

# 블록체인 동향정보

## [2020년 하반기]



금융보안원  
FINANCIAL SECURITY INSTITUTE

## 목 차

I. 연구 동향 .....	1
II. 정책 동향 .....	10
III. 언론 동향 .....	17
IV. 주요 행사 .....	21
[특집1] 블록체인 금융[가상자산, 디파이(DeFi), CBDC] 동향 .....	23
[특집2] 분산ID 환경에서의 개인정보 보호 대책 .....	34


금융보안원은 사원기관의 블록체인 관련 이해를 돕기 위해 '블록체인 동향정보'를 제공합니다(비정기). 관련하여 문의, 건의 사항, 다음 호에 실리기를 원하는 주제가 있을 경우 보안신기술팀([tech@fsec.or.kr](mailto:tech@fsec.or.kr), 02-3495-9822)으로 연락주시기 바랍니다.

참고로 본 문서의 정보들은 보고서 및 언론 등을 종합한 결과이며, 확인 시점에 따라 내용에 다소 차이가 있을 수 있으므로 이점 참고하여 주시기 바랍니다.

## I. 연구 동향 (출처 클릭 시 게시글로 이동)


- |                    |                      |
|--------------------|----------------------|
| ① 블록체인 핵심기술 및 적용사례 | ② 금융산업 블록체인 기술 도입 현황 |
| ③ 블록체인 기술 전망       | ④ 블록체인 활용 및 개발 현황    |
| ⑤ 블록체인 기술표준 동향     | ⑥ 블록체인 컨소시엄 선택 기준    |
| ⑦ 서비스형 블록체인 동향     | ⑧ 중앙은행 디지털화폐 기본원칙    |
| ⑨ 블록체인 기술표준 평가 지침  |                      |

### 1. 블록체인 핵심기술 및 적용사례

<출처>  [블록체인 핵심기술 및 국내외 산업 분야별 적용사례](#)  
(정보통신기획평가원, '20.6월)

- ☐ **(개요)** 국방부 산하 국방통합데이터센터가 분석한 국내·외 산업 분야별 안전한 거래를 위한 블록체인 기술 동향 소개
- ☐ **(핵심기술)** 블록체인을 구성하는 기술을 조사
  - **(공개키 암호화)** 개인키·공개키 쌍을 사용하여 무결성 보장\*
    - \* 개인키를 가진 사람만 서명값을 생성하고 누구든 공개키를 사용하여 서명값 (무결성 여부) 검증 가능
  - **(P2P\* 네트워크)** 거래 내역이 분산 저장(복제)되어 관리되며, 별도의 추가적인 신용기관 없이 P2P(1:1)로 바로 검증
  - **(블록체인 프로토콜)** 블록체인 네트워크 내에서 합의에 도달하고 거래를 검증
- ☐ **(금융권 적용사례)** 국가별 블록체인 적용사례를 조사
  - **(한국)** 스마트폰에 전자지갑을 탑재하여 가상자산 저장·송금
  - **(미국)** 블록체인을 응용한 지급 결제 시스템
  - **(중국)** 정보의 포괄적 관리를 위한 블록체인 기반 정보 공유 플랫폼

## 2. 금융산업 블록체인 기술 도입 현황

<출처>  [금융산업 블록체인 기술 도입 현황과 우체국 금융에의 시사점](#)  
(정보통신정책연구원, '20.6월)

- **(개요)** 정보통신정책연구원은 금융 분야의 블록체인 활용 사례와 시사점을 담은 보고서를 발간
- **(도입현황)** 국내·외 은행, 보험사의 블록체인 기술 활용 사례 조사
  - **(자격검증시스템)** 대출업무 관련 증명서류를 블록체인에 저장하여 증명서류의 정보 확인 절차를 간소화하고 대출 실행기간을 단축
  - **(P2P 금융증서 블록체인 서비스)** P2P 금융 투자자의 원리금 수취권 증서를 블록체인에 저장하여 증서의 무결성을 보장하고 모바일 애플리케이션으로 조회
  - **(보험금 지급체계 간소화)** 블록체인 기반 지급체계 공동망을 구축하여 보험정보와 통계 관리
  - **(해외송금 서비스)** 블록체인 기술로 구동되는 전자지갑 플랫폼을 이용해 타 국가로 안전하게 송금하고 그 과정을 추적
- **(우체국 금융에의 시사점)** 국내·외 도입사례를 통해 우체국 금융 업무에 블록체인 기술을 활용한 다양한 적용 가능성 확인

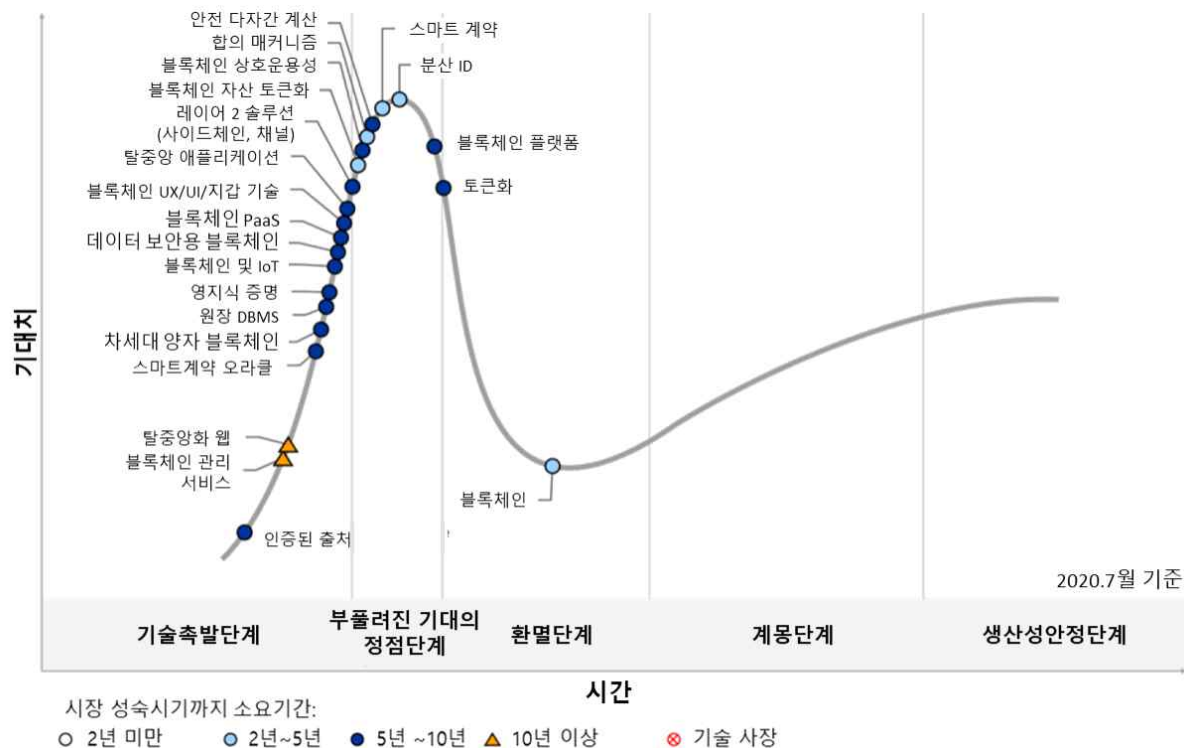


### 3. 블록체인 기술 전망

<출처>  [Hype Cycle for Blockchain Technologies, 2020](#) (Gartner, '20.7월)


- 가트너는 블록체인 기술 하이프사이클을 통해 향후 유망할 것으로 판단되는 블록체인 관련 기술을 분석

[ 블록체인 하이프사이클 2020 ]




- **(토큰화)** 유형자산, 금융증서를 블록체인 토큰에 연결하는 개념으로 자산의 소유자를 표기
- **(블록체인 자산 토큰화)** 자산(금전적 가치 또는 데이터)의 생성 또는 가치 표기, 자산의 사용권을 전달하는 과정
- **(블록체인 지갑)** 블록체인 자산 및 사용자 신원 데이터를 저장·관리하는 지갑으로 사용자와 블록체인 간 인터페이스 제공
- **(스마트 계약 오라클)** 현실 세계의 데이터, 사건 기반으로 스마트 계약을 실행하는 소프트웨어 메커니즘
- **(인증된 출처)** 블록체인에서 기록하고 추적할 수 있는 자산에 대한 인증으로 블록체인 참가자가 디지털 방식으로 출처 확인

## 4. 블록체인 활용 및 개발 현황

<출처>  [데이터 주권 시대의 블록체인 기술 활용 가능성과 개발 현황](#)  
(정보통신기획평가원, '20.7월)

- **(개요)** 고려대 권현영 교수가 분석한 자기정보통제권 실현을 위한 대안적 기술로서 블록체인의 활용 가능성과 개발 현황 소개
- **(데이터 주권 관련 정책)** 유럽 GDPR(일반데이터보호규정), 미국 HIPAA\*, 일본 개인정보보호법 개정, 브라질 개인정보보호법(LGPD) 개정
  - \* HIPAA : Health Insurance Portability and Accountability Act
- **(블록체인 기반 자기주권신원)** 중앙집중기관을 대신하여 개인이 신원 데이터를 제어·관리 가능
  - 블록체인은 자기주권신원 요소 중 투명성<sup>1)</sup>, 지속성<sup>2)</sup>, 호환성<sup>3)</sup> 성질을 만족시킬 수 있는 기술임
    - 1) 모든 시스템과 알고리즘은 사용자에게 투명 / 2) 데이터 장시간 보관 / 3) 데이터 호환
  - uPort, Sovrin, Veres One 등 자기주권신원 시스템은 개별적인 자기주권신원 모델을 구축 중
- **(블록체인 기반 접근제어)** 사용자 간의 신뢰 관계를 별도로 검증할 필요가 없으며 변경 불가능하고 추적 가능한 데이터 제어 구현 가능
  - FairAccess, PrivacyGuard 프레임워크 등의 연구 진행 중
- **(블록체인 기반 신원관리 플랫폼)** GDPR 요구사항(합법성, 투명성, 목적 제한, 데이터 최소화, 무결성 및 기밀성 등)이 구현 가능함을 보여주고 있음
  - uPort, Sovrin, Shocard, Civic 등 프라이버시 보존형 신원관리 플랫폼을 통해 신원증명 서비스 등 제공

## 5. 블록체인 기술표준 동향

<출처>  [ISO/TC 307 블록체인 정보보호 표준기술 동향](#)  
(한국정보보호학회, '20.8월)

- ☐ **(개요)** ETRI는 ISO/TC 307(블록체인·분산원장 기술위원회)의 국제 표준화 동향을 정리한 논문을 한국정보보호학회에 발표
- ☐ **(WG1(기반기술))** ①용어표준(IS 22739)은 '20년 제정 예정, ②참조구조 표준(IS 23257)은 '21년 제정 예정, ③텍사노미(분류체계) 및 온톨로지(사물간관계) 표준(TS 23258)은 '22년 제정 예정  
※ WG(working group) : 기술위원회(TC) 산하 표준안 논의를 위한 작업반
- ☐ **(WG2/WG4(정보보호/신원관리))** ①가상자산 거래소 정보보호 가이드라인(TR 23576), ②신원관리를 위한 분산원장기술 시스템(TR 23249) 등이 기술보고서로 개발 중
- ☐ **(WG3(스마트 계약 및 응용))** ①스마트 계약 상호작용 및 개요 표준(TR 23455)은 오류 정정 예정, ②합법 스마트 계약 표준안(TS 23259)은 관련 법적 내용을 포함해 기술규격으로 개발하기로 결정
- ☐ **(WG5(거버넌스))** 거버넌스 지침(TS 23635) 문서는 위원회 검토 단계로 거버넌스 콘텍스트\*를 기반으로 작성 중  
\* 데이터, 프로토콜, 응용, 조직
- ☐ **(WG6(유스케이스))** ①20여 개 유스케이스에 대한 초안(working draft) 투표 진행('20.10월), ②신규 아이템으로 인증, 에너지 트레이딩, 공급망 등 8개 진행 중


## 6. 블록체인 컨소시엄 선택 기준

<출처>  [How to Choose a Blockchain Consortium for Digital Business Collaboration and Acceleration](#) (Gartner, '20.9월)

- (개요) 가트너는 적절한 블록체인 컨소시엄의 선택을 위한 기준 제시
- (컨소시엄 가입 목적) 학습, 협력, 위험 관리로 분류
  - (학습) 회사 간 아이디어 교환 목적이나 컨소시엄 장기간 유지 어려움  
※ 비즈니스로 이어지지 않아 컨소시엄에 지속적으로 투자하지 않을 수 있음
  - (협력) 독점 우려 해소를 위한 규제산업에 적합
  - (위험 관리) 컨소시엄에서 개념검증(PoC), 개발, 구현 등 테스트
- (컨소시엄 선택 기준) 컨소시엄 가입 시 9가지 평가 기준 제시
  - 1) (목적) 왜 컨소시엄에 가입하는지
  - 2) (지적재산권) 누가 무엇을 소유하는지
  - 3) (비용) 누가 무엇을 위해 비용을 지불하는지
  - 4) (거버넌스) 누가 무엇을 결정하는지
  - 5) (책임) 누가 무엇을 위해 책임을 지는지
  - 6) (배당 구조) 누가 이익을 얻는지
  - 7) (외부 소통) 누가 소통을 담당하며 공을 차지하는지
  - 8) (기술 지원) 어떻게 기술 관련 의사결정이 이루어지는지
  - 9) (출구 전략) 누가 무엇을 위해 비용을 지불하는지



## 7. 서비스형 블록체인 동향

<출처>  [블록체인 강국의 인프라 서비스형 블록체인\(BaaS\)](#)  
(정보통신산업진흥원, '20.9월)

- ☐ **(개요)** 정보통신산업진흥원은 서비스형 블록체인(BaaS)\*의 개요와 시장동향에 대해 분석 정리
  - \* BaaS : Blockchain as a Service
- ☐ **(개념)** 블록체인 개발과 구축을 쉽고 빠르게 할 수 있도록 필요한 기능을 인터넷으로 제공하는 블록체인 클라우드 서비스
- ☐ **(장점)** 초기비용을 절감할 수 있고 낮은 개발 난이도로 개발 기간이 단축되며 노드의 안전성과 확장성을 보장
- ☐ **(해외 동향)** 글로벌 클라우드 서비스 기업\*들은 BaaS 사업에 진입 중이며 중국은 정부 주도형 BaaS 네트워크를 발표하고 글로벌 서비스를 개시
  - \* 마이크로소프트, IBM, 아마존, 오라클 등
- ☐ **(국내 동향)** 일부 대기업과 블록체인 전문기업에서 BaaS 사업을 진행 중이나 시장 확보 및 규모의 경제 측면에서 해외 기업보다 열세
- ☐ **(시사점)** 국내 BaaS의 발전 현황을 확인했으며 경쟁력 확보를 위한 정책적인 밀바침 필요

## 8. 중앙은행 디지털화폐(CBDC) 기본원칙

<출처>  [Central Bank Digital Currencies: Foundational Principles and Core Features](#) (국제결제은행, '20.10월)

□ **(개요)** 국제결제은행(BIS)은 7개국 중앙은행\*과 함께 디지털화폐를 이용한 통화정책의 시행에 관한 핵심 원칙을 담은 보고서를 발표

\* 미국, 스위스, 스웨덴, 영국, 유럽, 일본, 캐나다

□ **(기본원칙)** CBDC\* 발행에 대한 중앙은행의 공통원칙 조사

\* Central Bank Digital Currency

○ **(안정)** 공공 정책 목표 달성을 지원하며 통화와 금융 안정에 피해를 주지 말아야 함

○ **(공존)** 서로 다른 유형의 중앙은행 화폐\*는 공공정책 목표를 위해 서로를 보완하며 상업은행 계좌와 같은 기존 화폐와 공존

\* CBDC, 현금, 지급준비금 또는 청산 계좌(reserve or settlement account), 외화보유계좌

○ **(혁신과 효율성 증진)** 공공기관과 민간단체는 안전하고 효율적인 결제 시스템을 만들기 위한 역할을 수행


□ **(주요요건)** 기본원칙을 충족시키는 데 필요한 핵심 요건 조사

○ **(화폐 특성)** 현금 및 개인 화폐와 동등하게 교환되어야 하며 현금처럼 사용이 간편하고 오프라인 결제가 가능해야 함

○ **(시스템 특성)** 언제든지 결제할 수 있고 사이버 공격에 대비할 수 있으며 자연재해나 정전과 같은 상황에서 회복할 수 있어야 함

○ **(제도적 특성)** 중앙은행은 CBDC 발행을 뒷받침하는 명확한 권한을 가져야 하며 CBDC 시스템은 규제 기준을 따라야 함

## 9. 블록체인 기술표준 평가 지침

<출처>  [Global Standards Mapping Initiative: An overview of blockchain technical standards](#) (세계경제포럼, '20.10월)

□ **(개요)** 세계경제포럼은 블록체인 및 가상자산 환경의 평가와 행동 지향적 지침을 담은 기술표준 보고서를 발간

□ **(주요사항)** 다양한 블록체인 기술표준을 평가

○ **(용어)** 정의가 명확하지 않으며 일관성이 없음

○ **(과장 광고)** 이니셔티브\*는 많지만 일부 이니셔티브는 중단되거나 실질적인 결과물 미발표

\* Initiative : 문제나 상황을 해결 또는 대응하기 위한 시도 및 행위

○ **(표준 범위)** 기술 스택의 계층을 나누는 방식은 조직마다 다르며 분산원장기술과 산업 분야의 관련 구성 요소와의 경계가 모호

○ **(차이 및 중복)** 표준 제정 환경에서 통일되지 않은 부분 다수 존재

○ **(표준 보급)** 분산원장기술이 거버넌스를 위한 새로운 모델을 도입함에 따라 표준 구현을 위한 최상의 모델 필요

□ **(권장사항)** 표준 평가에 따른 권장사항 제시


○ **(표준 제정 기관)** 기관 간 협력 사항을 확실하게 하고 표준화에 대한 논의가 필요한 부분을 구체화

○ **(표준 도입 기관)** 표준 제정에 있어서 원하는 수준의 범위(표준 개발 또는 검토 참여 등)를 설정하고 표준 도입 의사결정 및 절차를 정의

## II. 정책 동향 (출처 클릭 시 게시글로 이동)

- |                    |                      |
|--------------------|----------------------|
| ① 국내 블록체인 기술확산 전략  | ② 중국의 블록체인 정책        |
| ③ 국내 블록체인 기술 개발 사업 | ④ 한국은행의 CBDC 파일럿 시스템 |
| ⑤ 미국의 가상자산 프레임워크   | ⑥ 중국의 CBDC 관련 암호법    |
| ⑦ 해외 가상자산 시장 동향    |                      |

### 1. 국내 블록체인 기술확산 전략

<출처>  [7대 분야 블록체인 전면 도입, 분산 신원 증명 집중 육성](#)  
(과학기술정보통신부, '20.6월)

- ☐ **(개요)** 과학기술정보통신부는 초연결·비대면 신뢰 사회를 위한 블록체인 기술 확산 전략을 발표
- ☐ **(중점 추진과제)** 5대 전략 및 중점 추진과제 도출
  - **(블록체인 7대 분야 도입)** ①온라인 투표시스템, ②기부내역 기록, ③중복수급 방지, ④신재생에너지 거래, ⑤지역 디지털 화폐, ⑥부동산 거래, ⑦우정 서비스 통합 고객관리 체계
  - **(분산신원증명 서비스 활성화)** 분산신원증명(분산ID) 기술 활성화 정책을 추진하여 비대면 환경에서 신원증명을 제공하고 사용자가 개인정보를 직접 관리
  - **(블록체인 기업 통합지원체계 구축)** 국내 기업의 국제 경쟁력을 높이기 위한 종합적인 기업 지원체계 구축
  - **(차세대 블록체인 핵심기술 개발)** 핵심기술 개발과 우리 기업의 시장 경쟁력 확보를 위한 글로벌 표준 대응 강화
  - **(블록체인 혁신생태계 조성)** 법제도 개선, 부산규제 자유 특구와 연계한 시범사업, 시장 수요 맞춤형 인력 양성


## 2. 중국의 블록체인 정책

<출처>  [중국의 블록체인 육성정책 최근 동향](#) (한국과학기술기획평가원, '20.6월)

- **(개요)** 한국과학기술기획평가원은 2019년 이후 중국의 블록체인 육성정책을 조사
- **(블록체인 서비스 네트워크(BSN) 운영)** 공공 인프라 네트워크로서 저렴한 비용으로 블록체인 애플리케이션을 개발, 배포 및 운영
  - **(목표)** 블록체인 응용과 대중화를 촉진하여 블록체인 프로젝트에 신뢰성을 더하고 확장 가능한 인프라를 제공
  - **(기대점)** BSN을 상용화하여 지역 간 공공 인프라 네트워크로 블록체인 기술 확산을 촉진하고 기술 역량을 강화
- **(디지털 위안화 시범운영)** 중국 정부가 발행·규제하며 위안화에 1:1로 연동되는 중국 유일의 디지털 법정화폐를 운영
  - ※ 중국인민은행은 디지털 위안화의 공식 명칭을 '디지털화폐·전자결제(DCEP, Digital Currency Electronic Payment)'로 표기
  - **(목적)** 민간 디지털화폐로 인한 위안화의 국제적 지위 위협에 대비하고 자금세탁 및 테러 자금조달을 방지하며 화폐 발행 비용을 절감
  - **(운영방식)** 거액결제용\*과 소액결제용\*\*을 구분하여 발행
    - \* 중앙은행과 금융기관 간 거액결제용 네트워크를 구축
    - \*\* 금융기관이 국민에게 공급·회수하며, 기관마다 각자의 소액결제용 네트워크 구축
- **(블록체인 산업단지 운영)** 중국 공산당 중앙위원회는 디지털화폐 연구와 활동 지원 계획을 발표하면서 산업생태계 확충 노력




### 3. 국내 블록체인 기술 개발 사업

<출처>  「데이터 경제를 위한 블록체인 기술 개발 사업」 예타 통과  
(과학기술정보통신부, '20.6월)

- **(개요)** 과학기술정보통신부는 데이터 경제를 위한 블록체인 기술 개발 사업이 예비타당성 조사를 최종 통과함을 발표
- **(사업계획)** '21년~25년 블록체인 처리성능 향상 및 프라이버시 보호를 위한 핵심 원천기술 개발을 추진(사업비 : 1,133억 원)
- **(추진사업)** 총 4개의 기술 개발
  - **(합의기술)** 탈중앙화를 유지하면서 블록체인 참여자가 증가하더라도 서비스의 안정적인 성능 확보
  - **(스마트 계약\* 보안 기술)** 스마트 계약 코드의 취약점을 탐지하고 방어하여 보안 취약점을 개선
    - \* 분산원장 기술에서 거래의 일정 조건을 만족시키면 당사자 간에 자동으로 거래가 체결되는 기술
  - **(개인정보 처리 및 신원관리 기술)** 블록체인 환경에서 개인정보 보호를 위한 분산신원증명(분산ID) 기술을 관리하고 데이터 활용 과정에서 프라이버시를 보호
  - **(데이터 주권 보장 데이터 관리 기술)** 블록체인 플랫폼을 사용하여 대용량 데이터를 관리하고 블록체인 서비스의 활용성을 강화

## 4. 한국은행의 CBDC 파일럿 시스템

<출처>  한국은행, 「중앙은행 디지털화폐 파일럿 시스템 컨설팅」 사업 추진  
(한국은행, '20.8월)

□ (개요) 한국은행은 CBDC 파일럿 시스템 구축을 위한 외부 컨설팅 사업을 추진

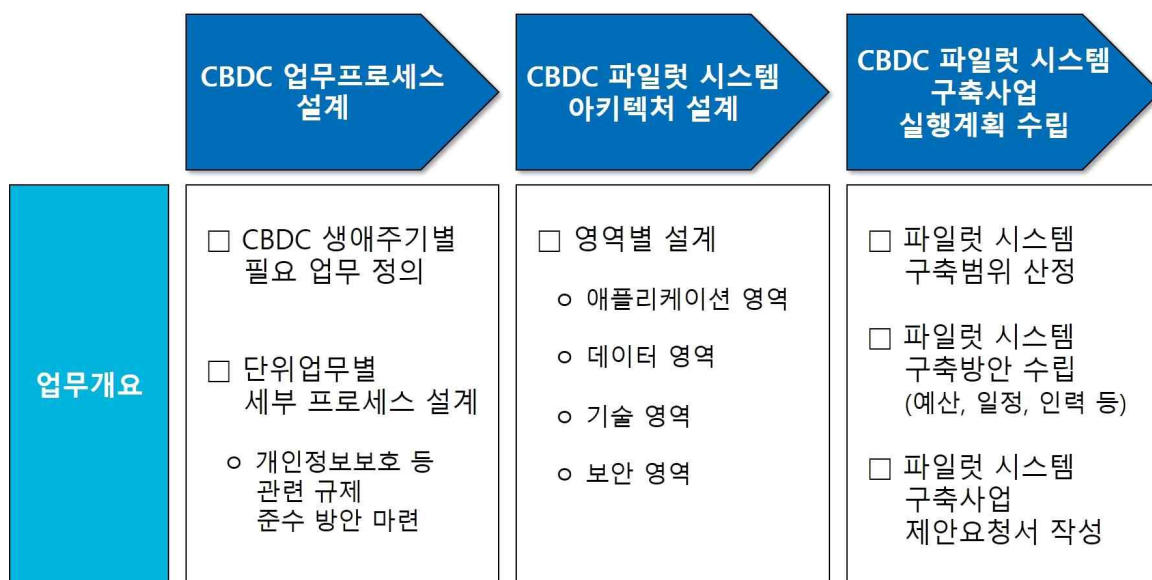
□ (목적) CBDC와 관련된 제도적, 기술적 필요사항 선제적 검토

□ (사업내용) 1단계\* 연구 결과('20.7월)를 기초로 CBDC 업무 프로세스 및 시스템 아키텍처\*\*를 설계하고 CBDC 파일럿 시스템 구축 사업('21년 예정)의 세부 실행계획을 마련

\* CBDC 기반업무(설계 및 요건 정의와 구현기술 검토)

\*\* 전산시스템의 구조, 동작 방식, 구성 요소 간 관계 등을 애플리케이션, 데이터 관리, 구현 기술, 보안 등의 관점에서 구조적으로 정리한 체계

### [ CBDC 파일럿 시스템 컨설팅 사업 범위 ]




## 5. 미국의 가상자산 프레임워크

<출처>  [Cryptocurrency: An Enforcement Framework](#) (美 법무부, '20.10월)

- **(개요)** 미국 법무부는 향후 가상자산을 다루는 데 있어 적용될 프레임워크를 발표
- **(사용 현황)** 가상자산에 관련된 안보 위협사항을 조사
  - **(불법 거래)** 불법 용품과 테러 지원 도구 구매, 테러 자금 마련, 강탈 및 갈취의 수단으로 사용
  - **(법적 의무 회피)** 자금을 세탁하고 탈세의 수단으로 사용되며 무허가 거래소를 운영
  - **(해킹 및 도난)** 전자지갑, 거래소 등을 공격하여 가상자산을 도난
- **(규제사항)** 미국 법무부가 관할권을 가질 수 있는 경우를 규정
  - 가상자산거래가 미국 내 금융, 데이터 서버, 기타 컴퓨터 시스템에 접근하거나 영향을 미칠 시
  - 가상자산을 이용해 불법 제품을 미국 내로 수입 시
  - 미국 국민을 사취하거나 도용할 수 있는 불법 서비스 제공 시
- **(해결전략)** 가상자산 위협 해결을 위한 전략을 제시
  - **(범죄 활동 저해)** 거래소 운영 조직은 FinCEN\* 규제 준수
    - \* Financial Crimes Enforcement Network : 미국 재무부 산하의 금융 범죄 단속 네트워크
  - **(익명성 저해)** 익명성 제공 가상자산\*의 사용을 고위험 활동으로 간주하고 기존 자금세탁 방지·테러 자금조달 규정을 우회하는 서비스 운영자에 형사 책임을 부과
    - \* 모네로(Monero), 대시(DASH), 지캐시(Zcash) 등

## 6. 중국의 CBDC 관련 암호법

<출처>  [중앙은행 디지털화폐 관련 중국 암호법의 시사점](#)  
(국회입법조사처, '20.11월)

□ **(개요)** 국회입법조사처는 디지털 위안화 발행의 법적 기반으로 평가받는 중국 암호법을 조사

□ **(중국 암호법)** 암호 기술에 대한 규제와 활성화 도모

○ **(목적)** 암호의 적용과 관리를 규제하고 암호산업의 발전을 촉진하며 네트워크, 정보, 국가안보 및 사회적 공익을 보호

○ **(핵심암호·일반암호\*)** 국가 기밀정보를 보호할 목적으로 중국 정부의 지도, 감독, 검사 등의 통제를 받음

\* 핵심암호는 '극비' 등급의 정보를, 일반암호는 '기밀' 등급의 정보를 보호

○ **(상용암호)** 국가 기밀이 아닌 정보를 보호하며 국민경제·생활, 공익 등과 관련될 때 인증기관의 인증을 받아야 함

□ **(시사점)** 중국 암호법의 시사점을 고찰

○ 우리나라는 상황에 따라 암호제품의 사용을 제한하고 암호 기술의 접근에 대해 조치할 수 있지만 적용 범위와 내용의 구체화 필요

○ 디지털화폐 관련 암호기술 사업을 지원하고 특히 확보 등을 통해 우리나라 지급 결제 시스템의 선진화 모색 필요

## 7. 국외 가상자산 시장 동향

<출처>  가상화폐 Update: 눈여겨볼 가상화폐 시장 이벤트(하이투자증권, '20.12월)

- **(개요)** 하이투자증권은 가상자산 시장의 동향과 전망을 조사
- **(동향)** 가상자산 시장의 동향 조사
  - **(디지털 위안)** 중국인민은행이 디지털 위안의 대규모 공개 시험을 시작하면서 국제 결제통화 입지를 강화
  - **(디엠(Diem) 출시)** 페이스북 주도 가상자산인 리브라(Libra)의 새 이름으로 달러화 연동 스테이블코인 방식으로 출시 계획
  - **(규제)** 주요 7개국(G7)\*에서 디지털자산에 대한 규제 필요성을 제기했으며 미국 통화감독청(OCC)은 규제 제정 중임을 발표
    - \* 미국, 영국, 프랑스, 독일, 이탈리아, 캐나다, 일본
  - **(거래 확대)**페이팔에서 가상자산의 매매 허용 및 법정화폐 환전을 통한 상품 구매를 가능하게 할 예정
- **(전망)** 가상자산에 대한 규제 강화 속에 가상자산 혹은 디지털 화폐에 대한 관심은 갈수록 증가
- **(시사점)** 가상자산이 점차 일상생활에 침투하며 거래 수단으로서 활용도가 높아질 수 있으며 새로운 자산군으로 부상할 가능성 존재




### Ⅲ. 언론 동향 (기사명 클릭 시 뉴스기사로 이동)

'20년 하반기 블록체인 관련 주요 기사를 서비스, 인증, 정책, 디지털화폐, 보안 분야 등으로 나누어 등록일 순으로 정리

#### < 블록체인 서비스 >

 [신한銀, 금융권 첫 DID 실명인증 ‘쫄’ 도입](#) (파이낸셜뉴스, 8.26.)

- 금융위 혁신금융서비스(규제샌드박스)로 지정된 분산ID(DID) 서비스로 비대면 실명확인 절차 간소화에 대한 특례 적용
- ‘쫄’ 발급 후 타 기관에 제출 시 비대면 실명확인 절차 반복 없이 지문만 확인하여 간편하게 제출 가능하며 신원정보 위·변조 여부는 블록체인으로 검증


 [부산 블록체인 통합서비스 ‘B PASS’ 출시... “플라스틱 카드 대체”](#)  
(서울경제, 10.27.)

- 부산 시민은 앱을 통해, 부산 거주 확인 자격증명, 모바일 방문증, 도서관 회원증, 비대면 공공기관 방문증 등 이용 가능
- 분산신원증명(DID) 연계 서비스를 추진하여 전자지갑의 활성화 목표

 [기업용 블록체인들, 내년 대거 상용화](#) (파이낸셜뉴스, 11.9.)

- 미국 시장조사업체 포레스터는 '21년에 글로벌 블록체인 프로젝트의 30%가 상용화에 들어갈 것으로 전망
- 대부분 클라우드 기반 기업용 블록체인 플랫폼으로 알리바바, IBM, 마이크로소프트, 오라클 등이 두각을 보일 것으로 예상

## < 블록체인 보안 >

 [사토시도 몰랐던 비트코인 ‘에러버스’ 공격, 대책 필요하다](#) (매일경제, 7.15.)

- 비트코인(BTC)에서 자금을 갈취하는 ‘에러버스’ 공격\* 취약점 발견
  - \* 공격자가 블록체인 네트워크에 ‘스파이 노드’를 서서히 침입시키며 장기간 숨어있다가 해당 노드를 완전히 차지하는 순간 자금을 갈취하는 공격법
- 가상자산 거래소, 채굴 네트워크 등 비트코인을 취급하는 곳이 모두 취약하므로 후속 패치 연구 필요

 [블록체인 노드에 디도스 공격 발생할 수 있어 주의 필요](#) (매일경제, 10.7.)

- 블록체인 노드 사이에 메시지를 주고받는 구조에서 분산 서비스 거부(DDoS) 공격 발생 가능
- 레이어 2 솔루션\* 사용 시 공격에 치명적이므로 주의 요구
  - \* 블록체인의 확장성 향상을 위해 블록체인 바깥에서 처리하는 레이어를 추가하는 방식

 [블록체인-개인정보보호규범 기술·제도적 해법 필요](#) (디지털타임스, 11.18.)

- 프라이빗 블록체인은 여러 노드가 분산해 책임을 지는 법적 구조가 복잡하며, 퍼블릭 블록체인은 네트워크에 참여하는 모든 노드에 공문을 보내거나 개발자에게 책임을 묻기 힘들
- 현재로서는 블록체인에 개인정보 기록이 불가능한 것이 중론으로 블록체인, 개인정보보호 간 사회적·기술적 틈을 만들 필요

## < 블록체인 기반 신원인증 >

### [진짜 ‘모바일 운전면허증’은 내년.. “카드 발급도 가능”](#) (ZDNet Korea, 6.23.)

- 이통사는 본인확인 자격을 가지고 있어 이를 활용해 등록된 운전면허 정보를 불러와 미성년자 확인, 운전 관련 서비스 등에 사용 가능
- 정부가 발급하는 모바일 운전면허증은 운전면허 정보와 함께 주민등록번호 등 신원정보도 함께 조회되어 용도 확대 가능

### [‘모바일 공무원증’ 내년 초 도입... 모바일 신분증 가속화](#) (연합뉴스, 10.26.)

- 행정안전부는 모바일 공무원증을 시작으로 운전면허증, 장애인 등록증 순으로 추진 계획
- 자기주권 개념 강화, 블록체인 기반 DID 기술적용, 온·오프라인을 통합한 디지털 신분증이란 점에서 획기적인 변화 예상

### [공인인증서 대체할 미래형 인증기술 특허출원 증가](#) (보안뉴스, 11.24.)

- 미래형 인증기술은 생체인식 및 DID 기술이 특허출원을 주도
- DID 기술 특허출원이 '19년 14건에서 '20.9월까지 36건으로 급증

### [커지는 사설인증 시장, 생체인증·블록체인·양자암호 주목](#) (글로벌이코노믹, 12.2.)

- FIDO, DID, 양자난수암호를 통한 신원증명 등 보안 신기술을 도입한 인증 서비스가 확대될 것으로 예상
- 블록체인을 활용한 DID는 신원주체가 정보의 이용에 직접 관여·통제하고 블록체인을 활용해 빠른 위·변조 여부 검증이 가능

## < 블록체인 정책 >

 [‘민관 합동 DID 협의체’ 출범...블록체인 활성화 앞당긴다](#) (아주경제, 7.16.)

- 과학기술정보통신부는 민관합동 DID 협의체의 출범을 통해 DID 생태계 육성을 본격화한다는 방침
- 시스템 간 호환 등 연동을 통해 국민들이 DID 적용 서비스를 편리하게 이용할 수 있도록 하는 취지로 협의체를 구성

## < 디지털화폐 >

 [인민은행, 디지털 위안화 소매 현장 지불 준비](#) (ZDNet Korea, 11.16.)

- 중국인민은행은 위챗, 알리페이 같은 지불 서비스가 ‘지갑’ 역할을, 디지털 위안화가 ‘돈’ 역할을 한다고 설명함
- 지불 기업들이 디지털 위안화 지갑 운영을 맡으면서 인민은행의 지불 체인에 들어가 지불 서비스 수수료를 받게 될 전망

 [美 Fed도 ‘디지털화폐’ 발행 본격 검토](#) (문화일보, 11.17.)

- 중국이 ‘디지털 위안화’ 발행에 박차를 가하자 미국 연방준비제도(Fed)가 디지털화폐를 발행하지 않겠다는 견해를 선회하고 발행 본격 검토
- 본격적인 글로벌 新통화 패권전쟁이 시작될 것으로 예상

 [한은 “오프라인에서도 결제 가능한 CBDC 연구 중”](#) (IT조선, 11.20.)

- 한국은행은 인터넷이 있어야 사용 가능한 간편결제와 달리 CBDC는 오프라인에서도 결제할 수 있어야 한다는 전제를 가지고 연구 중
- 한국은행 내부적으로 원칙을 만들었고 이를 토대로 설계하고 테스트하는 단계로 CBDC가 발행되는 단계가 아님을 강조


## IV. 주요 행사 [행사명 클릭 시 홈페이지로 이동]

'21년 상반기 개최 예정인 블록체인 관련 주요 행사를 개최일 순으로 소개

※ 코로나19 확산으로 인해 행사가 연기 또는 취소될 수 있음

 [AIBC summit - malta](#) (몰타, '21.2.17.~18.)

- **(주요내용)** AI, 블록체인 및 기타 신흥 기술에 대한 전문가들의 강연과 컨퍼런스 및 워크숍 진행

 [IEEE International Conference on Blockchain and Cryptocurrency](#)  
(온라인, '21.3.3.~6.)

- **(주요내용)** 블록체인과 가상자산에 대한 최신 기술 보고서와 규제, 정책, 표준 등을 주제로 논문 및 포스터 발표 등 진행

 [World Crypto-Bitcoin, Blockchain and Cyber-Security](#) (캐나다, '21.3.4.~5.)

- **(주요내용)** 전문가와 새로운 블록체인과 비트코인의 연구 결과 논의 및 아이디어와 최근 개발사항 교환

 [Blockchain Week Rome](#) (이탈리아, '21.3.9.~13.)

- **(주요내용)** 전문가·기업 경영진의 연설, 전시회 관람, 기업 미팅

 [Blockchain Expo Virtual 2021](#) (온라인, '21.3.17.~18.)

- **(주요내용)** 금융 서비스를 포함한 블록체인 생태계에 대한 전문가 기조연설, 패널 토론 및 솔루션 기반 사례 연구 발표



 [Blockchain Africa Conference 2021](#) (남아프리카공화국, '21.3.18.~19.)

- **(주요내용)** 블록체인 기술과 가상화폐가 개인, 정부, 스타트업, 기업 등에 어떻게 기회와 혜택을 제공하는지에 대해 발표

 [International Conference on Blockchain Technology](#) (중국, '21.3.26.~28.)

- **(주요내용)** 전문가의 기조연설 및 연구 성과 공유 및 발표 등

 [Blockchain Summit London](#) (영국, '21.6월 중)

- **(주요내용)** 강연자와 차세대 공급업체가 최신 산업 및 블록체인 혁신에 대해 토론하고 시연

## [특집1] 블록체인 금융[가상자산, 디파이(DeFi), CBDC] 동향

가상자산과 더불어 최근 주목받고 있는 디파이(가상자산 기반 탈중앙 금융서비스), CBDC(중앙은행 디지털화폐)에 대해 특성 및 보안 이슈를 조사

### 1. 가상자산(Virtual Assets)

#### □ (개요) 전자적으로 거래·이전될 수 있는 자산을 의미

※ '19.2월부터 자금세탁방지기구(FATF)에서 가상자산(Virtual Assets)이라는 통일된 용어를 사용하며, 국내 특정금융정보법(20.3.24 개정)에서도 가상자산으로 정의

[ 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제2조(정의) ]

3. "가상자산"이란 경제적 가치를 지닌 것으로서 전자적으로 거래 또는 이전될 수 있는 전자적 증표(그에 관한 일체의 권리를 포함한다)를 말한다. 다만, 다음 각 목의 어느 하나에 해당하는 것은 제외한다.

가. 화폐·채화·용역 등으로 교환될 수 없는 전자적 증표 또는 그 증표에 관한 정보로서 발행인이 사용처와 그 용도를 제한한 것

나. 「게임산업진흥에 관한 법률」 제32조제1항제7호에 따른 게임물의 이용을 통하여 획득한 유·무형의 결과물

다. 「전자금융거래법」 제2조제14호에 따른 선불전자지급수단 및 같은 조 제15호에 따른 전자화폐

라. 「주식·사채 등의 전자등록에 관한 법률」 제2조제4호에 따른 전자등록주식등

마. 「전자어음의 발행 및 유통에 관한 법률」 제2조제2호에 따른 전자어음

바. 「상법」 제862조에 따른 전자선하증권

사. 거래의 형태와 특성을 고려하여 대통령령으로 정하는 것

#### □ (특성) 중개자 없이 가상자산 거래 내용을 분산원장(블록체인)에 저장하여 무결성을 보장

○ 단, 사용자의 거래 편의를 위한 가상자산 거래소 존재

□ **(분류)** 독립된 블록체인 네트워크 유무에 따라 코인 또는 토큰으로 분류

○ **(코인\*)** 독립된 블록체인 네트워크(메인넷) 기반의 가상자산

\* 예 : 비트코인(BTC), 이더리움(ETH)

○ **(토큰\*)** 타 블록체인 네트워크를 기반으로 생성된 가상자산으로 대체 가능 토큰(FT)과 대체 불가 토큰(NFT)으로 분류 가능

\* 예 : 이오스(EOS)는 이더리움 기반 토큰이었으나, '18.6월 메인넷 출시로 코인으로 분류

- **(대체 가능 토큰\*)** 현금과 같이 가치가 동일하여 대체 가능한 토큰

\* FT: Fungible Token

※ 가상자산 거래소에서 구입한 토큰 1개는 다른 토큰 1개로 대체 가능

- **(대체 불가 토큰\*)** 고유한 정보를 가져 대체 불가능한 토큰으로 소유자가 명시된 것이 특징

\* NFT: Non-Fungible Token

※ 예 : 각각의 고양이는 모두 고유 특성이 있어 다른 고양이로 대체 불가

[ 대체 가능 토큰(FT) 및 대체 불가 토큰(NFT) 비교 ]

	FT	NFT
상호교환성	O	X
분할성	O (예 : 0.001 토큰)	X
소유자 명시	X	O
활용	송금, 거래	자산 소유권 보장

□ **(현황)** 5,000가지 이상의 가상자산이 거래 중

○ 유명 가상자산이 대부분의 거래량을 차지\*

\* '20.3분기 기준 비트코인 62.3%, 이더리움 12.7%

○ 일부 가상자산은 거래량 부족, 문제 발생\* 등으로 상장폐지됨

\* 시세 및 거래량 조작, 가상자산 임의 발행, 개발사 파산 등

○ 사기 목적의 스캠 코인\*에 유의 필요

\* 거짓 홍보로 투자자금을 모은 뒤 잠적

- **(분실)** 가상자산을 보관하는 전자지갑의 개인키 분실 시 가상자산의 소유권을 증명할 수 없는 문제 발생

[ 가상자산 분실 주요 사례 ]

- 비트코인 소유자가 갑작스럽게 사망하면서 개인키를 모르는 가족은 비트코인에 접근할 수 없게 되었으며 사망자의 비트코인 개수 또한 파악 불가('13년)
- 가상자산 거래소 직원이 개인키를 분실하여 60억 원 상당 가상자산에 접근할 수 없어 거래소가 파산됨('19년)

- 거래소에서는 **개인키 복구 메커니즘\***을 지원 중이며 금융사에서는 안전한 가상자산 보관을 위한 **커스터디(수탁) 서비스** 검토 중

\* 장문의 복구 단어를 입력하여 암호학적으로 개인키를 복구

- **(공격)** 공격자는 사용자 및 가상자산 거래소 직원 등을 대상으로 해킹을 시도하여 **개인키 탈취 등을 통해 가상자산을 송금**

※ 사용자의 개인키 또한 가상자산 거래소에 저장되어 있는 경우가 대부분으로 사용자는 비밀번호 및 OTP 등으로 거래소에 로그인 후 개인키 사용

- 해킹으로 인한 가상자산 무단 송금 사실을 인지하더라도 이를 중단할 수 없어\* 피해는 더욱 심각

\* 중개자가 없는 가상자산 특성상 누가 정당한 개인키 소유자인지 구별 불가

- 국회입법조사처는 ISMS 이외에 가상자산 거래소 보호 방안이 필요하다고 평가('20.8월)

## 2. 디파이(DeFi)

- (개요) 탈중앙화 금융(Decentralized Finance)의 약자로 중개자 없는 금융서비스 관련 프로젝트를 통칭
- (특성) 이자지급, 담보대출 등 전통 금융서비스를 가상자산에서도 제공
  - 블록체인 기반의 스마트 계약을 활용하여 구현함으로써 중개자 없이도 금융서비스의 무결성 및 투명성을 확보
    - ※ 스마트 계약을 최초로 지원한 이더리움이 디파이 생태계를 지탱 중
- (동작 방식) 스마트 계약 코드를 호출하여 가상자산 기반 거래를 자동으로 수행
  - ※ 무분별한 실행(불필요한 자원 낭비)을 방지하기 위해 스마트 계약 호출 시 수수료를 가상자산으로 지불

### [ 스마트 계약 기반 가상자산 송금 예시 ]

```
/* Send coins */  
function transfer(address _to, uint256 _value) public {  
    require(balanceOf[msg.sender] >= _value); // Check if the sender has enough  
    require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows  
    balanceOf[msg.sender] -= _value; // Subtract from the sender  
    balanceOf[_to] += _value; // Add the same to the recipient  
}
```

- 법정화폐(달러화), 실물자산\*(주식, 금) 등과 연동 가능
  - \* 실물자산의 소유권을 기록한 대체 불가 토큰(Non-Fungible Token, NFT) 발행
- (생태계) 스테이블코인, 대출, 탈중앙거래소 등의 프로젝트 진행 중
  - (스테이블코인) 가격 변동성을 최소화하는 가상자산으로 ①법정화폐 담보, ②가상자산 담보, ③알고리즘 기반으로 분류 가능



## [ 스테이블코인 분류 ]

분류	스테이블코인 발행 방식
법정화폐 담보	법정화폐를 담보로 스테이블코인을 발행 (법정화폐 담보 보유분을 투명하게 공개)
가상자산 담보	타 가상자산(이더리움 등)을 담보로 법정화폐 가치와 연동되는 스테이블코인을 발행
알고리즘 기반	알고리즘 기반으로 스테이블코인을 발행 또는 회수 (코인 공급량을 조절하여 코인 가격을 일정하게 유지)

- **(대출)** 이더리움 등을 담보로 달러화 연동 스테이블코인을 대출  
※ 자산의 공급·수요에 기초한 스마트 계약 알고리즘으로 대출이자를 자동으로 결정
- **(탈중앙거래소\*)** P2P 방식으로 가상자산을 교환하는 거래 플랫폼으로  
거래소 개입 없이 개인이 직접 자산을 관리

\* Decentralized Exchange (DEX)

- **(현황)** 디파이 내 담보로 잡혀있는 자산이 '20.6월부터 증가하여  
145억 달러 상단에 육박

※ '20.11월부터 이더리움 담보량은 줄어들었으나 시세 상승으로 담보 가치 또한 상승

Total Value Locked (USD) in DeFi



ETH Locked in DeFi



※ [출처] 오픈 커뮤니티(DeFi Pulse), 2020.12.

- **(공격 사례)** '20년, 가상자산 6,000만 달러 이상이 공격으로 탈취

- ① **(플래시 론)** 자산 간 대량 교환으로 가치 변동\*을 일으켜 차익  
편취('20.2월 당시 100만 달러 상당, '20.10월 당시 3,400만 달러 상당)

\* 이더리움 - 비트코인 교환 비율, 스테이블코인 가격 폭등 등

- **(문제점)** 특정 플랫폼 내 낮은 가상자산 유동성, 가상자산  
시세 데이터를 외부 네트워크 한 곳에 의존한 제도적 문제

- **(대응조치)** 급격한 교환 비율 변동 시 거래 취소, 가상자산 시세 데이터를 다양한 곳에서 반영

② **(제로-비드)** 3만 이더리움(당시 24만 달러 상당)을 **1달러 미만에 낙찰**(’20.3월)

[ 제로-비드(zero-bid) 공격 발생 흐름 ]

- 1) 이더리움 시세 약 60% 급락(194달러→80달러 대), 이더리움 네트워크 마비
- 2) 대출 담보인 이더리움 자산 가치가 낮아져 대규모 강제 청산 위기
- 3) 대출 상환을 위한 스테이블코인 수요 증가로 시세 상승 및 구입 어려움
- 4) 스테이블코인으로 상환하지 못하여 대규모 담보 경매(강제 청산) 진행
- 5) 공격자는 더 비싼 경매 수수료를 지불하여 담보 경매에 응찰
- 6) 네트워크 마비로 인한 경매 입찰자 부족으로 공격자는 1달러 미만에 담보 낙찰

- **(대응조치)** 스테이블코인을 담보로 추가하여 시세 변동에 따른 강제 청산 위험을 최소화

③ **(스마트 계약)** 스마트 계약 코드의 보안 취약점으로 가상자산 탈취 또는 시세 조작으로 차익 편취

- **(무제한 출금)** 대출 서비스의 스마트 계약 내 출금 코드에 재진입하여 가상자산 탈취(’20.4월 당시 2,500만 달러 상당)
- **(시세조작)** 가상자산 소각 코드를 반복 호출하여 시세 급등 후 차익 편취(’20.6월 당시 45만 달러 상당)
- **(대응조치)** 기존 스마트 계약 폐기 후 새로운 스마트 계약 구동

□ **(전망)** 디파이에 실물자산(부동산, 화물 송장 등)이 결합되어 성장 예상

- 단, 디파이의 기술적\* 및 제도적\*\* 문제를 해결할 필요

\* 스마트 계약 코드의 취약점으로 인한 해킹

\*\* 낮은 가상자산 유동성, 블록체인 내부·외부 데이터의 불일치

- 또한, 디파이 관련 법률적 이슈\*를 고려할 필요

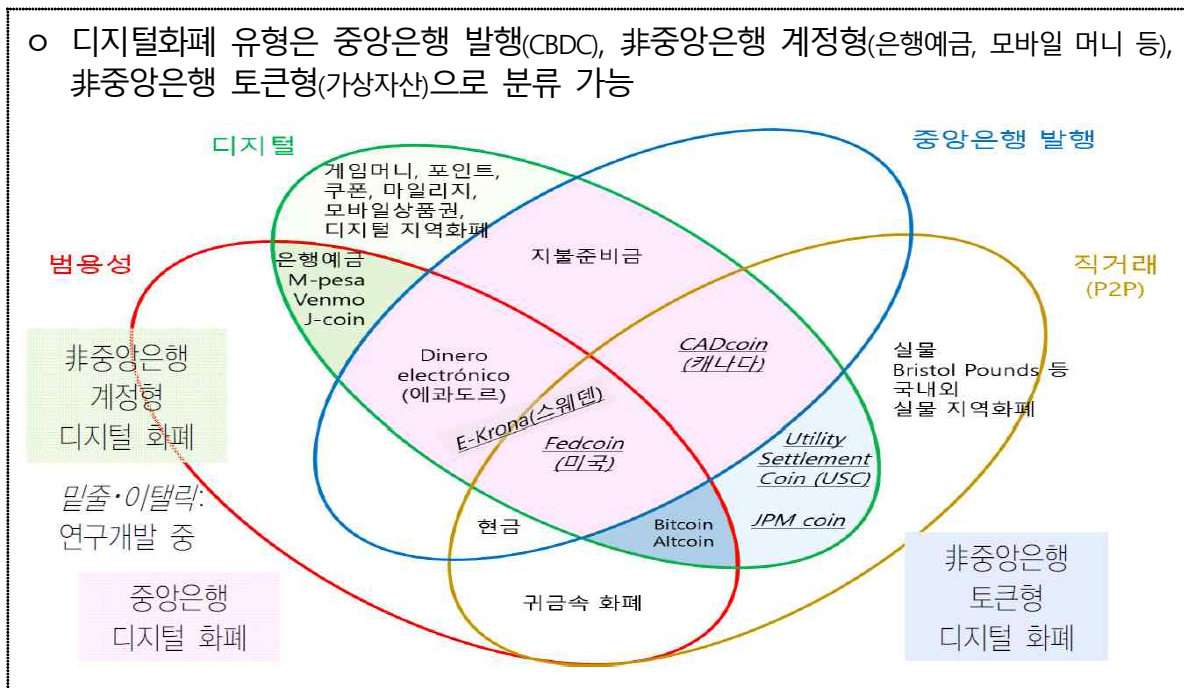
\* 중개자가 없는 디파이에서 기존 법령 적용이 어려움, 이용자 본인 식별 필요

### 3. 중앙은행 디지털화폐(CBDC)

□ (개요) 지급준비금·결제성 예금과 별도로 중앙은행이 발행하는 전자적 형태의 화폐

○ 법정화폐와 1:1 교환이 보장된다는 점에서 가상자산과 구분

#### [ 국제결제은행(BIS)의 3가지 디지털화폐 유형 ]



※ [출처] KDB미래전략연구소, 국제결제은행의 화폐 분류에 따른 디지털 화폐의 유형별 특징 및 시사점, 2019.5.

□ (특성) 거래의 ①익명성을 제한할 수 있으며 정책 목적에 따라 ②이자 지급, ③보유 한도 설정, ④이용 시간의 조절 가능

#### [ 현금, 기존 중앙은행 예금, CBDC 간 특성 비교 ]

	현금	기존 중앙은행 예금	CBDC
거래 익명성	보장	없음	보장 여부 선택 가능
이자 지급	불가능	가능	가능
보유 한도	없음	없음	설정 가능
이용 시간	제한 없음	제한	설정 가능

※ [출처] 한국은행, 중앙은행 디지털화폐, 2019.1.

□ **(발행목적)** 법정화폐 위상 제고, 자금세탁방지, 현금사용량 감소 대비, 공공 결제수단 확보 등 국가별 상이

□ **(이용목적)** 소액결제용 CBDC와 거액결제용 CBDC로 구분

○ **(소액결제용)** 모든 경제주체(개인, 기업 등) 이용 가능

※ 추진 국가 : 스위스, 싱가포르, 일본-ECB, 캐나다, 태국-홍콩, 프랑스

○ **(거액결제용)** 은행 등 금융기관 위주로 이용 가능

※ 추진 국가 : 노르웨이, 동카리브, 바하마, 스웨덴, 영국, 중국

□ **(구현방식)** 단일원장방식(계좌기반)과 분산원장방식(토큰기반)으로 구분

○ **(단일원장방식)** 중앙은행 또는 은행이 CBDC 계좌 및 관련 거래정보를 보관·관리하는 방식

○ **(분산원장방식)** 다수가 동일한 거래기록을 관리하는 방식으로 허가형(일부 참여자만 참여 가능) 및 비허가형(누구나 참여 가능)으로 분류

[ 구현방식 간 특성 비교 ]

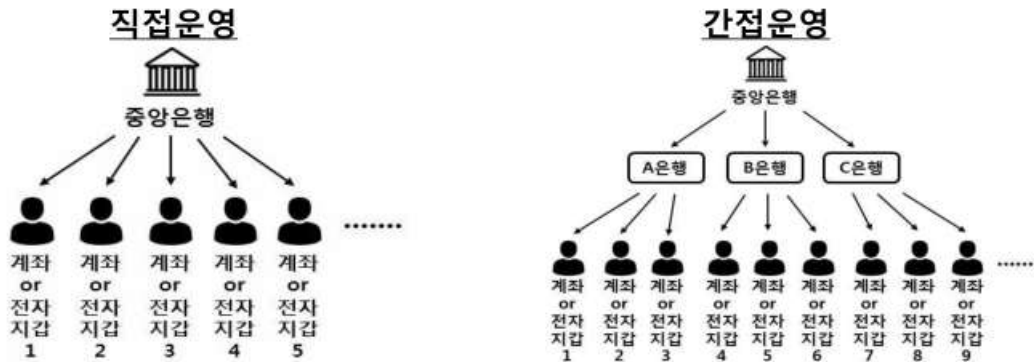
구분	단일원장방식	분산원장방식	
		허가형	비허가형
원장보유 주체	단일 주체	복수의 참여자(노드)	
거래검증·원장관리권한	제한	제한 없음	
결제완결성* 보장	가능	불가능	
적용 예시	지준예치금, 은행예금, <u>CBDC</u>	<u>CBDC</u>	비트코인, 이더리움
신뢰의 원천	은행·중앙은행에 대한 법적 규제 및 평판	원장관리 노드에 대한 법적 규제 및 평판	거래검증 및 원장관리 개방성과 경제적 유인체계

\* 거래당사자 간 지급·결제가 이루어진 후 이를 되돌릴 수 없도록 법적으로 보장하는 것으로 CBDC도 현금과 같이 결제완결성이 보장되어야 함

※ [출처] 한국은행, 중앙은행 디지털화폐, 2019.1.

- **(운영방식)** 고객 업무의 수행주체에 따라 직접 운영(중앙은행) 및 간접 운영(은행 등 위탁)으로 구분

[ CBDC 운영 방식 ]



※ [출처] 한국은행, 중앙은행 디지털화폐, 2019.1.

- **(현황)** 전 세계 중앙은행의 80%가 연구·실험 및 파일럿 프로그램 진행
- **(한국)** CBDC 컨설팅 사업자를 선정하고 관련 작업에 착수했으며 가상환경에서 CBDC 실험 유통 예정
  - **(중국)** 홍콩에서 대규모 공개시험을 시작할 예정으로 인터넷이 연결되지 않은 상황에서도 거래가 잘 이뤄지는지 함께 시험
  - **(미국)** 소규모 기술 테스트 진행 및 가상의 CBDC 개발 연구 수행
  - **(유럽)** ‘디지털유로’ 상표등록 출원('20.9월) 및 '21년 도입 여부 결정 예정
  - **(싱가포르)** ‘프로젝트 우빈(Ubin)’을 통해 분산원장 기반의 결제 플랫폼을 국가 단위로 구축하고 도매용 CBDC 개발 중
  - **(사우디아라비아·UAE)** 공동실험을 통해 개발한 CBDC 출시 예정으로 타 국가와 네트워크 연결 가능성을 언급
- **(보안)** 각 국에서는 구현방식 및 운영방식별 CBDC 운영, 기밀성, 무결성, 접근성, 사이버 공격 대응 요구사항 등 보안연구 진행

※ 중국인민은행은 '2020년 중국금융안정보고서('20.11월)'에서 분산원장은 체계적인 보안 부족, 거래 취소 불가 등의 이유로 CBDC에는 부적합하다는 의견 제시

#### 4. 가상자산/디파이, CBDC, 간편결제 간 비교

□ (가상자산/디파이) 중개자 없이 가상자산 기반의 전통 금융서비스\* 제공

\* 이자지급, 담보대출 등

□ (CBDC) 중앙은행이 발행하며 법정화폐와 1:1 교환 보장

□ (간편결제) 핀테크업체 등에서 구매자와 판매자를 중계하는 결제 시스템 제공

[ 디파이, CBDC 간 특성 비교 ]

	가상자산(디파이)	CBDC	간편결제
중개자	블록체인 네트워크	중앙은행(직접운영), 금융사(간접운영)	핀테크업체 등
자산의 발행	블록체인 프로토콜	중앙은행	-
자산의 관리	개인 (전자지갑)	중앙은행 (금융사 위임 가능)	핀테크업체 (자산 예치)
거래 지역	제약 없음	국가(또는 관할권) 내	국가(또는 관할권) 내 (제휴 서비스 한정)
거래 익명성	보장	보장 여부 선택 가능	보장 불가

## < 참고문헌 >

- [1] Forbes Advisor, What Is Cryptocurrency?, 2020.11.  
<https://www.forbes.com/advisor/investing/what-is-cryptocurrency>
- [2] 팩스넷뉴스, 글로벌 금융사 '커스터디 진출 러시' 국내 은행도 합류, 2020.7.  
<https://paxnetnews.com/articles/63389>
- [3] 국회입법조사처, 2020 국정감사 이슈 분석 제8권, 2020.8.
- [4] SK증권, 디파이(DeFi)에 대해 알아보자, 2020.9.
- [5] KB금융지주 경영연구소, 모두를 위한 자유로운 금융서비스 디파이(DeFi), 2020.10.
- [6] 중앙일보, 디파이 열풍은 스쳐지나가는 것이 아닌 시대적 요청, 2020.10.  
<https://news.joins.com/article/23897102>
- [7] CoinGecko, 2020 Q1 Cryptocurrency Report, 2020.4.
- [8] ConsenSys Codefi, The Q2 2020 DeFi Report, 2020.7.
- [9] ConsenSys Codefi, The Q3 2020 DeFi Report, 2020.10.
- [10] PeckShield, Balancer Hacks: Root Cause and Loss Analysis, 2020.6.  
<https://peckshield.medium.com/balancer-hacks-root-cause-and-loss-analysis-4916f7f0fff5>
- [11] DeFi Pulse, 2020.12. <https://defipulse.com>
- [12] 한국은행, 중앙은행 디지털화폐, 2019.1.
- [13] 한국은행, 해외 중앙은행의 CBDC 추진 현황, 2020.5.
- [14] 한국은행, 중앙은행 디지털화폐 파일럿 시스템 컨설팅 사업 추진, 2020.8.
- [15] KDB미래전략연구소, 국제결제은행의 화폐 분류에 따른 디지털 화폐의 유형별 특징 및 시사점, 2019.5.
- [16] 이코노믹리뷰, 화폐전쟁 2R 디지털 통화 선점경쟁 불붙었다, 2020.10.  
<https://www.econovill.com/news/articleView.html?idxno=501336>
- [17] UPI뉴스, 중국 중앙은행 CBDC 블록체인 기반 아닐 수 있다, 2020.11.  
<https://www.upinews.kr/newsView/upi202011120023>
- [18] 아주경제, [현금 없이도 산다] ①시동 건 디지털화폐 개발...세계 각국 어디까지 왔나, 2020.12. <https://www.ajunews.com/view/20201210145359114>
- [19] IT 조선, CBDC 전쟁 준비하는 中...韓·美은 뒷단서 연구 박차, 2020.12.  
[http://it.chosun.com/site/data/html\\_dir/2020/12/10/2020121002554.html](http://it.chosun.com/site/data/html_dir/2020/12/10/2020121002554.html)



## [특집2] 분산ID 환경에서의 개인정보 보호 대책

### 1. 개인정보 보호 위협 조사·분석

#### □ 분산ID 환경에서의 개인정보 보호 위협

- (1) **(개인정보 수집·저장 관련 위협)** 수집 목적에 따른 최소성의 원칙 위배 가능성, 소유자의 동의 없는 목적 범위를 초과한 개인정보 처리, 부적절한 개인정보 저장 위치 설정
- (2) **(개인정보 이용·제공 관련 위협)** 발급자 또는 검증자가 소유자의 정보를 수집 목적에서 벗어난 범위 이용, 소유자의 사전 동의 없이 소유자의 개인정보를 제3자에게 제공
- (3) **(개인정보 관리 위협)** 식별정보 또는 여러 가지 인증정보에 대한 기술적인 보호 조치 미흡, 부적절한 비식별조치

### 2. 신원증명 환경에서의 개인정보 보호 기술

#### ① 영지식 증명(ZKP, Zero-Knowledge Proof)\*

\* 증명자가 상대방에게 자신의 비밀정보를 노출시키지 않고 '자신이 비밀정보를 알고 있다는 것을 증명'하는 암호 기술

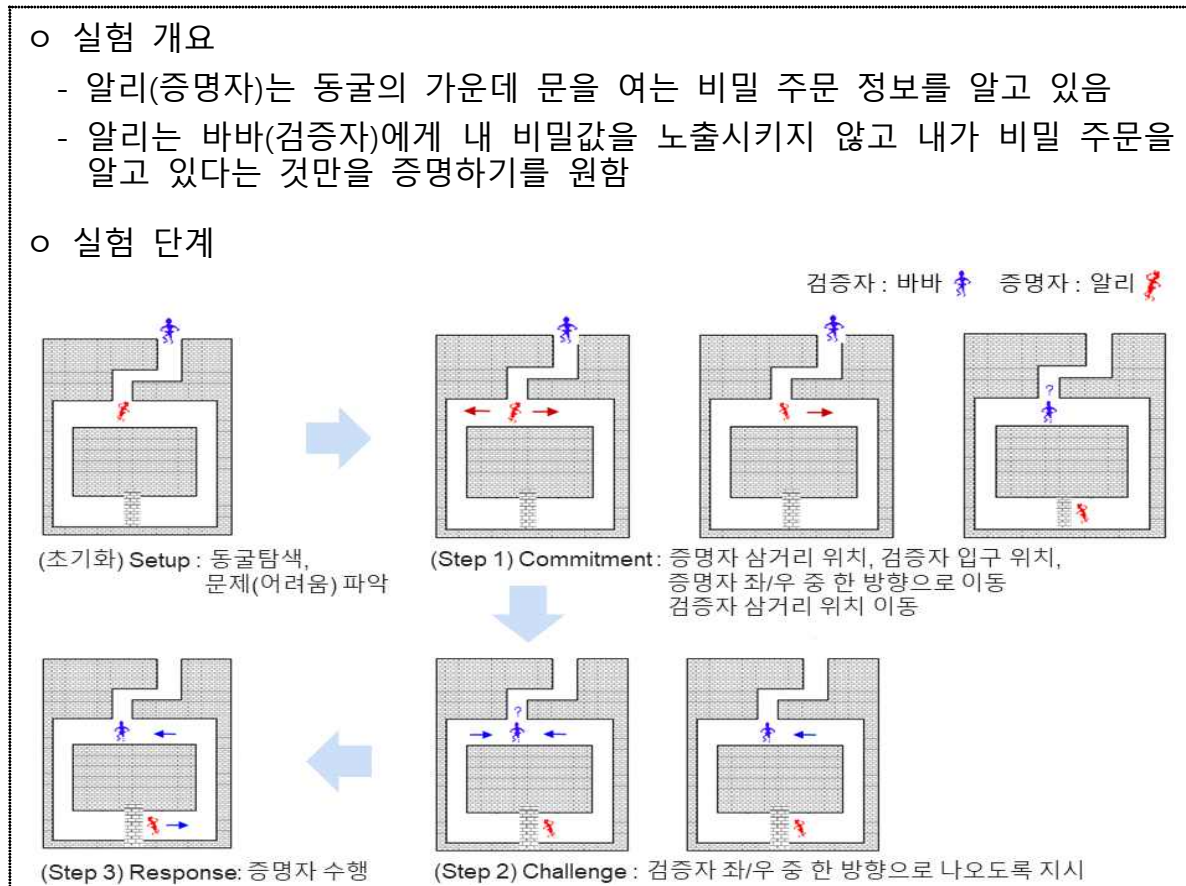
##### (1) 영지식 증명의 구성 요소

- **(ZKP-증명자)** 영지식 증명에서 자신이 가지고 있는 어떤 문장이 참이라는 사실을 증명하고자 하는 개체
- **(ZKP-검증자)** 영지식 증명에서 어떤 문장이 참이라고 주장하는 ZKP-증명자의 주장을 확인하는 개체

## (2) 영지식 증명의 동작 원리

- ①초기화(setup), ②위임(commitment), ③요청(challenge), ④응답(response)
- 대표적인 예 : 이상한 동굴에 대한 사고 실험

### [ 영지식 증명을 위한 동굴 실험 ]



- 완전성<sup>1)</sup>, 건전성<sup>2)</sup>, 영지식성<sup>3)</sup> 만족 필요

- 1) 증명자는 증명에 실패하지 않음(completeness)
- 2) 거짓 증명자는 증명에 성공하지 못함(soundness)
- 3) 비밀 지식에 대한 정보 노출이 없음을 보장(zero-knowledge property)

## (3) 영지식 증명 기법

- Schnorr ZKP, Fiat-Shamir ZKP, Feige-Fiat-Shamir ZKP 등이 대표적인 영지식 증명 기법임
- 메시지 통신 형태에 따라서 상호적 영지식 증명(interactive ZK)과 비상호적 영지식 증명 기법(non-interactive ZK, NIZK)으로 구분

- 최근 영지식 증명 기법은 검증 가능한 계산(Verifiable Computation) 기법과 결합하여 연구개발 중으로 대표적으로 zk-SNARKs, zk-STARKs, Bulletproofs가 알려짐
- 영지식 증명 기법은 범위 증명(Range Proofs), 셋 멤버십(Set Membership), OR, AND, 일반 연산 등을 효과적으로 지원해 주므로 신원증명과 결합되어 활용될 수 있음

## 2 선택적 노출(selective disclosure)\*

\* 어떤 정보를 공유할지에 대해 소유자가 세분화된 결정을 내릴 수 있는 능력

(1) **(구성 요소)** 기본 시스템으로 발급자, 소유자, 검증자로 구성되는 분산ID 관리 시스템을 고려할 수 있음

- **(W3C 검증 가능한 크리덴셜(vc))** 선택적 노출 기술을 실행하기 위한 핵심 데이터 모델의 주요 개념과 구조

[ 선택적 노출 증명을 위한 핵심 데이터 모델 개념 ]

데이터	설명	구조
클레임	주체(subject)의 속성에 대한 정보를 설명	
크리덴셜	동일한 개체에 대한 하나 이상의 클레임의 집합. 크리덴셜에는 발급자, 유효기간, 공개키 등과 같은 크리덴셜의 속성을 설명하는 메타데이터도 포함 가능	
검증 가능한 크리덴셜	위·변조 사실을 암호학적으로 검증할 수 있는 크리덴셜. (정보 주체에 대한 클레임과 해당 크리덴셜을 해석해주는 메타데이터 그리고 이를 검증해주는 암호학적 요소들이 포함된 증명들로 구성) 예. 전자직원신분증, 전자 출생 증명서, 전자 교육 증명서 등	
프레젠테이션	하나 이상의 발급자로부터 제공 받은 다수의 크리덴셜 또는 변형된 크리덴셜 집합	
검증 가능한 프레젠테이션	위·변조 사실이 암호학적으로 검증 가능한 프레젠테이션	

(2) **(선택적 노출 증명)** 발급자, 소유자, 검증자의 상호 독립적 또는 의존적이며 유기적인 관계에 의해서 제공 가능

- TTP(신뢰 가능한 제3자) 개입 시: PMI와 MS의 Cardspace 등
- TTP 비개입 시: 분산ID 관리 시스템, (W3C) VC 데이터 모델, 영지식 증명 기술 결합

(3) **(속성인증)** TTP가 개입되는 선택적 노출 증명의 예로 속성인증 개념인 PMI(Privilege Management Infrastructure)\* 고려 가능

\* 권한 관련 자원과 소유자 간의 관계를 인증기관이 인증하고 유지하는 구조로 신원의 세부 속성(예 : 체류허가(비자) 소유 등)과 결합 가능

- PKI(공개 키 기반 구조)는 주로 사용자의 신원을 확인하는 역할, PMI는 사용자의 권한을 확인하는 역할임

※ 예 : PKI는 여권, PMI는 비자 역할

#### [ PKI와 PMI의 비교 ]

구분	PKI	PMI
역할	- 사용자의 신원을 확인 - 여권과 같은 의미	- 사용자의 권한을 확인 - 비자와 같은 의미
repository	- 인증기관과 등록기관 관리 - X.509 포맷	- 별도의 권한 처리 기관 또는 기업 내부 부서
공통점	- 비대칭키를 사용한 검증 - 제3의 기관에서 공신력 제공 - 개인별 인증. 저장을 위한 객체 관리	

- PMI와 분산ID의 구성 요소는 유사함

#### [ PMI와 분산ID의 구성 요소 간 유사성 비교 ]

PMI	분산ID
속성 권한 (source of authority, attribute authority)	발급자(issuer)
소유자(holder)	소유자(holder)
권한 검증자 (privilege verifier)	검증자(verifier)
속성인증서 (attribute certificate)	검증 가능한 크리덴셜 (verifiable credential)

### 3. 분산ID 환경에 적합한 개인정보 보호 대책

#### □ 분산ID 환경에 적합한 영지식 증명 시나리오 연구

##### ○ 퀘딧(QEDIT)

- 분산 네트워크 환경에서 영지식 증명을 사용하여 자산을 전송 시 기밀 유지 솔루션 제공함
- 정보를 비공개 상태로 유지하면서 전체 생태계 내에서 공급 관리망 설정이 가능하며 중요한 자산은 완전한 비공개 발행으로 제공됨
- VMware는 퀘딧(QEDIT)과 협력하여 개인정보보호 측면이 강화된 블록체인 기술 개발

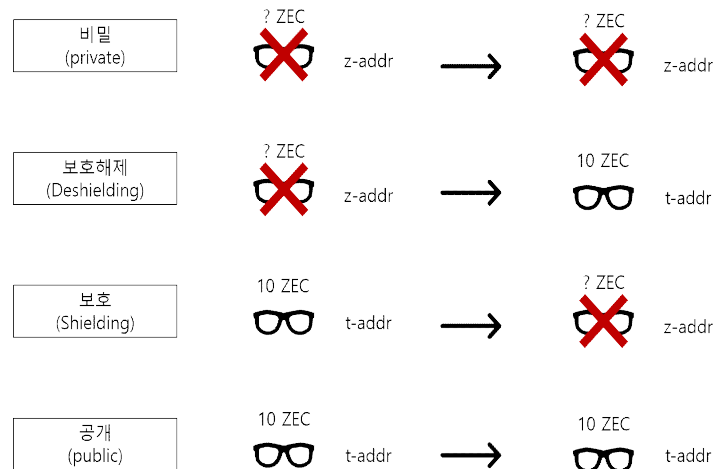
##### ○ 딜로이트(Deloitte)

- 퀘딧과 제휴하여 자체 기업용 블록체인 서비스 Eduscript에 회계 처리에 영지식 증명 기술 적용
- 블록체인이 자신의 교육 및 경력 데이터를 어떻게 공유할 수 있는지 사용자에게 보다 많은 개인정보 통제권 부여
- 조직은 직원의 자격 신빙성을 신뢰하는 동시에 기본 데이터의 완전한 개인정보 보호를 보존하고 규제 컴플라이언스를 유지함

##### ○ 지캐시 재단(Zcash Foundation)

- 영지식 증명 기법 중 하나인 zk-SNARK를 이용하여 내역이 공개되는 t-addr와 비밀이 보장되는 z-addr 두 가지 종류의 주소를 제공받아 거래하는 방식을 취함
- 거래 과정 중에 보내는 사람, 받는 사람뿐 아니라 거래되는 금액에 대한 정보가 노출되지 않으나 거래의 유효성을 거래 당사자들 외에도 다른 노드들에게 검증 가능

[ 지캐시를 이용한 거래 방식의 종류(출처 : 지캐시) ]



□ 분산ID 환경에 적합한 선택적 노출 시나리오 연구

- (SKT(이니셜 컨소시엄)) - 모바일 전자증명, 이니셜(initial)
  - SKT가 개발한 분산 신원검증 플랫폼으로 모바일 앱을 통해 정부24와 연동되는 방식
  - 서로 다른 서비스 접속 시마다 서로 다른 DID를 생성하여, 하나의 단일한 DID로 여러 개의 사이트 접속 시 발생 가능한 프라이버시 이슈를 제거

□ 선택적 노출 및 영지식 증명의 기술 결합 방법

- 모든 신원 증명에 영지식 증명 기술을 사용한다면 규모 확장성 (scalability) 또는 서비스 성능 측면에서 단점\*을 지니므로 서비스별 프라이버시 민감도를 고려해야 함
  - \* 시스템에 참여하는 모든 사용자가 자기의 아이디를 스스로 관리해야 하는 근본적인 특징에 기인함
- 프라이버시 민감도가 낮은 경우 : 신뢰된 제3자가 개입되어 선택적 노출 기능을 제공하는 신원인증 서비스(예 : PMI) 이용
- 프라이버시 민감도가 높은 경우 : 영지식 증명을 이용하여 선택적 노출 기능 제공(예 : 분산ID 시스템, VC, 영지식 증명 결합)

## □ 향후 금융권 적용 방안

### (1) (은행 서비스 분야) 잔고증명 서비스

- 영지식 증명 방법을 이용하여 계좌번호나 통장잔고의 구체적인 값을 노출하지 않고 증명 가능

### (2) (자산 관리 서비스 분야) 포트폴리오 관리자 평판 시스템 구축

- 포트폴리오 관리자는 포트폴리오에 포함된 내용 중 원하는 내용을 선택적으로 영지식 증명함
- 펀드 매니저는 경쟁자에게 정보 노출 없이 자신의 신뢰도 관리

### (3) (보험 서비스 분야) 실손의료보험(실비보험) 중복가입 방지

※ 현재 국내에서 약 123만 6,000여 명이 실손의료보험에 중복으로 가입

- 보험회사 측에서 피보험자가 타 보험사에 실손의료보험이 가입되어 있는지 파악 시 영지식 증명을 통하여 타 보험회사에의 가입 여부만 확인

※ 단체 계약 시의 대표 계약자 외에 피보험자 당사자가 직접 중복가입을 확인할 수 있도록 하는 법안 발의됨

#### [ 영지식 범위 증명 또는 셋 멤버십을 활용한 시나리오 ]

분류	시나리오
범위 증명	특정 나이 범위에 있음을 증명(예: 통장 개설을 위한 성인 인증)
	대출 서류에 급여가 특정 범위 내에 있다는 것을 증명
	정확한 금액을 표시하지 않고도 결제 가능 금액이 한도 내에 있음을 증명
셋 멤버십	know-your-customer 체크 시, 사용자가 예를 들면 EU 시민임을 증명
	특정 집단에 소속된 사람들을 익명으로 인증(예: VIP 고객인지의 여부)
	특정 명단에 포함되어 있거나, 포함되지 않았음을 증명 (예: 대출 위험 명단 포함 여부)

### (4) (금융권 증명서) 속성증명 방법을 활용하면 개인정보 보호가 강화된 다양한 금융권 증명서 기반 서비스가 활성화될 것





금융보안원  
FINANCIAL SECURITY INSTITUTE

작성일 2020년 12월

작성자 융합보안부 보안신기술팀