

KISA INSIGHT

DIGITAL & SECURITY POLICY

2023 VOL. 07

중앙은행 디지털화폐(CBDC) 도입 관련 글로벌 동향과 보안 이슈 점검

민경식



중앙은행 디지털화폐(CBDC) 도입 관련 글로벌 동향과 보안 이슈 점검

민경식

CONTENTS

I	디지털 대전환과 디지털경제의 확대	5
II	디지털화폐 도입 관련 주요 글로벌 논의	9
III	주요국의 디지털화폐 도입 동향	16
IV	중앙은행 디지털화폐의 보안이슈	23
V	정책적 시사점	29

『KISA Insight』는 디지털·정보보호 관련 글로벌 트렌드 및 주요 이슈를 분석하여 정책 자료로 활용하기 위해 한국인터넷진흥원에서 기획, 발간하는 심층보고서입니다.

한국인터넷진흥원의 승인 없이 본 보고서의 무단전재나 복제를 금하며 인용하실 때는 반드시 『KISA Insight』라고 밝혀주시기 바랍니다. 본문 내용은 한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

[작성]

한국인터넷진흥원(KISA) 미래정책연구실 디지털정책팀

민경식 팀장

☎ 061-820-1454

✉ kyoungsik@kisa.or.kr

■ 중앙은행 디지털화폐(CBDC)가 촉발한 Web3.0 패러다임 전환 가속

- 한국은행을 비롯한 각국의 중앙은행은 ① 현금 이용 감소세가 지속, ② 경제의 디지털 전환 가속화, ③ 빅테크 기업의 시장지배력과 데이터 집중, ④ 글로벌 스테이블 코인의 등장 등으로 금융·경제 여건의 빠른 변화를 배경으로 CBDC 도입을 검토
- 중앙은행의 디지털화폐 도입논의는 Web3.0 패러다임 전환 필요와 맥락을 같이하고 있어 본격적인 글로벌 금융시스템으로의 추진은 웹 패러다임 변화의 속도를 높일 것으로 전망
- 최근 금융위원회의 STO 발행 허용 및 한국은행의 CBDC 활용성 테스트사업 추진 등을 고려해 보았을 때, Web3.0 패러다임 내에서 디지털경제는 새로운 기회를 맞이할 것으로 전망

■ 글로벌 CBDC 금융네트워크 선점을 위한 주요국 경쟁심화 본격화

- COVID-19 이후의 글로벌 경제 불안정과 미·중 패권경쟁, 러시아-우크라이나 전쟁에 따른 지급결제망의 경제 무기화 속에서 대안적 국경 간 결제 시스템 도입 및 각국의 통화주권 확보를 위한 대안으로 CBDC 도입논의와 실증실험이 신흥국과 개도국 외에도 선진국 중앙은행 중심으로 확산
- 국제결제은행(BIS)의 보고서(23.7)에 따르면 향후 10년 내 CBDC를 유통시킬 것으로 예상되는 신흥국·선진국이 24개 중앙은행에 달할 것으로 전망 (22년 하반기 86개 중앙은행 대상으로 조사)
- EU는 회원국의 CBDC 도입을 위한 입법 준비에 착수하였으며, 영국은 디지털 파운드 도입 로드맵을 완성하였으나 도입 시기에는 신중
- 미국은 FRB 주도로 기반기술 연구를 진행 중이나 행정부와 의회의 견해 차이로 본격적인 도입 여부는 아직 불투명
- 일본은 민간이 참여하는 시범사업을 추진하며 본격적인 도입을 검토하는 단계이고, 우리 정부는 CBDC 시스템에 대한 기술검증을 완료하고 활용 테스트 단계로 진입하기 위한 준비 중

■ CBDC 에코시스템을 대상으로 하는 사이버공격에 대비한 철저한 사전 준비 필요

- CBDC 도입에 있어 가장 중요한 것은 사이버보안과 프라이버시 보호로 인식되고 있으며 주요국의 기술 연구에서도 가장 중요한 검토 포인트가 되고 있음
- BIS를 중심으로 CBDC 에코 시스템의 보안 취약점분석과 대응방안 마련이 논의되고 있는 상황으로 향후 CBDC 기반의 디지털 경제의 확산과 파급력을 고려했을 때 사전적이고 체계적인 대응책 마련이 필요

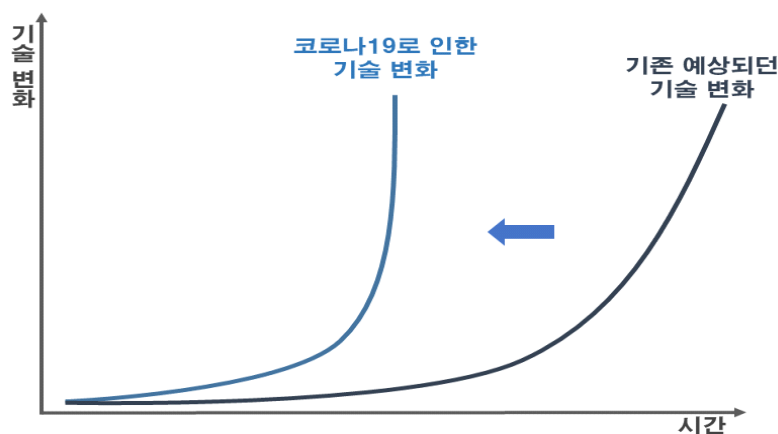
I

디지털 대전환과 디지털 경제의 확대

1-1 팬데믹 이후 빠른 디지털 대전환이 기술을 통한 사회변화를 유도

- 코로나 팬데믹을 통한 반강제적인 디지털 전환의 필요성으로 촉발된 이른바 ‘디지털 대전환’은 경제·사회 전반을 변화시키는 동인이 됨
- 글로벌 차원의 코로나 팬데믹의 확산으로 우리는 이른바 언택트(Untact) 환경에서 미래의 불확실성이 가중되는 상황을 경험
- 언택트를 위한 사회적 거리두기 시행으로 원격근무, 온라인 교육 등이 일상화되면서 그동안 거부감이 있었던 ICT 기술들을 일상생활에 과감히 도입할 수 있는 계기가 됨¹
- 위기 극복을 위한 시대변화 요구는, 우리들의 디지털기기 의존도 증가 및 관련 기술의 발전·확산 속도를 가속화 시키는 기폭제로 작용하여 기존의 예측보다 빠른 사회변화를 가져옴

[그림1] 기술변화의 가속화



출처) 금융위원회(2021), “4차산업혁명시대의 디지털금융 종합혁신방안” 재구성

¹ KISA, 언택트에서 온택트 시대로, 민경식·장한나, 2021.6.30.

- 디지털 대전환은 ICT 기술을 통한 사회 혁신뿐만 아니라, 기술의 역할에 대한 사회적 인식에도 새로운 변화를 유발
- 메타버스, 블록체인, 인공지능 등 핵심 기술을 통해 경제, 사회, 일상 등 모든 영역이 새로운 디지털 패러다임으로 전환되는 현상이 전 세계적으로 확산

[그림2] 플랫폼 패러다임의 변화 예상



출처) Kevin Kelly, 『The Next 5000 Days(5000日後の世界)』, PHP, p.29 재구성

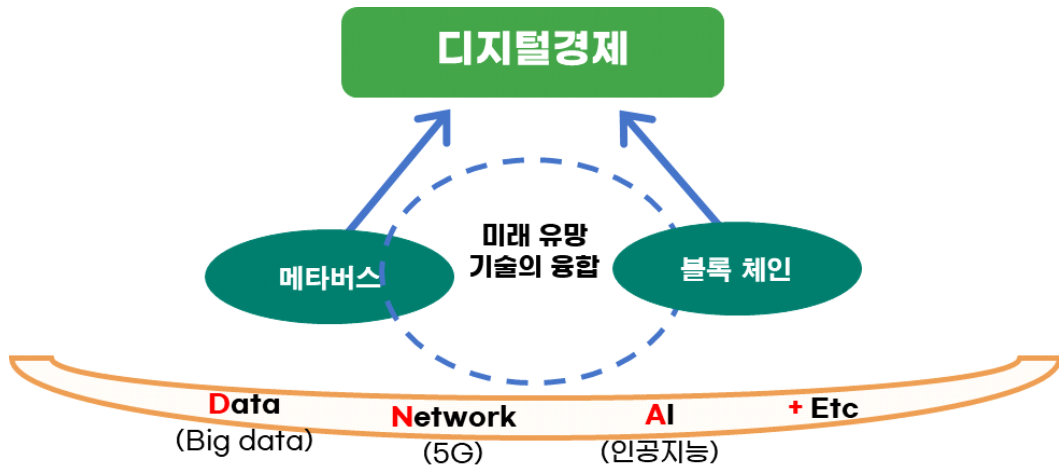
- 디지털 패러다임 전환이 진행됨에 따라 기술의 편리함과 유용성을 넘어 다양한 측면에서 디지털 기술을 바라보게 되었으며, 이에 따라 현행의 중앙 집중형 시스템의 문제점, 빅테크 기업에 대한 과도한 의존도, 대규모 개인정보 유출 등 다양한 우려가 발생하였고, 개선을 위한 사회적 요구도 증가

1-2 미래 유망기술의 융합으로 만들어 가는 새로운 디지털 패러다임

- 코로나19로 촉발된 '디지털 대전환'에 대응하여 미국, EU 등은 디지털 투자 확대를 통한 경제위기 극복과 글로벌 주도권 확보 경쟁이 가속화 되고 있는 상황
- 메타버스, AI, 블록체인을 대표로 하는 미래 유망기술을 주축으로 상호 결합과 융합된 서비스가 속속 등장
- 언택트 비대면 환경에서 디지털 소통이 일상화되면서, 게임, 교육, 업무, 소비 등의 분야를 중심으로 가상화 서비스 수요가 급증하면서 메타버스 산업이 주목받기 시작
- 가상자산으로 대중에게 소개된 블록체인 기술은 금융 분야를 선두로 다양한 영역에서 새로운 비즈니스 또는 서비스, 인프라 등이 개발되고 있음
- 이러한 움직임은 오프라인 경제와 디지털경제의 융합을 통해 현실과 사이버 세계 간 경계를 허물고 우리의 활동공간을 확장시키며, 이로 인해 사이버공간에서 경제주체 간 상호작용이 확대되어 개인의 일상과 기업 활동의 변화가 일어남

- 향후 디지털경제의 성장은 D·N·A(Data, Network, AI)를 기반으로 블록체인 등 신기술 발전과 더불어 폭발적으로 성장할 것으로 예측

[그림3] 디지털 경제 개념도



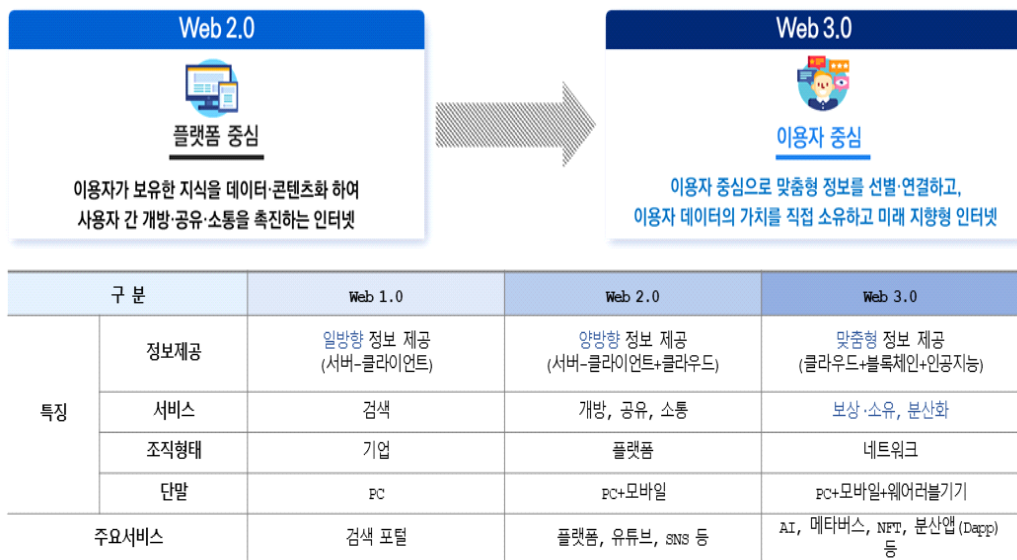
출처) 필자 작성

1-3 Web3.0 패러다임 등장과 동반한 디지털 경제의 새로운 기회

- 디지털 대전환으로 시작된 사회변화 중 하나는 기존 웹 2.0 환경의 문제점 극복에서 시작된 웹 3.0 패러다임 전환에 대한 논의
- 그동안 웹 2.0은 구글, 메타, 아마존 등 주요 기업을 필두로 모바일 인터넷 및 소셜 네트워크 발전과 함께 경제·사회·문화 등 다양한 분야에서 혁신과 성장을 견인
- 그러나 웹 2.0에서 감시자본주의 도래, 빅테크(Big Tech) 기업의 출현과 독과점 이슈, 대규모 개인정보 유출 등 기업들의 과도한 영향력과 사회적 문제가 발생함에 따라, 이를 극복하고자 새로운 웹 패러다임 전환에 대한 필요성이 지속적으로 제기됨
- 웹 3.0은 아직 개념적 정의·범위가 명확하지 않은 초기 단계지만, 기존 웹2.0 환경에서 제기된 문제점을 기반으로 이용자 중심의 데이터 주권확보와 신뢰받는 웹 생태계 구축을 목표로 다양한 기술적 시도가 진행되고 있음
- 최근 논의 되고 있는 중앙은행 디지털화폐(CBDC; Central Bank Digital Currency) 발행에서도 빅테크 기업의 시장지배력 및 데이터 집중 현상에 대한 우려가 도입 배경으로 거론되고 있음

- 한국은행(22.1)² 보고서에 따르면 빅테크 기업의 시장지배력 강화와 개인정보 집중 심화 우려에 대한 대응의 일환으로 개방적 공공화폐 인프라의 중요성이 두드러진다고 지적하고, 빅테크 기업의 영향력 확대는 높은 수수료 뿐 아니라 개인정보의 상업적 이용, 데이터 사일로(Silo)화로 인한 혁신 저해, 독과점 구조 고착화 등을 유발할 수 있다고 지적
- 기존 웹2.0을 포함한 현행 디지털 생태계의 변화 요구는 향후 웹3.0 패러다임을 중심으로 재편될 가능성이 커지고 있음
- 최근 금융위원회의 블록체인 기반의 STO(증권형 토큰발행, Security Token Offering)발행 허용 및 한국은행의 CBDC 활용성 테스트사업 추진을 고려해 보았을 때, 웹3.0 패러다임 내에서 디지털경제는 새로운 기회와 알려지지 않은 보안위험에 직면할 수 있을 것으로 생각됨

[그림4] Web3.0의 주요 특징



출처) 필자 작성

- 본 고는 국내외에서 검토되고 있는 중앙은행 디지털화폐 발행에 관한 글로벌 동향을 살펴보고 주요 활용기술의 보안 이슈를 점검하는 것을 목표로 함
- 구체적으로는 중앙은행 디지털화폐 기본 개념 및 국가별 추진 현황을 분석하고 분산원장 기술을 기반으로 논의되고 있는 CBDC 설계, 운영 방식에서 제기될 수 있는 보안 이슈에 한정하여 검토
- 이러한 검토가 CBDC가 가져올 새로운 디지털경제 시대변화에 있어 그 본연의 목적을 달성하는 과정에서 발생할 수 있는 보안 이슈를 사전에 점검하여 더 안전하고 신뢰받는 경제사회 구축에 일조하기를 기대

² 한국은행, 『중앙은행 디지털화폐(CBDC) 주요 이슈별 글로벌 논의 동향』 한국은행 금융결제국, 2022.1. p21.

II

디지털화폐 도입 관련 주요 글로벌 논의

2-1 디지털화폐(CBDC)의 개념과 정의

■ 분산원장 기술의 발전과 암호자산의 확산을 계기로 논의 활성화

- 중앙은행 디지털화폐(이하, CBDC)에 대한 논의는 비트코인을 대표로 하는 분산원장 기술이 주목받기 시작한 이후 본격화되기 시작
- 2015년 영국 중앙은행이 처음으로 CBDC란 용어를 사용하여 ‘일반 대중이 사용할 수 있는 중앙은행 디지털화폐 발행 필요성’을 제시
- CBDC는 중앙은행이 전자적 형태로 발행하는 디지털화폐를 의미 하나, 구체적인 활용 목적과 설계 및 운영 방식에 대해서는 다양한 의견이 존재

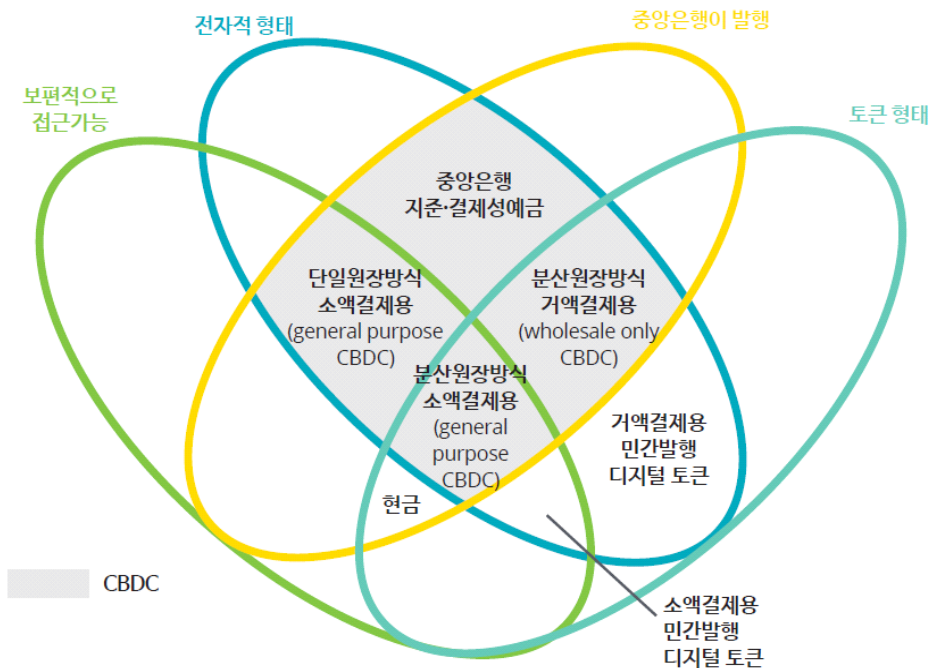
[표 1] BIS와 IMF의 CBDC 정의

BIS	<p>(1) A CBDC is a digital form of central bank money that is different from balances in traditional reserve or settlement accounts (CPMI-MC, 2018)</p> <p>(2) A CBDC is a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank (BIS et al., 2020)</p>
IMF	<p>(1) A digital representation of a sovereign currency issued by and as a liability of a jurisdiction's central bank or other monetary authority (Kiff et al., 2020)</p>

출처) 한국은행(2022). p.5.

- CBDC는 중앙은행의 직접적인 채무(Central bank liability)로서, 현금 등 법화와 일대일 교환이 보장된다는 점에서 암호자산과는 구분
- 이용목적에 따라 모든 경제주체(개인, 기업 등)가 이용할 수 있는 소액 결제용(General-purpose CBDC)과 은행 등 금융기관들만 이용할 수 있는 거액 결제용(Wholesale only) CBDC 발행³

[그림5] CBDC 범위



출처) BIS(2018), Central Bank Digital Currencies, Deloitte(2021), 중앙은행 디지털화폐와 돈의 미래 재인용

2-2 CBDC의 특징과 도입배경

■ 전자적 방식으로 구현된, 현금과 유사한 화폐이지만 다양한 장점을 보유

- CBDC는 전자적 방식으로 구현됨에 따라 현금과 달리 ① 관련 거래의 익명성을 제한하거나 그 수준을 조절할 수 있고 ② 이자 지급, ③ 보유 한도 설정과 ④ 이용가능시간 조절 등도 가능하며, 정책목표에 맞게 특정한 특성들을 갖는 다양한 형태로 발행 가능⁴
- CBDC 구현 시 거래의 익명성을 보장할 수도 있으나, 필요에 따라서는 익명성의 제한도 가능
- CBDC는 이자 지급이 가능하고, 금리 수준에 따라 CBDC뿐만 아니라 CBDC의 대체재라고 할 수 있는 현금·은행예금 등에 대한 수요도 조절 가능
- CBDC가 자금세탁·테러자금 조달 등의 수단으로 악용되는 것을 막기 위해 경제주체별로 보유(또는 사용) 한도 설정도 가능
- CBDC를 연중무휴, 24시간 내내 사용할 수 있게 하거나, 특정 시간대(예: 0시~4시)의 이용을 제한하는 것도 가능

³ 소액 결제용은 소매형(Retail) 또는 범용 결제로도 부르며 거액 결제용은 도매형으로도 부른다. 본고에서는 경우에 따라 혼용해 사용한다.

⁴ 한국은행(2019), 『중앙은행 디지털화폐』 한국은행, pp.8-9.

[표 2] 현금- CBDC-지준예치금 간 특성 비교

	현금	CBDC	기존 중앙은행 예금 (지준예치금)
거래 익명성	보장	보장 여부 선택 가능	무
이자 지급	불가능	가능	가능
보유 한도	무	한도 설정 가능	무
이용 가능 시간	제한없음	설정 가능	제한됨

출처) 한국은행(2019), p.9.

■ ICT 기술의 보급과 확산에 따른 화폐 이용환경 변화에 대응하기 위한 노력

- 한국은행(2022)⁵은 CBDC 도입에 관한 배경으로 ① 현금 이용 감소세가 지속, ② 경제의 디지털 전환 가속화, ③ 빅테크 기업의 시장지배력과 데이터 집중, ④ 글로벌 스테이블 코인의 등장 등으로 금융·경제 여건이 빠르게 변화하고 있다고 분석
- ICT가 경제활동의 중요한 활용 수단이 되면서 현금 이용 감소가 지속됨에 따라 편의성과 안전성 및 신뢰성을 갖춘 저비용의 새로운 보편적 지급수단을 제공하는 공공 인프라 구축의 필요성 증가
- 디지털 대전환을 계기로 금융권과 빅테크 기업 등 민간 주도로 새로운 지급결제 서비스가 등장하여 디지털 경제 활동을 뒷받침하고 있으나 중앙은행 화폐가 디지털화된 금융 및 경제를 뒷받침하는 중추적 역할을 할 필요가 있다고 판단
- 한편, 빅테크 기업의 시장지배력 강화와 개인정보 집중 심화 우려에 대한 대응의 일환으로 개방적 공공 화폐 인프라의 중요성이 부각
- 또한, 금융당국이 최근 급성장하고 있는 민간 스테이블 코인의 부작용을 방지할 책임이 있으며 이에 대한 정책 대응의 일환으로 CBDC 도입 필요성이 거론

⁵ 한국은행(2022), pp.11-12.

2-3 시스템 설계 및 운영 방식에 관한 논의

■ CBDC의 구체적인 설계 및 운영 방식에 대한 다양한 의견 제기

- 운영 구조 측면에서는 중앙은행이 단독으로 운영 책임을 지는 직접형(Direct)은 바람직하지 않다는 것이 대체적 입장이며⁶, 중앙은행과 민간 부문 간 적절한 역할 분담 방안에 대한 세부 논의 진행 중
 - **(직접형)** 중앙은행이 CBDC를 직접 발행·환수하고 유통 및 대고객 서비스 제공도 직접 수행하며 이를 위한 전산시스템 및 관련 인프라의 구축·운영도 직접 담당
 - **(간접형)** 정부가 지정한 민간 은행이 중앙은행에 대한 직접적인 청구권(예: 현금, 지급준비 예치금)을 담보로 CBDC를 발행·환수하고, 유통 및 고객 지급 서비스 제공과 이를 위한 시스템의 구축·운영도 담당
 - **(혼합형)** 중앙은행이 제조·발행·환수는 직접 수행하되 유통은 민간은행과 공동으로 수행하며, 중앙은행이 개별 거래정보를 보관
 - **(중개형)** 혼합형과 같이 중앙은행이 제조·발행·환수를 직접 수행하고 유통은 민간은행과 공동으로 수행하나, 중앙은행은 지급 서비스 제공기관별 총액 정보(Wholesale ledger)만 보관하며, 개별 거래정보는 각 민간은행이 보관
- 민간은행이 디지털화폐를 발행하는 간접형(Indirect)은 CBDC로 볼 수 없다는 견해가 지배적이며 중앙은행과 민간은행이 역할을 각각 분담하는 혼합형(Hybrid) 또는 중개형(Intermediated) 운영 방식이 주로 검토되고 있음
 - 국제결제은행(BIS)이 각국의 중앙은행을 대상으로 실시한 조사에 따르면⁷, CBDC 관련 연구 및 실증을 진행 중인 국가가 증가 추세, 22년도 기준 약 50%가 실험/개념검증을 시행, 약 25%가 개발/파일럿 테스트 중이라고 응답
 - 각국 중앙은행의 소액 CBDC 발행(6년 이내) 예정에 대해서는 약 20% 국가가 발행할 가능성이 높다고 응답, 나머지 80% 국가는 구체적인 발행에 대해 지속적으로 검토를 계속하겠다는 입장
 - BIS 조사에서 신흥국과 개도국이 선진국에 비해 소액 CBDC 발행에 적극적인 것으로 나타남
- 현시점에서 주요국 중앙은행들은 아직 시스템 설계 및 운영 방식에 대하여 최종적인 결론을 내리지 않고 있으며, 다양한 가능성을 열어두고 충분한 시간을 가지면서 기술적, 제도적 측면에서 각 방안의 장단점을 분석·점검하고 있는 상황

⁶ 한국은행(2022), p.52. BIS (2021): Annual Economic Report, June.

⁷ BIS(2023) Making headway-Results of the 2022 BIS survey on central bank digital currencies and crypto, July.

참고 1

CDBC 시스템 운영 구조

구분	업무 흐름도 ¹⁾	기관별 역할
직접형 (direct)		<ul style="list-style-type: none"> - 발행·환수: 중앙은행 - 유통: 중앙은행 - 시스템운영: 중앙은행 - 참가기관간 결제: 불필요 - 계좌·지갑관리: 중앙은행 - 이용자원장 관리: 중앙은행
간접형 (indirect)		<ul style="list-style-type: none"> - 발행·환수: 민간 참가기관 - 유통: 민간 참가기관 - 시스템운영: 민간 참가기관 - 참가기관간 결제: 필요 - 계좌·지갑관리: 민간 참가기관 - 이용자원장 관리: 민간 참가기관 - 참가기관원장 관리: 중앙은행
혼합형 (hybrid)		<ul style="list-style-type: none"> - 발행·환수: 중앙은행 - 유통: 민간 참가기관 - 시스템운영: 중앙은행·민간 분담 - 참가기관간 결제: 불필요 - 계좌·지갑관리: 중앙은행·민간 분담 - 이용자원장 관리: 중앙은행
중계형 (Inter-mediated)		<ul style="list-style-type: none"> - 발행·환수: 중앙은행 - 유통: 민간 참가기관 - 시스템운영: 중앙은행·민간 분담 - 참가기관간 결제: 불필요 - 계좌·지갑관리: 중앙은행·민간 분담 - 이용자원장 관리: 민간 참가기관 - 참가기관원장 관리: 중앙은행

주: 1)

법적 권한(청구권)
 지급 및 결제 정보의 송수신 방식
 실시간 방식
 지연(Deferred) 방식

금융소비자(계좌방식의 경우 실명, 토큰방식의 경우 가명)
 가맹점

출처) Raphael Auer and Rainer Bohme(2021), Central bank digital currency: the quest for minimally invasive technology, BIS Working Papers No948. 한국은행(2022), p.51.재인용

■ 원장관리 방식에 대해 다양한 논의가 지속되고 있으며 분산원장 기술에 대해 주로 연구 중

- CBDC 도입 시 고려하는 원장관리 방식은 기존 중앙집중형 네트워크 기반기술 이용방식과 블록체인 기술 기반의 분산원장(Distributed ledger technology, DLT) 방식으로 나뉘어 논의가 지속
- 미국, EU, 영국, 일본 등 주요국의 경우, 블록체인 기술 기반의 분산원장 방식을 염두에 두고 연구와 실증 실험을 진행하고 있음
- 그러나, 최근 들어 분산원장 방식의 한계 등을 들어 중앙집중형 단일원장 방식으로도 새로운 지급결제 서비스를 충분히 구현할 수 있다는 견해도 제기
- 최근, 영국 중앙은행(2023)⁸은 디지털 파운드에 관한 기술보고서에서 중앙집중적으로 관리되는 분산 데이터베이스(Distributed databases) 기술을 활용하는 것이 더욱 효율적인 접근방법이라고 지적, 또한 보고서에서는 DLT의 분산적인 거버넌스가 시스템 공격의 대상(Attack surface)을 증가시켜 접근관리를 비롯한 보안 강화가 필요하다고 언급하며 이러한 점이 사용 편의성에 악영향을 미칠 것이라고 분석
- 분산원장 기술을 활용해 CBDC를 설계할 경우 기존 중앙집중형 시스템에 비해 복원력, 보안성에서 우수하고 미래형 지급결제 환경 변화에 탄력적으로 대응할 수 있다는 것이 장점으로 거론⁹
- **(복원력)** 다수 기관이 동일 정보를 관리하므로 특정 기관에 기인한 오류로 전체 시스템이 중단되는 사고 발생 가능성이 감소하며 시스템 운영 복원력(Resilience)이 높다고 평가
- **(보안성)** 저장된 정보를 위·변조하기 위해서는 분산 관리되는 모든 원장에 접근하여 이를 조작해야 하므로 해킹방지 등 보안성이 우수
- **(미래 대응)** 탈중앙화금융(DeFi)과 대체불가토큰(NFT), 사물인터넷(IoT) 등 새로운 지급결제 수요에 부응하기 위해서는 분산원장 방식이 보다 효율적일 수 있음
- 한편 분산원장 기술은 확장성과 효율성, 상호운용성 측면에서 해결하기 어려운 근본적인 한계가 존재한다는 견해도 다수¹⁰
- **(확장성)** 거래 종결을 위하여 참가기관 간 합의 등 추가적인 절차가 필요하므로 단위시간 당 처리 가능한 거래건수(TPS; Transactions Per Second)가 충분하지 않을 수 있음
- **(효율성)** 참가 기관 모두가 각각 처리 능력을 갖추어야 하므로 단일원장 기반보다 IT시스템 구축 및 운영 비용이 증가
- **(상호운용성)** 기존 지급결제시스템과의 기술적인 연동이 복잡하여 시스템 간 호환이 어려울 가능성

⁸ Bank of England (2023), The digital pound: Technology Working paper, CBDC Unit Bank of England.

⁹ 한국은행(2022), p.56

¹⁰ 한국은행(2022), p.57

참고 2

단일원장과 분산원장(DLT) 비교

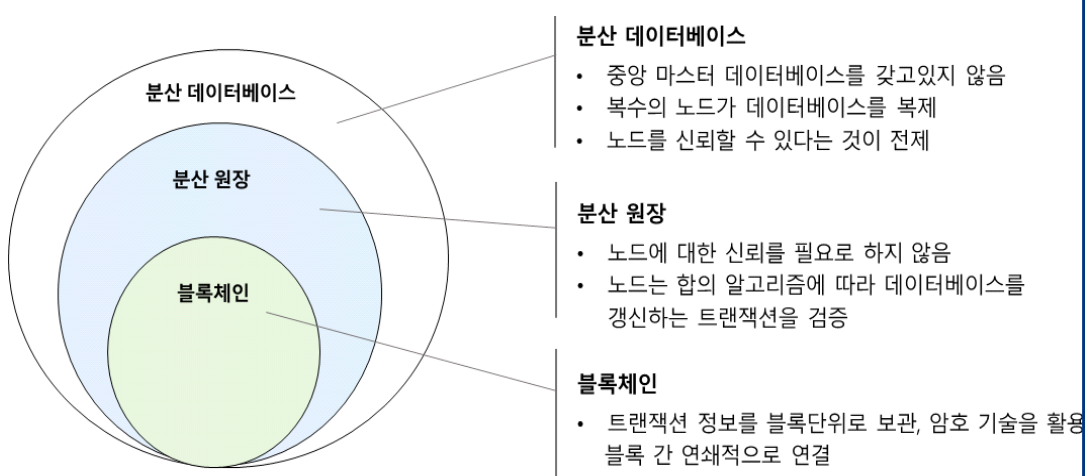
- 원장방식에 따라 장단점이 다르게 나타나고 있어 원장방식에 대한 논란과 연구가 계속 진행 중

[표 2] 단일원장 및 분산원장 방식 비교

	단일원장	분산원장
확장성	분산원장에 비해 처리속도가 빠름	단일원장에 비해 처리속도가 느림
효율성	특정 기관만 원장을 관리하기에 분산원장에 비해 구축·운영 비용 절감	모든 중개기관이 동일 수준의 IT시스템이 필요하여 구축 및 운영
상호 운영성	기존 지급결제시스템에 사용 중인 보편적 기술로 호환성이 우수	기존 지급결제시스템과의 기술적 연동이 복잡하여 호환성이 낮을 가능성
복원력	단일 실패 점 문제 발생 가능	특정 기관 장애로 전체 시스템의 중단될 가능성이 줄어 시스템 운영 복원력이 향상
보안성	고도의 사이버 공격 대응책 마련 필요	데이터 위·변조를 위해서는 분산된 정보 및 블록으로 연결된 모든 정보의 수정이 필요하여 보안성 우수
혁신성	스마트계약 기능 지원이 어려움	스마트계약 기반의 프로그램 가능 화폐 설계 용이

출처) 한국은행(2022), p.58.

- 분산원장과 블록체인은 다양한 정의가 존재하나 분산원장이 블록체인보다 넓은 개념을 가지고 있는 것은 사실



출처) Cambridge Center for Alternative Finance (2017) "Global Blockchain Benchmarking Study", p23-24

III

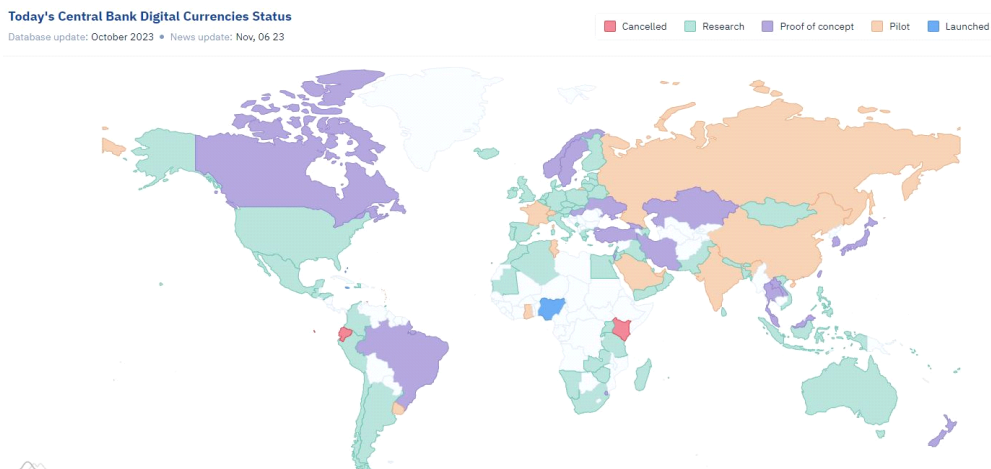
주요국의 디지털화폐 도입 동향

3-1 글로벌 차원의 CBDC 도입 관련 연구 및 실험 현황

I 디지털경제의 확산과 함께 다양한 이슈로 CBDC 도입 논의가 빠르게 진전

- COVID-19 이후의 글로벌 경제 불안정과 미·중 패권 경쟁, 러시아-우크라이나 전쟁에 따른 지급결제망의 경제 무기화 속에서 대안적 국경 간 결제시스템 도입 및 각국의 통화주권 확보를 위한 대안¹¹으로 CBDC 도입 논의와 실증실험이 신흥국과 개도국 외에도 선진국 중앙은행 중심으로 확산
- 신흥국과 개도국은 금융 포용성, 현금 사용 감소 등에 대응하는 차원에서 CBDC 도입에 적극적이지만, 글로벌 기축통화로서 높은 비중을 갖는 미국, EU, 일본 등은 상대적으로 소극적인 입장을 견지
- 우리나라를 포함한 주요국 중앙은행은 CBDC 도입에 따른 실질적 편익과 실현 가능성, 기존 금융시스템에 미치는 영향 위주로 연구 및 실증 실험 진행

[그림6] 전세계 CBDC 관련 연구 및 실험현황 (23년 11월 현재)



출처) CBDC tracker HP

11 하나은행(2023), “디지털화폐 도입 관련 글로벌 동향과 시사점”, 『하나 금융동향 및 이슈』 하나금융경영연구소,p.4..

- 국제결제은행(BIS)의 보고서(23.7)에 따르면¹² 향후 10년 내 CBDC를 유통할 것으로 예상되는 신흥국·선진국이 24개 중앙은행에 달할 것으로 전망 (22년 하반기 86개 중앙은행 대상으로 조사)
- 새롭게 유통될 CBDC 대부분은 소매형이 될 전망으로 이미 도입한 바하마, 東카리브, 자메이카, 나이지리아에 11개 중앙은행이 추가될 가능성이 높고, 도매형은 9개 중앙은행에서 발행될 것으로 보임
- 어떤 형태이든 CBDC에 대해 검토하고 있는 비율은 93%로 급증, 전체 60% 중앙은행은 스테이블코인 등 가상자산의 현금 대체 대응 차원이라고 응답

[그림기] 각국 중앙은행 CBDC 관련 실험현황

인도	브라질	호주
<p>-22년3월, 은행권에 디지털 형식도 포함하는 개정 중앙은행법 성립</p> <p>-22년 12월 디지털 루피 실험 시작</p> 	<p>-23년3월, CBDC 파일럿 프로젝트 시작, 24년 후반 완료</p> <p>-23년 8월, CBDC의 명칭을 「Drex」로 변경</p> 	<p>-23년3월, CBDC 파일럿 프로젝트 시작</p> <p>-23년 8월, 파일럿 실험 보고서 발표</p> 

출처) 각국 중앙은행 HP

■ CBDC에 대한 긍정적인 평가만큼 화폐로서의 기능 수행 여부에 대해서는 여전히 의문

- 국제통화기금(IMF)은 CBDC의 향후 통화로서의 가능성을 충분히 인정하면서도 동시에 이를 가능하게 하는 통일된 인프라 미비 등을 이유로 CBDC의 기능 수행 여부에 대해서는 여전히 의문을 제기¹³
- 나이지리아 CBDC인 eNaira 도입은 나이지리아의 금융포용 등 잠재적 이익을 가져올 수 있으나, 재무건전성 및 자금세탁 등의 잠재적 위험에 대한 평가가 필요하다고 지적
- 또한, 바하마 CBDC인 Sand Dollar에 대해 현재 사용이 제한적이며, 사이버보안, 관련 시스템의 탄력성 확대 등의 내부 역량 개선이 필요성을 제기

¹² REUTERS, Twenty-four central banks will have digital currencies by 2030, survey shows, July 10.2023.

Kosse , Anneke and Ilaria Mattei , "Making headway Results of the 2022 BIS survey on central bank digital currencies and crypto," BIS , July 2023.

¹³ 김보경(2023), "IMF의 CBDC에 대한 입장 변화와 주요국의 개발현황", 『자본시장포커스』, 자본시장연구원, No.16. p.2.

- IMF 크리스탈리나 게오르기예바 총재는 23년 5월 개최된 글로벌 컨퍼런스에서 CBDC는 피할 수 없는 미래이지만 소액 결제용 CBDC는 금융시스템의 혁신과 동시에 전례 없는 리스크를 초래할 수 있다는 의견을 피력하였고, 최근 IMF는 국제결제 상호운용성을 보장하는 플랫폼 개발을 구상 중으로 알려짐¹⁴

3-2 주요국별 입장과 추진 현황

■ 중국은 CBDC 도입에 적극적이며 시범지역을 점차 확대 중

- 중국 중앙은행인 인민은행은 2014년 소액 결제형 CBDC(통칭 e-CNY)의 연구에 착수, 중국에서는 통칭 DCEP(Digital Currency Electronic Payment)로 부름, 단일원장과 분산원장 방식을 혼용한 형태로 보임
- 2019년 말부터 대상 지역을 순차적으로 확대해 가면서 파일럿 실험을 추진 중으로 현재 17개 성 26개(북경시, 상하이시, 광둥성 등) 지점에서 사용 중
- 누적통계로 거래횟수 약 3.6억 회, 거래금액 약 1,000억 위안(22년 8월 말), 유통잔고 136.1억 위안
- 장쑤성 창수시는 23년 5월부터 공무원과 공공기관 직원의 급여를 e-CNY로 지급
- 중국은 e-CNY를 중화권 지역 및 교역국을 중심으로 구축 통화화 하려는 목표를 갖고 중동 및 아프리카지역 내 통용을 적극적으로 모색 중인 상황
- 22년 3월 프랑스 토탈에너지와 중국 해양석유총공사(CNOOC)간 LNG 거래에서 첫 디지털 위안화 결제가 이루어졌으며 23년 10월 19일 상하이 석유천연가스 거래소(SHPGX)는 중국 에너지기업 페트로차이나 인터내셔널(PetroChina International)이 원유 100만 배럴에 대한 대금을 디지털 위안화로 결제했다고 발표

■ EU는 회원국의 CBDC 도입을 위한 법안 초안을 마련하고 디지털 유로 발행을 위한 2년간의 준비 단계에 돌입

- 2023년 6월 28일 EU 집행위원회(EC)는 “단일 통화패키지(Single currency package)”로서 개인과 기업에 의한 유로 지폐·화폐의 이용가능성 확보와 새로운 디지털 형태의 유로의 프레임워크를 만들 목적으로 「Digital euro package」를 발표, 주요 내용은 다음과 같음¹⁵
- **(법정통화)** 디지털 유로(Digital Euro)는 법정 화폐로서의 지위가 주어지고 특별한 이유가 없는 한 종이 화폐와 동일하게 사용됨

¹⁴ 블룸미디어, IMF 총재, 글로벌 CBDC 플랫폼 구상 중, 2023년 6월20일자 보도

¹⁵ 일본 재무성, CBDC 관련 전문가회의 자료(23년 9월5일자) 정리

- **(결제 서비스)** EU에서 인가한 결제 서비스 제공자는 디지털 유로 결제 서비스를 제공 가능, 이용자는 디지털 유로 결제계좌를 1개 이상 보유 가능
- **(이용제한)** EU 중앙은행(ECB)은 보유 제한을 포함, 가치저장으로써 이용을 제한하는 수단을 개발해야 한다, 또한 디지털 유로에 이자는 지급되지 않음
- **(기능)** 디지털 유로는 발행 초기부터 온·오프라인 모두 이용할 수 있어야 함
- **(프라이버시와 데이터 보호)** ECB·각국 중앙은행은 디지털 유로의 이용자를 특정할 수 없게 개인정보처리에 최선의 보안기술과 프라이버시 보호조치를 활용해야 함
- 최근 ECB는 10월18일 이사회를 통해 디지털 유로의 디자인과 유통에 관한 2021년 10월부터 2년간의 「조사 단계(Investigation phase)」를 끝내고 11월부터 다음 단계인 「준비 단계(Preparation phase)」에 들어간다고 공식 발표¹⁶
- 향후 2년간, EOB는 디지털 유로의 발행 규정집(Rulebook)을 완성하고 디지털 유로의 기반이 되는 플랫폼과 인프라를 개발하는 사업자를 선정하게 됨
- EOB는 보도를 통해 이번 준비 단계가 디지털 유로 발행의 정식결정은 아니라는 점을 강조하고 있으나 EOB의 Christine Lagarde 총재는 디지털 유로가 다양한 디지털 결제에 무료로 사용되고 최고의 프라이버시 기준을 만족시키는 디지털화폐가 될 수 있다고 언급

■ 영국은 디지털 파운드에 대한 도입 로드맵을 완성하였으나 도입 시기에는 신중

- 영국은 2020년부터 CBDC 연구를 진행하였으나 도입에는 신중한 입장이었으나 최근 중앙은행(Bank of England)과 재무성이 디지털 파운드화 도입 목적과 기본특성, 구성 시스템 측면을 검토한 보고서¹⁷를 공개
- 보고서에 공개된 CBDC 로드맵에는 2022년까지 1단계(Research and exploration) 기초연구를 끝냈고 2023년부터 2~3년간은 2단계(Design)로서 디지털 파운드의 기술적 실현 가능성을 종합적으로 평가하고 최적의 디자인과 기술 아키텍처를 정하는 기간으로 명시
- 빠르면 2025년부터 3단계(Build)로 진입하여 디지털 파운드의 프로토타입 구축, 파일럿 실험실시 등이 진행되어 2020년대 후반에는 도입될 수 있을 것으로 전망
- 영국은 CBDC의 기술적 검토 의견에서 분산원장과 블록체인 기반 솔루션이 CBDC의 핵심기술이 될 수 있다는 것은 인정하나 활용 면에서 한계를 가지고 있다고 지적하고 분산 데이터베이스까지를 시야에 둔 포괄적 기술 검토를 진행할 것으로 밝힘
- 영국 정부가 고려하는 CBDC 발행 형태는 현재로서는 금융기관을 대상으로 하는 거액 결제의 도매형 방식으로 일반이용자가 중앙은행과 거래하는 것은 없을 것으로 설명
- 다른 국가의 사례와 동일하게 CBDC에 대한 이자는 지급하지 않고 보유 상한을 두는 것을 검토하고 있음

¹⁶ ECB, "Eurosystème proceeds to next phase of digital euro project", 18 October 2023

¹⁷ Bank of England, The digital pound: Technology working Paper, 7 February 2023

■ 미국, FRB는 CBDC 기반기술 연구를 진행 중이며 대통령 행정명령 이후 필요성 인식

- 미국 연방준비은행(FRB)은 2022년 1월 20일, CBDC의 편익, 위험, 정책 검토사항 등을 정리한 보고서 「Money and Payments The US Dollar in the Age of Digital Transformation」를 발표
- FRB는 이 보고서에서 CBDC 도입 여부보다는 실질적으로 활용 가능한 분야 및 도입 시 이득과 이용자 보호 등 리스크 관점에서의 기본 방향 정도를 제시¹⁸
- 한편, 보스턴 연방준비은행(Federal Reserve Bank of Boston)은 MIT와 공동연구(Project Hamilton)를 2020년부터 시작하여 22년 2월 1단계로 보고서(A High Performance Payment Processing System Designed for CBDC)를 공개, 여기서는 소매형 CBDC 시스템구축을 테스트, 2단계로 프라이버시 등에 관한 기술 측면의 검토 보고서가 23년 중에 공개 예정
- 바이든 대통령은 22년 3월9일 각 부처에 대해 「디지털자산의 기술혁신을 촉구하는 대통령령(Executive Order on Ensuring Responsible Development of Digital Assets)」에 서명하고 중앙은행이 발행하는 디지털 통화의 연구 가속화를 요구
- 행정부의 CBDC 관련 필요성 인식에도 불구하고 CBDC로 인한 프라이버시, 개인정보 침해우려가 다수 지적되고 있고, 23년 9월 미 하원에서는 공화당 의원 중심으로 반CBDC 법이 통과되는 등 정치적 이슈로 부상

■ 일본, 2차례 CBDC 관련 실증 실험을 끝내고 민간이 참여하는 시범사업 추진 중

- 일본 중앙은행은 2020년 10월 「중앙은행 디지털화폐에 관한 일본은행 대처방침」¹⁹을 발표하고 본격적인 준비에 착수, 21년부터 3단계로 나누어 실증 실험을 시작
- 21년 4월~22년 3월까지 1단계 개념 실증에서는 시스템을 구축하여 CBDC의 발행, 유통, 환수의 기본기능에 관한 검증, 22년 4월~23년 3월까지 2단계 개념 실증에서는 1단계에서 구축한 시스템에 CBDC 주변 기능을 추가하여 실현 가능성을 검증
- 23년 4월부터 시작한 시범사업에서는 최종이용자 간의 처리 과정의 확인을 위해 실험용 시스템을 구축하고 성능시험을 시행, 또한 금융 분야를 포함한 폭넓은 민간사업자(60여 개)가 참여하는 포럼을 만들어 기술, 운영 측면의 연구 및 제도설계를 추진하기 위한 3개 연구반 구성²⁰
- 일본 재무성은 23년 4월부터 「CBDC 관련 전문가 회의」를 개최하여 주요국의 디지털화폐 관련 최신동향을 공유하고 일본은행의 CBDC 실증시험에 관한 이슈를 검토 중

¹⁸ 하나은행(2023),p.11.

¹⁹ 中央銀行デジタル通貨に関する日本銀行の取り組み方針

²⁰ 각 연구반은 WG1 (CBDC 시스템과 외부 인프라, 시스템 등의 접속), WG2 (추가 서비스와 CBDC 에코시스템), WG3(KYC와 이용자 인증, 인가)으로 나뉨

3-3 한국은행 CBDC 추진 현황

■ 비교적 초창기부터 CBDC 관련 연구와 전담 조직 운영으로 글로벌 트렌드에 대응

- 한국은행은 2019년 「중앙은행 디지털화폐」보고서 발간을 통해 CBDC 발행이 중앙은행에 미치는 전반적인 영향과 법적·기술적 이슈 등을 검토 시작
- 2020년 CBDC 전담 조직을 설치하고 본격적인 연구 수행, 21년부터(1단계) 22년까지(2단계) 모의실험을 통해 기술적 구현 가능성을 점검
- 2차례 모의실험을 통해 한국은행은 CBDC 기술 구현의 가능성을 확인하였고, 분산원장 등 신기술 적용의 한계를 극복하는 방안을 마련한 것으로 보임

[그림8] 한국은행 CBDC 모의실험 연구 범위



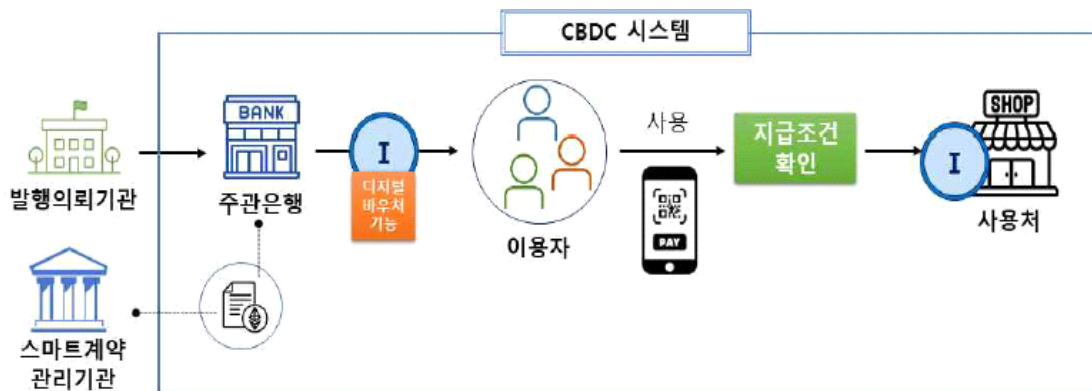
출처) 한국은행 (2022. 11. 7) 보도자료, 「CBDC 모의실험 연구」 사업 2단계 결과 및 향후 계획

■ 한국은행 등 금융 관계기관은 CBDC 활용성 확대를 위한 구체적인 추진 계획 마련

- 최근 한국은행, 금융위원회, 금융감독원 등 우리나라 금융 관련 핵심 3대 기관은 “CBDC 활용성 테스트” 세부 추진계획을 발표하면서 CBDC 구체화를 위한 새로운 단계에 들어섬 (23년11월23일)
- 이번 테스트에서는 CBDC 네트워크 내에서 I 형 통화(예금토큰), II 형 통화(e머니 토큰), III 형 통화(특수 지급 토큰)가 발행됨
- (실거래 테스트) 구체적으로는 다양한 형태의 디지털 바우처 기능이 부여된 CBDC 기반 예금토큰을 발행-유통-지급되는 일련의 프로세스를 검증하게 됨²¹

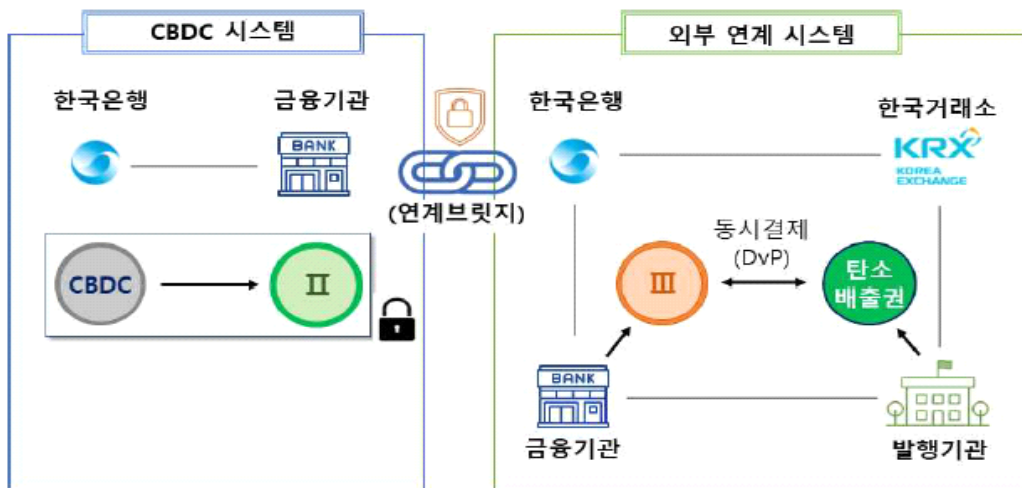
- 활용성 테스트에서 주목할 점은 모의실험을 통해 구체적인 성능을 확인한 CBDC 시스템을 기반으로 24년 4분기 중 실거래 테스트를 일반 이용자(10만 명 이내)도 참여하여 실시한다는 것
- (가상환경에서의 기술 실험) 탄소배출권과 같은 새로운 형태의 자산을 유통하는 이른바 가상환경에서의 기술 실험도 진행, 이번 유통실험은 한국거래소의 탄소배출권 시장 관련 분산원장 기술 모의실험과 연계, 또한 토큰화된 자산을 일반인에게 공모 형태로 발행하는 개념검증을 실시

[그림9] 디지털 바우처 기능을 활용한 실거래 테스트



출처) 한국은행 (2023. 11. 23) 보도자료, 한국은행-금융위원회-금융감독원, 「CBDC 활용성 테스트」 세부 추진계획 마련

[그림10] 탄소배출권 유통 기술실험 구성(안)



출처) 한국은행 (2023. 11. 23) 보도자료, 상동

²¹ 한국은행은 현행의 바우처의 경우 ①높은 수수료, ②복잡하고 느린 정산 프로세스, ③사후 검증 방식의 한계 및 부정수급 우려, ④민간 보조사업자에 대한 높은 의존 등의 문제점을 가지고 있는 것으로 지적 (보고서 p.2)

IV

중앙은행 디지털화폐의 보안 이슈

4-1 디지털화폐 발행에 대한 글로벌 보안 이슈

I CBDC 도입 및 활성화에 앞서 여러 가지 위험 요소를 고려해야

- 21년 딜로이트가 전 세계 10개국, 1,280명을 대상으로 실시한 조사²²에 따르면 디지털자산을 도입하는데 가장 큰 장애를 사이버보안 문제(응답률 71%)라고 응답, 또 다른 보고서²³는 디지털화폐 도입을 위한 중요한 해결 과제로 사이버보안과 개인정보보호를 지적
- 소액 결제용 CBDC 시스템의 경우, 자금의 이동 과정에서 많은 주체가 관여하기 때문에, 사이버 공격 대상 접점이 더 늘어날 수 있는 점에 대비해야 하고 각국 중앙은행은 이러한 위험을 최소화할 수 있는 철저한 프레임워크의 사전 마련 필요
- 한편, 소액 결제용 CBDC 사용으로 대량의 데이터가 시스템에 저장될 수 있는데, 이러한 시스템은 언제나 데이터 유출의 위험을 수반. 또한, CBDC가 특정 그룹의 소비 패턴을 추적하고 감시하는 도구로 악용되지는 않을 것인가라는 지적도 다수. 따라서 이러한 문제들을 방지할 수 있는 제도적, 기술적 장치 마련 필요

I G7 은 CBDC가 신뢰를 얻기 위한 필수원칙으로 엄격한 프라이버시 보호 기준 마련 제안

- 21년 10월, G7은 중앙은행 및 재무장관 회의를 통해 “중앙은행 디지털화폐(CBDC)에 관한 공공정책상의 원칙”을 발표하며 엄격한 프라이버시 기준, 이용자 보호에 관한 설명책임, 정보보호 및 이용 방법의 투명성은 모든 CBDC가 신뢰를 얻기 위해 필수 불가결한 원칙으로 천명(참고 3)
- CBDC가 현금과 유사한 수준의 익명성(Anonymity)을 갖추어야 하는지는 CBDC 설계 및 운영에 있어 주요 고려 사항, 익명성을 부여하지 않을 경우, 개인 정보가 국가에 집중될(big brother 이슈) 가능성이 커지나 국가별 의견이 다름

²² Deloitte (2021a), “Deloitte’s 2021 Global Blockchain survey : Anew age of digital assets” Deloitte Insights.

²³ Deloitte (2021b), “일과 산업의 미래 : 중앙은행 디지털화폐와 돈의 미래” Deloitte Insights.

참고 3

G7의 「소매형 CBDC에 관한 공공정책상의 원칙」

- 2021년 10월, 영국에서 개최된 G7 회의에서 CBDC 발행에 대한 기본원칙 “Public Policy Principles for Retail Central Bank Digital Currencies”을 공표, 8개의 기본과제(Foundational Issues, 1-8번)와 5개의 기회(Opportunities, 9-13번)로 구성

[표 5] ‘디지털 원칙’의 주요 사항

원칙(Principle)	내용
1. 통화·금융 시스템의 안정 (Monetary and financial stability)	- 모든 CBDC는 공공정책의 목적과 달성을 지원하고 금융시스템에 장애가 되지 않게 설계되어야 한다.
2. 법적·거버넌스 프레임워크 (Legal and governance frameworks)	- 법률준수, 건전한 경제 거버넌스, 투명한 국제통화시스템에 관한 G7의 가치관이 모든 CBDC의 설계와 운영의 지침이 되어야 한다.
3. 정보 프라이버시 (Data privacy)	- 엄격한 프라이버시 기준, 이용자 보호에 관한 설명책임, 정보보호 및 이용 방법의 투명성은 모든 CBDC가 신뢰를 얻기 위해 필수 불가결한 원칙이다.
4. 운영 복원력과 사이버보안 (Operational Resilience and Cyber Security)	- 신뢰성, 내구성 있고 변화에 유연한 디지털 결제를 실현하기 위해 모든 CBDC의 생태계는 사이버 리스크, 사기 리스크, 운영리스크에 대해 안전하고 복원력을 갖추어야 한다.
5. 경쟁 (Competition)	- CBDC는 기존 결제 수단과 공존해야 하며, 개방성, 안전성, 유연성, 투명성을 확보한 경쟁환경에서 운영되어야 한다.
6. 부정한 금융 (Illicit finance)	- 모든 CBDC는 범죄를 조장하는 이용 목적을 경감시키도록 노력해야 하며 보다 빠르고, 보다 많은 사람이 이용할 수 있으며 안전하고 저렴하게 이용할 수 있어야 한다.
7. 파급효과 (Spillovers)	- CBDC는 그 도입으로 국제통화·금융 시스템에 피해를 주는 리스크가 없도록 설계되어야 한다.
8. 에너지와 환경 (Energy and Environment)	- 모든 CBDC 인프라의 에너지 사용은 국제사회의 탄소배출 저감 경제(Net Zero Economy) 추진에 상응하는 수준으로 효율적이어야 한다.
9. 디지털경제와 혁신 (Digital economy and innovation)	- CBDC는 디지털경제의 혁신을 유도하고 기존금융과의 상호연동성을 확보해야 한다.
10. 금융 포용성 (Financial inclusion)	- 금융당국은 CBDC의 금융 포용성을 검토해야 하며, CBDC는 기존 금융시스템이 미치지 못했던 부분까지 가능한 포용할 수 있도록 해야 한다.
11. 공공부문 내의 결제 (Payments to and from the public sector)	- 모든 CBDC는 공공부문과 민간의 사용에 있어 평시나 위기 시에도 변함없이 빠르고 값싸게 이용할 수 있는 안전한 환경을 구축해야 한다.
12. 국제거래 기능 (Cross-border functionality)	- CBDC 발행에 있어 중앙은행과 관련 조직은 국제거래가 가능하도록 검토해야 한다.
13. 국제개발 (International development)	- 국제개발원조에 사용되는 모든 CBDC는 투명성을 제공하고 발행국 및 수혜국의 공공정책 목적을 보호해야 한다.

4-2 디지털화폐 보안 이슈에 대한 주요국의 입장²⁴

■ 결제 수단으로서 24시간/365일 이용 가능한 상시 시스템으로서 고도의 신뢰성이 보장되어야

- (EU) 디지털 유로를 구성하는 기능은 사이버보안과 사이버 복원력(Cyber Resilience) 평가에 근거한 요건을 충족해야 하며 데이터 암호화, 디지털 서명 등을 이용해 데이터의 안전성과 기밀성을 보증해야 함
- (미국) CBDC 시스템은 사이버 공격에 대해 적절한 관리가 이루어져야 하며 가용성이 확보되어야 함, 이를 위해 프라이버시 강화 기술이나 영지식증명 등 혁신적인 보안기술의 연구개발을 우선적으로 검토
- (영국) 디지털 파운드는 신용카드 네트워크와 같은 다른 결제 시스템처럼 정전이나 사이버 공격에 대한 리스크를 안고 있어 최고 수준의 내성(Tolerance)을 갖도록 시스템을 설계해야 함

■ 이용자 정보·거래정보의 취급에 있어 프라이버시 확보를 최우선으로 고려

- (EU) 디지털 유로 시스템은 프라이버시의 권리를 존중하여 설계하고 어떠한 경우라도 개인의 거래데이터에 관심을 두고 있지 않음, 디지털 유로 사용에 본인확인 필요하나 높은 수준의 프라이버시 보호를 유지, 한편 완전한 익명성은 공공정책의 관점에서 실현 가능한 선택지는 아님
- (미국) 프라이버시를 우선하여 중앙은행이 수집하는 거래 정보와 개인 식별정보는 최소화, 본인확인 기반의 계좌제한(보유제한/거래제한)은 가능할 것으로 봄, CBDC 시스템은 소비자에 대한 정부의 부적절한 감시를 막기 위한 거버넌스 구조를 갖추어야 함
- (영국) 디지털 파운드는 적어도 은행계좌와 같은 수준의 프라이버시 보호가 유지되어야 함, 관련 기관은 법률이 규정한 현행기준과 동일하게 이용자 정보에 접근을 엄격히 제한, 그러나 디지털 파운드는 익명화하지 않음 왜냐하면 이용자를 특정하고 본인확인 가능해야 금융범죄를 예방할 수 있음

4-3 BIS(프로젝트 폴라리스)의 CBDC 시스템 보안 위협진단

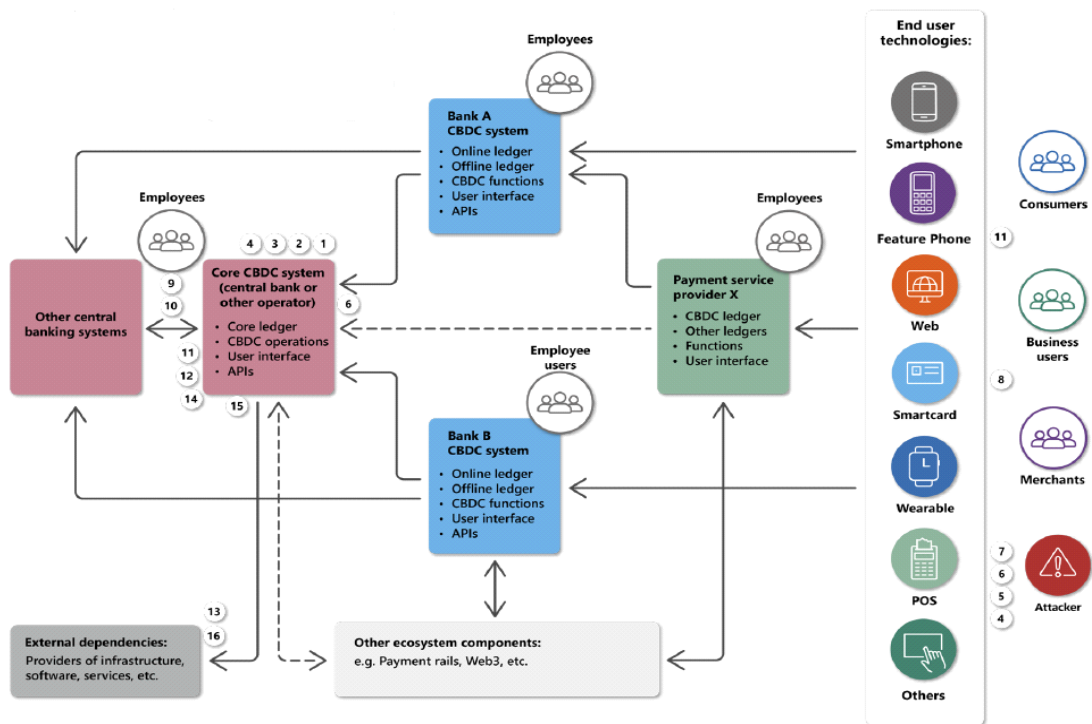
■ CBDC 도입은 예측할 수 없는 새로운 위협과 잠재적 위험을 제거해야 신뢰받을 수 있어

- 국제결제은행(BIS)는 23년 7월 블록체인 금융시스템에서 발생하는 사이버 공격이 중앙은행 디지털화폐 생태계에서도 발생할 수 있다는 전제하에 보안 계획인 “프로젝트 폴라리스(Project Polaris)”를 발표
 - 총 7단계로 나뉘는 프로젝트 폴라리스는 분산원장 및 스마트계약 기술관련 발생 가능한 위험을 제거하는데 초점
 - 사이버공격 방지의 7단계는 준비(prepare), 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 회복(Recover), 조정(Adapt)으로 구성

²⁴ 일본 재무성, CBDC 관련 전문가 회의 자료(23년 10월13일자) 정리

- BIS는 프로젝트 폴라리스 보고서²⁵를 통해 CBDC 에코시스템 모델을 제시하고 보안의 핵심요소인 기밀성, 무결성, 가용성을 위협할 수 있는 대표적인 16개 침해사고를 열거, 열거된 사고는 서로 상관관계가 없고 여러 개의 사건이 함께 발생할 수도 있음
- ①분산 서비스 거부(DDoS) 공격 : 컴퓨팅 리소스나 손상된 컴퓨터 또는 사물인터넷(IoT) 디바이스 네트워크를 사용하여 대량의 서비스 요청을 CBDC 시스템이나 해당 서비스에 전송함으로써 시스템 과부하로 인해 타임아웃 또는 성능 저하가 발생
- ②지능적 지속 위협(APT) 공격 : 일반적으로 국가 또는 조직화된 범죄 단체에서 미리 공격 대상을 정해두고 장기간에 걸쳐 공격 대상의 시스템에 침투하여 악성 소프트웨어를 설치하거나 백도어를 만들고, 네트워크 트래픽 및 사용자 및 시스템 동작을 분석하여 공격
- ③멀웨어(와이퍼웨어²⁶, 랜섬웨어 등) : 피해자의 컴퓨터와 네트워크에 악성 소프트웨어를 심어 특정 서비스를 파괴하거나, 피해자 네트워크 백도어 역할을 하고, 데이터 및 정보자산을 대상으로 한 랜섬 결제를 유도

[그림11] CBDC 에코시스템과 보안위협



출처) BIS(2023), p.22.

²⁵ BIS, Project Polaris, Part 2: A security and resilience framework for CBDC systems, July 2023.

²⁶ 감염된 컴퓨터의 하드디스크 드라이브를 사용자가 사용할 수 없도록 의도된 악성코드이다. 금전이나 데이터 탈취 목적이 아닌 주로 사용자가 PC를 이용할 수 없게 하고 시스템을 복원할 수 없게 만드는 목적으로 사용. 21년 7월, 이란 열차 시스템이 공격받은 사례가 있음

- ④**사회공학적 공격** : 다양한 공격 기술(피싱, 스피어 피싱, SIM 스왑, 중간자 공격, 크리덴셜 변조)을 활용하여 최종이용자의 CBDC 계정 또는 CBDC 시스템의 관리자 계정을 제어 가능
- ⑤**암호키 위변조** : 개인키를 얻어 CBDC 소유권을 탈취하기 위해 컴퓨터 또는 장비 해킹하거나, 이용자의 키를 활용하여 생성된 데이터를 기반으로 암호 해독 또는 부채널 공격을 수행
- ⑥**분산원장 기술(DLT) 또는 스마트 계약 관련 신기술 대상 공격** : 스마트 계약, 분산원장 기술(DLT) 합의 프로토콜, 원장 간 브릿지, 오라클, 프로토콜 거버넌스 등의 보안 취약점을 이용하여 공격 가능
- ⑦**결제 프로세스 위변조** : 결제 프로세스는 다양한 이해관계자들이 관련되어 있어 보안의 격차로 보안 취약점²⁷들이 존재
- ⑧**악의적인 최종이용자 공격** : CBDC 시스템의 최종이용자가 자신의 CBDC 결제 장비나 모바일 애플리케이션에서 사취하거나, 외부와 협력하여 CBDC를 이중 지급 또는 위조하는 등 다양한 공격 시도²⁸
- ⑨**내부자 방해 공격** : CBDC 시스템에 접근할 수 있는 직원(조직에 불만을 느끼고 있는) 또는 계약자는 하드웨어를 손상시켜 시스템이 오작동하게 하거나, 키 정보 삭제, 서비스 차단, 잘못된 데이터 입력, 위협 행위자를 돕는 행위를 수행
- ⑩**내부자 사기** : 악의적인 내부자는 개별 또는 외부와 협력하여 CBDC 시스템 접근권한과 비즈니스 로직에 대한 지식 등을 활용하여 금융사기를 야기
- ⑪**인식부족, 태만, 인적 실수** : 개발자는 사이버보안팀 검토나 어떠한 코드 분석 없는 보안 취약점이 있는 오픈 소스 패키지를 이용할 수 있으며(인식부족), 시스템 운영팀은 보안 패치나 기타 주요 업데이트를 지연시킬 수 있음(태만). 또한, 시스템 관리자가 시스템 유지보수 중 잘못된 명령어를 입력하거나 만료된 디지털 인증서를 갱신하는 것을 잊을 수 있음(인적 실수)
- ⑫**통제 부족으로 인한 정보노출** : 접근관리 통제력이 부족하거나 부재로 인해 직원이 무단접근 가능. 공유 IT 환경의 설정 오류 등의 문제 해결 중에 제3자 서비스 제공사업자는 CBDC 시스템과 관련된 민감한 정보를 볼 수 있음. 또한, 접근통제 로직의 공백 등으로 인해 데이터가 해커에게 노출 가능
- ⑬**인프라 운영 중단** : 자연재해로 인해 광범위하고 장기적인 정전이 발생하면 네트워크 서비스 제공자의 서비스 장애 발생, 사이버 공격으로 인한 광범위한 네트워크 서비스 중단 발생 가능, 또한 시스템 운영자의 실수로 서비스 중단을 초래할 수 있음
- ⑭**기술 오류로 인한 서비스 중단** : 소프트웨어 또는 하드웨어 버그, 완전히 테스트 되지 않은 소프트웨어 패치 및 업그레이드, 만료된 서비스 계정 자격증명 등은 CBDC 시스템 중단을 초래. 기술 구성요소가 많이 포함될수록 기술스택이 복잡하여 장애 발생 위험이 높아짐

²⁷ 결제 없이 구매를 유도, 결제를 타인에게 넘김, 결제 동의를 불필요한 지점에서 결제정보 수집하는 등 악용

²⁸ 이것은 물리적 디바이스나 어플리케이션의 암호 취약점을 노린 공격유형

- ⑮기술의 노후화 : CBDC 시스템에 사용되는 기술이 점차 노후화되고, 공급자들이 지원을 중지하게 되면 기술 업그레이드나 다른 기술로 전환이 필요. 어떤 공급자로부터도 보안 패치 또는 버그 수정이 가능하지 않을 경우, 중앙은행은 운영, 평판, 법적 위험에 직면하게 됨
- ⑯공급망 사업자 대상 공격 : (소프트웨어 또는 하드웨어, 클라우드 또는 데이터 센터 서비스 제공자 등) CBDC 시스템 공급망 관련 서비스 및 솔루션 사업자들은 해커의 주요 공격 대상이 될 수 있음. 어떠한 공격이라도 발생하게 되면 CBDC 시스템의 무결성, 가용성뿐만 아니라 시스템의 민감 정보 관련 기밀성에 영향을 초래할 수 있음

V

정책적 시사점

I 글로벌 주요국의 CBDC 도입 추진으로 더욱 가속화될 Web3.0 패러다임 전환

- 이미 우리 사회는 ICT의 보급·확대를 거치며 현금 없는 사회(Cashless society)로 진입하였고 코로나 팬데믹을 경험하며 비대면 거래가 일상적으로 자리 잡으면서 새로운 유형의 디지털 금융서비스가 소개됨
- 각국의 중앙은행은 이러한 금융경제의 변화에 개도국과 신흥국 중심으로 먼저 반응하기 시작하였고 이제는 선진국을 포함한 많은 나라들이 CBDC 도입을 통해 디지털 금융경제의 변화를 추진 중
- 최근에 추진되고 있는 G7, EU 등 주요국의 CBDC 도입에서 주목할 것은 첫째, 빅테크 기업을 중심으로 등장한 새로운 지급결제 수단에 대한 경계심이며, 둘째, 러시아, 중국 등 사회주의 주도권 국가의 디지털 금융 네트워크 구축에 대한 대응이라고 평가할 수 있음
- 향후 CBDC 기반 글로벌 금융 네트워크의 주도권을 누가 갖게 되는가에 따라 1944년 이후 공고히 유지되어 온 “브레튼우즈체제(Bretton Woods System)”가 붕괴되는 상황을 목격할 수도 있을 만큼의 파괴력을 보유하고 있음
- 더불어 디지털 경제의 축으로 활용될 CBDC의 본격적인 보급과 활용에 대한 기대는 Web3.0 패러다임 전환의 기폭제가 될 것으로 보임. 여기에 CBDC가 블록체인 기반의 암호자산과 어떤 관계를 유지하느냐에 따라 Web3.0 시대로의 변화 속도를 좌우할 것으로 평가됨

I CBDC 도입이 가져올 디지털경제의 확장과 새로운 위협의 증가

- CBDC의 기술스펙은 국가별 다양성이 존재하나 분산원장 방식을 사용하는 국가가 대다수를 차지하고 있으며 민간 시스템과 연동을 통한 활용성을 고려하면 디지털 금융경제의 핵심 축의 역할 수행할 것으로 예상
- 한국은행 등이 발표한 「CBDC 활용성 테스트 추진계획(23.10)」을 통해 제시한 것과 같이 CBDC를 통한 혁신 서비스가 개발되어 디지털경제는 더욱더 확장되어 갈 것으로 보임
- 이와 함께 BIS의 보고서에서 언급된 CBDC 에코시스템을 대상으로 한 다양한 사이버 공격 발생 가능성은 매우 중대한 위협이 될 것으로 생각됨, 그러나 이러한 위협은 기존 금융방식에서도 충분히 일어날 수 있는 위협으로 새로운 위협은 아님

- 우리가 대비해야 할 위협은 아직 알려지지 않은 위협으로 CBDC 및 관련 활용 서비스가 일반 대중에게 이용되는 만큼 단말기, 전자지갑, 블록체인 기반 네트워크를 대상으로 한 보안은 물론이고 새로운 형태의 사회공학적 기법의 공격에 대응할 필요성이 높아짐

■ 가상세계와 현실세계의 “동기화”에 대비한 체계적 준비 필요

- IoT, AI, 빅데이터, 클라우드, 메타버스 등 신기술과 서비스의 융합으로 만들어지는 가상세계의 확장은 글로벌 규모로 확대되고 일상화될 것이며 현실과 밀접해짐에 따라 현실과 가상은 동기화되어 움직일 것으로 예상
- 여기에 CBDC로 대표되는 디지털 금융 시스템이 결합되면서 우리는 지금까지 누리지 못했던 더 많은 혜택과 비즈니스 기회를 갖게 될 것으로 보임
- 현실과 가상의 동기화는 디지털 유용성이 증가하고 있지만, 보안 위협에도 동기화가 발생하여 이용자의 생명과 재산에 영향을 미칠 것으로 전망되고 있어 체계적인 보안 대비 방안을 강구해야 할 필요
- 디지털 확산으로 이미 보안은 일상화되었고, 이용자의 보안 인식 역시 높아졌으나, 그에 못지않게 공격은 더욱 기술은 고도화되고 방법은 교묘하고 치밀해지고 있어 언제든지 우리를 위협으로 몰고 갈 수 있는 상황에 노출되어 있음을 인식해야 함
- 따라서 서비스 도입과 함께 국민의 안전한 이용 환경 제공과 관련 기업의 비즈니스 기반 확대를 위한 민·관 협력체계 구축 및 보안 가이드 개발이 병행되어야 할 것이며, 중장기 정책 방향은 이용자 보호를 최우선으로 하되, 산업 경쟁력이 상실되지 않는 정책적 배려 필요

KISA INSIGHT

DIGITAL & SECURITY POLICY

2023 VOL. 07