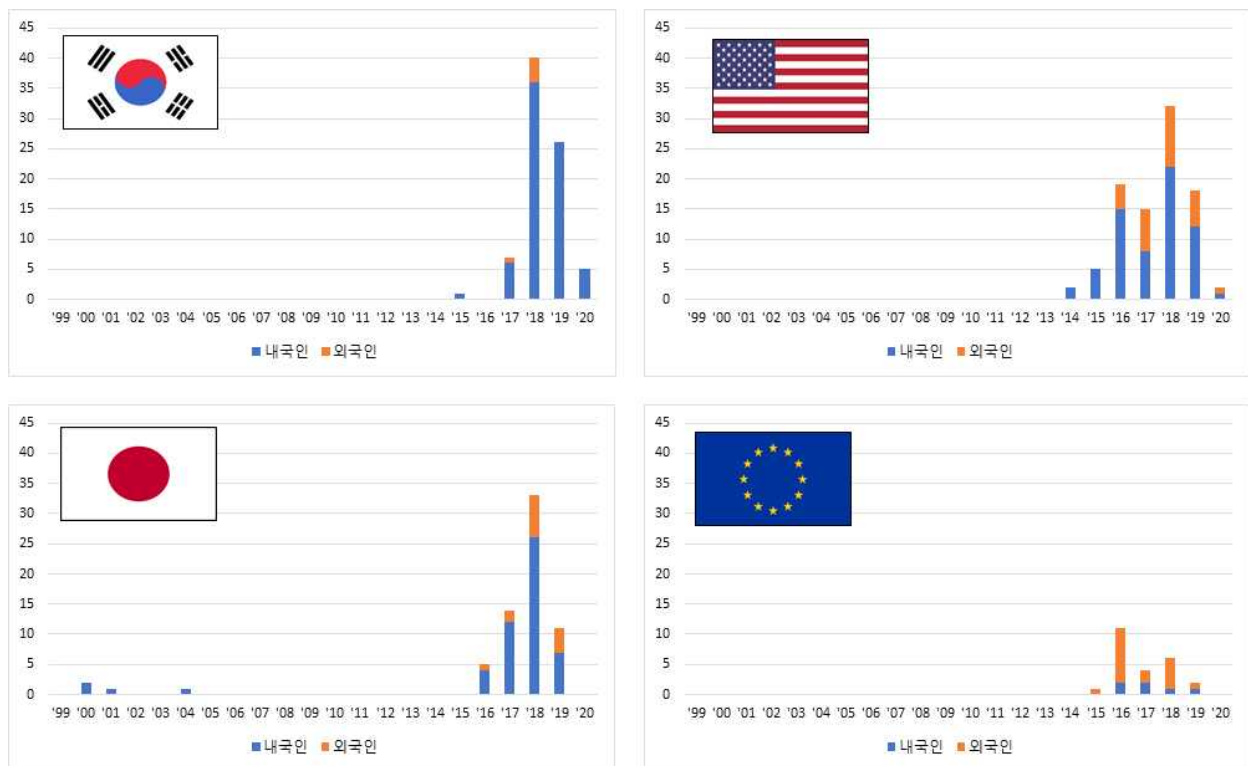
[블록체인 기반 소유자 이력 관리 시스템 연도별 출원동향]



(2) 국가별 출원현황

- ☐ 한국의 출원현황을 살펴보면, '17년부터 해당 기술의 출원이 급격히 증가하는 추세
 - 내국인 위주의 출원이 진행되고 있음
 - 한국 기술의 양적 흐름은 미국과 상당히 유사
 - 미국의 출원 수에 비해 85% 정도의 수준을 보임
- ☐ 미국의 출원현황을 살펴보면 분석구간 초기부터 전체 특허기술의 출원 증감 흐름에 영향을 주고 있는 것으로 나타남. 미국의 경우, 한국에 비해 외국인의 비중이 큰 것으로 나타남
- ☐ 유럽의 출원현황을 살펴보면 한국과 유사한 동향을 보임
- ☐ 일본의 출원현황은 '16년부터 해당 기술의 출원이 급격히 증가하는 추세이며, 한국과 유사한 동향을 보임

[국가별 출원현황]



(3) 기술 집중도 분석

□ 전략제품에 대한 최근 기술 집중도 분석을 위한 구간별 기술 키워드 분석 진행

- 전체 구간(1999년~2020년)에서 Block Chain, 블록 체인, Private Key 등 키워드가 다수 도출
- 최근 구간 분석 결과, 최근 1구간(2012년~2015년)과 비교할 때 2구간(2016년~2020년)에서 Distributed Ledger, Biometric Data Associated 키워드가 많이 등장하는 것으로 보아 블록체인 기반 소유자 이력 관리 시스템 분야에서는 거래내역 추적 기술, 생체인식 기술 관련 연구개발이 활발한 것으로 추정

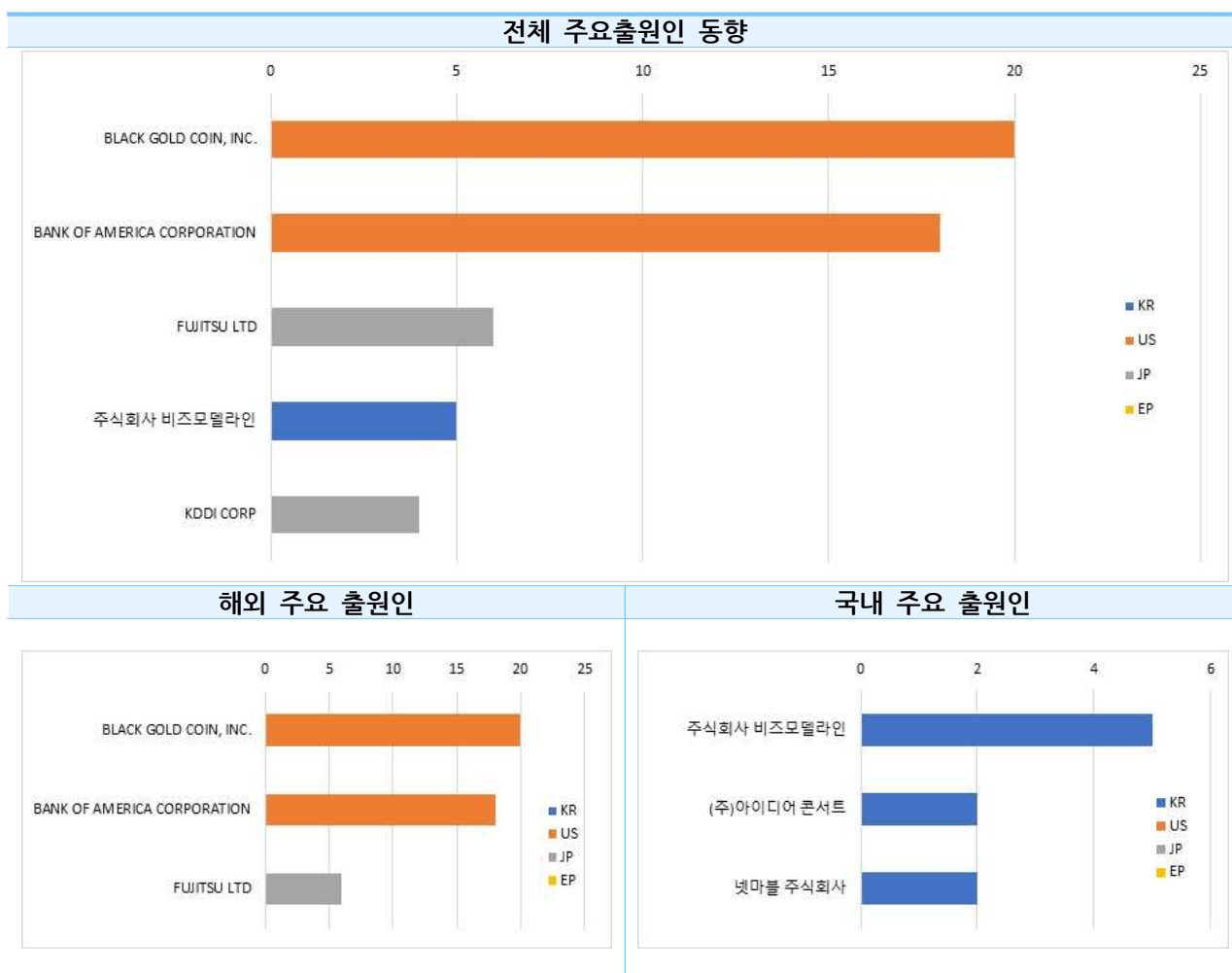
[특히 키워드 변화로 본 기술개발 동향 변화]



나. 주요 출원인 분석

- ☐ 블록체인 기반 소유자 이력 관리 시스템의 전체 주요출원인을 살펴보면, 주로 미국 국적의 출원인이 다수 포함되어 있는 것으로 나타났으며, 제 1 출원인으로는 미국의 BLACK GOLD COIN, INC.인 것으로 나타남
 - 제 1 출원인인 BLACK GOLD COIN, INC.의 출원은 미국에 집중된 경향을 보임
- ☐ 블록체인 기반 소유자 이력 관리 시스템 관련 기술로 인공지능을 다루는 대기업에 의한 출원이 대다수를 차지
 - 국내에서는 중소기업(개인)의 활발한 출원이 이루어짐

[블록체인 기반 소유자 이력 관리 시스템 주요출원인]



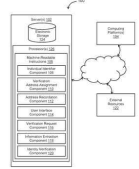
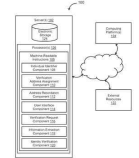
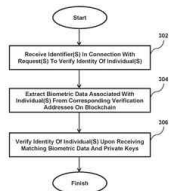
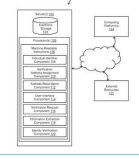
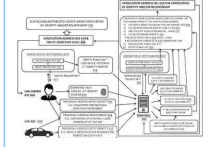
(1) 해외 주요출원인 주요 특허 분석

◎ BLACK GOLD COIN, INC.

□ BLACK GOLD COIN, INC.는 미국 기업으로 다수의 블록체인 관련 특허를 보유하고 있으며, 블록체인 기반 소유자 이력 관리 시스템 기술과 관련한 특허를 미국, 유럽, 일본에 출원

- 블록체인 기반 소유자 이력 관리 시스템과 관련하여 20건의 출원을 진행하였으며, 그 중 등록된 특허는 7건으로 파악

[BLACK GOLD COIN, INC. 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
US10389713 (2018.09.21)	Systems and methods for providing block chain-based multifactor personal identity verification	개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록함으로써, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공	
US10298572 (2018.09.21)	Systems and methods for providing block chain-based multifactor personal identity verification	개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록함으로써, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공	
US10298571 (2018.08.21)	Systems and methods for providing block chain-based multifactor personal identity verification	하나 이상의 개인들과 연관된 생체인증 데이터를 대응하는 확인 주소들로부터 추출하고, 매칭하는 생체인증 데이터 및 개인 키들을 수신할 때 하나 이상의 개인들의 신원을 확인	
US10182051 (2018.08.14)	Systems and methods for providing block chain-based multifactor personal identity verification	개인들과 연관된 식별자들 및 생체인증 데이터를 대응하는 확인 주소들에 기록함으로써, 블록 체인-기반 멀티팩터 개인 신원 확인을 제공	
US10749865 (2018.05.11)	Systems and methods for providing block chain or distributed ledger-based entity identity and relationship verification	개체 식별에 대한 블록체인/분산원장기반 검증 또는 둘 이상의 개체 간의 관계에 대한 검증이 제공	

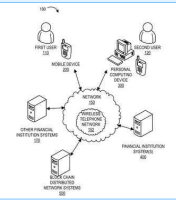
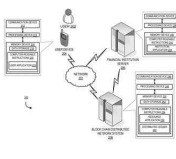
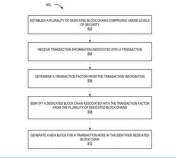
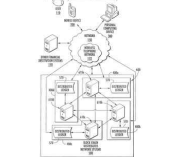

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ BANK OF AMERICA CORPORATION

□ BANK OF AMERICA CORPORATION은 미국의 상업 은행으로 블록체인 기반 소유자 이력 관리 시스템과 관련하여, 블록 체인 분산 네트워크를 활용한 기술에 특화된 특허를 다수 출원. 그 중 등록된 특허는 9건 보유

- 주요 특허들은 블록 체인 분산 네트워크를 사용하여 거래 데이터를 검증하는 기술 특허를 다수 출원하는 것으로 파악

[BANK OF AMERICA CORPORATION 주요특허 리스트]

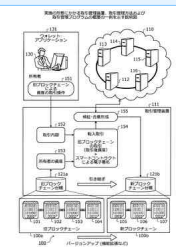
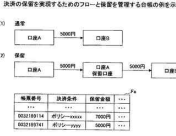
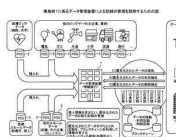
등록번호 (출원일)	명칭	기술적용분야	도면
US10614461 (2019.09.11)	System for implementing a distributed ledger across multiple network nodes	결제 트랜잭션의 검증을 위해 블록 체인 분산 네트워크를 사용하기 위해 블록 체인 분산 네트워크와 동작가능하게 접속된 시스템	
US10402796 (2016.08.29)	Application life-cycle transition record recreation system	클라이언트 발신으로부터 외부 클리어링으로 트랜잭션이 처리되는 방법의 이력 레코드를 재생성하기 위해 내부에 삽입된 검색가능한 메타데이터 코드를 갖는 블록들의 생성을 위해 블록 체인 분산 네트워크를 이용하기 위한 시스템	
US10438209 (2016.03.31)	System for secure routing of data to various networks from a process data network	계층화된 전용 블록 체인 구성을 용이하게 하기 위한 블록 체인 분산 네트워크 배열 시스템이 기능들의 상이한 조합들과 보안의 레벨들을 제공	
US10135870 (2016.02.22)	System for external validation of secure process transactions	호스트 및 소스 기관들은 블록 체인의 멤버인 호스트 기관이 블록 체인의 모든 소스 기관들의 트랜잭션 기록들을 획득할 수 있도록 멤버 기관들로부터 트랜잭션 기록들을 공유	
US10475030 (2016.02.22)	System for implementing a distributed ledger across multiple network nodes	결제 트랜잭션의 검증을 위해 블록 체인 분산 네트워크를 사용하기 위해 블록 체인 분산 네트워크와 동작가능하게 접속된 시스템	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ FUJITSU LTD

- FUJITSU LTD는 일본의 정보통신기술 기업으로 정부, 기업 대상 클라우드 서비스를 제공하며, '16년도 9월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- FUJITSU LTD의 공개특허를 대상으로 분석한 결과, 블록체인 기반 소유자 이력 관리 시스템 기술과 관련한 특허를 4건 출원

[FUJITSU LTD 주요특허 리스트]

공개번호 (출원일)	명칭	기술적용분야	도면
JP2020-042671 (2018.09.12)	거래 관리 장치, 거래 관리 방법 및 거래 관리 프로그램	거래 조작 정당성을 확인할 수 있었을 경우로, 거래 후 구블록 체인 소유자가 소유하는 자산으로 전자서명을 부여한 전입 거래를 생성하고, 생성된 전입 거래에 대해서 검증·합의를 형성하고, 신블록 체인 대장에 기록	
JP2020-030479 (2018.08.20)	결제 장치, 결제방법 및 프로그램	결제 장치는 서비스한 이용 요구에 따라, 상기 서비스한 이용에 관하는 지불한 보류를 나타내는 정보를 통해 거래의 신뢰성 향상	
JP2020-013175 (2018.07.13)	데이터 관리 프로그램, 데이터 관리방법 및 데이터 관리장치	블록 체인 기반의 선두 블록 해시값과 타임 스탬프를 이용하여 의사(擬似) 타임스탬프 토큰을 생성하여 익명화된 개인 데이터 거래 기록을 개인 데이터와 동일하게 안전하게 관리	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

(2) 국내 주요출원인 주요 특허 분석

◎ 주식회사 비즈모델라인

- ☐ 주식회사 비즈모델라인은 '18년도 3월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- 주식회사 비즈모델라인의 공개특허를 대상으로 분석한 결과, 블록체인 기반 소유자 이력 관리 시스템 기술에 있어서, 유통 정보 및 신용정보를 관리하는데 블록체인 기술을 이용한 특허를 4건 출원

[주식회사 비즈모델라인 주요특허 리스트]


공개번호 (출원일)	명칭	기술적용분야	도면
KR2020-0042093 (2018.10.12)	블록체인 기반 명품 유통 관리 방법	거점장치와 통신하는 운영서버 중 적어도 하나 포함하여 구현되는 시스템을 통해 블록체인 기반 명품 유통 관리 방법	
KR2019-0123177 (2018.04.23)	블록체인을 이용한 신용자의 신용정보 계량화 방법	블록체인을 이용한 신용자의 신용정보 계량화 방법은, 지정된 블록체인 네트워크를 구현하거나 블록체인 네트워크와 연동하는 적어도 하나의 컴퓨터를 포함하는 시스템	
KR2019-0123181 (2018.04.23)	블록체인 기반 토큰을 이용한 비신용자의 신용정보 거래 방법	지정된 블록체인 네트워크를 구현하거나 블록체인 네트워크와 연동하는 적어도 하나의 컴퓨터를 포함하는 시스템	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ (주)아이디어 콘서트

- ☐ (주)아이디어 콘서트는 한국 기업으로, 블록체인 기반 소유자 이력 관리 시스템 기술과 관련된 특허를 2건 출원

[(주)아이디어 콘서트 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
KR2152501 (2018.08.31)	블록체인을 이용한 콘텐츠 유통 관리 방법 및 시스템	콘텐츠 유통 관리 시스템은 블록체인을 활용하여 콘텐츠 유통 이력을 관리하고, 이에 근거하여 콘텐츠 수익을 분배하는 기술	 A flowchart showing the process of content distribution. It starts with '콘텐츠 제공' (Content Provision) with a value of 10, which splits into '콘텐츠 관리 시스템' (Content Management System) with a value of 100 and '콘텐츠 유통 개입소' (Content Distribution Intervention Point) with a value of 30. The '콘텐츠 관리 시스템' then splits into '소유자 제공' (Owner Provision) with a value of 20 and '콘텐츠 유통 개입소' with a value of 30. The '콘텐츠 유통 개입소' then splits into '소유자 제공' (Owner Provision) with a value of 20 and '콘텐츠 유통 개입소' (Content Distribution Intervention Point) with a value of 30.

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 넷마블 주식회사

- ☐ 넷마블 주식회사는 한국의 온라인 게임 전문 기업으로, 블록체인 기반 소유자 이력 관리 시스템 기술과 관련된 특허를 2건 출원

[넷마블 주식회사 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
KR2151731 (2019.02.27)	아이템 셀프 처리를 허용하기 위한 기법	이력 관리 서버의 하나 이상의 프로세서에 의해 실행되는 경우, 셀프 아이템 처리를 위한 컴퓨터 프로그램	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

다. 기술진입장벽 분석

(1) 기술 집중력 분석

- 블록체인 기반 소유자 이력 관리 시스템관련 기술에 대한 시장관점의 기술독점 현황분석을 위해 집중률 지수(CRn: Concentration Ratio n, 상위 n개사 특허점유율의 합) 분석 진행
- 상위 4개 기업의 시장점유율이 0.19로 블록체인 기반 소유자 이력 관리 시스템 분야에 있어서 독과점 정도는 낮은 수준으로 판단
 - 국내 시장에서 중소기업의 점유율 분석결과 0.82로 해당 기술에 대하여 중소기업이 진입하여 활동하고 있는 것으로 파악

[주요출원인의 집중력 및 국내시장 중소기업 집중력 분석]

주요 출원인 집중력	주요출원인	출원건수	특허점유율	CRn	n
	BLACK GOLD COIN, INC.(미국)	20	7.6%	0.08	1
	BANK OF AMERICA CORPORATION(미국)	18	6.8%	0.14	2
	FUJITSU LTD(일본)	6	2.3%	0.17	3
	주식회사 비즈모델라인(한국)	5	1.9%	0.19	4
	KDDI CORP(일본)	4	1.5%	0.20	5
	SIEMENS AKTIENGESELLSCHAFT(독일)	4	1.5%	0.22	6
	THE BOEING COMPANY(미국)	3	1.1%	0.23	7
	DELL PRODUCTS, LP(미국)	3	1.1%	0.24	8
	NOKIA TECHNOLOGIES OY(핀란드)	3	1.1%	0.25	9
	(주)아이디어 콘서트(한국)	2	0.8%	0.26	10
	전체	263	100%	0.19	
국내시장 중소기업 집중력	출원인 구분	출원건수	특허점유율	CRn	n
	중소기업(개인)	67	81.7%	0.82	
	대기업	9	11.0%		
	연구기관/대학	6	7.3%		
	전체	82	100%	CR중소기업=0.82	

(2) 특허소송 현황 분석

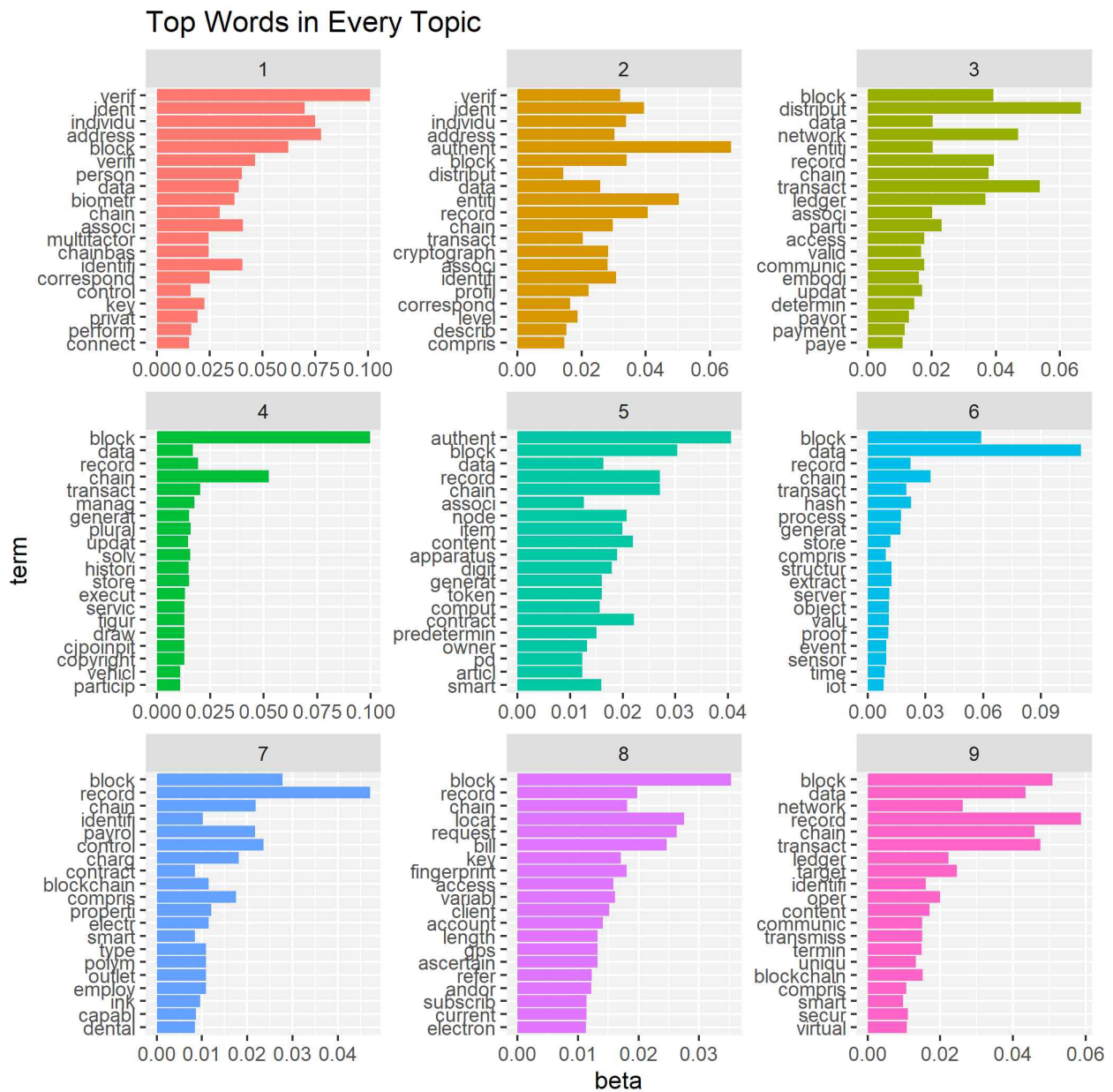
- ☐ 블록체인 기반 소유자 이력 관리 시스템 분야 관련 특허소송 이력은 검색되지 않음
 - 따라서 국내기업이 미국시장에 진입하는 경우, 해당 분야를 선점할 수 있을 것으로 판단
 - 다만, 블록체인과 관련해서는 4개의 소송이 검색

5. 요소기술 도출

가. 특허 기반 토픽 도출

- 166개의 특허의 내용을 분석하여 구성 성분이 유사한 것끼리 클러스터링을 시도하여 대표성이 있는 토픽을 도출

[블록체인 기반 소유자 이력 관리 시스템에 대한 토픽 클러스터링 결과]



나. LDA¹⁸⁾ 클러스터링 기반 요소기술 도출

[LDA 클러스터링 기반 요소기술 키워드 도출]

No.	상위 키워드	대표적 관련 특허	요소기술 후보
클러스터 01	verify, address, individual, identify, block, verification, association, identification, personal, data	<ul style="list-style-type: none"> • Systems and methods for providing block chain-based multi-factor personal identity verification • Systems and methods for realizing block chain-based multifactor personal identity verification 	블록체인 원장관리 기술
클러스터 02	authentication, entity, record, identify, block, individual, verify, identification, address, chain	<ul style="list-style-type: none"> • A distributed user profile identity verification system for e-commerce transaction security • Blockchannel scanner systems and methods 	실물/디지털 자산에 대한 소유권자 등록 기술
클러스터 03	block, data, authentication, chain, store, decrypt, encrypt, memories, process, client	<ul style="list-style-type: none"> • Power trading system • System for implementing a distributed ledger across multiple network nodes 	블록체인 원장관리 기술
클러스터 04	key, data, block, communic, encrypt, control, medic, decrypt, node, chain	<ul style="list-style-type: none"> • Collaborative internet-of-things anomaly detection • Blockchain payroll system 	불법 취득 자산 탐지 기술
클러스터 05	data, block, chain, encrypt, plural, process, subset, storage, configure, set	<ul style="list-style-type: none"> • Platform, system and method for diamond trading • Article information management apparatus, system, method and program 	실물-디지털 정보 매핑 기술
클러스터 06	encrypt, chain, block, node, blockchain, instruct, network, step, computing, code	<ul style="list-style-type: none"> • Blockchannel scanner systems and methods • System and method for verifying forgery of financial institution proof documents on basis of block chain 	블록체인 원장관리 기술
클러스터 07	record, block, control, chain, charge, comprise, property, electric, blockchain	<ul style="list-style-type: none"> • Oil-based ink for electrostatic ink jet recording • Charging system and charging method 	-
클러스터 08	block, locate, request, bill, record, chain, fingerprint, key, variable, access	<ul style="list-style-type: none"> • Method and computer for cryptographically protecting control communication in and/or service access to it systems, in particular in connection with the diagnosis and configuration in an automation, control or supervisory system • Method and apparatus for optimized access of security credentials via mobile edge-computing systems 	-
클러스터 09	key, block, chain, encrypt, message, data, public, store, value, access	<ul style="list-style-type: none"> • Electronic burial and its program that hands down information of the deceased to future generations in robust and long-term manner • System and method of validation of block chain by secondary chain having incentivization and insurance coverage powered by proof of work 	소유권 이전 이벤트 처리 기술

18) Latent Dirichlet Allocation

다. 특허 분류체계 기반 요소기술 도출

- 블록체인 기반 소유자 이력 관리 시스템 관련 특허에서 총 10개의 주요 IPC코드(메인그룹)를 산출하였으며, 각 그룹의 정의를 기반으로 요소기술 키워드를 아래와 같이 도출

[IPC 분류체계에 기반한 요소기술 도출]

IPC 기술트리		
(서브클래스) 내용	(메인그룹) 내용	요소기술 후보
(A63F) 카드게임, 보드게임 또는 룰렛게임; 작은 움직이는 물체를 사용하는 실내용게임; 그 밖에 분류되지 않는 게임	• (A63F-013) 게임과 관련된 표시를 나타내고, 예. 텔레비전, 스크린상에서 2차원 또는 그 이상의 차원을 가지는 전자적으로 생성된 표시화상을 이용한 게임양상	-
(G06F) 전기에 의한 디지털 데이터처리	• (G06F-012) 메모리 시스템 또는 아키텍처 내에서 액세스, 어드레스 지정 또는 할당	-
	• (G06F-021) 부정행위로부터 프로그램 또는 데이터, 그 컴퓨터 부품을 보호하기 위한 보안 장치	-
(G06Q) 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 데이터 처리 시스템 또는 방법; 그 밖에 분류되지 않는 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 시스템 또는 방법	• (G06Q-030) 거래, 예. 쇼핑 또는 전자상거래	부정 거래 탐지 기술
	• (G06Q-020) 지불 체계, 방식 또는 프로토콜	부정 거래 탐지 기술
	• (G06Q-010) 경영; 관리	공적 가시성을 위한 거래내역 추적 기술
	• (G06Q-050) 특정 사업 부문에 특히 적합한 시스템 또는 방법, 예. 공익사업 또는 관광	공적 가시성을 위한 거래내역 추적 기술
	• (G06Q-040) 금융; 보험; 세무 전략; 법인세 또는 소득세의 처리	-
(H04L) 디지털 정보의 전송, 예. 전신통신	• (H04L-009) 비밀 또는 보안통신을 위한 배치	-
	• (H04L-029) 그룹 1/00에서 H04L 27/00의 하나에도 포함되지 않는 배치, 장치회로 또는 시스템	-

라. 최종 요소기술 도출

- ☐ 산업·시장 분석, 기술(특허)분석, 전문가 의견, 타부처 로드맵, 중소기업 기술수요를 바탕으로 로드맵 기획을 위하여 요소기술 도출
- ☐ 요소기술을 대상으로 전문가를 통해 기술의 범위, 요소기술 간 중복성 등을 조정·검토하여 최종 요소기술명 확정

[블록체인 기반 소유자 이력 관리 시스템 분야 요소기술 도출]

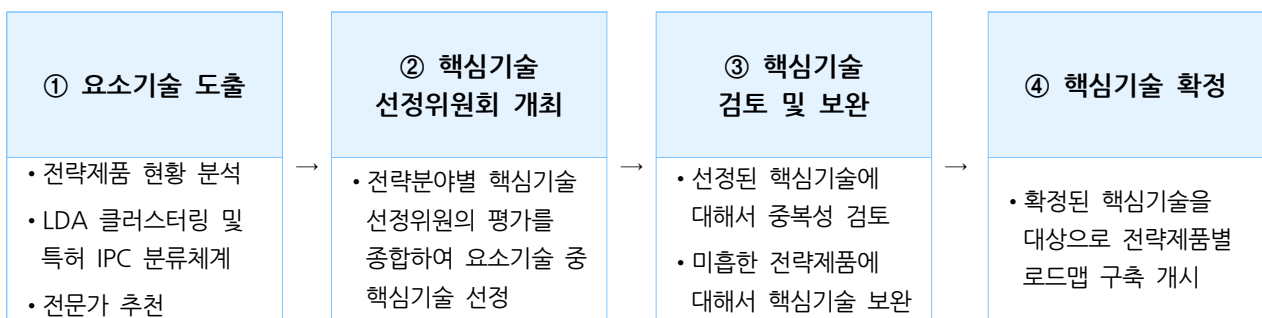
요소기술	출처
실물/디지털 자산에 대한 소유권자 등록 기술	특허 클러스터링, 전문가추천
공적 가시성을 위한 거래내역 추적 기술	IPC 기술체계, 전문가추천
실물-디지털 정보 매핑 기술	특허 클러스터링, 전문가추천
불법 취득 자산 탐지 기술	특허 클러스터링, 전문가추천
부정 거래 탐지 기술	IPC 기술체계, 전문가추천
소유권 이전 이벤트 처리 기술	특허 클러스터링, 전문가추천
블록체인 원장관리 기술	특허 클러스터링, 전문가추천
참여자 권한 설정 기술	전문가추천
블록체인 아카이빙	전문가추천
블록체인간 자산연계 및 교환서비스 기술	전문가추천

6. 전략제품 기술로드맵

가. 핵심기술 선정 절차

- ☐ 특허 분석을 통한 요소기술과 기술수요와 각종 문헌을 기반으로 한 요소기술, 전문가 추천 요소기술을 종합하여 요소기술을 도출한 후, 핵심기술 선정위원회의 평가과정 및 검토/보완을 거쳐 핵심기술 확정
- ☐ 핵심기술 선정 지표: 기술개발 시급성, 기술개발 파급성, 기술의 중요성 및 중소기업 적합성
 - 장기로드맵 전략제품의 경우, 기술개발 파급성 지표를 중장기 기술개발 파급성으로 대체

[핵심기술 선정 프로세스]



나. 핵심기술 리스트

[블록체인 기반 소유자 이력 관리 시스템 분야 핵심기술]

핵심기술	개요
실물/디지털 자산에 대한 소유권자 등록 기술	<ul style="list-style-type: none"> 다양한 종류의 자산 및 소유권자를 생성하여 분산환경에 안전하게 기록하고 관리. 블록체인과 현실 세계를 연결시켜주는 핵심 기술로 최근에는 SSI에 대한 연구가 증가
공적 가시성을 위한 거래내역 추적 기술	<ul style="list-style-type: none"> 공적 가시성을 위한 거래내역 추적 기술. 저작권료 징수 및 분배 등을 위한 디지털 저작물의 구매/사용 내역 추적 및 이에 대한 무결성을 시스템적으로 보장
실물-디지털 정보 매핑 기술	<ul style="list-style-type: none"> 생체 정보를 디지털화하여 실물과 디지털 정보 간에 매핑 수행. 실물과 디지털 정보의 진위성 검증 기술
불법 취득 자산 탐지 기술	<ul style="list-style-type: none"> 불법적인 거래에 의해 이루어진 자산 취득을 탐지하는 기술
부정 거래 탐지 기술	<ul style="list-style-type: none"> 자산에 대한 적절한 접근통제를 통하여 불법적인 거래를 방지하고, 인증을 통하여 신원의 부정사용을 방지






다. 중소기업 기술개발 전략

- ☐ 정부의 블록체인 기술 개발을 위한 R&D 지원 및 투자 정책을 활용
- ☐ 대기업 및 금융회사들의 블록체인 기술 수요에 따라 협업이나 컨소시엄 구성
- ☐ 해외 스타트업들과의 협업을 통해 지속적이고 선제적인 기술개발 수행

라. 기술개발 로드맵

(1) 중기 기술개발 로드맵

[블록체인 기반 소유자 이력 관리 시스템 분야 중기 기술개발 로드맵]

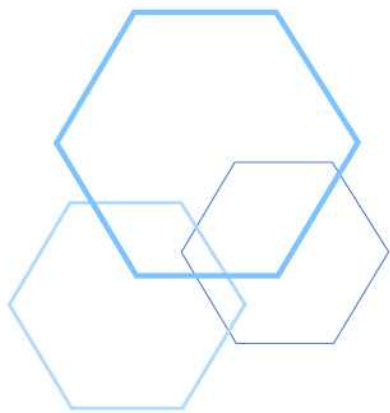
블록체인 기반 소유자 이력 관리 시스템	블록체인 이용 디지털 자산의 공적 가시성 확보 기술 개발			
	2021년	2022년	2023년	최종 목표
실물/디지털 자산에 대한 소유권자 등록 기술				분산환경에서의 상용화
공적 가시성을 위한 거래내역 추적 기술				분산환경에서의 상용화
실물-디지털 정보 매핑 기술				Prototype 개발
불법 취득 자산 탐지 기술				Prototype 개발
부정 거래 탐지 기술				Prototype 개발

(2) 기술개발 목표

- ☐ 최종 중소기업 기술로드맵은 기술/시장 니즈, 연차별 개발계획, 최종목표 등을 제시함으로써 중소기업의 기술개발 방향성을 제시

[블록체인 기반 소유자 이력 관리 시스템 분야 핵심요소기술 연구목표]

핵심기술	기술요구사항	연차별 개발목표			최종목표	연계R&D 유형
		1차년도	2차년도	3차년도		
실물/디지털 자산에 대한 소유권자 등록 기술	DHT	설계 및 구현	테스트	상용화	분산환경에서 의 상용화	산학연
공적 가시성을 위한 거래내역 추적 기술	DAG	설계 및 구현	테스트	상용화	분산환경에서 의 상용화	산학연
실물-디지털 정보 매핑 기술	FIDO/PUFF/Digital Signature	설계	구현	POC	Prototype 개발	산학연
불법 취득 자산 탐지 기술	Framework	정책 기획	설계	Prototype	Prototype 개발	산학연
부정 거래 탐지 기술	Framework	정책 기획	설계	Prototype	Prototype 개발	산학연



전략제품 현황분석

암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템



암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템

정의 및 범위

- 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템은 블록체인 운영 설정 및 블록체인 참여자의 블록체인 활동 시작 시 블록체인 암호키 수명주기 관리 정책에 따른 키 관리 프로세스를 통해 블록체인 암호키를 관리(생성, 발급, 저장, 백업, 폐기 등)할 수 있게 해주는 시스템을 의미

전략 제품 관련 동향

시장 현황 및 전망	제품 산업 특징
<ul style="list-style-type: none"> • (세계) 공개키 인프라의 세계시장 규모는 15.1%의 연평균 성장률로 2019년 17억 달러에서 2024년까지 36억 달러로 성장할 것으로 예상 • (국내) 금융서비스 분야의 블록체인의 국내시장 규모는 65%의 연평균 성장률로 2019년 98억 원에서 2024년까지 1,987억 원으로 성장할 것으로 예상 	<ul style="list-style-type: none"> • 암호자산 기반 서비스는 암호키에 대한 안전한 관리가 이뤄지지 않으면 전반적인 암호자산 기반 서비스의 안전성에도 문제가 발생 • 기관 투자자들의 가세로 암호화폐 보관 서비스(커스터디, Custody)가 부상 중으로, 이들을 위한 안전한 키 관리 시스템의 개발이 요구
정책 동향	기술 동향
<ul style="list-style-type: none"> • 4차산업혁명위원회는 '19년 10월 발표한 '4차 산업혁명 대정부 권고안'을 통해 암호자산의 법적 지위 마련 등을 포함하는 개선책을 제시함 	<ul style="list-style-type: none"> • 클라우드 문서 보안사고를 막는 Key 관리 방안개발 중 • 새로운 IoT 보안성 검증 프레임워크의 개발 및 보안성 검증을 수행하고 취약점 검증의 개념 증명을 위한 보안 IoT ASIC 칩 개발
핵심 플레이어	핵심기술
<ul style="list-style-type: none"> • (해외) Fujitsu, Nasdaq, Goldman Sachs, Fidelity, Coinbase, Bakkt, BitGo • (대기업) 카카오, 삼성, 네이버 • (중소기업) 펜타시큐리티, 케이사인 	<ul style="list-style-type: none"> • Secure Environment 관련 기술 • 키의 안전한 생성, 유통 보관 및 폐기를 위한 키 관리 기술(KMS: Key Management System) • 블록체인 자산 보호를 위한 전자지갑 기술 • 블록체인 암호키 복구 기술 • 블록체인 암호키 사용자 인증 기술

*생태계 취약 전략제품

중소기업 기술개발 전략

- 정부의 블록체인 기술 발전전략에 따른 R&D 지원 기회 활용 및 관련 업체 간 협력체 구성을 통해 적극적으로 블록체인 암호키 관리 시스템 개발 참여 및 관련 진출 전략 수립 필요
- 블록체인 플랫폼 도입 확대에 따라, 단기적으로는 전자지갑 기술과 같은 키 보호 제품 기술 개발을 실시하고, 중장기적으로는 암호키 복구 기술 등 키 관리 서비스 기술 개발로 시장 대응 필요

생태계 강화방안

- 신뢰 가능한 기관에서 발간한 안전한 키 생성에 대한 최신 보안 가이드 준수 등 법·제도 개정의 선제적 대응 방안 수립 필요
- 중앙집중식, 폐쇄적 금융 ICT 감독 체계에서 분산·개방형으로 전환하는 규제완화 정책의 병행이 요구

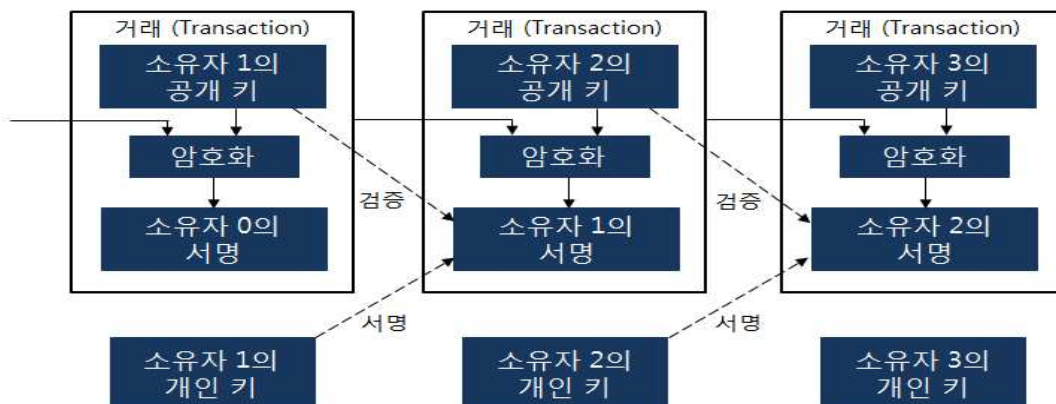
1. 개요

가. 정의 및 필요성

(1) 정의

- 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템은 암호자산 기반 서비스의 운영 과정에서 중요하게 활용되는 블록체인 암호키의 노출, 누출 및 위·변조 등 보안위협에 대한 대응 방안으로 활용될 수 있는 기술로 이를 통해 블록체인 운영의 안전성 제공이 가능하도록 구축하는 시스템을 의미
- 블록체인 암호키를 분실하여 자산을 거래하지 못하거나 도난당한 키가 공격자에 의해 악용되는 것을 방지하기 위한 시스템. 블록체인 참여자의 키를 안전하게 저장·관리할 수 있는 콜드 월렛 등 강화된 암호키 보호기술을 포함
 - 암호자산의 거래 처리 과정에서 공개키 및 개인키는 각각 코인 송·수신 시 활용되는 계좌번호 역할을 하거나 본인 여부를 증명하는 전자서명에서 필수적으로 활용

[암호자산 비대칭 키 암호화 개념도]



* 출처 : <http://new-flowing.com/9>, 2018. 1

- 이와 같이 거래 내역이 처리되는 암호자산 기반 서비스의 경우, 전자서명용 개인키에 대한 사이버공격의 위험성이 증가하고 있을 뿐 아니라, 개인키를 도난당하거나 분실했을 경우에는 이를 획득한 사용자에게 의해 다른 사용자의 전자서명이 불법적인 목적으로 악용될 수 있기 때문에 이를 방지하거나 대응할 수 있는 기술 개발(예, 블록체인 전자지갑 등)이 필요

(2) 필요성

□ 암호자산 기반 서비스를 위한 블록체인 시스템에서 ‘암호키 관리’는 핵심적인 필수보안요소

- 블록체인 시스템은 암호화 키 쌍을 보유하고 해당 키 쌍은 노드와 노드 사이를 연결하는 데이터 전송 구간을 암호화할 때 그리고 전자서명을 통한 노드 간 인증 시에 사용
- 따라서 블록체인 시스템의 키가 노출되면 데이터 전송 중에 사용자의 개인정보나 금융정보 등 중요한 데이터가 유출되거나 위·변조의 위험성이 높기 때문에 암호자산 기반 서비스에 있어서 암호키는 별도의 안전한 키 관리 시스템에 보관 및 관리가 필요

□ EU 산하 정보보호기구인 ENISA(European Union Agency For Network and Information Security)에서도 최근 발표한 보고서를 통해 블록체인 시스템 도입 시 고려해야할 보안 이슈와 보안 강화방안으로 블록체인 암호키 관리 제시

- 블록체인 도입 시 고려가 필요한 보안위협으로 블록체인 암호키 관리를 분류하고 키 도난 및 분실, 취약한 키 생성에 대한 보안위협 및 이에 대한 대응방안을 제시

[블록체인 암호키 보안위협 및 대응 방안]

보안위협	세부 내용	대응 방안
키 도난 및 분실	<ul style="list-style-type: none"> • 사용자 단말 암호키가 도난당할 경우 해당 키로 보호되던 자산 및 기밀거래 유출 가능 • 키가 암호화 등 보호기술이 적용되지 않은 경우 공격자가 접근 가능 • 자산 거래 서명과 거래 메시지 암호화에 동일한 키 사용 시 피해 확대 • 참여자가 키에 대한 접근권한을 상실하거나 키를 분실할 경우 자산 이전이 불가능해질 수 있으며 공격자가 키를 획득하여 악용한 경우에도 확인이 불가 	<ul style="list-style-type: none"> • 키 도난 및 분실 대비 다음과 같은 정책 및 기술을 적용 • 키를 분실 대비 키 복구 기능을 적용하고 복구 시 추가 인증절차 마련 • 다중 서명기술 적용 불법 거래를 시도하지 못하도록 대응 • 업무 및 용도(거래 서명, 거래 메시지 암호화 등)별 키 구분 운영 • 서명키가 파일 저장 시 암호화하거나 키 사용 후 메모리에서 즉시 삭제 등 보호기술 적용
취약한 키 생성	<ul style="list-style-type: none"> • 블록체인 암호키 재생성 공격을 통해 참여자의 키를 획득 가능 • 또한, 공격자가 양자 컴퓨팅을 활용할 경우 현재 안전한 키 생성방식도 취약해질 수 있으며, 장기적 관점에서 고려 필요 	<ul style="list-style-type: none"> • 신뢰 가능한 기관에서 발간한 안전한 키 생성에 대한 최신 보안 가이드 준수 • 검증기관으로부터 키 생성 알고리즘 등을 확인받고 키의 안전성을 검증

* 출처 : 보안기술팀, “블록체인 기술과 보안 고려사항”, 금융보안원, 2017. 8.

□ 특히, 은행과 같이 개인 데이터 교환을 관할하는 중앙 기관이 없다는 이점 때문에 블록체인 네트워크를 통해 전 세계적인 개인식별정보(PII) 교환을 실현하기 위한 여러 가지 프로젝트가 현재 진행 중이며 이 경우 안전한 암호키 관리가 매우 중요

- 블록체인 기반의 탈중앙화된 개인신원(ID) 검증이 5년 이내에 더 이상 새로운 개념이 아닌 표준으로 자리를 잡을 것으로 예상
- 개인식별정보가 포함된 암호자산 기반 서비스를 이용할 경우, 다른 사람이 이 토큰을 확보할 시 토큰 주인을 가장해 다른 용도로 사용할 가능성이 있기 때문에 블록체인 사용자의 ID토큰에 대한 액세스 권한을 철회하거나 분실된 개인키의 복구가 무엇보다 중요해질 것

나. 범위 및 분류

(1) 가치사슬

- ☐ 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템은 블록체인 플랫폼 사업영역에서 적용 필요성이 크고 중요한 역할을 담당
- ☐ (전방산업) 금융기관, 자동차/유통/헬스케어/에너지/미디어/자선 등 산업분야, 공공기관 및 민간기업 등으로 구성
 - 금융기관에서는 기존 금융시스템의 처리 소요시간, 절차 및 보안 개선 등을 위해 암호자산 기반 서비스 및 블록체인 기술을 도입하고 기관 간 송금, 결제 등 거래 시 중개 기관이 신뢰를 담보하던 번거로움을 제거하고, 상호 신뢰 하에 빠르고 간소화된 금융 서비스가 가능하도록 시스템 개선
 - 자동차/유통/헬스케어/에너지/미디어/자선 등 산업분야에서는 산업 생태계에 참여하는 이해관계자들에 의한 정보의 생성/갱신/저장이력을 활용하여 새로운 비즈니스 가치를 생성하는데 초점을 맞추고, 다양한 산업 분야의 참여자들이 비즈니스 대상에 대한 정보 이력을 암호자산 및 블록체인에 기반하여 연결하는 중
- ☐ (후방산업) 블록체인 암호키 관리 시스템 개발에 사용되는 주요 핵심요소기술인 정보보호 소프트웨어, 임베디드SW, 하드웨어 칩 및 인터넷 서비스 소프트웨어 등이 있음
 - 정보보호 소프트웨어에는 블록체인 암호키 관련 암호 기술, 인증 기술, 키 복구 기술 및 보안 위협 방지 기술 등 개발에 활용
 - 임베디드SW 및 하드웨어 칩에는 암호자산 기반 서비스의 보호를 위한 암호키의 안전한 관리를 위한 하드웨어 기반 전자지갑 개발에 활용
 - 인터넷 서비스 소프트웨어는 암호자산 기반 서비스의 보호를 위한 암호키 관리 서비스 제공에 필요한 서비스 기술 개발에 활용

[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야 산업구조]

후방산업	블록체인 암호키 관리 시스템 기술 분야	전방산업
정보보호 소프트웨어, 임베디드SW, 하드웨어 칩, 인터넷 서비스 소프트웨어	Secure environment 관련 기술, 전자지갑 기술, 블록체인 암호키 관리 서비스 기술, 블록체인 암호키 복구 기술	금융기관, 자동차/유통/헬스케어/에너지/ 미디어/자선 등 산업분야, 공공기관, 민간기업

(2) 용도별 분류

☐ 암호자산 기반 블록체인 사업영역에 활용 가능

- 암호자산 기반 블록체인 사업은 블록체인에 기초하여 암호자산 기반 서비스를 제공하는 것을 의미
- 암호자산 거래 서비스, 암호자산(디지털자산)의 전문 수탁 보관 서비스(커스터디·Custody), 증권형 토큰의 발행 및 유통 사업, 거래소간 암호화폐 거래 주문을 매칭·청산하는 통합 거래소 등

(3) 기술별 분류

- ### ☐ 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템은 하드웨어 또는 소프트웨어 기반의 안전한 키 보관 기술 및 신뢰 계산 기술 등의 개인 키 보관 및 안전한 사용을 위한 secure environment 관련 기술, 키의 안전한 생성, 유통 보관 및 폐기를 위한 키 관리 기술(KMS: Key Management System), 블록체인 자산 보호를 위한 전자지갑 기술, 블록체인 암호키 복구 기술로 분류 가능

[기술별 분류]

분류	상세 내용
Secure environment 관련 기술	• 암호자산 기반 서비스에 사용되는 암호키를 하드웨어 또는 소프트웨어 기반으로 안전하게 보관하거나 신뢰 계산 기술 등을 활용하여 암호키 보관뿐만 아니라 안전하게 사용할 수 있게 해주는 기술
키 관리 기술 (KMS)	• 블록체인 암호키 관리에 따른 암호키 생명주기에 따른 관리(생성, 저장, 백업, 폐기 등)를 지원하기 위한 서비스 기술
전자 지갑 기술	• 키를 분실하여 블록체인 자산을 거래하지 못하거나 도난당한 키가 공격자에 의해 악용되는 것을 방지하기 위한 기술
블록체인 암호키 복구 기술	• 사용자의 부주의 등으로 인해 키 분실 시 키 복구를 통해 블록체인 자산 분실을 방지하기 위한 기술

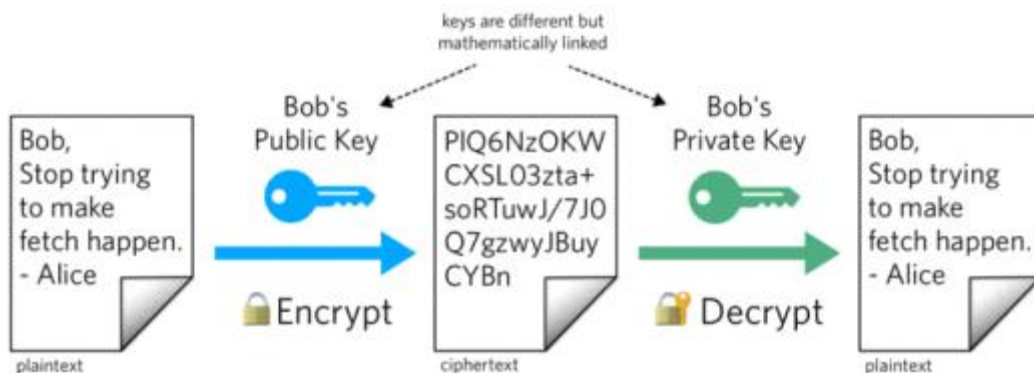
2. 산업 및 시장 분석

가. 산업 분석

◎ 공개키 암호화 보안기술 활용 다양한 응용서비스 구현

- 네트워크상의 모든 거래자가 공동으로 거래정보를 검증하고 기록함으로써 별도의 제삼자 없이 해시함수(Cryptography hash function), 전자서명(Digital Signature), P2P 네트워크를 통한 암호화(Cryptography) 등의 보안기술을 활용, 거래 기록의 신뢰성과 무결성 확보
 - 공개키 암호화는 공개키(Public key)와 개인키(Private key) 쌍을 이용하여 다른 작업을 수행하며, 공개키는 널리 배포되고 개인키는 비밀로 유지
 - 개인의 공개키를 사용, 개인키를 가진 사람만 암호 해독 및 읽을 수 있도록 메시지 암호화
 - 개인키를 사용하면 해당 공개키를 가진 사람은 누구나 개인키 소유자가 메시지 작성 후 수정 여부 확인할 수 있도록 디지털 서명 작성 가능하여 블록체인 공개키 암호화의 광범위한 사용 기대

[공개키 암호화 동작원리]



* 출처 : BlockchainJournal, "What is a public key of a cryptocurrency wallet?", 2019.6

◎ 블록체인 사업영역 및 암호키 관리 시장

- 블록체인 사업영역은 크게 암호화폐 비즈니스 사업영역, 블록체인 플랫폼 사업영역, 블록체인 응용 시스템 사업영역으로 구분할 수 있음
 - 블록체인 암호키 관리 시스템은 블록체인 플랫폼 사업영역에서 적용 필요성이 크고 중요한 역할을 담당
- 암호화폐 비즈니스 사업영역
 - 암호화폐는 전 세계 인터넷 네트워크에 P2P 방식으로 분산 저장되어 운영되고 있는 블록체인 기술을 활용하여 암호화폐를 발행하고 관리
 - 새로운 암호화폐 발행 비즈니스를 추진하기 위해 코인 공개(ICO) 등을 통해 운영 자금을 마련

□ 블록체인 플랫폼 사업영역

- 블록체인 플랫폼은 블록체인 서비스를 개발, 운영할 수 있도록 해주는 블록체인 시스템의 구성요소(분산 네트워크, 통신 프로토콜 등) 및 필요기능(거래정보 검증, 합의, 노드관리 기능 등)을 제공
- 블록체인 컨소시엄, 커뮤니티, IT 기업 등에서 플랫폼을 제공 중이며 플랫폼의 적용 대상 및 제공 방식 등에 따라 분류 가능

□ 블록체인 응용 시스템 구축 사업영역

- 금융분야에서 블록체인 응용 시스템으로는 은행, 증권 등에서 제공하는 증권 거래, 청산결제, 송금 등의 금융 서비스를 블록체인을 활용하여 개발
- 비금융 분야의 경우에는 신원관리, 공증, 소유권 증명, 투표 등과 같은 범용적으로 이용될 수 있는 응용 기술을 개발하는데 블록체인을 활용

□ 암호자산 기반 보호를 위한 암호키 관리 시스템은 블록체인 플랫폼 등의 보안위협에 대한 대응 방안으로 관련 산업 생태계를 위해 구축 필요하고 이를 통해 생태계 운영 환경에서 블록체인 사업 영역의 완성도 및 안전성을 결정

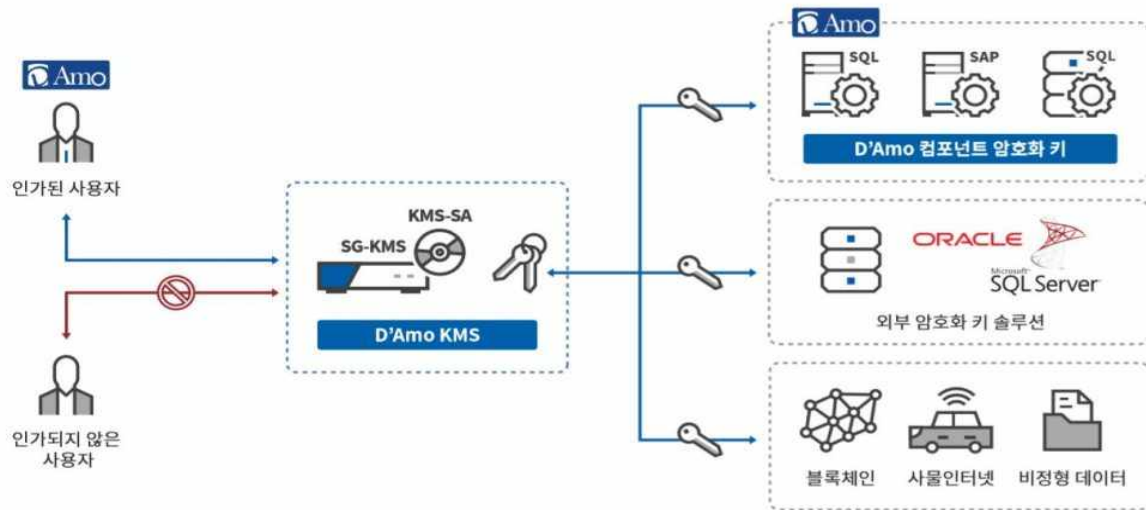
- 암호자산 보호용 암호키 관리 시스템 기술 분야는 정보보호 소프트웨어와 관련성이 크며, 이를 통해 전자지갑 기술, 커스터디 서비스 기술 및 안전한 다자간 계산 기술 등 개발에 활용
- 임베디드SW 및 하드웨어 칩을 활용하여 블록체인 암호키의 안전한 저장 관리를 위한 하드웨어 기반 전자지갑 개발에 활용
- 인터넷 서비스 소프트웨어 기술 등을 활용하여 블록체인 암호키에 대한 커스터디 서비스 제공에 필요한 서비스 기술을 개발에 활용
- 암호 소프트웨어 기술을 활용하여 암호키의 안전한 원격관리와 다자간 계산을 통해 안전한 전자서명 제공에 필요한 서비스 기술 개발에 활용

◎ 블록체인 KMS 및 HSM 시장

□ 국내외 암호자산 기반 서비스에 대한 보안솔루션으로 KMS 및 HSM 도입

- 탈레스(Thales)는 국내외 암호화폐 거래소에 암호화 및 키 관리 시스템에 활용되는 보안솔루션 ‘하드웨어 보안 모듈(HSM)’을 국내외 암호화폐 거래소에 공급
 - 결제회사 Saifu의 암호화폐 액세스 및 관리를 구현한 온라인 및 모바일 뱅킹 서비스, 써트온(CERTON)의 암호화폐 거래소인 ‘코인링크’ 등에서 탈레스 사의 하드웨어 보안 모듈을 이용 중
- 펜타시큐리티는 금융사 블록체인 공동인증 서비스 ‘체인 ID’에 자사 암호 키 관리 솔루션을 공급. 펜타시큐리티의 암호키 관리 솔루션 D’Amo KMS는 모든 암호화 키에 대한 통합 관리 기능, 강력한 키 관리 및 감사 기능, 보안관리자 및 DBA에 대한 접근제어 기능, 보안성 강화 패키지 등을 제공

[펜타시큐리티의 D'Amo KMS 시스템]



* 출처 : 펜타시큐리티 'D'Amo KMS' 제품 소개

◎ 커스터디(Custody) 서비스 시장

- 최근 기관 투자자들의 가세로 암호화폐 보관 서비스(커스터디, Custody)가 부상 중으로, 이들을 위한 안전한 키 관리 시스템의 개발이 요구되는 실정
- 커스터디는 안전한 자산 보관, 결제, 대여, 세금, 배당 회계 등 잦아 보유 시 발생할 수 있는 모든 부가 서비스를 포함하는 개념임. 암호화폐 업계에선 주로 암호화폐 계정에 접근하는 개인 키 관리를 가리키는 용어로 쓰임. 백트는 여기에 비트코인 결제 및 청산, 관련 보험까지 커스터디 업무의 요건으로 추가
- 미국에서는 최근 뉴욕증권거래소의 모회사 인터콘티넨탈거래소(ICE)이 디지털자산 거래소 백트(Bakkt) 출범 전 비트코인 커스터디(수탁업무) 서비스를 선보임. 미 선물 상품 거래 위원회(CFTC)와 뉴욕 금융청 승인하에 암호화폐의 안전한 보관과 관리 업무에 공을 들이고 있다는 것을 확인 가능
- 골드만삭스의 투자를 받은 비트코인 지갑업체 빗고(BitGo), 글로벌 코인거래소 코인베이스는 물론 글로벌 금융공룡 피델리티도 암호화폐 커스터디의 중요성을 강조하고 있음. 이는 코인거래소 제도화 정책과 관련 사업 확장을 위한 의지로 풀이
- 국내에서는 아톰릭스랩(Atomrigslab)이 KB 국민은행과 암호화폐를 포함해 디지털 자산 커스터디 사업을 위해 손을 잡았고, 하드웨어 지갑 회사인 아이오투러스트와는 다자간 보안 컴퓨팅(SecureMPC) 기술을 활용한 하드웨어 및 소프트웨어 개발을 위해 협력
- 커스터디 서비스가 암호화폐 뿐만 아니라 암호 자산 시장에까지 확대될 경우, 상당히 큰 시장이 될 전망
- 피어테크(Peertec)는 블록체인 자산 커스터디 사업을 위한 암호화폐 지갑 키 관리 메커니즘에 대한 특허 출원을 2019.10 마침. 이는 피어테크가 2019. 7 런칭한 디지털 자산 커스터디 파생토큰 서비스 '그로우(GROW)'에 적용

나. 시장 분석

(1) 세계시장

- ☐ 2019년 MarketsandMarkets의 보고서에 의하면 글로벌 공개키 인프라(PKI:Public Key Infrastructure) 시장 규모는 15.1%의 연평균 성장률(CAGR)로 2019년 17억 달러에서 2024년까지 36억 달러로 성장할 것으로 예상
 - PKI 솔루션은 데이터 흐름을 암호화하여 서버와 클라이언트 간의 통신을 보호하고 보다 많은 기관이 지속적인 규정 준수를 보장하기 위해 PKI 솔루션을 채택
 - PKI는 디지털 인증서를 생성, 관리, 배포 및 저장하고 공개 키 암호화를 관리하는 데 사용되는 역할, 정책 및 절차 세트를 정의하여 맬웨어 및 파일 기반 공격으로부터 조직을 보호하기 위해 PKI 솔루션이 주목
 - 공개키 인프라 시장에서 가장 큰 시장규모는 은행, 금융 서비스 및 보험 (BFSI) 산업

[공개키 인프라(PKI:Public Key Infrastructure) 세계시장 규모 및 전망]

(단위 : 십억 달러, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
합계	1.5	1.7	2	2.3	2.6	3.1	3.6	15.1

* 출처 : Public Key Infrastructure Market - Global Forecast to 2024, MarketsandMarkets(2019)

(2) 국내시장

- ☐ 블록체인 암호키 관련된 정확한 국내 시장규모는 없어 가장 유사한 시장인 금융서비스 분야의 블록체인의 국내시장 규모를 살펴본 결과 65%의 연평균 성장률(CAGR)로 2019년 98억 원에서 2024년까지 1,987억 원으로 성장할 것으로 예상

[국내 금융서비스 분야 블록체인 국내시장 규모 및 전망]

(단위 : 억 원, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
합계	98	186	274	505	735	1,361	1,987	65

* 출처: Blockchain Market by Component, MarketsandMarkets(2020)의 데이터를 기준으로 비트코인 화폐별 거래량 중 원화 점유율 2.97%(코인힐스 2020.12.30.)을 근거로 네모아이씨지 재가공(환율:1100원/달러)

- ☐ 국내 보안 기업들에게 블록체인 기술은 매력적인 신사업
 - 기존 퍼블릭 블록체인이 개인 간의 거래를 분산 저장하고 구성원들 간의 정보공유에 초점을 맞췄다면, 보안 업계에서는 블록체인 기술의 보안성에 초점을 맞추는 중
- ☐ 사용자 인증 분야에서는 통합 인증 플랫폼에 블록체인을 결합
 - 사용자 인증 분야에서는 데이터의 기밀성 보장, 암호키 라이프사이클 관리, 블록체인 기반 생체인증 등을 통해 보안성을 강화. 이 분야의 대표적인 기업으로 라온시큐어, 한컴시큐어 등이 있음

3. 기술개발 동향

☐ 기술경쟁력

- 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템은 미국이 최고기술국으로 평가되었으며, 우리나라는 최고기술국 대비 84.8%의 기술수준을 보유하고 있으며, 최고기술국과의 기술격차는 1.6년으로 분석
- 중소기업의 기술경쟁력은 최고기술국 대비 76.9%, 기술격차는 2.2년으로 평가
- EU(86.9%)>한국(84.8%)>중국(77.3%)>일본(73.0%)의 순으로 평가

☐ 기술수명주기(TCT)¹⁹⁾

- 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템은 4.19의 기술수명주기를 지닌 것으로 파악

가. 기술개발 이슈

☐ 클라우드 문서보안의 첫 걸음, 보안사고를 막는 키(Key) 관리 방안

- 다양한 디바이스의 보급과 5G로 대두되는 통신 기술의 발전에 따라 정보관리의 중요성 확산으로, 다양한 클라우드 서비스의 제공, 협력사와의 면밀한 협업, 모바일 업무환경, 사물 간 인터넷 혹은 개체 간 인터넷으로 정의되는 IoT(Internet of Things) 등 다양한 환경안에서 클라우드 문서보안은 필수
- 암호화의 핵심인 키 관리는 암호화 기법 및 프로그램을 사용하여 평문 정보를 알아볼 수 없는 정보로 변환하는 과정으로 허가된 이 외에는 읽을 수 없도록 정보 부호화
- 기업 및 공공 기관은 개인정보보호법에 의거, 필수적으로 개인정보를 암호화, 빈번하게 일어나는 개인정보 대량 유출 사고 등으로 개인정보를 포함한 기업의 중요정보를 안전하게 저장 및 관리하는 암호기술의 연구 필요성 확대

☐ HSM, TPM 등 하드웨어 칩 활용 기술 개발

- 보안토큰(Hardware Security Module: HSM)은 암호 프로세서를 하드웨어 내부에 탑재하여 개인키나 전자서명 등 기밀성을 요하는 정보를 생성 관리하도록 구현한 하드웨어 장치
 - HSM 내부에 개인키를 저장 관리함으로써 개인키에 대한 유출을 방지
- TPM(Trusted Platform Module)은 TCG(Trusted Computing Group)에서 키, 패스워드 등의 비밀정보를 안전하게 저장하기 위해 구현한 하드웨어 보안 디바이스
 - 개인키나 비밀 키 등과 같은 키 저장과 관리를 안전하게 지원

19) 기술수명주기(TCT, Technical Cycle Time): 특허 출원연도와 인용한 특허들의 출원연도 차이의 중앙값을 통해 기술 변화속도 및 기술의 경제적 수명을 예측

[암호화의 종류 및 특성]

암호화 종류	특성	방식
대칭키 암호화	대칭키 암호 알고리즘을 사용하여 전송하고자 하는 평문을 암호화하고 복호화하는데 동일한 키를 사용	<ul style="list-style-type: none"> • 공개키 암호화 방식에 비해 빠른 처리속도를 제공하고, 암호키의 길이가 공개키 암호화 방식보다 상대적으로 작아서 일반적인 정보의 기밀성을 보장하기 위한 용도로 사용 • 반면 정보 교환 당사자 간에 동일한 키를 공유하므로 여러 사람과 정보 교환 시 많은 키를 유지 및 관리해야 함 • 국내: SEED, ARIA, HIGHT • 국외: AES, Blowfish, Camelia
공개키 암호화	공개키 암호 알고리즘을 사용하여 암호화하며 공개키와 개인키의 키 쌍이 존재하며 평문을 암호화 하는데 서로 다른 키를 사용	<ul style="list-style-type: none"> • 공개키 암호화 방식은 데이터 암호화 속도가 대칭키 암호화 방식에 비해 느리기 때문에 일반적으로 대칭키 암호화 방식의 키 분배나 전자서명 또는 카드번호와 같은 작은 크기의 데이터 암호화에 많이 사용 • 국외: RSA, ElGamal, ECC
일방향 암호화	해시함수를 이용하여 암호화된 값을 생성하여 복호화 되지 않는 방식	<ul style="list-style-type: none"> • 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해시값 또는 해시 코드라 불리는 값을 생성 동일한 입력 메시지에 대해 항상 동일한 값을 생성하지만 해시값으로 입력메시지를 유추할 수 없어 비밀번호와 같이 복호화 없이 입력 값의 정확성 검증이 필요한 경우 등에 사용 • 국외: SHA-2, SHA-3, RIPEMD-160, Whirlpool

* 출처 : 한국인터넷진흥원 - 개인정보의 암호화 조치 안내서

□ IoT 장비 펌웨어 보안성 검증 기술개발 위해 펌웨어, 하드웨어, 통신채널, 서비스와 같은 서로 다른 4개의 계층에서 새로운 IoT 보안성 검증 프레임워크의 개발 및 보안성 검증을 수행하고 취약점 검증의 개념 증명을 위한 보안 IoT ASIC 칩 개발

- (펌웨어 계층) 모든 종류의 인증서, 개인키, 하드코딩된 암호 및 알려진 취약점과 알려지지 않은 취약점을 검색하기 위해 펌웨어 취약점에 대한 자동화된 분석 방법 개발
- (하드웨어 계층) 비밀키 및 펌웨어 역공학에 이용될 수 있는 명령어 정보가 공개되는지 확인하기 위한 효율적인 부채널 누설 평가 기법 개발
- (통신 계층) 통신 채널의 취약점 분석 기법 및 신뢰성 있는 환경 구축을 위한 보안 채널 프로토콜 개발
- (서비스 계층) 웹서버의 취약성 분석 방법과 연결된 모든 IoT 장치에서 보내진 신호 분석 및 멀웨어 탐지를 모니터링하는 방법 개발

□ 멀티 팩터 인증을 활용한 키 운영 통제 기술

- HSM, TPM과 같은 하드웨어 칩은 추가 디바이스를 사용하기 때문에 보안성은 향상되나 비용이 상승하고 벤더 종속성이 발생할 여지가 있음
- 개인키와 별도로 키 사용자 인증을 통해 키 운영 통제를 할 수 있도록 멀티 팩터 인증을 동시에 활용하는 방법으로 개인키 사용을 보호

[멀티 팩터 인증 활용 사례]

방식	설명	특징
개인키 + OTP	OTP 카드 발급 또는 기존 OTP 카드 등록	• OTP 인증과 관련한 추가 설계 및 비용 증가
개인키 + 생체인증	지문, 홍채, 서명 등의 인증 방식	• 생체정보 보관 방식과 미지원 단말 처리 방안
개인키 + SMS(알림톡 등)	SMS, MMS 등의 문자 메시지 추가 인증 방식	• 개인정보보호 및 연계 서비스 처리

* 출처 : 박준한, 김유성, 공수재, “블록체인 구현측면 정보보안 동향 및 시사점”, IITP, 2018.8

□ Secure MPC 관련 기술 부상

- 시큐어 MPC는 거래의 여러 참여자들이 상대방이 투입하는 값을 모르면서도 어떤 함수의 연산에 안전하게 참여할 수 있는 기술. 이와 같은 연산이 가능한 이유는 영지식증명, 동형암호화, 시크릿쉐어링 등 암호학의 모든 성과와 최신 기법들을 집대성한 성과. 시큐어 MPC 기술을 활용하면 보안 컴퓨팅에 지출되는 막대한 보안 비용도 절감할 수 있을 것으로 전망
- 시큐어 MPC의 핵심 알고리즘은 개인키 등 비밀값을 잘게 쪼개 필요할 때만 조합해 사용하는 시크릿쉐어링 알고리즘임. 시크릿쉐어링이라는 개념은 RSA 비대칭암호화 기술을 만드는 데 기여한 샤미르에 의해 수학적으로 고안
- MPC를 풀기 위한 접근에는 야오의 혼란 회로(Yao's garbled circuits)에 기반한 접근과 비밀 공유에 기반한 접근 두 가지 주요 접근이 존재

□ 블록체인 거래 보호를 위한 다중 서명(Multi-signature) 기술

- 기본 비트코인 시스템은 하나의 주소에 하나의 개인키가 연결된 단일 서명 거래 방식을 사용하여 개인키에 대한 해킹이 SPOF(Single Point of Failure)로 인지
- 다중 서명을 사용하는 경우에는 n개의 개인키 중에서 m개의 서명이 있어야 거래 인증이 가능하므로 블록체인 사용자를 보호하는 방법으로 다양하게 활용 가능

[전자지갑(Wallet) 기반의 다중 서명 활용 사례]



* 출처 : 어준선, “블록체인을 이용한 멀티 시그니처 전자지갑 기술 및 금융보안”, 코인플러그, 2016

□ 생체인식 기반 블록체인 암호 키 복구 기술

- 블록체인 참여자의 개인키 복구 시스템은 그 개인키를 특정 누군가에게 맡기는 것을 의미하므로 자칫 블록체인의 탈중앙기구화라는 중요한 장점을 없애지게 하기도 하며, 반대로 개인키 관리에 관한 책임을 개인에게 모두 지우면 블록체인이 대중적인 서비스로 나아가는데 장애요소가 되기도 함
- 산업계와 정부가 합리적인 기준을 만들기 위해 노력하고 있으며 특히 생체정보를 이용하고 물리적으로 분리된 공간에서만 개인키를 복구할 수 있도록 하는 방안에 대해 중점적으로 검토 중

□ 블록체인 암호화폐 거래소 해킹 방지를 위해 암호화폐를 안전하게 보관 및 관리할 뿐 아니라 블록체인 암호키(전자서명키)를 전자지갑 장치내부에서 운영할 수 있게 전자지갑 키 관리 기술이 개발, 상용화되고 있음

- 블록체인 서비스가 다양해짐에 따라서 암호키 관리 기술도 보다 심층적이고 다양하게 연구 및 개발이 요구
- 암호화폐 거래소 등은 암호화폐를 보관하는 지갑(Wallet)이라고 하는 파일 저장소에 가치를 저장하는 경우가 많은데, 이 때 컴퓨터의 다른 모든 가치 저장소와 마찬가지로 침해, 조작, 절도, 전송이 가능
- 사람들은 종종 보호용 PIN/비밀번호를 잊거나 저장소가 있는 하드 드라이브를 잃어버리는데, 이러한 경우에도 블록체인 암호화폐에 대한 해당 가치 저장소를 영원히 되찾을 수 없는 경우 발생

나. 생태계 기술 동향

(1) 해외 플레이어 동향

- ☐ (Fujitsu) Thales의 클라우드 HSM 및 키 관리 솔루션 도입하여 Managed PKI 보안 및 엔터프라이즈 데이터 암호화 제품 확대
 - Fujitsu가 Managed PKI(공개키 기반구조, Public Key Infrastructure) 보안 및 엔터프라이즈 데이터 암호화 제품을 지원하기 위해 주요 정보 시스템, 사이버 보안 및 데이터 보안의 선두업체인 Thales의 클라우드 하드웨어 보안 모듈(HSM)과 키 관리 솔루션 채택
 - 고객에게 안전한 암호키 라이프사이클 관리 제공을 위한 Thales 키 관리 플랫폼과 자사의 새로운 엔터프라이즈 데이터 암호화 서비스를 통합
 - PKI 인프라의 보안 수준을 높이고 규제를 준수하고자 Fujitsu의 핵심 보안 인프라 내에서 Thales의 클라우드 HSM인 DPoD(Data Protection on Demand)를 활용해 안전한 클라우드 기반의 키 관리 서비스와 서비스형 HSM제품 제공
 - 새로운 엔터프라이즈 데이터 암호화 서비스는 보호 포트폴리오의 일부로 고객들은 온프레미스 및 하이브리드, 멀티 클라우드 환경 전반에 걸쳐 데이터를 안전하게 보호할 수 있게 될 것으로 예상
- ☐ (Nasdaq) 비트코인 및 암호화폐를 도입하였으며, 엔터프라이즈 블록체인 솔루션을 개발하는 벤처 스타트업에 상당한 금액을 투자
- ☐ (Goldman Sachs) 실시간 주식, 채권 등에 대한 거래가 가능하고 블록체인의 분산된 네트워크 원장에 즉시 기록되는 세틀코인 개발
 - 거래 비용을 대폭 낮추고 보안성이 강화될 것으로 기대되며 금융비용 절감 효과가 연간 200억 달러에 달할 것으로 추정
- ☐ (Blocky Wallet) 미디움(Medium)에 의해 세계 최초로 마이크로 SD 카드를 기반으로 하는 전자지갑으로 인정받고 있음
 - 다른 콜드월렛과 달리 별도의 디바이스가 아닌 스마트폰에 내장하는 마이크로 SD 카드에 암호화폐를 담을 수 있다는 점에 차별화를 두고 개발
 - SD카드 내부에 마련된 트러스트존(Trust Zone)에 프라이빗키가 저장되도록 함으로써 스마트폰이 해킹을 당하더라도 마이크로 SD카드 안의 프라이빗키는 안전하게 관리 가능
 - 별도의 카드나 단말기 형태로 휴대해야 했던 기존의 콜드월렛과 달리 스마트폰에 장착하는 마이크로 SD 카드를 지갑으로 사용하기 때문에 분실 우려가 적고 편리함

[블로키월렛 제품 운용개념]



* 출처 : TheScienceTimes, '해킹 불가능한 암호화폐 지갑 탄생', 2019.3

□ (Thales eSecurity) 다양한 애플리케이션을 통해 클라우드 및 엔터프라이즈 환경의 암호키 관리를 간소화하고 보안을 강화한 키관리 솔루션 개발

- FIPS 140-2 인증을 받은 가상 어플라이언스 또는 하드웨어 어플라이언스를 기반으로 민감한 환경의 데이터 보호, 키 관리 중앙화 및 조직화를 통해 고객이 암호키에 대한 강력한 제어권과 보호를 할 수 있도록 지원
- CipherTrust Cloud Key Manager : 멀티클라우드, 하이브리드 등 다양한 기업 환경의 암호키에 대한 수명주기 관리를 중앙에서 관리할 수 있도록 지원
- Enterprise Key Management : Vormetric Data Security Platform의 일부인 Vormetric Key Management 솔루션은 데이터베이스 TDE, KMIP클라이언트 및 Vormetric Data Security Platform의 암호키를 관리하고 보호

□ (Fidelity, Coinbase, Bakkt, BitGo) 기관투자자를 위한 암호자산 커스터디 서비스를 제공

- 방대한 규모의 자금을 거래하거나 보관해야 하는 기관은 커스터디 서비스를 활용함으로써 직접 자산을 관리하는 것에 따른 해킹이나 분실, 도난 등의 위험을 낮추고자 전문 수탁 기관에 맡기고 있는데, 암호자산 관리에 적용할 경우 기관투자자들은 자금뿐만 아니라 암호자산 키(Key) 관리에 대한 우려 없이 투자를 진행할 수 있고, 외부 도난과 사고로 인한 손실도 방지할 수 있기 때문에 암호자산 시장이 제도권에 진입하기 위해서는 커스터디 서비스를 먼저 구축해야 한다고 지적
- (Fidelity Investment) '19년 3월에 기관투자자를 대상으로 커스터디 서비스를 출시
- (Coinbase) 뉴욕 금융서비스부 승인을 받아 '19년 7월부터 암호화폐 커스터디 서비스를 시작
- (Bakkt) '19.10월에 기관투자자를 대상으로 한 커스터디 서비스를 출시
- (BitGo) 전 세계 비트코인 거래량 중 20% 이상을 처리하며 가장 많은 암호화폐 거래소를 고객사로 확보

(2) 국내 플레이어 동향

- ☐ 국내 IT 대기업들은 암호화폐 이용자 확보 차원에서 암호화폐 지갑을 보유하거나 보안을 강화하는 움직임이 보임
- ☐ (카카오) 모바일 메신저 카카오톡과 연동되는 가상화폐 지갑 ‘클립(Klip)’ 공개
 - 카카오 블록체인 자회사 그라운드X의 ‘클레이튼’에서 메인넷을 개발한 가상화폐 지갑으로, 개발 중인 가상화폐 ‘클레이(KLAY)’를 비롯한 자체 블록체인 플랫폼 ‘클레이튼(Klaytn)’ 기반의 가상화폐를 보관하는 지갑
 - 단, 비트코인 등 시중에 이미 통용되는 가상화폐는 미보관할 예정
 - 사용자는 각종 게임 금융 콘텐츠 이용을 통해 보상 받은 가상화폐를 다시 여러 온라인 서비스 이용 과정에서 현금처럼 지급 하는 등 ‘클립’에서 한 번에 관리 가능
 - 별도의 애플리케이션을 설치하지 않아도 누구나 이용할 수 있도록 카카오톡 내 지갑 기능을 추가하여 카카이가 확보한 5,000만 명의 국내 외 이용자의 접근성을 높임
 - 거래 정보를 저장한 블록을 모든 구성원이 네트워크를 통해 분산 저장하고 일정 시간마다 암호화 후 체인 형태로 연결하여 저장하는 ‘클레이튼’의 기술로 높은 보안성을 보장
 - 이 외에도 ‘클레이튼’의 초당 거래량(TPS)은 8,000건으로 이더리움(Ethereum)보다 400배 빠른 정도로 다른 블록체인 플랫폼보다 빠른 거래 처리속도를 보일 것으로 보임
- ☐ (삼성) 갤럭시S10 시리즈에 처음으로 가상화폐 지갑 ‘삼성 블록체인 키 스토어’를 탑재하며 블록체인 기반 분산애플리케이션(DApp 디앱) 생태계 확장에 주력
 - 갤럭시S10 사용자는 ‘삼성 블록체인 키스토어’를 통해 스마트폰에 가상화폐를 저장했다가 필요할 때마다 지인에게 송금하거나 가상화폐로 결제가 가능한 상점에서 물건 구매 가능
 - 또한 ‘이더리움(ETH)’ 기반의 가상화폐만 지원했던 ‘삼성 블록체인 키스토어’에 ‘비트코인(BTC)’과 ‘클레이(KLAY)’를 추가하며 협력체계를 구축
 - 디앱 개발자 앱에서 ‘삼성전자 키스토어’를 훨씬 쉽게 연동할 수 있도록 ‘삼성 블록체인 소프트웨어 개발 키트(SDK)’를 공개
- ☐ (네이버) 일본 자회사 라인의 블록체인 플랫폼 ‘링크체인(LINK Chain)’을 지원하는 가상화폐 지갑 ‘링크미(LINK ME)’를 출시
 - 사용자는 개인정보를 필요로 하지 않는 소셜 로그인 방식으로 실명인증(KYC)을 거쳐 코인을 거래
 - 블록체인 개발자회사 ‘엔블락’과 ‘엔체인’을 통해 동영상 게임 쇼핑 결제 등 광범위한 분야의 디앱을 개발
 - 자체 블록체인 소프트웨어 개발자 키트(SDK)를 공개하여 개발자가 키트를 활용하여 디앱을 만들 수 있도록 개발 환경을 구축
 - 기존의 라인 메신저 사용자가 별도의 애플리케이션을 설치하지 않아도 서비스를 이용할 수 있도록 라인 메신저 내 지갑 기능을 추가

- (펜타시큐리티) 다양한 암호화폐를 한 곳에서 보관하고 관리하여 암호화폐 사용자와 암호화폐 서비스제공자에게 편의성과 보안성을 제공하는 암호화폐 전용 지갑 PALLET을 개발하여 모바일, 개인 사용자 디바이스 및 카드, 거래소 및 엔터프라이즈 제품으로 구성

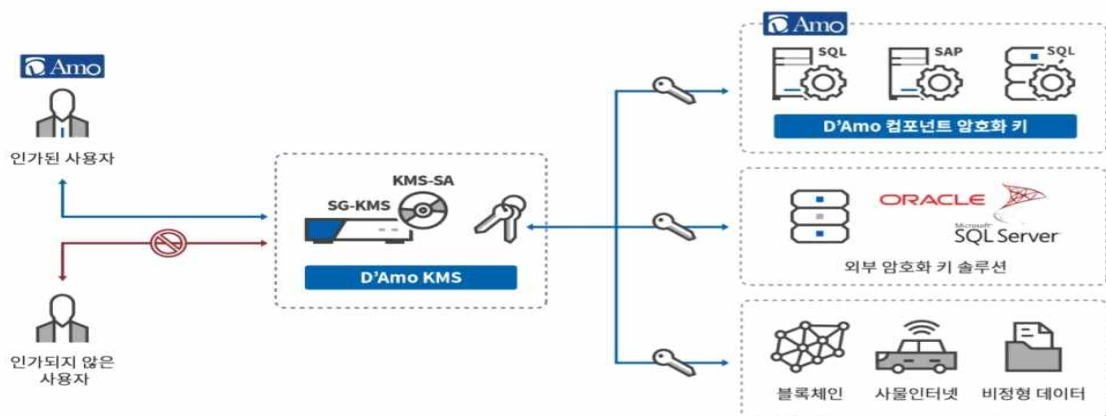
[펜타시큐리티 블록체인 솔루션, PALLET X]



*출처 : 펜타시큐리티 홈페이지

- (PALLET X) 거래소 및 암호화폐 취급 기업을 위한 암호화폐 지갑으로 핫 월렛과 콜드 월렛으로 구성. 또한 서버 Appliance 타입으로 제공되어 보다 높은 보안을 제공
- (D'Amo) KMS 개발. 양자난수 생성기와 하드웨어 보안모듈(HSM)을 추가한 보안성 강화 패키지 개발. KMIP 일부 준용

[펜타시큐리티의 D'Amo KMS 시스템 구성도]



* 출처 : 펜타시큐리티 'D'Amo KMS' 제품 소개

- (케이사인) 키관리시스템(KMS) 솔루션 개발

- 수협은행, MG새마을금고, KB손해보험 등 금융권과 경찰청, 한국전력, 한국교육학술정보원 등 공공기관, 그리고 일반기업 등 100여 고객사에 공급

다. 국내 연구개발 기관 및 동향

(1) 연구개발 기관

[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야 주요 기술개발 기관]

기관	소속	연구분야
한국전자통신연구원	정보보호연구본부	<ul style="list-style-type: none"> • 디바이스 DNA 기반 안전한 암호키 생성/사용/은닉 기술, 글로벌 표준(KMIP) 키관리 기술 및 이의 드론 보안 적용 기술 • 양자 암호, 인공지능 학습기반 암호 등의 신규 논리 기반의 암호 설계 기술 • 데이터 공유/활용 서비스 환경에서 데이터 프라이버시 보호를 위한 데이터 중심 암호 기술
소프트웨어정책연구소	SW정책·인재연구팀	<ul style="list-style-type: none"> • 블록체인 안전관리체계 리모델링 연구

(2) 기관 기술개발 동향

☐ (티모넷)

- 하드웨어 기반의 안전한 암호키 관리 기술을 적용한 가상자산 보호를 위한 전자지갑 서비스 기술 개발 (2020-11-12~2022-11-11)
 - 하드웨어 기반 암호키의 안전한 키관리 기술과 안전한 사용을 위한 secure environment 관련 기술
 - 블록체인 암호자산 암호키 복구기술
 - 블록체인 암호키 사용자 인증기술
 - 블록체인 자산 보호를 위한 전자지갑 기술

☐ (비트로봇)

- 안전한 암호키 관리를 위한 국내 최초 블록체인 기반 PKI 다중서명 솔루션 개발 (2019-12-02~2020-12-01)
 - Byzantine Fault Tolerance 합의 알고리즘 구현
 - 블록체인 네트워크 구축 및 마스터 노드 운영
 - m/n 다중서명 알고리즘 개발
 - 블록체인 간 데이터를 중계하는 오라클 프로그램 개발
 - 다중서명 방식의 백업/복구 시스템 개발
 - 암호키의 안전한 보관을 위한 하드웨어 연동 모듈 개발
 - 웹 사용자 인터페이스 개발
 - 감독기관 제출용 감사보고서 생성 및 검증 기능 개발

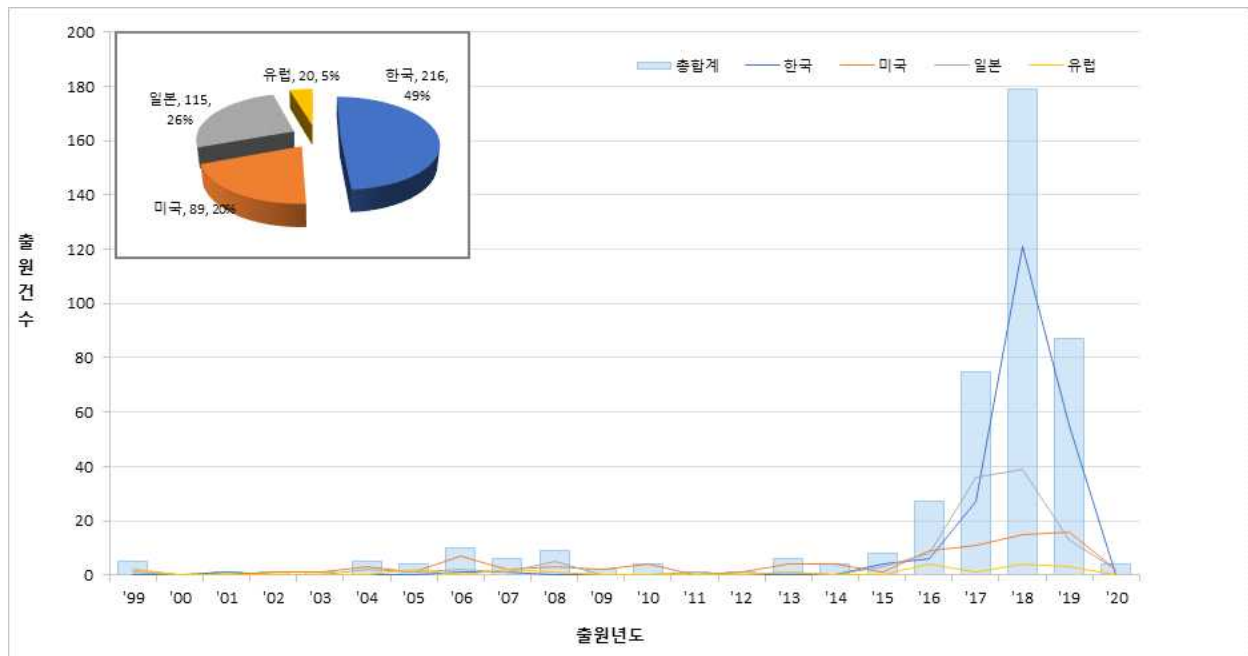
4. 특허 동향

가. 특허동향 분석

(1) 연도별 출원동향

- 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템은 '16년부터 급격한 성장을 보임
 - 각 국가별로 살펴보면 한국이 가장 활발한 출원활동을 보이고 있음
- 국가별 출원비중을 살펴보면 한국이 전체의 49%의 출원 비중을 차지하고 있어, 최대 출원국으로 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야를 리드하고 있는 것으로 나타났으며, 일본은 26%, 미국은 20%, 유럽은 5% 순으로 나타남

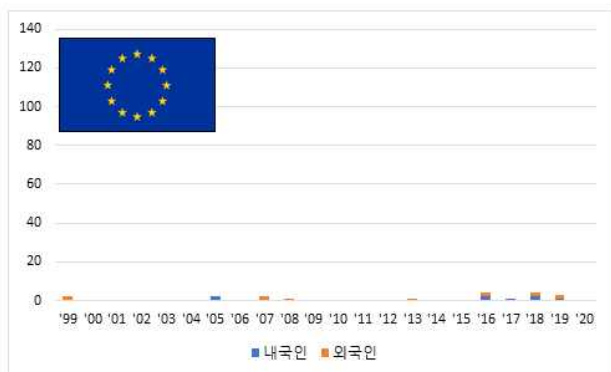
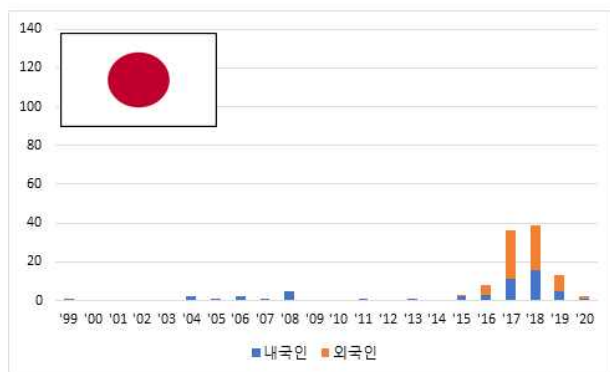
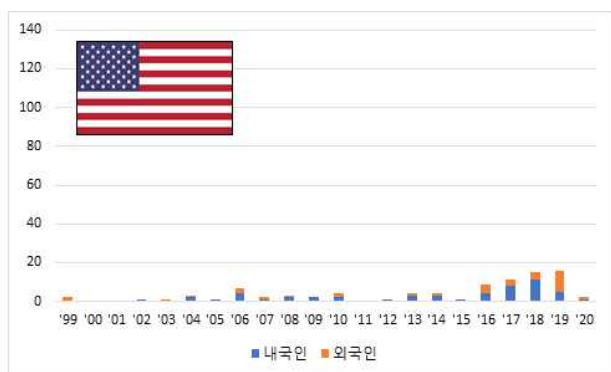
[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 연도별 출원동향]



(2) 국가별 출원현황

- ☐ 한국의 출원현황을 살펴보면, '17년부터 해당 기술의 출원이 급격히 증가하는 추세
 - 내국인 위주의 출원이 진행되고 있음
 - 한국 기술의 양적 흐름은 '18년에 가장 많은 특허를 출원
 - 한국의 출원 수는 미국, 유럽, 일본에 비해 가장 많은 특허를 출원
- ☐ 미국의 출원현황은 출원수가 매년 20건 이하로, 뚜렷한 증감 동향이 나타나지 않음
- ☐ 유럽의 출원현황은 출원수가 매년 10건 이하로, 뚜렷한 증감 동향이 나타나지 않음
- ☐ 일본의 출원현황을 살펴보면, 한국과 유사한 동향을 보임

[국가별 출원현황]



(3) 기술 집중도 분석

□ 전략제품에 대한 최근 기술 집중도 분석을 위한 구간별 기술 키워드 분석 진행

- 전체 구간(1999년~2020년)에서 블록 체인, 블록 체인 네트워크, Block Chain, 블록 체인 트랜잭션 등 키워드가 다수 도출
- 최근 구간 분석 결과, 최근 1구간(2012년~2015년)과 비교할 때 2구간(2016년~2020년)에서 스마트 컨트랙트, 분산 저장 키워드가 많이 등장하는 것으로 보아 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야에서는 블록체인 자산 보호와 암호키 복구 등의 기술 관련 연구개발이 활발한 것으로 추정

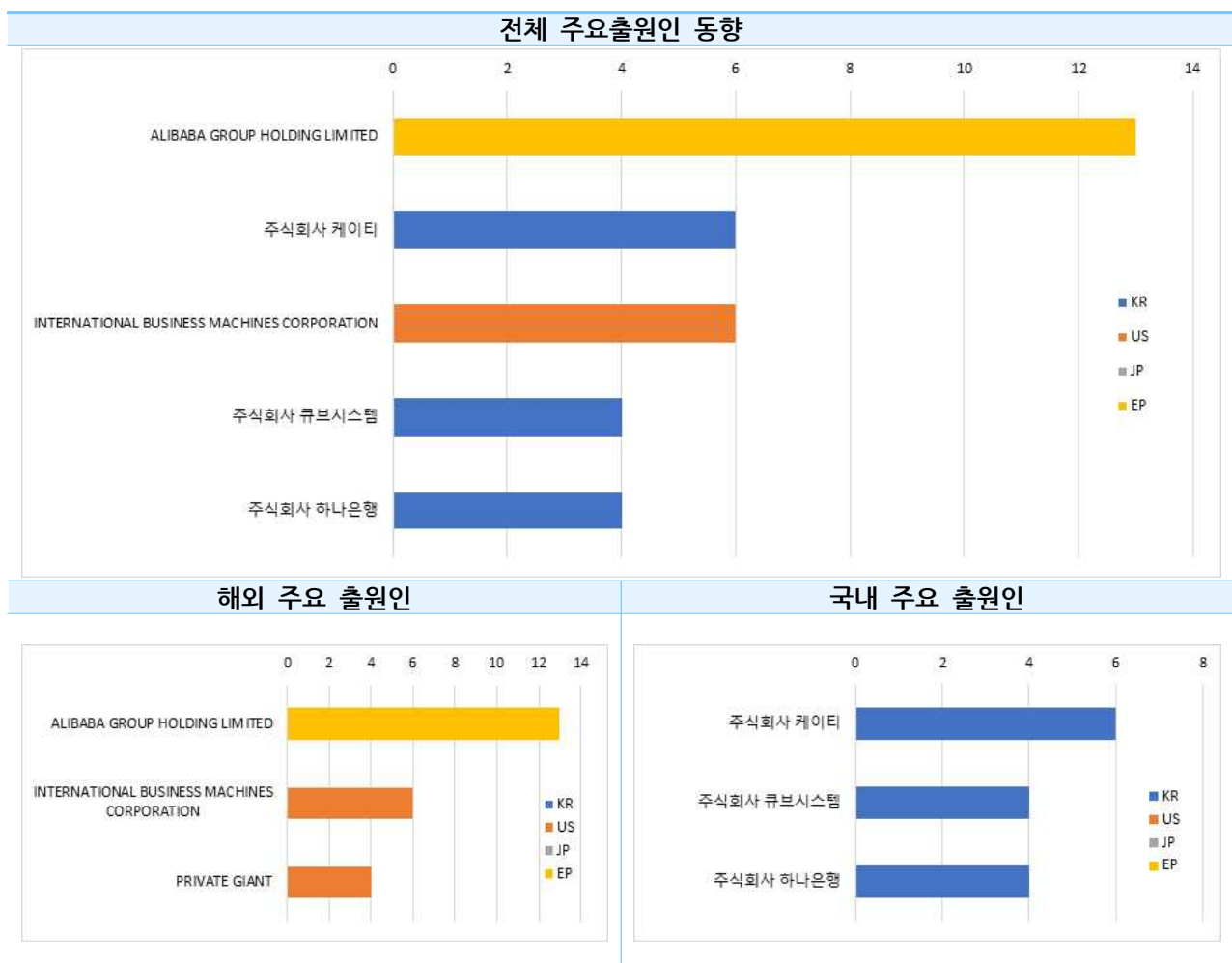
[특허 키워드 변화로 본 기술개발 동향 변화]

전체구간(1999년~2020년)	
<ul style="list-style-type: none"> • 블록 체인, 블록 체인 네트워크, Block Chain, 블록 체인 트랜잭션, 블록 체인 기술, Previous Block, 블록 체인 노드, 사용자 단말, 스마트 컨트랙트, 분산 저장 	
최근구간(2012년~2020년)	
1구간(2012년~2015년)	2구간(2016년~2020년)
<ul style="list-style-type: none"> • Encrypted Content, Encrypted Stream, Initialization Vector, Decrypt Block, Requiring Decryption, Previous Block, Access Distribution Point, Regulates Access, Distribution Point Provides, Corresponding Block 	<ul style="list-style-type: none"> • 블록 체인, 블록 체인 네트워크, Block Chain, 블록 체인 트랜잭션, 블록 체인 기술, 블록 체인 노드, 스마트 컨트랙트, 분산 저장, 사용자 단말, 트랜잭션 데이터

나. 주요 출원인 분석

- 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템의 전체 주요출원인을 살펴보면, 주로 한국 국적의 출원인이 다수 포함되어 있는 것으로 나타났으며, 제 1 출원인으로는 중국의 ALIBABA GROUP HOLDING LIMITED인 것으로 나타남
 - 제 1 출원인인 ALIBABA GROUP HOLDING LIMITED의 출원은 유럽에 집중된 경향을 보임
- 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 관련 기술로 블록체인을 다루는 대기업에 의한 출원이 대다수를 차지
 - 국내에서는 중소기업(개인), 대기업의 활발한 출원이 이루어짐

[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 주요출원인]



(1) 해외 주요출원인 주요 특허 분석

◎ ALIBABA GROUP HOLDING LIMITED

- ☐ ALIBABA GROUP HOLDING LIMITED은 중국 온라인 쇼핑몰을 운영하는 기업으로, 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템과 관련하여, 블록체인을 통한 서비스 요청 기술에 특화된 특허를 다수 출원

[ALIBABA GROUP HOLDING LIMITED 주요특허 리스트]


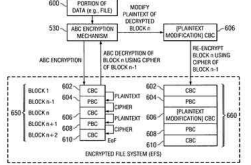
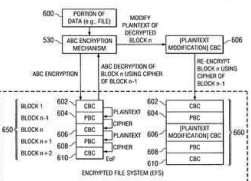
등록번호 (출원일)	명칭	기술적용분야	도면
JP6675518 (2018.03.19)	서비스 요구를 처리하기 위한 방법 및 장치	서비스 요청이 합의 검증을 통과하면, 각각의 합의 노드는 블록체인에 서비스 데이터를 저장하는 대신 블록체인에 서비스 데이터의 요약을 저장	<pre> graph TD S101[타겟 서비스에 서비스 요청] --> S102[서비스 요청을 타겟 서비스에 전송] S102 --> S103[타겟 서비스가 서비스 요청을 수신] S103 --> End[완료] </pre>

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ IBM(International Business Machines)

- IBM은 미국의 다국적 기업으로, 다수의 블록체인 관련 특허를 보유하고 있으며, 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템과 관련한 특허를 미국, 유럽, 일본에 출원

[IBM 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
US10644959 (2017.01.25)	Method and framework for protocol to optimize edge side dynamic response system with context propagation for iot	IoT에 대한 컨텍스트 전파(context propagation)를 갖는 에지 사이드 동적 응답 시스템을 최적화하기 위한 프로토콜	
US8107621 (2008.08.20)	Encrypted file system mechanisms	암호화된 파일 시스템 내의 파일에 필요한 복호화(decryption) 및 재암호화(re-encryption)의 양을 감소시키기 위해 암호화 방법	
US7428306 (2006.04.18)	Encryption apparatus and method for providing an encrypted file system	파일이 수정될 필요가 있는 경우에, 암호화된 파일 시스템 내의 파일에 필요한 복호화(decryption) 및 재암호화(re-encryption)의 양을 감소	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

☐ PRIVATE GIANT는 미국 기업으로, 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템과 관련한 특허를 미국 및 유럽에 출원

[PRIVATE GIANT 주요특허 리스트]

[illegible]


* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

(2) 국내 주요출원인 주요 특허 분석

◎ 주식회사 케이티

- ☐ 주식회사 케이티는 한국의 유무선 통신 서비스 기업으로, 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 기술과 관련된 특허를 6건 출원하였으며, 출원을 진행한 6건 중 1건의 특허가 등록

[주식회사 케이티 주요특허 리스트]

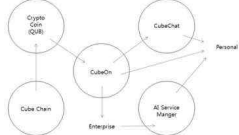
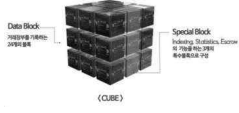
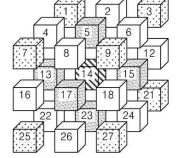
등록번호 (출원일)	명칭	기술적용분야	도면
KR2094497 (2017.08.16)	블록체인 기반의 스토리지 서비스 제공 시스템 및 방법	블록체인 기반의 스토리지 서비스 제공 시스템	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 주식회사 큐브시스템

- 주식회사 큐브시스템은 한국의 블록체인 기술과 전자상거래 전문 기업으로, '18년도 4월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- 주식회사 큐브시스템의 공개특허를 대상으로 분석한 결과, 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템과 관련된 특허를 4건 출원

[주식회사 큐브시스템 주요특허 리스트]

공개번호 (출원일)	명칭	기술적용분야	도면
KR2019-0115433 (2019.05.08)	큐브체인을 활용한 사회관계망 서비스 시스템	블록화와 큐브화 를 거치는 2중 암호화 방식으로 인터넷이라는 신뢰가 형성되지 않은 공간에서 신뢰를 만들어 데 이터를 이동시킬 수 있는 혁신적인 암호화 기술	
KR2019-0115431 (2019.05.08)	큐브 형태의 데이터 연결 구조 및 연결 방법	기존의 블록체인보다 더욱 빠르고, 정밀한 데이터 처리 및 강화된 보안시스템 을 가진 블록체인 플랫폼	
KR2019-0115354 (2018.04.02)	블록 체인 블록들의 연결 방법	블록들을 위상적 관계로 연결하여 블록들의 연결을 입체적으로 구성하는 각각의 블록의 연결을 다중화하는 방법	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 주식회사 하나은행

- ☐ 주식회사 하나은행은 한국의 금융 기업으로, '19년도 1월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- 주식회사 하나은행은 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 기술과 관련된 특허를 4건 출원

[주식회사 하나은행 주요특허 리스트]

공개번호 (출원일)	명칭	기술적용분야	도면
KR2020-0093917 (2019.01.29)	회원 관리 네트워크, 회원 관리 시스템 및 회원 관리 방법	회원 및 업체에게 관리의 편의성을 제공하고 위변조가 방지될 수 있는 식별 수단을 제공하며, 보상의 과정을 자동화하여 공정하고 편리한 회원 관리를 수행	
KR2020-0093882 (2019.01.29)	투표 관리 시스템, 투표자 단말 및 그의 투표 관리 방법	블록체인 기반의 플랫폼을 이용하여 투표를 진행하는 투표 관리 시스템	
KR2020-0093971 (2019.01.29)	생산 관리 네트워크, 금융 기관 시스템 및 생산 관리 방법	생산자 시스템 및 상기 배송자 시스템 중 적어도 하나는 정보를 암호화하여 블록체인 데이터로서 공유	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

다. 기술진입장벽 분석

(1) 기술 집중력 분석

- ☐ 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 관련 기술에 대한 시장관점의 기술독점 현황분석을 위해 집중률 지수(CRn: Concentration Ratio n, 상위 n개사 특허점유율의 합) 분석 진행
- 상위 4개 기업의 시장점유율이 0.07로 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야에 있어서 독과점 정도는 낮은 수준으로 판단
 - 국내 시장에서 중소기업의 점유율 분석결과 0.68로 해당 기술에 대하여 중소기업의 진입이 용이하다고 판단됨

[주요출원인의 집중력 및 국내시장 중소기업 집중력 분석]

주요 출원인 집중력	주요출원인	출원건수	특허점유율	CRn	n
	ALIBABA GROUP HOLDING LIMITED(중국)	13	3.0%	0.03	1
	주식회사 케이티(한국)	6	1.4%	0.04	2
	INTERNATIONAL BUSINESS MACHINES CORPORATION(미국)	6	1.4%	0.06	3
	주식회사 큐브시스템(한국)	4	0.9%	0.07	4
	주식회사 하나은행(한국)	4	0.9%	0.08	5
	서강대학교산학협력단(한국)	4	0.9%	0.08	6
	PRIVATE GIANT(미국)	4	0.9%	0.09	7
	SIEMENS AKTIENGESELLSCHAFT(독일)	4	0.9%	0.10	8
	AOL INC.(미국)	4	0.9%	0.11	9
	DELL PRODUCTS, LP(미국)	3	0.7%	0.12	10
	전체	440	100%	CR4=0.07	
국내시장 중소기업 집중력	출원인 구분	출원건수	특허점유율	CRn	n
	중소기업(개인)	123	68.0%	0.68	
	대기업	22	12.2%		
	연구기관/대학	36	19.9%		
	전체	181	100%	CR중소기업=0.68	

(2) 특허소송 현황 분석

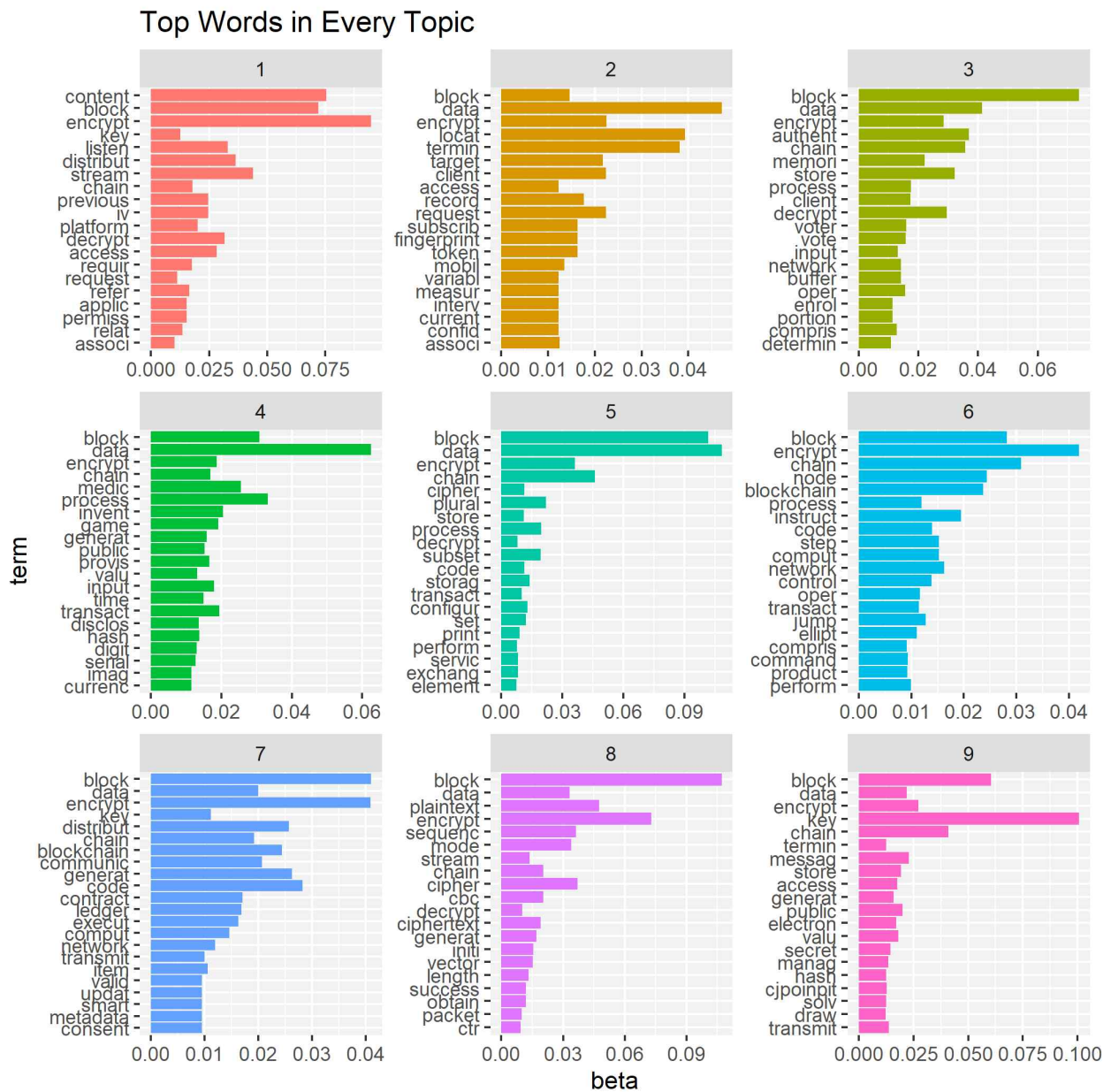
- ☐ 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야 관련 특허소송 이력은 검색되지 않음
 - 따라서 국내기업이 미국시장에 진입하는 경우, 해당 분야를 선점할 수 있을 것으로 판단
 - 다만, 블록체인과 관련해서는 4개의 소송이 검색

5. 요소기술 도출

가. 특허 기반 토픽 도출

- 149개의 특허의 내용을 분석하여 구성 성분이 유사한 것끼리 클러스터링을 시도하여 대표성이 있는 토픽을 도출

[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템에 대한 토픽 클러스터링 결과]



나. LDA²⁰⁾ 클러스터링 기반 요소기술 도출

[LDA 클러스터링 기반 요소기술 키워드 도출]

No.	상위 키워드	대표적 관련 특허	요소기술 후보
클러스터 01	encrypt, content, block, stream, distribute, listen, decrypt, access, previous	<ul style="list-style-type: none"> • The blockworld project • System and method for using a streaming protocol 	-
클러스터 02	data, locate, terminal, encrypt, client, request, target, record, fingerprint, subscribe	<ul style="list-style-type: none"> • Super cmos devices on a microelectronics system • Method and apparatus for optimized access of security credentials via mobile edge-computing systems 	하드웨어 또는 소프트웨어 기반의 안전한 키 보관 기술 및 신뢰 계산 기술 등의 개인 키 보관 및 안전한 사용을 위한 Secure Environment 관련 기술
클러스터 03	tamper, conversion, intent, mobile online, facial, administrate, estimate, signal, pos, fall	<ul style="list-style-type: none"> • Authentication method for a client over a network • Method and system for verifying a voter through the use of blockchain validation 	블록체인 암호키 사용자 인증 기술
클러스터 04	key, data, block, instruct, vote, communicate, encrypt, control, permission	<ul style="list-style-type: none"> • User identification management system and method • Secret key management system in distributed network and secret key management method 	키의 안전한 생성, 유통 보관, 폐기를 위한 키 관리 기술
클러스터 05	recommend, transmitted, confidential, mortal, hyper, android, duplicate, fix, ship	<ul style="list-style-type: none"> • Postage printing system including prevention of tampering with print data sent from a postage meter to a printer • Nonvolatile storage medium control device, nonvolatile storage medium control method, and nonvolatile storage medium control program 	암호키 관리 전송구간 보안 위협 방지 기술
클러스터 06	invest, transceiver, hyperspectral, inductor, debit, impair, decipher, anytime, page, intelligence	<ul style="list-style-type: none"> • Encryption method, decryption method, encryption device, and decryption device • Exchanging asset, maintenance, and spares parts information via blockchain 	블록체인 자산 보호를 위한 전자지갑 기술
클러스터 07	block, encrypt, code, generate, distribute, blockchain, communicate, data, chain, contract	<ul style="list-style-type: none"> • Authenticate transactions of secured file in blockchain • Blockchannel scanner systems and methods 	블록체인 암호키 관리 서비스 기술
클러스터 08	block, encrypt, plain text, cipher, sequence, mode, data, chain, cipher text	<ul style="list-style-type: none"> • Method and device for digital data blocks encryption and decryption • Method and apparatus for secure access to a mobile edge computing gateway device based on a subscriber location fingerprint 	블록체인 암호화 기술
클러스터 09	block-board, life, world, negate, tamper, fire, actual, sub-platform, fuse	<ul style="list-style-type: none"> • User identification management system and method • Secret key management system in distributed network and secret key management method 	블록체인 암호키 사용자 인증 기술

20) Latent Dirichlet Allocation

다. 특허 분류체계 기반 요소기술 도출

- ☐ 암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 관련 특허에서 총 10개의 주요 IPC코드(메인그룹)를 산출하였으며, 각 그룹의 정의를 기반으로 요소기술 키워드를 아래와 같이 도출

[IPC 분류체계에 기반한 요소기술 도출]

IPC 기술트리		
(서브클래스) 내용	(메인그룹) 내용	요소기술 후보
(G06F) 전기에 의한 디지털 데이터처리	• (G06F-021) 부정행위로부터 프로그램 또는 데이터, 그 컴퓨터 부품을 보호하기 위한 보안 장치	하드웨어 또는 소프트웨어 기반의 안전한 키 보관 기술 및 신뢰 계산 기술 등의 개인 키 보관 및 안전한 사용을 위한 Secure Environment 관련 기술
(G06Q) 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 데이터 처리 시스템 또는 방법; 그 밖에 분류되지 않는 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 시스템 또는 방법	• (G06Q-040) 금융; 보험; 세무 전략; 법인세 또는 소득세의 처리	블록체인 자산 보호를 위한 전자지갑 기술
	• (G06Q-050) 특정 사업 부문에 특히 적합한 시스템 또는 방법, 예. 공익사업 또는 관광	
	• (G06Q-010) 경영; 관리	
	• (G06Q-020) 지불 체계, 방식 또는 프로토콜	
	• (G06Q-030) 거래, 예. 쇼핑 또는 전자상거래	
(G09C) 암호 또는 비밀의 필요성을 포함하는 다른 목적에 의한 암호화 또는 암호해독장치	• (G09C-001) 주어진 부호의 순서, 예. 이해할 수 있는 원문,을 부호 또는 군을 바꿔 놓음으로써, 또는 그것들을 미리 정한 방식에 의한 원위치에 되돌림으로서 이해할 수 없는 부호의 순서로 변형시키는 장치 또는 방법	키의 안전한 생성, 유통 보관, 폐기를 위한 키 관리 기술 (KMS : Key Management System)
(H04K) 비밀통신; 통신방해	• (H04K-001) 비밀통신	
(H04L) 디지털 정보의 전송, 예. 전신통신	• (H04L-029) 그룹 1/00에서 H04L 27/00의 하나에도 포함되지 않는 배치, 장치회로 또는 시스템	
	• (H04L-009) 비밀 또는 보안통신을 위한 배치	

라. 최종 요소기술 도출

- ☐ 산업·시장 분석, 기술(특허)분석, 전문가 의견, 타부처 로드맵, 중소기업 기술수요를 바탕으로 로드맵 기획을 위하여 요소기술 도출
- ☐ 요소기술을 대상으로 전문가를 통해 기술의 범위, 요소기술 간 중복성 등을 조정·검토하여 최종 요소기술명 확정

[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야 요소기술 도출]

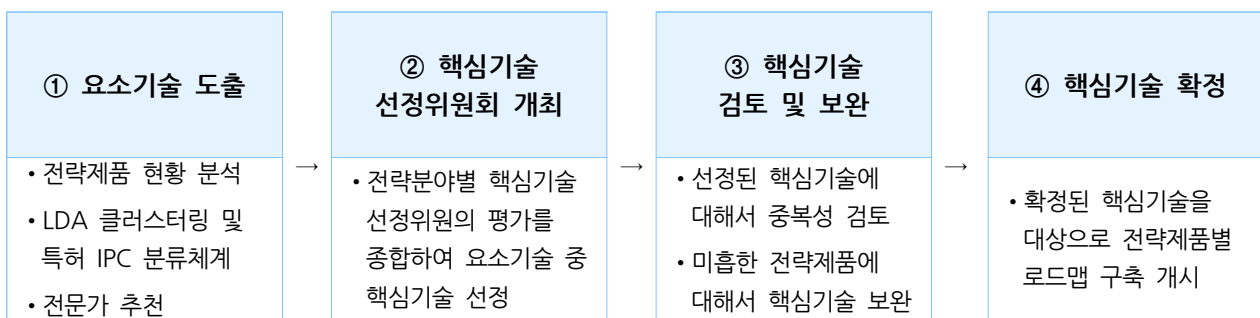
요소기술	출처
하드웨어 또는 소프트웨어 기반의 안전한 키 보관 기술 및 신뢰 계산 기술 등의 개인 키 보관 및 안전한 사용을 위한 Secure Environment 관련 기술	특허 클러스터링, IPC 기술체계, 전문가추천
키의 안전한 생성, 유통 보관, 폐기를 위한 키 관리 기술 (KMS : Key Management System)	특허 클러스터링, IPC 기술체계, 전문가추천
블록체인 자산 보호를 위한 전자지갑 기술	특허 클러스터링, IPC 기술체계, 전문가추천
블록체인 암호키 복구 기술	전문가추천
블록체인 암호키 사용자 인증 기술	특허 클러스터링, 전문가추천
암호키 관리 전송구간 보안 위협 방지 기술	특허 클러스터링, 전문가추천
블록체인 암호키 관리 서비스 기술	특허 클러스터링, 전문가추천
다중 전자 서명 기술	전문가추천
블록체인 암호화 기술	특허 클러스터링, 전문가추천
공개 키 기반구조 기술 (PKI : Public Key Infrastructure)	전문가추천

6. 전략제품 기술로드맵

가. 핵심기술 선정 절차

- ☐ 특허 분석을 통한 요소기술과 기술수요와 각종 문헌을 기반으로 한 요소기술, 전문가 추천 요소기술을 종합하여 요소기술을 도출한 후, 핵심기술 선정위원회의 평가과정 및 검토/보완을 거쳐 핵심기술 확정
- ☐ 핵심기술 선정 지표: 기술개발 시급성, 기술개발 파급성, 기술의 중요성 및 중소기업 적합성
 - 장기로드맵 전략제품의 경우, 기술개발 파급성 지표를 중장기 기술개발 파급성으로 대체

[핵심기술 선정 프로세스]



나. 핵심기술 리스트

[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야 핵심기술]

핵심기술	개요
하드웨어 또는 소프트웨어 기반의 안전한 키 보관 기술 및 신뢰 계산 기술 등의 개인 키 보관 및 안전한 사용을 위한 Secure Environment 관련 기술*	• 암호자산 운영환경에서 핵심적인 암호키의 안전한 보관과 더불어 해당 암호키를 활용한 전자서명 등 사용과정도 안전하게 수행할 수 있도록 해주는 기술
키의 안전한 생성, 유통 보관 및 폐기를 위한 키 관리 기술(KMS: Key Management System)*	• 암호자산 운영 시 사용되는 암호키의 생성부터 폐기까지 운영과정을 안전하게 해주면서 키의 생명주기 동안 암호키 보관 및 관리를 안전하게 할 수 있도록 지원해주는 기술
블록체인 자산 보호를 위한 전자지갑 기술	• 사용자의 암호자산을 사용자 단말 등 저장 관리 수단을 이용하여 안전하게 보관하고 관리할 수 있도록 제공해주는 기술
블록체인 암호키 복구 기술	• 암호자산 운영 시 사용되는 암호키 분실 또는 손실 시 해당 암호키를 복구할 수 있게 지원함으로써 암호자산 운영에 문제가 발생하지 않도록 지원하는 기술
블록체인 암호키 사용자 인증 기술	• 암호자산 운영환경에서 전자지갑 이용, 암호키 관리 및 복구 서비스 이용 등 과정에서 해당 서비스 이용을 통제하기 위해 암호키 사용 권한을 갖고 있는 사용자인지 확인할 수 있도록 지원해주는 기술

다. 중소기업 기술개발 전략

- ☐ 정부의 블록체인 기술 발전전략에 따른 R&D 지원 기회 활용 및 관련 업체 간 협력체 구성을 통해 적극적으로 블록체인 암호키 관리 시스템 개발 참여 및 관련 진출 전략 수립 필요
- ☐ 블록체인 플랫폼 도입 확대에 따라, 단기적으로는 전자지갑 기술과 같은 키 보호 제품 기술 개발을 실시하고, 중장기적으로는 암호키 복구 기술 등 키 관리 서비스 기술 개발로 시장 대응 필요

라. 기술개발 로드맵

(1) 중기 기술개발 로드맵

[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야 중기 기술개발 로드맵]

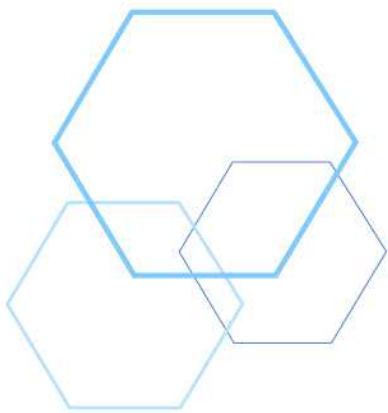
암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템	암호자산 기반 서비스의 보안 위협에 대한 안전성 제공			
	2021년	2022년	2023년	최종 목표
하드웨어 또는 소프트웨어 기반의 안전한 키 보관 기술 및 신뢰 계산 기술 등의 개인 키 보관 및 안전한 사용을 위한 Secure Environment 관련 기술				3개 노드가 암호키를 보관
키의 안전한 생성, 유통 보관 및 폐기를 위한 키 관리 기술(KMS: Key Management System)				100,000개 수준의 키 관리가 가능한 KMS
블록체인 자산 보호를 위한 전자지갑 기술				3종 이상의 전자 지갑에 대한 서비스 제공
블록체인 암호키 복구 기술				5개 이상의 노드에서 암호키 보관 및 복구가 가능
블록체인 암호키 사용자 인증 기술				6종 이상의 인증 수단 제공

(2) 기술개발 목표

- ☐ 최종 중소기업 기술로드맵은 기술/시장 니즈, 연차별 개발계획, 최종목표 등을 제시함으로써 중소기업의 기술개발 방향성을 제시

[암호자산 기반 서비스의 보호를 위한 암호키 관리 시스템 분야 핵심요소기술 연구목표]

핵심기술	기술요구사항	연차별 개발목표			최종목표	연계R&D 유형
		1차년도	2차년도	3차년도		
하드웨어 또는 소프트웨어 기반의 안전한 키 보관 기술 및 신뢰 계산 기술 등의 개인 키 보관 및 안전한 사용을 위한 Secure Environment 관련 기술	암호키 보관 노드의 수 확대	1개	2개	3개	3개	산학연
키의 안전한 생성, 유통 보관 및 폐기를 위한 키 관리 기술(KMS: Key Management System)	관리 대상이 되는 암호키의 수 확대	1,000	10,000	100,000	100,000	창업성장
블록체인 자산 보호를 위한 전자지갑 기술	다양한 종류의 전자지갑에 대해 서비스 제공	1종	2종	3종	3종	상용화
블록체인 암호키 복구 기술	암호키 보관 노드의 수 확대	2개	3개	5개	5개	기술혁신
블록체인 암호키 사용자 인증 기술	다양한 인증 수단 제공	2종	4종	6종	6종	상용화



전략제품 현황분석

블록체인 기반 불법 거래 탐지 시스템



블록체인 기반 불법 거래 탐지 시스템

정의 및 범위

- 블록체인 기반 불법 거래 탐지 시스템이란 다양한 블록체인 네트워크 실시간 모니터링 에이전트를 구동하여 모든 거래를 수집하고 수집된 거래 내역을 중앙 분석 서버에서 저장 및 분석, 중앙 분석 서버에서는 수집한 거래 내역을 분석하여 특정 주소가 전송하거나 수신한 내역, 주소 간의 상관관계, 다량의 거래 내역 발생 등의 이벤트를 추출하여 스팸 및 불법 거래를 탐지할 수 있는 시스템
- 거래 허용 참여자 관리 기술, 블록체인 모니터링 에이전트 데이터 수집 기술, 블록체인 스마트 컨트랙트 악성코드 탐지 기술, 블록체인 인프라 기술 등을 포함

전략 제품 관련 동향

시장 현황 및 전망	제품 산업 특징
<ul style="list-style-type: none"> • (세계) 금융서비스 분야의 세계시장 규모는 2018년 3억 달러에서 연평균 성장률 65% 성장하여 2024년 61억 달러 규모에 이를 것으로 전망 • (국내) 금융서비스 분야의 국내시장 규모는 2018년 98억 원에서 2024년 1,987억 원으로 연평균 성장률 65.0%로 성장 	<ul style="list-style-type: none"> • 블록체인 기술은 금융 및 ICT와의 융합 산업 등을 포함, 전 산업 분야에서 활용되면서 비즈니스 환경을 바꿀 것으로 예상 • 금융기관은 다량의 거래정보를 보유하고 있어 올바른 거래정보를 바탕으로 불법 거래를 탐지하는 시스템 개발 추진 중
정책 동향	기술 동향
<ul style="list-style-type: none"> • 미래창조과학부가 'K-ICT 시큐리티 발전 전략'의 4가지 중점 추진과제 발표. '글로벌 시장을 선점하는 원천 보안기술 개발' 과제에서 FDS 언급 • 파밍·스미싱 등 금융 사기 예방을 위한 능동형 모바일 결제사기 대응 기술과 개인용 이상거래탐지시스템(FDS)을 개발할 것이라 발표 	<ul style="list-style-type: none"> • 불법 거래 탐지 시스템의 각 요소 기술에 대한 충분한 표준화 논의가 필요 • 다크 코인의 익명성 악용사례 증가에 따른 암호화폐 거래 추적 기술 필요 • 다량의 거래 정보를 블록체인에 저장하여 불법 거래를 탐지하기 위해서는 다양한 요소기술이 검증되고 분석이 필요
핵심 플레이어	핵심기술
<ul style="list-style-type: none"> • (해외) Nestle, Carrefour, Hacera, Mipasa, IBM, Binance, Bitstamp, Nasdaq, Alibaba, ANSA • (대기업) 삼성 • (중소기업) 인섹시큐리티,페이게이트,아르고스,노르마,업비트 캐서레스트,수호 	<ul style="list-style-type: none"> • 블록체인 비정상거래 탐지 및 차단 기술 • 블록체인 모니터링 에이전트 데이터 수집 기술 • 블록체인 스마트 컨트랙트 악성코드 탐지 기술 • 거래 데이터 판독 시스템 • 공격 가시성을 위한 거래내역 추적 기술

중소기업 기술개발 전략

- 금융 분야에서의 수요가 가장 크지만, 스마트 컨트랙트를 사용하는 블록체인 기반의 각 활용 산업의 시장을 창출하려는 시도가 필요
- 3세대 블록체인에서 지원하는 다양한 개발 언어(파이썬, 자바 등)를 활용하여 기존에 있는 프로그램을 벤치마킹하는 개발 전략도 존재

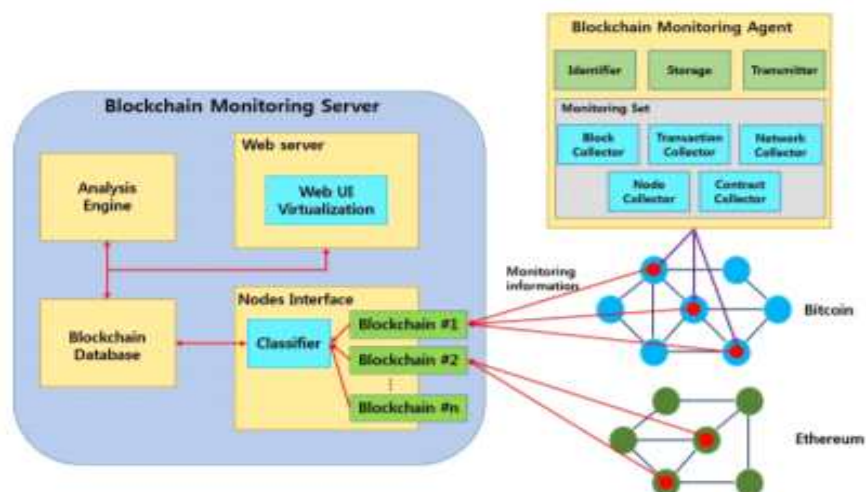
1. 개요

가. 정의 및 필요성

(1) 정의

- ☐ 블록체인 불법 거래 탐지 기술은 블록체인 상에서 거래 데이터를 수집하여 해당 거래가 비정상적인지 아닌지 판단하고, 탐지된 데이터와 연계된 블록을 블록체인에 등록하는 기술
- ☐ 다양한 블록체인 네트워크에 실시간 모니터링 에이전트를 구동하여 모든 거래를 수집하고 수집된 거래 내역을 중앙 분석 서버에서 저장 및 분석, 중앙 분석 서버에서는 수집한 거래 내역을 분석하여 특정 주소가 전송하거나 수신한 내역, 주소 간의 상관 관계, 다량의 거래 내역 발생 등의 이벤트를 추출하여 스팸 및 불법 거래를 탐지할 수 있는 시스템
- ☐ 머신러닝, 빅데이터 기술을 활용하고 시각화 기술을 접목해 중앙 서버에 저장된 다양한 다량의 거래 내역 및 스팸/불법 거래 내용을 분석하여 예측 가능
- ☐ 블록체인 불법 거래 탐지 기술은 다양한 유형의 불법 거래 탐지를 위해 필요한 기술로, 블록체인 거래 데이터의 유효성을 보장
 - 거래 데이터를 블록체인 상에서 수집하기 위한 블록체인 모니터링 에이전트 데이터 수집 기술, 거래 데이터의 유효성을 판단하는 거래 데이터 판독 시스템 기술이 존재
 - 블록체인 불법 거래 데이터 유형에는 이중 지불, 유출된 키 서명, 정책 미준수 거래, 악의적인 스마트 컨트랙트에 의한 거래 등
 - 불법 거래 데이터가 포함된 블록을 블록체인 상에 등록하여 해당 거래 데이터가 다른 유효한 거래의 입력 필드로 사용되는 것을 사용자들로 하여금 감시할 수 있도록 함

[블록체인 네트워크 모니터링 시스템]



* 출처 : '블록체인 네트워크 모니터링 및 분석시스템' 포항공과대학교

(2) 필요성

☐ 산업 전반에 블록체인 인프라 사용 증가

- 금융 분야에서는 암호화폐의 사용뿐만 아니라, 핀테크 기술, 해외 송금 및 결제 시스템과 연계하여 블록체인을 사용 중
- 산업 분야에서는 자동차, 유통, 헬스케어, 에너지 개발, 부동산, 미디어와 같은 다양한 전통적인 산업 분야에서 데이터 무결성, 투명성을 위해 블록체인을 사용 중
- 공공 분야에서는 국가 차원으로 공공 행정 정보와 국민 신원 데이터, 자산거래 내역 공증, 복지서비스 제공 등에 적극적으로 블록체인 도입을 진행하고 있음
- 기업 간의 컨소시엄 구축 시 데이터 공동 관리, 데이터 투명성 보장을 위해 하이브리드 블록체인을 사용 중

☐ 블록체인이 활용이 전 산업 분야로 확대되면서 불법 거래 탐지 기술에 대한 필요성 대두

- 블록체인 상의 블록, 거래, 스마트 컨트랙트의 유효하지 않은 행위로 인해 발생한 거래를 탐지하는 기술에 대한 요구 증대
- 블록체인이 산업 전반에 도입됨에 따라 블록체인 데이터의 양이 증가하고 있으며, 다량의 블록체인 거래 데이터의 유효성을 효율적으로 검증하기 위한 불법 거래 탐지 기술의 필요성이 증가
- 블록체인 거래 데이터는 블록체인 상에 존재하는 이전 거래 데이터에서 파생되기 때문에, 유효하지 않은 불법 거래 데이터로부터 거래 데이터가 파생되지 않도록 해당 불법 거래 데이터를 또 다른 블록체인 상에 등록하여 감시 필요

☐ 기존에 존재하는 블록체인 데이터 분석 서비스의 한계

- Blockexplorer, Etherscan과 같이 블록체인 네트워크상의 블록, 거래 내역 데이터를 제공하여, 이를 기반으로 블록체인 네트워크 데이터를 분석할 수 있는 웹 서비스가 존재
- Blockexplorer, Etherscan은 각각 비트코인 블록체인과 이더리움 블록체인에 대해서만 데이터를 제공하고, 이를 분석하는 것은 사용자의 몫으로, 불법 거래 데이터 탐지 서비스를 제공하지 않음
- 이더리움 블록체인에 등록되는 스마트 컨트랙트의 악의적인 행위를 분석하기 위한 스마트 컨트랙트 감시 도구의 사용은 블록체인 네트워크에 과부하를 초래
- 산업 전반에 걸쳐 사용되고 있는 모든 블록체인 네트워크의 거래 데이터를 수집, 분석하여 거래 데이터의 불법성을 판단하는 서비스는 현존하지 않음

나. 범위 및 분류

(1) 가치사슬

- ☐ 블록체인을 기반으로 한 불법거래 탐지 기술 산업은 후방산업으로 블록체인 모니터링 에이전트 데이터 수집 기술, 거래 허용 참여자 관리 기술 등이 있고 전방산업으로는 거래 추적 및 분석 기술, 기존 시스템 연동 기술 등이 포함
- (후방산업) 블록체인 모니터링 에이전트 데이터 수집 기술, 거래 허용 참여자 관리 기술 등 불법 거래를 추적하기 위해 필요한 데이터에 관한 산업과 블록체인 생성에 관련된 산업을 포함
 - (전방산업) 데이터를 바탕으로 하여 추적, 분석 등을 금융기관, 자동차/유통/헬스케어/에너지 등의 산업 분야와 공공기관 및 민간기업 등 데이터의 분석을 필수적으로 요하는 산업이 전방 산업에 포함

[블록체인 기반 불법거래 탐지 기술 산업구조]

후방산업	블록체인 기반 기술 분야	전방산업
블록체인 생성 기술, 블록체인 모니터링 에이전트 데이터 수집 기술, 거래 허용 참여자 관리 기술	고성능 저비용 합의 기술, 스마트 컨트랙트 검증 기술, 대용량 데이터 처리 기술, 외부 데이터 연동 기술	거래 추적 및 분석 기술, 기존 시스템 연동 기술, 서비스 분야별 특화 블록체인

(2) 용도별 분류

- ☐ 블록체인은 결제/송금, 화폐 등의 기능을 통해 금융 서비스 영역에 먼저 적용되면서 잠재성이 인식된 후, 현재는 다양한 비금융 산업에서의 활용이 확산 중
- 기존 금융시스템의 소요시간, 절차 및 보안 개선 등을 위해 블록체인 기술 도입
 - 기관 간 송금, 결제 등 거래 시 중개 기관이 신뢰를 담보하던 중앙 서버 및 보안 시스템 구축 비용과 같은 번거로움을 제거
 - 스마트 컨트랙트, 고객 정보 공동 관리, 송금, 결제, 채권발행 및 주식거래 등 금융 서비스 대부분에 적용 시도
 - 은행 간 송금 망에 블록체인 기술을 적용하여 중개 은행 없이도 상호 신뢰하에 직접 거래하여 절차를 간소화하여 수수료 비용 절감
 - 고객관리를 위해 블록체인 기반 단일 인증서를 실시간 공유하여 고객이 금융사마다 인증서를 확보해야 하는 번거로움을 제거

2. 산업 및 시장 분석

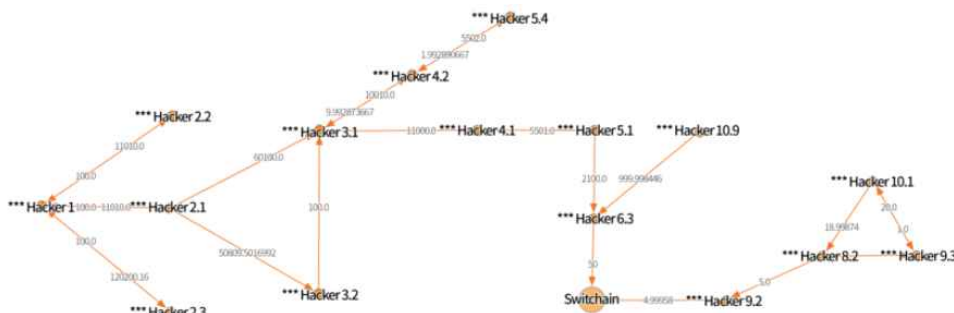
가. 산업 분석

◎ 암호화폐 거래소 보안 강화

□ 암호화폐 거래소 해킹 피해 사례

- 2019년 11월 27일 국내 한 거래소의 지갑에서 알 수 없는 지갑으로 342,000개(한화 약 580억 원)의 이더리움이 비정상 출금되는 사고 발생 후 거래소 측은 모든 암호화폐 입출금을 일시 중단, 이더리움 비정상 출금 사고 공지 및 다른 암호화폐 거래소 담당자들에게 비정상 출금이 발생한 이더리움 주소로부터의 입금을 막아달라 협조
- 공격자는 비정상 출금한 암호화폐를 수많은 지갑으로 분산시켜 그 중 일부를 이미 10여 개의 암호화폐 거래소에 입금한 것으로 확인, 현재 한국인터넷진흥원(KISA)이 침해사고분석단을 파견하여 원인을 분석하고 있지만 유출 경로를 특정하기까지 상당 시간 걸릴 것으로 사료

[Switchchain 거래소로 전송된 이더리움 트랜잭션]



* 출처 : SK인포섹(주) 공식 블로그

□ 암호화폐 거래소 보안

- 최근 발생한 일련의 해킹 사건들로 ISMS나 ISO 인증을 받아도 안전하지 않다는 인식 팽배하고, 실제로 공격자가 마음 먹으면 APT 공격을 통해 추가 보안 대책이 없는 기업에 침투해 정보 혹은 금전 탈취 가능
- 최근 공격 트렌드가 EP(End Point)를 정조준하고 있고 대량의 해킹 메일이나 특정인을 타킷으로 하는 스피어피싱 등이 빈번히 발생함으로 암호화폐 거래소들은 지속적인 보안 대책 필요

□ 암호화폐 관련 법안

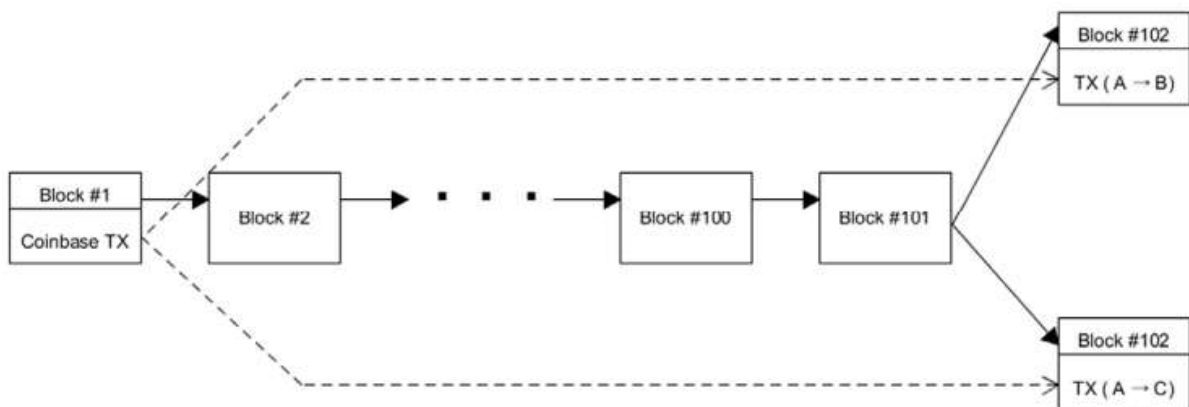
- 암호화폐 거래소의 보안과 관련된 법안으로 2019년 11월 21일 특정 금융거래정보의 보고 및 이용 등에 관한 법률(특금법) 개정안 의결
- 자금 세탁방지기구(FATF)의 권고를 따른 특금법 개정안의 입법으로 암호화폐 거래소들은 이용자의 신원 명시 및 다크 코인 미취급

◎ 금융 산업에서 전자 금융거래의 거래량 증가에 따른 이상거래 탐지시스템 도입 증가

☐ 트랜잭션 역추적을 통한 이중지불 탐지

- 트랜잭션의 고유한 TXID를 이용하여 IN에서 OUT으로의 연결을 지속적으로 따라가 모든 트랜잭션은 블록들에서 찾아낼 수 있음
- 이중지불 트랜잭션을 블록체인에 포함시키는 공격이 시도될 경우, 임의의 노드는 기존에 자신이 가지고 있던 블록체인과 공격자에 의해 만들어진 분기된 블록체인을 가진다는 점을 통해 이중지불 트랜잭션을 탐지

[이중지불 트랜잭션의 연결구조]



* 출처 : 정보과학회 - 블록체인의 이중지불 탐지 알고리즘

- ☐ 전자금융거래의 거래량 증가, 간편결제 수단의 다양화 및 사이버 금융사기 때문에 금융권에서 사전에 이상거래를 탐지 및 차단하여 거래의 보안성을 향상시키는 이상거래 탐지시스템 도입이 증가 중
- ☐ 특히, 암호화폐 거래소를 보이스피싱 탈취 자금의 출금 포인트로 삼으려는 범죄 행각이 늘어나면서, 암호화폐 거래소들이 이상거래 탐지 활동에 적극적으로 나서는 중
 - 주요 거래소들은 이상거래 탐지 시스템을 통해 보이스피싱 등의 범죄를 사전에 차단하는 추세로 업비트는 지난해에만 77건의 이상 거래를 고객 신고전 자체 모니터링으로 탐지하고 선제적으로 출금 정지를 조치하였고 빗썸 역시 지난해 75건의 보이스피싱 사기를 막고 출금을 차단
 - 정보보호관리체계(ISMS) 인증 획득 등과 더불어 핫라인 구축을 통한 자금세탁방지 공조가 암호화폐 산업의 건전성을 높일 것으로 기대
- ☐ 거래 데이터는 신뢰할만한 정보들이어야 하고 무결성이 보장되어야 하는데 블록체인의 확장성, 투명성, 안정성, P2P와 같은 특징이 이에 부합하여 불법 거래 탐지 시스템을 개발하는 데 있어 적합
- ☐ 암호화폐 발행과 거래, 채굴에 있어 양적 성장을 하면서 생긴 폐해를 막기위한 방안으로 이상거래탐지시스템(FDS) 연결을 의무화하고 거래소 투명·혁신 기술연동제 도입 법안을 추진

☐ 은행과 증권사를 중심으로 핀테크 및 IT 기업들과의 제휴를 통하여 블록체인 기술에 대한 투자 증가

- 기존 스위프트(SWIFT) 망을 이용한 해외 송금 소요기간 및 절차 효율화, 금융보안 서비스에 대한 소비자 요구 충족을 위해 블록체인 도입
- 금융보안 확보, 중개/청산 절차 간소화, 결제 및 고객인증 등에 초점을 두어 개발 및 도입 진행 중
- 국제/국내 은행 간 거래 전체를 대상으로 활발한 활동을 벌이는 해외 기업보다 국내 기업은 상대적으로 국제 은행 간 거래에 초점을 둠
- 국내 금융권에서도 블록체인 도입을 효율적으로 추진하기 위해 분야별 이해 관계자들이 공동 연구, 기술 검증 등을 함께 추진하는 컨소시엄을 구성

◎ 투명성을 요구하는 다른 산업 분야에서도 적용 사례 증가

☐ 물류/유통/제조산업 분야에서의 블록체인

- 최근 공급사슬관리(Supply Chain Management: SCM)가 복잡해지고 위조품의 생산과 불투명성이 커져가고 있어, 블록체인을 통해 가시성과 투명성을 제고시킬 수 있음
 - 2015년에 설립된 영국 스타트업 에버레저(Everledger)는 다이아몬드 특성 정보, 감정서, 소유권 상태 등의 정보를 블록체인에 저장 및 관리하는 서비스 제공

☐ 공공 서비스 분야에서의 블록체인

- 전 세계 여러 국가에서 우편 서비스, 토지대장 및 주택관리, 표결관리, 의료기록관리, 군사기밀 송·수신, 여론조사, 선거 등 공정성을 요하는 다양한 공공 서비스 영역에 블록체인 기술들을 적용하는 추세
- 블록체인을 활용하여 각종 공과금 및 과징금의 징수, 납세, 공공 서비스 관련 시민행정, 여권발급, 토지 등기 내역 등 일선 공공업무와 기록들을 통합 관리할 수 있으며 인건비와 서버 관리비 등 운영비용까지도 크게 절감 가능
- 2019년 5월, MirittPTE는 블록체인 기반으로 설문 및 여론조사 정보가 변조나 위조되지 않도록 통합하여 관리할 수 있는 이토니온(Ittonion)을 상장

☐ 사회/문화 분야에서의 블록체인

- 블록체인 상에 콘텐츠 정보가 저장되어 위·변조가 어려우며 복제한 내용도 쉽게 추적이 가능하여 저작권 보호에 뛰어난 장점이 있음
- 예술작품의 출처관리와 소유권 등의 중요한 지적재산권 문제를 해결하는데 유용한 예술산업의 플랫폼으로 자리 매김할 수 있을 것으로 전망

◎ 컨소시엄을 통한 블록체인 플랫폼 개발, 글로벌 기업 및 스타트업의 동향

- ☐ IT, 금융 등 여러 기업이 컨소시엄을 구성하여 블록체인 플랫폼을 함께 개발하는 방식으로 위험부담 감소 및 투자비용 절감
 - 컨소시엄을 통한 은행 간 중개/청산은행 없는 효율적 금융시스템 구현이 목적
 - 금융상품 거래, 무역 계약 등 스마트 계약 기술을 활용한 실증 실험 진행 및 토큰화된 자산 또는 가상 통화 등을 기반으로 은행 간 송금, 결제 업무 진행
- ☐ 기업 및 스타트업을 중심으로 기관이 추진하기 어려운 영역에서 기존 사업의 미비점을 보완하고 이를 통해 가치 창출 시도
 - IBM, MS 등 글로벌 기업은 클라우드 기반의 블록체인 서비스를 통해 별도의 하드웨어 구축 없이 블록체인 기술을 도입할 수 있도록 지원
 - 미국 스타트업들의 시장 점유 비중 및 진출 빈도가 높은 편이며 국내 스타트업의 경우 대부분 영세한 수준

나. 시장 분석

(1) 세계시장

- ☐ Markets and Markets의 보고를 근거로 전망할 때 금융서비스 분야의 세계시장 규모는 2018년 3억 달러에서 연평균 성장률 65% 성장하여 2024년 61억 달러 규모에 이를 것으로 전망

[금융서비스 블록체인 세계 시장규모 및 전망]

(단위 : 백만 달러, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
세계	300	570	839	1,545	2,251	4,167	6,083	65

* 출처 : Global Blockchain Technology Market 2016-2021, MarketsandMarkets(2016)과 Blockchain Market by Component, MarketsandMarkets(2020)을 근거로 네모아이씨지 재가공

(2) 국내시장

- ☐ Markets and Markets의 보고를 근거로 전망할 때 금융서비스 분야의 국내시장 규모는 2018년 98억 원에서 2024년 1,987억 원으로 연평균 성장률 65.0%로 성장
- 금융권, 기업, 스타트업의 지속적 연구와 컨소시엄을 통한 협력 연구 등을 통해 블록체인 기반 금융 서비스 시장은 지속적으로 성장할 전망

[금융서비스 블록체인 국내 시장규모 및 전망]

(단위 : 억 원, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
국내	98	186	274	505	735	1,361	1,987	65

* 출처: Blockchain Market by Component, MarketsandMarkets(2016,2020)의 데이터를 기준으로 비트코인 화폐별 거래량 중 원화 점유율 2.97%(코인힐스 2020.12.30.)을 근거로 네모아이씨지 재가공(환율:1100원/달러)

3. 기술개발 동향

□ 기술경쟁력

- 블록체인 기반 불법 거래 탐지 시스템은 미국이 최고기술국으로 평가되었으며, 우리나라는 최고기술국 대비 89.2%의 기술수준을 보유하고 있으며, 최고기술국과의 기술격차는 0.6년으로 분석
- 중소기업의 기술경쟁력은 최고기술국 대비 86.9%, 기술격차는 1.0년으로 평가
- EU(92.3%)>한국(89.2%)>중국(81.4%)>일본(77.1%)의 순으로 평가

□ 기술수명주기(TCT)²¹⁾

- 블록체인 기반 불법 거래 탐지 시스템은 5.58의 기술수명주기를 지닌 것으로 파악

가. 기술개발 이슈

◎ 블록체인 기반 불법 거래 탐지 시스템 기술 표준화

- 블록체인 기반 불법 거래 탐지 시스템 기술은 전 분야에 걸쳐 블록체인 사용이 증대됨에 따라 중요성이 새롭게 부각되는 기술
 - 현재 표준화가 진행되고 있는 ISO/TC 307(블록체인과 분산 원장 기술)에는 불법 거래 탐지 기술이 포함되지 않음
 - ISO/TC 307/WG2(보안, 프라이버시, 정보 식별을 담당하는 워킹 그룹)에서는 암호, 블록체인 프로토콜, 블록체인 애플리케이션, 프라이버시 보호 기법, 블록체인 구현 및 응용과 같은 기술들에 대한 표준화 논의가 주로 진행 중
- 블록체인 상에 존재하는 불법 거래는 블록체인 프로토콜을 악용하여 블록체인 네트워크 사용자 모두에게 악영향을 주기 때문에 불법 거래 탐지 시스템의 각 요소기술에 대한 충분한 표준화 논의가 필요

◎ 악용된 거래 내역 추적

- 미성년자 여성들의 성 착취물을 제작·유포한 일명 ‘n번방’ 주도자와 가입자들이 가상화폐로 결제한 것으로 파악돼 거래소들의 n번방 수사 협조
 - 빗썸·업비트·코인원·코빗 등 주요 국내 가상화폐거래소들은 n번방 사건과 관련해 수사당국에 협조 회원 정보와 거래 내역 등이 담긴 명단을 경찰에 제출
 - n번방 개설자들은 텔레그램 유료 대화방 회원들에게 입장료로 비트코인(BTC), 이더리움(ETH), 모네로(XMR) 등의 가상화폐를 받은것으로 파악

21) 기술수명주기(TCT, Technical Cycle Time): 특허 출원연도와 인용한 특허들의 출원연도 차이의 중앙값을 통해 기술 변화속도 및 기술의 경제적 수명을 예측

- 2019년 6월 국제자금세탁방지기구(FATF)가 내놓은 가상화폐 자금세탁방지 가이드라인에 따라 우리나라를 포함해 미국 일본 유럽 등 주요국은 기존 금융권에 적용되는 수준의 '트래블룰(송·수신자 간 개인식별정보 확인 절차)'을 적용하고 KYC 절차를 강화
- 국내에서도 이달 5일 가상화폐 거래소 등이 지켜야 할 규제 등을 명시한 '특정 금융거래정보의 보고 및 이용 등에 관한 법률(특금법)' 개정안이 국회를 통과

◎ 암호화폐의 익명성과 불법 거래문제 확산

□ 최근 발생 대부분 사이버 사건/사고에 암호화폐 관련 비중 증가

- 데이터를 암호화하여 데이터의 몸값을 암호화폐로 요구하는 랜섬웨어, 사용자 시스템에 설치되어 암호화폐를 채굴하는 크립토재킹 등 암호화폐의 익명성을 악용
- 이로 인한 공격자의 불법 수익 증가
- 국내 랜섬웨어 침해대응센터는 랜섬웨어로 인한 피해액을 2018년 1조 2천억, 2019년 1조 8천억 원으로 추정
- 2019년 발생 암호화폐 거래소 해킹사고 피해액은 국내 800억 원, 해외 1,100억 원으로 집계

[최근 주요 암호화폐 거래소 해킹 사고]



* 출처: 최근 주요 암호화폐 거래소 해킹 사고, 2020.01, SK 인포섹

□ 프라이버시 보호 측면의 익명성을 위한 다크코인이 불법, 마약, 도박, 탈세 등에 악용

- 암호화폐의 소유자 및 전송받는 사람의 정보를 알 수 없도록 암호화하여 비밀 보장한 기술로 블록체인이 탈중앙화를 표방하고 특정 정부로부터 감시받지 않는다는 자율성의 이념과 일치하며 차세대 암호학의 발전을 앞당긴다는 긍정적 반응으로 시작됨
- 각국에서 암호화폐 규제에 관심을 두기 시작하며, 불법으로 사용될 여지가 높은 다크코인으로 분류되는 암호화폐들을 문제 삼기 시작
- 국내의 한 거래소도 국제자금세탁방지기구(FATF)의 합의를 따라 다크코인으로 분류된 암호화폐들의 유의지정 종목과 함께 상장 폐지 예정 공지

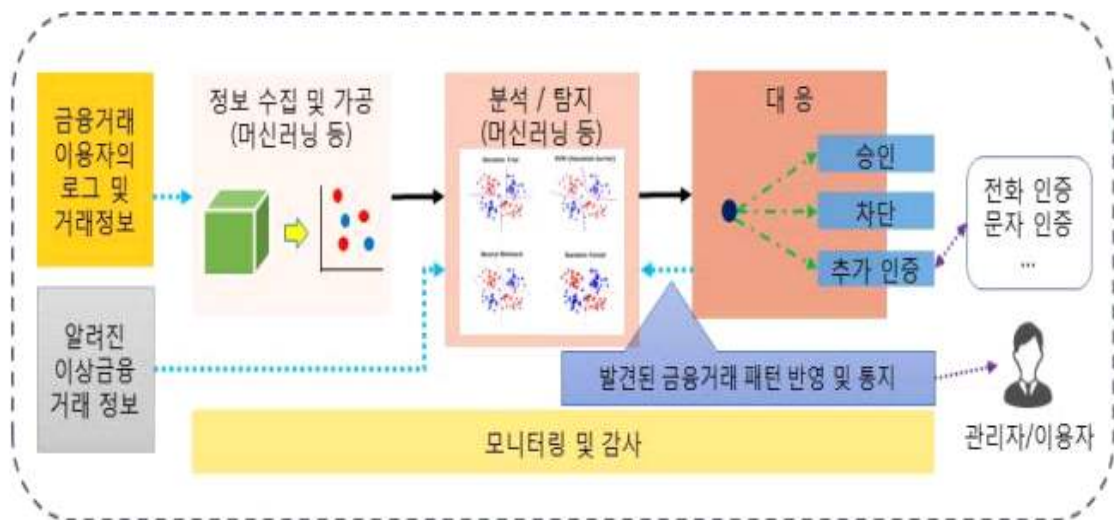
□ 다크 코인과 암호화폐 거래 추적

- 다크 코인의 성질로 인해 해킹 자금 추적 난해, 비트코인과 이더리움 등 시가총액이 높고 거래량이 많은 암호화폐를 탈취한 공격자가 이를 다크 코인으로 스왑하고 해당 코인을 자신의 지갑으로 전송하면 공격자를 추적할 수단이 영영 사라지는 점 악용
- 일반 암호화폐를 이용한 몇 공격자의 경우는 일반 코인 지갑을 수백 개 만들어 탈취한 코인을 분산 전송하는 방식으로 추적의 난항 유발
- 해당 문제들이 대두되며 암호화폐의 트랜잭션 추적 기술 연구 보안 없제의 발전 시작
- 기억 및 조직, 보안 전문가, 커뮤니티 등 집단 지성을 이용하는 읍살라 시큐리티의 보안 플랫폼인 센티넬 프로토콜은 데이터를 수집하고 해킹에 선제적으로 대응하여 수백 개로 쪼개진 해킹 자금의 트랜잭션을 전부 추적 가능 및 현재 국내 거래소의 해킹 자금을 공식적으로 실시간 추적 공지

◎ 비정상 거래 탐지 및 차단 기술

- (머신러닝 기반의 이상거래 탐지시스템) 금융회사에서는 FDS 성능 고도화 방안으로 머신러닝 기반 FDS 운영을 통해 시스템의 향상된 탐지율, 이상 행위에 대한 신속한 대응, 자동화된 탐지 결과 반영 등을 기대
- 머신러닝의 FDS 적용은 국내보다 국외에서 활발히 이루어졌으며, 금융회사들은 주로 머신러닝 기술 전문 업체와 협력하여 시스템을 구축

[이상거래 탐지 시스템(FDS) 구성 예시]



* 출처 : 금융보안원, 머신러닝 기반의 이상거래 탐지시스템 동향, 2017.8

- 금융거래 이용자의 PC, 모바일 등에서 수집한 정보(금융거래 단말기, 로그인, 거래은행 등)를 축적하고, 시스템(분석/탐지 단계)에서 필요한 형태로 전처리
 - 시스템에서 다양한 출처로부터 수집된 대량의 정보를 곧바로 사용하는 것은 어렵고, 시스템 복잡도를 증가시킬 수 있어 정보의 질적 향상 및 양적 감소 등을 위한 과정이 수행
 - 정보가공을 위해 정보의 질적 손실은 최소화하면서 양을 축소하는 머신러닝 방법 중 하나인 차원축소등이 주로 연구
- 전처리된 금융거래 정보와 이상금융거래 유형 정보를 머신러닝으로 분석하여 이상거래 탐지
 - 분석방법으로 오용탐지, 이상탐지 등이 존재
 - 이상탐지 방법에서 사용되는 주요 머신러닝 알고리즘으로 규칙 유도, 랜덤포레스트, 서포트 벡터 머신, 자기조직화맵, 은닉 마코브 모델, 유전 알고리즘, 딥러닝 등이 존재
 - 룰 기반의 오용탐지 방법이 많이 사용되고 있지만 딥러닝 기반의 이상탐지 또는 하이브리드 (오용+이상) 탐지 방법이 도입 중
- 블록체인 모니터링 에이전트 데이터 수집 기술은 블록체인 네트워크의 모든 노드들에 모니터링 에이전트를 구동해 실시간으로 블록 데이터, 거래 데이터, 스마트 컨트랙트 데이터, 노드 데이터를 수집하고 이를 모니터링 서버에 전송
 - 각 블록체인 네트워크마다 데이터의 양식이 다르기 때문에 데이터 수집 방법을 특성화시켜 해당 블록체인에 적합한 방법으로 데이터를 수집
 - 데이터 수집을 효율적으로 진행하기 위해 수집하는 데이터의 종류마다 검출 주기를 데이터 생성 주기에 맞게 다르게 설정
- 거래 데이터 판독 시스템은 필드 값(거래 데이터의 보낸 금액, 받은 금액, 거래 일자, 서명 값)과 연관된 거래 데이터를 바탕으로 분석하여 거래의 유효성을 판단
 - 거래 허용 참여자 관리 기술은 부주의, 해킹 사고로 유출된 개인키가 거래 데이터 서명에 사용되는 것을 제한할 수 있도록 거래 참여자 목록을 관리하는 기술로, 거래 허용 참여자를 추가/삭제 가능
 - 불법 거래로 판단된 거래 데이터를 포함하고 있는 블록을 블록체인 상에 등록하여, 해당 거래 데이터로부터 다른 거래가 파생되지 않도록 사용자들이 감시 가능
- 블록체인 스마트 컨트랙트 악성코드 탐지 기술은 스마트 컨트랙트 코드 상의 취약점, 비즈니스 로직 상의 문제, 악의적인 의도로 프로그래밍 된 스마트 컨트랙트 등으로 인해 발생 될 수 있는 비정상 거래를 차단하기 위해 스마트 컨트랙트의 취약점을 탐지하고 비즈니스 로직의 정확성을 검증

◎ 불법 거래를 탐지하기 위해서는 다양한 요소기술의 검증 및 분석이 필요

- ☐ 블록체인의 블록, 거래내역, 계약, 노드 등에 대한 데이터 수집
 - 불법 거래 탐지 시스템 탐지의 정확성을 위해 이용자 매체 환경정보와 유형 정보의 수집이 필수
 - 전자금융거래 정보, 거래내역(사용자 접속 단말기, OS 및 브라우저, IP 정보 등) 등을 합법적으로 수집하는 기술 필요.
- ☐ 수집된 데이터를 분석하여 고객별 일정 금융패턴 식별하여 분류
 - 실시간으로 많은 정보를 분석, 처리하는 기술 및 스팸 거래 요청을 판독하는 기술 필요
 - 수집된 거래 데이터는 이용자 유형별, 거래유형별 다양한 상관관계 분석 및 규칙 검사 등을 통해 이상 행위를 탐지하여 데이터에 연계된 블록을 블록체인에 등록하는 기술 필요
 - 블록체인에서는 비정상 거래가 발생하더라도 거래 취소 등의 대응이 어려우므로 사전에 탐지 및 차단하는 기술 필요
- ☐ 스마트 컨트랙트와 같은 블록체인 인프라 기술에 존재할 수 있는 보안 취약점을 악용한 악성 행위를 탐지하여 차단
 - 아직 스마트 컨트랙트 코드에 대한 분석 및 검증 과정이 미약한 상황
 - 스마트 컨트랙트는 전파를 통해 모든 블록체인 노드에서 실행되기 때문에 위험성이 더 증폭될 가능성 존재
- ☐ 거래 요청이 허가된 참여자 식별 및 접근 통제를 관리해주는 기술 필요
 - 일반적인 블록체인은 퍼블릭 블록체인으로 누구나 합의 알고리즘에 참여 가능.
 - 블록체인 내부 참여자가 담합하여 블록체인 내용을 위변조할 가능성 존재
 - IP 주소, 인증서 등을 기반으로 거래내역이 저장된 블록체인에 접근할 수 있는 참여자 목록을 관리해주는 기술 필요

◎ 블록체인 도입 시 예상되는 보안 위협에 대한 대응 방안

- ☐ 공격자에 의해 키가 유출되지 않도록 키를 안전하게 보관하고 키 도난 및 분실에 대응
 - 신뢰 가능한 기관에서 발간한 안전한 키 저장 및 보관에 대한 최신 보안 가이드 준수
 - 거래 서명에 다중 서명기술을 적용하여 공격자가 거래 서명에 필요한 모든 키를 획득하지 않는 한 불법 거래를 시도하지 못하도록 대응
 - 서명키가 원문 상태로 저장되지 않도록 파일 저장 시 암호화하거나 키 사용 후 메모리에서 즉시 삭제하는 등의 보호 기술 적용

- ☐ 내부 및 외부 공격자에게 장악된 노드로 인해 거래 유효성이 조작되지 않도록 모니터링 및 차단
 - 프라이빗 블록체인의 경우 참여자의 보안수준이 일관성 있게 유지되도록 신규 참여자에 대한 보안성 검증 기준을 강화하고 이를 지속해서 관리
- ☐ 블록체인에서 개인 정보 침해가 발생하지 않도록 참여자 권한 관리 기술 적용
 - 거래정보 보관기간에 대한 규정을 수립하고 기간 경과 후에는 거래 무결성 확인에 필요한 정보만 남기고 개인 정보 침해가 우려되는 세부 거래정보는 삭제
- ☐ 블록체인 S/W에 존재할 수 있는 보안 취약점을 이용한 악의적인 공격 차단
 - 블록체인 플랫폼 및 응용프로그램, 관련 라이브러리 등의 블록체인 S/W 개발 시 취약점 제거를 위하여 자체 또는 제3의 기관을 통해 코드 검토 수행
 - 블록체인 S/W에 대해 공격자 관점에서 모의 침투 테스트를 수행하여 개발 시 발견하지 못했던 취약점을 탐지 및 제거
- ☐ 스마트 컨트랙트 코드에 존재할 수 있는 보안 취약점을 악용한 비정상 거래 등 악성 행위를 차단
 - 스마트 컨트랙트 배포 이전에 코드 검토를 통해 보안 취약점 존재 여부와 악성코드 감염 여부를 확인

[스마트 컨트랙트 악성코드 탐지 도구]

도구명	분석방법	취약점 유형	세부 작동 방식
Oyente	정적 분석	RE, ME, TD	<ul style="list-style-type: none"> • 제어 흐름 그래프 모듈은 컨트랙트의 바이트 코드를 입력 받아 프로그램의 실행 흐름을 나타내는 제어 흐름 그래프(CFG)를 생성하고 이를 바탕으로 기호 실행을 수행 • 코어 분석 모듈은 기호 실행의 결과를 통해 취약점을 탐지 • 유효성 검증 모듈은 최종적으로 탐지된 결과물에 대한 거짓 양성케이스를 걸러내어 사용자에게 보고
Maian	정적 분석	RE, ME, SC	<ul style="list-style-type: none"> • 스마트 컨트랙트 바이트 코드를 구동시킬 수 있는 커스텀 이더리움 가상 머신을 직접 개발하여 바이트 코드에 대한 기호 실행 수행 • 기호 실행의 결과인 실행 흔적(Execution Trace)들을 분석해 특정 보안 속성을 만족하지 않는 실행 흔적을 도출 • 실행 흔적이 보안 취약점을 유발하는 실제 입력 값을 예시로 반환하여 이를 이용해 거짓 양성 케이스 필터링을 수행
Zeus	정형 검증	RE, IO, ME, TD, SC	<ul style="list-style-type: none"> • 바이트 코드가 아닌, 스마트 컨트랙트의 상위 레벨 소스 코드(Solidity)와, XML 형태의 보안 정책을 입력 받아 각 보안 정책들을 assert 함수의 형태로 소스 코드 상에 삽입 • 소스 코드 변환 모듈이 assert 함수가 추가된 소스 코드를 LLVM(Low Level Virtual Machine) 비트 코드로 변환 • 변환된 비트 코드에 대한 수학적 검증을 통해 스마트 컨트랙트가 보안 속성을 만족하는지를 정형 검증

* 취약점 유형: RE(Reentrancy), IO(Integer Overflow), ME(Mishandled Exception), TD(Timestamp Dependence), SC(Suicidal Contract)

나. 생태계 기술 동향

(1) 해외 플레이어 동향

◎ 암호화폐 거래소에서의 기술 동향

- ☐ (Binance) 체이널리시스가 개발한 KYT(Know Your Transaction) 보안 솔루션을 도입해 수상한 자금의 흐름을 차단
 - KYT는 암호화폐 거래를 실시간으로 점검할 수 있는 소프트웨어로 비트코인 지갑 주소를 기반으로 한 입출금 트랜잭션 분석 솔루션
 - 알고리즘을 통해 수상한 거래패턴을 걸러낸 후, 해당 현황을 소프트웨어 운영사나 개발사에 통보
 - 범죄(사기, 도박, 랜섬웨어 등)에 악용된 지갑 주소를 검색해 수사에 활용
- ☐ (Bitstamp) 이리시움과 함께 거래소 모니터링 플랫폼 구축을 위한 파트너십을 체결
 - 이리시움은 거래소와 규제기관 등의 기업을 대상으로 한 시장 모니터링 및 분석 소프트웨어 제공 기업으로, 이리시움은 360도 감시 기능(트랜잭션 분석)과 다중 자산 분석 기능을 제공
- ☐ (Coinpub) 블록체인 컴플라이언스 제공 업체으로 AML(자금세탁방지)/ KYC(고객인지) 법을 구현해야 하는 사업체들에게 솔루션을 제공
 - 최대 120개 알고리즘 활용해 AML, KYC 분석. 암호화폐 거래내역을 빅데이터를 통해 검사

◎ 식품·유통 분야에서의 기술 동향

- ☐ 식품의 생산부터 배송·유통 전 과정 실시간 추적 및 소비자가 스마트폰 하나로 모든 내용을 상세히 확인 가능하여 식품 안전과 신뢰도 향상 전망
 - 식품 포장지의 QR코드를 인식하면 생산과정, 원료 정보, 유통과정 확인 가능
- ☐ 블록체인 활용으로 위변조 봉쇄하여 식품의 투명성과 안전성 확보
 - 모든 정보가 센서와 IoT(사물인터넷) 엣지컴퓨팅, 모바일, 컴퓨터 등에 의해 디지털·자동화되고 관리되어 유통과정을 실시간 파악해 임의적인 정보 위조나 사기, 입력 오류 등 방지 가능
- ☐ (Nestle, Carrefour) 미국 IBM의 블록체인 기술을 활용하여 블록체인 유통 이력 추적 정보시스템 도입
 - IBM의 '푸드 트러스트(Food Trust)'에는 네슬레와 까르푸뿐만 아니라 월마트, 돌 등 글로벌 대형 식품·유통업체들이 대거 참여
 - 스타벅스는 마이크로소프트의 블록체인 기술을 2020년부터 시범도입해 커피 생산과 가공, 유통 과정을 효율화해 커피 생산농가에게 더 많은 수익을 돌려주는 방안 검토

◎ 의료분야에서의 기술 동향

☐ (Hacera) 코로나-19 데이터 허브 구축 팀 프로젝트 'Mipasa' 개발

- 세계보건기구(WHO), 미국, 중국, 유럽연합의 보건당국과 홍콩, 이스라엘, 캐나다 정부, IBM, 오라클, 마이크로소프트 같은 IT 기업과 존스홉킨스대학이 참여
- 기존 코로나-19 관련 정보는 각국 정부나 의료기관이 제공하는 데이터베이스 API(응용 프로그램 인터페이스) 형태로 공유되어 정부가 입력한 데이터의 오류 발견과 신뢰성 검증이 불가능했으나 블록체인 기반 기록된 데이터가 네트워크 내에 분산된 각 노드(개인)에 보관되고 실시간 동기화 되어 누구나 위변조가 불가능하여 전염병 추적과 개인정보보호 간 딜레마 해결 가능
- WHO와 각국 보건 당국, 의료기관, 개개인이 미파사에 코로나-19 관련 정보 제공, 데이터는 교차 검증 후 오류 수정 후 블록체인에 기록
- 블록체인 기술과 IBM, 오라클, 마이크로소프트 등 글로벌 클라우드 업체의 기술이 결합하여 데이터 출처 확인 및 검증 신속 처리
- 코로나-19 검사 대상자의 데이터, 환자 치료 기록, 건강 상태, 모니터링 상황 등 암호화되어 기록하여 일부 정부의 환자 축소·은폐 의혹 방지
- 허브에 모인 데이터는 글로벌 공동연구 자산이 돼 의학연구와의 시너지 효과 기대

☐ (IBM) 자금 세탁 방지에 응용가능한 블록체인 노드 데이터 이용에 관한 기술 특허를 미국 특허상표청(USPTO)에 신청

- 해당 특허는 '블록체인의 노드 특성화'란 시스템으로, 다양한 유형의 거래를 식별하기 위해 블록체인 네트워크의 노드로부터 데이터를 추출하는 기술로 파악

☐ (Koala) 블록체인 QR코드와 위조방지 지문서명 기능이 추가된 블록체인 추적시스템 도입

☐ (ANSA) 인터넷과 소셜미디어에 퍼지는 뉴스들의 출처와 수정 이력 등을 블록체인에 기록해 가짜 뉴스 추적 시작

(2) 국내 플레이어 동향

- ☐ (삼성) IBM과 함께 블록체인 개념을 사물인터넷(IoT)에 적용하려는 시도로 Adept 플랫폼 제안
 - 사물인터넷의 기반 기술로 블록체인을 활용하여 제품 제조 및 유통에 관한 모든 과정 관리
 - 블록체인상의 기록을 사물인터넷에 적용하면 제조사, 제품을 구성하고 있는 원자재들에 대한 정보 파악 용이
 - 거래에 있어 스마트 계약이 가능해지므로 공급사슬 가시성 및 투명성 향상
- ☐ (과학기술정보통신부) 블록체인 기반 데이터 공유 서비스의 보안 정책 방향은 사전 규제에서 사후 관리 및 점검 강화로 옮김
 - 금융 소비자들의 비대면 채널 이용이 급증, 개별 금융 기관들의 부정 사용이 의심되는 거래 행위를 탐지하고 사전에 차단하는 시스템인 '이상 금융거래 탐지시스템'을 고도화 중
 - 거래 데이터를 수집해 SI를 통해 정상 거래와 사기거래를 학습시키고, 지능화된 부정 거래 예방과 차단에 적극적으로 나서는 내용을 골자로 함. 자체적인 금융기관의 노력과 더불어 전 금융권 공동대응을 통한 사고예방 및 피해 확산 방지를 위해 부정 거래 관련 정보 공유가 필요
- ☐ (수호) 블록체인의 핵심 기술인 스마트컨트랙트의 취약점을 분석하는 솔루션을 개발하는 업체
 - 암호화폐 거래소 바이낸스가 개최한 글로벌 해커톤 행사에서 거래소, 암호화폐 지갑, 디앱(DApp)과 같은 서비스 관점에서 필요로 하는 이상 거래 탐지 서비스를 발표하여 최고 기술상을 수상
 - 발표한 자금세탁방지(AML)는 블록체인상에 존재하는 거래 내역인 '온체인 데이터'를 분석하는 방식의 KYT로, 기존 암호화폐 거래소나 블록체인 회사는 블록체인 밖 정보인 신원 등 '오프체인 데이터'를 분석하는 방식과 차이가 존재. 이를 통해 이상거래 탐지 및 실제 활용 가능성에서 높은 평가를 받음
 - 자체 기술로 6만 건 이상의 확인된 악성 주소를 수집하고, 이를 기반으로 해킹에 활용된 암호화폐 계정들은 바로 확인이 가능. 따라서, 거래소는 이들 주소와 관련된 거래를 발견하고 동결 조치를 취할 수 있음
 - 수호의 경우 분석 업무 자체까지 직접 해줘 차별화를 도모하고자 하며, 추후 공개된 블랙리스트 DB 대비 20배 정도 많은 DB를 바탕으로 자동화된 분석 서비스를 제공하는데 초점
- ☐ (페이게이트) '세이퍼트' 블록체인 지갑을 이용해 위조 신분 등으로 P2P 거래를 할 가능성을 낮춰, 가상화폐 거래소의 자금세탁 거래를 탐지하고 이상(사기) 거래를 방지할 수 있는 기술을 발표
 - 투자자, P2P 업체, 페이게이트 등 3자가 계정에 대한 통제권을 분산해 2곳 이상이 동의해야만 자산을 이동할 수 있는 기술을 세이퍼트에 적용. 다중 서명으로 계정을 통제하여 특정 사용자 계정이 탈취돼도 다른 사용자 계정을 통해 사고를 예방

- 세이퍼트 블록체인 지갑을 통해 여권 등 신분증과 은행 계좌를 통한 고객확인(KYC) 의심거래 모니터링 및 규제기관 보고 등을 종합적으로 한번에 해결해 가상통화 취급 과정에서 자금세탁방지 효율을 극대화할 수 있다고 밝힘
 - 세이퍼트가 ICO기업이나 가상화폐거래소의 자금세탁방지와 이상 거래 탐지, 입금자 확인 영역에서 역할을 할 수 있도록 최신 블록체인 기술과 빅데이터 활용 능력을 강화 중
- ☐ (노르마) 통합 보안 모듈을 개발, 네트워크와 디바이스, 어플리케이션 등 금융 거래의 모든 단계를 통합적으로 보안. 가짜 지갑 주소나 악성 사이트 정보 등을 DB화해 송금하는 과정에서 해킹 및 사기를 막는데 특화된 기술 개발
- 이더리움 기반 'ERC-20 토큰'의 스마트 컨트랙트 취약점을 발견
 - 자체 기술 활용은 물론 국내외 우수 보안 전문 기업(기관)과 협력해 보다 정교하고 강력한 솔루션 제공
 - 국내 최대 암호화폐 거래소와 업무협약(MOU)을 맺고 보안 모듈을 전자지갑에 탑재하는 방안 논의
- ☐ (업비트, 캐서레스트) 이상금융거래감지시스템(FDS)을 통해 보이스피싱 범죄시도를 포착하여 보이스피싱 사건 용의자 검거에 일조
- 암호화폐 거래에 익숙하지 않은 투자자를 속여 자산을 탈취하려는 시도를 사전에 차단
- ☐ (GDAC) 국내 암호화폐 거래소 지닥은 자체 강화 개발한 이상거래 탐지시스템(FDS)을 전격 도입하여 보이스피싱을 전면 차단
- 지닥은 ISMS 공인인증 심사원, 국방부 해커부대 출신 보안 전문가, 키움증권, 카카오, 안랩, 신한, 맥쿼리 등에서 경험을 쌓은 전문 인력들로 구성, 고객자산 보호를 위한 예치금 서비스까지 운영하는 등 믿을만한 암호화폐 거래소로 업계에서 각광 받는 중
 - 이 외에도 지닥을 운영하는 블록체인 기반 핀테크 기업 피어테크는 서비스 보안 강화 및 블록체인 인프라 보안 구축을 위해 2019년 10월 15일 정보 보안 전문 기업 펜타시큐리티와 파트너십을 체결
- ☐ (인섹시큐리티) 비트코인 지갑 주소를 기반으로 입출금 트랜잭션을 분석하는 솔루션.지갑 주소를 이용해 해당 지갑의 모든 트랜잭션 로그를 분석할 수 있는 체인널리시스 리액터 개발
- 범죄에 악용된 지갑 주소를 검색해 수사에 활용 가능
- ☐ (아르고스) 암호화폐 관련 프로젝트의 실명인증과 자금세탁방지 전문 솔루션 업체
- 실명인증을 개발하여 딥러닝 기반의 이미지 인식 등을 진행. 금융기관에서 사용하는 다우존스의 감시목록 데이터베이스를 사용해 이를 기반으로 한 자체 알고리즘을 통해 위험인물 등급을 나눠 자금세탁 방지를 실시

다. 국내 연구개발 기관 및 동향

(1) 연구개발 기관

[블록체인 기반 불법 거래 탐지 시스템 분야 기술개발 기관]

기관	소속	연구분야
고려대학교	블록체인보안연구센터	<ul style="list-style-type: none"> •블록체인 합의 알고리즘 안전성 •스마트 컨트랙트의 안전성
서강대학교	지능형 블록체인 연구센터	<ul style="list-style-type: none"> •적응형 블록체인을 위한 모듈 개발 및 블록체인 통합 플랫폼 개발 •신뢰기반의 도메인 특성을 반영한 블록체인 요소 알고리즘 개발 •품질속성 기반의 블록체인 플랫폼 아키텍처 수립 및 테스트 자동화 기술 개발 •IoT 및 금융환경에서의 보안성 강화 및 신뢰성 확보를 위한 적응형 블록체인 기반의 통합 플랫폼 구축 •적응형 블록체인에서 보안성 및 신뢰성 향상을 위한 고효율 P2P 네트워크 및 분산 저장 기술 개발
중앙대학교	블록체인서비스연구센터	<ul style="list-style-type: none"> •다양한 산업군의 블록체인 서비스 모델 연구 •에너지거래에 블록체인 기술을 적용해 고효율-고신뢰형 거래시스템을 개발

(2) 기관 기술개발 동향

- ☐ (팀블랙버드) 암호화폐 계좌 유형 분류를 통한 고성능 범죄 추적/예방 솔루션 (2019/12/01 ~ 2021/11/30)
 - 텍스트 인식 및 자동 분류 기술
 - 불법 다크웹 사이트 수집 기술 (Crawling)
 - 소유자 휴리스틱 클러스터링 (Entity Heuristic Clustering)
 - Graph DB 운영 성능 최적화 기술
 - 그래프 시각화 기술
 - 그래프 특성 추출 (Graph Feature Extraction)
 - 암호화폐 자금세탁 패턴 분석 기술
- ☐ (경희대학교) 머신러닝 활용한 블록체인 거래기록 분석 연구 (2020/09/01 ~ 2023/02/28)
 - 안전한 블록체인 거래 기반 확보 및 거래기록 연구에 대한 기초마련
 - 머신러닝에 기반한 이상거래 탐지를 위한 연구 체계 마련
- ☐ (계명대학교 산학협력단) 블록체인의 트랜잭션 모니터링 및 분석 기술개발 (2018/04/01 ~ 2020/12/31)
 - 기초 분석으로 블록체인 네트워크 성능 분석, 블록체인 노드 성능 분석, DDoS 탐지 분석, 스마트 컨트랙트 보안 취약성 분석
 - 응용 분석으로 불법거래탐지 분석, 블록체인 포렌식 분석, DDoS 공격 예측 분석, 프라이빗 블록체인 운영관리 분석
 - 블록체인에서 수집하는 정보는 트랜잭션 정보를 포함하여 노드, 네트워크, 블록 및 스마트 컨트랙트임

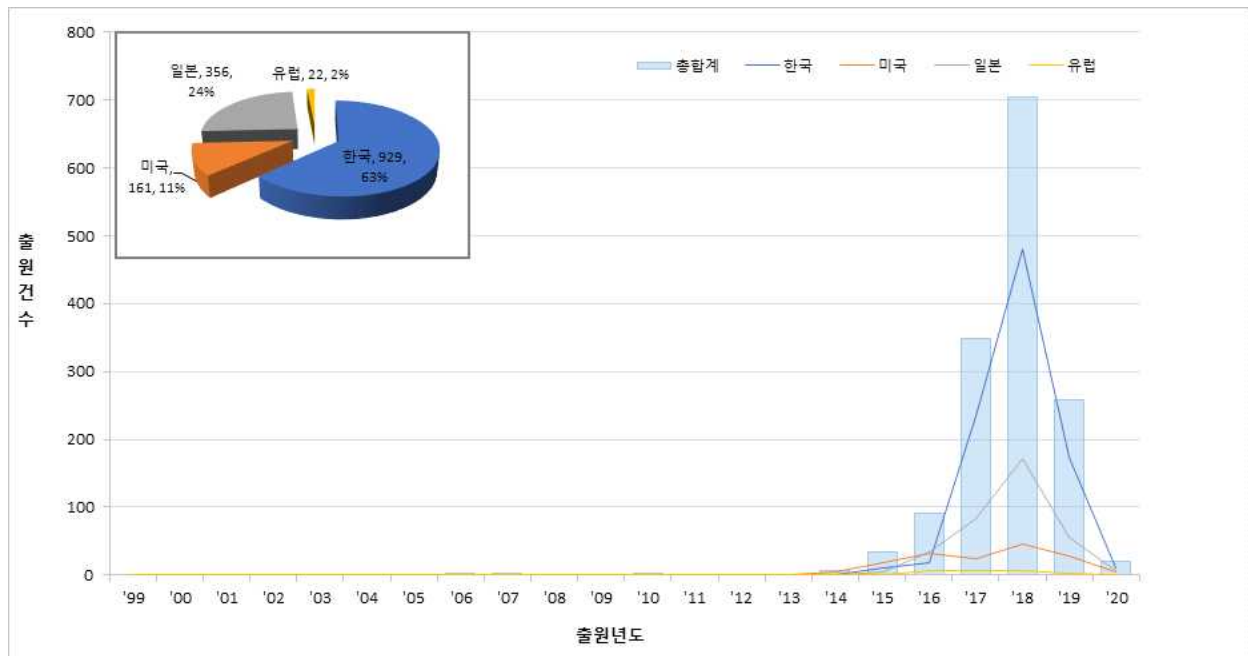
4. 특허 동향

가. 특허동향 분석

(1) 연도별 출원동향

- ☐ 블록체인 기반 불법 거래 탐지 시스템은 '17년부터 급격한 성장을 보임
 - 각 국가별로 살펴보면 한국이 가장 활발한 출원활동을 보이고 있음
- ☐ 국가별 출원비중을 살펴보면 한국이 전체의 63%의 출원 비중을 차지하고 있어, 최대 출원국으로 블록체인 기반 불법 거래 탐지 시스템 분야를 리드하고 있는 것으로 나타났으며, 일본은 24%, 미국은 11%, 유럽은 1% 순으로 나타남

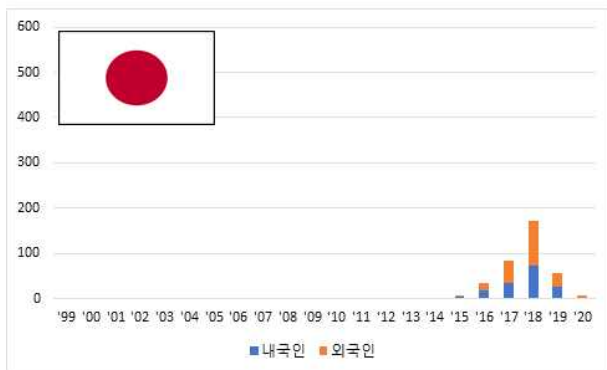
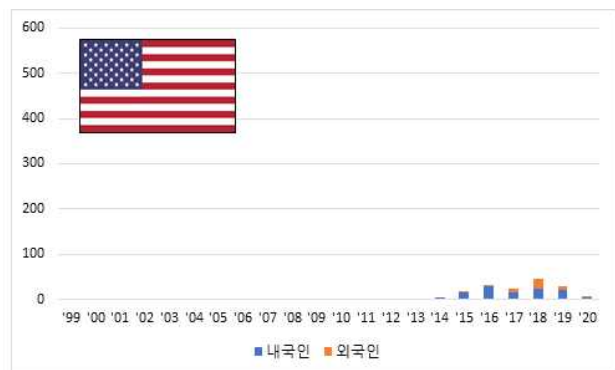
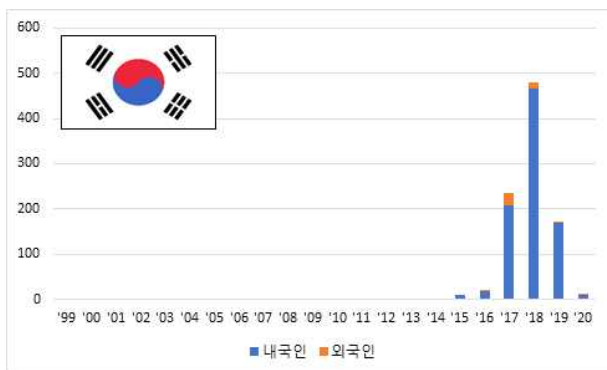
[블록체인 기반 불법 거래 탐지 시스템 연도별 출원동향]



(2) 국가별 출원현황

- ☐ 한국의 출원현황을 살펴보면, '17년부터 해당 기술의 출원이 급격히 증가하는 추세
 - 내국인 위주의 출원이 진행되고 있음
 - 한국 기술의 양적 흐름은 '18년에 가장 많은 특허를 출원
 - 한국의 출원 수는 미국, 유럽, 일본에 비해 가장 많은 특허를 출원
- ☐ 미국의 출원현황을 살펴보면, '15년 이후로 출원이 완만히 증가하는 동향을 보임
- ☐ 유럽의 출원현황을 살펴보면, 미국과 유사한 동향을 보임
- ☐ 일본의 출원현황을 살펴보면, 한국과 유사한 동향을 보임

[국가별 출원현황]



(3) 기술 집중도 분석

□ 전략제품에 대한 최근 기술 집중도 분석을 위한 구간별 기술 키워드 분석 진행

- 전체 구간(1999년~2020년)에서 블록 체인 네트워크, 블록 체인, 사용자 무선단말 등 키워드가 다수 도출
- 최근 구간 분석 결과, 최근 1구간(2012년~2015년)과 비교할 때 2구간(2016년~2020년)에서 고유식별, 연계 저장 키워드가 많이 등장하는 것으로 보아 블록체인 기반 불법 거래 탐지 시스템 분야에는 고유식별을 활용한 비정상거래 탐지 및 차단기술 관련 연구개발이 활발한 것으로 추정

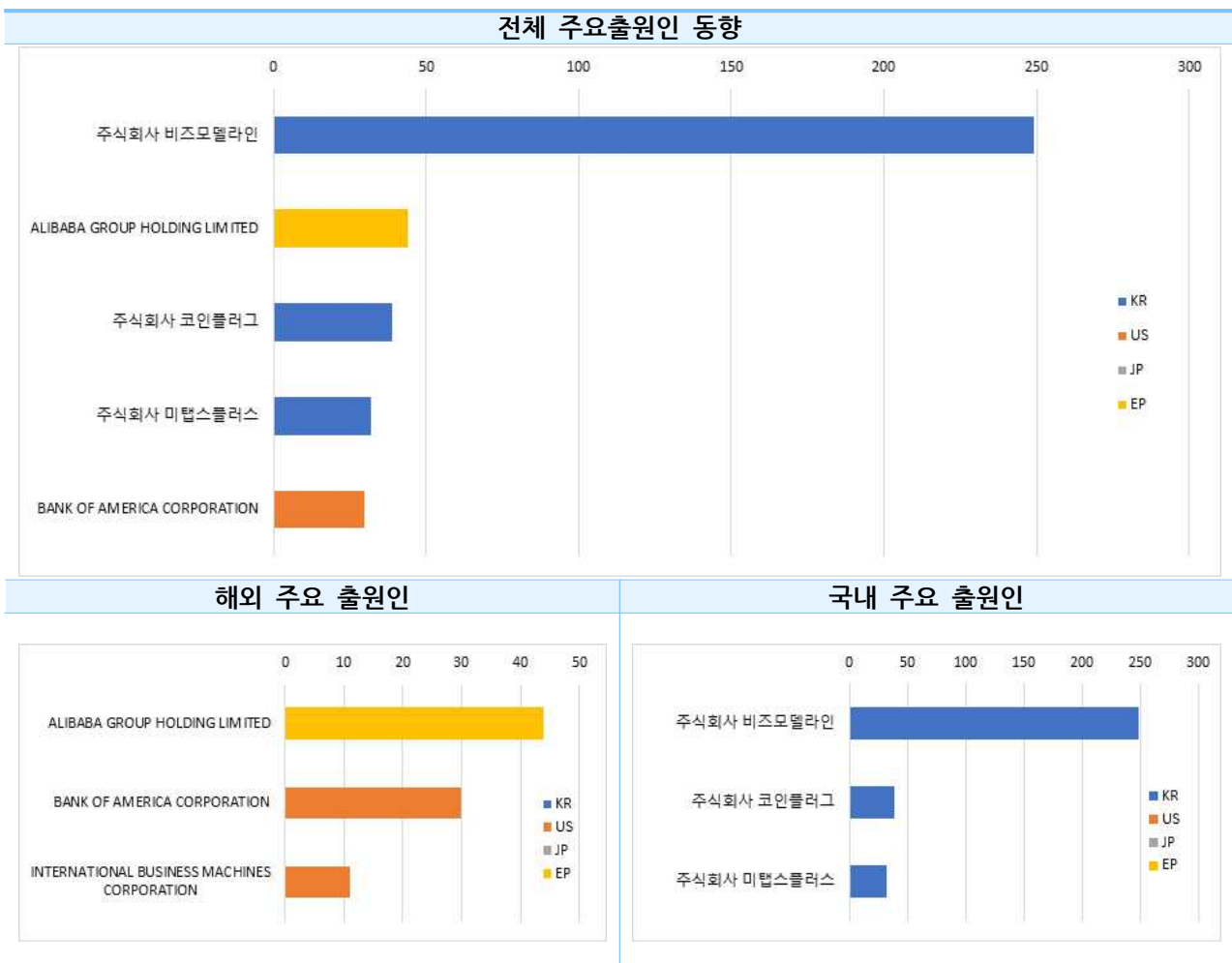
[특허 키워드 변화로 본 기술개발 동향 변화]

전체구간(1999년~2020년)	
<ul style="list-style-type: none"> • 블록 체인 네트워크, 블록 체인, 사용자 무선단말, 고유 식별, 고유 식별 인증, 특정 거래, 통신 가능, 연계 저장, 식별 인증, 사용자 무선단말 지정 	
최근구간(2012년~2020년)	
1구간(2012년~2015년)	2구간(2016년~2020년)
<ul style="list-style-type: none"> • Computer Program Product, Mobile Device, Rfid Tag, Computer Implemented, Computing Device, Real Time, Inventory Data, Inventory Management, Supply Chain, Communication Network 	<ul style="list-style-type: none"> • 블록 체인 네트워크, 블록 체인, 사용자 무선단말, 고유 식별, 고유 식별 인증, 특정 거래, 통신 가능, 연계 저장, 식별 인증, 사용자 무선단말 지정

나. 주요 출원인 분석

- ☐ 블록체인 기반 불법 거래 탐지 시스템의 전체 주요출원인을 살펴보면, 주로 한국 국적의 출원인이 다수 포함되어 있는 것으로 나타났으며, 제 1 출원인으로는 한국의 주식회사 비즈모델라인으로 나타남
 - 제 1 출원인인 주식회사 비즈모델라인의 출원은 한국에 집중된 경향을 보임
- ☐ 블록체인 기반 불법 거래 탐지 시스템 관련 기술로 블록체인을 다루는 대기업에 의한 출원이 대다수를 차지
 - 국내에서는 중소기업(개인)의 활발한 출원이 이루어짐

[블록체인 기반 불법 거래 탐지 시스템 주요출원인]

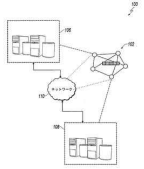
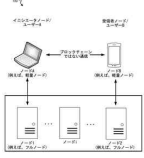
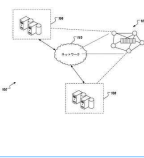
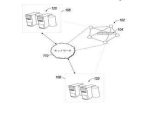


(1) 해외 주요출원인 주요 특허 분석

◎ ALIBABA GROUP HOLDING LIMITED

- ☐ ALIBABA GROUP HOLDING LIMITED은 중국 온라인 쇼핑몰을 운영하는 기업으로, 블록체인 기반 불법 거래 탐지 시스템과 관련하여, 블록체인을 통한 암호화 기술에 특화된 특허를 다수 출원
- 블록체인 기반 불법 거래 탐지 시스템 기술과 관련하여 48건의 출원을 진행하였으며, 그 중 등록된 특허는 4건으로 파악

[ALIBABA GROUP HOLDING LIMITED 주요특허 리스트]

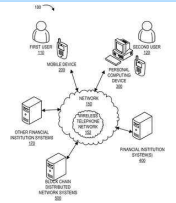
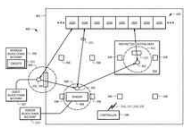
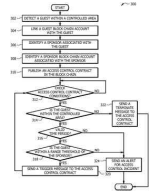
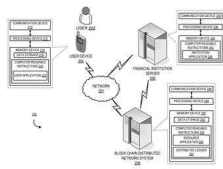
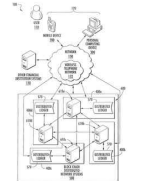
등록번호 (출원일)	명칭	기술적용분야	도면
JP6732321 (2018.12.13)	분산 시스템에서 네트워크 노드에 대한 회복 처리한 실행	분산 시스템(예를 들면 블록 체인 네트워크)에서 의견 일치 문제로 대처하기 위한 컴퓨터에 실행되는 방법	
JP6756041 (2018.11.27)	정보 보호용의 시스템 및 방법	입력 데이터 타입 및 출력 데이터 타입을 암호화하는 단계는 입력 데이터 타입 및 출력 데이터 타입을 해시 함수에 의해서 암호화하는 기술	
JP6647731 (2018.11.07)	블록 체인 기밀 트랜잭션(transaction) 관리	블록 체인 기술(블록 체인 기밀 트랜잭션(transaction), 또는 단순히, 기밀 트랜잭션(transaction)라고 칭한다)에 근거한 기밀 트랜잭션(transaction)을 위한 컴퓨터 실시 방법	
JP6727630 (2018.11.07)	실용적 비잔틴 폴트 톨러런스 블록 체인의 의견 일치 및 노드 동기화 촉진	가십(gossip) 기반의 통신 방법을 사용하고 합의 메시지에 디지털 서명을 추가함으로써 PBFT에 기초하여 블록체인 네트워크에서 합의 메시지 송신 및 노드 동기화 기술	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ BANK OF AMERICA CORPORATION

- ☐ BANK OF AMERICA CORPORATION은 미국의 상업 은행으로 블록체인 기반 불법 거래 탐지 시스템과 관련하여, 블록 체인 분산 네트워크를 활용한 기술에 특화된 특허를 다수 출원. 그 중 등록된 특허는 13건
- 블록체인 기반 불법 거래 탐지 시스템에서 블록 체인 분산 네트워크 및 블록 체인 계정 검증 등의 응용 특허를 다수 보유

[BANK OF AMERICA CORPORATION 주요특허 리스트]

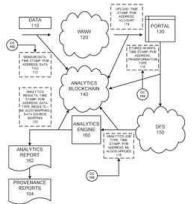
등록번호 (출원일)	명칭	기술적용분야	도면
US10614461 (2019.09.11)	System for implementing a distributed ledger across multiple network nodes	결제 트랜잭션의 검증을 위해 블록 체인 분산 네트워크를 사용하기 위해 블록 체인 분산 네트워크와 동작가능하게 접속된 시스템	
US10325428 (2018.05.23)	Access control using device location tracking and blockchains	제어된 영역 내에 사물인터넷 센서 및 제어기를 포함하는 액세스 제어 시스템	
US10601835 (2018.05.23)	Resource sharing using device location tracking and blockchains	스폰서에 대한 스폰서 블록 체인 계정(sponsor block chain account)을 식별하도록 구성	
US10402796 (2016.08.29)	Application life-cycle transition record recreation system	클라이언트 발신으로부터 외부 클리어링으로 트랜잭션이 처리되는 방법의 이력 레코드를 재생성하기 위해 내부에 삽입된 검색가능한 메타데이터 코드를 갖는 블록들의 생성을 위해 블록 체인 분산 네트워크를 이용하기 위한 시스템	
US10135870 (2016.02.22)	System for external validation of secure process transactions	호스트 및 소스 기관들은 블록 체인의 멤버인 호스트 기관이 블록 체인의 모든 소스 기관들의 트랜잭션 기록들을 획득할 수 있도록 멤버 기관들로부터 트랜잭션 기록들을 공유	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ IBM(International Business Machines)

- ☐ IBM은 미국의 다국적 기업으로, 다수의 블록체인 관련 특허를 보유하고 있으며, 블록체인 기반 불법 거래 탐지 시스템과 관련한 특허를 미국, 일본에 출원

[IBM 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
US10135870 (2016.02.22)	Enhanced chaincode analytics provenance in a blockchain	장부 검증(ledger verification) 및 정보 검색(information retrieval)을 위해 이해당사자에 의해 액세스할 수 있는 거래의 블록체인	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 주식회사 코인플러그

- 주식회사 코인플러그는 한국의 블록체인을 중점으로 하는 핀테크 기업으로, 블록체인 기반 불법 거래 탐지 시스템과 관련된 특허를 39건 출원하였으며, 39건의 특허 중 등록된 특허는 33건을 보유

[주식회사 코인플러그 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
KR2063628 (2018.06.29)	블록체인 기반의 결제 방법 및 이를 이용한 지급 결제 서버	승인 결과 정보를 결제 수단에 대응되는 펀드 소스 식별 아이디어에 해당하는 펀드 소스 서버로 전송하여 주는 블록체인 기반의 결제 방법	
KR2050271 (2018.06.29)	블록체인 기반의 결제 방법 및 이를 이용한 지급 결제 서버	승인 결과 정보에 대응한 승인 완료 정보를 서비스 제공 단말로 전송하여 주는 결제 방법	
KR2050276 (2018.06.29)	블록체인 기반의 결제 방법 및 이를 이용한 지급 결제 서버	블록체인 기반의 결제 방법에서 결제와 관련한 트랜잭션을 블록체인 기반 결제 방법	
KR2075956 (2018.06.29)	블록체인 기반의 결제 방법 및 이를 이용한 지급 결제 서버	사용자의 지급 수단을 블록체인에 등록하는 블록체인 기반의 결제 시스템	
KR1936417 (2017.07.04)	블록체인 기반의 전자상품권을 서비스하는 방법, 이를 이용한 전자상품권 자동판매기 및 서비스 지원 서버	전자상품권 자동판매기로 하여금 발급 전자상품권을 사용자의 저장 매체에 전송하도록 지원하는 블록체인 기반의 전자상품권을 서비스하는 방법	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 주식회사 미탭스플러스

- 주식회사 미탭스플러스는 한국의 모바일 마케팅 소프트웨어를 제작하는 기업으로, 블록체인 기반 불법 거래 탐지 시스템과 관련된 특허를 32건 출원하였으며, 32건의 특허 중 등록된 특허는 29건을 보유

[주식회사 미탭스플러스 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
KR2096658 (2019.07.29)	유전 알고리즘을 이용한 암호화폐 거래소 입금 승인 장치 및 방법	트랜잭션의 비율인 레putation(Reputation) 정보가 포함된 암호화폐 거래소 입금 승인 장치	
KR2096656 (2019.07.29)	트랜잭션 풀 정보를 이용한 암호화폐 거래소의 인공지능 입금 승인 장치 및 방법	거래소 입금 트랜잭션의 트랜잭션 정보를 기초로 입금 승인의 속도를 향상시킨 암호화폐 거래소 입금 승인 장치	
KR2096655 (2019.07.29)	인공지능을 이용한 암호화폐 거래소 입금 승인 장치 및 방법	입금 승인의 속도를 향상시키기 위해 인공지능을 이용한 암호화폐 거래소 입금 승인 장치	
KR2096657 (2019.07.29)	비지도학습을 이용한 암호화폐 거래소 입금 승인 장치 및 방법	사용자는 승인된 상기 특정 암호화폐의 상기 거래소 내에서의 매도가 가능한 비지도학습을 이용한 암호화폐 거래소 입금 승인 장치	
KR2096647 (2019.02.18)	인공지능을 이용한 암호화폐 거래소 입금 승인 장치 및 방법	입금 승인의 속도를 향상시키기 위해 인공지능을 이용한 암호화폐 거래소 입금 승인 장치	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

다. 기술진입장벽 분석

(1) 기술 집중력 분석

- ☐ 블록체인 기반 불법 거래 탐지 시스템 관련 기술에 대한 시장관점의 기술독점 현황분석을 위해 집중률 지수(CRn: Concentration Ratio n, 상위 n개사 특허점유율의 합) 분석 진행
- 상위 4개 기업의 시장점유율이 0.25로 블록체인 기반 불법 거래 탐지 시스템 분야에 있어서 독과점 정도는 보통 수준으로 판단
 - 국내 시장에서 중소기업의 점유율 분석결과 0.88로 해당 기술에 대하여 중소기업이 진입하여 활동하고 있는 것으로 파악

[주요출원인의 집중력 및 국내시장 중소기업 집중력 분석]

주요 출원인 집중력	주요출원인	출원건수	특허점유율	CRn	n
	주식회사 비즈모델라인(한국)	249	17.0%	0.17	1
	ALIBABA GROUP HOLDING LIMITED(영국)	44	3.0%	0.20	2
	주식회사 코인플러그(한국)	39	2.7%	0.23	3
	주식회사 미탭스플러스(한국)	32	2.2%	0.25	4
	BANK OF AMERICA CORPORATION(미국)	30	2.0%	0.27	5
	(주)디지털골드익스체인지(한국)	23	1.6%	0.28	6
	인포뱅크 주식회사(한국)	22	1.5%	0.30	7
	주식회사 하나은행(한국)	18	1.2%	0.31	8
	주식회사 케이티(한국)	13	0.9%	0.32	9
	INTERNATIONAL BUSINESS MACHINES CORPORATION(미국)	11	0.7%	0.33	10
	전체	1468	100%	0.25	
국내시장 중소기업 집중력	출원인 구분	출원건수	특허점유율	CRn	n
	중소기업(개인)	794	88.3%	0.88	
	대기업	56	6.2%		
	연구기관/대학	49	5.5%		
	전체	899	100%	CR중소기업=0.88	

(2) 특허소송 현황 분석

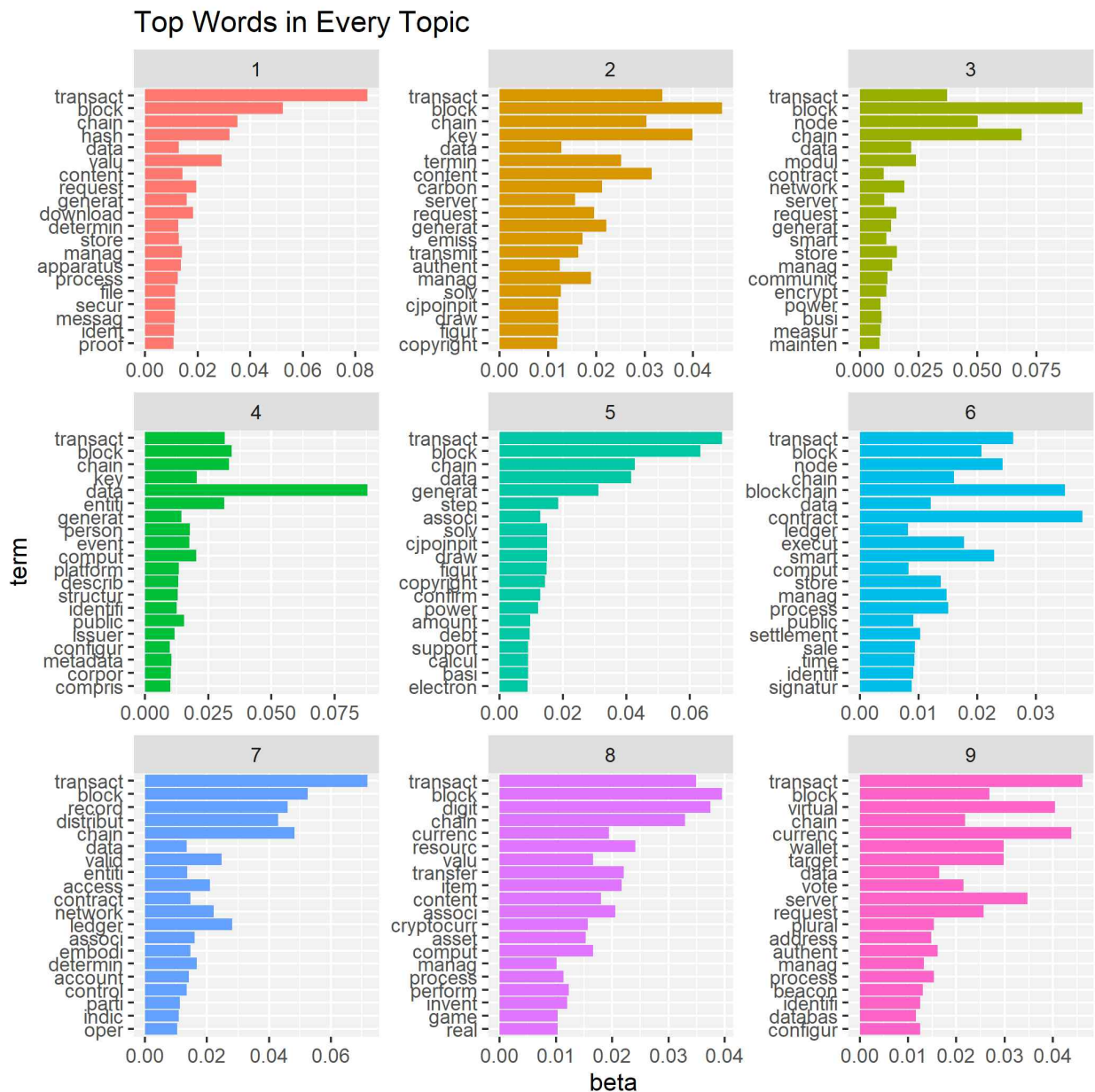
- ☐ 블록체인 기반 불법 거래 탐지 시스템 분야 관련 특허소송 이력은 검색되지 않음
 - 따라서 국내기업이 미국시장에 진입하는 경우, 해당 분야를 선점할 수 있을 것으로 판단
 - 다만, 블록체인과 관련해서는 4개의 소송이 검색

5. 요소기술 도출

가. 특허 기반 토픽 도출

- 292개의 특허의 내용을 분석하여 구성 성분이 유사한 것끼리 클러스터링을 시도하여 대표성이 있는 토픽을 도출

[블록체인 기반 불법 거래 탐지 시스템에 대한 토픽 클러스터링 결과]



나. LDA²²⁾ 클러스터링 기반 요소기술 도출

[LDA 클러스터링 기반 요소기술 키워드 도출]

No.	상위 키워드	대표적 관련 특허	요소기술 후보
클러스터 01	transact, block, chain, hash, value, request, download, generate, content, manage	<ul style="list-style-type: none"> Method and system for distributing digital content in peer-to-peer network Information processing unit and program Blockchain-based carbon trading system 	-
클러스터 02	block, key, transact, content, chain, terminal, generate, carbon, request, manage	<ul style="list-style-type: none"> Permission information management system, user terminal, right holder terminal, permission information management method, and permission information management program 	거래 허용 참여자 관리 기술
클러스터 03	block, chain, node, transact, module, data, network, store, request, manage	<ul style="list-style-type: none"> Business processing method and apparatus Power trading system 	블록체인 인프라 기술
클러스터 04	carbon, download, key, resource, payroll, currency, emission, movement, block, vote	<ul style="list-style-type: none"> The blockworld project Methods and systems using a computing platform for routing virtual receipts to customers with a scan-able code generated by the merchant 	-
클러스터 05	transact, block, chain, data, generate, step, solve, draw, figure	<ul style="list-style-type: none"> General-purpose body movement support system, general-purpose body movement support transaction management system, and general-purpose body movement support method System for implementing a distributed ledger across multiple network nodes 	이중지불방지 기술
클러스터 06	contract, blockchain, transact, node, smart, block, execute, chain, process, manage	<ul style="list-style-type: none"> Method of constructing scalable blockchain by using kanban to update off-chain transactions states Distributed ledger protocol to incentivize transactional and non-transactional commerce 	블록체인 모니터링 에이전트 데이터 수집 기술
클러스터 07	transact, block, chain, record, distribute, ledger, valid, network, access, determination	<ul style="list-style-type: none"> System for implementing a distributed ledger across multiple network nodes Access control using device location tracking and blockchains 	공적 가시성을 위한 거래내역 추적 기술
클러스터 08	block, digit, transact, chain, resource, transfer, item, association, currency, content	<ul style="list-style-type: none"> Mobile gaming and peer to peer gifting, receiving and donating platform using block chain integration of centralized or decentralized public ledgers for gaming elements to form, encrypt and distribute digital or crypto currency with quantum computing Sharing content within social network services 	-
클러스터 09	transact, currency, virtual, server, wallet, target, block, request, chain, vote	<ul style="list-style-type: none"> Point-to-point transaction guidance apparatuses, methods and systems Virtual currency clearing system 	블록체인 거래 검증 및 합의 기술

22) Latent Dirichlet Allocation

다. 특허 분류체계 기반 요소기술 도출

- ☐ 블록체인 기반 불법 거래 탐지 시스템 관련 특허에서 총 10개의 주요 IPC코드(메인그룹)를 산출하였으며, 각 그룹의 정의를 기반으로 요소기술 키워드를 아래와 같이 도출

[IPC 분류체계에 기반한 요소기술 도출]

IPC 기술트리		
(서브클래스) 내용	(메인그룹) 내용	요소기술 후보
(A63F) 카드게임, 보드게임 또는 룰렛게임; 작은 움직이는 물체를 사용하는 실내용게임; 그 밖에 분류되지 않는 게임	• (A63F-013) 게임과 관련된 표시를 나타내고, 예. 텔레비전, 스크린상에서 2차원 또는 그 이상의 차원을 가지는 전자적으로 생성된 표시화상을 이용한 게임양상	
(G06F) 전기에 의한 디지털 데이터처리	• (G06F-009) 프로그래머를 위한 장치, 예. 제어장치 • (G06F-021) 부정행위로부터 프로그램 또는 데이터, 그 컴퓨터 부품을 보호하기 위한 보안 장치	블록체인 비정상거래 탐지 및 차단 기술, 블록체인 스마트 컨트랙트 악성코드 탐지 기술
(G06Q) 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 데이터 처리 시스템 또는 방법; 그 밖에 분류되지 않는 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 시스템 또는 방법	• (G06Q-050) 특정 사업 부문에 특히 적합한 시스템 또는 방법, 예. 공익사업 또는 관광 • (G06Q-030) 거래, 예. 쇼핑 또는 전자상거래 • (G06Q-010) 경영; 관리 • (G06Q-040) 금융; 보험; 세무 전략; 법인세 또는 소득세의 처리 • (G06Q-020) 지불 체계, 방식 또는 프로토콜	거래 데이터 판독 시스템, 스팸거래 판독 기술 이중지불방지 기술
(H04L) 디지털 정보의 전송, 예. 전신통신	• (H04L-009) 비밀 또는 보안통신을 위한 배치 • (H04L-029) 그룹 1/00에서 H04L 27/00의 하나에도 포함되지 않는 배치, 장치회로 또는 시스템	

라. 최종 요소기술 도출

- ☐ 산업·시장 분석, 기술(특허)분석, 전문가 의견, 타부처 로드맵, 중소기업 기술수요를 바탕으로 로드맵 기획을 위하여 요소기술 도출
- ☐ 요소기술을 대상으로 전문가를 통해 기술의 범위, 요소기술 간 중복성 등을 조정·검토하여 최종 요소기술명 확정

[블록체인 기반 불법 거래 탐지 시스템 분야 요소기술 도출]

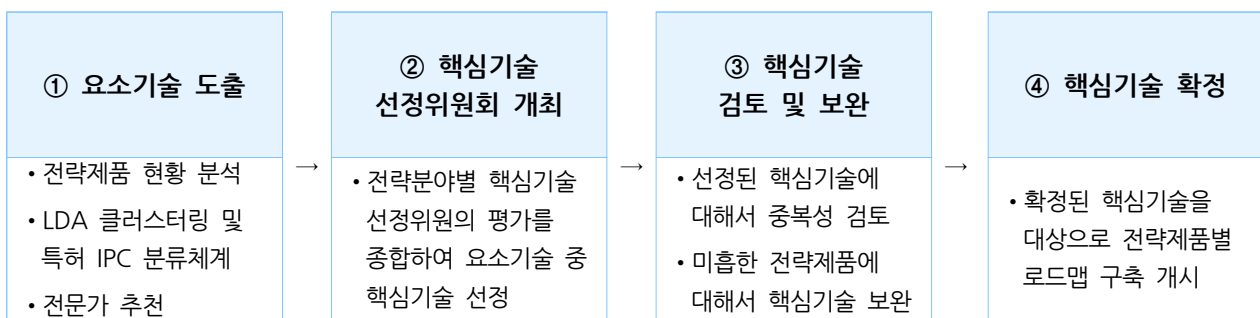
요소기술	출처
블록체인 비정상거래 탐지 및 차단 기술	IPC 기술체계, 전문가추천
블록체인 모니터링 에이전트 데이터 수집 기술	특허 클러스터링, 전문가추천
블록체인 스마트 컨트랙트 악성코드 탐지 기술	IPC 기술체계, 전문가추천
거래 데이터 판독 시스템	전문가추천
공적 가시성을 위한 거래내역 추적 기술	특허 클러스터링, 전문가추천
스팸거래 판독 기술	IPC 기술체계, 전문가추천
이중지불방지 기술	특허 클러스터링, IPC 기술체계, 전문가추천
거래 허용 참여자 관리 기술	특허 클러스터링, 전문가추천
블록체인 거래 검증 및 합의 기술	특허 클러스터링, 전문가추천
블록체인 인프라 기술	특허 클러스터링, 전문가추천

6. 전략제품 기술로드맵

가. 핵심기술 선정 절차

- ☐ 특허 분석을 통한 요소기술과 기술수요와 각종 문헌을 기반으로 한 요소기술, 전문가 추천 요소기술을 종합하여 요소기술을 도출한 후, 핵심기술 선정위원회의 평가과정 및 검토/보완을 거쳐 핵심기술 확정
- ☐ 핵심기술 선정 지표: 기술개발 시급성, 기술개발 파급성, 기술의 중요성 및 중소기업 적합성
 - 장기로드맵 전략제품의 경우, 기술개발 파급성 지표를 중장기 기술개발 파급성으로 대체

[핵심기술 선정 프로세스]



나. 핵심기술 리스트

[블록체인 기반 불법 거래 탐지 시스템 분야 핵심기술]

핵심기술	개요
블록체인 비정상거래 탐지 및 차단기술	• 서버에 수집된 대량의 거래 데이터에서 불법 거래를 탐지하는 기술과 탐지된 데이터에 연계된 블록을 블록체인에 등록하는 시스템을 의미
블록체인 모니터링 에이전트 데이터 수집 기술	• 거래, 계약, 노드 등의 블록 정보의 데이터를 수집하는 기술
블록체인 스마트 컨트랙트 악성코드 탐지 기술	• 스마트컨트랙트의 악성 패턴을 분석하여 AI로 반복적인 악성 코드 수행을 탐지하는 기술
거래 데이터 판독 시스템	• 공격자로 야기된 대량의 스팸 거래를 판독하는 시스템
공적 가시성을 위한 거래내역 추적 기술	• 공적 가시성을 위한 거래내역 추적 기술. 저작권료 징수 및 분배 등을 위한 디지털 저작물의 구매/사용 내역 추적 및 이에 대한 무결성을 시스템적으로 보장

다. 중소기업 기술개발 전략

- ☐ 금융 분야에서의 수요가 가장 크지만, 스마트 계약을 사용하는 블록체인 기반의 각 활용 산업의 시장을 창출하려는 시도가 필요
- ☐ 3세대 블록체인에서 지원하는 다양한 개발 언어(파이썬, 자바 등)를 활용하여 기존에 있는 프로그램을 벤치마킹하는 개발 전략도 존재

라. 기술개발 로드맵

(1) 중기 기술개발 로드맵

[블록체인 기반 불법 거래 탐지 시스템 분야 중기 기술개발 로드맵]

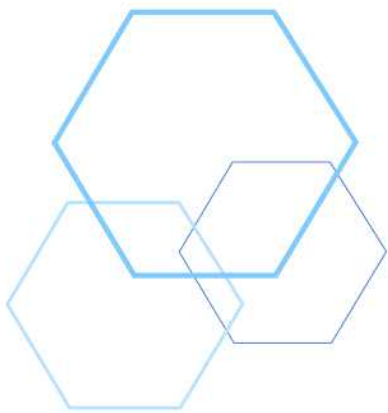
블록체인 기반 불법 거래 탐지 시스템	머신러닝 등 기술을 접목해 스팸/불법 거래 내용을 분석			
	2021년	2022년	2023년	최종 목표
블록체인 비정상거래 탐지 및 차단기술				불법거래탐지 및 관리
블록체인 모니터링 에이전트 데이터 수집 기술				모니터링 에이전트 커버리지 90%이상
블록체인 스마트 컨트랙트 악성코드 탐지 기술				기존 악성 패턴을 분석하여 신규 악성 패턴을 탐지
거래 데이터 판독 시스템				스팸거래 관리/차단
공적 가시성을 위한 거래내역 추적 기술				분산 환경에서의 상용화

(2) 기술개발 목표

- ☐ 최종 중소기업 기술로드맵은 기술/시장 니즈, 연차별 개발계획, 최종목표 등을 제시함으로써 중소기업의 기술개발 방향성을 제시

[블록체인 기반 불법 거래 탐지 시스템 분야 핵심요소기술 연구목표]

핵심기술	기술요구사항	연차별 개발목표			최종목표	연계R&D 유형
		1차년도	2차년도	3차년도		
블록체인 비정상거래 탐지 및 차단기술	대규모 불법 거래 탐지	불법 거래 패턴 규정	불법 거래 패턴 분석	불법 규정 거래 등록 관리	불법 거래 탐지 및 관리	산학연
블록체인 모니터링 에이전트 데이터 수집 기술	블록 정보 수집	10% 이상	50% 이상	90% 이상	모니터링 에이전트 커버리지 90% 이상	기술혁신
블록체인 스마트 컨트랙트 악성코드 탐지 기술	스마트컨트랙트 악성 패턴 분석 기술	악성 패턴 규정	악성 패턴 분석	악성 패턴 탐지 관리	기존 악성 패턴을 분석하여 신규 악성 패턴을 탐지	상용화
거래 데이터 판독 시스템	대량 스팸 거래 판독	10% 이상	50% 이상	90% 이상	스팸거래 관리/차단	상용화
공적 가시성을 위한 거래내역 추적 기술	DAG	설계 및 구현	테스트	상용화	분산 환경에서의 상용화	산학연



전략제품 현황분석

블록체인 기반 공유 경제 서비스



블록체인 기반 공유 경제 서비스

정의 및 범위

- 중앙화된 플랫폼에서 탈중앙화된 플랫폼으로의 이동과 동시에 공유거래 메커니즘에서 발생하는 가치들이 온전히 공유경제 거래참여자들에게 돌아가며, 참여자 네트워크를 확보
- 공유 경제서비스 실현을 위한 거래참여자 관리 및 합의, 참여자 평판시스템, 스마트계약 검증, 디지털 ID의 제공 및 확인, 토큰 시스템 및 페이먼트 기술 등을 포함

전략 제품 관련 동향

시장 현황 및 전망	제품 산업 특징
<ul style="list-style-type: none"> • (세계) 세계 계약 및 분쟁해결 관련 블록체인 시장을 추정한 결과 2018년 5천 5백만 달러 수준에서 연평균 60.5%로 성장하여 2024년 9억 4천만 달러 수준으로 성장할 것으로 예상 • (국내) 국내 계약 및 분쟁해결 관련 블록체인 시장을 추정한 결과 2018년 18억 원 수준에서 연평균 60.5%로 성장하여 2024년 307억 원 수준으로 성장할 것으로 예상 	<ul style="list-style-type: none"> • 블록체인 기반 공유 경제서비스 분야는 다양한 분야에의 융복합 가능성 및 높은 잠재 가치를 가져 특히 정부주도의 기술개발 및 투자 가속화 추세 • 사회적 요구에 맞추어 공유경제의 공공분야로의 공유경제 활용 및 확대 노력 • 블록체인 전문기업들은 기 보유 인프라 기반 토큰 이코노미 구현 및 이해관계자 간 제휴 등을 통해 변화를 시도
정책 동향	기술 동향
<ul style="list-style-type: none"> • 관련 시장의 성장가능성 및 유망성을 인지하고 정부주도의 관·민 시범사업 추진 등 공유경제 분야의 성장을 위한 다양한 시도가 이루어지고 있음 • 산업의 특성상 이종산업과의 융복합 구조로 인해 다양한 산업규제가 걸림돌이 되고 있어, 이에 대한 규제완화 및 제도적 장치 마련 노력 필요 	<ul style="list-style-type: none"> • 스마트계약의 한계점, 참여자 신뢰성확보 등 블록체인의 전제조건으로 인한 제한적 범위를 극복하기 위한 기술적 응용 및 개발 필요성 확대 • 블록체인 기반 공유경제서비스 실현을 위한 다양한 요소기술들의 검증 및 분석 요구
핵심 플레이어	핵심기술
<ul style="list-style-type: none"> • (해외) DHL, FLEXE, Amazon, Turo, Postmates, Omni, Origin Protocol, Slock.it • (국내) 위홈, 바르크플랫폼, 나르고 	<ul style="list-style-type: none"> • 부정거래 방지 기술 • 공적 가시성을 위한 거래내역 추적 기술 • 블록체인 기반 신원인증 서비스 기술 • 블록체인 거래검증 및 합의 기술 • 분산 공유플랫폼

중소기업 기술개발 전략

- 공유경제 참여자를 위한 블록체인 공유 네트워크 확보를 위한 핵심기술 개발 필요
- 거래참여자 관리 및 합의, 참여자 평판시스템, 스마트계약 검증, 디지털 ID의 제공 및 확인, 토큰 시스템 및 페이먼트 기술의 안정적 임무수행 지원 및 신뢰성 확보 필요
- 산·학 연계 및 테스트베드 확보를 통한 개발기술 검증으로 국내시장 개척 및 선점 필요

1. 개요

가. 정의 및 필요성

(1) 정의

- ☐ 수익형 공유기업의 플랫폼을 거치지 않고 블록체인(BlockChain) 기술을 공유경제 매커니즘에 적용함으로써 '온라인 네트워크상 분산화된 공개 장부'만으로도 거래참여자 간에 높은 신뢰(trust)를 제공하고, 공유경제가 궁극적으로 추구하는 개인과 개인 간의 거래를 활성화를 제공하는 블록체인 기반 공유 경제 서비스
 - 중앙화된 플랫폼에서 탈중앙화된 플랫폼으로의 이동과 동시에 공유거래 매커니즘에서 발생하는 가치들이 온전히 공유경제 거래참여자들에게 돌아가며, 참여자 네트워크를 확보할 수 있음
- ☐ 블록체인 기술이 적용된 스마트 계약(smart contract)을 통해 서비스 이용과 관련된 모든 정보 및 거래조건 등이 확인되고 은행이나 간편결제 기술과 같은 중간서비스 없이 이용료의 지급도 가능해짐
 - 또한, 중개 서비스에 더이상 수수료를 낼 필요도 없고 이들 기업이 정해놓은 여러 복잡한 규칙과 조건을 따를 필요도 없이 순수히 개인과 개인의 수요와 공급이 만나 공유거래 가능

(2) 필요성

- ☐ 공유경제는 참여자 간에 형성되는 시장인데, 현재 공유 경제서비스 시장에서는 '플랫폼 사업자'가 대부분 이윤을 가져가는 구조로 인해 진정한 공유경제의 실현에 어려움 존재
 - 특히, 공유경제의 가장 큰 문제로 기업의 독점(Monopoly) 이슈가 있는데, 이는 공유경제 시장에서 개인 간 거래를 차단하고 중개 수수료를 취하는 형태의 불공정 시장구조 형성
 - 이로 인해, 공유경제에서 발생하는 대부분 가치들이 플랫폼 참여자가 아닌 플랫폼 기업으로 흡수되는 플랫폼 이익 독점 현상이 발생
- ☐ 수익형 공유기업들이 제공하는 중앙집권화된 플랫폼은 공유거래 매커니즘을 실현하기 위해 다음과 같이 크게 세 가지 기능을 수행하고 있음
 - 다양한 개인들이 보유한 유희자원에 대해 데이터베이스를 구축하고 자원을 가진 공급자와 자원을 이용하고자 하는 이용자를 매칭하여 이들 사이에 거래가 이루어질 수 있는 네트워크를 형성
 - 공급자와 이용자 사이에 거래가 이루어질 수 있는 정보환경을 제공하여 거래의 투명성과 신뢰성을 확보
 - 거래 참여자 사이의 거래와 결제가 안전하게 이루어질 수 있도록 일정 수준의 보안 및 통제 기능을 제공

- ☐ 이 요소들은 블록체인을 통해 대체할 수 있음에 따라 ‘플랫폼 사업자’의 필요성은 없어지고 ‘블록체인 기반의 공유 경제서비스’의 필요성은 확대됨
- ☐ 공유경제 환경에서 블록체인 기술이 공유거래 참여자 간의 신뢰를 확보하는 과정은 다음 세 가지 중요한 특징을 갖고 있음

[공유 거래 참여자 간 신뢰 확보를 위한 블록체인의 주요 특징]

공개접근성	· 블록체인을 통해 저장된 모든 정보는 네트워크의 모든 사용자가 공개적으로 접근할 수 있으며 정보의 투명성을 제공
변경 불가	· 블록체인에 추가된 정보는 임의로 변경하거나 제거할 수 없으므로, 사용자는 스마트 계약을 통해 합의된 약관을 충실히 이행해야 함
복원력	· 네트워크의 모든 사용자는 블록체인의 분산된 장부의 모든 사본을 유지하므로, 어떤 시점에서든 오류나 오류로 인해 저장된 전체 정보의 가용성이 손상되지 않음

- 위와 같은 속성을 바탕으로 블록체인 기술은 스마트계약 (Smart Contract), 참여자 누구에게나 공개되는 사용자 평판시스템에 연결된 사용자 개인의 디지털 ID의 제공 및 확인 기능, 디지털화된 방식의 지급 결제 기능을 제공
 - 이 모든 것이 중앙집권화된 수익형 공유기업들이 제공하는 거래 중개의 필요성을 대체함에 따라 순수히 개인과 개인의 수요와 공급이 만나 공유거래가 가능해짐
 - 이에 따라 블록체인 기술은 소수의 플랫폼 독점을 막고, 참여자가 주인인 공유경제를 실현하며, 시민을 중심으로 공유경제의 패러다임을 바꾸는 핵심기술로 주목받을 필요가 있음
- ☐ 공유거래 메커니즘에서 블록체인과 스마트 계약기반이 활성화되면 공유비용은 낮아지고 거래 편의성은 더욱 높아질 것으로 기대
- 연결될 수 있는 거의 모든 유희자원이 공유경제의 수면 위로 떠오르게 되어 근본적인 개념과 소유체계를 흔들 것으로 예상
 - 스마트 계약을 통해 만들어진 블록체인은 자원을 누가 소유하고 누가 사용하는지, 자원의 특성과 상태가 어떠한지에 대한 모든 정보를 네트워크 노드에 저장·공유하고, 개인 간 거래를 활성화 시킬 것으로 예상
 - 모든 공유거래 메커니즘에서 상당한 비용과 시간이 절감되어 자원 탐사, 매칭 및 정산이 이루어지고, 자동화, 프로그래밍된 규칙에 따른 모든 프로세스가 그 어느 때보다 안전하고 신뢰할 수 있는 경제영역이 될 것으로 기대
 - 자원 활용과 유통의 효율성이 높아지면 낭비와 무분별한 자원 소비는 줄어들 것이고, 개인과 개인은 소유와 접근의 자유라는 편의성을 가지고 살 수 있는 여유를 가지게 될 것임

- 블록체인 기술은 공유 경제서비스 부문 외에도 금융서비스, 제조 및 유통, 공공서비스, 사회문화 등 다양한 산업 분야에 활용될 수 있는 범용성이 매우 높음
 - 금융서비스 분야의 경우 인증과 검증 과정을 간소화하면 거래 정산에 소요되는 시간이 줄고 대형 데이터베이스 구축 비용도 절감
 - 실시간 국제송금이나 환전 등에 제한이 없으며, 데이터 분석 활용도를 높여 맞춤형 상품과 서비스를 제공
 - 제조업 및 유통분야에서는 공급망의 가시성과 투명성을 제고할 수 있을 것이며, 제조업에 사물인터넷 기술 적용의 한계를 극복하는 수단이 될 것임
 - 블록체인의 기록은 제품을 구성하는 제조업체, 원료 등에 대한 정보를 제공하며 수십억 개의 기기 정보가 필요한 중앙집중식 시스템하에서 사물인터넷 기술이 확산되어 기술 적용의 한계를 극복하는 열쇠가 될 수 있음
 - 공공서비스 분야에서는 공공기록물 관리 및 예산 집행의 투명성과 효율성이 높아 운영비 등 비용이 크게 절감될 것으로 기대
 - 공공요금 및 과태료의 징수, 과세, 공공서비스 관련 민원행정, 여권발급, 토지등기내역 등 효율적인 공공업무 및 기록관리
 - 사회문화 분야에서는 업무의 출처의 정확성과 거래의 투명성을 확보함으로써 소유권의 진위여부 등 지적재산권 문제를 해결하는 데 유용하게 활용될 전망
 - 블록체인 기술을 활용해 미술, 음악 등 예술작품을 인증하면 작품의 출처를 파악하고 투명하게 활용할 수 있어 불법 복제와 유통을 사전에 예방할 수 있음
- 하지만, 공유경제뿐 아니라 다양한 분야에서 블록체인 기술이 적용되고 활성화되기 위해서는 법적 제도적 측면에서 이를 정비할 필요가 있으며, 블록체인의 잠재력을 극대화하기 위해서는 민관이 협력해 혁신 생태계를 조성하는 것이 중요
 - 상호 간 연동이 필요한 은행 전산망 특성상 시스템 구성을 위한 협의가 필수적이기 때문에 시스템의 효율적 운영을 위해 구성원들의 요구에 맞춘 산업표준 제정이 우선되어야 함
 - 세금혜택이나 보조금 지원과 같은 제도를 통해 신규 블록체인 스타트업들이 시장에 뛰어 들 수 있는 환경을 만들어 주는 것도 중요

나. 범위 및 분류

(1) 가치사슬

- (가치사슬) 블록체인 기반 공유 경제서비스의 경우 ‘수익형 공유기업’을 대체하여 공유 경제서비스의 본질적 목표를 실현할 뿐만 아니라, 더 나아가 모든 분야에서 ‘개인 ↔ 기업 ↔ 정부’가 주체가 되어 각자의 유희자원들을 공유하여 주체별 역할에 따라 산업의 패러다임이 변화할 것으로 기대
- (후방산업) 공유 경제서비스 실현을 위한 블록체인 참여자 식별 및 접근통제 기술, 계약에 따른 소유권 권한 인증 및 부여 기술, 스마트 계약 악성코드 탐지 기술, 소유자 및 대여자의 정보보호를 위한 소프트웨어 개발, 서비스 이용의 지급결제를 위한 암호화폐 기술, 계약규정의 합의 및 계약 실행 과정을 컴퓨터 네트워크를 통해 자동화 및 절차의 간소화 기술 등으로 구성되어 있음
 - (전방산업) 공공서비스 분야, 디지털콘텐츠, 금융·제조·유통·자동차·에너지 등의 대부분의 산업 분야로의 융·복합 및 확장 적용이 가능
 - 이로 인해 새로운 부가가치의 창출과 함께 위에서 언급된 바와 같이 참여 주체 간 공유 경제서비스의 본질적 목표를 실현할 수 있음
 - 특히, 공공서비스 부문에서는 공유재의 지원과 서비스 운영을 공공에서 주도하여 이용자들에게 더 많은 편의와 혜택을 줄 수 있을 것으로 기대하며, 블록체인을 기반으로 한 공유 경제서비스는 유희자원이 존재하는 모든 분야에서 공유경제의 실현을 위한 중요한 역할을 할 것으로 예상

[블록체인 기반 공유 경제서비스 분야 산업구조]

후방산업	블록체인 기반 공유 경제서비스 분야	전방산업
블록체인 참여자 식별 및 접근통제 기술, 권한의 인증 및 부여 기술, 정보보호 S/W, 암호화폐 결제 기술, 디지털 계약기술, 스마트 계약 악성코드 탐지 기술 등	거래 참여자 관리 및 합의 기술, 스마트 계약 검증 기술, 실물·디지털 정보 매칭 기술, 디지털 ID의 제공 및 확인 기술, 전자지갑 기술, 토큰 시스템 및 페이먼트 기술, 비정상 거래 탐지 및 차단 기술 등	공공서비스 분야, 디지털콘텐츠, 금융/보험/제조/유통/자동차/에너지 산업 분야 등

(2) 용도별 분류

- (공공분야) 주차장, 도서관, 공공시설 개방, 공공정보 공유, 이동수단(서울시 ‘따릉이’ 등)공유 등을 통해 기존 시설 및 시스템의 운영·관리에 있어 투입되는 막대한 인력 및 비용 등을 절감
 - 국민에게 편의성을 제공함과 동시에 공공재 지원과 이용에 따른 진입장벽을 낮추는 등의 후생경제 실현 가능
 - 보건·의료, 관광 등의 서비스 부문에서도 산업의 혁신적인 전략 기술로 활용할 수 있음
- (디지털콘텐츠 분야) 디지털콘텐츠를 공유경제로 활용함에 있어 블록체인 기술을 통해 위조 및 변조, 해킹 등의 위험을 최소화하고 투명한 거래가 가능해짐에 따라 디지털콘텐츠 산업의 진흥에 기여할 수 있을 것으로 기대
 - 스튜디오 등의 필요 시설·장비 등이 구비 된 작업공간을 공유하거나, 지식재산권 및 재능부문의 공유경제를 실현할 수도 있음
- (금융 분야) 중앙화된 금융기관을 통한 전통적인 금융거래 아니라 블록체인 공유 경제서비스 매커니즘을 활용한 디지털ID 식별, 신용정보 공유 등 다양한 기술 적용
 - ‘대출, 투자, 예금 등’의 형태가 다변화하게 되고 전통적인 금융기관의 독점적 서비스에서 탈피하여 상당한 거래비용을 절감할 수 있을 것으로 기대
 - 이 매커니즘을 이용하면 금융거래의 국경이 사라져 해외의 이용자와도 중간 매개체 없이 P2P 형태로 필요에 의한 거래를 할 수 있을 것으로 예상
- (제조·유통 분야) 산업단지 내에서도 유휴자원 매칭 및 기업 간 거래 활성화, 근로자 편의 증진을 위해 공유경제 서비스 플랫폼을 구축할 수 있음
 - 초기에는 기계장비 / 회의실·창고 / 주차장 / 기숙사 / 지게차·물류트럭 등의 ‘설비·공간’의 공유로 시작
 - 고도화 단계에서는 공동 구매 / 마케팅 / AS / 인력 / R&D / 비즈니스 기획 등의 ‘사업·서비스’의 공유까지 확대하여 블록체인 기반의 공유경제가 다양한 Value Chain으로 적용될 수 있을 것으로 기대
- 기타 자동차, 에너지, 정보 및 서비스 분야 등 블록체인 기반 공유 경제서비스 매커니즘의 활용성은 무궁무진하지만, 아직 초기단계인 블록체인 시장의 한계로 인해 이용자의 인식 부재, 규제 문제 등 많은 개선의 필요성이 존재
 - 정부는 규제의 개선과 정책·제도적 지원, 홍보를 통해 블록체인 기반의 공유경제가 활성화될 수 있도록 노력할 필요가 있음

2. 산업 및 시장 분석

가. 산업 분석

[국내 블록체인 공유 경제서비스 산업 SWOT 분석]

	긍정적	부정적
	〈 강점(Strengths) 〉	〈 약점(Weakness) 〉
내부	<ul style="list-style-type: none"> • 국내 공유 경제서비스 시장 약 10배 이상 성장 ('15, 204억 원 → '18, 1,978억 원) • 정책적 제도 기반 마련 의지 • 지자체 등 공공수요 적용 추세 • 글로벌 수준의 IT 경쟁력 	<ul style="list-style-type: none"> • 블록체인에 대한 인식의 부족 • 융복합에 따른 산업별 규제 • 공유경제에 대한 부정적 인식
	〈 기회(Opportunities) 〉	〈 위협(Threats) 〉
외부	<ul style="list-style-type: none"> • 세계 공유 경제서비스 시장 성장 추세 ('17, 186억 불 → '22, 402억 불) • 공유 경제서비스 시장 선점 시 이익 (특성상, 타 산업 대비 산업 전반 통용 가능성 높음) 	<ul style="list-style-type: none"> • 기존 아날로그 산업과의 충돌 • 경쟁국의 적극 투자 및 지원

◎ 블록체인 응용서비스의 확장

- ☐ 블록체인은 P2P를 기반으로 한 분산원장, 송금 및 암호화폐 중심의 기술과 서비스 형태의 1세대 블록체인에서 스마트 계약(Smart Contract) 기반의 지급·결제 시스템을 활용한 2세대 블록체인을 거쳐서 3세대 블록체인으로 속도·확장성·상호운용성에 중점을 두어 스마트 계약의 고도화를 통해 타 산업과의 융합 발전 및 활용 범위 확대
 - 블록체인 기반 공유 경제서비스 산업은 3세대 블록체인 기술 기반의 고도화된 분야로 특정 산업이 아닌 모든 산업에서의 적용이 가능한 혁신 서비스
- ☐ (공개키 암호화) 공개키 암호화는 공개키(Public key)와 개인키(Private key) 쌍을 사용하여 다른 작업을 수행하며, 공개키는 널리 배포되고 개인키는 비밀로 유지된다. 개인의 공개키를 사용하면 개인키를 가진 사람만 암호를 해독하고 읽을 수 있도록 메시지를 암호화
- ☐ (P2P) P2P(Peer-to-Peer)는 집합적으로 파일을 저장하고 공유하는 장치 그룹으로 구성되며 네트워크에 참여하는 노드는 블록체인 정보를 가지고 있으며, 동일한 거래 내역이 분산 저장되어 관리되며, 거래가 이상 없음을 확인하는 분산 합의 제도를 채택하고 있으며, 별도의 추가적인 신용기관 없이 P2P에서 검증하고 블록체인 기술에 내재된 P2P 아키텍처는 비트코인 및 기타 암호화폐를 중개자나 중앙 서버 없이 전세계로 전송 가능

◎ 정부는 “공유경제 활성화 방안” 추진과 샌드박스를 통해 지원 중

- ☐ 정부는 '19년 1월 9일 관계부처 합동으로 ‘공유경제 활성화 방안’²³⁾을 발표하였으며, 1인 가구 증가 등으로 인한 소비 패러다임의 변화(소유→공유)와, P2P 거래증가와 함께 공유경제가 확산 됨에 따라 진입 규제 개편 등을 통한 분야별 공유경제 활성화, 공유경제의 제도적 기반 마련 등을 추진 노력
- (숙박) 도시지역 내국인 대상으로 거주 주택의 빈방을 숙박용으로 제공하는 숙박 공유 허용 추진(年 180일 한도, 관광진흥법 개정)
 - 전통 숙박업계, 숙박중개 플랫폼 업체 등 이해관계자와 관계부처 참여
 - (교통) 기존 교통수단과 O2O(online to offline) 서비스를 결합한 新교통서비스 활성화를 목적으로 하며, 특히 승차 공유는 사회적 대타협을 통해 상생방안과 함께 추진
 - (공간) 주차장, 주거 공간, 공공자원 등의 개방 공유 활성화, 정부, 공공기관 등이 보유한 회의실, 강당, 체육시설 등 국내외 유휴 공간 공유를 위한 예약 결제 플랫폼 구축
 - 442개 기관의 회의실, 강당, 주차장, 연수원 등 개방정보를 통합·제공하는 시범사업 실시 중
 - (금융 지식 등 기타) P2P, 크라우드펀딩 등 자금공유, 온라인플랫폼을 이용한 지식공유 등 활성화
- ☐ 정부는 ICT규제 샌드박스를 활용하여 블록체인 공유경제 기업을 허가한 바 있음
- 과학기술정보통신부(과기부)는 2019년 11월 27일 ‘제7차 규제샌드박스 위원회’를 열고 공유숙박서비스 ‘위홈’등 8건을 규제 샌드박스로 지정
 - 현행 관광진흥법상 도시민박업은 외국인 관광객만을 대상으로 하고 있고, 내국인 대상 도시민박업은 찾아볼 수 없어 내국인들에 대한 역차별이 아니냐는 지적이 끊임없이 나왔고 이에 국회·정부 차원에서 ‘내국인 대상 도시민박업’ 제도화를 통해 세계적인 공유경제 흐름을 따르고, 국내 플랫폼을 기반으로 한 관광산업을 활성화해야 할 필요성으로 이를 허가

◎ 공유경제와 블록체인의 접목

- ☐ 호주의 공유경제 스타트업 ShareRing은 공유경제 시장이 Airbnb와 Uber 등 거대 업체로 집중화되고 틈새시장을 채우는 전문 사업자들의 생존 및 지속 가능성이 위협받는 상황에 대한 해결 방안을 제시
- ShareRing은 다채로운 공유 경제 서비스를 제공하는 수많은 업체와 서비스를 하나의 모바일 앱으로 통합해 효율적으로 접근할 수 있는 블록체인 기반의 시스템을 개발
 - 공유 경제 소비자의 편의를 위해서는 스마트폰 앱을 통해 광범위한 범주의 자산을 빌려 쓸 수 있도록 ShareLedger로 알려진 자체 플랫폼을 운영
 - 더불어 블록체인 기술을 기반으로 거래기록의 보안성 및 투명성을 확보함으로써 ShareToken라는 자체 토큰을 활용한 원활한 공유경제 생태계 조성에 기여한다는 목표를 제시

23) 관계부처합동(2019.1.9.), “공유경제 활성화 방안(서비스산업 혁신Ⅱ)”, 경제활력대책회의 19-2.

- 차량 공유 서비스를 제공하는 이스라엘 스타트업 라주즈(lazooz)는 자체 발행한 주즈라는 암호화폐를 만들어 차량 공유에 이용
 - 이 회사는 암호화폐가 생성되는 알고리즘을 만들었을 뿐 개인 간 거래에는 접근 권한이 없음
 - 운전자가 차량을 운행하면서 라주즈앱으로 자신의 위치를 공유하면 실시간 위치정보가 블록으로 등록되고 운전자 전자지갑에 주즈가 생성
 - 카풀을 원하는 사람이 접속해 목적지를 입력하면 근처를 지나는 운전자에게 알림이 뜨며, 운전자가 카풀을 수락하면 거래가 성사되고, 즉시 카풀 이용자의 전자지갑에서 운전자의 전자지갑으로 주즈가 이체
 - 운전자는 이렇게 쌓은 주즈를 현금화하거나 자신이 카풀을 이용할 때 사용

◎ 블록체인 전문기업의 변화: 블록체인 생태계 내 역량 강화를 위한 다양한 시도²⁴⁾

- 블록체인 전문기업들은 기 보유 인프라 기반 토큰 이코노미 구현 및 이해관계자 간 제휴 등을 통해 변화를 시도
 - (App Service 기업) 기존 블록체인 기반 서비스의 역량 강화를 통한 플랫폼 사용자 확대 및 유지
 - (Platform 기업) 기존 제공하던 서비스를 바탕으로 유사한 사업 분야로 확대 중, 이를 위해 Alliance를 형성하고 토큰의 사용 범위를 확대
 - (Infra) 메인넷을 보유하고 있는 기업은 기존에 블록체인을 사용하던 분야를 넘어, 공공, 제조업 등 타 산업으로 적용 사례 확보 중이며 블록체인 기반 공유 경제서비스 산업으로의 적용 및 확대 가능

[블록체인 전문기업의 변화방향성]



* 출처: 경기수·김대원(2019.12.17.), "블록체인 산업 현황 및 국외 정책 동향", SW산업본부 블록체인산업팀, 정보통신산업진흥원, 이슈리포트 2019-38호.

24) 경기수·김대원(2019.12.17.), "블록체인 산업 현황 및 국외 정책 동향", SW산업본부 블록체인산업팀, 정보통신산업진흥원, 이슈리포트 2019-38호.

나. 시장 분석

(1) 세계시장

- Marketsandmarkets(2020)의 보고서와 PwC의 2020년 'The trillion-dollar reasons to rethink blockchain'보고서를 종합하여 세계 계약 및 분쟁해결 관련 블록체인 시장을 추정하고 2018년 5천 5백만 달러 수준에서 연평균 60.5%로 성장하여 2024년 9억 4천만 달러 수준으로 성장할 것으로 예상

[계약 및 분쟁해결 관련 블록체인 세계 시장규모 및 전망]

(단위 : 백만 달러, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
세계	55	90	150	250	378	588	940	60.5

* 출처 : Blockchain Market by Component, marketsandmarkets(2020)과 The trillion-dollar reasons to rethink blockchain, PwC(2020)의 계약 및 분쟁해결 관련 블록체인 시장의 점유율을 기반으로 네모아이씨지 재가공

- PwC의 분석에 의하면, 크라우드펀딩, 온라인 직원채용, P2P 숙박, 카셰어링 서비스를 중심으로 전 세계 공유경제산업이 성장할 것으로 전망
- 인력공유가 연평균 성장률(CAGR) 37%로 가장 높으며, P2P 숙박이 31, 카셰어링 23%, 비디오스트리밍이 17%, 장비렌탈 5%, 도서대여 및 자동차가 각 3%로 나타나며, 이에 반해 DVD대여는 -5%로 성장률이 감소할 것으로 전망
 - 이는 비디오스트리밍, 디지털 콘텐츠 산업의 폭발적인 성장에 따른 결과로 볼 수 있음

[세계 공유 경제 시장규모 및 전망]

(단위 : 십억 달러, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
합계	21.7	25.3	29.6	34.5	40.3	47.0	54.8	16.7

* 출처 : 세계 공유 경제 시장규모 및 전망, 2019.01, 관계부처합동 공유경제 활성화 방안(서비스산업 혁신II)

(2) 국내시장

- 국내 계약 및 분쟁해결 관련 블록체인 시장을 추정한 결과 2018년 18억 원 수준에서 연평균 60.5%로 성장하여 2024년 307억 원 수준으로 성장할 것으로 예상

[계약 및 분쟁해결 관련 블록체인 국내 시장규모 및 전망]

(단위 : 억 원, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
국내	18	29	49	82	123	192	307	60.5

* 출처: Blockchain Market by Component, marketsandmarkets(2020)과 The trillion-dollar reasons to rethink blockchain, PwC(2020)의 계약 및 분쟁해결 관련 블록체인 시장의 점유율 기준으로 비트코인 화폐별 거래량 중 원화 점유율 2.97%²⁵⁾(코인힐스 2020.12.30.)을 근거로 네모아이씨지 재가공(환율:1100원/달러)

- 국내의 온라인 기반 개인 간(P2P) 공유경제 규모가 2015년 대비 3년 만에 10배로 성장했으나 시장 규모가 워낙 작고 또한, 이 중 숙박공유 서비스가 차지하는 비중이 90%로 한 분야에 치우쳐있으며, 국내의 많은 규제로 인해 성장이 더딘 것으로 보임
- 정부가 택시·숙박 업계 등 기존 사업자의 반발을 의식해 기존 규제를 풀지 못하며, 기존 산업의 생존권과 공유경제를 통한 창업·일자리 창출 사이에서 갈피를 잡지 못하여 한계에 봉착
 - '에어비앤비'가 불붙인 숙박공유업은 전 세계적으로 유행하고 있지만, 국내에선 일부만 합법이며 외국인 손님만 받을 수 있는 반쪽짜리 서비스라는 평가
 - 차량공유 사업을 둘러싼 갈등 지속, 세계적 차량공유 서비스 업체인 '우버'는 한국 시장에 진출한지 2년도 만에 사실상 서비스 종료
 - 2018년 택시업계와 스타트업계가 손잡고 규제 혁신형 플랫폼 택시사업 합의를 도출했지만, 지금까지 새로운 운송 서비스 전무, 택시업계는 승합차 공유 서비스인 '타다'가 개인택시 기사들의 생존권을 침해한다며 퇴출 요구
 - 최신 트렌드로 떠오르고 있는 공유주방 서비스도 식품위생법 규정으로 불가능

25) 미국달러:72.7%, 일본엔화:18.66%, 유로화:3.06%, 한국원화:2.97%

3. 기술 개발 동향

☐ 기술경쟁력

- 블록체인 기반 공유 경제 서비스는 미국이 최고기술국으로 평가되었으며, 우리나라는 최고기술국 대비 89.2%의 기술수준을 보유하고 있으며, 최고기술국과의 기술격차는 1.1년으로 분석
- 중소기업의 기술경쟁력은 최고기술국 대비 86.2%, 기술격차는 1.3년으로 평가
- EU(92.3%)>한국(89.2%)>중국(81.4%)>일본(77.1%)의 순으로 평가

☐ 기술수명주기(TCT)²⁶⁾

- 블록체인 기반 공유 경제 서비스는 3.33의 기술수명주기를 지닌 것으로 파악

가. 기술개발 이슈

◎ 현 스마트계약(Smart Contract)의 한계 및 개선점

- ☐ 블록체인 기반 스마트계약, 즉 자동 체결 계약은 매우 단순하고 엄격한 조건(예: 특정 이벤트 시 옵션을 행사할 수 있는 옵션 계약 또는 조건부 양도계약)에 근거해 중재기관 없이 자동으로 의무를 수행하고 암호 대금을 집행하는 방식으로 개발
- ☐ 스마트계약이 다양한 비즈니스 기회를 제공할 수 있지만, 스마트계약이 가지고 있는 중요한 한계점도 신중히 고려해야 함
- ☐ 스마트 계약의 한계점
 - 이더리움 기반의 플랫폼에서 실행되는 현재 스마트계약은 보안이 완벽하지 않으며, 프로그래밍 언어로 보안이 취약한 근시안적인 설계를 선택하는 것은 많은 이를 이용한 많은 비즈니스에 치명적인 결과를 가져올 위험이 존재
 - 스마트계약은 구두나 서면 형태로 체결되는 계약과 달리 '그저' 코드로 구축된 컴퓨터 프로그램으로 밖에 볼 수 없음
 - 스마트계약 당사자의 존재여부, 혹은 스마트계약이 단순히 분산된 컴퓨터 프로그래밍에 불과한 것인지 간에, 법률적 관점에서 스마트계약을 계약으로 볼 수 있을지는 여전히 불분명함
 - 스마트계약은 여타 코드와는 달리 스마트계약에는 패치를 적용할 수 없으므로 한 번 스마트계약이 배포되고 거기에 심각한 결함이 포함된 경우에는 스마트계약이 연관된 모든 시스템에 아주 큰 피해를 줄 수 있음
 - 블록체인의 모든 상태 변화는 전적으로 확정적이어야 한다는 스마트계약의 전제조건으로 인해 외부 사건에 대응해 스마트계약의 행위를 변경하는 것이 설계상 불가능

26) 기술수명주기(TCT, Technical Cycle Time): 특허 출원연도와 인용한 특허들의 출원연도 차이의 중앙값을 통해 기술 변화속도 및 기술의 경제적 수명을 예측

□ 스마트 계약의 개선점

- 현대 사회의 가치사슬은 고도로 복잡하며(예: 전 세계의 아이폰 공급자 네트워크), 확률적 및 동적인 자동 최적화와 수조의 프로세스 관련 거래 실행을 위해 점점 더 많은 인공지능, 머신러닝, 빅데이터 분석 알고리즘을 적용하여 위의 한계를 개선 또는 극복할 필요

◎ 다양한 요소기술의 검증 및 분석 필요

□ 스마트계약(Smart Contract)을 '거래'에 목적을 둔 기능이 아닌 '계약'의 본질적 기능 수행을 위한 구조적 응용 및 개발 필요

- 외부 사건에 대응하여 스마트계약의 행위 변경이 필요한 경우 인공지능 알고리즘과 같은 하이퍼스마트 알고리즘을 적용하여, 계약의 결함 해소 및 변경을 기술적으로 가능하도록 연구 필요
- 스마트계약 악성코드 탐지 시스템 고도화 필요
 - 공격자는 스마트 컨트랙트 기능을 악용하여 악성코드 등 악의적인 코드를 블록체인에 저장 및 실행 가능하며, 익명성이 보장되는 블록체인의 경우 블록체인상에서 악성코드 판매/구매를 위한 거래도 처리 가능

□ 거래에 참여하는 사용자 평판시스템의 관리·통제 기술 필요

- 평판시스템에 대한 참여자의 악용(위·변조 등) 가능성 존재
- 평판시스템에 연결된 사용자 개개인의 디지털 ID의 식별 및 통제 기능 고도화 필요

□ 공유경제 서비스 전반에 있어서 보안 이슈를 해소할 기술적 접근 필요

- 블록체인 간 자산교환, 기능 확장 등 연계 필요시 책임 주체 및 표준규격이 명확하지 않아 예상치 못한 보안위험 발생 가능
 - 블록체인 간 연계 및 상호운용을 위해서는 블록체인 간 자산교환에 대한 책임주체와 비정상 거래가 타 블록체인에 확산 될 경우 대책 등에 대한 고려 필요
 - 또한, 현재는 블록체인별로 서로 다른 지갑 S/W를 사용하여 키 생성 알고리즘, 거래요청 및 통신 프로토콜 등이 호환되지 않음
 - 블록체인 간 연계에 필요한 데이터 형식, 통신 프로토콜, 자산이전 절차, 키 생성·관리 등에 대한 표준 개발 필요
- 블록체인의 처리속도 한계, 거래정보 급증으로 인해 추가 서비스 개발 및 확대 제한 등의 가용성이 저하될 가능성 존재
 - 일반적으로 거래 유효성 확인은 모든 참여자가 수행하므로 참여자 수가 증가할수록 거래 처리속도가 저하되며 이로 인해 높은 처리능력이 요구되는 서비스 개발이 제한
 - * 참여자 간 처리능력이 일관되지 않을 경우 처리시간은 더 증가
 - 거래 유효성 검증을 전체 참여자가 아닌 신뢰 가능한 일부 검증노드와 수행하여 유효성 검증에 참여하는 노드의 수를 줄임으로써 처리속도를 개선

- 다수 참여자가 악성코드 등을 통해 공격자에게 장악될 경우 대량의 스팸거래를 발생 가능하며 이로 인해 블록체인 서비스가 중단 가능
 - DDoS 공격을 위한 스팸거래 요청은 악성코드에 감염된 참여자에 의해 발생될 수 있으며 분산 구조로 인해 전체 참여자에 대한 악성코드 감염여부 확인 등 대응이 어려움
 - 프라이빗 블록체인의 경우 의심 거래를 발생시키는 참여자를 네트워크에서 차단하는 등의 조치가 가능하지만, 공격자가 많은 수의 노드를 장악할 경우 여전히 DDoS 공격이 가능
 - 공격자가 대량의 스팸거래를 요청하지 못하도록 참여자별 거래요청 건수를 제한할 필요

□ 보안위협을 한 부분으로 거래의 검증 및 합의 기술

- 참여자 중 과반수(또는 운영주체)를 장악하여 블록체인의 합의 과정 조작 가능성
- 메인 체인에서 유효하지 않은 자산이 사이드 체인에서 거래 가능
 - * 비트코인 등 주요 블록체인(메인 체인)과 상호연계하여 가상화폐 호환성을 제공하거나 스마트 컨트랙트, 거래 기밀성 등의 기능을 추가 제공하는 블록체인
- 인증서 또는 IP 등을 기반으로 블록체인에 접근 가능하도록 참여자 목록 등을 관리하는 기술 필요

나. 생태계 기술 동향

(1) 해외 플레이어 동향

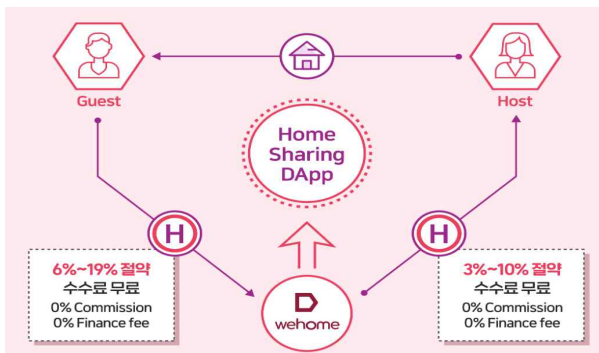
- ☐ 유헤공간 자원을 활용한 주요 공유물류 서비스는 다음과 같으며, 이 모델은 물류창고를 보유한 업체와 물류창고가 필요한 업체를 연결해 주는 플랫폼에서 공급자와 수요자를 매칭시키는 것이 핵심
 - (DHL) 세계 최대 물류 업체로, 자체적으로 보유한 물류센터 등 창고 공간 공유 플랫폼 서비스인 'Space'를 출시
 - 웹 및 모바일 환경에서 가용 공간을 탐색할 수 있도록 정보(창고의 위치 데이터, 공간에 대한 기본정보, 계약 관련 내용 등)를 제공
 - (FLEXE) 미국의 스타트업으로서 이 모델은 화물차를 비롯해 이용자가 창고 등의 물류시설을 소유하지 않아도 활용할 수 있음
 - 수요자가 스마트폰을 이용해 플렉스 모델 플랫폼에 접속해 필요한 물류창고 위치와 이용기간을 검색하여 조건에 부합하는 리스트를 중 선택하고, 물류창고의 최소 적재 단위인 팔렛(pallet) 수에 따라 요금이 계산
 - 물류창고의 경우 일반적으로 20~30% 정도의 유헤공간이 존재한다는데 착안해 개발된 이 공유 모델은 중소 유통업체와 제조업체의 라스트마일 경쟁력 제고를 지원
 - 상품 보관료는 아마존의 절반 정도에 불과하고, 성수기에 아마존은 보관료가 3배 이상 인상되지만 플렉스는 거의 동일하다는 것도 장점으로 볼 수 있음
 - (Amazon) 현재 Fedex와 UPS에 배송서비스를 의존하고 있는 상황으로, 자체적인 공유경제 서비스인 '아마존플렉스'를 개발·테스트 중
- ☐ (Turo) 투로는 개인이 소유한 자동차 자체를 공유하는 서비스를 제공하는데, 소유주는 자동차를 투로에 등록하여 자신이 이용하지 않는 기간에 차를 다른 사람에게 빌려주고 부가 수입을 얻을 수 있음
 - 35만대 차량이 투로에 등록되어 있으며 차주는 한 달에 평균 9일간 자신의 차를 공유하여 월 625달러(약 70만원)의 부가 수입을 올리고 있는 것으로 조사됨
- ☐ (Postmates) 포스트메이츠는 음식 배달서비스를 제공하는 업체인데, 빠른 서비스를 제공하기 위해 자체 배송 인력을 확보하는 동시에 등록만 하면 누구나 배송서비스를 제공할 수 있도록 하여 배송인력을 확보하고 있음
 - 이용자는 원하는 시간에 원하는 장소에서 원하는 시간만큼 배송서비스를 제공하고 그만큼의 수익을 창출할 수 있고, 포스트메이츠는 시간당 25달러 이상의 임금을 지불하고 있는 것으로 조사됨

- ☐ (Omni) 옴니는 도심 보관서비스에 공유경제형 서비스를 접목하여 도심 내에 빈 공간을 대거 확보한 뒤 원룸이나 공간이 부족한 아파트에 거주하는 사람들에게 물품 보관 서비스를 제공
 - Omni는 도심 내 유휴 공간이나 외곽지역을 활용해 집안에 보관하기 부담스러운 겨울옷과 겨울 이불 등을 보관해줌
 - 이에 대해 정형화되고 표준화된 물류서비스가 도달할 수 없었던 품질 중심의 혁신적 서비스 모델이라는 평가가 있음
- ☐ (Origin Protocol) 오리진프로토콜은 블록체인 위에 탈중앙화된 공유경제 마켓플레이스를 구축하는 플랫폼 사업, 중계자를 없애 수수료를 절감
 - 우버, 에어비앤비는 중앙화 플랫폼으로 공유경제에 적합하지 않다며, 자신들이 진정한 탈중앙화 플랫폼으로 20~30% 수수료 절감이 가능
- ☐ (Slock.it) 슬록잇은 에어비앤비(Airbnb)와 유사한 분권형 부동산 공유 애플리케이션인 'The DAO'를 배포
 - 2019년 6월 미국의 블록체인 인큐베이터이자 투자회사인 블록체인즈(Blockchains)가 독일의 이더리움 개발팀 Slock.it(슬록잇)을 인수

(2) 국내 플레이어 동향

- (위홈) 한국판 에어비앤비라 불리는 블록체인 기반의 공유 숙박 업체이며, 현재 2020 서울시 지정 공유기업으로 선정되어 2020년 8월 1일부터 공식적인 서비스를 개시하고 있음
- 2019년 11월 정부의 공유숙박, 규제샌드박스 실증특례 승인 및 2020년 7월15일부터 정식 서비스 허가
- ‘위홈’은 온디맨드 홈(On-demand Home)을 공유숙박을 통해 소비자 권익 증대와 함께 기존 대체숙박업과 상생을 넘어 더불어 도약하는 계기를 만들고자 함
 - 모바일을 포함한 정보통신기술(ICT)인프라를 통해 소비자의 수요에 맞춰 즉각적으로 맞춤형 제품 및 서비스를 제공하는 경제활동
- ‘위홈’의 비즈니스 모델은 아래 그림과 같으며, 현 코로나-19 사태로 인해 파생한 자가격리자와 가족을 위한 아웃스테이 추진, 바쁜 직장인을 위한 비즈스테이, 대형병원 환자가족을 위한 케어스테이 등 다양한 수요에 맞춤형으로 공유경제를 실현하고 있음

[공유숙박 ‘위홈’ 비즈니스 모델]



* 출처: 서울시 지정 공유기업 소개 - 위홈, 2020, 공유허브 홈페이지

[‘위홈’ 특례 공유숙박]



* 출처: 위홈 특례 공유 숙박, 위홈 공식홈페이지

- 정부가 위홈을 유일한 규제특례 공유숙박 플랫폼으로 지정하여 내외국인 게스트를 합법적으로 유치
- 위홈의 규제특례 호스트로 지정받으면 ‘위홈특례공유숙박업’을 합법적 운영할 수 있고, 지정 조건과 평가 기준에 따른 간단한 심사를 거쳐서 등록여부가 결정
 - (실증내용) 위홈의 ‘서울 지하철역 중심 내·외국인 공유숙박 서비스’가 가능하도록 내국인을 대상으로 도시민박을 중개할 수 있도록 2년간 실증특례 부여 (2 년간 연장 가능)
 - (실증범위) 전체 호스트를 4,000명 이내로 하며(1~9호선* 지하철역 반경 1Km 이내에 호스트 위치), 호스트별 영업일수는 연간 180일 이내로 한정 * 1호선은 ‘서울 1호선’으로 한정
 - (대상) 신규 호스트(타입A) 및 기존 외관민박업(외국인관광도시민박업) 호스트(타입B)

- (바르크 플랫폼)은 블록체인 기술을 통한 탈중앙화된 사람이 지닌 가치 교환 공유경제 서비스 플랫폼으로, 인간관계를 핵심가치로 생태계를 구성하는 참여자들의 다양한 자원과 부가가치를 서로 독점이 아닌 공유 형태로써 활동적으로 소비, 경제 활동을 하게 도움
 - 사람의 가치를 인정하고 인정받으며, 서로 교환을 통해 물건/노동/서비스/정보/컨텐츠/렌탈 등의 교환 거래가 이루어지며 긍정적 상관관계를 형성하는데 가장 큰 목적
 - 위 컨셉을 구체화하여 ‘액션마이닝’이라는 형태의 참여자 보상 시스템을 구축했으며, 이를 통해 해당 생태계 안에서 발생하는 모든 경제 생산 활동 및 상호작용으로 일어나는 참여자들의 기여도를 수치화하여 보상
 - 바르크는 최저가 쇼핑몰 메이버그와 제휴를 통해 바르크 회원들만 전용으로 사용할 수 있는 폐쇄물을 개설, 바르크 멤버스라는 이름의 폐쇄물은 바르크 코인을 바르크 토큰으로 전환해 메이버그에 일정 비율로 사용
 - 입점된 상품들은 유통수수료를 크게 낮춰 타 오픈마켓보다 낮은 가격에 제품을 판매
 - 회원제로만 운영되고 있으며, 제품들 외의 여행, 골프, 상조 등의 상품 및 서비스도 3만원 이하의 저렴한 가격을 통하여 거품 없는 가격으로 이용 가능
- (나르고)는 세계 최초의 지인 기반 광고 공유 플랫폼으로 기존의 인플루언스 마케팅 비즈니스 모델을 뛰어넘어, 바로 내 전화번호부 속의 지인 기반 인플루언스 네트워크를 활용한 광고 플랫폼과 보다 진화된 블록체인 액션마이닝을 결합
 - 나르고의 지인 기반 인플루언서 마케팅은 최근 2~3년 동안 급성장한 광고 마케팅 분야로서, 미디어믹스에 따르면, TV 시청 감소와 광고를 차단하는 '애드블록킹' 증가에 따른 광고 예산의 이동 등으로 인해 2020년 글로벌 인플루언서 마케팅 시장은 적게는 약 5조 원 규모에서 많게는 약 10조 원 규모로 성장할 것으로 예상
 - 상기 언급 된 국내 사례 ‘바르크’와 전략적 제휴 협약(MOU)을 2019년 11월 체결하고, 블록체인 토큰 비즈니스를 공동 추진
 - 발행된 토큰은 나르고의 다양한 광고 캠페인 참여에 사용할 수 있으며, 참여 충성도에 따라 액션마이닝을 통해 채굴되어 인플루언서에게 돌아감
 - 이는 브랜드에서 액세스 제품 및 서비스를 얻거나 쇼핑 시 할인 혜택을 제공받을 수 있고 고유한 토큰을 만들어 잠재 고객에게 보상도 할 수 있음
 - 또한 티머니처럼 사용할 수 있는 나르고 코인 교환 기능, 브랜드 및 충성도 높은 비즈니스와의 협업 기능, 맞춤형 인플레이스 토큰 생성 등 인플루언서를 위한 다양한 환경으로 편리함을 제공할 예정
 - 나르고 플랫폼에서 모든 콘텐츠 제작과 이용 내역은 투명하게 공개되고, 유저들의 플랫폼 활동(광고하기, 광고보기, 후원, 아이템 구매 등) 역시 블록에 기록
 - 위 기록을 스마트계약(Smart Contract)으로 전환하여 유저들의 플랫폼 활동에 따라 코인으로 보상하고, 모든 구성원들에게 합당한 수익이 돌아가도록 함

다. 국내 연구개발 기관 및 동향

(1) 연구개발 기관

[블록체인 기반 공유 경제 서비스 분야 주요 연구조직 현황]

기관	소속	연구분야
고려대학교	블록체인연구소	<ul style="list-style-type: none"> • 블록체인 기반 응용서비스 • 스마트 컨트랙트의 프로세스와 정책 등 연구
서강대학교	지능형 블록체인 연구센터	<ul style="list-style-type: none"> • 적응형 블록체인을 위한 모듈 개발 및 블록체인 통합 플랫폼 개발 • 신뢰기반의 도메인 특성을 반영한 블록체인 요소 알고리즘 개발
중앙대학교	블록체인 서비스 연구센터	<ul style="list-style-type: none"> • 각종 서류(연구기록 등)를 블록체인으로 관리하고, 블록체인의 실험과 검증을 위한 테스트베드 구축
한국전자기술연구원	지능정보연구본부	<ul style="list-style-type: none"> • 산업 빅데이터 분석 SW • 임베디드 AI 시스템 • 주력융합산업 임베디드 SW (자동차, 항공, 철도, 자동화시스템 등)
	초연결통신연구원	<ul style="list-style-type: none"> • 블록체인 ICT 인프라 구축을 위한 정책 및 사업기획 • 차세대 합의 알고리즘/스마트컨트랙트 등 핵심원천기술개발 • 공유 협업 플랫폼(퍼블릭, 프라이빗 포함) 기술개발 • 개발환경 및 검증 기술개발 • 융합서비스 개발 • 표준화 및 상용화 지원

(2) 기관 기술개발 동향

☐ (로지포커스주식회사)

- 소비자 보호를 위한 개인 간 거래용 블록체인 기반 차량 공유 서비스 플랫폼 개발 (2020-07-16~2021-07-15)
 - 강화학습 기반 루트 플래닝 기술 개발
 - 실시간 운임 산정 기술 설계
 - 블록체인 기반 운송정보 추적 기술 개발
 - 운전자 안전운전 지원 커넥티드카 기술 개발
 - 안전운전 지원 게이미피케이션 커넥티드카 모바일 인포테인먼트 콘텐츠 설계
 - 공유경제 기반 P2P 생활물류 공유 플랫폼 설계

☐ (한국전자기술연구원)

- 블록체인이 적용된 SAL(Secure Access Lock)모듈 기반의 사물 공유·거래 서비스 플랫폼 개발 (2019-04-01~2020-12-31)
 - 서비스 종속 SAL 디바이스 체인지 H/W 핵심 기술 개발
 - Lock & unlock 프로토콜 개발
 - 스마트 잠금장치 I/F 개발
 - 공유/거래 플랫폼 dApp 모니터링 기능 개발
 - 공유/거래 플랫폼 dApp 개발
 - 지정 서비스 특화 정보 보호 및 dApp 모니터링 모듈 개발
 - 이종 자원 공유 서비스를 위한 SAL 디바이스 기술 개발
 - 공유 경제 촉진을 위한 서비스 환경 구축

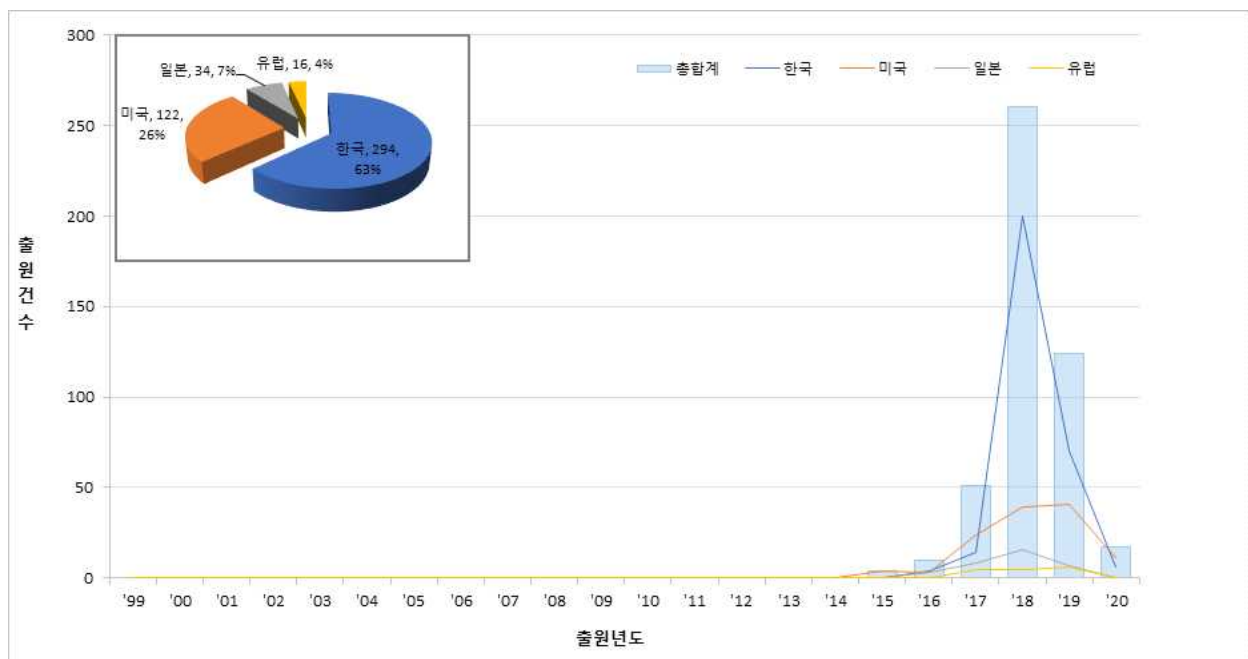
4. 특허 동향

가. 특허동향 분석

(1) 연도별 출원동향

- 블록체인 기반 공유 경제 서비스는 '17년부터 급격한 성장을 보임
 - 각 국가별로 살펴보면 한국이 가장 활발한 출원활동을 보이고 있음
- 국가별 출원비중을 살펴보면 한국이 전체의 63%의 출원 비중을 차지하고 있어, 최대 출원국으로 블록체인 기반 공유 경제 서비스 분야를 리드하고 있는 것으로 나타났으며, 미국은 26%, 일본은 7%, 유럽은 3% 순으로 나타남

[블록체인 기반 공유 경제 서비스 연도별 출원동향]



(2) 국가별 출원현황

☐ 한국의 출원현황을 살펴보면, '18년부터 해당 기술의 출원이 급격히 증가하는 추세

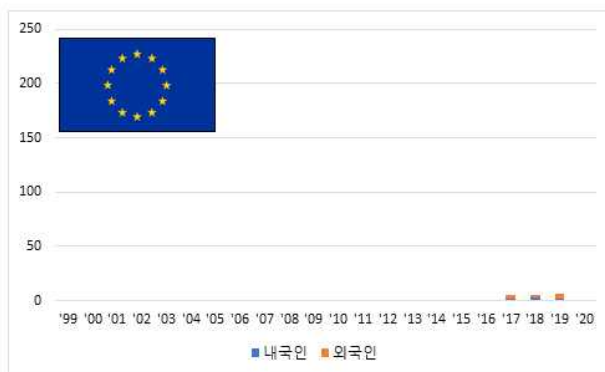
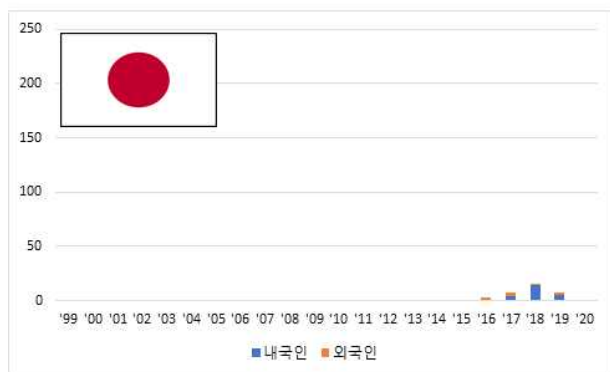
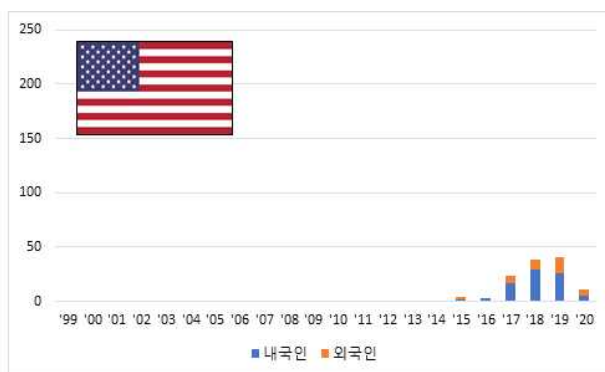
- 내국인 위주의 출원이 진행되고 있음
- 한국 기술의 양적 흐름은 '18년에 가장 많은 특허를 출원
- 한국의 출원 수는 미국, 유럽, 일본에 비해 가장 많은 특허를 출원

☐ 미국의 출원현황을 살펴보면, 한국과 유사한 동향을 보임

☐ 유럽의 출원현황은 출원수가 매년 10건 이하로, 뚜렷한 증감 동향이 나타나지 않음

☐ 일본의 출원현황을 살펴보면, 한국과 유사한 동향을 보임

[국가별 출원현황]

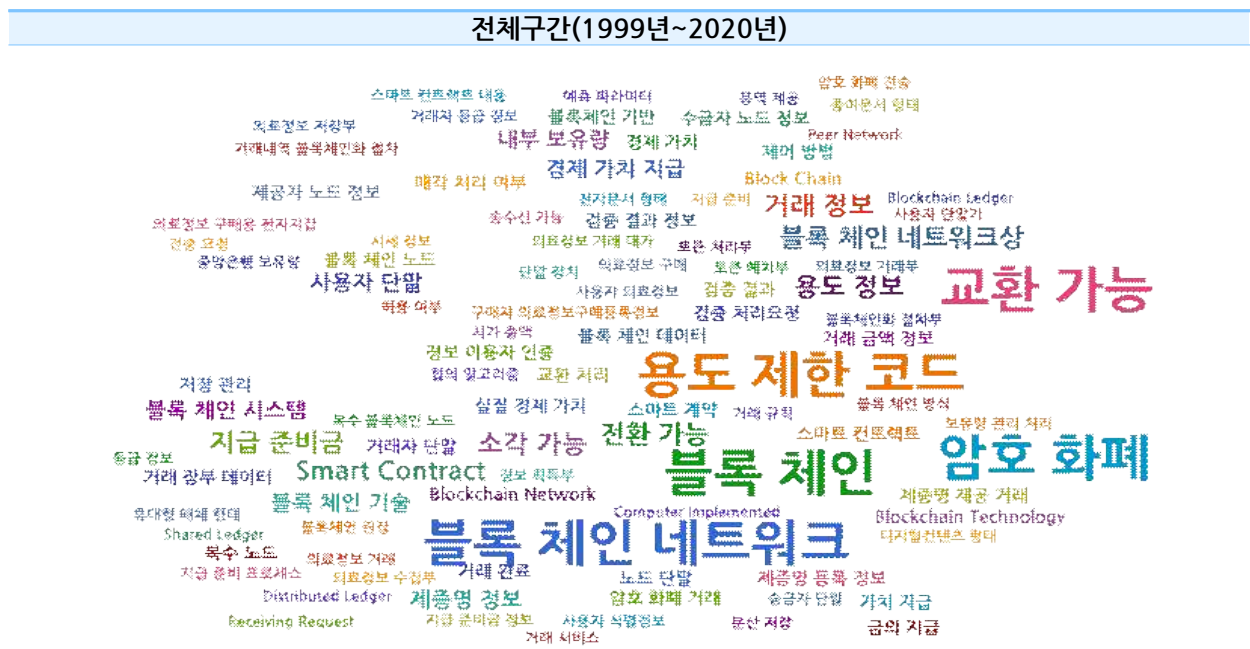


(3) 기술 집중도 분석

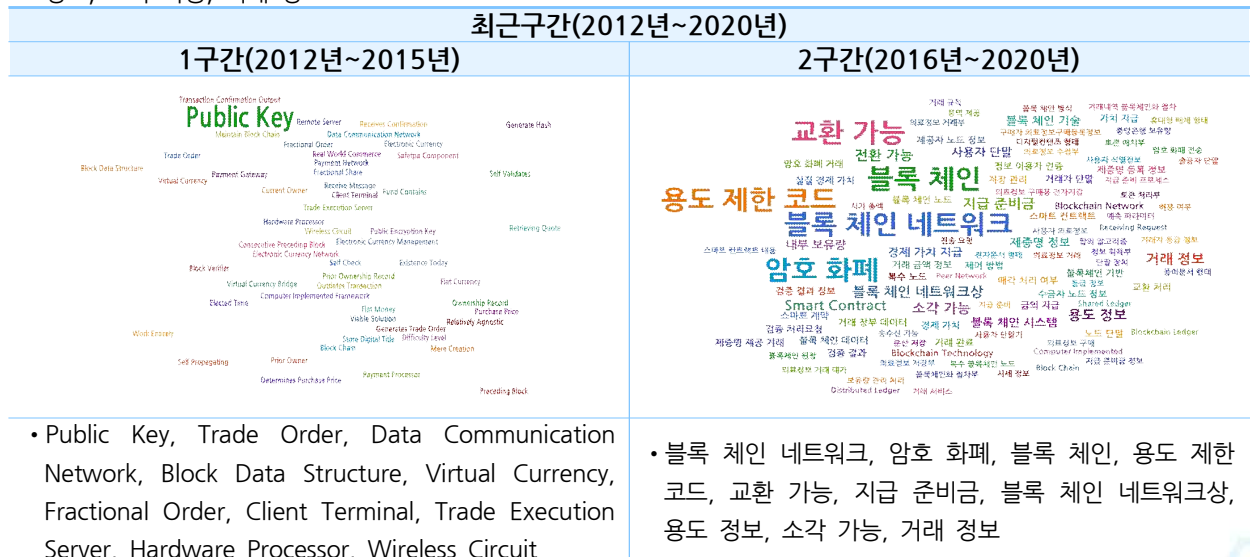
□ 전략제품에 대한 최근 기술 집중도 분석을 위한 구간별 기술 키워드 분석 진행

- 전체 구간(1999년~2020년)에서 블록 체인 네트워크, 암호 화폐, 블록 체인 등 키워드가 다수 도출
- 최근 구간 분석 결과, 최근 1구간(2012년~2015년)과 비교할 때 2구간(2016년~2020년)에서 용도 제한 코드, 교환 가능, 지급 준비금 키워드가 많이 등장하는 것으로 보아, 블록체인 기반 공유경제 서비스 분야에는 부정거래 방지기술, 공적가시성 확보를 위한 기술, 거래내역 추적 기술 관련 연구개발이 활발한 것으로 추정

[특히 키워드 변화로 본 기술개발 동향 변화]



- 블록 체인 네트워크, 암호 화폐, 블록 체인, 용도 제한 코드, 교환 가능, 지급 준비금, 블록 체인 네트워크상, 용도 정보, 소각 가능, 거래 정보



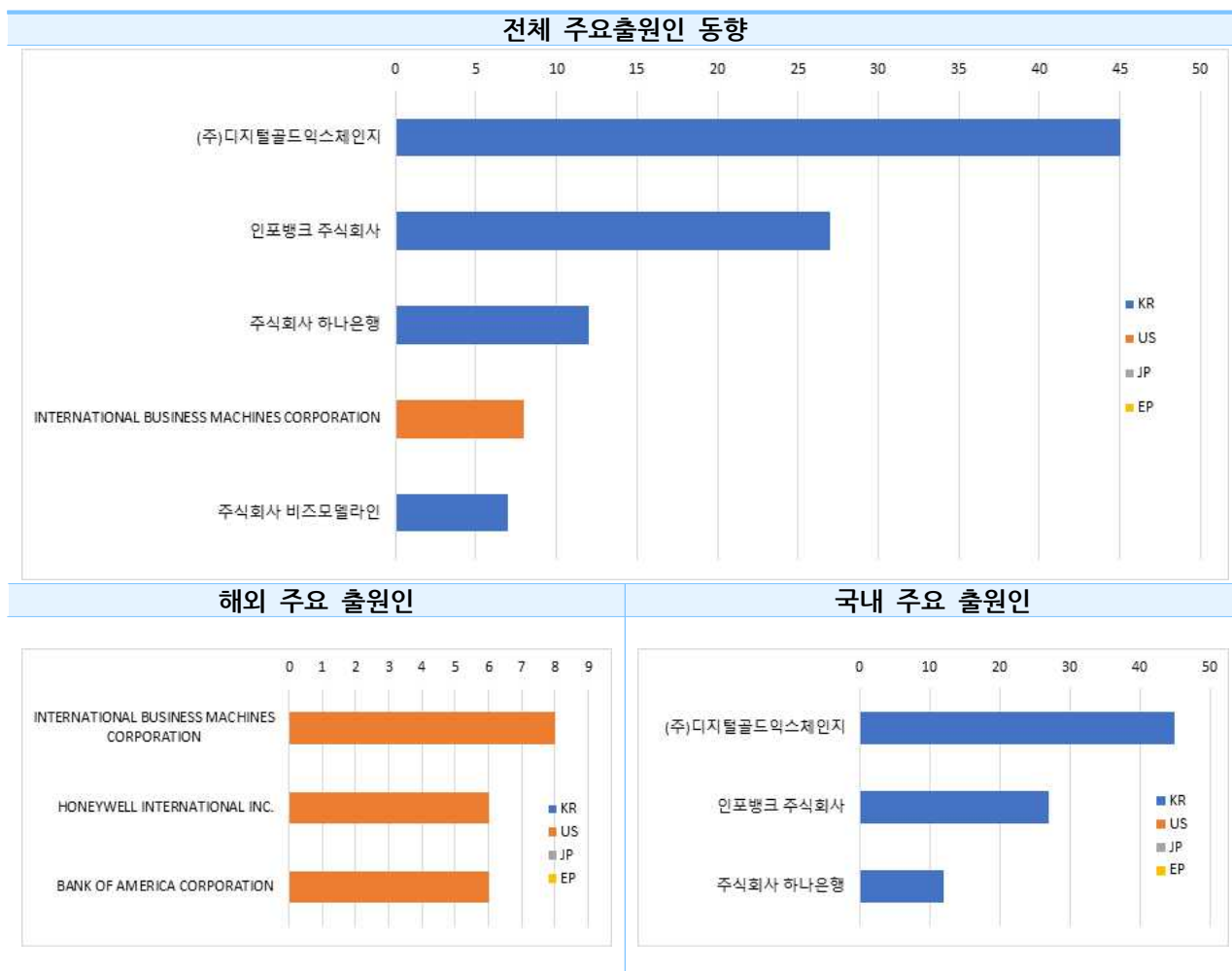
- Public Key, Trade Order, Data Communication Network, Block Data Structure, Virtual Currency, Fractional Order, Client Terminal, Trade Execution Server, Hardware Processor, Wireless Circuit

- 블록 체인 네트워크, 암호 화폐, 블록 체인, 용도 제한 코드, 교환 가능, 지급 준비금, 블록 체인 네트워크상, 용도 정보, 소각 가능, 거래 정보

나. 주요 출원인 분석

- ☐ 블록체인 기반 공유 경제 서비스의 전체 주요출원인을 살펴보면, 주로 한국 국적의 출원인이 다수 포함되어 있는 것으로 나타났으며, 제 1 출원인으로는 한국의 (주)디지털골드익스체인지가 나타남
 - 제 1 출원인인 (주)디지털골드익스체인의 출원은 한국에 집중된 경향을 보임
- ☐ 블록체인 기반 공유 경제 서비스 관련 기술로 소프트웨어를 개발하는 대기업에 의한 출원이 대다수를 차지
 - 국내에서는 중소기업(개인), 대기업의 활발한 출원이 이루어짐

[블록체인 기반 공유 경제 서비스 주요출원인]

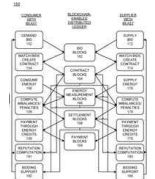


(1) 해외 주요출원인 주요 특허 분석

◎ IBM(International Business Machines)

- IBM은 미국의 다국적 기업으로, 다수의 블록체인 관련 특허를 보유하고 있으며, 블록체인 기반 공유 경제 서비스 기술과 관련한 특허를 미국에 출원
- 블록체인 기반 공유 경제 서비스에 관련하여 출원을 진행한 특허 모두 미국에 출원한 것으로, 자국내 출원 성향이 높은 것으로 사료

[IBM 주요특허 리스트]

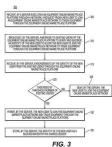
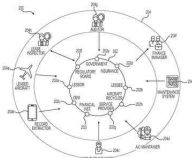
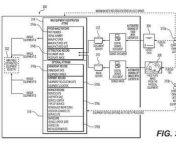
등록번호 (출원일)	명칭	기술적용분야	도면
US10762564 (2016.11.10)	Autonomous peer-to-peer energy networks operating on a blockchain	에너지 최적화 절차를 위한 분산 원장(distributed ledger)을 저장하기 위해 블록체인 구성	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ HONEYWELL INTERNATIONAL INC.

- HONEYWELL INTERNATIONAL INC.는 미국의 다국적 복합 기업으로, '18년도 10월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- HONEYWELL INTERNATIONAL INC.의 공개특허를 대상으로 분석한 결과, 블록체인 관련 특허를 다수 보유하고 있으며, 블록체인 기반 공유 경제 서비스 기술과 관련된 특허를 미국과 유럽에 출원
 - 블록체인 기반 공유 경제 서비스에서 블록체인을 이용하여 장비 임대에 대한 전자 거래 등의 응용 특허를 다수 보유

[HONEYWELL INTERNATIONAL INC. 주요특허 리스트]

공개번호 (출원일)	명칭	기술적용분야	도면
EP3651105 (2019.11.05)	Systems and methods for verifying identity of a user on an equipment online marketplace platform	블록체인을 이용한 온라인 마켓플레이스 플랫폼을 통해 장비를 거래하기 위해 신규 사용자의 신원 확인 방법	
US2020-0184548 (2019.10.07)	Systems and methods for leasing equipment or facilities using blockchain technology	장비 또는 설비를 임대하는 방법으로 블록체인 기술을 이용하여 임대인과 임차인 간의 전자 임대차 계약 거래	
US2020-0151784 (2019.08.05)	Systems and methods for generating a digital identity of equipment on an equipment online marketplace platform	온라인 마켓플레이스 플랫폼 상에서 장비의 디지털 아이덴티티를 생성하기 위한 컴퓨터 구현 방법	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

© BANK OF AMERICA CORPORATION

- ☐ BANK OF AMERICA CORPORATION은 미국의 상업 은행으로 블록체인 기반 공유 경제 서비스 기술과 관련하여, 등록특허 1건 보유

[BANK OF AMERICA CORPORATION 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
US10498808 (2018.03.28)	Blockchain-based property management	물리적 특성 아이템의 제조, 출하, 및 판매와 관련된 공급 체인을 따라 복수의 포인트들에서 설정하여 블록체인 기반 속성 관리를 위한 방법	

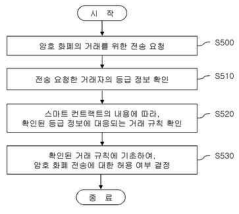
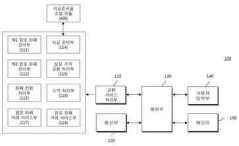
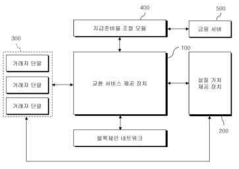
* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

(2) 국내 주요출원인 주요 특허 분석

◎ (주)디지털골드익스체인지

- (주)디지털골드익스체인지는 블록체인 기반 공유 경제 서비스 기술에 있어서, '18년도 10월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- (주)디지털골드익스체인지의 공개특허를 대상으로 분석한 결과, 블록체인 기반 암호화폐 기술과 관련된 특허를 다수 출원
 - (주)디지털골드익스체인지는 자체적으로 암호화폐를 개발하였으며, 블록체인 기반 공유 경제 서비스 기술과 관련하여 45건의 한국 출원을 진행

[(주)디지털골드익스체인지 주요특허 리스트]

공개번호 (출원일)	명칭	기술적용분야	도면
KR2020-0048548 (2018.10.30)	블록체인 기반 거래 규칙 적용 방법, 그를 수행하기 위한 단말 장치 및 프로그램	블록체인 기반 스마트 컨트랙트(SMART CONTRACT)에서 규정된 거래 규칙에 따라 거래를 처리하는 단말 장치와 프로그램	
KR2020-0048490 (2018.10.30)	블록 체인 기반 실질 경제 가치 거래 서비스 제공 방법 및 그 장치	블록 체인 기반의 실 경제 가치 연동 암호 화폐 거래 서비스 제공	
KR2020-0048483 (2018.10.30)	블록 체인 기반 실질 가치 교환 거래 시스템	블록 체인을 기반으로 하는 암호 화폐 데이터의 분산거래를 수행하여 실질 가치 연동 암호 화폐 교환 거래 시스템	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 인포뱅크 주식회사

- 인포뱅크 주식회사는 한국의 소프트웨어 개발 전문 기업으로, '18년도 5월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- 인포뱅크 주식회사의 공개특허를 대상으로 분석한 결과, 블록체인 기반 공유 경제 서비스 기술과 관련된 특허를 27건 출원

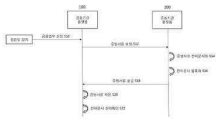
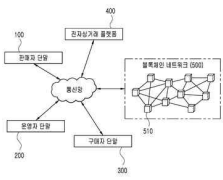
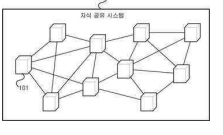
[인포뱅크 주식회사 주요특허 리스트]

공개번호 (출원일)	명칭	기술적용분야	도면
KR2019-0136594 (2018.05.31)	용도 지정형 암호 화폐의 거래 정보 처리 장치	용도 제한 코드를 포함하는 암호 화폐 거래 정보의 검증에 따라, 상기 암호 화폐를 수금한 수금자의 제3자 거래시 검증	

◎ 주식회사 하나은행

- ☐ 주식회사 하나은행은 한국의 금융 기업으로, '19년도 1월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- 주식회사 하나은행의 공개특허를 대상으로 분석한 결과, 블록체인 기반 공유 경제 서비스 기술과 관련된 특허를 12건 출원

[주식회사 하나은행 주요특허 리스트]

공개번호 (출원일)	명칭	기술적용분야	도면
KR2020-0097973 (2019.02.11)	블록체인 기반의 전자문서 공유 시스템 및 방법	블록체인 네트워크 상에서 금융기관과 증빙기관을 연결하여 금융기관 고객의 증빙서류 제출 프로세스를 간소화할 수 있는 블록체인 기반의 전자문서 공유 시스템	
KR2020-0094984 (2019.01.31)	전자상거래 시스템 및 그 운영 방법	전자상거래 플랫폼 운영자와 전자상거래 플랫폼에 입점하는 판매자 간의 계약 체결 프로세스 및 거래대사 프로세스를 간소화하는 기술	
KR2020-0095204 (2019.01.31)	지식 공유 시스템 및 그 방법	통신망을 이용해 이용자들 간에 질문 및 질문에 대한 답변을 공유할 수 있는 환경을 제공하는 복수의 블록체인 노드로 구성된 지식 공유 시스템	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

다. 기술진입장벽 분석

(1) 기술 집중력 분석

- 블록체인 기반 공유 경제 서비스 관련 기술에 대한 시장관점의 기술독점 현황분석을 위해 집중률 지수(CRn: Concentration Ratio n, 상위 n개사 특허점유율의 합) 분석 진행
- 상위 4개 기업의 시장점유율이 0.20로 블록체인 기반 공유 경제 서비스 분야에 있어서 독과점 정도는 낮은 수준으로 판단
 - 국내 시장에서 중소기업의 점유율 분석결과 0.82로 해당 기술에 대하여 중소기업이 진입하여 활동하고 있는 것으로 파악

[주요출원인의 집중력 및 국내시장 중소기업 집중력 분석]

주요출원인 집중력	주요출원인	출원건수	특허점유율	CRn	n
	(주)디지털골드믹스체인지(한국)	45	9.7%	0.10	1
	인포뱅크 주식회사(한국)	27	5.8%	0.15	2
	주식회사 하나은행(한국)	12	2.6%	0.18	3
	INTERNATIONAL BUSINESS MACHINES CORPORATION(미국)	8	1.7%	0.20	4
	주식회사 비즈모델라인(한국)	7	1.5%	0.21	5
	HONEYWELL INTERNATIONAL INC.(미국)	6	1.3%	0.23	6
	BANK OF AMERICA CORPORATION(미국)	6	1.3%	0.24	7
	TEMPLUM, INC.(미국)	4	0.9%	0.25	8
	주식회사 미탐스플러스(한국)	4	0.9%	0.26	9
	삼성에스디에스 주식회사(한국)	4	0.9%	0.26	10
	전체	466	100%	0.20	
국내시장 중소기업 집중력	출원인 구분	출원건수	특허점유율	CRn	n
	중소기업(개인)	235	81.6%	0.82	
	대기업	34	11.8%		
	연구기관/대학	19	6.6%		
	전체	288	100%	CR중소기업=0.82	

(2) 특허소송 현황 분석

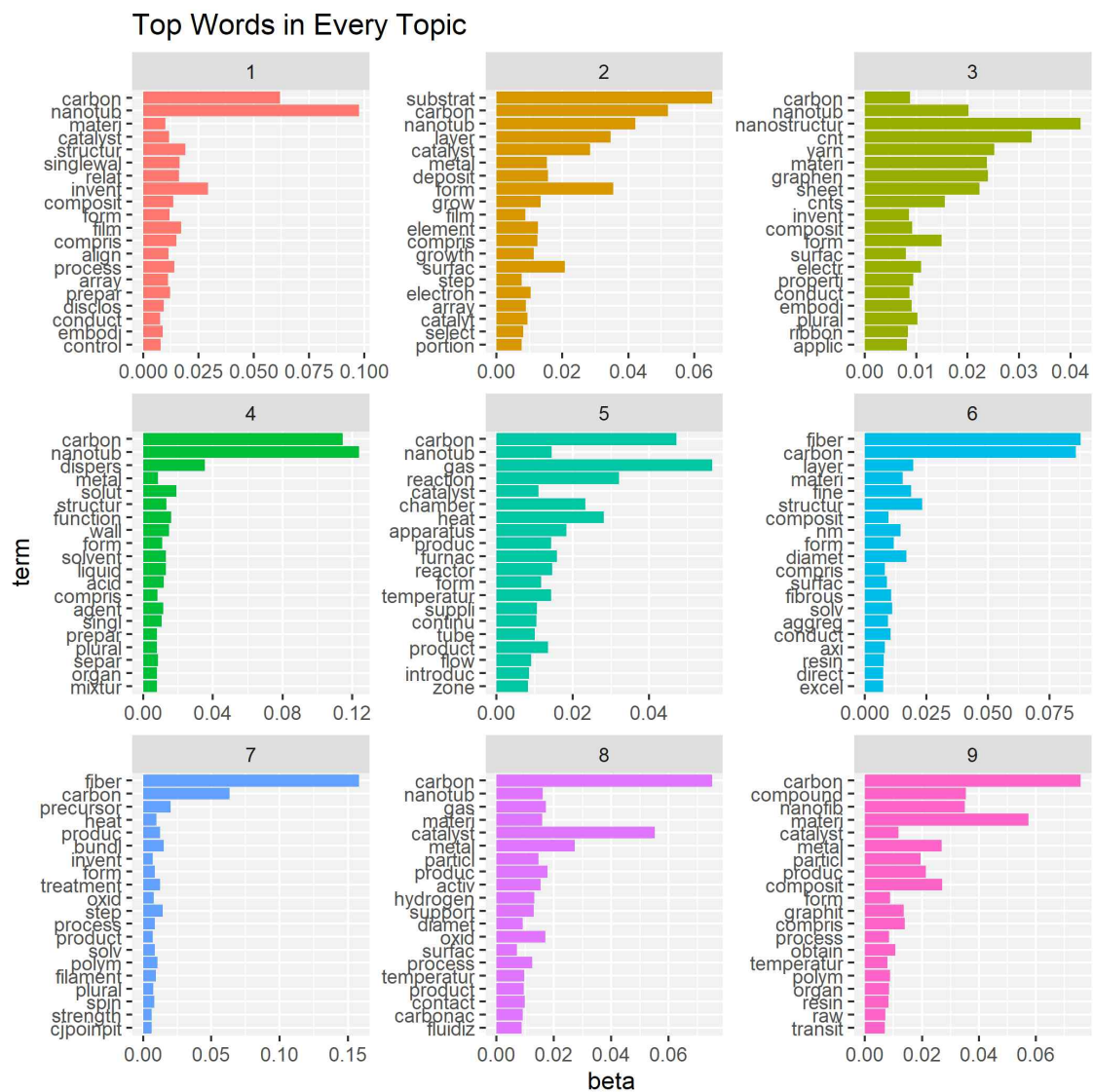
- ☐ 블록체인 기반 공유 경제 서비스 분야 관련 특허소송 이력은 검색되지 않음
 - 따라서 국내기업이 미국시장에 진입하는 경우, 해당 분야를 선점할 수 있을 것으로 판단
 - 다만, 블록체인과 관련해서는 4개의 소송이 검색

5. 요소기술 도출

가. 특허 기반 토픽 도출

- 152개의 특허의 내용을 분석하여 구성 성분이 유사한 것끼리 클러스터링을 시도하여 대표성이 있는 토픽을 도출

[블록체인 기반 공유 경제 서비스에 대한 토픽 클러스터링 결과]



나. LDA²⁷⁾ 클러스터링 기반 요소기술 도출

[LDA 클러스터링 기반 요소기술 키워드 도출]

No.	상위 키워드	대표적 관련 특허	요소기술 후보
클러스터 01	transact, plural, blockchain, account, data, generate, currency, block, virtual, hash	<ul style="list-style-type: none"> • Social aggregated fractional equity transaction partitioned acquisition apparatuses, methods and systems • Computer implemented frameworks and methods configured to create and manage a virtual currency 	분산 공유플랫폼
클러스터 02	blockchain, asset, service, apparatus, node, transact, block, vehicle, network, client	<ul style="list-style-type: none"> • Managing housing scores using smart contracts in blockchain networks • Decentralized blockchain oracle price discovery platform with bi-directional quotes 	-
클러스터 03	product, security, blockchain, identification, token, seller, computing, trade, data, transfer	<ul style="list-style-type: none"> • Platform, system and method for diamond trading • Method and system for tuning blockchain scalability, decentralization, and security for fast and low-cost payment and transaction processing 	블록체인 거래검증 및 합의 기술
클러스터 04	carbon, resource, emission, node, function, transact, der, exchange, data, product	<ul style="list-style-type: none"> • Blockchain-based carbon trading system • Wireless base station crowdfunding 	분산 공유플랫폼
클러스터 05	blockchain, equip, marketplace, share, online, network, target, rental, identify, platform	<ul style="list-style-type: none"> • Projector file for lighting installations • Systems and methods for leasing equipment or facilities using blockchain technology 	-
클러스터 06	transact, blockchain, ledger, server, manage, record, asset, distribute, computing, transfer	<ul style="list-style-type: none"> • Methods and system for managing intellectual property using a blockchain • Method for settling a blockchain asset 	블록체인 참여자 식별 및 접근통제 기술
클러스터 07	blockchain, record, asset, digit, function, real, value, estate, contract, process	<ul style="list-style-type: none"> • Decentralized blockchain oracle price discovery platform with bi-directional quotes • Apparatus, code, methods and systems for providing proof of trust related to smart contracts 	분산 공유플랫폼
클러스터 08	data, node, block, blockchain, plural, share, chain, shareholder, request, vote	<ul style="list-style-type: none"> • Method, system, and apparatus for managing focus groups • Authenticity verification of a digital model 	거래 데이터 판독 시스템
클러스터 09	content, item, property, block, terminal, computing, sale, platform, resource, chain	<ul style="list-style-type: none"> • Flexible payment services for travel and credit cards • Systems and methods for leasing equipment or facilities using blockchain technology 	-

27) Latent Dirichlet Allocation

다. 특허 분류체계 기반 요소기술 도출

- 블록체인 기반 공유 경제 서비스 관련 특허에서 총 10개의 주요 IPC코드(메인그룹)를 산출하였으며, 각 그룹의 정의를 기반으로 요소기술 키워드를 아래와 같이 도출

[IPC 분류체계에 기반한 요소기술 도출]

IPC 기술트리		
(서브클래스) 내용	(메인그룹) 내용	요소기술 후보
(G06F) 전기에 의한 디지털 데이터처리	• (G06F-021) 부정행위로부터 프로그램 또는 데이터, 그 컴퓨터 부품을 보호하기 위한 보안 장치	부정거래 방지 기술
	• (G06F-016) 정보 검색; 그 데이터베이스 구조; 그 파일 시스템 구조	-
(G06Q) 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 데이터 처리 시스템 또는 방법; 그 밖에 분류되지 않는 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 시스템 또는 방법	• (G06Q-020) 지불 체계, 방식 또는 프로토콜	이중지불방지 기술
	• (G06Q-010) 경영; 관리	블록체인 간 자산연계 및 교환서비스 기술
	• (G06Q-040) 금융; 보험; 세무 전략; 법인세 또는 소득세의 처리	-
	• (G06Q-030) 거래, 예. 쇼핑 또는 전자상거래	부정거래 방지 기술
	• (G06Q-050) 특정 사업 부문에 특히 적합한 시스템 또는 방법, 예. 공익사업 또는 관광	공적 가시성을 위한 거래내역 추적 기술
(H04L) 디지털 정보의 전송, 예. 전신통신	• (H04L-009) 비밀 또는 보안통신을 위한 배치	-
	• (H04L-029) 그룹 1/00에서 H04L 27/00의 하나에도 포함되지 않는 배치, 장치회로 또는 시스템	-
(H04N) 화상통신, 예. 텔레비전	• (H04N-021) 선택적 콘텐츠 분배, 예. 대화형(interactive) TV, VOD	-

라. 최종 요소기술 도출

- ☐ 산업·시장 분석, 기술(특허)분석, 전문가 의견, 타부처 로드맵, 중소기업 기술수요를 바탕으로 로드맵 기획을 위하여 요소기술 도출
- ☐ 요소기술을 대상으로 전문가를 통해 기술의 범위, 요소기술 간 중복성 등을 조정·검토하여 최종 요소기술명 확정

[블록체인 기반 공유 경제 서비스 분야 요소기술 도출]

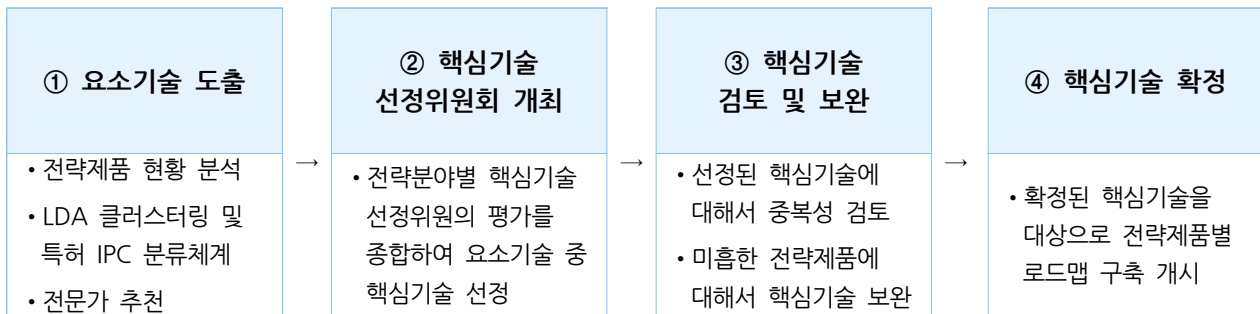
요소기술	출처
분산 공유플랫폼	특허 클러스터링, 전문가 추천
공급자 탐지 및 실시간 연결 기술	전문가추천
표준 언어 단위 로직 구현 및 관리	전문가추천
개방형 접근 통제 기술	전문가추천
공적 가시성을 위한 거래내역 추적 기술	IPC 기술체계, 전문가추천
블록체인 거래검증 및 합의 기술	특허 클러스터링, 전문가 추천
블록체인 참여자 식별 및 접근통제 기술	특허 클러스터링, 전문가 추천
블록체인 기반 신원인증 서비스 기술	전문가추천
이중지불방지 기술	IPC 기술체계, 전문가추천
사용자 데이터 관리 기술	전문가추천
거래 데이터 판독 시스템	특허 클러스터링, 전문가 추천
부정거래 방지 기술	IPC 기술체계, 전문가추천
블록체인 간 자산연계 및 교환서비스 기술	IPC 기술체계, 전문가추천

6. 전략제품 기술로드맵

가. 핵심기술 선정 절차

- ☐ 특허 분석을 통한 요소기술과 기술수요와 각종 문헌을 기반으로 한 요소기술, 전문가 추천 요소기술을 종합하여 요소기술을 도출한 후, 핵심기술 선정위원회의 평가과정 및 검토/보완을 거쳐 핵심기술 확정
- ☐ 핵심기술 선정 지표: 기술개발 시급성, 기술개발 파급성, 기술의 중요성 및 중소기업 적합성
 - 장기로드맵 전략제품의 경우, 기술개발 파급성 지표를 중장기 기술개발 파급성으로 대체

[핵심기술 선정 프로세스]



나. 핵심기술 리스트

[블록체인 기반 공유 경제 서비스 분야 핵심기술]

핵심기술	개요
부정거래 방지 기술	· 부정거래 방지를 위한 스마트컨트랙트 기술을 통해 이용자 간 거래내용을 보호함과 동시에 공정거래 구현
공적 가시성을 위한 거래내역 추적 기술	· 블록체인 기반 공정거래의 실현을 위해 거래정보 안정성 보장 및 비대칭성을 해소한 거래내역 추적 기술
블록체인 기반 신원인증 서비스 기술	· 기존의 중앙화된 인증 방식에서 벗어나 탈중앙화 방식으로 신원을 증명하기 위한 전자신원증명 기술
블록체인 거래검증 및 합의 기술	· 블록체인에서 가장 보편적으로 사용중인 합의 알고리즘인 작업증명(Proof of Work, PoW)은 컴퓨팅 파워를 이용하여 합의를 도출하며, 지분증명(Proof of Stake, PoS)은 PoW의 컴퓨팅 파워 낭비 문제를 해결하고자 개발된 합의 알고리즘으로 노드가 보유한 자산을 기준으로 권한을 분배하여 합의를 도출하고 보상을 분배하는 알고리즘
분산 공유플랫폼	· C/S기반의 공유 플랫폼을 분산 원장 기반의 공유 플랫폼으로 전환하는 기술 또는 설계기술

다. 중소기업 기술개발 전략

- ☐ 공유경제 참여자를 위한 블록체인 공유 네트워크 확보를 위한 핵심기술 개발 필요
- ☐ 거래참여자 관리 및 합의, 참여자 평판시스템, 스마트계약 검증, 디지털 ID의 제공 및 확인, 토큰 시스템 및 페이먼트 기술의 안정적 임무수행 지원 및 신뢰성 확보 필요
- ☐ 산·학 연계 및 테스트베드 확보를 통한 개발기술 검증으로 국내시장 개척 및 선점 필요

라. 기술개발 로드맵

(1) 중기 기술개발 로드맵

[블록체인 기반 공유 경제 서비스 분야 중기 기술개발 로드맵]

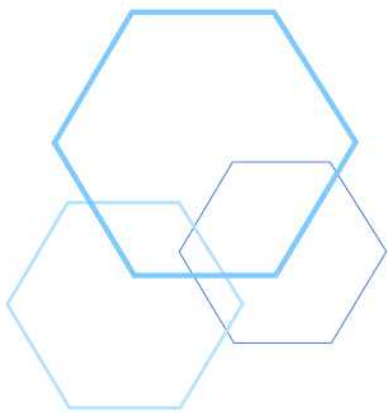
블록체인 기반 공유 경제 서비스	고도화된 스마트컨트랙트 기술 기반의 공정거래 구현			
	2021년	2022년	2023년	최종 목표
부정거래 방지 기술				부정거래 방지를 위한 스마트 컨트랙트 기술 구현 시 거래내용 보호
공적 가시성을 위한 거래내역 추적 기술				거래 정보 안정성 보장 및 비대칭성 해소
블록체인 기반 신원인증 서비스 기술				HSM(Hardware Security Module) 적용을 통한 공유 경제서비스 구현
블록체인 거래검증 및 합의 기술				랜덤 방식으로 노드 선출을 통한 예측에 의한 담합 방지, 다중 서명 기술 적용을 통한 메시지 복잡도 및 통신 비용 절감
분산 공유플랫폼				핵심기술요소 외 블록체인 기반 기술들의 통합을 통한 혁신 플랫폼 구축

(2) 기술개발 목표

- ☐ 최종 중소기업 기술로드맵은 기술/시장 니즈, 연차별 개발계획, 최종목표 등을 제시함으로써 중소기업의 기술개발 방향성을 제시

[블록체인 기반 공유 경제 서비스 분야 핵심요소기술 연구목표]

핵심기술	기술요구사항	연차별 개발목표			최종목표	연계R&D 유형
		1차년도	2차년도	3차년도		
부정거래 방지 기술	스마트컨트랙트에 대한 프라이버시 보호	50%	70%	95%	부정거래 방지를 위한 스마트컨트랙트 기술 구현 시 거래내용 보호	창업형
공적 가시성을 위한 거래내역 추적 기술	거래 투명성 제고 및 공급자 수요자 간 정보 비대칭 개선	55%	80%	95%	거래 정보 안정성 보장 및 비대칭성 해소	기술혁신
블록체인 기반 신원인증 서비스 기술	DID에서 발생 가능한 개인키 분실·도난 등에 대한 솔루션	30~50%	70%	80~90%	HSM(Hardware Security Module) 적용을 통한 공유 경제서비스 구현	산학연
블록체인 거래검증 및 합의 기술	PoN 알고리즘 적용	60%	80%	95%	랜덤 방식으로 노드 선출을 통한 예측에 의한 담합 방지, 다중서명 기술 적용을 통한 메시지 복잡도 및 통신 비용 절감	상용화
분산 공유플랫폼	블록체인 기술 통합 솔루션	70%	80%	95%	핵심기술요소 외 블록체인 기반 기술들의 통합을 통한 혁신 플랫폼 구축	창업형·산학연



전략제품 현황분석

블록체인 기반 디지털 컨텐츠 관리 플랫폼



블록체인 기반 디지털 콘텐츠 관리 플랫폼

정의 및 범위

- 음원, 영상, 게임 등 디지털 콘텐츠를 블록체인 네트워크에 저장함으로써 디지털 콘텐츠 및 그에 관한 권리들의 발생 시점을 투명하고 명확하게 관리하여 고수수료를 청구하는 별도의 중개기관 없이 디지털 콘텐츠에 대한 효율적인 관리를 달성하기 위한 플랫폼
- 블록체인 기반 디지털 콘텐츠의 관리 플랫폼은, 플랫폼을 구현하기 위한 기술로 재분류 가능

전략 제품 관련 동향

시장 현황 및 전망	제품 산업 특징
<ul style="list-style-type: none"> (세계) 콘텐츠 및 엔터테인먼트 블록체인 세계 시장은 '18년 8,500만 달러에서 연평균 69.6%의 성장률로 '24년에는 20억 달러 규모에 도달할 것으로 전망 (국내) 블록체인 기반 콘텐츠 및 엔터테인먼트 국내 시장규모는 '18년 28억 원에서 연평균 성장률 69.6% 성장하여 '24년 662억 원 규모에 이를 것으로 전망 	<ul style="list-style-type: none"> 블록체인을 이용한 플랫폼 사업 분야 중 가장 먼저 사업화가 진행되고 있는 분야 중 하나 이미 비즈니스 모델이 상당히 정착된 해외와 달리, 국내에서는 안정적으로 정착한 비즈니스 모델이 발견되지 않음 코로나-19로 인해 의료분야에서도 환자의 데이터 식별 및 의심 환자의 접촉자 추적 기능 탑재
정책 동향	기술 동향
<ul style="list-style-type: none"> 해외 정부들의 스마트시티화 하기 위한 디지털 행정 서비스 추진 및 해외 중앙은행들의 디지털 화폐 추진 블록체인 기술을 지식재산 및 산업재산권 분야에 적용하려는 논의가 활발하게 진행 중 	<ul style="list-style-type: none"> 해외 중앙은행들은 CBDC 모델 검증을 위해 IT시스템 개발에 분산원장 등 최신 IT 기술을 적용 불법 복제 추적 기술개발 및 이용 블록체인을 이용한 저작권 관리 기술 연구 활발
핵심 플레이어	핵심기술
<ul style="list-style-type: none"> (해외) Tencent, Tradedoubler, Ubrich, IBM, Kodak, JCB, 이취치예지환, 중국은행, Propy, Ubitquity, Ujo music, Steemit, Decent, Colu, Spotify, Feedbands, RecordGram, Decentraland, VibeHub, Matrixx (중소기업) 토큰포스트, 케이체인, 삼성 SDS, 보라, CJ올리브네트웍스, 왓차, 블로터앤미디어, 픽션네트워크, 피블, 기프트, 유니오, 예스24 	<ul style="list-style-type: none"> 블록체인 기반의 토큰 경제 시스템 스마트 컨트랙트 기술 저작권 도용방지 기술 및 해킹 방지 기술 블록체인 기반 지갑 관리 기술 공적 가시성을 위한 거래내역 추적 기술

중소기업 기술개발 전략

- 정부의 블록체인 기술 개발을 위한 R&D 지원 및 투자 정책을 활용
- 해외 스타트업들과의 협업을 통해 지속적이고 선제적인 기술 개발 수행
- 협업을 통해 블록체인 기반 기술의 약점에 대한 인식과 함께 이에 대응할 수 있는 저작권 관리 기술, 스마트 컨트랙트 기술, 지갑 관리 기술에 대한 기술 협력 강화

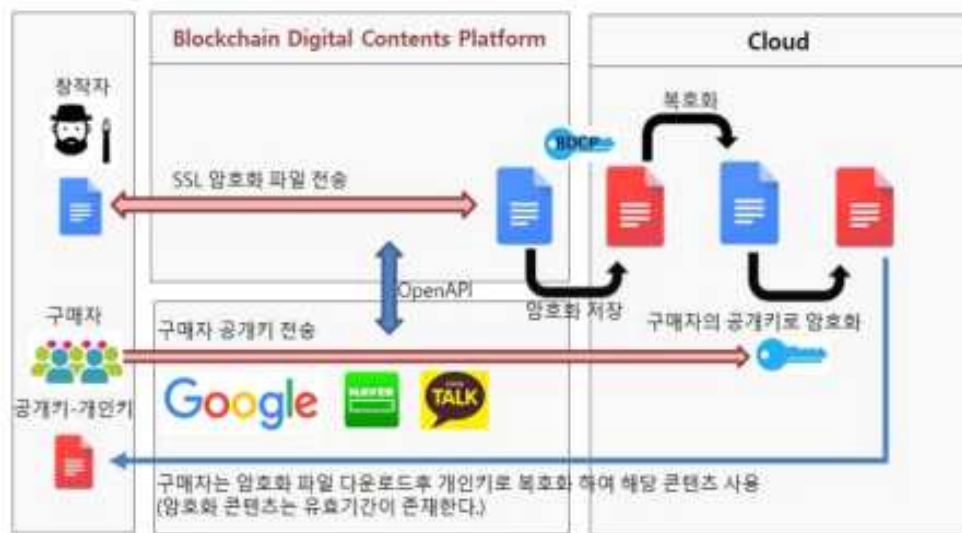
1. 개요

가. 정의 및 필요성

(1) 정의

- 음원, 영상, 게임 등 디지털 콘텐츠를 블록체인 네트워크에 저장함으로써 디지털 콘텐츠 및 그에 관한 권리들의 발생 시점을 투명하고 명확하게 관리하여 고수수료를 청구하는 별도의 중개기관 없이 디지털 콘텐츠에 대한 효율적인 관리를 달성하기 위한 플랫폼²⁸⁾
 - 기존 디지털 콘텐츠 및 저작권과 관련한 문제들인 불법복제 방지, 사용권과 소유권의 다양한 적용, 중간자의 역할 변화, 신인의 활동이나 작품 유통, 마이크로 페이먼트, 광고 생태계 변화 등에 활용할 수 있어, 콘텐츠 산업에 대한 적용 가능성이 무궁무진
 - 블록체인과 콘텐츠 산업과의 접목은 생산자와 소비자를 직접 연결한다는 점에서 다양한 역할을 할 수 있고, 중간 유통자의 수수료를 절감하여 공정하고 투명한 서비스 제공 가능

[블록체인 기반 디지털 콘텐츠 관리 플랫폼 개념도]



* 출처 : '블록체인을 이용한 디지털 콘텐츠 관리 플랫폼', 2018.05, 한국 저작권 위원회

28) 한국콘텐츠진흥원, "신뢰의 기술' 블록체인, 콘텐츠산업 지각변동 예고', 2017.12

(2) 필요성

- 복잡한 중간유통으로 인해 콘텐츠 크리에이터들의 권익이 제대로 보호받지 못하고 있으며, 전통적인 문화산업계에서 이러한 관행을 개선할 의지가 부족
 - 음반 산업의 경우, 유통회사나 제작회사가 시장을 거의 지배하고 있으며, 유통회사가 높은 수수료를 기반으로 많은 수익을 올리고 있으나 가수나 연주자 등 실연자와 저작권자는 제 값을 제대로 받지 못하는 실정
- 블록체인 기술은 콘텐츠 생태계 유통 구조를 개선하고 저작권 보호를 강화할 수 있는 새로운 기술
 - 블록체인 기술의 경우, 분산 원장 기술 및 스마트 컨트랙트 기술을 활용해 기존의 저작권 시스템을 대체하고, 개인 간 음반 거래를 실현함으로써 실연자와 저작권자에게 더 많은 수익을 배분 가능
 - 창작자가 저작물에 대한 데이터를 블록체인에 기록하면, 블록체인의 특성상 가장 먼저 기록된 저작물의 저작권을 인정할 수 있으므로, 저작권 인정과 관련한 법률적 이슈에 블록체인이 효과적으로 이용 가능
 - 스마트 컨트랙트를 이용해 저작물과 관련한 법률적 문제에 대응하기 위한 비용을 절감 가능

[블록체인을 적용한 음원 유통]



*출처: 블록체인을 적용한 음원 유통, 2018.02.13, 머니투데이

나. 범위 및 분류

(1) 가치사슬

- ☐ 저작물의 관리 및 유통 서비스를 처리할 수 있을 정도의 확장성을 갖춘 블록체인 프로토콜 기술의 개발은, 다양한 디지털 콘텐츠 영역에서 블록체인 기술이 이용될 예정. 이에 따라 디지털 콘텐츠 생산자와 소비자 간 불필요한 유통과정이 생략될 수 있어, 새로운 부가가치 창출이 가능
- ☐ 블록체인 기반 디지털 콘텐츠 관리 플랫폼이 다양한 영역에서 이용되면, 콘텐츠 생산자들의 창작에 대한 수익이 증대. 이에 따라, 문학, 음악, 영화 등 다양한 분야에서 콘텐츠 창작이 더욱 활발해질 것으로 기대되며, 이에 따라 새로운 부가가치 창출이 가능
- ☐ 또한, 기록의 위조 및 변조가 어려운 블록체인의 기술적 특징은 저작권 관련 분쟁을 줄여, 문화 산업 전반에서의 불필요한 사회적 비용이 감소 예상

[블록체인 기반의 디지털 콘텐츠 관리 플랫폼 분야 산업구조]

후방산업	블록체인 기반 디지털 콘텐츠 관리 플랫폼	전방산업
블록체인 프로토콜 기술	디지털 콘텐츠 관리 플랫폼 콘텐츠 유통을 위한 토큰 시스템 마이크로 페이먼트 기술 시장 등	문학, 음악, 영화 등 문화산업 엔터테인먼트 산업 게임 산업

(2) 용도별 분류

- ☐ 문학, 음악 및 영화 등 문화 산업 전반에 블록체인 기술이 적용되어 새로운 부가가치가 발생할 것으로 예상
 - 블록체인 기반 디지털 콘텐츠 관리 플랫폼은 콘텐츠 크리에이터와 콘텐츠 소비자가 블록체인 네트워크를 통해 직접적으로 디지털 콘텐츠의 창작 및 소비 활동을 할 수 있도록 하고, 동시에 디지털 콘텐츠의 보호 및 관리가 이루어지도록 하는 기술
- ☐ 기존의 문화 산업 분야뿐만 아니라, 게임 분야에 있어서 게임 관련 IP 관리에 블록체인 기술을 적용하여 새로운 부가가치가 발생할 것으로 예상

(3) 기술별 분류

- ☐ 블록체인 기반 디지털 콘텐츠 관리 플랫폼은 콘텐츠 크리에이터와 콘텐츠 소비자가 블록체인 네트워크를 통해 직접적으로 디지털 콘텐츠의 창작 및 소비 활동을 할 수 있도록 하고, 동시에 디지털 콘텐츠의 보호 및 관리가 이루어지도록 하는 기술
- 크리에이터에 대한 보상이 이루어질 수 있도록 하는 토큰 경제 시스템 및 스마트 컨트랙트 기술
 - 소비자가 디지털 콘텐츠를 원활히 이용할 수 있도록 돕는 마이크로 페이먼트, 블록체인 기반 지갑 기술
 - 디지털 콘텐츠의 관리를 위한 저작권 도용방지 및 해킹 방지 기술

[기술별 분류]

분류	상세 내용
블록체인 기반 토큰 경제 시스템	<ul style="list-style-type: none"> • 콘텐츠 생성자에게 투명하게 혜택이 돌아갈 수 있도록 하는 블록체인 기반의 토큰 경제를 구현
스마트 컨트랙트 기술	<ul style="list-style-type: none"> • 효과적으로 작성된 스마트 컨트랙트를 통해서 콘텐츠의 생산자와 소비자가 합리적인 비용을 지불하고 콘텐츠를 이용하도록 구현
저작권 도용방지 및 해킹 방지 기술	<ul style="list-style-type: none"> • 블록체인상의 블록에 저작권정보를 기록하게 함으로써 최초 저작자의 권리를 보장하고, 변조불가능한 블록체인의 특성을 이용한 해킹방지 가능
블록체인 기반의 지갑 관리 기술	<ul style="list-style-type: none"> • 콘텐츠의 생산자와 소비자는 각자의 고유한 개인키/공개키를 사용하여 투명하고 효과적인 콘텐츠 소모 가능

2. 산업 및 시장 분석

가. 산업 분석

◎ 블록체인 기반 디지털 콘텐츠 저작권 및 유통 분야 현황

- ☐ 지식재산 분야에서도 콘텐츠 저작권 분야를 중심으로 저작물 이용에 따른 이익배분의 문제 등을 해결하기 위하여 블록체인 기반 거래 플랫폼이 등장
 - 블록체인은 디지털 재화의 거래에 적합하고, 인공지능 및 가상화폐와 결합하기 용이하나, 탈중앙화 및 합의에 의한 의사결정구조가 현행 저작권 제도와 상충될 여지 존재
 - 저작권의 양도 및 이용허락, 고아저작물의 이용, 법정 허락의 영역에서는 스마트 컨트랙트 등의 이용이 가능
 - 블록체인 기술을 저작권 제도에 이용하기 위해서는 블록체인 구축의 주체, 확장성, 과금, 가상화폐에 대한 국가정책 등 선행적으로 해결하여야 할 문제들이 존재
 - 블록체인 생태계에서는 관리적 이슈, 법·제도적 이슈, 기술적 이슈 관점에서 해결해야 할 과제들이 존재하고 있는 상황
 - 저작권 보호, 거래 및 결제, 계약, 정보기록 등에 블록체인 기술이 활용되기 위해서는 관련 법 개정 및 제정 등 대응방안 마련이 필요
- ☐ 미디어 콘텐츠 저작권 보호 및 유통 분야
 - 콘텐츠 저작권 보호와 유통에서도 블록체인 활용이 시도 중. 콘텐츠의 최초 등록 시에 고유한 식별자를 블록 인에 등록하고 사용 시 검증하는 방법으로 복제된 콘텐츠 불법 유통을 예방
 - 거대 콘텐츠 유통 업자에 맞서 Spankchain, StreamSpace 블록체인 기반의 콘텐츠 유통을 시도 중. 기존 음악 스트리밍 업체인 스포티파이(Spotify)는 음원 수익 분배, 저작권 보호 등을 위해 미디어체인랩스 등의 블록체인 업체를 인수하여 음악 블록체인 시장을 선점하려는 시도 중
 - 블록체인 기술은 미디어 및 엔터테인먼트 기업이 보다 효율적이고 투명하게 운영되도록 함으로써 비용 절감, 불법 복제 감소 및 소비자 충성도 증가로 인해 미디어 엔터테인먼트 업계의 많은 과제를 해결할 수 있을 것으로 기대
 - 주된 관련 관심 분야는 콘텐츠 지불 문제, 소비자 건전한 콘텐츠 소비 형태 분석, 공연 발권 시스템과 파생 수익의 공정 배분, 디지털 미디어 출처 인증(선거감시, 사기 감시, 공급망 감시, 반부패 방법 시행), 가짜 뉴스 검증, AI를 이용한 가짜 비디오 진위 추적, 텔레비전 및 미디어 산업 전체 광고를 배포/콘텐츠 제작/검증/수익배분/개인정보 보호/중개인 영향 최소화를 위한 방안으로 블록체인에 대한 관심이 커지는 중
 - 콘텐츠 제작자와 구매자 간 거래 효율성을 높인 ‘올라이트즈(AllRites)’, 사진작가 정보와 구매한 고객의 정보를 블록체인으로 저장한 ‘코닥 원(Kodak One)’, 봇 같은 자동화된 광고 시스템을 차단하고 검증된 소비자에게만 광고를 내보내는 ‘테리노(Terino)’ 등이 대표적
 - 국내에서는 왓챠(Watcha)의 콘텐츠 프로토콜 프로젝트, IT 미디어의 블로터의 레벨(LEVEL) 프로젝트가 존재

□ 디지털 콘텐츠 유통 및 관리 서비스 제공 스타트업 등장

- 블록체인 기반의 콘텐츠 유통시스템인 디센트(Decent), 블록체인 기반의 저작권 관리 API 제공회사 콜루(Colu), 픽션 네트워크, 피블, 기프트 등이 디지털 콘텐츠 유통 및 관리 서비스를 제공
- 바이두의 외부 투자 유치를 통해 금융사업부로 분사한 별도의 자회사인 '두샤오만(度小满金融)'은 디파이 산업 발전에 필요한 기술 표준화 솔루션 '도타(DOTA, DeFi-Oriented Technical Architecture)'를 기반으로 구축한 디파이 시스템이 고객 관리와 디지털 자산관리, 디지털 지급 및 지불, 사물인터넷(IoT) 정산 네트워크 등에 널리 쓰일 수 있다고 전망

◎ 블록체인 기반으로 확산 중인 콘텐츠 서비스 분야

□ 기존 서비스를 해치지 않으면서 새로운 수익 구조를 만들어내는 콘텐츠 서비스 등장

- 스팀잇(Steemit), 우조 뮤직(Ujo music) 등이 블록체인을 이용해 새로운 수익 구조를 발생시키는 콘텐츠 서비스

□ 게임 분야

- 게임 산업에 블록체인 기술이 접목될 경우, 기존의 사업 모델과 겹치지 않으면서 새로운 시장을 개척하기 용이하고, 게임 분야는 블록체인 기술을 가상으로 시뮬레이션하기에 좋은 환경이기 때문에 블록체인 기술은 게임 산업에서 특히 많은 시도가 있을 것으로 전망
- 아이템 거래와 같은 플레이어 간 상호작용에 블록체인이 도입되면 중간자의 도움 없이도 오프라인 사기를 피하면서 안전하고 투명한 직접 거래가 가능
- 또한, 암호화폐를 이용해 게임 내 구매가 빨라지고 간편해져 플레이어들의 지출이 자연스럽게 늘어나면 개발사의 수익 증가 예상
- 'CryptoKitties' 사례에서, 게임 속 모든 비용에 활동에 대해 플레이어에게 비용이 발생될 경우 플레이어에게 부담으로 돌아올 수 있기 때문에, 필수적인 활동에 대해서 블록체인을 선택적으로 활용할 필요가 존재
- 중국의 바이두는 본격적으로 독자 블록체인 상용화의 첫 걸음으로 비교적 빠른 출시가 가능한 게임 영역에서 자체 개발한 BaaS를 활용한 블록체인 기반 게임 '라이치고(莱茨够)'를 내놓음

□ 광고 콘텐츠 분야

- 실제 사람처럼 광고에 관여해 광고 트래픽을 측정할 때 광고주들에게 잘못된 결과를 제공하는 부정 광고의 대응이 가능
- 또한, 광고주들은 블록체인 기술을 활용해 최종 사용자가 승인하지 않으면 특정 데이터 수집을 완벽하게 거부하는 등 사용자 정보를 더욱 효과적으로 보호할 수 있어 승인되지 않은 거래가 진행되는 것을 방지하는 등 안정성 상승
- 블록체인을 통한 광고는 기존 디지털 광고의 트래커, 매체, 퍼블리셔 등 과한 관여를 줄임으로써 글로벌 플랫폼에서 개별 광고의 개발 및 배포에 참여하는 제3자의 수로 인해 증가하는 비용을 없애는 등 광고 구매 및 판매를 간소화

□ 저널리즘/블로그/뉴스 분야

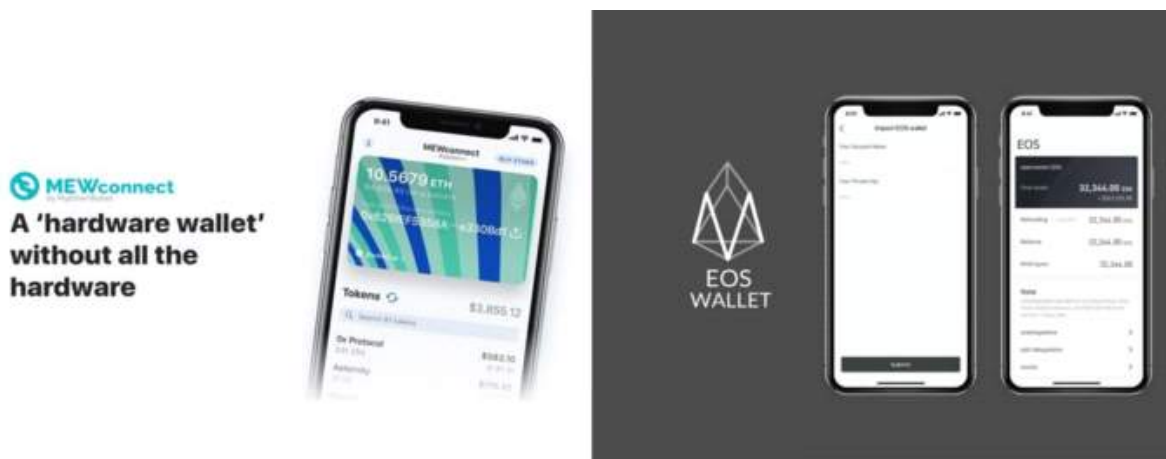
- Civil, Steemit 등의 플레이어가 해당 분야에서 블록체인 기술을 접목 중
- SNS를 통해 가짜 뉴스가 빠르게 전파되어 사람, 조직 간 불필요한 갈등이 조장되고, 사회 문제가 야기. 블록체인 기술을 이러한 분야에 적용하면 디지털 정보의 진위를 추적/검증할 수 있어, 문제 해결에 도움

◎ 블록체인 기반 결제 플랫폼

□ 마이크로 페이먼트 플랫폼의 확산

- 기존의 결제시스템은 카드, 현금, 상품권 등을 활용하여 비용을 지불을 해왔으나 가상화폐의 부상으로 가상화폐를 통한 결제가 증가. 특히 소액 결제 시스템과 블록체인의 접목으로 마이크로 페이먼트가 보다 안전하게 이루어지는 중. 이에 마이크로 페이먼트 플랫폼을 활용한 방식이 다변화 되면서 이를 활용할 수 있는 블록체인 시장이 확대
- 영국의 과학/기술 뉴스사이트 The Register는 블록체인 기술을 기반의 SatoshiPay를 활용한 마이크로 페이먼트로 Geek's Guide to Britain eBook을 판매
- Blendle은 네덜란드의 신문 기사와 주요 잡지를 제공하는 온라인 뉴스 플랫폼- 소비자들이 읽은 기사만큼 비용을 지불하는 방식으로 기사를 읽은 후 가치가 없다고 판단되면 환불할 수 있도록 지원

[이더리움 전용 월렛(MEW), 이오스 전용 월렛(Meet.one)]



* 출처 : 이더리움 전용 월렛(MEW), 이오스 전용 월렛(Meet.one), Medium

□ 다양한 가상화폐 지갑플랫폼의 도입확산

- 가상화폐는 거래소 지갑을 통해 코인, 토큰을 보관하여 관리되어 왔으나 잇따른 거래소 해킹으로 보안의 중요성이 확산되면서 가상화폐 지갑 플랫폼들이 다양하게 출시
- BitGo는 금융 개인 정보 보호를 위한 다중 서명보안을 활용하여 90개 이상의 동전과 토큰으로 저장 및 거래할 수 있는 플랫폼. 이중 인증, 매번 새로운 비트코인 주소를 활용하여 다른 사람이 잔고와 지불을 감시하기 어렵게 함
- Xapo는 블록체인 기반의 온라인 지갑으로 전자화폐 관리와 보안금고에 저장, 거래할 수 있는 금융서비스. 보안 시설이 스위스 알프스, 전 군용 벙커 등에 위치하여 물리적 절도에 대한 보안성과 더불어 한 장소의 보안에 문제가 생겨도 해결할 수 있도록 5대륙에 중복 글로벌 비트코인 스토리지 네트워크를 지님
- BitPay는 블록체인 기술을 활용한 비트코인 금융거래 및 가상화폐 지갑 플랫폼. 최대 12개의 기기에서 결제를 수락하도록 하여 결제를 보안하며 'Full Payment Protocol'을 활용해 지불 내역을 확인, 보안을 유지
- ABRA는 암호거래를 통한 비트코인 금융거래 서비스로 28개의 가상화폐를 안전하게 구입, 저장 및 투자 할 수 있는 플랫폼. P2P방식을 활용하여 중간의 유통, 관계자 없이 거래를 진행하며 '개인 키(본인을 나타내는 특수한 코드)'를 활용하여 보안
- API 제공회사 콜루(Colu)는 최근 클라우드 기반 음악서비스 회사인 레빌레이터(Revelator)와 협력해 블록체인 공공원장에 작품을 등록하고 비트코인 네트워크를 통해 교환할 수 있게 함
- 삼성SDS는 미국 라스베이거스에서 열린 CES2020에서 미국통신 서비스 기업 시니버스와 모바일 결제 플랫폼 관련 업무협약 맺음

◎ 의료산업에 적용되는 블록체인 기술

□ 환자 데이터 관리를 위한 솔루션 개발

- 아랍에미레이트(UAE) 기업 'in5'는 보도자료를 통해 환자식별 플랫폼 '리베르헬스(Liber Health)' 개발에 블록체인 기술을 도입한다고 밝힘
- in5는 비접촉식으로 생체 데이터를 인식해 코로나-19 의심 증상을 분석하며 블록체인 기술로 환자의 데이터를 식별 및 의심환자의 접촉자를 추적하는 기능 탑재하여 정부기관과의 협의를 통해 공공 의료 영역에 리베르헬스 도입하고자 함

□ 코로나-19 관련 데이터 교차 검증에 블록체인 기술 도입 확산

- 세계보건기구(WHO)는 최근 블록체인 플랫폼 개발 기업 하세라와 함께 블록체인 데이터 플랫폼 '미파사' 구축 착수
- 미국 질병통제센터, 존스홉킨스 대학병원, 캐나다보건국 등의 코로나-19 관련 데이터를 교차 검증 후 블록체인에 기록해 향후 각국 정부와 기업, 의료기관들이 코로나-19 연구에 활용할 수 있게하고 향후 의료정보들의 활발한 공유로 의료기술의 발전 전망

나. 시장 분석

(1) 세계시장

- Marketsandmarkets의 보고에 의하면 블록체인 관련 콘텐츠 및 엔터테인먼트 세계 시장은 2018년 8,500만 달러에서 연평균 69.6%의 성장률로 2024년에는 20억 달러 규모에 도달할 것으로 전망
- 디지털콘텐츠솔루션 시장은 저작물, 콘텐츠 보호, 모바일 솔루션, 과금/결제, CMS, CDN, 퍼블릭 클라우드 스토리지 시장 등으로 구분될 수 있음. 이중 콘텐츠 보호(DRM), 과금/결제, CMS 시장에 대해 블록체인 서비스가 우선적으로 적용될 수 있을 것으로 판단

[블록체인 기반 콘텐츠 및 엔터테인먼트 세계 시장규모 및 전망]

(단위 : 백만 달러, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
세계	85	161	237	465	692	1,359	2,025	69

* 출처 : Global Blockchain Technology Market 2016-2021, MarketsandMarkets(2016)과 Blockchain Market by Component, MarketsandMarkets(2020)을 근거로 네모아이씨지 재가공

(2) 국내시장

- 블록체인 기반 콘텐츠 및 엔터테인먼트 국내 시장규모는 2018년 28억 원에서 연평균 성장률 69.6% 성장하여 2024년 662억 원 규모에 이를 것으로 전망

[블록체인 기반 콘텐츠 및 엔터테인먼트 국내 시장규모 및 전망]

(단위 : 억 원, %)

구분	'18	'19	'20	'21	'22	'23	'24	CAGR
국내	28	53	77	152	226	444	662	69.6

* 출처: Blockchain Market by Component, MarketsandMarkets(2020)의 데이터를 기준으로 비트코인 화폐별 거래량 중 원화 점유율 2.97%²⁹⁾(코인힐스 2020.12.30.)을 근거로 네모아이씨지 재가공(환율:1100원/달러)

29) 미국달러:72.7%, 일본엔화:18.66%, 유로화:3.06%, 한국원화:2.97%

3. 기술 개발 동향

☐ 기술경쟁력

- 블록체인 기반 디지털 관리 플랫폼은 미국이 최고기술국으로 평가되었으며, 우리나라는 최고기술국 대비 89.1%의 기술수준을 보유하고 있으며, 최고기술국과의 기술격차는 0.9년으로 분석
- 중소기업의 기술경쟁력은 최고기술국 대비 81.4%, 기술격차는 1.3년으로 평가
- EU(90%)>EU(77.8%)>중국(77.1%)>일본(74.7%)의 순으로 평가

☐ 기술수명주기(TCT)³⁰⁾

- 블록체인 기반 디지털 콘텐츠 관리 플랫폼은 4.06의 기술수명주기를 지닌 것으로 파악

가. 기술개발 이슈

◎ 해외 중앙은행 디지털화폐(CBDC) 추진 현황

- ☐ 한국은행은 CBDC 파일럿 테스트를 위한 기술검토 참고를 위해 연구보고서가 공개된 14개 해외 중앙은행의 12개 사례 조사
- ☐ 해외 중앙은행들은 CBDC 모델 검증을 위해 IT시스템 개발에 분산원장 등 최신 IT 기술을 적용

[해외 디지털화폐(CBDC) 추진 현황]

국가	이용목적	운영방식	원장관리	개발단계	발행목적
스위스	거액	N/A	N/A	개념검증 준비중	발행 필요성 검토
프랑스		직접	분산	개념검증	유로화 위상 제고
싱가폴					최신 기술(분산원장) 적용 검토
일본-ECB					
캐나다					국가간 외환거래
태국-홍콩					
영국	소액	간접	분산	모델수립	복원력, 금융포용, 혁신성, 경쟁력 제고
노르웨이				요구사항 분석	현금사용량 감소 대비, 공공 소액결제수단 확보
동카리브				개념검증	금융포용
스웨덴				시범운영 준비중	현금사용량 감소 대비, 공공 소액결제수단 확보
중국				시범운영	자금세탁방지, 위안화 위상 제고
바하마					금융포용, 자금세탁방지

*출처: 해외 디지털화폐 추진 현황, 2020.5, 한국은행

30) 기술수명주기(TCT, Technical Cycle Time): 특허 출원연도와 인용한 특허들의 출원연도 차이의 중앙값을 통해 기술 변화속도 및 기술의 경제적 수명을 예측

◎ 블록체인 기반 콘텐츠 보호 기술

□ 블록체인을 이용한 콘텐츠 불법 복제에 대한 추적 기술

- 기존 콘텐츠 서비스 플랫폼상에서는 불법 복제 및 공유를 막기 어려웠으나, 블록체인 기술을 활용하면 불법 복제에 대한 추적이 가능
- 필름업체 Kodak이 발표한 블록체인 플랫폼 ‘코닥 원(Kodak One)’은 사진의 작가 정보 및 구매 고객의 정보를 블록체인에 저장해 유통하여 불법 복제 및 유통 가능성을 낮춤. 웹 크롤링(web crawling) 기술을 결합해 저작권 침해 방지 및 이미지 추적
- 일본의 Asobi market은 블록체인으로 콘텐츠 거래 기록이 모두 남는다는 점에 주목하여 해당 거래 정보를 바탕으로 2차(중고) 유통을 제공할 수 있는 플랫폼 ‘Asobi store’를 선보임. 블록체인을 활용해 디지털 콘텐츠 소유권을 명확히 하여, 디지털 콘텐츠 2차 유통 플랫폼 형성이 가능

□ 블록체인을 통한 저작권 관리 기술

- Microsoft, Intel, SONY 등 글로벌 IT 기업들이 블록체인을 활용한 저작권 보호 서비스를 공개하거나 관련 특허권을 신청하면서 기술 활용에 나서는 중
- Microsoft는 비디오 게임 저작권 및 로열티 관리용 블록체인 플랫폼을 출시
- SONY는 디지털 저작권 관리에 블록체인 도입, 콘텐츠가 제작된 날짜와 시간, 제작자에 대한 구체적인 정보까지 공유 및 확인이 가능해 효율적인 디지털 저작권 관리가 가능
- Intel은 소프트웨어를 이용해 각 이미지에 대한 저작권 정책을 자동으로 설정하는 방식으로 디지털콘텐츠 저작권 관리 플랫폼을 개발
- 일본 IT 업체 Any-Q는 블록체인 기술인 NFT(Non-Fungible Token)으로 거래 기록을 저장해 삽화 구매자에게 공식적인 소유권을 보장하고, 매매 및 양도 권한도 인정. 거래 활동 역시 역대 소유자의 내역이 남겨짐
- 블록체인에 업로드할 수 있는 데이터의 크기가 제한적이어서 음원이나 동영상 서비스 제공 시 발생하는 문제점의 해결이 요구
- 블록체인 상에 업로드된 디지털 콘텐츠에 대한 추후 수정 또는 삭제가 쉽지 않다는 문제점에 대한 해결이 요구
- 창작자보다 유통사가 더 많은 수익을 가져가는 구조에 따른 다양한 콘텐츠 개발의 한계를 극복하려는 블록체인 기반 생태계 프로젝트 ‘아라비안나이트’가 가시적인 성과를 보임
- 저작물 이용자들로부터 수령하는 로열티를 각 조건에 따라 정산, 배분해야 하는데, 이 중간 업무를 대행하는 에이전트들이나 플랫폼 업자들이 대가로 가져가는 상당한 수수료를 블록체인의 스마트컨트랙트 및 리카르디안컨트랙트를 활용하여 저작재산권 로열티 관리를 자동화 및 상당 금액의 로열티를 창작자, 투자자, 이용자에게 혜택이 가도록 배분, 조정할 수 있을 것으로 전망

◎ 블록체인의 확장성

☐ 저작물 파일의 유통에 따른 트랜잭션 처리에 관한 확장성 문제

- 블록체인 기술은 확장성 문제에 대한 해결이 완벽히 이루어지고 있지 않은 상태
- 따라서 블록체인을 접목한 디지털 콘텐츠 유통이 이루어질 경우, 사용자의 요청에 대한 서비스의 제공이 즉각적으로 이루어지지 못하는 중
- 이를 위해, IPFS, 클라우드 컴퓨팅 시스템, 오프체인, 사이드 체인 등의 기술이 제안되는 중

☐ 게임 분야에서의 확장성 문제

- 이더리움의 경우, 크립토 키티에서 발생하는 트랜잭션으로 인해 이더리움 트랜잭션 속도가 15% 가량 느려진 사례가 존재
- CryptoKitties와 같은 킬러 dApp이 많아질수록 이러한 확장성 문제는 커질 수밖에 없음. 따라서 이에 대한 해결책이 시급한 상황
- 확장성 문제로 인해 게임 활동에 요구되는 트랜잭션 비용도 따라서 증가. 따라서 수수료 문제로부터 자유로운 블록체인 게임 개발에 대한 요구도 존재
- 퍼블릭 블록체인을 직접 사용하기보다는 퍼블릭 블록체인에 연결된 하위 체인을 사용하는 방식이 대안으로 떠오르고 있음. 프라이빗 블록체인 성질을 지닌 하위 체인으로 개별 사용자 특성에 맞춘 네트워크를 구축하고, 해당 네트워크에 대한 공증을 퍼블릭 블록체인이 제공하는 방식이 그 일례. 아이콘(ICON), 에이치닥(Hdac) 등이 대표적

☐ 블록체인 기반 디지털 콘텐츠 유통을 위한 마이크로 페이먼트 기술 및 지갑 기술 발전

- 기존의 결제 시스템과는 상이한 암호화폐 기반 결제 시스템의 특성상, 다중 인증, PKI 시스템 등을 이용한 마이크로 페이먼트 및 지갑 기술의 발전이 요구

☐ 이더리움 및 하이퍼레저(Hyperledger) 플랫폼의 미디어 산업 적용 가능성 현황

- 하이버레저 패브릭과 이더리움은 모두 미디어 산업에서 요구하는 수준에 미치지 못하는 중
- 구체적으로, 하이퍼레저의 경우 성능 요건은 충족시키지만 합의 안정성과 토큰 이코노미를 실현할 수 있는 인프라를 제공하지 못하는 약점이 존재
- 이더리움의 경우 토큰은 제공하지만 성능이 기대를 충족시키지 못하고 있으며, 더욱이 dApp (distributed Application) 실행 시에 발생하는 추가적인 가스(gas) 비용은 비즈니스 설계를 매우 어렵게 함
- 미디어 산업 특성에 맞는 특화된 블록체인 엔진에 대한 연구개발이 필요한 시점

나. 생태계 기술 동향

(1) 해외 플레이어 동향

- ☐ (Tencent) 텐센트의 자체 블록체인 플랫폼은 트러스트SQL을 기반으로 제작된 블록체인 게임 “렛츠헌트몬스터(Let's Hunt Monster)”가 2019년 4월 중국 아이폰(iOS) 앱스토어에 무료게임 분야 다운로드 순위 1위를 기록
- ☐ (Tradedoubler) 스웨덴 디지털 광고업체 블록체인 기반 광고 네트워크 출시
 - 탈중앙형 데이터 스토리지의 기능을 갖춰 광고주와 퍼블리셔 사이의 투명한 소통 및 거래 가능한 블록체인 기반 디지털 광고 네트워크 출시
 - 투명하고 효율적인 디지털 광고를 위한 네트워크로, 퍼블리셔들에게 고객들의 의견 반영을 제공함과 동시에 딥 링크 생성기, 고객 지원 센터 및 최적화된 리포트 생성기 기능을 제공하여 광고 관련 기업들에게 빠른 결정과 실행을 통해 광고비 감소에 큰 도움 전망
- ☐ (Ubirch) 환자 데이터 관리에 블록체인 기술 도입
 - 독일 블록체인 스타트업 Ubirch가 바이오 기업 센토진(Centogene)과 함께 블록체인 기술을 기반으로 코로나-19 테스트 결과를 위변조 없이 안전하게 공유하며 유럽연합의 데이터보호법(GDPR)을 준수하는 솔루션 개발
- ☐ (IBM) 블록체인 네트워크 ‘Rapid supplier connect(신속한 공급 연결)’
 - 코로나-19 사태 가운데 의료장비가 필요한 곳에 공급업체를 연결
 - 미국 연방정부와 지방정부, 조달부서, 의료기관, 약국 등 연결하고 협력업체에 무상으로 제공
- ☐ (Kodak) 블록체인 기반 저작권 보호 플랫폼 코닥원(KodakONE)을 활용, 플랫폼 내에서 거래 시 코닥코인으로 체결
- ☐ (JCB) 블록체인 기반 결제시스템 구축
 - 일본 최대 카드업체 JCB는 기술 분야 엑셀러레이터 테크펀드(Techfund)와 파트너십을 맺고 STO(증권형토큰공개), 스테이킹 등 테크펀드가 보유한 블록체인 관련 기술을 활용해 결제 시스템을 구축할 전망
- ☐ (이취치예지탄) 중국의 부동산 기업 이취치예지탄은 2019년 1월 부동산거래, 정보서비스, 자산운용 등 네가지 기능을 갖춘 ‘중국자산정보컨설팅서비스(CIAC)’ 플랫폼 운영을 시작
- ☐ (중국은행) 2019년 4월 홍콩 ASRTI와 NWD가 공동 개발 중인 부동산 서류 공유 블록체인 플랫폼의 PropTech 활용, 거래서비스 개시
- ☐ (Propy) Propy는 이더리움을 기반으로 부동산 거래를 획기적으로 줄이고 안전한 거래가 가능
- ☐ (Ubitquity) Ubitquity는 블록체인 기반의 부동산 계약 보관 플랫폼으로 부동산 거래의 고질적인 문제를 해결할 것으로 기대

- ☐ (Ujo music) Ujo music은 사용자들이 암호화폐인 이더리움을 이용해 음원을 구입할 수 있는 곳임. 사용자가 음원을 구입하면 그 금액은 곧바로 프로듀서와 작사가, 엔지니어 등 곡 생산에 참여한 전문가들에게 배분 가능
- ☐ (Steemit) Steemit은 대표적인 블록체인 콘텐츠 서비스로, Steemit은 소셜 네트워크 사이트로서 콘텐츠에 대한 보상을 지급하는 플랫폼
 - 콘텐츠 생산자가 광고 없이 콘텐츠 그 자체로 수익을 얻는 것이 가능. 생산자의 게시물이 다른 사용자로부터 받은 투표 수에 따라, Steemit에서 사용되는 암호화폐를 보상으로 받을 수 있음
 - Steemit이 제공하는 블로그에 글과 사진 등을 포스팅하고, 게시 7일 동안 이웃이나 방문자들이 Facebook의 '좋아요'처럼 'Upvote'를 누르면, 저자와 투표 참가자는 75%대 25%로 암호화폐를 보상으로 받을 수 있음. Steemit에는 '스팀'과 '스팀파워'와 '스팀달러' 3가지 암호화폐가 유통
- ☐ (Decent) 블록체인 기반의 콘텐츠 유통시스템인 Decent는 Amazon이나 Apple보다 더 나은 콘텐츠 유통환경을 제공하는 것을 목표로, 콘텐츠 생산자에게 소유권은 물론 콘텐츠 유통에 대한 권한을 제공
- ☐ (Colu) 블록체인 기반의 저작권관리 API(Application Program Interface) 제공회사 Colu는 클라우드 기반 음악서비스 회사인 Revelator와 협력해 블록체인 공공원장에 작품을 등록하고 비트코인 네트워크를 통해 교환이 가능
- ☐ (Spotify) 음악 스트리밍 업체 Spotify는 블록체인 기업인 Mediachain Labs을 인수
 - Mediachain Labs은 블록체인 기술을 활용해 음악의 창작물에 대한 정보를 공유하고 콘텐츠 제작자와 저작권자 모두 적절한 보상이 이루어지는 시스템을 개발 중
 - Spotify는 서비스되는 음악의 작곡, 작사 소유권에 대한 충분한 정보를 확보하지 못해 로열티 문제로 어려움을 겪었음. 이로 인해 미국의 음악출판사 협회(NMPA)와 법적분쟁에 휘말려 약 3천만 달러의 합의금을 지불한 사례가 있으며, Mediachain Labs의 인수를 통해 작사, 작곡가에 대한 로열티 지급과 보상체계 시스템 문제를 해결하고자 노력 중
- ☐ (Feedbands) 뮤직 큐레이팅과 크라우드 펀딩 서비스를 결합한 형태의 음악 서비스 사이트 Feedbands
 - Feedbands 서비스는 아티스트가 플랫폼에 음악을 무료로 업로드하고 사용자는 자유롭게 음악을 선택해서 업로드한 음악을 듣고 투표를 할 수 있도록 함. 투표를 통해 가장 많은 호응을 얻은 뮤지션은 음반제작에 선정되며 선정된 뮤지션에 대한 펀딩을 받아 음반은 제작됨. 또한, 아티스트의 굿즈(goods)에 대한 판매도 가능
 - Feedbands 서비스는 암호화폐 대시(Dash)를 사용하여 운영되고, 이를 통해 아티스트에게 판매 수익의 대부분을 제공. 이를 통해 기존 음악 콘텐츠 유통구조를 혁신
- ☐ (RecordGram) 블록체인을 활용한 모바일 레코딩 스튜디오, RecordGram
 - RecordGram은 암호화폐의 하나인 튠 토큰(Tune Token)을 통해 화폐를 하나로 통합해 글로벌 음악소비를 좀 더 원활하게 만들고 레코딩 시스템을 모바일에서 구현해, 작곡가들이 올려놓은 곡에 자유롭게 가사를 붙이거나 편곡, 연주 레코딩이 가능

□ (Decentraland) 이더리움 기반 가상현실 플랫폼 서비스 Decentraland

- 가상현실 세계를 블록체인 기술 기반으로 구현하고 있으며, 가상세계에서의 부동산 거래를 다룸

□ (VibeHub) VR 이벤트 경험의 거래가 가능한 VibeHub

- VIBE 토큰을 이용하여 디지털 자산의 구매, 투표 등이 가능. 이더리움 네트워크 상에서 동작하며, 콘텐츠는 볼륨메트릭(Volumetric) 비디오를 사용한 라이브 공연을 캡처하여 제작된 결과를 스트리밍을 통해서 받고, 이런 홀로그램 콘텐츠를 통한 VR 경험을 제공

□ (Matryx) VR 및 블록체인 기반 협업을 통한 과학의 최대 과제를 해결하는 플랫폼 Matryx

- 블록체인 VR제품을 협업방식으로 사용하고 과학, 기술, 공학 및 수학분야의 혁신을 장려하기 위해 활용. 과학자들은 VR시스템을 사용하여 나노 스케일 정밀도로 가상 설계하고 그 안에서 실험을 시뮬레이션

□ (Civil) 블록체인 기술 기반 뉴스플랫폼 Civil

- 기자와 독자가 직접 뉴스를 거래할 수 있게 한 오픈마켓
- 광고주의 입김, 정치적 외압, 온갖 검열, 주요 기사를 선정해 메인 페이지에 배치하는 포털 영향으로부터 자유로운 뉴스 룸이 되도록 기자와 독자 간 P2P거래가 이뤄짐. 시빌 뉴스룸 동작 방식은 탈중앙화 자치조직(DAO, Decentralized, Autonomous, Organization)으로 운영. 이 뉴스 룸은 저널리즘 자문위원회, 관리자, 뉴스제작자, 시티즌, 팩트 체커 로 구성

[블록체인 기반 뉴스 플랫폼 'Civil' 개념도]



*출처: 블록체인 기반 미디어 산업 적용 사례 동향, 2018.07, 한국방송미디어공학회

(2) 국내 플레이어 동향

- (토큰포스트, 케이체인) 블록체인과 토큰 경제의 장점을 언론 산업에 도입하기 위한 프로젝트 퍼블리시(PUBLISH) 출시
 - 해당 플랫폼은 모든 참여자에게 공정하게 보상하며, 언론사가 실제 도입·구축해 경제적으로 유효한 모델을 가질 수 있도록 지원
 - 광고 수익에 상당히 의존하고 있는 시대 속 언론의 입지가 약화되고 있고 이외에도 독자층 분열, 미검증·허위 뉴스 확산, 언론 규제 완화 및 언론사 통합을 통한 경쟁 심화 등 업계가 당면한 문제 전망

[프로젝트 퍼블리시(PUBLISH) 개념도]



*출처: 프로젝트 퍼블리시 개념도, Tokenpost

- (삼성 SDS) 기업용 블록체인 플랫폼 넥스렛저 유니버설과 시니버스의 블록체인 솔루션 유니버설 커머스를 활용해 플랫폼 개발
 - 간편 모바일 결제 목표, 모바일 지갑들을 연결하는 플랫폼 개발 전망
 - ‘당신의 전화번호가 가장 쉬운 결제방법’을 모토로 모든 모바일 이용자가 돈, 로열티, 포인트 또는 여러 디지털 화폐를 보낼 수 있는 공동 플랫폼 역할을 하며 물류, 금융, 여행, 미디어 등 다양한 업종에 접목할 플랫폼 구상
- (보라) 암호화폐 지갑 편의성 향상
 - 블록체인 디지털 콘텐츠 플랫폼 보라(BORA)가 국내외 유저 누구나 손쉽게 블록체인 게임을 이용할 수 있는 환경을 구축하며 암호화폐 지갑 기능을 개선하여 보라 블록체인 기반 게임 유저들이 ‘보라 토큰’(BORA)과 보라 플랫폼 전용 화폐인 ‘셸 토큰’(SHELL)을 자유롭게 사용할 수 있는 서비스 예정

- (CJ올리브네트웍스) 아마존웹서비스(AWS)와 협력, 블록체인을 기반으로 한 음악 저작권 관리 시스템 구축
 - 국내기업 CJ올리브네트웍스는 블록체인 네트워크를 생성하고 관리하는 AWS의 ‘아마존 매니지드 블록체인(Amazon Managed Blockchain)’을 활용해 방송 콘텐츠의 음원 저작권을 체계적으로 관리할 계획이며 디지털 저작권 시스템을 구현하는 첫 번째 사례
- (왓차, 블로터앤미디어) 국내에서는 왓차가 블록체인 기반 ‘컨텐츠 프로토콜’ 프로젝트를, IT 블로터앤미디어가 블록체인 기반의 탈중앙화 미디어 네트워크 ‘LEVEL’을 시작
 - 왓차가 선보인 ‘컨텐츠 프로토콜(Contents protocol, CPT)’은 컨텐츠 생산자뿐 아니라 컨텐츠를 공유하는 사용자의 자발적 활동, 리뷰나 평점 행위에 보상을 제공

[왓차 컨텐츠 프로토콜(CPT) 개념도]



*출처: 왓차 컨텐츠 프로토콜 개념도, 왓차 컨텐츠 프로토콜 백서

- (픽션네트워크) 픽션네트워크는 블록체인 스타트업인 ‘픽션’이 블록체인 기술을 활용해 창작자와 유저를 직접 연결하는 네트워크.
 - 픽션은 웹툰 분야에 ‘픽션 네트워크’를 가장 먼저 적용. 픽션 네트워크는 콘텐츠를 배포하는 일종의 프로토콜 개념으로, 트래픽이 있는 모든 플랫폼들은 픽션이 제공하는 애플리케이션 프로그램 인터페이스 등을 적용해 콘텐츠를 제공 가능
- (피블) 피블은 일반인과 전문가 등 크리에이터들의 사진, 영상 콘텐츠를 공유하고, 사용자가 이 플랫폼에서 활동하면 보상이 이루어지는 블록체인 소셜 미디어 플랫폼을 구상
 - 사진과 동영상 등 미디어 콘텐츠를 업로드하고, 이를 추천하거나 공유하면 최초 콘텐츠 크리에이터와 참여자에게 피블코인과 피블러시라는 보상이 이루어지는 중
- (기프트, 유니오) 모든 소셜 미디어 플랫폼에서 사용할 수 있는 탈중앙화 통합 가상선물 프로토콜인 기프트와 콘텐츠 크리에이터들이 본인의 콘텐츠를 통해 수익을 얻고 성장할 수 있는 생태계를 조성하는 유니오 등이 존재

- (예스24) 예스24는 이스라엘 블록체인 업체 오브스(ORBS)와 협업하여 자체 기존 이더리움 메인넷보다 10배 이상 향상된 거래 속도로 디지털 콘텐츠 유통을 위한 블록체인 플랫폼 '세이(sey)체인' 메인넷을 론칭

- 독자들은 디지털 콘텐츠 플랫폼인 '시프트북스'에서 마음에 드는 작품을 응원하는 활동을 통해 세이코인을 얻을 수 있으며, 작가들은 독자 응원 순위에 따른 보상으로 세이코인 획득 가능

[세이체인 시스템]

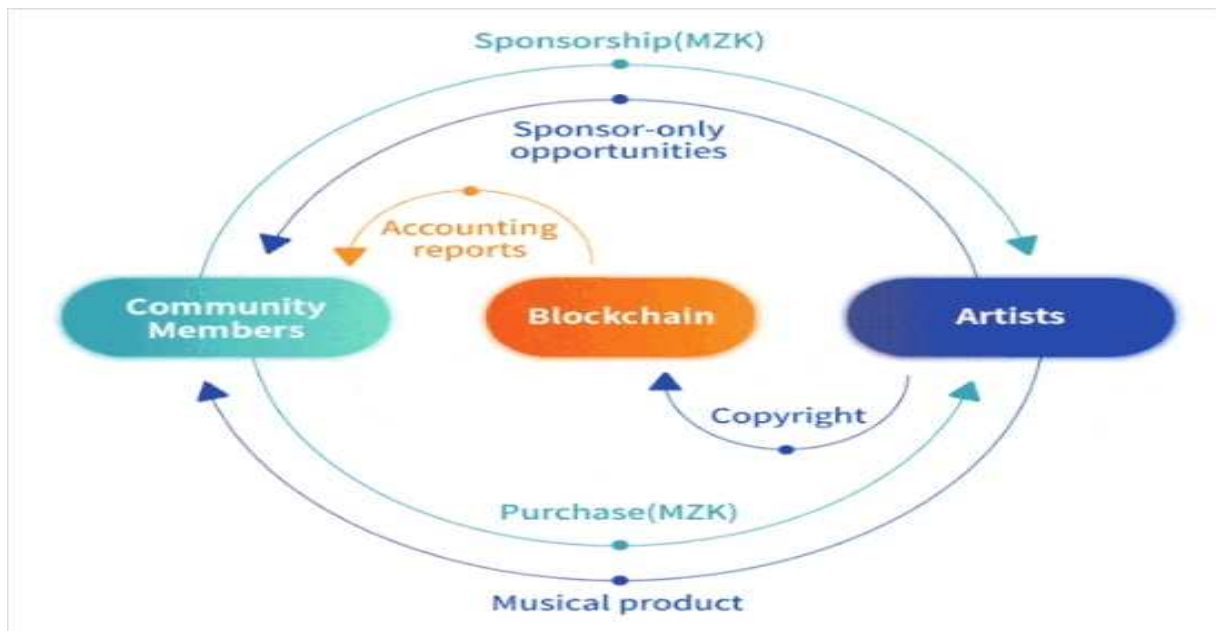


*출처: 예스24

- (후오비코리아) 블록체인 기반 음악산업 플랫폼 '뮤지카' 상장

- 뮤지카는 디지털 음악 생태계를 구축하는 것을 목표로 하는 블록체인 프로젝트이며, 암호화폐인 뮤지카 코인을 활용해 사용자가 아티스트 발굴, 후원, 음악의 생산 소비에 참여할 수 있는 특징

[뮤지카 생태계 개념도]



*출처: 해시넷, '뮤지카'.

다. 국내 연구개발 기관 및 동향

(1) 연구개발 기관

[블록체인 디지털 콘텐츠 관리 플랫폼 분야 기술개발 기관]

기관	소속	연구분야
한국전자통신연구원	미디어연구본부, 차세대콘텐츠연구본부	<ul style="list-style-type: none"> • 고성능 블록체인 플랫폼 기술 개발 (MS 윈도우, 애플 맥OS) • 탈중앙 합의 실행 엔진 개발 • Smart Contract 실행 엔진 개발 • Peer-to-Peer Overlay Network 개발 • 유통 콘텐츠 검색 모듈 개발 • 블록체인 기반의 탈중앙화 딥러닝 플랫폼
서울대학교 산학협력단	VMO(Virtual Machine and Optimization) 연구실	<ul style="list-style-type: none"> • 블록체인 부트스트래핑, 성능 및 공간 최적화 • 엣지 컴퓨팅 환경에서의 DNN 연산 오프로딩 플랫폼 • DRAM 테스트 패턴 프로그램의 변환 플랫폼 • 웹 플랫폼 성능 최적화

(2) 기관 기술개발 동향

☐ (캡슐미디어)

- 블록체인 기반, 디지털 동영상 콘텐츠 저작권 및 보상 시스템 (2019-10-01~2021-09-30)
 - 동영상 콘텐츠의 디지털 변환시스템
 - 블록체인을 활용한 동영상 디지털 자산의 지분을 관리 시스템
 - 동영상 저작권 블록체인 시스템
 - 참여자간의 스마트계약 (Smart Contract)

☐ (레코드팜)

- 블록체인 기반 저작권 관리 및 분산형 스트리밍 플랫폼 개발 (2018-06-01~2020-05-31)
 - 저작권 관리 기술 개발
 - 블록체인 기반 결제 및 거래내역 관리 기술 개발

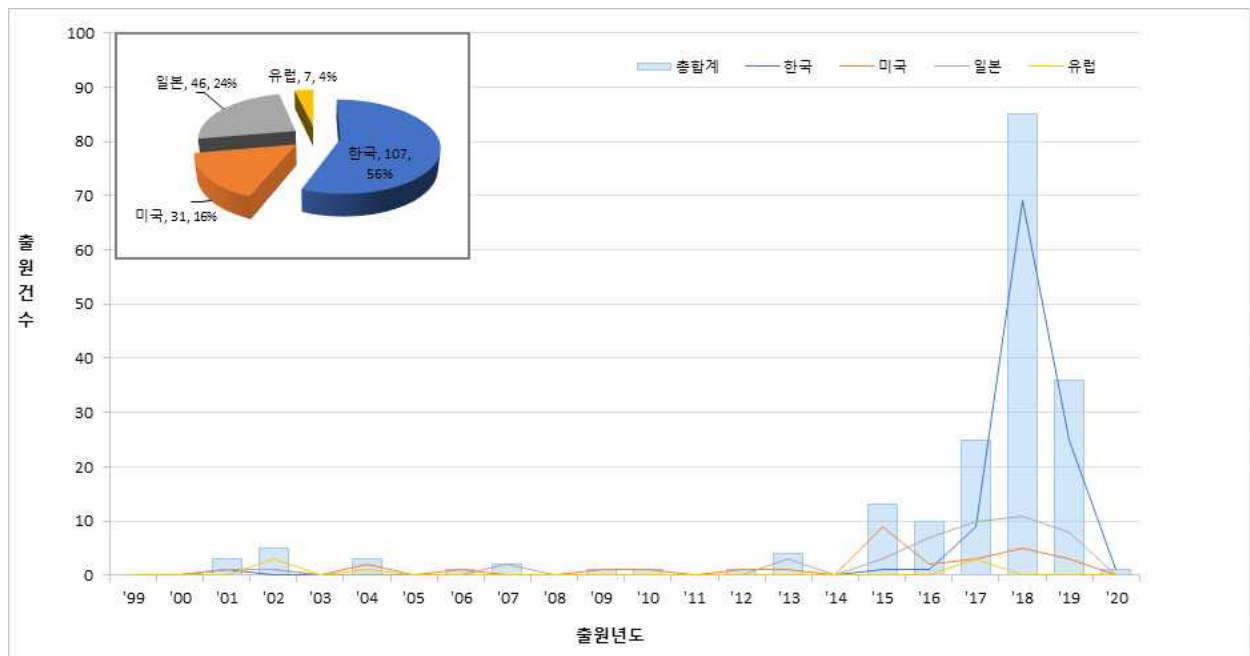
4. 특허 동향

가. 특허동향 분석

(1) 연도별 출원동향

- ☐ 블록체인 기반 디지털 콘텐츠 관리 플랫폼은 '17년부터 급격한 성장을 보임
 - 각 국가별로 살펴보면 한국이 가장 활발한 출원활동을 보이고 있음
- ☐ 국가별 출원비중을 살펴보면 한국이 전체의 56%의 출원 비중을 차지하고 있어, 최대 출원국으로 블록체인 기반 디지털 콘텐츠 관리 플랫폼 분야를 리드하고 있는 것으로 나타났으며, 일본은 24%, 미국은 16%, 유럽은 4% 순으로 나타남

[블록체인 기반 디지털 콘텐츠 관리 플랫폼 연도별 출원동향]



(2) 국가별 출원현황

☐ 한국의 출원현황을 살펴보면, '18년부터 해당 기술의 출원이 급격히 증가하는 추세

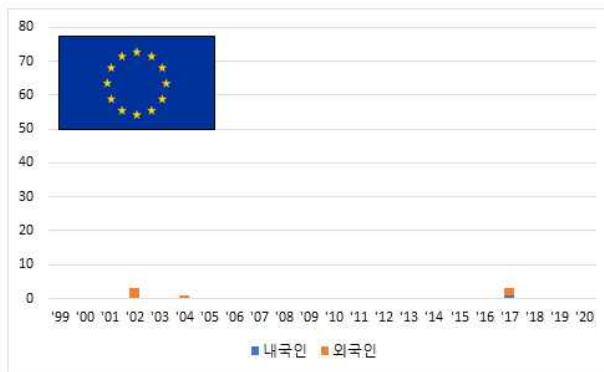
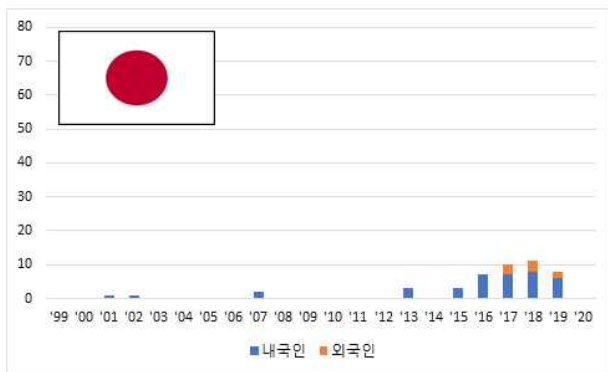
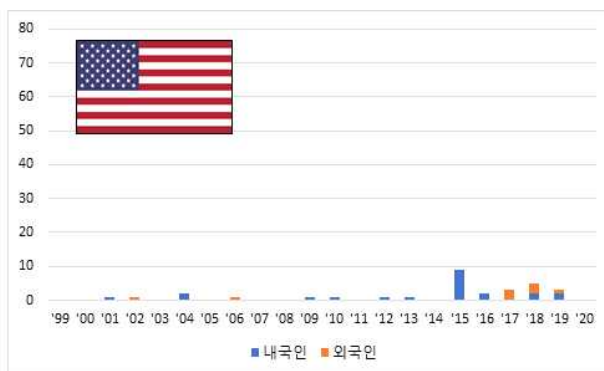
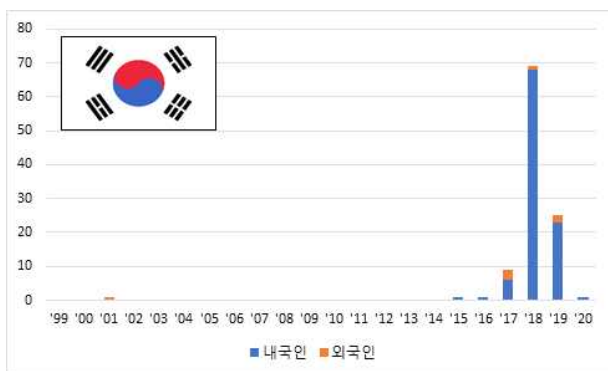
- 내국인 위주의 출원이 진행되고 있음
- 한국 기술의 양적 흐름은 '18년에 가장 많은 특허를 출원
- 한국의 출원 수는 미국, 유럽, 일본에 비해 가장 많은 특허를 출원

☐ 미국의 출원현황은 출원수가 매년 10건 이하로, 뚜렷한 증감 동향이 나타나지 않음

☐ 미국의 출원현황은 출원수가 매년 5건 이하로, 뚜렷한 증감 동향이 나타나지 않음

☐ 일본의 출원현황은 출원수가 매년 10건 이하로, 뚜렷한 증감 동향이 나타나지 않음

[국가별 출원현황]

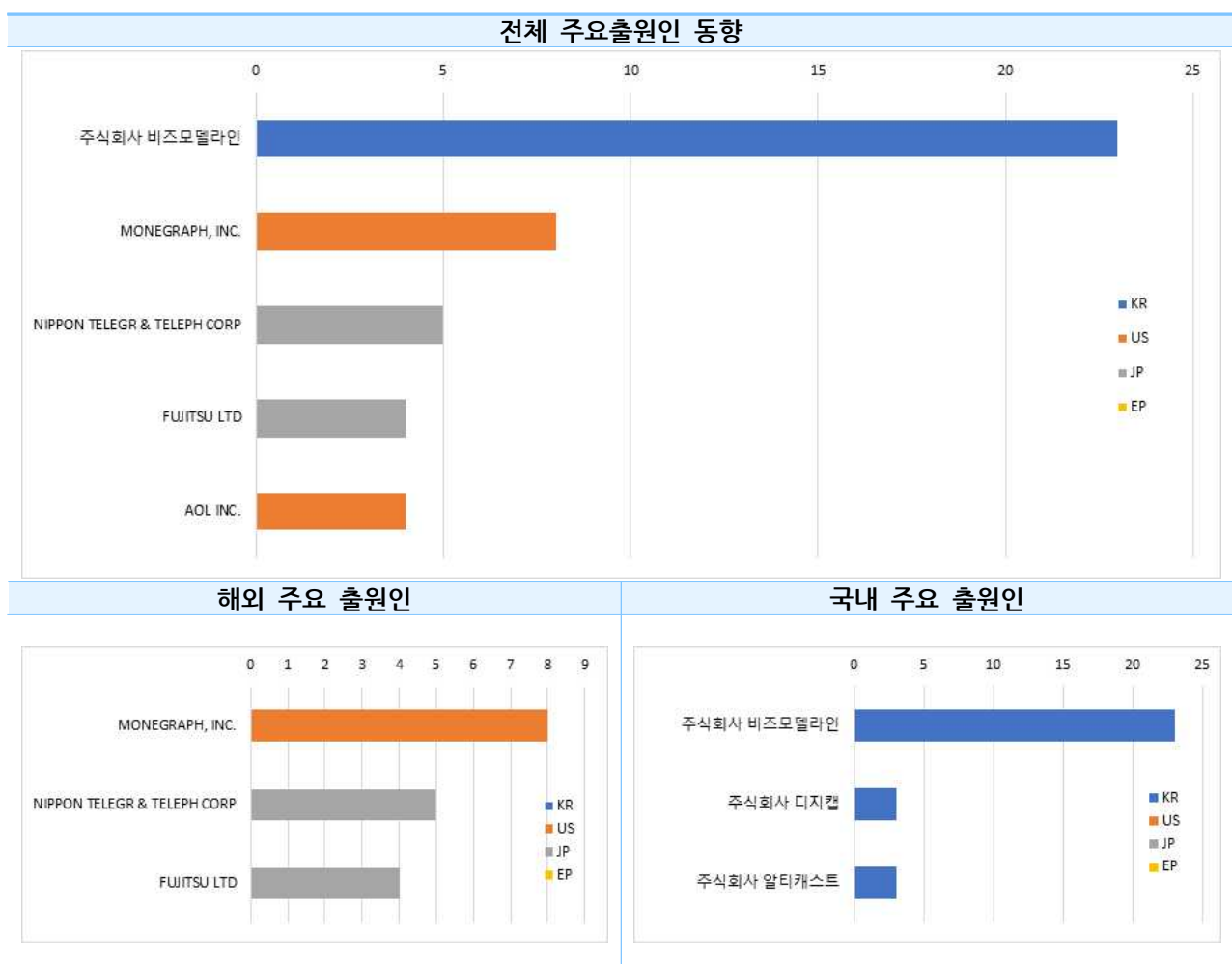


285

나. 주요 출원인 분석

- ☐ 블록체인 기반 디지털 콘텐츠 관리 플랫폼의 전체 주요출원인을 살펴보면, 주로 일본 국적의 출원인이 다수 포함되어 있는 것으로 나타났으며, 제 1 출원인으로는 한국의 주식회사 비즈모델라인으로 나타남
 - 제 1 출원인인 주식회사 비즈모델라인의 출원은 한국에 집중된 경향을 보임
- ☐ 블록체인 기반 디지털 콘텐츠 관리 플랫폼 관련 기술로 블록체인을 다루는 대기업에 의한 출원이 대다수를 차지
 - 국내에서는 중소기업(개인)의 활발한 출원이 이루어짐

[블록체인 기반 디지털 콘텐츠 관리 플랫폼 주요출원인]



(1) 해외 주요출원인 주요 특허 분석

◎ MONEGRAPH, INC.

- MONEGRAPH, INC.는 미국 블록체인 기업으로, 블록체인 기반 디지털 콘텐츠 관리 플랫폼 기술과 관련하여, 디지털 콘텐츠를 블록체인으로 관리하는 시스템과 관련하여 9건의 미국 출원을 진행하였으며, 그 중 등록된 특허는 1건으로 파악

[MONEGRAPH, INC. 주요특허 리스트]

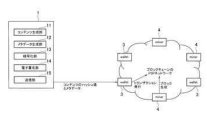
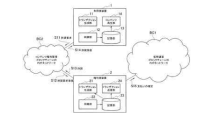
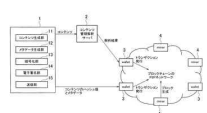
등록번호 (출원일)	명칭	기술적용분야	도면
US10380702 (2015.12.30)	Rights transfers using block chain transactions	디지털 콘텐츠 아이템에 대한 권리들의 수집을 블록체인에 등록하여 디지털 콘텐츠와 같은 미디어를 관리하는 시스템	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ NIPPON TELEGR & TELEPH CORP

- NIPPON TELEGR & TELEPH CORP은 일본의 통신 산업을 주관하는 기업으로, 다수의 블록체인 관련 특허를 보유하고 있으며, 블록체인 기반 디지털 콘텐츠 관리 플랫폼 기술과 관련한 특허를 5건 출원
- 블록체인 기반 디지털 콘텐츠 관리 플랫폼에 관련하여 출원을 진행한 특허 모두 일본에 출원한 것으로, 자국 내 출원 성향이 높은 것으로 사료

[NIPPON TELEGR & TELEPH CORP 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
JP6601623 (2016.05.10)	콘텐츠 유통 시스템, 콘텐츠 유통 방법, 콘텐츠 생성 장치 및 콘텐츠 생성 프로그램	블록 체인을 이용하여, 중앙집권 기구를 이용하지 않고, 콘텐츠의 정보를 등록하는 트랜잭션(transaction)를 발행하고, 트랜잭션(transaction)가 블록 체인으로 등록됨으로써 콘텐츠의 정보를 네트워크로 유통	
JP6628188 (2016.05.10)	결제 시스템, 결제방법, 트랜잭션 생성 장치 및 트랜잭션 생성 프로그램	블록 체인 기술을 이용하는 2개가 다른 시스템을 제휴하는 기술	
JP6601624 (2016.05.10)	콘텐츠 유통 시스템, 콘텐츠 유통 방법, 콘텐츠 생성 장치 및 콘텐츠 생성 프로그램	콘텐츠를 생성했을 때에, 콘텐츠의 해시값과 콘텐츠로 부수 하는 메타 데이터를 취득하고, 해시값과 메타 데이터를 블록 체인으로 등록	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

© FUJITSU LTD

- ☐ FUJITSU LTD는 일본의 정보통신기술 기업으로, 다수의 분산 파일 공유 시스템 관련 특허를 보유하고 있으며, 블록체인 기반 디지털 콘텐츠 관리 플랫폼 기술과 관련한 특허를 일본에 출원

[FUJITSU LTD 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
JP6610814 (2019.02.12)	통신 방법, 장치, 및 프로그램	애플리케이션만 인스톨하면, 분산 파일 공유 네트워크로 액세스 가능한 고시큐어인 파일 공유 공간을 구축	<p>도면 1: 시스템 구성도. 클라우드 서버(100)가 네트워크(200)를 통해 다수의 사용자 장치(300)와 연결되어 있다. 클라우드 서버(100)는 저장부(110)와 제어부(120)를 포함한다. 네트워크(200)는 라우터(210)와 스위치(220)를 포함한다. 사용자 장치(300)는 스마트폰(310)과 PC(320)를 포함한다.</p>
JP6533771 (2016.11.15)	통신 방법, 장치, 및 프로그램	사용자/그룹 인증이나, 콘텐츠의 일의성의 보증, 서비스리포지토리, 파일의 데이터/엑세스 로그 관리, 파일의 액세스 제어 등의 기능	<p>도면 2: 시스템 구성도. 클라우드 서버(100)가 네트워크(200)를 통해 다수의 사용자 장치(300)와 연결되어 있다. 클라우드 서버(100)는 저장부(110)와 제어부(120)를 포함한다. 네트워크(200)는 라우터(210)와 스위치(220)를 포함한다. 사용자 장치(300)는 스마트폰(310)과 PC(320)를 포함한다.</p>

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

(2) 국내 주요출원인 주요 특허 분석

◎ 주식회사 비즈모델라인

- 주식회사 비즈모델라인은 블록체인 기반 디지털 콘텐츠 관리 플랫폼 기술에 있어서, '18년도 9월부터 출원을 시작하여 아직까지 등록된 특허는 없는 것으로 파악됨
- 주식회사 비즈모델라인의 공개특허를 대상으로 분석한 결과, 블록체인 네트워크를 통해 거래하는 기술을 이용한 특허를 23건 출원

[주식회사 비즈모델라인 주요특허 리스트]

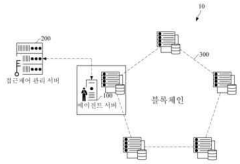
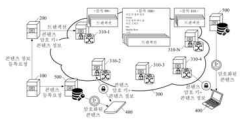
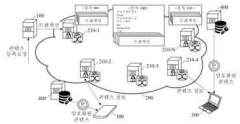
공개번호 (출원일)	명칭	기술적용분야	도면
KR2020-0088958 (2019.01.15)	사용자 의향정보를 이용한 토큰 제공 방법	사용자 의향정보를 이용한 토큰 제공 방법에 따라 지정된 블록체인 네트워크를 구현	
KR2020-0088956 (2019.01.15)	블록체인을 이용한 사용자 의향정보 처리 방법	지정된 블록체인 네트워크를 통해 상기 거래내역의 블록체인화 절차를 수행	
KR2020-0074324 (2018.12.14)	피부상태정보 거래 방법	블록체인 네트워크 상의 토큰을 이용하여 상기 저장매체에 저장된 사용자 피부상태정보의 거래	

* 공개특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 주식회사 디지캡

- 주식회사 디지캡은 한국의 디지털콘텐츠 보안 및 저작권 관리 솔루션 전문 기업으로, 블록체인 기반 디지털 콘텐츠 관리 플랫폼기술과 관련된 특허를 3건 출원하였으며, 3건의 특허 모두 등록된 것으로 파악

[주식회사 디지캡 주요특허 리스트]

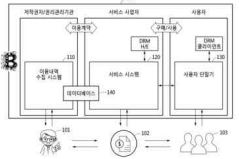
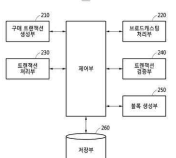
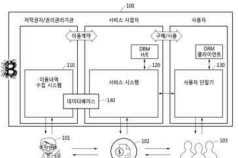
등록번호 (출원일)	명칭	기술적용분야	도면
KR2148130 (2018.08.20)	미디어 블록체인을 위한 접근제어 시스템 및 방법	블록체인에 기반한 DRM 시스템에서 블록체인에 기록하거나 블록체인에서 조회하기 위한 접근하는 서버 등의 접근을 제어하는 시스템	
KR2034449 (2017.12.12)	콘텐츠 블록체인에서의 콘텐츠 암호키 관리 및 배포 방법	블록체인 기반의 DRM 콘텐츠 암호키 배포 시스템에서의 콘텐츠 암호키 배포에 관한 기술	
KR1986482 (2017.12.12)	콘텐츠 정보 저장 및 관리를 위한 콘텐츠 블록체인	DRM 서비스 시스템은 콘텐츠 등록 에이전트와, 블록체인 네트워크와, 사용자 에이전트를 포함한 블록체인 기반의 DRM 서비스 시스템	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

◎ 주식회사 알티캐스트

- 주식회사 알티캐스트는 한국의 디지털 방송용 소프트웨어 개발 기업으로, 블록체인 기반 디지털 콘텐츠 관리 플랫폼 기술과 관련된 특허를 3건 출원하였으며, 3건의 특허 모두 등록된 것으로 파악

[주식회사 알티캐스트 주요특허 리스트]

등록번호 (출원일)	명칭	기술적용분야	도면
KR1941786 (2017.11.01)	블록체인기술을 이용한 콘텐츠 유통 관리 시스템 및 방법	블록체인 기술 기반의 콘텐츠 유통 관리에 있어, 분산원장을 효율적으로 관리하는 기술	
KR1941785 (2017.11.01)	블록체인기술을 이용한 콘텐츠 유통 관리 시스템 및 방법	블록체인 기술을 접목한 새로운 콘텐츠 유통 관리 플랫폼의 모델을 설계	
KR1953090 (2017.11.01)	블록체인기술을 이용한 콘텐츠 유통 관리 시스템 및 방법	콘텐츠 유통과 이와 관련된 흐름에 대한 무결성을 확보할 수 있는 블록체인기술을 이용한 콘텐츠 유통 관리 기술에	

* 등록특허 기준, 피인용문헌수 및 패밀리 국가수가 큰 특허를 주요특허로 도출

다. 기술진입장벽 분석

(1) 기술 집중력 분석

□ 블록체인 기반 디지털 콘텐츠 관리 플랫폼 관련 기술에 대한 시장관점의 기술독점 현황분석을 위해 집중률 지수(CRn: Concentration Ratio n, 상위 n개사 특허점유율의 합) 분석 진행

- 상위 4개 기업의 시장점유율이 0.21로 블록체인 기반 디지털 콘텐츠 관리 플랫폼 분야에 있어서 독과점 정도는 낮은 수준으로 판단
- 국내 시장에서 중소기업의 점유율 분석결과 0.89로 해당 기술에 대하여 중소기업이 진입하여 활동하고 있는 것으로 파악

[주요출원인의 집중력 및 국내시장 중소기업 집중력 분석]

주요 출원인 집중력	주요출원인	출원건수	특허점유율	CRn	n
	주식회사 비즈모델라인(한국)	23	12.0%	0.12	1
	MONEGRAPH, INC.(미국)	8	4.2%	0.16	2
	NIPPON TELEGR & TELEPH CORP(일본)	5	2.6%	0.19	3
	FUJITSU LTD(일본)	4	2.1%	0.21	4
	AOL INC.(미국)	4	2.1%	0.23	5
	주식회사 디지캡(한국)	3	1.6%	0.25	6
	주식회사 알티캐스트(한국)	3	1.6%	0.26	7
	(주)아이디어 콘서트(한국)	2	1.0%	0.27	8
	ALI TECHNOLOGIES CO LTD(일본)	2	1.0%	0.28	9
	한국전자통신연구원(한국)	2	1.0%	0.29	10
	전체	191	100%	0.21	
국내시장 중소기업 집중력	출원인 구분	출원건수	특허점유율	CRn	n
	중소기업(개인)	91	89.2%	0.89	
	대기업	4	3.9%		
	연구기관/대학	7	6.9%		
	전체	102	100%	CR중소기업=0.89	

(2) 특허소송 현황 분석

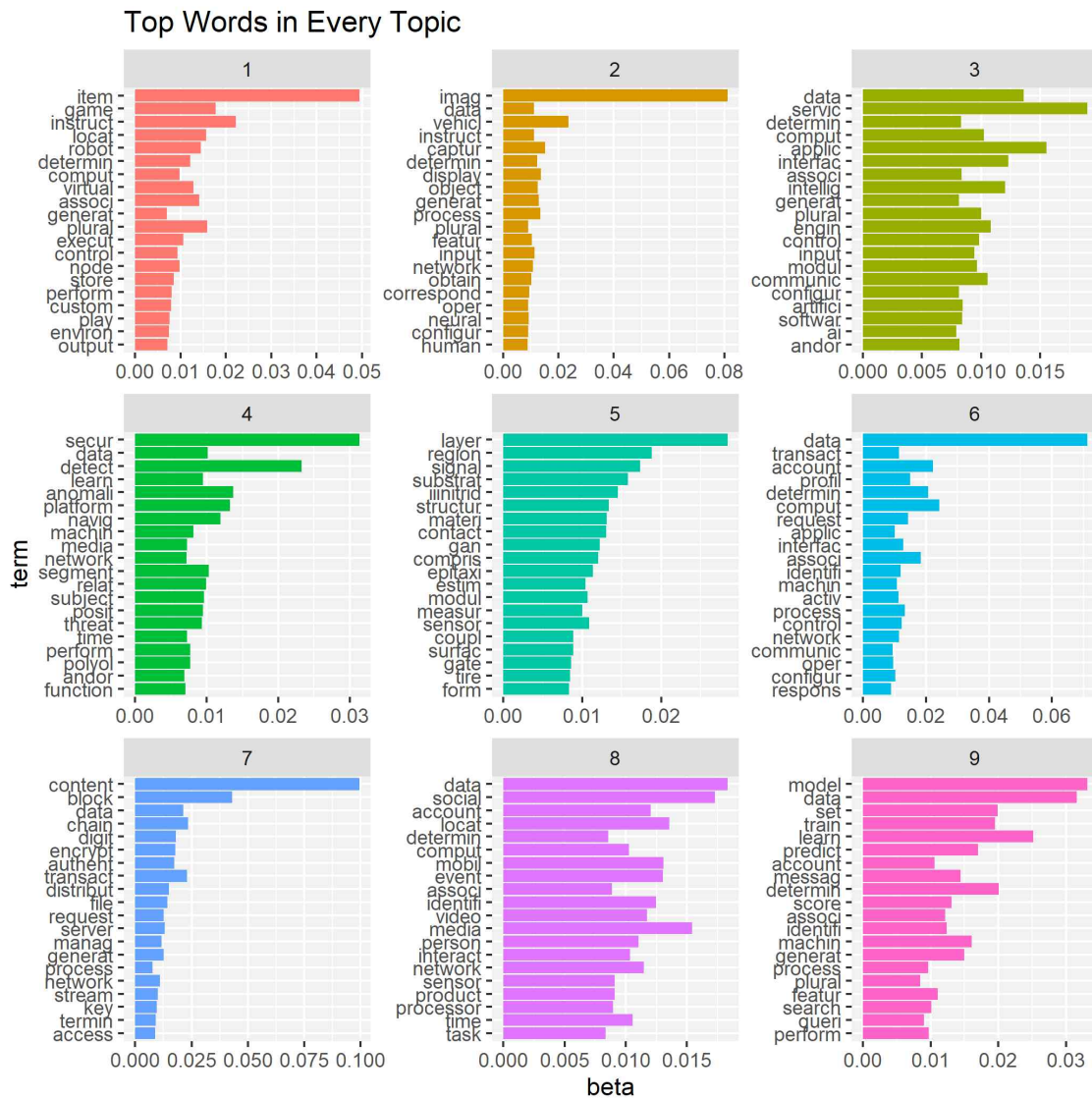
- ☐ 블록체인 기반 디지털 콘텐츠 관리 플랫폼 분야 관련 특허소송 이력은 검색되지 않음
 - 따라서 국내기업이 미국시장에 진입하는 경우, 해당 분야를 선점할 수 있을 것으로 판단
 - 다만, 블록체인과 관련해서는 4개의 소송이 검색

5. 요소기술 도출

가. 특허 기반 토픽 도출

- 1,103개의 특허의 내용을 분석하여 구성 성분이 유사한 것끼리 클러스터링을 시도하여 대표성이 있는 토픽을 도출

[블록체인 기반 디지털 콘텐츠 관리 플랫폼에 대한 토픽 클러스터링 결과]



나. LDA³¹⁾ 클러스터링 기반 요소기술 도출

[LDA 클러스터링 기반 요소기술 키워드 도출]

No.	상위 키워드	대표적 관련 특허	요소기술 후보
클러스터 01	item, instruct, game, plural, locate, robot, associate, virtual, determine, execute	<ul style="list-style-type: none"> • Providing customized and targeted performance improvement recommendations for software development teams • CUSTOMIZED ITEM DISPOSITION SYSTEM 	-
클러스터 02	image, vehicle, capture, display, process, generate, object, determine, input, data	<ul style="list-style-type: none"> • METHODS AND VEHICLES FOR CAPTURING EMOTION OF A HUMAN DRIVER AND CUSTOMIZING VEHICLE RESPONSE • Methods and vehicles for using determined mood of a human driver and moderating vehicle response 	-
클러스터 03	service, application, data, interface, intelligent, engine, communicate, compute, plural, control	<ul style="list-style-type: none"> • Computer code test script generating tool using visual inputs • Systems and methods of using an artificially intelligent database management system and interfaces for mobile, embedded, and other computing devices 	-
클러스터 04	secure, detect, anomaly, platform, navigate, segment, data, relate, subject, posit	<ul style="list-style-type: none"> • A METHOD AND SYSTEM FOR AUTOMATICALLY DETECTING AND MAPPING POINTS-OF-INTEREST AND REAL-TIME NAVIGATION USING THE SAME • Detection of anomalies, threat indicators, and threats to network security 	컨텐츠 불법 사용을 방지하기 위한 저작권 도용방지 기술 및 해킹방지기술
클러스터 05	layer, region, signal, substrate, structure, material, contact, GAN, comprise	<ul style="list-style-type: none"> • Load estimation system and method for a vehicle tire • Devices and systems for power conversion circuits 	-
클러스터 06	data, compute, account, determine, associate, profile, request, process, interface, control	<ul style="list-style-type: none"> • Capturing and extracting fragmented data and data processing using machine learning • Device for enabling patient self testing and treatment self-administration and system using the device for managing the patient's health care 	블록체인 참여자 식별 및 접근통제기술
클러스터 07	content, block, chain, transact, data, digit, encrypt, authentic, distribute, file	<ul style="list-style-type: none"> • Method and system for distributing digital content in peer-to-peer network • Electronic voting system, and, control method 	블록체인 기반 신원인증 서비스 기술
클러스터 08	data, social, media, locate, mobile, event, identify, account, video, network	<ul style="list-style-type: none"> • TOUCH SENSOR GESTURE RECOGNITION FOR OPERATION OF MOBILE DEVICES • Apparatus, systems and methods for event recognition based on a wireless signal 	-
클러스터 09	model, data, learn, determine, set, train, predict, machine, generate, message	<ul style="list-style-type: none"> • Collaboration using shared documents for processing distributed data • ASSESSMENT OF MACHINE LEARNING PERFORMANCE WITH LIMITED TEST DATA 	-

31) Latent Dirichlet Allocation

다. 특허 분류체계 기반 요소기술 도출

- ☐ 블록체인 기반 디지털 콘텐츠 관리 플랫폼 관련 특허에서 총 9개의 주요 IPC코드(메인그룹)를 산출하였으며, 각 그룹의 정의를 기반으로 요소기술 키워드를 아래와 같이 도출

[IPC 분류체계에 기반한 요소기술 도출]

IPC 기술트리		
(서브클래스) 내용	(메인그룹) 내용	요소기술 후보
(G06F) 전기에 의한 디지털 데이터처리	• (G06F-021) 부정행위로부터 프로그램 또는 데이터, 그 컴퓨터 부품을 보호하기 위한 보안 장치	콘텐츠 불법 사용을 방지하기 위한 저작권 도용방지 기술 및 해킹방지기술
(G06Q) 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 데이터 처리 시스템 또는 방법; 그 밖에 분류되지 않는 관리용, 상업용, 금융용, 경영용, 감독용 또는 예측용으로 특히 적합한 시스템 또는 방법	• (G06Q-040) 금융; 보험; 세무 전략; 법인세 또는 소득세의 처리	
	• (G06Q-020) 지불 체계, 방식 또는 프로토콜	사용자들이 쉽고 편하게 콘텐츠를 소모할 수 있는 블록체인 기반의 wallet 관리 기술
	• (G06Q-030) 거래, 예. 쇼핑 또는 전자상거래	
	• (G06Q-050) 특정 사업 부문에 특히 적합한 시스템 또는 방법, 예. 공익사업 또는 관광	공적 가시성을 위한 거래내역 추적 기술
(H04K) 비밀통신; 통신방해	• (H04K-001) 비밀통신	블록체인 참여자 식별 및 접근통제기술
(H04L) 디지털 정보의 전송, 예. 전신통신	• (H04L-009) 비밀 또는 보안통신을 위한 배치	블록체인 기반 신원인증 서비스 기술
	• (H04L-029) 그룹 1/00에서 H04L 27/00의 하나에도 포함되지 않는 배치, 장치회로 또는 시스템	
(H04N) 화상통신, 예. 텔레비전	• (H04N-021) 선택적 콘텐츠 분배, 예. 대화형(interactive) TV, VOD	

라. 최종 요소기술 도출

- ☐ 산업·시장 분석, 기술(특허)분석, 전문가 의견, 타부처 로드맵, 중소기업 기술수요를 바탕으로 로드맵 기획을 위하여 요소기술 도출
- ☐ 요소기술을 대상으로 전문가를 통해 기술의 범위, 요소기술 간 중복성 등을 조정·검토하여 최종 요소기술명 확정

[블록체인 기반 디지털 콘텐츠 관리 플랫폼 분야 요소기술 도출]

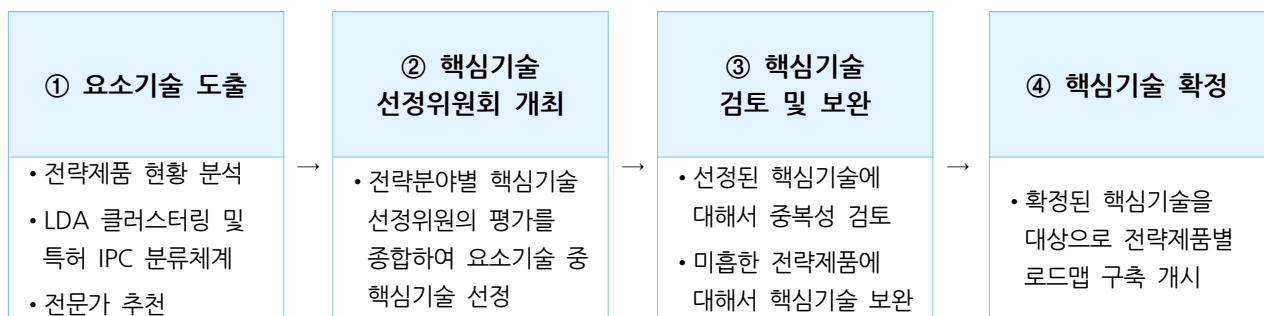
요소기술	출처
콘텐츠 생성자에게 투명하게 혜택이 돌아갈 수 있는 블록체인 기반의 토큰 경제 시스템	전문가추천
스마트 컨트랙트를 통해 해당 콘텐츠 사용시에 적절한 보상이 원작자에게 자동으로 배분될 수 있는 스마트 컨트랙트 기술	전문가추천
콘텐츠 불법 사용을 방지하기 위한 저작권 도용방지 기술 및 해킹방지기술	특허 클러스터링, IPC 기술체계, 전문가추천
사용자들이 쉽고 편하게 콘텐츠를 소모할 수 있는 블록체인 기반의 wallet 관리 기술	IPC 기술체계, 전문가추천
공적 가시성을 위한 거래내역 추적 기술	IPC 기술체계, 전문가추천
콘텐츠 저작자의 저작권을 관리하기 위한 블록체인 원장관리 기술	전문가추천
블록체인 기반 신원인증 서비스 기술	특허 클러스터링, IPC 기술체계, 전문가추천
블록체인 참여자 식별 및 접근통제기술	특허 클러스터링, IPC 기술체계, 전문가추천
블록체인 거래 검증 및 합의 기술	전문가추천
블록체인 인프라 기술	전문가추천

6. 전략제품 기술로드맵

가. 핵심기술 선정 절차

- ☐ 특허 분석을 통한 요소기술과 기술수요와 각종 문헌을 기반으로 한 요소기술, 전문가 추천 요소기술을 종합하여 요소기술을 도출한 후, 핵심기술 선정위원회의 평가과정 및 검토/보완을 거쳐 핵심기술 확정
- ☐ 핵심기술 선정 지표: 기술개발 시급성, 기술개발 파급성, 기술의 중요성 및 중소기업 적합성
 - 장기로드맵 전략제품의 경우, 기술개발 파급성 지표를 중장기 기술개발 파급성으로 대체

[핵심기술 선정 프로세스]



나. 핵심기술 리스트

[블록체인 기반 디지털 콘텐츠 관리 플랫폼 분야 핵심기술]

핵심기술	개요
콘텐츠 생성자에게 투명하게 혜택이 돌아갈 수 있는 블록체인 기반의 토큰 경제 시스템	• 블록체인의 취지에 맞게 공정하고 투명한 보상 배분 기반의 경제 시스템 필요
스마트 계약을 통해 해당 콘텐츠 사용시에 적절한 보상이 원작자에게 자동으로 배분될 수 있는 스마트 계약 기술	• 보상 지급 스마트계약 자동 생성 기술. 효과적으로 작성된 스마트 계약을 통해서 콘텐츠 생산자와 소비자가 합리적인 비용을 지불하고 콘텐츠를 이용하도록 구현
콘텐츠 불법사용을 방지하기 위한 저작권 도용방지 기술 및 해킹방지기술	• 블록체인을 활용한 저작권 관리 기술. 블록체인 상의 블록에 저작권 정보를 기록하게 함으로써 최초 저작자의 권리를 보장하고, 변조 불가능한 블록체인의 특성을 이용한 해킹방지 기능
사용자들이 쉽고 편하게 콘텐츠를 소모할 수 있는 블록체인 기반의 Wallet 관리 기술	• 지급 보상 관리를 수월하게 해줄 지급 관리 기술 개발. 콘텐츠 생산자와 소비자는 각자의 고유한 개인키/공개키를 사용하여 통여하고 효과적인 콘텐츠 소모 가능
공적 가시성을 위한 거래내역 추적 기술	• 공적 가시성을 위한 거래내역 추적 기술. 저작권료 징수 및 분배 등을 위한 디지털 저작물의 구매/사용 내역 추적 및 이에 대한 무결성을 시스템적으로 보장

다. 중소기업 기술개발 전략

- ☐ 정부의 블록체인 기술 개발을 위한 R&D 지원 및 투자 정책을 활용
- ☐ 해외 스타트업들과의 협업을 통해 지속적이고 선제적인 기술 개발 수행
- ☐ 협업을 통해 블록체인 기반 기술의 약점에 대한 인식과 함께 이에 대응할 수 있는 저작권 관리 기술, 스마트 컨트랙트 기술, 지갑 관리 기술에 대한 기술 협력 강화

라. 기술개발 로드맵

(1) 중기 기술개발 로드맵

[블록체인 기반 디지털 콘텐츠 관리 플랫폼 분야 중기 기술개발 로드맵]

블록체인 기반 디지털 콘텐츠 관리 플랫폼	중개 기관 없이 디지털 콘텐츠 관리 및 유통이 가능한 플랫폼 개발			
	2021년	2022년	2023년	최종 목표
컨텐츠 생성자에게 투명하게 혜택이 돌아갈 수 있는 블록체인 기반의 토큰 경제 시스템				공정한 투명한 토큰 보상 경제 설계
스마트 컨트랙트를 통해 해당 콘텐츠 사용시에 적정한 보상이 원작자에게 자동으로 배분될수 있는 스마트 컨트랙트 기술				스마트컨트랙트 생성 자동화
컨텐츠 불법사용을 방지하기 위한 저작권 도용방지 기술 및 해킹방지기술				블록체인 기반 등록을 통한 저작권 도용 관리
사용자들이 쉽고 편하게 콘텐츠를 소모할 수 있는 블록체인 기반의 Wallet 관리 기술				블록체인기반 지갑관리기술
공적 가시성을 위한 거래내역 추적 기술				분산 환경에서의 상용화

(2) 기술개발 목표

- ☐ 최종 중소기업 기술로드맵은 기술/시장 니즈, 연차별 개발계획, 최종목표 등을 제시함으로써 중소기업의 기술개발 방향성을 제시

[블록체인 기반 디지털 콘텐츠 관리 플랫폼 분야 핵심요소기술 연구목표]

핵심기술	기술요구사항	연차별 개발목표			최종목표	연계R&D 유형
		1차년도	2차년도	3차년도		
콘텐츠 생성자에게 투명하게 혜택이 돌아갈 수 있는 블록체인 기반의 토큰 경제 시스템	공정한 토큰 보상 경제 설계	토큰 이코노미 설계	시뮬레이션 수행 및 개선	실전 검증	공정한 투명한 토큰 보상 경제 설계	기술혁신
스마트 컨트랙트를 통해 해당 콘텐츠 사용시에 적절한 보상이 원작자에게 자동으로 배분될수 있는 스마트 컨트랙트 기술	스마트컨트랙트 자동 생성 기술	비즈니스 기능 분석	스마트 컨트랙트 설계	자동화	스마트 컨트랙트 생성 자동화	기술혁신
콘텐츠 불법사용을 방지하기 위한 저작권 도용방지 기술 및 해킹방지기술	블록체인 기록 관리 기술	블록체인 기반 저작권 등록	저작권 조회/관리	저작권 도용 차단 관리	블록체인 기반 등록을 통한 저작권 도용 관리	기술혁신
사용자들이 쉽고 편하게 콘텐츠를 소모할 수 있는 블록체인 기반의 Wallet 관리 기술	블록체인 기반 지갑 관리 기술 개발	기본 지갑 기능 개발	지원 기능 추가/개선	보안강화	블록체인 기반 지갑 관리 기술	상용화
공적 가시성을 위한 거래내역 추적 기술	DAG	설계 및 구현	테스트	상용화	분산환경에서의 상용화	산학연