계층2 블록체인 기반 중앙은행 디지털 화폐 시스템 설계 및 구현

황 재 승♦, 김 영 한°

A Design and Development of Layer 2 blockchain-based Central Bank Digital Currency System

Jae-seung Hwang♦, Young-han Kim°

요 약

CBDC(Central Bank Digital Currency)는 중앙은행이 발행하는 디지털 형태의 법정화폐로, 최근 많은 국가에서 관심을 갖고 기술적 완성도를 높이기 위한 실험을 진행하고 있다. CBDC 시스템 구현을 위해 블록체인 기술이 고려되고 있으나, 단순히 기존 블록체인 기술의 적용만으로는 CBDC에서 요구되는 높은 처리량을 감당하기 어렵다. 이를 해결하기 위해 하이퍼렛저 패브릭과 같은 프라이빗 체인을 활용하는 방식이 제안되었으나, 노드 수 증가에 따른 성능 저하와 합의 과정에서의 중앙집중화 경향이 문제점으로 지적되었다.

본 연구에서는 이러한 문제를 해결하기 위해 다양한 레이어 2 기술 중 롤업(Rollup)을 활용한 CBDC 시스템을 설계하였다. 롤업은 트랜잭션을 오프체인에서 처리하고 그 결과를 주기적으로 메인체인에 커밋하는 방식으로, 높은 처리량과 확장성을 제공할 수 있다. 제안된 시스템은 다수의 롤업을 병렬로 운영하여 CBDC의 요구사항을 충족시킬 수 있도록 설계되었다. 실험을 통해 제안 시스템이 단일 블록체인 대비 대폭 향상된 확장성을 달성함을 검증하였다.

Key Words : Blockchain, CBDC, Rollup

ABSTRACT

Central Bank Digital Currency (CBDC) is a digital form of fiat currency issued by the central bank, and is currently conducting experiments to increase technical completeness with interest in many countries. Blockchain technology is being considered to implement the CBDC system, but it is difficult to handle the high throughput required by CBDC simply by applying the existing blockchain technology. To solve this problem, a method of using a private chain such as hyperletzer fabric has been proposed, but the deterioration of performance due to the increase in the number of nodes and the tendency to centralize in the process of agreement have been pointed out as problems.

In this study, to solve this problem, a CBDC system using Rollup among various layer 2 technologies was designed. Rollup can provide high throughput and scalability by processing transactions off-chain and periodically committing the results to the main chain. The proposed system is designed to meet the requirements of CBDC by operating multiple rollups in parallel. Through experiments, it was verified that the proposed system achieves significantly improved scalability compared to a single blockchain.

[글살자(여백:위만2.3mmm, 기준위치:쪽, 틀배치:본문과의 배치, 위치:가로-0,세로-0, 서체:본문과 동일 크기:7.5pts)를 만들어 소속기관, e-mail 주소, 직위, 논문번호, 접수일자 및 본인 저한연째의 이름 등을 아래의 형식으로 넣는다. 삼호 후 삭제]

※본 연구는 한국연구재단 논문연구과제(95-0100-23-04-3) 지원 및 한국대학교 논문연구소 관리로 수행되었습니다.(스타일 숨송기관)

♦ First Author : Hankook University Department of Information Security(소속 영문표기), hong@paper.korean.ac.kr, 학생(석사), 정회원

° Corresponding Author : Hankook University Department of Information Security(소속 영문표기), lee@paper.korean.ac.kr, 정교수, 정회원

* 소속, 이메일, 정교수, 정회원

논문번호 : KICSXXXX-XX-XXX, Received December 22, 2014; Revised December 22, 2014; Accepted December 22, 2014

Ⅰ. 서 론

인터넷을 기반으로 하는 모든 거래는 그 거래 장부의 데이터 무결성을 지키기 위해 신뢰할 수 있는 제3자인 외부 금융기관에 의존하고 있다. 이 때문에 신뢰할 수 있는 제3자에게 많은 비용을 지불하고 있는 상황이다. 비트코인은 신뢰 대신 암호학적 증명(Cryptographic proof)에 기반한 전자화폐 시스템을 제안하며 이러한 문제점을 해결했다[1].

비트코인에 이어 다양한 블록체인 프로젝트들이 등장하게 됐는데, 이중 이더리움은 튜링 완전한 프로그래밍 언어가 심어진 블록체인을 위해 제안되었다[2]. 하지만 비트코인과 이더리움은 블록체인 트릴레마(Trilema)[3]로 인해 확장성(Scailability)이 부족했고 이를 해결하기 위한 움직임들이 생기기 시작했다. 최근 소개된 솔라나[4]와 아발란체[5]와 같은 블록체인 시스템은 단일 블록체인 상에서 더 높은 트랜잭션 처리량을 보여주고 있고, 그 외에도 여러 블록체인을 이용해 확장성 문제를 해결하려는 움직임이 있다[6].

앞에서 언급한 것처럼 확장성 솔루션은 두 가지로 분류할 수 있다. 첫 번째는 단일 블록체인을 활용한 트랜잭션 처리량 개선이다. 단일 블록체인을 이용한 확장성 개선은 블록 크기나 블록 생성시간과 같은 블록체인 시스템의 파라미터 변경을 하거나[7], 합의 알고리즘을 변경하거나, 네트워크를 작은 네트워크 단위로 샤딩(Sharding)하는 방법 등이 있다[8]. 이처럼 자체 합의 알고리즘을 기반으로 독자적으로 운영되는 네트워크를 레이어 1(Layer1, L1)이라고 부르기도 한다.

두 번째 방법은 다수의 블록체인을 활용하는 방법이다. 이 방법은 하나의 메인 블록체인을 두고 트랜잭션을 메인 블록체인 외부의 블록체인에서 처리하는 방식이다. 이때 외부의 블록체인은 보안성 등을 보장받기 위해 메인 블록체인과 지속적으로 상호작용을 해야 한다. 이러한 방식을 레이어 2(Layer2, L2) 라고 하며 스테이트 채널(State channels)[9], 사이드 체인(Side chains)[10], 플라즈마(Plasma)[11], 밸리디움 (Validiums)[12] 그리고 롤업(Rollups)[13] 등이 있다.

CBDC는 중앙은행에서 발행하는 전자적 형태의 법정화폐로서 기존 법정화폐와 동일한 화폐단위를 갖고 현금과 1:1로 교환되는 중앙은행의 직접 채무이다. 즉, CBDC는 중앙은행이 직접 발행 하는 전자적 형태의 현금이며, 예금이나 신용카드와 같은 지급 결제 수단 또는 소액 간편 결제 시스템이 아니라 기존 지폐나 주화 같은 실물 화폐가 디지털화 되었다는 의미이다[14].

블록체인의 등장으로 인해 세계 각국의 중앙은행에서 CBDC에 관한 연구를 촉진하는 계기가 됐다[15]. 이에 따라 CBDC에 관한 다양한 연구가 진행되고 있다. 특히 유럽과 영국에서 CBDC에 관한 연구가 활발하게 진행되고 있다. EU는 2022년 9월 디지털 유로의 자문보고서를 발간하였으며, 2021년 10월에 시작한 디지털 유로 프로젝트의 첫 단계인 조사단계를 2023년 가을에 마무리하고 실현단계를 진행할 예정이다[16]. 특히 달러 이후의 기축 통화로 자국 화폐를 사용하고자 하는 국가나 개발도상국이나 신흥국 등, 기존 금융시스템이 해결하지 못하고 있는 문제들을 개선이 필요한 국가들에서 많이 연구되고 있다.

하지만 CBDC에 관한 연구는 필요성과 요구조건에 관한 내용을 중심으로 진행되고 있으며, 위에서 언급한 확장성과 같은 세부적인 기술에 관한 연구는 부족한 실정이다.

결제 수단 및 디지털 법정화폐로서 CBDC는 결제 다양성을 증가하여야 하며, 현재의 법정화폐(현금)와 같이 CBDC는 국내 및 국경을 넘는 시나리오 등에 대비해 저렴한 비용으로 빠르고 안전한 결제를 제공할 수 있어야 한다. 통화 기능에 있어서 CBDC는 오프라인 및 즉석 결제, 익명성 및 프라이버시[17], 보안, 탄력성, 제어 가능한 규제, 가용성, 확장성, 편리성 및 사용자 친화성과 같은 기능을 제공해야 한다[18, 19]. CBDC 시스템은 범국가적인 시스템이기 때문에 다른 시스템에 비해 거래량이 기본적으로 많을 것이며, 거래량이 급증하는 상황에서도 안정적으로 운영될 수 있어야 한다.

그러나 이러한 시스템을 단일 블록체인으로 구성한다면, 성능의 한계에 도달했을 때 유연하게 대처하기가 어려울 것이다. 블록체인에서 발생하는 요청들을 처리하지 못하여 거래가 지연되거나 최악의 경우 거래 취소 및 오류가 생길 수도 있고, 이로 인해 블록체인 시스템 자체에 장애가 생길 수도 있다. 이에 본 논문에서는 CBDC의 확장성 개선을 위한 구조를 설계하였고 구현을 통해 검증하였다. 제안된 구조는 다수의 블록체인을 이용한 방법으로써 다양한 레이어 2 기술 중 롤업을 활용한 방식으로서 다수의 롤업을 병렬로 운영하여 CBDC의 요구사항을 충족시킬 수 있도록 설계되었다.

서론에 이어 제2장에서는 관련 기술을 고찰하고 3장에서는 확장성 기술을 적용한 CBDC 구조를 제시한다. 이어서 4장에서 구현된 시스템의 실험 결과를 제시하고 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

블록체인의 확장성을 높이는 방법으로는 Scale-up과 Scale-out 방식으로 분류된다. Scale-up은 한 블록에 많은 트랜잭션을 담을 수 있도록 블록의 크기를 키우는 방식이며 Scale-out 방식은 트랜잭션을 On-chain에서 처리하는 것이 아니라 기존 블록체인에 보안성(Security)을 의존하는 Off-chain에서 처리하는 것이다.
이 Off-chain은 최소 하나에서 여러 개가 될 수 있으며, Off-chain의 개수와 트랜잭션 처리량은 정비례한다. Scale-up은 한 번 정한 스펙을 변경하기 어려우므로 사용자가 증가했을 때 성능 문제가 발생할 확률이 높지만 Scale-out 방식은 시스템 사용량에 맞게 Off-chain의 숫자를 늘리거나 줄일 수 있어 Scale-up과 비교하면 훨씬 유연하며[20] 다음과 같은 대표적인 방법들이 제시되고 있다.

1. 플라즈마(Plasma)

플라즈마는 이더리움을 부모 체인으로 두고 별도의 자식 체인을 활용하여 트랜잭션을 처리하는 확장성 솔루션이다[11]. 각각의 자식 체인들은 서로 독립적으로 동작하기 때문에 각각의 필요에 따라 다양한 방법으로 구현될 수 있으며, 이에 따라 다양한 구현체들이 제시됐다[11][21][22]. 각각의 플라즈마 체인은 블록 헤더의 해시값을 주기적으로 부모 체인에 커밋(Commit) 한다. 플라즈마 체인의 블록 해시값만 부모 체인에 저장되기 때문에 부모 체인의 부담이 감소하기 때문에 확장성 문제를 개선할 수 있을 것으로 기대됐다.
플라즈마 체인에서 발생하는 트랜잭션은 이의 제기 기간을 갖게 되는데, 다음과 같은 5가지 단계를 거쳐 확정된다.

(1) 트랜잭션 생성
(2) 블록 생성: 플라즈마 체인의 운영자에 의해 플라즈마 체인의 블록이 생성된다.
(3) 트랜잭션 확인: 플라즈마 체인의 트랜잭션이 부모 체인에 커밋되는 것을 확인
(4) 챌린지(Challenge) 기간: 해당 트랜잭션에 대해 문제가 생겼을 경우 이에 대한 이의 제기를 하는 기간을 의미
(5) 트랜잭션 확정 또는 롤백

검증한 트랜잭션이 비정상적인 트랜잭션이라고 판명될 경우 해당 트랜잭션의 동작을 취소하는 롤백이 발생하고, 트랜잭션을 생성한 오퍼레이터에게 페널티를 부여하는 방식으로 플라즈마는 운영된다.

이 방식에서 플라즈마 체인의 운영자가 전적으로 체인에 대한 운영의 전권을 갖고 있다. 이럴 때 운영자가 블록 제출을 하지 않는다면, 악의적인 행위가 발생하더라도 이를 검증하기가 불가능하다는 문제가 있다. 이를 데이터 가용성 문제라고 하며, 플라즈마는 이 데이터 가용성 문제를 해결하지 못했기 때문에 상용화까지 이어지지 못했다.

2. Zk 롤업

Zk 롤업은 영 지식 증명(Zero knowledge proof) 프로토콜인 Zk-Snark를 활용한 확장성 솔루션이다. Zk-Snark의 특징 중 하나인 증명 과정에서 참여자들 간의 상호작용 없이 단방향의 데이터 제공을 통해 데이터 유효성 검증 과정에서 사용자들에게 전체 데이터를 공개하지 않아도 되며, 사용자는 데이터를 확인하지 않고 해당 데이터의 유효성을 인정할 수 있다[23].
Zk 롤업에는 두 종류의 역할 군이 있다. 첫 번째는 Transactor라 불리는데, 트랜잭션을 만들고 이를 네트워크에 전파하는 역할을 담당한다. 두 번째는 Relayers 라 하며 Transactor가 전파한 대량의 트랜잭션을 수집하여 하나의 트랜잭션으로 묶는다. 이 과정에서 Relayer는 영 지식 증명을 통해 해당 데이터가 유효하다는 증거를 생성해야 하며, 이 증거는 레이어 1에 배포되어 있는 스마트 컨트랙트에 의해 검증된다. 즉 Zk 롤업의 Relayer는 증명자[23], 레이어 1의 스마트 컨트랙트는 검증자[24] 역할을 수행한다.
Zk 롤업은 영 지식 증명을 통해 블록 유효성 검증을 위한 데이터의 양을 줄일 수 있다. 또한, 레이어 1의 스마트 컨트랙트에서 Relayer에 의해 묶인 트랜잭션을 다시 해체하여 이에 대한 유효성 검증을

진행하고 모든 데이터는 트랜잭션에서 함수 호출 시 파라미터로 포함된 데이터들이 위치하는 Calldata로 네트워크에 공개적으로 게시된다. Calldata는 수정을 할 수 없기에 한 번 공개된 데이터는 변경될 수 없다. 이 과정을 통해 앞에서 언급된 데이터 가용성을 해결할 수가 있다.

3. 옵티미스틱 롤업

옵티미스틱 롤업은 Zk 롤업과 검증 방법에서 큰 차이를 보인다. Zk 롤업은 레이어 1으로 제출되는 모든 트랜잭션을 검증하는 반면에 옵티미스틱 롤업은 문제가 제기된 트랜잭션에 한해서만 검증이 이루어진다.

세부 단계는 구체적인 구현에 따라 다르지만, 옵티미스틱 롤업 시스템은 일반적으로 동일한 상위 구조를 따른다. 옵티미스틱 롤업에는 시퀀서(Sequencer)라 불리는 운영자와 검증자라 불리는 레이어 2의 행위자가 참여한다. 먼저 트랜잭션은 레이어 2 네트워크에서 시퀀서 또는 스마트 컨트랙트에 의해 전파된다.해당 스마트 컨트랙트는 레이어 1과 레이어 2 체인 간의 상호작용을 수행하는 컨트랙트이다.

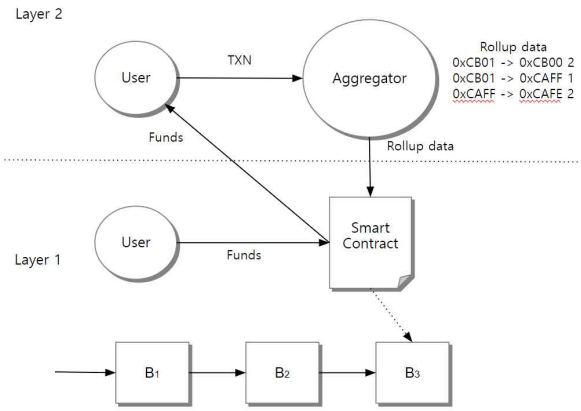

그림 1 롤업에서 스마트 컨트랙트 간 상호작용[26].
Fig. 1. Smart contract interactions in rollups

시퀀서는 임의의 트랜잭션을 처리한 후 압축된 트랜잭션 데이터와 레이어 1 체인에 스테이트 루트를 게시한다. 검증자는 시퀀서가 게시한 데이터를 지속적으로 모니터링 한다. 만약 검증자가 시퀀서가 제출한 데이터에 동의하지 않으면 분쟁을 해결하기 위한 절차가 시작된다. 분쟁 절차를 통해 시퀀서의 악의적인 행위가 발견될 경우 시퀀서가 미리 예치

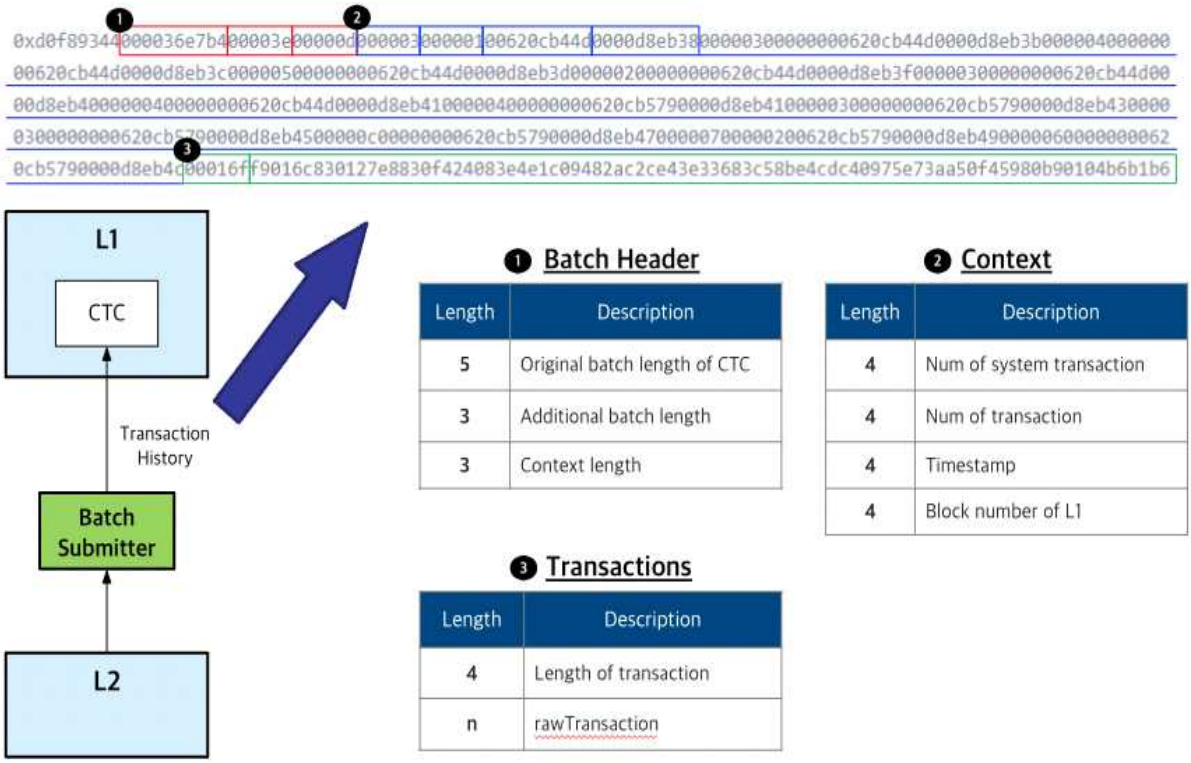

그림 2. Transaction data from L2
Fig 2. Transaction data from L2

한 금액은 삭감된다. 이때 시퀀서의 악의적인 행위를 발견하여 분쟁을 신청한 검증자는 보상을 받게 되는 방식으로 데이터 가용성을 보장할 수 있다.
즉, 옵티미스틱 롤업은 트랜잭션을 레이어 1 밖에서 처리해서 트랜잭션 처리 속도를 올리고 처리한 요약본을 레이어 1에 제출함으로써 레이어 1으로부터 보안성을 보장받는 방식을 택하고 있다.

표. 1 레이어 2 솔루션 간 비교
Table 1. Layer2 solution comparison

L2 Solution	TPS	Smart contracts enable
Plasma	up to 5000	no
Zk-Rollups	up to 2000	yes
Optimistic Rollups	Conditionally 2000	no

또한, 옵티미스틱 롤업은 레이어 1과 호환되는 스펙을 유지할 수 있는 특징이 있다. 앞서 소개한 플라즈마와 Zk 롤업은 레이어 1과 호환성이 떨어진다. 즉, 레이어 1에 배포된 스마트 컨트랙트를 그대로 레이어 2에 배포할 수가 없다. 하지만 옵티미스틱 롤업은 레이어 1에 배포된 컨트랙트를 그대로 레이어 2에 배포할 수 있기에 다양한 시스템을 구축할 수 있어서 본 논문에서 활용하는 기법으로 채택하였다. 표 1에 이러한 레이어 2 솔루션들을 비교하였다.

4. 브리지(Bridge)

블록체인은 기본적으로 고립된 환경에서 개발되며 서로 다른 규칙과 합의 메커니즘을 갖고 있다. 이는 기본적으로 블록체인 간 통신이 불가능하고, 자산의 이동이 자유롭지 않음을 의미한다. 블록체인 브리지는 두 블록체인 생태계를 이어주는 역할을 하며, 브리지를 통해 블록체인 간에 정보와 자산의 이동이 발생한다[27].
브리지는 여러 가지 방법으로 분류 할 수 있는데, 가장 많이 사용하는 방법은 신뢰(Trust)를 기반으로 한 분류다. 첫 번째는 신뢰할 수 있는 주체가 운영하는 브리지이다. 이는 중앙 기관이나 시스템에 의존하는 방법이며, 운영하는 주체의 평판에 의존하고, 해당 브리지의 사용자는 본인의 자산에 대한 제어 권한을 포기해야 한다. 두 번째 방식은 신뢰가 불필요(Trustless)한 경우이다. 신뢰가 불필요한 브리지는 스마트 컨트랙트를 활용하며, 특정 주체에 대한 신뢰가 필요하지 않다. 또한 스마트 컨트랙트를 통해 사용자가 자신의 자산에 대한 제어 권한을 그대로 갖고 있다.
아직 최적화된 브리지에 대한 설계는 발견되지 않았다. 두 종류 모두 리스크를 갖고 있으며, 스마트 컨트랙트 상에 버그가 존재하거나, 브리지가 연결되어 있는 블록체인이 해킹당하거나 할 경우 사용자가 갖고 있는 자산이 해커에 의해 탈취 당할 수 있기 때문에 보안이 중요하게 된다[28].

표 2 Smart contract configuration
Table 2. Smart contract configuration

Category	Contract name	Description
Smart contract in L1	CTC	Canonical transaction chain. Store transaction history of L2
	SCC	State commitment chain. Store state value changed
	L1 Bridge	Bridge contract which is deployed in L1. Store asset that are move to L2
Service contract for L2	Batch submitter	Submit transaction history and state root to L1
	DTL	Data transfer layer. Move asset from L1 to L2
	Relayer	Move asset from L2 to L1
L2 Smart contract	L1 bridge	Bridge which is exist in L2, using when asset is moved to L2 or returned to L1

Ⅲ. 제안구조

본 논문에서는 확장성 강화를 위해 옵티미스틱 롤업 방식을 이용하였다. 옵티미스틱 롤업의 구조를 간단하게 표현하면 그림 3과 같다. 그림에서 L2 chain과 L1 contracts는 각각 레이어 2와 레이어 1에 해당하고 Batch submitter, Data transport layer, Message relayer는 레이어 2 운영을 돕는 컨트랙트들이며, 각각의 역할은 표 2와 같다.

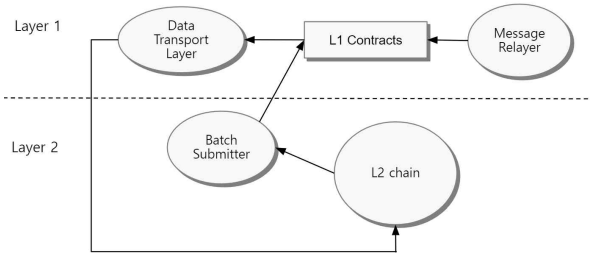

그림 3 Architecture of optimistic rollups
Fig 3. Architecture of optimistic rollups

Data transport layer는 L1의 컨트랙트를 모니터링하면서 L1 컨트랙트에 쌓인 트랜잭션 정보, L1의 상태 관리 컨트랙트에 쌓인 state root들을 자체 DB에 저장하고, 저장된 데이터들에 대한 API 서버 역할을 수행한다. Batch submitter는 L2 chain을 모니터링하면서 새로 생성되는 L2 블록에 대한 정보를 L1 contracts에 제출하는 역할을 수행한다. 마지막으로 Message relayer는 L2에서 L1으로 자산이동을 요청한 트랜잭션 중 챌린지 기간이 지난 트랜잭션을 처리하는 서비스를 담당한다. Message relayer가 필요한 상황은 여러 가지가 있는데, 다음은 Message relayer의 역할이 필요한 시나리오다.

1. 레이어 2에서 사용자가 본인의 토큰을 L1으로 출금하는 트랜잭션을 보낸 경우
2. 1의 트랜잭션이 L2 chain에서 블록에 담겼을 때
3. 2의 블록 정보를 Batch submitter가 L1 컨트랙트에 제출하는 트랜잭션을 보낸 경우
4. 3의 트랜잭션이 L1에서 블록에 담겼을 때
5. 4의 블록이 생성된 된 후 챌린지 기간이 지나고 난 뒤 Message relayer가 4의 후처리 트랜잭션을 보냈을 때
6. 5의 트랜잭션이 L1에서 블록에 담겼을 때, 사용자가 요청했던 주소로 토큰이 전송

Batch submitter에 의해 제출되는 데이터는 그림 2와 같은 형태이다. 해당 데이터의 헤더는 데이터의 길이에 대한 정보를 담고 있다. 그다음으로는 담겨 있는 트랜잭션의 숫자, 타임스탬프, L1 블록 넘버 등이 있고, 마지막으로는 트랜잭션의 길이와 rawTransaction 순으로 데이터가 구성 되어있다.

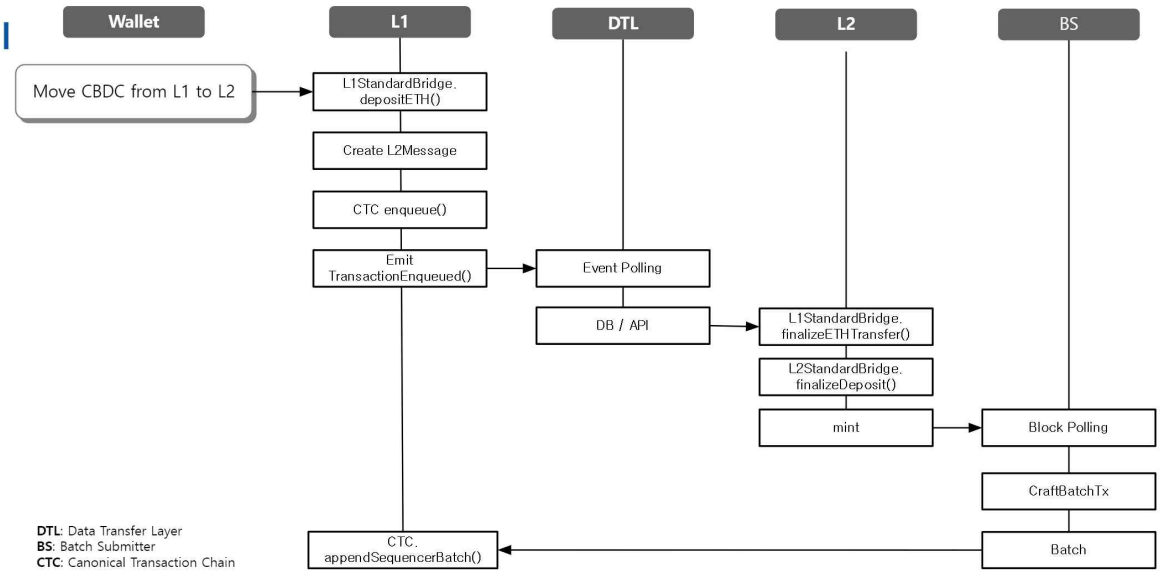

그림 4. Move CBDC from L1 to L2
Fig 4. Move CBDC from L1 to L2

옵티미스틱 롤업을 적용한 아키텍처를 활용할 경우 블록체인은 두 가지 계층이 존재하게 되는데 이러한 아키텍처의 특징은 전통적인 은행 시스템과 유

사한 구조를 갖고 있다는 점이다. 중앙은행과 시중은행 구조로 나누어져 있는 전통적은 은행 시스템을 2 계층(Two-tier) CBDC라고 한다[25].

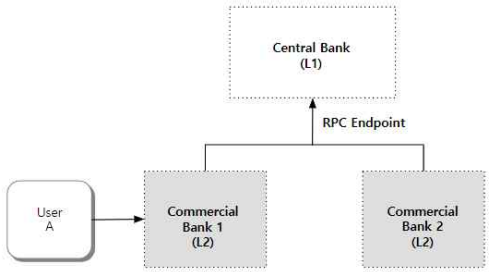

그림 5. Two-tier CBDC system
Fig. 5. Two-tier CBDC system

2 계층 구조에서 중앙은행이 담당하고 있는 첫 번째 계층을 레이어 1이 담당하고, 시중은행들이 담당하고 있는 두 번째 계층을 레이어 2가 담당한다. 중앙은행과 각 시중은행은 브리지를 통해 서로 연결되어 있으며 그림 5와 같은 구조를 갖고 있다. 브리지 컨트랙트는 시중은행과 중앙은행에 1:1 구조로 각각 배포되어 있다. 즉, 그림 5와 같은 경우에는 시중은행 1 - 중앙은행, 시중은행 2 - 중앙은행을 연결하는 총 4개의 브리지 컨트랙트가 배포됐다.

2 계층 구조에서는 중앙은행이 CBDC에 대한 발행과 회수를 담당하고 시중은행은 유통을 담당한다. 즉, CBDC 시스템 안의 모든 자산은 중앙은행이 관리하고 있으며, CBDC 시스템의 대부분의 거래를 차지할 사용자 간의 거래는 시중은행에서 발생하게 된다. 즉, 레이어 1에서 CBDC가 발행이 되면 실제 유통이 되기 위해서는 레이어 1에서 레이어 2로 CBDC의 이동이 있어야 한다.

1. CBDC 발행 및 시중은행으로 이동

위에서 언급한 것처럼 CBDC 거래를 위해서는 중앙은행인 레이어 1에서 발행한 CBDC를 시중은행이 있는 레이어 2로 가져와야한다. 본 연구에서는 시중은행에 지급된 CBDC가 사용자들에게 어떻게 분배되는지에 대해서는 논하지 않으며 중앙은행에서 발행된 CBDC가 시중은행으로 유통되는 과정을 deposit이라고도 하며, 자세한 deposit 과정은 그림 4와 같다.

deposit 과정을 간단히 요약하면 중앙은행에서 발행한 CBDC를 해당 시중은행과 연결되어 있는 브리지 컨트랙트에 예치한다. Data transport layer 컨트랙트가 예치 트랜잭션을 모니터링하여 자체 DB에 저장하고 L2 chain client에서 Data transport layer로부터 주기적인 정보 갱신을 통해 새로운 정보를 받아온다. 마지막으로 L2 chain client가 사용자가 L1 컨트랙트에 보냈던 예치 요청 트랜잭션을 처리하면, 레이어 2에서 사용자의 CBDC 잔액이 증가한다.

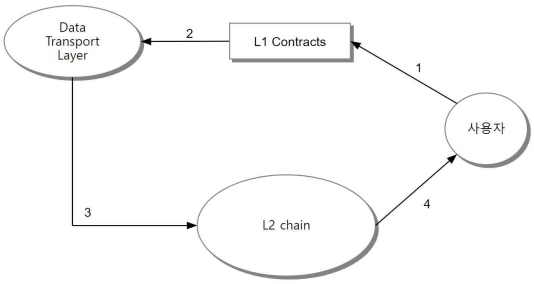

그림 6. Simple deposit process
Fig. 6. Simple deposit process

위와 같은 과정을 통해 CBDC가 사용자에게 지급이 되면 deposit 과정이 종료되며 그림 6은 이 과정을 간단하게 나타낸 도식이다.

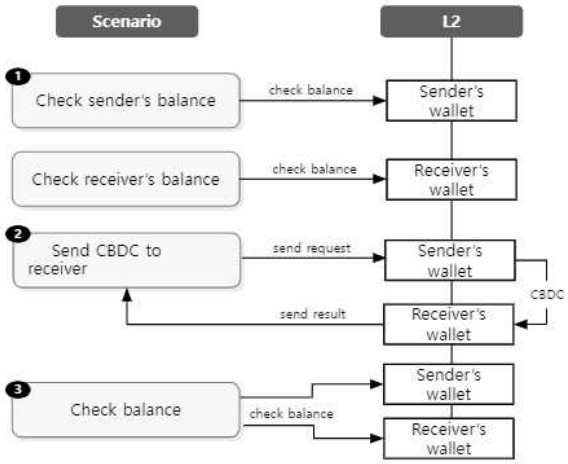

그림 7. Send balance flow
Fig. 7. Send balance flow

2. 같은 시중은행 간 CBDC 거래

사용자 간의 CBDC 거래는 전부 시중은행이 운영하는 레이어 2에서 이루어진다. CBDC를 보내는 절차는 먼저 보내는 사람의 계좌를 확인해서 보내고자 하는 금액 이상을 보유하고 있는지 확인한다. 그 다음 보내는 사람의 CBDC를 받는 사람에게 송금을 하고 그 결과를 가져온다. 받는 사람의 지갑과 보내는 사람의 지갑의 잔액을 조회하여 CBDC가 정상적으로 이체됐는지 확인하면 전송이 완료되며 그림 7이 이를 도식으로 나타낸 그림이다.

3. 다른 시중은행 간 거래

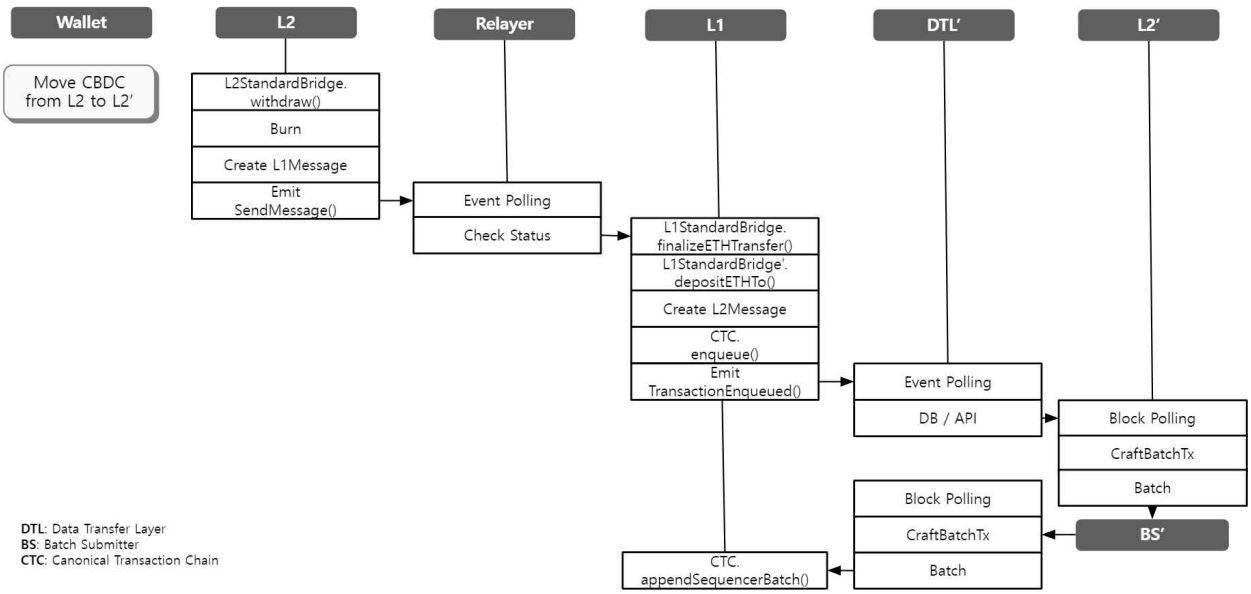

그림 9. Move CBDC from L2 to L2'
Fig. 9. Move CBDC from L2 to L2'

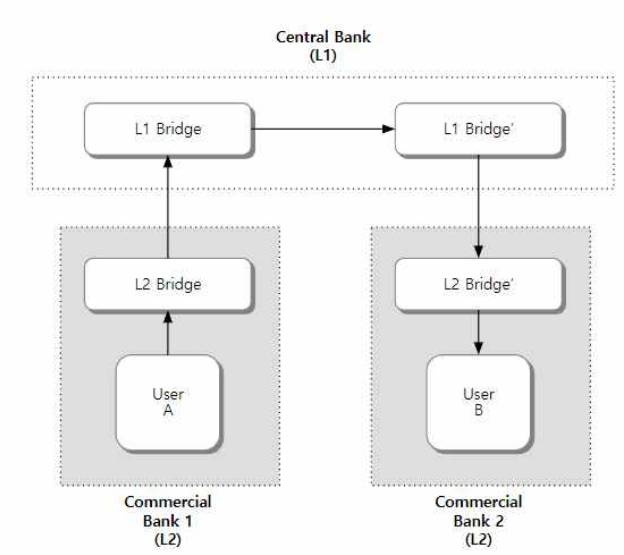

그림 8. Send CBDC to another layer2
Fig. 8. Send CBDC to another layer2

본 연구에서 제안한 CBDC 모델에서는 거래가 한 시중은행에서만 이루어지지 않는다. 같은 시중은행을 이용하는 사용자 간의 거래가 있을 수도 있지만, 다른 시중은행으로 금액을 보내는 거래도 발생할 수 있다.

다른 시중은행을 이용하는 사용자에게 CBDC를 보내면 시중은행에서 시중은행으로 직접 보내는 것이 아니라 그림 8처럼 중앙은행을 거쳐서 CBDC를 보내야 한다.

그림 8과같이 다른 시중은행에 있는 사용자에게 CBDC를 보내는 과정은 크게 두 가지로 구성되어 있다. 첫 번째는 시중은행 1에서 중앙은행으로 CBDC를 찾는 과정이다. 이 과정을 withdraw라고 하며 withdraw 과정은 그림 9와 같은 과정을 거쳐서 이루어진다.

그림 9의 과정을 간단히 살펴보면, 사용자가 가진 토큰에 대한 withdraw 요청을 L2 chain의 컨트랙트로 보내면, 해당 트랜잭션이 블록에 담긴 후, Batch submitter가 해당 트랜잭션을 모니터링한다. 그다음 Batch submitter가 해당 트랜잭션을 L1으로 보내고 Message relayer가 이에 대한 후처리 트랜잭션을 전송하여 해당 트랜잭션이 블록에 담기면 withdraw 절차가 완료 된다.

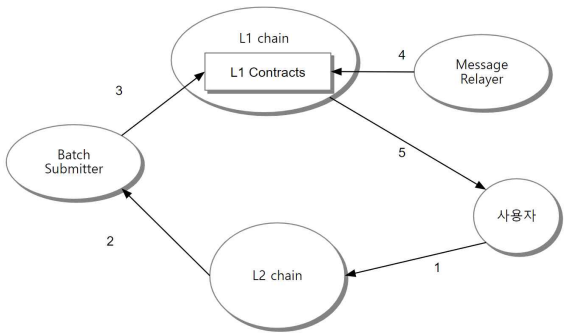

그림 10. Simple withdraw process
Fig. 10. Simple withdraw process

시중은행 1에서 인출이 완료되었다면, 그 다음 L1 Bridge'를 통해 시중은행 2로 deposit 되는 과정이 발생한다. 시중은행 2로 deposit이 완료되면 이용자 A가 전송한 CBDC는 이용자 B에게로 전달된다.

Ⅳ. 실험 및 성능분석

구현된 시스템의 실험에서는 먼저 On-chain 만을 이용해서 트랜잭션의 처리 속도를 측정한 다음, Off-chain에서 Off-chain의 개수를 점점 늘려가면서 초당 트랜잭션 처리량이 어떻게 변하는지 확인하였다.

1. 레이어 1에서의 확장성 실험

본 실험에 사용한 계정 개수는 500만 개며, 각 계정 사이의 임의 송금 거래가 일어났을 때 성능을 측정했다. 계정 개수는 전체 국민의 숫자를 5천만으로 가정하고 그중 10% 정도가 동시 거래하는 최대치라 가정하여 결정했다. 여기서 이야기하는 임의의 송금 거래란 임의의 계정에서 다른 임의의 계정으로 송금을 하는 거래를 의미한다.

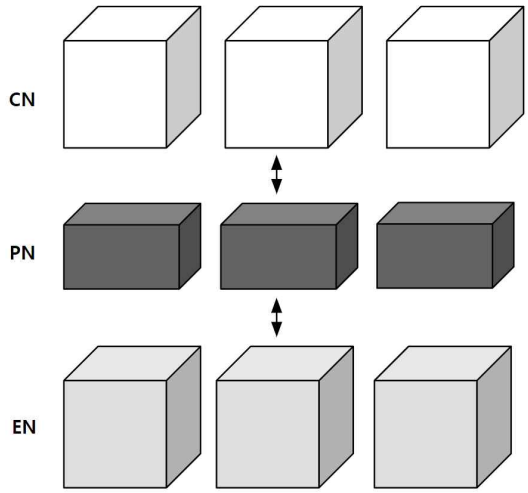

그림 11 Architecture of Klaytn
Fig. 11. Architecture of Klaytn

실험은 AWS와 네이버 클라우드에서 각각 진행되었으며, 노드 사양 및 대수는 클라우드 서비스와 관계없이 같다. 실험에 사용된 블록체인은 클레이튼이며, 실험에 사용된 노드와 노드의 스펙 및 실험 결과는 아래 표와 같다.

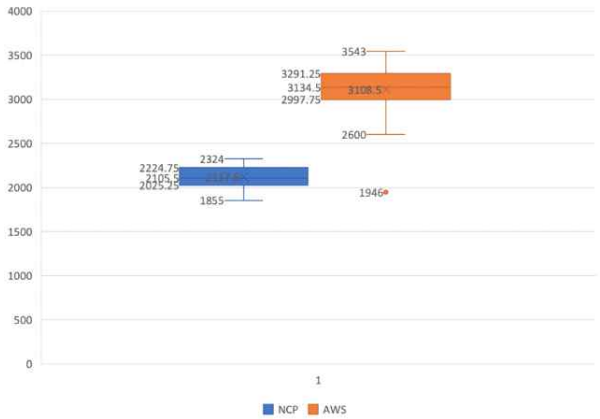

그림 12. Performance test result in layer1
Fig. 12. Performance test result in layer1

표 3 Test configuration
Table 3. Test configuration

구분	Detail node type	Node spec	Num of node
Layer1 node	Consensus node	32 vCPUs, 256GB	6
	Proxy node	16 vCPUs, 128GB	12
Transaction creator	-	2 vCPUs, 16GB	24

실험은 부하 생성기를 통해 트랜잭션을 발생시킨다. 발생한 트랜잭션은 레이어 1 노드로 전달되는데, 합의 노드는 블록 생성 프로세스에 참여하는 노드이고, 프록시 노드는 네트워크에 인터페이스를 제공하는 역할을 하며 해당 구조는 그림 11과 같다.
실험 결과 표 3 에서 제시한 부하 생성기의 스펙으로 트랜잭션을 30분간 발생시켰을 경우 초당 트랜잭션은 약 4200건 정도였다. 그리고 발생한 트랜잭션들을 실제로 블록체인 노드에서 처리한 양은 약 3,106건으로 측정되었다.

입력 TPS는 표 3의 부하 생성기를 통해 발생한 초당 트랜잭션의 개수를 의미하며 측정 TPS는 블록체인 노드에서 실제로 초당 처리한 트랜잭션을 의미한다.
표 4와 그림 12에서 클라우드 서비스 간 결과가 다른 것은 클라우드 서비스마다 서버의 프로비저닝 방식과 하드웨어의 세부 스펙에 차이가 있기 때문인 것으로 보인다. 이후의 실험에서는 더 우수한 성능을 보인 AWS에서만 진행할 예정이다.

표 4. Performance test result in layer1
Table 4. Performance test result in layer1

Input TPS	TPS in AWS	TPS in NCP
about 4,200	about 3,106	about 2,114

2. 레이어 2의 확장성 실험

위에서 언급한 것처럼 레이어 2를 이용한 확장성 실험에는 옵티미스틱 롤업을 사용한다. 옵티미스틱 롤업은 레이어 2에서 트랜잭션을 처리하고 트랜잭션들을 모아서 배치(Batch) 형태로 레이어 1에 기록함으로써 레이어 1과 동등한 보안 수준을 유지하면

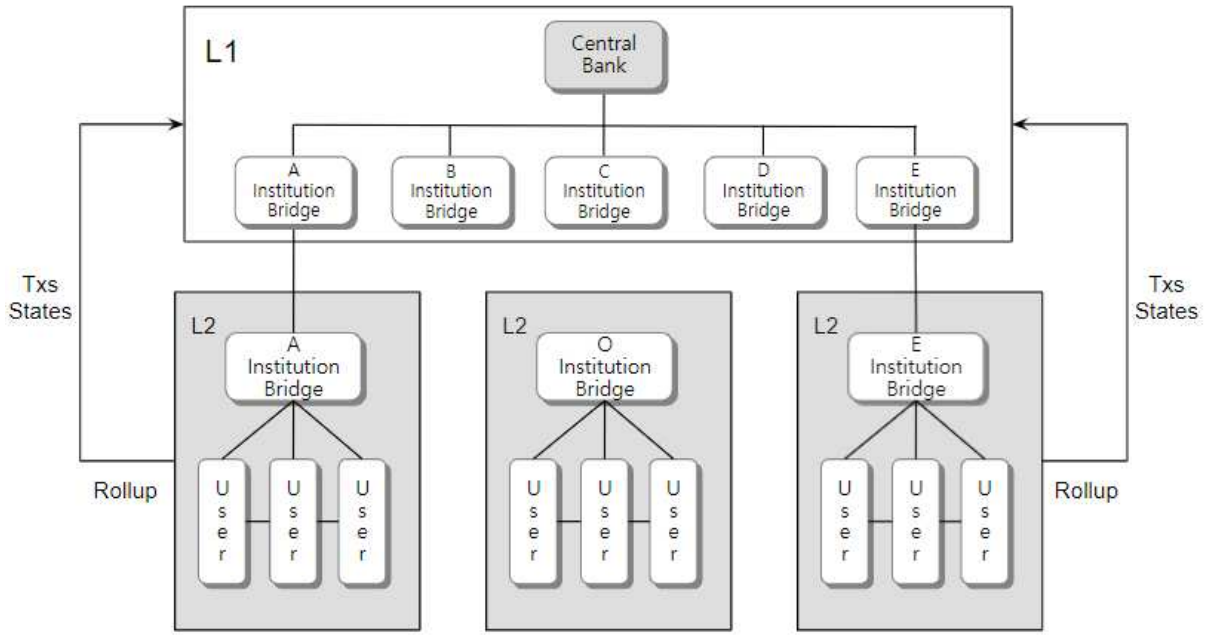

그림 13. Proposed architecture
Fig. 13. Proposed architecture

서 성능을 향상시킬 수 있다. Optimistic Rollup은 레이어 1에 트랜잭션을 기록하는 과정과 검증하는 과정을 분리한 효율적인 구조로 설계되었고, 레이어 1의 스마트 컨트랙트를 레이어 2에서 그대로 사용할 수 있기에 단순 송금 외에 다양한 금융시스템을 도입하기에 더 적합하다고 판단되어 확장성 실험의 도구로 채택했다.

본 논문에서는 롤업을 도입했을 때 성능실험에 중점을 두었기 때문에 검증자 임무를 수행하는 주체는 배제하였다. 이렇게 구성된 시스템의 아키텍처는 그림 13과 같다.

실험은 레이어 1과 연결된 레이어 2의 개수가 증가할수록 처리량이 증가하는지 확인할 수 있도록 아래 표와 같은 사양으로 레이어 2의 개수를 2개에서 15개까지 늘려가며 성능을 측정했으며, 각 구성요소의 스펙은 표 5에 제시된 내용과 같다.

표 5 Optimistic Rollup performance test environment
Table 5. Optimistic Rollup performance test environment

Item	Node spec	Number of node(EA)
Layer 2 node	16 vCPUs, 32GB	2 ~ 15
Transaction creator	4 vCPUs, 8GB	2 ~ 15

실험 방식은 앞선 실험과 같이 레이어 2에서 부하생성기를 이용해 트랜잭션을 발생시켰고, 레이어 1에 제출된 트랜잭션의 양을 계산하여 최대 처리량을 산출하였다. 실험에 참여한 계정의 수는 동일하게 500만 개로 설정하였으며, 노드의 개수가 늘어남에 따라 각 노드에 균등하게 분배되었다. 트랜잭션은 임의의 계정에서 임의의 계정으로 트랜잭션을 보내는 방식으로 진행됐으며 실험은 30분간 진행됐다.

실험 결과에서 확인할 수 있는 것처럼 노드의 개수가 증가함에 따라 처리하는 트랜잭션의 양이 선형적으로 증가함을 확인할 수 있다. 노드 개수가 5개 정도까지는 레이어 1을 사용하는 것과 성능 측면에

서 큰 차이는 없었으나, 그 보다 노드의 개수가 늘어났으면 처리량이 약 3배 정도 좋아진 것을 확인할 수 있다.

표 6 Throughput changes as the number of nodes changes
Table 6. Throughput changes as the number of nodes changes

L2 Node(EA)	Total throughput (TPS)	Average throughput per node (TPS)	Performance ratio
1	728	728	100%
2	1,433	717	98%
5	3,559	712	98%
10	7,123	712	98%
15	10,483	699	96%

표 6의 성능 측정 항목들에 관해 설명하자면, Total throughput은 노드 개수 변화에 따른 초당 트랜잭션 처리량을 나타낸 수치이고, Average throughput per node는 노드 당 평균 트랜잭션 처리량을 의미한다. 그리고 실험 결과를 살펴보면 노드 개수가 늘어날수록 Average throughput per node가 조금씩 줄어드는 것을 확인할 수 있는데, 이는 레이어 2 노드가 많아질수록 이를 레이어 1에 제출되는 배치가 늘어나게 되고 이에 따른 처리 속도에 지연이 발생하게 되면서 노드 당 평균 트랜잭션 처리 속도에 저하가 발생하는 것이다.
따라서, 노드 1개를 사용했을 때에 비해서 노드 당 처리량을 나타낸 수치로 Performance ratio로 표현했다. 그림 14는 노드 개수에 따른 최대 처리량을 그래프로 나타낸 것이다.

V. 결론

본 논문에서는 최근 블록체인 업계에서 주목받고 있는 레이어 2 솔루션을 적용해 확장성이 강화된 디지털 화폐 모델을 제시했다. 제시된 모델에서는 각 시중은행이 운영하는 레이어 2가 중앙은행이 운영하는 레이어 1에 연결되어 있다는 가정을 한다. 본 논문에서 제안하는 모델은 옵티미스틱 롤업의 특징 중 하나인 EVM과의 상호 운용성(Compatibility)[29]을 활용해 단순한 송금뿐만 아니

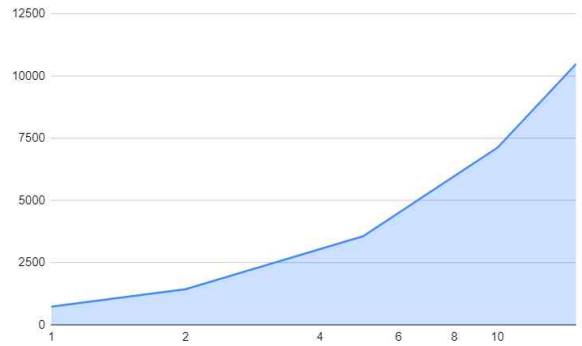

그림 14. 레이어 2 노드 개수에 따른 최대 처리량
Fig. 14. Maximum throughput based on the number of layer 2 nodes

라, 각 레이어 2에는 운영 주체인 각 시중은행이 제공하는 금융 서비스를 dApp화 하여 CBDC와 함께 서비스 할 수도 있다. 이 실험을 통해 하나의 레이어 1에 많은 수의 레이어 2를 연결해 전체적으로 더 많은 트랜잭션을 처리할 수 있음을 확인했다. 트랜잭션 처리량 외에도 다수의 레이어 2를 도입하는 것의 장점은 특정 레이어 2에 문제가 생기더라도 다른 레이어 2에 영향을 주지 않는다는 점이다. 만약 하나의 블록체인만을 이용해 시스템을 구성했을 때, 블록체인에 문제가 생긴다면 전체 시스템에 영향을 끼칠 것이다.
대부분의 중앙은행은 블록체인이 적용된 CBDC 체계에 긍정적이며, 많은 은행이 블록체인 기반 CBDC 프로토타입까지 제안했다. 그러나 이들 은행은 CBDC에서 블록체인 적용을 모색할 뿐 블록체인 기반 CBDC를 구현한 중앙은행은 없다. 성능, 확장성, 교차 체인 상호 운용성 및 사용 시나리오 등의 기술적인 문제[30]와 상업은행의 비즈니스 모델에 대한 위험, 민간 은행 부문의 시스템 위험성 증가, 개인 정보 보호 위험 등의 위험성 등의 비즈니스적인 문제[31] 등 다양한 영역에서 극복해야 할 몇 가지 과제가 여전히 남아 있기 때문이다.
본 논문에서 제시한 모델의 레이어 2는 레이어 1과 동일한 스마트 컨트랙트를 지원하는 옵티미스틱 롤업을 사용했기 때문에, 레이어 2에서도 모든 종류의 스마트 컨트랙트를 활용하여 레이어 1과 동일한 호환성을 유지하며 위에서 언급 CBDC에 필요한 다양한 요구사항을 만족하게 할 수 있을 것으로 판단된다.
다만 레이어 2에서 다양한 스마트 컨트랙트를 지원할 수 있다는 장점이 있지만, 레이어 1에 제출하는 트랜잭션들의 정보를 최적화하기에는 어느 정도의 한계가 있어 처리량을 극적으로 늘리기 어렵다는

단점이 있다.

추후 CBDC 환경에 필요한 시스템이 구체화되고 주로 사용하는 프로그램이 정형화된 후에는, 하나의 옵티미스틱 롤업에서 여러 종류의 스마트 컨트랙트를 사용하는 것이 아니라 프로그램에 맞게 최적화된 롤업을 따로 운영하는 것이 효율적일 수 있다.

예를 들어, 레이어 2에서 자산의 이동만을 지원하고자 하는 경우 레이어 2 자체는 물론이고 레이어 2가 레이어 1에 데이터를 올리는 과정까지 많은 최적화를 할 수 있다. 마찬가지로, 은행의 예치 상품이나 금융 상품만을 지원하고자 하는 롤업을 별도로 최적화하여 만들 수 있을 것이다. 이를 위해서는 다음과 같은 점들이 개선된다면 전반적인 성능을 기대할 수 있을 것으로 판단된다.

시중은행 간 거래 시 성능 개선: 시중은행 간 송금 시에는 시중은행에서 트랜잭션이 발생한 후 중앙은행이 운영하는 L1에서 트랜잭션이 발생하게 된다. 결국, 두 번의 트랜잭션이 순차적으로 일어나기 때문에 비효율적이고 시중은행이 운영하는 레이어 2에 부하가 커질수록 거래를 처리하는 데 오랜 시간이 걸리게 된다. 이런 문제를 개선하기 위해 시중은행에서 타 기관 송금을 위한 자산을 별도로 관리하게 된다면, 사용자가 타 기관으로 송금 요청 시에 중앙은행을 거치지 않고 시중은행 간 거래를 빠르게 처리할 수 있을 것이다.

시중은행이 생산하는 블록에 포함되는 거래 개수: 본 논문에서 사용한 옵티미스틱 롤업은 거래가 발생할 때 마다 state root hash를 확인하기 위해서 하나의 블록에 하나의 트랜잭션만 포함된다. 이를 통해서 검증자는 시중은행 블록체인에서 최종 값을 중앙은행에 반영할 때에 검증할 수가 있다. 만약 CBDC 환경을 고려하여 검증 절차를 변경하고 하나의 블록에 많은 트랜잭션을 포함할 수 있다면 시중은행 블록체인의 성능이 향상 될 수 있다.

결론적으로, 본 실험을 통해 CBDC를 하나의 블록체인이 아닌 여러 블록체인을 사용하는 모델에 도입했을 때의 사용 가능성을 확인할 수 있었다. 또한, 해당 모델을 CBDC 환경에 맞게 최적화한다면, 전체적인 네트워크의 처리량을 늘릴 수 있음을 확인했다.

References

[1] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, Nov. 2009.

[2] Buterin, Vitalik, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", https://ethereum.org/en/whitepaper/, 2014.

[3] Abadi, Joseph, and Brunnermeier, Markus, "Blockchain economics", National Bureau of Economic Research, No. w25407, 2018.

[4] Yakovenko, A., "Solana: A new architecture for a high performance blockchain V0. 8.13", White Paper, 2018.

[5] Sekniqi, K., Laine, D., Buttolph, S., and Sirer, E. G., "Avalanche Platform", https://www.avalabs.org/whitepapers, 2020.

[6] Hafid, A., Hafid, A. S., and Samih, M., "Scaling blockchains: A comprehensive survey", IEEE Access, vol. 8, pp. 125244 - 125262, 2020.

[7] Bitcoin Cash. Accessed: Sep. 1, 2019. [Online]. Available:https://www.bitcoincash.org/

[8] M. Zamani, M. Movahedi, and M. Raykova, “RapidChain: Scalingblockchain via full sharding,” in Proc. ACM SIGSAC Conf. Comput.Commun. Secur., Jan. 2018, pp. 931 - 948.

[9]A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, “Spritesand state channels: Payment networks that go faster than lightning,” inProc. Int. Conf. Financial Cryptogr. Data Secur. Frigate Bay, St. Kitts:Springer, 2019, pp. 508 - 526.

[10] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell,A. Miller, A. Poelstra, J. Timón, and P. Wuille. (2014).

EnablingBlockchain Innovations With Pegged Sidechains. [Online]. Available:http://www.opensciencereview.com/papers/123/enablingblockchaininnovations-with-pegged-sidechains

[11] Poon, Joseph, and Buterin, Vitalik, "Plasma: Scalable autonomous smart contracts", White paper, 2017.

[12] Validium And The Layer 2 Two-By-Two https://www.buildblockchain.tech/newsletter/issues/no-99-validium-and-the-layer-2-two-by-two, June 14, 2020

[13] An Incomplete Guide to Rollups. Vitalik Buterin. https://vitalik.ca/general/2021/01/05/rollup.html. Jan 05, 2021

[14] 김영식(서울대학교 경제학부), 권오익(한국은행 경제연구원 금융통화연구실), "중앙은행 디지털화폐(CBDC) 발행의 의의 및 필요성", [BOK] 경제분석, 28(4), 2022.

[15] Jung, Hyunjun, "ISO/IEC 11179-based Blockchain System for Exchange Between CBDCs", The Journal of Korean Institute of Information Technology, 18(7), pp. 43-50, 2020.

[16] 박동욱, "유럽 CBDC 논의 동향 및 주요 쟁점", https://www.kisdi.re.kr/report/view.do?key=m2101113025536&masterId=3934550&arrMasterId=3934550&artId=1149156, Jun. 2023.

[17] Yoon, Jae-ho, Kim, Yong-min, "CBDC Model with Enhanced Anonymity Using ID Certificate and Blockchain Encryption", Journal of the Korea Institute of Information Security & Cryptology, 33(2), pp. 139-149, 2023.

[18] BIS, "Central bank digital currencies: foundational principles and core features", https://www.bis.org/publ/othp33.pdf.

[19] Bank of England, "Discussion Paper: Central Bank Digital Currency", https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf.

[20] Qianrui Zhao, Yinan Wang, Bo Yang, et al.A Comprehensive Overview of Security Vulnerability Penetration Methods in Blockchain Cross-Chain Bridges.TechRxiv.October 18, 2023.

[21] Plasma MVP (Minimal Viable Plasma), https://ethresear.ch/t/minimal-viable-plasma/426, Accessed: Aug. 16. 2023.

[22] Dziembowski, Stefan, Fabiański, Grzegorz, Faust, Sebastian, and Riahi, Siavash, "Lower Bounds for Off-Chain Protocols: Exploring the Limits of Plasma", https://eprint.iacr.org /2020/175, Oct 2020.

[23] Chen, Thomas, et al., "A review of zk-snarks", arXiv preprint arXiv:2202.06877, 2022.

[24] Petkus, Maksym, "Why and how zk-snark works", arXiv preprint arXiv:1906.07221, 2019.

[25] Bindseil, Ulrich, "Tiered CBDC and the Financial System", Available at SSRN: https://ssrn.com/abstract=3513422, January 2020.

[26] Thibault, Louis Tremblay, Sarry, Tom, and Senhaji Hafid, Abdelhakim, "Blockchain scaling using rollups: A comprehensive survey", IEEE Access, 2022.

[27] Ethereum. Bridges – Bridge Types.

https://ethereum.org/en/developers/docs/bridges/#bridge-types
[28] Qianrui Zhao, Yinan Wang, Bo Yang, et al.A Comprehensive Overview of Security Vulnerability Penetration Methods in Blockchain Cross-Chain Bridges.TechRxiv.October 18, 2023.
[29] Jia, Ruizhe, and Yin, Steven, "To EVM or not to EVM: Blockchain compatibility and network effects", *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*, 2022.
[30] Zhang, Tao, and Huang, Zhigang, "Blockchain and central bank digital currency", *ICT Express*, Volume 8, Issue 2, Pages 264-270, ISSN 2405-9595, https://doi.org/10.1016/ j.icte.2021.09.014, 2022.
[31] Cunha, Paulo Rupino & Melo, Paulo & Sebastiao, Helder, "From Bitcoin to Central Bank Digital Currencies: Making Sense of the Digital Money Revolution", *Future Internet*, 13, 165, 10.3390/fi13070165, 2021.

김 길 동 (Gil-dong Kim)

2.5×3.0㎜
삽입그림으로

1992년 2월 : 한국대학교 전자 공학과 졸업
1994년 2월 : 한국대학교 전자 공학과 석사
1996년 3월~현재 : 한국대학교 전자공학과 박사과정

<관심분야> 전자공학, 통신공학, 광통신 공학
[ORCID:]

< 논문 게재 관련 알림 사항 >

1. 교신저자 및 제1저자는 논문게재년에 반드시 학회 '활동' 회원 이어야 합니다.
(가입 후 연회비를 납부하지 않은 회원께서는 논문이 게재되는 년도에 연회비를 납부하여 주시기 바라며, 비회원의 경우에는 회원자격을 확인하시어 membership@kics.or.kr로 메일 주시기 바랍니다.)

2. 통신학회 논문은 매월 마지막 날 발행됩니다.
(※ 제 36권 12호 : 2011년도 12월 31일 발행)