블록체인 기반 CBDC 아키텍처 및 트랜잭션 키 관리 시스템 설계

한정수, 김정헌, 허강욱*, 전윤서*, 우종수, 홍원기
포항공과대학교, *하나금융
{saw1515, kjheon1118, woojs, jwkhong}@postech.ac.kr
*{kwheo, yunsuh.chun}@hanafn.com

Design of Blockchain-based CBDC Architecture and Transaction Key Management System

Jungsu Han, Jeonheon Kim, *Kangwuk Heo, *Yunsuh Chun, †Jongsoo Woo, James Won-Ki Hong
Department of Computer Science and Engineering, POSTECH
* Hana Financial Group
†Graduate School of Information Technology, POSTECH

요 약

전자상거래와 전자결제 시스템의 등장으로 종이 화폐의 사용이 줄고 있다. 대부분의 종이 화폐가 사라지고 디지털 화폐가 주류가 될 것임은 충분히 예견할 수 있는 사실이다. 이러한 현상은 블록체인 기술 발전과 COVID-19 으로 인해 더욱 가속화 되었다. 중앙은행 디지털화폐(CBDC)가 최근 주목을 받기 시작한 것 역시 이와 같은 이유 때문이다. CBDC는 중앙은행이 발행하는 디지털 형태의 화폐이다. 현재 CBDC는 여러 국가에서 활발하게 연구되고 있으며 실제로 파일럿 테스트 중인 국가도 존재한다. 그러나 기존 CBDC 연구는 주로 필요성과 요구조건에 대한 내용들을 중심으로 진행되고 있으며 세부적인 기술 연구는 부족한 것이 현실이다. 본 논문에서는 CBDC를 구현하기 위한 아키텍처 설계와 필요한 구체적인 기술에 대한 제안을 담고 있다. 또한 기술적인 문제뿐만 아니라 CBDC가 실제 서비스단계에서 정상적으로 동작하기 위한 방안에 대해서도 다루고 있다.

Ⅰ. 서 론

블록체인의 기술 발전, 암호자산의 확산, 달러의 약세화 등을 배경으로 여러 국가에서 중앙은행 디지털화폐(Central Bank Digital Currency, CBDC)의 관심이 커지고 있다[1]. 국제결제은행 (Bank for International Settlements, BIS)는 CBDC를 중앙은행이 직접 책임지며 국가 회계 단위로 표시되는 디지털 결제수단으로 정의하였다[2]. 예를 들어 가치가 일정한 스테이블코인 (Stablecoin)[3]의 경우에는 중앙은행이 직접 발행하지 않기 때문에 CBDC가 될 수 없다. 또한 디지털 달러의 경우에는 한국 은행이 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 CBDC 이다.

현재 전 세계 중앙은행 중 80%가 CBDC 도입을 검토하고 있으며, 이들은 다음과 같은 6가지 이유로 CBDC에 관심을 갖고 있다. 첫째는 금융 포용력 때문이다. 현재 종이 화폐를 대신하여 신용카드, 페이앱 등 다양한 방법으로 결제가 이루어지고 있다. 이처럼 현금이 신뢰할 수 있는 결제 수단이긴 하지만, 현금은 점점 접근성과 유용성이 떨어지고 있다. 그렇기 때문에 여러 국가들에서 민간 결제수단을 대체할 수 있고 안정성이 보장된 결제 시스템을 CBDC를 통해 구축하고자 한다. 두번째는 복원력 때문이다. 결제 청산 시스템에서 셧다운이 일어났을 때 기존 시스템들은 단일 장애점 (Single Point of Failure) 문제를 겪고 있다. 블록체인을 기반으로 한 CBDC의 경우 분산시스템을 통해 이런 문제를 해결할 수 있는 기술력을 제공하므로 주목받고 있다. 세번째는 결제수단의 다양성 때문이다. 기존 민간 결제 플랫폼으로 인해 결제 시각 플랫폼에 맞는 QR 코드나 결제 방법을 사용해야 되는 불편함과 복잡성으로 인해 비용이 발생하게 된다. 하지만 특정 기업의 결제 방식으로 통일하기에는 독과점의 문제가 존재한다. 그렇기 때문에 중앙은행이 정하는 표준 시스템이 필요하며 CBDC가 이 문제에 대한 해결책으로 제시되고 있다. 네번째는 역외 거래 때문이다. 국가간의 송금이나 결제 시 복잡한 과정으로 인한 비효율성과 결제 외 비용이 발생하며, 이 과정이 불투명하게 진행된다는 문제가 존재한다. CBDC는 국가간의 표준 제정 및 시스템 호환성을 통해 이 문제를 해결하는 것이 가능하다. 다섯 번째는 추적 가능한 익명성 때문이다. 기존의 현금은 추적이 전혀 불가능 문제가 있어 범죄에 악용될 여지가 크다. 하지만 CBDC는 추적 가능한 익명성을 통해 프라이버시를 보장하면서 범죄 예방에 도움을 줄 수 있다. 마지막으로 재정 이전 때문이다. 예를 들어 COVID-19 상황 같이, 국가 재난 지원금을 금융 취약 계층도 받을 수 있는 시스템이 필요하며 DID (Decentralized Identity) 기반 신원 증명 서비스[4]와 연결되어 적절하고 안전하게 지급 될 수 있는 국가적 시스템이 필요하다. CBDC는 이런 형태의 재정 이전에서 효과적인 수단으로 주목받고 있다.

본 논문에서는 CBDC 구현을 위한 기술적 이슈에 대한 논의와 함께 시스템 아키텍처에 대한 제안을 다루고 있다. 중앙은행과 시중은행, 일반 고객의 계층적 구조에서 각 참여자의 역할과 요구조건에 대한 내용을 다루고 있으며 안전하고 신뢰할 수 있는 CBDC 유통과 거래 과정을 위한 기술적 요소들을 제시하고 있다.

Ⅱ. 관련 연구

1. Blockchain

블록체인 기반 CBDC의 개발을 위해서는 어떤 블록체인 플랫폼을 사용할 것인지를 결정하는 것이 중요한 이슈이다. 블록체인의 핵심 원장(core ledger)은 은행이나 고객 간의 거래 순서를 결정하며 거래 정보가 저장되어

야 하며 위변조가 불가능한 시스템이어야 한다. 또한 다수의 사용자들의 동시 거래를 지원하는 처리량과 짧은 지연 시간 내에 거래가 체결되도록 보장해야한다. 이를 위하여 [5]에서는 R3 Corda를, 그리고 [6]에서는 Hyperledger Fabric을 CBDC를 위한 블록체인 플랫폼으로 택하고 있지만, 이 플랫폼들은 역외 거래(cross border payment)를 구현하기에 적합하지 않다는 문제점이 있다. 이처럼 현재 CBDC 시스템을 위한 규격화된 블록체인 플랫폼이 제시되지 않은 상태이기 때문에 핵심 원장 개발 시 국가별로 상이한 플랫폼을 독자적으로 개발하거나, 기존 블록체인 플랫폼을 변형하여 개발 중인 경우가 대부분이다. 이 문제를 해결하기 위해 [7]은 역외 거래와 다른 블록체인 간의 연결을 지원하는 상호 운용성 프로토콜(interoperability protocol)의 중요성을 강조하고 있다. 본 논문에서는 블록체인 간 커뮤니케이션 기능을 가능하게 하는 인터체인 기반의 CBDC 시스템을 제안하고 있다.

2. Key Management

[8]은 블록체인을 통해 CBDC 트랜잭션이 이루어질 때 CBDC 실제 소유자의 개인키를 이용하여 트랜잭션에 서명하는 방법을 제안하고 있다. 개인키로 서명한 트랜잭션을 검증자(validator)가 공개키를 이용하여 검증하는 방식을 통해서 트랜잭션의 유효성을 검증하게 된다. 이때 만약 개인키가 외부로 노출될 경우 타인이 악의적인 목적을 가지고 임의로 유효한 서명을 생성하여 금전적인 피해를 줄 수가 있다. 그렇기 때문에 개인키를 안전하게 보관하고 관리하는 것이 CBDC 시스템을 구축할 때 중요한 요구사항 중 하나이다. 일반적으로 디지털 지갑이 개인키를 관리하게 되며 공개키 기반 구조(Public Key Infrastructure, PKI)[9]의 다양한 방법들이 제시되고 있다.

PKI 시스템의 보안 자체는 안전하지만 통신 중간 과정에서나 지갑 소프트웨어에서 공격 받아 개인키 유출이 될 가능성은 항상 존재한다. 그렇기 때문에 트랜잭션에 서명 시 다수의 관리자의 동의가 있어야만 서명이 가능한 방식들이 오랜 기간 연구되어왔다. 대표적인 예시가 다중 서명(multi signature)[10]과 다자간 연산(Multi Party Computation, MPC)[11] 방식이 존재한다. 다중 서명 방식의 경우 트랜잭션을 위한 복수의 키를 생성하여 키를 가진 자들이 동시에 서명해야만 트랜잭션의 서명이 유효한 방식을 말한다. 이와 달리 다자간 연산 방식의 경우 하나의 키를 생성하기 위해 서로 신뢰하지 않는 다수가 각자의 입력 값을 공유하지 않고, 암호화된 입력 값을 통해 서명 키를 생성하는 방식을 말한다. 본 논문에서는 CBDC 네트워크의 참여자들이 다자간 연산 방식을 통해 트랜잭션 서명을 생성하는 키 관리 시스템을 제안한다.

Ⅲ. 아키텍처 설계 및 구현

1. Entity

CBDC 시스템 참여자(entity)는 크게 중앙은행, 시중은행, 일반 고객 세가지로 나뉘게 된다. 그림 1 은 CBDC의 상위설계 구조를 보여주고 있다. 중앙은행은 기본적으로 CBDC 발행 및 배정 권한을 갖고 있으며 CBDC 원장(ledger)의 관리와 책임을 갖게 된다. 시중은행은 CBDC의 원활한 유통을 담당하며 일반 고객들의 CBDC 관리를 담당하게 된다. 일반 고객의 경우에는 CBDC 실사용 계층으로 KYC(Know-Your-Customer)[12] 유저와 non-KYC 유저로 나뉠 수 있다. KYC란 은행에서 고객의 신원을 확인하는 것을 말하며 은행 계좌를 통해 CBDC 거래를 하기 위해 KYC 과정이 필수적이다. 이에 반해 현재 사용되는 종이 화폐와 같이 오프라인 CBDC 거래에서는 사용자의 신원을 확인할 수 없기 때문에 KYC 과정없이 CBDC 거래를 하게 된다.

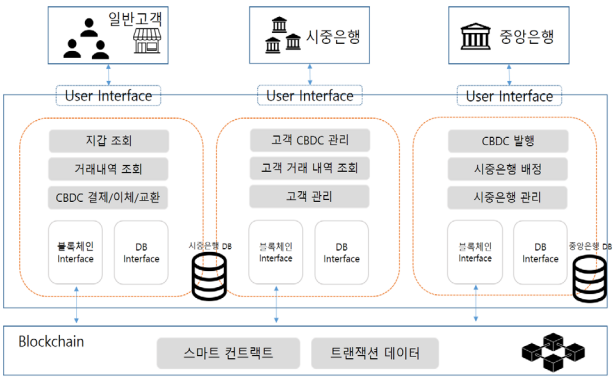

그림 1. CBDC High-level System Design

2. Blockchain

모든 CBDC 트랜잭션 기록은 블록체인 상에 저장된다. 블록체인에 요청을 보내면 이전 트랜잭션 기록을 간단하게 조회할 수 있다. 그렇지만 모든 단순 거래 조회나 검색과 같이 블록체인에 기록할 필요가 없는 CBDC 트랜잭션을 위해 블록체인에 수 많은 RPC (Remote Procedure Call) 요청을 보내는 것은 블록체인 노드의 병목현상으로 인해 지연이 발생시키고, 이는 CBDC 사용자의 불편함으로 이어질 가능성이 높다. 그렇기 때문에 새로운 블록체인에 트랜잭션이 기록되어야 하는 작업과 그렇지 않은 작업으로 나누어 노드의 부하를 최소화 시켜야 CBDC 사용성이 높아진다. 이는 블록체인의 트랜잭션 처리 속도와는 별개로 수 백, 수 천 만명의 CBDC 사용자의 요청에 대해 CBDC 블록체인 노드의 처리량이 감당할 수 있는지에 대한 것이다. 데이터 접근성과 관리의 용이성 측면에서 CBDC 블록체인과 실시간으로 동기화되는 별도의 데이터베이스를 생성하는 것이 가능하다. 즉, 사용자의 CBDC 트랜잭션 요청에 대해 은행 서버의 데이터베이스에서 응답할 정보가 존재할 경우에는 즉각적으로 전달하고, 만약 데이터가 부재한다면 블록체인에 스마트 컨트랙트를 호출하여 사용자에게 전달할 데이터를 받아오는 구조를 제안한다. 자세한 진행 과정은 그림 2 와 같으며 다음과 같은 과정으로 진행된다.

1. 사용자가 CBDC 이체, 교환, 결제, 조회 등의 트랜잭션을 발생시킨다.
2. 시중은행(server)은 사용자의 신원 인증을 요청한다.
3. 사용자는 자신의 신원 인증 정보를 담은 내용을 전달하고 은행은 이를 확인한다.
4.
   a. 시중은행 데이터베이스에 트랜잭션을 처리할 데이터가 존재하는 지 확인하고, 존재할 경우 다음 단계로 넘어간다. 만약 데이터가 없을 경우에는 4-b 와 같이 동작한다.
   b. 블록체인 상의 데이터를 호출하거나 트랜잭션을 발생시키기 위해 스마트 컨트랙트를 호출한다. 블록체인에서는 트랜잭션에 이상이 없는 지를 확인하고, 없다면 블록에 트랜잭션 정보를 기록한다. 시중은행 데이터베이스는 블록체인의 정보

를 실시간으로 동기화하여 동일한 데이터 요청이 있을 경우를 대비한다.

5. 트랜잭션 요청의 결과가 전달된다.
6. 사용자에게 트랜잭션 결과가 보여지게 된다.

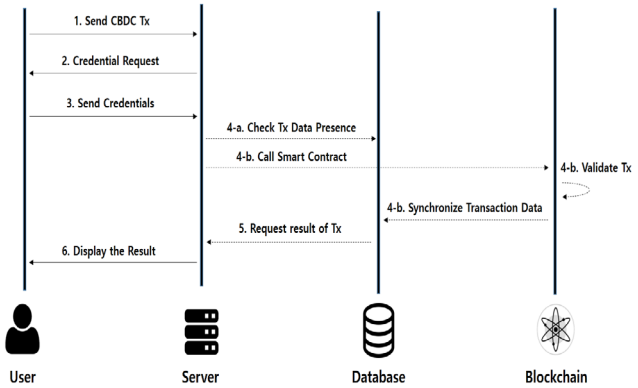

그림 2. CBDC Transaction Workflow

시중은행의 데이터베이스는 트랜잭션의 이상 유무를 확인하지 않으며 블록체인에 저장된 데이터와 동기화되어 응답 지연시간을 줄이기 위한 미들웨어 역할만을 하게 된다. 이를 통해 은행마다 자신들에게 특화된 데이터베이스 스키마를 설계하여 관리가 용이하며, 비교적 데이터 호출 시간이 긴 블록체인 RPC 요청을 최소화 하여 데이터 접근성을 높일 수 있다. 이는 현존하는 블록체인 플랫폼들의 낮은 트랜잭션 처리량(TPS)를 극복하기 위한 방법이다. 하지만 데이터베이스는 블록체인 원장에 비해 쉽게 위변조 될 가능성이 있고, 동기화를 위한 비용이 추가적으로 발생하기 때문에 이 방법은 근본적인 해결책이 아니다.

본 논문에서는 인터체인 기반의 블록체인을 CBDC에 가장 적합한 플랫폼으로 제안한다. 그 이유는 인터체인은 일종의 사이드체인(sidechain) 역할을 할 수 있기 때문에 앞서 말한 트랜잭션 처리량을 노드의 수평적 확장(horizontal scaling)을 통해 향상시키는 것이 가능하기 때문이다. 비트코인과 이더리움과 같이 단일 원장을 갖는 블록체인들과 달리 인터체인은 블록 데이터를 분산하여 저장할 수 있다. 이를 통해 메인체인이 모든 데이터를 저장하며 점점 무거워져 TPS가 낮아지고 트랜잭션 수수료가 증가하는 것을 방지하는 것이 가능하다. 또한 인터체인 기반의 블록체인은 현존하는 타 블록체인 플랫폼에 비해 역외 거래 및 은행 간 송금에 특화되어 있다는 장점이 있다. 기존 블록체인 프로토콜들은 신뢰할 수 있는 제 3 자 없이 상호 정보를 교환할 능력이 없는 폐쇄적인 구조를 띄고 있다. 즉, 비트코인이 이더리움과 거래 내역을 공유할 수 있는 해결책이 부재한다는 뜻이다. [1]은 이런 문제로 인해 국가별로 상이한 CBDC 블록체인 프로토콜로 인해 추후 국가 간의 역외 거래에 큰 장애물이 될 가능성이 높을 것이라는 지적을 하였다. 그렇기 때문에 [13, 14, 15]와 같이 블록체인 간의 통신을 가능하게 하는 인터블록체인을 CBDC 블록체인 플랫폼으로 선정될 가능성이 높다고 예상된다.

[13]과 같이 인터체인은 여러 개의 독립적인 병렬 블록체인인 존(zone)과 각 존을 연결하는 허브(hub)로 구성하는 것이 가능하다. 각 존은 국가, 정책, 사용 목적 등 다양한 특징에 특화된 형태로 독립적인 블록체인 네트워크를 형성하는 것이 가능하다. 허브는 각 존들 간의 트랜잭션이 가능하게 하여 상호 연계되어 동작하도록 한다. 이를 CBDC에 적용시킬 경우 은행 별 상황에 맞는 최적의 블록체인 플랫폼으로 개별 존으로 구현하고 이를 IBC (Inter-Blockchain Communication) 프로토콜을 이용하여 허브로 거래 정보를 전달하여 다른 존의 블록체인과 토큰을 교환하는 것이 가능하게 된다.

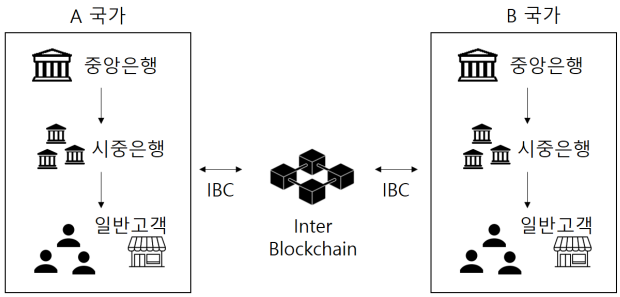

그림 3. 인터체인을 이용한 은행간 거래 시나리오

그림 3 에 볼 수 있듯이 이를 통해 은행 별 CBDC 블록체인 네트워크는 각각 하나의 존을 형성하게 되고 이는 허브를 통해 거래나 토큰 정보를 공유하는 것이 가능하다. 즉, A 국가에서 발행한 CBDC 화폐를 B 국가의 CBDC 화폐로 전환하는 것이 가능하다. 이를 통해 은행이나 환전소에 지불해야할 수수료를 줄이는 것이 가능하며 이중 환전과 같은 불필요한 과정이 사라질 것으로 예상된다.

3. Key management

본 논문에서는 CBDC 트랜잭션 생성 시 다자간 연산(MPC) 방식을 통한 서명 방식을 제안한다. MPC 는 서명 참여자의 민감 정보를 공유하지 않는 암호 기술로 별도의 키 관리 방법을 제시하지는 않는다. 그렇기 때문에 트랜잭션의 민감 정보 보호와 효율적인 키 관리를 위해서 본 논문은 MPC 와 함께 [16]에서 제시한 그룹 키 관리 시스템(Group Key Management, GKM) 을 사용하였다. GKM 은 계층적 구조를 갖고 있는 다수 노드들 간의 효율적인 키 관리에 적합한 방법이다. CBDC 블록체인 네트워크에 참여하는 사용자들은 트랜잭션을 생성할 권한 수준에 차등이 필요하다. 예를 들어, CBDC 를 발행하는 권한은 중앙은행에서만 가져야하며, CBDC 의 원활한 유통과 고객 관리를 위해서 시중은행은 일반고객보다는 더 많은 권한을 가져야 한다. 또한 무분별한 키 생성이 가능할 경우 KYC 과정이 어려워져 범죄에 사용될 가능성이 있다. 그렇기 때문에 CBDC 트랜잭션에 사용될 키 관리를 위한 계층적인 시스템이 필요하다. 그림 4 에서 볼 수 있듯이 CBDC 아키텍처에서 GKM 시스템은 각각 중앙은행, 시중은행, 일반 고객으로 구성되는 것이 가능하다.

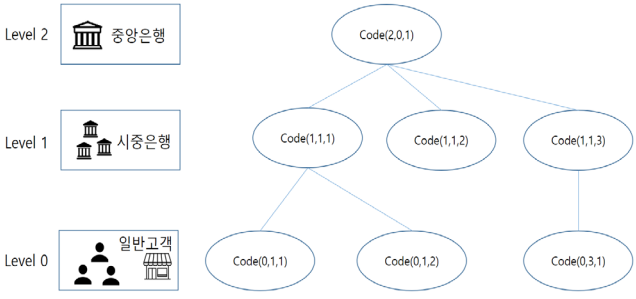

그림 4. Group Key Management in CBDC

각 레벨의 노드는 여러 개의 노드로 구성될 수 있으며, 상위 계층의 노드가 하위 계층의 노드 보다 더 많은 권한을 보유하고 있고 동일 계층에서 노드 간의 권한은 동일한 것으로 가정한다. 각 그룹에 적힌 숫자는 그룹을 식별하기 위한 코드로 Code (i, j, k)로 표기된다. 이 때 i는 자신의 그룹 레벨을 의미하며, j는 상위 그룹에서 부모 그룹의 위치를 의미하고, k는 현재 레벨에서의 자신의 그룹 위치를 의미한다. 예를 들어 (1, 1, 2)의 경우 레벨 1 에 상위 레벨의 첫 부모 그룹의 자식이며 현재 레이어에서 2 번째 위치에 해당하는 것을 의미한다. 부모 그룹이 없을 경우에는 (2, 0, 1)와 같이 j 값은 0 으로 표기한다. $GK_{i,j,k}$ 를Code (i, j, k)를 가진 그룹 키라고 할 때 $c_1, c_2, c_3 \ldots$ 자식 그룹에 대해 그룹 키는 다음과 같이 계산이 된다.

$$GK_{i,j,k} = f\left(GK_{i-1,k,c_1}, GK_{i-1,k,c_2}, \ldots\ldots GK_{i-1,k,c_l}\right)$$

이 때 f는 단방향 함수로 입력 값과 출력 값의 길이는 동일하다. 이를 통해 상위 계층의 그룹 키가 하위 계층의 그룹 키 값에 따라 갱신되게 된다. 그렇기 때문에 하위 계층의 경우 부모 그룹 내 노드 간의 합의를 통해 자식 그룹에 포함될 지 여부가 결정된다면 그룹 키가 배정되고, 이후 부모 그룹 키는 갱신된다. 또한 자식 그룹들의 그룹 키를 계산하는 f에서 MPC 방식을 이용하면 동일 그룹 내에서 그룹 키의 정보를 공유하지 않으며 $GK_{i,j,k}$ 를 만드는 것이 가능하다. 이를 통해 키 관리 시스템을 계층적으로 구현함으로써 트랜잭션 생성 시 계층 수준에 따라 권한을 차등하여 부여하는 것이 가능하게 된다.

Ⅳ. 결론 및 향후 연구

본 논문에서는 인터체인을 이용한 CBDC 아키텍처와 다자간 연산 방식을 활용한 그룹 키 관리 시스템을 제안하였다. 기존에 존재하는 대부분의 CBDC 관련 연구들은 시스템 요구사항이나 범용적인 아키텍처를 제안하는 것에 그치고 있다. 이와 달리, 본 논문은 구체적인 CBDC 시스템 개발을 위한 기술적 방법을 제안하였다. 인터체인이 CBDC에서 갖는 이점에 대하여 설명하였으며, MPC 기반의 그룹 키 시스템을 이용한 안전하고 효율적인 키 관리 방법을 제시하였다.

향후 연구에서는 실제 블록체인을 이용한 인터체인 기반의 CBDC 파일럿 프로젝트 진행할 예정이다. 특히 인터체인의 경우 수평적 확장이 가능한 장점이 있어 실제 CBDC가 상용화 되기 위한 트랜잭션 처리량를 달성하기에 적합하다는 평가를 받고 있다. 중앙은행 및 시중은행 간 거래 시나리오를 가정하여 블록체인 간의 커뮤니케이션의 정량적 성능 평가와 기존 시스템과의 차별점에 대해 연구할 계획이다.

ACKNOWLEDGMENT

본 연구는 2021 년도 하나금융그룹의 지원과 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터 육성지원사업의 연구결과로 수행되었음 (IITP-2021-2017-0-01633*).

참 고 문 헌

[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), July 2019.

[4] Luecking, M., Fries, C., Lamberti, R., & Stork, W., “Decentralized identity and trust management framework for Internet of Things.” 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020), pp. 1-9, Toronto, Canada, May 2020.

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

[6] 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.

[7] Qasse, I. A., Abu Talib, M., & Nasir, Q. “Inter blockchain communication: A survey,” ArabWIC 6th Annual International Conference Research Track, pp. 1-6, 2019.

[8] Han, X., Yuan, Y., & Wang, F. Y., “A blockchain-based framework for central bank digital currency,” IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 263-268, 2019.

[9] Pal, O., Alam, B., Thakur, V., & Singh, S., “Key management for blockchain technology,” ICT Express, 2019.

[10] Ohta, K., & Okamoto, T., “Multi-signature schemes secure against active insider attacks,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 82, no. 1, pp. 21-31, 1999

[11] Yao, A. C., “Protocols for secure computations,” In 23rd Annual Symposium on Foundations of Computer Science, pp. 160-164. 1982.

[12] Kapsoulis, N., et al., “Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture,” Future Internet, 12(2), 41, 2020.

[13] “Cosmos” [Online]. Available at https://cosmos.network/docs/resources/whitepaper.html

[14] “ICON” [Online]. Available at https://docs.icon.foundation/ICON-Whitepaper-EN-Draft.pdf

[15] “Aion” [Online]. Available at https://whitepaper.io/document/31/aion-whitepaper

[16] Pal, O., Alam, B., Thakur, V., & Singh, S., “Key management for blockchain technology,” ICT Express, 2019.