KNOM Review '21-02 Vol.24 No.02
https://doi.org/10.22670/knom.2021.24.2.1

블록체인 기반 CBDC 시스템 설계

한 정 수◆°, 김 정 헌*, 우 종 수**, 홍 원 기*

CBDC System Design using Blockchain

Jungsu Han◆°, Jeongheon Kim*, Jongsoo Woo** and James Won-Ki Hong*

요 약

최근 들어 국가별 다양한 이유로 CBDC (Central Bank Digital Currency)에 대한 연구가 활발하게 진행되고 있다. 아울러 블록체인 기술의 눈부신 발전에 따라 이를 기반으로 한 CBDC 시스템이 주목을 받고 있다. 이러한 배경하에 본 논문에서는 기존 은행권에서 효과적으로 사용할 수 있는 블록체인 기반의 CBDC 시스템을 제안하였다. CBDC의 개발과 상용화를 위한 은행권의 여러 요구사항을 분석하였으며, 이를 바탕으로 호환성, 상호운용성, 프라이버시 측면에서 효과적인 시스템 디자인과 이의 구현 방법을 제시하였다.

Key Words : Blockchain, CBDC, Digital Money

ABSTRACT

Recently, research on CBDC (Central Bank Digital Currency) has been actively conducted for various reasons by countries around the world. In addition, with the dazzling development of blockchain technology, blockchain technology is being adopted in CBDC. In this paper, we propose a blockchain-based CBDC system that can be effectively used in the traditional banking system. We also analyze the requirements of CBDC and suggest ways to commercialize CBDC. We present a system design and implementation method, especially in terms of compatibility, interoperability, and privacy.

※이 논문은 하나은행의 "하나은행 CBDC 운용시스템 개념설계 및 MVP 개발" 연구과제와 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (IITP-2021-2017-0-01633,대학ICT연구센터육성지원사업)

◆ First Authorr, ° Corresponding Author : Department of Computer Science Engineering, POSTECH, saw1515@postech.ac.kr
* Department of Computer Science Engineering, POSTECH, {kjheon1118, jwkhong}@postech.ac.kr
** Center for Crypto Blockchain Research, POSTECH, woojs@postech.ac.kr

논문번호 : KNOM2021-02-04, Received November 1, 2021; Revised November 12, 2021; Accepted December 12, 2021

Ⅰ. 서 론

최근 여러 국가에서 중앙은행을 중심으로 디지털 화폐 (Central Bank Digital Currency, CBDC)에 대한 연구가 활발하게 진행되고 있다 [1]. 국제결제은행 (Bank for International Settlements, BIS)은 CBDC를 중앙은행이 직접 책임지며 해당 국가 회계 단위로 표시되는 디지털 결제 수단으로 정의하고 있다 [2]. 예를 들어 가치가 일정한 스테이블코인 (Stable-coin) [3]의 경우에는 중앙은행이 직접 발행하지 않기 때문에 CBDC가 될 수 없다. 또한 디지털 달러의 경우에는 한국은행이 발행을 하더라도, 한국이 책임질 수 있는 회계 단위는 원화 밖에 없기 때문에 CBDC라고 부를 수 없다. 즉, 국가의 중앙은행에서 직접 발행하고 책임질 수 있는 지불 수단이 바로 CBDC이다.

코로나 19로 인한 현금 사용 환경이 줄어들고 비대면 결제가 확대됨에 따라 CBDC에 대한 관심도가 증가하였다. 종이 지폐에 따른 바이러스 전파 가능성에 대한 우려가 존재하며, 사회적 거리 두기나 영업점 봉쇄 등으로 인해 실제 현금을 통한 거래가 급격하게 줄어들게 되었다. 이에 따라 일부 국가의 경우 온라인 뱅킹의 발전으로 인한 시중은행의 지점을 폐쇄나 ATM 사용 제한 등으로 현금에 대한 접근성이 제약될 것이라는 관측이 나오게 되었다 [4]. 이와 달리 온라인 소비는 증가하여 비대면 결제는 확대 되었으며 재난 지원금과 같은 새로운 지급 수단이 등장하게 되었다. 이는 결제 서비스의 안정성에 대한 논의와 함께 정부 주도의 전자 화폐, 즉 CBDC의 필요성으로 이어졌다.

현재 국가별로 CBDC를 연구하는 이유는 크게 3가지로 나뉜다 [5]. 첫 번째는 민간 혁신 금융 발전에 대응하기 위한 것이다. 핀테크와 암호자산 기술 등 새로운 금융 시장이 발달하고, 페이스북이나 JP Morgan에서는 자체적인 스테이블 코인들을 발행하기 시작하여 독자적인 경제시스템을 구축하려고 시도하고 있다 [40]. 또한 엘살바도르에서 비트코인이 법정화폐로 공식적으로 도입되는 사례를 보면서 기존 금융시스템이 느끼는 위기감에 대응하고자 하는 중앙은행의 시도 중 하나가 바로 CBDC이다 [41]. 두 번째로는 글로벌 통화 패권 경쟁을 위해서이다. 현재 중국을 필두로 주요 통화국에서는 CBDC 도입을 위한 논의가 활발하게 진행 중인데, 여기에는 달러 다음의 기축 통화를 자국 화폐로 만들고자 하는 욕구가 반영되어 있다. 중국은 '22년 내에 CBDC 공식 발행을 계획하고 있고, 미국은 '23년 내에 CBDC 공개 계획을 발표하는 등 디지털 위안화나 달러의 국제화를 위한 공격적인 행보를 보이고있다. 마지막으로는 금융시스템을 개선하는 기회로 삼기 위해서다 [42]. 이는 주로 바하마, 동카리브연합, 캄보디아 등 개발도상국이나 신흥국 위주로 시도되고 있으며, CBDC를 공식적으로 사용하며 전통적인 금융시스템이 해결하지 못하고 있는 금융 포용성의 문제 등을 개선하기 위한 노력이다 [43]. 해당 국가들은 금융 접근성이 낮은 사람(Unbanked People)들의 수용을 위한 새로운 금융 인프라 구축 목적과 화폐 관리 비용 절감 등을 목적으로 CBDC를 적극적으로 검토하고 있다.

CBDC를 구현하는 방법은 다양하지만 본 논문에서는 블록체인 기반의 CBDC 시스템을 중심으로 논의하고 있다. 블록체인 기술은 비트코인 [6] 등장으로 주목받게 된 기술로 높은 보안성과 복원력 등이 특징이며, 차세대 금융의 핵심 기술로 주목받고 있다. 그렇기에 CBDC 시스템 구현에 있어 핵심적인 역할을 할 것으로 예상되어 블록체인을 CBDC 시스템의 기반 기술로 선택하게 되었다. 우리는 CBDC의 여러 가지 기술적 요구 기능 중 주로 3가지 요구사항에 대해서 다루고 있다. 이는 타 금융시스템과 쉽게 연동할 수 있는 '호환성', 타국의 CBDC 시스템과 연결 및 소통할 수 있는 '상호운용성' 그리고 현금과 같은 익명성을 구현하기 위한 '프라이버시'로 나뉘게 된다. 또한 각 요구사항을 만족시키는 CBDC 데모 시스템에 대한 설명을 포함하고 있다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 소개하며 3장에서는 시스템 기술 요구사항에 대한 분석과 디자인 및 구현 내용을 설명한다. 4장에서는 구현 시스템에 대한 분석과 함께 그에 대한 평가를 다루고 있으며, 마지막 5장에서는 결론 및 향후 연구 방향을 다루고 있다.

Ⅱ. 관련 연구

CBDC는 크게 거액 결제용(Wholesale) CBDC와 소액 결제용(Retail) CBDC로 나뉘게 된다. 거액 결제용 CBDC는 거래의 효율성과 블록체인의 불변성을 이용한 운영의 리스크 감소 등의 결제 시스템 개선을 목적으로 한다. 그렇기에 이미 금융 인프라가 효율화되어 있는 선진국들 위주로 연구개발 성

격의 많은 프로젝트가 진행되고 있다. 이와 달리 소액 결제용 CBDC의 경우 금융 인프라가 미흡하며 화폐 시스템이 불안정한 국가들에서 지급 결제 시스템의 안정성 유지와 금융 포용성 제고를 목적으로 연구되고 있다. 따라서 개발도상국이나 신흥국들에서 금융 인프라의 퀀텀 점프를 위한 다양한 프로젝트들이 진행되고 있다.

국가별 CBDC 프로젝트 진행현황은 다음과 같다. 캐나다는 Jasper 프로젝트를 통해 R3 Corda를 이용하여 예금과 주식 토큰화를 통한 증권 거래 청산 PoC를 시연한 성과가 있다 [7]. 또한 싱가포르는 Ubin 프로젝트와 연계하여 역외 거래(cross-border payment)에 대한 테스트 또한 완료하였다 [8]. 다수의 국가가 포함된 CBDC 플랫폼 내에서 국가 간 1:N 송금에 대한 필요성이 대두되어 mCBDC 프로젝트가 등장하기 시작하였다. 대표적으로 홍콩-태국을 중심으로 진행되는 Inthanon-LionRock 프로젝트가 있으며 최근 중국이 해당 프로젝트에 참여하게 되었다 [9]. 중국은 2020년 4월부터 쑤저우, 슝안, 청두, 선전에서 디지털 위안화 DCEP 공개 테스트를 진행하며 선진국 중에서 가장 공격적으로 CBDC 프로젝트를 진행하고 있다 [10]. 이외에 바하마의 Sand Dollar [11], 동카리브의 DCash [12] 그리고 캄보디아의 Bakong [13]과 같이 신흥국들 위주로 금융시스템 개선을 위한 CBDC 프로젝트들이 등장하고 있다. 그림 1은 도입 속도의 측면에서 주요 국가별 CBDC 단계 현황을 보여주고 있다.

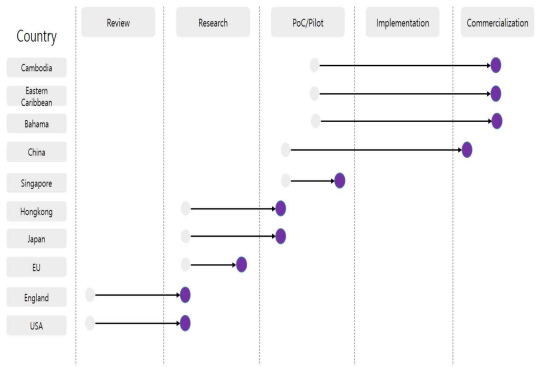


그림 1. 주요 국가별 CBDC 단계 현황
Fig. 1. Global Trends of CBDC Projects

2020년 3월 이후로 CBDC 발행 계획이 없던 일본, 한국, 대만, 유럽연합 등이 CBDC 관련 주제를 적극적으로 검토하게 되었다 [14]. 해당 국가들은 현금과 병행하여 CBDC를 빠르게 도입하고, 장기적으로는 현금을 완전히 대체할 수 있는 CBDC 시스템을 개발하고자 한다. 이런 움직임은 국가적인 차원에서만이 아니라 민간 기업에서도 여러 시도들이 등장하고 있다. Facebook에서는 Libra 프로젝트 [15]를 공식 발표하며, 달러와 유로화 등의 통화와 연동된 스테이블 코인을 발행하고자 하였다. 또한 JP Morgan에서는 이더리움을 변형 시킨 Quorum 기반의 JPM coin을 발행하였다 [16]. 하지만 이런 시도들은 중앙은행의 통화 주권에 대한 도전으로 여겨지면서 프로젝트의 방향성이 크게 바뀌기도 하였다.

블록체인 기반의 CBDC 시스템을 개발하기 위해서는 어떤 블록체인 플랫폼을 사용할 것인지 결정하는 것이 중요하다 [17]. 블록체인의 핵심 원장(core ledger)은 은행이나 고객 간의 거래 순서를 결정하며 거래 정보가 저장되어야 하고 위 변조가 불가능한 시스템이어야 한다. 또한 다수 사용자의 동시 거래를 지원하면서 처리량과 짧은 지연 시간 내에 거래가 체결되도록 보장해야 한다. R3 Corda [18]나 Hyperledger Fabric [19] 기반의 CBDC 시스템이 제안되기도 하였지만, 아직 국제적으로 채택된 표준 CBDC 블록체인 플랫폼은 없는 상태이다. 기존의 블록체인 플랫폼을 변형하여 시스템을 개발중인 경우가 대다수이며, 일부 국가에서는 블록체인 기술 자체를 활용하지 않는 경우도 존재한다. 그렇기 때문에 국가별로 상이한 플랫폼을 연결할 수 있는 기술이 요구된다. 이런 문제를 해결하기 위해 [20]은 이종 블록체인 간의 연결을 지원하는 인터 체인 커뮤니케이션 (Inter-blockchain Communication)의 중요성을 강조하고 있다.

Ⅲ. 시스템 디자인

본 장에서는 CBDC 시스템 개발을 위한 요구사항을 분석하고 이에 적합한 시스템 설계 방법에 대해 설명하고 있다. 또한 이를 적용시킨 CBDC 시스템 데모에 대해서 설명을 포함한다.

1. 기능적 요구사항

CBDC는 법적 제도에 민감하게 영향을 받지만 본 논문에서는 주로 기술적인 부분에 집중하여 시스템 디자인을 하였다. CBDC 시스템의 기술적 요구사항은 여러 프로젝트마다 표현 방법은 조금씩 상이하지만 결과적으로 다음과 같은 기능으로 설명이 가능하다. 우선 CBDC는 디지털 화폐 특성상 사

이버 공격으로부터 높은 보안성이 유지되어야 한다. 디지털화폐의 특징상 지속적인 해킹 공격이나 분실 등의 위험이 존재하기 때문에 보안 기술에 대한 연구가 필수적이다. 또한 거래나 결제 시 즉각적인 완결성을 보장해야한다. 기존의 금융 거래 정산 시스템과 달리 CBDC 즉각적인 결제 완결성을 통한 편의를 제공해야한다. 이는 자연재해나 정전 등의 극단적인 상황 속에서도 365일 무중단으로 운영되는 복원력을 갖춘 시스템으로 구현 되어야한다. 또한 재난 지원금, 지역 화폐 등 특정 조건 하에서 사용 가능한 지불 수단들이 대두되고 있음에 따라, CBDC가 이런 조건을 포용할 수 있도록 설계 되어야한다. 즉, 정부/민간의 다양한 사업 기능들을 구현할 수 있는 프로그램 가능한 시스템을 제공해야하는 것이다.

우리는 블록체인 기술을 통해 앞서 말한 보안성, 결제 완결성, 복원력, 프로그램 가능성을 충족시켰다. 블록체인은 비가역적인 해시함수를 통한 보안성, 합의 알고리즘을 통한 결제 완결성, 분산 노드 구현을 통한 복원력 그리고 스마트 컨트랙트 [21]를 이용한 프로그램 가능성을 제공한다. 이 때문에 본 논문에서는 블록체인 기반의 CBDC 시스템만을 고려하고 있다. 하지만 블록체인을 사용하여 CBDC 개발 시 다음과 같은 요구 기능들을 충족 시키기 위해서는 추가로 고려 해야하는 부분이 존재한다. 첫 번째로는 확장성 문제이다. 확장성은 크게 기능적 확장과 네트워크의 확장으로 나누어 설명 가능하다. 기능적 확장은 주로 CBDC 국내 유통 시 소액 결제에 사용될 수 있을 만큼의 TPS를 제공해야 한다는 것이고 네트워크의 확장은 국가 간의 CBDC 유통 시 상호운용성이 보장되어야 한다는 것이다. 우선 기능적 확장의 경우 TPS는 탈중앙화 정도와 그에 따른 합의 알고리즘 종류에 따라 크게 영향을 받는데 CBDC의 경우 중앙은행이라는 명확한 발행 주체가 존재하기 때문에 소액결제에 요구되는 TPS를 만족시키는 데 어려움이 없다. TPS를 향상시키는 다양한 연구들이 이미 활발하게 진행되고 있으며 예를들어 Solana 프로젝트 [22]의 경우 65,000 TPS를 제공하는 우수한 성능을 보여주고 있다. 하지만 이와 달리 네트워크의 확장은 추가적인 연구가 많이 필요한 분야이다. 현재 시중에는 비트코인, 이더리움과 같은 대형 플랫폼 이외에도 수많은 블록체인 프로젝트들이 존재한다. 현재 CBDC 시스템 규격에 대한 범국가적인 합의는 이루어지지 않은 상태이기 때문에 국가별로 다양한 기존 블록체인 프로젝트를 변형시키거나 독자적으로 플랫폼을 개발함으로써 CBDC를 개발하고 있다. 그러나 대부분의 블록체인 플랫폼들은 자체 플랫폼 내에서만의 트랜잭션을 지원할 뿐 이종 블록체인과의 트랜잭션을 지원하고 있지 않다. 그렇기 때문에 국가 간 CBDC 유통을 위해서는 블록체인 간의 트랜잭션 교환이 가능한 상호운용성이 보장되어야한다. 현재 Cosmos [23], Polkadot [24]과 같은 프로젝트에서 블록체인 간 통신(Inter-Blockchain Communication, IBC) 프로토콜에 대한 연구를 진행 중이며 본 논문에서는 Comos 블록체인을 역외 거래 시나리오를 구현하였다. 또한 국내 유통의 관점의 상호운용성에서는 기존 레거시 금융시스템과 적절하게 병행될 수 있는 호환성이 보장되어야 한다. 중앙은행-시중은행 형태로 나뉘어진 금융시스템과 쉽게 호환되어야만 CBDC의 저변 확대가 이루어질 것이다. 우리는 이를 위해 투 티어(two tiered) 아키텍처를 설계하였다.

마지막으로 CBDC는 사용자의 편의성과 프라이버시 보호를 위해 기밀성과 익명성을 갖추어야만 한다. 공개 장부(Public ledger)를 사용하는 CBDC의 경우 중요한 거래 정보들이 블록체인에 기록되어 쉽게 노출될 가능성이 있다. 또한 거래 송수신자의 지갑 주소와 거래 당사자의 신원이 1:1로 대응될 경우 개인 프라이버시에 심각한 침해를 끼치게 된다. 실제 현금을 신용카드와 같은 디지털 결제 수단보다 선호하는 이유도 이와 같다. 그렇기에 법적인 규제 내에서 프라이버시를 지킬 수 있는 암호화 기술이 적용되어야 한다. 하지만 규제를 벗어난 탈세, 돈세탁, 테러 자금 등에 사용 되는 거래에 대해서는 사용자 추적이 가능해야한다.

본 논문에서는 CBDC 시스템 개발을 위한 요구사항 중 호환성, 상호운용성, 프라이버시 3가지를 중심으로 다루고 있다. 다음 절 부터는 각 요구사항의 설계 방법과 구체적인 구현 방법에 대해 설명하고 있다.

2. 호환성

CBDC 시스템에서 호환성이란 중앙은행과 시중은행 구조로 나누어져 있는 전통적인 방식의 은행 시스템을 따르는 것을 말한다. 이는 투 티어 (two tier) CBDC 라고 불리며, 중앙은행에서는 발행과 회수 등 M0 CBDC 관리를 담당하고 시중은행에서는 CBDC의 원활한 유통을 관리하는 구조이다 [25]. 즉, 중앙은행에서는 CBDC의 돈으로써의 지불 기능을 중심적으로 담당하며 시중은행에서는 CBDC를

보관하고 관리하는 기능을 주로 담당하게된다. 이런 투 티어 시스템은 전통적인 은행 시스템에 적절하게 융합되어 초기 CBDC 도입 시 발생할 수 있는 다양한 문제들을 유연하게 해결할 수 있게 해줄 것으로 예상된다. 예를 들어 CBDC는 기존 종이 화폐보다 유통량을 쉽게 확인할 수 있어 발행량을 효율적으로 조정하며 관리의 용이성을 제공할 수 있다. 그림 2은 중앙은행에서 발행된 CBDC가 시중은행을 통해서 일반 고객이나 상점에 유통되는 과정을 모식도로 그린 것이다.

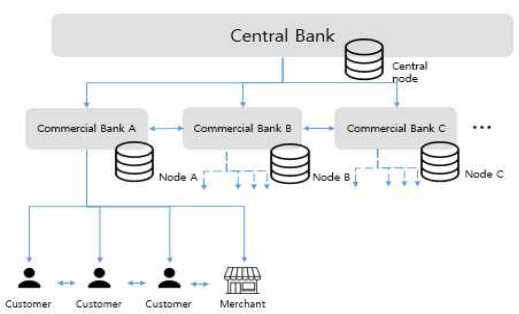


그림 2. 투 티어 (two tier) CBDC 시스템
Fig. 2. Two-tier CBDC System

중앙은행과 시중은행은 각각 독립적인 노드를 운영하며 CBDC 블록체인 네트워크에 구성원으로서 참여한다. 트랜잭션 발생 시 각 노드는 트랜잭션의 이상 여부를 확인하고 이상이 없을 시 새로운 블록에 트랜잭션을 기록하고 네트워크를 통해 연결된 다른 은행 노드에 블록을 전파하게 된다. 네트워크를 통해 해당 블록에 대한 합의가 이루어진다면 메인 체인에 기록되고 트랜잭션 수행이 성공적으로 종료된다. 이와 같이 블록체인을 이용할 경우 별도의 은행 간 정산 과정 이 필요한 기존 지급결제 시스템 보다 빠른 결제 완결성이 보장될 수 있다. 또한 거래 위변조가 어렵고 권한이 있을 경우 거래 기록을 조회하는 것이 쉽기에 개인이나 개별 은행의 악의적인 행위를 금융 당국에서 쉽게 감지할 수 있다.

CBDC 주 사용층인 개인이나 상점의 경우에는 네트워크에 직접적으로 참여하진 않는다. 이는 개인이 노드를 운영하기에는 리소스적인 한계가 있으며, 합의 과정이나 트랜잭션 생성 시 악의적인 행위를 할 위험성이 존재하기 때문이다. 그렇기에 본 논문에서는 개인, 상점 고객의 경우에는 시중은행을 통한 간접적인 방식으로 네트워크에 참여하게 된다.

중앙은행-시중은행-고객으로 구성된 투 티어 CBDC 시스템에서는 각 사용자들의 역할과 권한이 명확하게 구분되어야 한다. 예를 들어 CBDC 발행을 담당하는 중앙은행이 시중은행과 고객보다 CBDC에 더 높은 권한을 가져야 한다. 또한 시중은행의 경우 개인 고객을 관리하거나 CBDC 트랜잭션을 생성하는 등 개인 고객 보다 많은 권한을 가져야 한다. 앞서 설명하였듯이 개인 고객은 네트워크에 직접 참여하기 어렵기 때문에 시중은행을 통해서만 CBDC 거래가 가능하다. 이와 같은 투 티어 CBDC 시스템은 간접 CBDC (indirect CBDC) 구조라고도 불린다. 은행의 개입 없이 고객 간에 직접 CBDC 송금이 있을 경우에는 자금 세탁과 불법적인 행위로 CBDC가 사용될 위험이 크기 때문에 직접 CBDC (direct CBDC)가 아닌 간접 CBDC 디자인을 채택하게 되었다.

3. 상호운용성

상호운용성은 여러 국가 간의 CBDC 역외거래를 지원하기 위해 필요하다. Bank of Canada에서는 CBDC를 디자인할 때 국제적인 활용도 측면에서 고려되지 않으면, 기존의 지불 시스템과 큰 차이가 없을 것이라는 지적을 하였다 [26]. 전통적인 방식의 해외 송금과정은 SWIFT [27]라는 중개를 통해 진행된다. CBDC의 경우도 국가별로 다른 통화 단위를 동일하게 변환 시켜주는 국가나 중개자를 요구할 수가 있다. 그림 3는 CBDC가 역외거래 되는 시나리오의 예시이다.

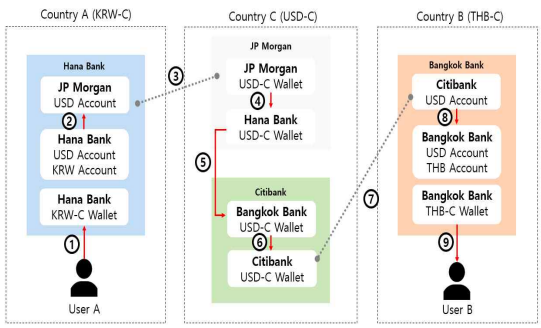


그림 3. CBDC 역외거래 시나리오 예시
Fig. 3. An Example of CBDC Cross-border Payment

현재 원화를 태국 바트로 바꾸기 위해서는 원화를 달러로 환전을 한 다음 달러를 바트로 바꾸어야 하는 이중 환전이 일어난다. CBDC 또한 동일한 과정으로 진행된다고 하였을 때 자세한 동작 과정은 다음과 같다.

1) User A가 하나은행 KRW-C 지갑에 KRW-C BDC (이하 KRW-C)를 송금한다.
2) 하나은행에 개설되어 있는 하나은행 USD 계좌에서 JP Morgan USD 계좌에 예치한다.
3) JP Morgan은 해당 예치 내역을 확인한다.
4) JP Morgan의 USD-CBDC (이하 USD-C) 지갑에서 하나은행 USD-C 지갑에 USD-C를 송금한다.
5) 하나은행의 USD-C 지갑에서 방콕은행 USD-C 지갑에 USD-C를 송금한다.
6) 방콕은행의 USD-C 지갑에서 시티은행 USD-C 지갑에 송금한다.
7) 시티은행에서 해당 송금 내역을 확인한다.
8) 시티은행 USD 계좌에서 방콕은행 USD 계좌로 USD를 출금한다.
9) 방콕은행의 THB-C 지갑에서 User B로 송금한다.

이와 같은 방법을 통해서 기존 방식과 유사하게 중개 CBDC (USD-C)를 이용하여 해외 송금 과정을 설계하는 것이 가능하다. 하지만 실제 CBDC 교환이 일어나는 국가 이외에 제 3자가 개입하게 된다면 수수료나 처리 속도 측면에서 비효율적이게 된다. 그렇기에 본 논문에서는 좀 더 효율적인 방법으로 블록체인 간 통신을 기술을 제안한다. A 국가에서 자체 CBDC 블록체인 플랫폼인 Chain A를 사용하고 B 국가에서는 Chain B를 사용한다고 가정한다. 이 때 Chain A와 Chain B가 동일한 플랫폼인 경우에는 두 국가 간의 CBCD 송금은 국내 송금과 동일하게 처리될 수 있다. 하지만 플랫폼이 다를 경우에는 이 둘을 연결할 시스템인 중계자(relayer)가 필요하다. 중계자는 인터체인 표준(interchain standard)를 만족시키는 이종 블록체인 간의 통신을 IBC (Inter-Blockchain Communication) 프로토콜을 이용하여 가능하게 한다. 그림 4는 IBC 프로토콜을 이용한 체인 간 통신을 표현한 것이다.

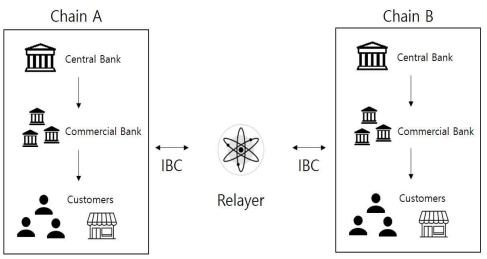


그림 4. IBC 프로토콜을 이용한 국가 간 송금 시나리오
Fig. 4. Cross-border Payment using IBC Protocols

본 논문에서는 IBC 프로토콜 구현을 위해 Cosmos 블록체인[23]을 이용하였다. Cosmos는 존(Zone)이라 불리는 독립적인 블록체인들로 네트워크를 구성하고 있다. 그리고 이는 허브(Hub)라고 불리는 블록체인을 통해 각기 다른 존을 연결하는 역할을 수행하게 된다. CBDC 시스템에서 이를 적용할 경우 허브는 각 국가의 CBDC 총액을 추적하는 역할을 수행하며 허브를 통과하며 다른 국가로 CBDC를 송금하는 형태로 구현하는 것이 가능하였다.

4. 프라이버시

프라이버시는 CBDC 사용 저변 확대를 위해 필수적인 부분이다. 블록체인을 활용한 CBDC의 특성상 모든 트랜잭션 정보가 CBDC 원장에 기록되게 된다. 이는 사생활 보호 측면에서 CBDC 보다 현금을 선호하게 만드는 요인이다. 그렇기 때문에 CBDC가 실생활에 적극적으로 사용되기 위해서는 거래 기록의 프라이버시가 보호되어야 한다. 본 논문에서는 CBDC 프라이버시를 크게 블록체인 내에서 암호화 기술을 통해 거래 기록을 숨기는 On-chain 프라이버시와 고객이 은행을 통해서 거래를 요청할 때 생길 수 있는 Off-chain 프라이버시로 나누고 있다.

우선 On-chain 프라이버시의 경우 Monero [28], Dash [29], Zcash [30]와 같은 프로젝트들에서 활발하게 연구되고 있다. 이 프로젝트들은 비트코인의 가명(pseudonymous) 주소가 트랜잭션 분석을 통해 추적 가능하여 익명성의 한계가 있는 문제를 해결하고자 한다. 링 서명(ring signature) [44]를 사용하여 송금자를 식별할 수 없게 하거나 송금 지갑 주소와 수신 지갑 주소를 섞는 믹싱(mixing) 서비스 [45]를 통해 트랜잭션을 추적하는 것을 어렵게 하는 것이 가능하다. 이런 방식의 경우 송신자와 수신자만이 거래를 알 수 있게 된다. 하지만 CBDC와 같이 중앙은행이나 금융당국이 거래 기록을 조회해야 할 경우가 발생할 경우 암호화 된 거래 기록을 복호화하는 것이 가능해야 한다. 자금 세탁과 탈세 등을 방지하기 위한 것으로 추적가능한 익명성이 요구된다. 이를 위해 우리는 CBDC 원장에 기록된 트랜잭션을 중앙은행이나 금융당국의 공개키로 암호화가 되어있으며 필요에 따라 복호화 하는 것이 가능하게 하였다.

Off-chain 프라이버시의 경우 시중은행과 고객 사이에서 발생하는 민감정보 유출 등의 문제에 대한 해결책을 중심으로 다루고 있다. 개인 고객의 경우

자체적인 노드를 구축하고 운영하는 것이 비용이나 보안의 측면에서 효율적이지 않기 때문에 은행을 통해서 CBDC 네트워크에 간접적으로 참여하게 된다. 하지만 이는 시중은행이 개인 고객의 잔고나 지갑주소와 같은 개인정보를 모두 다 소유하고 있어야만 한다는 것을 의미하지 않는다. 만약 On-chain 프라이버시를 통해서 원장 내에서 트랜잭션의 익명성이 보장된다 하더라도 은행을 통해 트랜잭션을 기록하는 은행에서 거래를 원장에 추가하기 전에 기록을 조회하는 것이 가능하다. 이는 On-chain 프라이버시를 무의미하게 만드는 행위이므로 Off-chain에서도 암호화 기술을 이용하여 민감 정보가 유출되지 않도록 해야한다. 즉, Off-chain 프라이버시는 은행이 트랜잭션을 CBDC 네트워크에 기록할 때 송신자와 수신자를 알 수 없게 하기 위한 것이다.

[31]는 거래 수단에 따른 프라이버시 수준을 분석하며 영지식 증명(Zero-Knowledg proof) [32], 다자간 서명 방식(Multi-party computation) [33], 차등 개인정보 보호(Differential privacy) [34] 등 CBDC 프라이버시를 위한 기술들을 제시하고 있다. 본 논문에서는 이 중 영지식 증명 방법을 이용한 Off-chain 프라이버시 보호 방법을 제시하고 있다. 영지식 증명이란 어떤 문제에 대한 해답은 제공하지 않으면서 해답을 알고 있다는 것을 증명하고 싶을 때 주로 사용된다. CBDC 거래 시 은행은 자신의 고객의 트랜잭션만을 서명 해야 할 것이다. 이 때, 우리는 은행이 고객에 대해 필요한 최소 정보인 CBDC 잔고와 해당 고객이 자신이 고객인지 여부에 대한 확인을 영지식 증명을 통해 증명하는 방식을 제안하고 있다. 그림 5는 Off-chain 프라이버시를 위한 영지식 증명 시스템의 동작 방법이다.

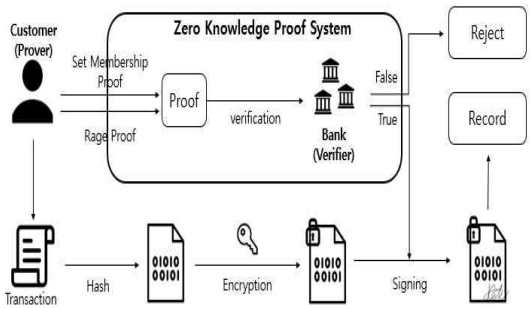


그림 5. 영지식 증명을 이용한 CBDC 프라이버시 시스템
Fig. 5. Zero Knowledge Proof System for CBDC Privacy

1) 고객은 자신의 은행에 수신자, 송신자, 송금 금액이 포함된 서명되지 않은 트랜잭션(unsigned transaction)을 생성하고 이를 암호화한다. 고객은 자신의 키로 트랜잭션을 암호화하는 것이 아니라 중앙은행이나 금융당국이 복호화할 수 있도록 해당 기관의 공개키로 암호화를 한다.
2) 고객은 자신이 거래하고자 하는 은행의 등록된 회원임과 거래를 정상적으로 성공시킬 잔고가 있다는 증명(proof)을 생성한다.
3) 은행은 고객이 보낸 증명을 통해 고객이 자신의 은행 회원이며 거래를 정상적으로 생성할 수 있다는 것을 확인한다.
4) 은행은 고객이 보낸 암호화된 서명되지 않은 트랜잭션을 서명하여 CBDC 원장에 기록한다.

이와 같은 과정을 통해 은행에게 거래 정보나 송수신자의 정보를 숨긴 채 노드를 운영하지 않는 개인 고객이 은행을 통해 트랜잭션을 생성하는 것이 가능하다.

Ⅳ. 구현 방법

1. 개발 환경

본 데모는 NodeJS [35] 기반의 React [36] 라이브러리를 사용하여 작성되었다. 데모에서 필요한 데이터의 요청과 저장을 위한 데이터베이스로는 편리한 개발을 위해 구글의 Firebase [37]를 사용하였다.

국가 간 송금 시나리오 데모를 위한 블록체인 플랫폼으로 중계자(relayer) 블록체인을 위해서는 Cosmos 블록체인을 사용하였다. 또한, 송금에 참여하는 두 국가가 이종 블록체인에서 역외거래가 발생하는 것을 시현하기 위해 각각 카카오에서 개발한 클레이튼 [38]과 라인에서 개발한 LFB (Line Financial Blockchain) [39]을 사용하였다. 그리고 두 이종 블록체인을 연결할 중계자 블록체인으로는 Cosmos [23] 블록체인을 이용하였다.

프라이버시 시스템을 개발하기 위해 zkrp 라이브러리 [46]와 easpki 라이브러리 [47]를 변형하여 사용하였다. 이 때, On-chain 상에는 중앙은행의 공개키로 암호화 되어 트랜잭션이 기록된다고 가정하였다. 본 논문의 한국어 버전의 데모 실행 영상은 유튜브 링크[1]를 통해 확인이 가능하다.

1) https://www.youtube.com/watch?v=DqvWH7rcHTU

2. 중앙 은행 및 시중은행

본 데모에서 중앙은행은 CBDC의 발행 일자, 사용처, 발행 금행, 시간에 따른 감소율 등을 설정할 수 있다. 발행된 CBDC는 유통을 위해 시중은행에 배정하게 되며 발행부터 배정까지의 기록은 모두 트랜잭션으로 만들어져 블록체인에 기록된다. 이를 통해 필요에 따라 블록체인에 요청을 보내 필요한 트랜잭션을 확인하는 것이 가능하다. 시중은행의 경우에는 배정받은 CBDC를 개인 고객에게 유통하는 것을 담당하게 된다. 이는 재난 지원금 같은 자금을 시중은행을 통해 수취하는 과정과 유사하게 진행되었으며 시중은행은 고객이 수취한 CBDC의 유효기한, 사용처, 사용금액 등을 확인이 가능하도록 하였다. 또한, 거래 기록을 확인하는 것이 가능한 대시보드를 구현하여 이상 거래나 불법 거래를 탐지할 수 있도록 하였다.

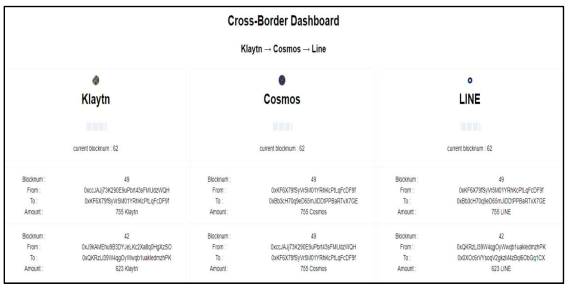


그림 6. 국가 간 CBDC 거래 대시보드
Fig. 6. CBDC Dashboard for Cross-border Payments

우리는 중앙은행과 시중은행의 CBDC 발행 및 유통 측면 이외에도 역외 거래를 위한 대시보드 또한 구현하였다. 상이한 블록체인 플랫폼을 사용하는 두 국가를 클레이튼(국가 A)과 LFB(국가 B)을 이용하여 구현하였으며 그를 연결하는 중계자를 Cosmos 블록체인을 이용하여 구현하였다. 국가 A에서 국가 B로 송금하는 시나리오는 곧 클레이튼을 Cosmos를 중계자로 이용해 LFB으로 전환하는 것과 동일하다. 이를 위해 Cosmos에서 제공하는 Atom 코인을 이용하여 우선 클레이튼을 Atom으로 전환하였다. 현재 Cosmos 블록체인은 클레인트과 LFB과의 호환성을 지원하지 않기 때문에 클레이튼과 LFB 네트워크에 별도의 Cosmos 지갑을 만들어 해당 지갑을 통해 역외 거래 데모를 진행하였다. 곧 클레이튼에서 Cosmos로 송금 시 클레이튼 상에 있는 Cosmos 지갑에 환전 금액만큼 송금하게 되고 이 값을 확인하여 LFB 네트워크 상에 있는 Cosmos 지갑에 서 수신자의 링크 코인 지갑 주소로 송금 값 만큼 링크 코인으로 전달하게 된다. 이 때 클레이튼과 Atom, LFB의 적용 환율은 거래소의 시장가를 이용하여 설정하였다. 해당 과정을 구현한 대시보드는 그림 6과 같다.

이와 같은 과정을 통해 네트워크에 참여한 사람들은 CBDC 해외 송금 시 발생하는 수수료나 거래 과정을 투명하게 확인하는 것이 가능하며 CBDC 시스템의 상호운용성을 확인을 확인할 수 있다.

3. 개인 고객

개인 고객은 CBDC 주 사용 계층으로 다양한 CBDC 거래를 은행에 요청하게 된다. 본 데모에서는 기본적으로 CBDC 교환, 결제, 송금 시스템을 구현하였다. 또한, 고객은 자신이 거래한 기록을 볼 수 있으며 결제를 취소할 수 있는 기능을 추가하였다. 그림 7 좌측 그림은 CBDC 사용자 인터페이스이며 우측 그림은 사용자의 행동에 따라 블록체인에 기록되는 것을 보여주는 인터페이스이다.

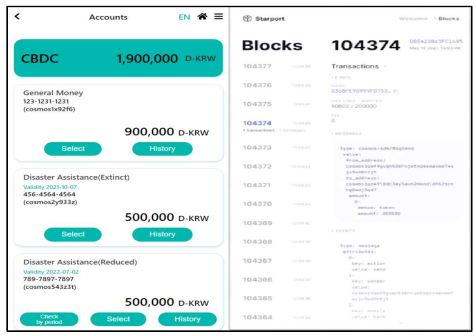


그림 7. CBDC 사용자 인터페이스
Fig. 7. User Interface of Demo Application

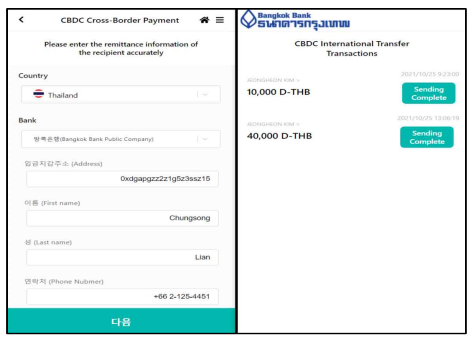


그림 8. 국가 간 CBDC 거래 유저 인터페이스
Fig. 8. User Interface of Cross-border Payments

이외에도 해외 송금 기능을 구현하여 원하는 국가 간에 송금 및 결제를 할 수 있도록 하였다. 본

데모에서는 고객이 직접 트랜잭션을 생성하는 것이 아니라 고객이 은행에 정보를 전달하고 은행이 트랜잭션을 생성하여 블록체인에 기록하는 형태로 구현되어있다. 그림 8는 해외 송금 실행 화면이다.
우리는 이를 통해 중앙은행-시중은행 형태의 투 티어 CBDC 모델을 통해 기존 금융 서비스와 호환이 가능하도록 하였다.

4. 프라이버시

프라이버시 시스템의 구현 가능성을 검증하기 위해 우리는 on/off-chain 각각에 대한 데모를 구현하였다. on-chain 프라이버시를 위해 고객의 거래를 암호화 시켜 이를 블록체인 네트워크에 기록하는 방법을 제시하였다. 이를 위해 우리는 PKI (Public Key Infrastructure) 시스템을 스마트컨트랙트를 이용하여 구축하였으며, 이를 이용하여 고객과 은행이 사용하는 키를 관리하도록 하였다. 스마트컨트랙트는 다음과 같은 기능으로 동작한다.

- *register(trustedEntity, PublicKey)*: 신뢰할 수 있는 엔터티(중앙은행)를 공개키를 이용하여 추가한다. 해당 기관은 디지털 인증서를 저장하고 발행하며 서명하는 역할을 한다.
- *append(data, hash)*: 은행이나 고객이 중앙은행으로부터 확인 받아야할 인증서를 전파한다.
- *sign(certId, expiry)*: 중앙은행이 인증서에 서명을 하고 유효기한을 설정한다.
- *revoke(signId)*: 중앙은행이 서명을 취소한다.

PKI를 이용하여 고객은 중앙은행이나 금융 당국만이 확인 가능하도록 트랜잭션을 암호화하는 것이 가능하다. 또한, 시중은행은 고객의 프라이버시를 지키면서 서명하는 것이 가능하다. 스마트컨트랙트 개발을 위해 우리는 [48]을 수정하여 이더리움 스마트컨트랙트를 작성하였으며 트랜잭션에 사용되는 가스 비용을 측정하였다. 표 1은 스마트컨트랙트에서 각 기능별로 사용되는 가스 사용량이다.

표 1. PKI 스마트컨트랙트 트랜잭션 비용
Table 1. Transaction Cost of PKI Smart Contract

Function	Transaction cost (gas)
Register	112,882
Append	95,016
Sign	23,567
Revoke	23,966

각 기능별 트랜잭션 비용은 현재 이더리움 네트워크에서 사용되는 다른 스마트컨트랙트들 보다 가스를 적게 사용하는 것으로 확인되었다.

off-chain 프라이버시를 위해서 우리는 고객이 거래를 위한 잔고가 충분한지와 은행의 고객인지 확인하기 위해 영지식 범위 증명(Zero-Knowledge Range Proof, ZKRP)를 생성하게 하였다. 고객이 은행에 속하였는지 확인하는 집합 증명(Set Membership, SM)은 집합을 수로 변환하는 것이 가능하기 때문에 범위 증명만을 이용하여 off-chain 프라이버시를 구현하는 것이 가능하다. ZKRP를 구현하기 위해 Bulletproof [49]를 활용하였다. Bulletproof는 증명크기가 작으며 매 트랜잭션 생성마다 신뢰 구축(trusted setup)을 하지 않아도 되어 블록체인 기반의 CBDC 시스템을 구현하는데 적합하였다.

우리는 [50]을 수정하여 ZKRP를 개발하였으며 데모는 Go 언어로 구현되어있다. off-chain 프라이버시를 CBDC 시스템에 적용하게 되면 추가적인 오버헤드 비용이 발생하게 된다. 우리는 증명 범위에 따른 증명의 크기와 증명 생성을 위한 3가지 과정의 소요 시간을 측정하였다. 실험 환경은 64-bit Intel(R) Core(TM) i9-9880H CPU @ 2.30GHz, 32GB RAM이며 운영체제는 ubuntu 19.04를 사용하였다. 실험 결과는 표 2와 같다.

표 2. 증명 범위에 따른 증명 크기 및 시간 복잡도
Table 2. Proof Size and Time Complexity of Range Proof

Range (param)	Proof Size (Byte)	Setup (ms)	Prove (ms)	Verify (ms)
0 ~ 16 (4bit)	16,633	1.33 ±0.12	1.46 ±0.90	9.23 ±0.28
0 ~ 256 (8bit)	25,289	2.40 ±0.46	28.43 ±0.6.	15.45 ±0.25
0 ~ 65,536 (16bit)	41,884	3.95 ±0.38	54.06 ±0.46	27.80 ±0.25
0 ~ 4,294,967,296 (32bit)	74,421	7.88 ±0.85	104.83 ±2.41	52.87 ±1.69

실험 결과 실제 거래에서 사용될 수 있는 범위 내에서 범위 증명을 생성하는 전체과정이 0.2초 이내에 완료되는 것을 확인하였다.

V. 결 론

본 논문에서는 CBDC 시스템 개발을 위한 요구사항을 분석하고 각각에 맞는 디자인 및 구현 방법에 대해 제안하였다. 블록체인을 활용하여 CBDC

시스템의 보안성, 결제완결성, 복원력 등을 확보하였으며, 기존 금융시스템과의 호환성과 국가간 거래를 위한 상호운용성 그리고 사용자 개인정보 보호를 위한 프라이버시에 대한 기술적 해결책을 제시하였다. 또한, 이 요구사항들을 충족시키는 데모 프로젝트를 개발하여 구현 가능성을 확인하였다.

향후 연구에서는 CBDC 시스템의 키 관리 방법이나 지갑 관리 방법, 그리고 기존 법적 규제를 준수하며 CBDC가 상용화될 수 있는 다양한 방법들에 대해 연구할 계획이다. 또한 이기종 블록체인간의 토큰 스왑(sawp) 기능 개발을 통한 우수한 호환성을 가진 CBDC를 연구할 계획이다.

References

[1] Auer, R. A., Cornelli, G., & Frost, J., "Rise of the central bank digital currencies: drivers, approaches and technologies," CESifo Working Paper, no. 8655, 2020.

[2] Boar, C., Holden, H., & Wadsworth, A., "Impending arrival – a sequel to the survey on central bank digital currency," BIS paper, no. 107, p. 19, 2020.

[3] Mita, M., Ito, K., Ohsawa, S., & Tanaka, H., "What is stablecoin?: A survey on price stabilization mechanisms for decentralized payment systems," 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), pp. 60-66, 2019.

[4] Center for Cryptocurrency & Blockchain Research [POSTECH CCBR]. Blockchain Trend. YouTube. https://www.youtube.com/channel/UCCKFHV5J8G1iFXar6kYAi6A

[5] Upbit [UDC]. (2021, 9). CBDC Global Trend & Future [Video]. YouTube. https://www.youtube.com/watch?v=eIoD1i1aHmY

[6] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019

[7] JASPER: James Chapman, Rodney Garratt, Scott Hendry, Andrew McCormack, and Wade McMahon. Project jasper: Are distributed wholesale payment systems feasible yet. Financial System, 59, 2017

[8] UBIN : Darshini Dalal, Stanley Yong, and Antony Lewis. The future is here – project ubin: Sgd on distributed ledger. Monetary Authority of Singapore & Deloitte, 2017.

[9] Inthanon :Chananun Supadulya, Kasidit Tansanguan, and Vijak Sethaput. Project inthanon and the project dlt scripless bond. 2019

[10] Peters, M. A., Green, B., & Yang, H. (2020). Cryptocurrencies, China's sovereign digital currency (DCEP) and the US dollar system.

[11] Sanddollar, "Digital Bahamian Dollar Sand Dollar" [Online]. Available: https://www.sanddollar.bs/

[12] ECCB, "What You Should Know" [Online]. Available: https://www.eccb-centralbank.org/p/what-you-should-know-1

[13] Bakong : The next-generation mobile payments and banking. Available at https: //bakong.nbc.org.kh/.

[14] Boar, C., Holden, H., & Wadsworth, A. (2020). Impending arrival – a sequel to the survey on central bank digital currency. BIS paper, (107).

[15] Facebook, "Diem" [Online]. Available: https://www.diem.com/

[16] Morgan, J. P. (2016). Quorum whitepaper. New York: JP Morgan Chase.

[17] Han, J et al., Design of Blockchain-based CBDC Architecture and Transaction Key Management System, KNOM Conference 2021, pp. 65-68, 2021.

[18] Calle, G., & Eidan, D., "Central Bank Digital Currency: an innovation in payments," R3 White Paper, 2020.

[19] Maharjan, S., Ko, K., Kang, C., Woo, J., & Hong, J. W., "A Study of CBDC Model Applicable for the Current Banking Environment", KNOM Conference 2020, pp. 56-60, 2020.

[20] Qasse, I. A., Abu Talib, M., & Nasir, Q. "Inter blockchain communication: A survey," ArabWIC 6th Annual Interna-tional Conference Research Track, pp. 1-6, 2019.

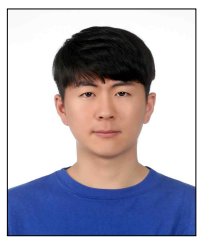
[21] Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday.

[22] Yakovenko, A. (2018). Solana: A new architecture for a high performance blockchain v0. 8.13. Whitepaper.

[23] Kwon, J., & Buchman, E. (2019). Cosmos whit

epaper. 2020-10-08]. https://cosmos. network/resources/whitepaper.
[24] Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. White Paper, 21.
[25] Bindseil, U. (2020). Tiered CBDC and the financial system, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3513422.
[26] Ledger Insight, "BIS, World Bank, IMF urge CBDC interoperability for cross border payments" [Online]. Available: https://www.ledgerinsights.com/bis-world-bank-imf-m-cbdc-cross-border-payments/
[27] SWIFT Inst., Swift [Online], Available: https://www.swift.com/
[28] Alonso, K. M., & Joancomartí, J. H. (2018). Monero-Privacy in the Blockchain. Cryptology ePrint Archive.
[29] Duffield, E., & Diaz, D. (2015). Dash: A privacycentric cryptocurrency.
[30] Electric Coin, "Zcash" [Online], https://z.cash.
[31] Darbha, S., & Arora, R. (2020). Privacy in CBDC technology (No. 2020-9). Bank of Canada.
[32] Blum, M., Feldman, P., & Micali, S. (2019). Non-interactive zero-knowledge and its applications. In Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali (pp. 329-349).
[33] Yao, A. C. (1982, November). Protocols for secure computations. In 23rd annual symposium on foundations of computer science (sfcs 1982) (pp. 160-164). IEEE.
[34] Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Found. Trends Theor. Comput. Sci., 9(3-4), 211-407.
[35] NodeJS, https://nodejs.org/
[36] React, https://reactjs.org/
[37] Firebase, https://firebase.google.com/
[38] GroundX, "Klaytn" [Online], Available: https://www.klaytn.com/Klaytn_PositionPaper_V2.1.0.pdf
[39] Line, "Line Financial Blockchain" [Online], Available: https://blockchain2-org.line-apps.com/whitepaper/
[40] JP Morgan, "J.P. Morgan Creates Digital Coin for Payments" [Online], Available: https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments
[41] Forbes, "An Economic History Of El Salvador's Adoption Of Bitcoin" [Online], Available: https://www.forbes.com/sites/rogerhuang/2021/06/27/an-economic-history-of-el-salvadors-adoption-of-bitcoin/?sh=b1bbd993fd41
[42] Central Banking, "PBoC's digital yuan on track for 2022 Winter Olympic debut" [Online], Available: https://www.centralbanking.com/fintech/cbdc/7879426/pbocs-digital-yuan-on-track-for-2022-winter-olympic-debut
[43] BIS, "Central bank digital currencies as superheroes?" [Online], Available: https://www.bis.org/cpmi/speeches/sp211026.htm
[44] Wikipedia, "Ring Signature" [Online], Available: https://en.wikipedia.org/wiki/Ring_signature
[45] Wikipedia, "Cryptocurrency tumbler" [Online], Available: https://en.wikipedia.org/wiki/Cryptocurrency_tumbler
[46] zkrp Library, https://github.com/ing-bank/zkrp
[47] easypki Library, https://github.com/google/easypki
[48] PKI implementation on a blockchain, https://giters.com/Antoineurban/SR2I206_PKI
[49] Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2018, May). Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 315-334). IEEE.
[50] zkrp Library, https://github.com/ing-bank/zkrp

한 정 수 (Jungsu Han)



2013 포항공과대학교, 컴퓨터공학과
2020 ~ 현재 포항공과대학교, 컴퓨터공학과 석사과정
<관심분야> 블록체인,머신러닝

김 정 헌 (Jungheon Kim)

2017 포항공과대학교, IT융합공학과
2020 ~ 현재 포항공과대학교, 컴퓨터공학과 석사과정

<관심분야> 블록체인,머신러닝

우 종 수 (Jongsoo Woo)

2020~ 현재 포항공대 정보통신대학원 연구교수
2018~ 현재 DGIST 이사장
2016~2019 포스코교육재단 이사장
2014~2016 산업과학기술연구원 원장
2011~2014 포스코 기술연구원 원장

<관심분야> 암호화폐, 블록체인

홍 원 기 (James Won-Ki Hong)

1995 ~ 현재 포항공과대학교, 컴퓨터공학과 교수
2007 ~ 2011 포항공과대학교, 정보통신대학원장
2007 ~ 2010 포항공과대학교, 정보통신연구소 연구소장
2008 ~ 2010 포항공과대학교, 컴퓨터공학과 주임교수
2008 ~ 2012 포항공과대학교 정보전자융합공학부장
2012 ~ 2014 KT 종합기술원 원장

<관심분야> 네트워크 트래픽 모니터링, 네트워크 및 시스템 관리, SDN/NFV, IoT, 무크기반 교육, 블록체인 및 암호화폐, Vmeeting 화상회의시스템