Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.1, Feb. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.1.129

강화학습 기반의 CBDC 처리량 및 네트워크 부하 문제 해결 기술*

이 연 주,[1†] 장 호 빈,[1] 조 수 정,[1] 장 규 현,[2] 노 건 태,[3] 정 익 래[2‡]
[1,2]고려대학교 (대학원생, 교수), [3]서울사이버대학교 (교수)

Enhancing Throughput and Reducing Network Load in Central Bank Digital Currency Systems using Reinforcement Learning*

Yeon Joo Lee,[1†] Hobin Jang,[1] Sujung Jo,[1] GyeHyun Jang,[2]
Geontae Noh,[3] Ik Rae Jeong[2‡]
[1,2]Korea University (Graduate student, Professor),
[3]Seoul Cyber University (Professor)

요 약

디지털 전환이 다양한 분야에서 가속되고 있는 가운데, 금융시장에서도 디지털·전자화된 화폐를 포함한 지급결제 수단 발전에 관한 관심이 집중되고 있다. 그중 중앙은행 디지털화폐(Central Bank Digital Currency, CBDC)는 기존 실물 화폐를 대체할 수 있는 미래 디지털화폐로 가치변동이 없으며 기존 실물 화폐인 현금과 1:1 등가교환이 가능하다. 최근 국내·외에서는 CBDC 출시를 위해 다양한 연구 및 개발을 진행하고 있다. 그러나, 현재 CBDC 시스템은 대용량 거래에 대한 처리 속도 지연, 응답대기시간 지연 및 네트워크 부하 등 CBDC 확장성에 관한 문제가 존재한다. 범용적인 CBDC 시스템을 구축하기 위해서는 기존 블록체인의 낮은 처리량 및 네트워크 부하 문제 등의 확장성 문제를 해결해야 한다. 따라서, 본 연구에서는 범용 CBDC 구축을 위한 강화학습 기반의 CBDC 환경에서 대용량 데이터에 대한 처리량 및 네트워크 부하 문제 해결 기술을 제안한다. 제안 기술은 기존 시스템 대비 최대 64배 이상의 처리량 증대 및 20% 이상의 네트워크 부하를 감소할 수 있다.

ABSTRACT

Amidst the acceleration of digital transformation across various sectors, the financial market is increasingly focusing on the development of digital and electronic payment methods, including currency. Among these, Central Bank Digital Currencies (CBDC) are emerging as future digital currencies that could replace physical cash. They are stable, not subject to value fluctuation, and can be exchanged one-to-one with existing physical currencies. Recently, both domestic and international efforts are underway in researching and developing CBDCs. However, current CBDC systems face scalability issues such as delays in processing large transactions, response times, and network congestion. To build a universal CBDC system, it is crucial to resolve these scalability issues, including the low throughput and network overload problems inherent in existing blockchain technologies. Therefore, this study proposes a solution based on reinforcement learning for handling large-scale data in a CBDC environment, aiming to improve throughput and reduce network congestion. The proposed technology can increase throughput by more than 64 times and reduce network congestion by over 20% compared to existing systems.

Keywords: CBDC(Central Bank Digital Currency), Scalability, Cross-Shard Transaction, Reinforcement Learning

Received(11. 21. 2023), Modified(01. 02. 2024), Accepted(01. 02. 2024)
* 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1F1A1060543).
† 주저자, lyjoo17@korea.ac.kr
‡ 교신저자, irjeong@korea.ac.kr(Corresponding author)

I. 서 론

디지털 전환(Digital Transformation)이 다양한 분야에서 가속됨에 따라 금융 분야에서도 디지털·전자화된 화폐를 포함한 지급결제수단 발전에 관심이 집중되고 있다. 그중 최근 국내·외에서는 기존 실물 화폐를 대체할 수 있는 중앙은행 디지털화폐(Central Bank Digital Currency, CBDC)에 관한 연구가 활발히 진행되고 있다[1]-[4].

CBDC는 중앙은행이 발행하는 법정통화로 가상화폐와 달리 가치변동의 위험이 없으며, 현금과 1:1 등 가교환이 가능하다. 이는 기존 실물 화폐와 달리 화폐 가치가 전자적으로 저장되어 사용자 간 자금 이체를 통해 지급 결제가 가능하다. 국제결제은행(Bank for International Settlements, BIS)의 연구 결과에 따르면 전 세계 중앙은행 84% 이상이 CBDC 연구에 착수하였으며, 그중 50% 이상이 실제 도입을 위해 파일럿을 진행하고 있음을 확인할 수 있다[5]. 이처럼 전 세계적으로 CBDC 실용화에 대한 관심이 증가하고 있으며, 한국에서도 「한국은행 지급결제제도 컨퍼런스」 및 「CBDC 모의 시스템 금융기관 연계 실험」 등 연구가 진행되고 있다[6][7].

그러나, 2023년 「CBDC 모의 시스템 금융기관 연계 실험」에 따르면, 현재까지 진행된 CBDC 시스템은 대용량 거래 처리에 대한 블록 처리 속도 지연, 낮은 처리량, 응답대기시간 지연 및 네트워크 부하 등 CBDC 확장성 문제가 존재한다[7]. 범용적인 CBDC 시스템을 구축하기 위해서는 기존 블록체인 낮은 처리량 및 네트워크 부하 문제 등의 확장성 문제를 해결해야 한다.

본 연구에서는 범용 CBDC 구축을 위한 강화학습 기반의 CBDC 환경에서 대용량 데이터에 대한 낮은 처리량 및 네트워크 부하 문제 해결 기술을 제안한다. 제안 기술은 기존 시스템 대비 최대 64배 이상의 처리량 증대 및 20% 이상 네트워크 부하를 감소할 수 있다.

본 연구는 강화학습 기반의 CBDC 처리 속도 및 네트워크 부하 문제를 해결하는 기술 제안으로 다음 세 가지 연구를 수행하였다.

- 대표적인 공개형 블록체인인 이더리움의 실 트랜잭션 데이터를 추출하여, 기존 블록체인의 확장성 문제를 분석하였다.
- 실 트랜잭션 데이터를 사용하여 네트워크 부하 감소 및 부하분산에 최적화되도록 심층 강화학습을 설계 및 학습하였다.
- 다양한 실험환경에서 처리량, 네트워크 부하 및 부하분산 정도 등을 측정하여 기존 시스템과 성능을 비교하였다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인과 강화학습의 배경지식과 금융권에서의 CBDC에 관하여 서술한다. 3장에서는 블록체인 트랜잭션 데이터 분석하고, 4장에서는 강화학습 기반 계정 재배치 기법을 제안한다. 마지막 5장에서는 제안한 기법의 성능을 평가하고, 6장에서는 결론에 대해 논한다.

II. 배경지식

2.1 블록체인 (Blockchain)

비트코인(Bitcoin)은 사토시 나카모토로 부터 처음 제안된 블록체인 기술로 기존 중앙화된 시스템 거래 방식을 탈피하여 시스템에 참여한 각 노드가 별도의 분산원장을 유지함으로써 탈중앙성, 데이터 무결성, 불변성 및 투명성을 보장한다[8]. 비트코인은 잔액 기반 블록체인으로 거래 내역을 블록체인에 기록하는 UTXO(Unspent Transaction Output) 방식을 사용한다. 또한 시스템에 참여한 각 노드는 구성원들 간 P2P(Peer-to-Peer) 방식을 기반으로 PoW(Proof-of-Work) 및 PoS(Proof-of-Stake) 등의 합의 알고리즘을 통해 분산원장에 데이터를 기록할 수 있으며, 시스템 상에 독단적인 데이터 수정이 불가하다는 보안상 이점을 가진다. 이러한 특성으로 현재 블록체인 기술은 IoT(Internet-of-Things), 의료 데이터 관리, 모바일 네트워크 등 다양한 분야로 확장되어 활용되고 있다[9]-[11].

이더리움은 비탈릭 부테린에 의해 제안된 블록체인 기술 기반의 암호화폐 플랫폼으로 2세대 암호화폐라 불린다. 이더리움은 거래 내역을 기록하는 비트코인과 다르게 계좌 잔액을 블록체인에 기록하는 계좌 기반 방식을 사용한다. 따라서 잔액 기반 블록체인보다 현재 상용되는 은행 모델과 유사한 계좌 기반 블록체인이 CBDC의 적용에 적합하다[12]. 이더리움은 확장성, 보안성, 지속가능성 개선을 위해 계속해서 업그레이드를 진행 중이다[13].

블록체인 기술이 다양한 분야로 적용됨에 따라, 각 네트워크에서 발생하는 대용량 데이터 처리에 관

한 확장성(Scalability) 문제가 대두되고 있다. 실제 공개형 블록체인인 비트코인과 이더리움의 경우, 초당 처리되는 트랜잭션 수인 TPS(Transaction-Per-Second)가 각각 5TPS와 14TPS로 초당 약 1,500 ~ 2,000건의 거래를 처리하는 VISA와 비교하면 현저히 낮다. 따라서, 블록체인 기술이 범용적으로 사용되기 위해서는 블록체인 확장성 문제 해결은 필수적이다.

2.1.1 샤드 블록체인(Sharded Blockchain)

블록체인의 확장성 문제를 개선할 수 있는 방법으로는 샤딩(Sharding)이 존재한다. 샤딩은 메인 네트워크의 처리량을 증대시키는 온체인(On-Chain) 솔루션으로 메인 네트워크를 샤드(Shard)라는 작은 서브 네트워크로 분할하여 트랜잭션을 병렬로 처리함으로써 블록체인 TPS를 향상시키는 기술이다. 샤드 블록체인 구조는 Fig. 1.과 같다.

시스템에 참여한 각 계정은 해시 기반의 고정된 주소 앞자리에 따라 각 샤드에 배치되며, 거래하는 계정 위치에 따라 IST(Intra-Shard Transaction)와 CST(Cross-Shard Transaction)를 생성할 수 있다. IST는 동일 샤드에 존재하는 계정 간의 트랜잭션으로 내부 합의 프로토콜을 통해 트랜잭션을 처리함으로써 네트워크의 부하가 적다. 반면, 서로 다른 샤드에 위치하는 계정 간의 트랜잭션인 CST는 두 샤드 간 동기/비동기 통신이 요구되어 수수료(fee)와 지연 시간(latency) 및 트랜잭션이 블록에 기록되는 확인 시간(confirmation time)이 높다. CST는 IST보다 샤드 간에 통신이 많이 요구되어 샤드에 높은 부하(load)를 야기하고, 확장성이 저하된다. 따라서, 블록체인 처리량을 확장하기 위해서는 CST보다 IST가 많아야 한다.

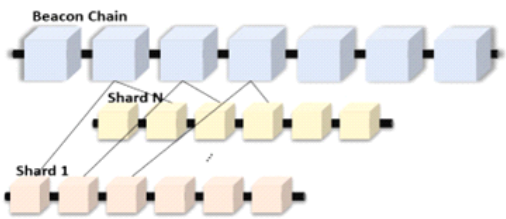

Fig. 1. The structure of sharded blockchain.

2.2 강화학습(Reinforcement Learning)

강화학습은 주어진 상황에서 최대의 보상을 얻도록 설계된 기계학습의 한 종류이다. 이는 MDP (Markov Decision Process)에 따라 현재 상황에서 다음 상황으로 가기 위한 최적의 방법을 결정하는 기술로 환경(environment) 안에 정의된 에이전트(agent)는 현재의 상태(state)를 인식해 선택 가능한 행동 중 최대의 보상(reward)을 받는 최적의 행동(action)을 선택한다.

강화학습 정의를 살펴보면 식 (1)과 같다. 현재와 미래 상태 s, s'와 행동 a, a'의 보상 r에 대한 식을 $Q(s,a)$라 할 때, 다음 상태와 행동을 포함한 식은 아래와 같다.

$$Q(s,a) = r + \max_{a}(Q(s',a')) \quad (1)$$

동적 프로그래밍 방식인 기존 강화학습 모델은 Q-learning으로 에이전트가 현재와 미래 상태를 학습하여 최적의 행동을 결정한다. 그러나, 이는 학습 상태와 행동에 대한 정량적 제약이 존재하여 대용량 데이터 학습 및 처리에 사용하기 어렵다.

심층 강화학습 기법은 기존 동적 프로그래밍으로 해결하기 어려운 대용량의 상태와 행동들을 딥러닝 모델을 통해 학습하여 최적의 행동을 결정하는 기술로 DQN(Double Q-learning), DDQN(Double DQN) 알고리즘 등이 존재한다. Fig. 2.는 두 종류의 강화학습 절차를 시각화한 그림으로 학습 주체가 상이하다[12]-[14].

DDQN은 단일 딥러닝 모델에서 학습하는 DQN의 미래 보상에 대한 오차를 반영하고자 현재와 미래의 학습 모델을 분리한 알고리즘이다. 이는 미래 보상에 대한 감가율(discount factor) γ와 학습 파

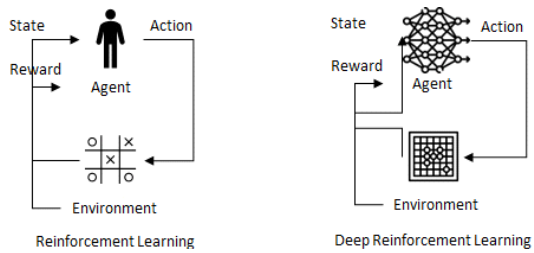

Fig. 2. The process of deep reinforcement learning

라미터 θ, θ', $\max_a(Q(s,a))$를 도출하는 행동 argmax를 사용하여 다중 딥러닝 모델을 학습하고 최적의 상태를 출력한다. DDQN은 식 (2)와 같다.

$$Q(S_t, a; \theta') = R_t + \gamma Q(S_{t+1}, \arg\max_a(Q(S_{t+1}, a; \theta)); \theta') \quad (2)$$

2.3 블록체인과 금융권

블록체인은 급변하는 디지털 전환 속 기존 지급결제시스템을 대체할 수 있는 미래 중앙은행 디지털화폐에 적합한 기술로 최근 국내·외 금융시장에서 주목받고 있다. 2014년 처음 발행된 스테이블 코인인 테더(Tether)를 기준으로 블록체인 기술을 기반한 암호자산 거래와 탈중앙화 금융(DeFi, Decentralized Finance) 등 다양한 결제 수단이 증가하였다[17][18]. 또한, 최근 디지털 자산의 소유주를 증명하는 가상 토큰인 NFT(Non- Fungible Token)와 같은 금융상품 및 시장이 빠르게 확장되고 있다[19].

2.3.1 블록체인 기반 CBDC 연구 동향

기존 실물 화폐를 대체하는 전자화된 법정통화로써의 역할을 하기 위해 CBDC의 거래율을 향상시키는 연구가 활발히 진행되고 있다[12][20].

Lovejoy 기타 등은 CBDC의 확장성을 확보하는 모델을 제안 및 구현하였다[20]. 트랜잭션 합의 과정을 서브 네트워크로 분리하여 구성하였고 지연에도 안전하게 거래를 처리할 수 있도록 샤드 블록체인을 도입하여 기존 거래 처리량보다 평균적으로 2배 이상 향상된 거래 처리량을 보였다. 이외에도 트랜잭션 구성 요소를 단순화하고 일원화하는 방식 등 향상된 거래 처리량을 확보하였다. 하지만 해당 모델은 잔액 기반 블록체인을 이용한 CBDC로 현존하는 은행 모델과 시스템 동작방식이 다소 상이하다. 따라서 실물화폐와 등가 교환이 가능한 전자화폐로서의 역할을 하는 시스템 설계 및 오프라인 지불과의 상호 작용에 대한 가능성 검증이 필요하다.

Tsai 기타 등은 계좌 기반 블록체인과 잔액 기반 블록체인을 이용하여 멀티체인 기반의 CBDC 모델을 설계하였다[12]. 해당 모델은 거래 확장성을 확보하기 위해 거래 대상 은행에서는 계좌 기반 블록체인을 이용하고, 서로 다른 은행 간에는 잔액 기반 블록체인을 이용하였다. 두 블록체인을 병합해 사용함으로써 기존의 은행 모델에 적합하며 확장성을 확보한 CBDC 시스템을 제안하였다. 해당 스킴은 계좌 기반 블록체인과 잔액 기반 블록체인의 혼합사용 시 처리량이 높아짐을 확인하는 실험을 진행했다. 하지만 각 블록체인의 노드에 따른 거래 처리량 변화 외 블록체인 자체의 처리량 저하에 큰 영향을 받을 것으로 예상된다. 또한 잔액 기반 블록체인과 계좌 기반 블록체인을 이용할 시 각 노드들은 단일 실패 지점이 될 가능성이 존재하여 이는 실 시스템상의 취약점이 될 수 있다.

최근 샤드 블록체인에서 높은 네트워크 부하를 야기하는 CST와 각 샤드에서의 부하 불균형(load imbalance) 문제를 해결하기 위해 다양한 연구 접근법이 제시되었다. 그중 계정 재배치 기법은 각 계정이 할당되는 샤드의 위치를 CST가 많이 발생되는 샤드로 재배치하는 기술이다. 이는 계정에 매핑된 샤드 번호를 단순 변경하는 기술로 기존 블록체인의 안전성을 보장한다. Okanami 등의 연구에서는 SA(Simulated Anneling) 휴리스틱 알고리즘을 사용하여 계정을 매번 랜덤하게 계정에 할당시켜 샤드에서 발생하는 CST를 감소하고자 하였다. 그러나, 해당 기법은 블록이 생성되는 매 에폭마다 계정을 랜덤하게 할당시키므로, 불필요한 계정 움직임이 초래되어 부하를 발생시킨다는 문제가 존재한다.

2.3.2 국내 시장 동향

한국은행은 기존 법정화폐와 동일한 화폐단위를 가지며, 현금과 1:1 등가교환이 가능한 CBDC를 도입하기 위하고자 지속적인 연구 및 프로젝트를 진행하고 있다[18][19].

Fig. 3.은 한국은행의 CBDC 개발 타임라인을 나타낸 그림으로 2020년을 기점으로 제도 및 기술적 실현 가능성에 관한 연구를 진행함을 보인다. 2단계로 분리된 CBDC 모의실험 연구사업은 CBDC 테스트베드 구축 및 분산원장 기술을 활용한 오프체인 기술 구현 검토로 구성된다[19].

한국은행은 2023년도 실 도입을 위해 원천기술 개발과 가상자산 거래 처리 성능 향상을 위한 연구를 활발히 진행 중이다[20][21]. 추가로, 2023년 7월 한국은행은 CBDC 테스트베드 실현을 위해 제주, 부산, 인천이 후보로 선정되었다[22].

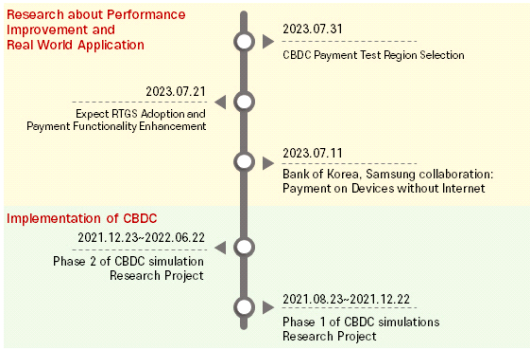

Fig. 3. The timeline for CBDC in Korea.

2.3.3 국외 시장 동향

Fig. 4.는 2023년 8월 기준의 세계 CBDC 도입 현황을 나타낸 그림이다. 현재 전 세계의 약 130개국이 CBDC의 연구 및 개발을 진행하고 있다. G20 국가 중 19개국은 현재 CBDC 개발의 고급 단계에 있으며 그중 9개국은 이미 시범 운영 중이다. 또한, 11개국은 CBDC 출시를 마무리하였으며, 중국의 파일럿은 2억 6천만 명이 참여하고 있다[23].

유럽중앙은행은 2023년도에 20개 이상의 국가에서 CBDC를 시범 운영할 예정이다[24]. 미국 역시 12개의 국가 간 도매 CBDC 프로젝트를 진행하고 있다[24]. 그 외에도 인도와 브라질은 2024년 CBDC의 출시를 계획하고 있는 등, CBDC는 세계적으로 활발히 연구되고 있다[24].

금융권에서의 블록체인 기술은 미래 디지털화폐로의 전환에 중요한 역할을 담당한다. 그러나, 2023년 CBDC 금융기관과의 모의 연계 실험 결과에서 한국은행의 CBDC 운용 시스템은 대용량 데이터 처리에 대한 확장성 문제 및 네트워크 지연 문제가 존재한다[7]. 이러한 문제는 CBDC의 범용성을 제한하며, 금융기관과의 연계에도 제약을 가져올 수 있다. 따라서, 범국가적인 CBDC 운용을 위해 블록체인 확장성 및 네트워크 부하 문제를 해결해야 한다.

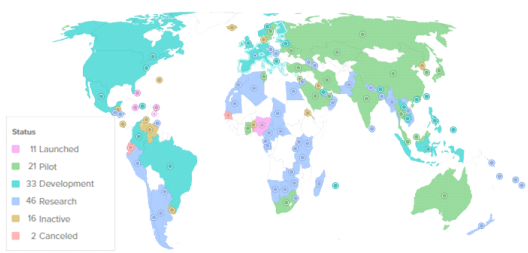

Fig. 4. The adoption status for CBDC in the world.

본 연구는 범용 CBDC 구축을 위한 강화학습 기반의 CBDC 처리량 및 네트워크 부하 문제를 해결하는 기술을 제안한다. 또한, 샤드 블록체인 구조의 CBDC 운용 시스템에서 대용량 데이터 처리에 대한 확장성 증대, 네트워크 부하를 발생하는 CST 감소 및 각 샤드의 부하분산(load balancing)을 목표로 둔다.

III. 블록체인 트랜잭션 데이터 분석

본 장에서는 실제 이더리움 트랜잭션 데이터 분석을 통해 샤드 블록체인의 문제점을 파악한다. 또한, 샤딩 기술의 한계점을 기반으로 향후 CBDC 운용 시스템 구축을 위한 시사점을 제시한다.

3.1 이더리움 실 트랜잭션 데이터 수집

이더리움 실 트랜잭션 데이터 분석을 수행하기 위해 블록 번호 16,000,001부터 16,100,000까지 총 10만 블록을 추출하였으며, 블록 내의 정보는 Table 1.과 같다. 블록은 총 13,697,320개의 트랜잭션과 총 4,827,700개의 EOA(Externally Owned Account) 및 CA(Contract Account) 계정이 존재한다.

샤드 블록체인에 속한 모든 계정은 해시 기반의 고정된 주소 앞자리에 따라 각 샤드에 배치되며, 거래하는 계정 위치에 따라 CST와 IST를 생성할 수 있다. CST는 두 샤드 사이의 많은 동기/비동기 통신이 요구되어 각 샤드에 네트워크 부하를 발생한다. 따라서, 샤드 블록체인에서 성능을 확장하기 위해서는 각 샤드가 처리하는 CST 수보다 IST 수가 더 많아야 한다.

Table 1. Transaction data of Ethereum

Parameter	Amount
Block	100,000
Transaction	13,697,320
Account	4,827,700
Sender Account	3,124,805
Receiver Account	1,961,972

3.2 이더리움 실 트랜잭션 데이터 분석

3.2.1 네트워크 부하량 비교분석

Fig. 5.은 8 샤드 환경에서 샤드별 네트워크 부하량을 나타낸 그림으로 각 샤드가 처리하는 CST와 IST 수를 나타낸다. 분석 결과, 각 샤드가 처리하는 트랜잭션에 대한 유형과 양이 서로 상이하므로 샤드 블록체인에서 부하 불균형(load imbalance) 문제가 발생함을 확인할 수 있다.

Fig. 6.은 8, 16, 32, 64 샤드 환경에서 샤드 개수에 따른 네트워크 부하량을 나타낸 그림으로 CST와 IST 비율을 나타낸다. 분석 결과, 샤드 수가 증가함에 따라 CST 발생량도 선형적으로 증가하므로 CST는 샤드 수에 비례함을 확인할 수 있다.

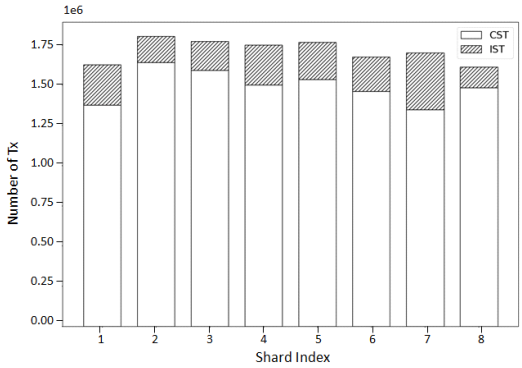

Fig. 5. The network loads for each shard.

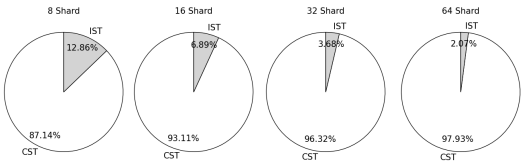

Fig. 6. The network loads for shard numbers.

3.2.2 처리량에 따른 네트워크 부하량 비교분석

Fig. 7.은 8 샤드 환경에서 처리량에 따른 네트워크 부하량을 측정한 그림으로 각 샤드에서 발생하는 CST 비율을 나타낸다. 분석 결과, 처리량은 CST 발생량에 큰 영향을 미치지 않음을 확인할 수 있다.

본 연구는 이더리움 트랜잭션 분석 결과를 통해

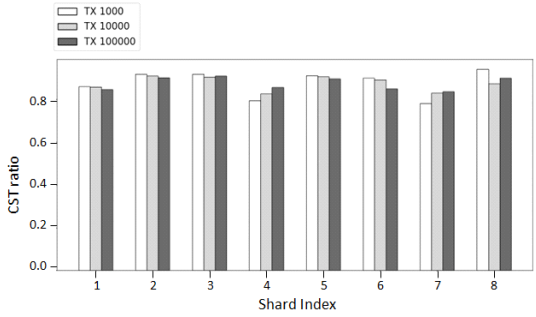

Fig. 7. The network loads for throughput.

샤드 블록체인의 높은 CST 발생량과 부하 불균형 문제를 확인하였다. 네트워크 부하를 발생하는 CST는 샤드별 동기/비동기 통신이 요구되어 거래 처리량 저하, 높은 수수료 및 대기시간 증가 등의 문제로 블록체인 확장성을 저해한다. 따라서, 샤드 환경에서 처리량을 향상하기 위해서는 CST 감소 및 부하분산이 요구된다.

IV. 강화학습 기반 계정 재배치 기법

본 장에서는 딥러닝 기술을 활용한 심층 강화학습 기반의 계정 재배치 기법을 제안한다.

4.1 개요

본 연구의 목표는 샤드 블록체인 환경에서 심층 강화학습을 통한 대용량 데이터 처리에 대한 확장성 증대, 네트워크 부하 감소 및 각 샤드의 부하분산이 가능한 자동화된 시스템 구축을 목표로 둔다.

Fig. 8.는 제안 기법의 전체 프로세스를 시각화한 그림으로 심층 강화학습 모델 속 에이전트는 각 샤드에 속한 계정 정보 및 블록 정보를 통해 최대 보상받는 최적의 재배치 샤드를 결정한다. 에이전트는 세 가지 행동인 CST 감소를 위한 재배치 샤드 결정, 부하분산을 위한 재배치 샤드 결정, 그리고 무작위로 선택된 재배치 샤드 결정으로 행동을 수행할 수 있다.

Table 2.는 모델 학습을 위해 사용되는 표기법을 정의한다. 블록이 생성되는 주기 시간인 에폭이 t일 때, 각 샤드 S_i에 속한 계정 ACC_{id}는 트랜잭션 내역인 $info_{id}(t) = [a_{i,1}, a_{i,2}, \ldots, a_{i,SHARD}]$와 ACC_{id}의 활동 시간인 τ를 가진다. 트랜잭션 내역은 각 샤드에 위치한 계정 간의 트랜잭션 수를 저장한다. 활동 시간 τ는 계정의 최초 트랜잭션 생성 시점부터

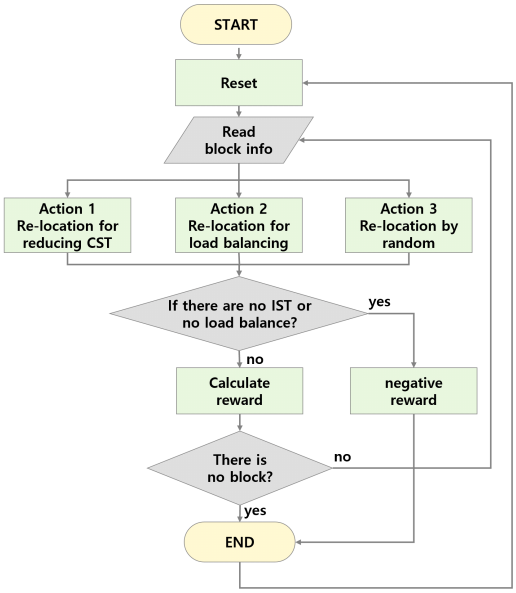

Fig. 8. Our system process.

Table 2. Notations.

Parameters	Description
t	epoch
S_i $(i \in SHARD)$	state of ith shard
ACC_{id}	account's id
$info_{id}(t)$	transaction counting vector for the ACC_{id}
τ	activity time of ACC_{id}
x	weight for CST
$IST_{S_i}(t)$	total number of IST
$CST_{S_i}(t)$	total number of CST

현재까지의 기간을 저장한다. 본 연구는 CST의 네트워크 부하량에 따른 각 샤드의 부하분산 수치를 측정하기 위해 CST에 대한 가중치 변수 x를 설정한다. 샤드의 부하분산 수치는 각 샤드에서 발생하는 총 CST와 IST의 트랜잭션 가중치에 따라 측정된다.

4.2 심층 강화학습 구조

Fig. 9.는 심층 강화학습 모델 구조를 시각화한 그림으로 학습 환경(environment) 및 샤드 상태(state), 최적의 재배치 샤드를 결정하는 행동(action), 그리고 학습 보상(reward)의 순서를 나타낸다.

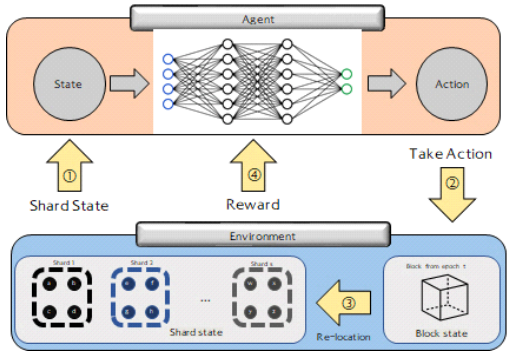

Fig. 9. Our deep reinforcement learning model.

4.2.1 학습 환경 및 샤드 상태

에이전트는 딥러닝 모델을 이용하여 샤드에 속한 계정들의 정보인 샤드 상태 $state(t)$를 기반으로 최대 보상을 얻기 위해 최적의 재배치 샤드 결정을 학습한다.

$SHARD \times SHARD$ 매트릭스로 구성된 샤드 상태 $state(t)$는 에폭 t일 때 각 샤드 사이에 발생한 전체 트랜잭션 수를 저장한다. 이는 각 샤드의 CST와 IST 발생량을 측정할 수 있다.

4.2.2 재배치 샤드 결정

에이전트는 최적의 재배치 샤드를 결정하기 위해 3가지 행동 중 최대의 보상을 받는 재배치 샤드를 결정한다. 본 연구는 송신 계정만 재배치를 수행하도록 제약을 둔다.

① CST 감소를 위한 재배치 샤드

송신 계정의 활동 시간 τ로부터 많은 양의 트랜잭션을 거래한 샤드로 계정을 재배치하기 위해 지수이동평균(Exponential Moving Averages, EMA) 알고리즘을 사용한다[25]. 에폭 t일 때 트랜잭션을 생성한 각 송신 계정은 아래 식 $acc_score_{id}(\tau)$와 같이 $info_{id}(t)$과 평활 요인(smoothing factor) δ에 따라 과거와 현재 에폭 때 발생한 트랜잭션에 가중치를 부여할 수 있다. $acc\_score_{id}(\tau)$ 식의 점수는 해당 계정이 활동한 전체 시간 동안 자주 상호작용한 수신 계정이 속한 샤드를 의미한다. 에이전트는 네트워크의 전체 CST 감소를 위해 높은 점수를 가지는

재배치 샤드를 선택한다.

$$acc\_score_{id}(\tau) = info_{id}(t) \times \delta + acc\_score_{id}(\tau-1) \times (1-\delta) \quad (3)$$

② 부하분산을 위한 재배치 샤드

각 샤드에서 발생하는 CST 발생량에 따라 샤드가 처리하는 트랜잭션 부하를 분산시키기 위해 라운드 로빈 알고리즘을 사용한다[26]. 에폭 t에서 트랜잭션을 생성한 각 샤드는 아래 식 $shard_score_i(t)$와 같이 이전 에폭 때의 점수와 에폭 t에서 발생한 CST와 IST의 부하를 차등을 주어 계산한다. 서로 다른 샤드 간에 많은 통신을 요구하는 CST는 가중치 x를 부과하여 계산한다. 에이전트는 각 샤드의 $shard\_score_i(t)$ 비율에 따라 송신 계정의 재배치 샤드를 결정한다.

$$shard\_score_i(t) = shard\_score_i(t-1) + IST_{S_i}(t) + x\,CST_{S_i}(t) \quad (4)$$

③ 무작위 선택된 재배치 샤드

송신 계정을 무작위로 선택된 재배치 샤드로 할당한다.

4.2.3 학습 보상

에이전트는 CST 발생량 감소 및 부하분산 정도에 따라 0~1 사이의 학습 보상받는다. 심층 강화학습 중 발생 가능한 예외를 처리하기 위해 모든 샤드에서 IST가 발생하지 않을 경우와 특정한 한 샤드에 트랜잭션 부하가 발생할 경우, 보상을 1 감소한다. 에이전트는 최대의 보상을 얻기 위해 CST 발생량 감소 및 부하분산을 위한 최적의 행동을 선택한다.

CST 발생량 감소에 대한 보상 $tx_reward(t)$는 식 (5)와 같으며, 에폭 t일 때 각 샤드에서 발생한 전체 트랜잭션에 대한 IST의 비율로 보상을 측정한다.

$$tx\_reward(t) = \frac{\sum_{i=1}^{SHARD} \frac{IST_{S_i}(t)}{IST_{S_i}(t) + CST_{S_i}(t)}}{SHARD} \quad (5)$$

부하분산에 대한 보상 $lb_reward(t)$은 아래 식과 같으며, 에폭 t일 때 각 샤드의 트랜잭션 발생량에 대한 분포와 균등 분포 간의 유사도를 Kullback-Leibler 발산을 이용해 비교한다 [27]. $P_{S_i}(t)$는 에폭 t일 때 전체 트랜잭션 발생량에 대한 i번 샤드의 트랜잭션 발생량의 비율이다.

$$P_{S_i}(t) = \frac{IST_{S_i}(t) + x \cdot CST_{S_i}(t)}{\sum_{k=1}^{s}(IST_{S_k}(t) + x \cdot CST_{S_k}(t))} \quad (6)$$

$Q_i(t)$는 이상적인 분포인 균등 분포를 의미하며, $D_{KL}(P(t)\|Q(t))$는 $P_i(t)$와 $Q_i(t)$에 대한 Kullback-Leibler 발산을 의미한다.

$$D_{KL}(P(t)\|Q(t)) = \sum_{i=1}^{SHARD} P_{S_i}(t)\log_2\left(\frac{P_{S_i}(t)}{Q_{S_i}(t)}\right) \quad (7)$$

부하분산에 대한 보상 식은 식 (8)과 같다.

$$lb\_reward(t) = 1 - \frac{D_{KL}(P(t)\|Q(t))}{\log_2(s)} \quad (8)$$

따라서, 에이전트가 받는 CST 발생량 감소 및 부하분산에 대한 전체 학습 보상은 식 (9)와 같다.

$$reward(t) = \frac{tx\_reward(t) + lb\_reward(t)}{2} \quad (9)$$

4.3 계정 재배치 기법

제안하는 DDQN 알고리즘 기반의 계정 재배치 기법은 Fig. 10.과 같다. 에이전트는 입력된 상태를 통해 최대의 보상을 얻기 위해 최적의 행동을 결정하기 위해 탐험(exploration)을 수행한다.

본 연구의 심층 강화학습은 메인 네트워크와 타겟 네트워크 간의 경사 하강법을 사용한다. 또한, 각 상태, 행동, 보상은 미니 배치(mini-batch) 구조로 입출력되며, 매 주기마다 메인과 타겟 네트워크 간의 학습 파라미터를 공유하여 학습한다.

Algorithm 1. DDQN for Account Relocation

Input

Initial Q function $Q(s,a;\theta), Q(s,a;\theta')$
where s is state, a is action, θ is a parameter for main network,
θ' is a parameter for target network.
Learning rate α, discounting factor γ, epsilon for exploration ϵ, decaying factor δ
Replay memory D for batch sampling
Total train step (epoch) T, total episode M, network update period P
Train dataset $block_0 \sim block_T$

Procedure

For episode 1 to M **do**:
  Reset $s = s_0$ with initial block $block_0$ using Modularity sharding
  For train step $t = 1$ to T **do**:
    If random value $< \epsilon$ **then**:
      do exlporation to action a_t
    Otherwise then:
      do action $a_t = argmax(Q(s_t, a_t; \theta))$
    End If

    execute action a_t to do relocation accounts that create sending transactions in $block_t$, and observe reward r_t, next state s_{t+1}

    store (s_t, s_{t+1}, r_t, a_t) to D

    train with $mini-batch$ samples $\{(s_i, s_{i+1}, r_i, a_i) | i \text{ is randomly selected}\}$

    $$y_i = \begin{cases} r_i & , \text{ if terminated} \\ r_i + \gamma Q(s_{i+1} \cdot argmax(Q(s_{i+1}, a_{i+1}; \theta)); \theta'), & else \end{cases}$$

    perform a gradient descent step on $(y_i - Q(s_t, a_t; \theta))^2$

    If training count % $P = 0$ **then**:
      update network parameter to $\theta' = \theta$
    End If
    ϵ is decayed with δ
  End For
End For

Fig. 10. DDQN for Account Relocation Algorithm.

V. 성능평가

본 장에서는 심층 강화학습의 파라미터를 설정 과정과 제안된 기법, 그리고 계정 재배치를 수행하지 않는 'No-relocation' 방식과 랜덤하게 계정을 재배치하는 'Random-relocation' 방식의 처리량, 네트워크 부하 발생량 및 부하분산 등의 성능을 평가한다. 실험은 Ⅲ장에서 추출한 10만 블록의 이더리움 실 트랜잭션 데이터를 사용하며, 실험 파라미터는 Table 3.과 같다.

Table 3. Performance parameters.

Parameters	Value
gradient descent algorithm	Adam
loss function	MSE
smoothing factor	0.5
initial epsilon	1.0
decaying factor	0.98
mini-batch sampling size	128
network update period	10
the number of shards	8, 16, 32, 64
weight for CST	2, 4, 6, 8

5.1 심층 강화학습 파라미터 설정

심층 강화학습 모델의 학습률(learning rate)과 감가율(discount factor) 설정하기 위해 300블록의 데이터를 활용하여 300번의 에피소드(episode)를 진행하였다. Fig. 11.과 Fig. 12.는 제안 모델에서 0.1, 0.01, 0.001의 학습률과 0.9, 0.99, 0.999일 때의 누적 보상을 나타낸다. 수렴된 누적 보상은 에이전트가 매번 최적의 행동을 선택함을 나타낸다. 따라서, 본 연구는 0.01의 학습률과 0.99인 감가율을 사용하여 심층 강화학습 모델을 생성한다.

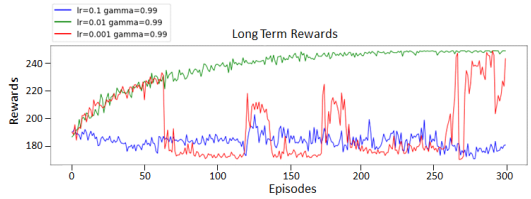

Fig. 11. Appropriate learning rate selection

Fig. 12. Appropriate discounting factor selection

5.2 샤드 수에 따른 거래 처리량 성능 결과

Fig. 13.은 샤드 수에 따른 네트워크 전체 처리량을 나타낸 그림이다. 샤드 블록체인은 기존 블록체인

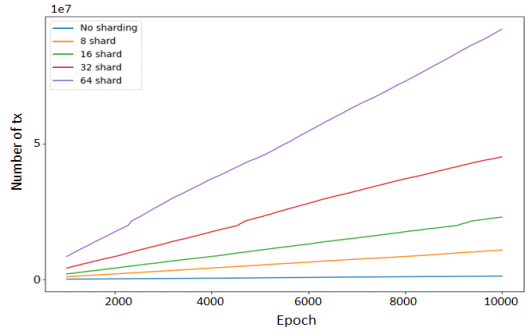

Fig. 13. Throughput by shard numbers.

처리량 대비 샤드 수에 따라 트랜잭션을 처리량이 선형적으로 증가한다.

5.3 샤드 수에 따른 네트워크 부하 발생량 성능 결과

Fig. 14.는 샤드 수에 따른 CST 발생량을 나타낸 그림이다. CST 발생량은 샤드 수와 영향을 받으며, 제안 기법은 기존 기법 대비 20% ~ 30%의 CST를 감소할 수 있다.

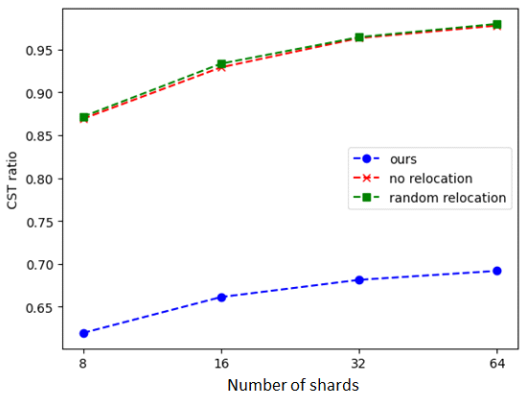

Fig. 14. CST ratio for the number of shards

5.4 트랜잭션 가중치에 따른 네트워크 부하 발생량 성능 결과

Fig. 15.는 8 샤드 환경에서 CST의 가중치 변화량에 따른 CST 발생량을 나타낸 그림이다. CST 발생량은 네트워크 부하 가중치에 영향을 받지 않는다.

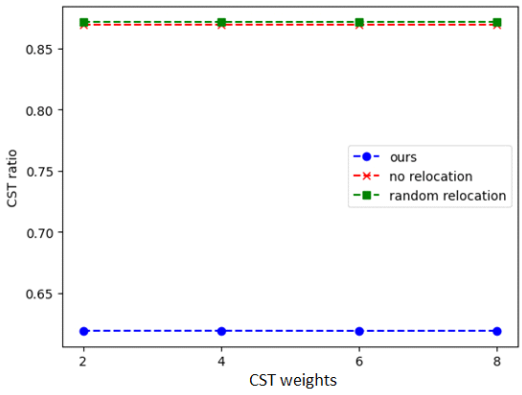

Fig. 15. CST ratio for weights of CST

5.5 샤드 수에 따른 부하 분산 성능 결과

Fig. 16.는 샤드 수에 따른 각 샤드의 부하분산 정도를 나타낸 그림이다. 제안 기법은 기존 기법에 비해 적은 네트워크 부하를 발생하는 반면, 특정 샤드에 트랜잭션 과밀집으로 인해 상대적으로 많은 부하를 보인다.

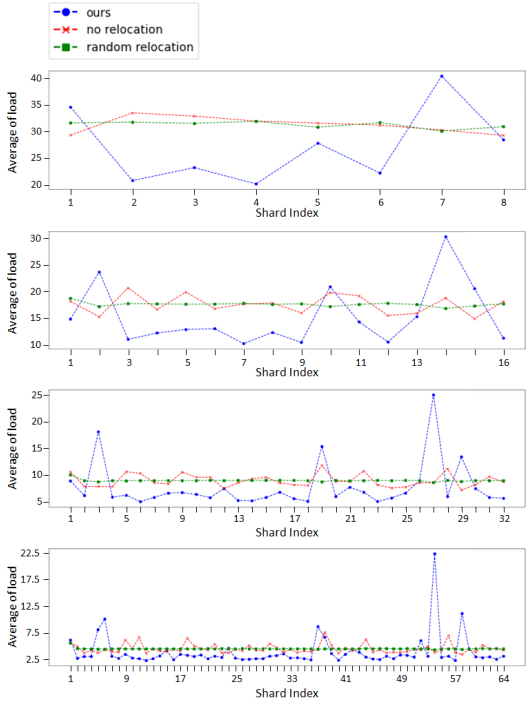

Fig. 16. Load balancing per shards

VI. 결 론

본 연구에서는 범용 CBDC 구축을 위한 강화학습 기반의 CBDC 환경에서 대용량 데이터에 대한 낮은 처리량 및 네트워크 부하 문제 해결 기술을 제안하였다. 샤드 블록체인 환경에서 방대한 네트워크 부하를 발생하는 특정 계정을 다른 샤드로 재배치시킴으로써 전체적인 블록체인 성능을 증진할 수 있었다. 강화학습 기반의 제안 기술은 기존 시스템 대비 최대 64배 이상의 처리량 증대 및 20% 이상의 네트워크 부하를 감소함으로써 기존 대비 높은 성능을 가진다.

References

[1] Young-ki Kang, Young-mi Ko, "Review of the Need for Central Bank Digital Currency(CBDC) and the Issues Involved in Introducing CBDC - Focusing on the Discussion on the Introduction of CBDC in Japan," Law Review, 26(1), pp. 67-99, Mar. 2023.

[2] Jin-soul Choi and Sun-jong Park, "The Current State of Research in CBDC and Legal Challenges of CBDC in South Korea," The Korean Association of Comparative Private Law, 29(2), pp. 199-225, May. 2022.

[3] Ja-young Seo, "Central Bank Digital Currency and Personal Data Protection," The Justice, 289, pp. 285-326, Apr. 2022.

[4] Jung-su Han, Jeong-Heon Kim, Jong-soo Woo and Won-ki Hong, "CBDC System Design using Blockchain," KNOM Review, 24(2), pp. 358-359, Feb. 2021.

[5] C. Boar and A. Wehrli, "Ready, steady, go? -Results of the third BIS survey on central bank digital currency", BIS Papers, no. 114, pp. 6, Jan. 2021.

[6] Bank of Korea, "2022 payment system conference held", Available: https://www.bok.or.kr/portal/bbs/P0000559/view.do?nttId=10073671&menuNo=200690&pageIndex=1, 2023.11.17.

[7] Bank of Korea. "Results of 「CBDC Simulation System Financial Institution Linkage Experiment」", Available: https://www.bok.or.kr/portal/bbs/P0000559/view.do?nttId=10077218&menuNo=200690, 2023.11.17.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, Bitcoin, Decentralized business review" Available: https://bitcoin.org/bitcoin. pdf, 2023.11.17.

[9] G. Yu, X. Zha, X. Wang, et. al. , "Enabling attribute revocation for fine-grained access control in blockchain-IoT systems," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1213-1230, Nov. 2020.

[10] P. K. Sharma and Jong-Hyuk Park, "Blockchain based hybrid network architecture for the smart city, Future Generation Computer Systems," The International Journal of eScience, vol 86, pp. 650-655, May. 2018.

[11] A. Azaria, A. Ekblaw, T. Vieira, et. al., "Medrec: Using blockchain for medical data access and permission management," 2016 2nd international conference on open and big data (OBD), pp. 25-30, Nov. 2016.

[12] Tsai, W. T., Zhao, Z., Zhang, C., Yu, L., & Deng, E. . "A multi-chain model for CBDC," In 2018 5th International Conference on Dependable Systems and Their Applications (DSA) . IEEE, pp. 25-34, Sep. 2018.

[13] Ethereum, "what is Ethereum?", Available: https://ethereum.org/ko/what-is-ethereum/, 2023.11.17

[14] V. Mnih, K. Kavukcuoglu, D. Silver, et.al., "Playing Atari with Deep Reinforcement Learning," arXiv preprint, arXiv:1312.5602, Dec. 2013.

[15] H. Hasselt, "Double Q-learning," Advances in Neural Information Processing Systems 23 (NIPS 2010), vol. 23, Dec. 2010.

[16] H. Hasselt, A. Guez and D. Silver, "Deep Reinforcement Learning with Double Q-learning," arXiv preprint, arXiv:1509.06461, Feb. 2016.

[17] Tether, "Tether: Flat currencies on the Bitcoin blockchain", Available: https://assets.ctfassets.net/v yse88cgwfbl/5U

WgHMvz071t2Cq5yTw5vi/c9798ea8db99311bf90ebe0810938b01/TetherWhitePaper.pdf, 2023.11.17.

〔18〕 I. Makarov and A. Schoar, "Cryptocurrencies and Decentralized Finance", BIS Papers, no. 1061, pp. 22, Dec. 2022.

〔19〕 Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges," arXiv preprint arXiv:2105.07447, Oct. 2021.

〔20〕 Lovejoy, J., Fields, C., Virza, M., Frederick, T., Urness, D., Karwaski, K., ... & Narula, N. "A high performance payment processing system designed for central bank digital currencies," Cryptology ePrint Archive. Feb. 2022.

〔21〕 Bank of Korea, "Bank of Korea, CBDC simulation experiment research project phase 1 performance and management plan", Available: https://www.bok.or.kr/portal/bbs/P0000559/view.do?nttId=10068650&menuNo=200690, 2023.11.17.

〔22〕 Bank of Korea, "Bank of Korea, CBDC simulation experiment research project phase 2 performance and management plan", Available: https://www.bok.or.kr/portal/ bbs/P0000559/view.do? nttId=10073660&menuNo=200690&pageIndex=1, 2023.11.17.

〔23〕 Zdnet korea, "Bank of Korea "Introduction of RTGS, expected to improve payment backend"", Available: https://zdnet.co.kr/view/?no=20230721112222, 2023.11.17.

〔24〕 Chosun Ilbo Co., "〔CBDC Experiment〕 ② Payment between devices without internet 'Haneun Pay-Samsung Collaboration'", Available: https://it. chosun.com/site/data/html_dir/2023/07/10/202307100 1948.html, 2023.11.17.

〔25〕 Chosun Ilbo Co., "〔Exclusive〕 Bank of Korea selects CBDC payment pilot area… 'Jeju, Busan, Incheon' 3-way match", Available: https://it.chosun.com/site/data/html_dir/2023/07/31/202307310113 5.html, 2023.11.17.

〔26〕 Tong-wook Park, "Prospects and implications of the internationalization of digital yuan", Korea Information Society Development Institute, ISSN 2233-6583, Jun. 2022.

〔27〕 Atlantic countcil, "Future of Money", Available: https://www.atlanticcouncil.org/programs/geoeconomics-center/future-of-money/ 2023.11.17.

〔28〕 J. S. Hunter, "The Exponentially Weighted Moving Average," Journal of Quality Technology, vol. 18, no. 4, pp. 203-210, Feb. 2018.

〔29〕 J. Fürnkranz, "Round robin classification," The Journal of Machine Learning Research 2, pp. 721-747, Mar. 2002.

〔30〕 J. M. Joyce, "International Encyclopedia of Statistical Science", Springer, Berlin, Heidelberg, pp. 720-722, 2011.

〈저자소개〉

이 연 주 (Yeon Joo Lee) 학생회원
2021년 2월: 백석대학교 ICT학부 정보보호학전공 졸업
2023년 2월: 고려대학교 정보보호학과 석사
2023년 3월~현재: 고려대학교 정보보호학과 박사과정
〈관심분야〉 블록체인, 프라이버시 향상 기술, 디지털포렌식

장 호 빈 (Hobin Jang) 학생회원
2022년 2월: 서울시립대학교 수학과 졸업
2022년 3월~현재: 고려대학교 융합보안학과 석사과정
〈관심분야〉 정보보호, 데이터 보안, 프라이버시 향상 기술, 블록체인

조 수 정 (Sujung Jo) 학생회원
2023년 2월: 국민대학교 정보보안암호수학과 졸업
2023년 3월~현재: 고려대학교 융합보안학과 석사과정
〈관심분야〉 프라이버시 향상 기술, 블록체인

장 규 현 (GyeHyun Jang) 정회원
2009년 8월: 고려대학교 산업시스템정보공학과 졸업
2019년 2월: 고려대학교 정보보호학과 박사
2019년 3월~현재: 고려대학교 정보보호대학원 연구교수
〈관심분야〉 사이버안보, 디지털자산, 블록체인

노 건 태 (Geontae Noh) 종신회원
2008년 2월: 고려대학교 산업시스템정보공학과 졸업
2010년 2월: 고려대학교 정보경영공학과 석사
2014년 8월: 고려대학교 정보보호학과 박사
2014년 9월~2017년 2월: 고려대학교 정보보호연구원 박사후 연구원, 연구교수
2017년 2월~현재: 서울사이버대학교 빅데이터·정보보호학과 조교수
2020년 3월~현재: 서울사이버대학교 빅데이터·AI센터 센터장
〈관심분야〉 암호 이론, 데이터 보안, 프라이버시 향상 기술

정 익 래 (Ik Rae Jeong) 종신회원
1998년 2월: 고려대학교 전산학과 졸업
2000년 2월: 고려대학교 전산학과 석사
2004년 8월: 고려대학교 정보보호학과 박사
2006년 3월~2008년 2월: 한국전자통신연구원 암호기술연구팀 선임연구원
2008년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호 이론, 프라이버시 향상 기술 (PET), 데이터베이스 보안, 생체인증